iSHARE Scheme version 0.5

iSHARE scheme (WIP)

Welcome to Confluence and welcome to the iSHARE scheme!

The iSHARE scheme 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 focusses 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.

On Confluence, we co-create the iSHARE scheme "on the go". Here, we bring the v0.1 version or "startdocument" to a v1.0 scheme document that is ready for implementation. What iSHARE is - and how we will co-create exactly - is described in the Introduction. The Key features, guiding principles & assumptions and the Roles & Responsibilities are described in separate chapters. All remaining Legal, Operational, Functional and Technical topics of the iSHARE scheme are described in detail in separate chapters as well.

Glossary

ABAC

Access

Responsibility vs Accountability

Authentication

Authorisation

Authorisation Registry

Availability

Broadcast

Broker

Certificate Authority

CIA Triad

Co-creation

Confidentiality

Credentials

Service Consumer

Service Provider

Data retention

Delegation

EAN

EORI

Exchange (of Data)

Identification

Identity Broker

Identity Provider

Integrity

IPsec

Levels of Assurance

Multicast

PDP

PEP

Public Key Infrastructure (PKI)Public Key Infrastructure (PKI)

PKI root

PKI trusted list

RBAC

Responsibility vs Accountability

Scheme

Service provision

Session

SSL/TLS

Token

Trust framework

ABAC

ABAC (Attribute-Based Access Control) 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.

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

Process or action of proving something to be true or valid, e.g. the process or action of verifying the identity of a user.

Authentication is the process of validating the identity attributes presented by the user during the identification process. The goal of the authentication is to check the authenticity of the presented identity attributes before the user is allowed to enter the third and last step in the service request of the iSHARE exchange which is authorisation. Authentication can be achieved by asking the user to enter credentials ("something you know") to prove that they are the legitimate holder of the presented identity.

The picture below is the official iSHARE logo for authentication (used in presentations and external communication) and illustrates the user that gets a checkmark after presenting his/her identity attributes during the identification process. The checkmark symbolises the successful outcome of the validation of the identity attributes.

Authorisation

Authorisation is the process of validating authorisation attributes and policies before giving users access to an environment for data, services and other functionalities. The owner of the environment (Service Provider) can decide to perform the authorisation management and validation process internally (internal Authorisation Registry) or to rely on an external Authorisation Registry for that. The Service Provider decides the granularity of the authorisation and which authorisation attributes have to be presented by the user to pass the third and last step of the iSHARE exchange which is the authorisation before getting access to the service.

The picture below is the official iSHARE logo for authorisation (used in presentations and external communication) and illustrates the user that is authorised to access an environment (for data/services/functionalities). The opened lock symbolises the authorised access of a user to the environment which is the last required step in the service request of the iSHARE exchange.

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.

CIA Triad

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

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 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).

EAN

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

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.

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.

The picture below is the official iSHARE logo for identification (used in presentations and external communication) and illustrates the user that presents his/her identity card. The identity card symbolises the identity attributes that the user presents at the identity provider to log in to the environment for further steps (access requests for service).

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.

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.

Note that message encryption/decryption is not the same as message signing/validation. In message encryption/decryption, messages are encrypted with a public key and decrypted with a private key, meaning that the message is kept secret and can be read only by the single holder of the private key. For digital signatures, it is reverse. Messages are signed with a private key and validated by a public key. With a digital signature, you are trying to prove that the document signed by you and that the message is sent out by you. You want to prove the authenticity of the message by signing it with your private key to proof to the whole world (publicly) that the message originated from you.

Digital signatures are verified using a 'chain of trust'. All certificates in the chain of trust are signed with the Certificate Authority's private key. So when members in the trust framework exchange messages including their digital certificates, the authenticity of the messages can be validated by all other members in the trust framework as they hold the public key which they can use to validate digital signatures and therefore be sure of the authenticity of the sender (to be a member of 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 (PKI).

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).

Scheme

A scheme can have different meanings but what we mean here is a collaborative effort of organisations to achieve a common goal which can be different for every scheme. In page Goals and scope of the iSHARE scheme the goals and scope of the iSHARE scheme are described.

Another example is a card scheme. Examples for card schemes are Visa, MasterCard, American Express etc. which are all payment networks linked to payment cards with different payment products (credit, debit, pre-paid). Banks and other financial institutions can become a member of a card scheme with the goal to receive licenses to issue payment products and process payment transactions of the payment networks.

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).

SSL/TLS

SSL/TLS (Secure Sockets Layer/Transport Layer Security) are protocols that provide for secure communication in computer networks. SSL is the predecessor of TLS.

Token

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

Trust framework

A trust framework consists of a group of participants who all work with combined efforts towards the same goal, namely building a system that works and that all participants trust. And by trust we mean: willing to participate in and rely on. To achieve both goals, all possible risks have to be addressed by technical, functional and operational specifications and legal rules.

Technical, functional and operational specifications are needed to ensure

- The system's processes, policies, procedures, performance rules and requirements, assessment criteria, etc.
- Make it work
- Make it trustworthy

Legal Rules are needed to ensure

- Existing law
- Contractual obligations
- Regulate technical, functional and operational specifications
- Make technical, functional and operational specifications legally binding on the participants
- Define and govern the legal rights and responsibilities of the participants

Validation

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

Introduction

The iSHARE project was initiated by the Neutral Logistics Information Platform (NLIP) through a tender project. NLIP asked 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 eventually won the tender with their plan to set-up a scheme of multilateral agreements instead of, for instance, a more technology centric approach to build a software platform. Since June 2016 the iSHARE project team worked towards the realisation of this 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, results in startdocument v0.1 which provides 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 involved organisations work collaboratively towards iSHARE scheme v1.0 which contains the first full set of agreements for improved data exchanging conditions. Involved organisations work towards a full set of agreements in four working groups: Legal, Operational, Functional and Technical. The set of agreements will be realised and tested in the iSHARE reference implementation that will be developed alongside.
- 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.

This document is, at the time of writing in January 2017, the iSHARE Scheme v0.1 "startdocument" and the result of phase 1. The startdocument serves as the output of phase 1 and the input for phase 2, during which working group members will take ownership of the document and make it evolve towards iSHARE scheme v1.0. The document contains and proposes a number of topics which need to be detailed further by the iSHARE co-creation working groups. The document serves as a discussion starter and is by no means meant as a prescription. Working groups are free to propose additions, removals or modifications to the topics in this document (read more on the purpose of the startdocument).

The remainder of this document contains all the topics that need to be detailed by workgroup members. This chapter further describes the context of the iSHARE project and provides background information (read more about the goals and scope of the iSHARE scheme, read more about the co-creation in working groups). The chapters that follow provide insight into what key features, guiding principles and assumptions are considered for the iSHARE scheme, which roles and responsibilities are foreseen, and what Legal, Operational, Functional and Technical agreements are needed.

Goals and scope of the iSHARE scheme

The iSHARE scheme is a collaborative effort to improve data-sharing of organisations involved with the Dutch logistics sector.

The ambition of the iSHARE project is to take away barriers in the way of 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 we are able to improve our common skill to handle data in a smart and efficient way, this 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 of importance in any data exchange context:

1. Identification
2. Authentication
3. Authorisation

These three aspects are considered crucial in any communication between parties, also in the context of exchanging logistical data. Within the iSHARE scheme, agreements are made on these 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 for how long.

These three aims can only be reached when a variety of perspectives is 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 invested 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: The iSHARE scheme can in some way be compared with the institute of the passport: the iSHARE scheme will be useable by anyone who acquires an identity applicable within the iSHARE scheme and acquired through the rules of the scheme. This will greatly simplify authentication and authorisation processes, also between different organisations (although not ruling out possible malign intentions).

Co-creation in working groups

The iSHARE scheme is established by its participating organisations. Through the iSHARE co-creation process, the collective expertise of participants will lead 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 at the beginning of the co-creation process there is no clear description of what the eventual scheme must look like: what the iSHARE scheme entails or doesn't 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 topics with dedicated working groups: Legal, Operational, Functional and Technical (LOFT). The assumption is that for a fully functional scheme, at least these topics need to be discussed and organised.
- The working groups 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.
- The regular meeting of working groups and the agreements made within the working groups are facilitated by the chairman and secretary of the working groups.

The participants of the co-creation process have a variety of backgrounds: private and public organisations, bigger and smaller organisations, (serving) different modalities, both providers and receivers of data. The variety of organisations ensures that the iSHARE scheme will be widely applicable.

Purpose of this document

This document (of which version 0.1 is known as "startdocument") contains the current state of agreements within the iSHARE scheme. Version 1.0 and up of this document will contain a full set of agreements and relevant standards as decided within the working groups of the co-creation process. This document therefore is a growing document to which additions and changes are constantly made. The following working groups bear the responsibility to add detail to this document:

- Legal
- Operational
- Functional
- Technical

All named working groups focus on their respective topic within the iSHARE scheme.

Version 0.1 of this document is meant as a discussion starter for the working groups. This startdocument provides a first draft of topics that should be addressed and detailed during the co-creation phase of iSHARE. Next to a preliminary table of contents, some topics contain descriptions of possible solutions to be considered. The startdocument aims to be complete in scope, but is by definition not complete in detail.

This document is present in the online environment of "Confluence", which allows for collective editing/commenting. All participants are encouraged to comment on the topics addressed within this environment so that all relevant arguments are considered.

Please note: Any statements in this document are in no way intended to favour a certain solution; all statements (even firmly stated texts) should be seen as open to discussion.

Notational conventions

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).

Other conventions might be added later.

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: in the course of 2017 it will be decided under what terms these pages will be governed and a final position on intellectual property rights will be established.

Other legal notices might be added later.

Versioning

Unique version numbers will be assigned to unique states of the iSHARE scheme. The v0.1 version of the scheme is called the "Startdocument" - one of the deliverables of iSHARE Phase 1.

The Startdocument is co-developed into new versions in the four working groups, with a v0.8 version ready at the start of Q2 2017 and a v1.0 version at the end of Q2.

Previous versions of the iSHARE scheme can be found here.

Key features, guiding principles & assumptions

This section provides a high level overview of the features and requirements that the iSHARE scheme aims to support:

Key features

Based on the inventory of use cases taken during Phase 1, the iSHARE scheme should at least support the following:

- Provide trust framework for PKI certificates
- Provide flexibility in authorisation
- Allow for management of consent
- Support multiple interaction models

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

Provide trust framework for PKI certificates

The iSHARE scheme requires public key encryption for the following purposes:

- Proof of origin of data
- Authenticity of identities
- Protection of data against unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction

A 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

The iSHARE scheme should provide a PKI root list that contains trusted PKI roots that meet the iSHARE requirements. Trusted PKI roots within the iSHARE PKI root list can be (and should be) trusted by every iSHARE participant. The term "PKI root" is otherwise known as C ertificate Authority (read more on Public Key Infrastructure (PKI)) .

It is assumed that existing PKIs are sufficient to meet all iSHARE requirements. If, during the course of phase 2, this assumption turns out to be false, an additional iSHARE specific PKI can be created (Read more on what iSHARE's own PKI might entail).

Provide flexibility in authorisation

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

- **Authorisation scope**
  The authorisation scope refers to the objects or resources (most of the times data) from 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). Either way, the scope is always governed by a formal agreement and implemented by technical means.
- **Authorisation granularity**
  The authorisation granularity refers to the characteristics of both the data and the rules (policies, conditions) that apply. Authorisations to data 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.
- **Authorisation source**
  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.

The final architecture will be dependent on requirements such as data ownership, formal agreements, communication and security.

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 supports several interaction models:

- Both machine to machine (M2M) and human to machine (H2M) interfaces should be supported. Possible human to human (H2H) interfaces like Peer2Peer might be included as well.
- Both request-response and publish(-subscribe) models are supported.

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):

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.

The following principles must be kept in mind at all times during the development of the iSHARE scheme (please find the older version of the guiding principles at the bottom of this page):

Principle 1	**Generic building block for data exchange**
Statement	iSHARE is a generic identification, authentication and authorisation building block 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**
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 consider the use of 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

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 role 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

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

Assumptions

The iSHARE scheme starts from the following assumptions. If these assumption turn out to be false this has to be addressed. This is not necessarily a task of the iSHARE project.

1. **Data ownership**
   The Data Owner is the (legal) person who is accountable for the confidentiality, integrity, availability and accurate reporting of data. The data owner is also responsible for the classification of his or her data and decides who has access to it. Note that the iSHARE scheme will not try to resolve any debates on data ownership.
2. **Data formats and semantics**
   In order to be able to exchange data a mutual understanding of the meaning of data and the way data is structured is required. It is assumed this mutual understanding exists and data exchanging can therefore commence and be meaningful.
3. **Service requests and responses**
   Related to formats, but separated here because of the relation with iSHARE. In order to exchange (data) services an interface should be defined. In this interface both a service request and the resulting response should be defined, next to push messaging and publish-subscribe-models. Since iSHARE is data agnostic it is assumed that these definitions either exist or are created during the course of implementing specific data exchanging cases.
4. **Data classification**
   The classification of data in categories is an important pre-requisite for the authorisation. Data can be classified in categories defining their type, location, sensitivity and protection level. Authorisation depends on the access rights of the 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 Service Consumers. A risk analysis is part of the data classification process.

Roles & Responsibilities

This section describes the roles and their general responsibilities that are part of the iSHARE scheme. A more detailed explanation of their functional behaviour and interaction between roles is described in Functional.

The market for the iSHARE scheme will encompass the entire national logistics sector. Since logistics crosses borders frequently, all communication will be in English. Thus, the iSHARE scheme can be applied in other countries as well.

First, the two-sided market model of iSHARE will be described, consisting of the primary roles Service Provider and Service Consumer. Next to this, both these primary roles and the supporting roles will be explained in more detail:

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.

Basic framework: Two-sided 'market' of service provision

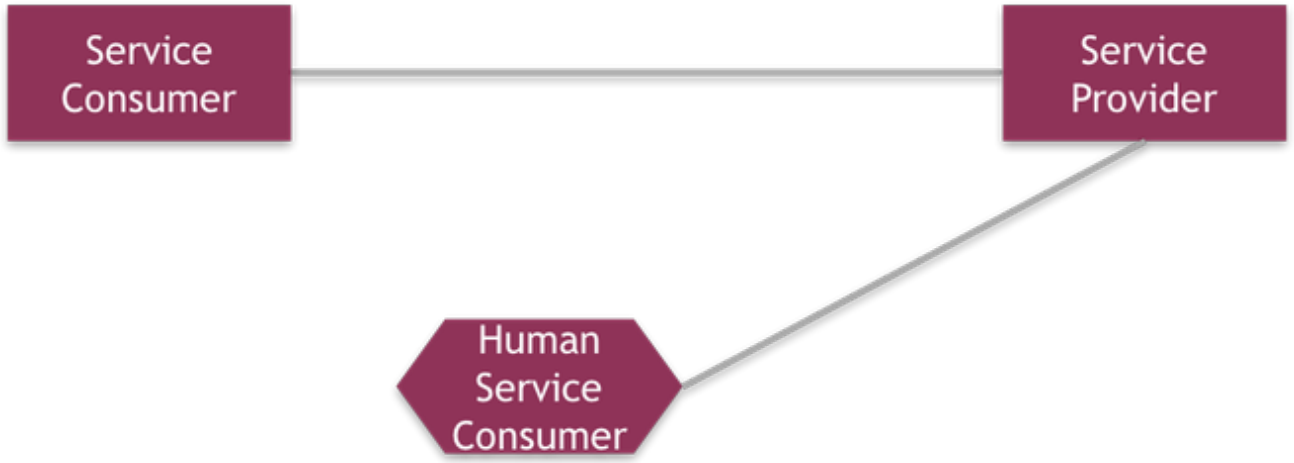
Note that because data exchange was deemed too narrow for iSHARE, the term service provision was introduced.

The market for service provision is two-sided; there are two primary sides that have their own distinct needs and behaviour. Every time a service is provided within the iSHARE scheme, there will *at least* be a Service Consumer or a Human Service Consumer and a Service Provider. This basic framework is applicable to any situation in which service is provided in an iSHARE context. Its intention is to facilitate discussion on the various contexts in which service provision will be required.

The term Service Consumer always refers to a *machine* of some type, e.g. an information system, a device, a database or an application. When a *human* is involved, he will be refered to as Human Service Consumer. A Human Service Consumer may either interact directly with a Service Provider (through some interface) or may interact via a Service Consumer with a Service Provider. In the latter case, the Human Service Consumer may use a mobile app to activate the Service Consumer.

Notice that the two primary roles (Human) 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 same goes true for any supporting roles, such as the Identity Broker, the Identity Provider and the Authorisation Registry.

The basic relation between the primary roles is as follows:



Note that the basic framework depicted above does not state anything about the legal and/or operational environment, in which it functions. Depending on the agreements made within the iSHARE scheme, certain provisions of service(s) might be fuelled by functional and technical agreements, while not falling within the scope of any legal and operational agreement.

Service Consumer

The Service Consumer is an abstract role that represents a machine that (requests,) receives, and uses certain services, such as data, from a Service Provider. The Service Consumer represents the entity that is on the receiving end of service provision.

Human Service Consumer

The Human Service Consumer represents a human (person) who requests, receives, and uses certain services, such as data, from a Service Provider. The Human Service Consumer represents the entity that is on the receiving end of service provision.

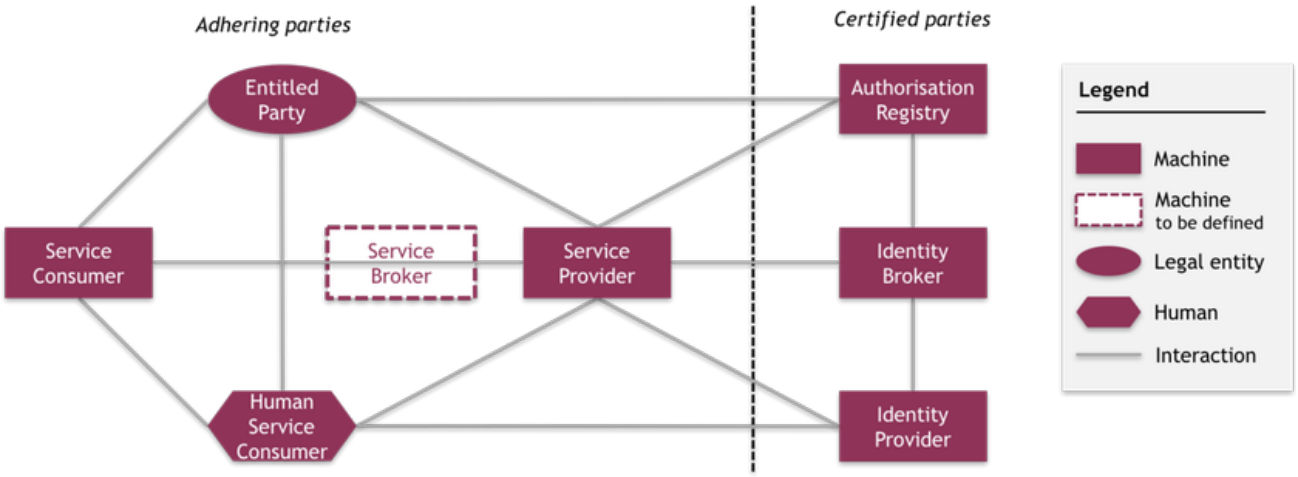
Service Provider

The Service Provider is an abstract role that represents a machine that provides certain services, such as data, to (a) (Human) Service Consumer(s). The Service Provider is either the Data Owner (when the service pertains to data), or has explicit consent of the Data Owner to provide (data) services with the (Human) Service Consumer.

The Service Provider is responsible for the availability of services, and accountable if he or she is also the Data Owner.

Supporting roles

Next to the main roles of Service Consumer and (Human) Service Provider present every time service is provided within the iSHARE context, the iSHARE scheme describes the following supporting roles that are optionally present:



Note that parties fulfilling a certain role can be iSHARE adhering or -certified, as explained here.

Each role is described in its own section:

- Entitled Party
- Authorisation Registry
- Identity Provider
- Identity Broker
- Service Broker

Entitled Party

Description

An Entitled Party can be explained as the legal entity that has one or more rights to something, e.g. determining who may access data that it owns or determining who may access data at a Service Provider that it has a legal agreement with.

The Entitled Party registers authorisations of entities (such as Service Consumers or Human Service Consumers), that are allowed to access the services of a Service Provider, at the Service Provider or at an Authorisation Register.

The Entitled Party may also delegate its rights to third parties. Note that if a third party is delegated by the Entitled Party, this delegated party can also be considered Entitled Party. In such case, there are two (and potentially more) Entitled Parties in the roles framework.

Authorisation Registry

Description

An **Authorisation Registry**:

- Manages records of authorisations of users/entities within the scheme
- Checks on the basis of the registered permission(s), or a representative of a company, if an entity is entitled 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. An internal Authorisation Registry is assumed to be implicitly present at the Service Provider.

In the situation of high speed/high volume data provision it is possible to establish a 'session'. In this case the (internal or external) Authorisation Registry checks the Authorisation and sets a time or amount of exchanges-limit for the next check. Therefore, the processes can run smoothly without interruption by entities who are familiar to each other.

Relevance

The Authorisation Registry works together with a Certificate Authority and/or the Identity Provider to make sure whether the Service Consumer is authorised to fulfil the requested exchange. Without an authorisation from the Authorisation Registry, an exchange will not ta ke place.

Identity Provider

Description

An **Identity Provider (IDP)**:

- Provides identifiers for human users looking to interact with a system;
- Asserts to the system that such an identifier presented by a user is known to the IDP, and;
- Possibly provides other information (which are frequently referred to as attributes) about the user that is known to the IDP.

An Identity Provider can be either a separate entity within the iSHARE scheme or be a part of the Service Provider, depending on the size and preferred choice in architecture, as depicted below.

In the iSHARE scheme, several states and process flows can be identified. The Identity Provider will play an important role when (new) e ntities will come on board into the iSHARE scheme and when provision of services will take place. The Identity Provider will be called upon every time when an entity needs to be verified before provision is initiated.

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

Note: It is possible that the Identity Provider will not play a role every time data is provided within the iSHARE scheme (e.g. for scaling reasons in low-risk situations).

Relevance

Data Provision

The Identity Provider plays a role in the iSHARE scheme when humans have to interact with the scheme, e.g. in the situation where the size/weight of a truckload needs to be edited at the source of the Service Provider. When the identity of the user is not valid or known, the service will not be provided.

Registered identities

All human users of the iSHARE scheme need to have a registered identity to be able to interact with the system.

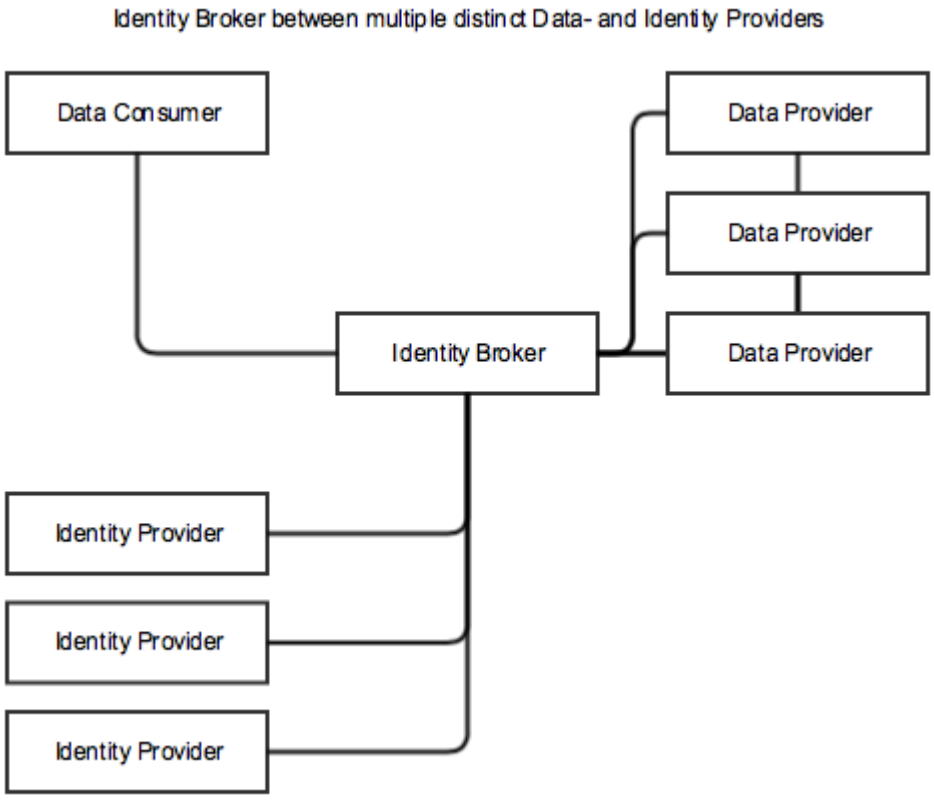
Identity Broker

Description

If multiple distinct Service Providers exist where each data set is protected under a distinct trust domain, multiple Identity Providers may be needed that allow Service Consumers to select their preferred Identity Provider. 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.

Depiction



Relevance

The iSHARE scheme will consist of various organisations that will take roles as Service Consumer and Service Provider. To keep the scheme clear and effective, there will not be a direct connection from every Service Provider to every Service Consumer and all the other necessary roles. The Identity Broker will be the solution to link these parties to each other. Besides that, in the spirit of freedom of choice, the iSHARE scheme should support that several parties can offer similar services. Also, the broker makes it possible to broker provision by Service Providers who are yet unknown by a Service Consumer, but can be reached through iSHARE standards.

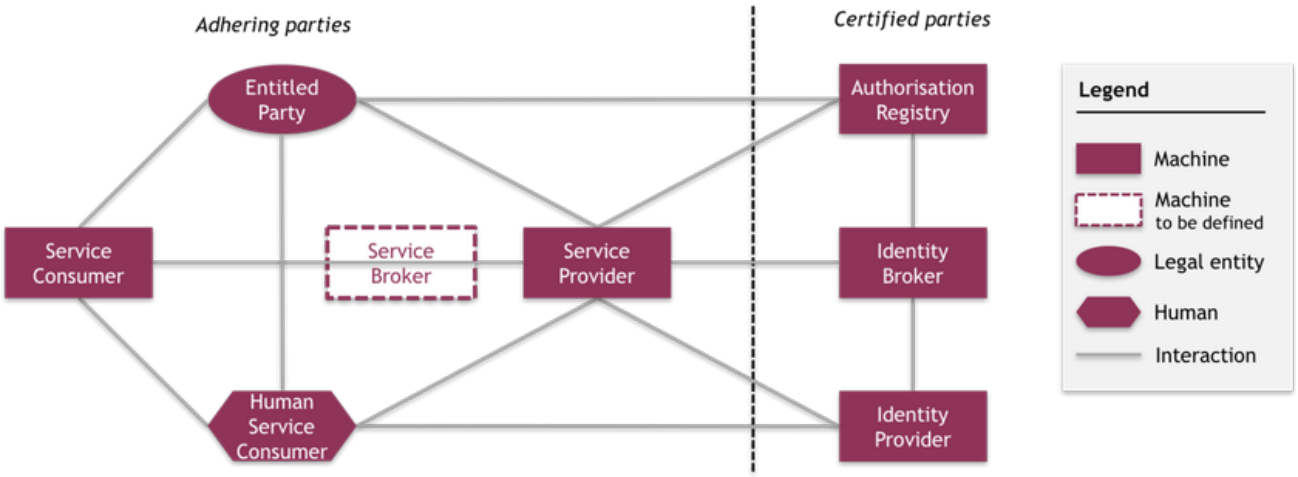
Service Broker

Description

A Service Broker can provide technical services on behalf of the Service Provider, such as messaging, queuing and processing.

The Service Broker role is to be defined by the Functional working group. Hence, the Service Broker will not be described nor be depicted in any of the use cases (yet).

iSHARE adhering, -certified and -compatible



Parties fulfilling a role in the above framework can be iSHARE adhering and/or -certified – as depicted. Note that a party can fulfil more than one role.

iSHARE adhering parties adhere to the - to be developed by the Legal working group - iSHARE terms of use. All adhering parties must declare that they comply to the iSHARE terms of use. This compliance can be registered centrally (in a central register or a certificate system) or decentrally.

iSHARE certified parties are certified and registered as such at the - to be set up - iSHARE governing body. These parties adhere to the iSHARE terms of use and have additional responsibilities and requirements. While the exact bases for certification need to be determined, the eHerkenning responsibilities and requirements per role can serve as a starting point:

- Authorisation Registry
  eHerkenning responsibilities and requirements plus iSHARE requirements for fine-grained authorisation
- Identity Broker
  eHerkenning responsibilities and requirements plus a(n) (potential) iSHARE interface
- Identity Provider
  eHerkenning responsibilities and requirements

Therefore, the eHerkenning admission process can (potentially) be reused.

Next to iSHARE adhering and -certified parties, it could be beneficial to both the iSHARE scheme and organisations to add the possibility of being **iSHARE compatible**. iSHARE compatible organisations comply to the iSHARE agreements and standards, but are not part of the iSHARE scheme (and have not declared their adherence to it). Organisations can show that they or their products (in the case of software vendors) are 'up to iSHARE standards', and thus gain trustworthiness in the market. At the same time, more organisations carrying the iSHARE name means more visibility for the iSHARE brand. A conformity test will be developed by the Operational working group to affirm iSHARE compatibility.

Processes

The iSHARE scheme SHALL support the following processes:

- Encryption
- Hashing
- Signing

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.

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.

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.

Legal

This section covers the relevant Legal topics of the iSHARE scheme:

- Relevant Rules & Regulations
- Possible operational business models
- Required contracts: what are the contracts that bind the different roles to the iSHARE scheme?
- Branding & licensing

These topics (and possibly others that arise during Phase 2) are detailed by the Legal working group.

Relevant Rules & Regulations

About relevant rules an regulation the following can be stated: the solution should comly:

- The (legal and professional) standards for information security
- Dutch legislation and regulations insofar as they are applicable
- European regulations insofar as they are applicable, notably eIDAS regulation and GDPR

A detailed inventory of the relevant laws and regulations must still places available.

The scheme should pay attention to the current legal framework, in order to verify whether the scheme can lead to a full and proper arrangement of iSHARE. The scheme must guarantee that iSHARE can be used for the processes of private and public organisations, without this leading to legal or security problems. Within the scheme there should be a focus on these two situation in which:

- Unauthorised acces get wrongly authorised
- Authorised users wrongly don't get access

Legal Framework

The iSHARE scheme should be arranged according to the privacy rules by design principles. This means that personal data may not be processed more often than is necessary for the purpose for which the personal data is obtained. This is in accordance with the Data Protection Act.

- There must be compliance with legal and professional standards for information security.
- There must be according Dutch laws and regulations as applicable.
- There must be complied with European legislation where applicable.

Electronic Access Services are focused on providing "trust". Clear legal frameworks contribute to this as well as a well-organised control system based on clear roles and responsibilities detailed in "Structure & Roles". Moreover, to provide legal requirements regarding reliability of iSHARE services, regarding identification, authentication and authorisation of importance for the understanding and the development of the iSHARE scheme.

The eIDAS regulation

The eIDAS regulation & trusted list of service providers and services

The eIDAS regulation obliges EU Member States to establish, maintain and publish trusted lists about qualified trust service providers (including trusted certificate authorities) and qualified trust services provided by the trust service providers.

Note that we include the eIDAS regulation of trusted list of service providers and their services because we might want iSHARE to support international PKI roots.

The trust service providers have to cover the following list of trust services:

- Time stamping: The date and time on an electronic document which proves that the document existed at a point-in-time and that it has not changed since then
- Electronic seal: The electronic equivalent of a seal or stamp which is applied on a document to guarantee its origin and integrity
- Electronic delivery: A service that is provided in the digital world through the internet or by means of other information and communication technologies (i.e. opening a bank account, transferring money etc. which used to be provided by people in the physical world)
- Legal admissibility of electronic documents to ensure their authenticity and integrity
- Website authentication: Trusted information on a website (e.g. a certificate) which allows users to verify the authenticity of the website and its link to the entity/person owning the website

Here is the link to the website: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

Possible operational business models

This section will describe the possible operational business models of the iSHARE scheme - it will be detailed by the Legal working group.

Required contracts

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

This section will describe the required contracts of the iSHARE scheme - it will be detailed by the Legal working group.

Branding & licencing

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

Note: both general terms and conditions and dispute management will be detailed by the Legal working group later.

Entrance criteria

1. Entry Requirements - All participants in the scheme MUST meet the general entry requirements. The entry requirements are set for a number of reasons. The main one is the knowledge that the scheme will only be able to function as recipients of services have sufficient confidence in the scheme. Confidence in the scheme and the use of the scheme, supplied in connection with the scheme requires trust in the individual participants
2. Surveillance, monitoring and control - Proper adherence to the agreed system is essential for confidence in the scheme (for Electronic Access Services). Monitoring and maintaining compliance is the responsibility of the regulator. The management organisation responsible for the control and monitoring of compliance with the scheme agreements on behalf of the owner and for the regulator. Enforcing compliance with system arrangements is the task of the regulator.

Liability

Within the scheme, each participant SHALL be responsible for his own actions and / or omissions in the role he plays. The liability is subject to the general rules of Dutch/EU law regarding the content and extent of liability to pay damages. Participants MAY derogate from these general rules. How these rules work out in a particular case depends on the facts and circumstances of the case.
The participant MAY limit his liability in the contract which he concludes with a Service Consumer or a Service Provider. In addition, he remains subject to the general rules of the Dutch/EU law on liability and compensation.

Although the Certificate Authority (CA) MAY not be a member of the iSHARE scheme, the CA plays a vital role within the network of the scheme in the CA domain. For the CA registry is that it is liable for its own acts and / or omissions in the role it plays. The service intermediary SHALL be liable for its own acts and / or omissions.

Level of assurance

Determining the level of assurance (LoA) for a particular service/request is determined by the Service Provider. The Service Provider MUST ensure compliance with the AWB (General Administrative Law Act) to give substance to the standard of a reliable and confidential communications.
The Service Provider SHALL therefore continue with the provision of a service and SHOULD carry out a risk assessment and must consider what measures should be taken to allow electronic communication sufficiently reliable and confidential. This includes an option for the required level of assurance for a particular service that will be used. In addition to determining the LoA chosen by the Service Provider to the service provider will have to take other measures to reliably electronically to provide a service in accordance with the requirements of the AWB. The additional measures to be taken are dependent on the confidence level.
Where Electronic Access Services is used for e-services outside the government (B2B and B2C) specific AWB naturally do not apply requirements. In the case of B2B and B2C services is that means publishers permission registers and the respective service providers an "information society service" and / or a 'remote service' (as defined in the Civil Code) offer. These parties are responsible to meet the associated information obligations and duties regarding the establishment of a legal agreement, as contained in the Civil Code.

Operational

This section covers the relevant Operational topics of the iSHARE scheme:

- Service Level Agreements
- Audits
- Incident Management
- Change Management
- Governing Body

These topics (and possibly others that arise during Phase 2) are detailed by the Operational working group.

Service Level Agreements

This document describes the service level agreements that apply to participants of the iSHARE scheme. It is a description of the minimum service level which should provide the participants with each other and their customers service and minimum service level management that the governing body provides to its participants/users. A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive.

Up time / Response time / Maintenance reports/windows

This section will describe the performance of the service that will be provided as agreed in the SLA.

Monitoring / Logging / Archiving / Reporting

This section will describe the behaviour of the background of the service that will be provided as agreed in the SLA.

Customer Support / Helpdesk

This section will describe the how problems reported by users will be handeled as agreed in the SLA.

Up-time

Up-time is a measure of the time a machine, in this case the scheme and it's servers, has been working and available. Uptime is the opposite of downtime.

The times which are issued by participants and the management organisation guaranteed the availability the iSHARE scheme.

Response time

Response time is the time it takes for a device, network or service, when subjected to a change in input signal, to change its state by a specified fraction of its total response to that change. In the iSHARE environment the response time will be for the user the time it takes to proces a request and return a signal.

Purpose of setting performance standards is to ensure a good user experience, especially at peak times.

The norm for processing of messages for participants

1. 95% of messages MUST be returned within 2 seconds
2. 99% of the messages MUST be returned within 5 seconds
3. Each participant MUST be able to process at least 100 simultaneous messages while still meet the performance requirements

Maintenance reports

Maintenance reports are intended to monitor the growth of the scheme and the service level agreements within the scheme. To be able to keep track on the growth number, guarantee it's uptime and service and be able to take action if it exceeds it's possible usage.

The participants and the management organisation collect personal information management reporting period (which runs from the first day of a calendar month 0:00 pm till the last day 24:00).

Each participant must reach the 5th of each month, provide reporting on the previous reporting period, the management organisation for 24:00. To this end, the participant must use the reporting tool made available by the management organisation. The management organisation will aggregate information sharing within 5 working days with all the participants and service providers.

Monitoring

The **monitoring** of the agreements made in the service level will be performed by the management organisation. The management organisation will use the analysis of the reports delivered by the participants as input for the monitoring. Other input will also be used like sample testing.

Logging

Logging is the proces that records events that occur in the iSHARE scheme, and/or messages and communication between different users of the iSHARE scheme.

Archiving

Archiving is the process of moving iSHARE data that is no longer actively used to a separate storage device for long-term retention.

Reporting

Data **reporting** is the process of collecting and submitting data to authorities entrusted with compiling statistics. Accurate data reporting gives rise to accurate analyses of the facts on the ground; inaccurate data reporting can lead to vastly uninformed decisions based on erroneous evidence. When data is not reported, the problem is known as underreporting; the opposite problem leads to false positives.

Audits

An **audit** is a systematic and independent examination of records that inform about performed actions by a system to check if the system safeguards the assets, maintains data integrity and operates effectively to achieve the predefined goals. Audits offer a great opportunity to periodically check the effectivity of implemented functionalities and is therefore recommended to put into place.

In the context of incident management, audits should be performed as security measure on executed service provisions to spot fraudulent and unauthorised actions and the instances who are accountable for that.

The scope and process of audits will be determined in the course of the iSHARE functional working group.

Incident Management

The goal of the process **Incident Management** is to settle different types of incidents within the iSHARE scheme - in a structured way. Disruption of the service(s) should be (as) limited (as possible).

An **incident** is every event that is not part of iSHARE's standard operation and that has (potential) impact or risk with respect to the quality, availability, integrity and/or confidentiality of (information within) the iSHARE scheme. Incidents could include:

- Disruptions: events that lead to (parts of) the iSHARE service(s) being partially or entirely unavailable;
- Information security incidents: events such as the loss of a USB stick, laptop, harddrive but also signals of attempts of hacking, attempts to enter the iSHARE scheme or malware;
- Fraud or the presumption of fraud by, for example, an employee or a hacker.

Who is responsible for Incident Management, and how the Incident Management process is setup will be established in the Operational working group.

Change Management

The process **Change Management** structures changes in:

- Scheme documentation
- Scheme implementations

It will be detailed by the Operational working group.

Governing body

The iSHARE scheme is an initiative with a long-term ambition to improve the circumstances for data exchange in the logistics sector. To operationalise this long-term ambition, iSHARE needs to become a sustained endeavour which is constantly improved by its stakeholders. To organise the constant improvement, a **governing body** needs to be shaped. Which form this governing body needs to take to optimally support the long-term ambitions needs to be discussed and decided upon within the iSHARE project together with involved stakeholders.

The governing body could take any shape, of which the most evident options would be:

- Establish a new governing organisation, either in the form of an association or a company depending on what is deemed most appropriate for the scheme
- Bestow governing responsibilities upon an existing association or company. This option is plausible when the existing organisation's capabilities and mandate are aligned with iSHARE goals and when the organisation enjoys the support of a significant majority of iSHARE stakeholders.

The responsibilities of the governing body will exist out of some or all of the following activities (non-exhaustive):

- Organise regular processes to constantly improve iSHARE scheme specifications with stakeholders;
- Develop, maintain and improve relevant core documents and standards for the iSHARE scheme;
- Define, maintain and execute certification procedures for organisations that want to participate or need to adhere to the iSHARE scheme rules;
- Develop, maintain and improve software or testing environments that facilitate the iSHARE scheme (e.g. testing suite, certification tools, software libraries, directory services or incident notification portals);
- Report on scheme performance where possible and where necessary to relevant stakeholders;
- Facilitate dispute management procedures;
- Facilitate incident management procedures;

Depending on the results of the co-creation phase and the direction of the iSHARE scheme at the end of the co-creation phase, the form of the future governing body for the iSHARE scheme can be determined.

Functional

This section covers the relevant Functional topics of the iSHARE scheme:

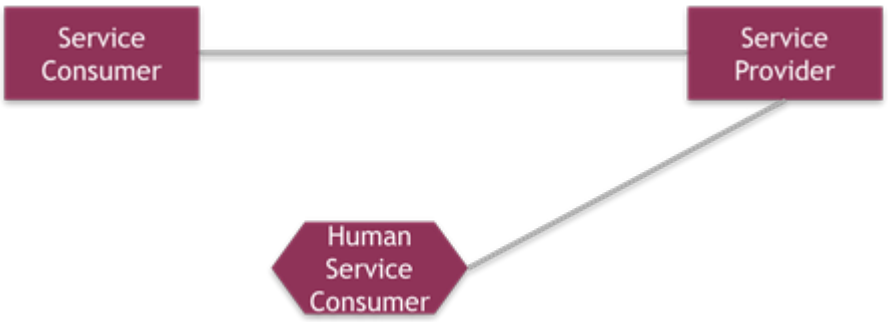
- Primary use cases (new)
- Primary use cases (old)
- Secondary use cases
- Detailing key features
- Functional requirements per role
- User interface requirements
- Identifiers

These topics (and possibly others that arise during Phase 2) are detailed by the Functional working group.

Primary use cases (new)

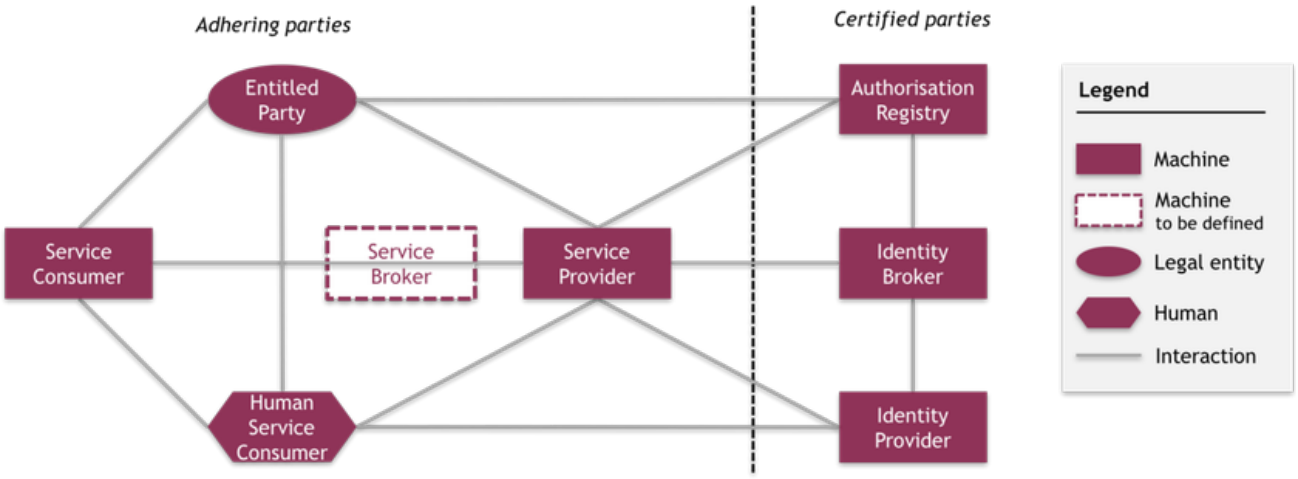
In this section we elaborate on the three primary use cases that iSHARE supports.

Every primary use case involves *at least* two roles; either the Service Consumer and the Service Provider, or the Human Service Consumer and the Service Provider. Whether a Service Consumer (use case 1) or a Human Service Consumer (use case 2 and 3) interacts with the Service Provider is based on the two basic interaction models: Machine to Machine (M2M) and Human to Machine (H2M).



Note that the basic framework depicted above does not state anything about the legal and/or operational environment in which it functions. Depending on the agreements made within the iSHARE scheme, service provision might be fuelled by functional and technical agreements, while not falling within the scope of any legal and operational agreement.

Depending on variations of the basic use cases, parties other than the (Human) Service Consumer and the Service Provider interact. All roles are described under Roles & Responsibilities and depicted as follows:



Note that parties fulfilling a certain role in the above can be iSHARE adhering or -certified, as explained here.

The basic use cases and their variations are presented in the tables below. Variations exist because delegation can take place, and because different types of info can be held by different roles:

- **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 another Entitled Party
- **Identity info:** information about a Human Service Consumer's identity - only needed in the H2M use cases
- **Authorisation info:** information indicating which Human Service Consumers are authorised to act on an Entitled Party's behalf - only needed in the H2M use cases

Entitlement info is always held by the Service Provider or the Authorisation Registry and therefore not visualised in the tables below.

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 following tables:

Use case 1 (and variations)*: M2M service provision

	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Use case variation	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 Service Consumer acts as a proxy between the Human Service Consumer and the Service Provider as described.

Use case 2 (and variations): H2M service provision with identity info held at the SP

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

Use case 3 (and variations): H2M service provision with identity info held at the IDP

		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 the use cases that contain a hyperlink are detailed on their own Confluence page - as follows:

- Roles
- Depiction
- Description
- Practical examples
- Sequence diagram

Possible unhappy flows for each use case will be detailed at a later stage. Unhappy flow communication should not include any clues about data - "no freight found", for example, can also be valuable information.

1. M2M service provision

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

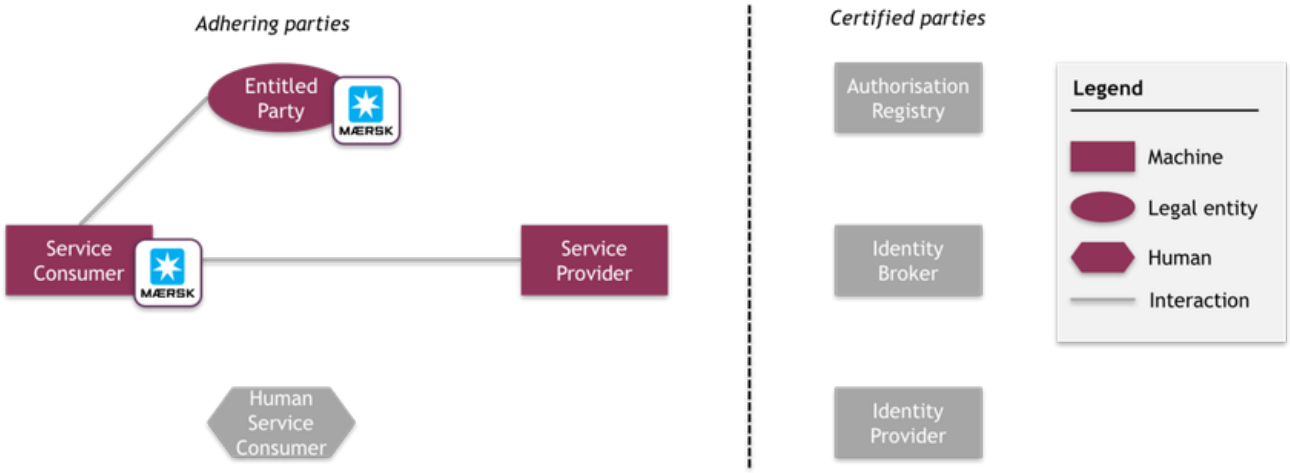
Note that this use case is exactly the same as the old use case 1A.

Roles

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

As there is no delegation, the Entitled Party acts as Service Consumer

Depiction



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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer

- In this use case the Entitled Party acts as Service Consumer

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

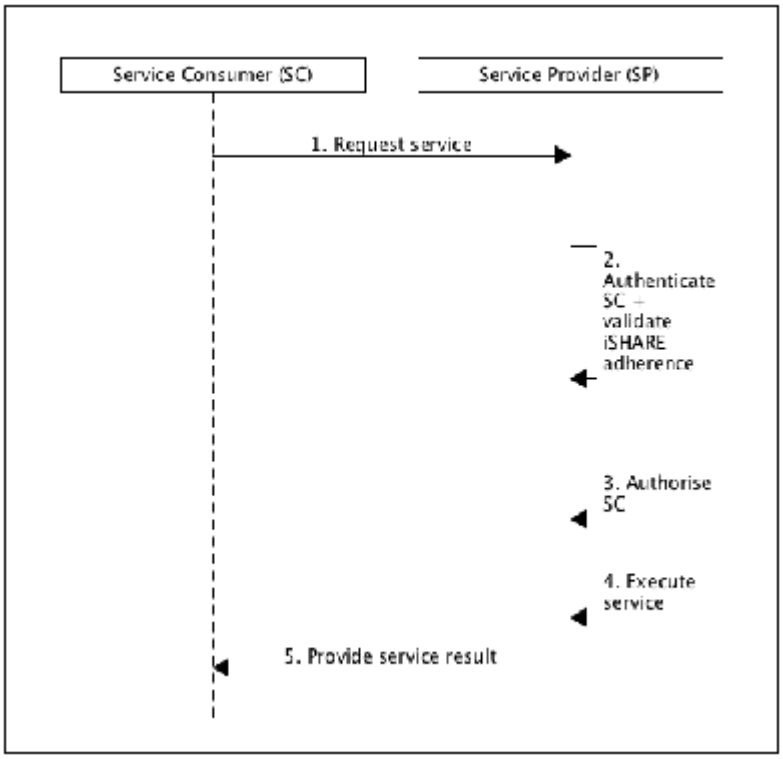
The use case consists of the following steps:

1. The Service Consumer requests a service from the Service Provider
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider authorises the Service Consumer based on the authorisation information registered with the Service Provider
4. The Service Provider executes the requested service
5. The Service Provider provides the service result to the Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



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

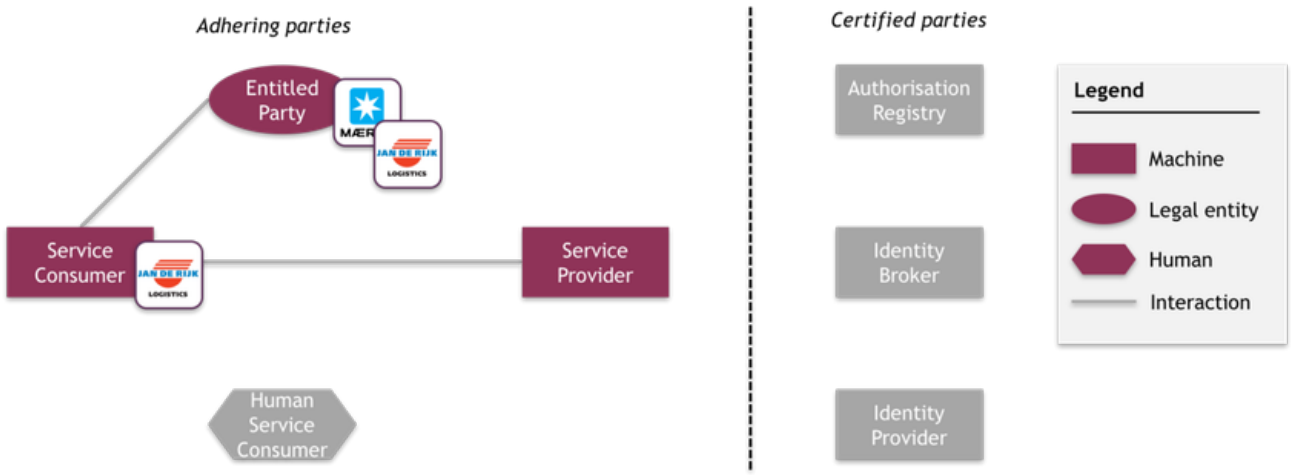
In use case 1b, a service is provided by the Service Provider to the Service Consumer, who has been delegated by the Entitled Party.

Note that this use case is exactly the same as the old use case 2.

Roles

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

Depiction



Note that for this use case, the Entitled Party (Maersk) delegates its rights to a third party (Jan de Rijk). If a third party is delegated by the Entitled Party, this delegated party can also be considered Entitled Party. In this use case, therefore, two Entitled Parties appear.

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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer
- The Entitled Party delegates (part of) its rights (as registered at the Service Provider) to the Service Consumer of another legal entity. He provides the delegated Service Consumer with evidence of this delegation

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

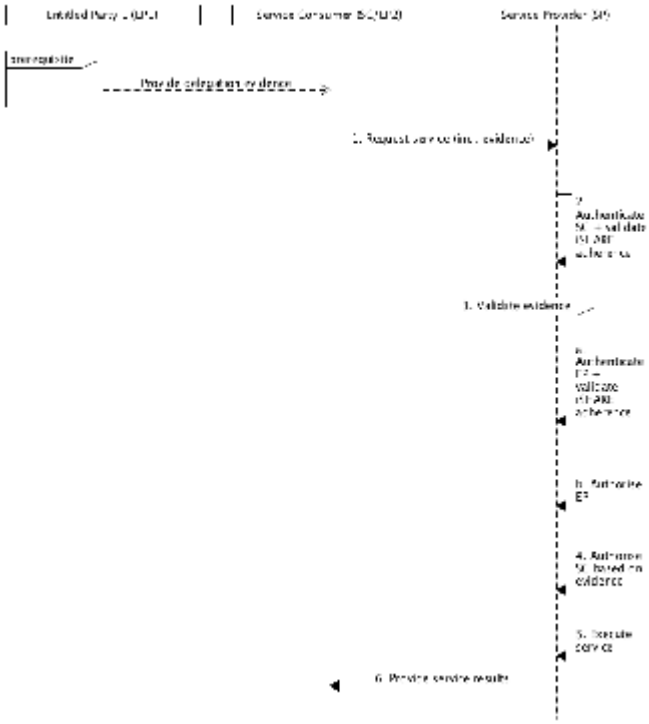
The use case consists of the following steps:

1. The Service Consumer requests a service from the Service Provider. With this requests he includes the evidence obtained from the Entitled Party
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider validates the received delegation evidence through the following steps:
    a. The Service Provider authenticates the Entitled Party and validates it as an iSHARE adhering party based on the delegation evidence
    b. The Service Provider authorises the Entitled Party based on the authorisation information registered with the Service Provider
4. The Service Provider authorises 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 Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



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

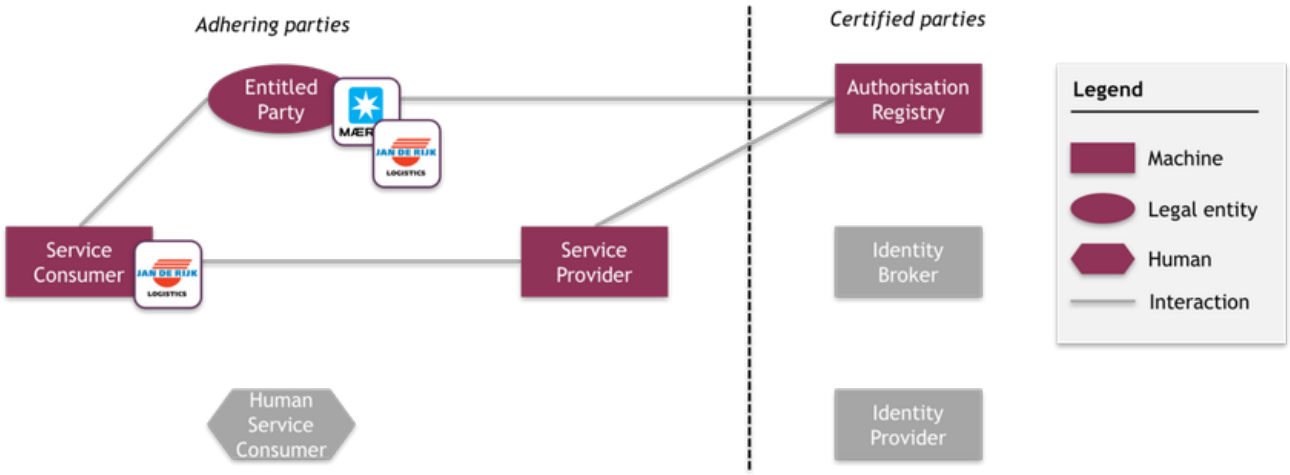
In use case 1c, a service is provided by the Service Provider to the Service Consumer, who has been delegated by the Entitled Party. Delegation evidence is now registered at a Authorisation Registry.

Note that this use case is exactly the same as the old use case 3.

Roles

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

Depiction



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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer
- The Entitled Party delegates (part of) its rights (as registered at the Service Provider) to the Service Consumer of another legal entity. 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:

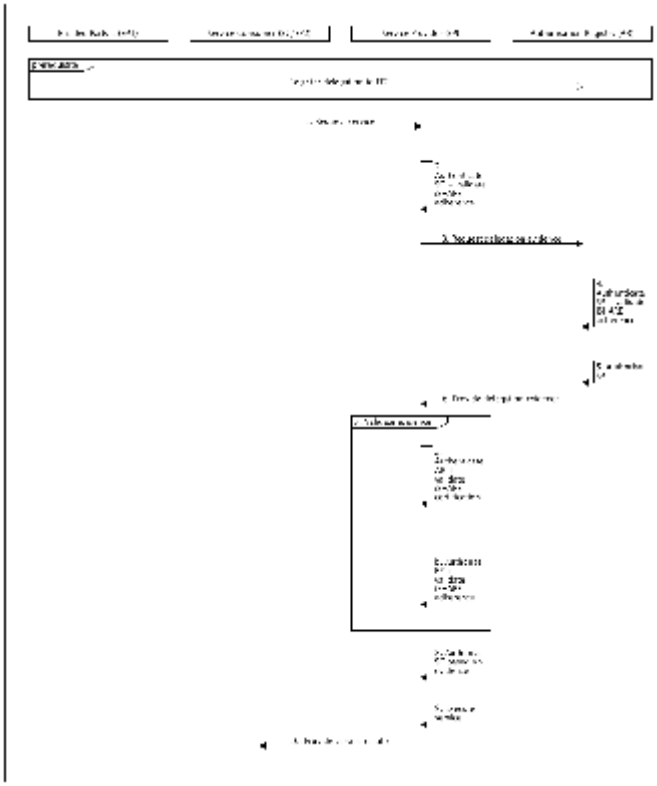
1. The Service Consumer requests a service from the Service Provider
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider requests delegation evidence from the Authorisation Registry
4. The Authorisation Registry authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE adhering party based on the delegation evidence
    b. The Service Provider authorises the Entitled Party based on the authorisation information registered with the Service Provider
8. The Service Provider authorises 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 Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



M2M service provision including an app

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

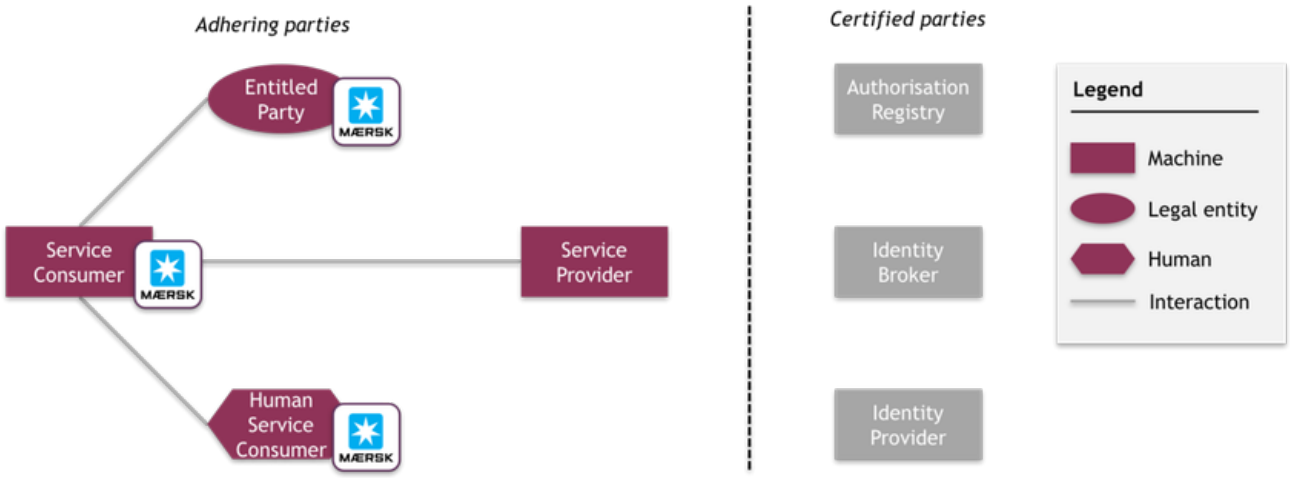
Note that this use case is exactly the same as the old use case 1B.

Roles

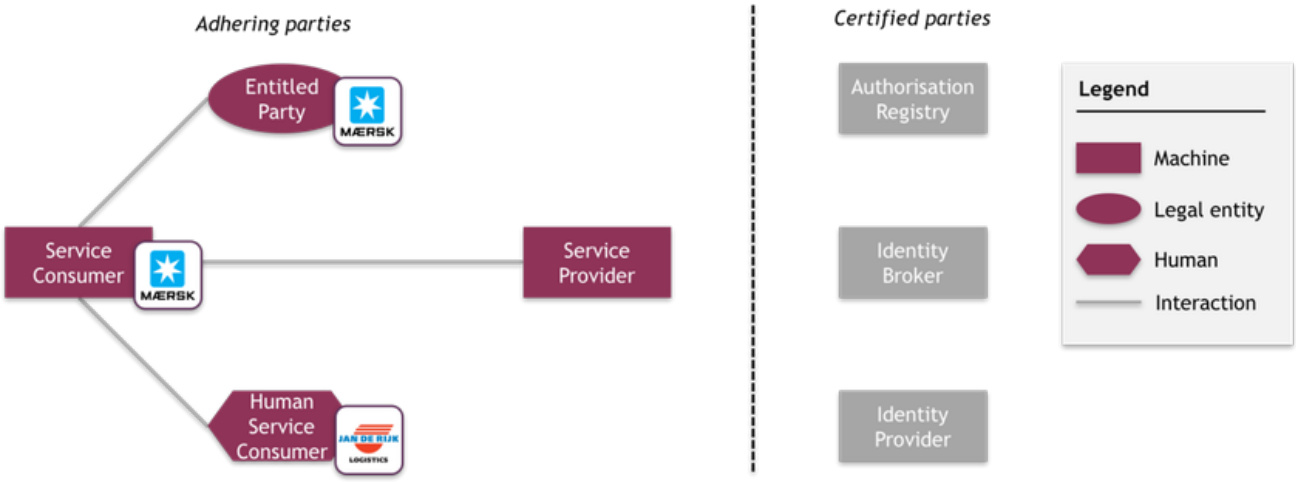
	Delegation info PIP			
	No delegation	Service Provider	Entitled Party	Authorisation Reg
Use case variation	1	1a	1b	1c

Depiction

Human Service Consumer at the Entitled Party



Human Service Consumer at another party



Description

As to use case 1, 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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer

- In this use case the Entitled Party acts as Service Consumer

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

Note that if the Human Service Consumer that is using an app to initiate use case 1 is at another party than the Entitled Party, bilateral agreements are needed between the Entitled Party and the third party about what Human Service Consumers of the third party can and cannot do.

The use case consists of the following steps:

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

1. The Service Consumer requests a service from the Service Provider
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider authorises the Service Consumer based on the authorisation information registered with the Service Provider
4. The Service Provider executes the requested service
5. The Service Provider provides the service result to the Service Consumer

- The Human Service Consumer accesses the result through app

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram

To follow.

2. H2M service provision with identity info at the SP

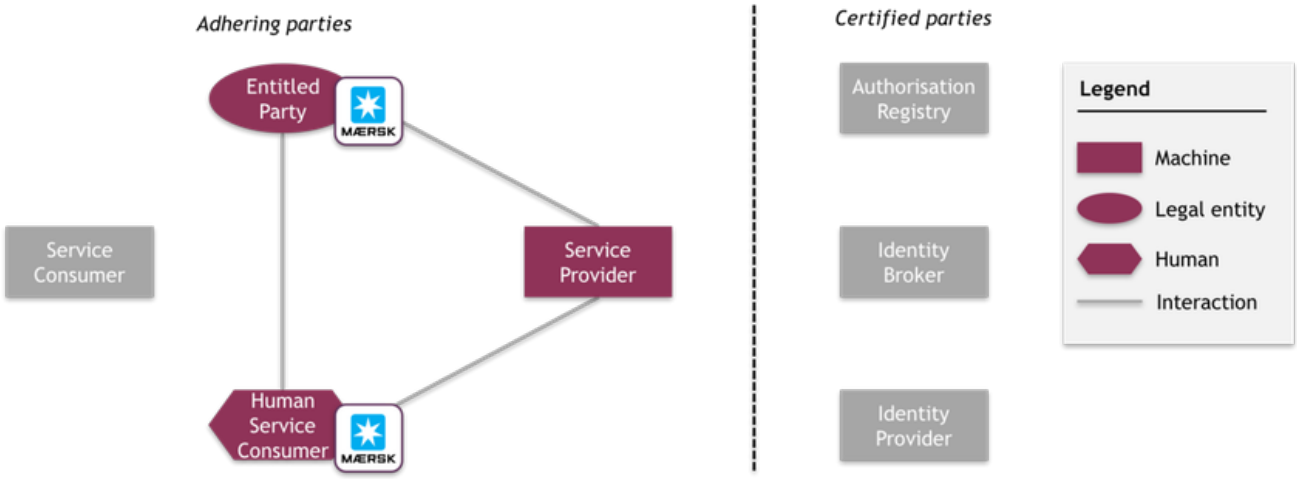
In use case 2, a service is provided by the Service Provider to the Human Service Consumer. Identity info is held at the Service Provider.

Roles

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

As there is no delegation, the Entitled Party acts as Human Service Consumer

Depiction



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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party 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 acts as Human Service Consumer

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

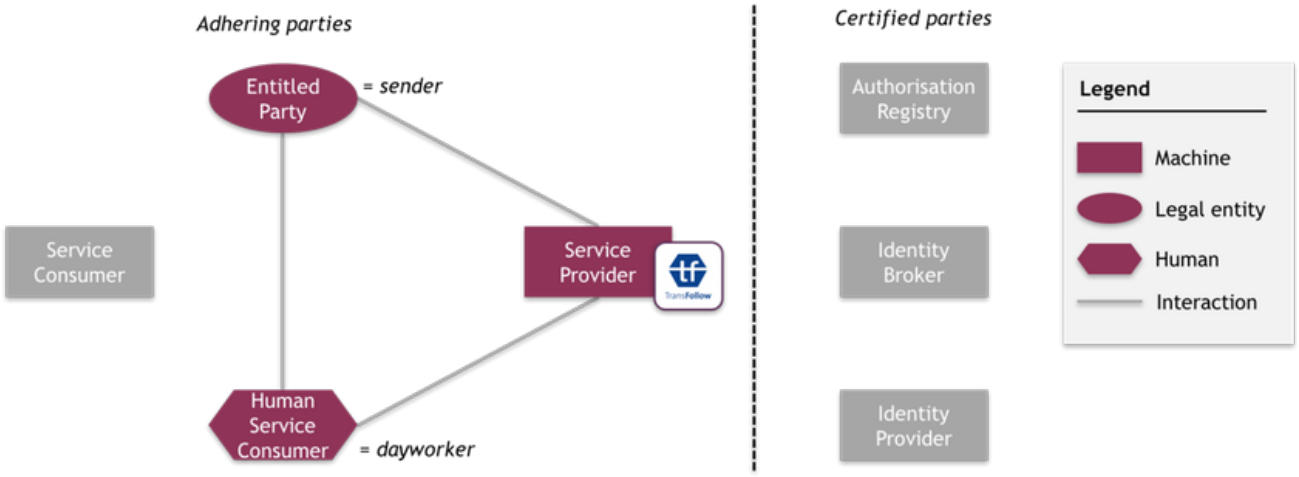
The use case consists of the following steps:

1. The Human Service Consumer requests a service from the Service Provider
2. The Service Provider authenticates the Human Service Consumer
3. The Service Provider authorises the Human Service Consumer based on the authorisation information registered with the Service Provider
4. The Service Provider executes the requested service
5. The Service Provider provides the service result to the Human Service Consumer

Practical examples

Transfollow: "A sender authorises a dayworker to sign a single Freight Document"

Depiction



Description

It is prerequisite of this use case that:

- TransFollow (the Service Provider) has and manages its own authorisation information indicating what Entitled Parties (e.g. senders) are entitled to what (parts of) services
- The sender (Entitled Party) has and manages its own authorisation information indicating which dayworkers (Human Service Consumers) are authorised to act on its behalf**
- The sender registers the authorisation information at TransFollow
- The dayworker is able to authenticate TransFollow
- TransFollow is able to authenticate the dayworker
- The dayworker has been issued identity credentials by TransFollow

** The sender can outsource this function to a third party

The use case consists of the following steps:

1. The dayworker requests a service from TransFollow
2. TransFollow authenticates the dayworker
3. TransFollow authorises the dayworker based on the authorisation information it has
4. TransFollow executes the requested service
5. TransFollow provides the service result to the dayworker

Sequence diagram

To follow.

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.

Note that this use case is exactly the same as the old use case 4B.

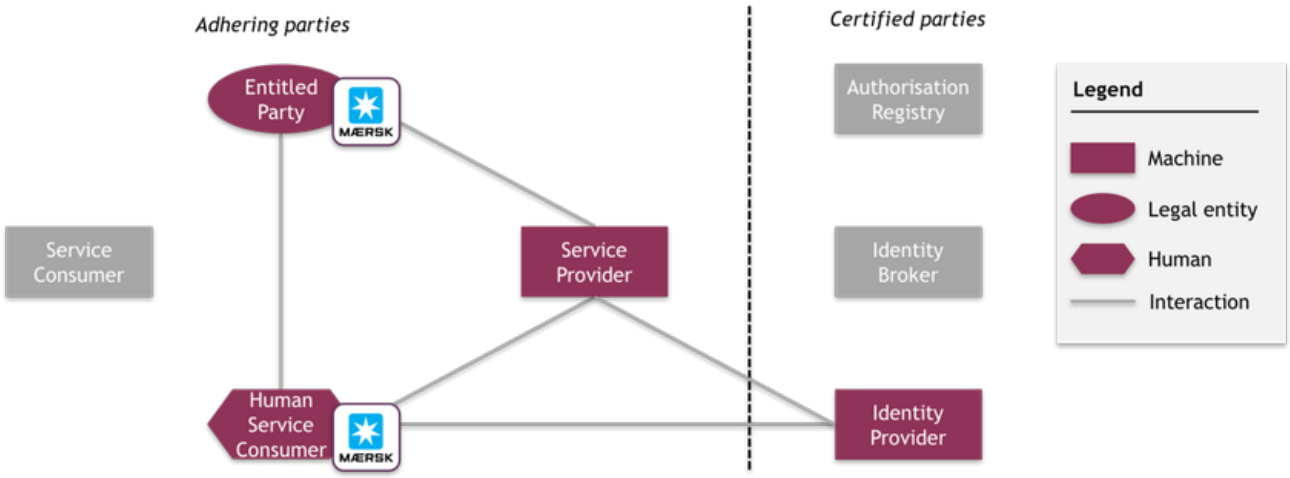
Roles

		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	3b.1
	Authorisation Reg	3.2	3a.2	3b.2	3b.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 there is no delegation, the Entitled Party acts as Human Service Consumer

Depiction



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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party 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 acts as Human 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:

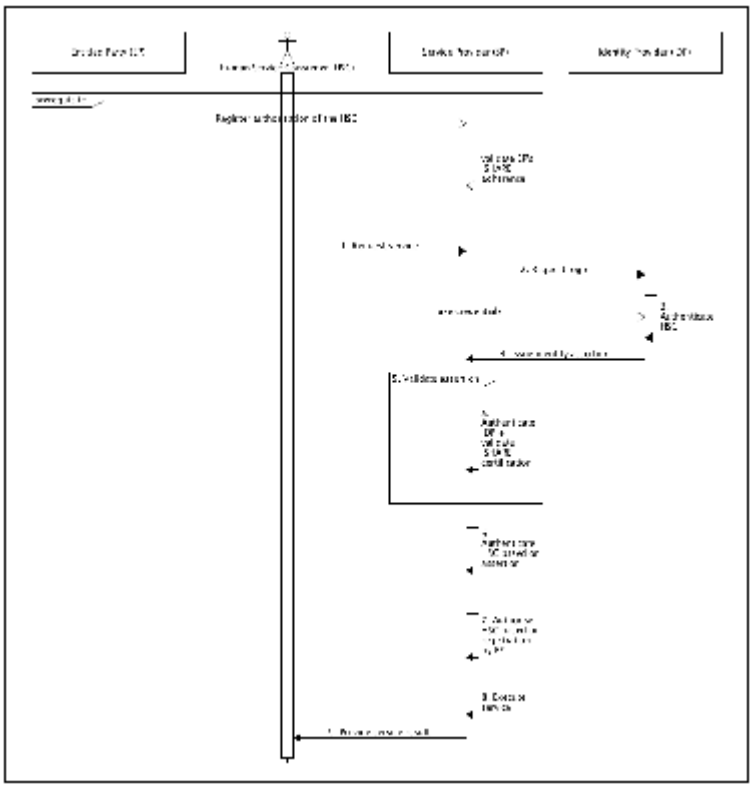
1. The Human Service Consumer requests a service from the Service Provider

2. The Service Provider requests a login from the Identity 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 it as an iSHARE certified party
6. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
7. The Service Provider authorises the Human Service Consumer based on the authorisation information registered with the Service Provider
8. The Service Provider executes the requested service
9. The Service Provider provides the service result to the Service Consumer

Practical examples

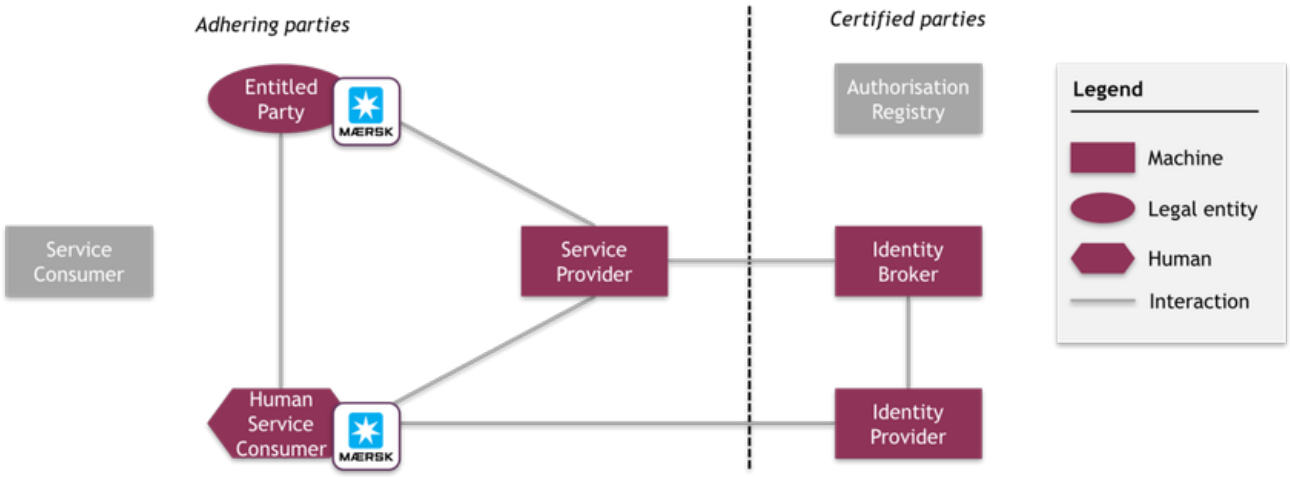
All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that an Identity Broker can be introduced to broker the relation between the Service Provider and both the Authorisation Registry and the Identity Provider; this is optional and useful in situations with several Authorisation Registries and (especially) several Identity Providers. This use case would look as follows with a Service Broker:

Depiction with Identity Broker



Description with Identity Broker

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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party 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 acts as Human Service Consumer

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

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

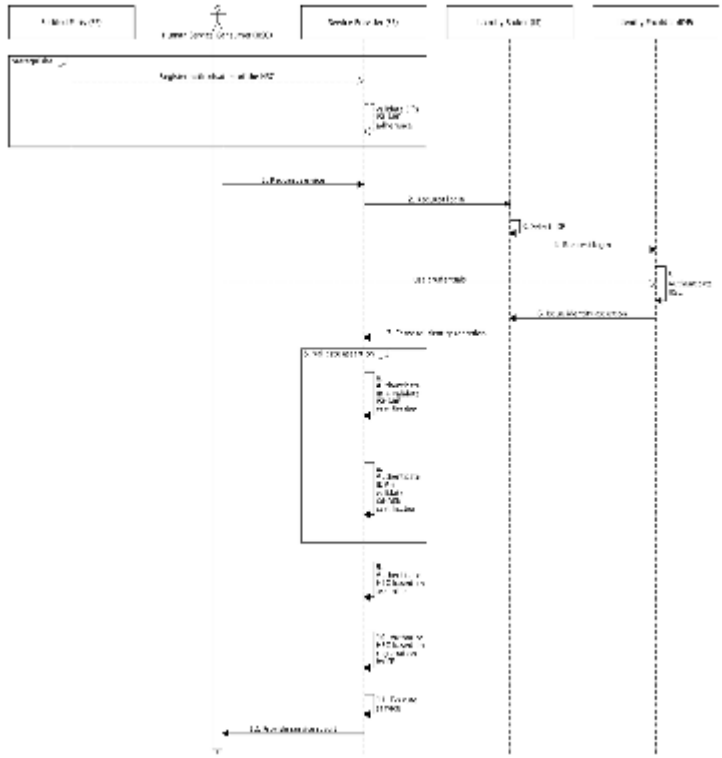
The use case consists of the following steps:

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 it as an iSHARE certified party
    b. The Service Provider authenticates the Identity Provider and validates it as an iSHARE certified party
9. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
10. The Service Provider authorises the Human 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 Service Consumer

Practical examples with Identity Broker

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram with Identity Broker



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

In use case 3.2, a service is provided by the Service Provider to the Human Service Consumer.

Note that this use case is exactly the same as the old use case 6.

Roles

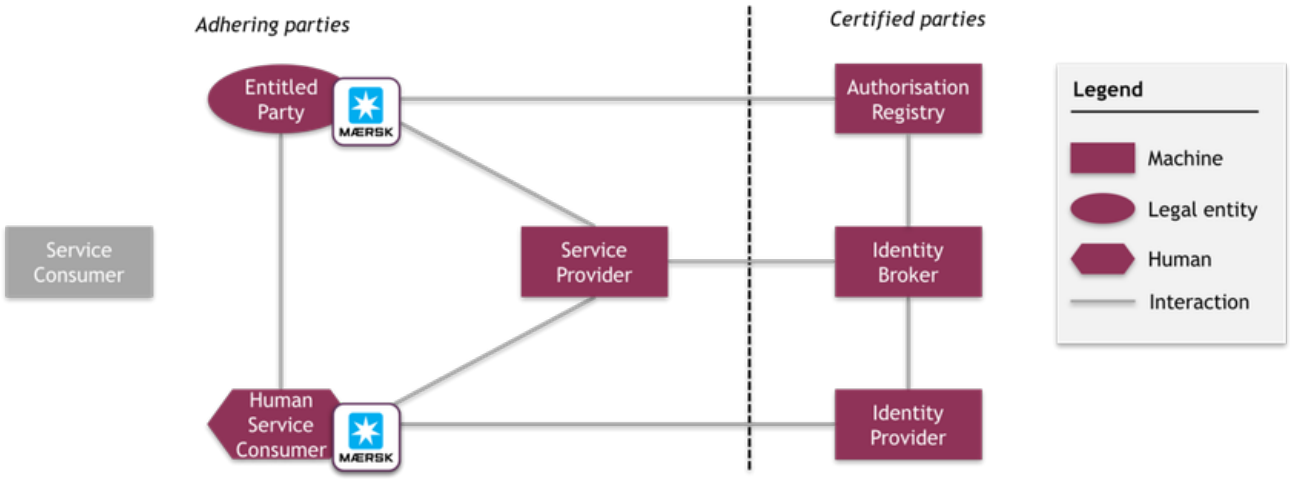
		Delegation info PIP			
		No delegation	Service Provider	Entitled Party	Authorisation Reg
Auth info PIP	Service Provider	3	3a	3b	3c
	Entitled Party	3.1	3a.1	3b.1	3c.1
	Authorisation Reg	3.2	3a.2	3b.2	3c.2
	Identity Provider*	3.3	3a.3	3b.3	3c.3

*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 there is no delegation, the Entitled Party acts as Human Service Consumer

Note that an Identity Broker is introduced to broker the relation between the Service Provider and both the Authorisation Registry and the Identity Provider; this is optional and useful in situations with several Authorisation Registries and (especially) several Identity Providers.

Depiction



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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party registers the authorisation information at the 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 acts as Human Service Consumer

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

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

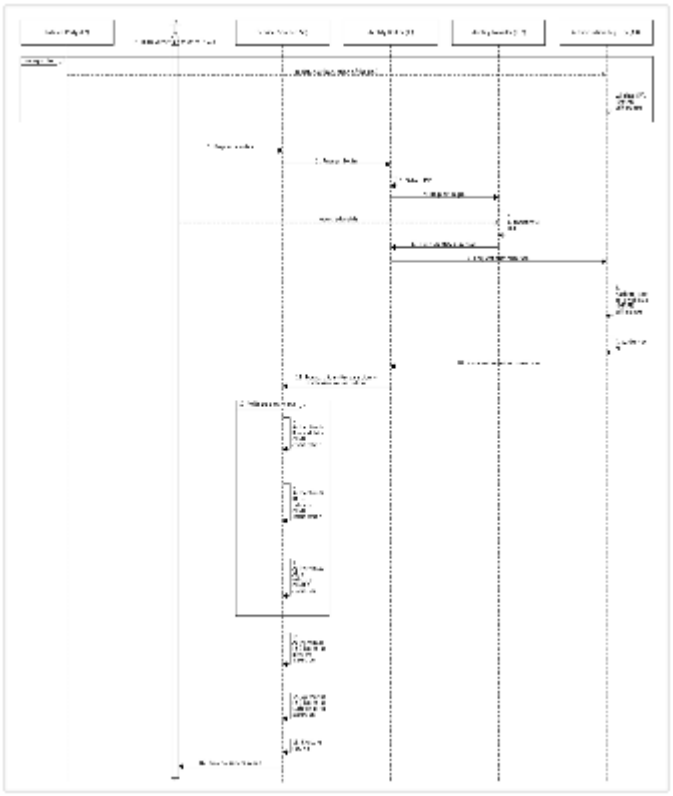
The use case consists of the following steps:

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 requests authorisation evidence from the Authorisation Registry
8. The Authorisation Registry authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE certified party
    b. The Service Provider authenticates the Identity Provider and validates it as an iSHARE certified party
    c. The Service Provider authenticates the Authorisation Registry and validates it as an iSHARE certified party
13. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
14. The Service Provider authorises the Human 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

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



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

In use case 3c.2, a service is provided by the Service Provider to the Human Service Consumer, who has been delegated by the Entitled Party. Delegation evidence is now registered at a Authorisation Registry.

Note that this use case is exactly the same as the old use case 7.

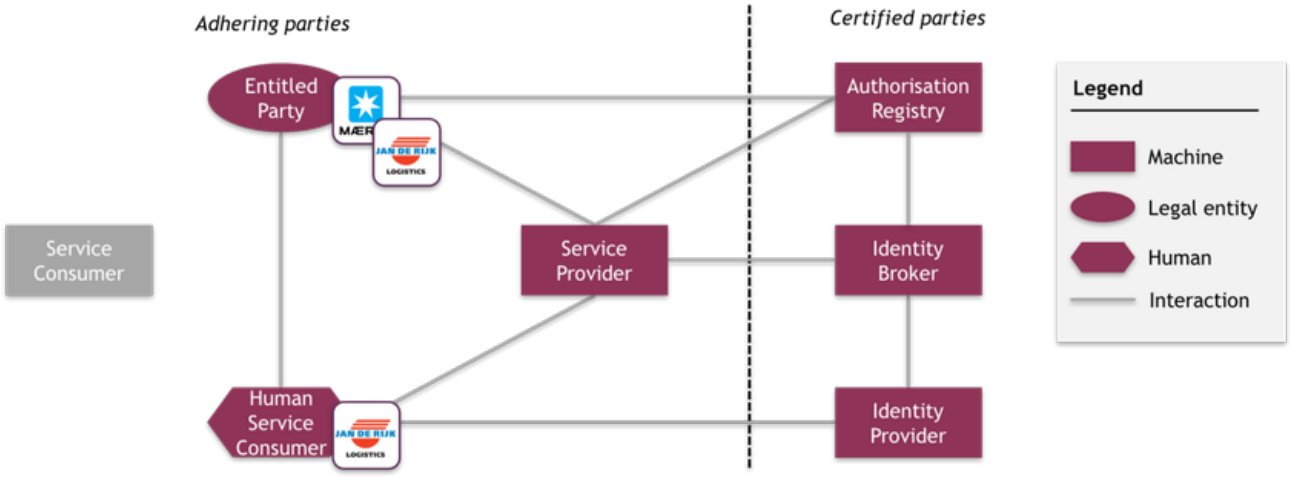
Roles

		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 both the Authorisation Registry and the Identity Provider; this is optional and useful in situations with several Authorisation Registries and (especially) several Identity Providers.

Depiction



Note that for this use case, the Entitled Party (Maersk) delegates its rights to a third party (Jan de Rijk). If a third party is delegated by the Entitled Party, this delegated party can also be considered Entitled Party. In this use case, therefore, two Entitled Parties appear. Because both Entitled Parties utilise another Authorisation Registry (Maersk to register its delegation and Jan de Rijk to register its authorisations), two Authorisation Registries appear as well.

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 Entitled Party (Entitled Party 1) delegates (part of) its rights (as registered at the Service Provider) to Entitled Party 2. He registers this delegation in Authorisation Registry 2
- Entitled Party 2 has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- Entitled Party 2 registers the authorisation information at 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 evidence 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 In this use case the Entitled Party acts as Human 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:

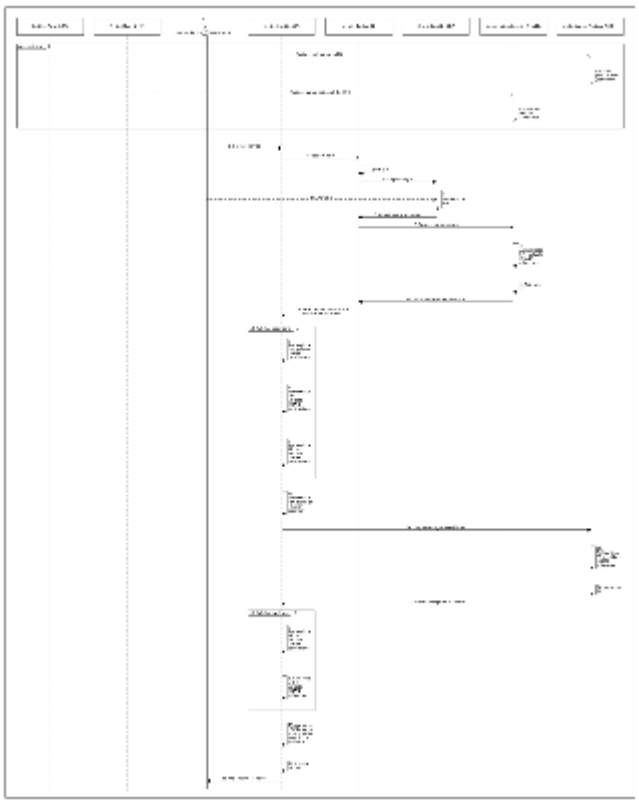
1. The Human Service Consumer requests a service from the Service Provider
2. The Service Provider requests a login from the Identity Broker
3. The Identity Broker asks the Human Service Consumer to select his Identity Provider
4. The Identity Broker requests a login from the Identity Provider
5. The 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 requests authorisation evidence from Authorisation Registry 1
8. Authorisation Registry 1 authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE certified party
    b. The Service Provider authenticates the Identity Provider and validates it as an iSHARE certified party
    c. The Service Provider authenticates Authorisation Registry 1 and validates it as an iSHARE certified party
13. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
14. The Service Provider requests delegation evidence from Authorisation Registry 2
15. Authorisation Registry 2 authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE certified party
    b. The Service Provider authorises Entitled Party 1 based on the authorisation information registered with the Service Provider, and validates it as an iSHARE adhering party
19. The Service Provider authorises the Human 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

Practical examples

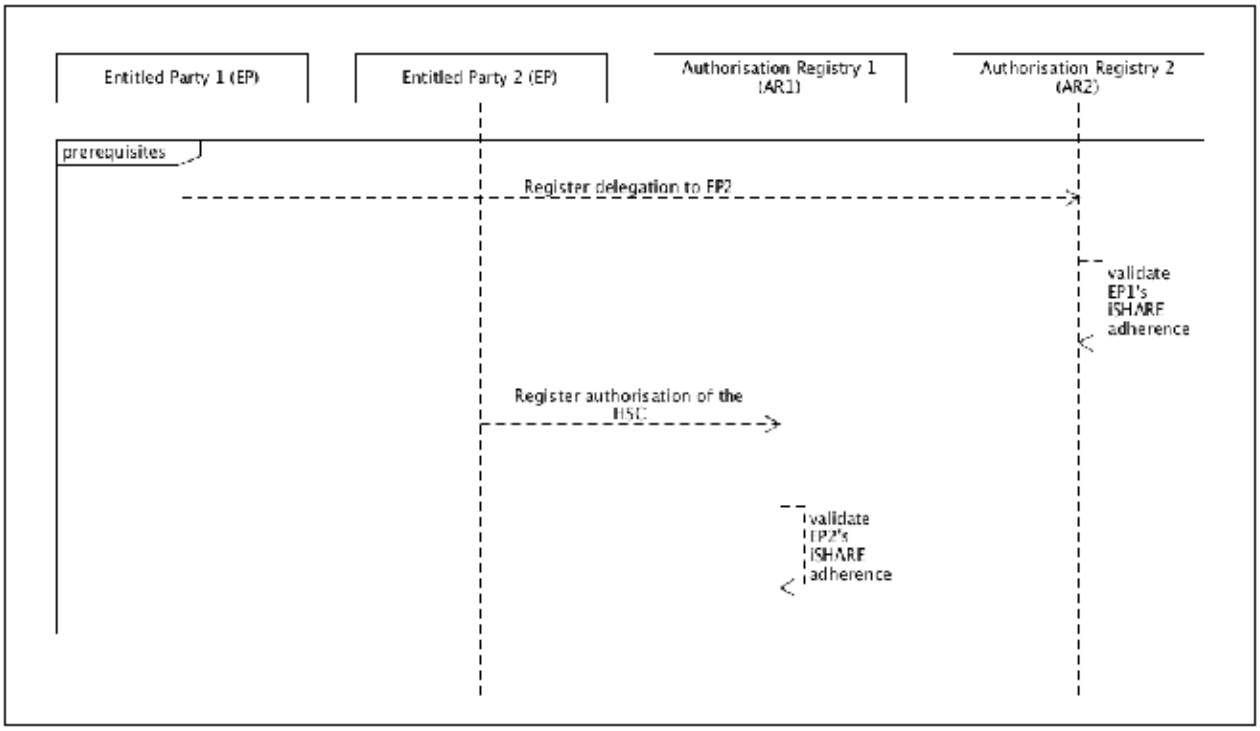
All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagrams

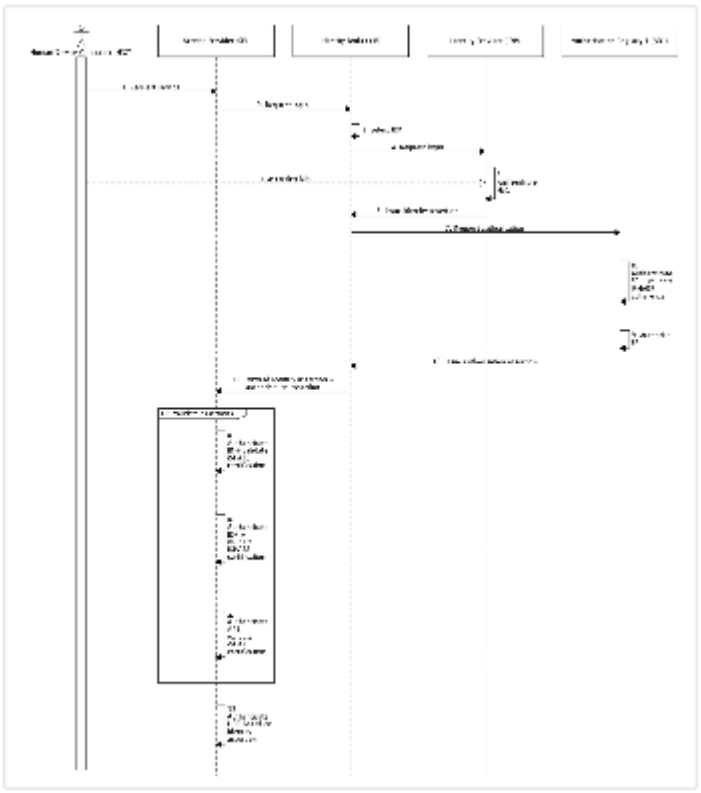
Total



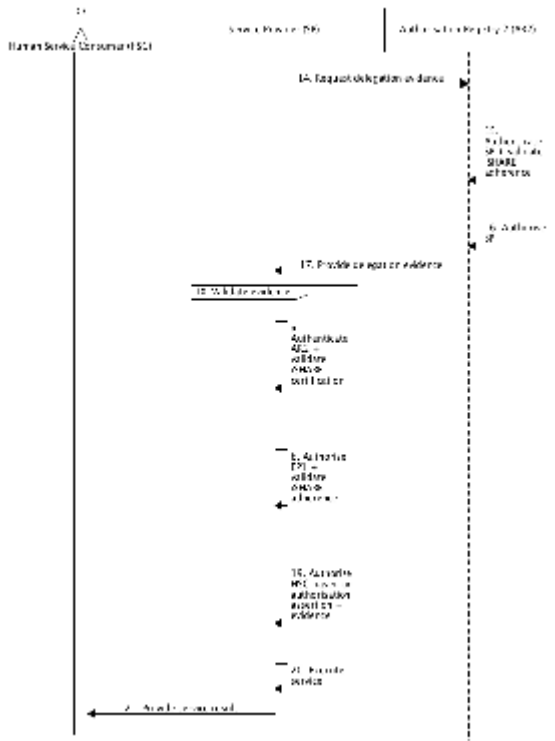
Prerequisites



Authentication and Authorisation



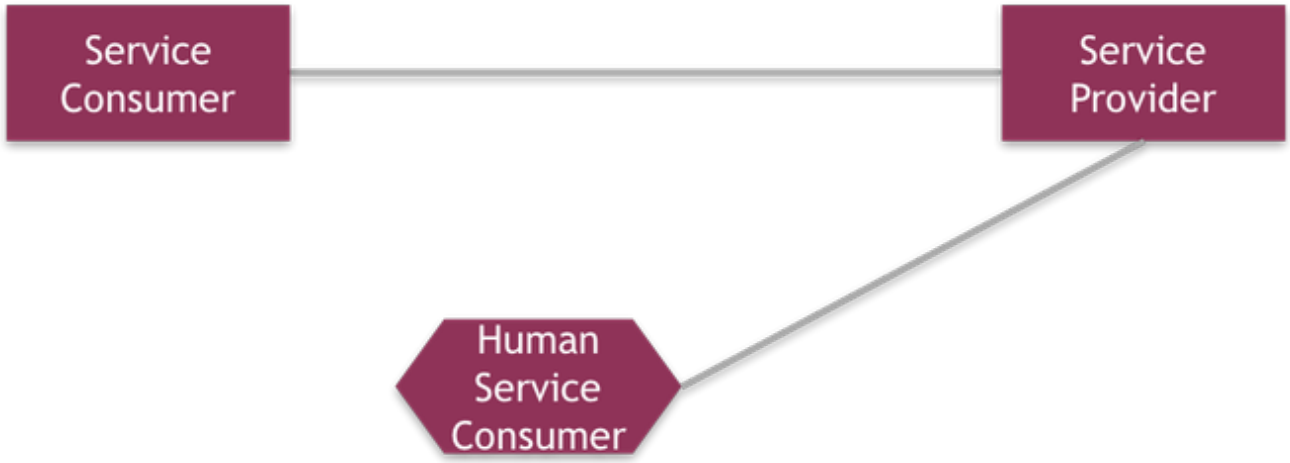
Delegation



Primary use cases (old)

In this section we elaborate on the primary use cases that iSHARE supports.

Every primary use case involves *at least* two roles; either the Human Service Consumer or the Service Consumer, and the Service Provider:



Note that the basic framework depicted above does not state anything about the legal and/or operational environment, in which it functions. Depending on the agreements made within the iSHARE scheme, certain exchanges of data might be fuelled by functional and technical agreements, while not falling within the scope of any legal and operational agreement.

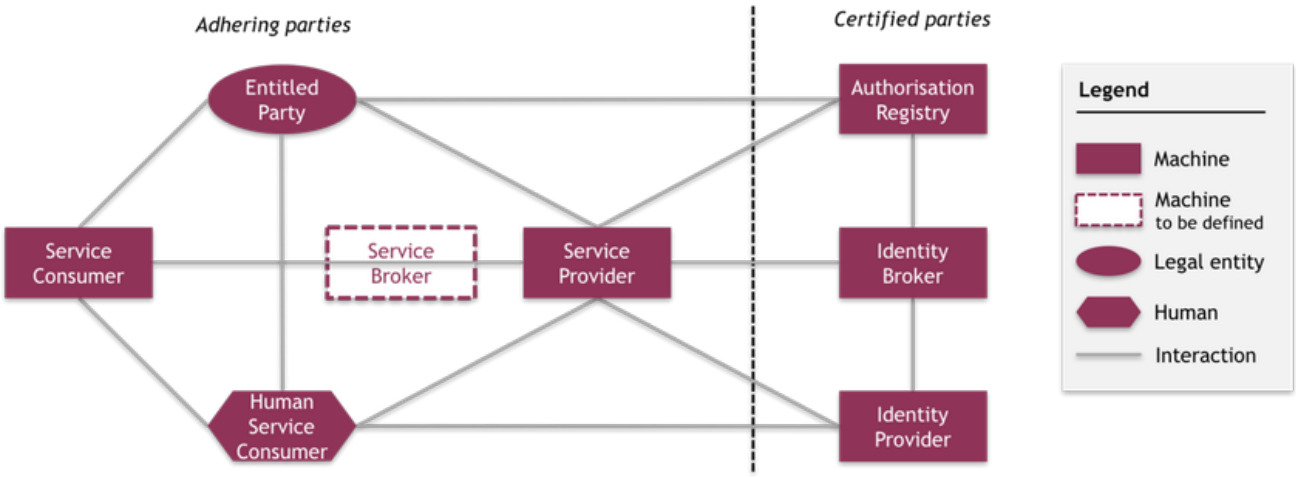
There are two basic interaction models: Machine to Machine (M2M) and Human to Machine (H2M). All primary use cases are related to either one of these models. Based on the functional requirements per interaction model, the following primary use cases can be distinguished:

Interaction model	**M2M**				**H2M**				
Use cases	**1A**	**1B**	**2**	**3**	**4A**	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

! Note that use case 4A is considered irrelevant until proven otherwise - as it seems no Service Consumer will request login from an Identity Provider before requesting a service from the Service Provider.

All roles are depicted as follows:



Note that parties fulfilling a certain role can be iSHARE adhering or -certified, as explained here.

Use case presentation

All of the use cases are described on a separate Confluence-page, as follows:

- Roles
- Depiction
- Description
- Practical examples
- Sequence diagram

Unhappy flows

Possible unhappy flows for each use case will be detailed. Unhappy flow communication should not include any clues about data - "no freight found", for example, can also be valuable information.

Interaction models

In this section the two types of interaction models will be explained: Machine to Machine (M2M) and Human to Machine (H2M).

Machine to Machine (M2M)

Sometimes called server-to-server, **machine-to-machine (M2M)** communication stands for any technology that enables the automated exchange of information and the performance of actions between electronic devices without requiring the assistance of humans. In some M2M applications, the electronic devices exchange their information with a central control unit/application which processes the information for humans.

To exchange (send and receive) information (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 (H2M)

Human-to-machine (H2M) communication is used for data transmission between a human (user) and a 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.

Even though the term H2M can be used in a much broader sense (see "Note" hereunder) we mean the human-computer interaction where humans and computers interact through a user interface and perform activities for each other. This includes software (i.e. what is visible to the human on the computer monitor) and hardware (i.e. the mouse, keyboard and other devices).

1A. M2M – Basic service provision

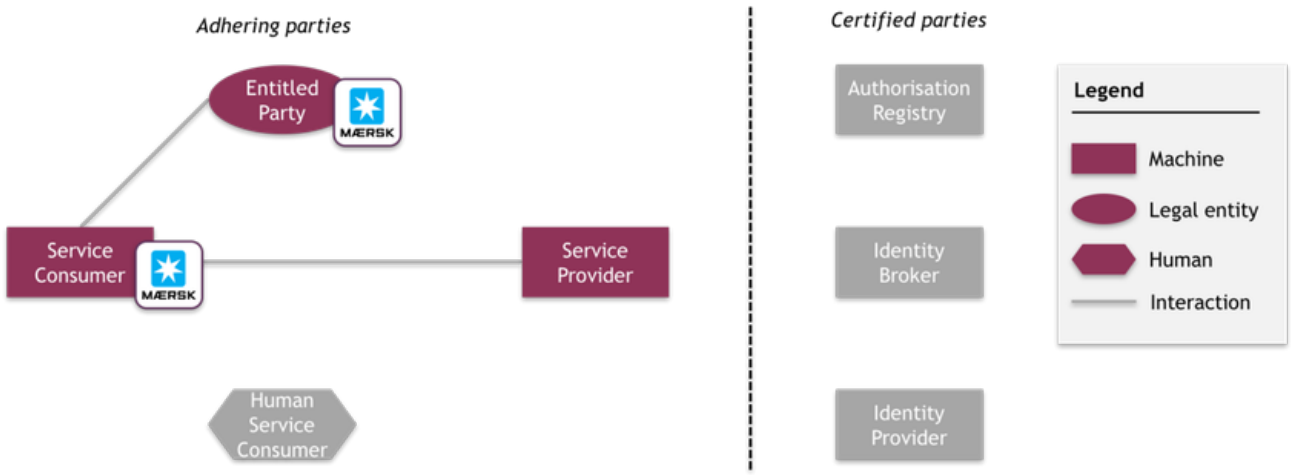
In use case 1A, a service is provided by the Service Provider to the Service Consumer.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	**4A**	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer

- In this use case the Entitled Party acts as Service Consumer

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

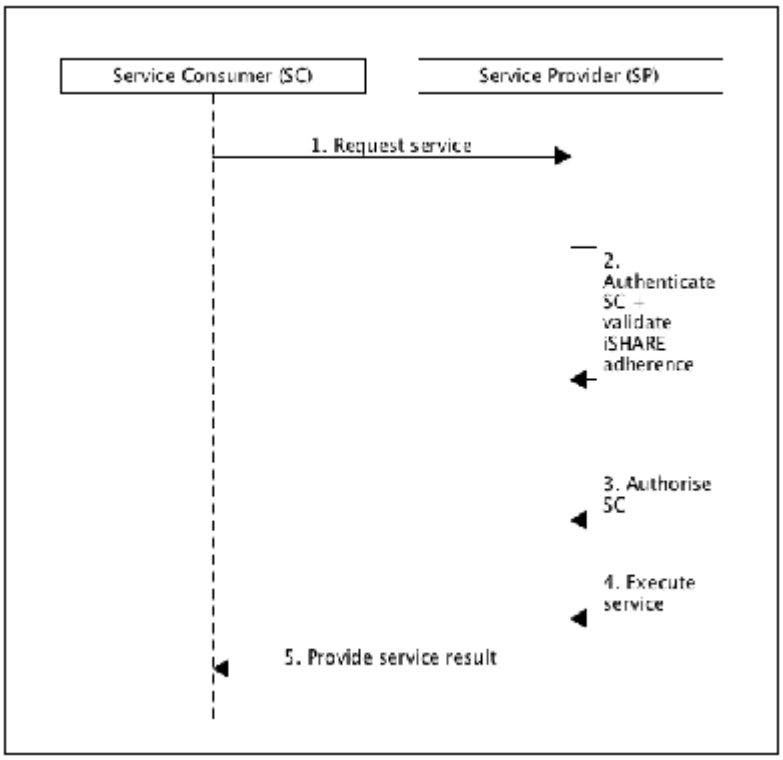
The use case consists of the following steps:

1. The Service Consumer requests a service from the Service Provider
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider authorises the Service Consumer based on the authorisation information registered with the Service Provider
4. The Service Provider executes the requested service
5. The Service Provider provides the service result to the Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

1B. M2M – Basic service provision including an app

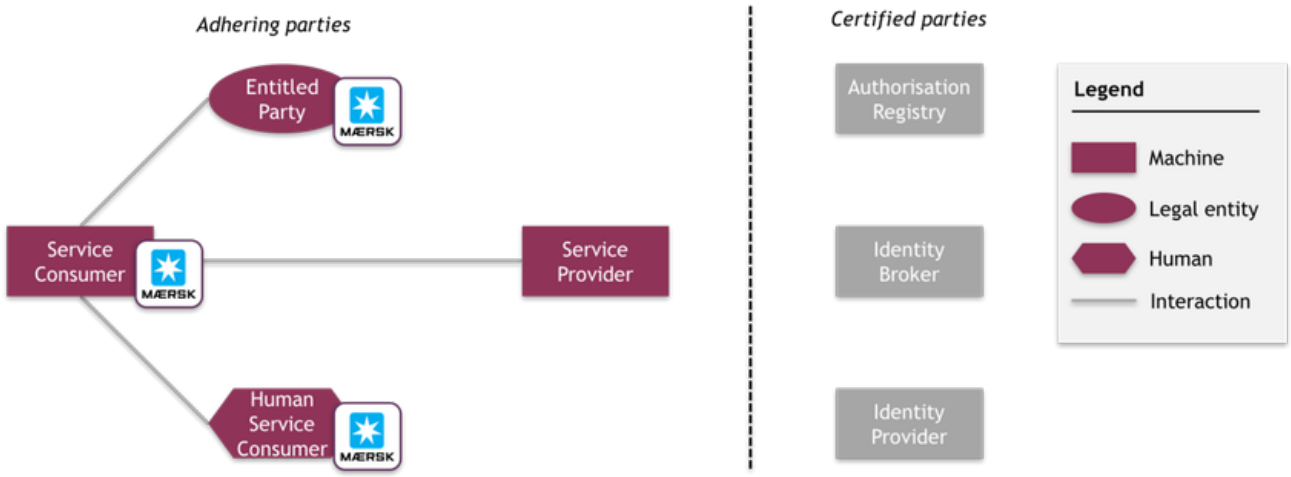
In use case 1B, a service is provided by the Service Provider to the Service Consumer after initiation by the Human Service Consumer through an app.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	**4A**	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer

- In this use case the Entitled Party acts as 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 Service Consumer
- The request is mapped to a service request

1. The Service Consumer requests a service from the Service Provider
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider authorises the Service Consumer based on the authorisation information registered with the Service Provider
4. The Service Provider executes the requested service
5. The Service Provider provides the service result to the Service Consumer

- The Human Service Consumer accesses the result through app

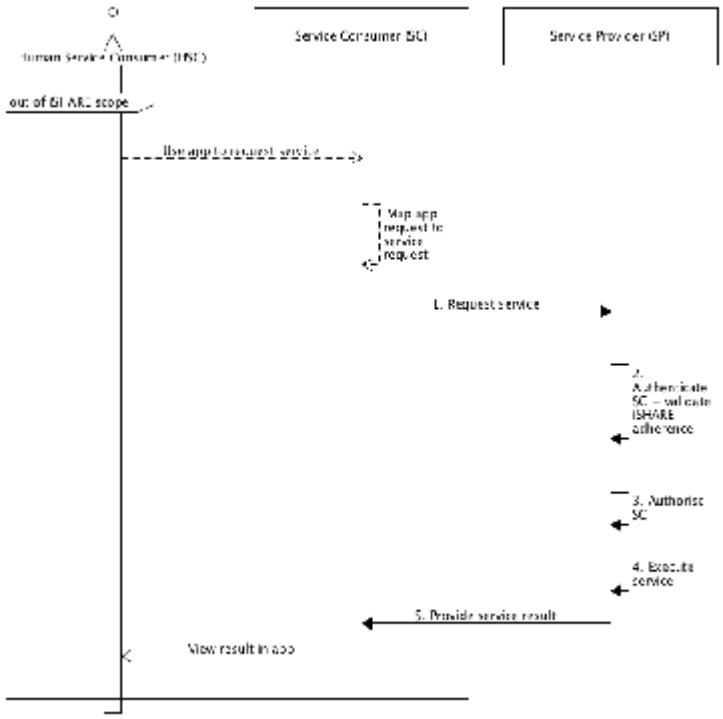
Note that for the Service Provider, there is no difference between use case 1A and 1B – and that both use cases are considered M2M.

Also note that in use case 2 and 3, the same steps can be added to include the usage of an app. These steps are not included, however.

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

2. M2M – Service provision based on delegation

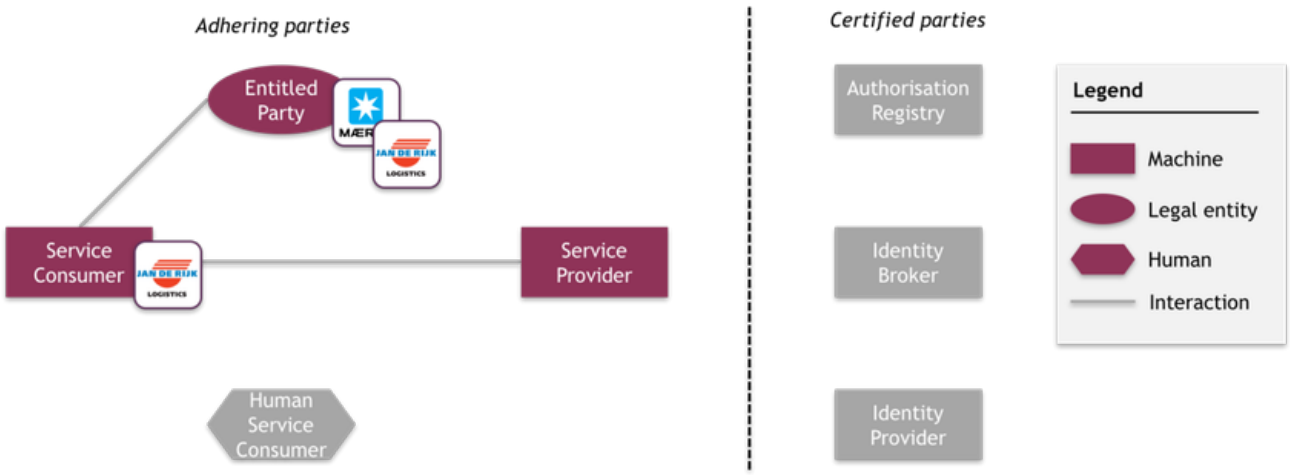
In use case 2, a service is provided by the Service Provider, to the Service Consumer, who has been delegated by the Entitled Party.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	**4A**	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



Note that for this use case, the Entitled Party (Maersk) delegates its rights to a third party (Jan de Rijk). If a third party is delegated by the Entitled Party, this delegated party can also be considered Entitled Party. In this use case, therefore, two Entitled Parties appear.

Description

Note that in use case 2, the same steps as in use case 1B can be added to include the usage of an app. These steps are not included, however.

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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer
- The Entitled Party delegates (part of) its rights (as registered at the Service Provider) to the Service Consumer of another legal entity. He provides the delegated 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:

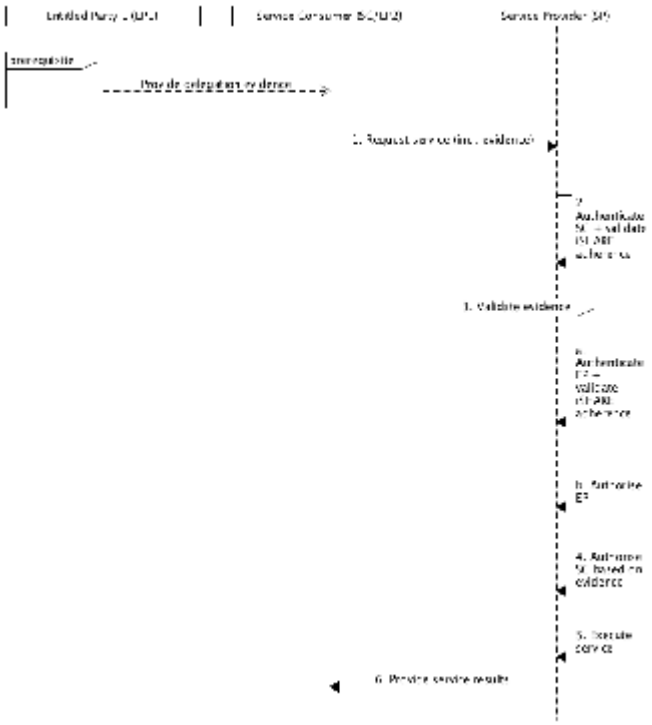
1. The Service Consumer requests a service from the Service Provider. With this requests he includes the evidence obtained from

the Entitled Party
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider validates the received delegation evidence through the following steps:
    a. The Service Provider authenticates the Entitled Party and validates it as an iSHARE adhering party based on the delegation evidence
    b. The Service Provider authorises the Entitled Party based on the authorisation information registered with the Service Provider
4. The Service Provider authorises 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 Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

3. M2M – Service provision based on delegation involving an Authorisation Registry

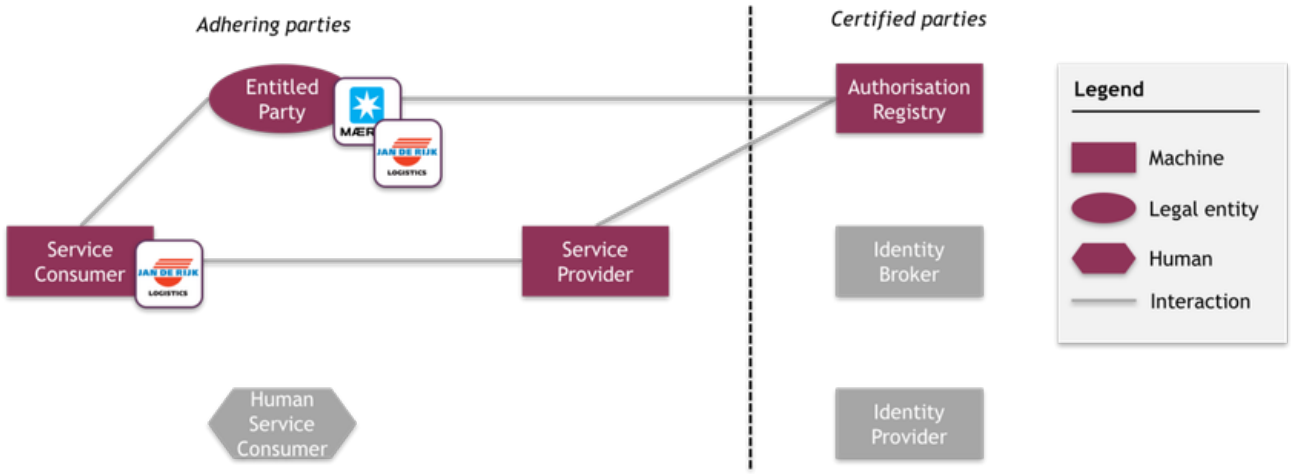
In use case 3, a service is provided by the Service Provider to the Service Consumer, who has been delegated by the Entitled Party. Delegation evidence is now registered at a Authorisation Registry.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	**4A**	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



Description

Note that in use case 3, the same steps as in use case 1B can be added to include the usage of an app. These steps are not included, however.

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 is able to authenticate the Service Provider
- The Service Provider is able to authenticate the Service Consumer
- The Entitled Party delegates (part of) its rights (as registered at the Service Provider) to the Service Consumer of another legal entity. 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

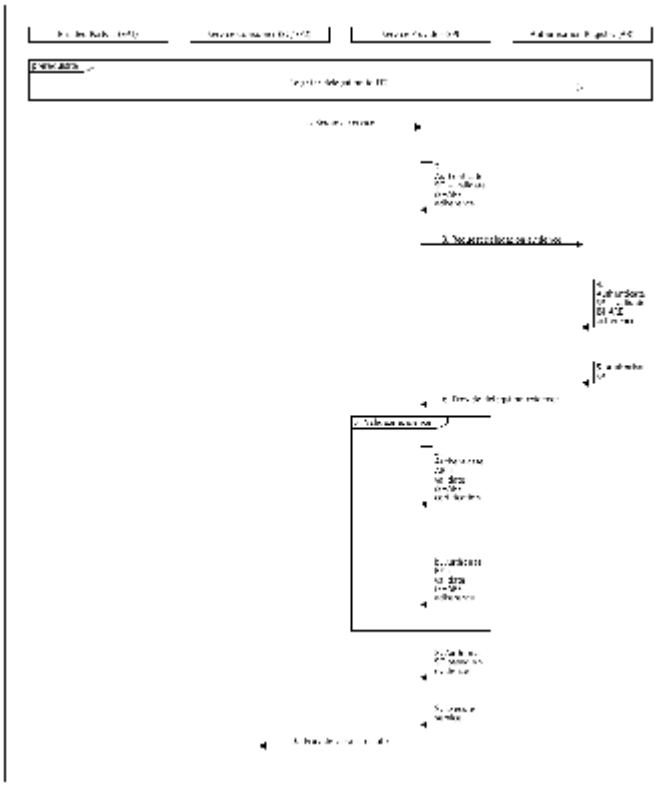
The use case consists of the following steps:

1. The Service Consumer requests a service from the Service Provider
2. The Service Provider authenticates the Service Consumer and validates it as an iSHARE adhering party
3. The Service Provider requests delegation evidence from the Authorisation Registry
4. The Authorisation Registry authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE adhering party based on the delegation evidence
    b. The Service Provider authorises the Entitled Party based on the authorisation information registered with the Service Provider
8. The Service Provider authorises 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 Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

4A. H2M – Basic service provision

In use case 4A, a service is provided by the Service Provider to the Human Service Consumer.

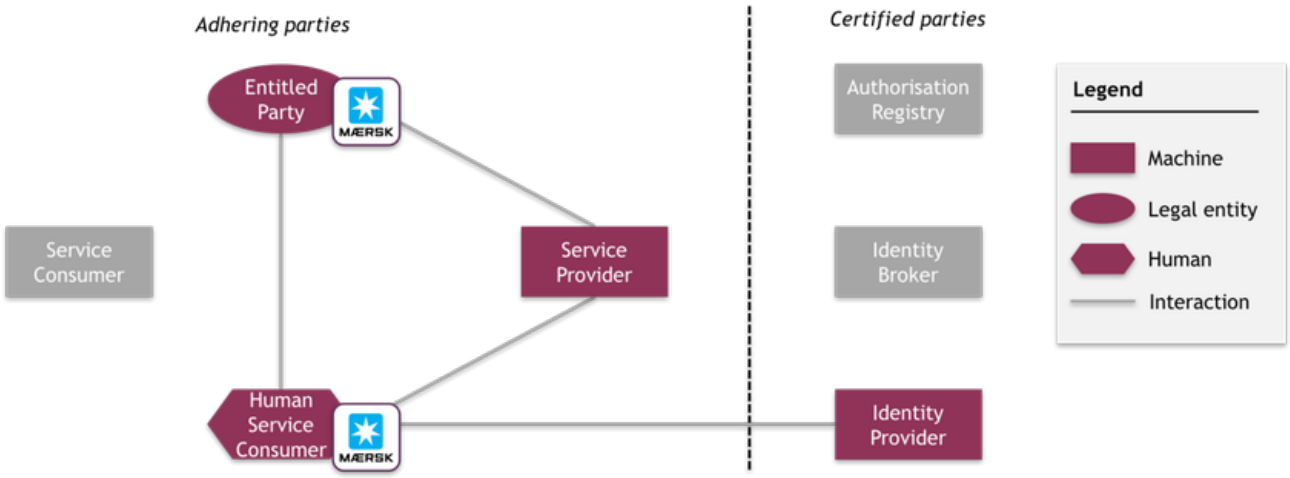
! Note that use case 4A is considered irrelevant until proven otherwise - as it seems no Service Consumer will request login from an Identity Provider before requesting a service from the Service Provider.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	4A	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party 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 acts as Human Service Consumer

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

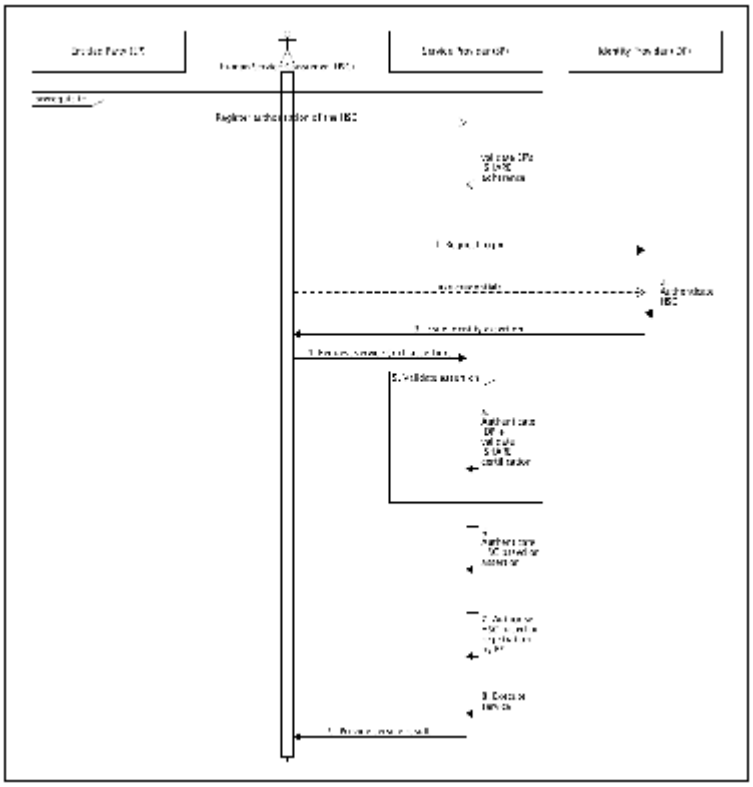
The use case consists of the following steps:

1. The Service Provider requests a login from the Identity Provider
2. The Identity Provider authenticates the Human Service Consumer
3. The Identity Provider issues an identity assertion to the Service Provider
4. The Human Service Consumer requests a service from the Service Provider, including its identity assertion
5. The Service Provider validates the identity assertion through the following steps:
    a. The Service Provider authenticates the Identity Provider and validates it as an iSHARE certified party
6. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
7. The Service Provider authorises the Human Service Consumer based on the authorisation information registered with the Service Provider
8. The Service Provider executes the requested service
9. The Service Provider provides the service result to the Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

4B. H2M – Basic service provision

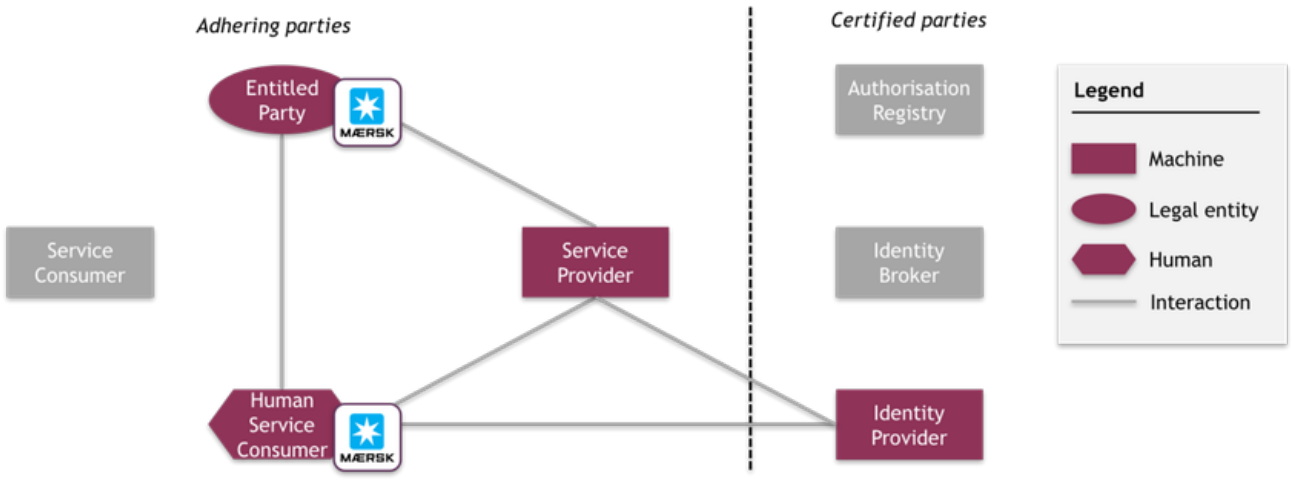
In use case 4B, a service is provided by the Service Provider to the Human Service Consumer.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	4A	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party 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 acts as Human 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:

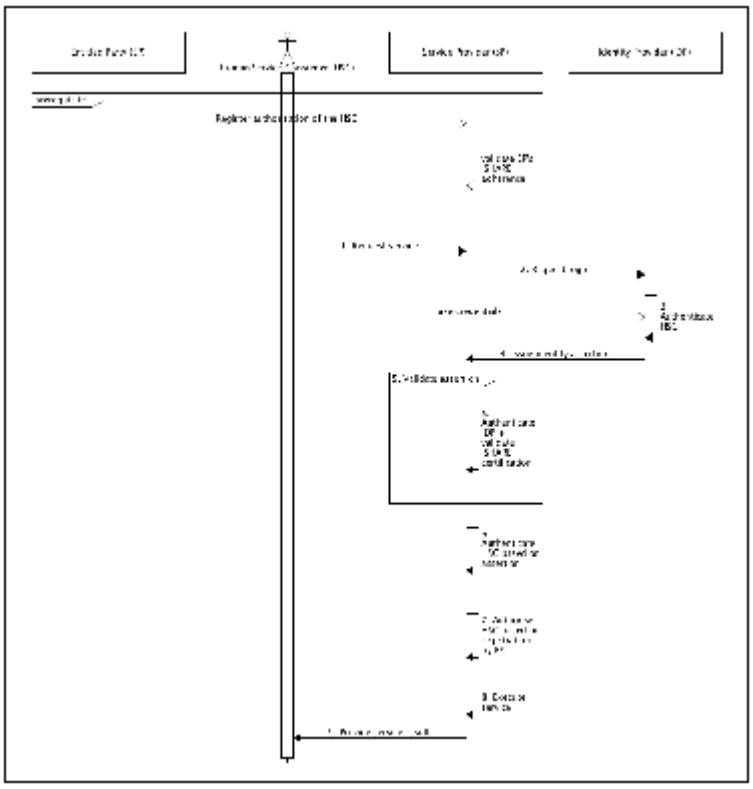
1. The Human Service Consumer requests a service from the Service Provider

2. The Service Provider requests a login from the Identity 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 it as an iSHARE certified party
6. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
7. The Service Provider authorises the Human Service Consumer based on the authorisation information registered with the Service Provider
8. The Service Provider executes the requested service
9. The Service Provider provides the service result to the Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

5. H2M – Service provision involving an Identity Broker

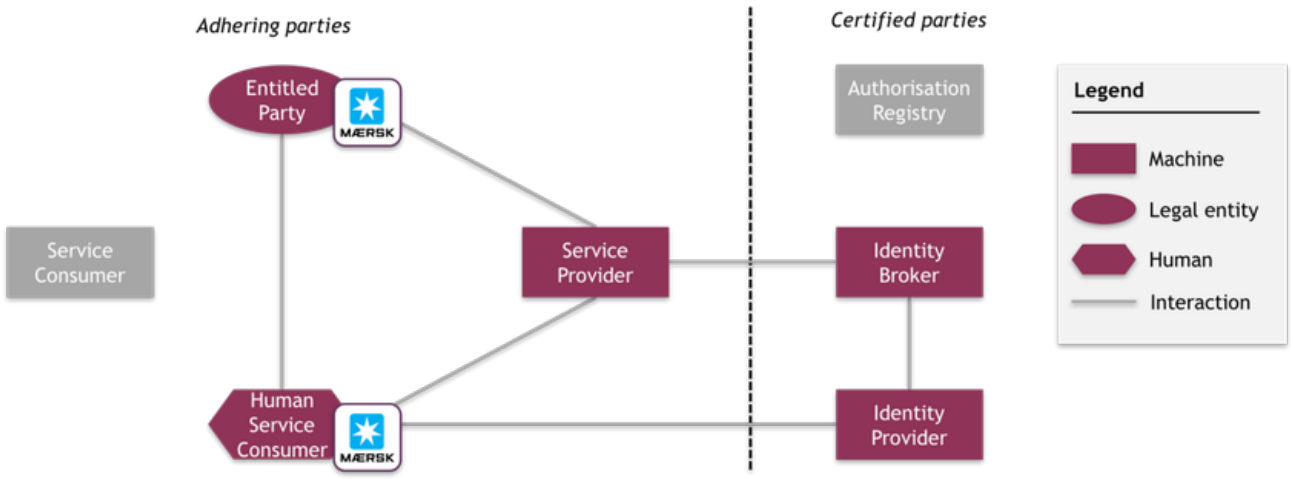
In use case 5, a service is provided to the Human Service Consumer by the Service Provider.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	4A	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party 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 acts as Human Service Consumer

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

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

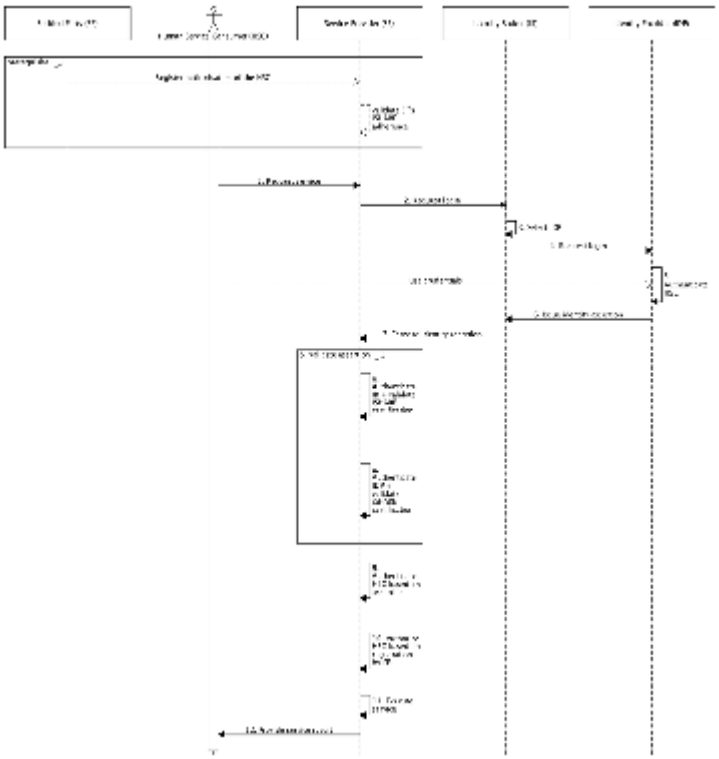
The use case consists of the following steps:

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 it as an iSHARE certified party
    b. The Service Provider authenticates the Identity Provider and validates it as an iSHARE certified party
9. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
10. The Service Provider authorises the Human 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 Service Consumer

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

6. H2M – Service provision based on eHerkenning model

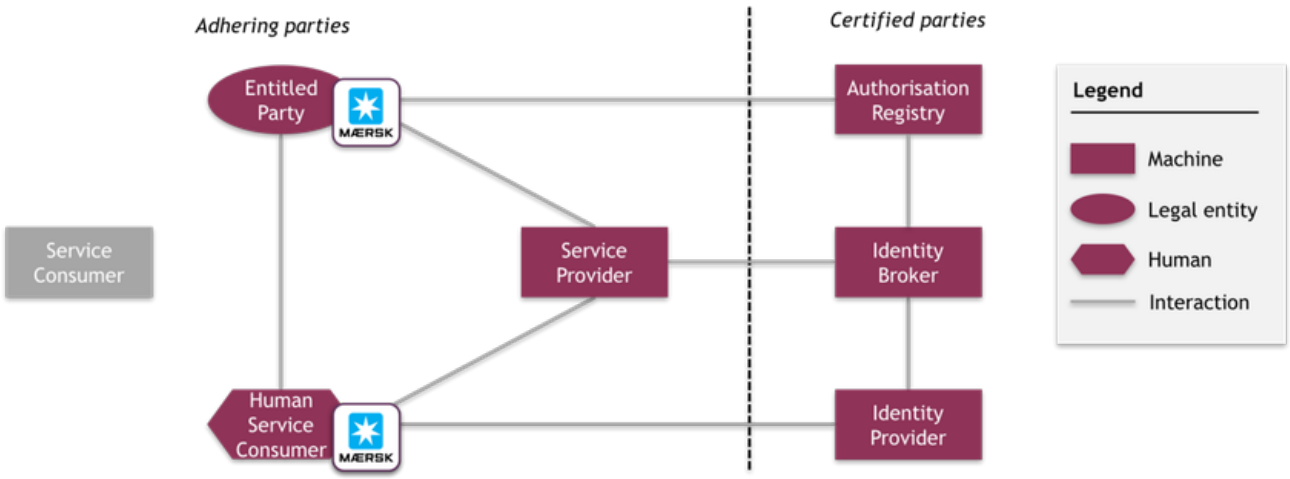
In use case 6, a service is provided by the Service Provider to the Human Service Consumer.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	**4A**	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



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 Entitled Party has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- The Entitled Party registers the authorisation information at the 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 acts as Human Service Consumer

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

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

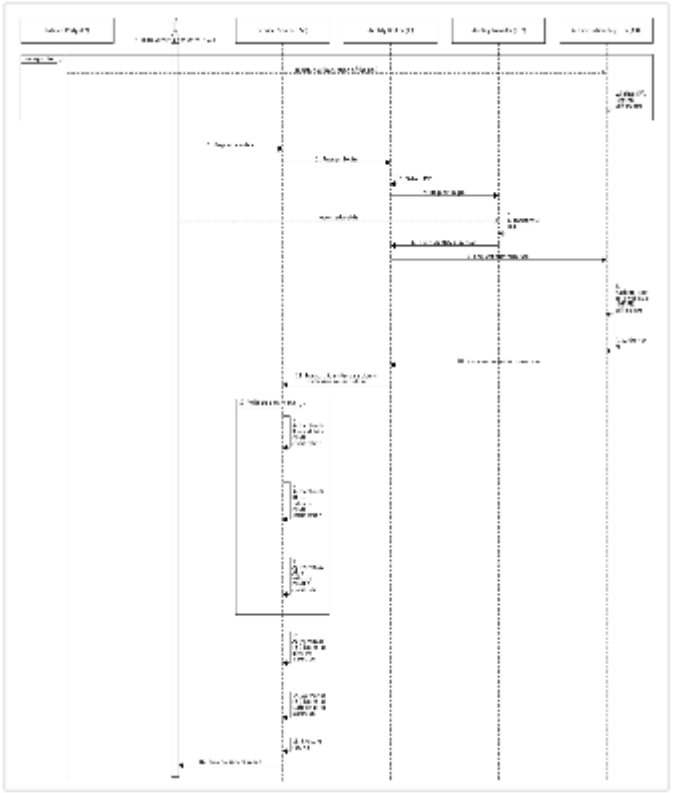
The use case consists of the following steps:

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 requests authorisation evidence from the Authorisation Registry
8. The Authorisation Registry authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE certified party
    b. The Service Provider authenticates the Identity Provider and validates it as an iSHARE certified party
    c. The Service Provider authenticates the Authorisation Registry and validates it as an iSHARE certified party
13. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
14. The Service Provider authorises the Human 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

Practical examples

All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagram



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

7. H2M – Service provision based on delegation, involving an Identity Broker and an Authorisation Registry

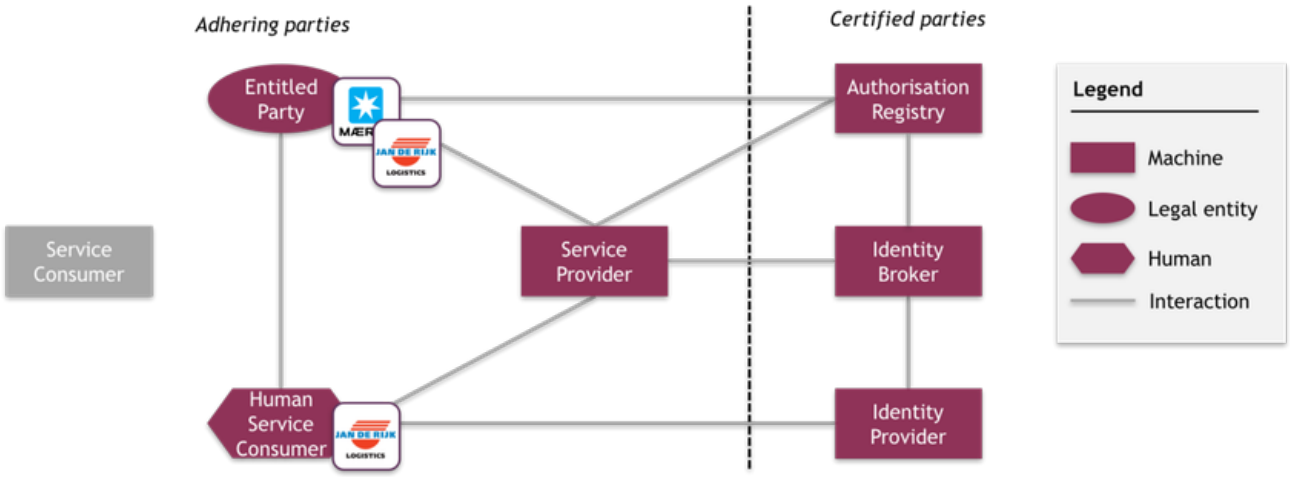
In use case 7, a service is provided by the Service Provider to the Human Service Consumer, who has been delegated by the Entitled Party. Delegation evidence is now registered at a Authorisation Registry.

Roles

Interaction model	M2M				H2M				
Use cases	**1A**	**1B**	**2**	**3**	**4A**	**4B**	**5**	**6**	**7**
Roles:									
Service Consumer	X	X	X	X					
Human Service Consumer		X			X	X	X	X	X
Service Provider	X	X	X	X	X	X	X	X	X
Entitled Party	X*	X*	X**	X**	X*	X*	X*	X*	X**
Authorisation Registry				X			X	X	X**
Identity Provider					X	X	X	X	X
Identity Broker							X	X	X

* Acting as (Human) Service Consumer
** Appears twice

Depiction



Note that for this use case, the Entitled Party (Maersk) delegates its rights to a third party (Jan de Rijk). If a third party is delegated by the Entitled Party, this delegated party can also be considered Entitled Party. In this use case, therefore, two Entitled Parties appear. Because both Entitled Parties utilise another Authorisation Registry (Maersk to register its delegation and Jan de Rijk to register its authorisations), two Authorisation Registries appear as well.

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 Entitled Party (Entitled Party 1) delegates (part of) its rights (as registered at the Service Provider) to Entitled Party 2. He registers this delegation in Authorisation Registry 2
- Entitled Party 2 has and manages its own authorisation information indicating which Human Service Consumers are authorised to act on its behalf**
- Entitled Party 2 registers the authorisation information at 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 evidence 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 In this use case the Entitled Party acts as Human 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:

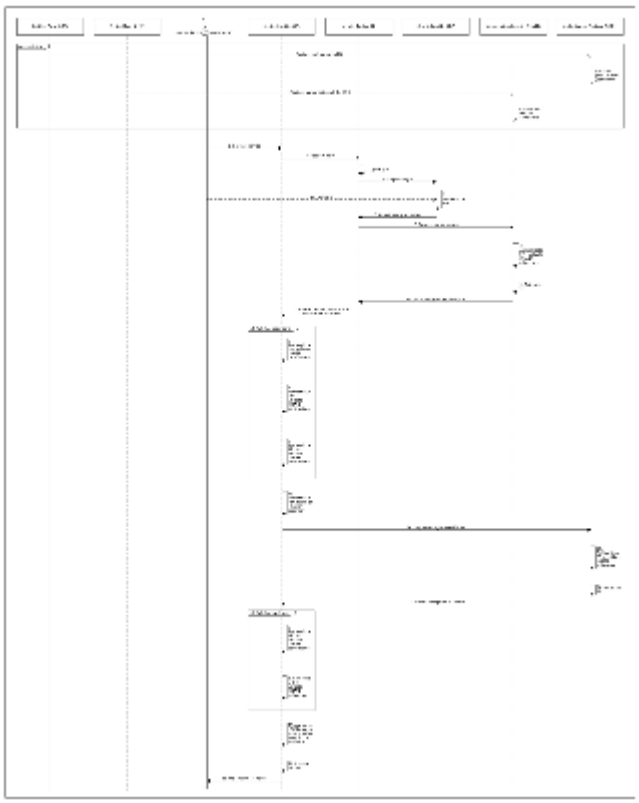
1. The Human Service Consumer requests a service from the Service Provider
2. The Service Provider requests a login from the Identity Broker
3. The Identity Broker asks the Human Service Consumer to select his Identity Provider
4. The Identity Broker requests a login from the Identity Provider
5. The 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 requests authorisation evidence from Authorisation Registry 1
8. Authorisation Registry 1 authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE certified party
    b. The Service Provider authenticates the Identity Provider and validates it as an iSHARE certified party
    c. The Service Provider authenticates Authorisation Registry 1 and validates it as an iSHARE certified party
13. The Service Provider authenticates the Human Service Consumer based on the validity of the identity assertion
14. The Service Provider requests delegation evidence from Authorisation Registry 2
15. Authorisation Registry 2 authenticates the Service Provider and validates it as an iSHARE adhering party
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 it as an iSHARE certified party
    b. The Service Provider authorises Entitled Party 1 based on the authorisation information registered with the Service Provider, and validates it as an iSHARE adhering party
19. The Service Provider authorises the Human 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

Practical examples

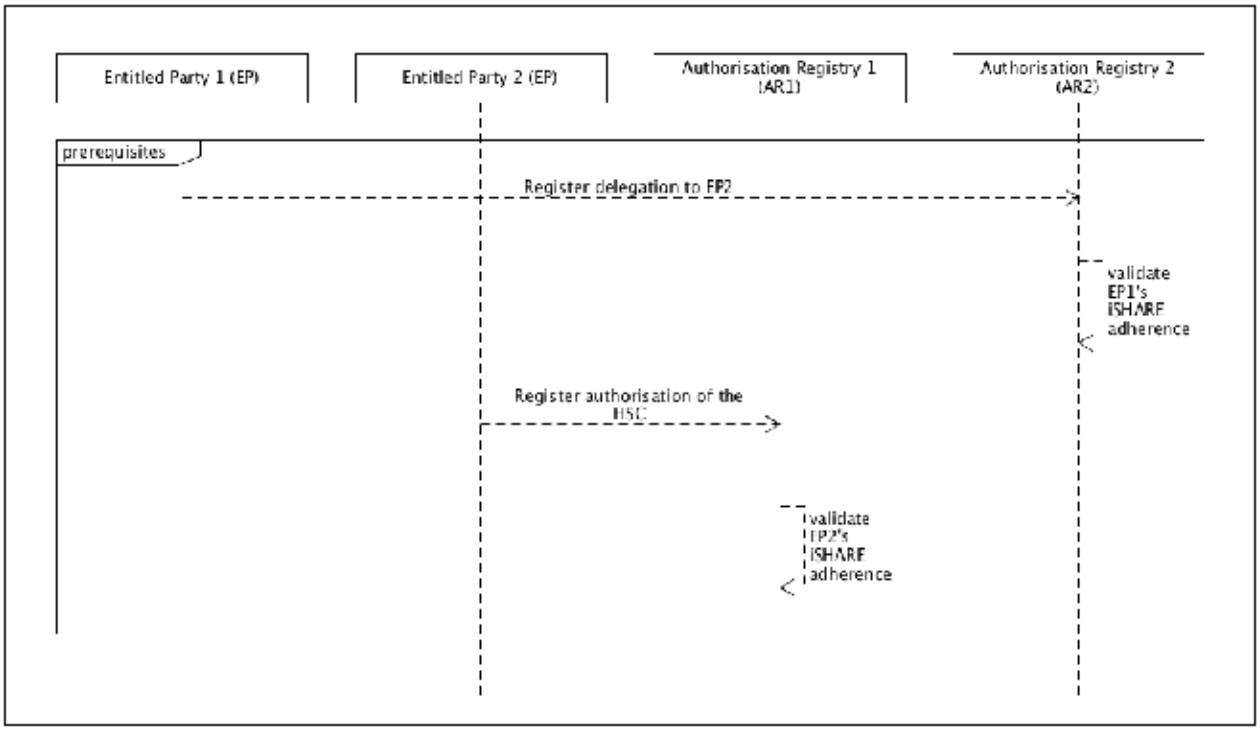
All Functional working group-members are invited to add practical examples of this use case in the comment section.

Sequence diagrams

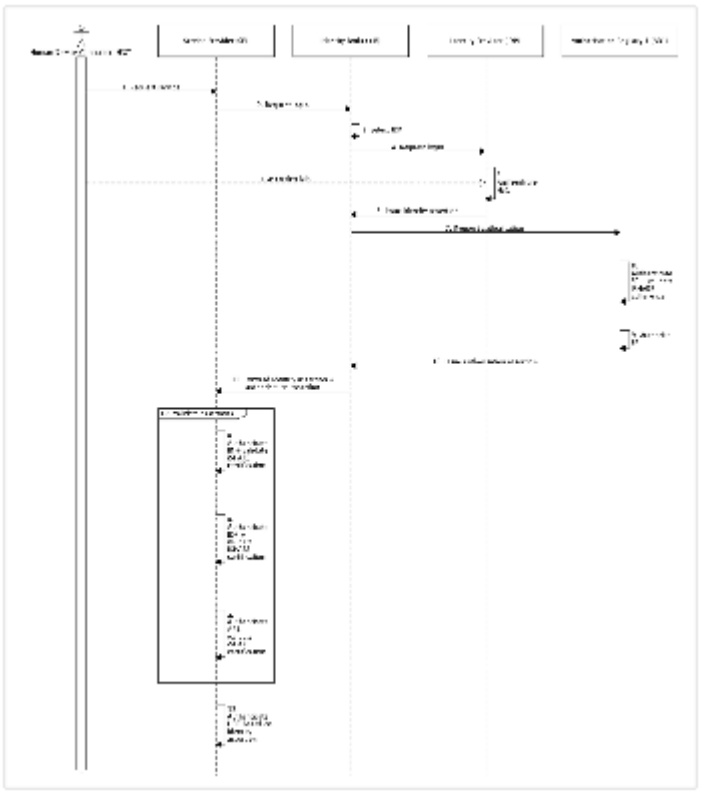
Total



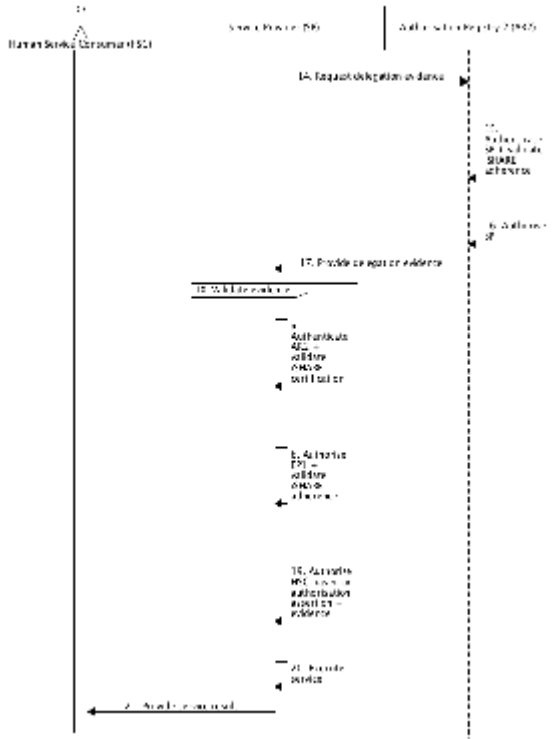
Prerequisites



Authentication and Authorisation



Delegation



Note that for every use case, the interface specifications between interacting roles and the technical standards & specifications according to which the use case is functioning, will be detailled in the Functional and Technical iSHARE working groups.

Secondary use cases

In this section we elaborate on the secondary use cases.

The secondary use cases have an administrative background, and support and form the basis for the primary use cases. The following secondary use cases have been defined:

- 1. Digital Certificates
  - 1a. Issuance of a digital certificate
  - 1b. Revocation of a digital certificate
- 2. (Issuance of) Credentials
- 3. iSHARE adherence/registration
  - 3a. Adherence of iSHARE party
  - 3b. Registration of an Entitled Party
- 4. Authorisations
  - 4a. M2M registration of authorisations
  - 4b. H2M registration of authorisations
- 5. Delegations
  - 5a. Management of delegations
  - 5b. Revocation of delegations
- 6. Auditing
  - 6a. Registration of an auditor
  - 6b. Audit and reporting
    - Audit and reporting of anonymised data
- 7. Service and support

Note that the above use cases are detailed on their own Confluence page - as follows:

- Roles
- Depiction
- Description
- Sequence diagram

1. Digital Certificates

1a. Issuance of a digital certificate

In secondary use case 1a, a digital certificate is issued to an applicant by the Certificate Authority.

Description

The use case consists of the following steps:

1. The applicant applies for a digital certificate at the Registration Authority
2. The Registration Authority verifies the identity of the applicant (eIDAS level of assurance 3) and notifies the Certificate Authority
3. The Certificate Authority issues a digital certificate to the applicant

Sequence diagram

To follow.

1b. Revocation of a digital certificate

In secondary use case 1b, a digital certificate is revoked by the Certificate Authority.

Description

The use case consists of the following steps:

1. A party submits a revocation request to the Registration Authority
2. The Registration Authority verifies the request and notifies the Certificate Authority
3. The Certificate Authority revokes the digital certificate

Sequence diagram

To follow.

2. (Issuance of) Credentials

In secondary use case 2, credentials are issued to a Human Service Consumer by an Identity Provider.

Description

The use case consists of the following steps:

1. The Human Service Consumer applies for credentials at the Identity Provider
2. The Identity Provider verifies the legitimacy of the application
3. The Identity Provider verifies the identity of the applicant (eIDAS level of assurance 3)
4. The Identity Provider issues the credentials to the Human Service Consumer

Sequence diagram

To follow.

3. iSHARE adherence/registration

3a. Adherence of iSHARE party

In secondary use case 3a, a party is registered as an iSHARE adhering party.

Description

The use case consists of the following steps:

1. An iSHARE party applies for or is designated to participate in the iSHARE scheme
2. The iSHARE party is verified whether it complies to the iSHARE terms of use
3. The iSHARE party is registered as an iSHARE adhering party

Sequence diagram

To follow.

3b. Registration of an Entitled Party

In secondary use case 3b, a party is registered as an Entitled Party within the iSHARE scheme.

Description

The use case consists of the following steps:

1. An organisational entity applies for or is designated to join the iSHARE scheme
2. The legal status of the organisational entity is verified (by checking the relevant information at the Chamber of Commerce or similar)
3. The identity of the legal person of the organisational entity is verified (eIDAS level of assurance 3)
4. The organisational entity is registered as Entitled Party within the iSHARE scheme

Sequence diagram

To follow.

4. Authorisations

4a. M2M registration of authorisations

In secondary use case 4a, authorisations are registered by an Entitled Party through a M2M connection.

Description

The use case consists of the following steps:

1. The Entitled Party (which acts equivalent to how a Service Consumer acts in use case 1) requests a service from the Authorisation Registry (which acts equivalent to how a Service Provider acts in use case 1)
2. The Authorisation Registry authenticates the Entitled Party and validates it as an iSHARE adhering party
3. The Authorisation Registry authorises the Entitled Party
4. The Authorisation Registry executes the requested service (creating, updating, or deleting authorisations)

Note that this secondary use case is based on primary use case 1

Sequence diagram

To follow.

4b. H2M registration of authorisations

In secondary use case 4a, authorisations are registered by an Entitled Party through a H2M connection.

Description

The use case consists of the following steps:

1. The Entitled Party (which acts equivalent to how a Human Service Consumer acts in use case 4) requests a service from the Authorisation Registry (which acts equivalent to how a Service Provider acts in use case 4)
2. The Authorisation Registry requests a login from the Identity Provider
3. The Identity Provider authenticates the Entitled Party
4. The Identity Provider issues an identity assertion to the Authorisation Registry
5. The Authorisation Registry validates the identity assertion through the following steps:
    a. The Authorisation Registry authenticates the Identity Provider and validates it as an iSHARE certified party
6. The Authorisation Registry authenticates the Entitled Party based on the validity of the identity assertion
7. The Authorisation Registry authorises the Entitled Party
8. The Authorisation Registry executes the requested service (creating, updating, or deleting authorisations)

Note that this secondary use case is based on primary use case 4

Sequence diagram

To follow.

5. Delegations

5a. Management of delegations

In secondary use case 5a, delegation evidence is issued to an applicant by an Entitled Party.

Description

The use case consists of the following steps:

1. The applicant applies for authorisations at the Entitled Party
2. The Entitled Party verifies the legitimacy of the application
3. The Entitled Party verifies the identity of the applicant (eIDAS level of assurance 3)
4. The Entitled Party defines the authorisations of the applicant
5. The Entitled Party registers the authorisations of the applicant
6. The Entitled Party issues delegation evidence to the applicant

Sequence diagram

To follow.

5b. Revocation of delegations

In secondary use case 5b, a delegation is revoked by the Entitled Party.

Description

The use case consists of the following steps:

1. The applicant (either the delegated party or some other party) notifies the Entitled Party to revoke the authorisations
2. The Entitled Party verifies the legitimacy of the application
3. The Entitled Party verifies the identity of the applicant (eIDAS level of assurance 3)
4. The Entitled Party revokes the authorisations of the delegated party and all other delegated parties down the same delegation chain

Sequence diagram

To follow.

6. Auditing

6a. Registration of an auditor

In secondary use case 6a, a party is registered as auditor by an appropriate entity.

Description

The use case consists of the following steps:

1. Some party (either external or internal) applies for evidence to audit
2. The appropriate entity (to be defined in the legal workgroup) verifies the legitimacy of the application
3. The appropriate entity verifies the identity of the applicant (eIDAS level of assurance 3)
4. The appropriate entity registers the party as auditor

Sequence diagram

To follow.

6b. Audit and reporting

In secondary use case 6b, requested evidence is provided to the auditor by the Service Provider and/or the Entitled Party.

Description

The use case consists of the following steps*:

1. An auditor requests for relevant evidence
2. The Service Provider and/or the Entitled Party verifies the identity of the auditor
3. The Service Provider and/or the Entitled Party verifies the legitimacy of the request
4. The Service Provider and/or the Entitled Party provides the auditor with (access to) the requested evidence

*Note that audit and reporting is considered the responsibility of the iSHARE adhering or -certified party. All iSHARE parties are expected to have their own policies and procedures in place to be compliant to iSHARE standards and relevant regulations. Who will verify compliance (the iSHARE governing body, a party in the scheme, or a third party) with these standards and regulations is to be decided.

Sequence diagram

To follow.

Audit and reporting of anonymised data

In this secondary use case, read access to anonymised data is provided to the auditor by the Service Provider and/or the Entitled Party.

Description

The use case consists of the following steps*:

1. An auditor requests for certain anonymised data
2. The Service Provider and/or the Entitled Party verifies the identity of the auditor
3. The Service Provider and/or the Entitled Party verifies the legitimacy of the request
4. The Service Provider and/or the Entitled Party provides the auditor with (read access to) the requested anonymised data

*Note that this use case is a variant of the previous use case (Audit and reporting), in order to facilitate parties such as Customs who may need 'read minus' access to certain data as required by.regulations.

Sequence diagram

To follow.

7. Service and support

In secondary use case 7, a reported incident is solved by a support team.

Description

The use case consists of the following steps:

1. A participating entity within the iSHARE scheme reports an incident or problem
2. The incident or problem is registered at the service desk
3. The service desk generates and provisions a ticket with information about the incident or problem to the appropriate incident response team or support team
4. The incident response team or support team solves the incident or problem
5. The service desk closes the ticket and informs the participating entity

Sequence diagram

To follow.

Detailing key features

This section dives deeper into the key features of the iSHARE scheme. What we detail per key feature is the following:

- Key feature: Provide trust framework for PKI certificates
  - PKI trusted list (to be changed)
  - iSHARE's own PKI (to be changed)
- Key feature: Provide flexibility in authorisation
  - Granular authorisation
  - Multiple authorisation registration points
- Key feature: Allow for management of consent
- Key feature: Support multiple interaction models

A section on Federated identity is also added here - as it is related to the above key features.

PKI trusted list

One of iSHARE's key features is to provide a trust framework for PKI certificates including a list of certificate roots (also called PKI roots), or Certificate Authority in other words, that meet the iSHARE requirements and can be trusted by all iSHARE participates. We call it the PKI trusted list that will be developed and provided by the iSHARE scheme.

The European Union (EU) implemented the eIDAS regulation providing a list of criteria for Certificate Authorities which can be re-used within iSHARE.

However, the eIDAS regulation does only hold for EU member states and not for countries outside of the EU. As iSHARE might not be restricted to only European countries in the future, Certificate Authorities outside of the EU do not have to comply with the eiDAS regulation. In that case, we cannot fully rely on the criteria provided by eIDAS and would want to deviate from that in order to be able to work with Certificate Authorities from outside the EU.

Also, it might turn out in the course of the workshops in phase 2 that not all criteria listed in the eIDAS regulation are necessary and applicable to the iSHARE requirements. A reduced version of the eIDAS regulation could be sufficient for the iSHARE objectives. Equally, the iSHARE scheme could encounter that stronger criteria are needed which are not listed in eIDAS.

During the co-creation process we could also come across the need for specific certificates, i.e. to prove the authenticity of Authorisation Registries, that are currently not provided by Certificate Authorities. In that case, the need for iSHARE's own PKI could arise.

Here a list of questions we need to ask ourselves in this regard during the co-creation process in phase II:

- Based on which criteria do we evaluate Certificate Authorities and put them on our PKI trusted list?
    - 'Level of Assurance' (LoA)?
    - Interoperability?
    - Issuing process of certificates?
    - Supervision and control of Certificate Authorities?
- To which extend are we going to re-use the criteria listed in the eIDAS regulation?Will the criteria be a 'light' or 'heavy' version of the eiDAS regulation?
- Are we going to include criteria that are not listed in eIDAS yet?
- Is there a need to create specific certificates and establish our own Certificate Authority?

iSHARE’s own PKI

It is assumed that existing PKIs are sufficient to meet all iSHARE requirements. If, during the course of phase 2, this assumption turns out to be false, an additional iSHARE specific PKI can be created.

We foresee the following scenario's for the role of iSHARE (non-exhaustive):

- iSHARE could be part of an existing PKI scheme and make use of certificates issued by existing certificate authorities
- iSHARE could be part of an existing PKI scheme and take the role of a certificate authority issuing its own certificates
- iSHARE could implement its own PKI scheme and make use of certificates issued by existing certificate authorities
- iSHARE could implement its own PKI scheme and take the role of a certificate authority issuing its own certificates

Granular authorisation

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

By granular authorisation we mean the level of details an authorising process requires to limit and separate privileges (= 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

It 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).

Example for 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.

Multiple authorisation registration points

One of the iSHARE key features is the flexibility in authorisation with regards to the authorisation scope, granularity and source. In this section we will expand on the authorisation sources and the possibility of having multiple registration points. Service Providers have different options when it comes to the management of their authorisation information.

Authorisation registration point resides at Service Provider

The authorisation information can reside very close to the data, namely at the Service Provider. They register, validate and execute their own authorisation policies.

Authorisation registration point resides at separate source

The authorisation information can be handled by an external third party separated from the Service Provider.

Authorisation registration point resides at Service Consumer that delegates rights

Service Providers can give permission to Service Consumers to delegate their right to access a specific resource to another Service Consumer. In that case authorisation information of the Service Provider can partly reside at a Service Consumer that delegates its own right to another Service Consumer.

Federated identity

A federated identity is a 'summarised' identity that is spread out and recognised across multiple systems. A person's electronic identity and attributes are linked and stored across multiple, distinct identity management systems.

The use of federated identities could reduce costs by eliminating the need for proprietary identity solutions. By proprietary solutions we mean products and services provided by one vendor. The lack of competition of other vendors can make the acquisition and maintenance of the solution costly. Secondly, it may not be fully interoperable with other solutions in the field. Cloud service providers for instance are known for having proprietary identity management systems.

Single Sign On (SSO) is a federated identity solution.

Open standards & specs for federated identities

For the implementation of federated identity solutions and the realisation of interoperability between parties, the use of open industry standards and openly published specifications is a must.

Examples for technical specifications & standards of federated identity solutions are SAML, OAuth, OpenID, Security Tokens (Simple Web Tokens, JSON Web Tokens, and SAML assertions), Web Service Specifications, Microsoft Azure Cloud Services, and Windows Identity Foundation. If you want to read more about them, we refer to the section Technical.

Examples for digital federated identity platforms that allow their users to log onto other third party mobile & web applications are Google Account, Twitter, LinkedIn, PayPal, Foursquare, MySpace, AOL, Amazon.

Single Sign On (SSO)

Single Sign On (SSO) is a federated identity solution.

It is however 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 all previously signed-in environments.

Functional requirements per role

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

This section will describe the functional requirements (e.g. accountability) per role in the iSHARE scheme - it will be detailed by the Functional working group.

User interface requirements

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

Accessibility

The iSHARE scheme is fundamentally designed to work for all people, organisations and companies who are related to the logistics sector and would like to exchange data.

Language

To encourage the international possibilities of the iSHARE scheme, interfaces will *at least* be in English and *optionally* in several (other) languages

Note that this section will be further detailed by the Functional working group.

Identifiers

A unique identifier (UID) including the related processes is required, in order to be able to uniquely identify all users in the entire iSHARE scheme.

Identity attributes

Before users are issued digital certificates and other credentials (i.e. authentication and authorisation means) to request (as Service Consumer) or provide services (as Service Provider), they first need to pass through an on-boarding or registration process. Hereunder a list of personal identifiers that uniquely identify persons:

- Unique identifier (i.e. unique serial, random numbers linked to a person's identity)
- Biometrics (i.e. fingerprints, iris scan, voice recognition etc.)
- Name
- Organisation
- Job title
- Role within organisation

Note that personal data such as passport numbers or social security numbers are not allowed to be registered according to the privacy regulations set by the European Union and the Dutch government.

At it stands now, it is proposed that iSHARE is going to reuse existing identity solutions in the Dutch market such as eHerkenning and iDIN, and once expanding to other countries, international identity solutions. In this light, iSHARE is going to accept existing on-boarding solutions and processes that are already put in place and to which iSHARE users adhere. However, the possibility of developing a new iSHARE identity solution (opposed to re-using existing identity solution such as i.e. eHerkenning) is not excluded and has to be decided in the iSHARE set of agreements.

The on-boarding process and identity attributes should be thoroughly discussed in the course of the iSHARE functional workshop, because based on the outcome of the on-boarding process, it is decided if a user is allowed to make use of iSHARE and is issued the required credentials for further use,.

Authorisation attributes

Attributes can serve as additional information in the authorisation validation process as they play a role in the validation of authorisation policies (examples are authorisation policies are i.e. "All DC's holding the role of manager get access to document X" or "All DC's at a distance from X meters from location Y get access to document Z").

Before Service Providers can give access to their data, they might want to receive additional information from Service Consumers proving that they meet the authorisation policies. To trust the authenticity of the additionally provided information from the Service Consumer, there might be the need for a proving mechanism.

The following questions have to be addressed in the course of the functional work groups:

1. Which attributes do we foresee to play a role in the authorisation policies defined by Service Providers?
2. How can Service Consumers prove the authenticity of their delivered attributes?
3. How to proof the authenticity of
    - location?
    - role?
    - containers?

Technical

This section covers the relevant Technical topics of the iSHARE scheme:

- Interface specifications: the eHerkenning interface specifications that (can) serve as input for the interface specifications for iSHARE
- Security: five important key aspects of information security are listed. They (can) form the basis and have tobe covered by the technical requirements of iSHARE
- Relevant standards: a number of existing technical standards are listed that are successfully implemented in well-established digital services related to authentication, access management and the secure exchange of information

These topics (and possibly others that arise during Phase 2) are detailed by the Technical working group.

Interface specifications

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

- iSHARE APIs
- API example use case 1c

> For an impression of how interfaces are described in eHerkenning, the following link leads to the interface specifications for all participating roles in eHerkenning: https://afsprakenstelsel.etoegang.nl/display/as/Interface+specifications

iSHARE APIs

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

A complete overview of the current draft of the iSHARE API specifications (work in progress) can be found here on SwaggerHub.

Use of Oauth 2.0 in iSHARE in general

OAuth 2.0 is used in iSHARE M2M use cases directly and as part of OpenID Connect 1.0 in iSHARE H2M use case.

For both 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 [1]
- Clients MUST authenticate through the `private_key_jwt` method as specified in OpenID Connect 1.0 Chapter 9 .[1] [2]
- The `private_key_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 `private_key_jwt` MUST be signed using a certificate containing the client's valid iSHARE identifier
- The `private_key_jwt` MUST be set to expire in 30 seconds
- A server SHALL NOT accept a `private_key_jwt` more than once. However within it's time to live a Service Provider MAY forward a `private_key_jwt` from a Service Consumer to another server (Entitled Party or Authorisation Registry) to obtain additional evidence on behalf of the Service Consumer
- A server SHALL only accept a forwarded `private_key_jwt` if the `aud` claim of the forwarded `private_key_jwt` matches the `iss` claim of the `private_key_jwt` from the client
- For interoperability reasons clients MUST only make `HTTP POST` calls to all OAuth `/token` and iSHARE `/delegation` endpoints. (Services are free to implement other HTTP verbs)
- Servers SHALL only issue access tokens with "bearer" token type
- Servers SHALL NOT issue refresh tokens
- Access tokens SHOULD expire within 3600 seconds by default. Depending on scope, servers MAY choose to limit the expiration period

Additional rationale

[1] In OAuth 2.0 clients are generally pre-registered. Since in iSHARE we want to interact with clients that have been previously unknown this doesn't suit us. We go for a generic client identification and authentication scheme, based on iSHARE whitelisted PKI roots.

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

Use of Oauth 2.0 in iSHARE M2M

For use of OAuth 2.0 in iSHARE M2M use cases the following additional requirements apply:

- Only the Client Credentials Grant SHALL be used

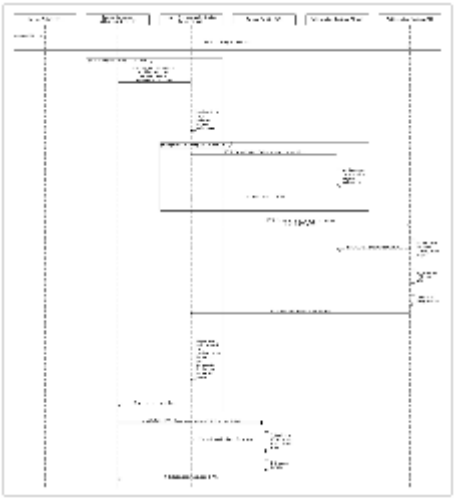
Use of OpenID Connect 1.0 in iSHARE H2M

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

- Only the Authorization Code Grant SHALL be used
- Since clients aren't pre-registered, the `redirect_uri` parameter MUST be present in the authorization request.
- OpenID Connect clients MUST use the `state` parameter
- iSHARE only allows the following scope values:
  - openid - REQUIRED scope value
  - name - OPTIONAL scope value requests access to: name, family_name, given_name, middle_name and gender
  - contact_details - OPTIONAL scope value requests access to: email, email_verified, phone_number and phone_number_verified
  - company_id - OPTIONAL scope value requests access to: company_id
  - company_info - OPTIONAL scope value requests access to: `company_name`, `company_type`, `company_address` and `company_url`
- 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.

API example use case 1c

Step by step detailed technical overview of use case 1c



Pre-requisite for calling service APIs at Service Provider

Access Token request from Service Consumer

```
POST /oauth/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-assertio
n-type%3Ajwt-bearer
&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxM
jNkZGRkYXNkYXNkYXNkYXNkZGQ0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRta
W4iOnRydWV9.w-OFT6yHL2cnXHiCWvKKNlhd1nTFt8jHSFLL_FitO3ir88bMY_WyzYu-
cwnaIr20gLWZIQ3W7dq4--JqMWnlVb3xuNr6YHm4ivGftvdVbpS2sPqoLxNHCsYgb2L2
X0NJKurhpgZ_0OB5FwPHJ1nqvX_fwymwNejPZPgqFLvUN-U
&authorisation_registry=NL123456789
```

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

Access Token request from Service Provider

```
POST /oauth/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-assertio
n-type%3Ajwt-bearer
&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhc2RzYXN1Y
iI6IjEyM2RkZGRhc2Rhc2Rhc2Rhc2RkZDQ1Njc4OTAiLCJuYW1lIjoiSm9obiBEb2UiL
CJhZG1pbiI6dHJ1ZX0.ay5Ghz_X6It4h8KnNUiarO3hTPWJ_ahqfaTzZ_NwNGJecC0GX
LJefmONyCOUq9jlYzel8_mmrfbtDZDZixoV8QEInoC7Eihsq07o9xih0vhCRTbNx_G98
UV8X2STGiN0Ppz3TDWKEH-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

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

service_consumer_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJz
dWIiOiIxMjNkZGRkYXNkYXNkYXNkYXNkZGQ0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9l
IiwiYWRtaW4iOnRydWV9.w-OFT6yHL2cnXHiCWvKKNlhd1nTFt8jHSFLL_FitO3ir88b
MY_WyzYu-cwnaIr20gLWZIQ3W7dq4--JqMWnlVb3xuNr6YHm4ivGftvdVbpS2sPqoLxN
HCsYgb2L2X0NJKurhpgZ_0OB5FwPHJ1nqvX_fwymwNejPZPgqFLvUN-U
```

Delegation Evidence response from Authorisation Registry

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

{
  "delegation_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibm
FtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.EkN-DOsnsuRjRO6BxXemmJDm3Hbxr
bRzXglbN2S4sOkopdU4IsDxTI8jO19W_A4K8ZPJijNLis4EZsHeY559a4DFOd50_OqgH
GuERTqYZyuhtF39yxJPAjUESwxk2J5k_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
```

Service response from Service Provider

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

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

iSHARE '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.

Cases that must at least be supported:

Delegation and authorisation cases in natural language	JSON
I, Maersk, grant Jan de Rijk access to the ETA of Container #12345	tbd
I, Maersk, grant Jan de Rijk access to the ETA of all my Containers	
I, Maersk, grant Jan de Rijk access to all information of Container #12345	
I, Maersk, grant Jan de Rijk access to all my information	
I, Shipper A, grant RWS access to my 'hazardous goods information' if my ship is within 5 miles of critical infrastructure	
I, RWS, grant access to the police to all objects that have a 'calamity' flag raised	

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 Servi ce 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

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"
  },
  "Delegate": {
    "type": "NL.KVK",
    "value": "12345678"
  },
  "DelegatedAction":
[
    {
      "DelegatedResource":
[
        {
          "name": "OBJECTS.CONTAINER",
          "value": "12345"
        },
        {
          "name": "OBJECTS.CONTAINER",
          "value": "67890"
        }
      ],
      "attributes":
{
        "NAME",
        "SPEED",
        "DIRECTION",
        "CONTAINS_DANGEROUS_GOODS"
      },
      "Condition":
[
        {
          "name": "RANGE_IN_KM",
          "value": "5"
        }
```

```
        ],
        "DelegatedAction":
{
          "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 duration

The duration of the delegation ('time to live') depends on several aspects. These can be summarised as follows:

- Data classification: the more sensitive the data the shorter the lifetime of the delegation token
- Authorisations (CRUD): the more authorisations the shorter the lifetime of the delegation token. For example, the lifetime of the delegation token with delete rights should be very short, whereas the lifetime of the delegation token with read rights may be longer
- Scope: the greater the extent of the data the shorter the lifetime of the delegation token

Notice that the exact lifetime of the delegation token still needs to be determined. It is the responsibility of the Service Provider to determine each of the aspects described above.

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 instead 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.

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
Delegate	Someone authorized by an administrative policy to issue policies
Forward chaining	Finding a chain of administrative and access policies beginning at a trusted policy, such that each policy authorize s 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

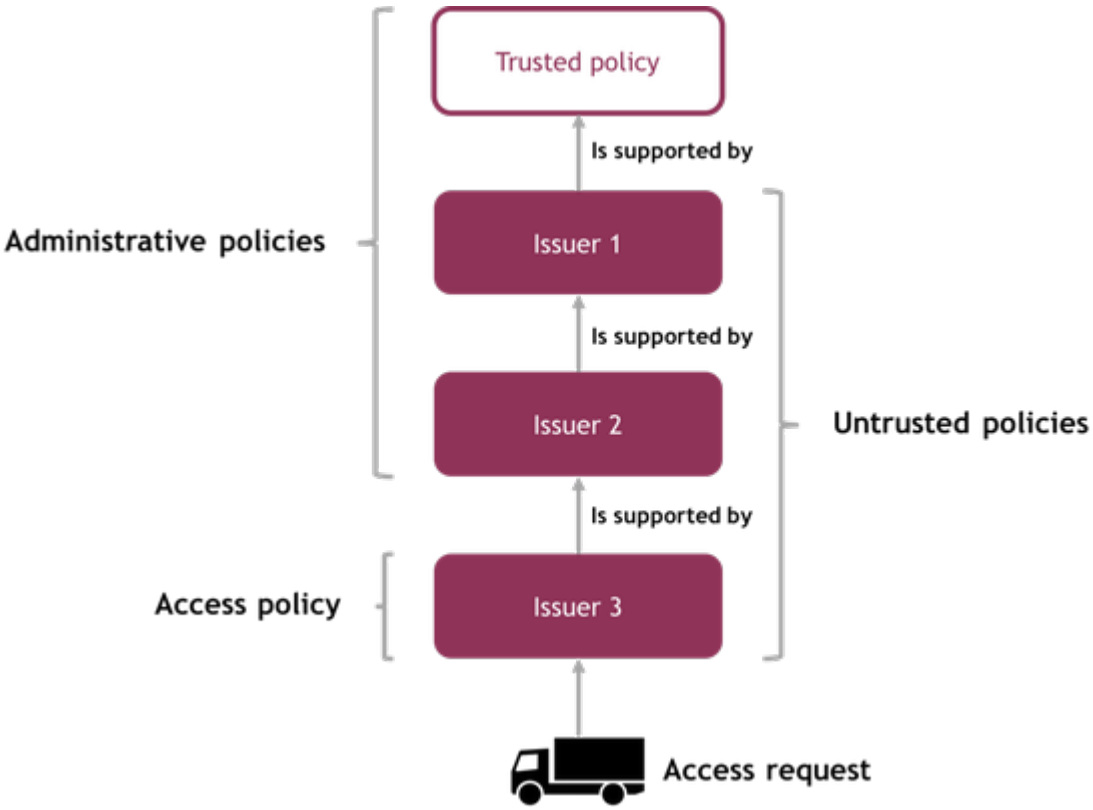
JSON attributes

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
Delegate	The subject authorised by an administrative policy to issue policies
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

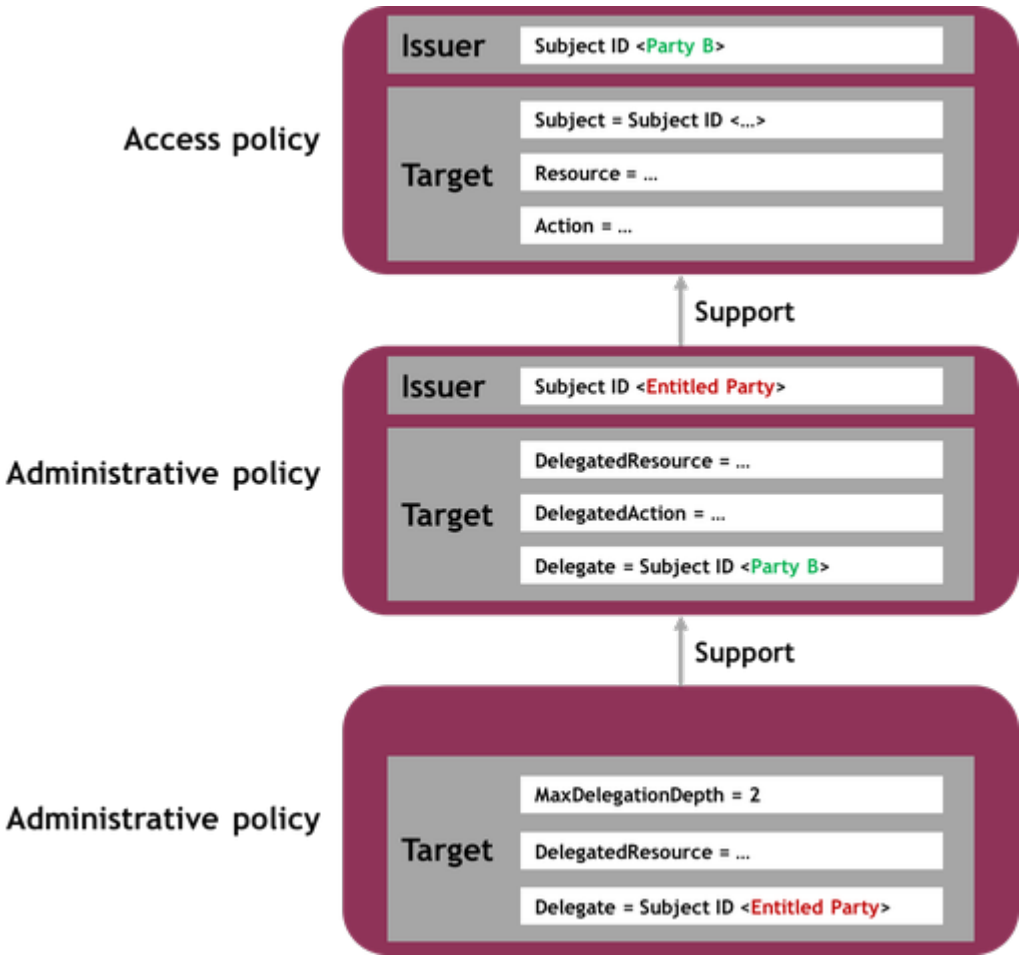
Delegation policy chain

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	Yes
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)

Security

In this section we describe the following five key concepts of information security whose purpose it to prevent the unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information:

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

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 and that the information is kept between the sender and recipient. Confidentiality can be achieved by i.e. the use of cryptography and the encryption of information, as well as through the enforcement of file permissions and access control lists to restrict access to sensitive information.

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 a chieved by i.e. hash functions (hashing the received data and comparing it with the hash of the original message).

Authenticity

Authenticity (from Greek: *authentikos*, "real, genuine") in the context of information security refers to the truthfulness of messages and if they have been sent by an authentic sender. There are ways for a recipient to prove if the received message has been sent by a "genuine, true" positively-identified sender.

Authenticity can be achieved by i.e. 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 and private key pairs are issued by Certificate Authorities. Those are entities within a Public Key Infrastructure (PKI) facilitating the trust framework.

Availability

Availability in the context of information security refers to the ability of authorised parties to access their resources whenever they need to.

Availability can be achieved by i.e. back-ups to limit the damage caused by incidents (such as broken hard drives, natural disasters etc.).

Non-repudiation

Non-repudiation means "onweerlegbaarheid" in Dutch and refers in the context of information security to the guarantee that a message is actually sent by the sender and received by the recipient. The broadcast and receipt (the authenticity) of the message cannot be denied by neither of the involved parties (sender and recipient).

Non-repudiation can be achieved by digital signatures in combination with message tracking.

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.

OAuth's phishing vulnerability

The most shocking OAuth security breach is the phishing vulnerability: every application/website using OAuth is visually (not technically) asking the end users to fill in their credentials of the master system (where the resources are stored).

Hacker's can visually emulate this process of third party clients and let end users believe that they are filling in their credentials on a genuine website. In doing so, hackers can succeed in stealing credentials. Two-factor authentication (two types of evidence/credentials) does not add extra security as phishing website can steal those extra types of credentials as well.

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 a nd 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 certificate
- Validity period
    - Not Before
    - Not After
- Subject name: Name of the person, or entity identified
- Subject Public Key Info
- Public Key Algorithm
- Subject 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).

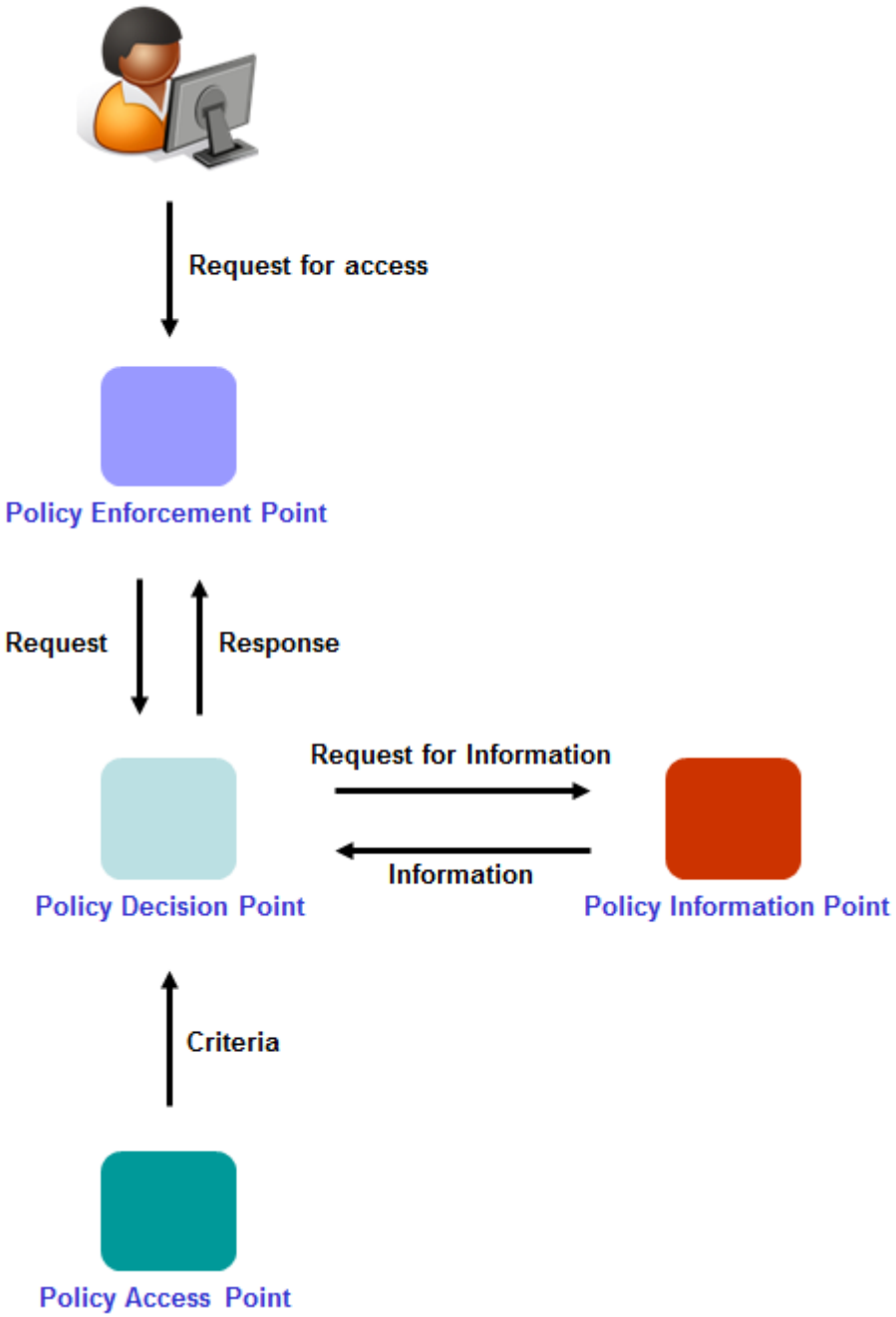
Moreover, with the help of XACML authorisations can be arranged and managed in detail. This is called fine-grained authorisation. XACML supports the use of security labels, rules with arbitrary attributes, rules with a certain duration and dynamic rules.

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.