iSHARE scheme (v1.6)

iSHARE

Exported on 05/11/2018

Table of Contents

iSHARE

This document provides a full overview of the iSHARE scheme, starting with the introduction (see page 9).

1 Introduction

iSHARE is a collaborative effort to improve conditions for data-sharing for organisations involved in the Dutch logistics sector. The functional scope of the iSHARE scheme focuses on topics of authentication, authorisation and identification. As of 2018, the iSHARE scheme is publicly available to the market.

The purpose of this document is to provide a complete overview of the current state of the iSHARE scheme.

1.1 Reader's guide

- iSHARE's introductory section describes the scheme's starting points: its goals, the guiding principles and the iSHARE governance framework;
- The 'releases' (see page 16) section describes the release notes, planning of future releases and version history of the iSHARE scheme;
- The 'main scheme aspects (see page 20)' section summarises the most important functionality of the iSHARE scheme, its framework and roles, and the technical, operational and legal provisions enabling it;
- The 'use cases (see page 31)' section showcases the scheme's key functionalities in four use cases;
- The 'detailed descriptions (see page 51)' section explains the in-depth Functional, Technical, Legal and Operational agreements that, together, improve data-sharing conditions for the logistics sector;
- The scheme concludes with the 'glossary and legal notices (see page 213)' section;
- The project history provides some background information (see page 226) about the project and assumptions on the basis of which the scheme was co-created.

Within the iSHARE scheme documentation, the following notational conventions apply:

- The keywords 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in this document are to be interpreted as described in IETF RFC 2119[1] whenever this note is at the top of the chapter:
  - *This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.*

1.2 Goals and scope of the iSHARE scheme

The iSHARE scheme is a collaborative effort to improve the exchange of data between organisations involved with the Dutch logistics sector. The iSHARE scheme results in a set of agreements which improve circumstances for data exchange.

The ambition of iSHARE is to lower barriers for sharing data, to empower new forms of collaboration in chains and to help scale up existing initiatives that aim to improve conditions for data exchange. The underlying assumption is that if data can flow in a controlled and smart way, it will lead to a more efficient use of infrastructure, less carbon emissions and a more competitive logistics sector.

The iSHARE scheme's scope focuses on three main topics that are crucial in any data exchange context:

1. Identification[2];

1 http://www.ietf.org/rfc/rfc2119.txt
2 https://innopay.atlassian.net/wiki/spaces/IS/pages/53407800/Identification

2. Authentication[3];
3. Authorisation[4].

iSHARE focuses on these three aspects as they are considered indispensable in any communication between parties, also in the context of exchanging logistical data. Within the iSHARE scheme, agreements are made on the above three topics with the aim of to work towards a more uniform, straightforward and controlled way of exchanging data on a bigger scale than is possible right now*.

- Uniform: one uniform way of working across all types of modalities, small and large organisations, public and private organisations, suppliers and receivers of data or their softwarepartners, etc. iSHARE aims to create new possibilities for efficiency improvements, time gains and cost savings.
- Straightforward: Easy to connect with new, existing and third-party business partners throughout the sector, more certainty on trustworthiness of parties you exchange data with, a building block which is easy to implement by your software partners or your IT department and an addition that empowers your existing solutions.
- Controlled: The basic principle within iSHARE is that the owner of the data stays in control at all times; the owner decides with whom what data is exchanged on what terms.

These three aims can only be reached when a variety of perspectives are considered during the establishment of the scheme. To this end, a variety of organisations are involved in defining the agreements for iSHARE. During the co-creation phase of the iSHARE project, the involved organisations invest in the iSHARE scheme in terms of expertise.

*Notes:

- The scope of the iSHARE scheme does not include the specification of possible business models for sharing data and/or payments related to data exchange;
- The iSHARE scheme can in some way be compared with the institute of the passport: the iSHARE scheme will be usable by anyone who owns a digital identity compatible with the iSHARE scheme. This will greatly simplify authentication and authorisation processes, also between different organisations (however: even though organisations can have valid certificates, it does not rule out possible malign intentions).

1.3 Guiding principles

To achieve the goals of the iSHARE scheme, it is paramount to stay close to a set of guiding principles. As time progresses new principles can be defined, existing principles can be adapted or dropped if deemed necessary. The guiding principles were defined using the format as suggested* by TOGAF 8.1.1 architectural principles[5].

The following principles define the iSHARE scheme and must be kept in mind at all times during further development (see details of guiding principles below):

Principle #	Principle name
1	Generic building block to enable data exchange
2	Limited scope: identification, authentication, and authorisation

3 https://innopay.atlassian.net/wiki/spaces/IS/pages/53407664/Authentication
4 https://innopay.atlassian.net/wiki/spaces/IS/pages/53407889/Authorisation
5 http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap29.html

Principle #	Principle name
3	Leverage existing (international) building blocks
4	Agnostic towards nature and content of data
5	Benefits outweigh investment for all types of participants
6	International orientation

Guiding principles details:

Principle 1	Generic building block to enable data exchange
Statement	iSHARE is a generic identification, authentication and authorisation scheme to be used as enabler for data exchange in logistics
Rationale	In every exchange of data, identification, authentication and authorisation are fundamental factors. iSHARE aims to simplify processes of identification, authentication and authorisation as a generic solution to facilitate data exchange in the logistics sector.
Implications	• The iSHARE scheme will allow for extension or adaptability so it can be used in situation/sector specific cases; • The iSHARE scheme will not cater to a specific sector or market, it is applicable in an N amount of cases; • The iSHARE scheme will not be a point solution.

Principle 2	Limited scope: identification, authentication, and authorisation
Statement	The iSHARE scheme's scope is limited to topics of identification, authentication and authorisation in the context of data exchange
Rationale	iSHARE aims to improve the circumstances for data exchange throughout the logistics sector and provides focus on the topic of identification, authentication and authorisation. Identification, authentication and authorisation are a fundamental part of any data exchange, but are not solved in a scalable or standardised way at the moment.
Implications	• Without this principle, there is a risk of 'scope creep': related topics could take away the focus off the intended topics

Principle 3	Leverage existing (international) building blocks
Statement	Where possible, iSHARE should be realised using existing and proven standards, technology or initiatives
Rationale	By reusing building blocks already available and in use, the impact on organisations to participate in iSHARE and the time to realise the iSHARE scheme are lowered. Standards, technology and initiatives preferably have a broad (international) usage base and are backed by a professional organisation charged with maintenance of the standards, technology or initiatives.
Implications	• the iSHARE scheme will build on or use existing (international) standards, technology or initiatives where possible; • the iSHARE scheme will aim to use open standards, technology or initiatives; • the iSHARE scheme may use proprietary standards, technology or initiatives; • if existing and/or proven standards, technology or initiatives do not provide what is needed, alternative solutions will be sought.

Principle 4	Agnostic towards nature and content of data
Statement	The iSHARE scheme does not concern itself with the contents or nature of data
Rationale	Given the generic nature of the iSHARE scheme and the aim to be applicable throughout the logistics sector, iSHARE needs to function with any type of possible data and/or any relevant data exchange interaction model. To this end, the contents of data are only considered where it concerns the facilities needed within iSHARE to adequately exchange various types of data (e.g. requirements to security, encryption, etc.). It is up to the participating organisations to ensure that iSHARE adequately fulfills requirements to the process of identification, authentication and authorisation in the context of data exchange.
Implications	• the iSHARE scheme will not specify the (allowed) content of data exchanges done within an iSHARE context; • the iSHARE scheme does not specify content specific data standards; • the iSHARE scheme should not have limitations connected to types of data or standards used.

Principle 5	Benefits outweigh investment for all types of participants
Statement	The iSHARE scheme needs to be attractive to use and implement for all types of participants/roles.

Principle 5	Benefits outweigh investment for all types of participants
Rationale	The iSHARE scheme knows different roles with different responsibilities. When a potential participant considers taking a (or multiple) role(s) in the iSHARE scheme, the iSHARE scheme should aim to have the lowest possible threshold to participate for the potential participant. Depending on what the character of the potential participant is (e.g smaller size or larger size organisations) and which role the participant wants to take, this could mean that the impact of implementation needs to be small or that the implementation is kept relatively simple.
Implications	• the ISHARE scheme aims to keep thresholds to participate in the iSHARE scheme (e.g. in terms of implementation impact or onboarding/certification effort) as low as possible for all possible roles; • the iSHARE scheme strives for the lowest possible impact for participants when changes occur in the future. Changes to used standards will take place; within the iSHARE scheme and its specifications thought needs to be given to how change is dealt with in an efficient way.

Principle 6	International orientation
Statement	The iSHARE scheme needs to look over geographic boundaries to foster international involvement and cooperation
Rationale	The logistics sector is per definition an international sector. The iSHARE scheme needs to facilitate, to the extent that it is practical and possible, international involvement.
Implications	• the iSHARE scheme needs its participants to provide knowledge and experience on how the iSHARE scheme can stay (and become) attractive in the international context

*Format used for defining guiding principles, based on TOGAF standard:

Principle name	Should both represent the essence of the rule as well as be easy to remember. Specific technology platforms should not be mentioned in the name or statement of a principle. Avoid ambiguous words in the Name and in the Statement such as: 'support', 'open', 'consider', and for lack of good measure the word 'avoid', itself, be careful with 'manage(ment)', and look for unnecessary adjectives and adverbs (fluff).
Statement	Should succinctly and unambiguously communicate the fundamental rule. For the most part, the principles statements for managing information are similar from one organisation to the next. It is vital that the principles statement be unambiguous.
Rationale	Should highlight the business benefits of adhering to the principle, using business terminology. Point to the similarity of information and technology principles to the principles governing business operations. Also describe the relationship to other principles, and the intentions regarding a balanced interpretation. Describe situations where one principle would be given precedence or carry more weight than another for making a decision.

Implications	Should highlight the requirements, both for the business and IT, for carrying out the principle - in terms of resources, costs, and activities/tasks. It will often be apparent that current systems, standards, or practices would be incongruent with the principle upon adoption. The impact to the business and consequences of adopting a principle should be clearly stated. The reader should readily discern the answer to: 'How does this affect me?' It is important not to oversimplify, trivialise, or judge the merit of the impact. Some of the implications will be identified as potential impacts only, and may be speculative rather than fully analysed.

1.4 Governance framework

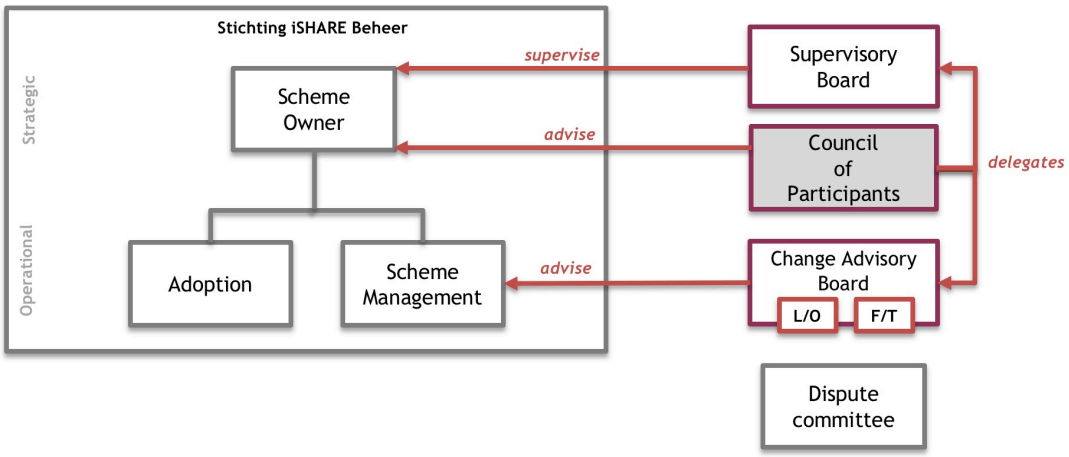
This page describes the governance framework for iSHARE. Please take into account that currently, the precise working of every organ has not been determined yet, nor has the desired dynamic between the various organs been established.

For the iSHARE scheme- and network to operate and grow in a sustainable way, it needs to be organised accordingly. There needs to be an effective executive branch of the organisation that can manage all day to day activities for the scheme (e.g. maintenance of tools, growth of the network and management of changes to the specifications), while at the same time there need to be appropriate checks and balances that allow participants of iSHARE to provide input, supervise ongoing activities and collaboratively influence the decision making within the scheme.

Three main governance principles to abide by were determined by the Operational working group:

1. Independence;
2. Transparency;
3. Collaboration.

The governance consists of a Scheme Owner, a Supervisory Board and two advisory councils (consisting of (a representation of) iSHARE participants), and a dispute committee. The following image depicts this governance. The organs depicted are defined below.



1.4.1 Scheme Owner

The Scheme Owner is the core of all activities related to iSHARE and bares all responsibility related to it. The iSHARE Scheme Owner knows the following constituting parts:

- **The Board** consists of members of the iSHARE community (adhering- and certified parties). Members of the Board are selected and chosen by the Supervisory Board. The Board is the highest organ of the Scheme Owner;
- If the Board so chooses, it can organise an executive branch that manages day to day activities of iSHARE. Day to day activities include (amongst others) the following responsibilities:
    - Management of the iSHARE network (participants);
    - Management of the iSHARE scheme (specifications + brand management).

1.4.2 Supervisory Board

The **Supervisory Board** consists of members from the community and is assigned by the Council of Participants. The Supervisory Board supervises the correct functioning of the Board and elects/dismisses the members of the Board.

1.4.3 Council of Participants

The **Council of Participants** advises the Board and assigns members of the Supervisory Board. Consists of adhering- and certified parties (or representations of these parties) willing to participate in the Council of Participants' activities.

1.4.4 Change Advisory Board

The **Change Advisory Board** advises the Scheme Owner concerning changes to the specifications of the iSHARE scheme. The Change Advisory Board knows two committees: Legal/Operational (L/O) and Functional/Technical (F/T).

1.4.5 Dispute committee

The **Dispute committee** can be asked to resolve disputes between parties participating in the iSHARE network or disputes between a participating party and the iSHARE Scheme Owner. The dispute committee consists of independent and neutral members.

2 Releases

This section describes the release notes, planning of future releases and version history of the iSHARE scheme.

2.1 Versioning guidelines

In terms of versioning, for any changes considered major, an increase of version of the first or second degree will be used (e.g. v1.5 to v2.0 for first degree version increases; v1.5 to v1.6 for second degree version increases).

Minor adjustments in the scheme will lead to an increase of the scheme's version number of the third degree (e.g. v1.6.1 to v1.6.2).

2.2 Release notes

The release notes show the release history and the main differences between releases.

Release 1.6 (current)	
Purpose	Lowering barriers for parties to start using iSHARE
Release date	11 May 2018
Change log	**Functional:** - **Technical:** • For authentication purposes the use of digital certificates within iSHARE will be limited initially to certificates issued under PKIOverheid. **Operational** • The admission process for Certified Parties and Adhering Parties are merged to one generic process. Role-specific requirements may apply. • The order of admission steps is changed to enable new iSHARE entrants to start testing before a contract is signed. **Legal** - **Miscellaneous** • Rearranged pages and sections to improve readability • The governance framework is updated

Release 1.5	
Purpose	First public version the iSHARE scheme that can be used by launching customers
Release date	14 December 2017
Change log	• Updated specifications for all content of the iSHARE scheme: • Functional • Technical • Operational • Legal • Significantly updated and rearranged sections for readability, including a main scheme aspects (see page 20)- and illustrative use cases (see page 31) chapter with new depictions; Integrated (technical) specifications, generic and per iSHARE role

2.3 Release planning

The release planning provides detailed information about changes that are planned for future releases of the scheme. See the Operational Process Release Management (see page 179) section for details about the release management process of the iSHARE scheme.

2.3.1 **Planned releases**

Release 1.6		
Purpose	Lowering barriers for parties to start using iSHARE	
Planned release date	11 May 2018	
	RFC 001	**PKIOverheid certificates**
	Status	Positive advice CAB
	Relevant for	• Adhering parties (incl. software parties) • Certified parties • Prospects • Scheme Owner

Release 1.6		
	Summary	For at least the coming year and as a temporary specification of the current iSHARE specifications, PKIOverheid certificates are recommended by the Scheme Owner.
	RFC 004	**Start testing without contract**
	Status	Positive advice CAB
	Relevant for	• Prospects • Scheme Owner
	Summary	Enable new iSHARE entrants to start testing before a contract is signed.

Release 1.7		
Purpose	Create a better overview of all API specs in a singular space	
Planned release date	End June 2018 (subject to change)	
	RFC 003	**Move API specs to Dev portal**
	Relevant for	• Adhering parties (incl. software parties) • Certified parties • Prospects • Scheme Owner
	Summary	• Incorporate the to-be Production Scheme Owner API within the Scheme • Clarify Conformance Requirements in a single page to minimise cross-referencing and duplication. (The content may eventually be extracted from the specification itself and presented on a dedicated Developer Portal)
	Other planned changes	
	• Update of the government framework • Readability of the service levels	

2.3.2 **Backlog**

If you have any suggestions to improve the iSHARE scheme, please let us know. Send an email to info@iSHAREWorks.org[6]

2.4 Version history

- iSHARE v1.6, 11 May 2018 (current version)
- iSHARE v1.5[7], 14 December 2017
- iSHARE v1.2[8], 25 October 2017
- iSHARE v1.0[9], 23 June 2017
- iSHARE v0.5[10], 24 March 2017
- iSHARE v0.3[11], 27 February 2017
- iSHARE v0.2[12], 13 February 2017
- iSHARE v0.1[13] (start document)

6 mailto:info@iSHAREWorks.org
7 https://innopay.atlassian.net/wiki/download/attachments/53495699/171214A%20iSHARE%20scheme%20v1.5.pdf?api=v2&cacheVersion=1&modificationDate=1525863708289&version=1
8 https://innopay.atlassian.net/wiki/download/attachments/53495699/171025A%20iSHARE%20scheme%20v1.2.pdf?api=v2&cacheVersion=1&modificationDate=1512476617788&version=1
9 https://innopay.atlassian.net/wiki/download/attachments/53495699/170623A%20iSHARE%20scheme%20v1.0.pdf?api=v2&cacheVersion=1&modificationDate=1498640929587&version=1
10 https://innopay.atlassian.net/wiki/download/attachments/53495699/170324A%20iSHARE%20Scheme%20v0.5.pdf?api=v2&cacheVersion=1&modificationDate=1490881318297&version=1
11 https://innopay.atlassian.net/wiki/download/attachments/53495699/170227A%20iSHARE%20v0.3.pdf?api=v2&cacheVersion=1&modificationDate=1488300063025&version=3
12 https://innopay.atlassian.net/wiki/download/attachments/53495699/170213A%20iSHARE%20v0.2.pdf?api=v2&cacheVersion=1&modificationDate=1486999387363&version=1
13 https://innopay.atlassian.net/wiki/download/attachments/53495699/170126A%20iSHARE%20v0.1.pdf?api=v2&cacheVersion=1&modificationDate=1485421776278&version=1

3 Main scheme aspects

The iSHARE scheme is a combination of Functional, Technical, Operational and Legal agreements to which participating parties adhere. This chapter provides a bird's eye view on the main aspects of iSHARE, and an introduction to more in depth details of the scheme.

This section describes the iSHARE scheme's:

3.1 Key functionality

The iSHARE scheme aims to support the following key functionalities:

In line with iSHARE's guiding principles (see page 10), these key functionalities might be realised by (re)using existing standards or initiatives.

3.1.1 Support Machine to Machine (M2M) interaction

The iSHARE scheme aims to support multiple interaction models, of which Machine to Machine (M2M) is one. M2M interaction can be characterised as communication between machines, without interference by a human. In contemporary data communication there is a heavy reliance on M2M interaction.

Example:

- Every day, the ERP system (machine) of party A requests a status update from the ERP system (machine) of party B. Party B's ERP system automatically responds with the requested status update. No humans are needed to interfere.

This example is detailed under use cases (see page 31).

The opposite of the M2M interaction model is the Human to Machine interaction model (see page 21).

3.1.2 Support Human to Machine (H2M) interaction

The iSHARE scheme aims to support multiple interaction models, of which Human to Machine (H2M) is one. H2M interaction can be characterised as communication between a human and (a) machine(s). A user interface is necessary to enable H2M communication.

Example:

- Human X, working for Party A, requests a status update from the ERP system (machine) of Party B. It does so via a user interface.

This example is detailed under use cases (see page 31).

The opposite of the H2M interaction model is the Machine to Machine interaction model (see page 20).

3.1.3 Facilitate portable identity(s) for parties and humans

iSHARE aims to facilitate (but not impose) the use of one or more so called 'federated identity(s)'. A federated identity is an identity that is spread out and recognised, i.e. portable, across multiple, independent systems.

Within iSHARE, the use of federated identities would reduce costs by eliminating the need for proprietary, or newly issued identity solutions. In order for an identity to become part of iSHARE's federation, the legal entity provider the identity must be certified under the iSHARE scheme.

Example:

- Human X, working for Party A, has a personal keycard issued by iSHARE certified Identity Provider Y. The card, and thus the identity of Human X, can be used to identify and authenticate Human X at party B.

This example is detailed under use cases (see page 38).

3.1.4 Facilitate flexible authorisations, applicable in any context

iSHARE aims to enable parties to grant other parties or persons access to (parts of) their data or services. Parties within the iSHARE scheme have greatly varying backgrounds, however. Private and public, large and small, different value chains, different geographies, different modalities, etc. For that reason, iSHARE needs to have a flexible way of expressing authorisations.

Two examples can illustrate different levels of required flexibility:

1. Some parties or contexts require management of authorisations on a very detailed level, e.g. Party A's ERP system (machine) is ONLY allowed to request status updates concerning line X of bill of lading Y;
2. Some contexts require less detailed authorisations, e.g. Party A's ERP system (machine) is allowed to request ANY information about ANY (part of a) bill of lading.

Both examples are explained under use cases: fine-grained (see page 31); coarse-grained (see page 34).

The iSHARE scheme envisions a world in which (access) authorisations are flexible in three ways:

- Flexible authorisation scope;
  iSHARE aims to provide a way to add a layer of authorisation to any resource or any selection or combination of resources. The authorisation scope refers to the objects or resources of a specific party, to which authorisations need to be assigned. The scope can include many or all resources (e.g. all data), or

only some resources (e.g. specific data fields or services). Either way, the scope is always governed by a formal agreement and implemented by technical means.

- Granular authorisations, and;
  iSHARE aims to provide a granular way to use authorisations for resources. The authorisation granularity refers to the characteristics of both the requested resources and the rules (policies, conditions) that apply. Authorisations to resources can be coarse-grained (e.g. someone has access to all data in a certain data scope) or fine-grained (e.g. someone has access to only data with a low sensitivity level). The rules (policies, conditions) that control the authorisations can be fine-grained as well, meaning that many different types of rules can apply, such as time of day, location, organisation, role, and competence level.
- Flexible authorisation source.
  iSHARE aims to provide flexibility to where authorisation rules are stored and can be retrieved. The authorisation source refers to the location of the rules (policies, conditions) and the attributes (e.g. subject attributes, object attributes) that govern the authorisations. These can be located near the data, at a dedicated source, or a combination thereof. In the current version of the iSHARE scheme, the flexibility in authorisation source is described as 'Policy Information Point' or PIP in the detailed functional descriptions (see page 51).

3.1.5 Enable data exchange based on delegations - even between unknown parties

One of the barriers to exchanging data is often that parties do not know each other sufficiently, and therefore are not able to share data. Often this can only be done after some form of contract has been established.

Within iSHARE it is the explicit aim to make it possible to exchange data for parties that are unknown to each other based on delegations. A delegation within iSHARE functions as evidence that a party is directly or indirectly operating in name of a known party. Based on the delegation a certain (unknown) party has given, a party can decide if this party may receive certain data or not.

Example:

- Party A hires Trucking Company B to deliver Container X to Party C. Trucking Company B's ERP system asks Party C's ERP system at what time it should deliver the container. Party C's ERP system does not know Trucking Company B, but can check the delegation to Trucking Company B that Party A has registered at Authorisation Registry D. Because this delegation is in order, Party C's ERP system shares a time slot with Trucking Company B's ERP.

This example is detailed under use cases (see page 44).

3.1.6 Enable control over own data through management of consent

As described under key functionalities 'facilitate flexible authorisations (see page 21)' and 'enable data exchange based on delegations (see page 22)', iSHARE aims to enable parties to grant other parties or persons access to (parts of) their data or services. At least as important is iSHARE's aim to allow parties to modify or withdraw these access rights, to their data or services, whenever they wish. This is called management of consent, and enables full control over own data at any moment in time.

Example:

- In the example described under key functionality 'enable data exchange based on delegations (see page 22)', Party A hires Trucking Company B to deliver Container X to Party C. Trucking Company B's ERP system asks Party C's ERP system at what time it should deliver the container. Party C's ERP system does not know Trucking Company B, but can check the delegation to Trucking Company B that Party A has registered at Authorisation Registry D. Because this delegation is in order, Party C's ERP system shares a time slot with Trucking Company B's ERP.

- Now imagine that moments before Trucking Company B's ERP system asks Party C's ERP system for a time slot, Party C revokes Party A's access to requesting a time slot. Consequently, Trucking Company B's request for a time slot gets an access forbidden message; Trucking Company B's request is NOT accepted because Party A, and therewith delegated Trucking Company B, is no longer authorised to ask for a time slot.

Party C, as showcased, remains in full control over its own data and services at any moment in time. This example is detailed under use cases (see page 44).

3.1.7 Provide a trust framework

Within iSHARE, it is the explicit aim to define a trust framework based on a synthesis between technological and legal aspects. In practical terms the aim is to let iSHARE participants sign one contract with the Scheme Owner, on the basis of which they have a contract with all participants within iSHARE. In other words, participants within iSHARE do not need to sign separate contracts with each other to share data with each other (although they are free to define additional contracts that do not conflict with the iSHARE framework).

An important tool within the trust framework are licenses which define the conditions under which data can be exchanged or services can be consumed. For functional details on licenses, see the detailed Functional descriptions (see page 93).

The trust framework is depicted under detailed Functional descriptions (see page 51) and needs appropriate technological underpinning so that parties can authenticate each other in a reliable way.

3.2 Technical overview

The iSHARE scheme can be characterised as an API (Application Programming Interface)[14] architecture for identification, authentication and authorisation based on a modified version of the widely used OAuth and OpenID Connect standards. The APIs specified for every role within iSHARE enable standardised interaction between computer systems.

Important

APIs manage access to services of an organisation, services that can be consumed by other parties. Services accessible through APIs can let those (machines or humans) that access the service do anything between reading simple data, to receiving complex instructions, to adding information to a database. If a truck's systems send a time and location to another party's 'Estimated Time of Arrival'-service, for example, this service might respond with an an optimal route to take and an Estimated Time of Arrival. Within iSHARE, the terms 'service consumption' and 'service provision' are used to specify how parties interact with each other (with, in this example, the truck's owner the Service Consumer, and the other party the Service Provider). Note that while the word data exchange is not literally in these terms, API service provision and consumption ALWAYS entails data exchange.

The API architecture of iSHARE also builds upon the following components:

- **PKI and digital certificates;**
  For the authentication of parties and machines, iSHARE uses PKI and digital certificates.

14 https://innopay.atlassian.net/wiki/spaces/IS/pages/173179148/API

- **HTTP over TLS (HTTPS);**
  iSHARE uses the commonly used HTTP protocol for its communications, including TLS to encrypt the communications.

- **RESTful architectural style;**
  iSHARE uses the RESTful architectural style to structure APIs and HTTP calls.

- **JSON/JWT;**
  Data exchanged in the iSHARE context is structured using the JSON standard. Where non-repudiation is required, JWT's are used;

- **XACML.**
  Delegations are structured according to a JSON port of the XACML standard.

The combination of the above standards and protocols leads to a certain dynamic between the roles in the iSHARE framework (see page 24). In essence, Service Consumers acquire a token which allows them to access certain services from certain Service Providers. The roles specified in the iSHARE framework are loosely based on the OAuth standard.

For a full explanation and description of all APIs, standards and protocols, please refer to the detailed Technical descriptions (see page 100).

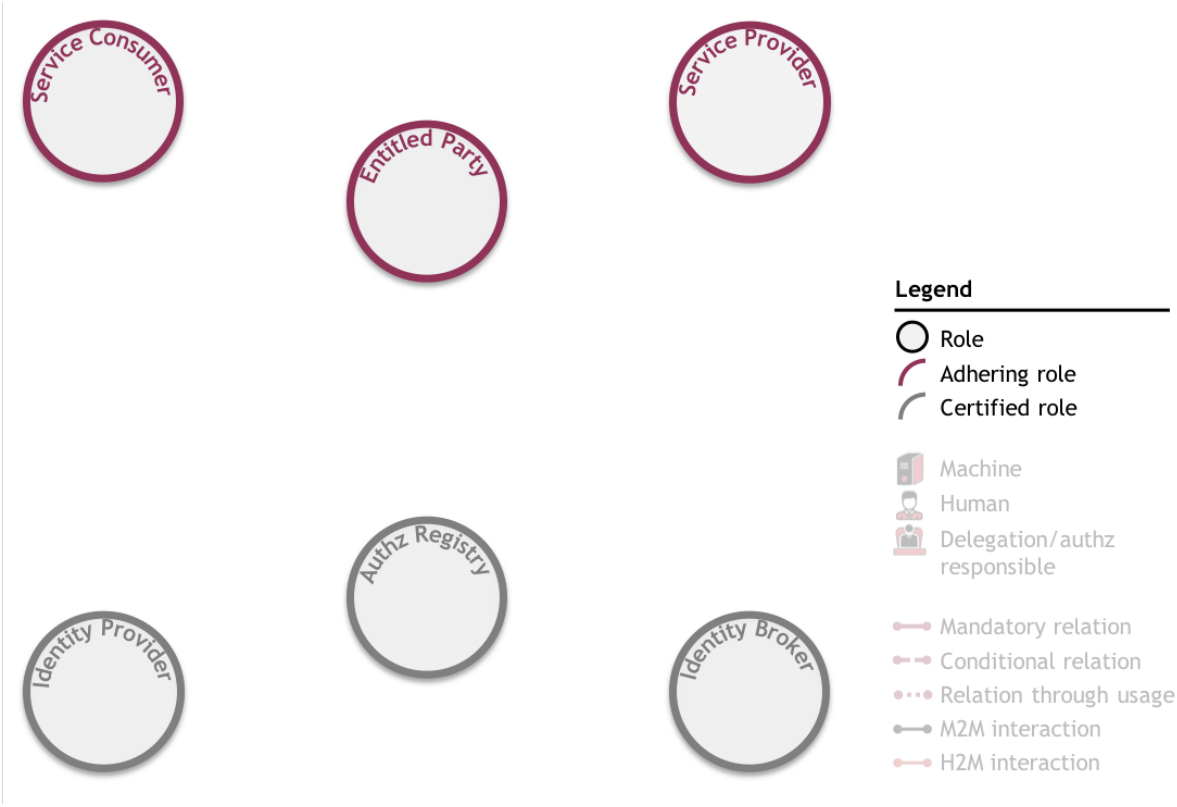
3.3 Framework and roles

iSHARE aims to provide a generic building block for service provision, widely applicable in the logistics sector. This requires a framework that can be applied to the wide variety of use cases possible in practice. This chapter explains the iSHARE framework, its roles, and its relations, step-by-step.

Important (and as under technical overview)

APIs manage access to services of an organisation, services that can be consumed by other parties. Services accessible through APIs can let those (machines or humans) that access the service do anything between reading simple data, to receiving complex instructions, to adding information to a database. If a truck's system sends a time and location to another party's 'Estimated Time of Arrival'-service, for example, this service might respond with an an optimal route to take and an Estimated Time of Arrival. Within iSHARE, the terms 'service consumption' and 'service provision' are used to specify how parties interact with each other (with, in this example, the truck's owner the Service Consumer, and the other party the Service Provider). Note that while the word data exchange is not literally in these terms, API service provision and consumption ALWAYS entails data exchange.

The iSHARE framework consists of six roles that, depending on the situation, interact with each other based on the iSHARE scheme agreements. Each role has a certain function in the scheme and bears certain responsibilities, as described below:



Any party fulfilling a role in the iSHARE framework must be iSHARE adhering or iSHARE certified:

- Parties fulfilling **adhering roles,** depicted in purple, provide and consume services under iSHARE. These parties adhere to the iSHARE terms of use;
- Parties fulfilling **certified roles**, depicted in grey, facilitate functions that adhering parties can rely upon when providing or consuming services. To become certified, these parties must not only prove adherence to the iSHARE terms of use, but also meet several role-specific criteria.

3.3.1 Adhering roles

In any iSHARE use case, the three adhering roles appear: a Service Consumer always consumes a Service Provider's service on the basis of the Entitled Party's entitlements.

Adhering role:	**Role description:**
Service Consumer	The Service Consumer-role is fulfilled by a legal entity that consumes a service, such as data, as provided by a Service Provider. This legal entity is in need of the result of a service; for example, a trucking company that needs to know its optimal route and Estimated Time of Arrival. A Service Consumer can be represented by a machine (its system) or a human (e.g. the trucker), fittingly called the Machine Service Consumer and the Human Service Consumer.

Adhering role:	Role description:
Service Provider	The Service Provider-role is fulfilled by a legal entity that provides a service, such as data, for consumption by a Service Consumer. This legal entity provides the result of a service that Service Consumer(s) need; for example the party that uses a truck's a time and location to calculate and communicate the truck's optimal route and Estimated Time of Arrival.
Entitled Party	The Entitled Party-role is fulfilled by a legal entity that has one or more rights to a service provided by a Service Provider, for example to data. These rights, or entitlements, are established in a legal relation between the Entitled Party and the Service Provider. The Entitled Party- and Service Consumer-roles can be fulfilled by the same entity - i.e. a legal entity that consumes a service based on its own entitlements to this service (for example, the trucking company's entitlement to request Estimated Time of Arrival- and optimal route information) - but this is not necessary. Legal entities that are entitled to a service can delegate other entities to consume this service on its behalf: the legal entity consuming the service, then, does so on the basis of *another entity's* entitlements. In such use cases, as always, the Service Consumer consumes a Service Provider's service on the basis of the Entitled Party's entitlements, but the Service Consumer-role is fulfilled by another entity than the Entitled Party-role. Our trucking company, for example, could have been delegated the right to request Estimated Time of Arrival- and optimal route information by an Entitled Party, that had originally planned to transport its goods itself but instead hired the trucking company to do so. It therefore delegated its own right to request Estimated Time of Arrival- and optimal route information to the trucking company.

3.3.2 Certified roles

For the controlled provision and consumption of services, adhering parties (and specifically, the humans and machines representing them) must be identified, authenticated, and authorised. The tooling necessary for these processes *can* be implemented by adhering parties. Such tooling is expensive, however, and must be constantly updated to keep in check with the latest security standards. To make sure no such tooling needs to be implemented by adhering parties before they start providing or consuming services under iSHARE (and therefore, to improve iSHARE's scalability), iSHARE recognises several certified roles fulfilled by legal entities that offer outsourced identification, authentication, and authorisation tooling to adhering parties.

Certified role:	Role description:
Identity Provider	The Identity Provider-role is fulfilled by a legal entity whose tooling identifies and authenticates humans (and specifically, Human Service Consumers representing Service Consumers). An Identity Provider: • Provides identifiers for humans; • Issues credentials[15] (i.e. a password or electronic keycard) to humans; • On the basis of this identification information, identifies and authenticates humans for Service Providers. As a result, Service Providers can outsource identification and authentication to an Identity Provider instead of implementing their own tooling.
Identity Broker	Different humans might hold identifiers at different Identity Providers. Also, Service Providers might need to connect to several Identity Providers. To make sure Service Providers do not need a relation with each Identity Provider individually, an Identity Broker is introduced. The **Identity Broker**-role is fulfilled by a legal entity that provides Service Providers access to different Identity Providers, and that offers humans the option to choose with which Identity Provider to identify and authenticate themselves throughout the iSHARE scheme. As a result, if Service Providers choose to outsource identification and authentication to more than one Identity Provider, they can connect to an Identity Broker instead of to several Identity Providers.
Authorisation Registry	The Authorisation Registry-role is fulfilled by a legal entity who provides solutions for adhering parties for the storage of delegation- and authorisation information. An Authorisation Registry: • Can holds information on delegations to Service Consumers; i.e. information indicating what parts of the rights of an Entitled Party are delegated to a Service Consumer. • Can holds information on authorisations of humans representing a Service Consumer; i.e. information indicating which humans are authorised to act on a Service Conumer's behalf. • Can check, on the basis of this information, whether a human or machine representing a legal entity is authorised to take delivery of a service; • Can confirm whether this is the case to the Service Provider. As a result, Adhering Parties can outsource tasks concerning the management of authorisation and delegation information to an Authorisation Registry instead of implementing their own tooling.

As detailed under functional requirements per role (see page 96), and in line with guiding principle 3 (see page 10), to become an iSHARE certified party, a legal entity must (first) be admitted as a participant in the Afsprakenstelsel elektronische toegangsdiensten[16] (in the relevant role).

3.3.3 iSHARE compatible software

Next to iSHARE adherence and certification, the concept of iSHARE compatibility exists. This concept is reserved for software that technically adheres to the iSHARE scheme (i.e. is iSHARE compatible), and can be sold to

15 https://innopay.atlassian.net/wiki/spaces/IS/pages/53840953/Credentials
16 https://afsprakenstelsel.etoegang.nl/display/as/Startpagina

parties fulfilling adhering- and certified roles. Note that parties using iSHARE compatible software within an iSHARE context must be adhering or certified, whereas a party that delivers iSHARE compatible software does not need to be so.

3.3.4 Role of the Scheme Owner

One last role, not part of the basic iSHARE framework, is that of the Scheme Owner. The Scheme Owner-role is fulfilled by the legal entity that keeps the scheme, and its network of participants, operating properly. How exactly is found under the detailed Operational descriptions (see page 170). It is this Scheme Owner that decides whether a party is admitted to the iSHARE network (and whether this is as an adhering- or certified party).

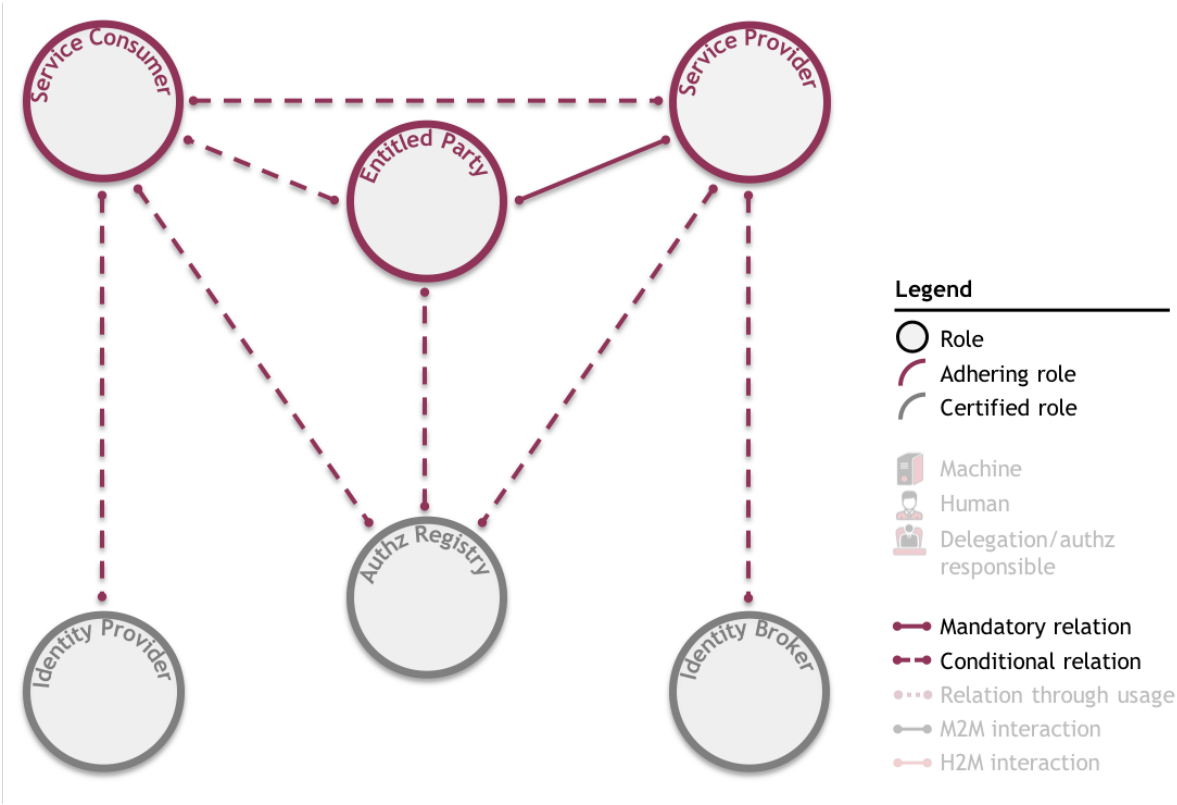
The Scheme Owner plays a fundamental role in any iSHARE use case. Every participant to the iSHARE scheme must have a relation with the Scheme Owner, and can check at the Scheme Owner whether other parties participate in iSHARE. These are prerequisites, however, which is why the Scheme Owner does not play a direct role (and is not depicted) in any of the use cases. Please refer to the detailed Functional descriptions (see page 51)for details on how the Scheme Owner facilitates trust in the iSHARE scheme.

3.3.5 Framework and roles in use cases

All of iSHARE's use cases can be depicted in the iSHARE framework. Their complexity is dependent on:

- The interaction model (Machine to Machine or Human to Machine);
  i.e. whether the Service Consumer is represented by a machine or a human.
- Whether delegation takes place;
  i.e. whether the Service Consumer-role is fulfilled by another entity than the Entitled Party-role. How delegations work exactly is explained here (see page 94).
- Whether parties fulfilling adhering roles use their own tooling for identification, authentication, and authorisation or outsource these processes and the information necessary for these processes to certified roles instead.

Hypothetically, and dependent on the above, a use case could include all of the following relations between roles:



Note that the only relation mandatory in all use cases is the relation between the Entitled Party and the Service Provider, which establishes the entitlements of the Entitled Party. In the depiction of iSHARE's use cases (see page 31), all legal relations are shown before the actual interaction is plotted in the framework.

3.4 Legal provisions

The legal underpinning of iSHARE and its trust framework consists of a contract between all iSHARE participants and the iSHARE Scheme Owner (the so called Accession Agreement). Based on this one contract with the Scheme Owner, all participants are bound to the common iSHARE terms of use and can appeal to each other to abide by these rules (in legal terms this is called perfection (Dutch: *derdenwerking*)).

Two main documents make up iSHARE's legal provisions:

1. **The Accession Agreement;**
   The main contract between the participant and the iSHARE Scheme Owner. This contract refers to the terms of use, including all iSHARE specifications, to which all participants must abide. After signing the Accession Agreement, a party becomes a participant of the iSHARE scheme either as an Adhering Party or a Certified Party. There are two separate Accession Agreements: one for adhering parties (see page 191) and one for certified parties (see page 192)).

2. **The Terms of Use.**
   The Terms of Use (see page 193) further define the rights and obligations of every iSHARE participant and the Scheme Owner. The Terms of Use apply to any party that has signed the Accession Agreement. The Terms of Use also state that participants fully abide by the iSHARE scheme specifications.

For the details of the Accession Agreements, the full version of the Terms of Use and the information available on legal context, please refer to the detailed Legal descriptions (see page 190).

3.4.1 Licenses

Within iSHARE it is possible to explicitly provide instructions on how a service may be consumed or under which conditions data is exchanged. These instructions or conditions are called 'licenses'. Licenses are a crucial part of iSHARE, because they provide its participants the possibility to clearly state what is and what is not allowed. Since all iSHARE participants are bound to the same contract and underlying scheme rules, participants can appeal to each other to follow the provided licenses. Please refer to the iSHARE Terms of Use (see page 193) for a detailed legal explanation.

3.5 Operational provisions

The iSHARE scheme is constantly improved in collaboration with its stakeholders. Keeping the scheme, and its network of participants operating properly is facilitated by the iSHARE Scheme Owner.

The main responsibilities of the Scheme Owner include:

- Management of the iSHARE scheme (specifications);
- Management of the iSHARE network (participants);
- Management of the iSHARE brand.

To fulfil its responsibilities, the Scheme Owner facilitates the correct operation of the iSHARE scheme and -network through administering several aspects:

- Operational processes (see page 171)
- Service levels (see page 181)
- Communication (see page 189)

The Scheme Owner is part of a wider governance framework, which can be found in the introduction of the scheme (see page 14).

4 Use cases

This section builds on the iSHARE framework (see page 24) to showcase the scheme's key functionalities (see page 20) in four use cases:

1. **Use case:** M2M interaction (with fine-grained authorisation) (see page 31) showcases:
    - Support Machine to Machine (M2M) interaction (see page 20);
    - Facilitate flexible authorisations, applicable in any context (see page 21).

    (see page 21)
2. **Use case:** H2M interaction (with coarse-grained authorisation) (see page 34) showcases:
    - Support Human to Machine (H2M) interaction (see page 21);
    - Facilitate flexible authorisations, applicable in any context (see page 21).

3. **Use case:** portable identity (see page 38) showcases:
    - Facilitate portable identity(s) for parties and humans (see page 21).

4. **Use case: delegation (and management of consent)** showcases:
    - Enable data exchange based on delegations - even between unknown parties (see page 22);
    - Enable control over own data through management of consent (see page 22).

Structure

Each use case includes:

- A description and depiction of the roles and relations;
- A description of the prerequisites, and a depiction of prerequisite registration;
- A description and depiction of the use case;
- A sequence diagram;
- A reference to what needs to be technically implemented for this use case.

The depicted use cases are only a selection of iSHARE's use case scope. For the full scope, please refer to the detailed Functional descriptions (see page 51).

4.1 Use case: M2M interaction (with fine-grained authorisation)

This use case showcases iSHARE's key functionality 'support Machine to Machine (M2M) interaction (see page 20)'.

The example described in the linked chapter is as follows:

- Every day, the ERP system (machine) of Party A requests a status update from the ERP system (machine) of Party B. Party B's ERP system automatically responds with the requested status update. No humans are needed to interfere.

To also showcase iSHARE's key functionality 'facilitate flexible authorisations (see page 21)', Party A's ERP system (machine) is ONLY allowed to request status updates concerning line X of bill of lading Y. This can be considered a fine-grained authorisation.

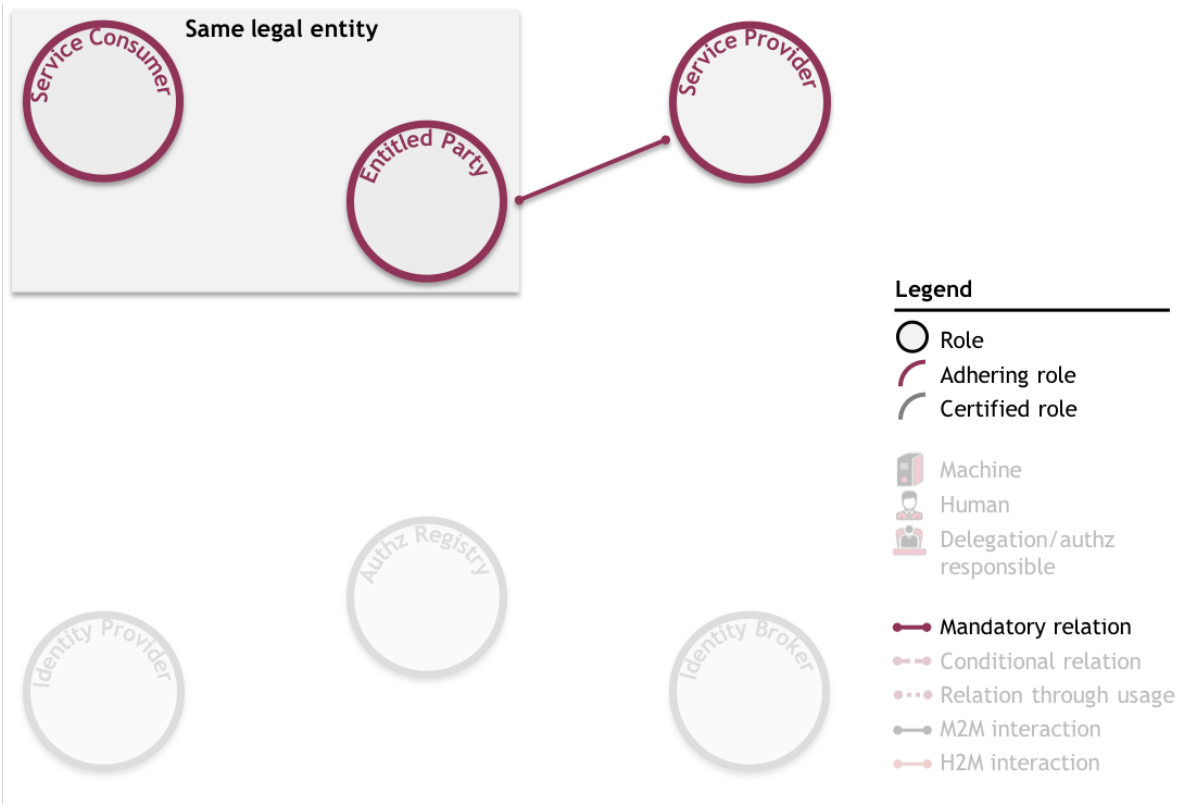
The following explains this example in detail, utilising the iSHARE framework.

4.1.1 Roles and Relations

The following roles are fulfilled in this use case:

- Party A requests a status update, so it is the legal entity fulfilling the **Service Consumer**-role;
- Party B responds with the status update, so it is the legal entity fulfilling the **Service Provider**-role;
- No delegation takes place, so Party A also fulfils the **Entitled Party**-role;
- As this is a M2M use case, a **Machine Service Consumer** represents Party A.

The only **legal relation** is the mandatory relation between the Entitled Party (Party A) and the Service Provider (Party B), which establishes the entitlements of the Entitled Party (Party A). As depicted:



4.1.2 Prerequisites

It is prerequisite of this use case that:

- The Service Provider (Party B) has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services, i.e. Party B has information indicating that Party A is allowed to request status updates concerning line X of bill of lading Y from its ERP system;
- The Service Consumer (Party A) is able to authenticate the Service Provider (Party B);
- The Service Provider (Party B) is able to authenticate the Service Consumer (Party A).

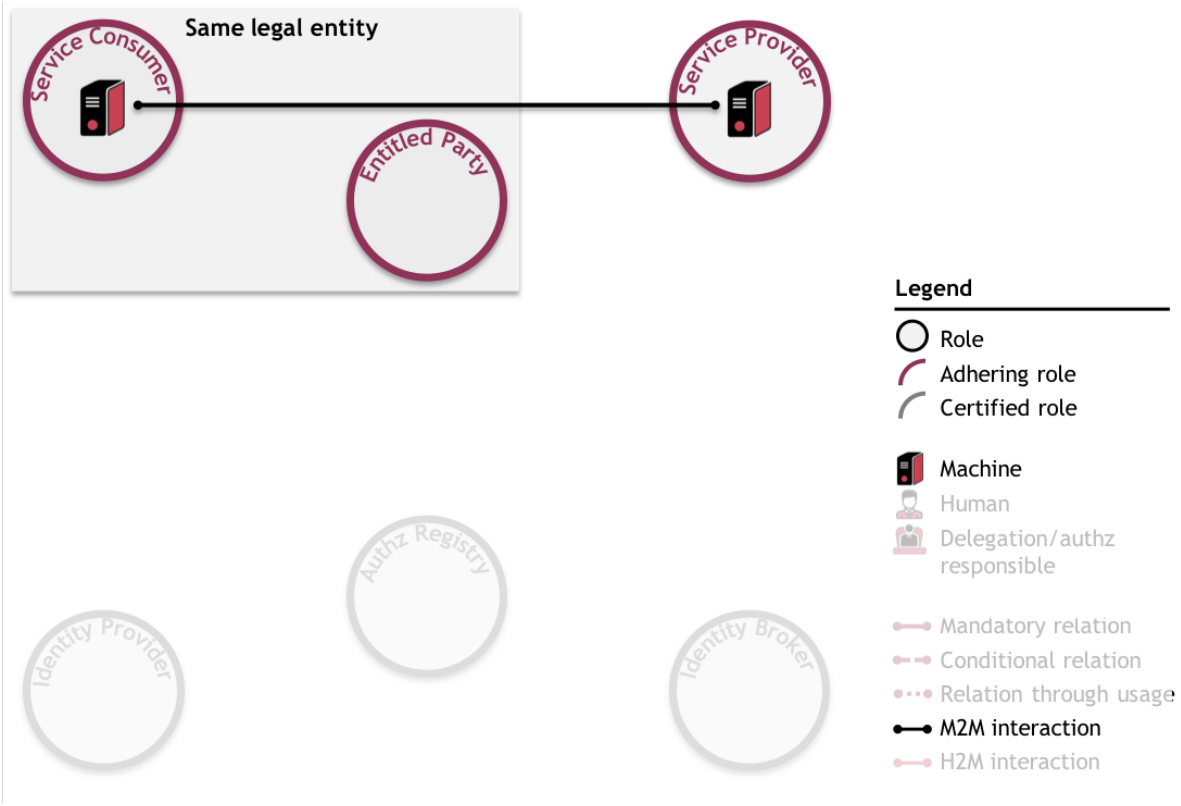
4.1.3 Use case

The use case consists of the following steps:

1. The Machine Service Consumer (of Party A) requests a service from the Service Provider (Party B);
2. The Service Provider (Party B) authenticates the Machine Service Consumer (of Party A) and validates the iSHARE adherence of the Service Consumer (Party A);

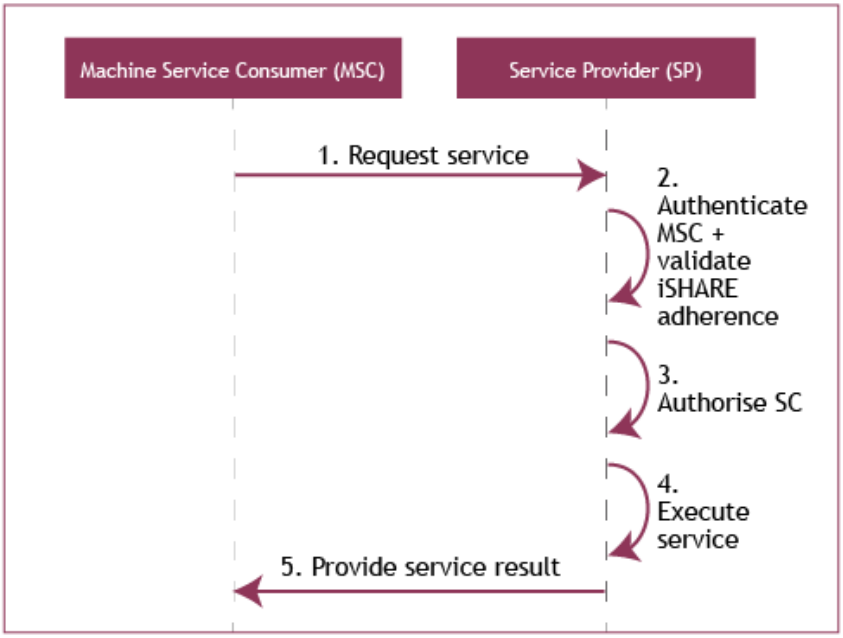
3. The Service Provider (Party B) authorises the Machine Service Consumer of the Service Consumer (Party A) based on the entitlement information registered with the Service Provider (Party B);
4. The Service Provider (Party B) executes the requested service;
5. The Service Provider (Party B) provides the service result to the Machine Service Consumer (of Party A).

As depicted:



Note that this use case is exactly the same as primary use case 1, as found under detailed Functional descriptions (see page 56).

4.1.4 Sequence diagram



What needs to be implemented technically for this use case is described generically (see page 100), and specifically per role:

- Service Consumer (see page 119);
- Service Provider (see page 125);
- Entitled Party (see page 119).

4.2 Use case: H2M interaction (with coarse-grained authorisation)

This use case showcases iSHARE's key functionality 'support Human to Machine (H2M) interaction (see page 21)'.

The example described in the linked chapter is as follows:

- Human X, working for Party A, requests a status update from the ERP system (machine) of Party B. It does so via a user interface.

To also showcase iSHARE's key functionality 'facilitate flexible authorisations (see page 21)', Party A's ERP system (machine) is allowed to request ANY information about ANY (part of a) bill of lading. This can be considered a coarse-grained authorisation.

The following explains this example in detail, utilising the iSHARE framework.

4.2.1 Roles and Relations

The following roles are fulfilled in this use case:

- Party A requests a status update, so it is the legal entity fulfilling the **Service Consumer**-role;
- Party B responds with the status update, so it is the legal entity fulfilling the **Service Provider**-role;

- No delegation takes place, so Party A also fulfils the **Entitled Party**-role;
- Human X is the **Human Service Consumer** that represents Party A.

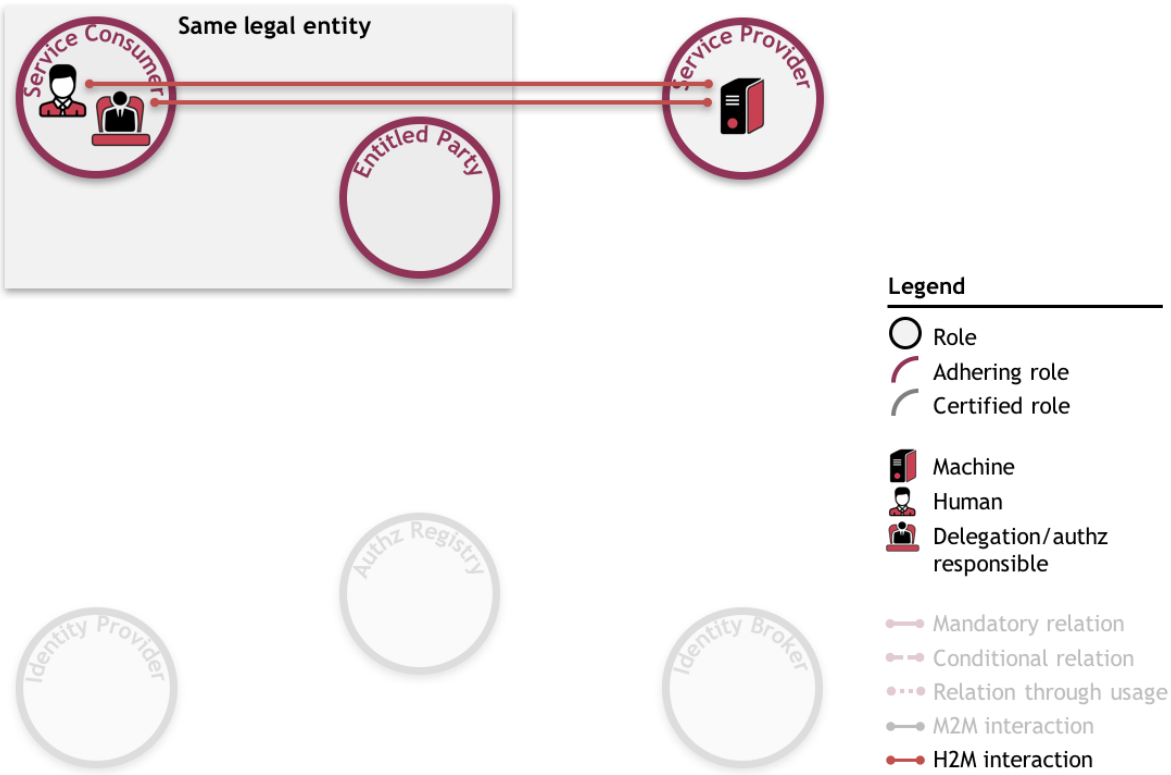
The only **legal relation** is the mandatory relation between the Entitled Party (Party A) and the Service Provider (Party B), which establishes the entitlements of the Entitled Party (Party A). As depicted:

4.2.2 Prerequisites

It is prerequisite of this use case that:

- The Service Provider (Party B) has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services, i.e. Party B has information indicating that Party A is allowed to request ANY information about ANY (part of a) bill of lading from its ERP system;
- The Service Consumer (Party A) has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf;
- **The delegation/authorisation responsible at the the Service Consumer (Party A) registers the authorisation information at the Service Provider (Party B);**
- The Human Service Consumer (Human X) is able to authenticate the Service Provider (Party B);
- The Service Provider (Party B) is able to authenticate the Human Service Consumer (Human X);
- **The Human Service Consumer (Human X) has been issued identity credentials by the Service Provider (Party B).**

The prerequisites in bold are depicted as follows:

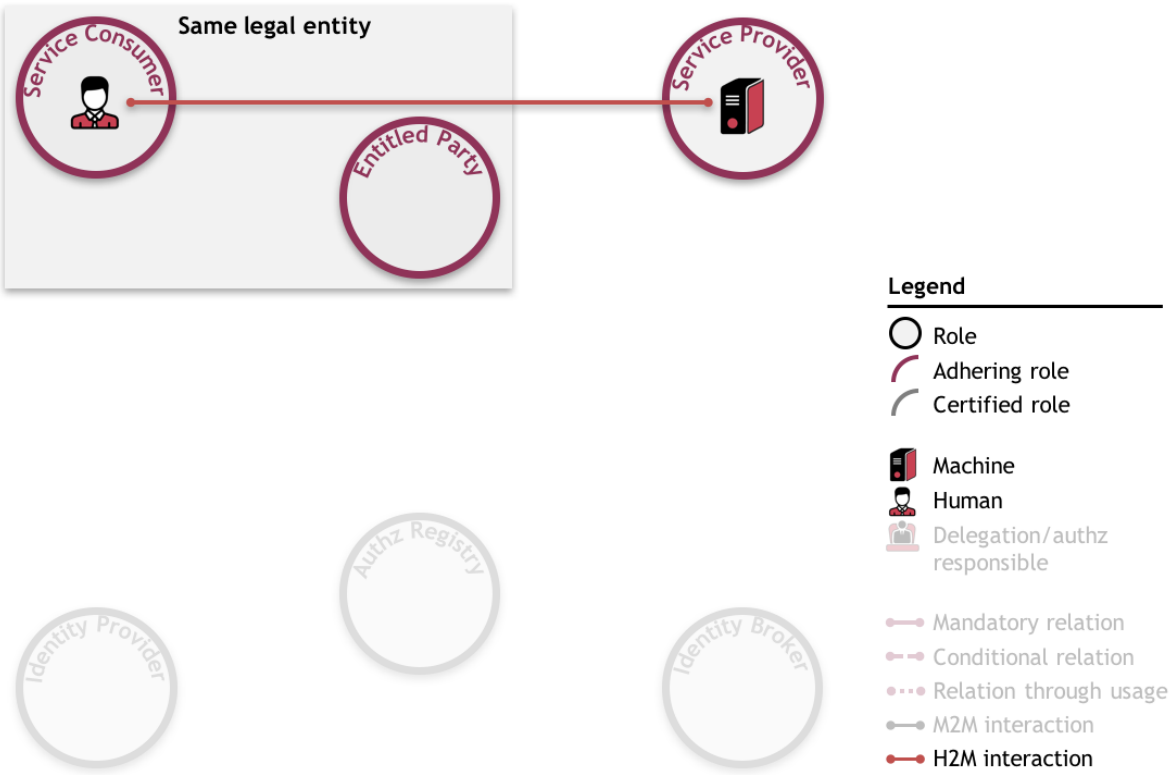


4.2.3 Use case

The use case consists of the following steps:

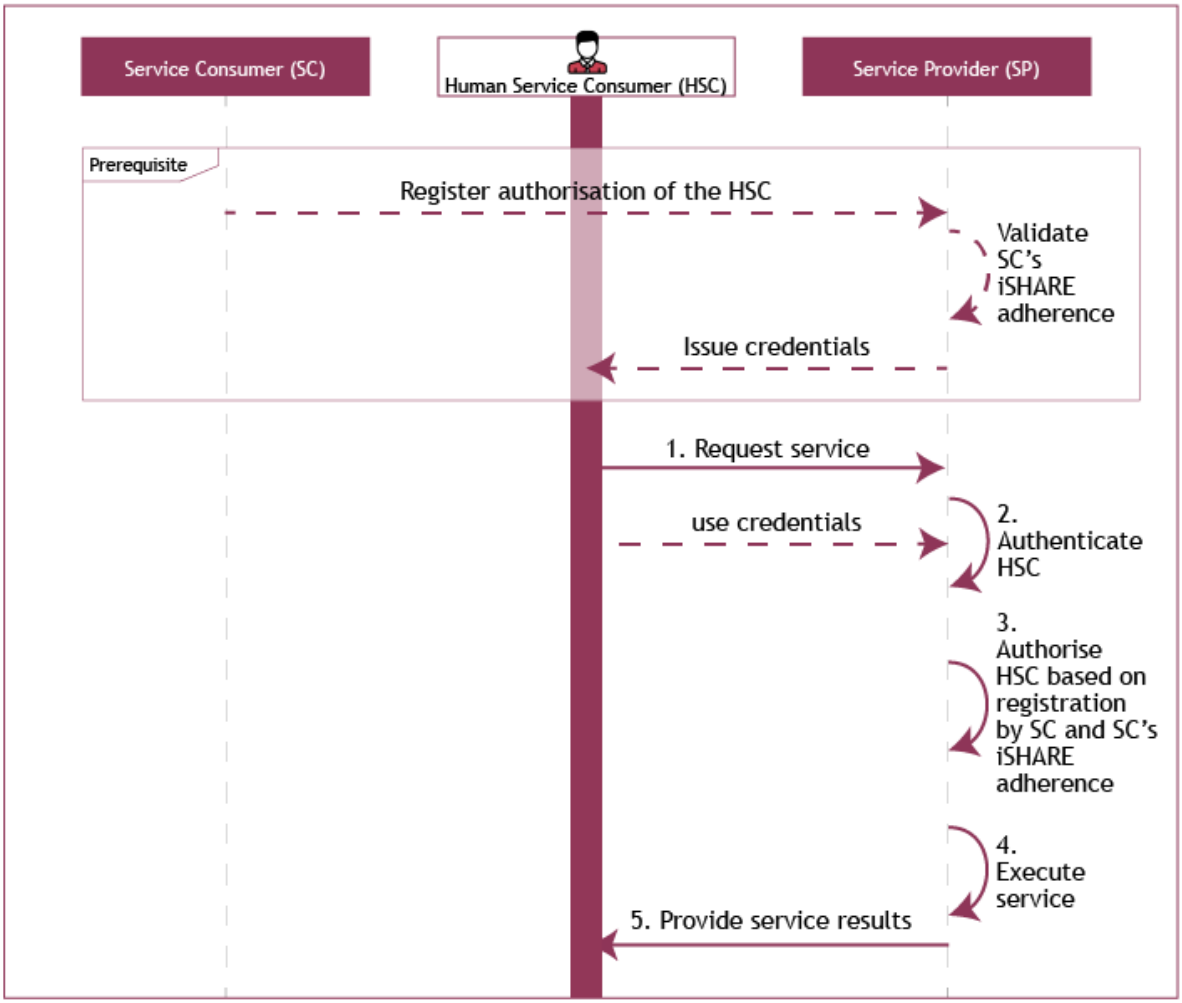
1. The Human Service Consumer (Human X) requests a service from the Service Provider (Party B);
2. The Service Provider (Party B) authenticates the Human Service Consumer (Human X), and validates the iSHARE adherence of the Service Consumer (Party A);
3. The Service Provider (Party B) authorises the Human Service Consumer (Human X) of the Service Consumer (Party A) based on the entitlement- and authorisation information registered with the Service Provider (Party B);
4. The Service Provider (Party B) executes the requested service;
5. The Service Provider (Party B) provides the service result to the Human Service Consumer (Human X).

As depicted:



Note that this use case is exactly the same as primary use case 2, as found under detailed Functional descriptions (see page 69).

4.2.4 Sequence diagram



What needs to be implemented technically for this use case is described generically (see page 100), and specifically per role:

- Service Consumer (see page 119);
- Service Provider (see page 125);
- Entitled Party (see page 119).

4.3 Use case: portable identity

This use case showcases iSHARE's key functionality 'facilitate portable identity(s) for parties and humans (see page 21)'.

The example described in the linked chapter is as follows:

- Human X, working for Party A, has a personal keycard issued by iSHARE certified Identity Provider Y. The card, and thus the identity of Human X, can be used to identify and authenticate Human X at party B.

Human X will now use its Identity Provider Y keycard to request a status update from the ERP system (machine) of Party B.

The following explains this example in detail, utilising the iSHARE framework.

4.3.1 Roles and Relations

The following roles are fulfilled in this use case:

- Party A requests a status update, so it is the legal entity fulfilling the **Service Consumer**-role;
- Party B responds with the status update, so it is the legal entity fulfilling the **Service Provider**-role;
- No delegation takes place, so Party A also fulfils the **Entitled Party**-role.

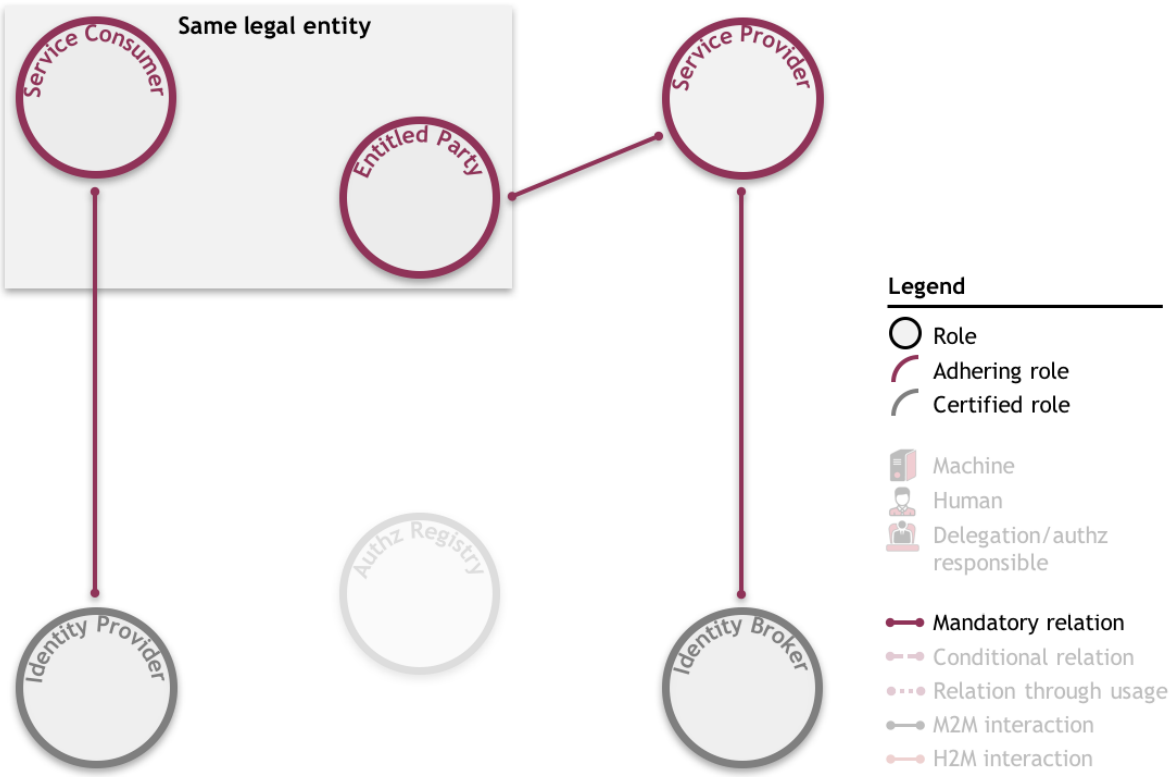
- Human X is the **Human Service Consumer** that represents Party A;
- Identity Provider Y is one of the **Identity Providers** to which Party B has outsourced identification and authentication of humans, and the party that has given Human X his keycard.

- Optionally (and shown in this case), Identity Broker Z is the **Identity Broker** that provides Party B access to different Identity Providers, and that offers Human X the option to choose with which Identity Provider to identify and authenticate itself.

4.3.1.1 Legal relations

- As always, a mandatory relation between the Entitled Party (Party A) and the Service Provider (Party B) establishes the entitlements of the Entitled Party (Party A);
- A mandatory relation between the Service Provider and the Identity Broker covers the use of Identity Broker Z's services, including a connection to several Identity Providers, by the Service Provider (Party B);
- A mandatory relation between the Service Consumer (Party A) and Identity Provider Y covers the use of Identity Provider Y's keycards by the the Service Consumer's (Party A's) humans, including Human X.

As depicted:

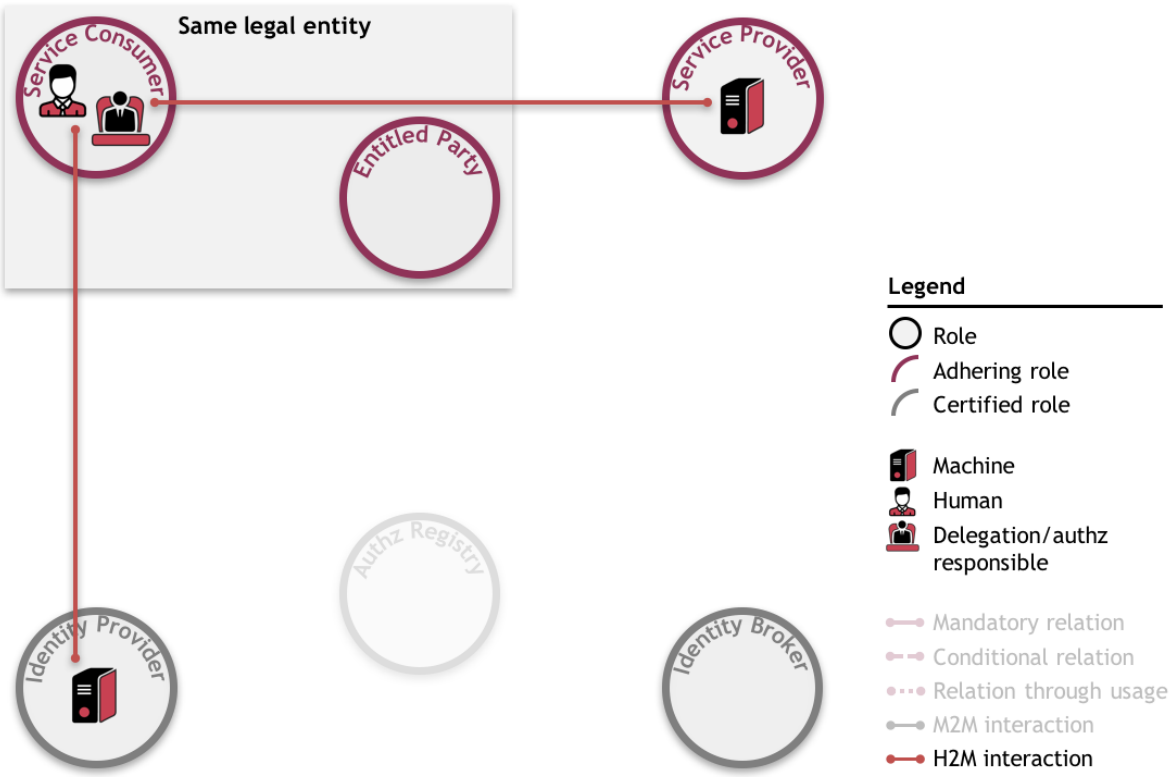


4.3.2 Prerequisites

It is prerequisite of this use case that:

- The Service Provider (Party B) has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services, i.e. Party B has information indicating that Party A is entitled to status updates from its ERP system;
- The Service Consumer (Party A) has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf;
- **The delegation/authorisation responsible at the the Service Consumer (Party A) registers the authorisation information at the Service Provider;**
- The Human Service Consumer (Human X) is able to authenticate the Service Provider (Party B);
- The Service Provider (Party B) is able to authenticate the Human Service Consumer (Human X);
- The Identity Provider (Y) is able to authenticate the Service Provider (Party B);
- The Service Provider (Party B) is able to authenticate the Identity Provider (Y);
- The Identity Broker (Z) is able to authenticate the Service Provider (Party B);
- The Service Provider (Party B) is able to authenticate the Identity Broker (Z);
- **The Human Service Consumer (Human X) has been issued identity credentials (a keycard) by the Identity Provider (Y).**

The prerequisites in bold are depicted as follows:

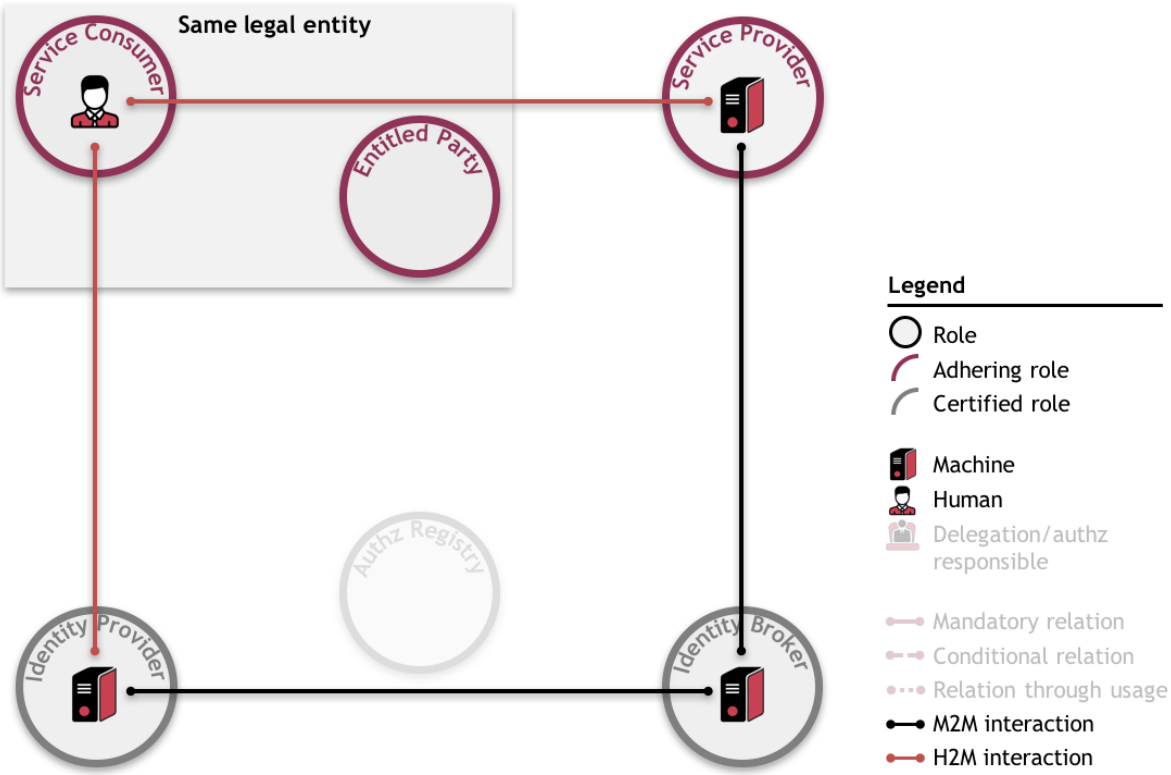


4.3.3 Use case

The use case consists of the following steps:

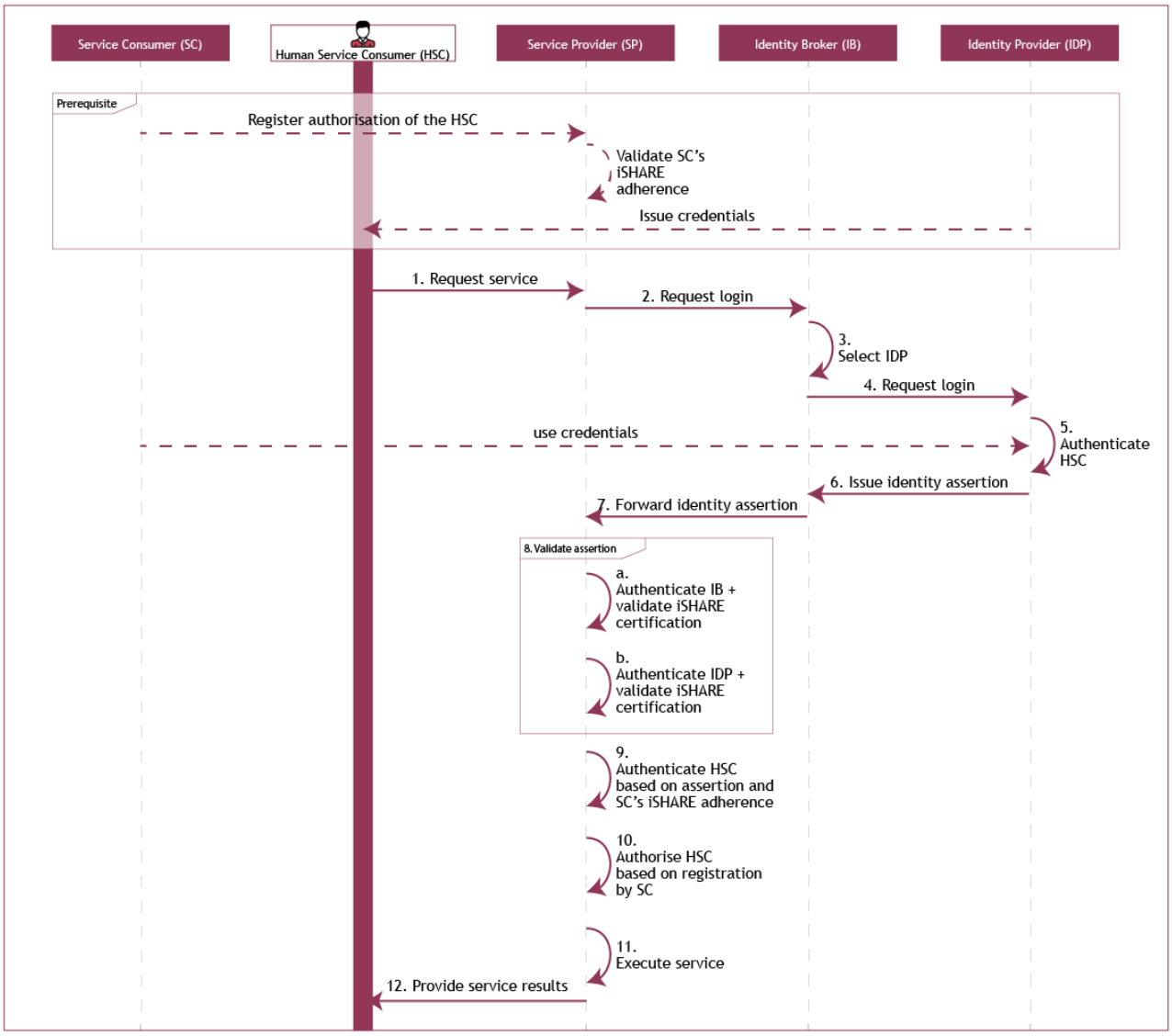
1. The Human Service Consumer (Human X) requests a service from the Service Provider (Party B);
2. The Service Provider (Party B) requests a login from the Identity Broker (Z);
3. The Identity Broker (Z) asks the Human Service Consumer (Human X) to select his Identity Provider (Y);
4. The Identity Broker (Z) requests a login from the Identity Provider (Y);
5. The Identity Provider (Y) authenticates the Human Service Consumer (Human X) (on the basis of Human X's keycard);
6. The Identity Provider (Y) issues an identity assertion for the Service Provider (Party B) to the Identity Broker (Z);
7. The Identity Broker (Z) forwards the identity assertion to the Service Provider (Party B);
8. The Service Provider (Party B) validates the identity assertion through the following steps:
    a. The Service Provider (Party B) authenticates the Identity Broker (Z) and validates its iSHARE certification;
    b. The Service Provider (Party B) authenticates the Identity Provider (Y) and validates its iSHARE certification.
9. The Service Provider (Party B) authenticates the Human Service Consumer (Human X) based on the validity of the identity assertion, and validates the iSHARE adherence of the Service Consumer (Party A);
10. The Service Provider (Party B) authorises the Human Service Consumer (Human X) of the Service Consumer (Party A) based on the entitlement- and authorisation information registered with the Service Provider (Party B);
11. The Service Provider (Party B) executes the requested service;
12. The Service Provider (Party B) provides the service result to the Human Service Consumer (Human X).

As depicted:



Note that this use case is exactly the same as primary use case 3, as found under detailed Functional descriptions (see page 73). In this section, the same use case is also explained without an Identity Broker.

4.3.4 Sequence diagram



What needs to be implemented technically for this use case is described generically (see page 100), and specifically per role:

- Service Consumer (see page 119);
- Service Provider (see page 125);
- Entitled Party (see page 119);
- Identity Provider (see page 136);
- Identity Broker (see page 141).

4.4 Use case: delegation (and management of consent)

This use case showcases iSHARE's key functionality 'enable data exchange based on delegations - even between unknown parties (see page 22)'.

The example described in the linked chapter is as follows:

- Party A hires Trucking Company B to deliver Container X to Party C. Trucking Company B's ERP system asks Party C's ERP system at what time it should deliver the container. Party C's ERP system does not know Trucking Company B, but can check the delegation to Trucking Company B that Party A has registered at Authorisation Registry D. Because this delegation is in order, Party C's ERP system shares a time slot with Trucking Company B's ERP.

The following explains this example in detail, utilising the iSHARE framework.

After explanation of the delegation use case, a scenario is introduced that showcases key functionality 'enable control over own data through management of consent (see page 22)'. In this scenario (see page 48), Party C decides to revoke Party A's access to requesting a time slot.

4.4.1 Roles and Relations

The following roles are fulfilled in this use case:

- Delegation takes place, with Party A the party originally entitled to request a time slot. Party A therefore fulfils the **Entitled Party**-role;
- Trucking Company B is delegated the right to request a time slot, so it is the legal entity fulfilling the **Service Consumer**-role;
- Party C responds with the time slot, so it is the legal entity fulfilling the **Service Provider**-role;
- Authorisation Registry D is the **Authorisation Registry** to which Party A has outsourced managing delegation information.

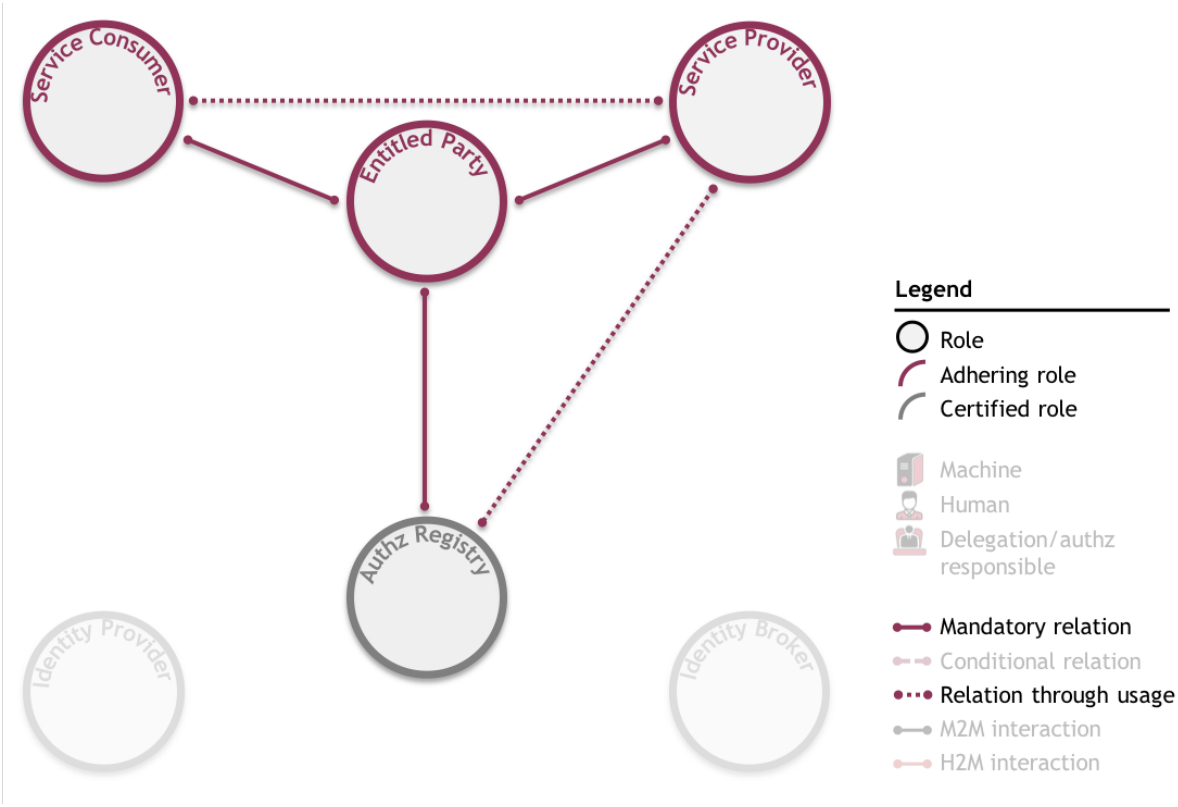
- As this is a M2M use case, a **Machine Service Consumer** represents Trucking Company B.

4.4.1.1 Legal relations

- As always, a mandatory relation between the Entitled Party (Party A) and the Service Provider (Party C) establishes the entitlements of the Entitled Party (Party A);
- A mandatory relation between the Entitled Party (Party A) and the Service Consumer (Trucking Company B) covers the delegation of the right to request a time slot;
- A mandatory relation between the Entitled Party (Party A) and the Authorisation Registry (D) covers the outsourcing of managing delegation information.

- No relation between the Service Consumer (Trucking Company B) and the Service Provider (Party C) is mandatory before service consumption, i.e. the Service Consumer and the Service Provider do not need to know each other. This relation only commences through usage;
- No relation between the Service Provider (Party C) and the Authorisation Registry (D) is mandatory before communication. This relation also commences through usage.

As depicted:

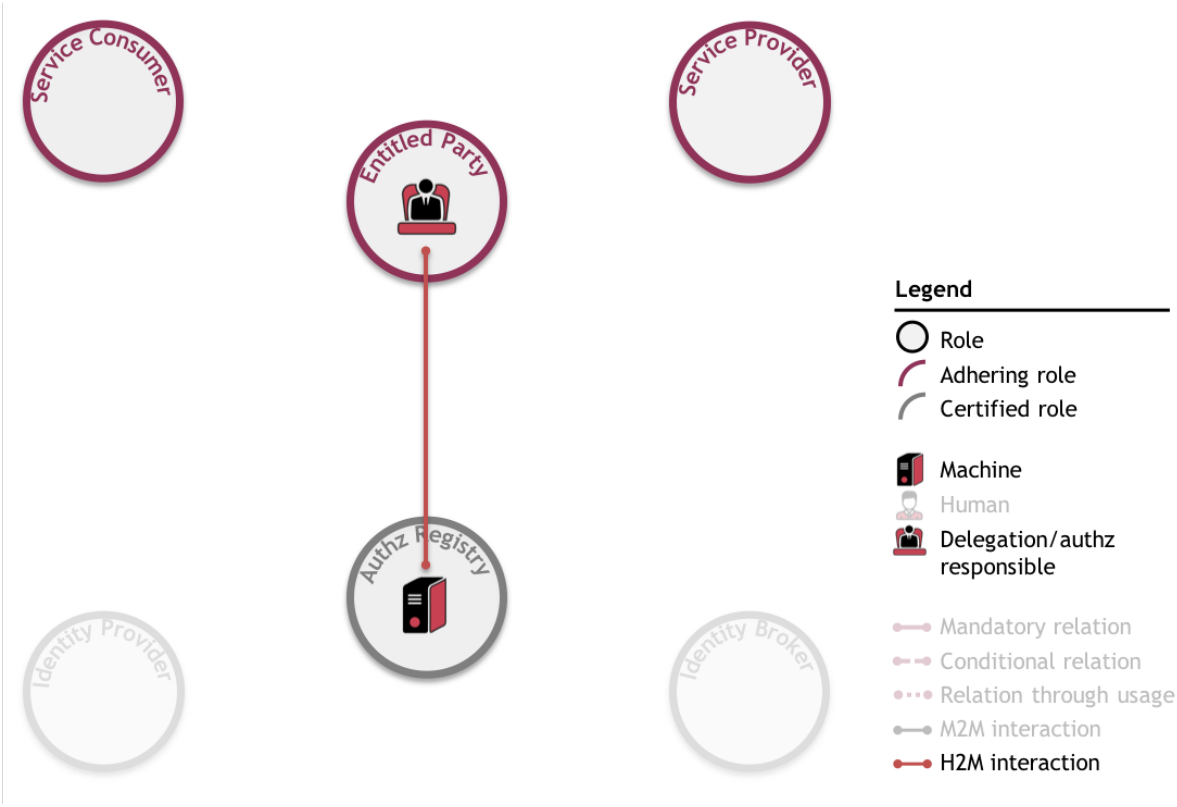


4.4.2 Prerequisites

It is prerequisite of this use case that:

- The Service Provider (Party C) has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services, i.e. Party C has information indicating that Party A is entitled to request a time slot;
- The Service Consumer (Trucking Company B) is able to authenticate the Service Provider (Party C);
- The Service Provider (Party C) is able to authenticate the Service Consumer (Trucking Company B);
- **The delegation/authorisation responsible at the Entitled Party (Party A) delegates (part of) the Entitled Party's (Party A's) rights (as registered at the Service Provider (Party C)) to the Service Consumer (Trucking Company B). He registers this delegation in an Authorisation Registry (D);**
- The Service Provider (Party C) knows which Authorisation Registry (D) to request the delegation evidence from;
- The Service Provider (Party C) is able to authenticate the Authorisation Registry (D);
- The Authorisation Registry (D) is able to authenticate the Service Provider (Party C);
- It is clear, through scheme agreements, under what conditions an Authorisation Registry can provide delegation information to a Service Provider.

The prerequisites in bold are depicted as follows:

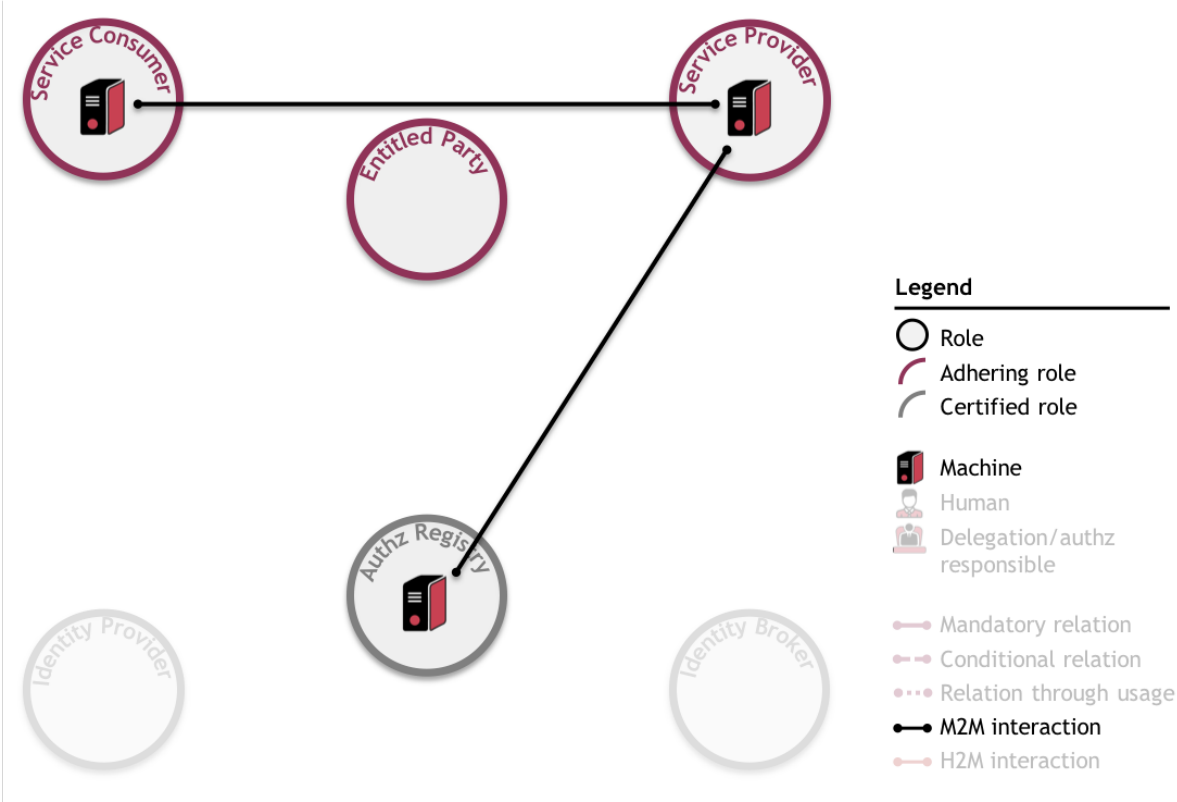


4.4.3 Use case

The use case consists of the following steps:

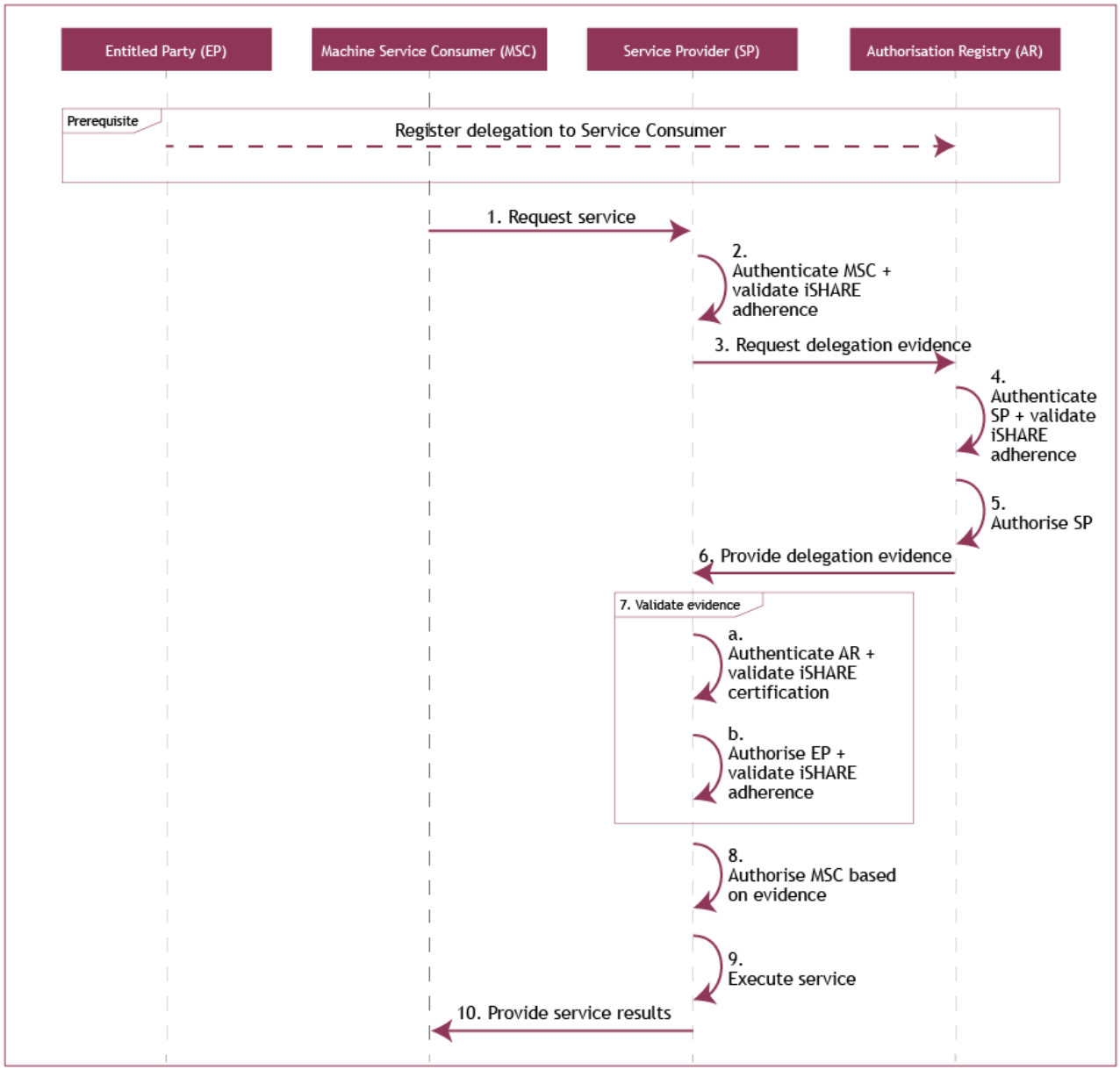
1. The Machine Service Consumer (of Trucking Company B) requests a service from the Service Provider (Party C);
2. The Service Provider (Party C) authenticates the Machine Service Consumer (of Trucking Company B) and validates the iSHARE adherence of the Service Consumer (Trucking Company B);
3. The Service Provider (Party C) requests delegation evidence from the Authorisation Registry (D);
4. The Authorisation Registry (D) authenticates the Service Provider (Party C) and validates its iSHARE adherence;
5. The Authorisation Registry (D) authorises the Service Provider (Party C) based on the scheme agreements for providing delegation information;
6. The Authorisation Registry (D) provides the delegation evidence;
7. The Service Provider (Party C) validates the received delegation evidence through the following steps:
    a. The Service Provider (Party C) authenticates the Authorisation Registry (D) and validates its iSHARE certification;
    b. The Service Provider (Party C) authorises the Entitled Party (Party A) based on the entitlement information registered with the Service Provider (Party C), and validates its iSHARE adherence.
8. The Service Provider (Party C) authorises the Machine Service Consumer of the Service Consumer (Trucking Company B) based on the validity of the delegation evidence;
9. The Service Provider (Party C) executes the requested service;
10. The Service Provider (Party C) provides the service result to the Machine Service Consumer (of Trucking Company B).

As depicted:



Note that this use case is exactly the same as derived use case 1c, as found under detailed Functional descriptions (see page 63). This section also includes delegation use cases with delegation information held by other roles than an Authorisation Registry.

4.4.4 Sequence diagram



4.4.5 Alternative scenario on management of consent

This alternative scenario showcases key functionality 'enable control over own data through management of consent (see page 22)'.

The example detailed in the above is as follows:

- Party A hires Trucking Company B to deliver Container X to Party C. Trucking Company B's ERP system asks Party C's ERP system at what time it should deliver the container. Party C's ERP system does not know Trucking Company B, but can check the delegation to Trucking Company B that Party A has registered at

Authorisation Registry D. Because this delegation is in order, Party C's ERP system shares a time slot with Trucking Company B's ERP.

Now imagine:

- Moments before Trucking Company B's ERP system asks Party C's ERP system for a time slot, Party C decides to revoke Party A's access to requesting a time slot. Consequently, Trucking Company B's request for a time slot gets an access forbidden message; Trucking Company B's request is NOT accepted because Party A, and therewith delegated Trucking Company B, is no longer authorised to ask for a time slot.

4.4.5.1 Prerequisites

To the prerequisites, ONLY the following changes:

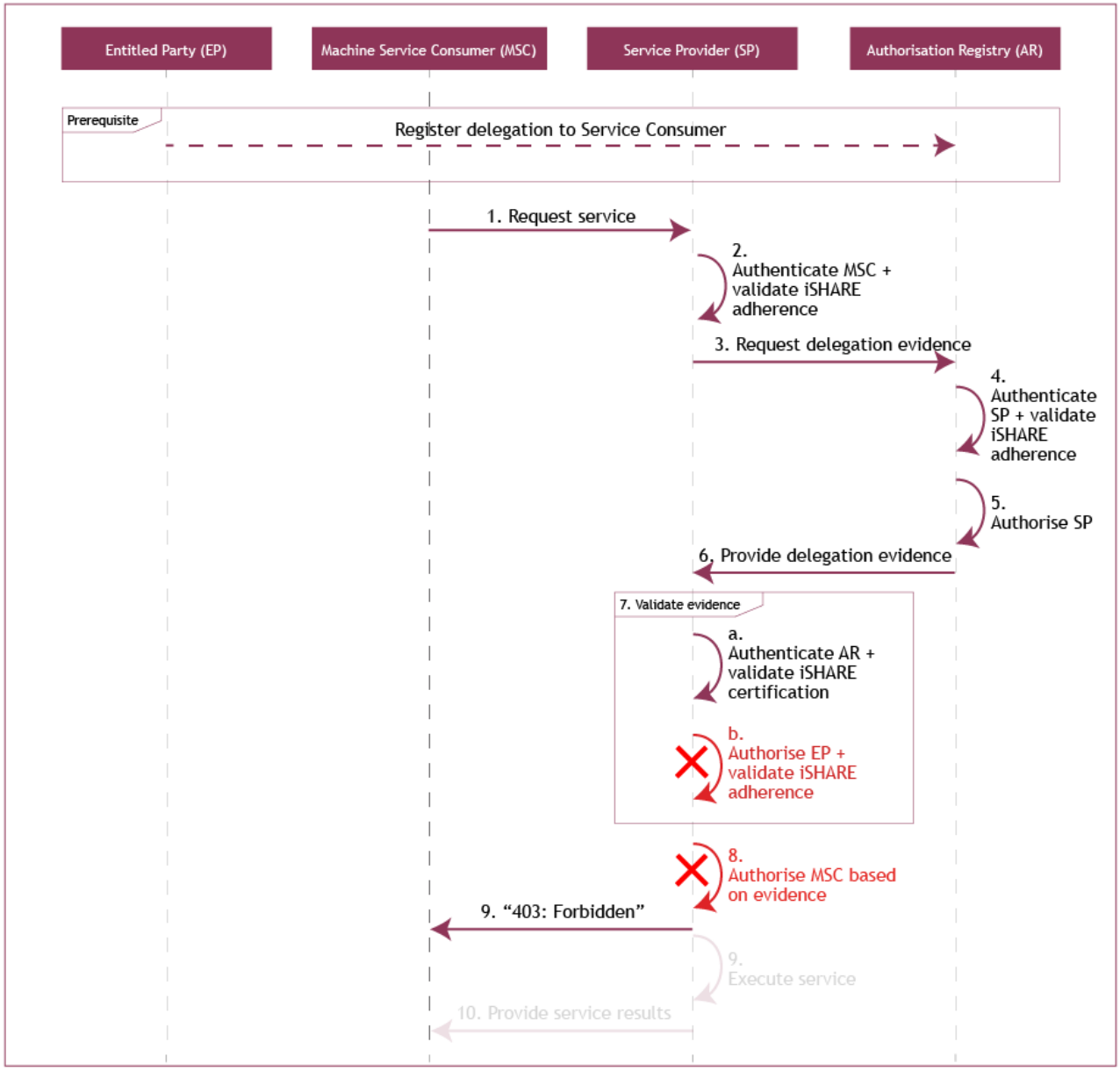
- The Service Provider (Party C) changes its entitlement information indicating what Entitled Parties are entitled to what (parts of) services, i.e. Party C deletes the information indicating that Party A is entitled to request a time slot.

4.4.5.2 Use case

The alternative use case consists of the following steps, with changes to the above use case in bold:

1. The Machine Service Consumer (of Trucking Company B) requests a service from the Service Provider (Party C);
2. The Service Provider (Party C) authenticates the Machine Service Consumer (of Trucking Company B) and validates the iSHARE adherence of the Service Consumer (Trucking Company B);
3. The Service Provider (Party C) requests delegation evidence from the Authorisation Registry (D);
4. The Authorisation Registry (D) authenticates the Service Provider (Party C) and validates its iSHARE adherence;
5. The Authorisation Registry (D) authorises the Service Provider (Party C) based on the scheme agreements for providing delegation information;
6. The Authorisation Registry (D) provides the delegation evidence;
7. The Service Provider (Party C) validates the received delegation evidence through the following steps:
    a. The Service Provider (Party C) authenticates the Authorisation Registry (D) and validates its iSHARE certification;
    b. **The Service Provider (Party C) CANNOT authorise the Entitled Party (Party A) based on the entitlement information registered with the Service Provider (Party C)**
8. **The Service Provider (Party C) CANNOT authorise the Machine Service Consumer of the Service Consumer (Trucking Company B) based on the validity of the delegation evidence;**
9. **The Service Provider (Party C) communicates an access forbidden message to the Machine Service Consumer (of Trucking Company B).**

4.4.5.3 Sequence diagram



What needs to be implemented technically for this use case (and the alternative scenario) is described generically (see page 100), and specifically per role:

- Service Consumer (see page 119);
- Service Provider (see page 125);
- Entitled Party (see page 119);
- Authorisation Registry (see page 141).

5 Detailed descriptions

This chapter provides an in depth overview of all the Functional, Technical, Operational and Legal details of the iSHARE scheme. The following chapters are present in this section:

5.1 Functional

This section details iSHARE's functionality.

The use cases depicted in earlier chapters (see page 31) are only a selection of iSHARE's full use case scope. This scope is based on three 'primary' use cases (see page 51):

1. Machine to Machine service provision;
2. Human to Machine service provision with authorisation and identity info held at the Service Provider;
3. Human to Machine service provision with identity info held at the Identity Provider.

These primary use cases have several 'derived' use cases which cover all possible uses.

The primary use cases are supported by 'secondary' use cases (see page 91), that include processes related to registration, and processes that recur in primary use cases. This section is concluded by functional requirements - those per role in the scheme (see page 96) and those to the iSHARE user interface (see page 99) in H2M use cases.

5.1.1 Primary use cases

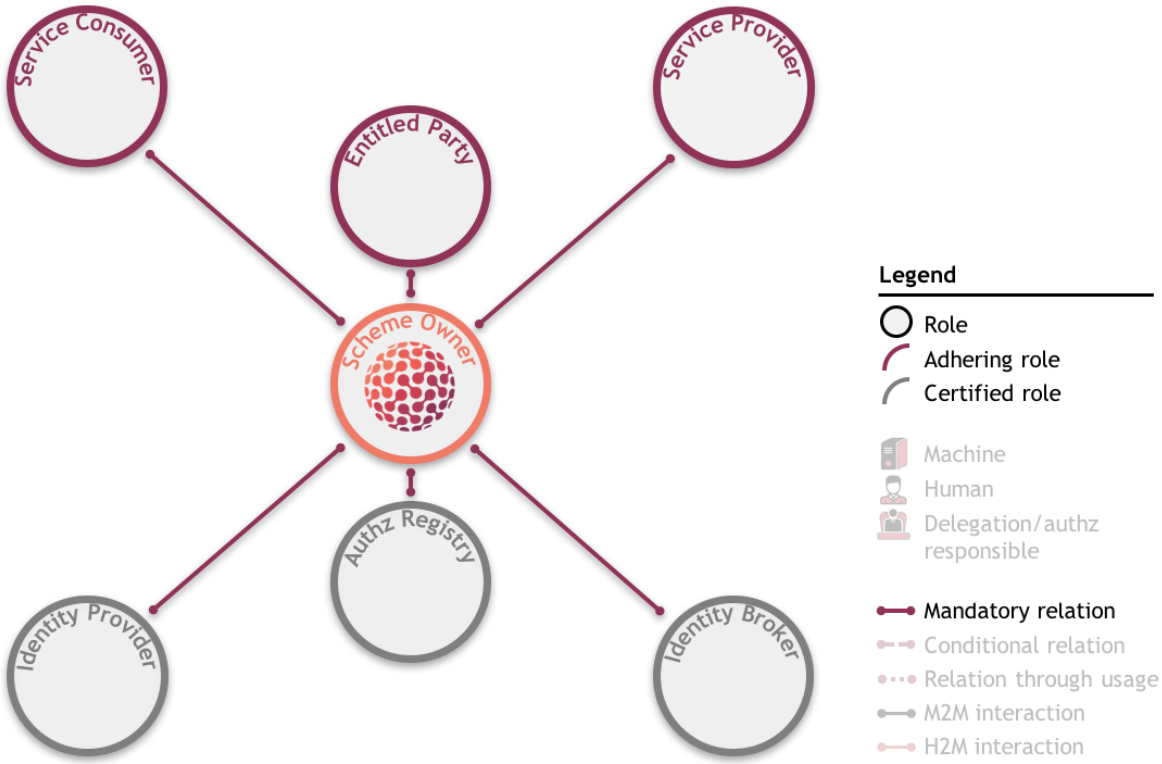
This most important part of the Functional descriptions explains the following in detail:

- The iSHARE framework, including the Scheme Owner and and what role can hold what types of information;
- The three primary use cases: Machine to Machine, Human to Machine with authorisation info and identity info held at the Service Provider, and Human to Machine with identity info held at an Identity Provider;
- The possible variations to the three primary use cases, depending on where identity information, authorisation information and/or delegation information is held.

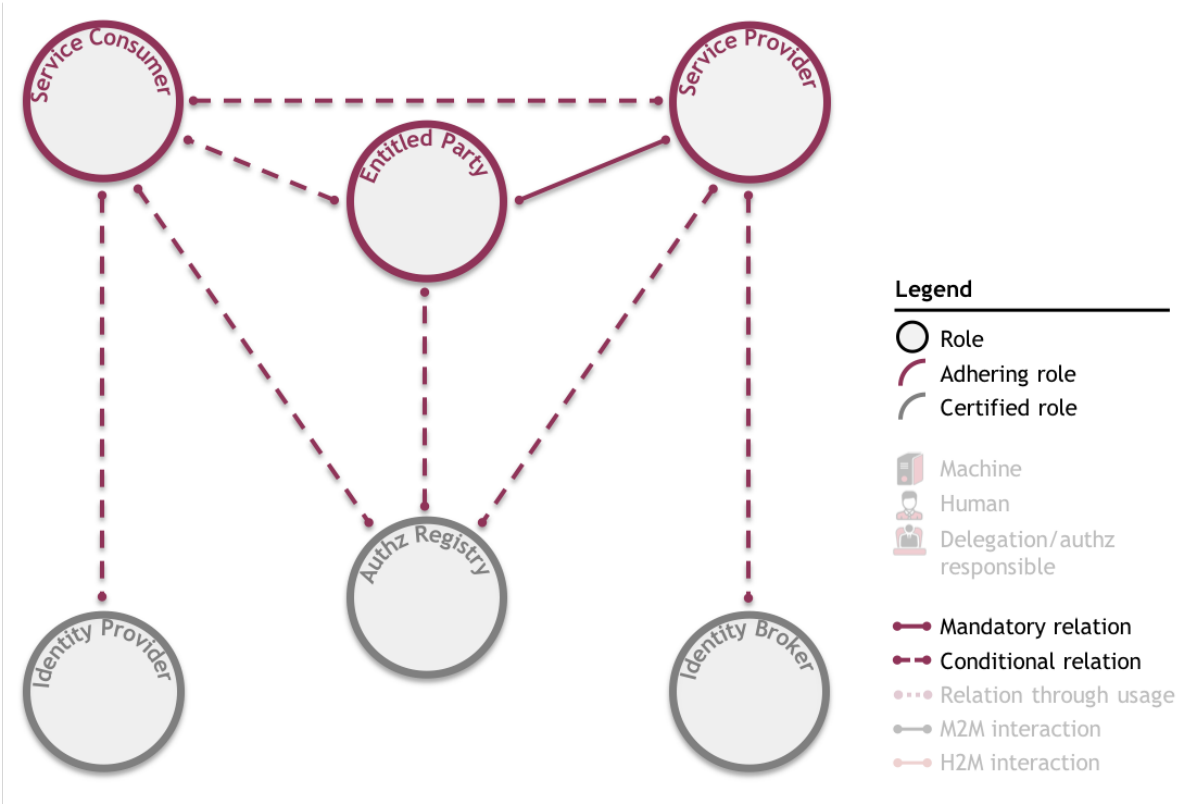
5.1.1.1 iSHARE framework

The iSHARE framework was explained under use cases (see page 24). It consists of six roles that, depending on the situation, interact with each other based on the iSHARE scheme agreements. Each role has a certain function in the scheme and bears certain responsibilities. To fulfil a other role in the framework, a party must fulfil specific admittance criteria, as explained.

What was not explained under use cases was how the iSHARE and the Scheme Owner-role provide a trust framework. The Scheme Owner-role is fulfilled by the legal entity that governs the iSHARE scheme and its participant network. It is this Scheme Owner that decides whether a party is admitted to the iSHARE network. To be admitted, this party must sign an agreement with the Scheme Owner. The fact that every legal entity fulfilling a role in the iSHARE scheme agrees to the scheme rules - as proven by its agreement with the Scheme Owner - creates trust between parties in the iSHARE network. This is why the following depiction of the iSHARE framework, showing the mandatory relation between the Scheme Owner and every other role, can be called the **trust framework**:



In order to know whether a party is an iSHARE participant before sharing data with it, the Scheme Owner can be asked about this party's adherence/certification (as detailed in secondary use case 5a (see page 91)). This and the trust framework as a whole are not reflected in the primary use cases because *every relation or interaction* within iSHARE is build upon the trust framework. The framework used to depict use cases was already presented as follows:



It was stated that all of iSHARE's use cases can be depicted in the above framework.

Their complexity is dependent on:

- The interaction model (Machine to Machine or Human to Machine);
  i.e. whether the Service Consumer is represented by a machine or a human.
- Whether delegation takes place, and;
  i.e. whether the Service Consumer-role is fulfilled by another entity than the Entitled Party-role. How delegations work exactly is explained here (see page 94).
- Whether parties fulfilling adhering roles use their own tooling for identification, authentication, and authorisation or outsource these processes and the information necessary for these processes to certified roles instead.

Zooming in on the latter, four types of information are recognised that are needed to facilitate identification, authentication and authorisation (see page 9):

- **Entitlement info:** information indicating what Entitled Parties[17] are entitled to what (parts of) services;
- **Delegation info:** information indicating which (parts of) an Entitled Party's rights (as registered at the Service Provider or the Authorisation Registry) are delegated to a Service Consumer;
- **Authorisation info:** information indicating which Human Service Consumers are authorised to act on a Service Conumer's behalf;
- **Identity info:** information about a Human Service Consumer's identity (only applicable in H2M use cases).

17 https://innopay.atlassian.net/wiki/spaces/IS/pages/53954734/Entitled+Party

All complexity can be brought back to three primary use cases, with 21 variations.

5.1.1.2 Three primary use cases

1. Machine to Machine service provision;
   Primary use case 1 caters to all Machine to Machine cases.
2. Human to Machine service provision with authorisation and identity info held at the Service Provider;
   Primary use case 2 caters to all Human to Machine cases where the Service Provider resides over both identity information and authorisation information. He has not outsourced identification, authentication and authorisation, and therefore does not need to consult certified parties
3. Human to Machine service provision with identity info held at the Identity Provider.
   Primary use case 3 caters to all Human to Machine cases where identity information is held at an Identity Provider. The Service Provider has outsourced identification and authentication, and therefore needs to consult the Identity Provider.

5.1.1.3 Derived use cases

The primary use cases all know a variety of derived use cases. Derived use cases are variations of the primary use cases in which delegation- and authorisation information required by the Service Provider is held by (i.e. outsourced to) and retrieved from different parties. In technical terms, we call the party holding information a **Policy Information Point (PIP).** This PIP, as in XACML 3.0 (see page 115), acts as the source of the information. There are different use case variations for different PIPs for delegation- and/or authorisation information, as presented in the use case tables below. Note that entitlement info is always held by the Service Provider which is (consequently) not depicted in the tables below.

The Service Provider requests (from the PIP(s)) and evaluates the information required to decide whether or not to grant a Service Consumer access to a service. After making its decision based on the received information, it grants this access (or not) to the Service Consumer. Technically, the Service Provider therefore acts as **Policy Enforcement Point (PEP)** *and* **Policy Decision Point (PDP)** in all use cases.

Primary use case 1 (and derived use cases)*: M2M service provision

Use case initiated by the Machine Service Consumer

	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Derived use cases**	1 (see page 56)	1a	1b (see page 59)	1c (see page 63)

*Use case 1 and its variations can also be initiated by a Human Service Consumer through an app. In such case, the Machine Service Consumer acts as a proxy between the Human Service Consumer and the Service Provider's machine as described here (see page 67).

**Primary use case 1 assumes that authorisation information is always present in a valid token used by the Machine Service Consumer. Therefore primary use case 1 has no derived use cases where authorisation information is retrieved from other parties.

Note that interaction sequences are not described in the table above. In derived use cases 1b and 1c, several interaction sequences are possible depending on who requests delegation info from the PIP. If the Entitled Party is the delegation info PIP:

1. The Service Provider can request delegation info after a service request from the Service Consumer;
2. The Machine Service Consumer can request delegation info and include it in its service request to the Service Provider;
3. The Entitled Party can push delegation info to the Machine Service Consumer, so it can include it in its service request to the Service Provider.

If the Authorisation Registry is the delegation info PIP:

1. The Service Provider can request delegation info after a service request from the Service Consumer;
2. The Machine Service Consumer can request delegation info and include it in its service request to the Service Provider.

Use case 1 only has one interaction pattern as there is no delegation info PIP. Derived use case 1a also has one interaction pattern as the Service Provider is the Delegation info PIP and therefore already has the delegation info it needs.

Primary use case 2 (and derived use cases): H2M service provision with authorisation info and identity info held at the SP

Use case initiated by the Human Service Consumer

		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	2 (see page 69)	2a	2b	2c

Primary use case 3 (and derived use cases): H2M service provision with identity info held at the IDP

Use case initiated by the Human Service Consumer

		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	3 (see page 73)	3a	3b	3c
	Entitled Party	3.1	3a.1	3b.1	3c.1
	Authorisation Reg	3.2 (see page 81)	3a.2	3b.2	3c.2 (see page 85)
	Identity Provider*	3.3	3a.3	3b.3	3c.3

*The Identity Provider cannot hold explicit authorisation info, but it can hold info about a Human Service Consumer's identity that implies authorisation - i.e. 'working for truck company X'

Note again that interaction sequences are not described in the tables above. A Human Service Consumer cannot include delegation (or authorisation) info in its service request to the Service Provider. In use cases 2 and 3 (and derived use cases), therefore, the Service Provider will always request delegation- and/or authorisation info from the respective PIP(s) after a service request from the Human Service Consumer.

Several interaction sequences are still theoretically possible depending on who requests a login from the Identity Provider. During the Functional working groups, however, it appeared that in practice, a Human Service Consumer will never request login from an Identity Provider before requesting a service from the Service Provider. Until proven otherwise, therefore, the only interaction sequence in scope for use cases 2 and 3 (and derived use cases) is the one in which the Service Provider (also) requests login from the Identity Provider after a service request from the Human Service Consumer.

In use case 3 (and derived use cases), an Identity Broker[18] can be introduced to broker the relation between the Service Provider and the Identity Provider(s) and/or the Service Provider and the Authorisation Registry(s). This is optional and useful in situations with several Identity Providers and/or Authorisation Registries. Use case 3 (see page 73) is detailed both without an Identity Broker and with one, while derived use cases 3.2 (see page 81) and 3c.2 (see page 85) both include an Identity Broker.

5.1.1.4 Rest of this section

Please note that all use cases that contain a hyperlink (in their respective tables) are detailed on their own page - as follows:

- Roles;
- Depiction of legal relations, prerequisite registration and use case interaction;
- Description of prerequisites and use case interaction;
- Sequence diagram.

For both use case 2 and 3 (and derived use cases), an interface is required. Requirements to this interface are summarised here (see page 99).

5.1.1.5 1. M2M service provision

In use case 1, a service is provided by the Service Provider to the Machine Service Consumer.

Roles

	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Use case variation	1 (see page 56)	1a	1b (see page 59)	1c (see page 63)

As no delegation takes place, the legal entity fulfilling the Entitled Party-role also fulfils the Service Consumer-role.

18 https://innopay.atlassian.net/wiki/spaces/IS/pages/49741978/Identity+Broker

Depiction

Legal relations

Use case interaction

Description

It is prerequisite of this use case that:

- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Service Consumer.

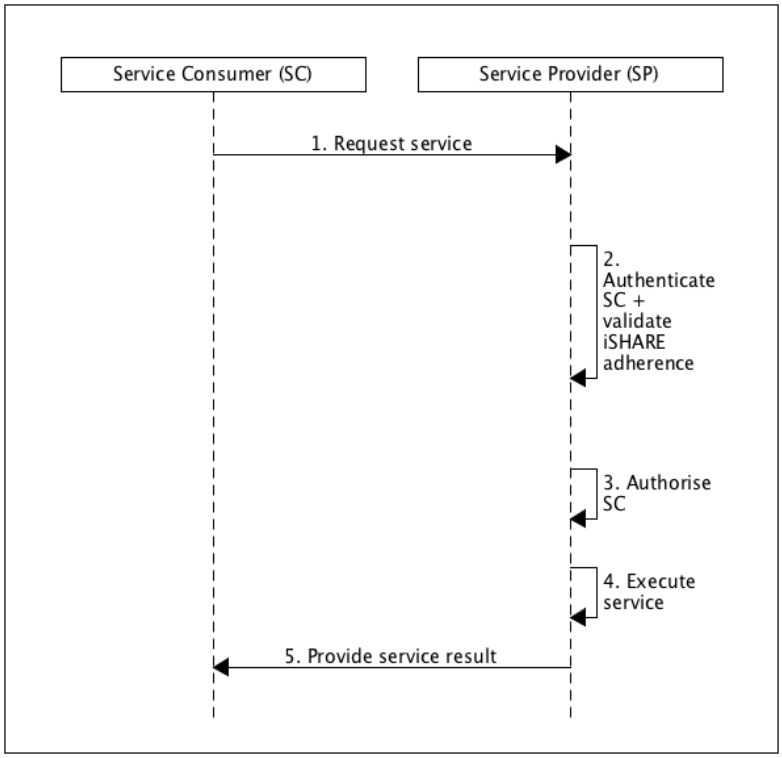
- In this use case the Entitled Party is also the Service Consumer.

*The Service Provider can outsource this function to a third party

The use case consists of the following steps:

1. The Machine Service Consumer requests a service from the Service Provider;
2. The Service Provider authenticates the Machine Service Consumer and validates the iSHARE adherence of the Service Consumer;
3. The Service Provider authorises the Machine Service Consumer of the Service Consumer based on the entitlement information registered with the Service Provider;
4. The Service Provider executes the requested service;
5. The Service Provider provides the service result to the Machine Service Consumer.

Sequence diagram



1b. M2M service provision with the EP as the delegation info PIP

In use case 1b, a service is provided by the Service Provider to the Machine Service Consumer. The Service Consumer has been delegated by the Entitled Party.

Roles

	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Use case variation	1 (see page 56)	1a	1b (see page 59)	1c (see page 63)

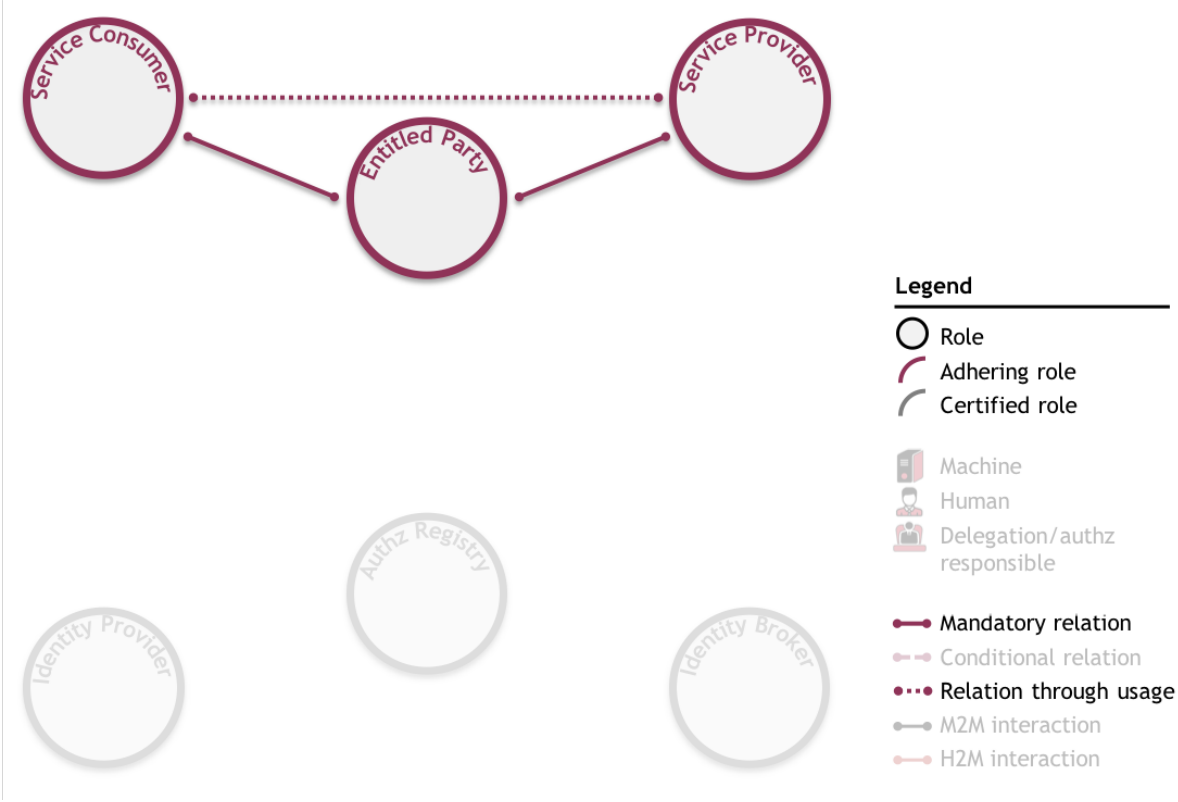
Note that interaction sequences are not described in the table above. In derived use case 1b, three interaction sequences are possible depending on who requests delegation info from the PIP:

1. The Service Provider can request delegation info after a service request from the Service Consumer;
2. The Machine Service Consumer can request delegation info and include it in its service request to the Service Provider;
3. The Entitled Party can push delegation info to the Machine Service Consumer, so it can include it in its service request to the Service Provider.

Interaction sequence 3 is detailed below.

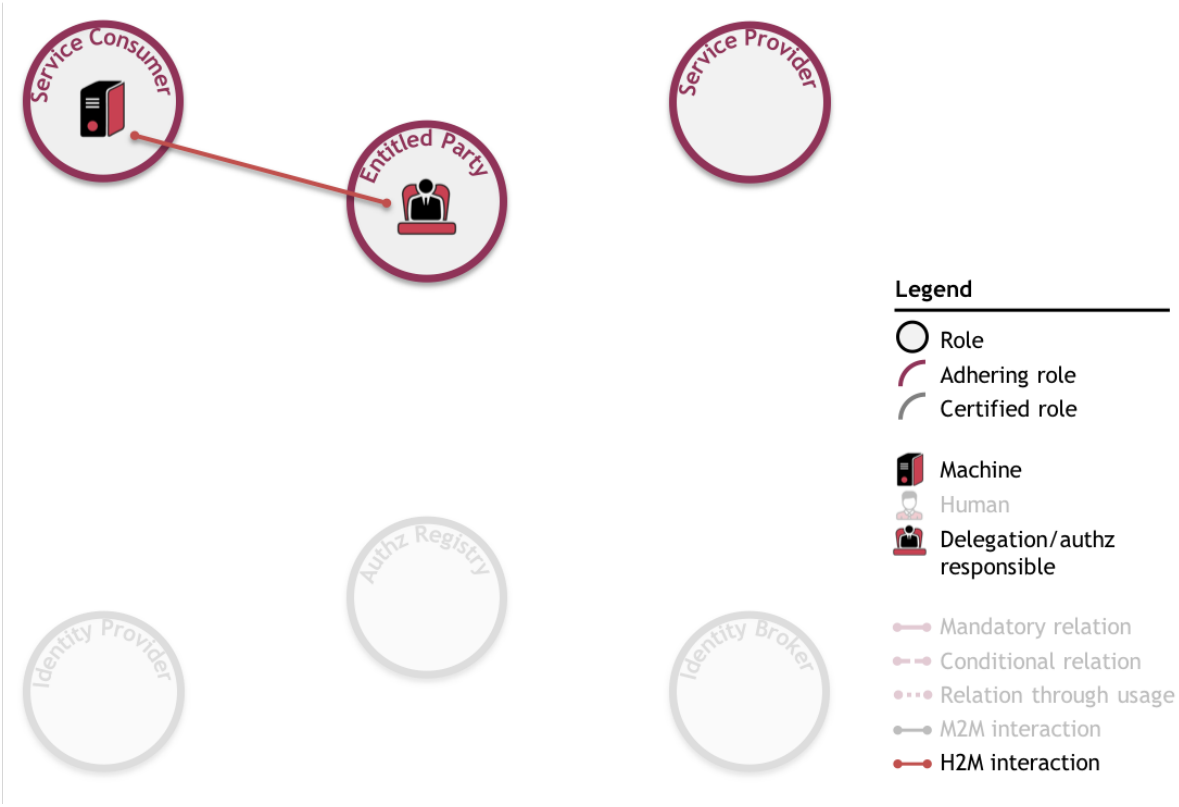
Depiction

Legal relations

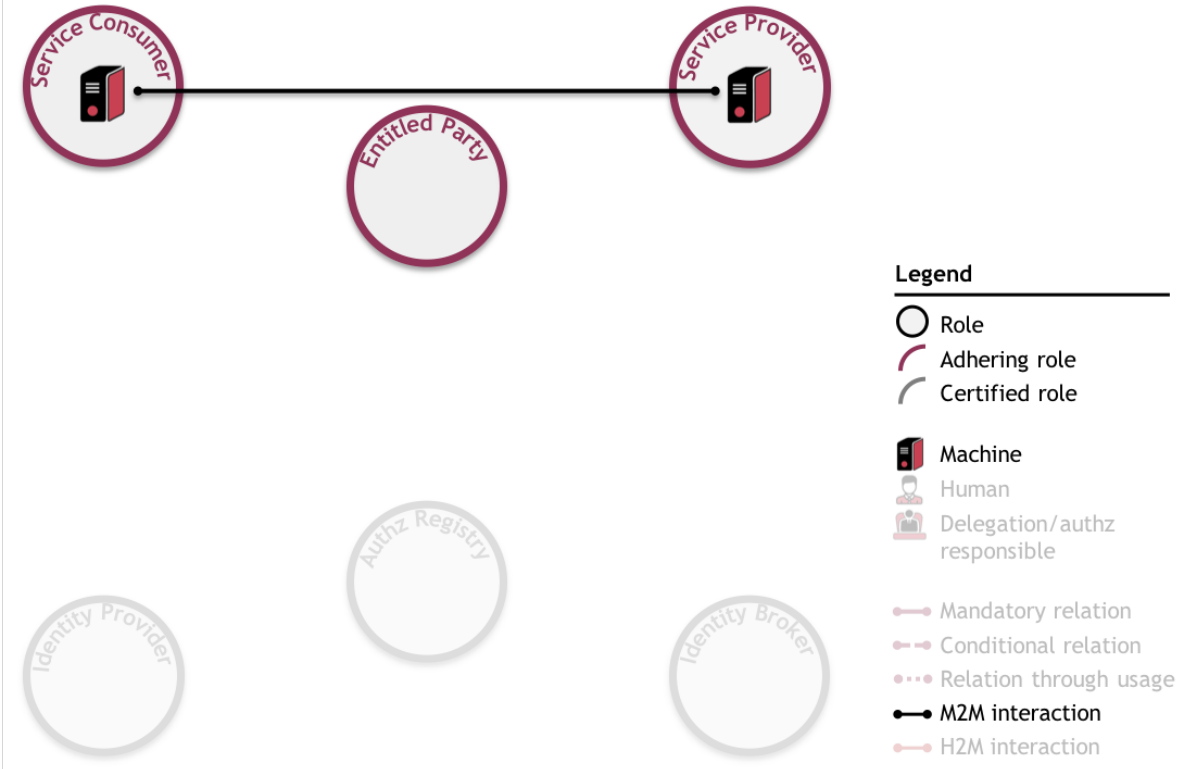


Note that no prior legal relation exists between the Service Consumer and the Service Provider. Which services can be consumed by the Service Consumer, as delegated by the Entitled Party, is set out in the mandatory relation between this Entitled Party and the Service Provider.

Prerequisite registration



Use case interaction



Description

It is prerequisite of this use case that:

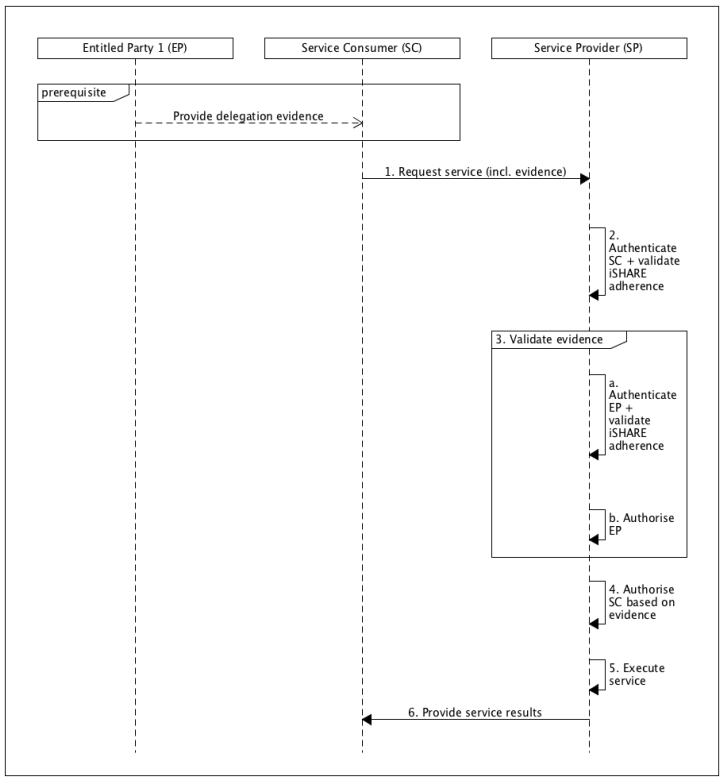
- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Service Consumer;
- The delegation/authorisation responsible at the Entitled Party delegates (part of) the Entitled Party's rights (as registered at the Service Provider) to the Service Consumer. He provides the Machine Service Consumer of the Service Consumer with evidence of this delegation.

*The Service Provider can outsource this function to a third party

The use case consists of the following steps:

1. The Machine Service Consumer requests a service from the Service Provider. With this requests it includes the evidence obtained from the Entitled Party;
2. The Service Provider authenticates the Machine Service Consumer and validates the iSHARE adherence of the Service Consumer;
3. The Service Provider validates the received delegation evidence through the following steps:
    a. The Service Provider authenticates the Entitled Party and validates its iSHARE adherence based on the delegation evidence;
    b. The Service Provider authorises the Entitled Party based on the entitlement information registered with the Service Provider.
4. The Service Provider authorises the Machine Service Consumer of the Service Consumer based on the validity of the delegation evidence;
5. The Service Provider executes the requested service;
6. The Service Provider provides the service result to the Machine Service Consumer.

Sequence diagram



1c. M2M service provision with the AR as the delegation info PIP

In use case 1c, a service is provided by the Service Provider to the Service Consumer. The Service Consumer has been delegated by the Entitled Party, and delegation evidence is registered at an Authorisation Registry.

Roles

	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Use case variation	1 (see page 56)	1a	1b (see page 59)	1c (see page 63)

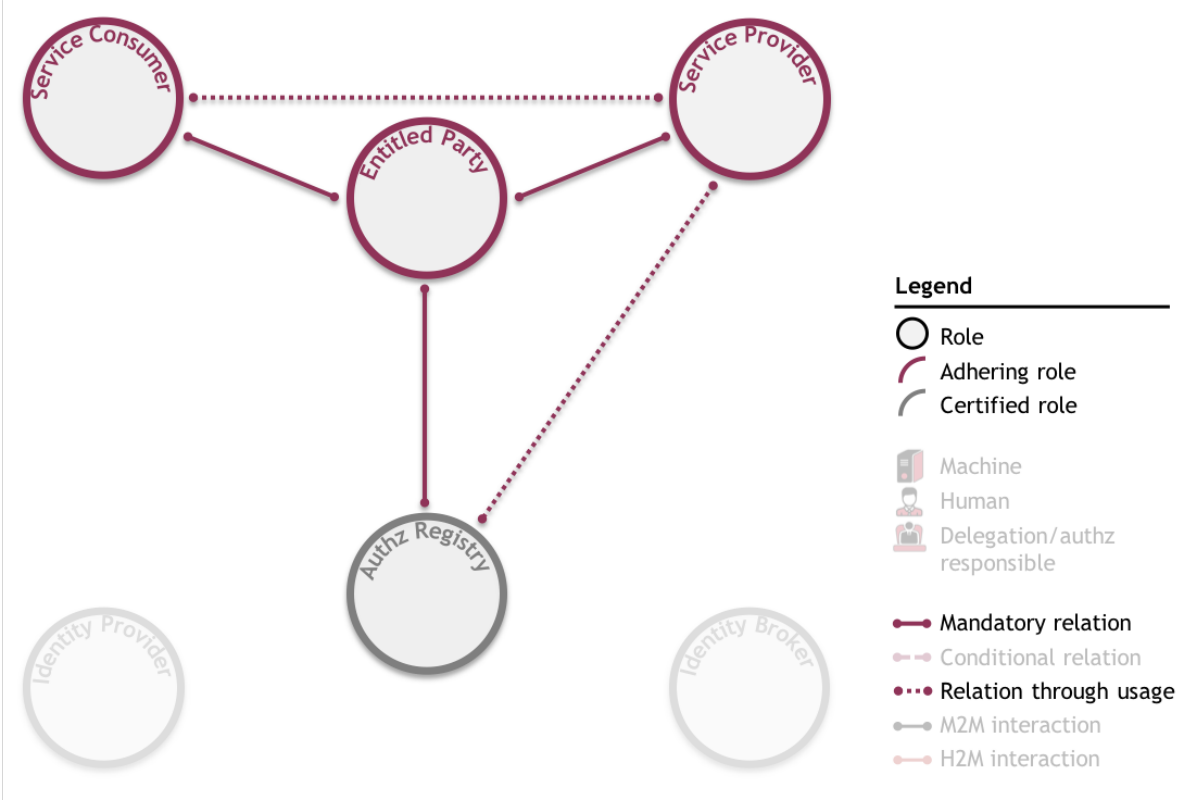
Note that interaction sequences are not described in the table above. In derived use case 1c, two interaction sequences are possible depending on who requests delegation info from the PIP:

1. The Service Provider can request delegation info after a service request from the Service Consumer;
2. The Machine Service Consumer can request delegation info and include it in its service request to the Service Provider.

Interaction sequence 1 is detailed below.

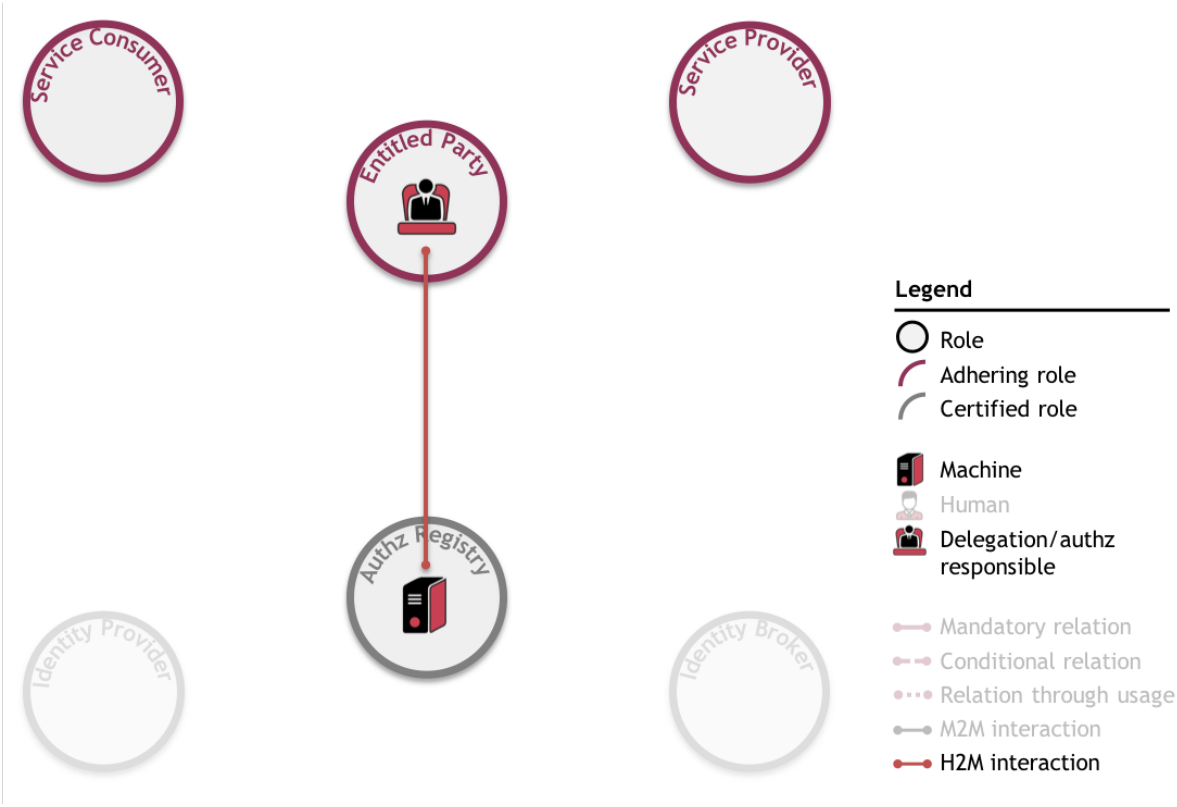
Depiction

Legal relations

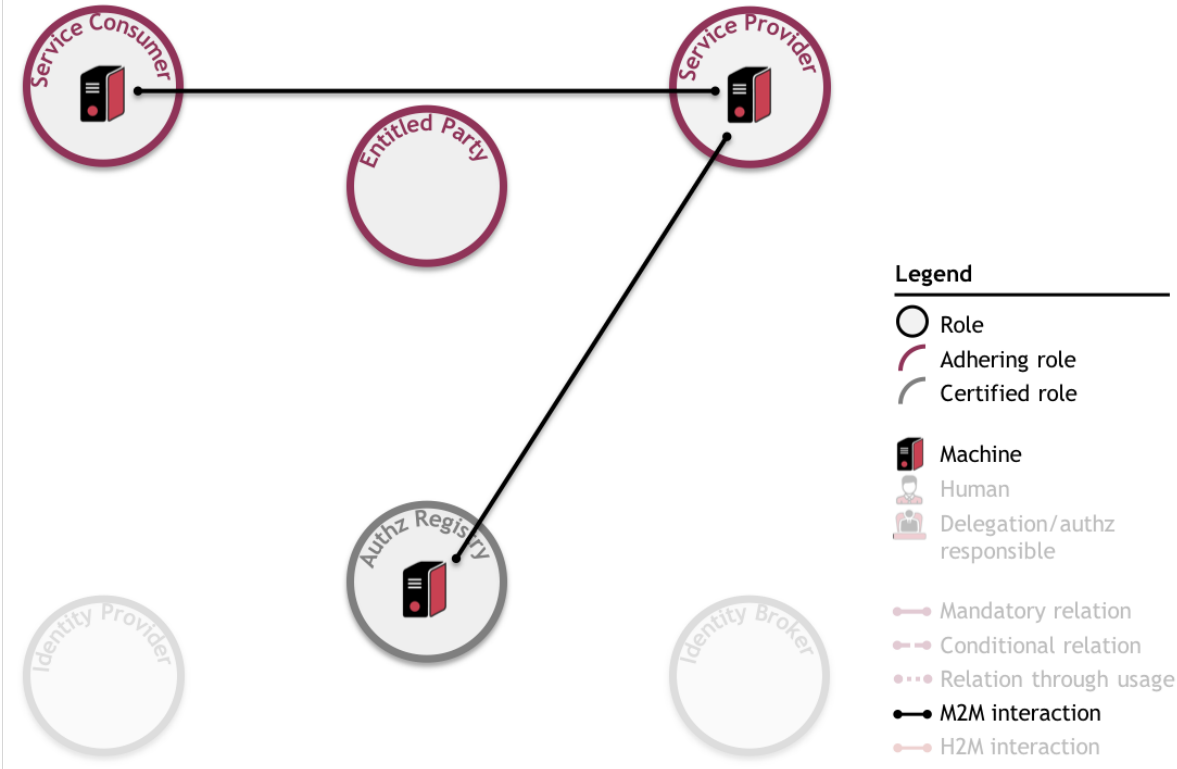


Note that no prior legal relation exists between the Service Consumer and the Service Provider. Which services can be consumed by the Service Consumer, as delegated by the Entitled Party, is set out in the mandatory relation between this Entitled Party and the Service Provider.

Prerequisite registration



Use case interaction



Description

It is prerequisite of this use case that:

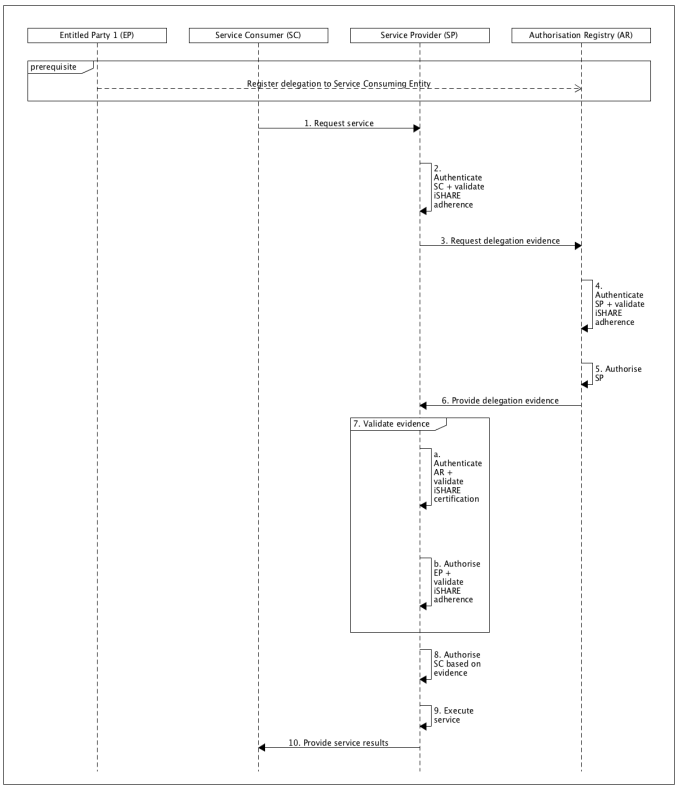
- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Service Consumer;
- The delegation/authorisation responsible at the Entitled Party delegates (part of) the Entitled Party's rights (as registered at the Service Provider) to the Service Consumer. He registers this delegation in an Authorisation Registry;
- The Service Provider knows which Authorisation Registry to request the delegation evidence from;
- The Service Provider is able to authenticate the Authorisation Registry;
- The Authorisation Registry is able to authenticate the Service Provider;
- It is clear, through scheme agreements, under what conditions an Authorisation Registry can provide delegation information to a Service Provider.

*The Service Provider can outsource this function to a third party

The use case consists of the following steps:

1. The Machine Service Consumer requests a service from the Service Provider;
2. The Service Provider authenticates the Machine Service Consumer and validates the iSHARE adherence of the Service Consumer;
3. The Service Provider requests delegation evidence from the Authorisation Registry;
4. The Authorisation Registry authenticates the Service Provider and validates its iSHARE adherence;
5. The Authorisation Registry authorises the Service Provider based on the scheme agreements for providing delegation information;
6. The Authorisation Registry provides the delegation evidence;
7. The Service Provider validates the received delegation evidence through the following steps:
    a. The Service Provider authenticates the Authorisation Registry and validates its iSHARE certification;
    b. The Service Provider authorises the Entitled Party based on the entitlement information registered with the Service Provider, and validates its iSHARE adherence.
8. The Service Provider authorises the Machine Service Consumer of the Service Consumer based on the validity of the delegation evidence;
9. The Service Provider executes the requested service;
10. The Service Provider provides the service result to the Machine Service Consumer.

Sequence diagram



M2M service provision including an app

Use case 1 and its variations can be initiated by a Human Service Consumer through an app. In such case, the Machine Service Consumer acts as a proxy between the Human Service Consumer and the Service Provider's machine.

Roles

	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Use case variation	1 (see page 56)	1a	1b (see page 59)	1c (see page 63)

Depiction

Legal relations

Use case interaction

Description

As to use case 1, it is prerequisite of this use case that:

- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Service Consumer.

- In this use case the Entitled Party is also the Service Consumer.

*The Service Provider can outsource this function to a third party

The use case consists of the following steps:

- The Human Service Consumer uses an app to request a service at the Machine Service Consumer - the Human Service Consumer's identity is included in the request;
- The request is mapped to a service request;

1. The Machine Service Consumer requests a service from the Service Provider;
2. The Service Provider authenticates the Machine Service Consumer and validates the iSHARE adherence of the Service Consumer;
3. The Service Provider authorises the Machine Service Consumer of the Service Consumer based on the entitlement information registered with the Service Provider;
4. The Service Provider executes the requested service;
5. The Service Provider provides the service result to the Machine Service Consumer;

- The Human Service Consumer accesses the result through app.

5.1.1.6 2. H2M service provision with identity info at the SP

In use case 2, a service is provided by the Service Provider to the Human Service Consumer. Identity info is held at the Service Provider.

Roles

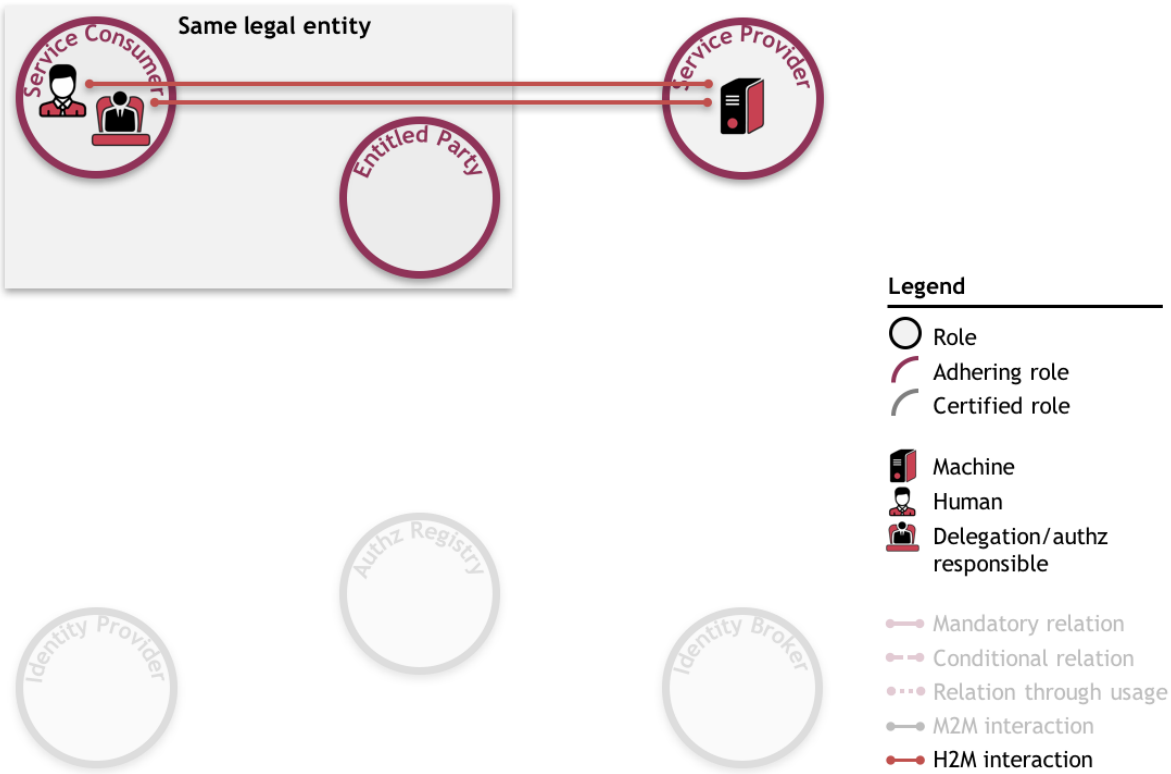
		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	2 (see page 69)	2a	2b	2c

As no delegation takes place, the legal entity fulfilling the Entitled Party-role also fulfils the Service Consumer-role.

Depiction

Legal relations

Prerequisite registration



Use case interaction

Description

It is prerequisite of this use case that:

- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**;
- The delegation/authorisation responsible at the the Service Consumer registers the authorisation information at the Service Provider;
- The Human Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Human Service Consumer;
- The Human Service Consumer has been issued identity credentials by the Service Provider.

- In this use case the Entitled Party is also the Service Consumer.

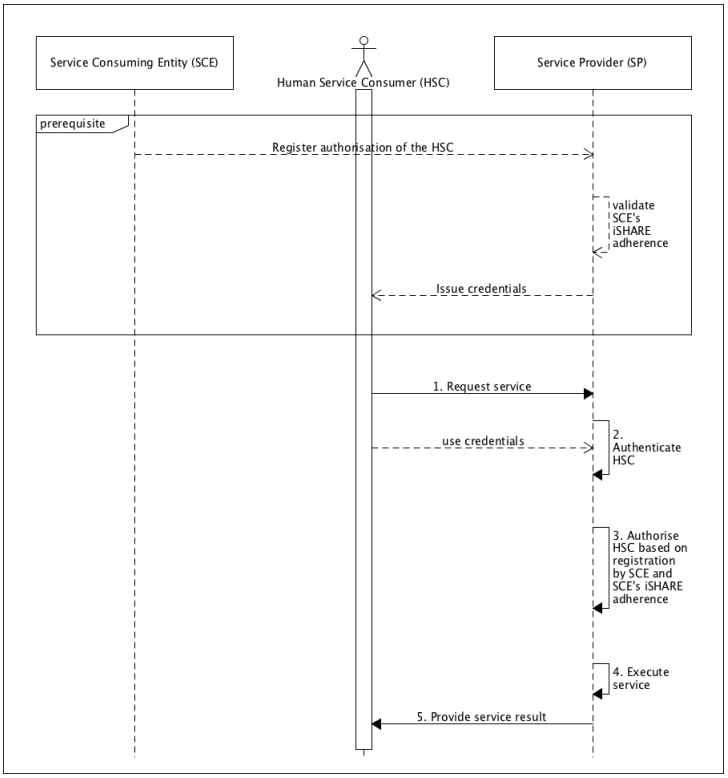
*The Service Provider can outsource this function to a third party
**The Service Consumer can outsource this function to a third party

The use case consists of the following steps:

1. The Human Service Consumer requests a service from the Service Provider;
2. The Service Provider authenticates the Human Service Consumer, and validates the iSHARE adherence of the Service Consumer;

3. The Service Provider authorises the Human Service Consumer of the Service Consumer based on the entitlement- and authorisation information registered with the Service Provider;;
4. The Service Provider executes the requested service;
5. The Service Provider provides the service result to the Human Service Consumer.

Sequence diagram



5.1.1.7 3. H2M service provision with identity info at the IP

In use case 3, a service is provided by the Service Provider to the Human Service Consumer. Identity info is held at the Identity Provider.

Roles

		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	3 (see page 73)	3a	3b	3c
	Entitled Party	3.1	3a.1	3b.1	3c.1
	Authorisation Reg	3.2 (see page 81)	3a.2	3b.2	3c.2 (see page 85)

	Identity Provider*	3.3	3a.3	3b.3	3c.3

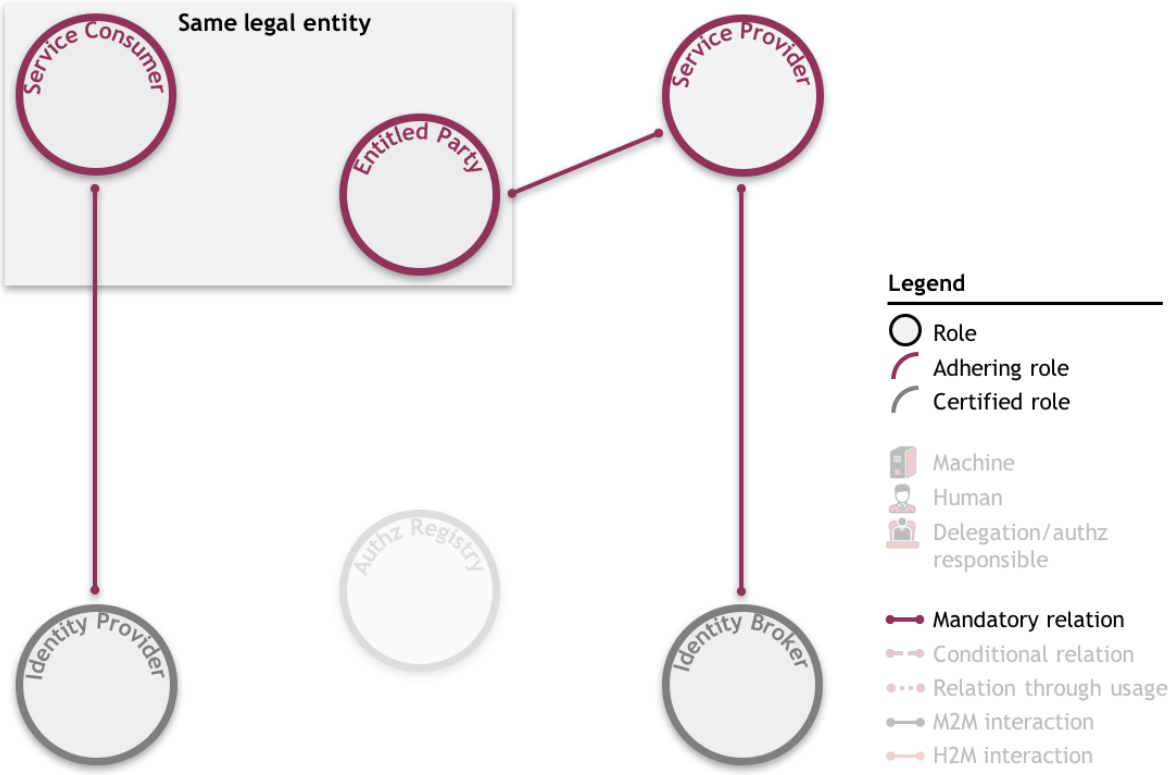
*The Identity Provider cannot hold explicit authorisation info, but it can hold info about a Human Service Consumer's identity that implies authorisation - i.e. 'working for truck company X'

As no delegation takes place, the legal entity fulfilling the Entitled Party-role also fulfils the Service Consumer-role.

Note that an Identity Broker[19] is introduced to broker the relation between the Service Provider and the Identity Provider(s) and/or the Service Provider and the Authorisation Registry(s). This is optional and useful in situations with several Identity Providers and/or Authorisation Registries.

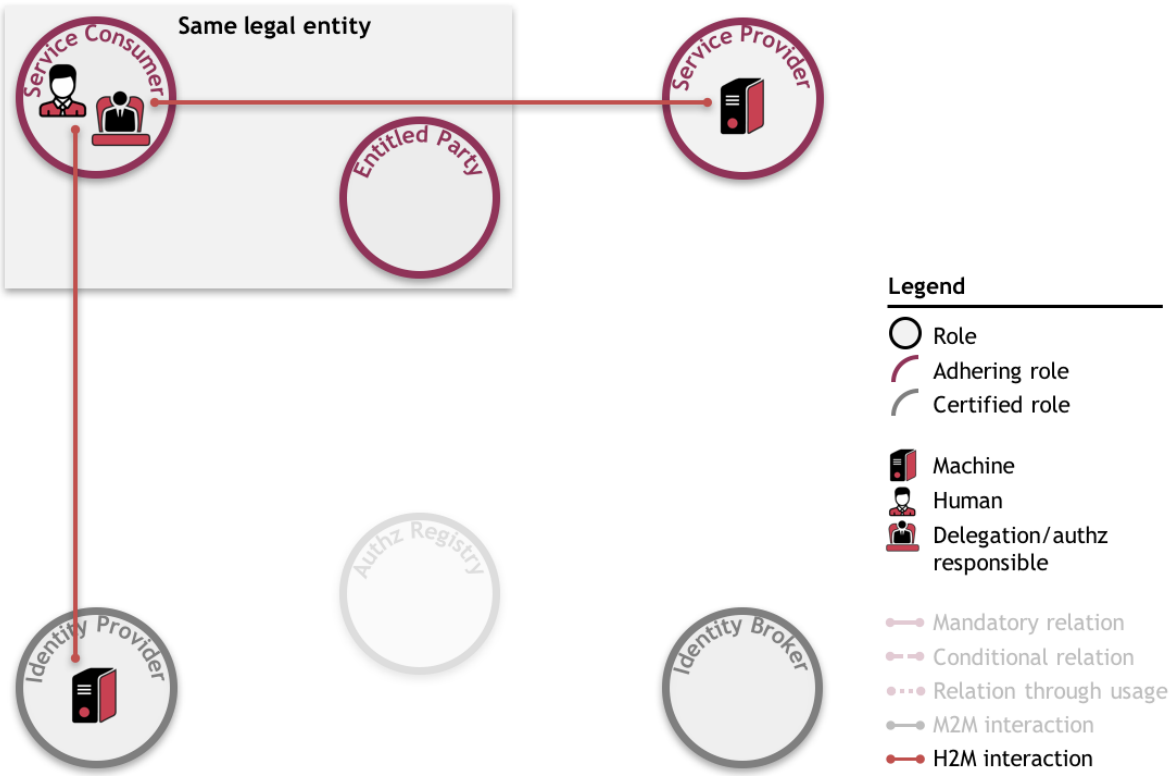
Depiction

Legal relations

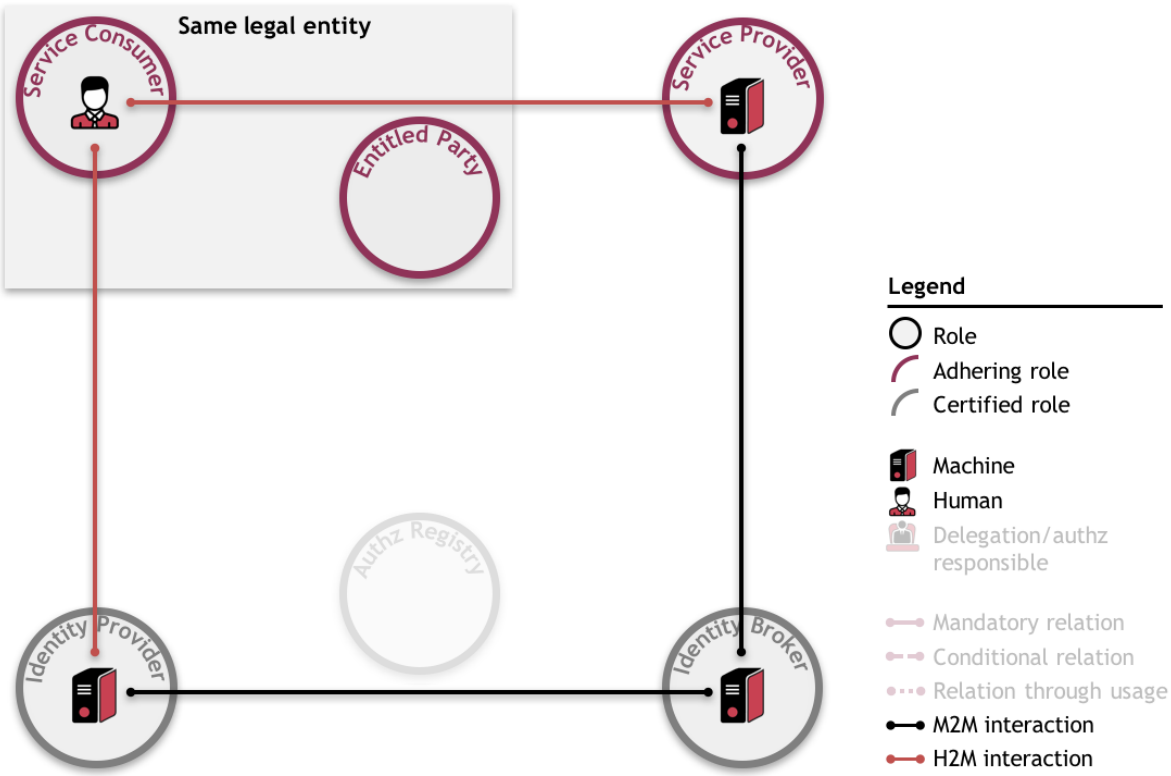


19 https://innopay.atlassian.net/wiki/display/IS/Identity+Broker

Prerequisite registration



Use case interaction



Description

It is prerequisite of this use case that:

- The Service Provider has and manages its own authorisation information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**;
- The delegation/authorisation responsible at the the Service Consumer registers the authorisation information at the Service Provider;
- The Human Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Human Service Consumer;
- The Identity Provider is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Identity Provider;
- The Identity Broker is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Identity Broker;
- The Human Service Consumer has been issued identity credentials by the Identity Provider.

- In this use case the Entitled Party is also the Service Consumer.

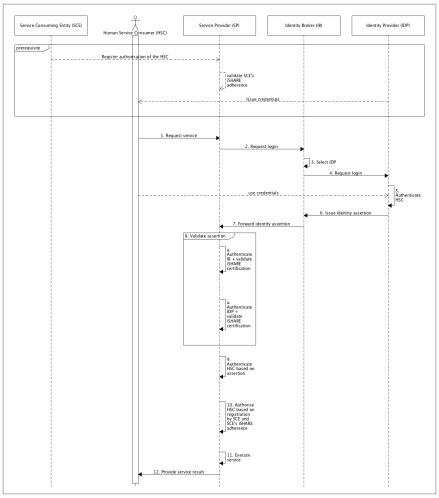
*The Service Provider can outsource this function to a third party

**The Entitled Party can outsource this function to a third party

The use case consists of the following steps:

1. The Human Service Consumer requests a service from the Service Provider;
2. The Service Provider requests a login from the Identity Broker;
3. The Identity Broker asks the Human Service Consumer to select his Identity Provider;
4. The Identity Broker requests a login from the Identity Provider;
5. The Identity Provider authenticates the Human Service Consumer;
6. The Identity Provider issues an identity assertion for the Service Provider to the Identity Broker;
7. The Identity Broker forwards the identity assertion to the Service Provider;
8. The Service Provider validates the identity assertion through the following steps:
    a. The Service Provider authenticates the Identity Broker and validates its iSHARE certification;
    b. The Service Provider authenticates the Identity Provider and validates its iSHARE certification.
9. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion, and validates the iSHARE adherence of the Service Consumer;
10. The Service Provider authorises the Human Service Consumer of the Service Consumer based on the authorisation information registered with the Service Provider;
11. The Service Provider executes the requested service;
12. The Service Provider provides the service result to the Human Service Consumer.

Sequence diagram

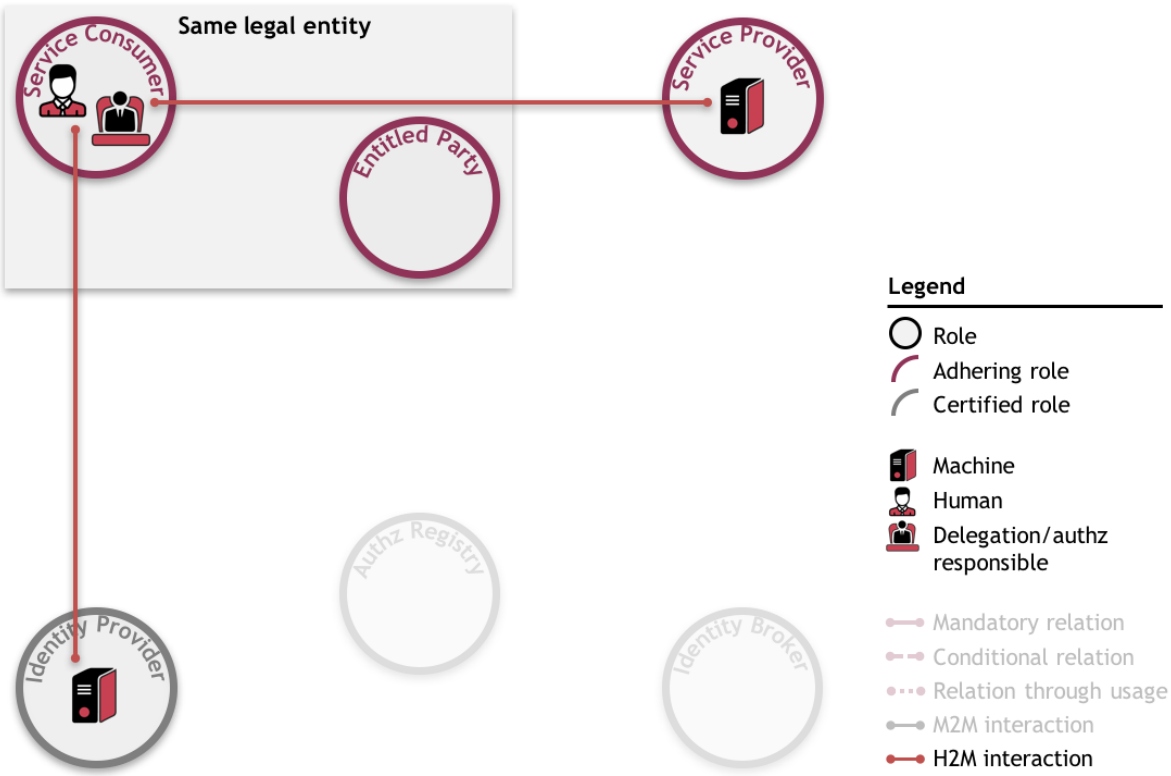


This use case would look as follows without an Identity Broker:

Depiction without Identity Broker

Legal view

Prerequisite registration



Interaction

Description without Identity Broker

It is prerequisite of this use case that:

- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**;
- The Service Consumer registers the authorisation information at the Service Provider;
- The Human Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Human Service Consumer;
- The Identity Provider is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Identity Provider;
- The Human Service Consumer has been issued identity credentials by the Identity Provider.

- In this use case the Entitled Party is also the Service Consumer.

*The Service Provider can outsource this function to a third party

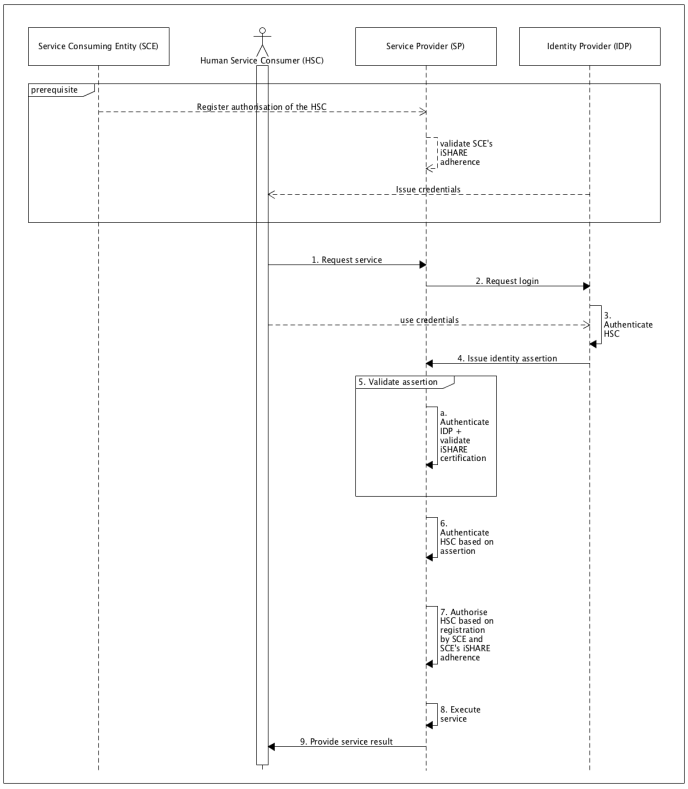
**The Service Consumer can outsource this function to a third party

The use case consists of the following steps:

1. The Human Service Consumer requests a service from the Service Provider;
2. The Service Provider requests a login from the Identity Provider;

3. The Identity Provider authenticates the Human Service Consumer;
4. The Identity Provider issues an identity assertion to the Service Provider;
5. The Service Provider validates the identity assertion through the following steps:
    a. The Service Provider authenticates the Identity Provider and validates its iSHARE certification.
6. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion, and validates the iSHARE adherence of the Service Consumer;
7. The Service Provider authorises the Human Service Consumer of the Service Consumer based on the entitlement information registered with the Service Provider;
8. The Service Provider executes the requested service;
9. The Service Provider provides the service result to the Human Service Consumer.

Sequence diagram without Identity Broker



3.2. H2M service provision with identity info at the IP and the AR as the authorisation info PIP

In use case 3.2, a service is provided by the Service Provider to the Human Service Consumer. Identity info is held at the Identity Provider. Authorisation info is registered in an Authorisation Registry.

Roles

		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	3 (see page 73)	3a	3b	3c

Entitled Party	3.1	3a.1	3b.1	3c.1
Authorisation Reg	3.2 (see page 81)	3a.2	3b.2	3c.2 (see page 85)
Identity Provider*	3.3	3a.3	3b.3	3c.3

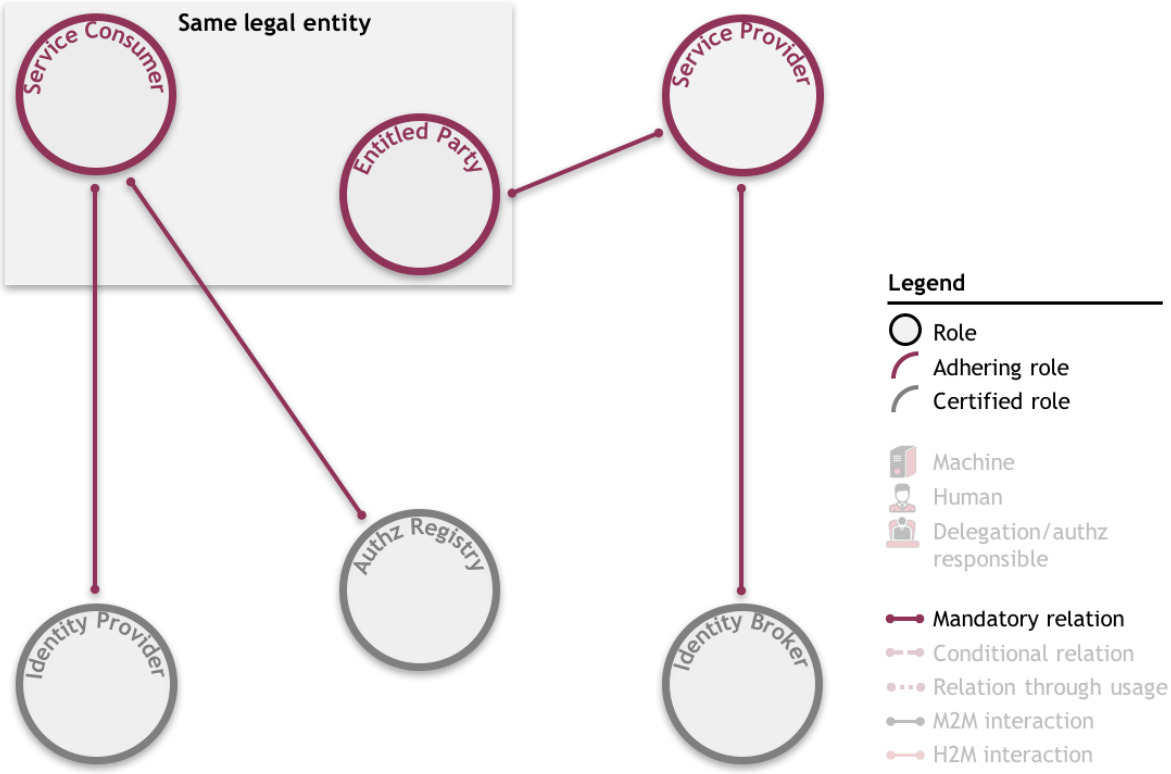
*The Identity Provider cannot hold explicit authorisation info, but it can hold info about a Human Service Consumer's identity that implies authorisation - i.e. 'working for truck company X'

As no delegation takes place, the Entitled Party is also the Service Consumer.

Note that an Identity Broker[20] is introduced to broker the relation between the Service Provider and the Identity Provider(s) and/or the Service Provider and the Authorisation Registry(s). This is optional and useful in situations with several Identity Providers and/or Authorisation Registries.

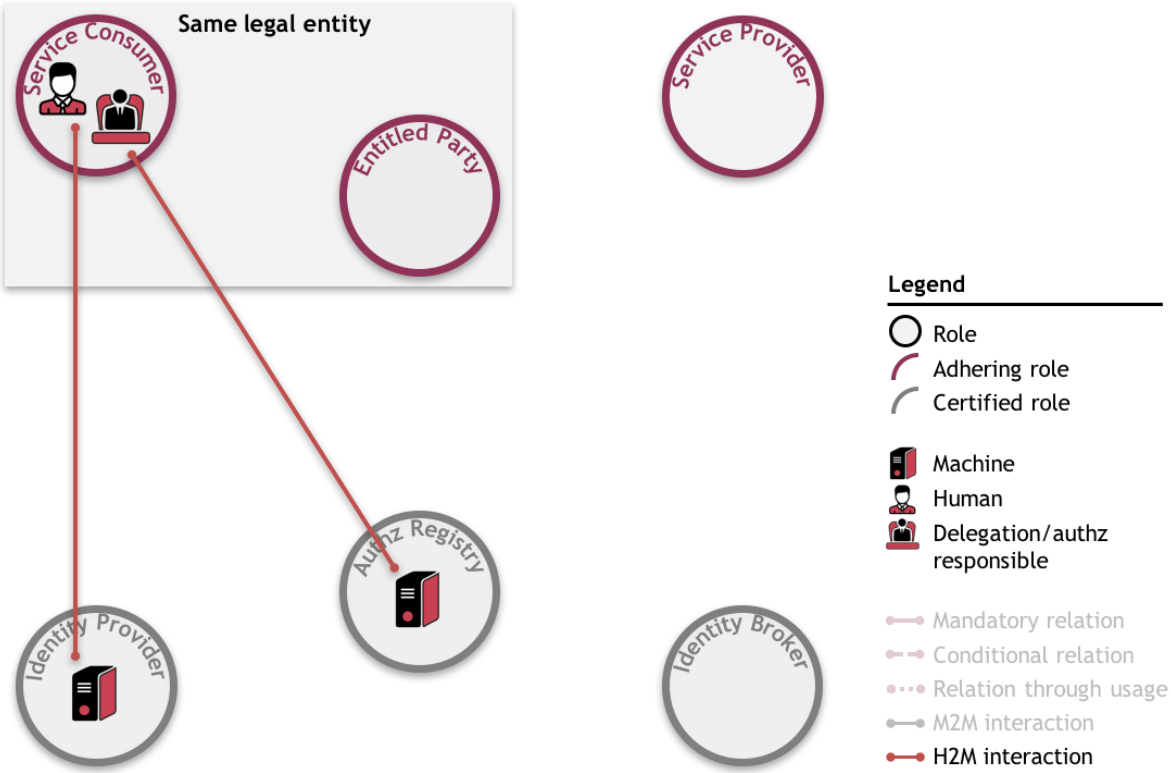
Depiction

Legal relations

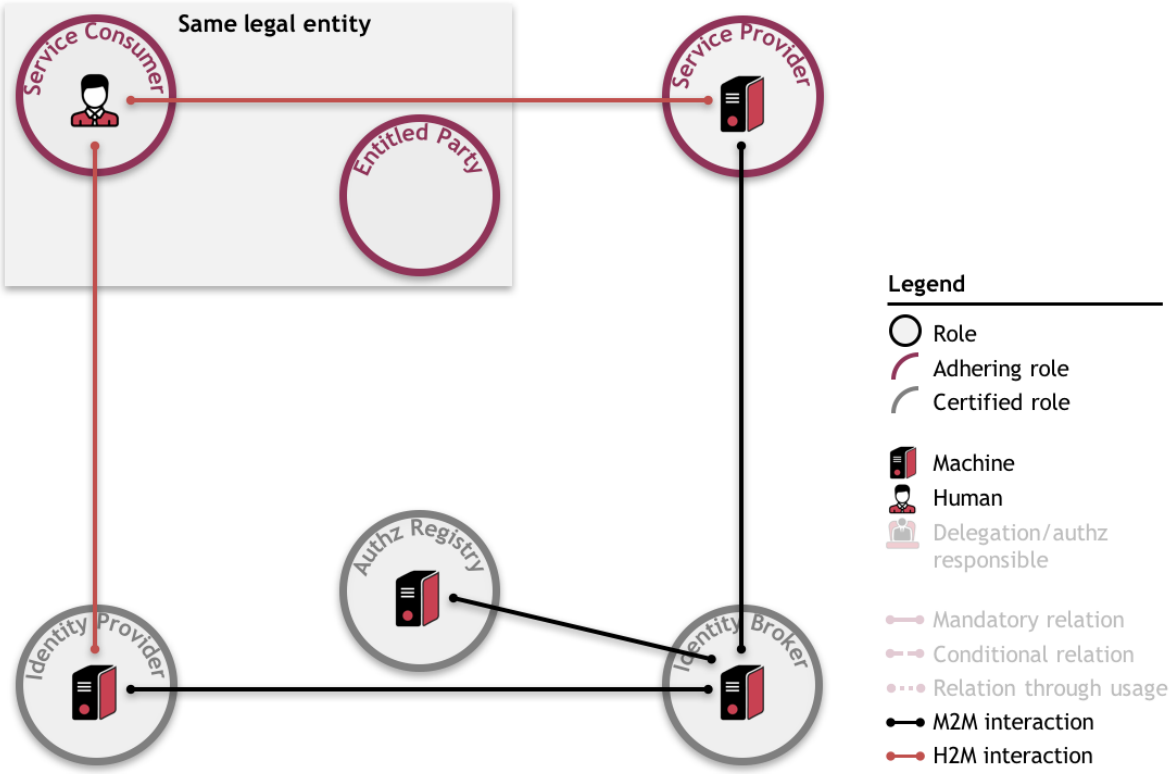


Prerequisite registration

20 https://innopay.atlassian.net/wiki/display/IS/Identity+Broker



Use case interaction



Description

It is prerequisite of this use case that:

- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**;
- The delegation/authorisation responsible at the the Service Consumer registers the authorisation information in an Authorisation Registry;
- The Human Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Human Service Consumer;
- The Authorisation Registry is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Authorisation Registry;
- The Identity Provider is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Identity Provider;
- The Identity Broker is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Identity Broker;
- The Identity Broker knows which Authorisation Registry to request the authorisation evidence from;
- The Human Service Consumer has been issued identity credentials by the Identity Provider.

- In this use case the Entitled Party is also the Service Consumer.

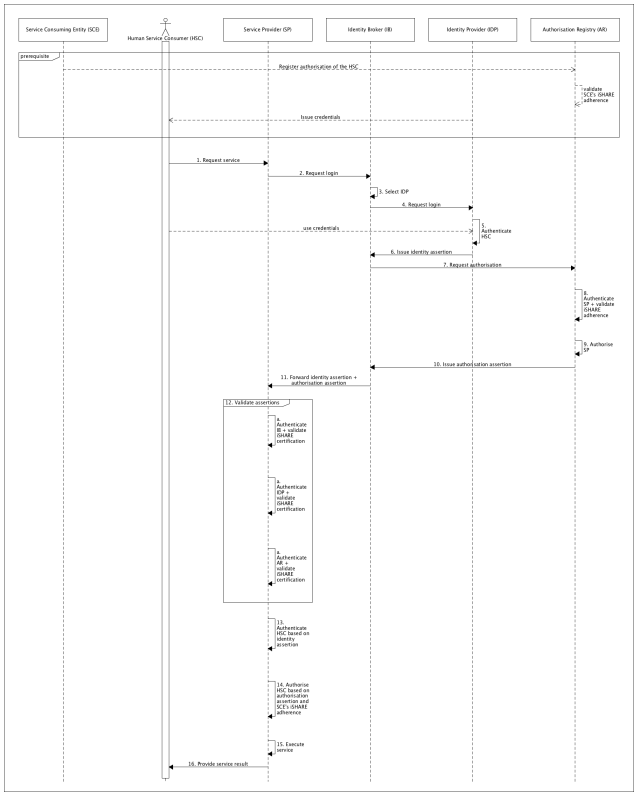
*The Service Provider can outsource this function to a third party

**The Service Consumer can outsource this function to a third party

The use case consists of the following steps:

1. The Human Service Consumer requests a service from the Service Provider;
2. The Service Provider requests a login from the Identity Broker;
3. The Identity Broker asks the Human Service Consumer to select his Identity Provider;
4. The Identity Broker requests a login from the Identity Provider;
5. The Identity Provider authenticates the Human Service Consumer;
6. The Identity Provider issues an identity assertion for the Service Provider to the Identity Broker;
7. The Identity Broker requests authorisation evidence from the Authorisation Registry;
8. The Authorisation Registry authenticates the Service Provider and validates its iSHARE adherence;
9. The Authorisation Registry authorises the Service Provider;
10. The Authorisation Registry issues an authorisation assertion for the Service Provider to the Identity Broker;
11. The Identity Broker forwards the identity assertion and the authorisation assertion to the Service Provider;
12. The Service Provider validates the identity assertion through the following steps:
    a. The Service Provider authenticates the Identity Broker and validates its iSHARE certification;
    b. The Service Provider authenticates the Identity Provider and validates its iSHARE certification;
    c. The Service Provider authenticates the Authorisation Registry and validates its iSHARE certification.
13. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion, and validates the iSHARE adherence of the Service Consumer;
14. The Service Provider authorises the Human Service Consumer of the Service Consumer based on the validity of the authorisation assertion;
15. The Service Provider executes the requested service;
16. The Service Provider provides the service result to the Human Service Consumer.

Sequence diagram



3c.2. H2M service provision with identity info at the IP, an AR as the authorisation info PIP, and another AR as the delegation info PIP

In use case 3c.2, a service is provided by the Service Provider to the Human Service Consumer, who has been delegated by the Entitled Party. Delegation evidence is registered in one Authorisation Registry, while authorisation info is registered in another Authorisation Registry.

Roles

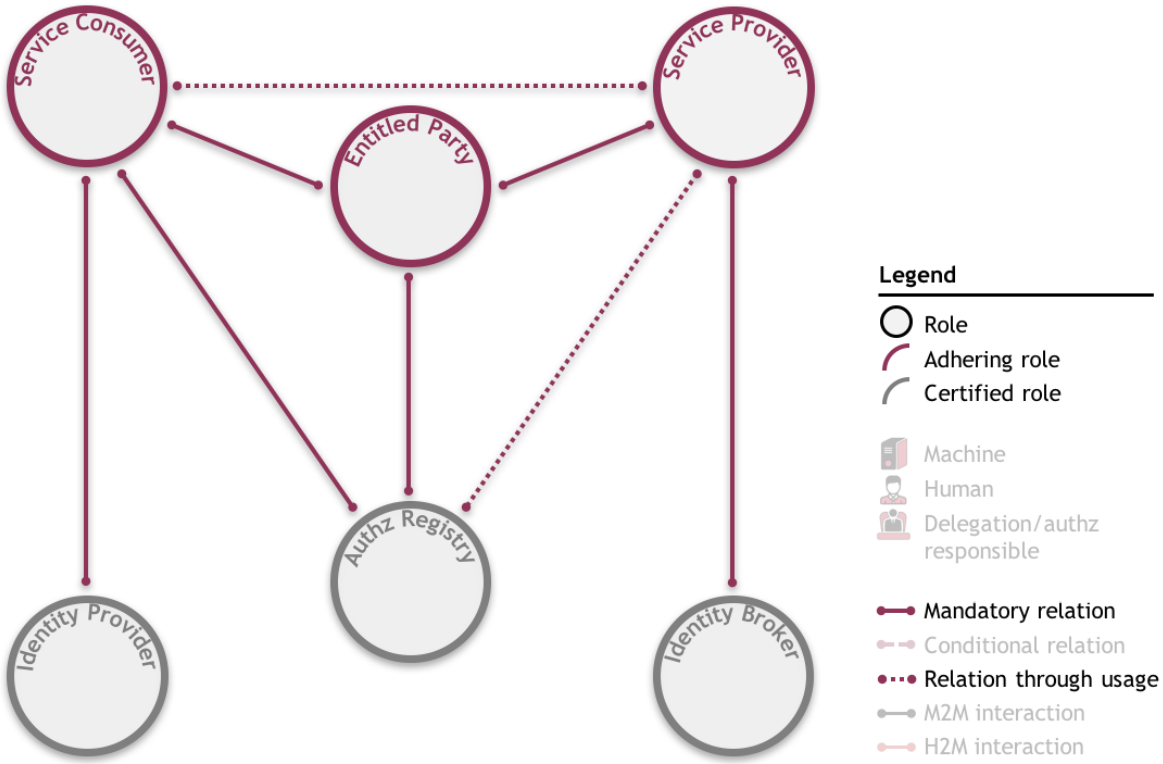
		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	3 (see page 73)	3a	3b	3c
	Entitled Party	3.1	3a.1	3b.1	3c.1
	Authorisation Reg	3.2 (see page 81)	3a.2	3b.2	3c.2 (see page 85)
	Identity Provider*	3.3	3a.3	3b.3	3c.3

*The Identity Provider cannot hold explicit authorisation info, but it can hold info about a Human Service Consumer's identity that implies authorisation - i.e. 'working for truck company X'

Note that an Identity Broker[21] is introduced to broker the relation between the Service Provider and the Identity Provider(s) and/or the Service Provider and the Authorisation Registry(s). This is optional and useful in situations with several Identity Providers and/or Authorisation Registries.

Depiction

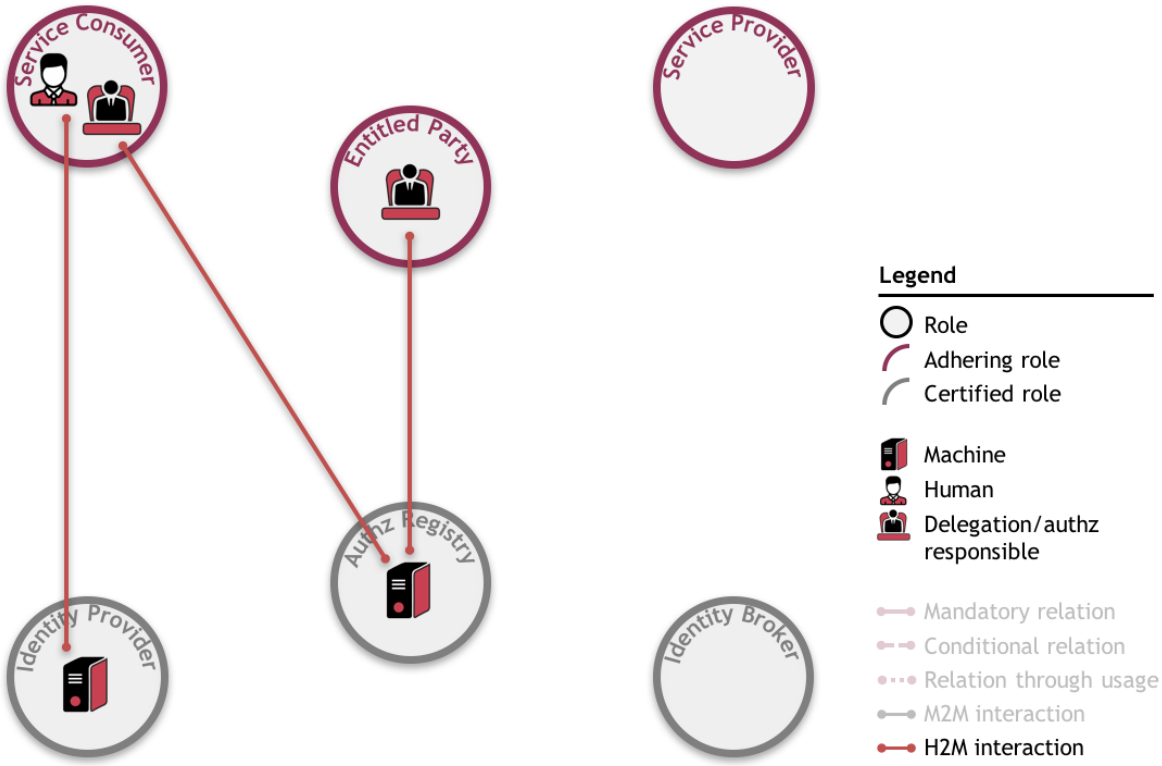
Legal relations



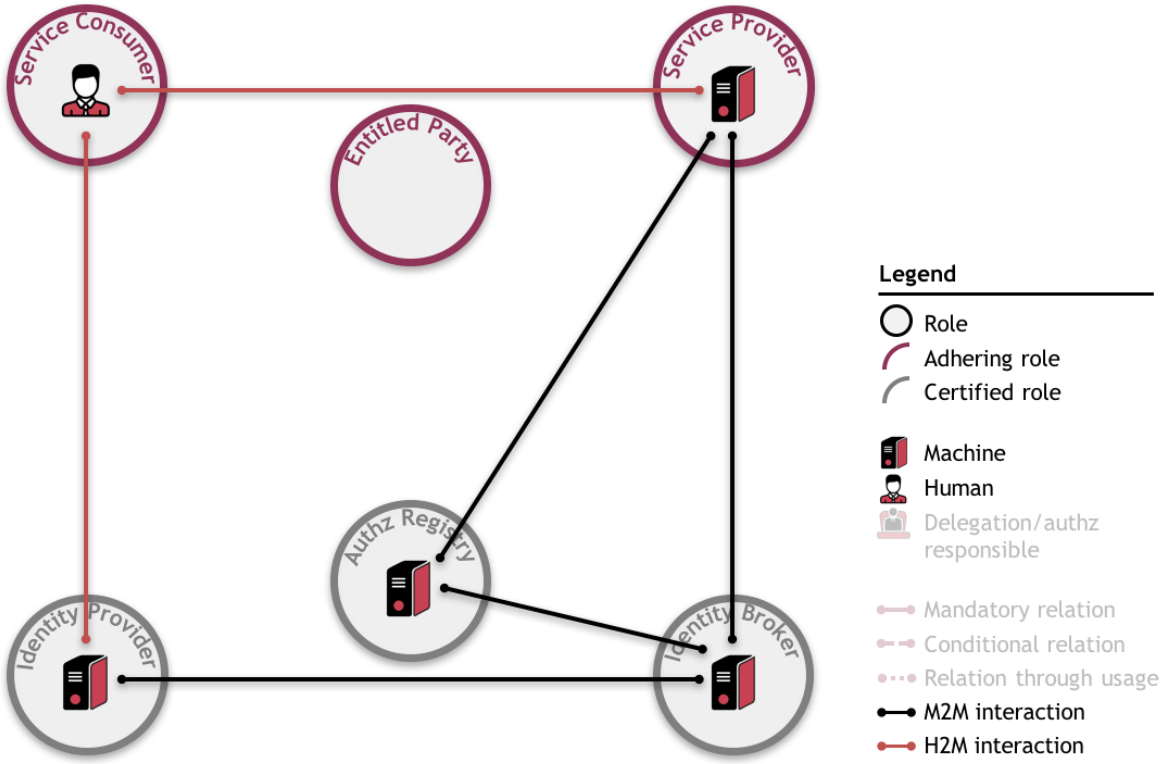
Note that no prior legal relation exists between the Service Consumer and the Service Provider. Which services can be consumed by the Service Consumer, as delegated by the Entitled Party, is set out in the mandatory relation between this Entitled Party and the Service Provider.

Prerequisite registration

21 https://innopay.atlassian.net/wiki/display/IS/Identity+Broker



Use case interaction



Description

In this derived use case, the Entitled Party delegates its rights to the Service Consumer. Note that because the Entitled Party utilises another Authorisation Registry to register its delegation info than the Service Consumer to register its authorisation info, two Authorisation Registries appear.

It is prerequisite of this use case that:

- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The delegation/authorisation responsible at the Entitled Party delegates (part of) the Entitled Party's rights (as registered at the Service Provider) to the Service Consumer. He registers this delegation in Authorisation Registry 2;
- The Service Consumer has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**;
- The delegation/authorisation responsible at the the Service Consumer registers the authorisation information in Authorisation Registry 1;
- The Human Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Human Service Consumer;
- Both Authorisation Registries are able to authenticate the Service Provider;
- The Service Provider is able to authenticate both Authorisation Registries;
- The Service Provider knows which Authorisation Registry to request the delegation/authorisation info from;
- It is clear, through scheme agreements, under what conditions an Authorisation Registry can provide delegation/authorisation information to a other parties;
- The Identity Provider is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Identity Provider;
- The Identity Broker is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Identity Broker;
- The Identity Broker knows which Authorisation Registry to request the authorisation evidence from;
- The Human Service Consumer has been issued identity credentials by the Identity Provider

* The Service Provider can outsource this function to a third party

** The Entitled Party can outsource this function to a third party

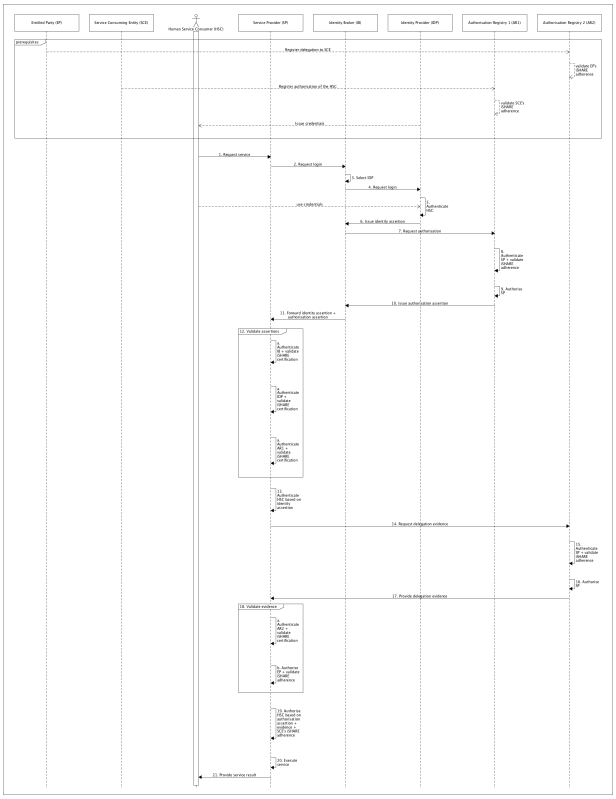
The use case consists of the following steps:

1. The Human Service Consumer requests a service from the Service Provider;
2. The Service Provider requests a login from the Identity Broker;
3. The Identity Broker asks the Human Service Consumer to select his Identity Provider;
4. The Identity Broker requests a login from the Identity Provider;
5. The Identity Provider authenticates the Human Service Consumer;
6. The Identity Provider issues an identity assertion for the Service Provider to the Identity Broker;
7. The Identity Broker requests authorisation evidence from Authorisation Registry 1;
8. Authorisation Registry 1 authenticates the Service Provider and validates its iSHARE adherence;
9. Authorisation Registry 1 authorises the Service Provider;
10. Authorisation Registry 1 issues an authorisation assertion for the Service Provider to the Identity Broker;
11. The Identity Broker forwards the identity assertion and the authorisation assertion to the Service Provider;
12. The Service Provider validates the identity assertion through the following steps:
    a. The Service Provider authenticates the Identity Broker and validates its iSHARE certification;
    b. The Service Provider authenticates the Identity Provider and validates its iSHARE certification;
    c. The Service Provider authenticates Authorisation Registry 1 and validates its iSHARE certification.

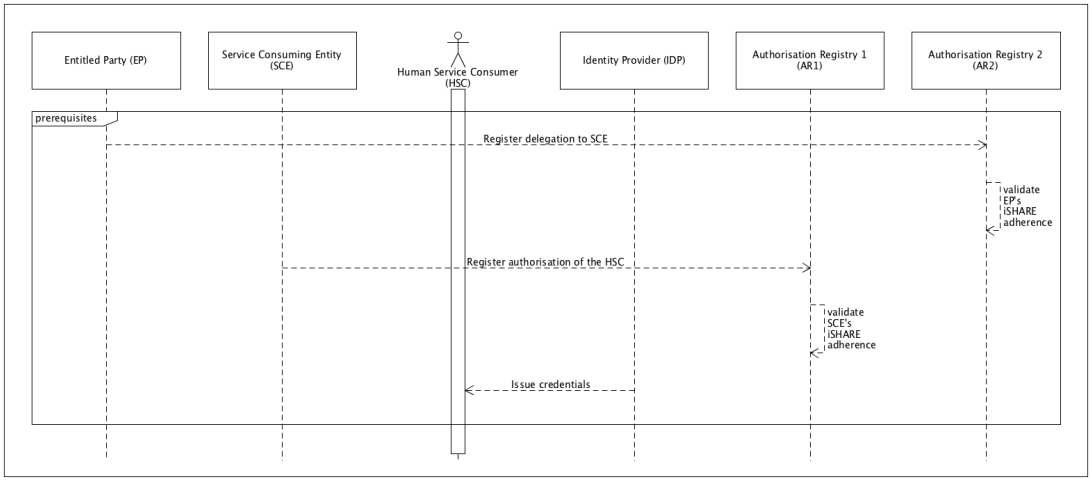
13. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion, and validates the iSHARE adherence of the Service Consumer;

14. The Service Provider requests delegation evidence from Authorisation Registry 2;
15. Authorisation Registry 2 authenticates the Service Provider and validates its iSHARE adherence;
16. Authorisation Registry 2 authorises the Service Provider based on the scheme agreements for providing authorisation information;
17. Authorisation Registry 2 provides the delegation evidence;
18. The Service Provider validates the received delegation evidence through the following steps:
    a. The Service Provider authenticates Authorisation Registry 2 and validates its iSHARE certification;
    b. The Service Provider authorises Entitled Party 1 based on the entitlement information registered with the Service Provider, and validates its iSHARE adherence.
19. The Service Provider authorises the Human Service Consumer of the Service Consumer based on the validity of the delegation evidence;
20. The Service Provider executes the requested service;
21. The Service Provider provides the service result to the Human Service Consumer.

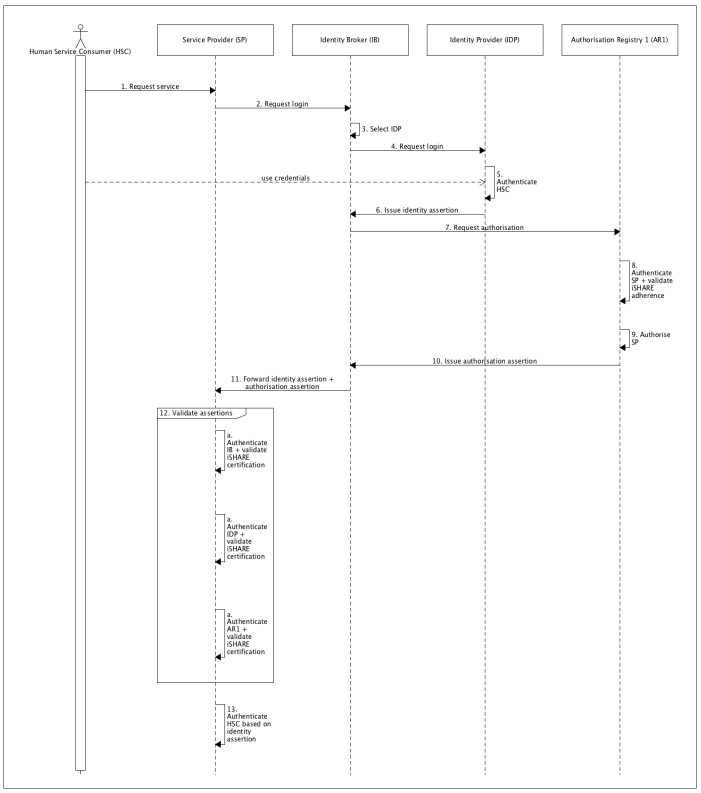
Sequence diagrams
Total



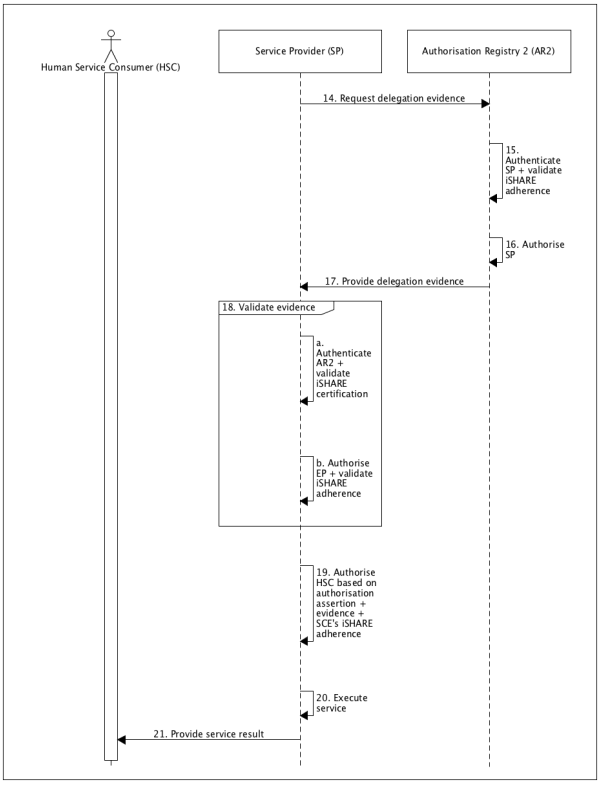
Prerequisites



Authentication and Authorisation



Delegation



5.1.2 Secondary use cases

iSHARE's three primary use cases (see page 51) are supported by seven secondary use cases. These include:

- Processes related to registration;
- Processes that recur in primary use cases.

5.1.2.1 **Processes related to registration**

These four secondary use cases need to be completed before any, or specific, primary use cases can be initiated.

Any party needs to:

1a. Register adherence/certification at Scheme Owner

and later needs to be able to:

1b. Modify adherence/certification at Scheme Owner

Before initiating Human to Machine use cases, the **Service Consumer** needs to:

2a. Create Service Consumer and/or Human Service Consumer identity at Identity Provider
Prerequisites:

- An agreement needs to be in place between Service Consumer and Identity Provider;
- An agreement needs to be in place between Service Provider and Identity Provider.

later, a Service Consumer needs to be able to:

2b. Modify Service Consumer and/or Human Service Consumer identity at Identity Provider

When delegating rights, the **Entitled Party** needs to:

3a. Register delegation at Service Provider, Entitled Party, or Authorisation Registry
Prerequisite:

- For registration at Service Provider or Authorisation Registry, an agreement needs to be in place between Entitled Party and Service Provider or Authorisation Registry.

later, an Entitled Party needs to be able to:

3b. Modify delegation at Service Provider, Entitled Party, or Authorisation Registry

When authorising something or -one, the **Service Consumer** needs to:

4a. Register authorisation at Service Provider, Entitled Party, or Authorisation Registry
Prerequisite:

- For registration at Service Provider or Authorisation Registry, an agreement needs to be in place between Service Consumer and Service Provider or Authorisation Registry.

later, a Service Consumer needs to be able to:

4b. Modify authorisation at Service Provider, Entitled Party, or Authorisation Registry

5.1.2.2 **Processes that recur in primary use cases**

These three secondary use cases form the wiring of all primary use cases. Without them, primary use cases cannot be completed successfully.

In any primary use case, **any party** needs to:

5a. Check whether its counterparty is iSHARE adherent/certified (with the Scheme Owner)

5b. Check whether its counterparty's certificate is valid

In any primary use case, the **Service Provider** *also* needs to:

6. Determine an authorisation decision based on entitlement-, delegation-, and/or authorisation info in its own contract administration and/or from external PIPs

When delegation- or authorisation info is requested by a Service Provider, an **Authorisation Registry** or **Entitled Party** also needs to:

7. Determine authorisation decision based on Service Consumer assertion included in Service Provider's request

Please note that the secondary use cases will not be detailed more than the above. No depictions or sequence diagrams are to be developed (contrary to for the primary use cases). This (deliberately) leaves freedom in implementation.

5.1.3 Licenses

Within iSHARE it is possible to explicitly provide instructions on how a service may be consumed or under which conditions data is exchanged. These instructions or conditions are called 'licenses'. Licenses are a crucial part of iSHARE, because they provide its participants the possibility to clearly state what is and what is not allowed. Since all iSHARE participants are bound to the same contract and underlying scheme rules, participants can appeal to each other to follow the provided licenses.

5.1.3.1 License code list

Purpose code	Description
0000	No limitations
0001	Re-sharing with Adhering Parties only
0002	Internal use only
0003	Non-commercial use only: licensee may not use the data to generate revenue
0004	Licensee may enrich received data with own data before re-sharing
0005	Licensee may enrich received data with data of others before re-sharing

Purpose code	Description
0006	Licensee may enrich received data with own data before re-sharing on a non-commercial basis
0007	Licensee may enrich received data with data of others before re-sharing on a non-commercial basis
9999	As determined between Parties

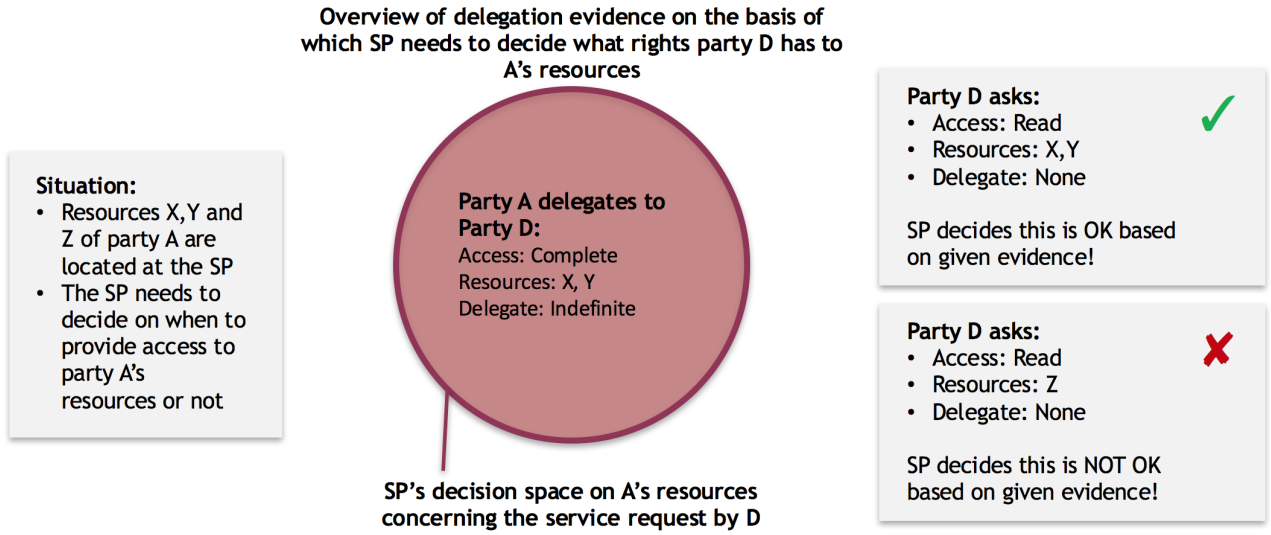
5.1.4 Delegation paths

A key functionality of iSHARE is delegating rights to another party, authorising them to act on your behalf. A single delegation was described in the delegation use case (see page 44).

In essence, Service Providers need to decide whether a Service Consumer is allowed access to a certain resource. To take the right access decisions, Service Providers need to interpret all relevant evidence to come to a decision: in other words: a 'logical sum' of evidence. This page further elaborates on situations where more than one delegation are issued that have overlapping properties.

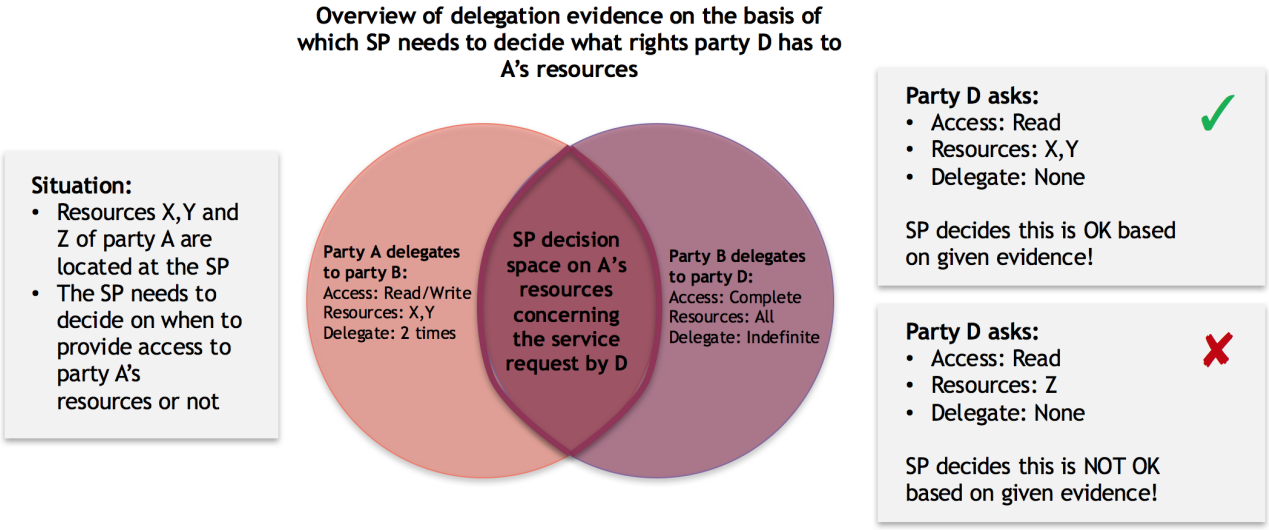
5.1.4.1 Example 1: Single delegation

In the situation of a single delegation, a Service Provider could encounter the following situation:



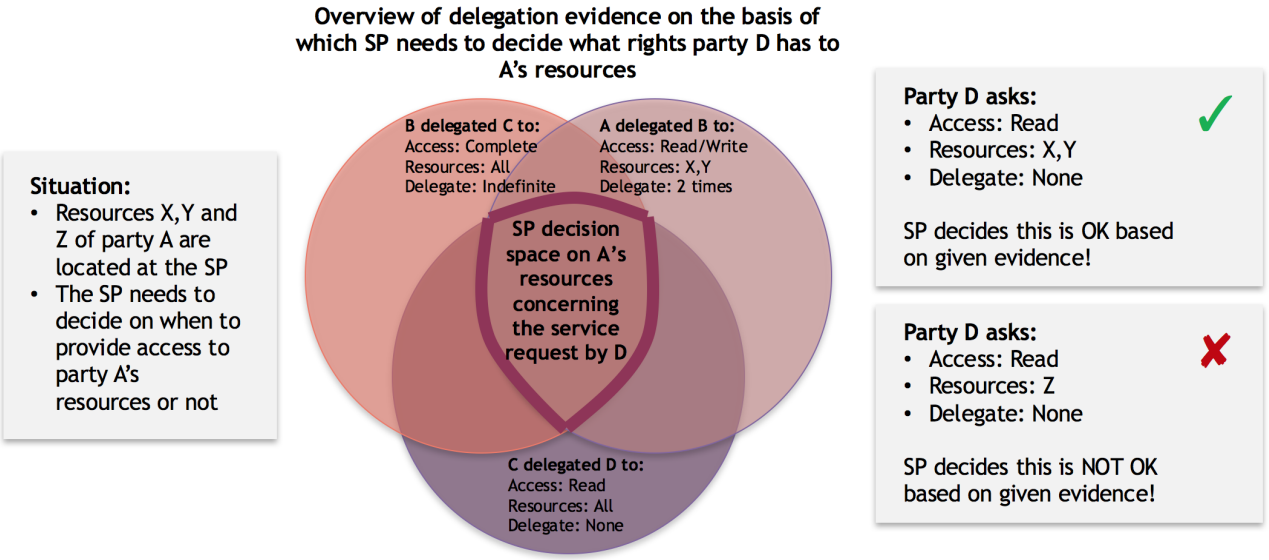
5.1.4.2 Example 2: Simple path of delegation

In practice, it can occur that various organisation delegate rights to various other organisation. Combining these delegations, a 'path of delegation' can be established, as is illustrated in the following example:



5.1.4.3 Example 3: Complex path of delegation

The following example illustrates a more complex delegation situation, where specific rights are delegated in terms of actions, resources and the right to further delegate these rights:



Party Q resides over party A's resources. When evaluating the available delegation evidence, organisation Q can conclude that organisation D has 'read' rights to resources X and Y but is not allowed to delegate these reading rights any further.

What is important to note for this path of delegation, is that the delegation rights **do not have to be given in a chronological order**. If party C just now delegated rights to D while party D would have requested access earlier than party C would have delegated rights, the delegation path would not exist.

Within iSHARE, it is possible to define more detailed rights to resources - as described in the key functionality section in the introduction (see page 21). For a detailed technical explanation of delegations, please refer to the 'structure of delegation evidence (see page 158)' chapter.

5.1.5 Functional requirements per role

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter summarises the responsibilities and functional requirements per role:

- Adhering roles:
  - Service Consumer (see page 96);
  - Service Provider (see page 96);
  - Entitled Party (see page 97).
- Certified roles:
  - Identity Provider (see page 97);
  - Identity Broker (see page 98);
  - Authorisation Registry (see page 98).

One requirement to any legal entity fulfilling a role is that they MUST provide a unique identifier (see page 99).

5.1.5.1 Adhering roles

Please refer to the detailed Operation descriptions (see page 171) for what criteria need to be met to be admitted to the iSHARE network.

Service Consumer

The Service Consumer-role is fulfilled by a legal entity that consumes a service, such as data, as provided by a Service Provider.

A Service Consumer can be represented by a machine (its system) or a human, fittingly called the Machine Service Consumer and the Human Service Consumer.

The **functional requirements** applicable to Service Consumers are as follows:

- iSHARE adherence is REQUIRED.

Service Provider

The Service Provider-role is fulfilled by a legal entity that provides a service, such as data, for consumption by a Service Consumer.

The **functional requirements** applicable to Service Providers are as follows:

- iSHARE adherence is REQUIRED;
- All user interfaces available in an iSHARE context MUST comply with the iSHARE's user interface requirements (see page 99).

Entitled Party

The Entitled Party-role is fulfilled by a legal entity that has one or more rights to a service provided by a Service Provider, for example to data. These rights, or entitlements, are established in a legal relation between the Entitled Party and the Service Provider.

The Entitled Party- and Service Consumer-roles can be fulfilled by the same entity - i.e. a legal entity that consumes a service based on its own entitlements to this service - but this is not necessary. Legal entities that are entitled to a service can delegate other entities to consume this service on its behalf: the legal entity consuming the service, then, does so on the basis of *another entity's* entitlements. In such use cases, as always, the Service Consumer consumes a Service Provider's service on the basis of the Entitled Party's entitlements, but the Service Consumer-role is fulfilled by another entity than the Entitled Party-role.

The **functional requirements** applicable to Entitled Parties are as follows:

- iSHARE adherence is REQUIRED.

5.1.5.2 Certified roles

In line with guiding principle 3 (see page 10), iSHARE utilises the Afsprakenstelsel elektronische toegangsdiensten[22] as a building block for certifying Identity Providers, Identity Brokers, and Authorisation Registries. Therefore, to become an iSHARE certified party, a legal entity MUST (first) be admitted to the Afsprakenstelsel elektronische toegangsdiensten[23] (in the relevant role). The relevant roles include:

- Authenticatiedienst[24] and Middelenuitgever[25] for potential Identity Providers;
- Herkenningsmakelaar[26] for potential Identity Brokers;
- Machtigingenregister[27] for potential Authorisation Registries.

Please refer to the detailed Operation descriptions (see page 171) for what (other) criteria need to be met to be admitted to the iSHARE network.

Identity Provider

The Identity Provider-role is fulfilled by a legal entity whose tooling identifies and authenticates humans (and specifically, Human Service Consumers representing Service Consumers). An Identity Provider:

- Provides identifiers for humans;
- Issues credentials[28] (i.e. a password or electronic keycard) to humans;
- On the basis of this identification information, identifies and authenticates humans for Service Providers.

As a result, Service Providers can outsource identification and authentication to an Identity Provider instead of implementing their own tooling.

The **functional requirements** applicable to Identity Providers are as follows:

---

22 https://afsprakenstelsel.etoegang.nl/display/as/Startpagina
23 https://afsprakenstelsel.etoegang.nl/display/as/Startpagina
24 https://afsprakenstelsel.etoegang.nl/pages/viewpage.action?pageId=26247508
25 https://afsprakenstelsel.etoegang.nl/pages/viewpage.action?pageId=26247423
26 https://afsprakenstelsel.etoegang.nl/pages/viewpage.action?pageId=26247485
27 https://afsprakenstelsel.etoegang.nl/pages/viewpage.action?pageId=26247407
28 https://innopay.atlassian.net/wiki/spaces/IS/pages/53840953/Credentials

- All functional requirements applicable to *Afsprakenstelsel elektronische toegangsdiensten* roles Authenticatiedienst[29] and Middelenuitgever[30].

- iSHARE certification is REQUIRED;
- All user interfaces available in an iSHARE context MUST comply with the iSHARE's user interface requirements (see page 99).

Identity Broker

Different humans might hold identifiers at different Identity Providers. Also, Service Providers might need to connect to several Identity Providers. To make sure Service Providers do not need a relation with each Identity Provider individually, an Identity Broker is introduced. The **Identity Broker**-role is fulfilled by a legal entity that provides Service Providers access to different Identity Providers, and that offers humans the option to choose with which Identity Provider to identify and authenticate themselves throughout the iSHARE scheme.

As a result, if Service Providers choose to outsource identification and authentication to more than one Identity Provider, they can connect to an Identity Broker instead of to several Identity Providers.

The **functional requirements** applicable to Identity Brokers are as follows:

- All responsibilities and functional requirements applicable to *Afsprakenstelsel elektronische toegangsdiensten* role Herkenningsmakelaar[31].

- iSHARE certification is REQUIRED;
- All user interfaces available in an iSHARE context MUST comply with the iSHARE's user interface requirements (see page 99).

Authorisation Registry

The Authorisation Registry-role is fulfilled by a legal entity who provides solutions for adhering parties for the storage of delegation- and authorisation information. An Authorisation Registry:

- Can holds information on delegations to Service Consumers;
  i.e. information indicating what parts of the rights of an Entitled Party are delegated to a Service Consumer.
- Can holds information on authorisations of humans representing a Service Consumer;
  i.e. information indicating which humans are authorised to act on a Service Conumer's behalf.
- Can check, on the basis of this information, whether a human or machine representing a legal entity is authorised to take delivery of a service;
- Can confirm whether this is the case to the Service Provider.

As a result, Adhering Parties can outsource tasks concerning the management of authorisation and delegation information to an Authorisation Registry instead of implementing their own tooling.

The **functional requirements** applicable to Authorisation Registries are as follows:

- All responsibilities and functional requirements applicable to *Afsprakenstelsel elektronische toegangsdiensten* role Machtigingenregister[32].

- iSHARE certification is REQUIRED.

29 https://afsprakenstelsel.etoegang.nl/display/as/Verantwoordelijkheden+Authenticatiedienst
30 https://afsprakenstelsel.etoegang.nl/display/as/Verantwoordelijkheden+Middelenuitgever
31 https://afsprakenstelsel.etoegang.nl/display/as/Verantwoordelijkheden+Herkenningsmakelaar
32 https://afsprakenstelsel.etoegang.nl/display/as/Verantwoordelijkheden+Machtigingenregister

5.1.5.3 Identification by EORI

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

In order for parties to identify other parties, any party fulfilling a role in the iSHARE framework MUST provide a unique identifier.

For this purpose, the Economic Operators Registration and Identification (EORI[33]) number is reused. An EORI is unique and valid throughout the European Community and is assigned by a customs authority or designated authority in a Member State. Even non-European Community parties doing business in/with Europe have an EORI, but if no EORI is available, a party is also allowed to supply its Chamber of Commerce number as alternative identifier.

Currently the following identifiers are supported in iSHARE:

Identifier	Example	Description
EORI number	EU.EORI.NL123456789	Economic Operators Registration and Identification
KvK number	NL.KVK.12345678	Dutch Chamber of Commerce number
Scheme Owner Identifier	iSHARE Scheme Owner POC[1]	String from the `common name` field in the certificate used by the Scheme Owner

[1] For POC purposes only. Production and test certificates have yet to be obtained.

Role identifiers

In certain cases, when identifying a certified party it is also important to identify their iSHARE 'role'. For this purpose iSHARE specifies the following identifiers:

Role identifier
IDENTITY_PROVIDER
IDENTITY_BROKER
AUTHORISATION_REGISTRY

5.1.5.4 User interface requirements

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

For all Human to Machine interactions, as in primary use case 2 (see page 69) and 3 (see page 73), an interface is required. This interface MUST comply with the following guidelines:

33 https://innopay.atlassian.net/wiki/spaces/IS/pages/53842635/EORI

- The name of the legal entity that provides a broker service or identity provisioning service MUST be clearly visible;
- During the process of authentication, information not directly relating to the identity provision process or supporting the identity provision process MAY NOT be present. Links to websites irrelevant to the identity provisioning process or advertisements MAY NOT be present;
- Parties facilitating the identity provision process MAY use their own corporate styling and logos;
- The iSHARE brand MUST be shown during the identity provision process. Showing the iSHARE brand MUST be in line with iSHARE communication[34] guidelines;
- Human Service Consumer that are being identified through the use of a browser MUST be able to verify the URL and used SSL certificate during all steps of identity provisioning process.

Please note that extra guidance will need to be added for the context of apps: how can Human Service Consumers verify that they are not being tricked?

5.2 Technical

This section covers the Technical details of the iSHARE scheme.

The section starts out with a chapter containing an overview of relevant technical standards (see page 100) that apply to the iSHARE scheme in general. The section also includes chapters with role-specific API requirements (see page 116) and the APIs that are exposed by the Scheme Owner (see page 148). Finally, this section provides a dedicated chapter on the 'delegation evidence structure' (see page 158), a JSON data structure which specifies how Authorisation Registries and Entitled Parties need to be able to present delegation evidence upon request.

5.2.1 Generic technical standards

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter contains information on the generic technical standards that are applied in the iSHARE scheme, relevant to all parties involved.

iSHARE can be described as an API architecture, which enables all parties involved to engage in direct communication. For interoperability reasons, iSHARE makes use of widely used open standards. Modified implementations of OAuth 2.0 and OpenID Connect 1.0 are used to facilitate an ecosystem in which parties can interact with previously unknown parties. Pre-registration, therefore, is not a prerequisite and this requires alterations to the official standards. Also, for the authentication of parties within an iSHARE context, iSHARE uses PKI and digital certificates relating to all participating parties.

5.2.1.1 Technical standards used in iSHARE and configuration aspects

The iSHARE scheme also prescribes various general interface specifications regarding **Caching**, **Dates & Times**, **Party Identifiers**, **Response Codes** and **Web Server configuration**. These are described in the following table and corresponding topic pages as referred to in the table.

34 https://innopay.atlassian.net/wiki/spaces/HRM/pages/67338304/Communication

***BOLD: Contains specific iSHARE specifications**

Technical standard	Character	Description
API	Architectural principle	Application Programming Interface API's are used in iSHARE to facilitate direct and realtime communication between different parties, eliminating the need for a central platform. *An API (Application Programming Interface) is a technical interface, consisting of a set of protocols and data structuring standards ('API specifications') which enables computer systems to directly communicate with each other. Data or services can be directly requested from a server by adhering to the protocols. APIs are used to hide the full complexity of software and make it easy for third parties to use parts of software or data services. APIs are mainly meant for developers to make the creation of new applications depending on other applications easier.* iSHARE prescribes caching requirements (see page 105) relating to the use of APIs in various situations.
PKI (see page 103)	Architectural principle	Public Key Infrastructure System for issuing and managing digital certificates. For authentication purposes, iSHARE requires adhering and certified parties to acquire an X.509 certificate which is distributed by a trusted root under certain PKI's (Public Key Infrastructure). For interoperability on a European scale, all trusted roots under the eIDAS regulation will be trusted within iSHARE. However, initially, this will be limited to certificates issued under PKIoverheid.
OAuth 2.0 (see page 106)	Open standard for authentication	Authentication standard, used in iSHARE to gain access to services through access tokens. iSHARE has modified the OAuth 2.0 standard to work without pre-registration. Pre-registration of clients MUST NOT be used. Certificate and status validation with the iSHARE Scheme Owner is sufficient for authentication purposes. If needed, clients can be registered after authenticating. To ensure security in unknown clients, iSHARE prescribes whitelisted Certificate Authorities that MUST be used.
OpenID Connect 1.0 (see page 111)	Open standard for authentication of humans	Authentication standard for the authentication of humans in an online context. Functions as an additional layer on top of the OAuth 2.0 protocol.

Technical standard	Character	Description
HTTP(S)	Communication protocol	HyperText Transfer Protocol (Secure) iSHARE scheme communication MUST be carried out over the HTTP protocol, and secured through TLS 1.2 resulting in HTTPS. iSHARE authentication/authorisation data is generally transferred in HTTP Headers. These headers can become very large when containing multiple encrypted certificates or JWT's. iSHARE parties SHOULD configure their web servers to accept HTTP headers of 100K length to minimise implementation impact on current services The most recent version of the HTTP specification can be found here[35]. An overview of relevant iSHARE HTTP (see page 104) response codes can be found here (see page 104).
TLS 1.2 (see page 105)	Cryptographic protocol	Transport Layer Security Transport Layer Security (TLS) is a cryptographic protocol that describes communication security for computer networks. It is used to secure the HTTP protocol, resulting in HTTPS. Within iSHARE, TLS 1.2 MUST be used for securing all HTTP communications. For the most recent version of the specification click on this link[36].
RESTful	Architectural style for API design	Representational State Transfer REST is an architectural style for building systems and services, systems adhering to this architectural style are commonly referred to as 'RESTful systems'. REST itself is not a formal standard, but it is an architecture that applies various common technical standards such as HTTP, JSON and URI. Within iSHARE RESTful architectural principles MUST be applied to the APIs that are specified. A RESTful API indicates that the API architecture follows REST 'constraints'. Constraints restrict the way that servers respond and process client requests, in order to preserve the design goals which are intended by applying REST. Goals of REST are, among others, performance and scalability. Both are of utmost importance in iSHARE. RESTful systems are able to process common HTTP operations, such as GET, POST and DELETE.

35 https://www.w3.org/Protocols/
36 https://tools.ietf.org/html/rfc5246

Technical standard	Character	Description
JSON	Open standard for file formatting	JavaScript Object Notation JSON is an open standard data format that does not depend on a specific programming language. This compact data format makes use of human-readable (easy to read) text to exchange data objects (structured data) between applications and for data storage. Within iSHARE, JSON is used as data structuring standard for scheme related communication. For the most recent version of the JSON specification click on this link[37].
JSON Web Token (JWT) (see page 112)	Open standard for definition of access tokens	JSON Web Token A JSON Web Token (JWT) is used in iSHARE when non-repudiation between parties is required. A statement, of which the data is encoded in JSON, is digitally signed to protect the authenticity and integrity of the statement. All iSHARE JWTs MUST be signed using the JWS specifications[38].
XACML 3.0 (see page 115)	Access control policy language	eXtensible Access Control Markup Language Standard for defining authorisation policies. Within iSHARE, a JSON port of XACML 3.0 is used to enable parties to communicate delegation evidence. For the most recent version of the specification click on this link[39].
X.509	Standard for the format of public key certificates	X.509 is a cryptographic standard for public key infrastructures (PKI's) that specifies the management of digital certificates and public-key encryption and keys of the Transport Layer Security (TLS) protocol that is used to secure web and email communication. For the most recent version of the specification click on this link[40].
UTC	Time standard	In iSHARE all dates and times MUST be communicated in UTC time. All dates and times MUST be formatted in the Unix timestamp format.

5.2.1.2 PKI

For authentication purposes, iSHARE requires adhering and certified parties to acquire an X.509 certificate which is distributed by a trusted root under certain PKI's (Public Key Infrastructure). For interoperability on a European

37 http://www.json.org/
38 https://tools.ietf.org/html/rfc7515
39 http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
40 https://tools.ietf.org/html/rfc5280

scale, all trusted roots under the eIDAS regulation will be trusted within iSHARE. However, initially, this will be limited to certificates issued under PKIoverheid.

Brief description

A PKI is a system for distribution and management of digital keys and certificates, which enables secure authentication of parties interacting with each other.

Generally, three different methods exist for creating trust within PKI's. These are through 'Certificate Authorities', 'Web of Trust' and 'Simple PKI'. Within iSHARE the 'Certificate Authority' approach is used, and as such the other methods will not be discussed.

A PKI can be considered as a chain of certificates. At the beginning of the chain is the root 'Certificate Authority' (CA), a public trusted party which is allowed to digitally sign their own certificates (SSC, self-signed certificate). This 'Root CA' distributes certificates and encryption keys to organisations. The certificate is signed by the 'root CA' as proof that the owner of the certificate is trusted. These organisations can start distributing certificates as well, if allowed by their root. They become CA's, and as such sign the certificates that they distribute. Repeating these steps, a chain of certificates is created, with each certificate signed by the CA who distributed the certificate.

Parties need to trust a certificate for authentication purposes. Instead of trusting individual certificates of organisations, root certificates can be trusted. By trusting a root, all certificates that have the root within their PKI chains are automatically trusted. Most large root CA's are automatically trusted within web browsers, enabling computers to safely interact with most web servers.

Trusted roots and eIDAS

The eIDAS regulation aims to provide secure and seamless electronic interactions between businesses, citizens and public authorities throughout the entire EU. A main part of this regulation is that each EU country is required to establish and maintain 'trusted lists', among which trusted root information is found. Each EU country is required to implement these trusted lists in their own countries. Therefore, iSHARE aims to make use of these trusted lists as trust roots within iSHARE to ensure secure and seamless interaction throughout the EU.

During the initial phase of iSHARE, the use of digital certificates will be limited to PKIoverheid certificates only.

5.2.1.3 HTTP response codes

After sending a HTTP request to a server, the server responds with (among others) a Status Code which indicates the outcome of the request made to the server.

Within the iSHARE scheme, the HTTP standard concerning response codes is followed as established by the IETF. Please refer to the IETF website[41] for further specification. Within iSHARE the HTTP response codes 401, 403, 406, 409 and 412 are most relevant.

HTTP Verb	CRUD	Entire Collection (e.g. /customers)	Specific Item (e.g. /customers/{id})
POST	Create	201 (Created), 'Location' header with link to /customers/{id} containing new ID.	404 (Not Found), 409 (Conflict) if resource already exists..

41 https://www.ietf.org/assignments/http-status-codes/http-status-codes.xml

HTTP Verb	CRUD	Entire Collection (e.g. /customers)	Specific Item (e.g. /customers/{id})
GET	Read	200 (OK), list of customers. Use pagination, sorting and filtering to navigate big lists.	200 (OK), single customer. 404 (Not Found), if ID not found or invalid.
PUT	Update / Replace	404 (Not Found), unless you want to update/ replace every resource in the entire collection.	200 (OK) or 204 (No Content). 404 (Not Found), if ID not found or invalid.
PATCH	Update /Modify	404 (Not Found), unless you want to modify the collection itself.	200 (OK) or 204 (No Content). 404 (Not Found), if ID not found or invalid.
DELETE	Delete	404 (Not Found), unless you want to delete the whole collection—not often desirable.	200 (OK). 404 (Not Found), if ID not found or invalid.

5.2.1.4 TLS 1.2

HTTP communication within iSHARE is encrypted using the TLS 1.2 protocol.

On this page a brief description of TLS is provided. For the most recent version of the specification click on this link[42].

Description

Transport Layer Security (TLS) is a cryptographic protocol that describes communication security for computer networks. The first version of TLS 1.0 is built upon and is an upgrade of SSL 3.0 (Secure Sockets Layer).

Differences and similarities between TLS and SSL

Both TLS and SSL provide means for data encryption and authentication between applications, machines and servers when data is sent through insecure network.

The differences between TLS and its forerunner 'Secure Sockets Layer' (SSL) are the addressed vulnerabilities. TLS for instance works with

- a wider variety of hash functions.
- more secure and stronger cipher suites, such as the Advanced Encryption Standard (AES) cipher suits which are integrated into TLS version 1.1.
- browser security warnings. TLS has more alert descriptions than SSL.

5.2.1.5 Caching

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Often data is temporarily stored on a different medium, to enable faster access to the data.

42 https://tools.ietf.org/html/rfc5246

For every API exposed under iSHARE caching MUST Be made explicit to the API consumer.

If a response is not cacheable it MUST contain the following headers:

Adherence information
`Cache-Control: no-store` `Pragma: no-cache`

If a response is cacheable it MUST contain the following headers:

Adherence information
`Cache-Control: max-age=31536000`

Note: max-age MAY vary

5.2.1.6 OAuth 2.0

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

iSHARE uses the OAuth 2.0 protocol for authenticating parties and providing access tokens when requesting access to a service within iSHARE.

On this page a brief description of OAuth is provided. For the most recent version of the OAuth 2.0 specification click on this link[43].

iSHARE facilitates an ecosystem within which parties can interact with previously unknown parties, pre-registration is therefore not a prerequisite and thus requires alterations to the official standard.

Generic OAuth 2.0 requirements

In addition to the specifications below, for all uses of OAuth 2.0 the following requirements apply:

- Clients MUST NOT be pre registered. A look-up in the iSHARE adherence registry is sufficient. It is up to the server create a new entry for Clients that perform requests for the first time [1]
- The `client_id` MUST contain the valid iSHARE identifier of the client
- For interoperability reasons clients SHALL only make `HTTP GET` calls to the `/oauth2.0/token` endpoint.
- Servers SHALL NOT issue refresh tokens

Additional rationale

43 https://oauth.net/2/

[1] In OAuth 2.0 clients are generally pre-registered. Since in iSHARE servers interact with clients that have been previously unknown this is not a workable requirement. Therefore iSHARE implements a generic client identification and authentication scheme, based on iSHARE whitelisted PKIs (see page 103).

Access token specifications in OAuth 2.0

Used to obtain an OAuth access token from a party that exposes an iSHARE API.

Based on the requirements in https://tools.ietf.org/html/rfc6749

OAuth access token API specifications example

GET /authorisation_registry/oauth2.0/token

Used to obtain an OAuth access token from the Authorisation Registry

Parameter	Contained in	Type	Required	Description
`grant_type`	query	string	Yes	OAuth 2.0 grant type. MUST contain “authorization_code”
`scope`	query	string	No	OAuth 2.0 scope. Defaults to "iSHARE", indicating all rights are requested. Other values MAY be specified by the API owner and allow to get tokens that do not include all rights
`client_id`	query	string	Yes	OpenID Connect 1.0 client ID. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain a valid iSHARE identifier[44]
`client_assertion_type`	query	string	Yes	OpenID Connect 1.0 client assertion type. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”

44 https://innopay.atlassian.net/wiki/spaces/IS/pages/93782017/Party+identifiers

client_assertion	query	string	Yes	OpenID Connect 1.0 client assertion. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain JWT conform iSHARE specifications (see page 112)

Example OAuth token request

```
https://randomserver.com/authorisation_registry/oauth2.0/token?
grant_type=client_credentials&
scope=iSHARE&client_id=EU.EORI.NL000000001&client_assertion_type=urn:ietf:params:oauth:clie
nt
-assertion-type:jwt-
bearer&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNS
UlHQVRDQ0ErbWdBd0lCQWdJQ0VBb3dEUVlKS29aSWh2Y05BUUVMQlFBd2daQXhDekFKQmdOVkJBWVRBazVNTVFzd0NR
WU
RWUVFJREFKT1NERVBNQTBHQTFVRUNnd0dhVk5JUVZKRk1SRXdEd1lEVlFRTERBaFRaV04xY21sMGVURW9NQ1lHQTFVR
UF
3d2ZhVk5JUVZKRklFNU1JRU5sY25ScFptbGpZWFJsSUVGMWRHaHZjbWwwZVRFbU1DUUdDU3FHU0liM0RRRUpBUllYYV
c1
bWIwQnBjMmhoY21VdGNISnZhbVZqZEM1dmNtY3dIaGNOTVRjeE1ERXlNRGd6TXpVNVdoY05NVGd4TURJeU1EZ3pNelU
1V
2pDQmxURUxNQWtHQTFVRUJoTUNUa3d4Q3pBSkJnTlZCQWdNQWs1SU1SSXdFQVlEVlFRSERBbEJiWE4wWlhKa1lXMHhE
ek
FOQmdOVkJBb01CbWxUU0VGU1JURVdNQlFHQTFVRUN3d05SSFZ0YlhrZ1ptOXlJRkJQUXpFVU1CSUdBMVVFQXd3TFRrd
3d
NREF3TURBd01ERXhKakFrQmdrcWhraUc5dzBCQ1FFV0YybHVabTlBYVhOb1lYSmxMWEJ5YjJwbFkzUXViM0puTUlJQk
lq
QU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUF2LzVmdElwdTE0bnl2MG9DUmRydEpsVk9icEV0Tmp
kT
FNNSSs3SzJOL05GWHlOUGFQM3c0ajB2a29Ma0lVUmJEaTJ3S29oUXNqanJEM21yR1RWN1ZqdWlaSzM1WlZPMGtlczly
ZU
hoeTNHNnIxMTJ4S2x1N3QwWmJxU2I2U3hrMW94c0FxQWppOUsyemtwN055UW00NVd4OFJEQzBsTytYalBpbExUZEp2V
lV
nWktlVkRmc1l6QjV5NXc2WG90aE1VNGgyNzBoVUNibkYwZ1FyQjFzL0RPeC9yd2xqMHc5ZmRTYjlsZk9SdzE2SUM5T3
B3
VzdsQU5kdTFkeTY4RnpGdHdxK1BHNXJBWThXOGU3MGNiT0hSSVRERjNKSjRlelEzY0NsaFlBQ3JPdUEvdkV2bnU0MzN
Ob
ml3UGVGa2VWSGhqQlIzOG53RzljQWJGU2d2Sm9rM1FJREFRQUJvNElCWERDQ0FWZ3dDUVlEVlIwVEJBSXdBREFSQmds
Z2
hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWklBWWI0UWdFTkJDWVdKRTl3Wlc1VFUwd2dSMlZ1WlhKaGRHVmtJRk5sY
25
abGNpQkRaWEowYVdacFkyRjBaVEFkQmdOVkhRNEVGZ1FVZnpHMElFMEV2OFBxZUNTbHJvTXVOTmlkNFA0d2diNEdBMV
Vk
SXdTQnRqQ0JzNEFVamtaTjB4U0pxbGNpWlZTTDFQYlZtd0kzM091aGdaYWtnWk13Z1pBeEN6QUpCZ05WQkFZVEFrNU1
NU
XN3Q1FZRFZRUUlEQUpPU0RFU01CQUdBMVVFQnd3SlFXMXpkR1Z5WkdGdE1ROHdEUVlEVlFRS0RBWnBVMGhCVWtVeEVU
QV
BCZ05WQkFzTUNGTmxZM1Z5YVhSNU1SUXdFZ1lEVlFRRERBdHBVMGhCVWtVZ1VtOXZkREVtTUNRR0NTcUdTSWIzRFFFS
kF
SWVhhVzVtYjBCcGMyaGhjbVV0Y0hKdmFtVmpkQzV2Y21lQ0FoQUFNQTRHQTFVZER3RUIvd1FFQXdJRm9EQVRCZ05WSF
NV
RUREQUtCZ2dyQmdFRkJRY0RBVEFOQmdrcWhraUc5dzBCQVFzRkFBT0NBZ0VBRGpvUVlxdjVIS3pKckY5bUttUy9PQjM
vM
0FodFJQVm1WRHFkTmNPdytHVTE0SXNLczQwN3ArbFhuMmhON2VaUEpwSVpyVDdqQzl2ZnVOTG1PbzEybXZ0YlBGeTdD
cT
krU1lCNkEvZ2NXK0NZemIrKzBWM3o0ZlR5Y1ZjRXVRQWc4ODM5TWM2clNhSXRha0Q3YnN1Y2EvTldyZFVqSUU1eDBNQ
2Z
```

```
YQ21WTS9NeXdlNHdGdEE5ZU5yN0Z1SUN4L0JhdkVnSU8rVmRFdDBKVUp6WGNYK0wrbGM1T0FCQlNidHZjT2pWblRHRD
Vu
T3ZodFdrQy80eWpaVmx3Y2EyK1E4OVBGcVI2OTRYRjhvc0szWFZTWGZVK2pmUk50K0EyeXpWTmpaemVucDF6a1RiZkd
ua
XBDek9QcllaMGxDUzZPUkF3cDdoZ1BrS3hJb1BqTjJkTE11TzAyWVZkV2t2SFVvTXNoN0F0Mjh0RGM2TEVsTjc1Zlgx
bn
VPdjgxMUcyYURxU0d6Rnc0SkdRU25lR3hsaDlMekdzaEkxaWorTm5pQm5uOTYrMGpHSm5OSjJGY3F1Y2dpZ21tSWVvY
0h
6QjlLV3Q3eFRzZmdnVFduZjd3dzA3OGgvZStrNFZ3V2JITjUrcXdURHFra2poTHh6Vm9jTzRHVWw2RzZXUmg2VHp6ek
Fq
SUNiS1BZclI5VWcxaGYxSFNOcG93RHU1MWlxVStmV1VZV0FRcVVSakV2Z0k0aFBmcVhya0x5NVR6OVdLQ1diR0hyRnR
5Z
VlXdGpxenhXdzlpN3Fwc3d3S002M1RLQ1dVVWJoNTlJTitFSTZqczhUMTc2b2tkSkVUUFRaOXpGcjNvNHBIVERBS0VO
RE
hmcjJwT293emZsazlhM3F3RTkvNndxMlhhalI1R289Il19.eyJpc3MiOiJFVS5FT1JJLk5MMDAwMDAwMDAxIiwic3Vi
Ij
oiRVUuRU9SSS5OTDAwMDAwMDAwMSIsImp0aSI6InpGMXFHS0J2NzgiLCJpYXQiOiIxNTEzMDcwODY3IiwiZXhwIjoxN
TE
zMDcwODk3LCJuYmYiOjE1MTMwNzA4NjcsImF1ZCI6Ik5MLkVPUkkuTkw4MTI0NTg4MzcifQ.bPOTFBBg8pedWkfoRKM
t1
uaa0albfWkgSObePtOSKxV0VOPUb1uencLihV086HWJeqO7DBZ2jx_rn96FfpojJnn2z2aQnBSX06IYPTYYcze543-
wb-
8vCor7hM6idGBbDCmeKQvFrIYaYmt34GeU0UjWnNMPGdh90vzbhqgPUlZixtUWfQYn0NxYJf7RGmEhmRybXm2zFl0oo
om
1d-zoZzwuTAzfZqa2rM986VG8WikewxN2IUafhKoQ_w42MB6WpPki8a0EJ07xUZozSybSQvFRWyKxN-
TCtixp3B5nGo9T
uZvkOf1f0RpL8-zTU2DQOFnhz8p7gwF10srNYYv3Sw
```


Responses

Code	Description
200	OK

Example value


```
{
  "access_token": "string",
  "token_type": "string",
  "expires_in": 3600
}
```


OAuth 2.0 general description

OAuth is an open standard for authorisation which is used by i.e. Google, Facebook, Microsoft, Twitter etc. to let their users exchange information about their accounts with other applications or websites. OAuth is designed to work with HTTP.

Through OAuth users can authorise third party applications or websites to access their account information on other "master" systems without the need of exchanging with them their credentials to login onto the platform.

OAuth provides a "secure delegated access" to resources (email accounts, pictures accounts, etc.) on behalf of the resource owner.

It specifies a method for resource owners to authorise third parties access to their resources without exchanging their credentials (username, password). Authorisation servers (of the platform) issue access tokens to third party clients (applications or websites) with the approval of the resource owner (= end user). The third party client needs the access token to get access to the resources that are stored on the resource server (of the master system).

5.2.1.7 OpenID Connect 1.0

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Used to obtain identity information for a human subject

Based on the requirements in http://openid.net/specs/openid-connect-core-1_0.html.

iSHARE facilitates an ecosystem within which parties can interact with previously unknown parties, pre-registration is therefore not a prerequisite and thus requires alterations to the official standard.

Generic OpenID Connect 1.0 requirements

In addition to the endpoint specifications described in the role-specific technical standards for Identity Providers (see page 136), for all uses of OpenID Connect 1.0 the following requirements apply:

- Clients MUST NOT be pre registered. See Generic /oauth2.0/token[45] for more details.
- The `client_id` MUST contain the valid iSHARE identifier[46] of the client
- For interoperability reasons clients SHALL only make `HTTP GET` calls to the `/oauth2.0/token` endpoint.
- Servers SHALL NOT issue refresh tokens

Description

OpenID Connect (OIDC) is the authentication layer that is built on top of OAuth 2.0 protocol which is an authorisation framework. The OIDC authentication layer allows clients to verify the ID and obtain basic profile information of their end-users

The authentication is performed by the authorisation server (managing the access rights and conditions) in an interoperable and REST-like manner.

OpenID Connect's building blocks

OIDC specifies a RESTful HTTP API using JSON as data format.

REST (Representational state transfer) or RESTful web services provide a method to achieve interoperability between computer systems and the internet.

45 https://innopay.atlassian.net/wiki/spaces/IS/pages/93323307
46 https://innopay.atlassian.net/wiki/spaces/IS/pages/49741942/Identifiers

APIs (Application Programming interfaces) enable Machine to Machine (M2M) communication where one machine calls upon the software functionality of another machine. They facilitate connectivity between applications. It is a software architectural approach that revolves around the view on digital interfaces that APIs provide self-service, one-to-many, reusable interfaces.

With OIDC a broad range of clients (web-based, mobile, JavaScript) can request and receive data about authentication sessions end-user profiles.

The specification is extensible (meaning it takes future growth into consideration) and supports optional features for encryption, ID data, discovery of OpenID providers and session management

OpenID Connect 1.0

Open ID Connect 1.0 is an adapted version of OpenID, combined with OAuth 2.0.

OpenID Connect performs many of the same tasks as OpenID 2.0, but in an API-friendly way and usable by native and mobile applications.

OpenID Connect defines optional mechanisms for robust signing and encryption.

Whereas the integration of OAuth 1.0a with OpenID 2.0 required an extension, in OpenID Connect, OAuth 2.0 capabilities are integrated with the protocol itself.

5.2.1.8 JSON Web Token (JWT)

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

A JSON Web Token (JWT) is used when non-repudiation between parties is required. A statement, of which the data is encoded in JSON, is digitally signed to protect the authenticity and integrity of the statement.

iSHARE uses signed JWTs in the following ways:

1. In a request for an OAuth Access Token or an OpenID Connect ID token the client sends a signed JWT. The client is authenticated based on the verification of the JWT's signature.
2. Delegation evidence is presented as a signed JWT. The signature of the Authorisation Registry or Entitled Party provides proof to other parties.
3. In a response from a server iSHARE metadata is presented as a signed JWT. The signature is used to bind the iSHARE metadata (such as license information) in the JWT to the content of the response.
4. A service from an iSHARE Service Provider MAY require a request to be signed.

On this page the generic requirements for a signed iSHARE JWT are specified.

General

All iSHARE JWTs MUST be signed using the JWS specifications[47].

Header

For the header of an iSHARE signed JWT the following requirements apply:

47 https://tools.ietf.org/html/rfc7515

- Signed JWTs MUST use and specify the `RS256` algorithm in the `alg` header parameter
- Singed JWTs MUST contain an array of the complete certificate chain that should be used for validating the JWT's signature in the `x5c` header parameter
- Certificates MUST be formatted as base64 encoded DER
- The certificate of the client MUST be the first in the array, the root certificate MUST be the last
- Except from the `alg`, `typ` and `x5c` parameter, the JWT header SHALL NOT contain other header parameters

Example JWT header


```
{
  "alg": "RS256",
  "typ": "JWT",
  "x5c": [ "MIIGCDCCA/
CgAwIBAgICEAQwDQYJKoZIhvcNAQELBQAwgZAxCzAJBgNVBAYTAk5MMQswCQYDVQQIDAJOSDEPMA0GA1UECgwGaVNIQVJFMREwDwYDVQQLD
AhTZWN1cml0eTEoMCYGA1UEAwwfaVNIQVJFIE5MIENlcnRpZmljYXRlIEF1dGhvcml0eTEmMCQGCSqGSIb3DQEJARYXaW5mb0Bpc2hhcmUt
cHJvamVjdC5vcmcwHhcNMTcwNjI3MDgyOTIzWhcNMTgwNzA3MDgyOTIzWjCBnDELMAkGA1UEBhMCTkwxCzAJBgNVBAgMAk5IMRIwEAYDVQQ
HDAlBbXN0ZXJkYW0xDzANBgNVBAoMBmlTSEFSRTERMA8GA1UECwwIU2VjdXJpdHkxIDAeBgNVBAMMF2lTSEFSRSBTY2hlbWUgT3duZXIgUE
9DMSYwJAYJKoZIhvcNAQkBFhdpbmZvQGlzaGFyZS1wcm9qZWN0Lm9yZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALp1Yk0cu
6U7M13mcQupWj+TADy/
hwEHWmmGGFFRaLMURuujDsKCHeu89Lvq71QQWkxxJWAHP6oRe3UCzCdMjXh6PoEQnnyC3dUgX3pGjQG1oT0a7tyMdMWzAW92MJW2BF8P7ZR
MlDskf7BJh1QPrF/p53+S0uexZNNSB3/
ZZjLpantIL3iF9mxPKBJX2c5dY666rt3+fadLhGf0AtG950M6BV3GmMNbx8sNQV+hCQ0OeIirhkIi+08ovcHTE7DP7+3BB2edDoCgSXStLH
rodB8wZBBGLBgm7tqcDz5pkaDetIrsYKNXQqERFjU2TYurBlnll64pce/
SOUiy+KDxhjcCAwEAAaOCAVwwggFYMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgZAMDMGCWCGSAGG+EIBDQQmFiRPcGVuU1NMIEdlbm
VyYXRlZCBTZXJ2ZXIgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFBEdKZ61hpM+ZDLNWLKlbxbBlIVoMIG+BgNVHSMEgbYwgbOAFI5GTdMUiapXI
mVUi9T21ZsCN9zroYGWpIGTMIGQMQswCQYDVQQGEwJOTDELMAkGA1UECAwCTkgxEjAQBgNVBAcMCUFtc3RlcmRhbTEPMA0GA1UECgwGaVNI
QVJFMREwDwYDVQQLDAhTZWN1cml0eTEUMBIGA1UEAwwLaVNIQVJFIFJvb3QxJjAkBgkqhkiG9w0BCQEWF2luZm9AaXNoYXJlLXByb2plY3Q
ub3JnggIQADAOBgNVHQ8BAf8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggIBAANm0QHtsbfkVqxr6jJgtD
vvIGQqmuryMpue1Log6HZZ2QowZWrG8o/4SAglpMPTuVU0UfABk5dVfOXnmBa5lRMI7hl9dSM1HNle6C9WA7RQtNV/
v4qBe0OlgfaD4cUAJDkHsIwWSMlcelOoxVZNcdOwadXAQHgYduzBSdR8/
Ps3plvIDIE9lrGt7GkUzxS3WU1XVss6nKZFWlZktqQH5Y+WEG//60+1Wf4aI6VHIuoRj10/
NlEvjct0Zx0yiZU2RrqwPqsrtBYbCPIuO+Cl9QM73pHY3zYqkWY4CLaewvyPZaY5KDBh7nZOp9NJ1Z2XWFuVIDTZReH2ARXFpkWDaHmhAcM
Z9BiqM+hx4IXeC68Vvwua+guypPJZfRyE33sox/lu8ecL2L7/ehDgji8IESymUPI32CpKfMN1KKNL/
KEtftGPpuV+6iQNTE4hTCBcBaSf3dxsGHclOSC6Ke9tL4YRLiX3+YsHqYD98vLRRObIQZGWXiqvSFsLCwK0M1RIwsfb6B9S+XMRAiwr1iez
BdHxXaH81lT+WxJfnDun6uxXUz4xTuzaVXsV0gvcY3quYp64LR6Rrhnc2DkNDzZU6JHyF7LX70rn8Lj180jjG1ge6ll9DLPQTkVyShTqCUV
+9wrU2aE16rqe2YAq/lLJ0dWOHS2pJcQjh1iDpAqGObwT",
"MIIGBDCCA+ygAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgZAxCzAJBgNVBAYTAk5MMQswCQYDVQQIDAJOSDESMBAGA1UEBwwJQW1zdGVyZG
FtMQ8wDQYDVQQKDAZpU0hBUkUxETAPBgNVBAsMCFNlY3VyaXR5MRQwEgYDVQQDDAtpU0hBUkUgUm9vdDEmMCQGCSqGSIb3DQEJARYXaW5mb
0Bpc2hhcmUtcHJvamVjdC5vcmcwHhcNMTcwNjI3MDYxNDM0WhcNMjcwNjI1MDYxNDM0WjCBkDELMAkGA1UEBhMCTkwxCzAJBgNVBAgMAk5I
MQ8wDQYDVQQKDAZpU0hBUkUxETAPBgNVBAsMCFNlY3VyaXR5MSgwJgYDVQQDDB9pU0hBUkUgTkwgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSY
wJAYJKoZIhvcNAQkBFhdpbmZvQGlzaGFyZS1wcm9qZWN0Lm9yZzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKiuQXA3R14zhA
Z59xu4J6j8h5LaMYoMzFIRzeV+665E8bnoK2eQSC5aYMvsb80o8DxHHjiqPJiJW1n1oT86UAKgaEEnJ8/
GhF+2kyOlybdpM21Q6bNwkJ5vL4SD/GYBPmWsVt7X6pLAkFsweXu6wRzvrYXWcVm/z/3SHX9AZFg6HDZRsGGDnnRw14nHYpb/
oh7p5h6atI+X0aOD4HhQJ1ahQLVozIbbCFDfpKu9mrDXzKYDaNstrYn2DmbtV40BC5FW1OT0HLO/
texnnhtNrjq6IVgUkZ54NHT8Y2EQNmajy8RilrLU1FHS/
ka03w8sV0sXDsLeBwbxl3BYHpisPMWpMJDFU8b92tlYjk2lUDnHqDUi5BHRdRYqVZeWBSL+Qevpezr3mCL9ynhGPy+tNyDjyVjb/
y7hlftAzZzodRwItQPzpKHCWQLsWX+JwM9lwu5uq6lcqxHGPSAB0o/ME80KE3a4KnjCGYvlZiPJtrad0HZDRR/
hEAnen3HE3fTZE42u2wBLTfZB1D8Kxjc44vJv8L4JOaLlt/ooMT913sGCSJDPQUwv+/
VvYDV8ngkgzRCpFng2NrPaWao6RKJ99bBMkKFQ4vsdtvwi42GK2OBK7ozXnNS7B5qcljdVnrmmH8fCPJ/s7L9BDYw/IKrd5wHaSH1kZ7/
DRa0fa2mMJjfLAgMBAAGjZjBkMB0GA1UdDgQWBBSORk3TFImqVyJlVIvU9tWbAjfc6zAfBgNVHSMEGDAWgBRLYazzoNpuBb//
4Sr1Ior0iP04RjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/
wQEAwIBhjANBgkqhkiG9w0BAQsFAAOCAgEAQ7GRIQ3Q+TRUumxOXc+dGJnx98EK1qD8E1uEptlS+VROWAZ22QeLCPk/
```

```
nNDVs2AmCADZF0JoX2+RJNjq7pX2+AxcL1owWQoi3GRtL6GABHByulTfJfvodYjUipI1zmIvcWKzNnNCC9A0rdtUJyRjZvGZt32K77aiRNG
iSCtVyCBuFBPtqCkXIz86e/wzQ1fwBeCRB0WDMoSdXbSkt/
tapyGoU7oAj2DVWbtKaCnkKiysE19r1RCiZI2WAHLcuU9iLvNM1Mfowv9avI+rVq2YlKUOuCIrD7s/
ILRLXg55VwqMJT33/50NFnu3H8ebmqEhkGYStk7p3FGRxgptd2OJnqAt5nG1pspHQuD+vYBoKkkMw40qvy+eeYkhyzKcJTKeOsfI29fyQx/
eFSmWRheT188+jZQyCqEQpZRgtku+2KPQbCBxVeCfHacyS16+9ZOVs1zXWGfIqXKXwZF1v6CDyL7bedJZEuTU1wUpkEUJH/
IPmdp2ZMNMcss/BIdyf/+pYwyMnB6DJocDwMjlm3cUEsbtT393wIie0mohWiu8myTxkCfN1VJs4W9chSx5/
DxVwDtFoT4nsqVK9F6DKYJAJ95UR+C+RiCS+x7t4r8cup0AiJpg7JEGr5I9kdlBXKAk78Pr/
oqZogFymWPzoWUy48Ye6WxaAA1s+h6hVQ22MCg=",
"MIIGCDCCA/
CgAwIBAgIJAN7kMSjuGT9KMA0GCSqGSIb3DQEBCwUAMIGQMQswCQYDVQQGEwJOTDELMAkGA1UECAwCTkgxEjAQBgNVBAcMCUFtc3RlcmRhb
TEPMA0GA1UECgwGaVNIQVJFMREwDwYDVQQLDAhTZWN1cml0eTEUMBIGA1UEAwwLaVNIQVJFIFJvb3QxJjAkBgkqhkiG9w0BCQEWF2luZm9A
aXNoYXJlLXByb2plY3Qub3JnMB4XDTE3MDYyNzA2MDY1NFoXDTM3MDYyMjA2MDY1NFowgZAxCzAJBgNVBAYTAk5MMQswCQYDVQQIDAJOSDE
SMBAGA1UEBwwJQW1zdGVyZGFtMQ8wDQYDVQQKDAZpU0hBUkUxETAPBgNVBAsMCFNlY3VyaXR5MRQwEgYDVQQDDAtpU0hBUkUgUm9vdDEmMC
QGCSqGSIb3DQEJARYXaW5mb0Bpc2hhcmUtcHJvamVjdC5vcmcwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCuvV8gSQDx7g1PY
vxcuK6uDIwWZNZKdF0wJoGjcIlqPJWF3pP2xCJq5ZRnUQnpW0WTCWw9A4uZfCIWqJSoISh4nE7UmMmfw45ms+7SwJxfc7E+Y4ffMDMyLcmv
HYYLqGDoZu4qnpytsz+Xs1e8ESyNtIlXooZ6O+C1he+XmXpSChOjh5Pnz7RHz4cS7Zw38B9aNA3WktF+yR7ijkTUN887aZAplmrNZoioGnM
/E1RFwnLqrk5E84kOTzexsNILBpBzoZkLPz8yYI0OJ42/RT5m9YPOIRWMwWcgQqmBHIgMCaUOjAslex2Bx1uQtBJcti+DIf+ZIGPm/
TcwsaCC+RbE51SmMqwXYe/BoAlAZKYSgG8outN+Fd3Ew3h3YJcA86wDT9bKMzS9oSV1EjXc8v+40pp//AdWMPf2q15i/
QotTj+SGP2cJQvcfRBJ94IfG41IBolEK7jEUN2JUcowAdNsYfM7EdoKGhIn+bkCXnZR3bnfBKBAXH64MOp7Ii1NukjPpEqemyM3//XKn/
1lXzU43rbazwbxyGBYq3AHv5io7MS1TwegD/hNmTOEGHffZ/CzJghm6WvgmcmUALu2IFcDpmYZI3UI3SKzwaddi7/
vcGer5VVDglRtVtvHk3eJRT0L9SFqHIWsLunI/dZSJE8pKpStG5Lzj7Y/psOlBpahnwIDAQABo2MwYTAdBgNVHQ4EFgQUS2Gs86DabgW//
+Eq9SKK9Ij9OEYwHwYDVR0jBBgwFoAUS2Gs86DabgW//+Eq9SKK9Ij9OEYwDwYDVR0TAQH/BAUwAwEB/
zAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggIBABt+I4ZnS45c2IFsKV+BA8JP5OWCPoaJyl3PCELjedVfB4rXyF946+ILARcB
Zg35F07WzHtmi/
afXh6entvVMEAlEmH6ln8sR9hoM3rHnYRtSIJmJs2gSF8wgCOZd1pyfrBVu3f3SXbUgNjoe5tEW6xsOQsjjqNnQiJMJx6ea56L2kbW7E6kO
s+Mck9Kz8ZQQB58iPGyx3ahMLOrxbPoItbqKuyDwco7AzLf7ea9zye0up8ubNDYFaKJfiIDsnVbUPA6FbTn4fSQpeeOK1fjrzSaUpeMOdOo
mj0Zjwt6K7W7ckxoIfOecW4dcPENpXImkBPQXsGxvClDf/6e/
jPti3CPgxJF3747Hq6tBSH0GzCrYv4bForQu43MzqZKHbX8FF1PpHSaiXJK/Hu8WJDXXBq5Pedel/lJSajdTsUDsiFXkj/pY0uJ6M0x/
EonozaCPcHwdPsvr6nrrHWQXo4ayP7ntegJA3GrGXcaP+peEQmF9nWgVwPq33C1TrPNaiMxHz5toxl0YhnbA+5eH2CTBjDFJnr2uaeh8Bzb
kdE29WkOsqJZAIUEMmRwxcxBW20JGAlhF6MPFADjPYG0Ljdjbwq2H+LQtRf+tE6Z7nwM/
cAT4dEB7Me1uJrYucVjLLSNXCRKQaDKKZMoHhAciLeKLMrSgUDaAi0AUKXduCymUw3n"
]
}
```


Payload

For the payload of an iSHARE signed JWT the following requirements apply:

- The JWT payload MUST conform to the `private_key_jwt` method as specified in OpenID Connect 1.0 Chapter 9[48] [1] [2]
- The JWT MUST always contain the `iat` claim
- The `iss` and `sub` claims MUST contain the valid iSHARE identifier[49] of the client [1]
- The `aud` claim MUST contain only the valid iSHARE identifier[50] of the server. (Including multiple audiences creates a risk of impersonation and is therefore not allowed)
- The JWT MUST be set to expire in 30 seconds. The combination of `iat` and `exp` claims MUST reflect that. See Dates and times[51] for requirements

48 http://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication
49 https://innopay.atlassian.net/wiki/spaces/IS/pages/93782017/Party+identifiers
50 https://innopay.atlassian.net/wiki/spaces/IS/pages/93782017/Party+identifiers
51 https://innopay.atlassian.net/wiki/spaces/IS/pages/93749265/Dates+and+times

- Depending on the use of the JWT other JWT payload data MAY be defined

Additional rationale

[1] In OAuth 2.0 clients are generally pre-registered. Since in iSHARE servers interact with clients that have been previously unknown this is not a workable requirement. Therefore iSHARE implements a generic client identification and authentication scheme, based on iSHARE whitelisted PKIs (see page 103).

[2] Since OAuth 2.0 doesn't specify a PKI based authentication scheme, but OpenID Connect 1.0 does, iSHARE chooses to use the scheme specified by OpenID Connect in all use cases. This is preferred above defining a new proprietary scheme.

Example JWT payload

```
{
  "iss": "EU.EORI.NL123456789",
  "sub": "EU.EORI.NL123456789",
  "aud": "NL.KVK.12345678",
  "jti": "378a47c4-2822-4ca5-a49a-7e5a1cc7ea59", // Note this is not necessary a GUID
  "exp": 1504683475, // Equals iat + 30 seconds
  "iat": 1504683445
}
```

Processing a JWT

- A server SHALL NOT accept a JWT more than once for authentication of the Client. However within it's time to live a Service Provider MAY forward a JWT from a Service Consumer to one or more other servers (Entitled Party or Authorisation Registry) to obtain additional evidence on behalf of the Service Consumer. These other servers SHALL accept the JWT for indirect authentication of the Service Consumer during the JWT's complete time to live
- A server SHALL only accept a forwarded JWT if the `aud` claim of the forwarded JWT matches the `iss` claim of the JWT from the client that forwards the JWT
- JWT contents that are not specified within the iSHARE scope SHOULD be ignored

5.2.1.9 XACML 3.0

Within iSHARE, it is essential to provide fine-grained authorisation. Besides rules on the authorisation, it is important to have varying options to describe the resources and its attributes to which the rules apply.

XACML 3.0 is a specification for describing such authorisation rules, but it is XML-based. For iSHARE, a JSON port was created for expressing the XACML specifications regarding authorisation. This 'delegation evidence structure' is discussed in more detail in the chapter on delegation evidence structure (see page 158).

On this page a brief description of XACML is provided. For the most recent version of the specification click on this link[52].

52 http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

Description

XACML (eXtensible Access Control Markup Language) is an XML-based specification that is designed to control access to applications. One of the main advantages of this specification is that applications and systems with their own and different authorisation structure can be integrated into one authorisation scheme. Authorisations and the rules surrounding it can be managed centrally regardless of authorisation mechanism of the applications themselves. This phenomenon is called externalisation. XACML is derived from SAML and provides the underlying specification for ABAC (Attribute-Based Access Control). XACML is also suitable to be used in combination with RBAC (Role-Based Access Control).

Moreover, with the help of XACML authorisations can be arranged and managed in detail. This is called fine-grained authorisation. XACML supports the use of security labels, rules with arbitrary attributes, rules with a certain duration and dynamic rules.

In XACML two main functions can be distinguished. One function defines the criteria with which authorisations are assigned, such as 'only an experienced user from department X is allowed to modify documents'. The other function compares the criteria with the rules or policies to determine whether a person is allowed to perform the operation on the object or not.

The architecture of XACML is fairly complex. This is partly due to the fact that it is difficult to fit the various components of XACML in the application landscape. These components should be positioned in such a way that the owner of the data can somehow control the authorisations to his or her data, but at the same time the components should be positioned in such a way that the performance is not negatively influenced. This is extra important when independent parties need to cooperate with each other and want to jointly organise the access to their applications. Finally, applications need to be compatible with XACML.

5.2.2 Role-specific technical specifications

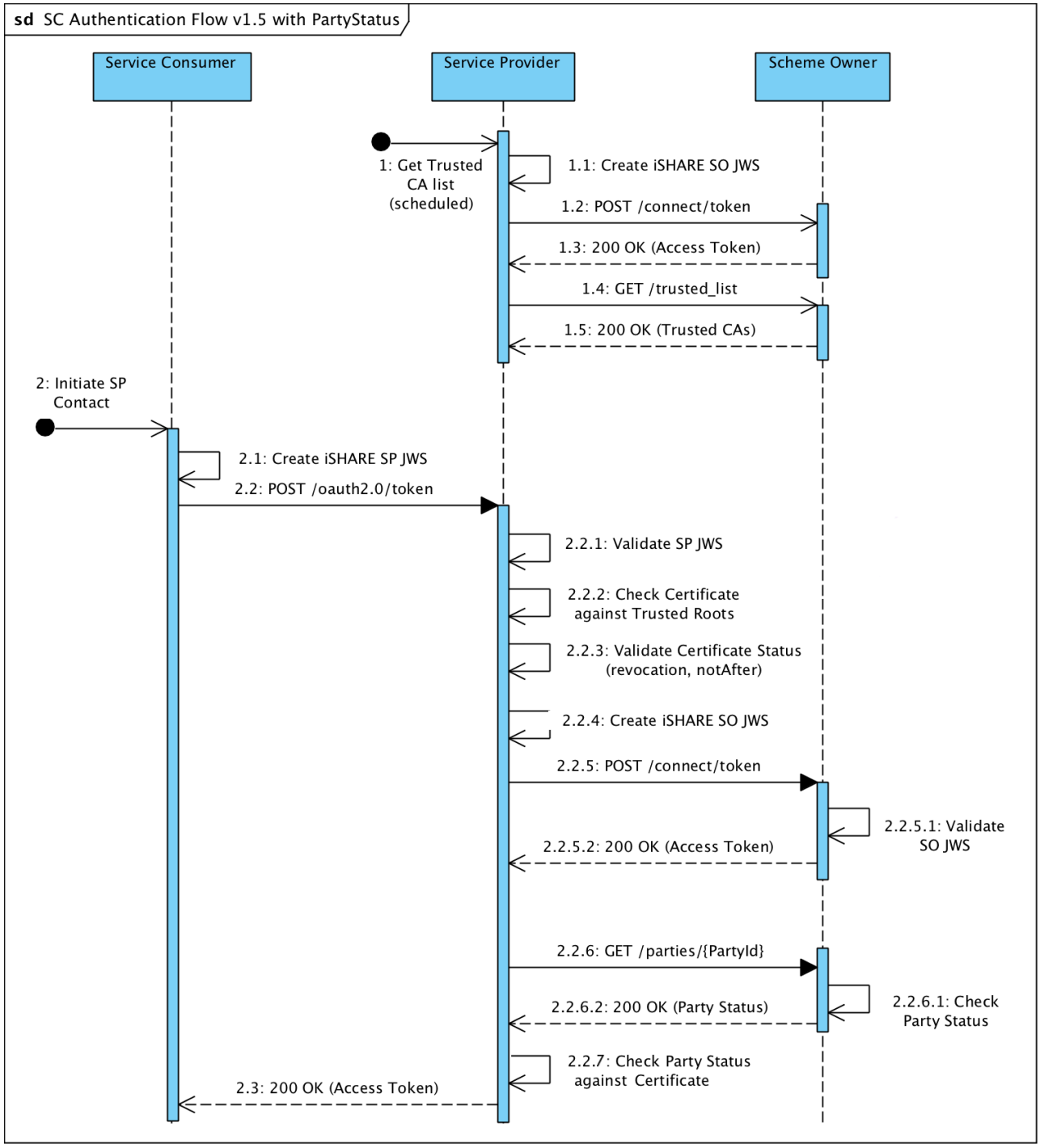
This section contains information on role-specific technical specifications, to be implemented by a legal entity fulfilling iSHARE role(s):

5.2.2.1 For all roles

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Based on the described standards and specifications in this document, the generic iSHARE Authentication flow is described in the following sequence diagram.

The sequence diagram refers to Service Consumer, Service Provider and Scheme Owner. Please note that this Authentication flow applies to various possible interactions. Each party that needs to authenticate another party requesting data or services can be authenticated through this flow.



This chapter specifies the API 'iSHARE function support'. This API MUST be implemented by all parties that implement one or more other iSHARE APIs.

iSHARE function support

GET /any_ishare_party/ishare/capabilities

Retrieves the iSHARE capabilities (supported versions and optional features) of the iSHARE party.

Specifically does not specify the iSHARE version in the URL, as it is used to request which iSHARE versions are supported by a party.

Parameter	Contained in	Type	Required	Description
authorization	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer" + access token value

Responses

Code	Description
200	OK

Example value

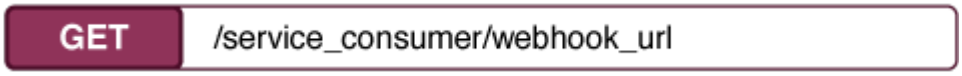
```
Content-Type: application/json

{
  "party_id": "string",
  "ishare_roles": [
    {
      "role": "string"
    }
  ],
  "supported_versions": [
    {
      "version": "string",
      "supported_features": [
        {
          "feature": "string"
        }
      ]
    }
  ]
}
```

5.2.2.2 Role: Service Consumer (concept)

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter specifies the API for event handling that MAY be implemented by a Service Consumer. If a Service Consumer decides to implement the API, it MUST also implement the 'iSHARE function support' API described separately (see page 116).

Broadcast function



Service Consumer defined URL that is registered to recieve certain event types from the Service Provider

Parameter	Contained in	Type	Required	Description
`event_id`	query	string	Yes	Event ID of the service provide that can be used to retieve event information

Responses

Code	Description
200	OK

5.2.2.3 Role: Entitled Party

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter specifies the APIs that MAY be implemented by an Entitled Party. IF an Entitled Party decides to implement one or both APIs, it MUST also implement the 'iSHARE function support' API described separately (see page 116).

OAuth access token

POST /entitled_party/oauth2.0/token

Used to obtain an OAuth access token from the Entitled Party.

Parameter	Contained in	Type	Required	Description
`grant_type`	body	string	Yes	OAuth 2.0 grant type. MUST contain “client_credentials”
`scope`	body	string	No	OAuth 2.0 scope. Defaults to "iSHARE", indicating all rights are requested. Other values MAY be specified by the API owner and allow to get tokens that do not include all rights
`client_id`	body	string	Yes	OpenID Connect 1.0 client ID. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain a valid iSHARE identifier[53]
`client_assertion_type`	body	string	Yes	OpenID Connect 1.0 client assertion type. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”
`client_assertion`	body	string	Yes	OpenID Connect 1.0 client assertion. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain JWT conform iSHARE specifications[54]

53 https://innopay.atlassian.net/wiki/spaces/IS/pages/93782017/Party+identifiers
54 https://innopay.atlassian.net/wiki/spaces/IS/pages/79364112/Generic+iSHARE+JWT+specifications

Example OAuth token request

```
POST /token HTTP/1.1
Host: randomserver.com/entitled_party/oauth2.0/token
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&
scope=iSHARE&client_id=EU.EORI.NL000000001&client_assertion_type=urn:ietf:params:oauth:clie
nt
-assertion-type:jwt-
bearer&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNS
UlHQVRDQ0ErbWdBd0lCQWdJQ0VBb3dEUVlKS29aSWh2Y05BUUVMQlFBd2daQXhDekFKQmdOVkJBWVRBazVNTVFzd0NR
WU
RWUVFJREFKT1NERVBNQTBHQTFVRUNnd0dhVk5JUVZKRk1SRXdEd1lEVlFRTERBaFRaV04xY21sMGVURW9NQ1lHQTFVR
UF
3d2ZhVk5JUVZKRklFNU1JRU5sY25ScFptbGpZWFJsSUVGMWRHaHZjbWwwZVRFbU1DUUdDU3FHU0liM0RRRUpBUllYYV
c1
bWIwQnBjMmhoY21VdGNISnZhbVZqZEM1dmNtY3dIaGNOTVRjeE1ERXlNRGd6TXpVNVdoY05NVGd4TURJeU1EZ3pNelU
1V
2pDQmxURUxNQWtHQTFVRUJoTUNUa3d4Q3pBSkJnTlZCQWdNQWs1SU1SSXdFQVlEVlFRSERBbEJiWE4wWlhKa1lXMHhE
ek
FOQmdOVkJBb01CbWxUU0VGU1JURVdNQlFHQTFVRUN3d05SSFZ0YlhrZ1ptOXlJRkJQUXpFVU1CSUdBMVVFQXd3TFRrd
3d
NREF3TURBd01ERXhKakFrQmdrcWhraUc5dzBCQ1FFV0YybHVabTlBYVhOb1lYSmxMWEJ5YjJwbFkzUXViM0puTUlJQk
lq
QU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUF2LzVmdElwdTE0bnl2MG9DUmRydEpsVk9icEV0Tmp
kT
FNNSSs3SzJOL05GWHlOUGFQM3c0ajB2a29Ma0lVUmJEaTJ3S29oUXNqanJEM21yR1RWN1ZqdWlaSzM1WlZPMGtlczly
ZU
hoeTNHNnIxMTJ4S2x1N3QwWmJxU2I2U3hrMW94c0FxQWppOUsyemtwN055UW00NVd4OFJEQzBsTytYalBpbExUZEp2V
lV
nWktlVkRmc1l6QjV5NXc2WG90aE1VNGgyNzBoVUNibkYwZ1FyQjFzL0RPeC9yd2xqMHc5ZmRTYjlsZk9SdzE2SUM5T3
B3
VzdsQU5kdTFkeTY4RnpGdHdxK1BHNXJBWThXOGU3MGNiT0hSSVRERjNKSjRlelEzY0NsaFlBQ3JPdUEvdkV2bnU0MzN
Ob
ml3UGVGa2VWSGhqQlIzOG53RzljQWJGU2d2Sm9rM1FJREFRQUJvNElCWERDQ0FWZ3dDUVlEVlIwVEJBSXdBREFSQmds
Z2
hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWklBWWI0UWdFTkJDWVdKRTl3Wlc1VFUwd2dSMlZ1WlhKaGRHVmtJRk5sY
25
abGNpQkRaWEowYVdacFkyRjBaVEFkQmdOVkhRNEVGZ1FVZnpHMElFMEV2OFBxZUNTbHJvTXVOTmlkNFA0d2diNEdBMV
Vk
SXdTQnRqQ0JzNEFVamtaTjB4U0pxbGNpWlZTTDFQYlZtd0kzM091aGdaYWtnWk13Z1pBeEN6QUpCZ05WQkFZVEFrNU1
NU
XN3Q1FZRFZRUUlEQUpPU0RFU01CQUdBMVVFQnd3SlFXMXpkR1Z5WkdGdE1ROHdEUVlEVlFRS0RBWnBVMGhCVWtVeEVU
QV
BCZ05WQkFzTUNGTmxZM1Z5YVhSNU1SUXdFZ1lEVlFRERBdHBVMGhCVWtVZ1VtOXZkREVtTUNRR0NTcUdTSWIzRFFFS
kF
SWVhhVzVtYjBCcGMyaGhjbVV0Y0hKdmFtVmpkQzV2Y21lQ0FoQUFNQTRHQTFVZER3RUIvd1FFQXdJRm9EQVRCZ05WSF
NV
RUREQUtCZ2dyQmdFRkJRY0RBVEFOQmdrcWhraUc5dzBCQVFzRkFBT0NBZ0VBRGpvUVlxdjVIS3pKckY5bUttUy9PQjM
vM
```

0FodFJQVm1WRHFkTmNPdytHVTE0SXNLczQwN3ArbFhuMmhON2VaUEpwSVpyVDdqQzl2ZnVOTG1PbzEybXZ0YlBGeTdD
cT
krU1lCNkEvZ2NXK0NZemIrKzBWM3o0ZlR5Y1ZjRXVRQWc4ODM5TWM2clNhSXRha0Q3YnN1Y2EvTldyZFVqSUU1eDBNQ
2Z
YQ21WTS9NeXdlNHdGdEE5ZU5yN0Z1SUN4L0JhdkVnSU8rVmRFdDBKVUp6WGNYK0wrbGM1T0FCQlNidHZjT2pWblRHRD
Vu
T3ZodFdrQy80eWpaVmx3Y2EyK1E4OVBGcVI2OTRYRjhvc0szWFZTWGZVK2pmUk50K0EyeXpWTmpaemVucDF6a1RiZkd
ua
XBDek9QcllaMGxDUzZPUkF3cDdoZ1BrS3hJb1BqTjJkTE11TzAyWVZkV2t2SFVvTXNoN0F0Mjh0RGM2TEVsTjc1Zlgx
bn
VPdjgxMUcyYURxU0d6Rnc0SkdRU25lR3hsaDlMekdzaEkxaWorTm5pQm5uOTYrMGpHSm5OSjJGY3F1Y2dpZ21tSWVvY
0h
6QjlLV3Q3eFRzZmdnVFduZjd3dzA3OGgvZStrNFZ3V2JITjUrcXdURHFra2poTHh6Vm9jTzRHVWw2RzZXUmg2VHp6ek
Fq
SUNiS1BZclI5VWcxaGYxSFNOcG93RHU1MWlxVStmV1VZV0FRcVVSakV2Z0k0aFBmcVhya0x5NVR6OVdLQ1diR0hyRnR
5Z
VlXdGpxenhXdzlpN3Fwc3d3S002M1RLQ1dVVWJoNTlJTitFSTZqczhUMTc2b2tkSkVUUFRaOXpGcjNvNHBIVERBS0VO
RE
hmcjJwT293emZsazlhM3F3RTkvNndxMlhhalI1R289Il19.eyJpc3MiOiJFVS5FT1JJLk5MMDAwMDAwMDAxIiwic3Vi
Ij
oiRVUuRU9SSS5OTDAwMDAwMDAwMSIsImp0aSI6InpGMXFHS0J2NzgiLCJpYXQiOiIxNTEzMDcwODY3IiwiZXhwIjoxN
TE
zMDcwODk3LCJuYmYiOjE1MTMwNzA4NjcsImF1ZCI6Ik5MLkVPUkkuTkw4MTI0NTg4MzcifQ.bPOTFBBg8pedWkfoRKM
t1
uaa0albfWkgSObePtOSKxV0VOPUb1uencLihV086HWJeqO7DBZ2jx_rn96FfpojJnn2z2aQnBSX06IYPTYYcze543-
wb-
8vCor7hM6idGBbDCmeKQvFrIYaYmt34GeU0UjWnNMPGdh90vzbhqgPUlZixtUWfQYn0NxYJf7RGmEhmRybXm2zFl0oo
om
1d-zoZzwuTAzfZqa2rM986VG8WikewxN2IUafhKoQ_w42MB6WpPki8a0EJ07xUZozSybSQvFRWyKxN-
TCtixp3B5nGo9T
uZvkOf1f0RpL8-zTU2DQOFnhz8p7gwF10srNYYv3Sw

Responses

Code	Description
200	OK

Example value

```
Content-Type: application/json

{
  "access_token": "string",
  "token_type": "string",
  "expires_in": 3600
}
```

Delegation evidence

Entitled Parties can be able to provide delegation information concerning rights that the Entitled Party itself has delegated to a Service Consumer.

If the Entitled Party is able to provide these delegations in a M2M context, then the Entitled Party should provide a delegation endpoint.

POST /entitled_party/ishare1.0/delegation

Used to obtain delegation evidence from an Entitled Party. Note a Service Provider MUST validate the Entitled Party only provides information about his own delegations.

Parameter	Contained in	Type	Required	Description
`Authorization`	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
`delegation_mask`	body	string	No	iSHARE specific, optional, base64 encoded JSON structure that acts as a mask to delegation evidence
`previous_steps`	body	string	No	iSHARE specific, optional, base64 encoded JSON array of previous steps. A step can be a previous delegation evidence statement or a client assertion. Used when the party requesting delegation evidence is not the delegator or the delegate of that delegation. The previous steps are used to prove that the requesting party indeed has legitimate reason to request the delegation evidence

Responses

Code	Description

200 OK

example value JWT


```
{
"delegationEvidence":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZWxlZ2F0aW9
uRXZpZGVuY2UiOnsibm90QmVmb3JlIjoxNTA5NjMzNjgxLCJub3RP
bk9yQWZ0ZXIiOjE1MDk2MzM3NDEsInBvbGljeUlzc3VlciI6IkVVL
kVPUkkuTkwxMjM0NTY3ODkiLCJ0YXJnZXQiOnsiYWNjZXNzU3Viam
VjdCI6IkVVLkVPUkkuTkwwMTIzNDU2NzgifSwicG9saWN5U2V0cyI
6W3sibWF4RGVsZWdhdGlvbkRlcHRoIjoyLCJ0YXJnZXQiOnsiZW52
aXJvbm1lbnQiOnsibGljZW5zZXMiOlsiSVNIQVJFLjAwMDEiLCJJU
0hBUkUuMDAwMyJdfX0sInBvbGljaWVzIjpbeyJ0YXJnZXQiOnsicm
Vzb3VyY2UiOnsidHlwZSI6IkdTMS5DT05UQUlORVIiLCJpZGVudGl
maWVycyI6WyIqIl0sImF0dHJpYnV0ZXMiOlsiR1MxLkNPTlRBSU5F
Ui5BVFRSSUJVVEUuRVRBIiwiR1MxLkNPTlRBSU5FUi5BVFRSSUJVV
EUuV0VJR0hUIl19LCJhY3Rpb25zIjpbIklTSEFSRS5SRUFEIiwiSV
NIQVJFLkNSRUFURSJdLCJlbnZpcm9ubWVudCI6eyJzZXJ2aWNlUHJ
vdmlkZXJzIjpbIkVVLkVPUkkuTkwxMjM0MTIzNDUiXX19LCJydWxl
cyI6W3siZWZmZWN0IjoiUGVybWl0In0seyJlZmZlY3QiOiJEZW55I
iwidGFyZ2V0Ijp7InJlc291cmNlIjp7ImF0dHJpYnV0ZXMiOlsiR1
MxLkNPTlRBSU5FUi5BVFRSSUJVVEUuRVRBIl19LCJhY3Rpb25zIjp
bIklTSEFSRS5DUkVBVEUiXX19LHsiZWZmZWN0IjoiRGVueSIsInRh
cmdldCI6eyJyZXNvdXJjZSI6eyJpZGVudGlmaWVycyI6WyJHUzEuQ
09OVEFJTkVSLklELjAwMDAwMDAwMDAxIl19fX1dfV19XX19.iB1cp
lUm5TtGqzxcmVJU5ZtKve-2yPSelE1xLMLwI_0"
}
```


Example value - delegationEvidence


```
{
    "delegationEvidence": {
        "notBefore": 1509633681,
        "notOnOrAfter": 1509633741,
        "policyIssuer": "EU.EORI.NL123456789",
        "target": {
            "accessSubject": "EU.EORI.NL012345678"
        },
        "policySets": [
            {
                "maxDelegationDepth": 2,
                "target": {
                    "environment": {
                        "licenses": ["ISHARE.0001", "ISHARE.0003"]
                    }
                },
                "policies": [
                    {
```

```
                        "target": {
                            "resource": {
                                "type": "GS1.CONTAINER",
                                "identifiers": ["*"],
                                "attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA",

"GS1.CONTAINER.ATTRIBUTE.WEIGHT"]
                            },
                            "actions": ["ISHARE.READ", "ISHARE.CREATE"],
                            "environment": {
                                "serviceProviders": ["EU.EORI.NL123412345"]
                            }
                        },
                        "rules": [
                            {
                                "effect": "Permit"
                            },
                            {
                                "effect": "Deny",
                                "target": {
                                    "resource": {
                                        "attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA"]
                                    },
                                    "actions": ["ISHARE.CREATE"]
                                }
                            },
                            {
                                "effect": "Deny",
                                "target": {
                                    "resource": {
                                        "identifiers": ["GS1.CONTAINER.ID.00000000001"]
                                    }
                                }
                            }
                        ]
                    }
                ]
            }
        ]
    }
}
```


5.2.2.4 Role: Service Provider

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter specifies the APIs that can be implemented by a Service Provider:

- POST OAuth access token MUST be implemented;
- GET OpenID Connect return (redirect) MUST be implemented IF the Service Provider wants to facilitate Human to Machine interaction;
- GET service MAY be implemented;

- POST service MAY be implemented;
- PATCH service MAY be implemented;
- DELETE service MAY be implemented;
- PUT service MAY be implemented.

A Service Provider MUST also implement the 'iSHARE function support' API described separately (see page 116).

Additionally, a concept version of APIs for event handling can be found here[55].

OAuth access token

POST /service_provider/oauth2.0/token

Used to obtain an OAuth access token from the Service Provider.

Parameter	Contained in	Type	Required	Description
`grant_type`	body	string	Yes	OAuth 2.0 grant type. MUST contain “client_credentials”
`scope`	body	string	No	OAuth 2.0 scope. Defaults to "iSHARE", indicating all rights are requested. Other values MAY be specified by the API owner and allow to get tokens that do not include all rights
`client_id`	body	string	Yes	OpenID Connect 1.0 client ID. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain a valid iSHARE identifier[56]
`client_assertion_type`	body	string	Yes	OpenID Connect 1.0 client assertion type. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”

55 https://innopay.atlassian.net/wiki/pages/createpage.action?fromPageId=173211792&linkCreation=true&spaceKey=IS&title=Event+handling+APIs+%28concept%29
56 https://innopay.atlassian.net/wiki/spaces/IS/pages/93782017/Party+identifiers

`client_assertion`	body	string	Yes	OpenID Connect 1.0 client assertion. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain JWT conform iSHARE specifications[57]

57 https://innopay.atlassian.net/wiki/spaces/IS/pages/79364112/Generic+iSHARE+JWT+specifications

Example OAuth token request

```
POST /token HTTP/1.1
Host: randomserver.com/service_provider/oauth2.0/token
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&
scope=iSHARE&client_id=EU.EORI.NL000000001&client_assertion_type=urn:ietf:params:oauth:clie
nt
-assertion-type:jwt-
bearer&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNS
UlHQVRDQ0ErbWdBd0lCQWdJQ0VBb3dEUVlKS29aSWh2Y05BUUVMQlFBd2daQXhDekFKQmdOVkJBWVRBazVNTVFzd0NR
WU
RWUVFJREFKT1NERVBNQTBHQTFVRUNnd0dhVk5JUVZKRk1SRXdEd1lEVlFRTERBaFRaV04xY21sMGVURW9NQ1lHQTFVR
UF
3d2ZhVk5JUVZKRklFNU1JRU5sY25ScFptbGpZWFJsSUVGMWRHaHZjbWwwZVRFbU1DUUdDU3FHU0liM0RRRUpBUllYYV
c1
bWIwQnBjMmhoY21VdGNISnZhbVZqZEM1dmNtY3dIaGNOTVRjeE1ERXlNRGd6TXpVNVdoY05NVGd4TURJeU1EZ3pNelU
1V
2pDQmxURUxNQWtHQTFVRUJoTUNUa3d4Q3pBSkJnTlZCQWdNQWs1SU1SSXdFQVlEVlFRSERBbEJiWE4wWlhKa1lXMHhE
ek
FOQmdOVkJBb01CbWxUU0VGU1JURVdNQlFHQTFVRUN3d05SSFZ0YlhrZ1ptOXlJRkJQUXpFVU1CSUdBMVVFQXd3TFRrd
3d
NREF3TURBd01ERXhKakFrQmdrcWhraUc5dzBCQ1FFV0YybHVabTlBYVhOb1lYSmxMWEJ5YjJwbFkzUXViM0puTUlJQk
lq
QU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUF2LzVmdElwdTE0bnl2MG9DUmRydEpsVk9icEV0Tmp
kT
FNNSSs3SzJOL05GWHlOUGFQM3c0ajB2a29Ma0lVUmJEaTJ3S29oUXNqanJEM21yR1RWN1ZqdWlaSzM1WlZPMGtlczly
ZU
hoeTNHNnIxMTJ4S2x1N3QwWmJxU2I2U3hrMW94c0FxQWppOUsyemtwN055UW00NVd4OFJEQzBsTytYalBpbExUZEp2V
lV
nWktlVkRmc1l6QjV5NXc2WG90aE1VNGgyNzBoVUNibkYwZ1FyQjFzL0RPeC9yd2xqMHc5ZmRTYjlsZk9SdzE2SUM5T3
B3
VzdsQU5kdTFkeTY4RnpGdHdxK1BHNXJBWThXOGU3MGNiT0hSSVRERjNKSjRlelEzY0NsaFlBQ3JPdUEvdkV2bnU0MzN
Ob
ml3UGVGa2VWSGhqQlIzOG53RzljQWJGU2d2Sm9rM1FJREFRQUJvNElCWERDQ0FWZ3dDUVlEVlIwVEJBSXdBREFSQmds
Z2
hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWklBWWI0UWdFTkJDWVdKRTl3Wlc1VFUwd2dSMlZ1WlhKaGRHVmtJRk5sY
25
abGNpQkRaWEowYVdacFkyRjBaVEFkQmdOVkhRNEVGZ1FVZnpHMElFMEV2OFBxZUNTbHJvTXVOTmlkNFA0d2diNEdBMV
Vk
SXdTQnRqQ0JzNEFVamtaTjB4U0pxbGNpWlZTTDFQYlZtd0kzM091aGdaYWtnWk13Z1pBeEN6QUpCZ05WQkFZVEFrNU1
NU
XN3Q1FZRFZRUUlEQUpPU0RFU01CQUdBMVVFQnd3SlFXMXpkR1Z5WkdGdE1ROHdEUVlEVlFRS0RBWnBVMGhCVWtVeEVU
QV
BCZ05WQkFzTUNGTmxZM1Z5YVhSNU1SUXdFZ1lEVlFRERBdHBVMGhCVWtVZ1VtOXZkREVtTUNRR0NTcUdTSWIzRFFFS
kF
SWVhhVzVtYjBCcGMyaGhjbVV0Y0hKdmFtVmpkQzV2Y21lQ0FoQUFNQTRHQTFVZER3RUIvd1FFQXdJRm9EQVRCZ05WSF
NV
RUREQUtCZ2dyQmdFRkJRY0RBVEFOQmdrcWhraUc5dzBCQVFzRkFBT0NBZ0VBRGpvUVlxdjVIS3pKckY5bUttUy9PQjM
vM
```

0FodFJQVm1WRHFkTmNPdytHVTE0SXNLczQwN3ArbFhuMmhON2VaUEpwSVpyVDdqQzl2ZnVOTG1PbzEybXZ0YlBGeTdD
cT
krU1lCNkEvZ2NXK0NZemIrKzBWM3o0ZlR5Y1ZjRXVRQWc4ODM5TWM2clNhSXRha0Q3YnN1Y2EvTldyZFVqSUU1eDBNQ
2Z
YQ21WTS9NeXdlNHdGdEE5ZU5yN0Z1SUN4L0JhdkVnSU8rVmRFdDBKVUp6WGNYK0wrbGM1T0FCQlNidHZjT2pWblRHRD
Vu
T3ZodFdrQy80eWpaVmx3Y2EyK1E4OVBGcVI2OTRYRjhvc0szWFZTWGZVK2pmUk50K0EyeXpWTmpaemVucDF6a1RiZkd
ua
XBDek9QcllaMGxDUzZPUkF3cDdoZ1BrS3hJb1BqTjJkTE11TzAyWVZkV2t2SFVvTXNoN0F0Mjh0RGM2TEVsTjc1Zlgx
bn
VPdjgxMUcyYURxU0d6Rnc0SkdRU25lR3hsaDlMekdzaEkxaWorTm5pQm5uOTYrMGpHSm5OSjJGY3F1Y2dpZ21tSWVvY
0h
6QjlLV3Q3eFRzZmdnVFduZjd3dzA3OGgvZStrNFZ3V2JITjUrcXdURHFra2poTHh6Vm9jTzRHVWw2RzZXUmg2VHp6ek
Fq
SUNiS1BZclI5VWcxaGYxSFNOcG93RHU1MWlxVStmV1VZV0FRcVVSakV2Z0k0aFBmcVhya0x5NVR6OVdLQ1diR0hyRnR
5Z
VlXdGpxenhXdzlpN3Fwc3d3S002M1RLQ1dVVWJoNTlJTitFSTZqczhUMTc2b2tkSkVUUFRaOXpGcjNvNHBIVERBS0VO
RE
hmcjJwT293emZsazlhM3F3RTkvNndxMlhhalI1R289Il19.eyJpc3MiOiJFVS5FT1JJLk5MMDAwMDAwMDAxIiwic3Vi
Ij
oiRVUuRU9SSS5OTDAwMDAwMDAwMSIsImp0aSI6InpGMXFHS0J2NzgiLCJpYXQiOiIxNTEzMDcwODY3IiwiZXhwIjoxN
TE
zMDcwODk3LCJuYmYiOjE1MTMwNzA4NjcsImF1ZCI6Ik5MLkVPUkkuTkw4MTI0NTg4MzcifQ.bPOTFBBg8pedWkfoRKM
t1
uaa0albfWkgSObePtOSKxV0VOPUb1uencLihV086HWJeqO7DBZ2jx_rn96FfpojJnn2z2aQnBSX06IYPTYYcze543-
wb-
8vCor7hM6idGBbDCmeKQvFrIYaYmt34GeU0UjWnNMPGdh90vzbhqgPUlZixtUWfQYn0NxYJf7RGmEhmRybXm2zFl0oo
om
1d-zoZzwuTAzfZqa2rM986VG8WikewxN2IUafhKoQ_w42MB6WpPki8a0EJ07xUZozSybSQvFRWyKxN-
TCtixp3B5nGo9T
uZvkOf1f0RpL8-zTU2DQOFnhz8p7gwF10srNYYv3Sw

Responses

Code	Description
200	OK

Example value


```
{
  "access_token": "string",
  "token_type": "string",
  "expires_in": 3600
}
```

OpenID Connect redirect_uri

GET /service_provider/openid_connect1.0/return

OpenID Connect end-point for recieving the redirect from the Identity Provider or Identity Broker. Not bound to name 'return'. MAY have any name the Service Provider chooses

Parameter	Contained in	Type	Required	Description
code	query	string	Yes	OAuth 2.0 authorisation code for retrieving access_token & id_token
state	query	string	Yes	OpenID Connect 1.0 state. MUST contain the state as provided by the Service Provider in the request to the Identity Provider or Identity Broker

Responses

Code	Description
200	OK

Service Provision

POST /service_provider/service

This is an example service to show how any Service Provider that adheres to iSHARE MUST apply iSHARE conformant OAuth to every iSHARE enabled service. Not bound to name 'service'. MAY have any name the Service Provider chooses

Parameter	Contained in	Type	Required	Description
authorization	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
service_consumer_assertion	header	string	No	iSHARE specific optional client assertion. Used when a Service Consumer is requesting a service on behalf of another Service Consumer in a 'service broker' pattern. It is used to prove that the 'brokering' Service Consumer indeed has had a request from the original Service Consumer
Do-Not-Sign	header	boolean	No	Optional iSHARE specific boolean indicating the response SHALL not be signed
License	header	string	No	Optional iSHARE specific value describing the license the Service Consuming Entity requests for the data in the service response
Service-Headers	header	string	No	Any service specific headers
Responses				
Code	**Description**			

200	OK
	Example value
	{
	"service_content_1": "string",
	"service_content_n": "string"
	}
	Headers:
	Name / **Description** / **Type**
	License / Optional iSHARE specific value describing the license the Service Consuming Entity receives for the data in the service response / string

Service Provision

PATCH /service_provider/service

This is an example service to show how any Service Provider that adheres to iSHARE MUST apply iSHARE conformant OAuth to every iSHARE enabled service. Not bound to name 'service'. MAY have any name the Service Provider chooses

Parameter	Contained in	Type	Required	Description
authorization	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
service_consumer_assertion	header	string	No	iSHARE specific optional client assertion. Used when a Service Consumer is requesting a service on behalf of another Service Consumer in a 'service broker' pattern. It is used to prove that the 'brokering' Service Consumer indeed has had a request from the original Service Consumer

Do-Not-Sign	header	boolean	No	Optional iSHARE specific boolean indicating the response SHALL not be signed
License	header	string	No	Optional iSHARE specific value describing the license the Service Consuming Entity requests for the data in the service response
Service-Headers	header	string	No	Any service specific headers

Responses

Code	Description
200	OK **Example value** `{ "service_content_1": "string", "service_content_n": "string" }` **Headers:** **Name** / **Description** / **Type** License / Optional iSHARE specific value describing the license the Service Consuming Entity receives for the data in the service response / string

Service Provision

DELETE /service_provider/service

This is an example service to show how any Service Provider that adheres to iSHARE MUST apply iSHARE conformant OAuth to every iSHARE enabled service. Not bound to name 'service'. MAY have any name the Service Provider chooses

Parameter	Contained in	Type	Required	Description
authorization	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
service_consumer_assertion	header	string	No	iSHARE specific optional client assertion. Used when a Service Consumer is requesting a service on behalf of another Service Consumer in a 'service broker' pattern. It is used to prove that the 'brokering' Service Consumer indeed has had a request from the original Service Consumer
Do-Not-Sign	header	boolean	No	Optional iSHARE specific boolean indicating the response SHALL not be signed
License	header	string	No	Optional iSHARE specific value describing the license the Service Consuming Entity requests for the data in the service response
Service-Headers	header	string	No	Any service specific headers
Responses				
Code	**Description**			

200	OK
	
	Example value
	
	{
	"service_content_1": "string",
	"service_content_n": "string"
	}
	
	Headers:
	
	Name / **Description** / **Type**
	License / Optional iSHARE specific value describing the license the Service Consuming Entity receives for the data in the service response / string

Service Provision

PUT /service_provider/service

This is an example service to show how any Service Provider that adheres to iSHARE MUST apply iSHARE conformant OAuth to every iSHARE enabled service. Not bound to name 'service'. MAY have any name the Service Provider chooses

Parameter	Contained in	Type	Required	Description
authorization	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
service_consumer_assertion	header	string	No	iSHARE specific optional client assertion. Used when a Service Consumer is requesting a service on behalf of another Service Consumer in a 'service broker' pattern. It is used to prove that the 'brokering' Service Consumer indeed has had a request from the original Service Consumer

Do-Not-Sign	header	boolean	No	Optional iSHARE specific boolean indicating the response SHALL not be signed
License	header	string	No	Optional iSHARE specific value describing the license the Service Consuming Entity requests for the data in the service response
Service-Headers	header	string	No	Any service specific headers

Responses

Code	Description
200	OK

Example value

```
{
  "service_content_1": "string",
  "service_content_n": "string"
}
```

Headers:

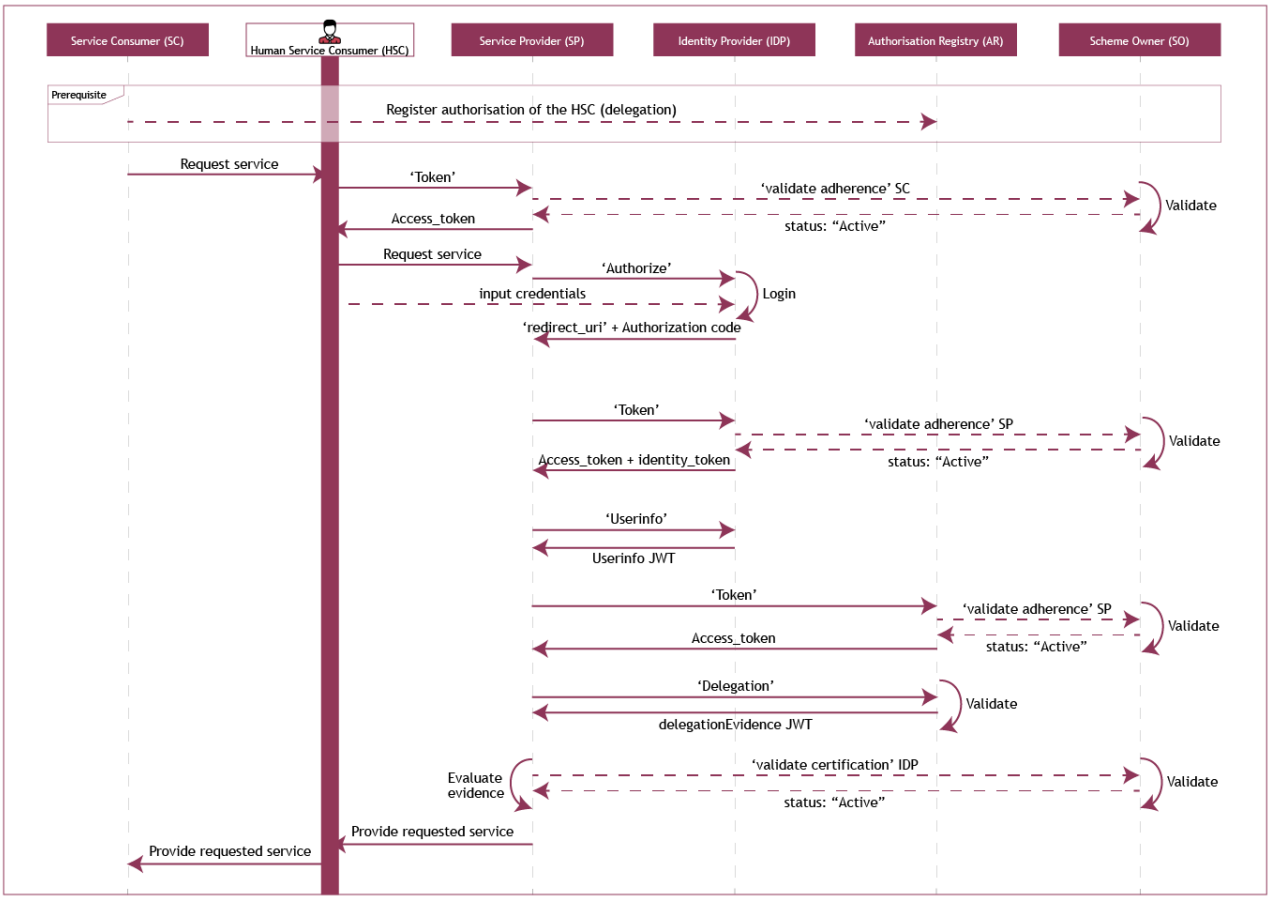
Name	Description	Type
License	Optional iSHARE specific value describing the license the Service Consuming Entity receives for the data in the service response	string

5.2.2.5 Role: Identity Provider

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter specifies the APIs that MUST be implemented by an Identity Provider. An Identity Provider MUST also implement the 'iSHARE function support' API described separately (see page 116).

The OpenID Connect 1.0 identification and authentication flow consists of three consecutive API calls, 'Authorize', 'Token' and 'Userinfo':



OpenID Connect 1.0 - Authorize

GET `/identity_provider/openid_connect1.0/authorize`

OpenID Connect endpoint for redirecting Human Service Consumer for authentication by the Identity Provider

Parameter	Contained in	Type	Required	Description
`response_type`	query	string	Yes	OAuth 2.0 Response Type. For iSHARE using the Authorization Code Flow, with value 'code' is REQUIRED.

client_id	query	string	Yes	OpenID Connect 1.0 client ID. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain a valid iSHARE identifier of the Service Provider
redirect_uri	query	string	Yes	OpenID Connect 1.0 redirection URI to which the response will be sent
scope	query	string	Yes	OAuth 2.0 scope for OpenID Connect 1.0. MUST contain the ‘openid’ scope value. Other supported scopes under iSHARE are 'name’, 'contact_details’, ‘company_id’ and ‘company_info’
state	query	string	Yes	Opaque value used to maintain state between the request and the callback. MUST be used in iSHARE
language	query	string	No	iSHARE specific two-letter indicator that guides the language of the user interface shown by the Identity Provider

Responses

Code	Description
200	OK **Example value** `{ "authorization_code": "string" }`

OpenID Connect 1.0 - Token

POST /entitled_party/oauth2.0/token

Used to obtain an OAuth access token from the Authorisation Registry

Parameter	Contained in	Type	Required	Description
`grant_type`	body	string	Yes	OAuth 2.0 grant type. MUST contain “client_credentials”
`code`	body	string	Yes	Oauth 2.0 authorization code. MUST contain value of authorisation code received from the Identity Provider
`redirect_uri`	body	string	Yes	OpenID Connect 1.0 redirection URI to which the response was sent, used to verify that the user will be redirected to the same uri as the Authorize endpoint.
`client_id`	body	string	Yes	OpenID Connect 1.0 client ID. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain a valid iSHARE identifier of the Service Provider
`client_assertion_type`	body	string	Yes	OpenID Connect 1.0 client assertion type. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”
`client_assertion`	body	string	Yes	OpenID Connect 1.0 client assertion. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain JWT token conform iSHARE specifications, signed by the client.
Responses				
Code	**Description**			

200	OK
	Example value
	<pre>{
	  "access_token": "string",
	  "token_type": "string",
	  "expires_in": 3600,
	  "id_token": "string"
	}</pre>
	Cache-Control: MUST contain 'no-store' string
	Pragma: MUST contain 'no-cache' string

OpenID Connect 1.0 - Userinfo

GET /identity_provider/openid_connect1.0/userinfo

OpenID Connect endpoint for obtaining attributes of a Human Service Consumer conform scope defined in access token

Parameter	Contained in	Type	Required	Description
authorization	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
Do-Not-Sign	header	boolean	No	Optional iSHARE specific boolean indicating the response SHALL not be signed

Responses

Code	Description

200	OK
	Example value
	{
	"userinfo_token": "string"
	}

5.2.2.6 Role: Identity Broker

v1.5 of the iSHARE scheme does not yet include specifications for the Identity Broker role.

5.2.2.7 Role: Authorisation Registry

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter specifies the APIs that MUST be implemented by an Authorisation Registry. An Authorisation Registry MUST also implement the 'iSHARE function support' API described separately (see page 116).

OAuth access token

POST /authorisation_registry/oauth2.0/token

Used to obtain an OAuth access token from the Authorisation Registry.

Parameter	Contained in	Type	Required	Description
grant_type	body	string	Yes	OAuth 2.0 grant type. MUST contain “client_credentials”
scope	body	string	No	OAuth 2.0 scope. Defaults to "iSHARE", indicating all rights are requested. Other values MAY be specified by the API owner and allow to get tokens that do not include all rights

`client_id`	body	string	Yes	OpenID Connect 1.0 client ID. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain a valid iSHARE identifier[58]
`client_assertion_type`	body	string	Yes	OpenID Connect 1.0 client assertion type. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain "urn:ietf:params:oauth:client-assertion-type:jwt-bearer"
`client_assertion`	body	string	Yes	OpenID Connect 1.0 client assertion. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain JWT conform iSHARE specifications[59]

58 https://innopay.atlassian.net/wiki/spaces/IS/pages/93782017/Party+identifiers
59 https://innopay.atlassian.net/wiki/spaces/IS/pages/79364112/Generic+iSHARE+JWT+specifications

Example OAuth token request

```
POST /token HTTP/1.1
Host: randomserver.com/authorisation_registry/oauth2.0/token
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&
scope=iSHARE&client_id=EU.EORI.NL000000001&client_assertion_type=urn:ietf:params:oauth:clie
nt
-assertion-type:jwt-
bearer&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNS
UlHQVRDQ0ErbWdBd0lCQWdJQ0VBb3dEUVlKS29aSWh2Y05BUUVMQlFBd2daQXhDekFKQmdOVkJBWVRBazVNTVFzd0NR
WU
RWUVFJREFKT1NERVBNQTBHQTFVRUNnd0dhVk5JUVZKRk1SRXdEd1lEVlFRTERBaFRaV04xY21sMGVURW9NQ1lHQTFVR
UF
3d2ZhVk5JUVZKRklFNU1JRU5sY25ScFptbGpZWFJsSUVGMWRHaHZjbWwwZVRFbU1DUUdDU3FHU0liM0RRRUpBUllYYV
c1
bWIwQnBjMmhoY21VdGNISnZhbVZqZEM1dmNtY3dIaGNOTVRjeE1ERXlNRGd6TXpVNVdoY05NVGd4TURJeU1EZ3pNelU
1V
2pDQmxURUxNQWtHQTFVRUJoTUNUa3d4Q3pBSkJnTlZCQWdNQWs1SU1SSXdFQVlEVlFRSERBbEJiWE4wWlhKa1lXMHhE
ek
FOQmdOVkJBb01CbWxUU0VGU1JURVdNQlFHQTFVRUN3d05SSFZ0YlhrZ1ptOXlJRkJQUXpFVU1CSUdBMVVFQXd3TFRrd
3d
NREF3TURBd01ERXhKakFrQmdrcWhraUc5dzBCQ1FFV0YybHVabTlBYVhOb1lYSmxMWEJ5YjJwbFkzUXViM0puTUlJQk
lq
QU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUF2LzVmdElwdTE0bnl2MG9DUmRydEpsVk9icEV0Tmp
kT
FNNSSs3SzJOL05GWHlOUGFQM3c0ajB2a29Ma0lVUmJEaTJ3S29oUXNqanJEM21yR1RWN1ZqdWlaSzM1WlZPMGtlczly
ZU
hoeTNHNnIxMTJ4S2x1N3QwWmJxU2I2U3hrMW94c0FxQWppOUsyemtwN055UW00NVd4OFJEQzBsTytYalBpbExUZEp2V
lV
nWktlVkRmc1l6QjV5NXc2WG90aE1VNGgyNzBoVUNibkYwZ1FyQjFzL0RPeC9yd2xqMHc5ZmRTYjlsZk9SdzE2SUM5T3
B3
VzdsQU5kdTFkeTY4RnpGdHdxK1BHNXJBWThXOGU3MGNiT0hSSVRERjNKSjRlelEzY0NsaFlBQ3JPdUEvdkV2bnU0MzN
Ob
ml3UGVGa2VWSGhqQlIzOG53RzljQWJGU2d2Sm9rM1FJREFRQUJvNElCWERDQ0FWZ3dDUVlEVlIwVEJBSXdBREFSQmds
Z2
hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWklBWWI0UWdFTkJDWVdKRTl3Wlc1VFUwd2dSMlZ1WlhKaGRHVmtJRk5sY
25
abGNpQkRaWEowYVdacFkyRjBaVEFkQmdOVkhRNEVGZ1FVZnpHMElFMEV2OFBxZUNTbHJvTXVOTmlkNFA0d2diNEdBMV
Vk
SXdTQnRqQ0JzNEFVamtaTjB4U0pxbGNpWlZTTDFQYlZtd0kzM091aGdaYWtnWk13Z1pBeEN6QUpCZ05WQkFZVEFrNU1
NU
XN3Q1FZRFZRUUlEQUpPU0RFU01CQUdBMVVFQnd3SlFXMXpkR1Z5WkdGdE1ROHdEUVlEVlFRS0RBWnBVMGhCVWtVeEVU
QV
BCZ05WQkFzTUNGTmxZM1Z5YVhSNU1SUXdFZ1lEVlFRERBdHBVMGhCVWtVZ1VtOXZkREVtTUNRR0NTcUdTSWIzRFFFS
kF
SWVhhVzVtYjBCcGMyaGhjbVV0Y0hKdmFtVmpkQzV2Y21lQ0FoQUFNQTRHQTFVZER3RUIvd1FFQXdJRm9EQVRCZ05WSF
NV
RUREQUtCZ2dyQmdFRkJRY0RBVEFOQmdrcWhraUc5dzBCQVFzRkFBT0NBZ0VBRGpvUVlxdjVIS3pKckY5bUttUy9PQjM
vM
```

0FodFJQVm1WRHFkTmNPdytHVTE0SXNLczQwN3ArbFhuMmhON2VaUEpwSVpyVDdqQzl2ZnVOTG1PbzEybXZ0YlBGeTdD
cT
krU1lCNkEvZ2NXK0NZemIrKzBWM3o0ZlR5Y1ZjRXVRQWc4ODM5TWM2clNhSXRha0Q3YnN1Y2EvTldyZFVqSUU1eDBNQ
2Z
YQ21WTS9NeXdlNHdGdEE5ZU5yN0Z1SUN4L0JhdkVnSU8rVmRFdDBKVUp6WGNYK0wrbGM1T0FCQlNidHZjT2pWblRHRD
Vu
T3ZodFdrQy80eWpaVmx3Y2EyK1E4OVBGcVI2OTRYRjhvc0szWFZTWGZVK2pmUk50K0EyeXpWTmpaemVucDF6a1RiZkd
ua
XBDek9QcllaMGxDUzZPUkF3cDdoZ1BrS3hJb1BqTjJkTE11TzAyWVZkV2t2SFVvTXNoN0F0Mjh0RGM2TEVsTjc1Zlgx
bn
VPdjgxMUcyYURxU0d6Rnc0SkdRU25lR3hsaDlMekdzaEkxaWorTm5pQm5uOTYrMGpHSm5OSjJGY3F1Y2dpZ21tSWVvY
0h
6QjlLV3Q3eFRzZmdnVFduZjd3dzA3OGgvZStrNFZ3V2JITjUrcXdURHFra2poTHh6Vm9jTzRHVWw2RzZXUmg2VHp6ek
Fq
SUNiS1BZclI5VWcxaGYxSFNOcG93RHU1MWlxVStmV1VZV0FRcVVSakV2Z0k0aFBmcVhya0x5NVR6OVdLQ1diR0hyRnR
5Z
VlXdGpxenhXdzlpN3Fwc3d3S002M1RLQ1dVVWJoNTlJTitFSTZqczhUMTc2b2tkSkVUUFRaOXpGcjNvNHBIVERBS0VO
RE
hmcjJwT293emZsazlhM3F3RTkvNndxMlhhalI1R289Il19.eyJpc3MiOiJFVS5FT1JJLk5MMDAwMDAwMDAxIiwic3Vi
Ij
oiRVUuRU9SSS5OTDAwMDAwMDAwMSIsImp0aSI6InpGMXFHS0J2NzgiLCJpYXQiOiIxNTEzMDcwODY3IiwiZXhwIjoxN
TE
zMDcwODk3LCJuYmYiOjE1MTMwNzA4NjcsImF1ZCI6Ik5MLkVPUkkuTkw4MTI0NTg4MzcifQ.bPOTFBBg8pedWkfoRKM
t1
uaa0albfWkgSObePtOSKxV0VOPUb1uencLihV086HWJeqO7DBZ2jx_rn96FfpojJnn2z2aQnBSX06IYPTYYcze543-
wb-
8vCor7hM6idGBbDCmeKQvFrIYaYmt34GeU0UjWnNMPGdh90vzbhqgPUlZixtUWfQYn0NxYJf7RGmEhmRybXm2zFl0oo
om
1d-zoZzwuTAzfZqa2rM986VG8WikewxN2IUafhKoQ_w42MB6WpPki8a0EJ07xUZozSybSQvFRWyKxN-
TCtixp3B5nGo9T
uZvkOf1f0RpL8-zTU2DQOFnhz8p7gwF10srNYYv3Sw

Responses

Code	Description
200	OK

Example value

```
Content-Type: application/json

{
  "access_token": "string",
  "token_type": "string",
  "expires_in": 3600
}
```

Delegation evidence

POST /authorisation_registry/ishare1.0/delegation

Used to obtain delegation evidence from an Authorisation Registry

Parameter	Contained in	Type	Required	Description
`Authorization`	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
`delegation_mask`	body	string	No	iSHARE specific, optional, base64 encoded JSON structure that acts as a mask to delegation evidence

delegation_path	body	array	No	iSHARE specific, optional, array containing iSHARE identifiers (optionally combined with source of their authorisation) that describe a path of delegation that should be resolved
				
				delegation_path structure example
				
				{
				[
				{
				"partyID": "EU.EORI.NL000000001", // Note that this is the Service Consumer (the third accessSubject in this example)
				},
				{
				"partyID": "EU.EORI.NL123456789", // Second accessSubject & third policyIssuer
				"delegationEvidenceSource": ["EU.EORI.NL123456789"] // In this example, this is where the delegation evidence can be requested
				},
				{
				"partyID": "NL.KVK.12345678", // First accessSubject & second policyIssuer
				"delegationEvidenceSource": ["EU.EORI.NL012345678", "EU.EORI.NL012345679", "EU.EORI.NL012345680"] // In this example, evidence can be requested at any of these three sources (useful for availability reasons)
				},
				{
				"partyID": "NL.KVK.12345679" // ID of the resource owner & first policyIssuer
				// In this example, knowledge of the source of the delegation evidence for this step is assumed to be present
				}
				]
				}

previous_steps	body	string	No	iSHARE specific, optional, base64 encoded JSON array of previous steps. A step can be a previous delegation evidence statement or a client assertion. Used when the party requesting delegation evidence is not the delegator or the delegate of that delegation. The previous steps are used to prove that the requesting party indeed has legitimate reason to request the delegation evidence
Responses				
Code	**Description**			

200 OK

example value JWT


```
{
"delegationEvidence":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkZWxlZ2F0aW9
uRXZpZGVuY2UiOnsibm90QmVmb3JlIjoxNTA5NjMzNjgxLCJub3RP
bk9yQWZ0ZXIiOjE1MDk2MzM3NDEsInBvbGljeUlzc3VlciI6IkVVL
kVPUkkuTkwxMjM0NTY3ODkiLCJ0YXJnZXQiOnsiYWNjZXNzU3Viam
VjdCI6IkVVLkVPUkkuTkwwMTIzNDU2NzgifSwicG9saWN5U2V0cyI
6W3sibWF4RGVsZWdhdGlvbkRlcHRoIjoyLCJ0YXJnZXQiOnsiZW52
aXJvbm1lbnQiOnsibGljZW5zZXMiOlsiSVNIQVJFLjAwMDEiLCJJU
0hBUkUuMDAwMyJdfX0sInBvbGljaWVzIjpbeyJ0YXJnZXQiOnsicm
Vzb3VyY2UiOnsidHlwZSI6IkdTMS5DT05UQUlORVIiLCJpZGVudGl
maWVycyI6WyIqIl0sImF0dHJpYnV0ZXMiOlsiR1MxLkNPTlRBSU5F
Ui5BVFRSSUJVVEUuRVRBIiwiR1MxLkNPTlRBSU5FUi5BVFRSSUJVV
EUuV0VJR0hUIl19LCJhY3Rpb25zIjpbIklTSEFSRS5SRUFEIiwiSV
NIQVJFLkNSRUFURSJdLCJlbnZpcm9ubWVudCI6eyJzZXJ2aWNlUHJ
vdmlkZXJzIjpbIkVVLkVPUkkuTkwxMjM0MTIzNDUiXX19LCJydWxl
cyI6W3siZWZmZWN0IjoiUGVybWl0In0seyJlZmZlY3QiOiJEZW55I
iwidGFyZ2V0Ijp7InJlc291cmNlIjp7ImF0dHJpYnV0ZXMiOlsiR1
MxLkNPTlRBSU5FUi5BVFRSSUJVVEUuRVRBIl19LCJhY3Rpb25zIjp
bIklTSEFSRS5DUkVBVEUiXX19LHsiZWZmZWN0IjoiRGVueSIsInRh
cmdldCI6eyJyZXNvdXJjZSI6eyJpZGVudGlmaWVycyI6WyJHUzEuQ
09OVEFJTkVSLklELjAwMDAwMDAwMDAxIl19fX1dfV19XX19.iB1cp
lUm5TtGqzxcmVJU5ZtKve-2yPSelE1xLMLwI_0"
}
```


Example value - delegationEvidence


```
{
    "delegationEvidence": {
        "notBefore": 1509633681,
        "notOnOrAfter": 1509633741,
        "policyIssuer": "EU.EORI.NL123456789",
        "target": {
            "accessSubject": "EU.EORI.NL012345678"
        },
        "policySets": [
            {
                "maxDelegationDepth": 2,
                "target": {
                    "environment": {
                        "licenses": ["ISHARE.0001", "ISHARE.0003"]
                    }
                },
                "policies": [
                    {
```

```
                        "target": {
                            "resource": {
                                "type": "GS1.CONTAINER",
                                "identifiers": ["*"],
                                "attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA",

"GS1.CONTAINER.ATTRIBUTE.WEIGHT"]
                            },
                            "actions": ["ISHARE.READ", "ISHARE.CREATE"],
                            "environment": {
                                "serviceProviders": ["EU.EORI.NL123412345"]
                            }
                        },
                        "rules": [
                            {
                                "effect": "Permit"
                            },
                            {
                                "effect": "Deny",
                                "target": {
                                    "resource": {
                                        "attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA"]
                                    },
                                    "actions": ["ISHARE.CREATE"]
                                }
                            },
                            {
                                "effect": "Deny",
                                "target": {
                                    "resource": {
                                        "identifiers": ["GS1.CONTAINER.ID.00000000001"]
                                    }
                                }
                            }
                        ]
                    }
                ]
            }
        ]
    }
}
```


5.2.2.8 Role: Scheme Owner

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This chapter specifies the APIs that MUST be implemented by the Scheme Owner.

OAuth access token

POST /scheme_owner/oauth2.0/token

Used to obtain an OAuth access token from the Scheme Owner.

Parameter	Contained in	Type	Required	Description
`grant_type`	body	string	Yes	OAuth 2.0 grant type. MUST contain “client_credentials”
`scope`	body	string	No	OAuth 2.0 scope. Defaults to "iSHARE", indicating all rights are requested. Other values MAY be specified by the API owner and allow to get tokens that do not include all rights
`client_id`	body	string	Yes	OpenID Connect 1.0 client ID. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain a valid iSHARE identifier[60]
`client_assertion_type`	body	string	Yes	OpenID Connect 1.0 client assertion type. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”
`client_assertion`	body	string	Yes	OpenID Connect 1.0 client assertion. Used in iSHARE for all client identification for OAuth/OpenID Connect. MUST contain JWT conform iSHARE specifications[61]

60 https://innopay.atlassian.net/wiki/spaces/IS/pages/93782017/Party+identifiers
61 https://innopay.atlassian.net/wiki/spaces/IS/pages/79364112/Generic+iSHARE+JWT+specifications

Example OAuth token request

```
POST /token HTTP/1.1
Host: randomserver.com/scheme_owner/oauth2.0/token
Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&
scope=iSHARE&client_id=EU.EORI.NL000000001&client_assertion_type=urn:ietf:params:oauth:clie
nt
-assertion-type:jwt-
bearer&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNS
UlHQVRDQ0ErbWdBd0lCQWdJQ0VBb3dEUVlKS29aSWh2Y05BUUVMQlFBd2daQXhDekFKQmdOVkJBWVRBazVNTVFzd0NR
WU
RWUVFJREFKT1NERVBNQTBHQTFVRUNnd0dhVk5JUVZKRk1SRXdEd1lEVlFRTERBaFRaV04xY21sMGVURW9NQ1lHQTFVR
UF
3d2ZhVk5JUVZKRklFNU1JRU5sY25ScFptbGpZWFJsSUVGMWRHaHZjbWwwZVRFbU1DUUdDU3FHU0liM0RRRUpBUllYYV
c1
bWIwQnBjMmhoY21VdGNISnZhbVZqZEM1dmNtY3dIaGNOTVRjeE1ERXlNRGd6TXpVNVdoY05NVGd4TURJeU1EZ3pNelU
1V
2pDQmxURUxNQWtHQTFVRUJoTUNUa3d4Q3pBSkJnTlZCQWdNQWs1SU1SSXdFQVlEVlFRSERBbEJiWE4wWlhKa1lXMHhE
ek
FOQmdOVkJBb01CbWxUU0VGU1JURVdNQlFHQTFVRUN3d05SSFZ0YlhrZ1ptOXlJRkJQUXpFVU1CSUdBMVVFQXd3TFRrd
3d
NREF3TURBd01ERXhKakFrQmdrcWhraUc5dzBCQ1FFV0YybHVabTlBYVhOb1lYSmxMWEJ5YjJwbFkzUXViM0puTUlJQk
lq
QU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUF2LzVmdElwdTE0bnl2MG9DUmRydEpsVk9icEV0Tmp
kT
FNNSSs3SzJOL05GWHlOUGFQM3c0ajB2a29Ma0lVUmJEaTJ3S29oUXNqanJEM21yR1RWN1ZqdWlaSzM1WlZPMGtlczly
ZU
hoeTNHNnIxMTJ4S2x1N3QwWmJxU2I2U3hrMW94c0FxQWppOUsyemtwN055UW00NVd4OFJEQzBsTytYalBpbExUZEp2V
lV
nWktlVkRmc1l6QjV5NXc2WG90aE1VNGgyNzBoVUNibkYwZ1FyQjFzL0RPeC9yd2xqMHc5ZmRTYjlsZk9SdzE2SUM5T3
B3
VzdsQU5kdTFkeTY4RnpGdHdxK1BHNXJBWThXOGU3MGNiT0hSSVRERjNKSjRlelEzY0NsaFlBQ3JPdUEvdkV2bnU0MzN
Ob
ml3UGVGa2VWSGhqQlIzOG53RzljQWJGU2d2Sm9rM1FJREFRQUJvNElCWERDQ0FWZ3dDUVlEVlIwVEJBSXdBREFSQmds
Z2
hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWklBWWI0UWdFTkJDWVdKRTl3Wlc1VFUwd2dSMlZ1WlhKaGRHVmtJRk5sY
25
abGNpQkRaWEowYVdacFkyRjBaVEFkQmdOVkhRNEVGZ1FVZnpHMElFMEV2OFBxZUNTbHJvTXVOTmlkNFA0d2diNEdBMV
Vk
SXdTQnRqQ0JzNEFVamtaTjB4U0pxbGNpWlZTTDFQYlZtd0kzM091aGdaYWtnWk13Z1pBeEN6QUpCZ05WQkFZVEFrNU1
NU
XN3Q1FZRFZRUUlEQUpPU0RFU01CQUdBMVVFQnd3SlFXMXpkR1Z5WkdGdE1ROHdEUVlEVlFRS0RBWnBVMGhCVWtVeEVU
QV
BCZ05WQkFzTUNGTmxZM1Z5YVhSNU1SUXdFZ1lEVlFRERBdHBVMGhCVWtVZ1VtOXZkREVtTUNRR0NTcUdTSWIzRFFFS
kF
SWVhhVzVtYjBCcGMyaGhjbVV0Y0hKdmFtVmpkQzV2Y21lQ0FoQUFNQTRHQTFVZER3RUIvd1FFQXdJRm9EQVRCZ05WSF
NV
RUREQUtCZ2dyQmdFRkJRY0RBVEFOQmdrcWhraUc5dzBCQVFzRkFBT0NBZ0VBRGpvUVlxdjVIS3pKckY5bUttUy9PQjM
vM
```

0FodFJQVm1WRHFkTmNPdytHVTE0SXNLczQwN3ArbFhuMmhON2VaUEpwSVpyVDdqQzl2ZnVOTG1PbzEybXZ0YlBGeTdD
cT
krU1lCNkEvZ2NXK0NZemIrKzBWM3o0ZlR5Y1ZjRXVRQWc4ODM5TWM2clNhSXRha0Q3YnN1Y2EvTldyZFVqSUU1eDBNQ
2Z
YQ21WTS9NeXdlNHdGdEE5ZU5yN0Z1SUN4L0JhdkVnSU8rVmRFdDBKVUp6WGNYK0wrbGM1T0FCQlNidHZjT2pWblRHRD
Vu
T3ZodFdrQy80eWpaVmx3Y2EyK1E4OVBGcVI2OTRYRjhvc0szWFZTWGZVK2pmUk50K0EyeXpWTmpaemVucDF6a1RiZkd
ua
XBDek9QcllaMGxDUzZPUkF3cDdoZ1BrS3hJb1BqTjJkTE11TzAyWVZkV2t2SFVvTXNoN0F0Mjh0RGM2TEVsTjc1Zlgx
bn
VPdjgxMUcyYURxU0d6Rnc0SkdRU25lR3hsaDlMekdzaEkxaWorTm5pQm5uOTYrMGpHSm5OSjJGY3F1Y2dpZ21tSWVvY
0h
6QjlLV3Q3eFRzZmdnVFduZjd3dzA3OGgvZStrNFZ3V2JITjUrcXdURHFra2poTHh6Vm9jTzRHVWw2RzZXUmg2VHp6ek
Fq
SUNiS1BZclI5VWcxaGYxSFNOcG93RHU1MWlxVStmV1VZV0FRcVVSakV2Z0k0aFBmcVhya0x5NVR6OVdLQ1diR0hyRnR
5Z
VlXdGpxenhXdzlpN3Fwc3d3S002M1RLQ1dVVWJoNTlJTitFSTZqczhUMTc2b2tkSkVUUFRaOXpGcjNvNHBIVERBS0VO
RE
hmcjJwT293emZsazlhM3F3RTkvNndxMlhhalI1R289Il19.eyJpc3MiOiJFVS5FT1JJLk5MMDAwMDAwMDAxIiwic3Vi
Ij
oiRVUuRU9SSS5OTDAwMDAwMDAwMSIsImp0aSI6InpGMXFHS0J2NzgiLCJpYXQiOiIxNTEzMDcwODY3IiwiZXhwIjoxN
TE
zMDcwODk3LCJuYmYiOjE1MTMwNzA4NjcsImF1ZCI6Ik5MLkVPUkkuTkw4MTI0NTg4MzcifQ.bPOTFBBg8pedWkfoRKM
t1
uaa0albfWkgSObePtOSKxV0VOPUb1uencLihV086HWJeqO7DBZ2jx_rn96FfpojJnn2z2aQnBSX06IYPTYYcze543-
wb-
8vCor7hM6idGBbDCmeKQvFrIYaYmt34GeU0UjWnNMPGdh90vzbhqgPUlZixtUWfQYn0NxYJf7RGmEhmRybXm2zFl0oo
om
1d-zoZzwuTAzfZqa2rM986VG8WikewxN2IUafhKoQ_w42MB6WpPki8a0EJ07xUZozSybSQvFRWyKxN-
TCtixp3B5nGo9T
uZvkOf1f0RpL8-zTU2DQOFnhz8p7gwF10srNYYv3Sw

Responses

Code	Description
200	OK

Example value


```
{
  "access_token": "string",
  "token_type": "string",
  "expires_in": 3600
}
```

Party iSHARE status

GET /scheme_owner/ishare1.0/parties/{party_id}

Used to obtain information on an iSHARE participant from the iSHARE Scheme owner. By default returns current state and party OIN (see page 213) (OIN is used by parties consuming this API service to verify that the provided certificate and EORI belong to the same party)

Parameter	Contained in	Type	Required	Description
`authorization`	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
`party_id`	path	string	Yes	iSHARE specific identifier of the party for which information is requested
`date_time`	query	string	No	Date time for which the information is requested. If provided the result becomes final and therefore MUST be cacheable

example party status request

```
GET /scheme_owner/ishare1.0/parties/EU.EORI.NL000000001
HTTP/1.1
Host: randomserver.com

?
access_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IkM4OTQ5OTdDNTQ1MzAwNUE3NzQ3Qjk0Q0QxNzdCQjdDNzdFRjA1OUI
iLCJ0eXAiOiJKV1QiLCJ4NXQiOiJ5SlNaZkZSVEFGcDNSN2xNMFhlN2ZIZnZCWnMifQ.eyJuYmYiOjE1MTMyNTMwNTgsImV4
cCI6MTUxMzI1NjY1OCwiaXNzIjoiaHR0cHM6Ly9yZWZpbXAuaXNoYXJlLXByb2plY3Qub3JnIiwiYXVkIjpbImh0dHBzOi8v
cmVmaW1wLmlzaGFyZS1wcm9qZWN0Lm9yZy9yZXNvdXJjZXMiLCJpU0hBUkUiXSwiY2xpZW50X2lkIjoiRVUuRU9SSS5OTDAw
MDAwMDAwMSIsImNsaWVudF9jbGllbnRfYWxsb3dlZF9zZXJ2aWNlIjoic2NoZW1lX293bmVyIiwic2NvcGUiOlsiaVNIQVJF
Il19.Fdw_QjNylyrNajb-V9IfSS3-OiwZOgmIeSD63HEb6EzVm3zp5Asf7CVmVVcj07YFQPfZ-rSHMavk2sxpJAiQKDs-
RhC0hOIMWKXQVxKQJcxHZ11TuqKp74WlxxxWKtfkFz1UYrxYIc_7NwKQXpfQnRcmjvvQJVqP5s8etyrcYSfJhl9FaB42dPZ4
YCEEAR1AeUHn9KvlT6Tx4-vIgdyeoYbuUiUNTZcyCMHeJRpAVe9DSTJ1f1-2cQ7lyQUgYY6e11-Oy_rP-
k2siO8CYc6_B0rTwKqi0EQ1yhG6LxhNg2ZoRu90D4f3hEULGfPzKfmGa13pOk_z_J1z2MRDcaDLMA

Authorization:
eyJhbGciOiJSUzI1NiIsImtpZCI6IkM4OTQ5OTdDNTQ1MzAwNUE3NzQ3Qjk0Q0QxNzdCQjdDNzdFRjA1OUIiLCJ0eXAiOiJK
V1QiLCJ4NXQiOiJ5SlNaZkZSVEFGcDNSN2xNMFhlN2ZIZnZCWnMifQ.eyJuYmYiOjE1MTI3NDM0MjksImV4cCI6MTUxMjc0N
zAyOSwiaXNzIjoiaHR0cHM6Ly9yZWZpbXAuaXNoYXJlLXByb2plY3Qub3JnIiwiYXVkIjpbImh0dHBzOi8vcmVmaW1wLmlza
GFyZS1wcm9qZWN0Lm9yZy9yZXNvdXJjZXMiLCJpU0hBUkUiXSwiY2xpZW50X2lkIjoiRVUuRU9SSS5OTDAwMDAwMDAwMSIsI
mNsaWVudF9jbGllbnRfYWxsb3dlZF9zZXJ2aWNlIjoic2NoZW1lX293bmVyIiwic2NvcGUiOlsiaVNIQVJFIl19.CPHF9pBf
QwQNN0zHabqeoy8LC7fnM-ejVtyJtgGnox6Lk1GP6XV0pwBLJRECoJ_lV3iUjzvD0B_y3uL74Prf-
NLrxad-8_W3gbc1rAj8DLX3LZ5i7Ezcvlyn0t3tiHCfdwfP_1ggRFo6s_XmhyITAdM1p-Vd7-
rKY3RzKzf8AIbo0sM3hU9l3h36fWXG2Stv8ywQIC2___eaWAeXmbnsxNSlYMoq2_VWVfd3naokYx8w0Jlo5xg8S4_7ZWyIgy
_YJBPfkqbjacOhPZ01IO_HE-vzLc5RLQVKSQp1ymemtraoevVTOxe5IaLopAWAjskHxaIHymHDqHS8cVG2fMhkhQ
```

Responses

Code	Description
200	OK

Example value

```
{
    "date_time": "2017-12-14T12:07:38Z",
    "party_id": "EU.EORI.NL000000001",
        “party_oin”: “00000000100000001000”,
    "adherence": {
        "status": "ACTIVE",
        "start_date": "2017-12-01T00:00:00Z",
        "end_date": "2018-01-31T00:00:00Z"
    }
}
```

Overview of iSHARE certified parties

GET /scheme_owner/ishare1.0/certified_parties

Used to obtain certification information on all iSHARE participants from the iSHARE Scheme owner

Parameter	Contained in	Type	Required	Description
`authorization`	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value
`date_time`	query	string	No	Date time for which the certification information is requested. If provided the result becomes final and therefore MUST be cacheable

example party status request

```
GET /scheme_owner/ishare1.0/certified_parties
HTTP/1.1
Host: randomserver.com

?
access_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IkM4OTQ5OTdDNTQ1MzAwNUE3NzQ3Qjk0Q0QxNzdCQjdDNzdFRj
A1OUIiLCJ0eXAiOiJKV1QiLCJ4NXQiOiJ5SlNaZkZSVEFGcDNSN2xNMFhlN2ZIZnZCWnMifQ.eyJuYmYiOjE1MTMyNT
MwNTgsImV4cCI6MTUxMzI1NjY1OCwiaXNzIjoiaHR0cHM6Ly9yZWZpbXAuaXNoYXJlLXByb2plY3Qub3JnIiwiYXVkI
jpbImh0dHBzOi8vcmVmaW1wLmlzaGFyZS1wcm9qZWN0Lm9yZy9yZXNvdXJjZXMiLCJpU0hBUkUiXSwiY2xpZW50X2lk
IjoiRVUuRU9SSS5OTDAwMDAwMDAwMSIsImNsaWVudF9jbGllbnRfYWxsb3dlZF9zZXJ2aWNlIjoic2NoZW1lX293bmV
yIiwic2NvcGUiOlsiaVNIQVJFIl19.Fdw_QjNylyrNajb-V9IfSS3-
OiwZOgmIeSD63HEb6EzVm3zp5Asf7CVmVVcj07YFQPfZ-rSHMavk2sxpJAiQKDs-
RhC0hOIMWKXQVxKQJcxHZ11TuqKp74WlxxxWKtfkFz1UYrxYIc_7NwKQXpfQnRcmjvvQJVqP5s8etyrcYSfJhl9FaB4
2dPZ4YCEEAR1AeUHn9KvlT6Tx4-vIgdyeoYbuUiUNTZcyCMHeJRpAVe9DSTJ1f1-2cQ7lyQUgYY6e11-Oy_rP-
k2siO8CYc6_B0rTwKqi0EQ1yhG6LxhNg2ZoRu90D4f3hEULGfPzKfmGa13pOk_z_J1z2MRDcaDLMA

Authorization:
eyJhbGciOiJSUzI1NiIsImtpZCI6IkM4OTQ5OTdDNTQ1MzAwNUE3NzQ3Qjk0Q0QxNzdCQjdDNzdFRjA1OUIiLCJ0eXA
iOiJKV1QiLCJ4NXQiOiJ5SlNaZkZSVEFGcDNSN2xNMFhlN2ZIZnZCWnMifQ.eyJuYmYiOjE1MTMyNTM1ODksImV4cCI
6MTUxMzI1NzE4OSwiaXNzIjoiaHR0cHM6Ly9yZWZpbXAuaXNoYXJlLXByb2plY3Qub3JnIiwiYXVkIjpbImh0dHBzOi
8vcmVmaW1wLmlzaGFyZS1wcm9qZWN0Lm9yZy9yZXNvdXJjZXMiLCJpU0hBUkUiXSwiY2xpZW50X2lkIjoiRVUuRU9SS
S5OTDAwMDAwMDAwMSIsImNsaWVudF9jbGllbnRfYWxsb3dlZF9zZXJ2aWNlIjoic2NoZW1lX293bmVyIiwic2NvcGUi
OlsiaVNIQVJFIl19.etPVJsBePPLIu4WU_u7pPO395LBxbgtuWSu9S5QGwrRquxDy5iYaVAcAeF3hXV91vLmudeXBGV
G-jaev3nKN3nZH1KeYNbrJyu8WF12Gecu6mPsUGvzKFdtcN9qMNHA5U-2pIR65FEy360GbMzhJ7yjGWiA5jU-
Ri0r3iZhiu79jNHNcJ8r71V3FuSs1W8c8TyJfP5549Ow5xyOUELA0DLMfMPOfXlJ9dwbwhQzJlXyhxIQ4eVWiCp4ZBD
l_dJaCEChwNB35x4gqLTEdGJcu74QPCga57hU7CMOIj6jGKB84m3iZfZ1yes1YkfJLPNhkSiQgoyDi0Sgz9pNMbJtg5
w
```

Responses

Code	Description

200 OK

Example value


```
{
    "date_time": "string",
    "certified_parties": [
        {
            "party_id": "string",
            "adherence": {
                "status": "NOTACTIVE"
            },
            "certifications": [
                {
                    "certification": {
                        "role": "iSHARE.IDENTITY_PROVIDER",
                        "start_date": "string",
                        "end_date": "string"
                    }
                }
            ]
        },
        {
            "party_id": "string",
            "adherence": {
                "status": "ACTIVE",
                "start_date": "string"
            },
            "certifications": [
                {
                    "certification": {
                        "role": "iSHARE.IDENTITY_PROVIDER",
                        "start_date": "string"
                    }
                }
            ]
        },
        {
            "party_id": "string",
            "adherence": {
                "status": "ACTIVE"
            },
            "certifications": [
                {
                    "certification": {
                        "role": "iSHARE.AUTHORISATION_REGISTRY",
                                                "start_date": "string"
                    }
                }
            ]
        }
        ]
```

```
}
```

Overview of PKI roots which are trusted in the iSHARE scheme

GET /scheme_owner/ishare1.0/trusted_list

Used to obtain the iSHARE trusted list of certificate/seal roots

Parameter	Contained in	Type	Required	Description
authorization	header	string	Yes	Oauth 2.0 authorisation based on bearer token. MUST contain "Bearer " + access token value

example party status request

```
GET /scheme_owner/ishare1.0/trusted_list
HTTP/1.1
Host: randomserver.com

Authorization:
eyJhbGciOiJSUzI1NiIsImtpZCI6IkM4OTQ5OTdDNTQ1MzAwNUE3NzQ3Qjk0Q0QxNzdCQjdDNzdFRjA1OUIiLCJ0eXA
iOiJKV1QiLCJ4NXQiOiJ5SlNaZkZSVEFGcDNSN2xNMFhlN2ZIZnZCWnMifQ.eyJuYmYiOjE1MTMyNTM5MjEsImV4cCI
6MTUxMzI1NzUyMSwiaXNzIjoiaHR0cHM6Ly9yZWZpbXAuaXNoYXJlLXByb2plY3Qub3JnIiwiYXVkIjpbImh0dHBzOi
8vcmVmaW1wLmlzaGFyZS1wcm9qZWN0Lm9yZy9yZXNvdXJjZXMiLCJpU0hBUkUiXSwiY2xpZW50X2lkIjoiRVUuRU9SS
S5OTDAwMDAwMDAwMSIsImNsaWVudF9jbGllbnRfYWxsb3dlZF9zZXJ2aWNlIjoic2NoZW1lX293bmVyIiwic2NvcGUi
OlsiaVNIQVJFIl19.iWV9szKNqLhNVMwMmta2I1i8FNPJv4Gxlb7eJTiujOj1NGDYh05zbmUIR737YhE83PDaZm1ySA
YyBOUTl2z1FDmx9tg1t3JpU1bAtDSSj1_z220Ok0daGzxALiWdkrX5hHF0hRGgv61gtVIoN0RFWWrLkWeBNW7hzLRFo
NCLEySndtCvATb6RNSXtUWJYfzltvnroL7sJD4qcTr3xC-
qR8odO_hFtELTnBTRHSmwL8UZCQFSpAJ5_R4ron329DyzdXsTOZ5VLPU4MxRHiNxCZYyIzIVMaH6u-ysRT2-
IdNDD_li4SqYCLLjLvuVp9p2uaLm6eXMogeiOlTzChp1XEw
```

Responses

Code	Description

200	OK
	Example value
	{
	"trusted_list_token": "string"
	}

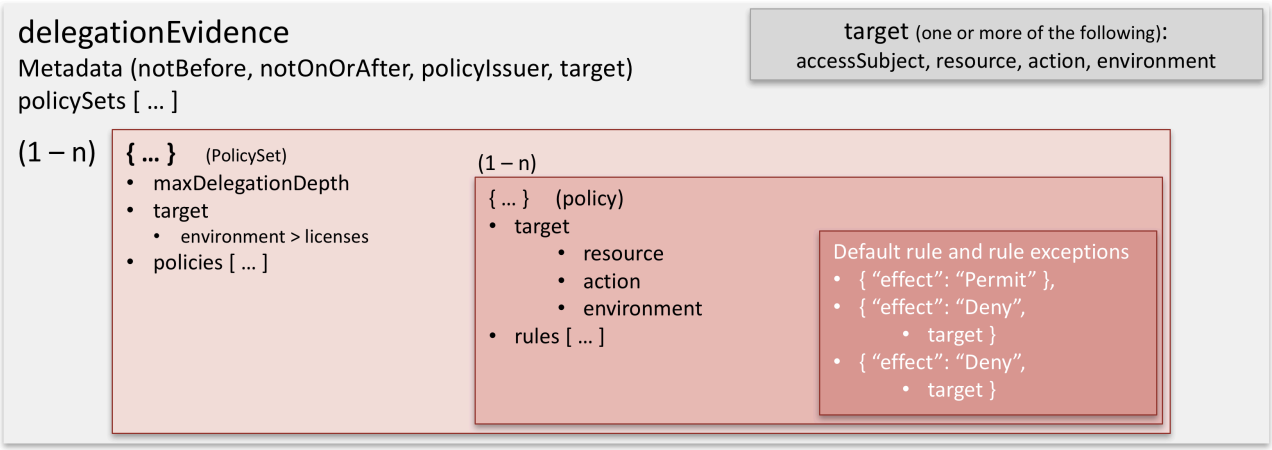
5.2.3 Structure of delegation evidence

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This page describes (and prescribes) how, in iSHARE, delegation is communicated between different parties.

In iSHARE, delegation evidence expresses the delegation of rights from a delegator (the party that delegates rights; the `policyIssuer`) to the delegate (the party that receives the delegated rights; i.e. the `accessSubject`). Rights are expressed in `rules` in terms of allowed `actions` to be performed on resources, under the `license(s)` as defined in `policySets`.

Delegation evidence is modeled as a JSON object inspired by the XACML 3.0 specifications and structured as follows:



The JSON object consists of a root `delegationEvidence` element (modeled after an XACML `PolicySet` element) containing one or more `policySet` objects in the `policySets` array. The root element is only meant as a container element and extends the XACML specifications to cater for some iSHARE required metadata such as timestamps. Each of the second level `policySet` elements only acts as a container for actual `policy` elements with an indication of the rights in this `policySet` can be further delegated (with `maxDelegationDepth`) and what `license`(s) do apply. No other delegation logic is conveyed a second level `policySet`. Each `policy` element is used to express the actual rights being delegated.

The root `delegationEvidence` element contains the following parameters.

Parameter	Contained in	Type	Required	Description
`delegationEvidence`		{}	Yes	The root of any delegation evidence
`notBefore`	`delegationEvidence`	int	Yes	Unix timestamp in UTC indicating the start of validity period of this delegation evidence. SHOULD equal the time of issuing of the evidence unless historic evidence is requested.
`notOnOrAfter`	`delegationEvidence`	int	Yes	Unix timestamp in UTC indicating the end of validity period of this delegation evidence. It is up to the issuer off the evidence to set this time. Note that a reasonable amount of time SHOULD be allowed for processing of longer delegation paths. Also note that evidence cannot be revoked, so setting very long validity periods SHOULD be avoided.
`policyIssuer`	`delegationEvidence`	string	Yes	iSHARE identifier of the delegator (the delegating entity)
`target`	`delegationEvidence`	{}	Yes	MUST for the root level contain an `accessSubject`. No other elements are allowed. It makes the entire delegation evidence applicable only to this `accessSubject`.
`accessSubject`	`target`	string	Yes	iSHARE identifier of the delegate (the entity that receives the delegated rights)
`policySets`	`delegationEvidence`	[]	Yes (1..n)	Container for one or more objects containing `policy` elements with an indication for further delegation. Note that `policySet` elements within one `delegationEvidence` MUST not restrict each other, but rather offer a mechanism to express additional rights. They MUST be evaluated in a "permit-override" manner, allowing a "Permit" if only one of the `policySet` elements evaluates to "Permit".

The second level objects in `policySets` each contain the following parameters. Other parameters are not allowed. Note that XACML spec is heavily restricted, a.o. for the reason to prevent redundancy (and resulting possible conflicts) with the root `policySet` element.

Parameter	Contained in	Type	Required	Description
maxDelegationDepth	policySets	int	No	Optional element that, if present, indicates that further delegation of the rights, conveyed in the policy elements that are part of this PolicySet, is allowed. The value indicates the delegation steps that are allowed after this step in order to evaluate the entire delegation path to "Permit"
target	policySet	{}	Yes	
environment	target	{}	Yes	
licenses	environment	[]	Yes	Array which describes which iSHARE licenses apply to this policySet.
policies	policySets	[]	Yes (1..n)	Used to express the actual rights being delegated. Note that policies within one policySets object MUST not restrict each other, but rather offer a mechanism to express additional rights. They MUST be evaluated in a "permit-override" manner, allowing a "Permit" if only one of the policy elements evaluates to "Permit".

A Policy element contains the following parameters.

Parameter	Contained in	Type	Required	Description
target	policies	string	Yes	Describes the target, in terms of resource and action, this policy applies to. It is also the scope that is permitted through the default Rule. Additional Rule elements can be described to exclude Resources and Actions from the default policy rights
resource	target	{}	Yes	
type	resource	string	Yes	String which describes the type of resource to which the rules apply.
identifiers	resource	[]	Yes	Array of strings containing one or more resource identifiers. Depending on the Type an identifier SHOULD be a urn.
attributes	resource	[]	No	Optional array of attributes of the resources the delegated rights apply to. If omitted defaults to all attributes. Depending on the Type an attribute SHOULD be a urn.
actions	target	[]	Yes	

Parameter	Contained in	Type	Required	Description
environment	target	{}	No	
serviceProviders	environment	[]	Yes	Array which lists the iSHARE client ID's of serviceProviders which are allowed to provide services to the accessSubject as described within this policy.
rules	policies	[]	Yes (1..n)	The first rule element is the default rule that applies to the target at policies level. Note that additional rule elements within one policies object are intended to restrict each the default rule. All rule elements in a Policy MUST be evaluated in a "deny-override" manner, allowing a "Permit" only if all of the rule elements evaluate to "Permit".

The default Rule element contains the following parameters.

Parameter	Contained in	Type	Required	Description
effect	rules	string	Yes	MUST contain 'Permit'

Additional Rule elements contains the following parameters.

Parameter	Contained in	Type	Required	Description
effect	rules	string	Yes	MUST contain 'Deny'
target	rules	{}	Yes	Describe the target, in terms of resource and action, this additional rule applies to. Additional rule elements are limitations of the default rule and resource scope.
resource	target	{}	Yes	
type	resource	string	No*	Optional string which describes the type of resource to which the rule applies. Defaults to none if not specified.
identifiers	resource	[]	No*	Optional array of strings containing one or more resource identifiers. Depending on the type an identifier SHOULD be a urn.

Parameter	Contained in	Type	Required	Description
attributes	resource	[]	No*	Optional array of attributes of the resources the delegated rights apply to. If omitted defaults to all attributes. Depending on the type an attribute SHOULD be a urn.
actions	target	[]	No	Optional array of actions, the additional rule applies to the actions listed. If no actions are listed then the default is to all iSHARE actions defined within the policy.

* Note: Although not individually required, at least one of the parameters within the resource object needs to be specified to which the additional rules apply.

Example delegation JSON

```
//Organisation A delegates rights to organisation B. A allows B READ and CREATE access to all ETA and
WEIGHT of A's containers of which the data is located at service provider C and can only be accessed with
service provider C. However, A does not allow B to CREATE to ETA information and completely denies access
to data regarding container ID.00000000000001. Furthermore, all rights of B are allowed under iSHARE
licenses 1 and 3, and B has the right to delegate it's right two more times.

{
    "delegationEvidence": {
        "notBefore": 1509633681,
        "notOnOrAfter": 1509633741,
        "policyIssuer": "EU.EORI.NL123456789",
        "target": {
            "accessSubject": "EU.EORI.NL012345678"
        },
        "policySets": [
            {
                "maxDelegationDepth": 2,
                "target": {
                    "environment": {
                        "licenses": ["ISHARE.0001", "ISHARE.0003"]
                    }
                },
                "policies": [
                    {
                        "target": {
                            "resource": {
                                "type": "GS1.CONTAINER",
                                "identifiers": ["*"],
                                "attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA",
"GS1.CONTAINER.ATTRIBUTE.WEIGHT"]
                            },
                            "actions": ["ISHARE.READ", "ISHARE.CREATE"],
                            "environment": {
                                "serviceProviders": ["EU.EORI.NL123412345"]
```

```
                        }
                    },
                    "rules": [
                        {
                            "effect": "Permit"
                        },
                        {
                            "effect": "Deny",
                            "target": {
                                "resource": {
                                    "attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA"]
                                },
                                "actions": ["ISHARE.CREATE"]
                            }
                        },
                        {
                            "effect": "Deny",
                            "target": {
                                "resource": {
                                    "identifiers": ["GS1.CONTAINER.ID.00000000001"]
                                }
                            }
                        }
                    ]
                }
            ]
        }
    ]
  }
}
```

example code - for copying purposes

```
{"delegationEvidence":{"notBefore":1509633681,"notOnOrAfter":
1509633741,"policyIssuer":"EU.EORI.NL123456789","target":
{"accessSubject":"EU.EORI.NL012345678"},"policySets":[{"maxDelegationDepth":2,"target":{"environment":
{"licenses":["ISHARE.0001","ISHARE.0003"]}},"policies":[{"target":{"resource":
{"type":"GS1.CONTAINER","identifiers":["*"],"attributes":
["GS1.CONTAINER.ATTRIBUTE.ETA","GS1.CONTAINER.ATTRIBUTE.WEIGHT"]},"actions":
["ISHARE.READ","ISHARE.CREATE"],"environment":{"serviceProviders":["EU.EORI.NL123412345"]}},"rules":
[{"effect":"Permit"},{"effect":"Deny","target":{"resource":{"attributes":
["GS1.CONTAINER.ATTRIBUTE.ETA"]},"actions":["ISHARE.CREATE"]}},{"effect":"Deny","target":{"resource":
{"identifiers":["GS1.CONTAINER.ID.00000000001"]}}}]}]}}
```

Please note that although in XACML the attributes PolicySetId, Version and PolicyCombiningAlgId are mandatory in XACML they are not ported to the iSHARE JSON structure. iSHARE follows the "**deny-override"** Policy Combining Algorithm. This implies that if at least one policy is evaluated as “deny”, the integrated output must also be “deny”.

5.2.3.1 Example cases

The main variations in the JSON code for delegationEvidence are the (1-n) `policySets`, `policies` and `rules` arrays. These variations are based on the most efficient way of expressing the rights that an `accessSubject` has.

Various examples are described in the table below.

Description	Code

Organisation A delegates rights to organisation B. A allows B READ and CREATE access to all ETA and WEIGHT of A's containers of which the data is located at service provider C and can only be accessed with service provider C. However, A does not allow B to CREATE to ETA information and completely denies access to data regarding container ID. 00000000000001. Furthermore, all rights of B are allowed under iSHARE licenses 1 and 3, and B has the right to delegate it's right two more times.
 	
The code shows default access to a set of resources, with a few exceptions in terms of actions or specific resources. This results in additional "Deny" rules within the policy.
	Code - for visual/reading purposes
	
	{
	"delegationEvidence": {
	"notBefore": 1509633681,
	"notOnOrAfter": 1509633741,
	"policyIssuer": "EU.EORI.NL123456789",
	"target": {
	"accessSubject": "EU.EORI.NL012345678"
	},
	"policySets": [
	{
	"maxDelegationDepth": 2,
	"target": {
	"environment": {
	"licenses": ["ISHARE.0001", "ISHARE.0003"]
	}
	},
	"policies": [
	{
	"target": {
	"resource": {
	"type": "GS1.CONTAINER",
	"identifiers": ["*"],
	"attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA",
	"GS1.CONTAINER.ATTRIBUTE.WEIGHT"]
	},
	"actions": ["ISHARE.READ", "ISHARE.CREATE"],
	"environment": {
	"serviceProviders": ["EU.EORI.NL123412345"]
	}
	},
	"rules": [
	{
	"effect": "Permit"
	},
	{
	"effect": "Deny",
	"target": {
	"resource": {
	"attributes":
	["GS1.CONTAINER.ATTRIBUTE.ETA"]
	},
	"actions": ["ISHARE.CREATE"]
	}
	},
	{
	"effect": "Deny",
	"target": {
	"resource": {

Description	Code

```
                                        "identifiers": ["GS1.CONTAINER.ID.
00000000001"]
                                    }
                                }
                            }
                        ]
                    }
                ]
            }
        ]
    }
}
```

Code - for copying purposes

```
{"delegationEvidence":{"notBefore":1509633681,"notOnOrAfter":
1509633741,"policyIssuer":"EU.EORI.NL123456789","target":
{"accessSubject":"EU.EORI.NL012345678"},"policySets":[{"maxDelegationDepth":
2,"target":{"environment":{"licenses":["ISHARE.0001","ISHARE.0003"]}},"policies":
[{"target":{"resource":{"type":"GS1.CONTAINER","identifiers":["*"],"attributes":
["GS1.CONTAINER.ATTRIBUTE.ETA","GS1.CONTAINER.ATTRIBUTE.WEIGHT"]},"actions":
["ISHARE.READ","ISHARE.CREATE"],"environment":{"serviceProviders":
["EU.EORI.NL123412345"]}},"rules":[{"effect":"Permit"},{"effect":"Deny","target":
{"resource":{"attributes":["GS1.CONTAINER.ATTRIBUTE.ETA"]},"actions":
["ISHARE.CREATE"]}},{"effect":"Deny","target":{"resource":{"identifiers":
["GS1.CONTAINER.ID.00000000001"]}}}]}]}]}}
```

Description	Code

Organisation A delegates rights to organisation B. A allows B READ access to all ETA of A's containers of which the data is located at service provider C and can only be accessed with service provider C. A also allows B CREATE access to all WEIGHT of A's containers, at any service provider possible. Furthermore, all rights of B are allowed under iSHARE licenses 1 and 3, and B has the right to delegate it's right two more times.
 	
The code shows that the same delegation rights and licenses apply to a resource set, but different actions are allowed to different subsets of these resources. This results in variations in policies within the policySets.
	Code - for visual/reading purposes
	
	{
	"delegationEvidence": {
	"notBefore": 1509633681,
	"notOnOrAfter": 1509633741,
	"policyIssuer": "EU.EORI.NL123456789",
	"target": {
	"accessSubject": "EU.EORI.NL012345678"
	},
	"policySets": [
	{
	"maxDelegationDepth": 2,
	"target": {
	"environment": {
	"licenses": ["ISHARE.0001", "ISHARE.0003"]
	}
	},
	"policies": [
	{
	"target": {
	"resource": {
	"type": "GS1.CONTAINER",
	"identifiers": ["*"],
	"attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA"]
	},
	"actions": ["ISHARE.READ"],
	"environment": {
	"serviceProviders": ["EU.EORI.NL123412345"]
	}
	},
	"rules": [
	{
	"effect": "Permit"
	}
	]
	},
	{
	"target": {
	"resource": {
	"type": "GS1.CONTAINER",
	"identifiers": ["*"],
	"attributes": ["GS1.CONTAINER.ATTRIBUTE.WEIGHT"]
	},
	"actions": ["ISHARE.CREATE"]
	},
	"rules": [
	{
	"effect": "Permit"
	}

Description	Code

```
                        ]
                    }
                ]
            }
        ]
    }
}
```

Code - for copying purposes

```
{"delegationEvidence":{"notBefore":1509633681,"notOnOrAfter":
1509633741,"policyIssuer":"EU.EORI.NL123456789","target":
{"accessSubject":"EU.EORI.NL012345678"},"policySets":[{"maxDelegationDepth":
2,"target":{"environment":{"licenses":["ISHARE.0001","ISHARE.0003"]}},"policies":
[{"target":{"resource":{"type":"GS1.CONTAINER","identifiers":["*"],"attributes":
["GS1.CONTAINER.ATTRIBUTE.ETA"]},"actions":["ISHARE.READ"],"environment":
{"serviceProviders":["EU.EORI.NL123412345"]}},"rules":[{"effect":"Permit"}]},
{"target":{"resource":{"type":"GS1.CONTAINER","identifiers":["*"],"attributes":
["GS1.CONTAINER.ATTRIBUTE.WEIGHT"]},"actions":["ISHARE.CREATE"]},"rules":
[{"effect":"Permit"}]}]}]}}
```

Description	Code
Organisation A delegates rights to organisation B. A allows B READ and CREATE access to all ETA and WEIGHT of A's containers of which the data is located at service provider C, and rights can only be used with service provider C. Furthermore, all rights of B are allowed under iSHARE licenses 1 and 3, and B has the right to delegate it's right two more times. A also provides B READ access to the Container origins, but does not allow delegation for this information and it is only accessible under iSHARE license 2. The code shows two groups of resources with specific policies, executed under different licenses and delegation rights. This results in variations on the `policySets` level within the `delegationEvidence`.	**Code - for visual/reading purposes** `{ "delegationEvidence": { "notBefore": 1509633681, "notOnOrAfter": 1509633741, "policyIssuer": "EU.EORI.NL123456789", "target": { "accessSubject": "EU.EORI.NL012345678" }, "policySets": [{ "maxDelegationDepth": 2, "target": { "environment": { "licenses": ["ISHARE.0001", "ISHARE.0003"] } }, "policies": [{ "target": { "resource": { "type": "GS1.CONTAINER", "identifiers": ["*"], "attributes": ["GS1.CONTAINER.ATTRIBUTE.ETA", "GS1.CONTAINER.ATTRIBUTE.WEIGHT"] }, "actions": ["ISHARE.READ", "ISHARE.CREATE"], "environment": { "serviceProviders": ["EU.EORI.NL123412345"] } }, "rules": [{ "effect": "Permit" }] }] }, { "target": { "environment": { "licenses": ["ISHARE.0002"] } }, "policies": [{ "target": { "resource": {`

Description	Code

```
                                "type": "GS1.CONTAINER",
                                "identifiers": ["*"],
                                "attributes": ["GS1.CONTAINER.ATTRIBUTE.ORIGIN"]
                            },
                            "actions": ["ISHARE.READ"]
                            },
                        "rules": [
                            {
                            "effect": "Permit"
                            }
                        ]
                        }
                    }
                ]
            }
        ]
    }
}
```

Code - for copying purposes

```
{"delegationEvidence":{"notBefore":1509633681,"notOnOrAfter":
1509633741,"policyIssuer":"EU.EORI.NL123456789","target":
{"accessSubject":"EU.EORI.NL012345678"},"policySets":[{"maxDelegationDepth":
2,"target":{"environment":{"licenses":["ISHARE.0001","ISHARE.0003"]}},"policies":
[{"target":{"resource":{"type":"GS1.CONTAINER","identifiers":["*"],"attributes":
["GS1.CONTAINER.ATTRIBUTE.ETA","GS1.CONTAINER.ATTRIBUTE.WEIGHT"]},"actions":
["ISHARE.READ","ISHARE.CREATE"],"environment":{"serviceProviders":
["EU.EORI.NL123412345"]}},"rules":[{"effect":"Permit"}]}]},{"target":{"environment":
{"licenses":["ISHARE.0002"]}},"policies":[{"target":{"resource":
{"type":"GS1.CONTAINER","identifiers":["*"],"attributes":
["GS1.CONTAINER.ATTRIBUTE.ORIGIN"]},"actions":["ISHARE.READ"]},"rules":
[{"effect":"Permit"}]}}]}]}
```

5.3 Operational

This section covers the Operational details of the iSHARE scheme.

The Scheme Owner facilitates the correct operation of the iSHARE scheme and the iSHARE network through administering several aspects:

- Operational processes (see page 171)
- Service levels (see page 181)
- Communication (see page 189)

The Scheme Owner is part of a wider governance framework, which can be found in the introduction of the scheme (see page 14).

The assumptions underlying the processes and service levels can be found here (see page 227).

5.3.1 Operational processes

This section describes the operational processes necessary to administer the iSHARE scheme (specifications), network and brand.

Per process described in this section, the goal and responsibilities (per party) are described, before a process sequence is included.

The following processes are described:

5.3.1.1 Admission

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This admission process describes the steps that all parties MUST take to be admitted to the iSHARE network. For Certified Parties, additional steps are required and are described below. The process is the responsibility of, and facilitated by, the Scheme Owner.

Admission of prospective ISHARE participant includes:

- A potential Adhering Party wants to start fulfilling one or more adhering role(s) in the network.
- A potential Certified Party wants to start fulfilling one or more certified roles(s) in the network.
- An already Adhering and/or Certified Party wants to expand its current role(s) by one or more role(s) in the network.

The admission process for Certified Parties builds on the admission process of the Afsprakenstelsel elektronische toegangsdiensten[62].

Note: prospective iSHARE participants can start testing at any moment in time before initiating the admission process.

Goal

The goal of the admission process is to let prospective iSHARE participants join iSHARE in a simple and controlled way. A controlled admission process is important to warrant trust in the iSHARE scheme. It provides assurance that all parties signing an accession agreement fulfil the scheme's accession criteria.

Admission criteria

To be admitted to the iSHARE network, prospective iSHARE participants need to comply with several criteria*:

- Provide a signed iSHARE accession agreement;
- Provide a valid EORI number (or other nationally recognised chamber of commerce number which can be verified);
- Provide the certificate that will used for iSHARE;

62 https://afsprakenstelsel.etoegang.nl/display/as/Startpagina

- Provide a successful test report of iSHARE certification tool (or otherwise acceptable proof that party's technical implementation adheres to iSHARE specifications, e.g. in case of using 'iSHARE compatible' software).

* For operational reasons, additional admission criteria MAY apply.

Responsibilities

Several parties have responsibilities and tasks in the admission process:

- The **Scheme Owner** is responsible for facilitation of the process while safeguarding the integrity of the iSHARE scheme;
- The prospective iSHARE participant is responsible for implementing the guidelines set out in iSHARE, and for showing compliance with the relevant admission criteria.

Sequence

1. A representative of the prospective iSHARE participant registers with the Scheme Owner and provides the Scheme Owner with:
    a. Primary contact details: name, role, e-mail.
    b. Description of how they will be using iSHARE
    c. A valid EORI number (or other nationally recognised chamber of commerce number which can be verified);
2. The Scheme Owner checks whether there are potential impediments that could block the completion of the admission process for the prospective iSHARE participant:
    a. E.g. previous exclusions from the iSHARE scheme in the recent past;
3. The Scheme Owner will facilitate testing and certification of the prospective iSHARE participant.
    a. The Scheme Owner may provide testing material and documentation on the Scheme test environment: certificates, keys, SDKs, etc.;
    b. For prospective Certified Parties this will include role-specific non-technical requirements.
4. The prospective iSHARE participant formally requests admission to the iSHARE network to the Scheme Owner by providing:
    a. An iSHARE accession agreement signed by an authorised representative of the prospective iSHARE participant;
    b. The certificate that you will use for iSHARE;
    c. Acceptable proof that the prospective participant’s technical implementation adheres to iSHARE specifications;
    d. For prospective Certified Parties additional verification may be required.
5. The Scheme Owner has 5 working days to verify the acceptance of the prospective participant’s admission request and its conformance with the admission criteria.
6. A legal representative of the Scheme Owner signs the participant’s iSHARE accession agreement, and communicates the verified acceptance to the new participant;
7. The Scheme Owner records the participant’s status within the scheme in the iSHARE participant registry.

5.3.1.2 Withdrawal

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

The withdrawal process describes the steps that parties MUST take to withdraw from the iSHARE network.

Withdrawal includes:

- A certified and/or adhering party wants to withdraw from the iSHARE network;

- A certified party wants to downgrade to an adhering party;
- Any other situation in which an adhering or certified party (un)expectedly withdraws from the iSHARE network (e.g. bankruptcy).

The **term of notice** for withdrawal is 1 month for adhering parties, and 6 months for certified parties.

Goal

The goal of the withdrawal process is to let parties withdraw from iSHARE in a simple and controlled way, minimising impact to the trust in the iSHARE scheme and disruption to the functioning of the iSHARE network.

Responsibilities

Several parties have responsibilities and tasks in the withdrawal process:

- The **Scheme Owner** is responsible for facilitation of the process, so that continued operation of the iSHARE network is not disrupted in any way;
- The **withdrawing/downgrading party** is responsible for delivering a withdrawal plan and to minimise the disruption to the functioning of the iSHARE network. The withdrawing party also benefits from a controlled process itself, as it should help to minimise disruption to internal operations.

Sequence

Withdrawal of an adhering party

1. The withdrawing party formally indicates its intention to withdraw from the iSHARE network to the Scheme Owner.
2. The Scheme Owner has 5 working days to acknowledge the intention to withdraw of the withdrawing party; the Scheme Owner makes the acknowledgement known to the withdrawing party, and provides a date on which the withdrawing party will be considered withdrawn from the iSHARE scheme by the Scheme Owner;
3. The withdrawing party communicates its withdrawal to the parties it interacts (interacted) with under iSHARE;
4. The withdrawing party, in cooperation with the Scheme Owner, withdraws from the iSHARE network.

Withdrawal of a certified party, downgrade of a certified party

1. The withdrawing/downgrading party formally indicates its intention to withdraw/downgrade from the iSHARE network to the Scheme Owner. It includes a withdrawal plan based on the (to be set up) template withdrawal procedure;
2. The Scheme Owner has 5 working days to acknowledge the intention to withdraw/downgrade of the withdrawing/downgrading party; the Scheme Owner makes the acknowledgement known to the withdrawing/downgrading party, and provides up to date guidelines;
3. If necessary, the withdrawing/downgrading party sends an updated withdrawal plan to the Scheme Owner, keeping in mind the guidelines provided by the Scheme Owner;
4. The Scheme Owner accepts the withdrawal/downgrading plan or indicates where it requires changes;
5. The Scheme Owner and the withdrawing/downgrading party communicate the intended withdrawal with the iSHARE network per date dd-mm-yyyy;
6. The withdrawing/downgrading party, in cooperation with the Scheme Owner, withdraws/downgrades from the iSHARE network in accordance with the withdrawal plan;
7. The Scheme Owner communicates the completed withdrawal to the iSHARE network.

5.3.1.3 Warnings, Suspension and Exclusion

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

The warnings, suspension and exclusion process describes the steps that the Scheme Owner MUST take to temporarily suspend or permanently exclude participating parties from the iSHARE network in case of non-compliance with scheme rules and guidelines, or actions with significant negative impact on the normal operation of the iSHARE network.

Three classifications of non-compliance are recognised within iSHARE. Note that the impact or risk described is non-exhaustive.

Classification	Impact or risk
Minor non-compliance	• Non-compliance with the iSHARE admission criteria, and/or; • Non-compliance with the iSHARE service levels, and/or; • Expired information security certification (e.g. ISO27001, ISAE 3402), and/or; • Minor data* security breach, for example through the loss of a USB stick, laptop, hard disk, or because of hacking attempts or found malware, and/or; • Fraud or presumption of fraud by, for example an employee or a hacker.
Major non-compliance	• Recurring minor non-compliance, and/or; • Combinations of minor non-compliance, and/or • Serious impediment(s) to other adhering/certified party(s), and/or; • Major data security breach and/or breach that needs to be reported in line with meldplicht datalekken[63], and/or; • (Other) impact on confidentiality and integrity of (data* within) the iSHARE scheme.
Critical non-compliance	• Recurring major non-compliance, and/or; • Network-wide impediment(s) to other parties, and/or; • (Other) impact on confidentiality and integrity of entire iSHARE scheme.

*Data includes the data used for identification, authentication and authorisation purposes in the context of data exchange, but NOT the contents of the actual data exchange.

- **Warnings** are cautionary advices about non-compliance, about what is needed to rectify non-compliance, and by when;
- **Suspension** involves temporary deactivation of adhering/certified credentials within the iSHARE network;
- **Exclusion** involves permanent deactivation of adhering/certified credentials within the iSHARE network of the excluded party, and involves an iSHARE network wide notification of exclusion for information purposes.

Before the Scheme Owner issues warnings, suspends or even excludes parties, it MUST take into consideration/ weigh the interests of the iSHARE scheme and -network (i.e. all adhering/certified parties).

Goal

The goal of the warnings, suspension and exclusion process is to warrant trust in the iSHARE's brand, as well as protecting the confidentiality and/or integrity of (data within) the iSHARE network.

63 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Responsibilities

Several parties have responsibilities and tasks in the warnings, suspension and exclusion process:

- The **Scheme Owner** is responsible for facilitation of the process, to protect the confidentiality and/or integrity of (data within) the iSHARE scheme. More than in other processes he can also take an active role;
- The **adhering/certified party** is responsible for acting, at all times but especially after receiving a warning or suspension, in line with scheme rules and guidelines.

Sequence

1. The reporting party (i.e. any adhering/certified party or the Scheme Owner itself) reports non-compliance to the Scheme Owner, including an estimation of the non-compliance classification;
2. The Scheme Owner assesses the non-compliance and the estimated non-compliance classification by the reporting party, and:
    a. Accepts the non-compliance classification and moves to step 3;
    or
    b. Changes the non-compliance classification and moves to step 3;
    or
    c. Rejects the reported behaviour as non-compliance, and communicates why to the reporting party.
3. If non-compliance leads to a minor incident, calamity or crisis, the incident management process (see page 176) is initiated. Otherwise, step 2 is followed by step 4;
4. The Scheme Owner registers the non-compliance and:
    a. If classified as minor non-compliance, notifies the non-complying party of its non-compliance, the reason(s), and the rectifications/adjustments needed within what timespan;
    b. If classified as major non-compliance, issues the non-complying party an official warning, and communicates its reason(s) and the rectifications/adjustments needed within what timespan;
    c. If classified as critical non-compliance, suspends the non-complying party, by updating the party's status in the scheme registry to 'suspended', until necessary rectifications/adjustments are in place. The Scheme Owner communicates this suspension to the iSHARE network.
5. The non-complying party either:
    a. Rectifies or adjusts within the indicated time span, and informs the Scheme Owner of the rectifications/adjustment;
    or
    b. Communicates its disagreement with the notification/warning to the Scheme Owner within 5 working days, to which the Scheme Owner MUST reply within 5 working days. The non-complying party is given another 5 working days to respond to the Scheme Owner's latest reply (which can include adjustments to its earlier notification/warning);
    or
    c. Does not take any action.
6. If sufficient rectifications/adjustments follow in time, step 8 follows. Otherwise, the Scheme Owner:
    a. If classified as minor non-compliance:
        i. Issues the non-complying party a warning, and communicates its reason(s) and the rectifications/adjustments needed within what timespan.
    b. If classified as major non-compliance:
        i. Issues the non-complying party a last warning before suspension, and communicates its reason(s) and the rectifications/adjustments needed before within what timespan in order not to be suspended.
    c. If classified as critical non-compliance:
        i. Issues the non-complying party a last warning before exclusion, and communicates its reason(s) and the rectifications/adjustments needed before within what timespan in order not to be excluded.

7. If the non-complying party continues to dishonour the (final) warning after a reasonable time, the Scheme Owner:
    a. If classified as minor non-compliance:
        i. Upscales the non-compliance level to major and goes back to step 6b.
    b. If classified as major non-compliance:
        i. Upscales the non-compliance level to critical and goes back to step 4c.
    c. If classified as critical non-compliance:
        i. The Scheme Owner terminates the participation of the non-compliant party by cancellation of the Accession Agreement;
        ii. Excludes the non-complying party from iSHARE, by updating the party's status in the scheme registry to 'ended', and initiates its withdrawal in line (as much as is reasonable) with the withdrawal process (see page 172);
        iii. The Scheme Owner communicates this exclusion to the iSHARE network. The excluded party will not be allowed to take part in the admission process[64] for the next 12 months. Step 7c is followed by step 9.
8. The Scheme Owner considers (new) actions taken by the party adequate, considers the notification or warning honoured and closes the process;
9. The Scheme Owner evaluates the incident with the reporting and/or (an)other party(s), and registers the evaluation for future learning.

5.3.1.4 Incident Management

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

The incident management process describes the steps that the Scheme Owner and adhering- and certified parties MUST take to solve incidents in the iSHARE network.

An **incident** is an event, not part of the standard service operation, that results in a potential impact or risk with regards to the quality, availability, confidentiality and/or integrity of (data within) the iSHARE scheme. This includes the data used for identification, authentication and authorisation purposes in the context of data exchange, but not the contents of the actual data exchange.

Note incident resolution is NOT part of regular maintenance, and therefore is NOT subject to maintenance windows as described under service levels (see page 181).

Three classifications of incidents are recognised within iSHARE. Note that the impact or risk described is non-exhaustive.

Classification	Impact or risk
Minor incident	• Expected unavailability of < 8 hours of an adhering party or < 4 hours of a certified party or < 2 hours of the Scheme Owner, and/or; • (Potential) data security breach, for example through the loss of a USB stick, laptop, hard disk, or because of hacking attempts or found malware, and/or; • Fraud or presumption of fraud by, for example an employee or a hacker.

64 https://innopay.atlassian.net/wiki/spaces/IS/pages/78446637/Admission+of+adhering+parties

Classification	Impact or risk
Calamity	• Direct involvement of three or more adhering/certified parties, and/or; • Serious impediment(s) to other adhering/certified party(s), and/or; • Expected unavailability of > 8 hours of an adhering party or > 4 hours of a certified party or > 2 hours of the Scheme Owner, and/or; • Data security breach that needs to be reported in line with meldplicht datalekken[65], and/or; • (Other) impact on confidentiality and integrity.
Crisis	• Involvement of 10 or more adhering/certified parties, and/or; • Serious impact on image and trustworthiness of iSHARE, and/or; • Expected unavailability of > 48 hours of a certified party or > 12 hours of the Scheme Owner, and/or; • Political implications, and/or; • Fundamental legal or technical vulnerability.

Goal

The goal of the incident management process is to handle and solve different levels of incidents in a structured way and with minimal disruption to the functioning of the iSHARE network.

Responsibilities

Several parties have responsibilities and tasks in the incident management process:

- The **Scheme Owner** proactively coordinates the handling and solving of incidents, and assists if necessary;
- **Adhering/certified parties** are responsible for reporting all incidents in the iSHARE network, and taking the steps necessary to handle and solve incidents.

Sequence

Before initiating the process as below, the reporting party, in conjunction with the causing party (if not the same) MUST assess together whether the event deemed an incident is indeed an incident.

1. The reporting party (i.e. any adhering/certified party or the Scheme Owner itself) reports an incident to the Scheme Owner, including an estimation of the incident classification;
2. The Scheme Owner assesses the incident and the estimated incident classification by the reporting party, and:
    a. Accepts the incident classification and moves to step 3;
    or
    b. Changes the incident classification and moves to step 3;
    or
    c. Rejects the reported event as an incident, and communicates why to the reporting party.
3. The Scheme Owner registers the incident and initiates incident handling, as follows:
    a. If classified as a **minor incident:**
        i. If the minor incident is assessed the result of non-compliance with scheme rules and guidelines, and/or if it has had significant negative impact on the normal operation of the

65 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

iSHARE network, the warnings, suspension and exclusion process (see page 174) will also be initiated;

ii. The Scheme Owner gives the reporting party, the causing party and/or (an)other party(s) - whichever it deems most capable/suitable - the responsibility of handling the minor incident, under supervision of the Scheme Owner (see step 4);

iii. The party(s) responsible for handling the minor incident communicates the minor incident, the incident manager, and that the minor incident is being solved, to the parties impacted by it.

b. If classified as a **calamity**:

i. If the calamity is assessed the result of non-compliance with scheme rules and guidelines, and/or if it has had significant negative impact on the normal operation of the iSHARE network, the warnings, suspension and exclusion process (see page 174) will also be initiated;

ii. The Scheme Owner gives the reporting party, the causing party and/or (an)other party(s) - whichever it deems most capable/suitable - the responsibility of handling the calamity, under supervision of the Scheme Owner (see step 4);

- IF there is a data security breach that needs to be reported in line with meldplicht datalekken[66], the party(s) responsible for handling the calamity report the data security breach to the *Autoriteit Persoonsgegevens* (personal data authority) and follow the authority's guidelines on the rest of the incident management process;

iii. The Scheme Owner informs the iSHARE network of the calamity (and that it is being solved) and who the incident manager is, as well as any parties outside the network that it deems necessary to inform (e.g. branch organisations, the NCSC or even law enforcement);

iv. The Scheme Owner sets up an action plan to minimise risks and damage.

c. If classified as a **crisis**:

i. If the crisis is assessed the result of non-compliance with scheme rules and guidelines, and/or if it has had significant negative impact on the normal operation of the iSHARE network, the warnings, suspension and exclusion process (see page 174) will also be initiated;

ii. The Scheme Owner gives the reporting party, the causing party and/or (an)other party(s) - whichever it deems most capable/suitable - the responsibility of handling the crisis, under supervision of and assisted by the Scheme Owner (see step 4). Different to the process for minor incidents and calamities, the Scheme Owner can also choose to take the responsibility of handling the crisis itself even if it is not the causing party;

- IF there is a data security breach that needs to be reported in line with meldplicht datalekken[67], the party(s) responsible for handling the calamity report the data security breach to the *Autoriteit Persoonsgegevens* (personal data authority) and follow the authority's guidelines on the rest of the incident management process;

iii. The Scheme Owner informs the iSHARE network of the crisis (and that it is being solved) and who the incident manager is, as well as any parties outside the network that it deems necessary to inform (e.g. branch organisations, the NCSC or even law enforcement);

iv. The Scheme Owner sets up an action plan to minimise risks and damage.

4. The Scheme Owner coordinates the contact with the involved parties, monitors progress and assists in handling the incident if necessary. The Scheme Owner also communicates progress to the iSHARE network in case of a calamity or crisis. If progress is non-compliant to the incident service level, the Scheme Owner MAY choose to upscale (from incident to calamity or from calamity to crisis);
5. When the incident is handled and therefore solved, the Scheme Owner closes the incident;
   a. In case of a minor incident, the responsible party communicates the incident closure to the parties impacted by it;
   b. In case of a calamity or crisis, the Scheme Owner communicates the incident closure to the iSHARE network.

66 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
67 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

6. The Scheme Owner evaluates the incident with the reporting and/or (an)other party(s), and registers the evaluation for future learning. It can choose to share the gained insights with (selected) parties in the iSHARE network.

5.3.1.5 Release Management

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

The iSHARE scheme is dynamic. The release management process describes the steps that the Scheme Owner MUST take to make changes that impact the legal or technical iSHARE scheme agreements.

These **changes** include alterations to:

- iSHARE scheme documentation and -specifications;
- The Scheme Owner API;
- Scheme Owner tools (e.g. test- and certification tools).

Goal

The goal of the release management process is to:

- Decide in a standardised, transparent way on what changes are (not) made;
- Release changes in a standardised way, with minimal disruption to the functioning of the iSHARE network.

Responsibilities

Several parties have responsibilities and tasks in the release management process:

- The **Scheme Owner** is responsible for facilitation of a swift course of the process, and for minimising the impact of changes and releases for all participants;
- The **Change Advisory Board** has the responsibility to advise the Scheme Owner on proposed changes;
- **Adhering/certified parties** can (cooperatively) prepare and submit a Requests for Change (RFC) to the Scheme Owner.

Sequence

The following sequence is based on ITIL v3[68].

1. One or several submitting parties (this can also include the Scheme Owner) submit an RFC which describes at a minimum:
    a. A description of the desired change;
    b. A description of the context/immediate cause;
    c. An indication of what priority the change should have;
    d. The potential solution (direction);
    e. The impact for certified and/or adhering parties and the Scheme Owner;
    f. The justification of the change in a business case.
2. The RFC is logged by the Scheme Owner;
3. The Scheme Owner assesses the feasibility and impact of the submitted RFC and:
    a. Schedules the proposed RFC for review by the Change Advisory Board. He communicates this to the submitting party(s);
    b. Does NOT schedule the proposed RFC for review by the Change Advisory Board. He issues a written statement to the submitting party(s) explaining why;

68 https://wiki.en.it-processmaps.com/index.php/Change_Management

4. The Change Advisory Board assesses the RFC and provides the Scheme Owner with advice on how to proceed;
5. On the basis of the CAB advice, a draft solution and the estimated impact, the Scheme Owner either:
    a. Accepts the RFC and prioritises the change;
    or
    b. Rejects the RFC;
6. The Scheme Owner issues a written statement to the CAB and the submitting party(s), explaining the reasoning behind the acceptance/rejection of an RFC and the change's priority;
7. If relevant, the Scheme Owner updates the release calendar and the priority of upcoming changes;
8. The Scheme Owner alters the iSHARE scheme based on the release calendar, and publishes a new version of the scheme accordingly.

Emergency changes are changes that MUST be implemented as soon as possible, for example to resolve a major or critical incident. In case of an emergency change the Scheme Owner accelerates the execution of the process. He can choose to consult (members of) the CAB on an ad-hoc basis if timing permits and deemed necessary.

If a change does NOT impact the legal or technical scheme agreements, the change MAY be made without taking the steps described here. Such changes include but are not limited to the restructuring of content, correcting grammatical mistakes, and maintenance to hyperlinks and labels.

5.3.1.6 Management reporting

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

The management reporting process describes the steps that parties MUST take to deliver management information about the use and working of the iSHARE network.

Goal

The goal of the management reporting process is to monitor compliance to service level agreements, and to distribute info about the use of the iSHARE network.

Responsibilities

Several parties have responsibilities and tasks in the management reporting process:

- The **Scheme Owner** is responsible for delivering its own management information on a monthly basis, and to process received management information into a report that does not include commercially sensitive information;
- The **certified party** is responsible for delivering management information timely on a monthly basis.

Sequence

1. On a monthly basis, certified parties and the Scheme Owner collect management information about:
    a. the use of the iSHARE network;
    b. compliance with the service level agreements.
2. Certified parties and the Scheme Owner deliver the collected management information to the Scheme Owner in compliance with the standard format and service level;

3. The Scheme Owner processes the received management information on compliance, and, if non-compliance is detected, follows the warnings, suspension and exclusion process (see page 174)to assess whether this is an incident or structural non-compliance;
4. The Scheme Owner verifies whether each certified party's management information on the use of the iSHARE scheme is correct:
    a. If correct, step 5 follows directly.
    b. If incorrect, a maximum of 5 working days are available for the certified party(s) to rectify. If 5 working days are not enough, step 5 follows without the incorrect information;
5. Quarterly, the Scheme Owner processes and anonymises (if necessary) the management information on the use of the iSHARE scheme into a report containing:
    a. Number of certified parties (also compared to last month and this month previous years);
    b. Number of adhering parties;
    c. Other information deemed necessary (to be decided);
    If incorrect information was found and could not be rectified within 5 days in step 4, a description of the missing management information.
6. The Scheme Owner distributes the management report.

5.3.2 Service levels

This section describes the service levels that apply to iSHARE certified parties[69], adhering parties[70], and the Scheme Owner[71].

A **service level** measures the performance of a service. Per service level described in this section, an explanation of the service level is given before both the norm and the minimum level are defined.

The following service levels are described per party. Please click on the 'X' in each column to be redirected to the specific service level description.

	Adhering parties	Certified parties	Scheme Owner
Service level			
Availability	X (see page 182)	X (see page 182)	X (see page 183)
Performance	X (see page 184)	X (see page 184)	X (see page 185)
Incidents	X (see page 185)	X (see page 186)	X (see page 186)
Support	X (see page 187)	X (see page 187)	X (see page 188)
Reporting		X (see page 188)	X (see page 188)

The service levels are monitored by the Scheme Owner through:

- Analysis of certified party reports;
- Random sampling.

No norm is set for monitoring frequency or detail.

69 https://innopay.atlassian.net/wiki/spaces/IS/pages/78282844/Certified+parties
70 https://innopay.atlassian.net/wiki/spaces/IS/pages/78610472/Adhering+parties
71 https://innopay.atlassian.net/wiki/spaces/IS/pages/78282851/Scheme+Owner+service+levels

5.3.2.1 Availability

Availability is a measure of the time a service is in a functioning condition. It includes the availability window and the maintenance window.

Availability service levels are defined for adhering (see page 182)- and certified parties (see page 182) and the Scheme Owner (see page 183).

APs | Availability

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Availability is a measure of the time a service is in a functioning condition. It includes the availability window and the maintenance window.

Availability window

The **availability window** includes the times at which adhering parties guarantee the availability of their service.

No norm is set for adhering parties' availability window, to leave Service Providers free to run their service whenever they deem appropriate (e.g. a trucking company does not need to leave its trucks' board computers on 24 hours * all days of the year).

Minimum level required at times deemed appropriate to run service**:** guideline of 95% availability* per calendar month, from 00:00-23:59h

*Planned maintenance does NOT count as unavailability

Maintenance window

The **maintenance window** includes the times at which adhering parties can perform planned maintenance, that is likely to result in downtime, to their service. If no downtime is expected, maintenance can take place outside of the maintenance window. Planned maintenance does NOT include incident resolution, as this can take place outside the maintenance window as described under incidents (see page 186).

Norm:

- The maintenance window includes all times outside office hours;
- **No norm** is set for communication about (different forms of) maintenance, as this is a matter between adhering parties.

CPs | Availability

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Availability is a measure of the time a service is in a functioning condition. It includes the availability window and the maintenance window.

Availability window

The **availability window** includes the times at which certified parties guarantee the availability of their service.

Norm: 24 hours * all days of the year

Minimum level required: 99% availability* per calendar month, from 00:00-23:59h

*Planned maintenance does NOT count as unavailability

Maintenance window

The **maintenance window** includes the times at which certified parties can perform planned maintenance, that is likely to result in downtime, to their service(s). If no downtime is expected, maintenance can take place outside of the maintenance window. Planned maintenance does NOT include incident resolution, as this can take place outside the maintenance window as described under incidents (see page 186).

Norm:

- The maintenance window includes the nights from Friday to Saturday and from Saturday to Sunday, from 00:00-5.59h;
- Maintenance MUST be announced to the impacted parties directly as well as to the Scheme Owner**;
- Announcements MUST be made at least 10 working days before the maintenance and MUST include date, time, and impacted service(s).

**The Scheme Owner presents an overview of its own and certified parties' current and planned maintenance on its website

SO | Availability

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Availability is a measure of the time a service is in a functioning condition. It includes the availability window and the maintenance window.

Availability window

The **availability window** includes the times at which the Scheme Owner guarantees the availability of its service.

Norm: 24 hours * all days of the year

Minimum level required: 99% availability* per calendar month, from 00:00-23:59h

*Planned maintenance does NOT count as unavailability

Maintenance window

The **maintenance window** includes the times at which the Scheme Owner can perform planned maintenance, that is likely to result in downtime, to its service(s). If no downtime is expected, maintenance can take place outside of the maintenance window. Planned maintenance does NOT include incident resolution, as this can take place outside the maintenance window as described under incidents (see page 186).

Norm:

- The maintenance window includes the nights from Friday to Saturday and from Saturday to Sunday, from 00:00-5.59h;

- The maintenance MUST be announced**;
- Announcements MUST be made at least 10 working days before the maintenance and MUST include date, time, and impacted service(s).

**The Scheme Owner presents an overview of its own and certified parties' current and planned maintenance on its website

5.3.2.2 Performance

Performance includes the time it takes for a service to respond when requested or called upon; i.e. the time a party's service takes to respond to a received message.

Performance service levels are defined for adhering (see page 184)- and certified parties (see page 184) and the Scheme Owner (see page 185).

APs | Performance

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Performance includes the time it takes for a service to respond when requested or called upon; i.e. the time an adhering party's service takes to respond to a received message.

Before an adhering party knows whether it may respond to a request, however, it often needs to request (more) information from one or more certified parties; e.g. delegation info or authorisation info. It therefore needs to send out a new message itself, and wait for this message to be responded to by a certified party. While certified parties' response times are short (see page 184), the process of sending out and receiving (sometimes several) new messages before the original request can be answered takes time. Consequently, **no norm** is set for adhering parties' total performance. The following **guidelines** are set:

- 95% of adhering parties' messages SHOULD be responded within 2 seconds of receiving all information needed from certified parties;
- 99% of adhering parties' messages SHOULD be responded within 5 seconds of receiving all information needed from certified parties;
- Each adhering party SHOULD be able to process at least 100 simultaneous messages while meeting above requirements.

CPs | Performance

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Performance includes the time it takes for a service to respond when requested or called upon; i.e. the time a certified party's service takes to respond to a received message.

Norm:

- 95% of messages MUST be responded within 2 seconds;
- 99% of the messages MUST be responded within 5 seconds;
- Each certified party MUST be able to process at least 100 simultaneous messages while meeting above requirements.

SO | Performance

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Performance includes the time it takes for a service to respond when requested or called upon; i.e. the time the Scheme Owner's service takes to respond to a received message.

Norm:

- 95% of messages MUST be responded within 2 seconds;
- 99% of the messages MUST be responded within 5 seconds;
- The Scheme Owner MUST be able to process at least 100 simultaneous messages while meeting above requirements.

5.3.2.3 Incidents

An **incident** is an event, not part of the standard service operation, that results in a potential impact or risk with regards to the quality, availability, confidentiality and/or integrity of (data within) the iSHARE scheme. This ONLY includes the data used for identification, authentication and authorisation purposes in the context of data exchange, but not the contents of the actual data exchange.

Three classifications of incidents are recognised within iSHARE, as explained in the incident management process (see page 176):

- Minor incident;
- Calamity;
- Crisis.

Incident service levels are defined for adhering (see page 185)- and certified parties (see page 186) and the Scheme Owner (see page 186).

APs | Incidents

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

An **incident** is an event, not part of the standard service operation, that results in a potential impact or risk with regards to the quality, availability, confidentiality and/or integrity of (data within) the iSHARE scheme. This ONLY includes the data used for identification, authentication and authorisation purposes in the context of data exchange, but not the contents of the actual data exchange.

Three classifications of incidents are recognised within iSHARE, as explained in the incident management process (see page 176):

- Minor incident;
- Calamity;
- Crisis.

Norm:

- All incidents MUST be communicated by the adhering party(s) to the Scheme Owner directly after they are discovered;
- Communication MUST include date, time, incident level as estimated by the adhering party(s), argumentation including impacted service(s), and a potential incident manager;

- In case of a calamity or crisis, the adhering party MUST have an incident manager available during working days, and SHOULD have an incident manager available 24 * 7;
- An update on the incident MUST be communicated to the Scheme Owner*:
    - For minor incidents, at the end of each working day;
    - For calamities, within 2 hours of every significant update and at the end of each working day;
    - For crises, within 2 hours of every significant update and every 4 hours.
- All incidents SHOULD be handled by the adhering party (in cooperation with the Scheme Owner as per the incident management process (see page 176)) within 3 working days after being appointed as the responsible party - unless agreed otherwise.

*In line with the incident management process (see page 176), the Scheme Owner presents an overview of current calamities and crises on its website

CPs | Incidents

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

An **incident** is an event, not part of the standard service operation, that results in a potential impact or risk with regards to the quality, availability, confidentiality and/or integrity of (data within) the iSHARE scheme. This ONLY includes the data used for identification, authentication and authorisation purposes in the context of data exchange, but not the contents of the actual data exchange.

Three classifications of incidents are recognised within iSHARE, as explained in the incident management process (see page 176):

- Minor incident;
- Calamity;
- Crisis.

Norm:

- All incidents MUST be communicated by the certified party(s) to the Scheme Owner directly after they are discovered;
- Communication MUST include date, time, incident level as estimated by the certified party(s), argumentation including impacted service(s), and a potential incident manager;
- In case of a calamity or crisis, the certified party MUST have an incident manager available during working days, and SHOULD have an incident manager available 24 * 7;
- An update on the incident MUST be communicated to the Scheme Owner*:
    - For minor incidents, at the end of each working day;
    - For calamities, within 2 hours of every significant update and at the end of each working day;
    - For crises, within 2 hours of every significant update and every 4 hours.
- All incidents SHOULD be handled by the certified party (in cooperation with the Scheme Owner as per the incident management process (see page 176)) within 3 working days after being appointed as the responsible party - unless agreed otherwise.

*In line with the incident management process (see page 176), the Scheme Owner presents an overview of current calamities and crises on its website

SO | Incidents

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

An **incident** is an event, not part of the standard service operation, that results in a potential impact or risk with regards to the quality, availability, confidentiality and/or integrity of (data within) the iSHARE scheme. This ONLY includes the data used for identification, authentication and authorisation purposes in the context of data exchange, but not the contents of the actual data exchange.

Three classifications of incidents are recognised within iSHARE, as explained in the incident management process (see page 176):

- Minor incident;
- Calamity;
- Crisis.

Norm:

Incident at the Scheme Owner:

- In case of a calamity or crisis, the Scheme Owner MUST have an incident manager available 24 * 7;
- An update on the incident MUST be communicated*:
    - For calamities, within 2 hours of every significant update and at the end of each working day;
    - For crises, within 2 hours of every significant update and every 4 hours.
- All incidents SHOULD be handled by the Scheme Owner within 3 working days - unless unreasonable.

Incident at another party:

- In case of any crisis, the Scheme Owner SHOULD be available 24 * 7 for assistence.

*In line with the incident management process (see page 176), the Scheme Owner presents an overview of current calamities and crises on its website

5.3.2.4 Support

Support includes answering questions and requests from other parties.

Incident service levels are defined for adhering (see page 187)- and certified parties (see page 187) and the Scheme Owner (see page 188).

APs | Support

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Support by adhering parties could include answering questions, requests, and complaints from other adhering parties.

No norm is set for adhering parties as it is a matter between them (and other adhering parties). The following **guidelines** are set, however:

- Adhering parties are available for support via e-mail;
- They SHOULD confirm receiving a question/request within 1 working day. They SHOULD send an underpinned reaction (with an answer/solution or at the very least a direction) within 5 working days.

CPs | Support

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Support by certified parties includes answering questions and requests from adhering parties.

Norm: certified parties are available for support via e-mail; they MUST confirm receiving a question/request within 1 working day. They SHOULD send an underpinned reaction (with an answer/solution or at the very least a direction) within 5 working days.

SO | Support

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Support by the Scheme Owner includes answering questions and requests from certified parties (other than incidents (see page 176) and NOT from adhering parties).

Norm: the Scheme Owner is available for support via e-mail; it MUST confirm receiving a question/request within 1 working day. It SHOULD send an underpinned reaction (with an answer/solution or at the very least a direction) within 5 working days.

5.3.2.5 Reporting

Reports are meant to monitor both compliance to the service level agreements and the (growing) use of the iSHARE network, as described in the management reporting process (see page 180).

Reporting service levels are defined for certified parties (see page 188) and the Scheme Owner (see page 188).

CPs | Reporting

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Reports are meant to monitor both compliance to the service level agreements and the (growing) use of the iSHARE network, as described in the management reporting process (see page 180). The following will be reported on (non-exhaustive):

- Availability;
- Number of relations with adhering parties;
- Number of transactions;
- Number of transactions per adhering party;
- Number of incidents.

Certified parties are expected to collect management information about each month: 0:00h on the first day to 23:59h on the last.

Norm: each certified party MUST deliver the management information about the last month, conform the iSHARE template, before 23:59h on the 5th working day of the current month

SO | Reporting

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

Reports are meant to monitor both compliance to the service level agreements and the (growing) use of the iSHARE network, as described in the management reporting process (see page 180).

The following will be reported on (non-exhaustive):

- Availability;
- Number of relations with adhering parties;
- Number of transactions;
- Number of transactions per adhering party;
- Number of incidents.

The Scheme Owner is expected to collect its own management information about each month - 0:00h on the first day to 23:59h on the last - *and* to collect and process certified parties' management information into a quarterly management report.

Norm:

- The Scheme Owner MUST have collected its own management information about the last calendar month before 23:59h on the fifth working day of the current month;
- In January, April, July and October, the Scheme Owner MUST process and anonymise its own and the received management information about the last three months into a quarterly report, and distribute this report before 16:59h on the 10th working day of the current month

5.3.3 Communication

This part of the iSHARE scheme is considered normative and is therefore compliant with RFC 2119.

This section describes the agreements concerning communication about and with the iSHARE brand that is applicable for all adhering- and certified parties.

It includes the guidelines for using iSHARE's name, brand, and iSHARE logo.

5.3.3.1 Usage of iSHARE name and brand

The following communication rules apply when using the iSHARE name and brand:

- All participating parties MUST use the visuals and logos as provided by the iSHARE Style Guide and MUST apply the notation and terminology as described in the Glossary. This creates clarity in the communication and brand image of iSHARE;
- The term iSHARE is used as a brand for machine-to-machine and human-to-machine iSHARE-services;
- Participating parties within the iSHARE scheme MAY use the phrase ‘powered by iSHARE’ to support their own branding;
- If iSHARE is integrated in human-to-machine software, the iSHARE logo SHOULD be used in user interfaces;
- Adhering- and certified parties COULD use standard texts, key messages and other textual and visual elements as provided in the communication toolkit provided by the Scheme Owner.

5.3.3.2 Usage of iSHARE logo

The following basic principles apply to the use of the iSHARE logo:

- Please use enough white space around the logo;
- Do not alter the colouring of the logo (or use the black and white logo).

iSHARE logo material can be downloaded here[72].

5.4 Legal

The iSHARE scheme is underpinned by legal agreements to which all participants (both adhering parties and certified parties) need to adhere. This section contains all of the legal aspects present within iSHARE:

Legal Aspect:	Description:
Accession Agreement (for adhering parties (see page 191) **and** certified parties (see page 192)**)**	The main contract between the participant and the iSHARE Scheme Owner. This main contract refers to the terms of use, including all iSHARE specifications, to which all participants must abide. After signing the Accession Agreement, an organisation becomes a participant of the iSHARE scheme either as an adhering party or a certified party.
Terms of Use (see page 193)	The Terms of Use are an appendix to and integral part of the Accession Agreement. The Terms of Use further define the rights and obligations of the various roles within the iSHARE scheme. The Terms of Use provide a uniform set of rules for both the participants and the scheme owner, thereby fostering a level playing field between all parties involved. The Terms of Use are drafted in such a way that data can be exchanged by participants even if they have no other contractual arrangement in place. In that case, the default requirements as set forth in the Terms of Use govern their legal relationship. This includes the (license) conditions that apply to the exchange of data. But the Terms of Use leave room for participants to derogate from or further detail the provisions of the Terms of Use on a bilateral basis. However, there will be certain requirements that participants should comply with at any time, and from which they will not be able to deviate. These are the requirements that deal with the proper functioning of the iSHARE scheme, such as each party's responsibility to safeguard the security of its IT-systems (articles 3.5 and 4.1). Furthermore, the Terms of Use include a number of annexes, amongst which the pre-defined conditions of exchange, the Legal Framework and the iSHARE scheme standards and specifications.
Legal[73]Context (see page 198)	The Legal Framework deals with the legal context of the iSHARE scheme. It describes the laws and regulations that are of particular importance for participants when exchanging data within the iSHARE scheme: the eIDAS regulation, the General Data Protection Regulation, competition law and the Dutch civil code. As stipulated in the Accession Agreement and the Terms of Use, all participants are expected to comply with these and all other applicable national and international pieces of legislation.

72 https://www.ishareworks.org/press-room/beeldmateriaal
73 https://innopay.atlassian.net/wiki/spaces/IS/pages/55602397/Legal+Framework

5.4.1 Accession Agreement for adhering parties

5.4.1.1 ACCESSION AGREEMENT FOR PARTICIPATION

ADHERING PARTIES - iSHARE SCHEME

The Scheme Owner and the [COMPANY NAME] (hereafter: 'the Adhering Party') enter into an agreement which specifies the terms and conditions under which:

- the Adhering Party shall participate in the exchange of Data under the rules and specifications of the iSHARE scheme;
- the Scheme Owner shall [SPECIFY ROLE SCHEME OWNER IN RESPECT OF ADHERING PARTIES].

The Adhering Party hereby declares to comply with the following rules for participation in the iSHARE scheme:

- The Adhering Party must comply to the iSHARE specific requirements <TBD by other working group> as defined in the (annexes to the) Terms of Use.
- The Adhering Party can apply for participation in the iSHARE Council of Participants and the Change Advisory Board as defined in the statutes of the Scheme Owner <not yet set up or established / depending on further development and role of the iSHARE scheme>.
- The Adhering Party agrees with and accepts the Terms of Use as specified in Appendix 1.
- Participation in the iSHARE scheme is subject to a [TBD: ANNUAL/MONTHLY] participation fee as stated in Appendix 2. The Scheme Owner may adjust participation fee rates once a year with effect from January the 1st with two (2) months' prior written notice to the Adhering Party. If the Adhering Party cancels this Accession Agreement in accordance with the Terms of Use, the Scheme Owner will refund any participation fee paid upfront for the remaining months of the year.
- The Scheme Owner's invoices are due upon receipt and must be fully paid within 30 days after the invoice date.

Duration

The Accession Agreement is entered into for an initial period of twelve (12) months. During the initial period, the Adhering Party may only terminate the Accession Agreement as set forth in the Terms of Use. After the initial period, the Accession Agreement shall be tacitly extended for an indefinite period of time and may be terminated subject to the notice period as stated in the Terms of Use.

The Adhering Party declares compliance to all rules set forth in this Accession Agreement, including the referenced appendices.

	Adhering Party	**Scheme Owner**
Name		

Company		
Place		
Date		
Signature		

APPENDIX 1: TERMS OF USE iSHARE SCHEME (see page 193)

APPENDIX 2: PARTICIPATION FEES

5.4.2 Accession Agreement for certified parties

5.4.2.1 ACCESSION AGREEMENT FOR PARTICIPATION

CERTIFIED PARTIES - iSHARE SCHEME

The Scheme Owner and the [COMPANY NAME] (hereafter: 'the Certified Party') enter into an agreement which specifies the terms and conditions under which:

- the Certified Party shall [SPECIFY SERVICES] under the rules and specifications of the iSHARE scheme;
- the Scheme Owner shall [supervise that the Certified Party shall act in a reliable and professional manner, in compliance with applicable law and all relevant technical specifications, to safeguard consistency across the whole iSHARE scheme].

The Certified Party hereby declares to comply with the following rules for participation in the iSHARE scheme:

- The Certified Party must comply to the iSHARE specific requirements and specifications as defined in the (annexes to the) Terms of Use.
- The Certified Party can apply for participation in the iSHARE Council of Participants and the Change Advisory Board as defined in the statutes of the Scheme Owner <not yet set up or established / depending on further development and role of the iSHARE scheme>.
- The Certified Party agrees with and accepts the Terms of Use as specified in Appendix 1.
- Participation in the iSHARE scheme is subject to a [TBD: ANNUAL/MONTHLY] participation fee as stated in Appendix 2. The Scheme Owner may adjust participation fee rates once a year with effect from January the 1st with two (2) months' prior written notice to the Certified Party. If the Certified Party cancels this Accession Agreement in accordance with the Terms of Use, the Scheme Owner will refund any participation fee paid upfront for the remaining months of the year.
- The Scheme Owner's invoices are due upon receipt and must be fully paid within 30 days after the invoice date.

Duration

The Accession Agreement is entered into for an initial period of twelve (12) months. During the initial period, the Certified Party may only terminate the Accession Agreement as set forth in the Terms of Use. After the initial period, the Accession Agreement shall be tacitly extended for an indefinite period of time and may be terminated subject to the notice period as stated in the Terms of Use.

The Certified Party declares compliance to all rules set forth in this Accession Agreement, including the referenced appendices.

	Certified Party	**Scheme Owner**
Name		
Company		
Place		
Date		
Signature		

APPENDIX 1: TERMS OF USE iSHARE SCHEME (see page 193)

APPENDIX 2: PARTICIPATION FEES

5.4.3 Terms of Use

TERMS OF USE

iSHARE SCHEME

ARTICLE 1. APPLICABILITY

1.1 These Terms of Use apply to each party participating in the iSHARE scheme.

1.2 In addition to the laws and regulations described in the Legal Framework, these Terms of Use will apply to each party participating in the iSHARE scheme and govern the rights and obligations of each party as well as the relationships between the parties.

1.3 In the event of a conflict between the parties' private agreement(s) and these Terms of Use, the private agreement(s) will prevail, with the exception of the matters covered by the Articles 3.5, 4.1, 6.3 and the Annexes. [other mandatory articles to be determined in consultation with other working groups].

ARTICLE 2. DEFINITIONS

The terms used in these Terms of Use, both in the singular and plural, shall be understood to mean the following:

2.1 **Accession Agreement**: the agreement that governs the admission of adhering parties and certified parties to the iSHARE scheme. In the event of a conflict with the Terms of Use, the provisions in the Accession Agreement will prevail.

2.2 **Adhering party**: an Entitled Party, a Service Consumer or a Service Provider.

2.3 **Annex(es)**: the annex(es) that are inextricably linked with the Terms of Use. In the event of a conflict with the Terms of Use, the provisions in the Terms of Use will prevail.

2.4 **Authorisation Registry**: a party that holds authorisation information that Service Providers can use to determine the rights of the Service Consumer in relation to a specific Dataset.

2.5 **Certified party**: an Authorisation Registry, an Identity Broker or an Identity Provider that has been certified by the Scheme Owner.

2.6 **Conditions of Exchange**: the licence conditions that are inextricably linked to an exchanged Dataset.

2.7 **Data or Dataset**: the data exchanged in the context of the iSHARE scheme.

2.8 **Entitled Party**: a legal entity that has one or more rights to specific Datasets.

2.9 **Human Service Consumer**: a natural person who acts on behalf of and under the responsibility of the Service Consumer.

2.10 **Identity Broker**: a party whose services a Service Provider can use to connect to one or more Identity Providers.

2.11 **Identity Provider**: a party that holds the digital identity information on a Human Service Consumer which that Human Service Consumer can use to identify himself/herself towards a Service Provider.

2.12 **iSHARE scheme**: the set of specifications which govern the relationships between the parties in the iSHARE scheme, including, without limitation, the exchange mechanism and the actual exchange of Data.

2.13 **Legal Framework**: the non-exhaustive overview of relevant and applicable laws and regulations in respect of the iSHARE scheme. The Legal Framework is described in Annex II to these Terms of Use.

2.14 **Scheme Owner**: the entity <not yet set up or established / depending on further development of the scheme> responsible for management and continued development of the iSHARE scheme[, as well as for controlling and monitoring the parties' compliance with the iSHARE scheme].

2.15 **Party**: an entity that participates in the iSHARE scheme as an adhering party and/or as a certified party.

2.16 **Service Consumer**: a party who requests the Service Provider to provide a service relating to the exchange of Data, or any ancillary services, such as services rendered on the basis of an authorisation established within the iSHARE scheme.

2.17 **Service Provider**: a party who provides a service relating to the Data to be exchanged with a Service Consumer, or any ancillary services, such as services rendered on the basis of an authorisation established within the iSHARE scheme.

2.18 **Terms of Use**: this document, including the Annexes.

ARTICLE 3. RIGHTS AND OBLIGATIONS OF ADHERING PARTIES

3.1 To the extent applicable, the adhering party who is sending the Data is responsible for linking the Conditions of Exchange to the Data to be exchanged. Each Dataset can be provided with an attribute. This is a code to which

the Conditions of Exchange of the adhering party who is exchanging the Data are linked. It is up to the adhering parties who are exchanging the Data to agree on any commercial arrangements with regard to that exchange.

3.2 The Service Provider is responsible for determining the assurance level of identification of the Human Service Consumer within the iSHARE scheme.

3.3 To the extent applicable, the rights of the Service Consumer related to the exchange of a specific Dataset is determined by the Conditions of Exchange. The various licence conditions are linked to the Dataset by means of a data exchange code. The data exchange codes and their meaning are described in Annex I to these Terms of Use. If a Dataset does not contain a data exchange code, the default Conditions of Exchange as indicated in Annex I apply. The Service Provider and the Service Consumer agree to comply with the Conditions of Exchange.

3.4 Service Consumers will supervise and are responsible for their Human Service Consumers. Service Consumers will not permit any practice that could lead to improper handling by their Human Service Consumers, including, without limitation, the unauthorised use of authentication tokens linked to individuals and/or the organisation, or the use of authentication tokens for any purpose other than the purpose for which they were issued. Service Consumer will make their Human Service Consumers aware of these Terms of Use.

3.5 An adhering party is responsible for the security and monitoring of the network connections and systems that it uses in the context of the iSHARE scheme. An adhering party will take appropriate technical and organisational measures in order to safeguard the security, including those measures and use of standards as described in Annex III.

3.6 In case an adhering party notices or suspects irregularities in the Data it receives, that party shall immediately notify the Service Consumer(s) and/or the Service Provider concerned. Where applicable, the Service Provider shall immediately notify the Entitled Party.

3.7 The Scheme Owner grants the adhering party a limited, non-exclusive and non-transferable license to use - during the term of the Accession Agreement - the trademarks and trade names 'iSHARE' and 'iSHARE adhering party' and any other trademarks or trade names related to the iSHARE scheme, as determined by Scheme Owner. The trademarks and trade names may only be used in accordance with the communication guidelines as described Annex III.

ARTICLE 4. RIGHTS AND OBLIGATIONS OF CERTIFIED PARTIES

4.1 The certified party is responsible for the security and monitoring of the network connections and systems that it uses in the context of the iSHARE scheme. All certified parties will take appropriate technical and organisational measures in order to safeguard the security, including those measures and use of standards as described in Annex III.

4.2 In addition to its own statutory obligations, the certified party shall notify the Scheme Owner of a (potential) network failure or (suspicion of) a security breach in the accordance with the incident management process as described in Annex III. The certified party shall warrant that the information it provides is complete and accurate.

4.3 The Scheme Owner grants the certified party a limited, non-exclusive and non-transferable license to use - during the term of the Accession Agreement - the trademarks and trade names 'iSHARE' and 'iSHARE certified party' and any other trademarks or trade names related to the iSHARE scheme, as determined by the Scheme Owner from time to time hereafter. The trademarks and trade names may only be used in accordance with the communication guidelines as described Annex III.

ARTICLE 5. RIGHTS AND OBLIGATIONS OF THE SCHEME OWNER

5.1 The Scheme Owner is not allowed to access exchanged Data.

5.2 The Scheme Owner will maintain and publish a publicly accessible registry of parties and their respective roles within the iSHARE scheme.

5.3 The Scheme Owner is entitled to suspend a party, or terminate its participation and registration in the iSHARE scheme in accordance with the warnings, suspension and exclusion process included in Annex III, or if that party breaches the Accession Agreement, these Terms of Use and/or applicable laws and regulations in respect of the iSHARE scheme. Termination of a party's participation is done by cancellation of the Accession Agreement with that party by the Scheme Owner.

5.4 The Scheme Owner determines which parties can be admitted to the iSHARE scheme and on what conditions. The standards and (technical) specifications under which certified parties will be accredited are specified in Annex III to these Terms of Use.

5.5 Every 24 months, the certified party shall conduct an audit through an independent certified auditor to verify compliance with the conditions, standards and (technical) specifications under which the certified party is accredited. In addition to the bi-annual audit, the Scheme Owner in its sole discretion, may determine that more frequent audits are required when there are specific grounds for suspecting a possible breach of these conditions, standards or (technical) specifications. Unless otherwise agreed with the Scheme Owner, the certified party will conclude each audit within a period of thirty (30) days. The findings resulting from any audit will be evaluated in mutual consultation by the Scheme Owner and the certified party. The costs of all audits will be borne by the certified party.

ARTICE 6. CONFIDENTIALITY AND PRIVACY

6.1 The party to whom information (including the Data) is provided shall only use that information for the purpose for which it has been provided. Neither party shall provide the information to any third party other than those to whom he may provide information within the framework of the iSHARE scheme, or as otherwise agreed between the parties, unless it is obliged to do so in pursuance of a statutory duty or required by court order. Furthermore, the parties shall accept the duty to observe strict secrecy when the information is marked as confidential or when the receiving party knows or should reasonably suspect that the information was intended to be confidential.

6.2 The parties shall protect the information against unauthorised access using a level of protection that is reasonable given the nature of the information.

6.3 The parties only process personal data if and to the extent necessary for the performance of its rights and obligations within the framework of the iSHARE scheme. The processing of personal data shall be in accordance with applicable privacy and data protection law.

ARTICLE 7. LIABILITY

7.1 The liability of the parties shall be in accordance with and determined by the general rules of Dutch law.

7.2 To the extent permitted by law, the Scheme Owner expressly disclaims any and all liability for damages of any kind incurred by any party. However, the Scheme Owner's liability is not limited regarding damages that are the result of deliberate recklessness or wilful misconduct by the Scheme Owner and/or its management.

ARTICLE 8. SETTLEMENT OF DISPUTES

8.1 In the event of disputes between the parties arising from and/or in connection with the performance of operations within the framework of the iSHARE scheme, including disputes regarding compensation for damages, the parties should first endeavour to resolve the disputes by mutual agreement.

8.2 If the dispute cannot be resolved through constructive dialogue between the parties, the parties may submit the dispute for resolution to the Complaints and Disputes Committee <rules not available / discuss iSHARE role or role of external dispute resolution body>. Furthermore, the parties may always submit disputes to the competent civil courts or any other dispute resolution body.

ARTICLE 9. AMENDING THE TERMS OF USE

9.1 The Scheme Owner is entitled to amend or supplement these Terms of Use and its Annexes in accordance with the release management process as described in Annex III.

9.2 Notwithstanding article 10, if an adhering party does not accept an amendment to the Terms of Use, that party's participation in the iSHARE scheme can be terminated on the date on which the amended Terms of Use take effect.

ARTICLE 10. DURATION

10.1 These Terms of Use shall remain in force as long as a party remains registered with the Scheme Owner or for the duration described in the Conditions of Exchange, whichever is longer.

10.2 A party can cancel his registration by terminating the Accession Agreement. Termination is subject to a one month's notice period for adhering parties, and a six months' notice period for certified parties. After giving notice of termination of the Accession Agreement, a certified party shall communicate the termination of its participation in accordance with the withdrawal process described in Annex III.

ARTICLE 11. FINAL PROVISIONS

11.1 These Terms of Use are governed by Dutch law and the parties agree to submit to the courts of [TBD].

11.2 The parties are not authorised to transfer their rights and obligations under the iSHARE scheme to any third party, except with written permission from the Scheme Owner. The parties agree that the Scheme Owner is entitled to transfer its rights and obligations to a third party. The Scheme Owner is entitled, without further permission from a party being required, to transfer its rights and obligations under the iSHARE scheme to any third party. In such case, the parties shall provide their full cooperation as reasonably requested by the Scheme Owner and/or the respective third party.

11.3 The parties have a continuous obligation to keep their registration with the iSHARE scheme up-to-date and to notify the Scheme Owner of any material changes in the corporate structure and/or ownership of its business.

11.4 If any provision of these Terms of Use (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of these Terms of Use, and the validity and enforceability of the other provisions of these Terms of Use shall not be affected. In such an event, the Scheme Owner shall include a suitable replacement provision.

ANNEXES

Annex I: Conditions of Exchange

Annex II: Legal framework

Annex III: Standards and specifications of the iSHARE scheme

5.4.4 Legal context

This section on iSHARE's legal context clarifies which rules and regulations may apply to iSHARE participants, and provides information and formats that participants can use to improve their understanding. This section does not aim to be all-encompassing in the sense that it covers all the rules and regulations applicable to the participants, but it aims to provide useful information to iSHARE's participants. Please note that depending on an organisation's context and specific focus, different rules and regulations might apply, both stemming from national and international law, which might not be mentioned in this section.

5.4.4.1 Relevant rules, regulations and templates

5.4.4.2 Dutch Civil Code

In setting up the iSHARE scheme, the relevant provisions of the Dutch Civil Code need to be taken into account. This primarily relates to the Accession Agreements and the Terms of Use, which need to be drafted in accordance with Dutch contract law. With the expansion of the iSHARE scheme, other national laws may become relevant as well. Any specific (national and international) rules for the transport and logistics sector, such as rules for agreements on the carriage of goods, fall outside the scope of this legal framework. These types of sector specific rules are not relevant for operating and using the iSHARE scheme, although participants may need to adhere to them when contracting services through the scheme.

5.4.4.3 Regulation on Electronic Identification and Trust Services (eIDAS)

The eIDAS Regulation – formally the Regulation on electronic identification and trust services for electronic transactions in the internal market – was adopted on 23 July 2014. It aims is to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities throughout the entire EU. It ensures that people and businesses can use their own eIDs to access public services in other EU countries and enhances cross-border interoperability of electronic trust services.

The first section of the eIDAS Regulation relates to the government-recognized eIDs and establishes a legal framework that will allow all EU countries to recognize each other's eIDs. The second section of eIDAS deals with the various electronic signatures (i.e. simple, advanced and qualified). It clarifies existing rules, but also introduces a new legal framework for electronic signatures, seals and timestamps. The new legal framework is not mandatory but introduces certain requirements that can be followed in order to grant greater legal certainty and to improve the reliability of these services.

Furthermore, the eIDAS Regulation draws a distinction between the parties providing the electronic signatures: qualified and non-qualified trust service providers. The eIDAS Regulation sets forth certain requirements that the qualified trust service providers must adhere to. Furthermore, each EU country is required to 'establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them'.

For the purpose of the iSHARE scheme, the governing body will determine which eID providers are to be used, which trust service providers are to be engaged and the roles these trust service providers have within the iSHARE scheme. The selection of eIDAS and trust service providers is also relevant for the international orientation of the iSHARE scheme and to foster the cross-border interoperability of electronic trust services.

5.4.4.4 Applicable competition law

Agreements

Depending on whether an agreement or other behaviour has an effect in the entire EU or not, EU competition law or national competition law (and enforcement) applies. Competition law prohibits agreements that restrict competition, unless there is a justification for them.

There are different types of agreements with different rules. The rules for agreements between companies at the same level of the production chain are generally stricter than those for companies at different levels of the production chain. The iSHARE scheme facilitates both horizontal and vertical exchanges of information.

What is problematic under competition law, is the exchange of information that is sensitive to competition, such as price lists, data on turnover, etc. Restrictive effects may, for instance, be found in cases where exchanges of information enables companies to be better aware of each other's market strategies. Agreements that have as their purpose or effect the restriction of competition (such as price fixing, market sharing) are very likely to be prohibited. On the other hand, a justification for exchanging information can be found if this leads to efficiency gains. To determine whether there are indeed efficiency gains, three conditions must be taken into account:

1. The efficiency must at least be partially passed on to the consumers which are affected by the restriction (e.g. quicker delivery of products or reduction of search costs).
2. The agreement must not restrict competition more than is necessary for the attainment of the efficiency gains (proportionality requirement).
3. The restriction of competition must not result in the total elimination of competition. As a result, competition law leaves room for such agreements.

The iSHARE scheme could lead to efficiencies (e.g. in terms of costs or by removing barriers).

It is important to carefully draft the agreements and always assess whether they could restrict competition, and whether a restriction could be justified by – for example – efficiencies. Admittedly, it is mainly up to the participants sharing data to comply with competition law, but the iSHARE scheme itself is not designed in a way to directly or indirectly have an adverse effect on competition. In all cases, an important principle of the iSHARE scheme is to create a level playing field.

Dominant position

Competition law also deals with the abuse of a dominant position. Companies can also have a dominant position collectively. Whether there is a dominant position, is assessed on the basis of market shares, amongst other factors. When there is a (collective) dominant position, it is important to assess whether, for example, parties not participating in iSHARE are excluded from the market via abuse of dominance. A dominant position is not in itself anti-competitive. Only when that position is exploited to eliminate competition, it is considered an abuse. Examples of practices that can (but do not necessarily have to) lead to abuse of dominance are exclusive dealing agreements, a refusal to supply, and certain pricing practices.

The iSHARE scheme is intended to be an open framework, accessible to any party – admitted to the iSHARE scheme or not - seeking to use its functionalities

5.4.4.5 General Data Protection Regulation (GDPR)

On the 25th of May 2018, our Dutch privacy law (*Wet bescherming persoonsgegevens*) is set to be overhauled by a European privacy regulation, the 'General Data Protection Regulation' (GDPR). This regulation will ensure that the same privacy rules apply throughout the entire EU and will entail substantial changes for businesses and industry.

Two of those changes are the requirements of 'privacy by design' and 'privacy by default'. Broadly speaking, this means that privacy must be taken into account throughout the entire process in which products and services are developed. This can be achieved by using techniques such as pseudonymisation and by processing as few personal data as possible, i.e. by processing only the necessary personal data. This requirement of necessity also applies to the accessibility of data (i.e. who has access to which data) and the period for which data are retained. The default settings of a product or service must also be as privacy-friendly as possible. Products and services will therefore have to be developed and designed in such a way as to ensure that they are 'privacy proof'.

Personal data must be protected adequately, via technical and organisational measures. For example: passwords, encryption, secure (SSL/TLS) network connections and pseudonymisation of data. Technical norms such as the ISO 27001 are not mandatory, but in practice they are the best way to make sure a service provider uses adequate protection. Service providers who are able to provide a statement from an independent auditor offer even more security. The most well-known statements are the ISAE 3402 and the SSAE No. 16. When you exchange data within the iSHARE scheme and you adhere to the iSHARE technical specifications, this means that you comply with GDPR with respect to the *technical* security measures required for the exchange of personal data.

Although the majority of data shared via the iSHARE scheme may not be personal data, there could be personal data involved. For example, data relating to employees or clients of participating parties. If personal data is shared via the iSHARE scheme, the participating parties will need to have a legal basis to do so. A legal basis can be, for example, consent of the data subjects, or an agreement to which the data subject is a party.

When data is exchanged between two data controllers, both need a legal basis for this. A data exchange agreement then also needs to be concluded. When a data processor processes personal data on behalf of the controller, they are obliged to enter into a data processing agreement. The GDPR explains what such an agreement should contain (also refer to the two available templates provided in this section for a Data Exchange Agreement (see page 202)and Data Processing Agreement (see page 207)).

Within the iSHARE scheme, the participating parties are in control with respect to the types and amount of data they like to share and in this respect should also easily facilitate the conclusion of data processing or data sharing agreements. Consequently, iSHARE includes two model contracts which can facilitate the participants in their GDPR compliance efforts. Depending on the role of the respective parties, they can either use the Data Processing Agreement (see page 207) or the Data Exchange Agreement (see page 202) as a basis for their contractual arrangements. Before using any of these model contracts, it should first and foremost be assessed whether the personal data can actually be lawfully processed or exchanged.

In certain cases, the GDPR requires that the privacy effects of a project are assessed in advance (a Privacy Impact Assessment). This is the case when the processing of personal data constitutes a high risk for the data subjects. For certain companies, for example, companies which monitor individuals or systematically process sensitive data, it will become mandatory to have a Privacy Officer.

GDPR factsheet

What is changing, and what do you need to change?

The General Data Protection Regulation (GDPR) is a new pan-European privacy law. From 25 May 2018, your organisation must comply with this strict new law. So, what is changing? And what do you need to change?

1. Your activities are much more likely to be covered by EU privacy legislation

If your organisation processes personal data of individuals residing in the EU, you must comply with the GDPR. It does not matter whether or not your organisation is established in the EU or if the processing takes place within the EU or not. And if there was any doubt before: the definition of personal data now explicitly includes online identifiers, such as IP addresses or cookie IDs.

2. Some of the legal grounds for processing personal data become more stringent
As with current privacy legislation, the GDPR prescribes that there must be a legal basis for all processing of personal data. Consent provides such a legal basis. Although the legal bases have remained the same, obtaining consent under the GDPR may become significantly harder. The GDPR now clearly states that consent must be given by a statement or a clear affirmative action. Silence, pre-ticked boxes and inactivity do not constitute consent. Other legal bases for the processing of personal data are:

- processing which is necessary for the performance of a contract;
- compliance with legal obligations*;
- protecting the vital interests of individuals;
- the fulfilment of a public interest; and
- a legitimate interest pursued by the controller or a third party, which is not disproportionate to the interest of the individual(s) whom it concerns.

*However, legal obligations are now explicitly narrowed down to compliance with EU law or the laws of a Member State. Consequently, organisations that are subject to non-EU legislation may face challenges in this respect.

3. Your privacy statement must be even more transparent
You must explain clearly and fully, using plain language, how and why you use personal data. Furthermore, you must inform individuals of their enhanced rights, such as the right to view their data, to amend or erase the data if there are clear mistakes, to object to processing, and to transmit their data to another service provider (*right to data portability*). If you create profiles based on individuals' data, you must destroy them upon their request. Finally, you should remember to explicitly mention the right to file a complaint with the supervisory authority.

4. You may need to enable ‘data portability’
If you offer an online service that allows people to store their personal information, they must be able to transmit all their information in structured, commonly used and machine-readable format to another organisation. For instance, this might involve downloading photos, social media posts or forum contributions. This right does, however, not apply where the processing of personal data is based on a legal ground other than consent or a contract, such as the processing of personal data necessary for compliance with a statutory obligation.

5. You must also publish an internal privacy policy
You need to document how personal data is handled and secured within your organisation. Raising awareness of this policy among employees is key. Periodic training will also be required.

6. You must keep records of all personal data processing activities
These records must include, among other things, a description of the personal data being processed, the purposes for which they are processed, and how they are secured. This obligation applies to organisations with more than 250 employees, but also to organisations with fewer than 250 employees if they process personal data on a regular basis or they process special categories of personal data (e.g. biometric data or data concerning an individual’s health).

7. You must document all data breaches internally
Under current privacy legislation, you are required to document only those data breaches that you are obliged to report to the supervisory authority. The GDPR makes it compulsory to document *all* data breaches internally, even those which you are not required to report. If you process personal data on someone else's behalf (a 'controller'), the GDPR also imposes a legal obligation to report all data breaches that occur during such activities to the controller, so that the controller can notify the supervisory authority.

8. You need to know where your personal data is stored, and may need extra safeguards

If you store personal data with a third party in another country, you must check whether the data is stored within or outside the EU. The latter is only permitted if the third party meets strict legal requirements, for instance when the country in question has been certified by the European Commission. With regard to third parties in the United States, the so-called Privacy Shield offers the necessary safeguards. However, please note that customers may demand that their data simply does not leave the EU at all.

9. Your data processing agreements with suppliers and customers must be revised
The GDPR contains more specific requirements for data processing agreements, which must be concluded if you process personal data on behalf of another organisation (a 'controller'), or if another organisation (a 'processor') processes personal data on your behalf. For example, if you process personal data on behalf of a controller, you need permission before subcontracting any of your processing activities.

10. You must carry out a thorough Privacy Impact Assessment (PIA) for activities posing a high risk
A PIA is an extensive assessment intended to identify privacy risks, and to eliminate such risks as much as possible, so that the privacy of individuals is not put in jeopardy beyond what is strictly necessary and proportionate. You may not carry out a processing activity which poses a risk to privacy until after the PIA has been conducted and its outcomes have been implemented.

11. 'Privacy by design' and 'privacy by default'
This means that privacy considerations must be identified and incorporated at every step in the development process. This can be achieved by using techniques such as pseudonymisation and by processing as little personal data as possible, e.g. by processing only the necessary personal data. This requirement of necessity also applies to the accessibility of data (i.e. who has access to which data) and the period for which data is stored. The default settings of a product or service must also be as privacy-friendly as possible. Products and services will therefore have to be developed and designed in such a way as to safeguard that they are 'privacy proof'.

12. Your security measures must be fit for purpose, both now and in the future
The security of personal data is of paramount importance. If you don't restrict access to only those users with a need-to-know, using strong (multi-factor) authentication and encryption, if you don't use TLS, firewalls, anti-virus software, or if you don't patch your software and systems in time, you are at serious risk. You are also at risk if the security measures are not regularly evaluated and updated.

13. You may need to appoint a Data Protection Officer (DPO)
A data protection officer is an independent person advising and reporting on GDPR compliance. Appointing a DPO is compulsory if you are a public body, if you process sensitive personal data (such as medical records) on a large scale, or if you are engaged in regular and systemic monitoring of people's activities on a large scale. The DPO can be appointed either internally or externally.

14. You may need to pay special attention to biometric data
Does your organisation make use of fingerprints or other biometrics, e.g. for access control? Then you need to comply with the GDPR's strict protection regime for biometric data.

15. Fines under the GDPR are drastically higher
Under the GDPR, the supervisory authorities may issue penalties of up to EUR 20 million or 4% of the annual worldwide turnover, whichever is higher. Furthermore, not complying with the GDPR may have a severe impact on your organisation's reputation.

Template Data Exchange Agreement

DATA EXCHANGE AGREEMENT

[THIS DATA EXCHANGE AGREEMENT FORMS AN INTERGRAL PART OF THE AGREEMENT CONCLUDED BETWEEN THE PARTIES ON XX-XX-XXXX]

THE PARTIES:

- **[ORGANISATION, LEGAL ENTITY]**, having its registered office in [ADDRESS], and registered with the Chamber of Commerce under number XXXXXX, legally represented in this matter by XXXXXX, (hereinafter referred to as: '[**COMPANY X**]');

and

- **[ORGANISATION, LEGAL ENTITY]**, having its registered office in [ADDRESS], and registered with the Chamber of Commerce under number XXXXXX, legally represented in this matter by XXXXXX, (hereinafter referred to as: '[**COMPANY Y**]');

hereinafter collectively referred to as '**the Parties**' and individually '**the Party**',

HAVING REGARD TO THE FACT THAT:

- [THE PARTIES / [COMPANY X] / [COMPANY Y]] [IS/ARE] in the possession of various types of data, including Personal Data;
- the Parties shall process the Personal Data under their own responsibility, as they independently determine the purpose and means of the processing of Personal Data and are both individually responsible for having a lawful basis for the processing of Personal Data;
- accordingly, both Parties can be deemed a controller within the meaning of article 1 (d) of the Dutch Data Protection Act (hereinafter referred to as: 'Wbp'), and are not each other's processor within the meaning of article 1(e) of the Wbp;
- the Parties undertake to comply with this data exchange agreement (hereinafter: 'the Data Exchange Agreement') and to abide by the security obligations and all other aspects of the Wbp and the EU Data Protection Regulation (Regulation 2016/679) or all other applicable laws and regulations relating to the processing of Personal Data (together with the Wbp hereinafter collectively referred to as: 'Applicable Data Protection Law');
- the Parties, with a view to the careful processing of Data, wish to make arrangements regarding the exchange of Personal Data within this Data Exchange Agreement;
- where, within the meaning of this Data Exchange Agreement, the Wbp is referred to, from the 25th of May 2018 onwards, the corresponding provisions of the General Data Protection Regulation are meant;

HAVE AGREED AS FOLLOWS:

ARTICLE 1. DEFINITIONS

The terms used in this Data Exchange Agreement shall be understood to mean the following:

1.1 **Annex 1**: the annex to this Data Exchange Agreement, specifying the Dataset.

1.2 **Personal Data**: personal data within the meaning of Article 1 (a) of the Wbp.

1.3 **Dataset**: the Personal Data to be exchanged between the Parties in the form of a dataset, as specified in Annex 1.

ARTICLE 2. OBLIGATIONS OF THE PARTIES

2.1 For the purpose of [SPECIFY PURPOSE], [THE PARTIES / [COMPANY X] / [COMPANY Y]] shall make the Dataset available to [EACH OTHER / [COMPANY X] / [COMPANY Y]] and shall use reasonable endeavours to safeguard the quality of the Dataset.

2.2 The Parties declare to process the Personal Data, as specified in Annex 1, in a proper and careful manner.

2.3 With respect to the processing of Personal Data, each Party is individually responsible for compliance with applicable laws and regulations, including but not limited to Applicable Data Protection Law. In particular, each Party is individually responsible for having a lawful basis to process the Personal Data. Both Parties are individually responsible for the creation of retention periods regarding the Personal Data processed under this Data Exchange Agreement.

2.4 The Parties will only provide each other with the amount of Personal Data necessary to fulfil the purpose referred to in Article 2.1. The Parties shall not use the Personal Data for any other purpose than referred to in Article 2.1.

2.5 The obligations arising under this Data Exchange Agreement apply also to whomsoever processes Personal Data under the respective Party's instructions and/or authority.

2.6 If one of the Parties engages a third party (hereinafter referred to as: 'Sub-Processor') for the processing of Personal Data, this Party shall ensure that the Sub-Processor processes the Personal Data in a proper and careful manner, in accordance with Applicable Data Protection Law and this Data Exchange Agreement. The Party that engages a Sub-Processor, shall in any event ensure that the Sub-Processor will be obliged to agree in writing to obligations no less stricter than the obligations agreed by and between the Parties.

2.7 The Parties shall indemnify each other for any claims and procedures of third parties, including but not limited to supervisory authorities, such as the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), and data subjects, resulting from such Party's breach of Applicable Data Protection Law and/or this Data Exchange Agreement.

2.8 Nothing in this Data Exchange Agreement shall be construed so as to transfer any form of (intellectual) property rights in or to the Data(set) from one Party to the other Party.

ARTICLE 3. DUTY TO REPORT

3.1 In the event of a security breach (a failing or breach of the security of Personal Data) and/or a data breach (a breach on the security of Personal Data that leads to a considerable chance on negative consequences, or has negative consequences, on the protection of Personal Data as referred to in article 34a of the Wbp) with respect to the Personal Data processed in relation to this Data Exchange Agreement, the Parties shall, to the best of their ability, notify the other Party thereof without undue delay, but in any event not later than thirty six (36) hours. The notification obligation applies regardless of the impact of the breach.

3.2 After notification of the breach (as referred to in Article 3.1), the Parties will discuss in good faith what the (potential) consequences of the breach are for either of the Parties, and how each Party should minimise the (potential) damage.

3.2 The Parties are and remain individually responsible for reporting a data breach, occurred during the processing under its own responsibility, to the relevant supervisory authority and/or the affected data subjects.

3.4 The Parties will provide each other with all reasonably necessary assistance (e.g. by providing relevant information), in order to help the other Party in reporting the breach to the relevant supervisory authority and/or the affected data subjects.

ARTICLE 4. SECURITY

4.1 The Parties shall each take adequate technical and organisational measures to protect the Dataset against loss or any form of unlawful processing (such as unauthorised disclosure, deterioration, alteration or disclosure of Personal Data).

4.2 Upon request, the Parties shall provide each other with information about the security measures that have been taken to adequately protect the Dataset.

4.3 None of the Parties shall reverse or circumvent any of the security measures implemented by the other Party.

ARTICLE 5. NONDISCLOSURE AND CONFIDENTIALITY

5.1 All Personal Data exchanged within the framework of this Data Exchange Agreement is subject to a duty of confidentiality vis-à-vis third parties.

5.2 This duty of confidentiality will not apply in the event that the Controller has expressly authorised the furnishing of such Personal Data to third parties, where the furnishing of the Data to third parties is reasonably necessary in view of the nature of the obligations and the implementation of this Data Exchange Agreement, or if there is a legal obligation to make the Personal Data available to a third party.

5.3 If one of the Parties is summoned by a competent court or other authority to submit Personal Data of the other Party for the benefit of a judicial investigation or legal proceedings, it is entitled to do so. However, before submitting the Personal Data, the Party being summoned must inform the other Party as soon as possible about the summons, to provide it with the opportunity to object to the Personal Data being submitted, unless the summons bars it from doing so. Should such Party elect to do so, the other Party must delay the required disclosure to the greatest extent possible by applicable law.

ARTICLE 6. HANDLING REQUESTS FROM DATA SUBJECTS

6.1 Where a data subject submits a request to one of the Parties to exercise one of its legal rights under Applicable Data Protection Law, this Party will independently deal with such request if it falls within the scope of its own processing activities for which the Party concerned is responsible.

6.2 If the request, as referred to in Article 6.1, relates to the processing for which the requested Party is not responsible, then the request must be forwarded to the responsible Party. The data subject may be notified hereof.

6.3 In case it is necessary, the Parties will reasonably assist each other to enable the data subject to exercise its legal rights.

ARTICLE 7. DURATION AND TERMINATION

7.1 This Data Exchange Agreement enters into force upon its signing by both Parties on the date of the last signature.

7.2 This Data Exchange Agreement is entered for the duration of [SPEC IFY DURATION OF THE DATA EXCHANGE AGREEMENT [OR] THE AGREEMENT].

7.3 [SPECIFY NOTICE PERIOD FOR TERMINATION: THIS DATA EXCHANGE AGREEMENT MAY BE TERMINATED BY EITHER PARTY AT ANY TIME UPON SERVING [XX] MONTHS' WRITTEN NOTICE TO THE OTHER PARTY].

7.4 This Data Exchange Agreement may only be amended by the Parties subject to mutual agreement.

ARTICLE 8. MISCELLANEAOUS

8.1 The Data Exchange Agreement and its implementation will be governed by [SPECIFY] law.

8.2 Any dispute arising between the Parties in connection with and/or arising from this Data Exchange Agreement will be referred to the competent court in [SPECIFY].

8.3 The Parties shall provide their full cooperation in amending and adjusting this Data Exchange Agreement in the event of new or amended privacy legislation.

8.4 If any provision of the Data Exchange Agreement should appear void or otherwise unenforceable, this will not affect the validity of the Data Exchange Agreement as a whole. The Parties shall in that event agree a new provision or new provisions, by which the intention of the original provision(s) is as much as possible reflected.

IN WITNESS WHEREOF, the Parties have caused this Data Exchange Agreement to be executed by their duly authorized representatives:

[COMPANY X]	**[COMPANY Y]**
_____/_____/_____	_____/_____/_____
Date	*Date*
_____	_____
Name	*Name*
_____	_____
Signature	*Signature*

ANNEX 1: DATASET

[SPECIFY (PERSONAL) DATA TO BE EXCHANGED BETWEEN THE PARTIES]

Template Data Processing Agreement

DATA PROCESSING AGREEMENT

THE PARTIES:

- **[ORGANISATION, LEGAL ENTITY DATA CONTROLLER]**, having its registered office in [ADDRESS], and registered with the Chamber of Commerce under number XXXXXX, legally represented in this matter by XXXXXX, (hereinafter referred to as: '**the Controller**');

and

- **[ORGANISATION, LEGAL ENTITY DATA PROCESSOR]**, having its registered office in [ADDRESS], and registered with the Chamber of Commerce under number XXXXXX, legally represented in this matter by XXXXXX, (hereinafter referred to as: '**the Processor**');

hereinafter collectively referred to as '**the Parties**' and individually '**the Party**',

HAVING REGARD TO THE FACT THAT:

- the Controller has access to the personal data of various individuals (hereinafter referred to as: 'Data subjects');
- the Controller wants the Processor to execute certain types of processing in accordance with the agreement concluded with the Processor on XX-XX-XX (hereinafter referred to as: 'the Agreement'), in order to provide [CLEARLY SPECIFY THE SERVICES TO BE PROVIDED BY THE PROCESSOR];
- the Controller has determined the purpose of and the means for the processing of personal data as governed by the terms and conditions referred to herein;
- the Processor undertakes to comply with this data processing agreement (hereinafter: 'the Data Processing Agreement') and to abide by the security obligations and all other aspects of the Dutch Personal Data Protection Act (hereinafter referred to as: 'Wbp') and the EU Data Protection Regulation (Regulation 2016/679) or all other applicable laws and regulations relating to the processing of personal data (together with the Wbp hereinafter collectively referred to as: 'Applicable Data Protection Law');
- this Data Processing Agreement forms an integral part of the Agreement;
- the Controller is hereby deemed to be the responsible party within the meaning of Article 1 (d) of the Wbp;
- the Processor is hereby deemed to be the processor within the meaning of Article 1 (e) of the Wbp;
- where, within the meaning of this Data Processing Agreement, the Wbp is referred to, from the 25th of May 2018 onwards, the corresponding provisions of the General Data Protection Regulation are meant;
- as of 25 May 2018, the Controller and the Processor shall maintain a record of their processing activities under this Data Processing Agreement in accordance with the General Data Protection Regulation;
- the Parties, having regard to the provisions of Article 14 (5) of the Wbp, wish to lay down their rights and duties in writing in this Data Processing Agreement;

HAVE AGREED AS FOLLOWS:

ARTICLE 1. PROCESSING OBJECTIVES

1.1 The Processor undertakes to process personal data on behalf of the Controller in accordance with the conditions set forth in this Data Processing Agreement. The processing will be executed exclusively within the framework of the Agreement, and for all such purposes as may be agreed to by and between the Parties.

1.2 The personal data processed by the Processor, and the categories of Data subjects to whom the personal data relates, are specified in Annex 1.

1.3 When carrying out the processing activities, the Processor shall act only on the instructions from the Controller and for the purposes authorised by the Controller.

1.4 The Processor shall take no unilateral decisions regarding the processing of the personal data for other purposes, including decisions regarding the provision thereof to third parties and the storage duration of the personal data. Within the framework of this Data Processing Agreement or other agreements between the Parties, it is the Controller who shall have the say in regard to the personal data furnished to the Processor and in regard to the data processed by the Processor within that framework.

1.5 All rights attached to the personal data processed on behalf of the Controller shall remain with the Controller and/or the relevant Data subjects.

ARTICLE 2. PROCESSOR'S OBLIGATIONS

2.1 The Processor shall furnish the Controller immediately on request with details regarding the measures it has adopted to comply with its obligations under this Data Processing Agreement and Applicable Data Protection Law.

2.2 The Processor's obligations arising under the terms of this Data Processing Agreement apply also to whomsoever processes personal data under the Processor's instructions.

ARTICLE 3. TRANSMISSION OF PERSONAL DATA

3.1 The Processor may process the personal data in countries within the European Union. The transmission to countries outside the European Union shall at all times be subject to prior written approval of the Controller.

3.2 The Processor shall notify the Controller as to which country or countries the personal data will be processed in.

3.3 Any transfer of personal data outside the European Union to the Processor or any third party (hereinafter referred to as: 'Sub-Processors') in a non-adequate country shall be governed by the terms of the standard contractual clauses of the European Commission.

ARTICLE 4. ALLOCATION OF RESPONSIBILITY

4.1 The Processor shall be responsible for processing the personal data under this Data Processing Agreement in accordance with the Controller's instructions, irrespective of statutory obligations.

4.2 The Processor is explicitly not responsible for other processing of personal data, including but not limited to, the collection of personal data by the Controller, processing for purposes that are not reported by the Controller to the Processor and processing by third parties other than the Sub-Processors under this Data Processing Agreement.

ARTICLE 5. ENGAGING OF SUB-PROCESSORS

5.1 The Processor is authorised within the framework of the Agreement to engage Sub-Processors. The Processor shall inform the Controller about any intended changes concerning the addition or replacement of Sub-Processors.

5.2 The Controller has the right to object against any Sub-Processors engaged by the Processor. In case of objection by the Controller, the Parties hereby agree to resolve this matter in good faith.

5.3 The Processor shall in any event ensure that the Sub-Processors will be obliged to agree in writing to substantially similar duties that are agreed by and between the Parties.

ARTICLE 6. DUTY TO REPORT

6.1 In the event of a security breach (a failing or breach of the security of personal data) and/or a data breach (a breach on the security of personal data that leads to a considerable chance on negative consequences, or has negative consequences, on the protection of personal data as referred to in article 34a of the Wbp), the Processor shall, to the best of its ability, notify the Controller thereof without undue delay, but in any event not later than thirty six (36) hours, after which the Controller shall determine whether or not to inform the relevant supervisory authority and/or the Data subjects. The Controller is responsible for fulfilment of any statutory notification obligations. The Processor shall promptly take adequate remedial measures.

6.2 If required by law and/or legislation, the Processor shall fully cooperate in notifying the relevant Data subjects and/or the relevant supervisory authority.

6.3 The duty of the Processor to report a breach includes, in any event, the duty to report the fact that a breach has occurred and, as far as known by the Processor, the following details:

- information about the first point of contact regarding the notification;
- the date at which the breach has occurred (the period in which the breach occurred suffices in case the Processor is unable to determine the exact date at which the breach occurred);
- the (suspected) cause of the breach;
- the (currently known and or anticipated) consequences thereof;
- the number of Data subjects who are or may be affected by the breach (a minimum and maximum number of affected Data subjects suffices in case the exact number cannot be determined);
- a description of the group of Data subjects who are or may be affected by the data breach, including the type of personal data which has been breached;
- whether the personal data has been encrypted, hashed or in any manner has been made incomprehensible or inaccessible to unauthorized individuals;
- the proposed and or implemented remedial actions to end the breach and to limit its consequences.

ARTICLE 7. SECURITY

7.1 The Processor shall implement appropriate technical and organisational measures with regards to the processing of personal data in order to safeguard a level of security appropriate to the risk, in accordance with the Wbp and from 25 May 2018 onwards, in accordance with the General Data Protection Regulation, in particular from loss or any form of unlawful processing such as accidental or unlawful destruction or unauthorised disclosure or access, deterioration, alteration of personal data and against all other forms of unlawful processing, including, but not limited to, unnecessary collection or further processing in connection with the performance of processing personal data under this Data Processing Agreement.

7.2 Documentation regarding the implemented security measures shall be available upon the Controller's request.

ARTICLE 8. HANDLING REQUESTS FROM DATA SUBJECTS

8.1 Where a Data subject submits a request to the Processor to exercise one of its legal rights, the Processor shall deal with this request if it relates to processing that pertains to the Processor's own processing activities. In all other cases, the Processor will forward the request to the Controller and the request will then be dealt with by the Controller. The Processor may notify the Data subject hereof.

8.2 Where a Data subject submits an inspection request to the Controller, the Processor shall cooperate where requested by the Controller in so far as is possible and reasonable.

ARTICLE 9. NONDISCLOSURE AND CONFIDENTIALITY

9.1 All personal data received by the Processor from the Controller and/or compiled by the Processor within the framework of this Data Processing Agreement is subject to a duty of confidentiality vis-à-vis third parties. The Processor shall refrain from using this information for any purpose other than that for which it was furnished, even where made available in a manner that is not traceable to the Data subjects.

9.2 This duty of confidentiality will not apply in the event that the Controller has expressly authorised the furnishing of such information to third parties, where the furnishing of the information to third parties is reasonably necessary in view of the nature of the instructions and the implementation of this Data Processing Agreement, or if there is a legal obligation to make the information available to a third party.

ARTICLE 10. AUDIT AND COMPLIANCE

10.1 To confirm compliance with this Data Processing Agreement, the Controller has the possibility to conduct an audit by assigning an independent third party who shall be obliged to observe confidentiality of the Processor in this regard. The costs of the audit shall be borne by the Controller.

10.2 The audit may only be undertaken when there are specific grounds for suspecting the misuse of personal data, and no earlier than two (2) weeks after the Controller has provided written notice to the Processor. Furthermore, any such audit will follow the Processor's reasonable security requirements, and will not interfere unreasonably with the Processor's business activities.

10.3 The findings in respect of the audit will be discussed and evaluated by the Parties and, where applicable, implemented by one of the Parties or by both Parties jointly.

10.4 In case the Controller initiates a data protection impact assessment, the Processor shall reasonably assist the Controller in fulfilling this data protection impact assessment, by inter alia providing the required and available information to the Controller.

ARTICLE 11. DURATION AND TERMINATION

11.1 This Data Processing Agreement is entered into for the duration set out in the Agreement, and in the absence thereof, for the duration that personal data of the Controller are being processed by the Processor.

11.2 The Data Processing Agreement may not be terminated in the interim.

11.3 This Data Processing Agreement may only be amended by the Parties subject to mutual consent.

11.4 The Parties shall provide their full cooperation in amending and adjusting this Data Processing Agreement in the event of new privacy legislation.

11.5 Upon termination of the Data Processing Agreement, the Processor shall, at the request of the Controller, return the personal data to the Controller and/or shall securely destroy such personal data, except to the extent the Data Processing Agreement, the Agreement or applicable law provides otherwise.

ARTICLE 12. APPLICABLE LAW ANDDISPUTE RESOLUTION

12.1 The Data Processing Agreement and its implementation will be governed by [SPECIFY] law.

12.2 Any dispute arising between the Parties in connection with and/or arising from this Data Processing Agreement will be referred to the competent court in [SPECIFY].

12.3 If any provision of the Data Processing Agreement should appear void or otherwise unenforceable, this will not affect the validity of the Data Processing Agreement as a whole. The Parties shall in that event agree a new provision or new provisions, by which the intention of the original provision(s) is as much as possible reflected.

IN WITNESS WHEREOF, the Parties have caused this Data Processing Agreement to be executed by their duly authorized representatives:

The Controller	**The Processor**
_____/_____/_____	_____/_____/_____
Date	*Date*
_____	_____
Name	*Name*
_____	_____
Signature	*Signature*

ANNEX 1: PERSONAL DATA AND DATA SUBJECTS

PERSONAL DATA

Within the framework of the Agreement, the Processor will process the following categories of personal data:

- [SPECIFY]

CATEGORIES OF DATA SUBJECTS

The categories of Data subjects to whom the personal data relate are:

- [SPECIFY]

6 Glossary and legal notices

This section includes the iSHARE glossary and legal notices. It is presented as follows:

6.1 Glossary

DISCLAIMER: all descriptions are definitions written by iSHARE, unless specified otherwise

- Responsibility (see page 223)
- REST(ful) (see page 223)
- Scheme (see page 223)
- Scheme Owner (role) (see page 223)
- Service Consumer (role) (see page 224)
- Service Provider (role) (see page 224)
- Service provision (see page 224)
- Signing (see page 224)
- Status Code / Response Code (see page 224)
- TLS (see page 225)
- Token (see page 225)

6.1.1 ABAC

ABAC (Attribute-Based Access Control) is assigning authorisations based on attributes (contextual pieces of information that are relevant to an access decision, such as device type, RBAC (see page 222) role, time, location, or CRUD (see page 217) level). The attributes can be associated with all entities that are involved with certain actions, such as the subject, the object, the action itself and the context (e.g. time, location). The attributes are compared with policies to decide which actions are allowed in which context, granting access based on the policy outcomes.

6.1.2 Accountability

There is a clear distinction between accountability and responsibility (see page 223).

Accountability can be described as being liable or answerable for the completion of a certain task. Someone or something who is accountable oversees and manages the stakeholder(s) who are responsible for performing the work effort. In order to be effective, accountability should lie with a sole entity or role.

Responsibility may be delegated, but accountability cannot.

6.1.3 Adherence (iSHARE)

An **iSHARE adhering party** adheres to the iSHARE terms of use (see page 193). An iSHARE adhering party MUST sign an Accession Agreement with the Scheme Owner (see page 223).

6.1.4 API

An API (Application Programming Interface) is a technical interface, consisting of a set of protocols and data structuring standards ('API specifications') which enables computer systems to directly communicate with each other. Data or services can be directly requested from a server by adhering to the protocols. APIs are used to hide the full complexity of software and make it easy for third parties to use parts of software or data services. APIs are mainly meant for developers to make the creation of new applications depending on other applications easier.

6.1.5 Authentication

Authentication is the process of determining or validating whether someone or something is, in fact, who or what it is claming to be. There are several means of authenticating the identity of an entity, which can be used alone or in combination:

- Something the entity knows – examples includes a password, PIN, passphrase, or answer to a secret question;
- Something the entity possesses – examples include electronic keycard, smartcard, token, and smartphone;
- Something the entity is (biometrics) – examples include recognition by fingerprint, retina, iris, and face;
- Something the entity does (behavioral dynamics) – examples include recognition by voice pattern, swipe characteristics, handwriting characteristics, and typing rhythm;
- Something about the context of the entity – examples include IP address, device type, geolocation, and time of day.

6.1.6 Authenticity

In the context of information security, **authenticity** refers to the truthfulness of information and if this has been sent or created by an authentic sender.

Authenticity can be achieved by digitally signing (see page 224) a message with the private key from the sender. The recipient can verify the digital signature with the matching public key. Public keys are issued by a Certificate Authority (see page 216).

6.1.7 Authorisation

Authorisation is the process of giving someone or something permission to something, for example to access to services, data or other functionalities. Authorisation is enabled by authentication (see page 215). Policies and attributes determine what types of activitivities are permitted by an entity.

6.1.8 Authorisation Registry (role)

The **Authorisation Registry**:

- Manages records of delegations (see page 217) and authorisations (see page 215) of Entitled Parties (see page 218) and/or Service Consumers (see page 224);
- Checks on the basis of the registered permission(s) whether a Human (see page 219) or Machine (see page 220) Service Consumer is authorised to take delivery of the requested service, and;
- Confirms the established powers towards the Service Provider (see page 224).

Within the iSHARE scheme, the term Authorisation Registry always refers to an external Authorisation Registry (not part of the Service Provider (see page 224) or Entitled Party (see page 218)).

The Authorisation Registry is a role for which iSHARE certification (see page 216) is REQUIRED.

6.1.9 Caching

Web servers can temporarily store data in order to enable faster access to this data at a later moment, this is called 'caching'.

6.1.10 Certificate Authority

A **Certificate Authority (CA)** is:

- An entity that issues digital certificates;
- A trusted party, and;
- Responsible for the binding to a specific entity of the certificate (registration & issuance).

A digital certificate certifies the ownership of a public key by the named subject of the certificate, so other parties can rely upon signatures or assertions made with the private key that corresponds to the certified public key.

A **Registration Authority** verifies the identity of entities requesting digital certificates to be issued by the CA and validates the correctness of the registration.

A **Validation Authority** verifies the validity of digital certificates on behalf of the CA.

6.1.11 Certification (iSHARE)

Roles for which certification is required facilitate certain functions for the iSHARE scheme that every party within iSHARE must able to rely upon. An **iSHARE certified party** MUST apply to the Scheme Owner (see page 223) for certification and, after providing sufficient proof, MUST sign a certification agreement with the Scheme Owner (see page 223).

6.1.12 Confidentiality

In the context of information security, **confidentiality** refers to the protection of information from disclosure to unauthorised parties.

Confidentiality can be achieved by the use of cryptography, as well as access control; the message the recipient gets can be proven not to have been read by anyone else but the legitimate sender and recipient.

6.1.13 Credentials

In the context of information security, **credentials** are used to control access of someone or something to something, for example to services, data or other functionalities. The right credentials validate (i.e. authenticate (see page 215)) the identity claimed during identification (see page 219).

The best-known example of credentials is a password, but other forms include electronic keycards, biometrics and, for machines, public key certificates.

6.1.14 CRUD

CRUD (acronym for Create, Read, Update, Delete) are considered to be basic functions regarding stored data. In computer programming, possible actions are often mapped to these standard CRUD functions in order to clarify the actions. For example, standard HTTP (see page 218) actions GET and POST refer to Read and Create functions regarding stored data.

6.1.15 Data classification

The **classification of data** in categories is an important pre-requisite for proper authorisation (see page 215). Data can be classified in categories defining their type, location, sensitivity and protection level.

Clustering data in categories does not only simplify the authorisation process (i.e. giving someone or something permission to data), it also provides a clear overview and lowers the risk of exchanging sensitive data with unauthorised entities. A risk analysis is part of the data classification process.

6.1.16 Data exchange

Data exchange is the process of supplying data and receiving (an)other (set of) data in return.

6.1.17 Data Owner

The **Data owner** is the legal person accountable (see page 214) for the confidentiality (see page 216), integrity (see page 220), availability (see page 182) and accurate reporting of data.

The Data Owner can be the Service Provider (see page 224). In this case, he is not only accountable for the availability of data, but also responsible (see page 223).

6.1.18 Delegation

Delegation is the act of empowering someone or something to act for another or to represent other(s).

In the iSHARE network, a delegated Service Consumer (see page 224) acts on behalf of an Entitled Party (see page 218).

6.1.19 Encryption

Encryption is the process of converting data from plaintext to ciphertext. Plaintext (also called cleartext) represents data in its original (readable) format, whereas ciphertext (also called cryptogram) represents data in encrypted (unreadable) format.

Decryption is the process of converting data from ciphertext to plaintext.

The algorithm represents the mathematical or non-mathematical function used in the encryption and decryption process.

A cryptographic key represents the input that controls the operation of the cryptographic algorithm. With symmetric encryption the same key is use for encryption and decryption, whereas with asymmetric encryption two different, but mathematically related keys are used for either encryption or decryption, a so-called public key and a private key.

A crypto system represents the entire cryptographic environment, including hardware, software, keys, algorithms and procedures.

6.1.20 Entitled Party (role)

The **Entitled Party** is the legal entity that has one or more rights to something, e.g. to data at a Service Provider (see page 224) that it has a legal agreement with. The Entitled Party is either the same entity as the Service Consumer (see page 224), or delegates its rights to another Service Consumer. In the latter case, this other Service Consumer('s machines and humans) can consume services on the Entitled Party's behalf.

The Entitled Party is a role for which iSHARE adherence (see page 214) is REQUIRED.

6.1.21 EORI

An **EORI (Economic Operator Registration and Identification)** is an identification number, unique throughout the European Community, assigned by a customs authority or designated authority in a Member State to economic operators and other persons, and valid throughout the Community.

The format of the EORI number consists of a country code followed by a unique code which is established within an EU member state. For example, in the Netherlands the EORI consists of: NL, followed by an RSIN (*Rechtspersonen en Samenwerkingsverbanden Identificatie* number. If the NL-RSIN combination contains less than 9 digits, the EORI is prefixed with 0's.

In the iSHARE network, the EORI number is used to uniquely identify legal persons. Note that non-European Community legal persons doing business in/with Europe also have an EORI.

> **Source**
>
> EORI.eu[74]

6.1.22 HTTP(S)

HTTP stands for 'Hypertext Transfer Protocol', and when secured via TLS (see page 225) or SSL it is referred to as HTTPS (HTTP Secure). It is a protocol for (secure) communication over a computer network and is widely used on the Internet.

---

74 http://www.eori.eu/eori-general-information/

6.1.23 Human Service Consumer (role)

The **Human Service Consumer** is a role that represents a human (person) who requests, receives, and uses certain services, such as data, from a Service Provider (see page 224) on behalf of and authorised by the Service Consumer (see page 224).

The Human Service Consumer is not a separate role, but belongs to the adhering party Service Consumer.

6.1.24 Identification

Identification is the process of someone or something claiming an identity by presenting characteristics called identity attributes. Such attributes include a name, user name, e-mail address, etc. The claimed identity can be validated (i.e. authenticated (see page 215)) with the right credentials[75].

6.1.25 Identity Broker (role)

If multiple distinct Service Providers (see page 224) exist where each data set is protected under a distinct trust domain, multiple Identity Providers (see page 219) may be needed. Moreover, the iSHARE scheme may require different levels of assurance (see page 220) for specific data and may wish to designate specific Identity Providers for specific services.

In order to support multiple Identity Providers (with possible multiple rules) and Service Providers, an **Identity Broker** is required. An Identity Broker allows Human Service Consumers (see page 219) to select the Identity Provider they prefer to authenticate (see page 215) themselves at. It prevents the need for a direct relationship between all Service Providers and all Identity Providers.

The Identity Broker is a role for which iSHARE certification (see page 216) is REQUIRED.

6.1.26 Identity Provider (role)

The **Identity Provider**:

- Provides identifiers for Human Service Consumers (see page 0);
- Issues credentials to Human Service Consumers;
- Asserts to the system that such an identifier presented by a user is known to the Identity Provider, and;
- Possibly provides other information (which are frequently referred to as attributes) about the user that is known to the Identity Provider.

In the iSHARE environment an Identity Provider could support various methods of authentication (see page 215), such as:

- Password authentication;
- Hardware-based authentication (smartcard, token);
- Biometric authentication;
- Attribute-based authentication.

Depending on parameters such as the quality of the registration process, quality of credentials, use of biometrics or multiple authentication factors and information security, an Identity Provider can provide a client with a high or

75 https://innopay.atlassian.net/wiki/spaces/IS/pages/53840953/Credentials

low confidence in the claimed identity of the user which is known to the Identity Provider. This is also known as the Level of assurance (LoA) (see page 220).

The Identity Provider is a role for which iSHARE certification (see page 216) is REQUIRED.

6.1.27 Integrity

In the context of information security, **integrity** refers to the protection of information from being modified by unauthorised parties.

Integrity can be achieved by a.o. hash functions (hashing the received data and comparing it with the hash of the original message); the message the recipient receives from the sender can be proven not to have been changed during the transmission.

6.1.28 JSON

JSON is short for 'JavaScript Object Notation' and is an open standard data format that does not depend on a specific programming language. This compact data format makes use of human-readable (easy to read) text to exchange data objects (structured data) between applications and for data storage.

JSON is most commonly used for asynchronous communication between browsers and servers.

6.1.29 JWT

A JSON Web Token (JWT) is used when non-repudiation (see page 221) between parties is required. A statement, of which the data is encoded in JSON (see page 220), is digitally signed (see page 224) to protect the authenticity (see page 215) and integrity (see page 220) of the statement.

6.1.30 Levels of Assurance (LoA)

Within online authentication (see page 215), depending on the authentication protocol used, the server is to some extend assured of the client's identity. Depending on parameters such as the quality of the registration process, quality of credentials, use of biometrics or multiple authentication factors and information security, an authentication protocol can provide a server with a high or low confidence in the claimed identity of the client. For low-interest products, a low certainty might be sufficient, while for sensitive data it is essential that a server is confident that the client's claimed identity is valid.

6.1.31 Machine Service Consumer (role)

The **Machine Service Consumer** is a role that represents a machine that requests, receives, and uses certain services, such as data, from a Service Provider (see page 224) on behalf of and authorised by the Service Consumer (see page 224).

The Machine Service Consumer is not a separate role, but it belongs to the adhering party Service Consumer (see page 224).

6.1.32 Non-repudiation

In the context of information security, **non-repudiation** (Dutch 'onweerlegbaarheid') refers to the fact that the sending (or broadcast) and receipt of the message cannot be denied by either of the involved parties (sender and recipient).

Non-repudiation is closely related to authenticity (see page 215) and can be achieved by digital signatures (see page 224) in combination with message tracking.

6.1.33 OAuth

OAuth is an open standard for authorisation (see page 215) which is used by i.e. Google, Facebook, Microsoft, Twitter etc. to let their users exchange information about their accounts with other applications or websites. OAuth is designed to work with HTTP (see page 218). Within iSHARE, a modified version of OAuth 2.0 is used.

Through OAuth users can authorise third party applications or websites to access their account information on other 'master' systems without the need of exchanging with them their credentials (see page 216) to login onto the platform. OAuth provides a 'secure delegated access' to resources (email accounts, pictures accounts, etc.) on behalf of the resource owner.

It specifies a method for resource owners to authorise third parties access to their resources without exchanging their credentials (username, password). Authorisation servers (of the platform) issue access tokens to third party clients (applications or websites) with the approval of the resource owner (= end user). The third party client needs the access token to get access to the resources that are stored on the resource server (of the master system).

6.1.34 OIN

The OIN format is used to uniquely identify organisations. OIN stands for Organization Identifying Number. An OIN consists of the following concatenated elements:

- An 8-digit prefix that tells the register where the number is defined (e.g. Chamber of Commerce, RSIN etc.)
- A number whose value depends on the register

6.1.35 OpenID Connect

OpenID Connect (OIDC) is the authentication layer that is built on top of OAuth (see page 221) 2.0 protocol which is an authorisation framework. The OIDC authentication layer allows clients to verify the ID and obtain basic profile information of their end-users

The authentication is performed by the authorisation server (managing the access rights and conditions) in an interoperable and REST (see page 223)-like manner. Within iSHARE, OpenID Connect 1.0 is used.

6.1.36 PDP

Policy Decision Point. Entity that evaluates access requests that are received from the policy enforcement point (PEP (see page 222)). Subsequently an answer is sent back to the PEP.

6.1.37 PEP

Policy Enforcement Point. Entity that determines whether an action is permitted or not. It takes any access requests and forwards these to the policy decision point (PDP (see page 221)).

6.1.38 PIP

Policy Information Point. Entity that holds policy information and is contacted as a source of information regarding delegation (see page 217)/authorisation (see page 215) information.

6.1.39 PKI (Public Key Infrastructure)

A PKI is a system for distribution and management of digital keys and certificates, which enables secure authentication of parties interacting with each other.

Generally, three different methods exist for creating trust within PKI's. These are through 'Certificate Authorities', 'Web of Trust' and 'Simple PKI'. Within iSHARE the 'Certificate Authority' approach is used, and as such the other methods will not be discussed.

A PKI can be considered as a chain of certificates. At the beginning of the chain is the root 'Certificate Authority (see page 0)' (CA), a public trusted party which is allowed to digitally sign (see page 224) their own certificates (SSC, self-signed certificate). This 'Root (see page 222) CA' distributes certificates and encryption keys to organisations. The certificate is signed by the 'root CA' as proof that the owner of the certificate is trusted. These organisations can start distributing certificates as well, if allowed by their root. They become CA's, and as such sign the certificates that they distribute. Repeating these steps, a chain of certificates is created, with each certificate signed by the CA who distributed the certificate.

Parties need to trust a certificate for authentication (see page 215) purposes. Instead of trusting individual certificates of organisations, root certificates can be trusted. By trusting a root, all certificates that have the root within their PKI chains are automatically trusted. Most large root CA's are automatically trusted within web browsers, enabling computers to safely interact with most web servers.

6.1.40 PKI Root

A PKI root is another term for root certificate, and stands for an unsigned or self-signed public key certificate that identifies the Certificate Authority[76], the party who is trusted by all members in the trust framework. The most common type of PKI certificates are based on the X.509[77] standard and normally include the digital signature of the Certificate Authority. The certificate authority issues digital certificates to all members in the trust framework.

6.1.41 RBAC

Role-Based Access Control. Assigning authorisations through business roles. An RBAC role represents a set of tasks or activities translated into authorisations, reflecting one or more of the following:

76 https://innopay.atlassian.net/wiki/spaces/IS/pages/49741971/Certificate+Authority
77 https://innopay.atlassian.net/wiki/spaces/IS/pages/49742119/X.509

- Organisational structure
- Business processes
- Policies (rules)

RBAC authorisations can either give access to the front door of the information system or can be translated to access rights within the information system (often through application roles or groups).

6.1.42 Responsibility

There is a clear distinction between responsibility and accountability (see page 214).

Responsibility can be described as tasked with getting the job done. Someone or something who is responsible performs the actual work effort to meet a stated objective.

Responsibility may be delegated, but accountability cannot.

6.1.43 REST(ful)

REST stands for 'Representational State Transfer' and is an architectural style for building systems and services, systems adhering to this architectural style are commonly referred to as 'RESTful systems'. REST itself is not a formal standard, but it is an architecture that applies various common technical standards such as HTTP (see page 0), JSON (see page 220) and URI.

A RESTful API (see page 214) indicates that the API architecture follows REST 'constraints'. Constraints restrict the way that servers respond and process client requests, in order to preserve the design goals which are intended by applying REST. Goals of REST are, among others, performance and scalability. Both are of utmost importance in iSHARE.

6.1.44 Scheme

A **scheme** can be defined as a collaborative effort to establish and maintain a set of agreements, to achieve a common goal.

iSHARE is a scheme with common goals (see page 9). Other schemes include credit card schemes such as MasterCard and Visa, payment scheme iDEAL and identity scheme eHerkenning.

6.1.45 Scheme Owner (role)

The **Scheme Owner** represents the body that governs the iSHARE scheme and its participants. The Operational working Group is currently drafting the processes which the Scheme Owner will administer.

As part of the secondary use cases (see page 91), parties will need to register themselves as certified or adhering[78] at the Scheme Owner. They will also need to consult the Scheme Owner to check whether their counterparty is adherent or certified, and whether a counterparty's certificate is valid.

---

78 https://innopay.atlassian.net/wiki/spaces/IS/pages/54171042/Adherence%2C+certification+and+compatibility

6.1.46 Service Consumer (role)

The **Service Consumer** is the legal entity that consumes the Service Provider (see page 224)'s service on the basis of the Entitled Party (see page 218)'s rights to that service. It can do so because the Service Consumer is either the same legal entity as the Entitled Party (i.e. it already has these rights), or because the Entitled Party has delegated rights to the Service Consumer

The Service Consumer does not interact with the Service Provider; it authorises (and uses) a Machine Service Consumer (see page 220) or Human Service Consumer (see page 219) to do so.

The Service Consumer is a role for which iSHARE adherence (see page 214) is REQUIRED.

6.1.47 Service Provider (role)

The **Service Provider** is a role that provides certain services, such as data, to a Service Consumer (see page 224). In case the service pertains to data provisioning, the Service Provider is either the Data Owner (see page 217), or has explicit consent of the Data Owner to provide the services.

The Service Provider is responsible (see page 223) for the availability of services, and accountable (see page 214) for these services if it also the Data Owner.

The Service Provider is a role for which iSHARE adherence (see page 214) is REQUIRED.

6.1.48 Service provision

Service provision is the act of providing or supplying something for consumption or use. One of the most common forms of service provision is the exchange of data (see page 217).

6.1.49 Signing

Signing is the process of encrypting (see page 217) data (message, document, transaction) with the private key of the sender. It enables a receiver to confirm the authenticity (see page 215) of the data. Signing also provides for non-repudiation (see page 221), so that it is ensured that a sender cannot deny having sent a message.

In most cases, a hash of the data is encrypted. Thus, both the integrity (see page 220) and the authenticity (see page 215) of the data can be verified. Confirmation takes place by the receiver using the public key of the sender. The public key is contained in the digital certificate that is sent by the sender along with the signed data. The association of the key pair with the sender MUST be assured by a Certificate Authority (see page 0).

6.1.50 Status Code / Response Code

After sending a HTTP (see page 218) request to a server, the server responds with (among others) a Status Code which indicates the outcome of the request made to the server. A well known response is 404 Not found, indicating that the requested location or resource is not (yet) found.

6.1.51 TLS

TLS (Transport Layer Security) is a set of protocols that provides for secure communication in computer networks. TLS makes use of cryptography and is widely used by a variety of applications such as web browsing, email and voice-over-IP. Securing HTTP (see page 218) communication via (among others) TLS results in the HTTPS (see page 218) protocol. Securing communication with TLS v1.2 is mandatory for all iSHARE communication.

6.1.52 Token

Something that serves as a verifiable representation of some fact, e.g. an identity or entitlement.

Within iSHARE, Tokens are issued after successfully completing API (see page 214) requests which are then used to process the next request. For example, to access a certain service, first an access token is required. Upon receiving this access token, it can be used to request the service itself.

6.2 Legal notices

7 Project history

7.1 Background information

The project to establish the iSHARE scheme was initiated by the Neutral Logistics Information Platform (NLIP), as part of the government programme 'Topsector Logistiek[79]', through a tender project in 2016. NLIP requested market parties to present plans to lower barriers for more efficient data exchange in the Dutch logistics sector. The combination of the parties INNOPAY and Maxcode won the tender, with its plan to set-up a scheme of multilateral agreements instead of, for instance, a technology-centric approach relying on a software platform. Since June 2016, the iSHARE project team facilitated the realisation of a scheme which is scheduled to go live in the course of 2018.

The establishment of the iSHARE scheme was set out in four phases:

- Phase 1 (Jun 2016 - Jan 2017): Preparatory phase, in which organisations were openly invited to participate in the initiative and which resulted in the so called 'startdocument v0.1'. Startdocument v0.1 provided the preliminary scope for the iSHARE scheme based on identified challenges and use cases of involved organisations;
- Phase 2 (Part I: Jan 2017 - Jun 2017; part II: Jul 2017 - Dec 2017): Co-creation phase, in which participating organisations worked collaboratively towards iSHARE scheme v1.0 (and later versions 1.2 and 1.5) which contains the first full set of agreements for improved data exchanging conditions. Participating organisations worked in four working groups to produce the first full version of the iSHARE scheme: the Functional, Technical, Operational and Legal working groups. Participating organisations realised Proofs of Concept to verify the correct functional and technical workings of the iSHARE scheme;
- Phase 3 (Jan 2018 - Jun 2018): Soft launch phase, in which the involved organisations organise how the iSHARE scheme's integrity and sustainability are kept in check. This involves establishing/designating an organisation entrusted with the responsibility to safeguard the integrity of the iSHARE scheme;
- Phase 4 (Jul 2018 and onwards): iSHARE live; iSHARE opens up to any party interested and willing to abide by the agreements as set out by involved organisations.

7.1.1 Zooming in on Phase 2: Co-creation

iSHARE v1.5 was established through collaboration between its participating organisations. By going through a co-creation process, the collective expertise of all participants led to a practical and widely applicable scheme. This thinking is fuelled by the belief that a practical solution is the result of dialogue and deliberation: participants have to collaboratively think of a generic solution which solves both their own challenges but also those of other participants. It is important to note that the whole of the iSHARE scheme remains constantly scrutinised by its participants and constantly grows towards maturity. What the iSHARE scheme entails or does not entail is the result of the co-creation process and the agreements made by the participants.

The co-creation process of Phase 2 was structured in the following way:

- There are four main topics within the scheme agreements: Functional (see page 51), Technical (see page 100), Legal (see page 190), and Operational (see page 170) agreements. These topics were discussed and organised separately;
- The relevant working groups for these four topics started with input in the form of the 'startdocument v0.1'. This document provided an overview of relevant topics that were later detailed by the working groups;
- Working groups had regular meetings facilitated by a chairman and a secretary who logged and processed agreements in a transparent way;
- The working groups worked towards incremental new versions of the iSHARE scheme documentation.

79 http://www.topsectorlogistiek.nl

iSHARE's co-creation partners have a variety of backgrounds: private and public organisations, organisations of different sizes, (serving) different modalities, both providers and receivers of data, etc. The variety of organisations ensures that the iSHARE scheme is widely applicable.

7.2 Assumptions

The iSHARE scheme was developed with the following assumptions in mind:

1. **Conditions for the exchange of data are assumed to be established;**
   The iSHARE scheme needs to rely upon the responsibility of participants to know what rights they have to what data. iSHARE is meant as an instrument to exchange data in a uniform, controlled and straightforward way; it is not meant as a means to resolve questions of data ownership. In practice this means that a party sharing data bears responsibility to sufficiently establish whether the party receiving the data is authorised to receive it.

2. **Data formats and semantics are assumed to be in place;**
   In order to be able to exchange data, a mutual understanding of the meaning of data and the way data is structured is required. Within iSHARE, it is assumed that this mutual understanding exists and thus the exchange of data between involved parties is possible (in line with guiding principle 4 (see page 10)). Please note that this assumption emphasises the need for industry initiatives on data standards and formats.

3. **Data classification has taken place;**
   It is assumed that within the iSHARE scheme, participants have sufficiently identified and classified their data. iSHARE participants are responsible for the classification of their data; the iSHARE scheme does not prescribe its participants how to classify their resources. Please refer to data classification in the glossary[80] for further detail.

7.2.1 Operational assumptions:

The Operational details of the iSHARE scheme were developed with the following assumptions in mind:

1. **There will be a Scheme Owner of a yet to be defined form;**
   This can be an existing body or a new body, and/or responsibilities can be split between different bodies.

2. **The Scheme Owner is financed through some type of financing constellation;**
   This can be through participants paying some type of fee or in any other feasible way. The Operational working group did not decide upon the financing constellation of the Scheme Owner.

3. **The complexity of the operational processes is expected to be as follows:**
   - It is considered reasonable to expect between 1000 and 10000 adhering parties in the first 5 years after iSHARE goes live;
   - It is considered reasonable to expect between 20 and 50 certified parties in the first 5 years after iSHARE goes live;
   - It is considered reasonable to expect parties to participate from countries all over the world in the first 5 years;
   - The Scheme Owner aims to keep effort needed for admission as low as possible for both adhering- and certified parties without compromising the integrity of the iSHARE scheme and -network;
   - The Scheme Owner regularly tests the robustness of the scheme and plans for mitigation of risks/ threats (e.g. identifying Single Points of Failure);

80 https://innopay.atlassian.net/wiki/spaces/IS/pages/54973357/Data+classification

- The Scheme Owner is assumed to have at least some responsibility in realising sustainable growth of the iSHARE network;
- The management of disputes regarding the contents of the data shared through iSHARE is not a core role of the Scheme Owner; disputes should be handled by involved parties.

These assumptions are, in NO WAY, ambitions. They were simply defined to base processes and service levels upon.