iSHARE

Version 1.2

Exported on 10/25/2017

Table of Contents

iSHARE is a collaborative effort to improve conditions for data-sharing for organisations involved in the Dutch logistics sector. Within two years the project aims to establish a fully functional "scheme" which manages a set of agreements made between involved organisations. The scope of the iSHARE scheme focuses on topics of authentication, authorisation and identification. In January 2018, the iSHARE scheme will be ready to open up to the market after two years of building and adjusting agreements to improve the conditions for sharing data.

Introduction

This document provides a full overview of the iSHARE scheme.

iSHARE is a collaborative effort to improve conditions for data-sharing for organisations involved in the Dutch logistics sector. Within two years the project aims to establish a fully functional "scheme" which manages a set of agreements made between involved organisations. The functional scope of the iSHARE scheme focuses on topics of authentication, authorisation and identification. In January 2018, the iSHARE scheme will be ready to open up to the market.

This chapter further describes the history and context of the iSHARE scheme, how the iSHARE scheme is established through co-creation with participating organisations, and what the purpose of this document is. The remainder of this section is dedicated to the goals and scope of the iSHARE scheme, the key features, guiding principles and assumptions and a description of roles and responsibilities present within the scheme. For an overview of used terms and their explanation, please consult the glossary.

History and planning

The project to establish the iSHARE scheme was initiated by the Neutral Logistics Information Platform (NLIP), as part of the government programme "Topsector Logistiek", through a tender project in 2016. NLIP requested market companies to present plans to lower barriers for more efficient data exchange in the Dutch logistics sector. The combination of the companies Innopay and Maxcode won the tender with their 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 January 2018.

The establishment of the iSHARE scheme knows 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: (Jan 2017 - Jun 2017): Co-creation phase, during this phase participating organisations worked collaboratively towards iSHARE scheme v1.0 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 Legal, Functional and Technical working groups (the Operational working group was postponed to at the earliest phase 3). Participating organisations realised Proofs of Concept to verify the correct functional and technical workings of the iSHARE scheme;
- Phase 3: (Jun 2017 - Jan 2018): Soft launch phase, during this phase the involved organisations organise how the iSHARE scheme's integrity and sustainability are kept in check. This involves setting up procedures for accession to the scheme and/or establishing/designating an organisation entrusted with the responsibility to safeguard the integrity of the iSHARE scheme;
- Phase 4: (Jan 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.

Establishment of the iSHARE scheme through co-creation

The iSHARE scheme is established through collaboration between its participating organisations. By going through a co-creation process, the collective expertise of all participants leads to a practical and widely applicable scheme. This process is fueled 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 is constantly scrutinised by its participants and constantly grows towards maturity. What the iSHARE scheme eventually entails or does not entail is the result of the co-creation process and the agreements made by the participants.

The co-creation process is structured in the following ways:

- There are four main topics within the scheme agreements: Legal, Operational, Functional and Technical (LOFT) agreements (presented in FTLO order in the scheme, for readability). The assumption is that for a fully functional scheme, at least these topics need to be discussed and organised;
- The relevant working groups for these four topics start with input in the form of the "startdocument". This document provides an overview of relevant topics that will be detailed by the working groups;
- Working groups have regular meetings facilitated by a chairman and a secretary who registers made agreements.

The participants of the co-creation process 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 will be widely applicable.

Purpose of this document

The purpose of this document is to provide a complete overview of the current state of the iSHARE scheme. The iSHARE scheme and this document are a "growing document" to which additions and changes are regularly made.

Notes accompanying current version of this document (Version 1.2)

iSHARE scheme version 1.2 contains the first version of the Operational specifications, of which the processes and service levels are most mature. Furthermore:

- Under **Introduction** and **Functional**, the iSHARE framework has seen a makeover to make it more accessible;
- Under **Technical**, the interface specifications and language of delegation and authorisation have been constantly improved with input from Proof of Concepts;
- Under **Legal**, the legal framework has been extended, among others with an overview of GDPR, and (closely aligned) two template agreements have been set up which iSHARE participants *could* use when exchanging personal data.

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 will result in a set of agreements based on which improved data exchange can be achieved.

The ambition of the iSHARE project 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. Authentication;
3. Authorisation.

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 working towards a more uniform, straightforward and controlled way of exchanging data on a bigger scale than is possible right now*,**.

- Uniform: one way of working which is compatible with all types of modalities, big and small organisations, public or private organisations, suppliers or 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, 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. To read more about the co-creation process, we refer to the chapter on co-creation in working groups.

*Note: iSHARE's scope does not include the specification of possible business models for sharing data and/or payments related to data exchange.

**Note: The iSHARE scheme can in some way be compared with the institute of the passport: the iSHARE scheme will be useable by anyone who owns a digital identity compatible within 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).

Key features

Based on the research resulting from Phase 1, the iSHARE scheme should at least support the following key features:

- Provide flexibility in authorisation
- Allow for management of consent
- Support multiple interaction models
- Provide a PKI trust framework
- Facilitate the use of federated identity(s)

Please note: in line with the iSHARE guiding principles, these key features might be realised by (re)using existing standards or initiatives.

Provide flexibility in authorisation

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.In the current version of the iSHARE scheme, the flexibility of authorisations is captured in the language for delegation and authorisation.

- **Granular authorisations**
  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. In the current version of the iSHARE scheme, the granularity of authorisations is captured in the language for delegation and authorisation. For more information on granularity of authorisations, please consult the glossary.
- **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 under the Primary Use cases.

Allow for management of consent

For appropriate recognition of authorisations a mechanism to manage consent is required. This mechanism should support both rule based consent (e.g. based on information already residing in a company's ERP system) or case by case consent given by a natural person (e.g. through some sort of digital signature on a mobile device).

Any form of consent should be subject to a management procedure allowing Data Owners to modify or withdraw certain rights.

Support multiple interaction models

To cater for different user scenarios, the iSHARE scheme aims to support multiple interaction models. Within the current version of the iSHARE scheme, the "Human to machine (H2M)" and "Machine to Machine (M2M)" interaction models are foreseen. Both these models can be characterised as request-and-response models. For more information on the current use of these interaction models, please refer to the functional descriptions of the interaction models.

Depending on utility and future growth, other interaction models like "Peer to Peer (P2P)" and "Publish and Subscribe" might be added.

Provide a PKI trust framework

The iSHARE scheme relies on public key encryption for several core processes, amongst which the following:

- Proof of origin of data;

- Proof of authenticity of identities;
- Protection of data against unauthorised access or disclosure.

A Public Key Infrastructure (PKI) is required, in order to:

- Publish public keys (through digital certificates);
- Certify that public keys are tied to the right individuals or organisations;
- Verify the validity of public keys.

iSHARE aims to provide a list of certificate roots (also called PKI roots), or Certificate Authorities, that meet the iSHARE requirements. These Certificate Authorities can be (and must be) trusted by all iSHARE participants for the registration and issuance of digital certificates. iSHARE will at least trust the certificate authorities/service providers listed by the EU under EIDAS regulation (for a list of trusted service providers, click here. More information on EIDAS can be found here).

Facilitate the use of federated identity(s)

iSHARE aims to facilitate (but not impose) the use of one or more federated identity(s). A federated identity is an identity that is spread out and recognised 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 identity provider must be certified under the iSHARE scheme.

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 (external link).

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 & authorisation
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 & 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.
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.

Assumptions

The iSHARE scheme was developed with the following assumptions in mind:

1. **Conditions for the exchange of data - or calls upon services - 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 and/or services. iSHARE is meant as an instrument to exchange data or call upon services 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 for instance a Service Provider bears responsibility to sufficiently establish whether a Service Consumer is authorised to receive certain data or call upon certain services.

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 the iSHARE scheme it is assumed that this mutual understanding exists and thus the exchange of data between involved parties is possible (also see guiding principle 4: "Agnostic towards nature and content of data")

3. **Data and service classification has taken place**
   It is assumed that within the iSHARE scheme, participants have sufficiently identified and classified their data and services. Data owners are responsible for the classification of their data and services, the iSHARE scheme does not prescribe its participants how to classify their resources (See "Data Classification" in the glossary for an explanation of Data Classification)

Roles & Responsibilities

This section describes the iSHARE framework, the functional roles within the iSHARE framework, and the general responsibilities of the functional roles. A more detailed explanation of each role's functional behaviour, and interaction between roles is described in the section containing the Functional descriptions.

The section is presented as follows:

- Role framework
  - Scheme Owner(ship)
  - Entitled Party
  - Service Consumer
    - Machine Service Consumer
    - Human Service Consumer
  - Service Provider
  - Identity Provider
  - Identity Broker
  - Authorisation Registry
- Adherence, certification and compatibility

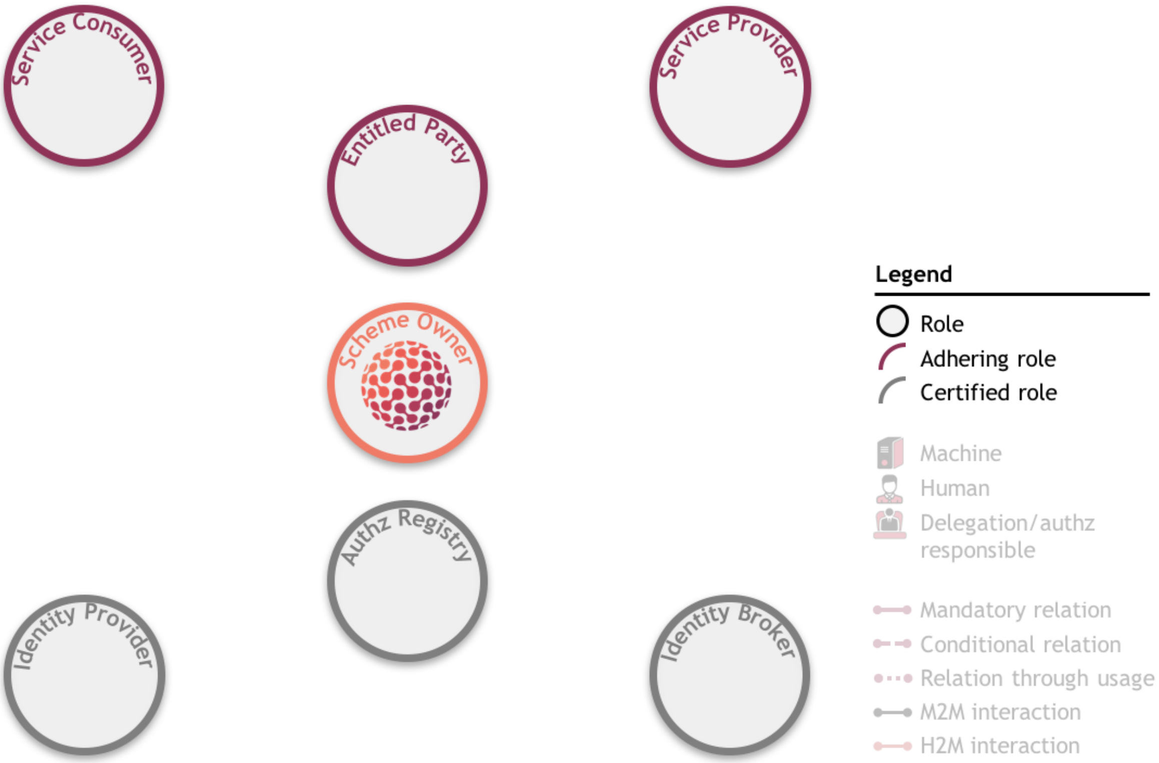
Role framework

Please note that the term data exchange was deemed too narrow for the scope of iSHARE, therefore the wider term of service provision was introduced.

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 cases possible in practice. This section explains the iSHARE framework, its roles, and its relations, step-by-step.

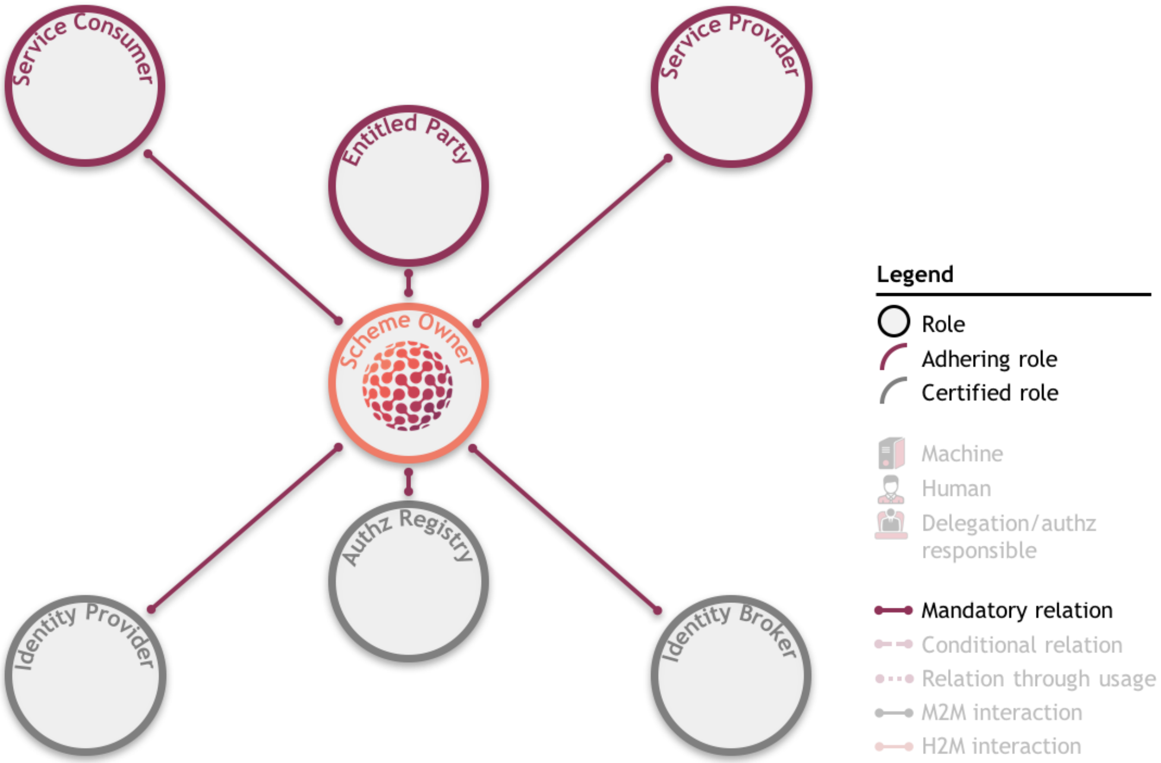
iSHARE framework

The iSHARE framework consists of seven functional roles that, depending on the situation, interact with each other based on the iSHARE scheme rules. Each role has a certain function in the overall scheme and bears certain responsibilities, in underlying pages. In principle, the iSHARE framework can be applied for service provision use cases throughout the logistics sector. Do note that a party can fulfill several roles within the scheme, depending on the context and what service is provided/consumed. The basic iSHARE framework looks as follows:



The right combination of the roles depicted above guarantees a more uniform, straightforward and controlled way of providing services. How exactly is explained under Functional.

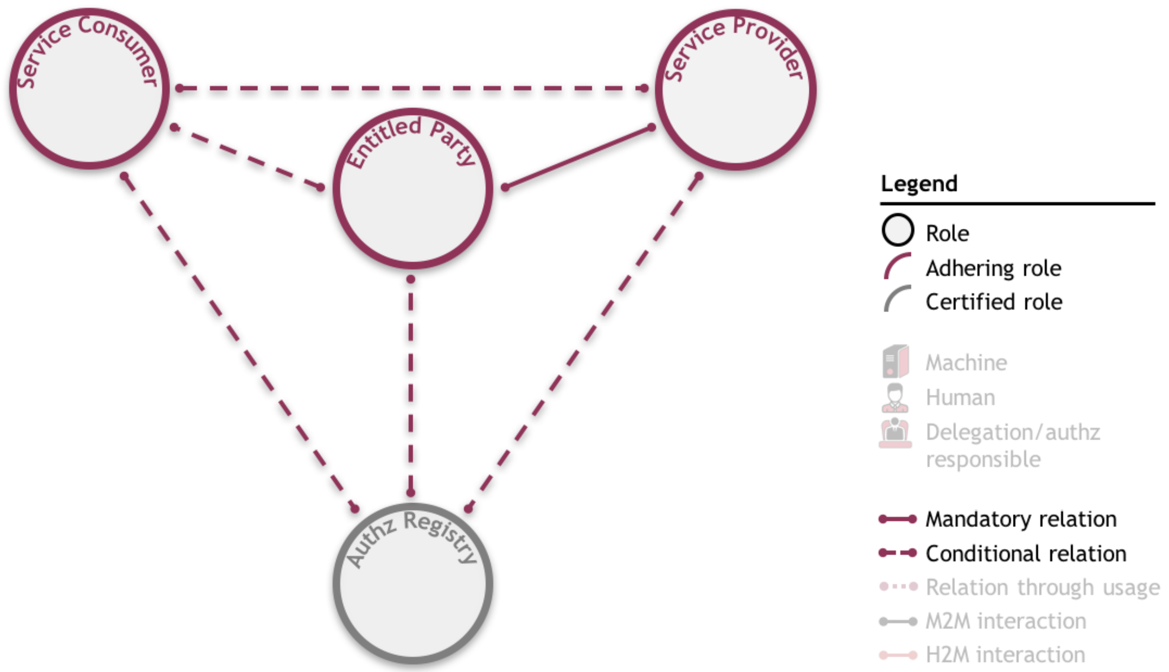
The Scheme Owner-role is taken by the party that governs the iSHARE scheme and its participants. To fulfil any other role in the framework, a party must fulfil admittance criteria and sign an agreement with the Scheme Owner. Different criteria and agreements exist for adhering roles and certified roles, as explained in more detail here. The fact that every party 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 scheme. This is why the following depiction of the iSHARE framework, showing the mandatory relation between the Scheme Owner and every other role, is called the **trust framework**:



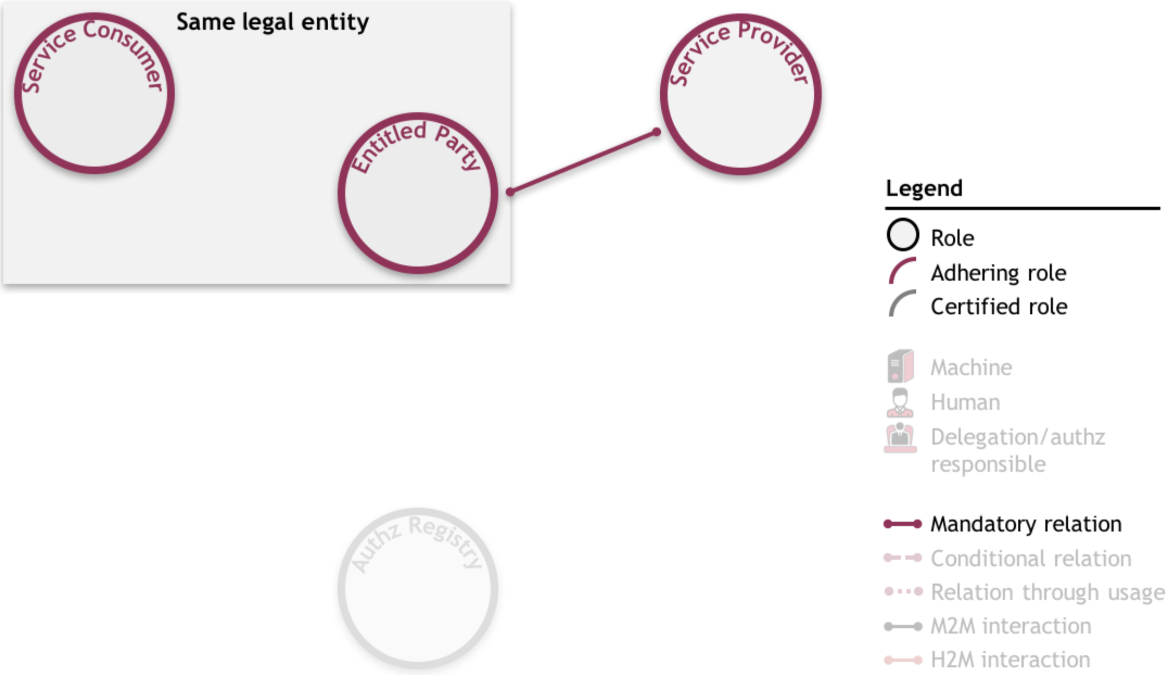
Every relation or interaction within iSHARE, other than those depicted here, is build upon the trust framework. This is why the trust framework is not depicted in the following.

M2M framework

Let us now zoom in at some very basic roles and real-world situations, using the iSHARE framework. The iSHARE framework can cater both Machine to Machine (M2M) and Human to Machine (H2M) and use cases, as explained in more detail here. The **M2M framework**, with all potential relations (but not those with the Scheme Owner, as these are in the trust framework) is as follows:



In the least complex of M2M situations, a machine at the Service Consumer interacts with a machine at the Service Provider, as depicted in the example below.

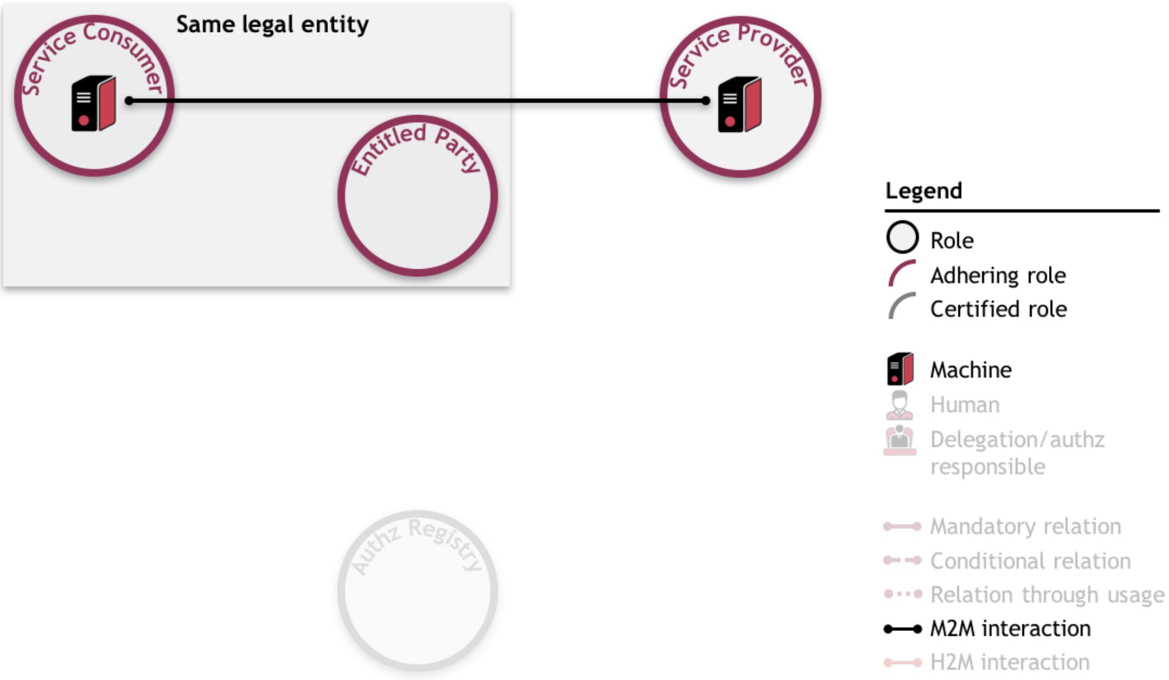


The **Entitled Party** is the legal entity that requires the right(s) to service(s) provided by a Service Provider. In this case, the Entitled Party arranges (in a legal agreement with a Service Provider) that it is has the right to consume its services.

The **Service Provider** provides certain services, such as data, to machines and humans at Service Consumer(s).

The **Service Consumer** consumes the Service Provider's service on the basis of the Entitled Party'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. In this case, as depicted, the Service Consumer is the same legal entity as the Entitled Party.

Now let's see what happens when the Service Consumer consumes the Service Provider's service on the basis of the Entitled Party's rights to it.

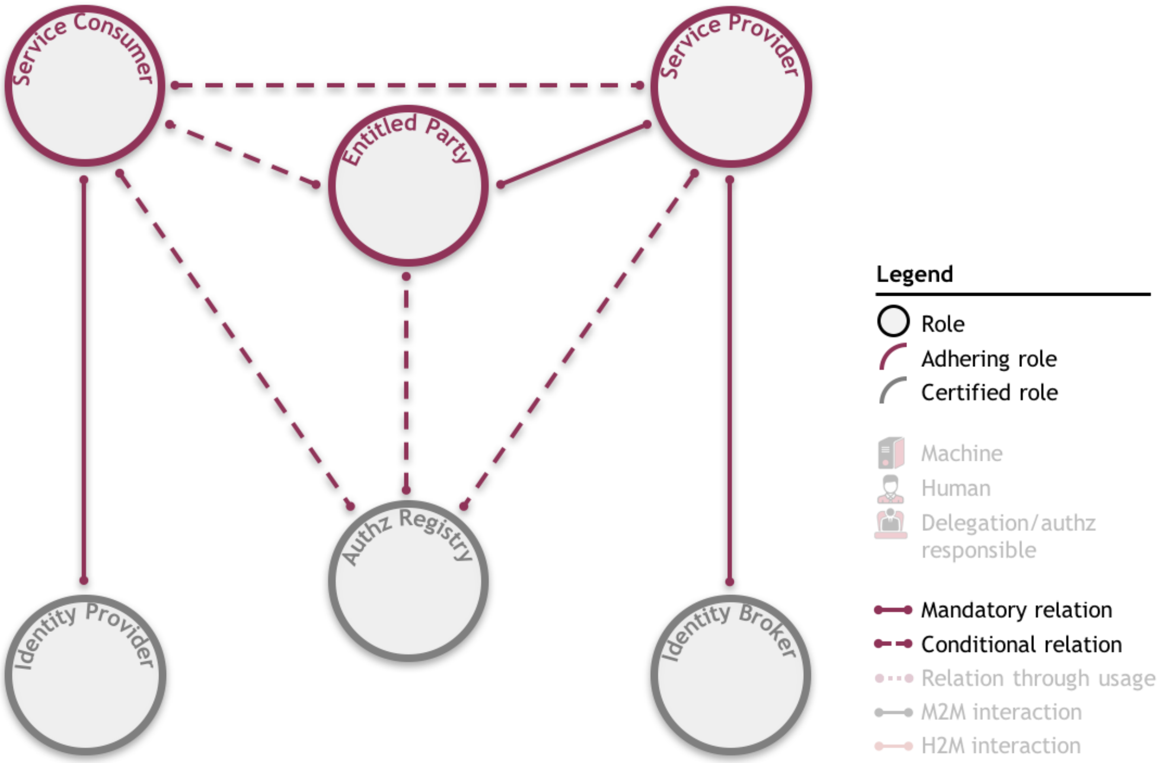


The **Machine Service Consumer** represents a machine that requests, receives, and uses certain services from a machine at a Service Provider. The Machine Service Consumer is managed by the Service Consumer. In this use case, it requests a service via M2M interaction. Because the Service Provider knows the Entitled Party's rights to the service through their legal agreement, and because the Entitled Party is the same legal entity as the Service Consumer, it provides the service to the Machine Service Consumer.

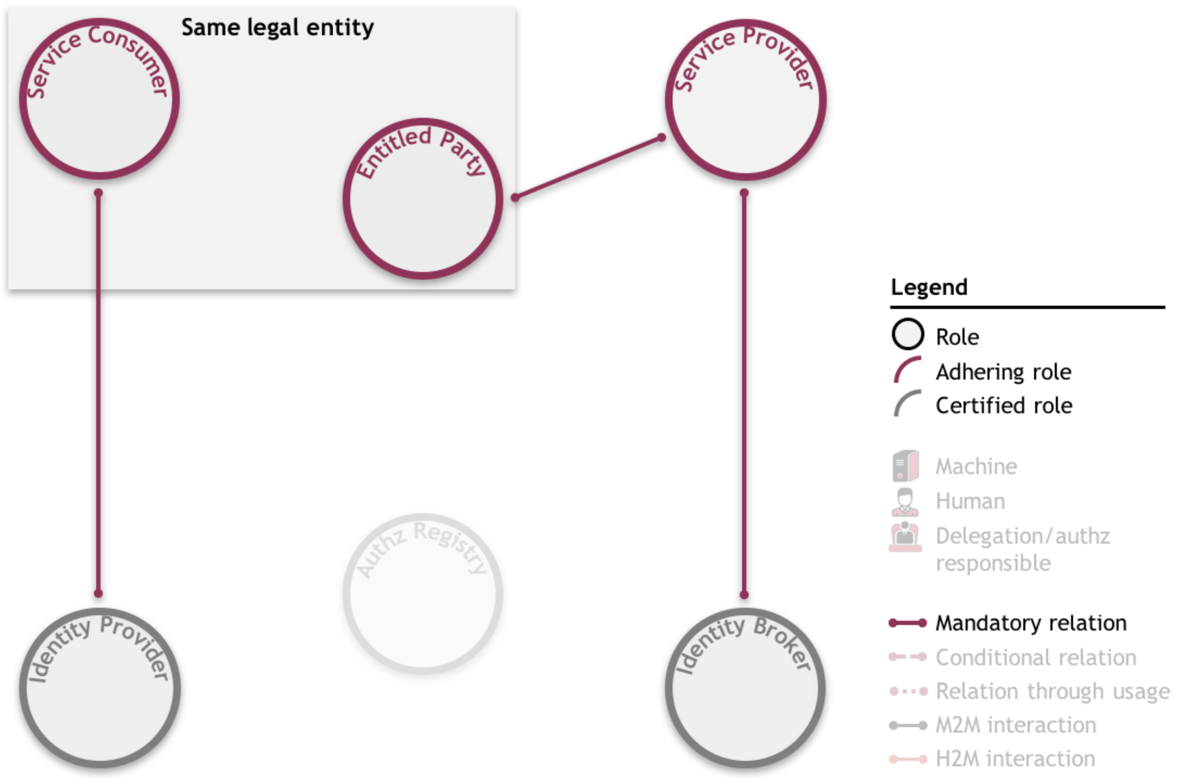
The above example is already very similar to primary use case 1 that is detailed under Functional. In the following example, a Human Service Consumer is involved instead of a Machine Service Consumer.

H2M framework

The H2M framework, with all potential relations (but not those with the Scheme Owner, as these are in the trust framework) is as follows:



In the least complex of H2M situations, a human at the Service Consumer interacts with a machine at the Service Provider, as depicted in the example below.

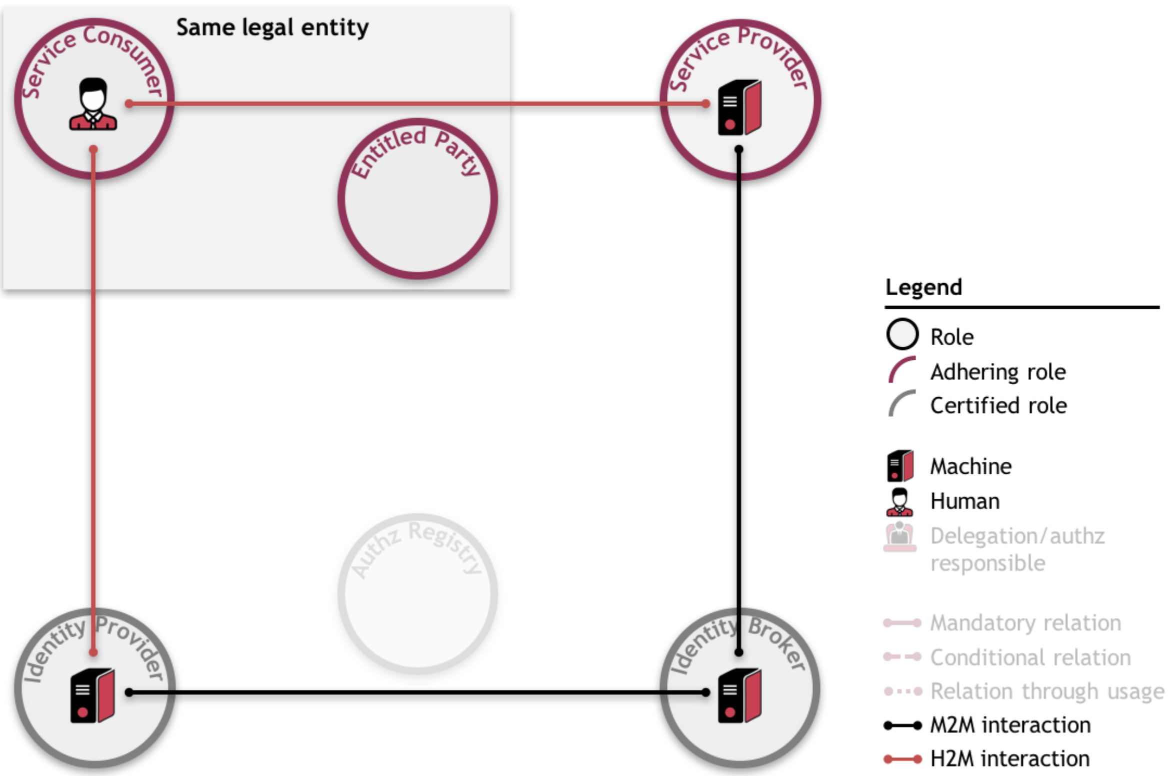


The Entitled Party, Service Provider and Service Consumer roles all come back as in the M2M use case above. As depicted, the Service Consumer is the same legal entity as the Entitled Party.

The **Identity Provider**, simply said, authenticates a human for the Service Provider. It can do this by letting the human log in with a username in password, or in other ways.

Because several Identity Providers could be present in the iSHARE scheme, an Identity Broker is introduced. The **Identity Broker** prevents the need for a direct relationship between all Service Providers and all Identity Providers. To a human, the Identity Broker offers a user interface in which the human can choose his preferred Identity Provider.

Now let's see what happens when the Service Consumer consumes the Service Provider's service on the basis of the Entitled Party's rights to it.



The **Human Service Consumer** represents the human (person) who requests, receives, and uses certain services, from a machine at a Service Provider. The Human Service Consumer works for the Service Consumer. In this use case, requests a service via H2M interaction. Because the Service Provider knows the Entitled Party's rights to the service through their legal agreement, because the Entitled Party is the same legal entity as the Service Consumer, and because the Service Provider knows which humans can request services on the Service Consumer's behalf, it provides the service to the Human Service Consumer.

This example is very similar to primary use case 2 as also detailed under Functional.

Note again that the roles Service Consumer and Service Provider are not fixed to particular entities. In other words, a Service Provider may be a Service Consumer in another context of service provision. Likewise, depending on the context, the concepts of data ownership, responsibility and accountability can take different forms.

The only role not mentioned here is the **Authorisation Registry**, which is explained in detail here.

Scheme Owner(ship)

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, parties will need to register themselves as certified or adhering 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.

Entitled Party

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

The **Entitled Party** is the legal entity that has one or more rights to something, e.g. to data at a Service Provider that it has a legal agreement with. The Entitled Party is either the same entity as the Service Consumer, 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 is REQUIRED.

Service Consumer

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

The **Service Consumer** is the legal entity that consumes the Service Provider's service on the basis of the Entitled Party'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 or Human Service Consumer to do so.

The Service Consumer is a role for which iSHARE adherence is REQUIRED.

Machine Service Consumer

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 on behalf of and authorised by the Service Consumer.

The Machine Service Consumer is not a separate role, but it belongs to the adhering party Service Consumer.

Human Service Consumer

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 on behalf of and authorised by the Service Consumer.

The Human Service Consumer is not a separate role, but belongs to the adhering party Service Consumer.

Service Provider

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

The **Service Provider** is a role that provides certain services, such as data, to a Service Consumer. In case the service pertains to data provisioning, the Service Provider is either the Data Owner, or has explicit consent of the Data Owner to provide the services.

The Service Provider is responsible for the availability of services, and accountable for these services if it also the Data Owner.

The Service Provider is a role for which iSHARE adherence is REQUIRED.

Identity Provider

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

The **Identity Provider**:

- Provides identifiers for Human Service Consumers;
- 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, such as:

- Password authentication;
- Hardware-based authentication (smartcard, token);
- Biometric authentication;
- Attribute-based authentication.

The Identity Provider is a role for which iSHARE certification is REQUIRED. This certification builds on the eHerkenning certifications for both 'Middelenuitgever' and 'Authenticatiedienst'.

Identity Broker

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

If multiple distinct Service Providers exist where each data set is protected under a distinct trust domain, multiple Identity Providers may be needed. Moreover, the iSHARE scheme may require different levels of certainty 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 to select the Identity Provider they prefer to authenticate 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 is REQUIRED. This certification builds on the eHerkenning certification for 'Herkenningsmakelaar'.

Authorisation Registry

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

The **Authorisation Registry**:

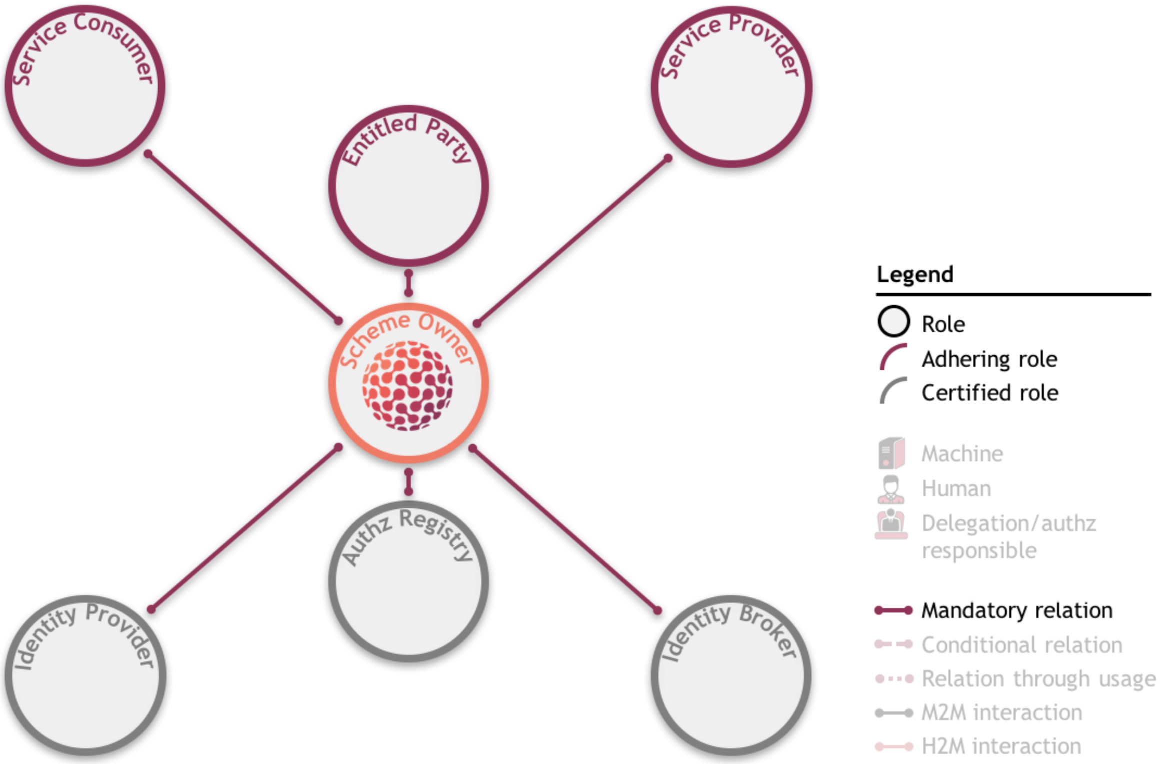
- Manages records of delegations and authorisations of Entitled Parties and/or Service Consumers;
- Checks on the basis of the registered permission(s) whether a Human or Machine Service Consumer is authorised to take delivery of the requested service, and;
- Confirms the established powers towards the Service Provider.

Within the iSHARE scheme, the term Authorisation Registry always refers to an external Authorisation Registry (not part of the Service Provider or Entitled Party).

The Authorisation Registry is a role for which iSHARE certification is REQUIRED. This certification builds on the eHerkenning certification for 'Machtigingenregister'.

Adherence, certification and compatibility

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



A party fulfilling a role in the iSHARE framework, except the Scheme Owner itself, MUST be iSHARE adhering or iSHARE certified – as required for that role. Note that a party can fulfil more than one role.

The iSHARE roles depicted in purple are roles for which parties MUST adhere to the iSHARE scheme. An **iSHARE adhering party** adheres to the iSHARE terms of use. An iSHARE adhering party MUST sign an accession agreement with the Scheme Owner.

The iSHARE roles depicted in grey are roles for which parties MUST be certified within the iSHARE scheme. 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 for certification and, after providing sufficient proof, MUST sign a certification agreement with the Scheme Owner. While the exact bases for certification need to be determined, the eHerkenning responsibilities and requirements per role serve as a starting point. In this way the eHerkenning admission process is completely reused. eHerkenning certified parties would be asked to fulfil only some extra responsibilities and requirements to also become iSHARE certified.

Next to iSHARE adherence and certification, it is considered to be beneficial to the iSHARE scheme to add the possibility of products and/or processes being assessed as **iSHARE compatible**. iSHARE compatible products and/or processes comply to the iSHARE agreements and standards, from a functional and technical perspective. A conformity test will be developed at a later stage to affirm iSHARE compatibility.

Conventions & Versioning

This section includes notational conventions and notes on versioning. The section is presented as follows:

- Notational conventions
- Versioning

Notational conventions

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 RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt).

Please note: Other conventions can be added in due time.

Versioning

Unique version numbers will be assigned to unique states of the iSHARE scheme. For a full overview of previous versions of the iSHARE scheme documentation, please consult the version history on Confluence.

Functional

This section covers the functionality that is in scope of the the iSHARE scheme.

It starts by explaining the two interaction models that are at the basis of iSHARE's primary use cases: Machine to Machine (M2M) and Human to Machine (H2M). This is followed by the three primary use cases, which form the core of the Functional section:

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, most of which are explained in detail.

The secondary use cases that follow the primary use cases include processes related to registration, and processes that recur in primary use cases. The section is then concluded by functional requirements - those per role in the scheme and those to the iSHARE user interface in H2M use cases.

Interaction models

At this moment in time, two interaction models are at the basis of iSHARE's primary use cases: Machine to Machine (M2M) and Human to Machine (H2M). This chapter explains both models.

Machine to Machine

Sometimes called Server to Server, **Machine to Machine** interaction is the automated exchange of data and the performance of actions between electronic devices without requiring the assistance of humans. In some M2M applications, electronic devices exchange their data with a central control unit or app(lication), which processes the data for humans.

To exchange (send and receive) data (in the form of electronic signals), a communication network or channel is required such as a telecommunication network, the internet (Wifi, 3/4G), radio-frequency identification (RFID) or Bluetooth.

Human to Machine

Human to machine interaction is data transmission between a human (user) and an electronic device, and vice versa. A prerequisite is an interface that allows the input of the user to be translated into signals that the device understands, and allows the device to provide the required result to the human. This interface can include software (i.e. what is visible to the human on the computer monitor) and hardware (i.e. the mouse, keyboard and other devices).

Depending on the interaction model and which roles hold information, three primary use cases have been defined.

Note that all of these use cases are based on a **request-response** interaction model - in which the Service Consumer requests a certain service, and a Service Provider responds. In line with iSHARE's key features, the **publish-subscribe** interaction model - in which the Service Consumer subscribes to a service that is (repeatedly) published by the Service Provider - remains in scope. No high-priority practical use cases of this interaction model have been been identified yet, however.

Primary use cases

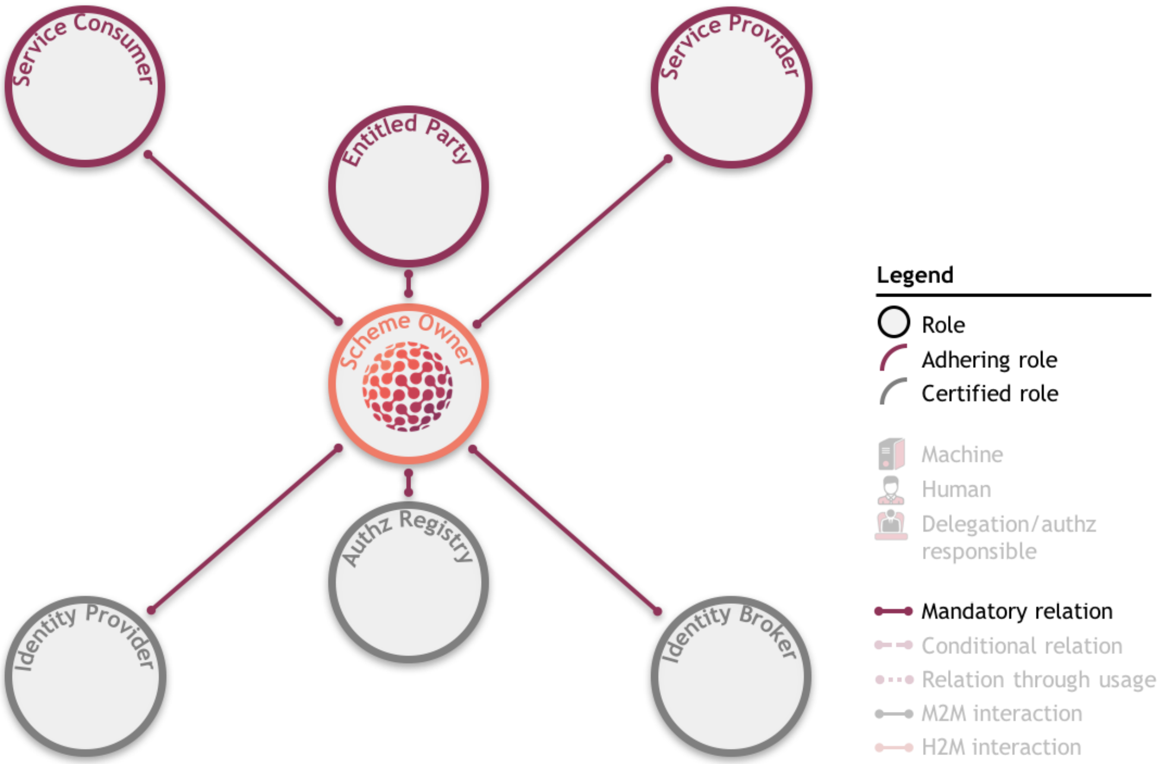
iSHARE knows three primary use cases that form the functional core of the scheme. This most important part of the Functional section explains the following:

- The iSHARE framework: its goal, roles, relations and 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 or delegation information is held.

iSHARE framework

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 cases possible in practice.

The iSHARE framework consists of seven functional roles that, depending on the situation, interact with each other based on the iSHARE scheme rules. Each role has a certain function in the overall scheme and bears certain responsibilities, as explained under Roles & Responsibilities. In principle, the iSHARE framework can be applied for service provision use cases throughout the logistics sector. Do note that a party can fulfill several roles within the scheme, depending on the context and what service is provided/consumed. The trust framework, created because every party that fulfils a role in the iSHARE scheme must agree to the scheme rules, was introduced as follows under Role framework:



In purple, there are so called adhering roles. These roles consume or provide services and adhere to the iSHARE terms of use. In grey are certified roles. These roles facilitate certain functions for the scheme relating to identification, authentication, authorisation and also delegation. Parties fulfilling certified roles need to register and certify themselves with the - to be established - iSHARE Scheme Owner. A third type of roles are compatible roles - as further explained here.

In the least complex situations, a Service Consumer interacts with a Service Provider. In the more complex situations, a Service Consumer interacts with a Service Provider that can only provide its service when it retrieves additional information from certified parties. This might be the case when authorisations for data are stored with a certified Authorisation Registry, or when a Human Service Consumer needs to be identified by an Identity Provider. Depending on the practical context, different roles of the iSHARE framework are called upon.

Within the iSHARE scheme, four types of information are recognised that are needed to facilitate identification, authentication and authorisation:

- **Entitlement info:** information indicating what Entitled Parties 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).

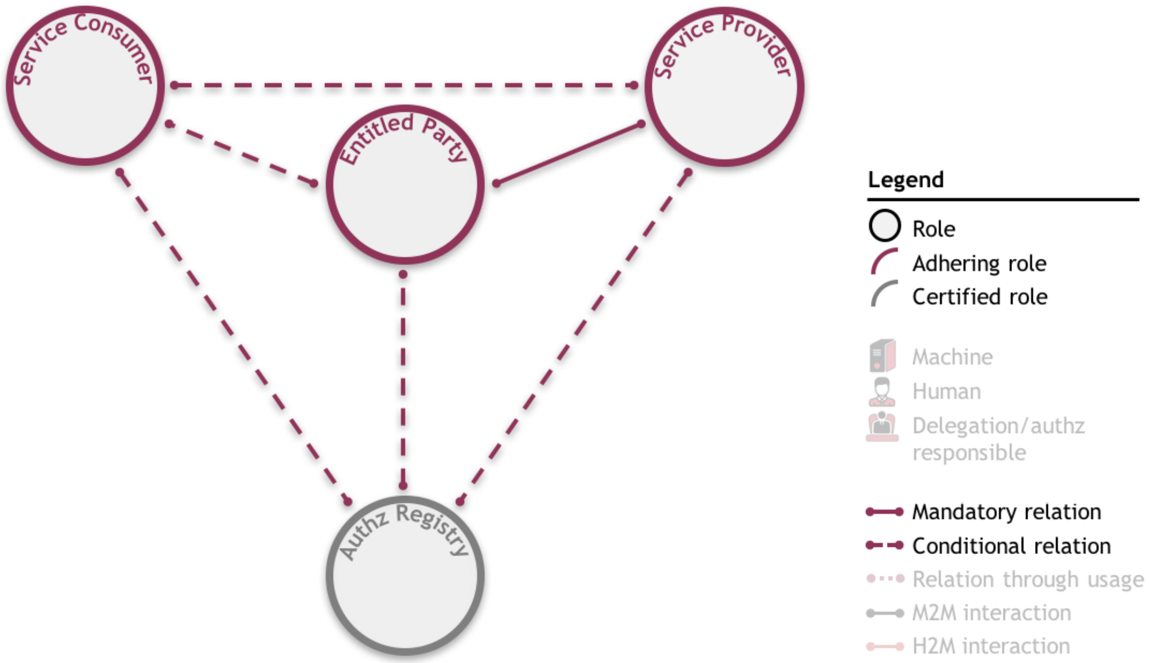
Depending on the specific situation, the required types of information, and which party can provide the required information, specific use cases can be derived. Within iSHARE, three primary use cases are recognised and 21 use cases derived from the primary use cases.

Three primary use cases

Two interaction models are recognised within iSHARE: Machine to Machine and Human to Machine. Depending on the interaction model and which roles hold the information summed up in the above, three primary use cases have been defined:

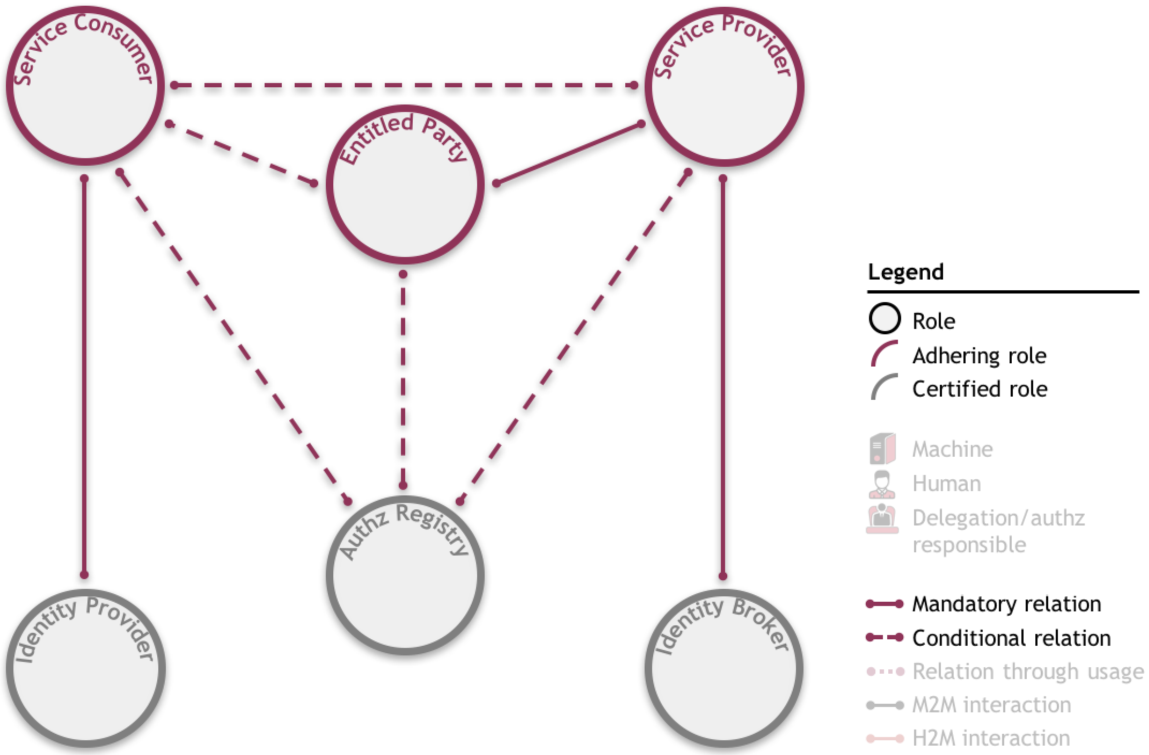
1. Machine to Machine service provision;
   Primary use case 1 caters to all Machine to Machine cases

For use case 1, the M2M iSHARE framework is used:



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 and does not need to consult other information points
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 the Identity Provider

For use cases 2 and 3, the H2M framework is used:



The primary use cases all know a variety of derived use cases. Derived use cases are variations of the primary use cases in which information required by the Service Provider is held by and retrieved from different parties. We call the party holding delegation- and/or authorisation information a **Policy Information Point (PIP).** This PIP, as in XACML, 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. 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	1a	1b	1c

*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.

**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	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	3a	3b	3c
	Entitled Party	3.1	3a.1	3b.1	3c.1

	Authorisation Reg	3.2	3a.2	3b.2	3c.2
	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 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 is detailed both without an Identity Broker and with one, while derived use cases 3.2 and 3c.2 both include an Identity Broker.

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

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

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

1. M2M service provision

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

Roles

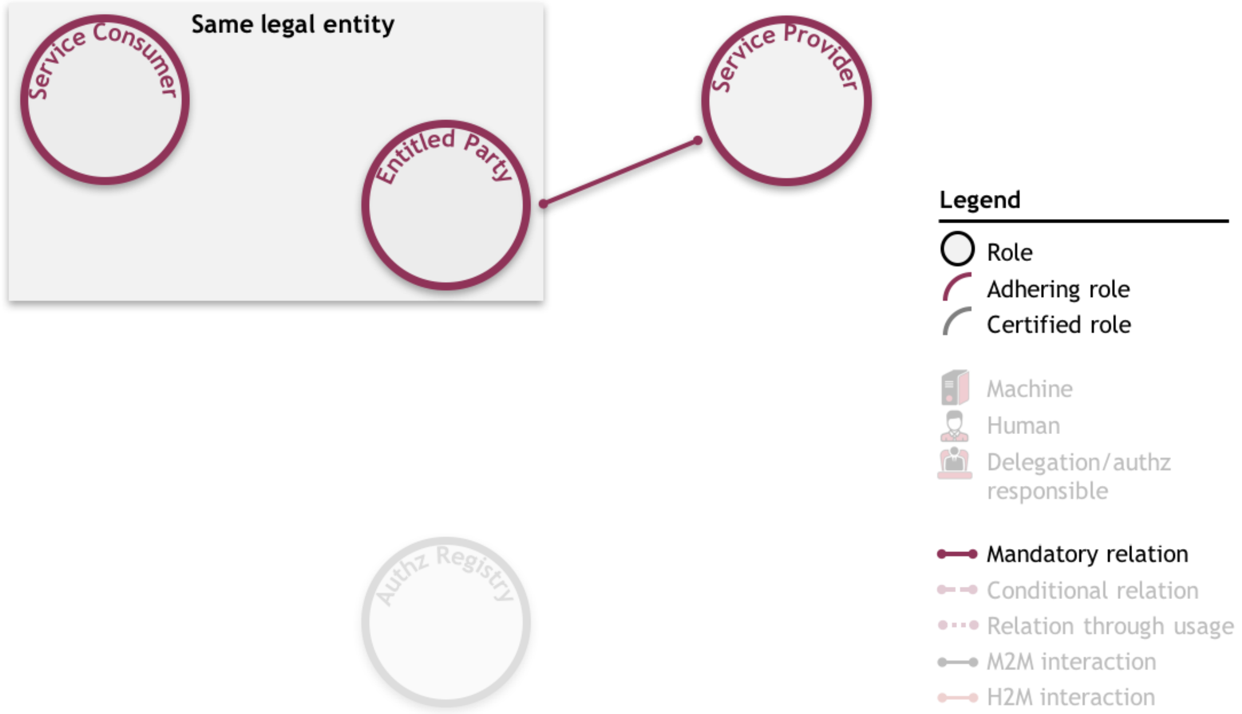
	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg

Use case variation	1	1a	1b	1c

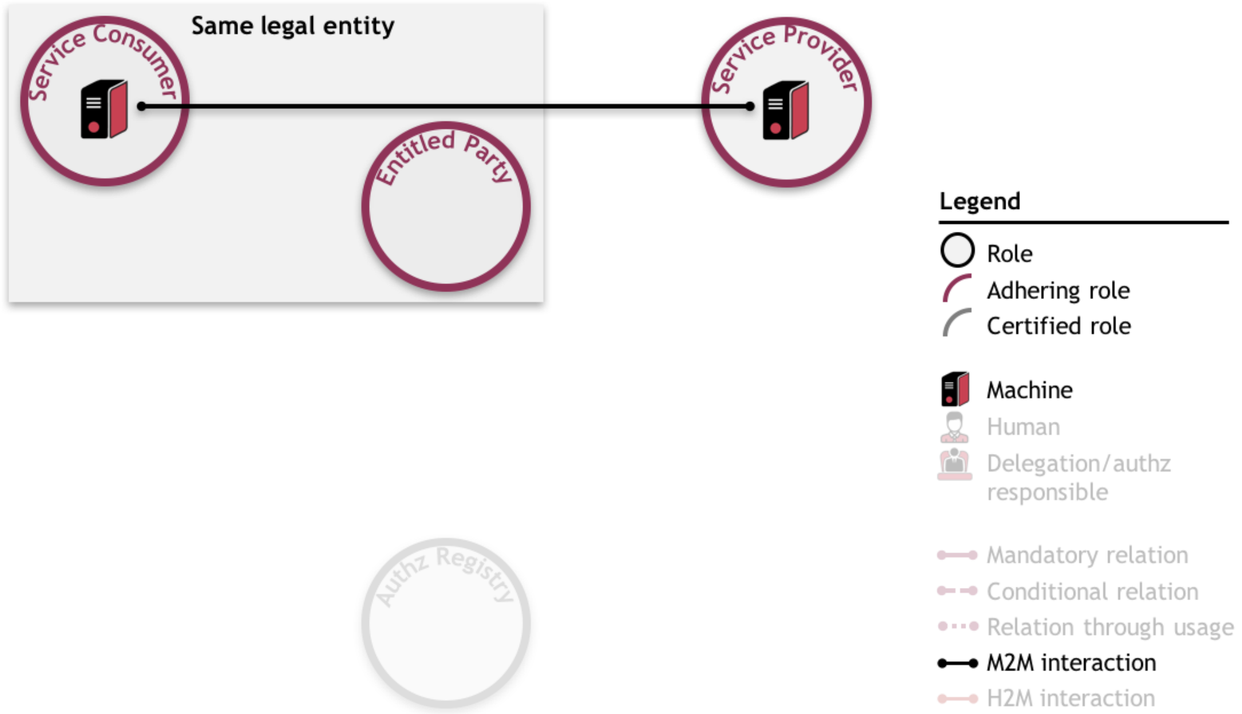
As no delegation takes place, the Entitled Party is also the Service Consumer.

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.

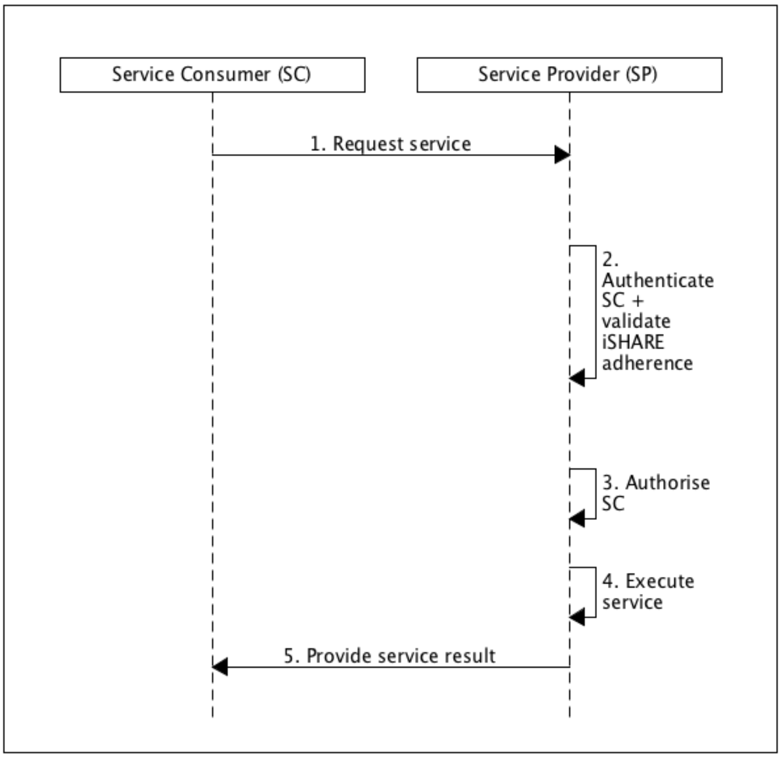
- In this use case the Entitled Party is also the Service Consumer.

*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	1a	1b	1c

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:

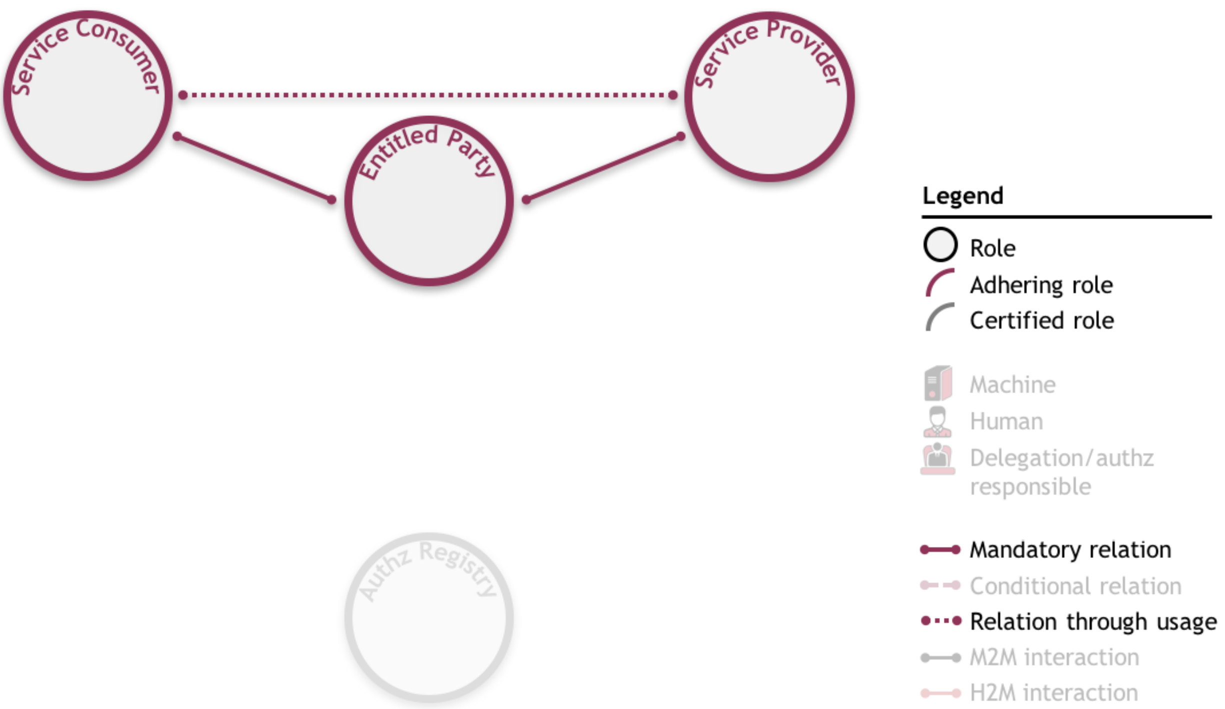
1. The Service Provider can request delegation info after a service request from the Service Consumer;
2. The Machine Service Consumer can request delegation info and include it in its service request to the Service Provider;

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.

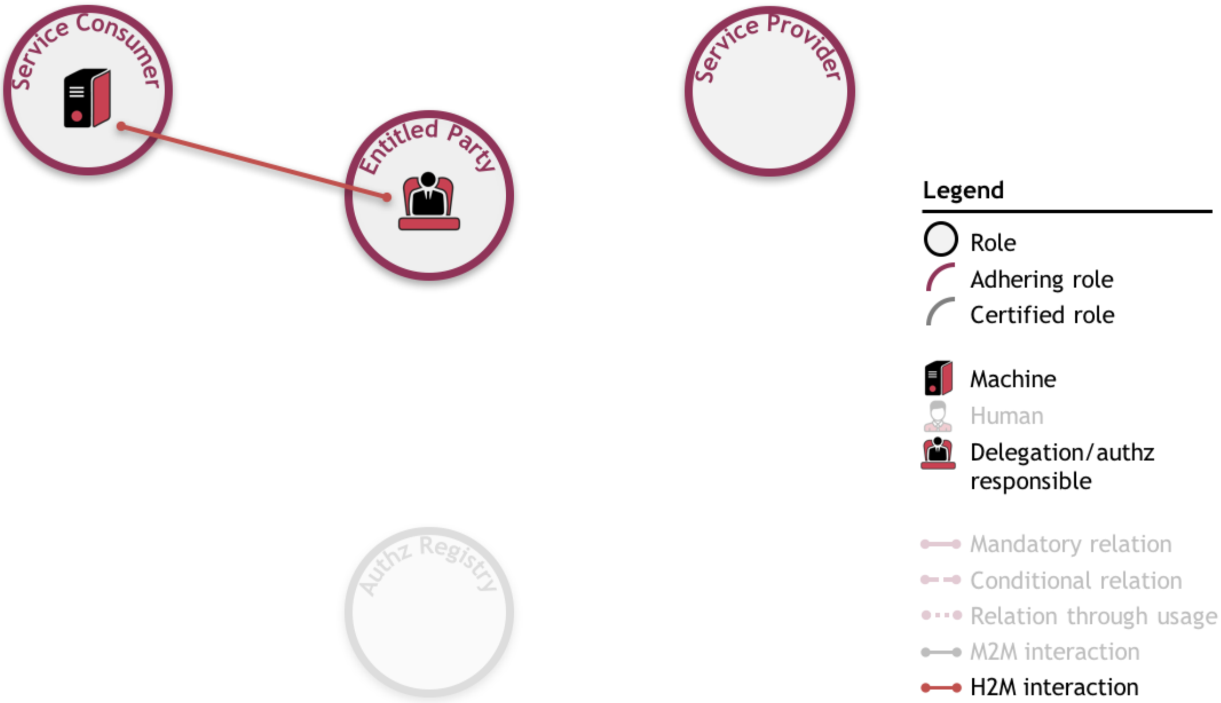
Depiction

Legal relations

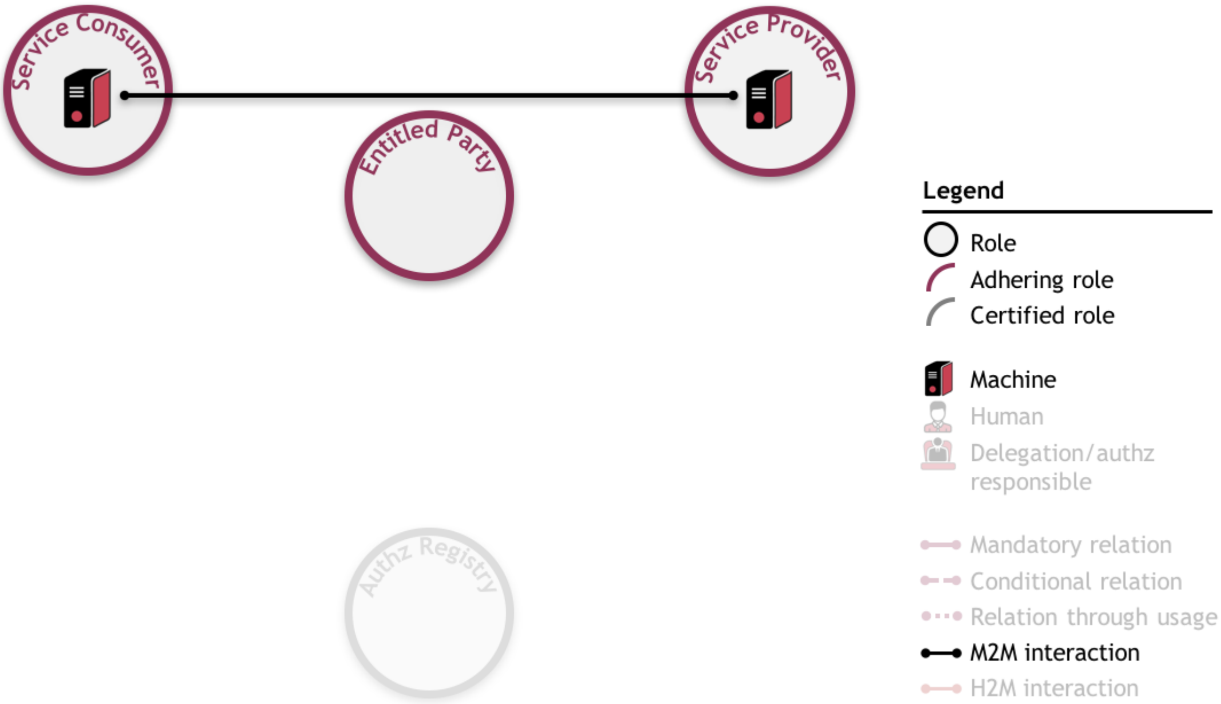


Note that no prior legal relation is exists between the Service Consumer and the Service Provider. Which services can be consumed by the Service Consumer, as delegated by the Entitled Party, is set out in the mandatory relation between this Entitled Party and the Service Provider.

Prerequisite registration



Use case interaction



Description

It is prerequisite of this use case that:

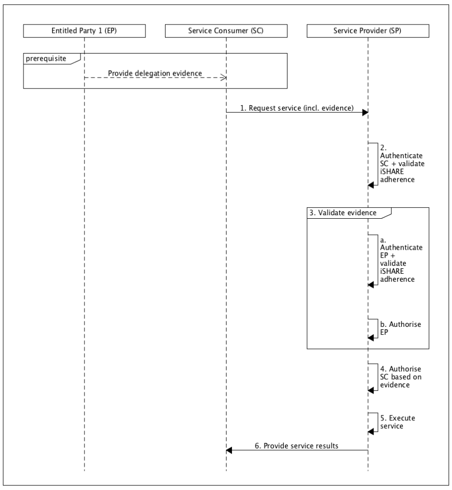
- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Service Consumer;
- The delegation/authorisation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


Entitled Party 1 (EP)
Service Consumer (SC)
Service Provider (SP)
prerequisite
Provide delegation evidence
1. Request service (incl. evidence)
2. Authenticate SC + validate iSHARE adherence
3. Validate evidence
a. Authenticate EP + validate iSHARE adherence
b. Authorise EP
4. Authorise SC based on evidence
5. Execute service
6. Provide service results

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	1a	1b	1c

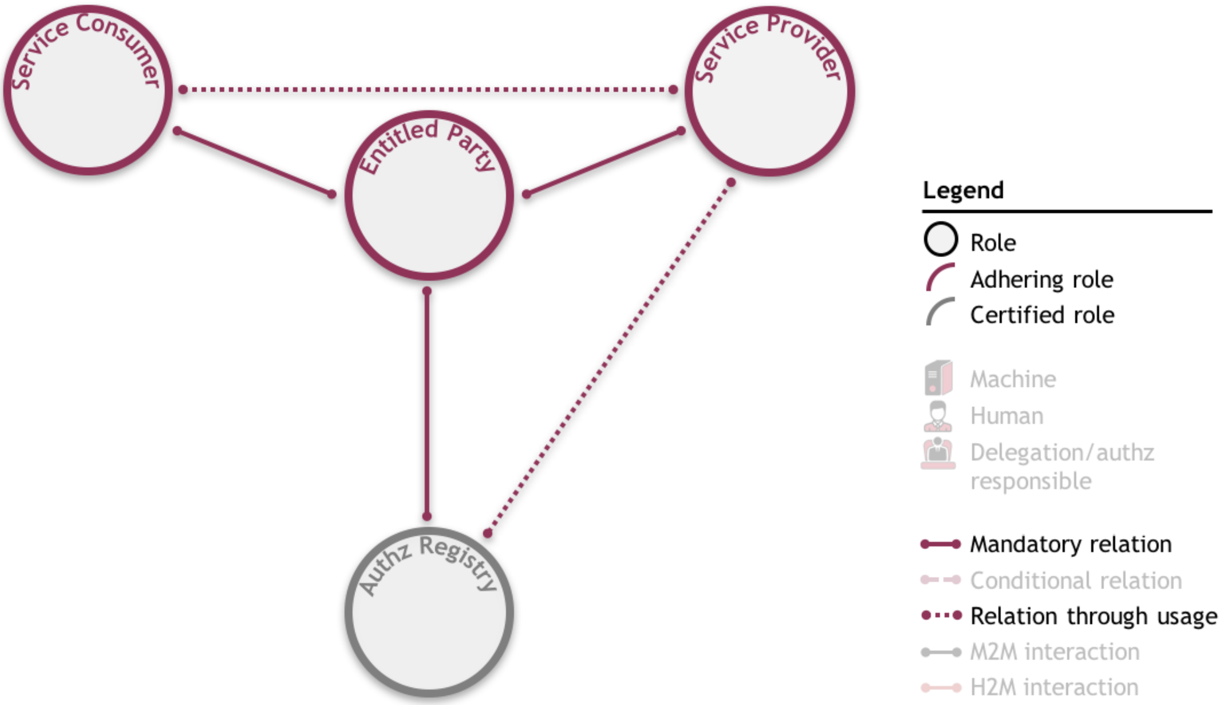
Note that interaction sequences are not described in the table above. In derived use case 1c, two interaction sequences are possible depending on who requests delegation info from the PIP:

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.

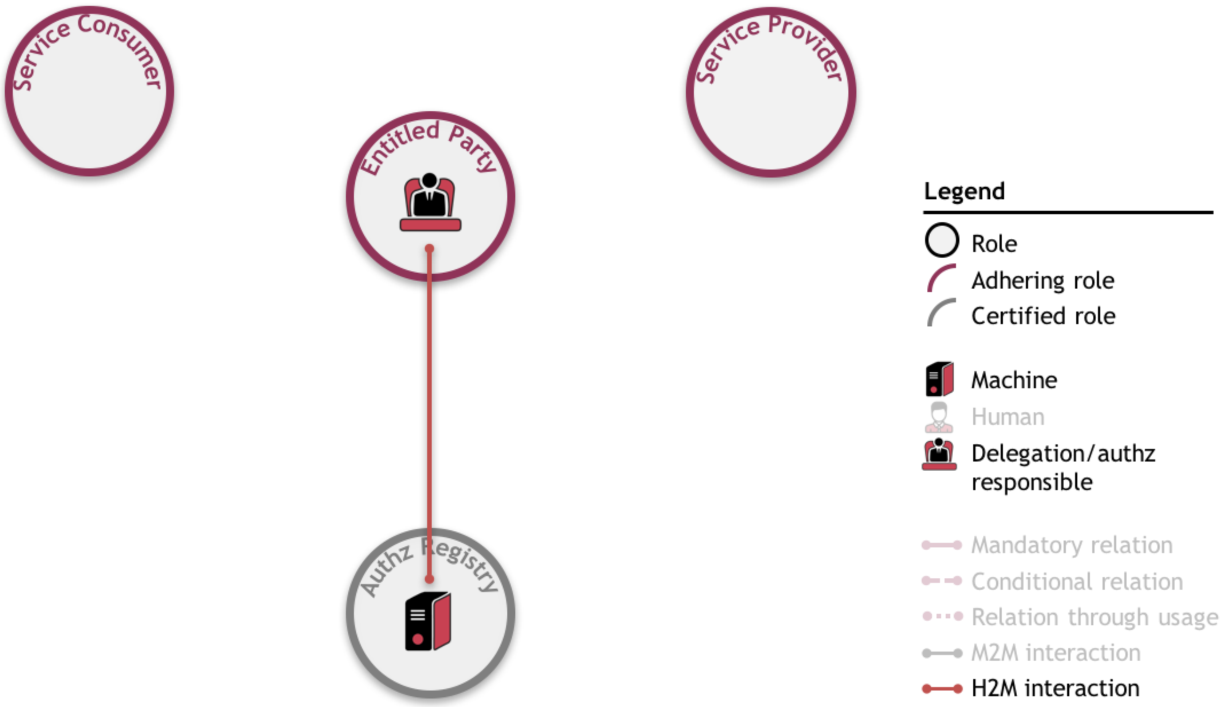
Depiction

Legal relations

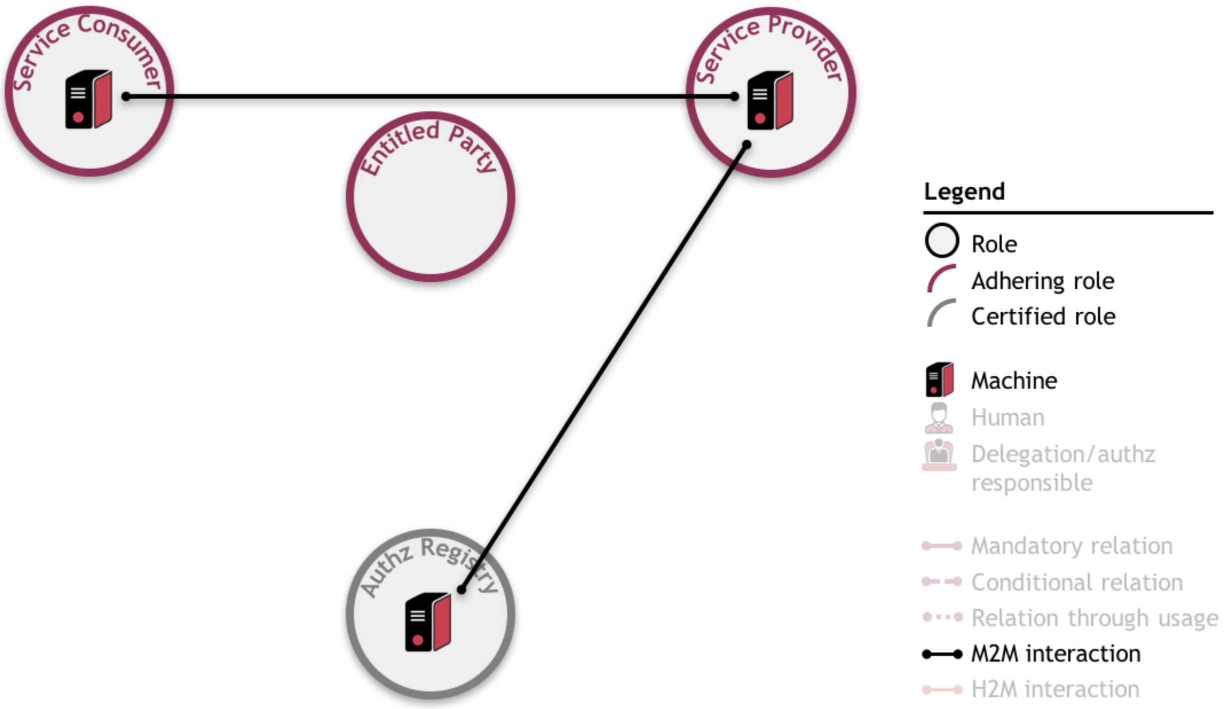


Note that no prior legal relation is exists between the Service Consumer and the Service Provider. Which services can be consumed by the Service Consumer, as delegated by the Entitled Party, is set out in the mandatory relation between this Entitled Party and the Service Provider.

Prerequisite registration



Use case interaction



Description

It is prerequisite of this use case that:

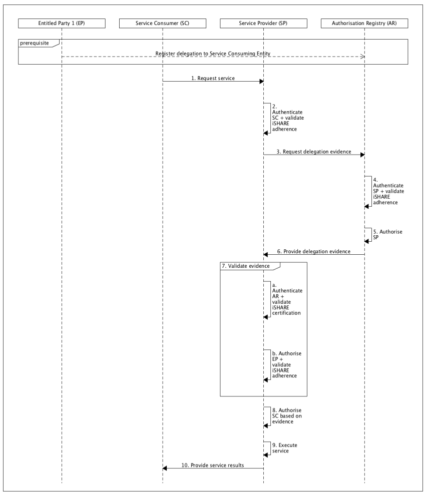
- The Service Provider has and manages its own entitlement information indicating what Entitled Parties are entitled to what (parts of) services*;
- The Service Consumer is able to authenticate the Service Provider;
- The Service Provider is able to authenticate the Service Consumer;
- The delegation/authorisation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


Entitled Party 1 (EP)
Service Consumer (SC)
Service Provider (SP)
Authorisation Registry (AR)
prerequisite
Register delegation to Service Consuming Entity
1. Request service
2. Authenticate SC + validate iSHARE adherence
3. Request delegation evidence
4. Authenticate SP + validate iSHARE adherence
5. Authorise SP
6. Provide delegation evidence
7. Validate evidence
a. Authenticate AR + validate iSHARE certification
b. Authorise EP + validate iSHARE adherence
8. Authorise SC based on evidence
9. Execute service
10. Provide service results

M2M service provision including an app

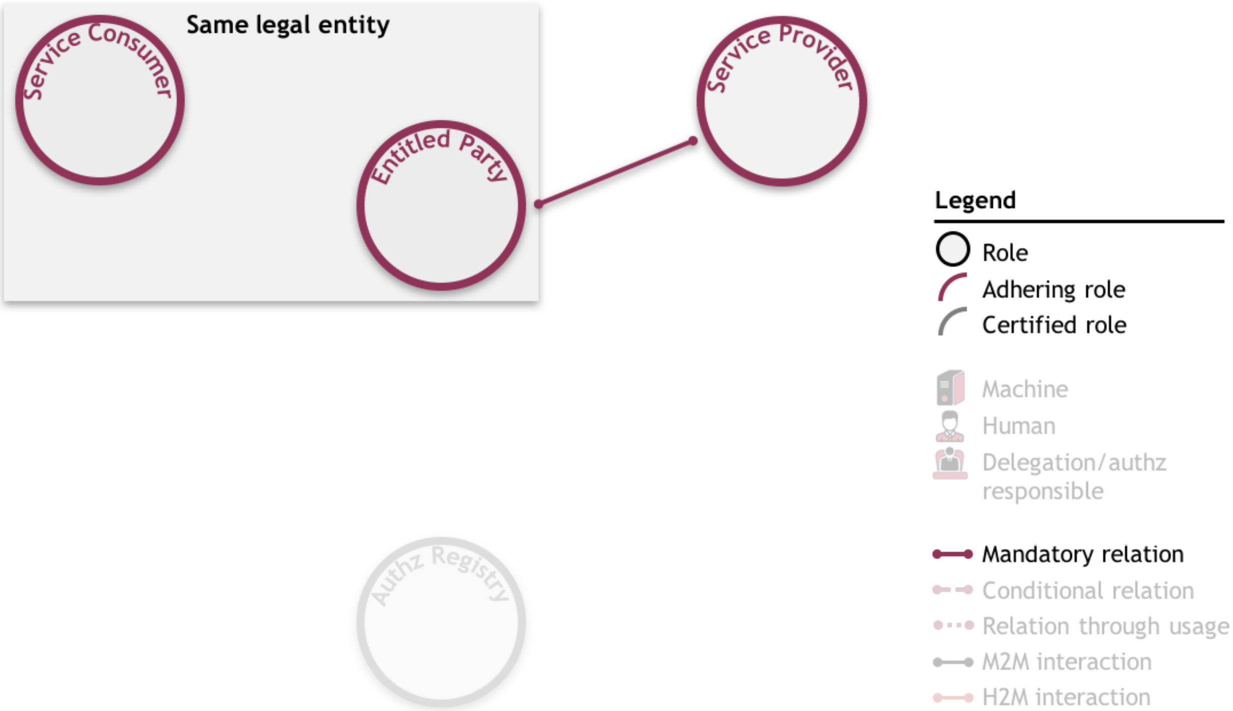
Use case 1 and its variations can be initiated by a Human Service Consumer through an app. In such case, the Machine Service Consumer acts as a proxy between the Human Service Consumer and the Service Provider's machine.

Roles

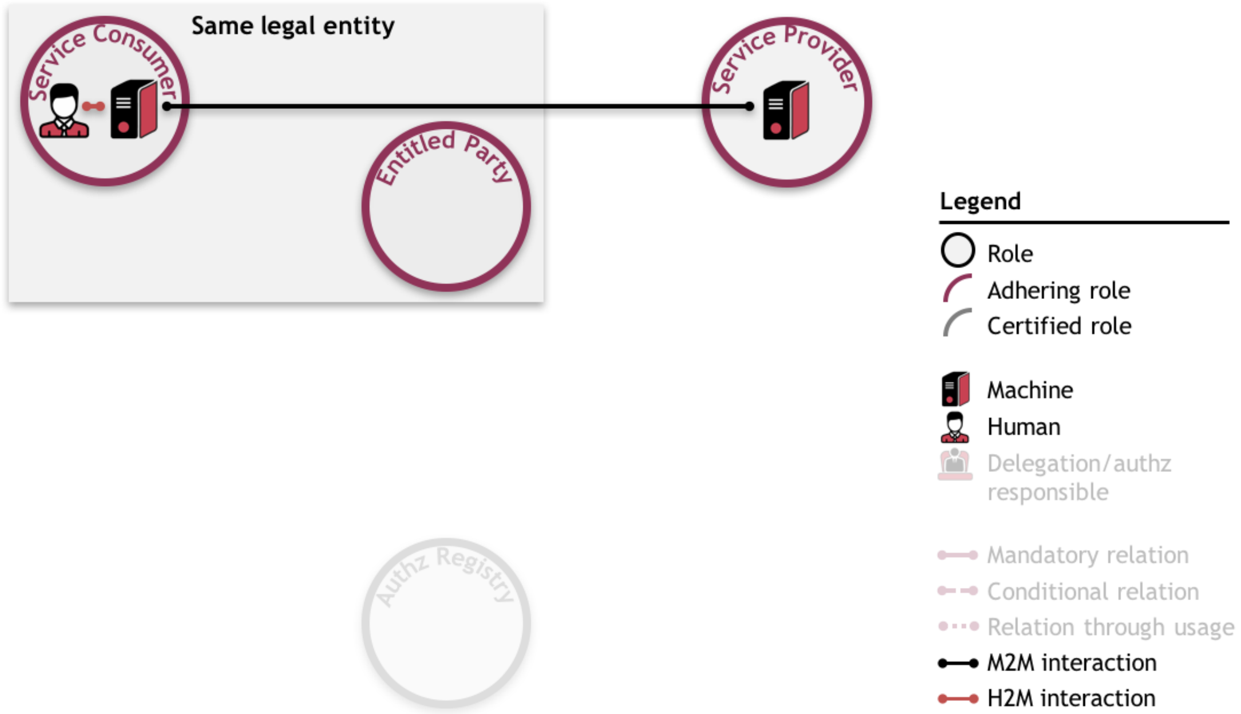
	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Use case variation	1	1a	1b	1c

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.

Sequence diagram

To follow.

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.

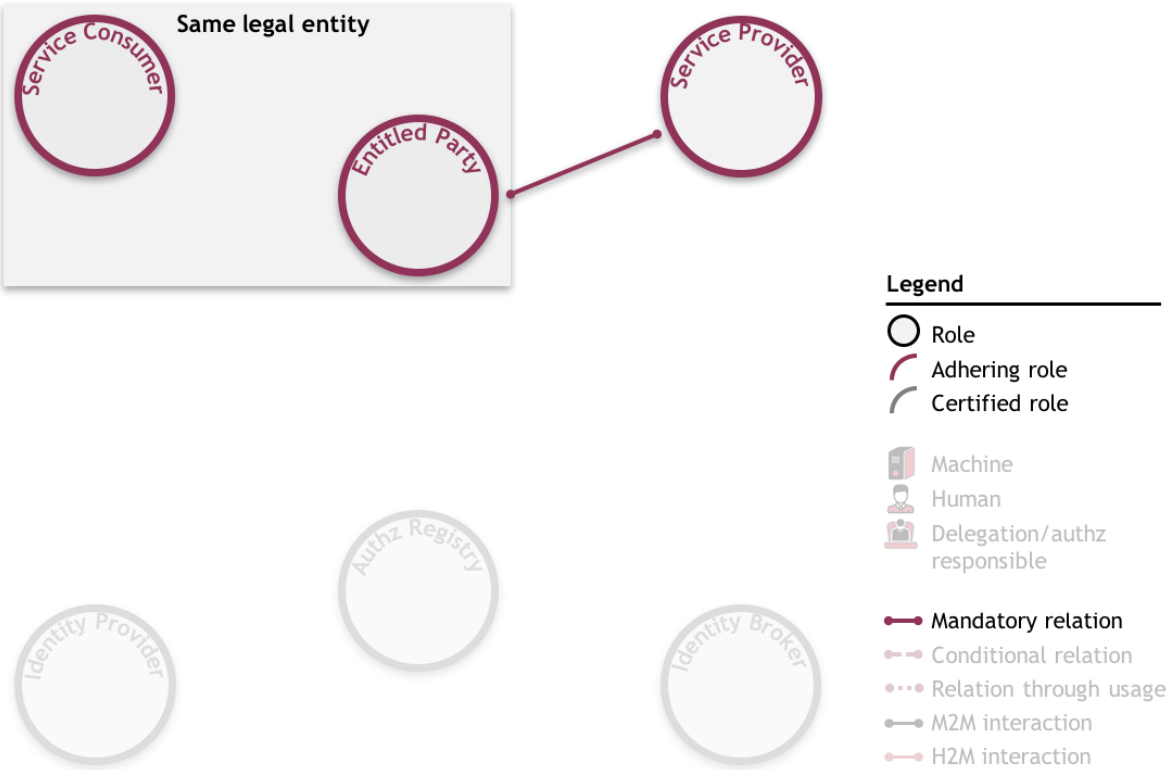
Roles

		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	2	2a	2b	2c

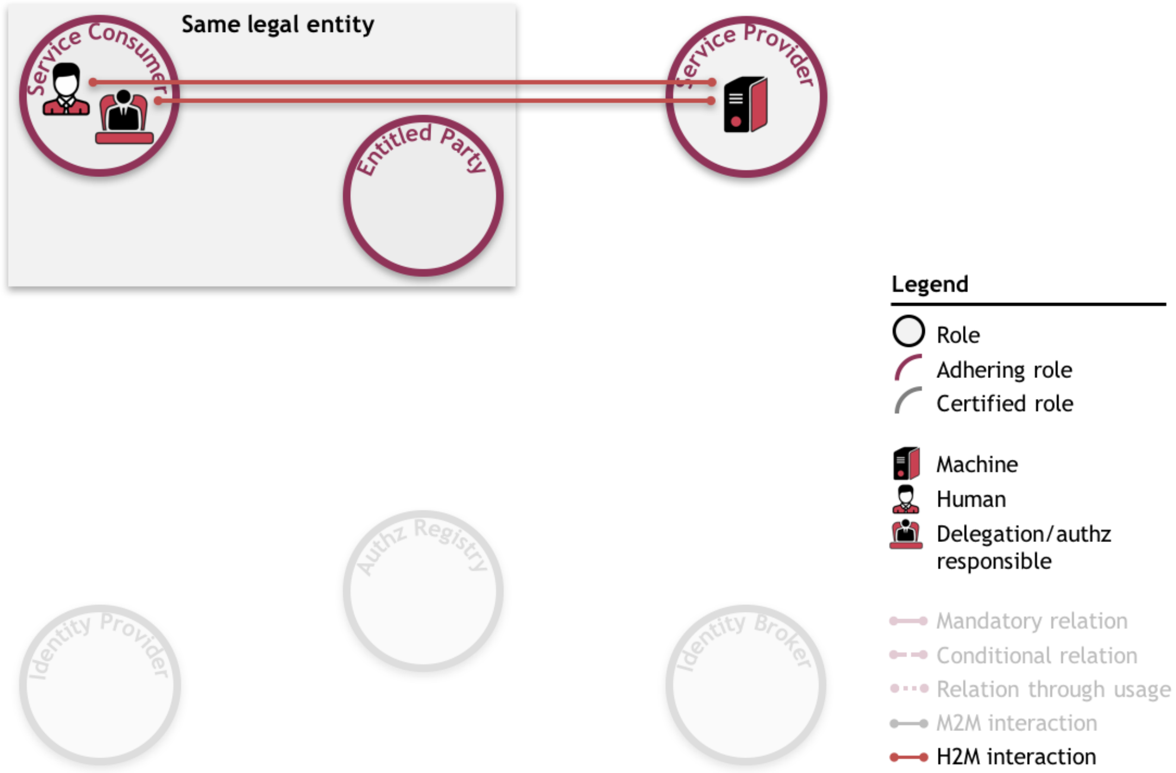
As no delegation takes place, the Entitled Party is also the Service Consumer.

Depiction

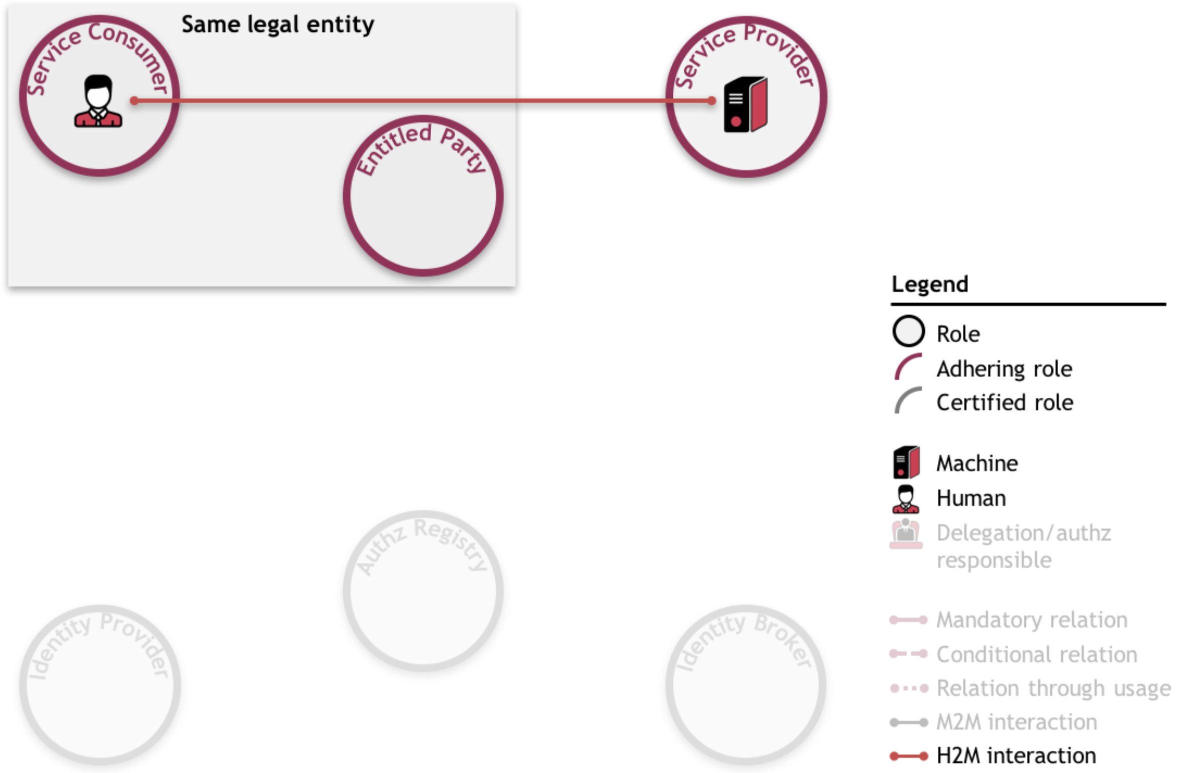
Legal relations



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.

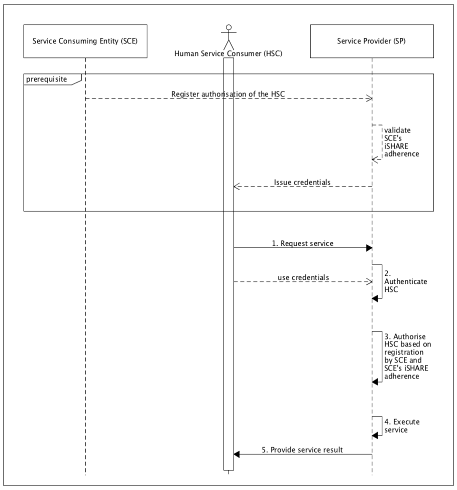
*The Service Provider can outsource this function to a third party
**The Service Consumer can outsource this function to a third party

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 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


Service Consuming Entity (SCE)
Human Service Consumer (HSC)
Service Provider (SP)
prerequisite
Register authorisation of the HSC
validate SCE's iSHARE adherence
Issue credentials
1. Request service
use credentials
2. Authenticate HSC
3. Authorise HSC based on registration by SCE and SCE's iSHARE adherence
4. Execute service
5. Provide service result

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	3a	3b	3c
	Entitled Party	3.1	3a.1	3b.1	3c.1
	Authorisation Reg	3.2	3a.2	3b.2	3c.2
	Identity Provider*	3.3	3a.3	3b.3	3c.3

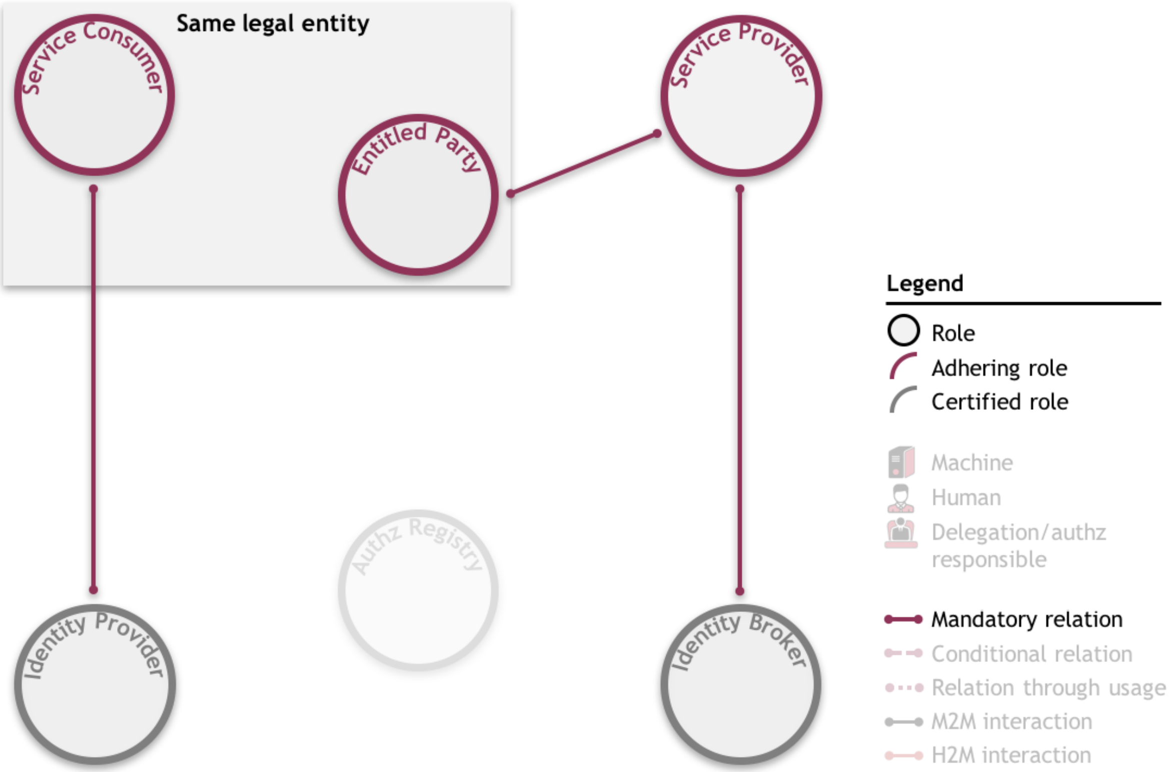
*The Identity Provider cannot hold explicit authorisation info, but it can hold info about a Human Service Consumer's identity that implies authorisation - i.e. 'working for truck company X'

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

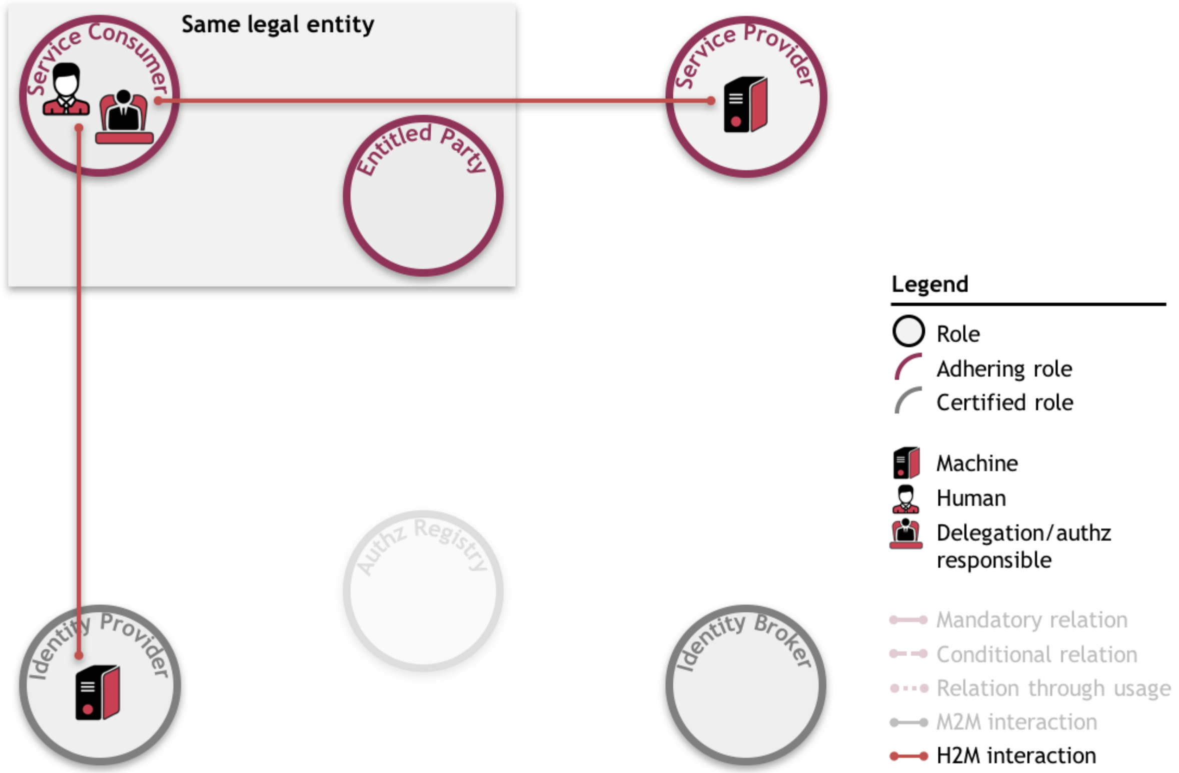
Note that an Identity Broker is introduced to broker the relation between the Service Provider and the Identity Provider(s) and/or the Service Provider and the Authorisation Registry(s). This is optional and useful in situations with several Identity Providers and/or Authorisation Registries.

Depiction

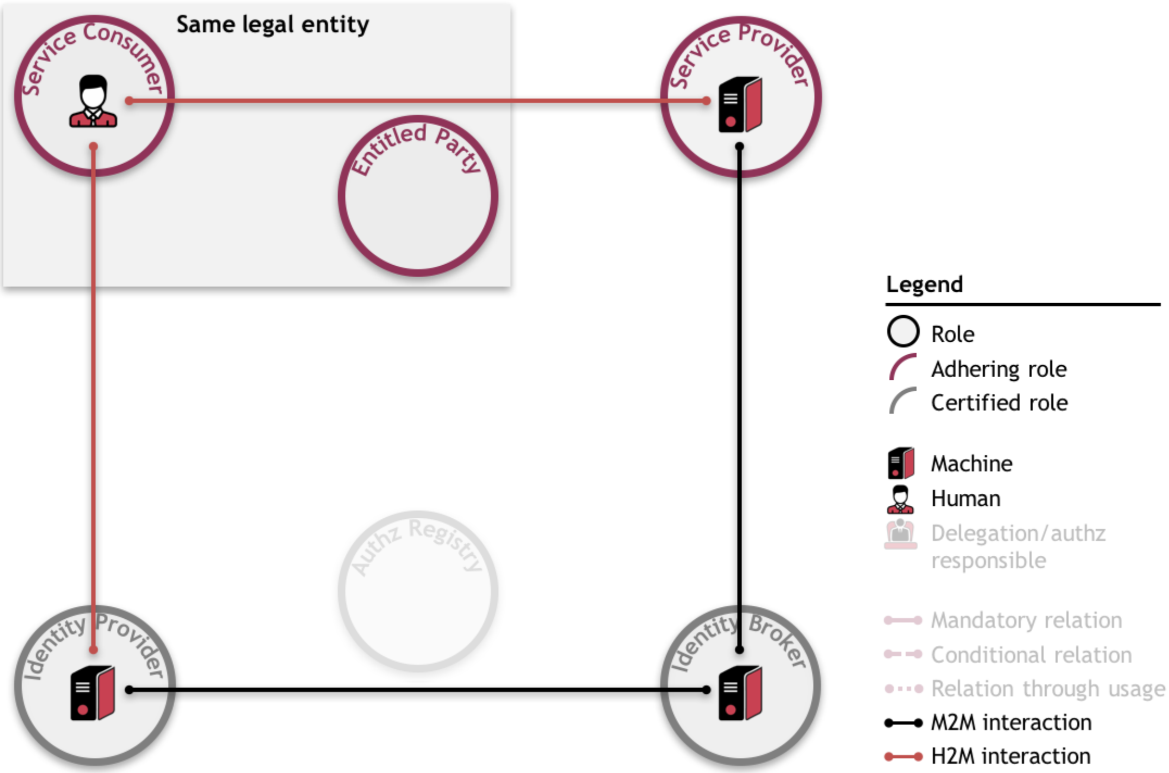
Legal relations



Prerequisite registration



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.

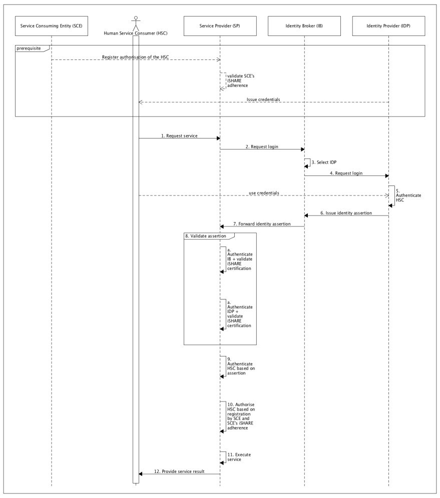
*The Service Provider can outsource this function to a third party

**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.

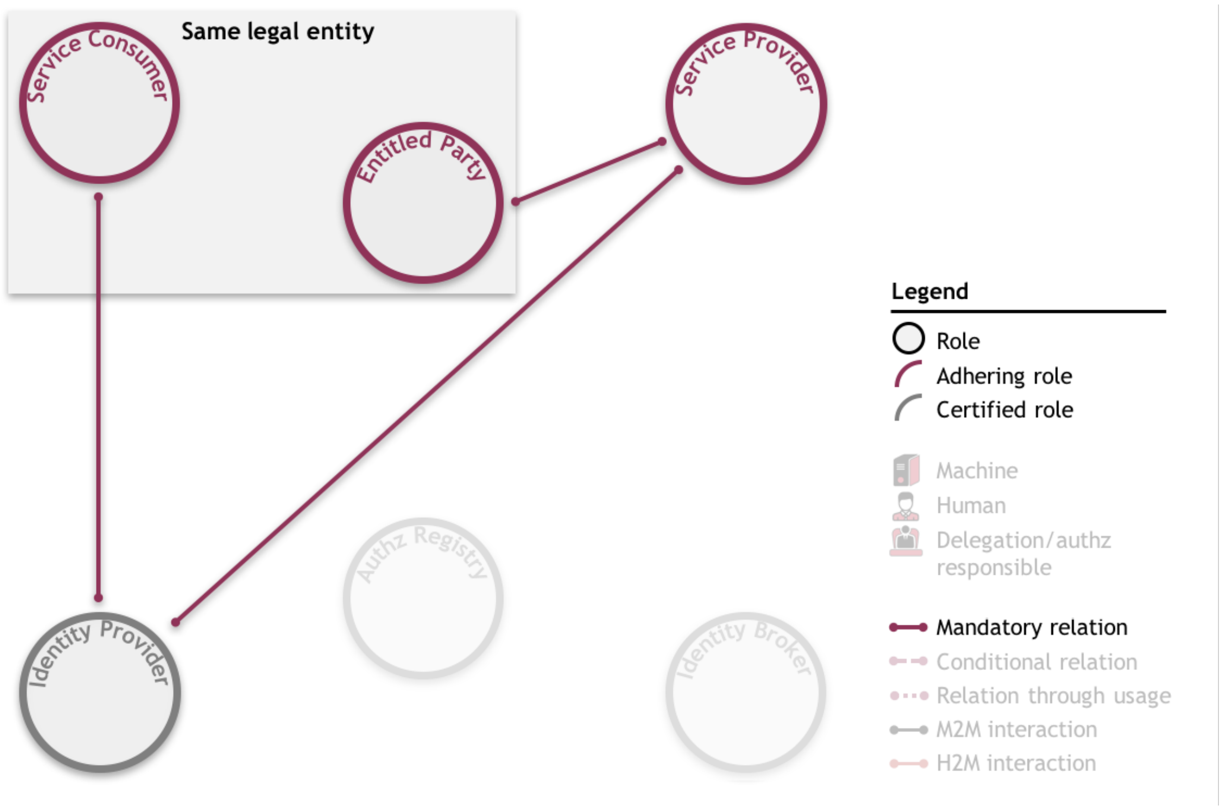
Sequence diagram


Service Consuming Entity (SCE)
Human Service Consumer (HSC)
Service Provider (SP)
Identity Broker (IB)
Identity Provider (IDP)
prerequisite
Register authorisation of the HSC
validate SCE's iSHARE adherence
Issue credentials
1. Request service
2. Request login
3. Select IDP
4. Request login
use credentials
5. Authenticate HSC
6. Issue identity assertion
7. Forward identity assertion
8. Validate assertion
a. Authenticate IB + validate iSHARE certification
a. Authenticate IDP + validate iSHARE certification
9. Authenticate HSC based on assertion
10. Authorise HSC based on registration by SCE and SCE's iSHARE adherence
11. Execute service
12. Provide service result

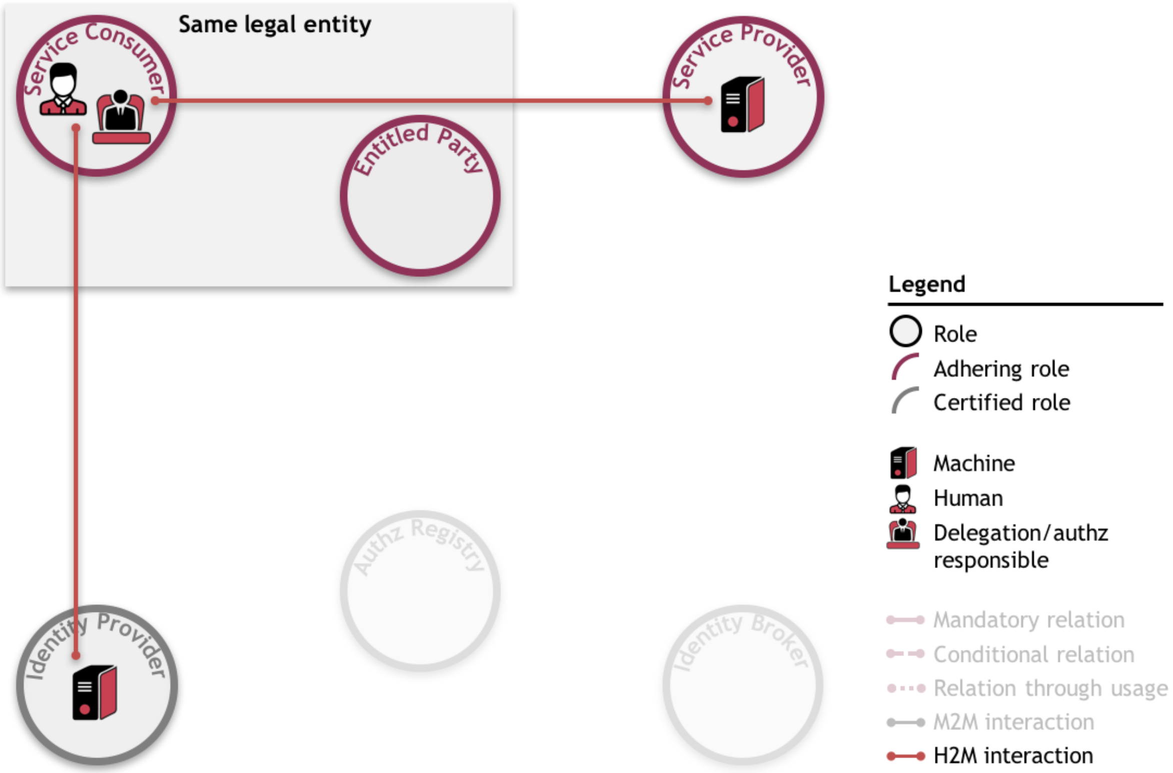
This use case would look as follows without an Identity Broker:

Depiction without Identity Broker

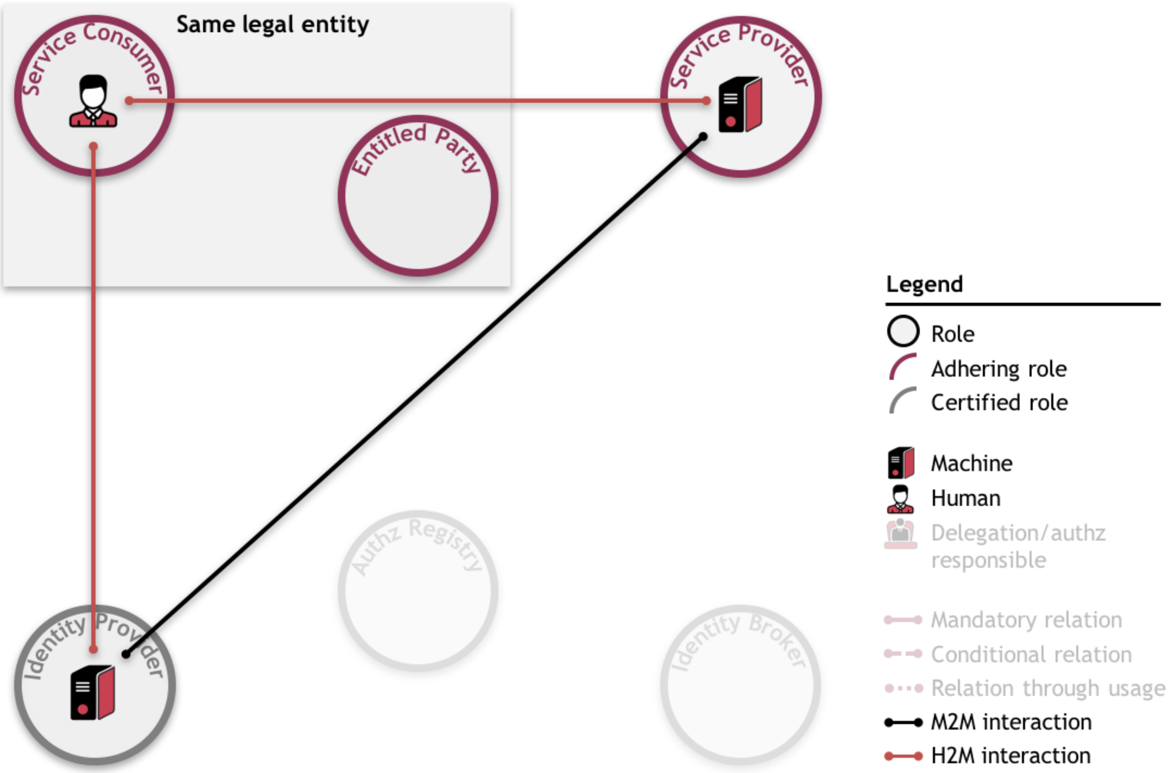
Legal view



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.

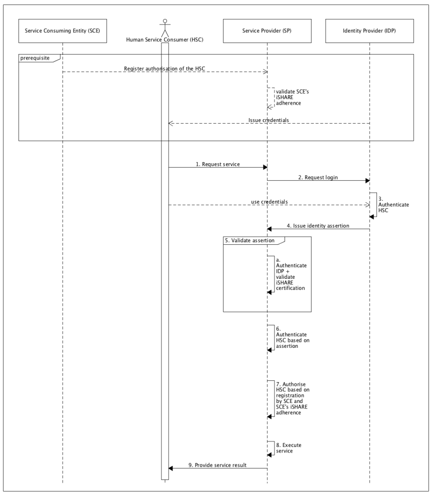
*The Service Provider can outsource this function to a third party

**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


Service Consuming Entity (SCE)
Human Service Consumer (HSC)
Service Provider (SP)
Identity Provider (IDP)
prerequisite
Register authorisation of the HSC
validate SCE's iSHARE adherence
Issue credentials
1. Request service
2. Request login
use credentials
3. Authenticate HSC
4. Issue identity assertion
5. Validate assertion
a. Authenticate IDP + validate iSHARE certification
6. Authenticate HSC based on assertion
7. Authorise HSC based on registration by SCE and SCE's iSHARE adherence
8. Execute service
9. Provide service result

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	3a	3b	3c

	Entitled Party	3.1	3a.1	3b.1	3c.1
	Authorisation Reg	3.2	3a.2	3b.2	3c.2
	Identity Provider*	3.3	3a.3	3b.3	3c.3

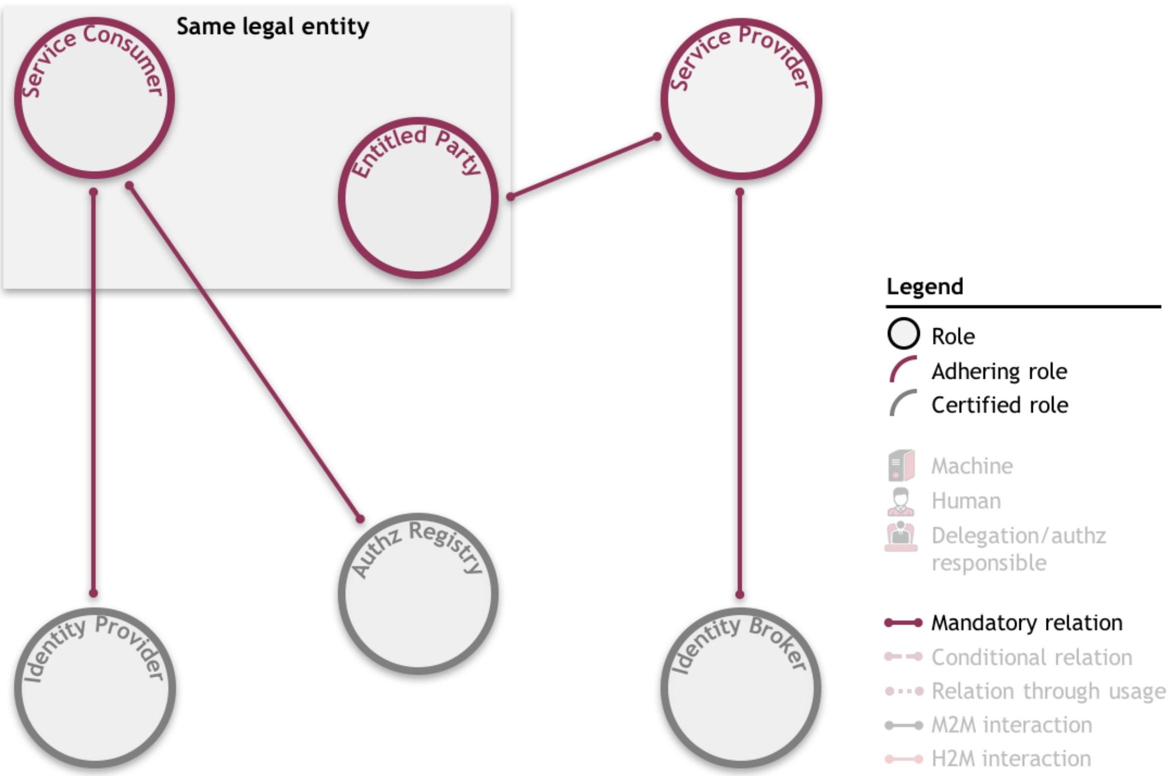
*The Identity Provider cannot hold explicit authorisation info, but it can hold info about a Human Service Consumer's identity that implies authorisation - i.e. 'working for truck company X'

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

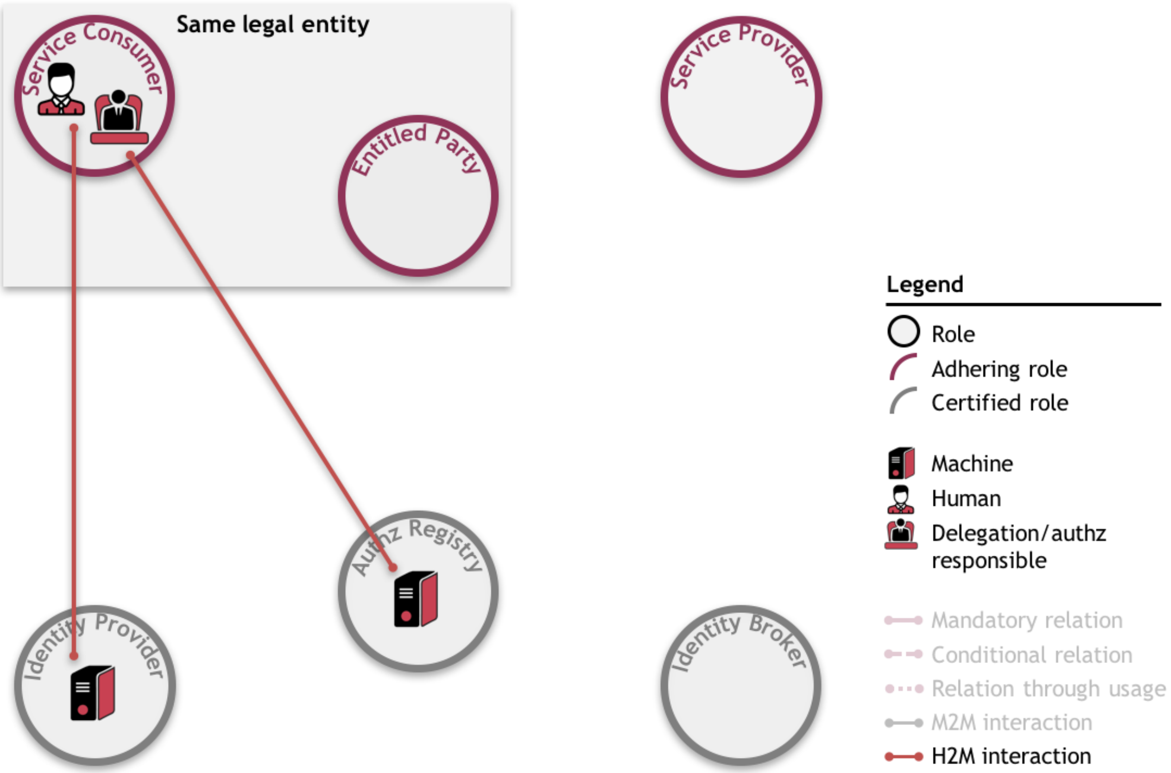
Note that an Identity Broker is introduced to broker the relation between the Service Provider and the Identity Provider(s) and/or the Service Provider and the Authorisation Registry(s). This is optional and useful in situations with several Identity Providers and/or Authorisation Registries.

Depiction

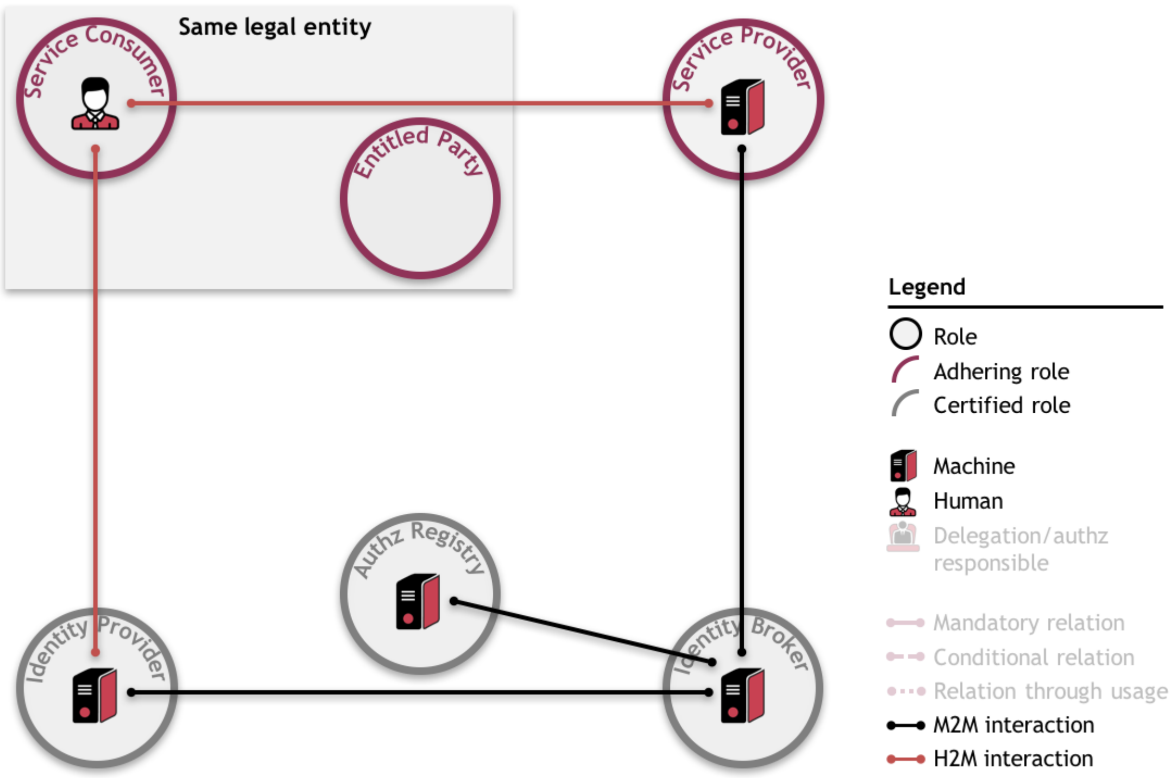
Legal relations



Prerequisite registration



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.

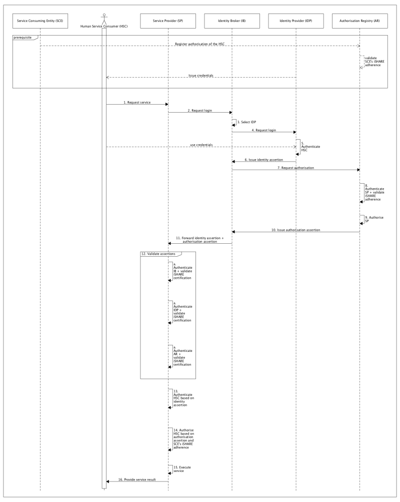
*The Service Provider can outsource this function to a third party

**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


Service Consuming Entity (SCE)
Human Service Consumer (HSC)
Service Provider (SP)
Identity Broker (IB)
Identity Provider (IDP)
Authorisation Registry (AR)
prerequisite
Register authorisation of the HSC
validate SCE's iSHARE adherence
Issue credentials
1. Request service
2. Request login
3. Select IDP
4. Request login
use credentials
5. Authenticate HSC
6. Issue identity assertion
7. Request authorisation
8. Authenticate SP + validate iSHARE adherence
9. Authorise SP
10. Issue authorisation assertion
11. Forward identity assertion + authorisation assertion
12. Validate assertions
a. Authenticate IB + validate iSHARE certification
a. Authenticate IDP + validate iSHARE certification
a. Authenticate AR + validate iSHARE certification
13. Authenticate HSC based on identity assertion
14. Authorise HSC based on authorisation assertion and SCE's iSHARE adherence
15. Execute service
16. Provide service result

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

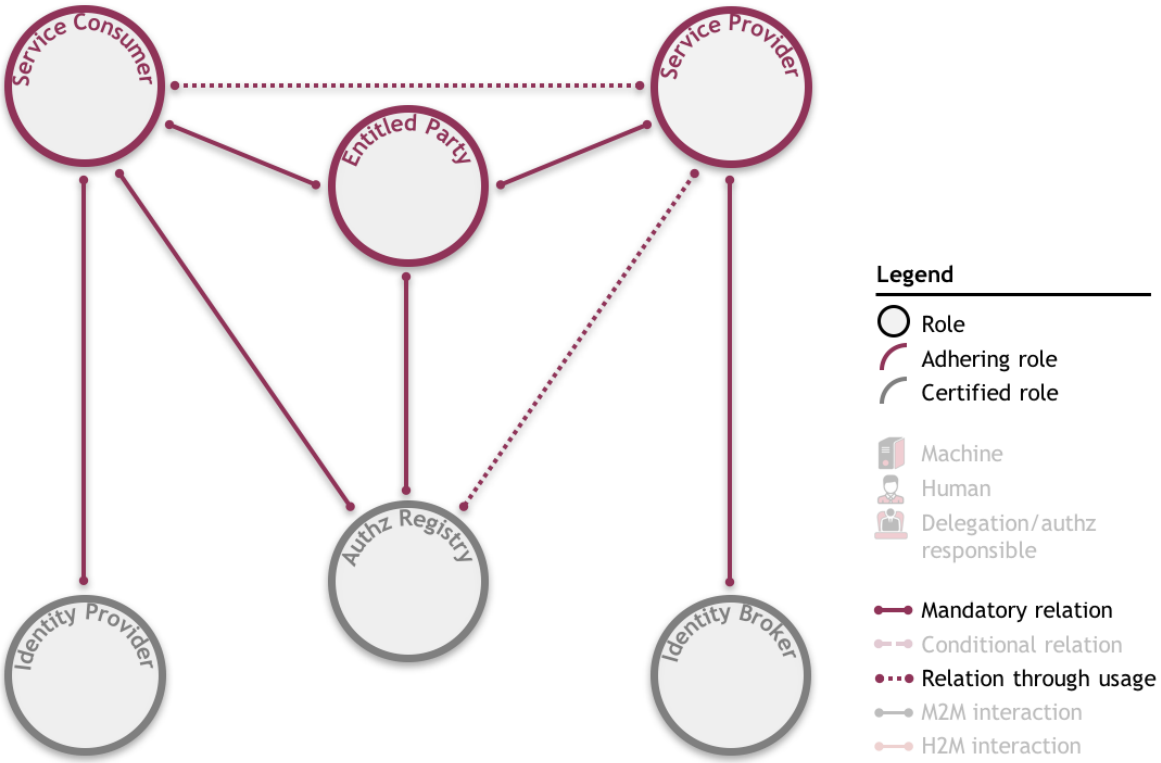
		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	3	3a	3b	3c
	Entitled Party	3.1	3a.1	3b.1	3c.1
	Authorisation Reg	3.2	3a.2	3b.2	3c.2
	Identity Provider*	3.3	3a.3	3b.3	3c.3

*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 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.

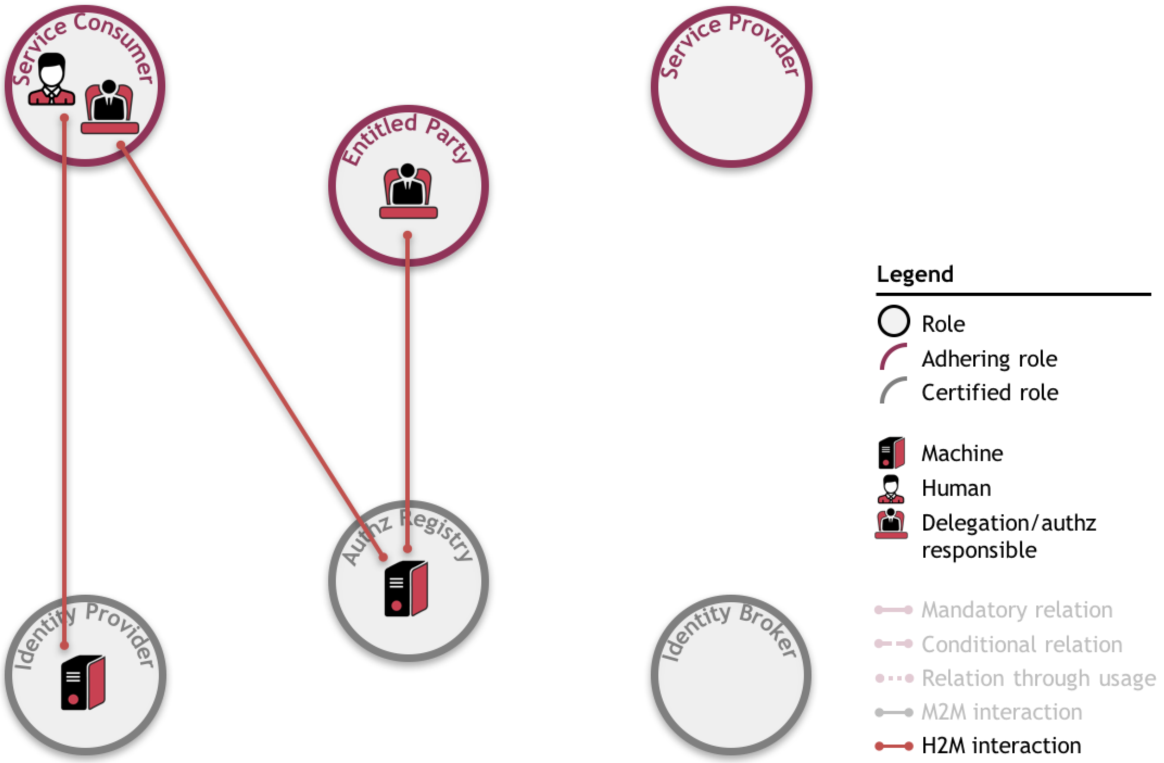
Depiction

Legal relations

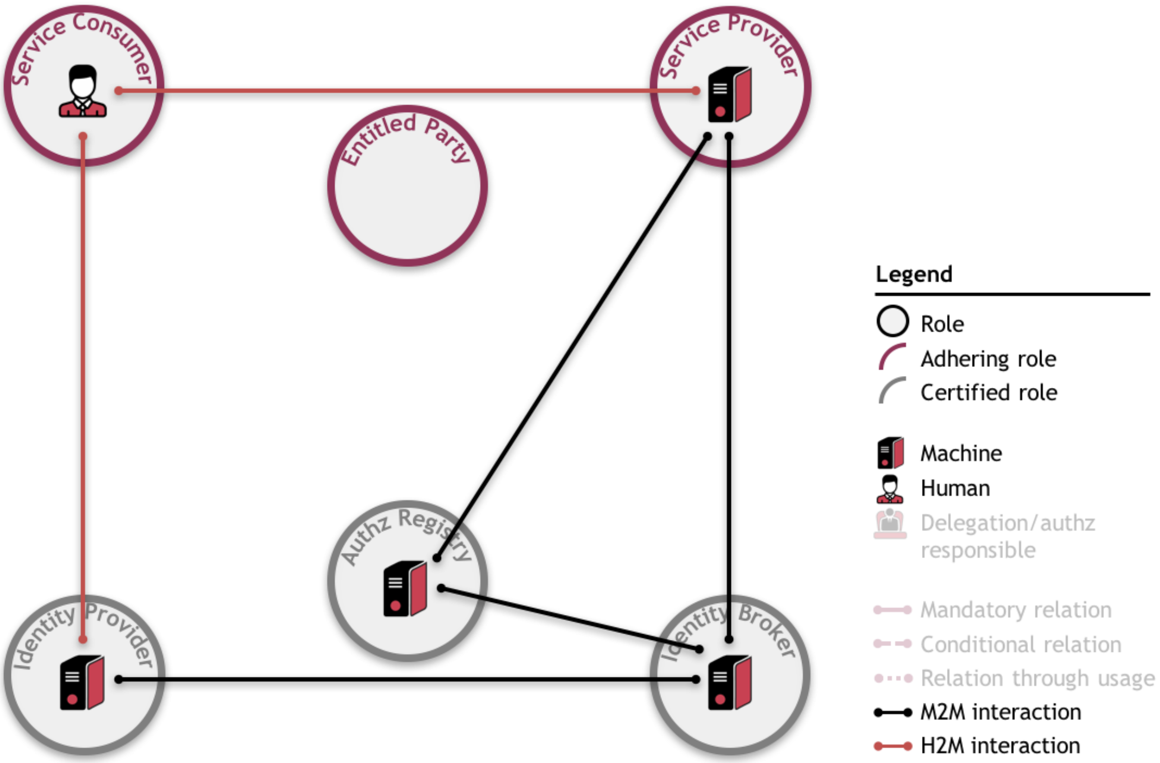


Note that no prior legal relation is exists between the Service Consumer and the Service Provider. Which services can be consumed by the Service Consumer, as delegated by the Entitled Party, is set out in the mandatory relation between this Entitled Party and the Service Provider.

Prerequisite registration



Use case interaction



Description

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;

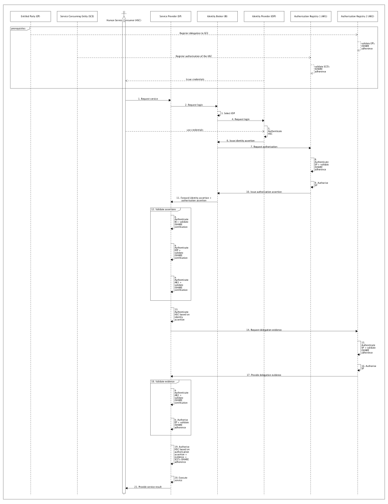
14. The Service Provider requests delegation evidence from Authorisation Registry 2;
15. Authorisation Registry 2 authenticates the Service Provider and validates its iSHARE adherence;
16. Authorisation Registry 2 authorises the Service Provider based on the scheme agreements for providing authorisation 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.

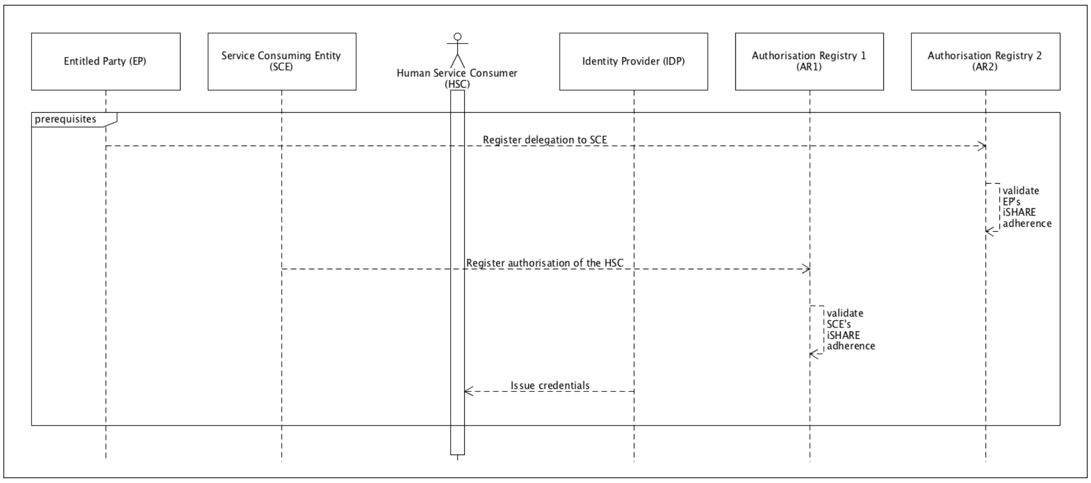
19. The Service Provider authorises the Human Service Consumer of the Service Consumer based on the validity of the delegation evidence;
20. The Service Provider executes the requested service;
21. The Service Provider provides the service result to the Human Service Consumer.

Sequence diagrams

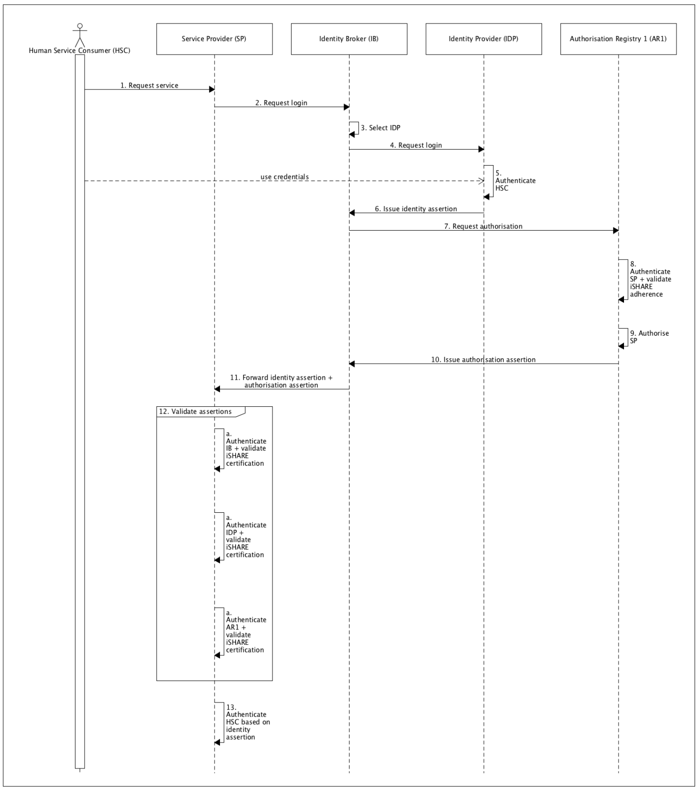
Total



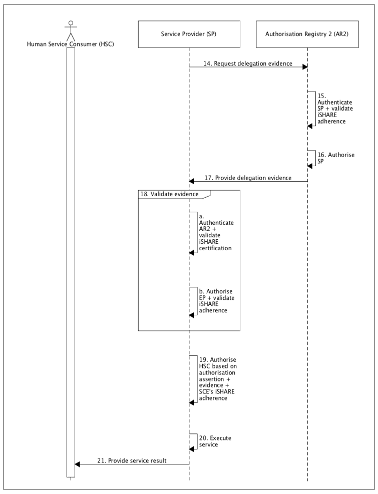
Prerequisites


Entitled Party (EP)
Service Consuming Entity (SCE)
Human Service Consumer (HSC)
Identity Provider (IDP)
Authorisation Registry 1 (AR1)
Authorisation Registry 2 (AR2)
prerequisites
Register delegation to SCE
validate EP's iSHARE adherence
Register authorisation of the HSC
validate SCE's iSHARE adherence
Issue credentials

Authentication and Authorisation


Human Service Consumer (HSC)
Service Provider (SP)
Identity Broker (IB)
Identity Provider (IDP)
Authorisation Registry 1 (AR1)
1. Request service
2. Request login
3. Select IDP
4. Request login
use credentials
5. Authenticate HSC
6. Issue identity assertion
7. Request authorisation
8. Authenticate SP + validate iSHARE adherence
9. Authorise SP
10. Issue authorisation assertion
11. Forward identity assertion + authorisation assertion
12. Validate assertions
a. Authenticate IB + validate iSHARE certification
a. Authenticate IDP + validate iSHARE certification
a. Authenticate AR1 + validate iSHARE certification
13. Authenticate HSC based on identity assertion

Delegation


Human Service Consumer (HSC)
Service Provider (SP)
Authorisation Registry 2 (AR2)
14. Request delegation evidence
15. Authenticate SP + validate iSHARE adherence
16. Authorise SP
17. Provide delegation evidence
18. Validate evidence
a. Authenticate AR2 + validate iSHARE certification
b. Authorise EP + validate iSHARE adherence
19. Authorise HSC based on authorisation assertion + evidence + SCE's iSHARE adherence
20. Execute service
21. Provide service result

Licenses

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

For a Service Consumer, the result of any of iSHARE’s primary use cases is consuming a service (for example: receiving data). Entitled Parties can specify what Service Consumers may and may not do with the result of a consumed service. For this purpose, **licenses** are introduced. A license contains statements about how a Service Consumer is supposed to use the result of a service it has consumed from a Service Provider. The license covering a service can consist of the following elements:

- LicensePurpose
    - A code indicating for what purpose the Service Consumer is allowed to use the received data
    - Optional, defaults to 0001, indicating resharing with iSHARE adhering parties*
- LicenseSubLicense
    - An integer indicating the number of times the Service Consumer can share the result with third parties
    - Optional, defaults to 9999
- LicenseEndDate
    - Within what timeframe the Service Consumer can keep and use the result of the service it has consumed
    - Optional, defaults to 9999-12-31

Establishing a license

Entitled Parties and/or Service Providers are responsible for establishing the license covering a service or services, either based on an agreement with a Service Consumer or unilaterally declared. Entitled Parties must register licenses at a PIP.

Entitled Parties can also choose *not* to establish a license; in this case a default applies - as described above.

Putting the license to use

Whenever a service is requested by a Service Consumer from a Service Provider, the request SHOULD include the requested LicensePurpose, as described in the technical interface specifications. The response from the Service Provider SHOULD include the LicensePurpose, LicenseSubLicense & LicenseEndDate for the license covering this specific service.

> ⚠ It is highly discouraged to set a LicenseEndDate since this puts high requirements on the implementation of the Service Consumer.

If *no* license is established by the Entitled Party and/or mentioned in the response from the Service Provider, the default license applies as described above. The details of licenses, and their legal value in case of a dispute, will be detailed in the Legal part of this scheme.

*During co-creation, it was suggested that the default should also include that the result of the service should not be used to damage the Entitled Party. This is a general requirement of service consumption, however, and will therefore be part of the Terms & Conditions for iSHARE adhering parties.

Purpose 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
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

Identifiers

Within iSHARE companies will mainly be identified by their Economic Operators Registration and Identification (EORI) number. The EORI number is used as an identifier for companies throughout the European Union. 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 number (Rechtspersonen en Samenwerkingsverbanden IdentificatieNummer). If the NL-RSIN contains less than 9 digits, the EORI is prefixed with 0's. For more information on the EORI number, please consult the European EORI website. For more information on the EORI for Dutch parties, please consult the website of the Dutch tax authorities.

If no EORI is available, it is alternatively allowed for Dutch entities to use the unique Chamber of Commerce number as alternative identifier.

Secondary use cases

iSHARE's three primary use cases are supported by seven secondary use cases. These include:

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

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

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 (with the Scheme Owner)

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.

Functional requirements per role

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

The functional requirements per role will be summarised and made explicit in the next iteration of the iSHARE scheme. They can already be found (implicitly) throughout the Roles & Responsibilities and primary use cases.

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 and 3, an interface is required. This interface MUST comply with the following guidelines:

- The name of the party 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 guidelines (Communication guidelines have not yet been determined).
- Users 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 users verify that they are not being tricked?

Technical

This section covers the technical details of the iSHARE scheme.

The section starts out with a chapter containing the basic API specifications, including an example implementation based on use case 1c. The chapter also includes role specific API requirements and the APIs that are exposed by the Scheme Owner.

The chapter on "Language of delegation and authorisation" explains how the process of delegation and authorisation are implemented within the iSHARE scheme.

The section then ends with an overview of relevant technical standards.

Interface specifications

This part of the iSHARE scheme and all its sub-parts are considered normative and are therefore compliant with RFC 2119.

API specifications on SwaggerHub

Note that, although this specification should be complete, a complete overview of the current iSHARE API specifications (work in progress) can be found here on SwaggerHub.

Please note that in case of contradictions the specifications on Confluence prevail over those on SwaggerHub

Interface specifications on Confluence

The iSHARE interface specifications are structured as follows:

- Generic specifications
    - HTTP methods
    - Party identifiers
    - Dates and times
    - Caching
    - Response codes
- API security
    - Generic /oauth2.0/token
    - Generic /ishare1.0/delegation
    - Generic use of OpenID Connect 1.0
    - Generic iSHARE JWT specifications
- Processing delegation evidence
- Scheme Owner APIs
    - Scheme Owner /oauth2.0/token
    - Scheme Owner /ishare1.0/parties/{party_id}
    - Scheme Owner /ishare1.0/parties/certified_parties
    - Scheme Owner /ishare1.0/trusted_list
    - Scheme Owner /ishare1.0/certificate_validation
- API example use case 1c
- Role specific API requirements

- The iSHARE JWT for iSHARE enabled services

Generic specifications

This page contains the generic specifications for iSHARE APIs.

- HTTP methods
- Party identifiers
- Dates and times
- Caching
- Response codes

HTTP methods

The iSHARE API makes use of standard HTTP methods inspired by the RESTful architectural style. Standard CRUD operations are mapped to standard HTTP methods in the following table:

HTTP Verb	CRUD
POST	Create
GET	Read
PUT	Update/Replace
PATCH	Update/Modify
DELETE	Delete

Party identifiers

Except for the Scheme Owner, all parties within iSHARE SHOULD be uniquely identified by their EORI number.

For those parties that not possess and cannot obtain an EORI number additional numbers may be specified.

The Scheme Owner is identified by the `common name` field in the certificate used by the Scheme Owner that is published here.

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

Dates and times

In iSHARE all dates and times MUST be communicated in UTC time.

All dates and times MUST be formatted in the Unix timestamp format.

Caching

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

Response codes

Within the iSHARE scheme, the HTTP standard concerning response codes is followed as established by the IETF. Please refer to the IETF website 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..
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.

API security

Organisations participating in the iSHARE scheme need to consider aspects of security. Depending on the character of services and data of an organisation, appropriate security measures need to be taken. Please refer to the following glossary topics for more guidance on security:

- Confidentiality
- Integrity
- Authenticity
- Availability
- Non-repudiation

iSHARE specific security specifications

For the purpose of authenticating parties interacting through APIs (M2M) PKI certificates are used.

For the purpose of confidentiality all HTTPS connections MUST be secured by TLS 1.2 using general purpose TLS certificates.

iSHARE uses OAuth 2.0 for all basic API access control. OAuth 2.0 is used in iSHARE M2M use cases directly and as part of OpenID Connect 1.0 in iSHARE H2M use case.

iSHARE uses OpenID Connect 1.0 for all authentication of Human Service Consumers in iSHARE H2M use cases.

In case non-repudiation is required (so in several cases) iSHARE uses signed JSON Web Tokens (JWTs).

Common security APIs

iSHARE specifies the following common security APIs that are used by multiple roles:

- `/oauth2.0/token` - used for obtaining an OAuth 2.0 access token

- `/ishare1.0/delegation` - used for obtaining delegation evidence

For purposes of consistency and ease of maintenance these APIs are specified only once. Optional additional requirements are specified on a per role basis.

Generic /oauth2.0/token

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

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

[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.

Request

The request contains the following parameters:

Parameter	Contained in	Type	Required	Description
`grant_type`	query	string	Yes	OAuth 2.0 grant type. MUST contain “client_credentials”
`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
`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”
`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
`authorisation_registry`	query	string	No	iSHARE specific identifier of the Authorisation Registry that SHOULD be queried by the server for additional authorisation/delegation rights of the client

Generic /oauth2.0/token request example

```
GET /oauth2.0/token HTTP/1.1
Host: example.server.com

grant_type=client_credentials&scope=iSHARE&client_id=EU.EORI.NL123456789&client_assertion_type=urn%3Aietf%3
Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer&client_assertion=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6Ik1JSUdDRENDQS9DZ0F3SUJBZ0lDRUFRd0RRWUpLb1pJaHZjTkFRRUxCUUF3Z1p
BeEN6QUpCZ05WQkFZVEFrNU1NUXN3Q1FZRFZRUUlEQUpPU0RFUE1BMEdBMVVFQ2d3R2FWTklRVkpGTVJFd0R3WURWUVFMREFoVFpXTjFjbW
wwZVRFb01DWUdBMVVFQXd3ZmFWTklRVkpGSUU1TUlFTmxjblJwWm1sallYUmxJRUYxZEdodmNtbDBlVEVtTUNRR0NTcUdTSWIzRFFFSkFSW
VhhVzVtYjBCcGMyaGhjbVV0Y0hKdmFtVmpkQzV2Y21jd0hoY05NVGN3TmpJM01EZ3lPVEl6V2hjTk1UZ3dOekEzTURneU9USXpXakNCbkRF
TE1Ba0dBMVVFQmhNQ1Rrd3hDekFKQmdOVkJBZ01BazVJTVJJd0VBWURWUVFIREFsQmJYTjBaWEprWVcweER6QU5CZ05WQkFvTUJtbFRTRUZ
TUlRFUk1BOEdBMVVFQ3d3SVUyVmpkWEpwZEhreElEQWVCZ05WQkFNTUYybFRTRUZTUlNCVFkyaGxiV1VnVDNkdVpYSWdVRTlETVNZd0pBWU
pLb1pJaHZjTkFRa0JGaGRwYm1adlFHbHphR0Z5WlMxd2NtOXFaV04wTG05eVp6Q0NBU0l3RFFZSktvWklodmNOQVFFQkJRQURnZ0VQQURDQ
0FRb0NnZ0VCQUxwMVlrMGN1NlU3TTEzbWNRdXBXaitUQUR5L2h3RUhXbW1HR0ZGUmFMTVVSdXVqRHNLQ0hldTg5THZxNzFRUVdreHhKV0FI
UDZvUmUzVUN6Q2RNalhoNlBvRVFubnlDM2RVZ1gzcEdqUUcxb1QwYTd0eU1kTVd6QVc5Mk1KVzJCRjhQN1pSTWxEc2tmN0JKaDFRUHJGL3A
1MytTMHVleFpOTlNCMy9aWmpMcGFudElMM2lGOW14UEtCSlgyYzVkWTY2NnJ0MytmYWRMaEdmMEF0Rzk1ME02QlYzR21NTmJ4OHNOUVYraE
NRME9lSWlyaGtJaSswOG92Y0hURTdEUDcrM0JCMmVkRG9DZ1NYU3RMSHJvZEI4d1pCQkdMQmdtN3RxY0R6NXBrYURldElyc1lLTlhRcUVSR
mpVMlRZdXJCbG5sbDY0cGNlL1NPVWl5K0tEeGhqY0NBd0VBQWFPQ0FWd3dnZ0ZZTUFrR0ExVWRFd1FDTUFBd0VRWUpZSVpJQVliNFFnRUJC
QVFEQWdaQU1ETUdDV0NHU0FHRytFSUJEUVFtRmlSUGNHVnVVMU5NSUVkbGJtVnlZWFJsWkNCVFpYSjJaWElnUTJWeWRHbG1hV05oZEdVd0h
RWURWUjBPQkJZRUZCRWRLWjYxaHBNK1pETE5XTEtsYnhiQmxJVm9NSUcrQmdOVkhTTUVnYll3Z2JPQUZJNUdUZE1VaWFwWEltVlVpOVQyMV
pzQ045enJvWUdXcElHVE1JR1FNUXN3Q1FZRFZRUUdFd0pPVERFTE1Ba0dBMVVFQ0F3Q1RrZ3hFakFRQmdOVkJBY01DVUZ0YzNSbGNtUmhiV
EVQTUEwR0ExVUVDZ3dHYVZOSVFWSkZNUkV3RHdZRFZRUUxEQWhUWldOMWNtbDBlVEVVTUJJR0ExVUVBd3dMYVZOSVFWSkZJRkp2YjNReEpq
QWtCZ2txaGtpRzl3MEJDUUVXRjJsdVptOUFhWE5vWVhKbExYQnliMnBsWTNRdWIzSm5nZ0lRQURBT0JnTlZIUThCQWY4RUJBTUNYUF3RXd
ZRFZSMGxCQXd3Q2dZSUt3WUJCUVVIQXdFd0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dJQkFBTm0wUUh0c2Jma1ZxeHI2akpndER2dklHUXFtdX
J5TXB1ZTFMb2c2SFpaMlFvd1pXckc4by80U0FnbHBNUFR1VlUwVWZBQms1ZFZmT1hubUJhNWxSTUk3aGw5ZFNNMUhObGU2QzlXQTdSUXROV
i92NHFCZTBPbGdmYUQ0Y1VBSkRrSHNJd1dTWxjZWxPb3hWWk5jZE93YWRYQVFIZ1lkdXpCU2RSOC9QczNwbHZJRElFOWxyR3Q3R2tVenhT
M1dVMVhWc3M2bktaRldsWmt0cVFINVkrV0VHLy82MCsxV2Y0YUk2VkhJdW9SajEwL05sRXZqY3QwWngweWlaVTJScnF3UHFzcnRCWWJDUEl
1TytDbDlRTTczcEhZM3pZcWtXWTRDTGFld3Z5UFphWTVLREJoN25aT3A5TkoxWjJYV0Z1VklEVFpSZUgyQVJYRnBrV0RhSG1oQWNNWjlCaX
FNK2h4NElYZUM2OFZ2d3VhK2d1eXBQSlpmUnlFMzNzb3gvbHU4ZWNMMkw3L2VoRGdqaThJRVN5bVVQSTMyQ3BLZk1OMUtLTkwvS0V0ZnRHU
HB1Vis2aVFOVEU0aFRDQmNCYVNmM2R4c0dIY2xPU0M2S2U5dEw0WVJMaVgzK1lzSHFZRDk4dkxSUk9iSVFaR1dYaXF2U0ZzTEN3SzBNMVJJ
d3NmYjZCOVMrWE1SQWl3cjFpZXpCZEh4WGFIODFsVCtXeEpmbkR1bjZ1eFhVejR4VHV6YVZYc1YwZ3ZjWTNxdVlwNjRMUjZScmhuYzJEa05
EelpVNkpIeUY3TFg3MHJuOExxqMTgwampHMWdlNmxsOURMUFFUa1Z5U2hUcUNVVis5d3JVMmFFMTZycWUyWUFxL2xMSjBkV09IUzJwSmNRam
gxaURwQXFHT2J3VCJ9.eyJpc3MiOiJFVS5FT1JJLk5MMTIzNDU2Nzg5Iiwic3ViIjoiRVUuRU9SSS5OTDEyMzQ1Njc4OSIsImF1ZCI6Ik5M
LktWSy4xMjM0NTY3OCIsImp0aSI6IjM3OGE0N2M0LTI4MjItNGNhNS1hNDlhLTdlNWExY2M3ZWE1OSIsImV4cCI6MTUwNDY4MzQ3NSwiaWF
0IjoxNTA0NjgzNDQ1fQ.gsVfvaTpjIf_ZkeYRqvkV14WqxROLsFSNeuAdw73v94FXKbjWHk0MFfgUCFy1J-dQQSMmY-
ixmvb1nHsKwNcpAUNI1ZTIf3N8MCrblwQqcLzROPDKOaL4FCdqxcv1oTX_p36jWNErxRDpIm5duIL601wiMjERFZMY7vXfMfqt2k&author
isation_registry=EU.EORI.NL000000001
```

Response

The response contains a JSON object with following parameters:

Parameter	Type	Required	Description
`access_token`	string	Yes	OAuth2.0 access_token. As determined by the server

`token_type`	string	Yes	OAuth2.0 token type. MUST contain "bearer"
`expires_in`	int	Yes	OAuth2.0 expiration time of the token. Access tokens SHOULD expire within 3600 seconds by default. Depending on scope and sensitivity of services, servers MAY choose to limit the expiration period. Access token expiration beyond 3600 seconds is discouraged

Generic /oauth2.0/token response example

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "access_token": "AGxpJB7hl9tooi8AUlLpncK1Kih5beXbjnbeODHp2EN48UO9BDpvtgScFO5aIXwH9T",
  "token_type": "bearer",
  "expires_in": 3600
}
```

Generic /ishare1.0/delegation

- For interoperability reasons clients SHALL only make `HTTP GET` calls to all OAuth `/token` and iSHARE `/delegation` endpoints. (Services are free to implement other HTTP verbs)

Generic use of OpenID Connect 1.0

Used to obtain identity information for a human subject

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

Generic OpenID Connect 1.0 requirements

In addition to the endpoint specifications below, for all uses of OpenID Connect 1.0 the following requirements apply:

- Clients MUST NOT be pre registered. See Generic /oauth2.0/token for more details.
- 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

Endpoints

For use of OpenID Connect 1.0 the following endpoints are specified:

- Generic /openid_connect1.0/authorize
- Generic /openid_connect1.0/token
- Generic /openid_connect1.0/userinfo

Generic /openid_connect1.0/authorize

Used to obtain a grant from the Human Service Consumer

Request

The request contains the following parameters:

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. MUST be identical to the `response_type` value in the `request` JWT.
`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. MUST be identical to the `client_id` value in the `request` JWT.
`scope`	query	string	Yes	OAuth 2.0 scope for OpenID Connect 1.0. MUST contain the 'openid' scope value and one or more scopes identifying the attributes from the Human Service Consumer that are requested. Supported scopes under iSHARE are described below. MUST be identical to the `scope` value in the `request` JWT.
`request`	query	string	Yes	OpenID Connect 1.0 signed JWT containing all request parameters. See below for JWT contents. See also Generic iSHARE JWT specifications for a.o. basic content and signing requirements.

Other request parameters SHOULD be ignored.

The `request` JWT MUST be composed, formatted and signed conform Generic iSHARE JWT specifications. In addition to the parameters specified there, the `request` JWT payload contains the following parameters:

Parameter	Type	Required	Description
`response_type`	string	Yes	OAuth 2.0 Response Type. For iSHARE using the Authorization Code Flow, with value 'code' is REQUIRED. MUST be identical to the `response_type` value in the query parameter.
`client_id`	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. MUST be identical to the `client_id` value in the query parameter.
`scope`	string	Yes	OAuth 2.0 scope for OpenID Connect 1.0. MUST contain the 'openid' scope value and one or more scopes identifying the attributes from the Human Service Consumer that are requested. Supported scopes under iSHARE are described below. MUST be identical to the `scope` value in the query parameter.
`redirect_uri`	string	Yes	OpenID Connect 1.0 redirection URI to which the response will be sent. Note that by transporting the `redirect_uri` in a signed JWT, security considerations regarding un-pre-registered `redirect_uri`'s are properly addressed.
`state`	string	Yes	OpenID Connect 1.0 opaque value used to maintain state between the request and the callback. MUST be used in iSHARE
`nonce`	string	Yes	OpenID Connect 1.0 value used to associate a Client session with an ID Token. MUST be used in iSHARE
`language`	string	No	iSHARE specific two-letter indicator that guides the language of the user interface shown by the Identity Broke or Identity Provider

Example request 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,
  "response_type": "code",
  "client_id": "EU.EORI.NL123456789",
  "scope": "openid name contact_details",
  "redirect_uri": "https://example.client.com/openid_connect1.0/return",
  "state": "af0ifjsldkj",
  "nonce": "c428224ca5a",
  "language": "nl"
}
```

Within iSHARE the following scopes for Open ID Connect 1.0 are defined:

TODO: Check against common used standards (GS-1?)

scope	included attribute	description
name	first_name	
	initials	
	middle_name	
	last_name	
	gender	
contact_details	personal_email	
	personal_email_verified	
	personal_phone	
	personal_phone_verified	
	personal_address	
	personal_postal_code	
	personal_city	
	personal_province	
	personal_country	
company_id	company_id	
company_info	company_name	
	company_type	
	company_email	

	company_phone	
	company_url	
	company_address	
	company_postal_code	
	company_city	
	company_province	
	company_country	

Note: a personal_email or personal_phone MUST NOT be confused with a private email/phone. It is personal in a business context.

Generic /openid_connect1.0/authorize request example

```
GET /openid_connect1.0/authorize HTTP/1.1
Host: example.server.com

response_type=code&client_id=EU.EORI.NL123456789&scope=openid%20name%20contact_details&request=<jwt value>
```

Response

Note: the request is a redirect of the Human Service Consumer to the Identity Broker / Identity Provider. There is no real-time response. The response described here is the redirect back to the `redirect_uri` of the client requesting the grant.

The response contains the following parameters:

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.

Generic /openid_connect1.0/authorize request example

```
GET /openid_connect1.0/return HTTP/1.1
Host: example.client.com

code=Lzvo6o5fLCCquSNrnSpc&state=af0ifjsldkj
```

Generic /openid_connect1.0/token

Used to obtain both an OAuth access token and an OpenID Connect id token

Except for details below, all requirements for Generic /oauth2.0/token apply.

Request

Compared to the request specifications in Generic /oauth2.0/token, the request changes one, adds one and removes two parameter (changes marked in red):

Parameter	Contained in	Type	Required	Description
grant_type	query	string	Yes	OAuth 2.0 grant type. MUST contain "authorization_code"
~~scope~~	~~query~~	~~string~~	~~Yes~~	~~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
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"

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
~~authorisation_registry~~	~~query~~	~~string~~	~~No~~	~~iSHARE specific identifier of the Authorisation Registry that SHOULD be queried by the server for additional authorisation/delegation rights of the client~~
code	query	string	Yes	Oauth 2.0 authorization code. MUST contain value of authorisation code received from the Identity Broker or Identity Provider

Generic /openid_conect1.0/token request example

```
GET /openid_conect1.0/token HTTP/1.1
Host: example.server.com

grant_type=authorization_code&client_id=EU.EORI.NL123456789&client_assertion_type=urn%3Aietf%3Aparams%3Aoau
th%3Aclient-assertion-type%3Ajwt-bearer&client_assertion=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6Ik1JSUdDRENDQS9DZ0F3SUJBZ0lDRUFRd0RRWUpLb1pJaHZjTkFRRUxCUUF3Z1p
BeEN6QUpCZ05WQkFZVEFrTU1NUXN3Q1FZRFZRUUlEQUpPU0RFUE1BMEdBMVVFQ2d3R2FWTklRVkpGTVJFd0R3WURWUVFMREFoVFpXTjFjbW
wwZVRFb01DWUdBMVVFQXd3ZmFWTklRVkpGSUU1TUlFTmxjblJwWm1sallYUmxJRUYxZEdodmNtbDBlVEVtTUNRR0NTcUdTSWIzRFFFSkFSW
VhhVzVtYjBCcGMyaGhjbVV0Y0hKdmFtVmpkQzV2Y21jd0hoY05NVGN3TmpJM01EZ3lPVEl6V2hjTk1UZ3dOekEzTURneU9USXpXakNCbkRF
TE1Ba0dBMVVFQmhNQ1Rrd3hDekFKQmdOVkJBZ01BazVJTVJJd0VBWURWUVFIREFsQmJYTjBaWEprWVcweER6QU5CZ05WQkFvTUJtbFRTRUZ
TUlRFUk1BOEdBMVVFQ3d3SVUyVmpkWEpwZEhreElEQWVCZ05WQkFNTUYybFRTRUZTUlNCVFkyaGxiV1VnVDNkdVpYSWdVRTlETVNZd0pBWU
pLb1pJaHZjTkFRa0JGaGRwYm1adlFHbHphR0Z5WlMxd2NtOXFaV04wTG05eVp6Q0NBU0l3RFFZSktvWklodmNOQVFFQkJRQURnZ0VQQURDQ
0FRb0NnZ0VCQUxwMVlrMGN1NlU3TTEzbWNRdXBXaitUQUR5L2h3RUhXbW1HR0ZGUmFMTVVSdXVqRHNLQ0hldTg5THZxNzFRUVdreHhKV0FI
UDZvUmUzVUN6Q2RNalhoNlBvRVFubnlDM2RVZ1gzcEdqUUcxb1QwYTd0eU1kTVd6QVc5Mk1KVzJCRjhQN1pSTWxEc2tmN0JKaDFRUHJGL3A
1MytTMHVleFpOTlNCMy9aWmpMcGFudElMM2lGOW14UEtCSlgyYzVkWTY2NnJ0MytmYWRMaEdmMEF0Rzk1ME02QlYzR21NTmJ4OHNOUVYraE
NRME9lSWlyaGtJaSswOG92Y0hURTdEUDcrM0JCMmVkRG9DZ1NYU3RMSHJvZEI4d1pCQkdMQmdtN3RxY0R6NXBrYURldElyc1lLTlhRcUVSR
mpVMlRZdXJCbG5sbDY0cGNlL1NPVWl5K0tEeGhqY0NBd0VBQWFPQ0FWd3dnZ0ZZTUFrR0ExVWRFd1FDTUFBd0VRWUpZSVpJQVliNFFnRUJC
QVFEQWdaQU1ETUdDV0NHU0FHRytFSUJEUVFtRmlSUGNHVnVVMU5NSUVkbGJtVnlZWFJsWkNCVFpYSjJaWElnUTJWeWRHbG1hV05oZEdVd0h
RWURWUjBPQkJZRUZCRWRLWjYxaHBNK1pETE5XTEtsYnhiQmxJVm9NSUcrQmdOVkhTTUVnYll3Z2JPQUZJNUdUZE1VaWFwWEltVlVpOVQyMV
pzQ045enJvWUdXcElHVE1JR1FNUXN3Q1FZRFZRUUdFd0pPVERFTE1Ba0dBMVVFQ0F3Q1RrZ3hFakFRQmdOVkJBY01DVUZ0YzNSbGNtUmhiV
EVQTUEwR0ExVUVDZ3dHYVZOSVFWSkZNUkV3RHdZRFZRUUxEQWhUWldOMWNtbDBlVEVVTUJJR0ExVUVBd3dMYVZOSVFWSkZJRkp2YjNReEpq
QWtCZ2txaGtpRzl3MEJDUUVXRjJsdVptOUFhWE5vWVhKbExYQnliMnBsWTNRdWIzSm5nZ0lRQURBT0JnTlZIUThCQWY4RUJBTUNYUF3RXd
ZRFZSMGxCQXd3Q2dZSUt3WUJCUVVIQXdFd0RRWUpLb1pJaHZjTkFRRUxCUUFFZ2dJQkFBTm0wUUh0c2Jma1ZxeHI2akpndER2dklHUXFtdX
J5TXB1ZTFMb2c2SFpaMlFvd1pXckc4by80U0FnbHBNUFR1VlUwVWZBQms1ZFZmT1hubUJhNWxSTUk3aGw5ZFNNMUhObGU2QzlXQTdSUXROV
i92NHFCZTBPbGdmYUQ0Y1VBSkRrSHNJd1dTTWxjZWxPb3hWWk5jZE93YWRYQVFIZ1lkdXpCU2RSOC9QczNwbHZJRElFOWxyR3Q3R2tVenhT
M1dVMVhWc3M2bktaRldsWmt0cVFINVkrV0VHLy82MCsxV2Y0YUk2VkhJdW9SajEwL05sRXZqY3QwWngweWlaVTJScnF3UHFzcnRCWWJDUEl
1TytDbDlRTTczcEhZM3pZcWtXWTRDTGFld3Z5UFphWTVLREJoN25aT3A5TkoxWjJYV0Z1VklEVFpSZUgyQVJYRnBrV0RhSG1oQWNNWjlCaX
FNK2h4NElYZUM2OFZ2d3VhK2d1eXBQSlpmUnlFMzNzb3gvbHU4ZWNMMkw3L2VoRGdqaThJRVN5bVVQSTMyQ3BLZk1OMUtLTkwvS0V0ZnRHU
HB1Vis2aVFOVEU0aFRDQmNCYVNmM2R4c0dIY2xPU0M2S2U5dEw0WVJMaVgzK1lzSHFZRDk4dkxSUk9iSVFaR1dYaXF2U0ZzTEN3SzBNMVJJ
d3NmYjZCOVMrWE1SQWl3cjFpZXpCZEh4WGFIODFsVCtXeEpmbkR1bjZ1eFhVejR4VHV6YVZYc1YwZ3ZjWTNxdVlwNjRMUjZScmhuYzJEa05
EelpVNkpIeUY3TFg3MHJuOExxqMTgwampHMWdlNmxsOURMUFFUa1Z5U2hUcUNVVis5d3JVMmFFMTZycWUyWUFxL2xMSjBkV09IUzJwSmNRam
gxaURwQXFHT2J3VCJ9.eyJpc3MiOiJFVS5FT1JJLk5MMTIzNDU2Nzg5Iiwic3ViIjoiRVUuRU9SSS5OTDEyMzQ1Njc4OSIsImF1ZCI6Ik5M
LktWSy4xMjM0NTY3OCIsImp0aSI6IjM3OGE0N2M0LTI4MjItNGNhNS1hNDlhLTdlNWExY2M3ZWE1OSIsImV4cCI6MTUwNDY4MzQ3NSwiaWF
0IjoxNTA0NjgzNDQ1fQ.gsVfvaTpjIf_ZkeYRqvkV14WqxROLsFSNeuAdw73v94FXKbjWHk0MFfgUCFy1J-dQQSMmY-
ixmvb1nHsKwNcpAUNI1ZTIf3N8MCrblwQqcLzROPDKOaL4FCdqxcv1oTX_p36jWNErxRDpIm5duIL601wiMjERFZMY7vXfMfqt2k&code=L
zvo6o5fLCCquSNrnSpc
```

Response

Compared to the response specifications in Generic /oauth2.0/token, the response adds one parameter (changes marked in red):

Parameter	Type	Required	Description
access_token	string	Yes	OAuth2.0 access_token. As determined by the server
token_type	string	Yes	OAuth2.0 token type. MUST contain "bearer"
expires_in	int	Yes	OAuth2.0 expiration time of the token. Access tokens SHOULD expire within 3600 seconds by default. Depending on scope and sensitivity of services, servers MAY choose to limit the expiration period. Access token expiration beyond 3600 seconds is discouraged
id_token	string	Yes	OpenID Connect 1.0 signed JWT. See below for id_token contents. See also Generic iSHARE JWT specifications for a.o. basic content and signing requirements.

Compared to the parameters specified in Generic iSHARE JWT specifications, the id_token JWT payload changes the definition of the sub parameter and adds the following parameters:

Parameter	Type	Required	Description
sub	string	Yes	OpenID Connect 1.0 locally unique and never reassigned identifier within the Identity Provider for the Human Service Consumer, which is intended to be consumed by the client.
auth_time	string	Yes	OpenID Connect 1.0 time when the Human Service Consumer authentication occurred.
nonce	string	Yes	OpenID Connect 1.0 value used to associate a Client session with an ID Token. Contains value as passed in to the /openid_connect1.0/authorize endpoint. MUST be used in iSHARE

`act`	string	Yes	OpenID Connect 1.0 authentication context class reference. MUST either contain `urn:eu.ishare.loa.low`, `urn:eu.ishare.loa.substantial` or `urn:eu.ishare.loa.high`, depending on the quality of the authentication method. Replace by EIDAS urn
`azp`	string	Yes	OpenID Connect 1.0 authorised party. MUST be identical to the `client_id` that requested the ID Token. Also identical to aud. MUST be used in iSHARE

Example request JWT payload

```
{
  "iss": "NL.KVK.12345678",
  "sub": "419404e1-07ce-4d80-9e8a-ec2b0899b600", // Note this is not necessary a GUID
  "aud": "EU.EORI.NL123456789",
  "jti": "378a47c4-2822-4ca5-a49a-7e5a1cc7ea59", // Note this is not necessary a GUID
  "exp": 1504683475, // Equals iat + 30 seconds
  "iat": 1504683445,
  "auth_time": 1504683435,
  "nonce": "c428224ca5a",
  "act": "urn:eu.ishare.loa.substantial",
  "azp": "EU.EORI.NL123456789"
}
```

Within

Generic /openid_conect1.0/token response example

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "access_token": "AGxpJB7hl9tooi8AUlLpncK1Kih5beXbjnbeODHp2EN48UO9BDpvtgScFO5aIXwH9T",
  "token_type": "bearer",
  "expires_in": 3600,
  "id_token": "<jwt_value>"
}
```

Generic /openid_connect1.0/userinfo

Used to obtain attributes of a Human Service Consumer conform scope defined in access token.

For use of OpenID Connect 1.0 in iSHARE H2M use cases the following additional requirements apply:

- A client SHALL only request claims from the `/userinfo` endpoint based on the access token. Scope values or claims request parameters SHALL NOT be used.
- For interoperability reasons clients MUST only make `HTTP GET` calls to the `/userinfo` endpoint.

Request

The request contains the following parameters:

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	string	No	Optional iSHARE specific boolean (TRUE or FALSE) indicating the response SHALL not be signed. Default is FALSE, resulting in signed responses

Generic /openid_connect1.0/userinfo request example

```
GET /openid_conect1.0/userinfo HTTP/1.1
Host: example.server.com
Authorization: AGxpJB7hl9tooi8AUlLpncK1Kih5beXbjnbeODHp2EN48UO9BDpvtgScFO5aIXwH9T
Do-Not-Sign: FALSE
```

Response

The response contains a JSON object with parameters conform scope definition in Generic /openid_connect1.0/authorize.

Generic /openid_connect1.0/userinfo response example

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "sub": "419404e1-07ce-4d80-9e8a-ec2b0899b600",
  "first_name": "Vincent",
  "last_name": "Jansen",
  "gender": "male",
  "company_id": "NL812458837",
  "company_name": "Innopay BV"
}
```

If request indicates the response to be signed, the response must be composed, formatted and signed conform Generic iSHARE JWT specifications.

Note that the "sub" parameter MUST contain the Human Service Consumer identifier also indicated in the ID token (see Generic /openid_connect1.0/token)

The Content-Type header MUST bestsellers set to "application/jwt"

Generic /openid_connect1.0/userinfo response example (signed)

```
HTTP/1.1 200 OK
Content-Type: application/jwt

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNSUlHQ0RDQ0EvQ2dBd0lCQWdJQ0VBUXdEUVlKS29aSWh2Y05BUUVMQlFBd2d
aQXhDekFKQmdOVkJBWVRBazVNTVFzd0NRWURWUVFJREFKT1NERVBNQTBHQTFVRUNnd0dhVk5JUVZKRk1SRXdEd1lEVlFRTERBaFRaV04xY2
1sMGVURW9NQ1lHQTFVRUF3d2ZhVk5JUVZKRklFNU1JRU5sY25ScFptbGpZWFJsSUVGMWRHaHZjbWwwZVRFbU1DUUdDU3FHU0liM0RRRUpBU
llYYVc1bWIwQnBjMmhoY21VdGNISnZhbVZqZEM1dmNtY3dIaGNOTVRjd05qSTNNRGd5T1RJeldoY05NVGd3TnpBM01EZ3lPVEl6V2pDQm5E
RUxNQWtHQTFVRUJoTUNUa3d4Q3pBSkJnTlZCQWdNQWs1SU1SSXdFQVlEVlFRSERBbEJiWE4wWlhKa1lXMHhEekFOQmdOVkJBb01CbWxUU0V
GU1JURVJNQThHQTFVRUN3d0lVMlZqZFhKcGRIa3hJREFlQmdOVkJBTU1GMmxUU0VGU1JTQlRZMmhsYldVZ1QzZHVaWElnVUU5RE1TWXdKQV
lKS29aSWh2Y05BUWtCRmhkcGJtWnZRR2x6YUdGeVpTMXdjbTlxWldOMExtOXlaekNDQVNJd0RRWUpLb1pJaHZjTkFRRUJCUUFEZ2dFUEFEQ
0NBUW9DZ2dFQkFMcDFZazBjdTZVN00xM21jUXVwV2orVEFFeS9od0VIV21tR0dGRlJhTE1VUnV1akRzS0NIZXU4OUx2cTcxUVFXa3h4SldB
SFA2b1JlM1VDekNkTWpYaDZQb0VRbm55QzNkVWdYM3BHalFHMW9UMGE3dHlNZE1XekFXOTJNSlcyQkY4UDdaUk1sRHNrZjdCSmgxUVByRi9
wNTMrUzB1ZXhaTk5TQjMvWlpqTHBhbnRJTDNpRjlteFBLQkpYMmM1ZFk2NjZydDMrZmFkTGhHZjBBdEc5NTBNNkJWM0dtTU5ieDhzTlFWK2
hDUTBPZUlpcmhrSWkrMDhvdmNIVEU3RFA3KzNCQjJlZERvQ2dTWFN0TEhyb2RCOHdaQkJHTEJnbTd0cWNEejVwa2FEZXRJcnNZS05YUXFFU
kZqVTJUWXVyQmxubGw2NHBjZS9TT1VpeStLRHhoamNDQXdFQUFhT0NBVnd3Z2dGWU1Ba0dBMVVkRXdRQ01BQXdFUVlKWUlaSUFZYjRRZ0VC
QkFRREFnWkFNRE1HQ1dDR1NBR0crRUlCRFFRbUZpUlBjR1Z1VTFOTUlFZGxibVZ5WVhSbFpDQlRaWEoyWlhJZ1EyVnlkR2xtYVdOaGRHVXd
IUVlEVlIwT0JCWUVGQkVkS1o2MWhwTStaRExOV0xLbGJ4YkJsSVZvTUlHK0JnTlZIU01FZ2JZd2diT0FGSTVHVGRNVWlhcFhJbVZVaTlUMj
Fac0NOOXpyb1lHV3BJR1RNSUdRTVFzd0NRWURWUVFHRXdKT1RERUxNQWtHQTFVRUNBd0NUa2d4RWpBUUJnTlZCQWNNQ1VGdGMzUmxjbVJoY
lRFUE1BMEdBMVVFQ2d3R2FWTklRVkpGTVJFd0R3WURWUVFMREFoVFpXTjFjbWwwZVRFVU1CSUdBMVVFQXd3TGFWTklRVkpGSUZKdmIzUXhK
akFrQmdrcWhraUc5dzBCQ1FFV0YybHVabTlBYVhOb1lYSmxMWEJ5YjJwbFkzUXViM0puZ2dJUUFEQU9CZ05WSFE4QkFmOEVCQU1DQmFBd0V
3WURWUjBsQkF3d0NnWUlLd1lCQlFVSEF3RXdEUVlKS29aSWh2Y05BUUVMQlFBRGdnSUJBQU5tMFFIdHNiZmtWcXhyNmpKZ3REdnZJR1FxbX
VyeU1wdWUxTG9nNkhaWjJRb3daV3JHOG8vNFNBZ2xwTVBUdVZVMFVmQUJrNWRWZk9Ybm1CYTVsUk1JN2hsOWRTTTFITmxlNkM5V0E3UlF0T
lYvdjRxQmUwT2xnZmFENGNVQUpEa0hzSXdXU01sY2VsT294VlpOY2RPd2FkWEFRSGdZZHV6QlNkUjgvUHMzcGx2SURJRTlsckd0N0drVXp4
UzNXVTFYVnNzNm5LWkZXbFprdHFRSDVZK1dFRy8vNjArMVdmNGFJNlZISXVvUmoxMC9ObEV2amN0MFp4MHlpWlUyUnJxd1Bxc3J0QlliQ1B
JdU8rQ2w5UU03M3BIWTN6WXFrV1k0Q0xhZXd2eVBaYVk1S0RCaDduWk9wOU5KMVoyWFdGdVZJRFRaUmVIMkFSWEZwa1dEYUhtaEFjTVo5Qm
lxTStoeDRJWGVDNjhWdnd1YStndXlwUEpaZlJ5RTMzc294L2x1OGVjTDJMNy9laERnamk4SUVTeW1VUEkzMkNwS2ZNTjFLS05ML0tFdGZ0R
1BwdVYrNmlRTlRFNGhUQ0JjQmFTZjNkeHNHSGNsT1NDNktlOXRMNFlSTGlYMytZc0hxWUQ5OHZMUlJPYklRWkdXWGlxdlNGc0xDd0swTTFS
SXdzZmI2QjlTK1hNUkFpd3IxaWV6QmRIeFhhSDgxbFQrV3hKZm5EdW42dXhYVXo0eFR1emFWWHNWMGd2Y1kzcXVZcDY0TFI2UnJobmMyRGt
ORHpaVTZKSHlGN0xYNzBybjhMajE4MGpqRzFnZTZsbDlETFBRVGtWeVNoVHFDVVYrOXdyVTJhRTE2cnFlMllBcS9sTEowZFdPSFMycEpjUW
poMWlEcEFxR09id1QiLCJNSUlHQkRDQ0EreWdBd0lCQWdJQ0VBQXdEUVlKS29aSWh2Y05BUUVMQlFBd2daQXhDekFKQmdOVkJBWVRBazVNT
VFzd0NRWURWUVFJREFKT1NERVNNQkFHQTFVRUJ3d0pRVzF6ZEdWeVpHRnRNUTh3RFFZRFZRUUtEQVpwVTBoQlVrVXhFVEFQQmdOVkJBc01D
Rk5sWTNWeWFYUjVNUlF3RWdZRFZRUURFQXRwVTBoQlVrVWdVbTl2ZERFbU1DUUdDU3FHU0liM0RRRUpBUllYYVc1bWIwQnBjMmhoY21VdGN
ISnZhbVZqZEM1dmNtY3dIaGNOTVRjd05qSTNNRFl4TkRNMFdoY05NamN3TmpJMU1EWXhORE0wV2pDQmtERUxNQWtHQTFVRUJoTUNUa3d4Q3
pBSkJnTlZCQWdNQWs1SU1ROHdEUVlEVlFRS0RBWnBVMGhCVWtVeEVUQVBCZ05WQkFzTUNGTmxZM1Z5YVhSNU1TZ3dKZ1lEVlFRRERCOXBVM
GhCVWtVZ1Rrd2dRMlZ5ZEdsbWFXTmhkR1VnUVhWMGFHOXlhWFI1TVNZd0pBWUpLb1pJaHZjTkFRa0JGaGRwYm1adlFHbHphR0Z5WlMxd2Nt
OXFaV04wTG05eVp6Q0NBaUl3RFFZSktvWklodmNOQVFFQkJRQURnZ0lQQURDQ0Fnb0NnZ0lCQUtpdVFYQTNSMTR6aEFaNTl4dTRKNmo4aDV
MYU1Zb016RklSemVWKzY2NUU4Ym5vSzJlUVNDNWFZTXZzYjgwbzhEeEhIamlxUEppSlcxbjFvVDg2VUFLZ2FFRW5KOC9HaEYrMmt5T2x5Ym
RwTTIxUTZiTndrSjV2TDRTRC9HWUJQbVdzVnQ3WDZwTEFrRnN3ZVh1NndSenZyWVhXY1ZtL3ovM1NIWDlBWkZnNkhEWlJzR0dEbm5SdzE0b
khZcGIvb2g3cDVoNmF0SStYMGFPRDRIaFFKMWFoUUxWb3pJYmJDRkRmcEt1OW1yRFh6S1lEYU5zdHJZbjJEbWJ0VjQwQkM1RlcxT1QwSExP
L3RleG5uaHROcmpxNklWZ1VrWjU0TkhUOFkyRVFObWFqeThSaWxyTFUxRkhTL2thMDN3OHNWMHNYRHNMZUJ3YnhsM0JZSHBpc1BNV3BNSkR
GVThiOTJ0bFlqazJsVURuSHFEVWk1QkhSZFJZcVZaZVdCU0wrUWV2cGV6cjNtQ0w5eW5oR1B5K3ROeURqeVZqYi95N2hsZnRBelp6b2RSd0
l0UVB6cEtIQ1dRTHNXCtKd005bHd1NXVxNmxjcXhIR1BTQUIwby9NRTgwS0UzYTRLbmpDR1l2bFppUEp0cmFkMEhaRFJSL2hFQW5lbjNIR
TNmVFpFNDJ1MndCTFRmWkIxRDhLeGpjNDR2SnY4TDRKT2FMbHQvb29NVDkxM3NHQ1NKRFBRVXd2Ky9WdllEVjhuZ2tnelJDcEZuZzJOclBh
V2FvNlJLSjk5YkJNa0tGUTR2c2R0dndpNDJHSzJPQks3b3pYbk5TN0I1cWNsamRWbnJtbUg4ZkNQSi9zN0w5QkRZdy9JS3JkNXdIYVNIMWt
aNy9EUmEwZmEybU1KamZMQWdNQkFBR2paakJrTUIwR0ExVWREZ1FXQkJTT1JrM1RGSW1xVnlKbFZJdlU5dFdiQWpmYzZ6QWZCZ05WSFNNRU
dEQVdnQlJMWWF6em9OcHVCYi8vNFNyMUlvcjBpUDA0UmpBU0JnTlZIUk1CQWY4RUNEQUdBUUgvQWdFQU1BNEdBMVVkRHdFQi93UUVBd0lCa
GpBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQWdFQVE3R1JJUTNRK1RSVXVteE9YYytkR0pueDk4RUsxcUQ4RTF1RXB0bFMrVlJPV0FaMjRZUxD
UGsvbk5EVnMyQW1DQURaRjBKb1gyK1JKTmpxN3BYMitBeGNMMW93V1FvaTNHUnRMNkdBQkhCeXVsVGZKZnZvZFlqVWlwSTF6bUl2Y1dLek5
uTkNDOUEwcmR0VUp5UmpadkdadDMySzc3YWlSTkdpU0N0VnlDQnVGQlB0cUNrWEl6ODZlL3d6UTFmd0JlQ1JCMFdETW9TZFhiU2t0L3RhcH
lHb1U3b0FqMkRWV2J0S2FDbmtLaXlzRTE5cjFSQ2laSTJXQUhMY3VVOWlMdk5NU1mb3d2OWF2SStyVnEyWWxLVU91Q0lyRDdzL0lMUkxYZ
zU1VndxTUpUMzMvNTBORm51M0g4ZWJtcUVoa0dZU3RrN3AzRkdSeGdwdGQyT0pucUF0NW5HMXBzcEhRdUQrdllCb0tra013NDBxdnkrZWVZ
a2h5ektjSlRLZU9zZkkyOWZ5UXgvZUZTbVdSaGVUMTg4K2paUXlDcUVRcFpSZ3RrdSsyS1BRYkNCeFZlQ2ZIYWN5UzE2KzlaT1ZzMXpYV0d
mSXFYS1h3WkYxdjZDRHlMN2JlZEpaRXVUVTF3VXBrRVVKSC9JUG1kcDJaTU5NY3NzL0JJZHlmLytwWXd5TW5CNkRKb2NEd01qbG0zY1VFc2
```

```
J0VDM5M3dJaWUwbW9oV2l1OG15VHhrQ2ZOMVZKczRXOWNoU3g1L0R4VndEdEZvVDRuc3FWSzlGNkRLWUpBSjk1VVIrQytSaUNTK3g3dDRyO
GN1cDBBaUpwZzdKRUdyNUk5a2RsQlhLQWs3OFByL29xWm9nRnltV1B6b1dVeTQ4WWU2V3hhQUExcytoNmhWUTIyTUNnPSIsIk1JSUdDREND
QS9DZ0F3SUJBZ0lKQU43a01TanVHVDlLTUEwR0NTcUdTSWIzRFFFQkN3VUFNSUdRTVFzd0NRWURWUVFHRXdKT1RERUxNQWtHQTFVRUNBd0N
Ua2d4RWpBUUJnTlZCQWNNQ1VGdGMzUmxjbVJoYlRFUE1BMEdBMVVFQ2d3R2FWTklRVkpGTVJFd0R3WURWUVFMREFoVFpXTjFjbWwwZVRFVU
1CSUdBMVVFQXd3TGFWTklRVkpGSUZKdmIzUXhKakFrQmdrcWhraUc5dzBCQ1FFV0YybHVabTlBYVhOb1lYSmxMWEJ5YjJwbFkzUXViM0puT
UI0WERURTNNRFl5TnpBMk1EWTFORm9YRFRNM01EWXlNakEyTURZMU5Gb3dnWkF4Q3pBSkJnTlZCQVlUQWs1TU1Rc3dDUVlEVlFRSURBSk9T
REVTTUJBR0ExVUVCd3dKUVcxemRHVnlaR0Z0TVE4d0RRWURWUVFLREFacFUwaEJVa1V4RVRBUEJnTlZCQXNNQ0ZObFkzVnlhWFI1TVJRd0V
nWURWUVFEREF0cFUwaEJVa1VnVW05dmRERW1NQ1FHQ1NxR1NJYjNEUUVKQVJZWGFXNW1iMEJwYzJoaGNtVXRjSEp2YW1WamRDNXZjbWN3Z2
dJaU1BMEdDU3FHU0liM0RRRUJBUVVBQTRJQ0R3QXdnZ0lLQW9JQ0FRQ3V2VjhnU1FEeDdnMVBZdnhjdUs2dURJd1daTlpLZEYwd0pvR2pjS
WxxUEpXRjNwUDJ4Q0pxNVpSblVRbnBXMFdUQ1d3OUE0dVpmQ0lXcUpTb0lTaDRuRTdVbU1tZnc0NW1zKzdTd0p4ZmM3RStZNGZmTURNeUxj
bXZIWVlMcUdEb1p1NHFucHl0c3orWHMxZThFU3lOdElsWG9vWjZPK0MxaGUrWG1YcFNDaE9qaDVQbno3Ukh6NGNTN1p3MzhCOWFOQTNXa3R
GK3lSN2lqa1RVTjg4N2FaQXBsbXJOWm9pb0duTS9FMVJGd25McXJrNUU4NGtPVHpleHNOSUxCcEJ6b1prTFB6OHlZSTBPSjQyL1JUNW05WV
BPSVJXTXdXY2dRcW1CSElnTUNhVU9qQXNsZXgyQngxdVF0QkpjdGkrRElmK1pJR1BtL1Rjd3NhQ0MrUmJFNTFTbU1xd1hZZS9Cb0FsQVpLW
VNnRzhvdXROK0ZkM0V3M2gzWUpjQTg2d0RUOWJLTXpTOW9TVjFFalhjOHYrNDBwcC8vQWRXTVBmMnExNWkvUW90VGorU0dQMmNKUXZjZlJC
Sjk0SWZHNDFJQm9sRUs3akVVTjJKVWNvd0FkTnNZZk03RWRvS0doSW4rYmtDWG5aUjNibmZCS0JBWEg2NE1PcDdJaTFOdWtqUHBFcWVteU0
zLy9YS24vMWxYelU0M3JiYXp3Ynh5R0JZcTNBSHY1aW83TVMxVHdlZ0QvaE5tVE9FR0hmZlovQ3pKZ2htNld2Z21jbVVBTHUySUZjRHBtWV
pJM1VJM1NLendhZGRpNy92Y0dlcjVWVkRnbFJ0VnR2SGszZUpSVDBMOVNGcUhJV3NMdW5JL2RaU0pFOHBLcFN0RzVMemo3WS9wc09sQnBha
G53SURBUUFCbzJNd1lUQWRCZ05WSFE0RUZnUVVTMkdzODZEYWJnVy8vK0VxOVNLSzlJajlPRVl3SHdZRFZSMGpCQmd3Rm9BVVMyR3M4NkRh
YmdXLy8rRXE5U0tLOUlqOU9FWXdEd1lEVlIwVEFRSC9CQVV3QXdFQi96QU9CZ05WSFE4QkFmOEVCQU1DQVlZd0RRWUpLb1pJaHZjTkFRRUx
CUUFEZ2dJQkFCdCtJNFpuUzQ1YzJJRnNLVitCQThKUDVPV0NQb2FKeWwzUENFTGplZFZmQjRyWHlGOTQ2K0lMQVJjQlpnMzVGMDdXekh0bW
kvYWZYaDZlbnR2Vk1FQWxFbUg2bG44c1I5aG9NM3JIbllSdFNJSm1KczJnU0Y4d2dDT1pkMXB5ZnJCVnUzZjNTWGJVZ05qb2U1dEVXNnhzT
1FzampxTm5RaUpNSng2ZWE1Nkwya2JXN0U2a09zK01jazlLejhaUVFCNThpUEd5eDNhaE1MT3J4YlBvSXRicUt1eUR3Y283QXpMZjdlYTl6
eWUwdXA4dWJORFlGYUtKZmlJRHNuVmJVUEE2RmJUbjRmU1FwZWVPSzFmanJ6U2FVcGVNT2RPb21qMFpqd3Q2SzdXN2NreG9JZk9lY1c0ZGN
QRU5wWElta0JQUVhzR3h2Q2xEZi82ZS9qUHRpM0NQZ3hKRjM3NDdIcTZ0QlNIMEd6Q3JZdjRiRm9yUXU0M016cVpLSGJYOEZGMVBwSFNhaV
hKSy9IdThXSkRYWEJxNVBlZGVsL2xKU2FqZFRzVURzaUZYa2ovcFkwdUo2TTB4L0Vvbm96YUNQY0h3ZFBzdnI2bnJySFdRWG80YXlQN250Z
WdKQTNHckdYY2FQK3BlRVFtRjluV2dWd1BxMzNDMVRyUE5haU14SHo1dG94bDBZaG5iQSs1ZUgyQ1RCakRGSm5yMnVhZWg4Qnpia2RFMjlX
a09zcUpaQUlVRU1tUnd4Y3hCVzIwSkdBbGhGNk1QRkFEalBZRzBMamRqYndxMkgrTFF0UmYrdEU2Wjdud00vY0FUNGRFQjdNZTF1SnJJZdWN
WakxMU05YQ1JLUWFES0taTW9IaEFjaUxlS0xNclNnVURhQWkwQVVLWGR1Q3ltVXczbiJdfQ.eyJpc3MiOiJFVS5FT1JJLk5MMTIzNDU2Nzg
5Iiwic3ViIjoiNDE5NDA0ZTEtMDdjZS00ZDgwLTllOGEtZWMyYjA4OTliNjAwIiwiYXVkIjoiTkwuS1ZLLjEyMzQ1Njc4IiwianRpIjoiMz
c4YTQ3YzQtMjgyMi00Y2E1LWE0OWEtN2U1YTFjYzdlYTU5IiwiZXhwIjoxNTA0NjgzNDc1LCJpYXQiOjE1MDQ2ODM0NDUsImZpcnN0X25hb
WUiOiJWaW5jZW50IiwibGFzdF9uYW1lIjoiSmFuc2VuIiwiZ2VuZGVyIjoibWFsZSIsImNvbXBhbnlfaWQiOiJOTDgxMjQ1ODgzNyIsImNv
bXBhbnlfbmFtZSI6Iklubm9wYXkgQlYifQ.EIiLVtjPsycuxwB0LyTpw7wvMSrs4nhg-Y3zHNv1pss
```

Generic iSHARE JWT specifications

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.

Header

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

- 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 [1] [2]
- The JWT MUST always contain the `iat` claim

- The `iss` and `sub` claims MUST contain the valid iSHARE identifier of the client [1]
- The `aud` claim MUST contain only the valid iSHARE identifier 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 for requirements
- 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.

[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

Processing delegation evidence

A Service Provider SHALL only grant access based on delegation evidence if the 'SUM' of all evidence evaluates to true.

A basic example (in pseudo code):

Case

```
A is owner of resources A-Z
```

Delegation 1 (last year)

```
B allows C COMPLETE access to all resources B has rights to and allows C to delegate indefinitely
```

Delegation 2 (one hour ago)

```
A allows B READ & WRITE access to X & Y and allows B to delegate an additional 2 times
```

Delegation 3 (last week)

```
C allows D READ access to A, B, X, Y & Z without the right to delegate
```

This resolves to (now)

```
D has READ access to X & Y without the right to delegate
```

Scheme Owner APIs

The iSHARE Scheme Owner exposes the following APIs:

- Scheme Owner /oauth2.0/token
- Scheme Owner /ishare1.0/parties/{party_id}
- Scheme Owner /ishare1.0/parties/certified_parties
- Scheme Owner /ishare1.0/trusted_list
- Scheme Owner /ishare1.0/certificate_validation

Note that, although this specification should be complete, a complete overview of the current iSHARE API specifications (work in progress) can be found here on SwaggerHub.

Please note that in case of contradictions the specifications on Confluence prevail over those on SwaggerHub

Scheme Owner /oauth2.0/token

This API is used by any iSHARE party to obtain an access token from the Scheme Owner.

This API is build on the generic `/oauth2.0/token` API. In addition to these generic requirement, the following specific requirements for the Scheme Owner `/token` API are defined:

- Scope MUST be iSHARE. No other scopes are supported. Any access token issued by the Scheme Owner grants access to any API of the Scheme Owner.

Scheme Owner /ishare1.0/parties/{party_id}

Used to obtain specific information on a iSHARE party.

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

Used to obtain adherence information on an iSHARE participant from the iSHARE Scheme owner

- The service request MUST contain the parameters `Authorisation`, and; `party_id`
- The service request MAY contain the parameter `date_time`
- The `Authorisation` parameter MUST contain "Bearer" + access token value
- The `date_time` parameter MUST be cacheable
- The api_root parameter must be present

Request

The request contains the following parameters:

Parameter	Contained in	Type	Required	Description
`Authorization`	header	string	Yes	OAuth 2.0 access token type + value. T
`party_id`	path	string	Yes	iSHARE identifier of the party
`date_time`	query	string	No	Note: if a date time is provided in the r

Generic /oauth2.0/token request example

```
GET /scheme_owner/ishare1.0/parties/EU.EORI.NL123456789?date_time=1506596432 HTTP/1.1
Host: ishare-project.org
Authorization: bearer AGxpJB7hl9tooi8AUlLpncK1Kih5beXbjnbeODHp2EN48UO9BDpvtgScFO5aIXwH9T
```

Response

The response contains a JSON object with following parameters:

Parameter	Contained in	Type	Required	Description
date_time		int	Yes	OAuth2.0 access_token. As determined by the server
party_id		string	Yes	OAuth2.0 token type. MUST contain "bearer"
api_root		string	No	
adherence		{}	Yes	OAuth2.0 expiration time of the token. Access tokens SHOULD expire expiration period. Access token expiration beyond 3600 seconds is d
status	adherence	string	Yes	
start_date	adherence	int	Yes	
certifications		{}	No	
certification	certifications	{}	No	
role	certification	string	Yes	
start_date	certification	int	Yes	
end_date	certification	int	No	

Returns a signed JWT containing the all registered information of the requested party.

Note: this is the registered information at the time, not describing certification at the time

Party information

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
  "date_time": "2017-06-07T06:17:23Z",
  "party_id": "EU.EORI.NL123456789",
  "adherence": {
      "status": "ACTIVE",
      "start_date": "2017-06-07T06:17:23Z"
    },
  "certifications": [
    "certification": {
      "role": "iSHARE.v10.IDENTITY_PROVIDER",
      "start_date": "2017-06-07T06:17:23Z",
      "end_date": "2017-12-31T23:59:59Z"
    },
    "certification": {
      "role": "iSHARE.v11.IDENTITY_PROVIDER",
      "start_date": "2017-06-07T06:17:23Z"
    },
    "certification": {
      "role": "iSHARE.v10.IDENTITY_BROKER",
      "start_date": "2017-06-07T06:17:23Z"
    },
    "certification": {
      "role": "iSHARE.v11.AUTHORISATION_REGISTRY"
      "start_date": "2017-06-07T06:17:23Z"
    }
  ]
}
```

Values for "adherence":status" can be:

- ACTIVE
- NOT_ACTIVE
- SUSPENDED

End_date for adherence and certification is optional.

Todo: Servers MUST register one or more domain names (URIs) in order to prevent https://tools.ietf.org/html/rfc6749#section-10.6

Note: if a date time is provided in the request, the result becomes final and therefor MUST be cashable.

HTTP Header for cacheable party information

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: max-age=31536000



...
```

/sche

Scheme Owner /ishare1.0/parties/certified_parties

GET /scheme_owner/ishare1.0/parties/certified_parties

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

- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameter `date_time`
- The `Authorisation` parameter MUST contain "Bearer" + access token value
- The `date_time` parameter MUST be cacheable

/scheme_owner/ishare1.0/certified_parties

Returns a signed JWT containing the certifications of all certified parties

Certification information

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
  "date_time": "2016-12-31T12:45:23Z",
  "certified_parties": [
    {
      "party_id": "EU.EORI.NL123456789",
      "adheres": "ACTIVE",
      "certifications": [
        "certification": {
          "role": "iSHARE.v10.IDENTITY_PROVIDER",
          "start_date": "2017-06-07T06:17:23Z",
          "end_date": "2017-12-31T23:59:59Z"
        },
        "certification": {
          "role": "iSHARE.v11.IDENTITY_PROVIDER",
          "start_date": "2017-06-07T06:17:23Z"
        },
        "certification": {
          "role": "iSHARE.v10.IDENTITY_BROKER",
          "start_date": "2017-06-07T06:17:23Z"
        },
        "certification": {
          "role": "iSHARE.v11.AUTHORISATION_REGISTRY"
          "start_date": "2017-06-07T06:17:23Z"
        }
      ]
    }
    {
      "party_id": "EU.EORI.NL234567890",
      "certifications": [
        "certification": {
          "role": "iSHARE.v11.IDENTITY_PROVIDER",
          "start_date": "2017-06-07T06:17:23Z"
        }
      ]
        }
  ]
}
```

Certfications are specified in the following format:

iSHARE.<version>.<role>

Note: if a date time is provided in the request, the result becomes final and therefor MUST be cashable.

Scheme Owner /ishare1.0/trusted_list

GET /scheme_owner/trusted_list

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

- The service request MUST contain the parameter `Authorisation`
- The `Authorisation` parameter MUST contain "Bearer" + access token value

Scheme Owner /ishare1.0/certificate_validation

GET /scheme_owner/ishare1.0/certificate_validation

Used to assess whether a PKI certificate is valid and trusted under iSHARE

- The service request SHOULD not be used more than x per y for each certificate

- The service request MUST contain the parameters `Authorisation`, and; `certificate`
- The `Authorisation` parameter MUST contain "Bearer" + access token value

/scheme_owner/ishare1.0/certificate_validation

Input is a x.509 certificate in PEM format. Note this includes the "-----BEGIN CERTIFICATE-----" header and the "-----END CERTIFICATE-----" footer. Note that the entire value MUST be url encoded.

Returns a signed JWT containing the validity of a certificate. The `certificate_id` contains the certificate serial number, assigned by the certificate issuer.

Adherence information

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
  "date_time": "2016-12-31T12:45:23Z",
  "party_id": "EU.EORI.NL123456789",
  "certificate_id": "1410"
  "validity": "TRUE"
}
```

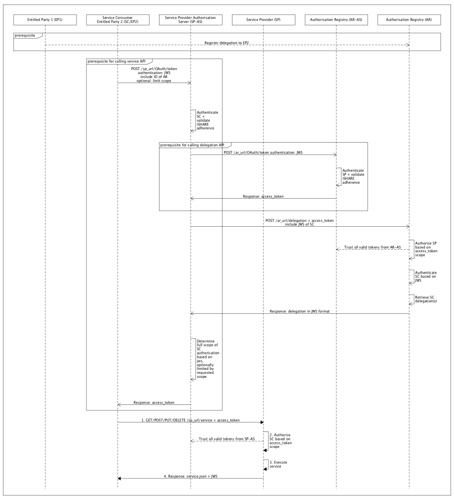
Note: if a date time is provided in the request, the result becomes final and therefor MUST be cachable.

Values for "validity" can be:

- TRUE
- FALSE
- UNKNOWN

API example use case 1c

Step by step detailed technical overview of use case 1c


Entitled Party 1 (EP1)
Service Consumer Entitled Party 2 (SC/EP2)
Service Provider Authorisation Server (SP-AS)
Service Provider (SP)
Authorisation Registry (AR-AS)
Authorisation Registry (AR)
prerequisite
Register delegation to EP2
prerequisite for calling service API
POST /sp_url/OAuth/token authentication: JWS include ID of AR optional: limit scope
Authenticate SC + validate iSHARE adherence
prerequisite for calling delegation API
POST /ar_url/OAuth/token authentication: JWS
Authenticate SP + validate iSHARE adherence
Response: access_token
POST /ar_url/delegation + access_token include JWS of SC
Trust all valid tokens from AR-AS
Authorise SP based on access_token scope
Authenticate SC based on JWS
Retrieve SC delegation(s)
Response: delegation in JWS format
Determine full scope of SC authorisation based on jws, optionally limited by requested scope
Response: access_token
1. GET/POST/PUT/DELETE /sp_url/service + access_token
Trust all valid tokens from SP-AS
2. Authorise SC based on access_token scope
3. Execute service
4. Response: service.json + JWS

Pre-requisite for calling service APIs at Service Provider

Access Token request from Service Consumer

```
GET /oauth2.0/token HTTP/1.1
Host: example.service-provider.com

grant_type=client_credentials
&scope=iSHARE
&client_id=NL000000001
&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer
&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjNkZGRkYXNkYXNkYXNkYXNkZGQ0NTY3ODkwIiwi
bmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.w-OFT6yHL2cnXHiCWvKKNlhd1nTFt8jHSFLL_FitO3ir88bMY_WyzYu-
cwnaIr20gLWZIQ3W7dq4--
JqMWnlVb3xuNr6YHm4ivGftvdVbpS2sPqoLxNHCsYgb2L2X0NJKurhpgZ_0OB5FwPHJ1nqvX_fwymwNejPZPgqFLvUN-U
&authorisation_registry=NL123456789
```

Pre-requisite for calling `/delegation` API at Authorisation Registry

Access Token request from Service Provider

```
GET /oauth2.0/token HTTP/1.1
Host: example.authorisation-registry.com


grant_type=client_credentials
&scope=iSHARE
```

```
&client_id=NL000000002
&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type%3Ajwt-bearer
&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhc2RzYXN1YiI6IjEyM2RkZGRhc2Rhc2Rhc2Rhc2RkZDQ1Njc4
OTAiLCJuYW1lIjoiSm9obiBEb2UiLCJhZG1pbiI6dHJ1ZX0.ay5Ghz_X6It4h8KnNUiarO3hTPWJ_ahqfaTzZ_NwNGJecC0GXLJefmONyCO
Uq9jlYzel8_mmrfbtDZDZixoV8QEInoC7Eihsq07o9xih0vhCRTbNx_G98UV8X2STGiN0Ppz3TDWKEH-R1dAFL6E5KFLG-
Ybi7ZqzplHbey-ZcEw
```

Access Token response from Authorisation Registry

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "access_token": "AGxpJB7hl9tooi8AUlLpncK1Kih5beXbjnbeODHp2EN48UO9BDpvtgScFO5aIXwH9T",
  "token_type": "bearer",
  "expires_in": 3600
}
```

Delegation Evidence request from Service Provider

```
GET /ishare1.0/delegation HTTP/1.1
Authorization: Bearer AGxpJB7hl9tooi8AUlLpncK1Kih5beXbjnbeODHp2EN48UO9BDpvtgScFO5aIXwH9T
Host: example.authorisation-registry.com

service_consumer_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjNkZGRkYXNkYXNkYXNkYXNkZGQ0NTY
3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.w-OFT6yHL2cnXHiCWvKKNlhd1nTFt8jHSFLL_FitO3ir88bMY_WyzYu-
cwnaIr20gLWZIQ3W7dq4--
JqMWnlVb3xuNr6YHm4ivGftvdVbpS2sPqoLxNHCsYgb2L2X0NJKurhpgZ_0OB5FwPHJ1nqvX_fwymwNejPZPgqFLvUN-U
```

Delegation Evidence response from Authorisation Registry

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "delegation_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.
EkN-
DOsnsuRjRO6BxXemmJDm3HbxrbRzXglbN2S4sOkopdU4IsDxTI8jO19W_A4K8ZPJijNLis4EZsHeY559a4DFOd50_OqgHGuERTqYZyuhtF3
9yxJPAjUESwxk2J5k_4zM3O-vtd1Ghyo4IbqKKSy6J9mTniYJPenn5-HIirE"
}
```

Access Token response from Service Provider

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "access_token": "beODHp2EN48UO9BDpvtgScFO5aIXwH9TAGxpJB7hl9tooi8AUlLpncK1Kih5beXbjn",
  "token_type": "bearer",
  "expires_in": 3600
}
```

Service request from Service Consumer

```
GET /service HTTP/1.1
Authorization: Bearer beODHp2EN48UO9BDpvtgScFO5aIXwH9TAGxpJB7hl9tooi8AUlLpncK1Kih5beXbjn
Host: example.service-provider.com
LicensePurpose: RESHARE_ISHARE
```

Service response from Service Provider

```
HTTP/1.1 200 OK
Content-Type: application/json
LicensePurpose: RESHARE_ISHARE
LicenseSubLicense: 10
LicenseEndDate: 9999-12-31

{
  ... service specific content ...
}
```

Role specific API requirements

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

The below is a summary of the requirements per service to be requested from a party with a certain role, as found in the iSHARE API specifications on SwaggerHub.

The roles from which a service can be requested covered here are Service Consumer, Service Provider, Entitled Party, Authorisation Registry, Identity Provider, and Scheme Owner. The services covered are GET, POST, PUT, PATCH, and DELETE as in standard HTTP methods inspired by the RESTful architectural style. Standard CRUD operations are mapped to standard HTTP methods in the table on this page.

Service Consumer

GET /service_consumer/webhook_url

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

- The service request MUST contain the parameter `event_id`

Service Provider

GET /service_provider/oauth2.0/token

Used to obtain an OAuth access token from a Service Provider

- The format of `access_token` MUST be defined by the Service Provider
- The format of `access_token` SHOULD be opaque to the Service Consumer
- The service request MUST contain the parameters `grant_type`; `client_id`; `client_assertion_type`, and; `client_assertion`
- The service request MAY contain the parameters `scope`; `delegation`; `authorisation_registry`, and; `entitled_party_registry`
- The `grant_type` parameter MUST contain "client_credentials"
  The `client_id` parameter MUST contain a valid iSHARE identifier of the Service Consumer
- The `client_assertion_type` parameter MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”
- The `client_assertion` parameter MUST contain a JWT token conform iSHARE specifications, signed by the client

GET /service_provider/openid_connect1.0/return

OpenID Connect end-point received by a Human Service Consumer after authentication

- This OpenID Connect end-point MAY have any name the Service Provider chooses
- The service request MUST contain the parameters `code`, and; `state`
- The `state` parameter MUST contain the state as provided by the Service Provider in the service request to the Identity Provider or Identity Broker

POST /service_provider/webhooks

Used to subscribe to certain events defined by the Service Provider by registering a webhook url

- The service request MUST contain the parameters `Authorisation`, and; `Request Body`
- The `Authorisation` parameter MUST contain "Bearer" + access token value

GET /service_provider/webhooks

Used to subscribe to certain events defined by the Service Provider by registering a webhook url

- The service request MUST contain the parameter `Authorisation`

- The `Authorisation` parameter MUST contain "Bearer" + access token value

GET / service_provider/webhooks/{webhook_id}

Used to obtain info on a certain webhook url

- The service request MUST contain the parameters `Authorisation`, and; `webhook_id`
- The `Authorisation` parameter MUST contain "Bearer" + access token value

DELETE /service_provider/webhooks/{webhook_id}

Used to delete a certain webhook url

- The service request MUST contain the parameters `Authorisation`, and; `webhook_id`
- The `Authorisation` parameter MUST contain "Bearer" + access token value

GET / service_provider/events/{event_id}

Used to obtain info on a certain event

- The service request MUST contain the parameters `Authorisation`, and; `event_id`
- The `Authorisation` parameter MUST contain "Bearer" + access token value

GET /service_provider/service

Example service of a Service Provider

- An iSHARE-adherent Service Provider MUST apply iSHARE conformant OAuth to every iSHARE enabled service
- An iSHARE enabled service MAY have any name the Service Provider chooses
- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameters `service_consumer_assertion`; `LicensePurpose`; `Do-Not-Sign`, and; `Service-Headers`
- The Authorisation parameter MUST contain "Bearer" + access token value

POST /service_provider/service

Example service of a Service Provider

- An iSHARE-adherent Service Provider MUST apply iSHARE conformant OAuth to every iSHARE enabled service
- An iSHARE enabled service MAY have any name the Service Provider chooses
- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameters `service_consumer_assertion`; `LicensePurpose`; `Do-Not-Sign`, and; `Service-Headers`
- The `Authorisation` parameter MUST contain "Bearer" + access token value

PUT /service_provider/service

Example service of a Service Provider

- An iSHARE-adherent Service Provider MUST apply iSHARE conformant OAuth to every iSHARE enabled service
- An iSHARE enabled service MAY have any name the Service Provider chooses
- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameters `service_consumer_assertion`; `LicensePurpose`; `Do-Not-Sign`, and; `Service-Headers`
- The Authorisation parameters MUST contain "Bearer" + access token value

PATCH /service_provider/service

Example service of a Service Provider

- An iSHARE-adherent Service Provider MUST apply iSHARE conformant OAuth to every iSHARE enabled service
- An iSHARE enabled service MAY have any name the Service Provider chooses
- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameters `service_consumer_assertion`; `LicensePurpose`; `Do-Not-Sign`, and; `Service-Headers`
- The Authorisation parameters MUST contain "Bearer" + access token value

DELETE /service_provider/service

Example service of a Service Provider

- An iSHARE-adherent Service Provider MUST apply iSHARE conformant OAuth to every iSHARE enabled service
- An iSHARE enabled service MAY have any name the Service Provider chooses
- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameters `service_consumer_assertion`; `LicensePurpose`; `Do-Not-Sign`, and; `Service-Headers`

- The Authorisation parameters MUST contain "Bearer" + access token value

Entitled Party

GET /entitled_party/oauth2.0/token

Used to obtain an OAuth access token from an Entitled Party

- The service request MUST contain the parameters `grant_type`; `client_id`; `client_assertion_type`, and; `client_assertion`
- The service request MAY contain the parameter `scope`
- The `grant_type` parameter MUST contain "client_credentials"
- The `client_id` parameter MUST contain a valid iSHARE identifier of the Service Consumer
- The `client_assertion_type` parameter MUST contain "urn:ietf:params:oauth:client-assertion-type:jwt-bearer"
- The `client_assertion` parameter MUST contain a JWT token conform iSHARE specifications, signed by the client

GET /entitled_party/ishare1.0/delegation

Used to obtain delegation evidence from an Entitled Party

- A Service Provider MUST validate that the Entitled Party only provides information about his own delegations
- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameters `scope`, and; `service_consumer_assertion`
- The Authorisation parameter MUST contain "Bearer " + access token value

Authorisation Registry

GET /authorisation_registry/oauth2.0/token

Used to obtain an OAuth access token from an Authorisation Registry

- The service request MUST contain the parameters `grant_type`; `client_id`; `client_assertion_type`, and; `client_assertion`
- The service request MAY contain the parameter `scope`
- The `grant_type` parameter MUST contain "client_credentials"
- The `client_id` parameter MUST contain a valid iSHARE identifier of the Service Consumer

- The `client_assertion_type` parameter MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”
- The `client_assertion` parameter MUST contain a JWT token conform iSHARE specifications, signed by the client

GET /authorisation_registry/ishare1.0/delegation

Used to obtain delegation evidence from an Authorisation Registry

- The service request MUST contain the parameters `Authorisation`
- The service request MAY contain the parameters `scope`, and; `service_consumer_assertion`
- The Authorisation parameter MUST contain "Bearer " + access token value

Identity Provider

GET /identity_provider/openid_connect1.0/authorize

OpenID Connect end-point for redirecting a Human Service Consumer for authentication by the Identity Provider

- The service request MUST contain the parameters `response_type`; `client_id`; `redirect_uri`; `scope`, and; `state`
- For the `response_type` parameter, using the Authorization Code Flow with value ‘code’ is REQUIRED
- The `client_id` parameter MUST contain a valid iSHARE identifier of the Service Provider
- The `scope` parameter MUST contain the ‘openid’ scope value and MAY contain ‘name’; ‘contact_details’; ‘company_id’, and; ‘company_info’ scope value(s)

GET /identity_provider/openid_connect1.0/token

OpenID Connect end-point for obtaining the OAuth access token and OpenID Connect id token

- The service request MUST contain the parameters `grant_type`; `code`; `redirect_uri`; `client_id`; `client_assertion_type`, and; `client_assertion`
- The `grant type` parameter MUST contain “authorization code”
- The `code` parameter MUST contain value of authorisation code received from the Identity Provider
- The `client_id` parameter MUST contain a valid iSHARE identifier of the Service Provider
- The `client_assertion_type` parameter MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”
- The {{client_assertion parameter}} MUST contain a JWT token conform iSHARE specifications, signed by the client

GET /identity_provider/openid_connect1.0/userinfo

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

- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameter `Do-Not-Sign`
- The `Authorisation` parameter MUST contain "Bearer " + access token value

Scheme owner

GET /scheme_owner/auth2.0/token

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

- The service request MUST contain the parameters `grant_type`; `client_id`; `client_assertion_type`, and; `client_assertion`
- The service request MAY contain the parameter `scope`
- The `grant_type` parameter MUST contain “client_credentials”
- The `client_id` parameter MUST contain a valid iSHARE identifier of the Service Provider
- The `client_assertion_type` parameter MUST contain “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”
- The `client_assertion` parameter MUST contain a JWT token conform iSHARE specifications, signed by the client

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

Used to obtain adherence information on an iSHARE participant from the iSHARE Scheme owner

- The service request MUST contain the parameters `Authorisation`, and; `party_id`
- The service request MAY contain the parameter `date_time`
- The `Authorisation` parameter MUST contain "Bearer" + access token value
- The `date_time` parameter MUST be cacheable

GET /scheme_owner/ishare1.0/parties/certified_parties

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

- The service request MUST contain the parameter `Authorisation`
- The service request MAY contain the parameter `date_time`

- The Authorisation parameter MUST contain "Bearer" + access token value
- The date_time parameter MUST be cacheable

GET /scheme_owner/trusted_list

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

- The service request MUST contain the parameter Authorisation
- The Authorisation parameter MUST contain "Bearer" + access token value

GET /scheme_owner/ishare1.0/certificate_validation

Used to assess whether a PKI certificate is valid and trusted under iSHARE

- The service request SHOULD not be used more than x per y for each certificate
- The service request MUST contain the parameters Authorisation, and; certificate
- The Authorisation parameter MUST contain "Bearer" + access token value

The iSHARE JWT for iSHARE enabled services

In order to add iSHARE specific information to services an iSHARE JWT structure is added to the HTTP headers of the service specific request/response message. Through this setup, the impact of implementing iSHARE in existing (data sharing) services is minimised, since existing request and response HTTP body payloads remain unaffected.

HTTP Header

The JWT MUST be added to the HTTP header as ishare-jwt.

Example HTTP header containing iSHARE JWT

```
GET /service_information_a HTTP/1.1
Authorization: Bearer
AGxpJB7hl9tooi8AUlLpncK1Kih5beXbjnbeODHp2EN48UO9BDpvtgScFO5aIXwH9T
Host: example.service-provider.com
ishare-jwt:
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6Ik1JSUdDRENDQS9DZ0F3SUJBZ0lDRUFRd0RRWUpLb1pJaHZjT
kFRRUxCUUF3Z1pBeEN6QUpCZ05WQkFZVEFrNU1NUXN3Q1FZRFZRUUlEQUpPU0RFUE1BMEdBMVVFQ2d3R2F
WTklRVkpGTVJFd0R3WURWUVFMREFoVFpXTjFjbWwwZVRFb01DWUdBMVVFQXd3ZmFWTklRVkpGSUU1TUlFTm
xjblJwWm1sallYUmxJRUYxZEdodmNtbDBlVEVtTUNRR0NTcUdTSWIzRFFFSkFSWVhhVzVtYjBCcGMyaGhjbVV0Y0
hKdmFtVmpkQzV2Y21jd0hoY05NVGN3TmpJM01EZ3lPVEl6V2hjTk1UZ3dOekEzTURneU9USXpXakNCbkRFTE1Ba
0dBMVVFQmhNQ1Rrd3hDekFKQmdOVkJBZ01BazVJTVJJd0VBWURWUVFIREFsQmJYTjBaWEprWVcweER6QU5C
Z05WQkFvTUJtbFRTRUZTUlRFUk1BOEdBMVVFQ3d3SVUyVmpkWEpwZEhreElEQWVCZ05WQkFNTUYybFRTRUZ
TUlNCVFkyaGxiV1VnVDNkdVpYSWdVRTlETVNZd0pBWUpLb1pJaHZjTkFRa0JGaGRwYm1adlFHbHphR0Z5WlMxd
2NtOXFaV04wTG05eVp6Q0NBU0l3RFFZSktvWklodmNOQVFFQkJRQURnZ0VQQURDQ0FRb0NnZ0VCQUxwMVlrM
```

```
GN1NlU3TTEzbWNRdXBXaitUQUR5L2h3RUhXbW1HR0ZGUmFMTVVSdXVqRHNLQ0hldTg5THZxNzFRUVdreHhKV
0FIUDZvUmUzVUN6Q2RNalhoNlBvRVFubnlDM2RVZ1gzcEdqUUcxb1QwYTd0eU1kTVd6QVc5Mk1KVzJCRjhQN1p
STWxEc2tmN0JKaDFRUHJGL3A1MytTMHVleFpOTlNCMy9aWmpMcGFudElMM2lGOW14UEtCSlgyYzVkWTY2NnJ0
MytmYWRMaEdmMEF0Rzk1ME02QlYzR21NTmJ4OHNOUVYraENRME9lSWlyaGtJaSswOG92Y0hURTdEUDcrM0JC
MmVkRG9DZ1NYU3RMSHJvZEI4d1pCQkdMQmdtN3RxY0R6NXBrYURldElyc1lLTlhRcUVSRmpVMlRZdXJCbG5sbD
Y0cGNlL1NPVWl5K0tEeGhqY0NBd0VBQWFPQ0FWd3dnZ0ZZTUFrR0ExVWRFd1FDTUFBd0VRWUpZSVpJQVliNFFn
RUJCQVFFQWdaQU1ETUdDV0NHU0FHRytFSUJEUVFtRmlSUGNHVnVVMU5NSUVkbGJtVnlZWFJsWkNCVFpYSjJa
WElnUTJWeWRHbG1hV05oZEdVd0hRWURWUjBPQkJZRUZCRWRLWjYxaHBNK1pETE5XTEtsYnhiQmxJVm9NSUc
rQmdOVkhTTUVnYll3Z2JPQUZJNUdUZE1VaWFwWEltVlVpOVQyMVpzQ045enJvWUdXcElHVE1JR1FNUXN3Q1FZR
FZRUUdFd0pPVERFTE1Ba0dBMVVFQ0F3Q1RrZ3hFakFRQmdOVkJBY01DVUZ0YzNSbGNtUmhiVEVQTUEwR0ExV
UVDZ3dHYVZOSVFWSkZNUkV3RHdZRFZRUUxEQWhUWldOMWNtbDBlVEVVTUJJR0ExVUVBd3dMYVZOSVFWSkZJ
Rkp2YjNRZEpqQWtCZ2txaGtpRzl3MEJDUUVXRjJsdVptOUFhWE5vWVhKbExYQnliMnBsWTNRdWIzSm5nZ0lRQUR
BT0JnTlZIUThCQWY4RUJBTUNYUF3RXdZRFZSMGxCQXd3Q2dZSUt3WUJCUVVIQXdFd0RRWUpLb1pJaHZjTkFR
RUxCUUFFZ2dJQkFBTm0wUUh0c2Jma1ZxeHI2akpndER2dklHUXFtdXJ5TXB1ZTFMb2c2SFpaMlFvd1pXckc4by8
0U0FnbHBNUFR1VlUwVWZBQms1ZFZmT1hubUJhNWxSTUk3aGw5ZFNNMUhObGU2QzlXQTdSUXROVi92NHFCZ
TBPbGdmYUQ0Y1VBSkRrSHNJd1dTTWxjZWxPb3hWWk5jZE93YWRYQVFIZ1lkdXpCU2RSOC9QczNwbHZJRElFOW
xyR3Q3R2tVenhTM1dVMVhWc3M2bktaRldsWmt0cVFINVkrV0VHLy82MCsxV2Y0YUk2VkhJdW9SajEwL05sRXZqY3
QwWngweWlaVTJScnF3UHFzcnRCWWJDUEl1TytDbDlRTTczcEhZM3pZcWtXWTRDTGFld3Z5UFphWTVLREJoN25
aT3A5TkoxWjJYV0Z1VklEVFpSZUgyQVJYRnBrV0RhSG1oQWNNWjlCaXFNK2h4NElYZUM2OFZ2d3VhK2d1eXBQSlp
mUnlFMzNzb3gvbHU4ZWNMMkw3L2VoRGdqaThJRVN5bVVQSTMyQ3BLZk1OMUtLTkwvS0V0ZnRHUHB1Vis2aVF
OVEU0aFRDQmNCYVNmM2R4c0dIY2xPU0M2S2U5dEw0WVJMaVgzK1lzSHFZRDk4dkxSUk9iSVFaR1dYaXF2U0ZzT
EN3SzBNMVJJd3NmYjZCOVMrWE1SQWl3cjFpZXpCZEh4WGFIODFsVCtXeEpmbkR1bjZ1eFhVejR4VHV6YVZYc1Yw
Z3ZjWTNxdVlwNjRMUjZScmhuYzJEa05EelpVNkpIeUY3TFg3MHJuOExqMTgwampHMWdlNmxsOURMUFFUa1Z5
U2hUcUNVVis5d3JVMmFFMTZycWUyWUFxL2xMSjBkV09IUzJwSmNRamgxaURwQXFHT2J3VCJ9.eyJzdWIiOiIxMj
M0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.nOLj8L1lTI9GKy06vUvJoERhMEEgTiom25ep
DEPDBvBg7kJ_mxaqWAzOGn2UEpbX387TOdWaUlcwhx02k0O_ePaTd93pEbwpFZAehILFiu8DuptFhkOZ_wC1zj
WUa7mm9NxMaoZh00wYZOfLKCaM0Wxb9YjFZCJpg3OH8c4Pr0A
```

JWT Signature

A JWT in a service request SHOULD be signed unless the Service Provider requires otherwise. This SHOULD be specified in the Service Provider's service definition.

A JWT in a response MUST be signed unless the Service Consumer has specified otherwise (either in the request or in an agreement with the Service Provider).

A signed JWT for iSHARE enabled services must meet the requirements in Generic iSHARE JWT specifications and MUST contain a hash of the HTTP body, service specific content (see next paragraph for hash definition) in the JWT.

JWT Payload

A signed JWT MUST contain the SHA256 hash of the HTTP body content in the element `HTTPBodySHA256`

A JWT MAY contain the following elements:

- `WantsResponseSigned` (request only and optional)
  Indicates that whether the Service Consumer expects the response to be signed or not. Defaults to TRUE.
- LicensePurpose (optional)
  Defaults to ...

- LicenseSubLicense (optional)
  Defaults to ...
- LicenseEndDate (optional)
  Defaults to ...
- Delegation evidence (optional)

JWT Payload for iSHARE services

```
{
        HTTPBodySHA256: "eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9"
        WantsResponseSigned: "TRUE",
        LicensePurpose: "",
        LicenseSubLicense: 0,
        LicenseEndDate: 9999-12-31,
        DelegationEvidence:
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.
TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ",

}
```

'Language' of Delegation and Authorisation

As suggested in the fourth Technical working group meeting, this is a first attempt to specify an iSHARE language for delegation and authorisation. We need this delegation and authorisation language to specify statements from the Entitled Party or Authorisation Registry. Possibly also for the restrictions of tokens. Preferably we use an existing standard (like a JSON port XACML 3.0).

Below you will find a list of authorisation and delegation cases that need to be supported both in natural language and JSON format, followed by a suggestion for "types of access" one can have. Lastly, a suggestion is done on how to represent delegation evidence in JWT/JWS format.

General cases that must at least be supported

Delegation and authorisation cases in natural language	JSON

I, Party X, grant Party Y read access to the ETA of Container #12345	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegator": { "type": "NL.KVK", "value": "Party X 12345678" },
	"type":"EU.EORI",
	"value":"Party Y NL123456789",
	"DelegatedResource":
	{
	"name":"OBJECTS.CONTAINER",
	"value":"12345"
	},
	"DelegatedAction":
	{
	"action":"READ"
	},
	"attributes":
	{
	"value":"ETA"
	}
	}

I, Party X, grant Party Y read access to the ETA of all my Containers	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": { "type": "NL.KVK", "value": "Party X 12345678" },
	"type":"EU.EORI",
	"value":"Party Y NL123456789"
	"DelegatedResource":
	{
	"name":"OBJECTS.CONTAINER",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	},
	"attributes":
	{
	"value":"ETA"
	}
	}

I, Party X, grant Party Y read access to all information of Container #12345	{
	  "NotBefore":"2017-02-24T15:04:29.329Z",
	  "NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	  "MaxDelegationDepth":"2",
	  "DelegationActive":"TRUE",
	"Delegate": { "type": "NL.KVK", "value": "Party X 12345678" },
	   "type":"EU.EORI",
	   "value":"Party Y NL123456789"
	"DelegatedResource":
	   {
	    "name":"OBJECTS.CONTAINER",
	    "value":"12345"
	   },
	  "DelegatedAction":
	    {
	    "action":"READ"
	     },
	  "attributes":
	     {
	    "value":"*"
	     }
	}

I, Party X, grant Party Y read access to all my information	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": { "type": "NL.KVK", "value": "Party X 12345678" },
	"type":"EU.EORI",
	"value":"Party Y NL123456789"
	"DelegatedResource":
	{
	"name":"*",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	},
	"attributes":
	{
	"value":"*"
	}
	}

I, Shipper A, grant RWS read access to my 'hazardous goods information' if my ship is within 5 miles of critical infrastructure	{
	 "NotBefore":"2017-02-24T15:04:29.329Z",
	 "NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	 "MaxDelegationDepth":"2",
	 "DelegationActive":"TRUE",
	"Delegate": { "type": "NL.KVK", "value": "Shipper A" },
	 "type":"EU.EORI",
	 "value":"RWS"
	"DelegatedResource":
	 {
	 "name":"*",
	 "value":"*"
	 },
	"DelegatedAction":
	 {
	 "action":"READ"
	 },
	 "attributes":
	 {
	 "NAME":"some value",
	 "SPEED":"some value",
	 "DIRECTION":"some value",
	 "CONTAINS_DANGEROUS_GOODS":"some value"
	 },
	 "Condition":
	 {
	 "name":"RANGE_IN_KM",
	 "value":"5"
	 }
	}

I, RWS, grant read access to the police to all objects that have a 'calamity' flag raised	{
	  "NotBefore":"2017-02-24T15:04:29.329Z",
	  "NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	  "MaxDelegationDepth":"2",
	  "DelegationActive":"TRUE",
	"Delegate": { "type": "NL.KVK", "value": "RWS" },
	   "type":"Investigation service",
	   "value":"PLW001828"
	"DelegatedResource":
	   {
	     "name":"*",
	     "value":"*"
	   },
	"DelegatedAction":
	   {
	     "action":"READ-"
	   },
	"attributes":
	   {
	     "value":"*"
	   },
	"Condition":
	   {
	   "flag":"CALAMITY",
	   "boolean":"TRUE"
	   }
	}

Real life example cases:

Delegation and authorisation cases in natural language	JSON

I, Planner from Carrier X, grant Substitute Carrier Y the right to delegate to third parties (such as other carriers and drivers)	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Carrier X"
	},
	"type":"EU.EORI",
	"value":"Substitute Carrier Y",
	"DelegatedResource":
	{
	"name":"*",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"*"
	},
	"attributes":
	{
	"value":"*"
	}
	}

I, Planner from Carrier X, grant Substitute Carrier Y the right to delegate to third parties (such as other carriers and drivers), except the right to delegate	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Carrier X"
	},
	"type":"EU.EORI",
	"value":"Substitute Carrier Y",
	"DelegatedResource":
	{
	"name":"*",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"*"
	},
	"attributes":
	{
	"value":"*"
	}
	}

I, Carrier X, grant ILT (Inspectie Leefomgeving enTransport) the right to view freight orders	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Carrier X"
	},
	"type":"EU.EORI",
	"value":"ILT",
	"DelegatedResource":
	{
	"name":"OBJECTS.FREIGHTORDER",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	},
	"attributes":
	{
	"value":"*"
	}
	}

I, Carrier X, grant Party Y the right to view RTIs (Reusable Transport Item) on the CMR (Convention Relative au Contract de Transport International de Marchandises par la Route)	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Carrier X"
	},
	"type":"EU.EORI",
	"value":"Party X",
	"DelegatedResource":
	{
	"name":"OBJECTS.CMR",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	},
	"attributes":
	{
	"value":"RTI"
	}
	}

<table>
<tr>
<td>I, Carrier X, grant IMS the right to update ETA on the CMR (Convention Relative au Contract de Transport International de Marchandises par la Route)</td>
<td>

```
{
 "NotBefore":"2017-02-24T15:04:29.329Z",
 "NotOnOrAfter":"2017-04-24T15:04:29.329Z",
 "MaxDelegationDepth":"2",
 "DelegationActive":"TRUE",
"Delegate": {
  "type": "NL.KVK",
  "value": "Carrier X"
 },
  "type":"EU.EORI",
  "value":"IMS",
 "DelegatedResource":
  {
   "name":"OBJECTS.CMR",
   "value":"*"
  },
 "DelegatedAction":
   {
   "action":"UPDATE"
    },
 "attributes":
    {
   "value":"ETA"
    }
}
```

</td>
</tr>
</table>

Delegation and authorisation cases in natural language	**JSON**

I, Ship X, grant Party Y the right to view the AIS (Automatic Identification System) during the journey from Basil to Rotterdam	{
	  "notBefore":"2017-02-24T15:04:29.329Z",
	  "notOnOrAfter":"2017-04-24T15:04:29.329Z",
	  "maxDelegationDepth":"1",
	  "delegationActive":"TRUE",
	  "delegator": {
	    "identifiers": [
	      {
	        "type": “EU.EORI”,
	        "value": "Jan de Rijk NL123456789"
	      },
	      {
	        "type": “NL.KVK”,
	        "value": "Jan de Rijk NL123456111”
	      }
	    ]
	  },
	  "delegatee": {
	    "identifiers": [
	      {
	        "type”:”NL.KVK",
	        "value":"Portbase NL123456788"
	      }
	    ]
	  },
	  "delegatedResource":
	    {
	      “serviceProvider”: [“TransFollow”],
	      "name":"OBJECTS.FREIGHT_DOCUMENT",
	      "value":"ALL_CREATED_BY_THIS_RULE"
	    },
	  "delegatedActions":
	    {

```
   "actions": ["CREATE","READ","UPDATE"]
  },
 "conditions":
  [
   {
    "name": "departure",
    "value": "Basel"
   },
   {
    "name": "direction",
    "value": "Rotterdam"
   }
  ],
 "attributes":
    {
   "value":"AIS"
    }
}
```

I, Ship X, grant RWS the right to view the AIS (Automatic Identification System) and cargo	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Ship X"
	},
	"type":"EU.EORI",
	"value":"RWS"
	"DelegatedResource":
	{
	"name":"OBJECTS.SHIP",
	"value":"*",
	"name":"OBJECTS.CARGO",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	}
	"attributes":
	{
	"value":"AIS",
	"value":"CARGO"
	}
	}

I, Ship X, grant RWS the right to view the AIS (Automatic Identification System) and cargo	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Ship X"
	},
	"type":"EU.EORI",
	"value":"RWS"
	"DelegatedResource":
	{
	"name":"OBJECTS.SHIP",
	"value":"AIS"
	},
	"DelegatedAction":
	{
	"action":"READ-"
	}
	}

I, Expeditor X, grant Airfreight Company Y the right to update weight and dimension of shipment item	{
	 "NotBefore":"2017-02-24T15:04:29.329Z",
	 "NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	 "MaxDelegationDepth":"2",
	 "DelegationActive":"TRUE",
	"Delegate": {
	 "type": "NL.KVK",
	 "value": "Expeditor X"
	 },
	 "type":"EU.EORI",
	 "value":"Airfreight Company Y"
	"DelegatedResource":
	 {
	 "name":"OBJECTS.CARGO",
	 "value":"dimension",
	 "value":"weight"
	 },
	"DelegatedAction":
	 {
	 "action":"UPDATE"
	 }
	}

I, Ship X, grant Expeditor Y the right to view (and subsequently publish) the ETA, if I carry his cargo	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Ship X"
	},
	"type":"EU.EORI",
	"value":"Expeditor Y"
	"DelegatedResource":
	{
	"name":"OBJECTS.CARGO",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	}
	"attributes":
	{
	"value":"ETA",
	},
	"Condition":
	{
	"carrier":"SHIP X",
	"classification":"public"
	}
	}

Delegation and authorisation cases in natural language	JSON

I, APM Terminals, grant Customs the right to clear documents for every container	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "KVK",
	"value": "APM Terminals"
	},
	"type":"Investigation Service",
	"value":"Customs"
	"DelegatedResource":
	{
	"name":"OBJECTS.CONTAINER",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	}
	"attributes":
	{
	"value":"*",
	},
	"Condition":
	{
	"clearance":"TRUE"
	}
	}

I, Party X, grant Party Y to pick up containers to APM Terminals	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Party X 12345678"
	},
	"type":"EU.EORI",
	"value":"Party X"
	"DelegatedResource":
	{
	"name":"OBJECTS.CONTAINER",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	}
	"attributes":
	{
	"value":"*",
	},
	"Condition":
	{
	"destination":"APM Terminals"
	}
	}

I, APM Terminals, grant Party X the right to provide clearance	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "APM Terminals"
	},
	"type":"EU.EORI",
	"value":"Party X"
	"DelegatedResource":
	{
	"name":"OBJECTS.CARGO",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	}
	"attributes":
	{
	"value":"*",
	},
	"Condition":
	{
	"clearance":"TRUE"
	}
	}

I, Secure Logistics, grant Portbase the right to read company information with EAN	{
	"NotBefore":"2017-02-24T15:04:29.329Z",
	"NotOnOrAfter":"2017-04-24T15:04:29.329Z",
	"MaxDelegationDepth":"2",
	"DelegationActive":"TRUE",
	"Delegate": {
	"type": "NL.KVK",
	"value": "Secure Logistics"
	},
	"type":"EU.EORI",
	"value":"Portbase"
	"DelegatedResource":
	{
	"name":"OBJECTS.ORGANISATION",
	"value":"*"
	},
	"DelegatedAction":
	{
	"action":"READ"
	}
	"attributes":
	{
	"value":"EAN",
	}
	}

Types of access*

Within iSHARE the following operations are defined:

Operation	Description
Create	Allows a Service Consumer to create new data at the Service Provider
Read	Allows a Service Consumer to view data from the Service Provider

Read-	Allows a Service Consumer to view anonymised data from the Service Provider. In order to use these rights a Service Provider MUST have available this kind of data. It is not an iSHARE reuirement to have available this kind of data, nor does iSHARE what is required to make data anonymised
Update	Allows a Service Consumer to modify data at the Service Provider
Delete	Allows a Service Consumer to remove data from the Service Provider
DelegatedAction	Indicates that an Entitled Party passes on its rights to another party. An Entitled Party SHOULD specify how many times rights can be delegated. However, this can never exceed two times. If an Entitled Party does not specify this, every party MUST assume rights can be delegated only once

As a result any combination of rights can be expressed.

	Create	Read	Read-	Update	Delete	DelegatedAction
RIGHT_1		X				
RIGHT_2		X		X		
RIGHT_3			X			
RIGHT_N	X	X		X	X	N

*Please note that the rights established here will be updated according to the latest insights on licenses soon

Possible representation of delegation evidence using JWT/JWS format

The most logical presentation of delegation evidence seems to be a signed JWT/JWS, format <header>.<payload>.<signature>

JWT Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

JWT Payload

```
{
  "NotBefore": "2017-02-24T15:04:29.329Z",
  "NotOnOrAfter":"2017-04-24T15:04:29.329Z",
  "MaxDelegationDepth":"2",
  "DelegationActive": "yes",
  "Delegate": {
    "type": "EU.EORI",
    "value": "NL123456789"
  },
    "type": "NL.KVK",
    "value": "12345678",
  "DelegatedAction":
[
    {
      "DelegatedResource":
[
        {
          "name": "OBJECTS.CONTAINER",
          "value": "12345"
        },
        {
          "name": "OBJECTS.CONTAINER",
          "value": "67890"
        }
      ],
      "attributes":
{
        "NAME":"some value",
        "SPEED":"some value",
        "DIRECTION":"some value",
        "CONTAINS_DANGEROUS_GOODS":"some value"
      },
      "Condition":
[
        {
          "name": "RANGE_IN_KM",
          "value": "5"
        }
      ],
      "DelegatedAction":
{
        "action":"READ",
        "DELEGATE":"1"
      }
    },
    {
      "DelegatedResource":
[
        {
          "name": "OBJECTS.CONTAINER",
          "value": "*"
        }
      ],
          "attributes":"*",
          "Action":"READ-",
    }
}
```

Delegation rules

In this page the rules are described, to which the processes of delegation should adhere. The rules will be implemented as policies in the policy information point(s) (PIP). The PIP provides the attribute values to the policy decision point (PDP) needed to make the decisions about delegations and authorisations.

Delegation can be explained as the act of empowering to act for another or to represent other(s). In the iSHARE scheme delegation always pertains to authorisation. Thus, one party can delegate another party to have access to services (data) on his or her behalf. However, the party who delegates always remains accountable for whichever actions are performed by the party to whom authorisations are delegated. In other words, accountability can never be delegated.

Delegation chain

A party to whom authorisations are delegated is allowed to delegate the same authorisations (or a subset thereof) to yet another party. This can occur with a total maximum of *two (2) times* (expressed by MaxDelegationDepth), excluding the originating party*.* The delegation information (token) must always contain the identity information of all previous delegating parties, including the originating party. It is the responsibility of the delegating party to know and trust the party to whom authorisations are delegated.

If any party revokes its delegation, all parties down the delegation chain will lose their authorisations that are acquired from the same delegation.

Delegation conditions

The operations (rights, actions) that are defined within the iSHARE scheme (see the table further below) may be subject to certain conditions. For example, a delegated party may read certain data and subsequently publish that data; or a delegated party may read certain data and subsequently share that data with other parties within the iSHARE scheme. Those conditions should adhere to the internal policies of the service provider. In turn, these policies are based on the data classification definitions of the service provider. The conditions only apply to the operations Read and Read-, as all other operations (i.e. Create, Update, Delete and DelegatedAction) can be enforced technically. Any conditions should be expressed in the JSON delegation policies of the PIP.

iSHARE conditions on the operations Read and Read-:

Condition	Description
Public	Data is intended to be shared with other parties outside the iSHARE scheme
For internal use	Data is intended to be shared with parties within the iSHARE scheme only
Confidential	Data is intended to be shared with explicitly designated parties within of outside the iSHARE scheme
Secret	Data is intented to be shared with explicitly designated parties within the iSHARE scheme only Security and privacy are the primary criteria here, efficiency and cost are secundary

iSHARE operations:

Operation	Description
Create	Allows a Service Consumer to create new data at the Service Provider
Read	Allows a Service Consumer to view data from the Service Provider
Read-	Allows a Service Consumer to view anonymised data from the Service Provider. In order to use these rights a Service Provider MUST have available this kind of data. It is not an iSHARE reuirement to have available this kind of data, nor does iSHARE what is required to make data anonymised
Update	Allows a Service Consumer to modify data at the Service Provider
Delete	Allows a Service Consumer to remove data from the Service Provider
DelegatedAction	Indicates that an Entitled Party passes on its rights to another party. An Entitled Party SHOULD specify how many times rights can be delegated. However, this can never exceed two times. If an Entitled Party does not specify this, every party MUST assume rights can be delegated only once

Specification

The XACML v3.0 Administration and Delegation Profile Version 1.0 will be used as the specification to define and implement delegation of authority in the iSHARE scheme. However, XACML v3.0 has been defined in traditional XML format, which is not lightweight enough for most use cases in the iSHARE scheme. Therefore, a JSON profile will be used to implement the delegation policies instead.

Notice that the XACML v3.0 specification has defined a JSON profile for XACML requests and responses only, not for the XACML policies. For this reason, the iSHARE scheme needs to provide for a JSON profile itself for implementing delegation of authority.

The RBAC (Role-Based Access Control) specification will not be implemented in the iSHARE scheme, since this is a local responsibility of the participating parties. However, the iSHARE scheme will provide for an attribute (DelegatedRole; see the table below) that can be used to support roles.

Terminology

The XACML v3.0 specification has defined the following terms as related to delegation of authority.

Definition	Explanation
Access policy	A policy that governs access
Access request	A request to determine whether access to a resource should be granted
Administrative policy	A policy that authorizes a delegate to issue policies about constrained situations

Administrative request	A request to determine whether a policy was issued by an authorized source
Backward Chaining	Finding a chain of administrative and access policies beginning with an access policy, such that each policy is authorized by the next one
Delegator	Someone authorized by an administrative policy to issue policies
Delegatee	Someone to whom something is delegated
Forward chaining	Finding a chain of administrative and access policies beginning at a trusted policy, such that each policy authorizes the next one
Issuer	A set of attributes describing the source of a policy
Reduction	The process by which the authority of a policy associated with an issuer is verified or discarded
Situation	A set of properties delineated by the Attributes elements of an access request context
Trusted policy	A policy without a PolicyIssuer element

JSON attributes

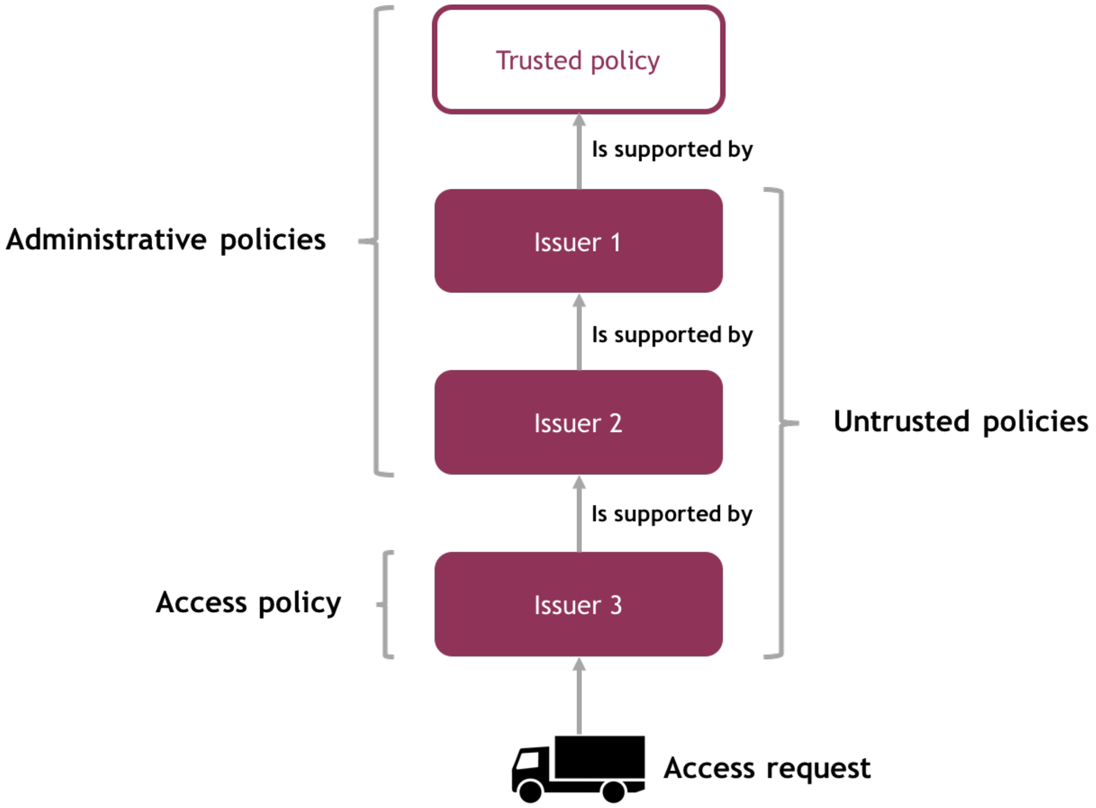
The following attributes that are related to the subject of delegation of authority will be used in the JSON profiles of the iSHARE scheme.

Attribute	Explanation
Action	The action or operation that the subject is allowed to, i.e. Create, Read, Read- (view anonymised data), Update, Delete
Condition	The condition or conditions, under which the action(s) or operation(s) are allowed
Delegator	The subject authorised by an administrative policy to issue policies
Delegatee	The subject to whom something is delegated
DelegatedRole	The role that is authorised by an administrative policy to perform a delegated action or operation
DelegatedAction	The delegated action or operation that the subject is allowed to, i.e. Create, Read, Read- (view anonymised data), Update, Delete
DelegatedResource	The object to which the delegated action or operation is allowed, i.e. Create, Read, Read- (view anonymised data), Update, Delete
DelegationActive	The boolean that determines whether the delegation is active or not

MaxDelegationDepth	The integer indicating the maximum depth of delegation that is authorised by the policy, excluding the initial node
NotBefore	The condition specifying the date and/or time, before which the delegation and delegated action(s) are not valid
NotOnOrAfter	The condition specifying the date and/or time, on or after which the delegation and delegated action(s) are not valid
Policy	The set of rules that is evaluated by the PDP, each time a subject performs an action or operation
PolicyIssuer	The source of the policy. A missing PolicyIssuer attribute means that the policy is trusted
Resource	The object to which the action or operation is allowed, i.e. Create, Read, Read- (view anonymised data), Update, Delete

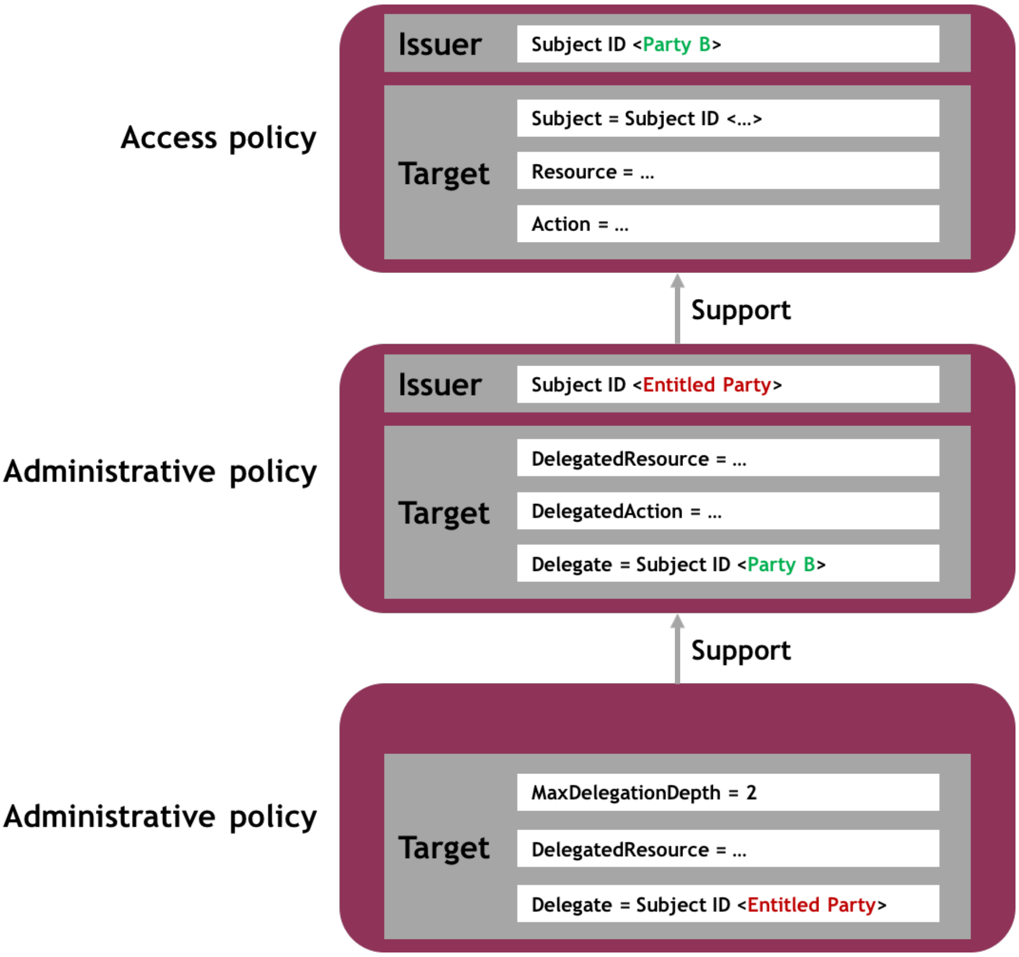
Delegation policy chain

The following figure depicts the chain of delegation policies as it will be implemented in the iSHARE scheme.



Delegation policy architecture

The following figure depicts the architecture with regard to delegation policies as it will be implemented in the iSHARE scheme.



The JSON attributes applied to primary use case 1b

The following table shows which JSON attributes are applied to primary use case 1b M2M service provision based on delegation.

Attribute	Explanation
Action	The Service Consumer performs an action or operation at the Service Provider (e.g. read data)
Condition	Not applicable in this use case
Delegate	The Entitled Party and the delegated party that issue policies

DelegatedAction	The delegated Service Consumer performs an action or operation at the Service Provider (e.g. read data)
DelegatedResource	The service at the Service Provider, to which the delegated action or operation of the Service Consumer is allowed (e.g. data)
DelegationActive	TRUE
MaxDelegationDepth	Not applicable in this use case
NotBefore	Not applicable in this use case
NotOnOrAfter	Not applicable in this use case
Policy	The set of rules at the PIP of the Service Provider that is evaluated by the PDP of the same Service Provider, each time the (delegated) Service Consumer performs an action or operation
PolicyIssuer	The source of the policy, i.c. both the Entitled Party and the delegated party (who has also become an Entitled Party through delegation)
Resource	The service at the Service Provider, to which the action or operation of the Service Consumer is allowed (e.g. data)

Token and delegation lifetime

The iSHARE scheme requires a window of time, during which signed tokens and delegation evidence are considered valid. Each token has a timestamp attribute as well as a time-to-live attribute indicating the allowable lifetime of the token (in milliseconds) after the token timestamp. Tokens that contain authorisation and/or delegation information should always have an expiration time, so that the time is limited a potential attacker can abuse a token that is intercepted by attacks (such as a man-in-the-middle attack, a session hijacking attack or a replay attack), so that the risk of impersonation or unauthorised access will be reduced.

Notice that the validity of delegation evidence may not only be determined by duration, but also by the number of times it is allowed to be used.

The Service Provider may also want to determine the lifetime during which it is allowed to access its services (data). This lifetime may overrule the central lifetime. The following provides some guidelines and a structure that can be used to determine the lifetime of the tokens.

The more sensitive the information that is accessed at the Service Provider with the token, the shorter the lifetime of the token should be. Also, the more intrusive the access rights a token provides, the shorter the lifetime of the token should be. The value of the lifetime of a token must be in milliseconds, whereas the value of the timestamp of a token must be in Unix time, i.e. the number of seconds that have elapsed since January 1, 1970 (midnight UTC/ GMT).

Refresh token

Tokens can be refreshed, but only for Human Service Consumers. Refresh tokens carry the information necessary to get a new token. A prerequisite to get a refresh token is that succesful authentication of the Human Service Consumer is required.

The following use cases apply to refresh tokens:

- A token has expired
- A Human Service Consumer accesses a new resource for the first time

Attributes

The following attributes must be used to express the timestamp and lifetime of tokens respectively:

- "Timestamp" : "some value"
- "TokenLiveTime" : "some value"

Error messages

Once the token has expired, the following error message will be displayed:

error="invalid_token",

error_description="The token has expired"

Relevant standards

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

The section "Relevant standards" covers a number of technical standards we consider to be relevant for the realisation of the iSHARE set of agreements. The table hereunder matches the technical standards to their main purposes (i.e. authentication, authorisation, cryptography, data exchange, data formatting).

Technical standard **(in alphabe-tical order)**	**Authentication**	**Authorisation**	**Cryptography**	**Data exchange**	**Data formatting**	**Description**
JSON					✓	*Formatting/structuring data in object units*

OAuth	(✓)**	✓				*Standard for authorisation (delegated access control, password handling)* *Version 2.0 MUST be used*
OpenID Connect	✓					*Authentication layer built on top of OAuth 2.0 protocol*
SAML	(✓)*	(✓)*			✓	*XML-based data format for exchange of authentication and authorisation data* *Version 2.0 MUST be used*
SOAP				✓	(✓)*	*Network protocol for the exchange of structured information*
TLS			✓			*Cryptographic protocol for secure communication of computer networks* *Version 1.2 MUST be used* *SSL (either version) MUST NOT be used*
UMA		✓				*OAuth-based access management protocol standard*
X.509			✓			*Cryptographic standard for PKI's (digital certificates & keys)* *Version 3.0 MUST be used*
XACML		✓				*Standard for authorisation policies (language, architecture, processing model)* *Either version 2.0 or 3.0 MUST be used*
XML					✓	*Formatting/structuring text documents to be both human- and machine-readable*
XML Signature			✓		(✓)*	*Standard defining an XML syntax for digital signatures to sign XML documents*

(✓)*: It is associated with the above-mentioned topic in the table, but not in the first place.

(✓)**: The use of OAuth as an authentication method may be referred to as pseudo-authentication where the access token is used as proof of identity.

HTTP

On this page a brief description of HTTP is provided. For the most recent version of the specification click on this link.

Description

HTTP is short for 'Hypertext Transfer Protocol'.

HTTPS stands for 'Hypertext Transfer Protocol Secure' (or HTTP over TLS or HTTP over SSL). It is a protocol for secure communication over a computer network and is widely used on the Internet.

Difference between HTTP and HTTPS

The difference between HTTP and HTTPS is that HTTPS consists of communication over the Hypertext Transfer Protocol that is encrypted by TLS or its forerunner SSL.

The main reason for the use of HTTPS is the authentication of the visited website and the protection of the privacy and integrity of the exchanged data.

JSON

On this page a brief description of JSON is provided. For the most recent version of the specification click on this link.

Description

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.

OAuth

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

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)

OAuth in relation to other standards & specifications

OAuth is not the same as OATH (Initiative for Open Authentication) which is a reference architecture for authentication and not a standard for authorisation.

OAuth is linked to OpenID Connect since OIDC is the authentication layer built upon OAuth 2.0.

OAuth is not the same as XACML which is an open standard for authorisation policies but can be use within XACML for ownership consent and access delegation.

OAuth 2.0

OAuth 2.0 provides specific authorisation flows for web applications, desktop applications, **mobile phones**, and living room devices.

OAuth 2.0 is not backwards compatible with OAuth 1.0.

Because OAuth 2.0 is more of a framework than a defined protocol, one OAuth 2.0 implementation is less likely to be naturally interoperable with another OAuth 2.0 implementation.

OAuth 2.0 does not support signature, encryption, channel binding, or client verification. It relies completely on TLS for some degree of confidentiality and server authentication.

OpenID Connect

On this page a brief description of OpenID Connect (which we would like to stress is the most recent version of OpenID and an authentication layer on top of OAuth) is provided. For the most recent version of the specification click on this link.

Description

Open ID 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.

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.

SAML

On this page a brief description of SAML is provided. For the most recent version of the specification click on this link.

Description

SAML is short for "Security Assertion Markup Language" and is an open standard and XML-based data format to exchange authentication and authorisation data between identity providers and service providers

SAML specifies the assertions (= claims) in XML passed from the user to identity provider and to the service provider.

After the user requests a service from the service provider, the service provider obtains an ID assertion from the ID provider which the service provider can use to make an access control decision ("Is user authorised to use the requested service?"). Before the ID provider shares the ID assertion with the service provider, the ID provider may ask for extra information from the user (i.e. user name, password, fingerprint) for authentication reasons.

In SAML, one single ID provider may provide SAML assertions to many service providers. Likewise, one single service providers may rely on assertions from multiple ID providers

One of SAML's most important requirement is that of Single Sign On (SSO): after users log in once for a service (web or local environment) for which they have authorisation, they can access the same service repeatedly/multiple times without log-in credentials being asked and validated again.

Important note: The most recent version SAML 2.0 was built with the assumption of the client being a web browser from desktops/laptops. Unfortunately because of this presumption it doesn’t adapt well into the mobile application ecosystem

SAML's basic standards

SAML is built on the following existing standards:

- XML (eXtensible Markup Language)
- XSD (XML Schema Definition)
- XML signature standard for authentication and message integrity
- XML encryption standard to encrypt identifiers, attributes and assertions. XML encryption is reported to have security concerns
- HTTPS (Hypertext Transfer Protocol Secure) as communications protocol
- SOAP (Simple Object Access Protocol): a network protocol for the exchange of structured information

The SAML specifications recommend and even mandate (for some cases) specific security standards and protocols such as TLS 1.0 (for transport-level security) and XML Signature and XML Encryption (for message-level security)

SAML's building blogs

SAML includes assertions, protocols, bindings and protocols.

- Assertions: the syntax and semantics of the assertions are described in "SAML Core", together with the protocol needed to request and transmit assertions
- Protocols: "SAML protocol" focusses on what is transmitted, not how (as this is determined by the choice of binding)
- Bindings: "SAML binding" describes how how SAML requests and responses map onto to other standard messaging or communication protocols. An example of an (synchronous) binding is the SAML SOAP binding
- Profiles: "SAML profile" is a specific form (profile) of a defined use case with a given combination of assertions, protocols and bindings

SAML 2.0

SAML 2.0 replaces SAML 1.1: In SAML 1.1 Web Browser SSO Profiles are initiated by the ID Provider. In SAML 2.0, however, the flow begins at the service provider who issues an explicit authentication request to the ID provider (significant new feature).

It makes use of security tokens containing assertions to pass information about a user.

It enables web-based authentication and authorisation scenarios including cross-domain SSO, which helps reduce the administrative overhead of distributing multiple authentication tokens to the user

When SAML 2.0 was built, it was built with the assumption of the client being a web browser from desktops/laptops. Unfortunately because of this presumption it doesn’t adapt well into the mobile application ecosystem

SOAP

On this page a brief description of SOAP is provided. For the most recent version of the specification click on this link.

Description

SOAP stands for 'Simple Object Access Protocol' and is a network protocol for the exchange of structured information. The SOAP message format follows the "XML Information Set" (XML InfoSet) which is a specification describing the data model for an XML document as a set of information items.

SOAP relies on application layer protocols for message negotiation and transmission such as HTTP or "Simple Mail Transfer Protocol (SMTP)".

TLS

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

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.

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.

TLS versions

TLS 1.0: upgrade of version SSL 3.0. The differences between TLS 1.0 and SSL 3.0 are not big, but significant enough to exclude interoperability between TLS 1.0 and SSL 3.0. Version TLS 1.0 does include a means by which a TLS implementation can downgrade the connection to SSL 3.0.

TLS 1.1: Added protection against cipher-block chaining (CBC) attacks. (CBC = each block of plaintext is XORed with the previous cipher text block before being encrypted), added support for Internet Assigned Numbers Authority (IANA) registration of parameters

TLS 1.2: improved hash functions (MD5-SHA-1), improvement in the client's and server's ability to specify which hash and signature algorithms they accept, expansion of support for authenticated encryption ciphers, added TLS Extensions definition and Advanced Encryption Standard cipher suites

TLS 1.3: removing support for some hash functions (MD5 and SHA-224), requiring digital signatures even when a previous configuration is used, integrating use of session hash

UMA

On this page a brief description of UMA is provided. For the most recent version of the specification click on this link.

Description

UMA is short for User-managed Access and is an OAuth-based access management protocol standard.

Its purpose is to “enable a resource owner to control the authorisation of data exchange and other protected-resource access made between online services on the owner’s behalf or with the owner’s authorisation by an autonomous requesting party”.

UMA in relation to other standards & specifications

UMA does not depend or have to use the OpenID protocols (most recent version is OpenID Connect) to identify users or (optionally) collect identity claims from a requesting party (for access policy checks).

In the same fashion, UMA does not depend or have to use XACML as policy language (to write access policies and rules) and validate authorisation requests based on the policies and rules.

UMA has no restrictions regarding the policy format, as the Authorisation Server is in charge and in control of the policy evaluation.

The UMA and XACML flows for requesting access have common features.

X.509

On this page a brief description of X.509 is provided. For the most recent version of the specification click on this link.

Description

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.

Apart from that, it also specifies the formats for public key certificates, certificate revocation lists (CRL’s), attribute certificates, and a certification path validation algorithm.

It assumes a strict hierarchical system of certificate authorities for issuing the certificates. Unlike web of trust models (i.e. encryption method "Pretty Good Privacy (PGP)") where anyone (not just special certificate authorities) may sign and thus verify the validity of others' key certificates.

Structure of X.509 certificates

The structure of X.509 digital certificates is expressed in a formal language: Abstract Syntax Notation One (ASN.1) which is a standard and notation that describes rules and structures for representing, encoding, transmitting, and decoding data in telecommunications and computer networking

The content of a digital certificate is structured and divided into fields. The fields of a X.509 digital certificate are listed hereunder:

- Certificate
- Version Number
- Serial Number: Used to uniquely identify the certificate
  Signature Algorithm ID: The algorithm used to create the signature ID.Issuer Name: Name of the entity that verified the information and issued the certificateValidity period
  - Not Before
  - Not After
- Subject name: Name of the person, or entity identified

Subject Public Key InfoPublic Key AlgorithmSubject Public Key

  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)

- Extensions (optional)
- Certificate Signature Algorithm: The algorithm used to create the certificate signature
- Certificate Signature: The actual certificate signature to verify that it came from the issuer

Each extension (additional field) has its own ID, expressed as object identifier, which is a set of values, together with either a critical or non-critical indication. If the critical value cannot be recognised or processed, the certificate is rejected. Non-critical values may be ignored if not recognised, but must be processed if recognised.

Types of extensions

- Information about a specific usage of a certificate
- Certificate filename extensions

XACML

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

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).

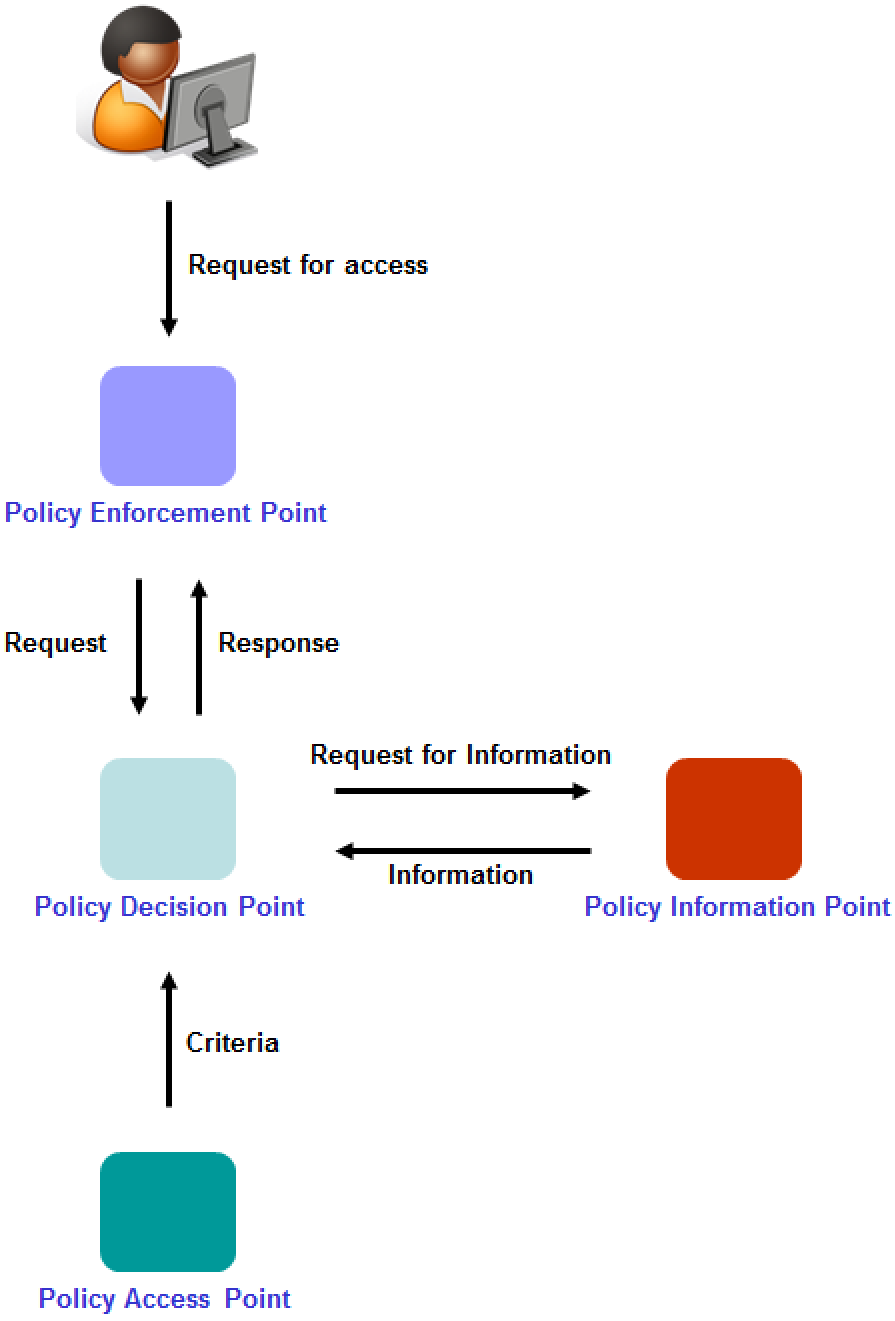
Moreover, with the help of XACML authorisations can be arranged and managed in detail. This is called fine-grained authorisation. XACML supports the use of security labels, rules with arbitrary attributes, rules with a certain duration and dynamic rules.

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 allowd 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.

Roles and interactions in XACML

The following figure shows the involved roles Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Access Point (PAP) and Policy Information Point (PIP) in XACML and how they are interacting in order to process the user's request for access.



XML

On this page a brief description of XML is provided. For the most recent version of the specification click on this link.

Description

XML is short for "eXtensible Markup Language" to encode text documents in a format that is both human- and machine-readable.

XML Signature

On this page a brief description of XML Signature is provided. For the most recent version of the specification click on this link.

Description

XML signature is a standard for authentication and message integrity that defines an XML syntax for digital signatures to sign primarily XML documents.

It is used within i.e. SOAP & SAML.

PKI

Here the (root) certificates in used in iSHARE are specified.

- Production PKI
- Test PKI
- POCs PKI

Production PKI

TBD

Test PKI

TBD

POCs PKI

This page contains the Certificate Root and Certificate Authorities that ar in use for the POCs. They SHOULD be trusted by all POC participants.

Root certificate

```
-----BEGIN CERTIFICATE-----
MIIGBDCCA+ygAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgZAxCzAJBgNVBAYTAk5M
MQswCQYDVQQIDAJOSDESMBAGA1UEBwwJQW1zdGVyZGFtMQ8wDQYDVQQKDAZpU0hB
UkUxETAPBgNVBAsMCFNlY3VyaXR5MRQwEgYDVQQDDAtpU0hBUkUgUm9vdDEmMCQG
CSqGSIb3DQEJARYXaW5mb0Bpc2hhcmUtcHJvamVjdC5vcmcwHhcNMTcwNjI3MDYx
NDM0WhcNMjcwNjI1MDYxNDM0WjCBkDELMAkGA1UEBhMCTkwxCzAJBgNVBAgMAk5I
MQ8wDQYDVQQKDAZpU0hBUkUxETAPBgNVBAsMCFNlY3VyaXR5MSgwJgYDVQQDDB9p
U0hBUkUgTkwgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSYwJAYJKoZIhvcNAQkBFhdp
bmZvQGlzaGFyZS1wcm9qZWN0Lm9yZzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCC
AgoCggIBAKiuQXA3R14zhAZ59xu4J6j8h5LaMYoMzFIRzeV+665E8bnoK2eQSC5a
YMvsb80o8DxHHjiqPJiJW1n1oT86UAKgaEEnJ8/GhF+2kyOlybdpM21Q6bNwkJ5v
L4SD/GYBPmWsVt7X6pLAkFsweXu6wRzvrYXWcVm/z/3SHX9AZFg6HDZRsGGDnnRw
14nHYpb/oh7p5h6atI+X0aOD4HhQJ1ahQLVozIbbCFDfpKu9mrDXzKYDaNstrYn2
DmbtV40BC5FW1OT0HLO/texnnhtNrjq6IVgUkZ54NHT8Y2EQNmajy8RilrLU1FHS
/ka03w8sV0sXDsLeBwbxl3BYHpisPMWpMJDFU8b92tlYjk2lUDnHqDUi5BHRdRYq
VZeWBSL+Qevpezr3mCL9ynhGPy+tNyDjyVjb/y7hlftAzZzodRwItQPzpKHCWQLs
WX+JwM9lwu5uq6lcqxHGPSAB0o/ME80KE3a4KnjCGYvlZiPJtrad0HZDRR/hEAne
n3HE3fTZE42u2wBLTfZB1D8Kxjc44vJv8L4JOaLlt/ooMT913sGCSJDPQUwv+/Vv
YDV8ngkgzRCpFng2NrPaWao6RKJ99bBMkKFQ4vsdtvwi42GK2OBK7ozXnNS7B5qc
ljdVnrmmH8fCPJ/s7L9BDYw/IKrd5wHaSH1kZ7/DRa0fa2mMJjfLAgMBAAGjZjBk
MB0GA1UdDgQWBBSORk3TFImqVyJlVIvU9tWbAjfc6zAfBgNVHSMEGDAWgBRLYazz
oNpuBb//4Sr1Ior0iP04RjASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQE
AwIBhjANBgkqhkiG9w0BAQsFAAOCAgEAQ7GRIQ3Q+TRUumxOXc+dGJnx98EK1qD8
E1uEptlS+VROWAZ22QeLCPk/nNDVs2AmCADZF0JoX2+RJNjq7pX2+AxcL1owWQoi
3GRtL6GABHByulTfJfvodYjUipI1zmIvcWKzNnNCC9A0rdtUJyRjZvGZt32K77ai
RNGiSCtVyCBuFBPtqCkXIz86e/wzQ1fwBeCRB0WDMoSdXbSkt/tapyGoU7oAj2DV
WbtKaCnkKiysE19r1RCiZI2WAHLcuU9iLvNM1Mfowv9avI+rVq2YlKUOuCIrD7s/
ILRLXg55VwqMJT33/50NFnu3H8ebmqEhkGYStk7p3FGRxgptd2OJnqAt5nG1pspH
QuD+vYBoKkkMw40qvy+eeYkhyzKcJTKeOsfI29fyQx/eFSmWRheT188+jZQyCqEQ
pZRgtku+2KPQbCBxVeCfHacyS16+9ZOVs1zXWGfIqXKXwZF1v6CDyL7bedJZEuTU
1wUpkEUJH/IPmdp2ZMNMcss/BIdyf/+pYwyMnB6DJocDwMjlm3cUEsbtT393wIie
0mohWiu8myTxkCfN1VJs4W9chSx5/DxVwDtFoT4nsqVK9F6DKYJAJ95UR+C+RiCS
+x7t4r8cup0AiJpg7JEGr5I9kdlBXKAk78Pr/oqZogFymWPzoWUy48Ye6WxaAA1s
+h6hVQ22MCg=
-----END CERTIFICATE-----
```

POC Certificate Authority certificate

```
-----BEGIN CERTIFICATE-----
MIIGCDCCA/CgAwIBAgIJAN7kMSjuGT9KMA0GCSqGSIb3DQEBCwUAMIGQMQswCQYD
VQQGEwJOTDELMAkGA1UECAwCTkgxEjAQBgNVBAcMCUFtc3RlcmRhbTEPMA0GA1UE
CgwGaVNIQVJFMREwDwYDVQQLDAhTZWN1cml0eTEUMBIGA1UEAwwLaVNIQVJFIFJv
b3QxJjAkBgkqhkiG9w0BCQEWF2luZm9AaXNoYXJlLXByb2plY3Qub3JnMB4XDTE3
MDYyNzA2MDY1NFoXDTM3MDYyMjA2MDY1NFowgZAxCzAJBgNVBAYTAk5MMQswCQYD
VQQIDAJOSDESMBAGA1UEBwwJQW1zdGVyZGFtMQ8wDQYDVQQKDAZpU0hBUkUxETAP
```

```
BgNVBAsMCFNlY3VyaXR5MRQwEgYDVQQDDAtpU0hBUkUgUm9vdDEmMCQGCSqGSIb3
DQEJARYXaW5mb0Bpc2hhcmUtcHJvamVjdC5vcmcwggIiMA0GCSqGSIb3DQEBAQUA
A4ICDwAwggIKAoICAQCuvV8gSQDx7g1PYvxcuK6uDIwWZNZKdF0wJoGjcIlqPJWF
3pP2xCJq5ZRnUQnpW0WTCWw9A4uZfCIWqJSoISh4nE7UmMmfw45ms+7SwJxfc7E+
Y4ffMDMyLcmvHYYLqGDoZu4qnpytsz+Xs1e8ESyNtIlXooZ6O+C1he+XmXpSChOj
h5Pnz7RHz4cS7Zw38B9aNA3WktF+yR7ijkTUN887aZAplmrNZoioGnM/E1RFwnLq
rk5E84kOTzexsNILBpBzoZkLPz8yYI0OJ42/RT5m9YPOIRWMwWcgQqmBHIgMCaUO
jAslex2Bx1uQtBJcti+DIf+ZIGPm/TcwsaCC+RbE51SmMqwXYe/BoAlAZKYSgG8o
utN+Fd3Ew3h3YJcA86wDT9bKMzS9oSV1EjXc8v+40pp//AdWMPf2q15i/QotTj+S
GP2cJQvcfRBJ94IfG41IBolEK7jEUN2JUcowAdNsYfM7EdoKGhIn+bkCXnZR3bnf
BKBAXH64MOp7Ii1NukjPpEqemyM3//XKn/1lXzU43rbazwbxyGBYq3AHv5io7MS1
TwegD/hNmTOEGHffZ/CzJghm6WvgmcmUALu2IFcDpmYZI3UI3SKzwaddi7/vcGer
5VVDglRtVtvHk3eJRT0L9SFqHIWsLunI/dZSJE8pKpStG5Lzj7Y/psOlBpahnwID
AQABo2MwYTAdBgNVHQ4EFgQUS2Gs86DabgW//+Eq9SKK9Ij9OEYwHwYDVR0jBBgw
FoAUS2Gs86DabgW//+Eq9SKK9Ij9OEYwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwDQYJKoZIhvcNAQELBQADggIBABt+I4ZnS45c2IFsKV+BA8JP5OWC
PoaJyl3PCELjedVfB4rXyF946+ILARcBZg35F07WzHtmi/afXh6entvVMEAlEmH6
ln8sR9hoM3rHnYRtSIJmJs2gSF8wgCOZd1pyfrBVu3f3SXbUgNjoe5tEW6xsOQsj
jqNnQiJMJx6ea56L2kbW7E6kOs+Mck9Kz8ZQQB58iPGyx3ahMLOrxbPoItbqKuyD
wco7AzLf7ea9zye0up8ubNDYFaKJfiIDsnVbUPA6FbTn4fSQpeeOK1fjrzSaUpeM
OdOomj0Zjwt6K7W7ckxoIfOecW4dcPENpXImkBPQXsGxvClDf/6e/jPti3CPgxJF
3747Hq6tBSH0GzCrYv4bForQu43MzqZKHbX8FF1PpHSaiXJK/Hu8WJDXXBq5Pede
l/lJSajdTsUDsiFXkj/pY0uJ6M0x/EonozaCPcHwdPsvr6nrrHWQXo4ayP7ntegJ
A3GrGXcaP+peEQmF9nWgVwPq33C1TrPNaiMxHz5toxl0YhnbA+5eH2CTBjDFJnr2
uaeh8BzbkdE29WkOsqJZAIUEMmRwxcxBW20JGAlhF6MPFADjPYG0Ljdjbwq2H+LQ
tRf+tE6Z7nwM/cAT4dEB7Me1uJrYucVjLLSNXCRKQaDKKZMoHhAciLeKLMrSgUDa
Ai0AUKXduCymUw3n
-----END CERTIFICATE-----
```

Scheme owner certificate

```
-----BEGIN CERTIFICATE-----
MIIGCDCCA/CgAwIBAgICEAQwDQYJKoZIhvcNAQELBQAwgZAxCzAJBgNVBAYTAk5M
MQswCQYDVQQIDAJOSDEPMA0GA1UECgwGaVNIQVJFMREwDwYDVQQLDAhTZWN1cml0
eTEoMCYGA1UEAwwfaVNIQVJFIE5MIENlcnRpZmljYXRlIEF1dGhvcml0eTEmMCQG
CSqGSIb3DQEJARYXaW5mb0Bpc2hhcmUtcHJvamVjdC5vcmcwHhcNMTcwNjI3MDgy
OTIzWhcNMTgwNzA3MDgyOTIzWjCBnDELMAkGA1UEBhMCTkwxCzAJBgNVBAgMAk5I
MRIwEAYDVQQHDAlBbXN0ZXJkYW0xDzANBgNVBAoMBmlTSEFSRTERMA8GA1UECwwI
U2VjdXJpdHkxIDAeBgNVBAMMF2lTSEFSRSBTY2hlbWUgT3duZXIgUE9DMSYwJAYJ
KoZIhvcNAQkBFhdpbmZvQGlzaGFyZS1wcm9qZWN0Lm9yZzCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALp1Yk0cu6U7M13mcQupWj+TADy/hwEHWmmGGFFR
aLMURuujDsKCHeu89Lvq71QQWkxxJWAHP6oRe3UCzCdMjXh6PoEQnnyC3dUgX3pG
jQG1oT0a7tyMdMWzAW92MJW2BF8P7ZRMlDskf7BJh1QPrF/p53+S0uexZNNSB3/Z
ZjLpantIL3iF9mxPKBJX2c5dY666rt3+fadLhGf0AtG950M6BV3GmMNbx8sNQV+h
CQ0OeIirhkIi+08ovcHTE7DP7+3BB2edDoCgSXStLHrodB8wZBBGLBgm7tqcDz5p
kaDetIrsYKNXQqERFjU2TYurBlnll64pce/SOUiy+KDxhjcCAwEAAaOCAVwwggFY
MAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgZAMDMGCWCGSAGG+EIBDQQmFiRP
cGVuU1NMIEdlbmVyYXRlZCBTZXJ2ZXIgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFBEd
KZ61hpM+ZDLNWLKlbxbBlIVoMIG+BgNVHSMEgbYwgbOAFI5GTdMUiapXImVUi9T2
1ZsCN9zroYGWpIGTMIGQMQswCQYDVQQGEwJOTDELMAkGA1UECAwCTkgxEjAQBgNV
```

```
BAcMCUFtc3RlcmRhbTEPMA0GA1UECgwGaVNIQVJFMREwDwYDVQQLDAhTZWN1cml0
eTEUMBIGA1UEAwwLaVNIQVJFIFJvb3QxJjAkBgkqhkiG9w0BCQEWF2luZm9AaXNo
YXJlLXByb2plY3Qub3JnggIQADAOBgNVHQ8BAf8EBAMCBaAwEwYDVR0lBAwwCgYI
KwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggIBAANm0QHtsbfkVqxr6jJgtDvvIGQq
muryMpue1Log6HZZ2QowZWrG8o/4SAglpMPTuVU0UfABk5dVfOXnmBa5lRMI7hl9
dSM1HNle6C9WA7RQtNV/v4qBe0OlgfaD4cUAJDkHsIwWSMlcelOoxVZNcdOwadXA
QHgYduzBSdR8/Ps3plvIDIE9lrGt7GkUzxS3WU1XVss6nKZFWlZktqQH5Y+WEG//
60+1Wf4aI6VHIuoRj10/NlEvjct0Zx0yiZU2RrqwPqsrtBYbCPIuO+Cl9QM73pHY
3zYqkWY4CLaewvyPZaY5KDBh7nZOp9NJ1Z2XWFuVIDTZReH2ARXFpkWDaHmhAcMZ
9BiqM+hx4IXeC68Vvwua+guypPJZfRyE33sox/lu8ecL2L7/ehDgji8IESymUPI3
2CpKfMN1KKNL/KEtftGPpuV+6iQNTE4hTCBcBaSf3dxsGHclOSC6Ke9tL4YRLiX3
+YsHqYD98vLRRObIQZGWXiqvSFsLCwK0M1RIwsfb6B9S+XMRAiwr1iezBdHxXaH8
1lT+WxJfnDun6uxXUz4xTuzaVXsV0gvcY3quYp64LR6Rrhnc2DkNDzZU6JHyF7LX
70rn8Lj180jjG1ge6ll9DLPQTkVyShTqCUV+9wrU2aE16rqe2YAq/lLJ0dWOHS2p
JcQjh1iDpAqGObwT
-----END CERTIFICATE-----
```

Legal

This section covers the legal specifications of the iSHARE scheme. The legal specifications consist of three documents:

1. Accession Agreement (separate versions for Adhering Parties and Certified Parties);

The Accession Agreement is a bilateral agreement between each separate participant and the Scheme Owner. The Operational working group is currently determining how the Scheme Owner will operate. By signing the Accession Agreement, an Adhering or Certified Party becomes a participant of the iSHARE Scheme, and declares and agrees with the conditions set forth in the Accession Agreement and the Terms of Use. A participant also declares that it will abide to all relevant laws and regulations that apply to its business, amongst which the laws and regulations described in the Legal Framework.

2. Terms of Use;

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.

3. Legal Framework.

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.

Accession Agreement for Adhering Parties

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. Participation fees are non-refundable fees and are 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.
- 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

APPENDIX 2: PARTICIPATION FEES

Accession Agreement for Certified Parties

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. Participation fees are non-refundable fees and are 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.
- 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

APPENDIX 2: PARTICIPATION FEES

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 following Articles [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, information on licences and information on proxies 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 with the exchanged Data as established by the Entitled Party.

2.7. **Data or Dataset**: the data exchanged in the context of the iSHARE Scheme.

2.8. **Entitled Party**: a Party that grants a (sub-)license to a Service Consumer in relation to a specific Dataset.

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 of 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.

2.16. **Service Consumer**: a Party who requests the Service Provider to provide a service relating to the exchange of Data.

2.17. **Service Provider**: a Party who provides a service relating to the Data to be exchanged with a Service Consumer.

2.18. **Terms of Use**: this document, including the Annexes.

2.19. **Website**: ishare-project.org

ARTICLE 3. RIGHTS AND OBLIGATIONS OF ADHERING PARTIES

3.1. 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. 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 Consumer 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 Consumers 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 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 from time to time hereafter. The trademarks and trade names may only be used in connection with iSHARE Scheme related activities. In the event the Scheme Owner decides to modify or discontinue the use of one or more of the trademarks and trade names or to use one or more additional or substitute trademarks or trade names, the Adhering Party agrees to immediately and fully comply with the instructions of the Scheme Owner in that respect.

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 that are specified in the iSHARE Scheme <include reference to document still to be drafted by another working group>.

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 within [XX] hours of becoming aware of said failure and/or breach and shall promptly take adequate remedial measures. The Certified Party shall warrant that the information it provides is complete and accurate.

4.3. The duty to notify as referred to in the previous paragraph includes in any event details regarding:

- the (suspected) cause of the network failure and/or security breach;
- the (currently known and/or anticipated) consequences thereof;
- the (proposed) solution;
- the contact details in connection with follow-up action;
- what measures have already been implemented.

4.4. 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 connection with iSHARE Scheme related activities. In the event the Scheme Owner decides to modify or discontinue the use of one or more of the trademarks and trade names or to use one or more additional or substitute trademarks or trade names, the Adhering Party agrees to immediately and fully comply with the instructions of the Scheme Owner in that respect.

ARTICLE 5. RIGHTS AND OBLIGATIONS OF THE SCHEME OWNER

5.1. The Scheme Owner is not allowed to access exchanged Data. [The Scheme Owner will facilitate the iSHARE Scheme and will only have an administrative role with regard to these Terms of Use and other legal documents associated with the iSHARE Scheme.] <depending on the role of the Scheme Owner>

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, if that Party breaches these Terms of Use and/or applicable laws and regulations in respect of the iSHARE Scheme.

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. <input from the functional working group is required here>

5.5. [The Scheme Owner will endeavour to make a decision within four (4) weeks regarding the possible admission of the Certified Party.]<depending on the admission procedure which will be described in Annex IV>

5.6. The Certified Party shall conduct an annual 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 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.

ARTICLE 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 rules and procedures as described in Annex V.

9.2. Amendments will apply subject to a term of 30 days following publication of the amendment on the Website or after announcement by electronic communication. Minor changes can be implemented at any time.

9.3. 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. Promptly after giving notice of termination of the Accession Agreement, a Certified Party shall communicate the termination of its participation to all Parties affected.

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.

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 (technical) specifications of the iSHARE Scheme

Annex IV: Admission procedure

Annex V: Change procedure

Legal Framework

As stipulated in the Accession Agreement and the Terms of Use, all iSHARE participants are expected to comply with all laws and regulations that apply to their business. The following rules and regulations are of particular relevance when exchanging data within the iSHARE scheme:

1. Competition law
2. Privacy and data protection law
3. eIDAS Regulation
4. Dutch Civil Code

1.1 Competition law

1.1.1 Agreements

First and foremost, it should be noted that it is not the intention of the iSHARE scheme to limit competition in any shape or form. In all cases, an important principle of the iSHARE scheme is to create a level playing field and foster efficiency gains. Nonetheless, it is important to carefully draft the agreements (i.e. the Accession Agreement and

Terms of Use) 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.

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 may be found for exchanging information. Exchanging information can lead to efficiency gains. For the determination of efficiency gains, there are three further conditions to 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).

1.1.2 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.

Currently, the iSHARE scheme is intended to be an open framework, accessible for just any party – admitted to the iSHARE scheme or not - seeking to use its functionalities. For the parties wishing to participate in iSHARE, the requirements that will be formulated in order to become a participant must also not restrict competition to the extent that they, for instance, could be perceived as a refusal to supply. In other words, the requirements must not be so exacting that they exclude specific parties, thereby enabling the participants to corner the market. The result of the foregoing may be that the economic competitiveness will be jeopardized.

1.2 Privacy and data protection law

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 organizational 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 SAS70, ISAE 3402 and the SSAE No. 16.

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 sharing 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. The iSHARE scheme should put the participating parties in control of 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.

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.

1.3 eIDAS Regulation

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. For instance, the qualified trust service providers need to inform the supervisory body of any change in the provision of its services and must maintain sufficient financial resources or obtain appropriate liability insurance. 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, it needs to be considered which eIDs are to be used (either offering ‘low’, ‘substantial’ or ‘high’ assurance levels) and which trust service providers are to be engaged (qualified or non-qualified) and the roles these trust service providers have within the iSHARE scheme. The selection of eIDS and trust service providers are also relevant for the international orientation of the iSHARE scheme and to foster the cross-border interoperability of electronic trust services.

1.4 Dutch Civil Code

In setting up the iSHARE scheme, the relevant provisions of the Dutch Civil Code should also be taken into account. This primarily relates to the Accession Agreement 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.

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 [SPECIFY SERVICES];

- 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;
- 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;
- 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”);

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 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]

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[PvdWI1]]

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][PvdWI2] 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, with a view to the careful processing of Data, wish to make arrangements regarding the exchange of 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;
- 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");

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. **Data**: all data exchanged between the Parties under this Data Exchange Agreement, including Personal Data.

1.3. **Personal Data**: personal data within the meaning of Article 1 (a) of the Wbp.

1.4. **Dataset**: the 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]] [PvdWI3] and shall use reasonable endeavours to safeguard the quality of the Dataset. [FS|I-N4]

2.2. The Parties declare to process the Data, as specified in Annex 1, in a proper and careful manner.

2.3. With respect to the processing of 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.

3.3. 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 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 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 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 Data available to a third party.

5.3. If one of the Parties is summoned by a competent court or other authority to submit 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 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 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 forward 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 [AND/OR] THE AGREEMENT[PvdWI5]].

7.3. 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]

[PvdWI1]It may be that the parties already have an agreement in place, in which case this data exchange agreement is supplementary to that agreement. In the event the parties do not have an agreement, this phrase should not be included.

[PvdWI2]It needs to be specified which parties are going to exchange data.

[PvdWI3]The purpose of exchanging the data must be specified as well as the parties that are exchanging this data.

[FS|I-N4]Should this not be limited to Personal Data?

[PvdWI5]In the event this data exchange agreement forms an integral part of the agreement already in place between the parties.

Operational

This section covers the operational topics of the iSHARE scheme.

iSHARE needs to become a sustainable endeavour which is constantly improved by its stakeholders. To organise the constant improvement, a governing body must be shaped: the Scheme Owner*. The Scheme Owner facilitates the correct operation of the iSHARE scheme through administering the aspects defined in this section:

- Operational processes
- Service levels
- Communication

*The exact scope/form of the Scheme Owner is yet to be defined. For an overview of the assumptions upon which processes and service levels are based, see operational assumptions

Operational assumptions

The aspects defined in this section are based on the following assumptions:

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. The Operational working group does not decide upon the form of the Scheme Owner; it focuses instead on the operational processes that the eventual Scheme Owner will need to administer
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 does not decide upon the financing constellation of the Scheme Owner

Main goals of the Scheme Owner include:

- Safeguard correct operation of the scheme (including the correct operation of any software operated by the Scheme Owner);
- Responsible for correctness of all scheme specifications;
- Facilitates and coordinates the continuous development and improvement of the scheme.

Other assumptions made to base the Operational section on include:

- 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 organisations 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 scheme;

- The Scheme Owner has the intention to keep onboarding time as low as possible. Guideline for Adhering Parties: within 5 minutes you can become iSHARE compliant;
- The Scheme Owner regularly tests the robustness of the scheme and plans for mitigation of risks/threats (e.g. identifying Single Points of Failure);
- The management of disputes regarding data shared through the use of iSHARE is not a core role of the Scheme Owner; disputes should be handled by involved parties.

Scheme Owner

The Scheme Owner is the entity that facilitates the correct operation of the iSHARE scheme by administering the operational processes, service levels and communication guidelines.

The exact scope/form of the Scheme Owner is yet to be defined. For an overview of the assumptions upon which processes and service levels are based, see operational assumptions.

Operational processes

This section describes the operational processes necessary to administer the iSHARE brand and scheme.

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

Admission

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

The admission process describes the steps that parties MUST take to be admitted to the iSHARE scheme. The process is the responsibility of, and facilitated by, the Scheme Owner.

Admission includes:

- An interested party - that has not signed an accession agreement yet - wants to fulfil one or more roles in the scheme (e.g.: adhering party roles, certified party roles or both);
- An adhering and/or certified party wants to expand its current role(s) by one or more role(s) (e.g. an adhering party also wants to start fulfilling a certain certified role);
- An adhering and/or certified party wants to change its legal form;
- A certified party wants to change its service offering substantially.

Goal

The goal of the admission process is to let interested parties join iSHARE in a simple and controlled way - as fast as possible. A controlled admission process is important to warrant trust in the iSHARE brand. It guarantees that all parties signing an accession agreement fulfil the scheme's accession criteria.

It SHOULD be possible to become an iSHARE adhering party within 5 minutes.

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 **interested party** is responsible for implementing the guidelines set out in iSHARE, and for delivering the documentation necessary to be admitted.

Expected administrative burden on the Scheme Owner

To be determined.

Sequence

1. The interested party formally requests admission to the iSHARE scheme as an adhering and/or certified party, to the Scheme Owner. The request MUST be approved by a legally responsible executive of the interested party;
2. The Scheme Owner has 5 working days to acknowledge the admission request, to check whether the interested party has not been excluded from iSHARE in the past 12 months, to check whether the interested party is a party recognised by relevant authorities in the country where the organisation in registered, and to invite the interested party for an intake;
3. During and after the intake, the Scheme Owner tests the admission against the relevant admission criteria for any impediments;
    - If impediments are found, the Scheme Owner issues a written statement (e.g. via an e-mail) to the interested party indicating what adjustments are desired.
4. If no impediments are found, the Scheme Owner requests the interested party to deliver the documents proving it is eligible for becoming an adhering and/or certified party;
5. On the basis of these documents, the Scheme Owner either:
    a. Accepts the admission of the interested party as an adhering and/or certified party and communicates the acceptance to the interested party;
    or
    b. Rejects the admission of the interested party, and communicates to the interested party indicating what adjustments are desired.
6. A legally responsible executive of the interested party signs the iSHARE accession agreement and is admitted to the iSHARE scheme;
7. The Scheme Owner and the adhering and/or certified party communicate the admission to the iSHARE network

Admission criteria

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

Adhering parties

Party	Entitled Party	Service Consumer	Service Provider
Criterium			
…			

Certified parties

Party	Authorisation Registry	Identity Broker	Identity Provider
Criterium			
Third party memorandum stating adequate data security measures			One of the following: ISO27001 ISAE 3402
…			

Template admission procedure

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

The following includes a template for what needs to be completed to be admitted to the the iSHARE scheme - from an interested party's perspective:

…

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 scheme.

Withdrawal includes:

- A certified and/or adhering party wants to withdraw from the iSHARE scheme;
- 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 scheme (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 iSHARE in a simple and controlled way, minimising impact to the trust in the iSHARE scheme and disruption to the functioning of the iSHARE scheme

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 scheme is not disrupted in any way;
- The **withdrawing/downgrading party** is responsible for delivering a withdrawal plan and to minimise the disruption the the function of the iSHARE scheme. The withdrawing party also benefits from a controlled process itself, as it should help to minimise disruption to internal operations.

Expected administrative burden on the Scheme Owner

To be determined.

Sequence

Withdrawal of a certified party, downgrade of a certified party

1. The withdrawing/downgrading party indicates to the Scheme Owner the intention to withdraw/downgrade from the iSHARE scheme and includes a withdrawal plan based on the 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 a withdrawal/downgrading 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 scheme in accordance with the withdrawal/downgrading plan;
7. The withdrawing/downgrading party has withdrawn from the iSHARE scheme or downgraded to adhering party. This is communicated by the Scheme Owner to all participating parties.

Withdrawal of an adhering party

1. The withdrawing party indicates to the Scheme Owner in written form (this includes for instance e-mail) the intention to withdraw from the iSHARE scheme;
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 the withdrawal to the parties it interacts (interacted) with under iSHARE;
4. The withdrawing party, in cooperation with the Scheme Owner, withdraws from the iSHARE scheme;
5. The withdrawing party has withdrawn from the iSHARE scheme.

Template withdrawal procedure

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

The following includes a template for what needs to be completed to withdraw from the iSHARE scheme - from a withdrawing party's perspective:

...

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 scheme in case of non-compliance with scheme rules and guidelines, or actions with significant negative impact on the normal operation of the iSHARE scheme.

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, and/or; • (Other) impact on confidentiality and integrity of (data* within) the iSHARE scheme.

Classification	Impact or risk
Critical non-compliance	• Recurring major non-compliance, and/or; • Scheme-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 scheme;
- **Exclusion** involves permanent deactivation of adhering/certified credentials within the iSHARE scheme of the excluded party and involves an iSHARE network wide notification of exclusion in order to inform all parties of the exclusion.

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 scheme.

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.

Expected administrative burden on the Scheme Owner

To be determined.

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 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;
    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 for the next 12 months.

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.

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.

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.

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, 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 scheme.

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.

Expected administrative burden on the Scheme Owner

To be determined.

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 iSHARE scheme, the warnings, suspension and exclusion process 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 scheme, the warnings, suspension and exclusion process will also be initiated;
      ii. If there is a data security breach that needs to be reported in line with meldplicht datalekken:
         1. [...]

      iii. If there is a different kind of calamity that does not qualify as a data security breach that needs to be reported in line with meldplicht datalekken:
         1. 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);
         2. 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);
         3. 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 scheme, the warnings, suspension and exclusion process will also be initiated;
      ii. [...]

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.
6. The Scheme Owner evaluates the incident with the reporting and/or (an)other party(s), and registers the evaluation for future learning.

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).

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.

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 scheme.

Responsibilities

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

- The **Scheme Owner** is responsible for facilitation of the process, to maximise the availability of the iSHARE scheme during and after changes;
- **Adhering/certified parties** can (cooperatively) prepare and submit a Requests for Change (RFC) to the Scheme Owner.

Expected administrative burden on the Scheme Owner

To be determined.

Sequence

1. One or several 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. The potential solution (direction);
    d. The impact for certified and/or adhering parties and the Scheme Owner;
    e. The justification of the change in a business case.
2. The Scheme Owner drafts a solution and estimates the impact of the change;
3. The submitting parties are asked whether this solution is in line with the requested change by the Scheme Owner, and:
    a. Accept the solution to move onto 4;
    or
    b. Reject the solution to move back to 2.
4. On the basis of the draft solution and impact estimation, the Scheme Owner either:
    a. Accepts the RFC and prioritises it;
    or
    b. Rejects the RFC and issues a written statement to the submitting parties indicating why and, potentially, what changes to the RFC are necessary for it to be accepted.
5. If 4a is followed, the Scheme Owner adds the change to the release calendar based on its priority;
6. The Scheme Owner alters the iSHARE scheme based on the release calendar, and publishes a new version of the scheme accordingly.

Releases are planned based on the number and priority of changes requested - i.e. there is no fixed release rhythm (at least not yet).

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 scheme.

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 scheme.

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.

Expected administrative burden on the Scheme Owner

To be determined.

Sequence

1. On a monthly basis, certified parties and the Scheme Owner collect management information about:
    a. the use of the iSHARE scheme;
    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 to assess whether this is an incident or structural non-compliance;
4. The Scheme Owner verifies whether the 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. 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. [...];
    d. 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.

Service levels

This section describes the service levels that apply to iSHARE certified parties, adhering parties, and the Scheme Owner.

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	X	X
Performance	X	X	X
Incidents	X	X	X
Support	X	X	X
Reporting		X	X

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.

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- and certified parties and the Scheme Owner.

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.

Norm: 24 hours * all days of the year

Minimum level required: guideline of 99% availability* per calendar month, from 00:00-23:59h, with 95% as hard requirement

*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.

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.

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.

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

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- and certified parties and the Scheme Owner.

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, 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.

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:

- Minor incident;
- Calamity;
- Crisis.

Incident service levels are defined for adhering- and certified parties and the Scheme Owner.

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:

- 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) within 3 working days after being appointed as the responsible party - unless agreed otherwise.

*In line with the incident management process, 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:

- 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) within 3 working days after being appointed as the responsible party - unless agreed otherwise.

*In line with the incident management process, 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:

- 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 mediation.

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

Support

Support includes answering questions and requests from other parties.

Incident service levels are defined for adhering- and certified parties and the Scheme Owner.

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 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.

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.

Reporting service levels are defined for certified parties and the Scheme Owner.

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. 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 week: 0:00h on Monday to 23:59h on Sunday.

Norm: each certified party MUST deliver the management information about the last week, conform the iSHARE template, before 23:59h on Tuesday of the current week

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.

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 week - 0:00h on Monday to 23:59h on Sunday - *and* to collect and process certified parties' management information into a management report.

Norm:

- The Scheme Owner MUST have collected its own management information about the last calendar month before 23:59h on Tuesday of the current week;
- The Scheme Owner MUST process and anonymise its own and the received management information about the last week into a report, and distribute this report before 16:59h on Friday of the current week.

Communication

This section describes the agreements concerning communication about and with the iSHARE brand that is applicable for all "certified parties" and all "adhering parties".

It includes the communication guidelines, guidelines for using iSHARE's name and brand, and a handbook on the latter for reference.

Communication guidelines

To follow.

Using iSHARE's name and brand

General

All participating parties MUST use the same visuals and logos as provided by the iSHARE Style Guide and MUST apply the same 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.

Communication toolkit

Adhering and certified parties can use standard texts, key messages and other textual and visual elements as provided in the communication toolkit provided by the Scheme Owner.

iSHARE styleguide

To follow.

Glossary & Legal Notices

This section includes the iSHARE glossary and legal notices. The section is presented as follows:

- Glossary
- Legal notices

Glossary

ABAC

Access

Accountability

Authentication

Authenticity

Authorisation

Authorisation Registry

Broadcast

Broker

Certificate Authority

CIA Triad

Co-creation

Confidentiality

Credentials

Machine Service Consumer

Service Provider

Data Owner

Data classification

Data retention

Delegation

EAN

Encryption

EORI

Exchange (of Data)

Granularity (of authorisations)

Hashing

Identification

Identity Broker

Identity Provider

ABAC

ABAC (Attribute-Based Access Control) or is assigning authorisations based on attributes (contextual pieces of information that are relevant to an access decision, such as device type, RBAC role, time, location, or CRUD 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.

Accountability

Accountability can be described as being liable or answerable for the completion of a certain task. A person who is accountable oversees and manages the stakeholder(s) who are responsible for performing the work effort. In order to be effective, accountability SHOULD be with a sole person or role.

Access

A way of getting near, at, or to something or someone. In the context of information technology access mostly refers to activities related to information systems and to activities (creating, reading, updating, deleting) to digital data.

Authentication

The process of determining or validating whether someone or something is, in fact, who or what it is declared 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.

Authenticity

Authenticity in the context of information security 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 the message with the private key from the sender. The recipient can verify the digital signature with the matching public key. The public key is issued by a Certificate Authority.

Authorisation

Authorisation is the process of giving someone or something permission to do or have, for example getting access to services, data or other functionalities. Authorisation is enabled by authentication. Policies and attributes determine what types of activitivities are permitted by the entity.

The owner of the environment (Service Provider) can decide to perform the authorisation management and validation process internally or to rely on an Authorisation Registry for that. The Service Provider decides which authorisation attributes have to be presented and which policies to adhere to by the entity before getting access to the service.

Broadcast

An act of casting or scattering in all directions, e.g. a message or a radio signal.

Broker

Person or entity that performs actions, arrangements or negotiations between parties, to provide for interoperability and to avoid n(n-1) connections between parties.

Certificate Authority

Description

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.

CIA Triad

Model with the three key principles confidentiality, integrity and availability, that is designed to guide policies for information security.

Confidentiality

In the context of information security, confidentiality refers to the protection of information from disclosure to unauthorised parties.

The message the recipient gets can be proven not to have been read by anyone else but the legitimate sender and recipient. Confidentiality can be achieved by the use of cryptography, as well as access control.

Credentials

Attestation or evidence of identity, authority, status, authorisations, rights, or entitlement. Can be in digital form (e.g. username combined with a password) or in written form (e.g. a name combined with a signature).

Data Owner

The Data Owner is the (legal) person who is accountable for the confidentiality, integrity, availability and accurate reporting of data.

The Data Owner can be the Service Provider. In this case, he is not only accountable for the availability of service, but also responsible. Read more on the relation between responsibility and accountability here.

Data Classification

The classification of data in categories is an important pre-requisite for proper authorisation. Data can be classified in categories defining their type, location, sensitivity and protection level. Authorisation depends on the access rights of the (Human) Service Consumer that are checked as part of the service requesting process. Clustering the data in categories does not only simplify the authorisation process, it also provides a clear overview to the

Service Provider over their data and lowers the risk of exchanging sensitive data with unauthorised (Human) Service Consumers. A risk analysis is part of the data classification process.

Data retention

Refers to the storage and archiving of data (records) for compliance, historical or business reasons.

Delegation

The act of empowering to act for another or to represent other(s). A delegated party acts on behalf of an Entitled Party and is either allowed to assign authorisations or to delegate yet another party, depending on the relevant policy.

EAN

(European Article Number; also called International Article Number) Used worldwide for marking products that are sold at retail point of sale.

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.

EORI

(Economic Operator Registration and Identification) Unique identification number that companies are required to use when exchanging data with customs in all EU member states.

Exchange (of Data)

An act of giving one thing and receiving another in return. A transaction is a type of exchange.

Granularity (of authorisations)

One of the iSHARE key features is flexibility in authorisation with regards to authorisation scope, granularity and source. In this section we will expand on the granularity for authorisations.

By granular authorisation we mean the level of detail that an authorisation process requires to limit and separate privileges (e.g. the right to access a resource).

A single authorisation may enable a number of privileges the same way as a privilege may require multiple authorisations. An authorising authority should be capable of handling both scenario's.

Granularity is not based on either authorisation requests or privileges, but on functions. Those functions are processed in computer algorithms that express the rules defined in authorisation policies. XACML for instance is a standard that defines a declarative, fine-grained, attribute-based access control policy language that can be used to write computer algorithms.

Fine-grained authorisation

Fine-grained authorisation defines very specific functions that are applicable to specific tasks. Each authorisation request is broken up into tasks and each task is then assigned to a function.

Role-based access control is an example for "fine-grained": access to a resource depends on user's role (not only on user), and user can have multiple roles (having access to multiple resources).

Attribute-based access control is an example for "finer-grained" authorisation: access to a resource depends on attributes that the user has to bring along to proof that they meet the authorisation requirements (the policies).

Coarse-grained authorisation

Course-grained authorisation is simpler and different from fine-grained authorisation as there are no lower detail tasks within the functions.

Access control lists (ACL's) are an example for "coarse-grained" authorisation: once the user is authenticated, the user is allowed access to the requested resource depending on whether that user's ID is on a whitelist (or blacklist, in case user is blocked).

Examples of coarse-, fine-, finer-grained authorisation

- Coarse: User A, User C, User F & User L can access container A.
- Fine: Truck companies have access to container A.
- Finer: The users that can proof to be a trucker from company B, working for the Service Provider in week X, can access container A.

Hashing

Hashing is a one-way mathematical function used to verify the integrity of data. Putting it differently, to ensure that data (message, file or software) has not been modified.

A thorough hash function has the following characteristics:

- The hash value (output) should not be predictable
- The hash value should be collision resistant. It should not be computationally feasible to find another input value that generates the same hash value
- The hash value should be impossible to invert. It should not be possible to derive the input value from the hash value, and
- The hash value should be deterministic. A given input should always generate the same hash value.

Identification

Identification is the process of claiming one's identity ("prove that you somebody") at an authority with the goal to enter the authority's environment by presenting identity attributes defined and accepted by the authority. In the case of iSHARE, it is proposed to reuse existing identity solutions from identity providers in the Dutch market such as eHerkenning and iDIN, and once expanding to other countries, international identity solutions. Identification is achieved by asking the user to present their identity attributes ("something they are") such that they can be validated within the second step in the service request of the iSHARE exchange which is authentication.

Integrity

In the context of information security, integrity refers to the protection of information from being modified by unauthorised parties.

The message the recipient receives from the sender can be proven not to have been changed during the transmission. Integrity can be achieved by i.e. hash functions (hashing the received data and comparing it with the hash of the original message).

IPsec

Protocol suite that provides for both encryption and authentication of IP packets in network communication. Since IPsec works at the internet layer of the TCP/IP model (network layer in the OSI model), applications do not need to be aware of it. Hence, IPsec is able to protect all traffic in an IP network, regardless of the application(s) used.

Levels of Assurance

The table below describes the three levels of assurance according to the eIDAS regulation. The first column states the level of assurance, the second column briefly explains the degree of confidence one can have in the assurance level and the third column states the associated risk with the assurance level.

Under the table, the link to the levels of assurance in eHerkenning are added.

Level of Assurance	Confidence degree in identity	Risk degree of identity
1 - Low assurance	Limited confidence in the identity of the signer	Reference to technical specifications, standards and procedures, including technical controls, the purpose of which is to **decrease the risk of misuse or alteration of the identity**

2 - Substantial assurance	Limited degree of confidence in the claimed identity of the signer	Reference to technical specifications, standards and procedures, including technical controls, the purpose of which is to **decrease substantially the risk of misuse or alteration of the identity**
3 - High assurance	High degree of confidence in the claimed identity of the signer	Reference to technical specifications, standards and procedures, including technical controls, the purpose of which is to **prevent misuse or alteration of the identity**

eHerkenning levels of assurance

As the Dutch identity solution eHerkenning is often referred to in the course of the iSHARE working groups, the link to the eHerkenning assurance levels is added on this page.

Handreiking over betrouwbaarheidsniveaus

The Dutch government published the following 'handreiking' about Levels of Assurance for authentication.

Multicast

An act of casting or scattering to a defined group of receivers, e.g. an electronic message.

Non-repudiation

Non-repudiation (Dutch 'onweerlegbaarheid') refers in the context of information security to the fact that the sending (or broadcast) and receipt of the message cannot be denied by neither of the involved parties (sender and recipient).

Non-repudiation is closely related to authenticity and can be achieved by digital signatures in combination with message tracking.

PDP

(Policy decision point) Entity that evaluates access requests that are received from the policy enforcement point (PEP). Subsequently an answer is sent back to the PEP.

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).

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, 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 standard and normally include the digital signature of the Certificate Authority. The certificate authority issues digital certificates to all members in the trust framework.

Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) is an infrastructure that consists of an architecture, organisation & technology and roles, policies & procedures to manage digital certificates and public-key encryption. The purpose of a PKI is to ensure secure digital communication and the trustful digital exchange of data to enable electronic (online, digital) services.

Digital certificates are issued and revoked by a Certificate Authority which is a role within a public key infrastructure.

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:

- 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).

Responsibility vs Accountability

There is a clear distinction between responsibility and accountability.

Responsibility can be described as tasked with getting the job done. A person who is responsible performs the actual work effort to meet a stated objective.

Accountability can be described as being liable or answerable for the completion of a certain task. A person who is accountable oversees and manages the stakeholder(s) who are responsible for performing the work effort. In order to be effective, accountability SHOULD be with a sole person or role.

Responsibility may be delegated, but accountability cannot.

Scheme

In the context of iSHARE a scheme can be defined as a collaborative effort of organisations to achieve a common goal. In Goals and scope of the iSHARE scheme the purpose of the iSHARE scheme is described.

An analogy is the card scheme, such as Visa, MasterCard, American Express etc.

Service provision

An act of providing or supplying something for consumption or use. One of the most common forms of service provision is the exchange of data.

Session

Interactive information exchange between two or more computers (or other communicating devices), or between a human and a computer (or another communicating device).

Signing

Signing is the process of encrypting data (message, document, transaction) with the private key of the sender. It enables a receiver to confirm the authenticity of the data. Signing also provides for non-repudiation, 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 and the authenticity 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.

Single Sign On (SSO)

Single Sign On (SSO) is often implemented as cross-domain SSO, which is a federated identity solution.

It is important to note that not all federated identity solutions include SSO. The difference between SSO and other federated identity solutions is that SSO has the requirement to authenticate the user once and remain in the authenticated state across multiple systems. The users fill in their credentials once for one particular website to prove their identity and can access multiple websites automatically without the need to re-enter their credentials until the sessions times out (password is remembered for a certain period of time). Ordinary federated identity systems do hold the requirement to be recognised across multiple systems as well, but not necessarily after authenticating once at one website to remain authenticated across many websites without being asked to enter credentials a second time.

It may also be interesting to know that Single Sign Off exists as well where a signing out action in one environment terminates the access to one or all previously signed-in environments.

SSL/TLS

SSL/TLS (Secure Sockets Layer/Transport Layer Security) are a set of protocols that provide for secure communication in computer networks. SSL/TLS make use of cryptography and are widely used by a variety of applications such as web browsing, email and voice-over-IP.

Token

Something that serves as a verifiable representation of some fact, e.g. an identity or entitlement.

Trust framework

Structure that aims to provide confidence in public internet environments. A trust framework is specified according to rules drawn up by a party or community that is inherently trusted, such as a government or a combination of profit and nonprofit parties. Service providers who wish to participate in the trust framework must comply with those rules to achieve a certain level of trust or level of assurance.

The rules include functional, technical, operational and legal rules.

Validation

Action of proving the validity or accuracy of something; declaring that something is legally or officially acceptable.

Legal notices

No part of these specifications may be reproduced in any form by print, photo print, microfilm or any other means or stored in an electronic retrieval system, without the prior written consent of the iSHARE project organisation, which must never be presumed.

Note: the Operational working group will, in coordination with other working groups and the iSHARE project organisation, decide under what terms these pages will be governed and a final position on intellectual property rights will be established. New legal notices might be added to this page in due time.