Distributed Ledger-based Infrastructure for Industrial Digital Twins

5 use cases enabled by Blockchain, IOTA Tangle and ECLASS

12/2020

ECLASS

Authors and contributors

Alaettin Dogan, Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg

Alexander Belyaev, Otto-von-Guericke-Universität Magdeburg

Dr.-Ing. Jörg Nagel, Neoception GmbH

Gonçalo Rijo, Neoception GmbH

Artur Bondza, Pepperl+Fuchs SE

Dr.-Ing. Christian Block, ECLASS Head Office

Gerald Lobermeier, Weidmüller

Josef Schmelter, Phoenix Contact

Prof. Dr.-Ing. Alexander Fay, Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg

Prof. Dr.-Ing. Christian Diedrich, ifak e.V.

Management Summary

To master digitalization of industry the comprehensive availability of information is a key requirement. This is why concepts like the asset administration shell (AAS) and digital twins (DT) have been created. The Plattform Industrie 4.0 as well as industry associations like VDMA (Verband Deutscher Maschinen- und Anlagenbauer) and ZVEI (Zentralverband Elektrotechnik- und Elektronikindustrie) continuously work on developing new standards which tackle the challenge of getting the right information at the right time with minimal effort. ECLASS with its semantic catalog and classification system builds the basis for a semantically correct description of information. Furthermore ECLASS enables machines to automatically identify information within an asset administration shell.

The DIN SPEC 91406 [1] describes a schema on how a globally unique ID of an asset can be generated in the form of a URL. This globally unique ID is meant to be used to link the physical asset to the information about the physical asset in IT systems. One possibility to link the AAS to the asset is to provide the AAS under the corresponding URL conforming to DIN SPEC 91406. This procedure is the most obvious way to use both standards together, but it has several downsides when it comes to referencing information via the internet.

- The assetID is static and cannot be changed. When directly using it as an AASID, the AAS must not be moved to another location as the assetID printed on the asset which is already deployed to the field cannot be changed anymore.
- The URL schema binds the asset to an owner of a domain name, a transfer to another domain is not possible.
- Current approaches for identity management in the context of Industrie 4.0 (I4.0) are based on centralized approaches. These are based on a centralized registry and authentication server to ensure the identification and authentication of assets and their DTs.
- From the authors' point of view, the centralized approach is a first valid step towards short term realization of I4.0 applications but does not fully correspond with the long term visions of I4.0, which underlines the highly decentralized character of future digital ecosystems without components that can assume a centralized monopoly position and whose nonavailability can affect the secure operation of the overall system.

Within this white paper an approach is introduced to realize a decentralized registry for services offered around I4.0 components. How this decentralized registry is applied in practice is explained using five practice-relevant use cases which span the whole lifecycle of the asset. The use cases show how the decentralized registry can be implemented, how external services can be associated to an I4.0 component and how users can access the services. Furthermore, the use cases show how operators can associate a second AAS beside the manufacturer’s AAS which is then under the control of the operator. Other use cases describe the possibility to qualify asset administration shells by third parties as well as a decentralized identity and access management for services listed in the decentralized registry. ECLASS is mainly used to describe the services as well as attributes within certificates for authorization and qualification of an AAS.

The concept of the I4.0 components, which are seen as decentralized building blocks for the future I4.0 system, and the decentralized registry complement each other and form an organically integrated whole. The proposed decentralized registry in combination with a decentralized identity management of assets and its DTs set a significant milestone on the way to the future open global digital ecosystems.

Table of Contents

Table of Figures

Terms, Definitions and Abbreviations

Terms & Definitions

In this document, the terms according to Decentralized Identifiers (DIDs), Verifiable Credentials Data Model and Industrie 4.0 apply.

- Decentralized Identifiers (DIDs): available at https://w3c.github.io/did-core/
- Verifiable Credentials Data Model: available at https://www.w3.org/TR/vc-data-model/
- Industrie 4.0: available at https://www.vdi.de/ueber-uns/presse/publikationen/details/industrie-40-begriffeterms

Definition of terms are only valid in a certain context. The current glossary applies to the context of this document. Definitions already defined in the previously mentioned Industry 4.0 glossary are only repeated if they are essential for this document.

digital twin

virtual digital representation of a physical asset

Note 1 to entry: In this document the term digital twin will be used as a synonym for the term asset administration shell.

Note 2 to entry: In the context of Industrie 4.0, the term asset administration shell is preferred.

operation

executable realization of a function

Note 1 to entry: The term method is synonym to operation

Note 2 to entry: An operation has a name and a list of parameters [2]

Note 3 to entry: This definition is taken from [3]

service

Limited scope of functionality which is offered by an entity or organization via interfaces

Note 1 to entry: One or multiple operations can be assigned to one service

Abbreviations

Abbreviations	Description
AAS	Asset Administration Shell
ABAC	Attribute-based access control
API	Application Programming Interface
CPS	Cyber-physical system
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DT	Digital Twin
I4.0	Industrie 4.0
IAM	Identity and Access Management
IoT	Internet of Things
IRDI	International Registration Data Identifier
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation - Linked Data
OPC UA	Open Platform Communications United Architecture
PKI	Public Key Infrastructure
REST	Representational State Transfer
RFC	Request for Comments
SSI	Self-sovereign identity
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3C	World Wide Web Consortium

Scope of this Document

The document specifies the use cases enabled by combining ECLASS with DLT as well as the corresponding processes and their value for the users.

Structure of the Document

This document is divided into 2 main parts, the first, called Basics, introduces basic concepts that will support the use cases defined in the second part. The first part contains a definition of underlying mechanisms and data models, which need to be created prior to implementing the use cases. The second part, shows 5 possible use cases that support some common cases on how to interact with the proposed decentralized registry. For each use case we will present a diagram that visually represents the use case action flow, key aspects and value added for the user.

Introduction

The digitalization is in full progress and leads to fundamental changes in all aspects of life. Not only the traditional IT companies are affected, but also companies from all industrial sectors and branches. Traditional business models in many different domains, such as industry, energy, mobility and health, are being put to the test. The Internet of Things (IoT) is coming and new business models are emerging. The intelligent networking of machines, systems and devices via the Internet provides new opportunities and potential. They are not only controlled by humans, but they also communicate independently in terms of machine-to-machine communication (M2M) directly with each other. Tasks and processes can be carried out automatically, thus ensuring greater efficiency, transparency and quality of life, improved use of resources and reduced costs. An essential requirement to I4.0 is to provide the data in a secure, standardized and machine-interpretable form in an automated way and across company boundaries to all parties involved in the value chain. The necessary prerequisites to achieve this are the standardization of communication structures, system security and language (semantics). This is where ECLASS comes into its own as a significant standard for semantics in industrial applications.

This document will provide concepts which strengthen ECLASS in the context of I4.0. I4.0 focuses on the integration of cyber-physical systems (CPS) and the IoT in production and logistics. The aim is to create dynamic, self-organizing, flexible cross-company and value chains. The visions of I4.0 describe open digital ecosystems in which the physical assets are represented by their DT. These DTs provide information about the assets in a machine-readable and interpretable language, describe provided capabilities and skills, some of them can directly interact with each other.

As a result, the Plattform Industrie 4.0 was founded in Germany. Its intention is to successfully implement the complex project of I4.0, giving the German manufacturing industry a competitive advantage. The Plattform Industrie 4.0 has developed the concept of the I4.0 component, in which standards as well as the technologies required for implementation are brought together, thus providing a solution for the implementation of the various I4.0 application scenarios [4, 5]. The I4.0 component consists of an asset and an AAS. The AAS is the standardized virtual representation of an asset, which is an object of value for an organization. It is uniquely identifiable worldwide and capable of establishing corporations and collaborations with other I4.0 components. The fundamental idea is that each asset provides at least one AAS and offers its information (properties and capabilities) to the interacting I4.0 components in a secure, standardized and machine-readable form. According to [6], identifiers are required to uniquely distinguish all elements of an AAS and to associate elements to external definitions to endow these elements with semantics information as provided by the ECLASS catalog. ECLASS enables the semantically correct and machine readable description of services offered around an I4.0 component. For ECLASS, this opens the door to new areas of standardization like digital and conventional services offered around an I4.0 component and extends the concept of the AAS to solve challenges in its application. In order to create a common understanding between the participants of I4.0, the reference architectural model Industrie 4.0 (RAMI 4.0) [7] was

made available as an orientation guide. For a well-structured approach to I4.0, all IT-relevant components and functionalities can be classified in a three-dimensional layer and life cycle model.

The security aspect is an elementary part of this concept. Criteria such as confidentiality, data integrity and reliability are essential for a successful implementation of I4.0 applications. A promising key technology in this context is DLT, which originated in the financial sector but is highly relevant for the implementation in almost all areas of I4.0 [8, 9]. In particular for decentralized systems without central authority, DLT offers the necessary security to record all data transactions in a tamper-proof and traceable manner by means of a complete register distributed among the system participants.

In order for the AASs to be able to find and trust each other, concepts are needed for the registration of AASs in a common register, to ensure a trustworthy identity and access management. Concepts currently discussed in the I4.0 community are based on the classic centralized approach, in which the central components are the anchor of trust that takes over the registration, authentication, authorization and certification of AASs. From the authors' point of view, however, this is in certain contrast to the visions of the I4.0, which highlights the highly decentralized character of future digital ecosystems.

By combining DLT with ECLASS semantics, several disadvantages of centralized systems can be overcome. The aspects are:

- Platform provider independence: In centrally organized registries, the registry provider acts as an intermediary between the registry users. The registry provider takes over an overview function, controls the registration process and manages the search queries. This carries certain risks. For example it cannot be excluded that registry providers may lose or misuse their control over the registry infrastructure or manipulate the functionality of the registry for their own benefit, i.e. make users pay for a higher rank to be found more easily than others.
- A centralized registry can be effective if the majority of users agree on registering to a single registry. In the global context and especially in the European B2B sector this is difficult to imagine. Rather, it is to be expected that the companies will try to create and operate their own registries. Based on collected experiences [10] , it can be assumed that there will be very limited exchange of information between individual company specific registries, so that critical masses of users on these independent platforms will not be reached and positive network effects will no longer come into play.
- The establishment of several independent and specific registers will require a significant administrative and communication overhead. If multiple entities claim to build a centralized registry the users would be forced to search through all independent registries to finally discover all relevant services associated with a single asset. Accordingly, the assets will have to be registered in different registers which requires the controller to maintain multiple identities.
- A DLT-based registry establishes a provider-neutral fully decentralized platform. There is no single party which could manipulate system content to their liking.

- By applying DLT the consistency of the data within the system is assured by technical means. Long term availability: A central registry is susceptible to attacks. A distributed registry is immune to single point attacks.
- Immutability: In DLT based systems all records sent to the register are immutable. This means they cannot be changed without the change being detected and prevented by the mechanisms in the system.
- History of all transactions (traceability): All transactions will be preserved and can be retraced to understand which entity changed which detail at which time.

This white paper presents an approach toward a completely distributed solution of these essential tasks and illustrates it using five practice-oriented use cases. The approach is based on the concept of the Plattform Industrie 4.0.

Basics

The basic extensions described in this part of the document contain concepts which extend the current state of the art. These extensions are the technological foundation which underlie all concepts and use cases described in this document.

The basics are:

- Basic A - Decentralized Registry
- Basic B - Service definition of an AAS in accordance with W3C DID specification

Basic A - Decentralized Registry

This chapter introduces the basic principles of distributed identifiers (DID) and how they are applied to create a decentralized registry for services offered around an AAS. Such a decentralized registry can be realized by application of DLT.

In the connected world of I4.0, it is not only access to information which becomes more and more important, but also a secure, standardized and machine-interpretable communication between assets. The identification forms the basis for all emerging processes. This results in new identification requirements, which are described using the example of the digital nameplate [11]. As part of the digital nameplate project started by ZVEI, a digital implementation of the nameplate was designed using an AAS. Besides the obligatory marking, the digital nameplate can also provide further information in several languages such as links to manuals, certificates, technical drawings and operating data. According to DIN SPEC 91406 [1], a globally unique identifier, a URL (Uniform Resource Locator) according to RFC 3986 [12], is required which is attached to the physical object and refers to the digital representation. The DIN SPEC 91406 uses the URL schema to define a globally unique identifier. Due to the similarity most companies also use the URL to host a web based service under this URL to deliver parts of the AAS via a web based service. Using such an identifier to directly refer to a resource on the internet may be difficult to keep up to date during the entire lifecycle of the asset. For example, restructuring the website (e.g. changing the domain) means that the identifier can no longer be resolved. Therefore, it is desirable to use an identifier that allows changes of the referenced information.

I4.0 concepts aim to provide the basic building blocks for the creation of future global digital ecosystems. Today's rigid and well-defined value chains are to be replaced by flexible, highly dynamic and globally networked value networks [13]. Therefore, in order for the AASs to be able to find and trust each other, concepts are needed which correspond to the visions of I4.0 and enable the registration of AASs in a common register, to ensure trustworthy identity and access management. Concepts currently being discussed in the I4.0 community are based on the classic centralized approach, in which the central components are the anchors of trust which takes off the registration, authentication, authorization and certification of AASs.

However, the centralized systems have some characteristics that may be less appropriate in the context of the emergence of global corporate and cross-national ecosystems.

These disadvantages include certain dependencies on the platform provider, who would act as an inevitable intermediary between platform users, certain risks associated with potential abuse of the platform by third parties, or manipulation of the platform by the provider to their own advantage.

To tackle this issue, a decentralized registry for AAS based on DIDs and DLT is introduced. The decentralized registry spreads across the networks of companies and forms an operator and vendor neutral platform, a so-called common backbone where all companies can register the AAS without becoming dependent on each other.

The DIDs serve as a bridge between the identities of assets and their associated AAS. Reading a DID allows the user to access the asset's services. In addition, the information to which the identifier refers to can be kept up to date throughout the asset's whole life cycle. ECLASS serves as the semantic basis to cleanly describe the services and their attributes.

What are decentralized identifiers?

DIDs are a new type of identifier for the identification, authentication and authorization of self-sovereign identities (SSI), developed by the W3C Credential Community Group, which do not require the use of a central authority such as an identity provider or certification authority [14]. DIDs are URIs (Uniform Resource Identifier) according to RFC 3986, referencing a resource, known as DID document, in a verifiable data registry (e.g. DLT network). The DID document contains a description of cryptographic authentication and authorization mechanism as well as a list of services for each type of interaction with the identity.

A DID is a string of characters and basically consists of three parts (Figure 1): the scheme (“did”), the name of a DID method and the method-specific ID. A DID method defines for a specific verifiable data registry the methods for creating, reading, updating and revoking DIDs and the associated DID documents. In addition, methods for usage, such as the authentication and authorization process, may also be included in a DID method. Furthermore, it must be specified how a globally unique method-specific ID can be generated in the respective verifiable data registry without a central authority. Based on this, the identities can issue mutually verifiable claims (e.g. qualifications, achievements or background information) in a cryptographically secure, data protection-friendly and machine-readable manner (verifiable credentials) [15]. This creates a meshed network of trust between the identities, also known as the Web of Trust. These verifiable credentials enable attribute-based access control (ABAC) in a decentralized system.

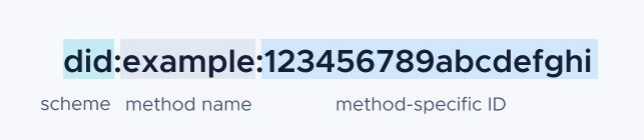

Figure 1: Structure of a DID

What is a distributed ledger?

A distributed ledger is a decentralized transaction register. In a corresponding network (DLT system), equal network participants (network nodes) manage exact copies of this transaction register. New transactions are distributed throughout the network and, by using appropriate mechanisms, a consensus on the current status of the transaction register is reached within the entire network. The distributed storage of the transaction register and the use of cryptographic procedures enable a transparent, tamper-proof and failure-resistant architecture.

In terms of implementation, a distinction is made between various DLTs. The distinction basically depends on the way a transaction is validated and stored. The most popular technology is the blockchain. An alternative technology is the Tangle [16], also called TDAG (transaction-based directed acyclic graph). A concrete implementation of the Tangle is the IOTA Tangle, which is primarily designed as a transaction and payment protocol for IoT devices.

Solution concept of a decentralized registry based on DIDs and DLT

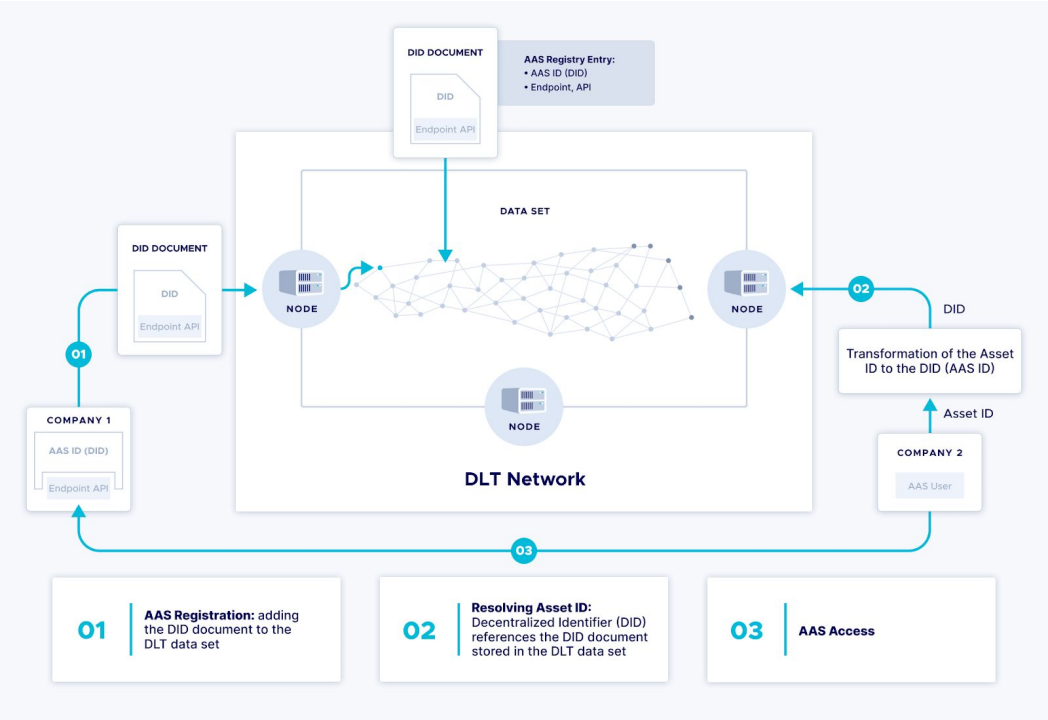

Figure 2: DLT as a decentralized registry of AAS: Architecture and interactions of participating parties.

Figure 2 represents the overall architecture of the decentralized registry based on DIDs and DLT. Companies operate the AAS of various assets in their private trusted networks. The partners in the value chain currently operating the asset want to access the AAS of these assets. The asset operators only know the DID of the AAS, which they can derive from a unique asset ID (e.g. ID according to DIN SPEC 91406 [1]). The process of transferring the asset ID into a DID is described in [17]. The exact information about the endpoint (port and communication technology they have to use) to access the AAS is not known to the asset operator.

The registration of an AAS (step 1) takes place with the submission of a DID document, which is stored as a transaction in a common data set (distributed ledger). This document is referenced by the AAS ID (step 2), which, in this system is the DID that can be derived from the unique asset ID. The asset operator connects to one of the public network nodes of the DLT system and finds the corresponding transaction in the data set. From this transaction the DID document can be extracted. The DID document contains a machine-readable description of how to access the AAS, including endpoint, port and API. The AAS is accessed from outside the DLT network (step 3).

The decentralized registry is a key concept which will be used by all use cases described in this document.

Basic B - Service definition of an AAS in accordance with W3C DID specification

In Basic A we described how the AAS or their particular contents can be accessed inside a decentralized registry using the DID service. The following part of the document introduces a concept how the services themselves can be defined within this decentralized registry, inside the DID document.

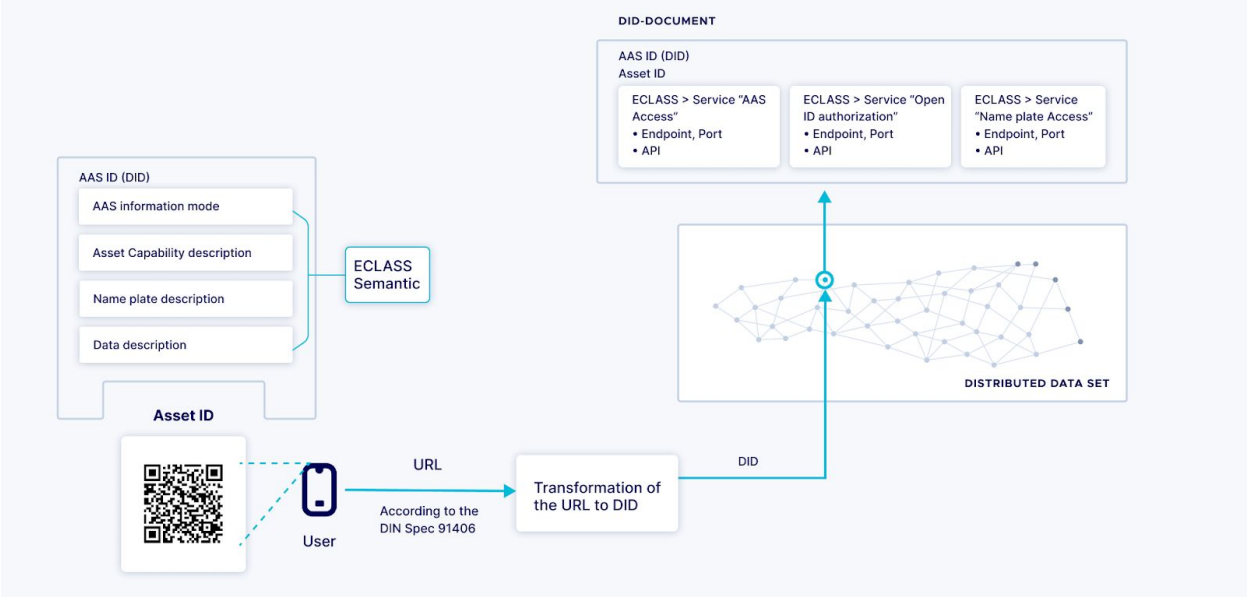

Figure 3: DID document contains a description of services for accessing the complete AAS or its selected content

All services associated with an AAS will be listed within the decentralized registry in the corresponding DID document. For the definition of services, the ECLASS catalogue is an essential part to ensure that the services are described in a semantically correct and machine-readable way. It is the recommended dictionary for standardized semantics to describe the elements of standardized meta information models. The DID document can be retrieved by a consumer via the mechanisms described in Basics A. As soon as the consumer has accessed the DID document, the user shall be able to

- List all services offered by the AAS
- Have all information at hand to access the services.

The controller of the DID is responsible to provide all required information within the DID document describing the services. The DID meta model (Figure 3) gives directions to the creator of a DID on how to structure and build the corresponding DID document to ensure compatibility and semantic correctness. Using a meta model will also enable automatic qualification of the

DID document as well as the services referenced by the DID document through a third party (see use case 5).

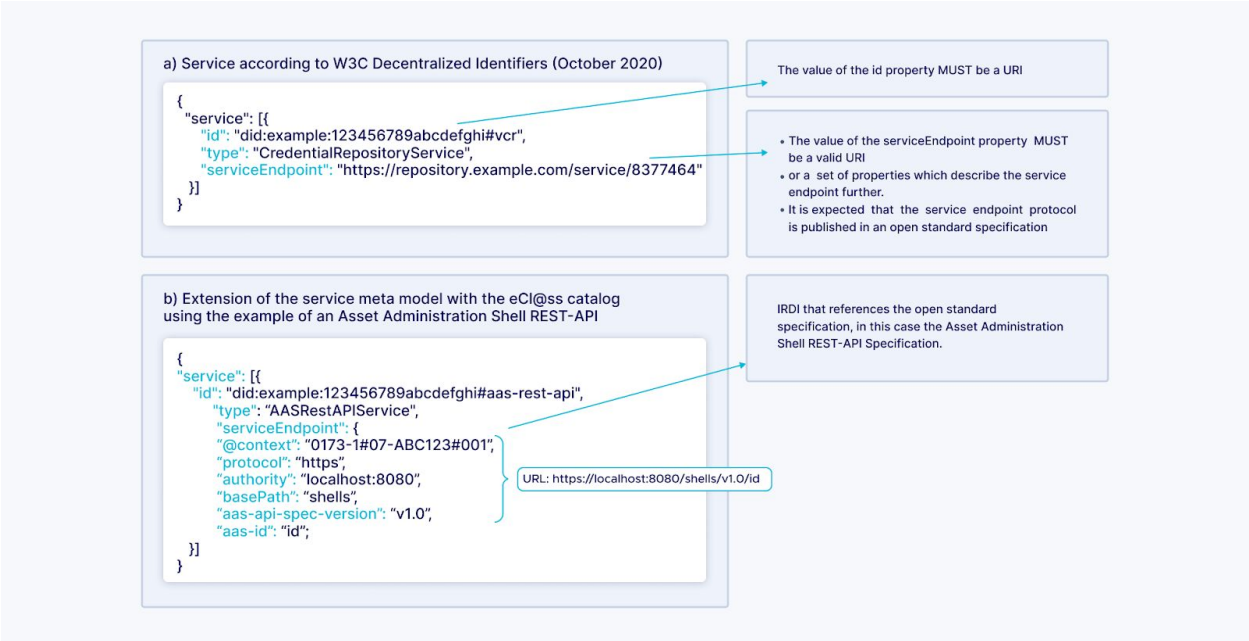

Figure 4: JSON-Serialization of a DID document

The proposed extension in this contribution is shown in Figure 4. As an AAS can be accompanied by several different services, the decentralized registry needs to hold a list of all services. Each entry describes a single service and is defined by a context. The context information ensures that two systems working with the same document use a commonly agreed terminology. The context is specified by an ECLASS IRDI referencing an open standard specification that defines the meaning of additional properties. The consumer of a service sometimes requires additional information to access the service. This additional information is described in the DID document by using properties. In the context, it is defined which properties are allowed. In case of a digital service the properties of the service contain information about the endpoint where the service can be retrieved. Some properties are mandatory, some are optional.

Examples for services are

- AAS REST-API endpoint
  - has a URL conformant to RFC 1738 [18]
  - describes multiple HTTP methods
- Website with human readable content
  - has a URL conformant to RFC 1738

    - can be accessed via a web browser and delivers a human readable website to navigate the information of the DT
- AAS OPC UA endpoint
    - has a URL conformant to RFC 1738
    - describes the OPC schema used
    - as well as the security mechanisms supported
- Authentication and authorization endpoint (e.g. according to [19] via OpenID Connect, OAuth 2.0 and X.509 certificate chain)

In the following, this definition of services around an AAS is used in combination with the decentralized registry to realize five use cases.

Use cases

In the following chapter we are about to introduce five use cases as well as their impact on the value chain. For each use case:

- The key aspects
- As well as the value added for the users

will be introduced. This gives a thorough understanding of each use case and describes how the defined base technology can help to leverage the value in each use case.

The use cases are:

- Use case 1 - Decentralized service registry
- Use case 2 - Multiple AAS referenced by one identifier
- Use case 3 - Transfer of ownership
- Use case 4 - Decentralized Identity and Access Management
- Use case 5 - Qualification of an asset administration shell

Use case 1 - Decentralized service registry

In the daily routine of service technicians, the collection of information takes a significant amount of their daily work. Instead of time-consuming and laborious manual searches for relevant information in physical and digital databases, the search is to be accelerated significantly by using innovative technologies such as the digital nameplate, e.g. to carry out maintenance on a machine. Staff members need to be able to access the most up-to-date asset information without time-consuming searches for the documents. Therefore, this use case describes how all the relevant information can be made available to staff members instantaneously, wherever it may be stored.

Diagram

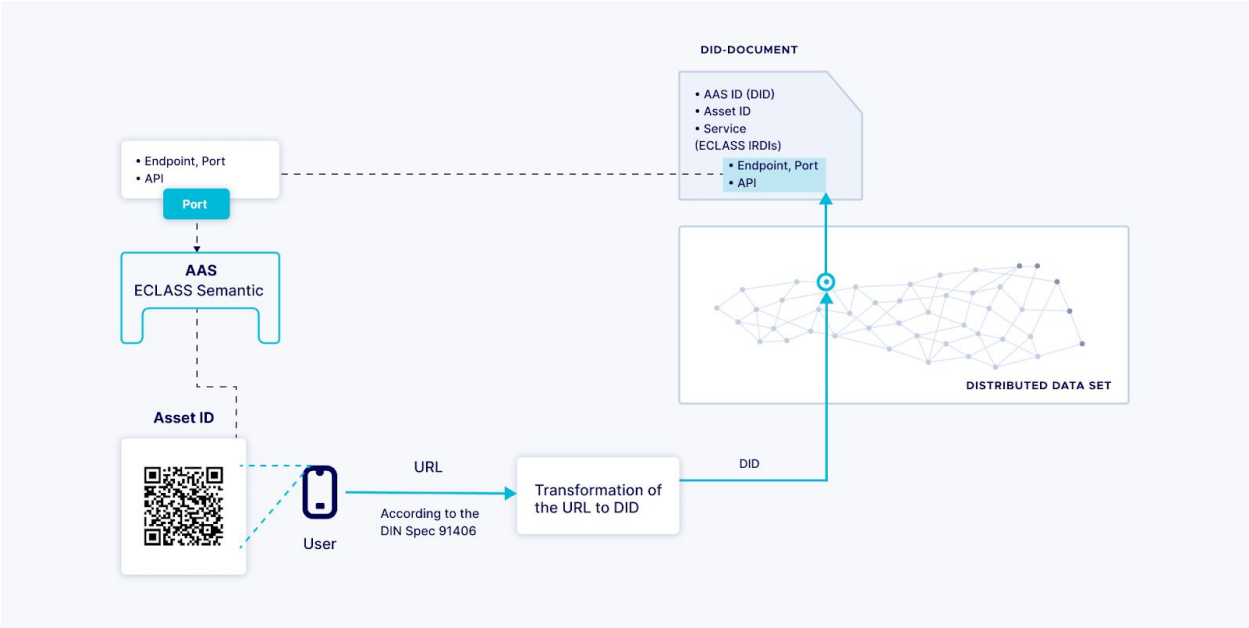

Figure 5: Decentralized service registry

Key aspects

Compulsory asset information aside, the digital nameplate can provide further information in several languages such as manuals, certificates, technical drawings and operating data. The DIN SPEC 91406 identifier is based upon a single domain provided and controlled by a manufacturer. But the need for information during a maintenance operation of a machine might require more information than a single service of a manufacturer can provide.

This use case shows how the shortcomings in the process of maintenance on a machine, based on a digital nameplate, can be remedied by using a decentralized registry.

As a first step, the device manufacturer uses a process to register an asset in the decentralized registry by deriving a DID from the identifier based upon the DIN SPEC 91406 and uploading a DID document containing a list of all services the manufacturer wants to offer around the asset.

The registration process includes the following steps:

1. Creation of an asset, its AAS and the services which shall be provided for the asset
2. Assignment of an identifier according to DIN SPEC 91406
3. Conversion of the identifier into a DID
4. Creating a DID document with the list of services provided
5. Publishing the DID document referenced by the DID

The service technician can utilize the services provided by the machine manufacturer by reading the identifier (AssetID) encoded in a 2D code labeled on the asset by using a reader (e.g. smartphone camera). The resolver (e.g. smartphone application) converts the identifier into the corresponding globally unique DID and calls the latest DID document provided by the manufacturer from the decentralized registry.

Examples for services the device manufacturer can offer are:

- The digital nameplate information
- An AAS of the asset potentially in different characteristics
- Access to real time data from the asset
- Human readable websites, like access to Product Information Management (PIM) systems
- Services executed by humans like installation services or maintenance services

Process to use the service

1. Read the identifier from the asset
2. Get a list of services from the DID document
3. Invoke the service by the consumer

Within this use case ECLASS IRDIs are used to ensure that the services are described in a semantically correct and machine-readable way (see Basic B). The services are described by use of ECLASS values (referencing an open standard specification, e.g. AAS REST API), ECLASS service descriptions (to identify the type of service, e.g. nameplate service or authorization service, using OpenID) and ECLASS properties.

Value added

- Registration is independent of a central authority that has the possibility to influence the processes.
- The data from AAS must be available where they are needed, regardless of department, location, company, country or continent. Prerequisite for this are the appropriate access rights. With internal company registries, this would hardly be conceivable and practically impossible. A common trustworthy register is needed.
- Registration needs to take place in one decentralized register only. There is no need to register the asset in several private registers to make the asset visible to as many potential users as possible. Correspondingly, administration costs can be kept to a minimum.
- Multiple services can be added to one DID document. The services do not necessarily need to be publicly available. It is also valid to list private or on-premise services in the DID document.
- Even brownfield assets can be registered and services can be offered for them.

- The validity of the referenced DID document is guaranteed since it is updateable even if the domain of a service changes.
- The DID document is always available. There is no single point of failure.
- It offers opportunities for several new digital business models like verification by a third party (see use case 5)

Use case 2 - Multiple AAS referenced by one identifier

For an operator it is important to access the data provided by the asset manufacturer. Based upon use case 1 an operator or any value chain partner can easily find all services and the associated information provided by the manufacturer in a structured and well-defined way. Hence,

- Nameplate information (e.g. serial number, date of manufacturing …)
- Manuals,
- Certification documents,
- Or lot number

are types of information which can be accessed and are controlled by the component manufacturer.

As soon as the operator installs the component in a plant or solution, new types of information, such as

- Installation location,
- Association to the plant,
- Replacement information (in case of replacement, which device has been replaced),
- Qualification documents,
- Or safety computations

are generated. Thus a new operator specific AAS is created. This new AAS also needs to be stored and listed in the registry of services, stating who was the issuer of the AAS. This is why in addition to the data provided by the manufacturer, operators also want to associate information of their own with the asset. *But how can the new AAS be associated with the asset, without adding a second operator specific identifier to the asset?* This question is solved by use case 2, which describes how an operator can attach an own AAS and correspond services under the operator's control to an asset of which the manufacturer originally holds the identifier as well as the original AAS. By applying the concepts of use case 2, the operator can, in a way, extend the information about the asset beyond the original AAS of the manufacturer.

Diagram

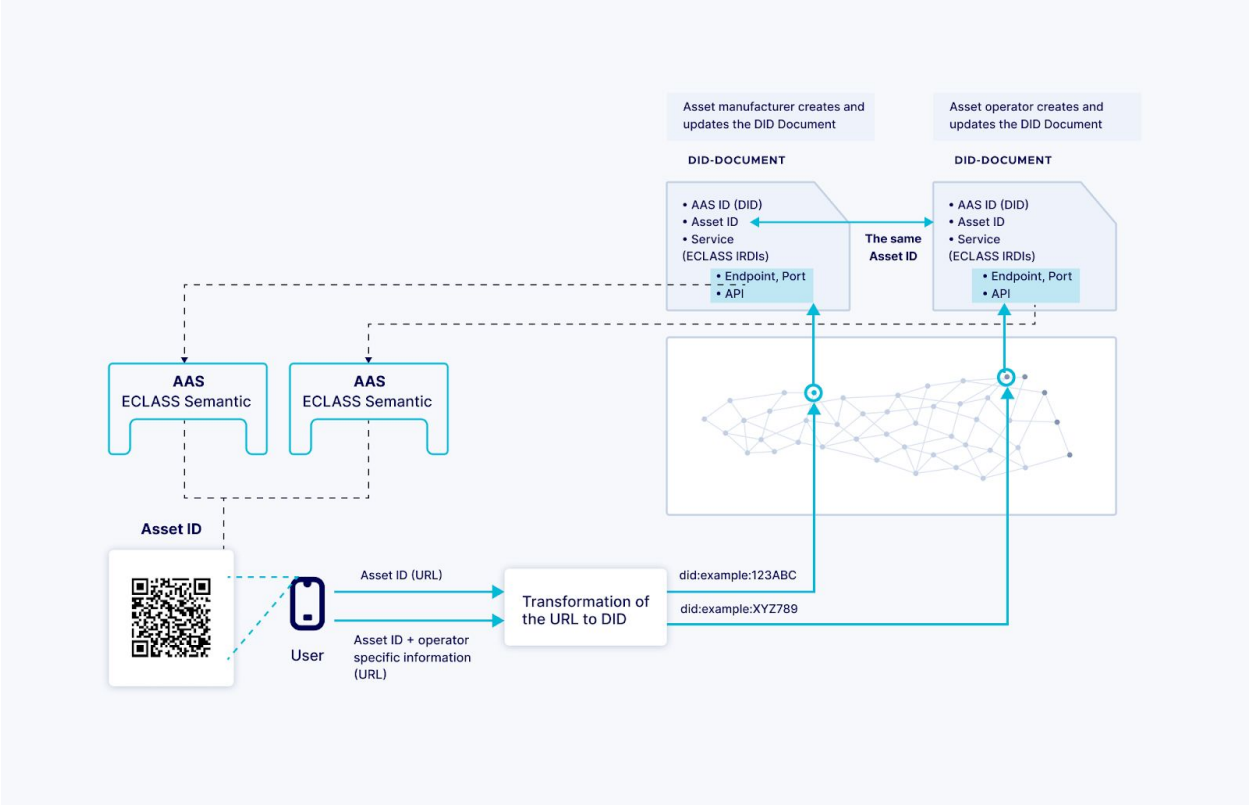

Figure 6: Multiple AAS referenced by one identifier

Key aspects

In principle, an asset can have more than one AAS along its life cycle. During the asset's life cycle there are different players around an asset, each operating one or more player-specific AAS. For instance, the asset manufacturer may operate a digital nameplate providing static asset information. In turn, live data is provided by the operator of an asset and can be accessed using the operator's AAS.

An identifier labeled on an asset is always globally and uniquely converted into a single DID and thus references exactly one DID document in the decentralized registry. This DID document can be updated only by the controller of the DID and not by any other entity. This leads to a situation where the operator will not be able to extend the DID document controlled by the manufacturer to own needs. The differentiation between the different players is realized by adding player-specific information to the identifier like shown in Figure 6. When resolving the extended DID, the registry returns a different DID for each player-specific extension. That way,

the manufacturer can be responsible for servicing a first DID document and the operator can add a second DID document to the same asset with the same identifier printed on the device. With this extension, once the scanning process is complete, the user gets references to two different DIDs, in this example. The operator-specific DID points to the DID document provided by the operator that in turn describes the operator's AAS, and the manufacturer-specific DID points to the DID document provided by the manufacturer and in turn describes the manufacturer's AAS.

The extensions used can be standardized by use of ECLASS values.

Figure 7: Direct vs. indirect linked information

Use case 2 is all about linking the asset ID with the information of different actors over the asset's life cycle. A distinction is made between two possible approaches (Figure 7):

1. Access to directly linked Information (without extension, Manufacturer in Figure 7)
   1.1. Conversion of identifier A into decentralized identifier A
   1.2. Resolving resource A in the decentralized registry
2. Access to indirectly linked information (with extension, Operator in Figure 7)
   2.1. Adding operator-specific information to the identifier A results in identifier B
   2.2. Conversion of identifier B into decentralized identifier B
   2.3. Resolving resource B in the decentralized registry

Value added

The proposed extension of the identifiers yields the following improvements regarding the value for a user:

- All data can be accessed via a single identifier

- The operator can easily extend information provided by the manufacturer
- Manufacturer and operator can update their AAS services by changing the DID document, independently from each other
- This extension mechanism is not limited to a single operator but can be used to attach an AAS for each partner in a value chain.
- An asset can be in different life cycle phases of different value chain partners and can be described with different information, i.e. it needs different AAS (with different information, access rights etc.). With the decentralized registry, the value chain partners can create their own AAS but still assign them to an asset.

Use case 3 - Transfer of ownership

The ownership of an asset can change during its life cycle. For instance, the device division of a manufacturer might be sold to another manufacturer. All information within the DID of all previously manufactured devices now needs to be updated to new service endpoints. The original manufacturer has to update or hand over the right to update the DID document to the new manufacturer without changing the identifier printed on the device already in operation. That way, the new controller of the DID will have the possibility to update all services and properties to its needs, without depending on the former controller.

Diagram

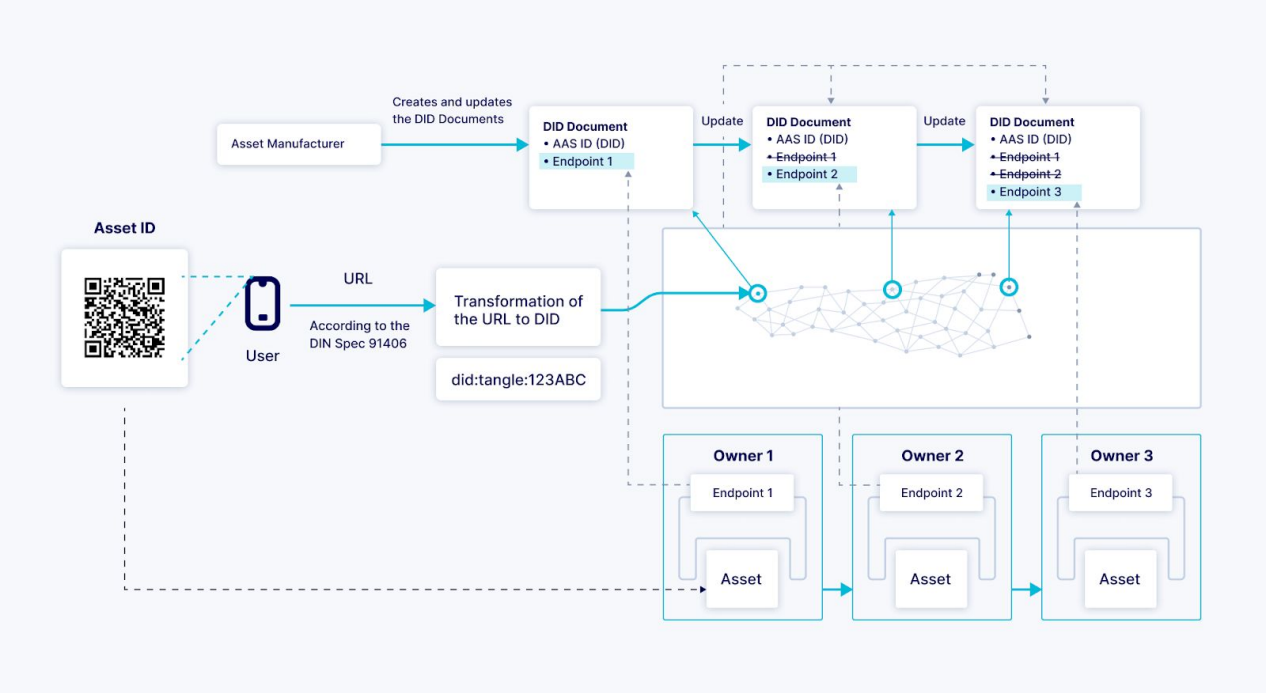

Figure 8: Transfer of ownership managed by the manufacturer

Key aspects

The identifier labeled on an asset can always be globally and uniquely converted into a single DID and thus references exactly one DID document in the decentralized registry. This DID document is controlled by an entity in the value chain, the one who first carries out the registration will be the controller of the DID. Usually this will be the asset manufacturer. If in any case the control of the DID needs to be transferred to a new owner, a transfer of ownership can be initiated/executed. There are two options to achieve this:

1. Managed by the manufacturer (Figure 8)
    1.1. Manufacturer registers asset in the decentralized registry
    1.2. Manufacturer updates registry entry containing information about the current owner whenever ownership of an asset is transferred
    1.3. This requires the manufacturer to be available and willing to update the DID document even after a long time.
2. Managed by the owner (Figure 9)
    2.1. Manufacturer registers asset in the decentralized registry
    2.2. Manufacturer updates registry entry containing information about the current owner when ownership of an asset is transferred and also transfers the control of the update process
    2.3. Procedure b will be executed with every following transfer

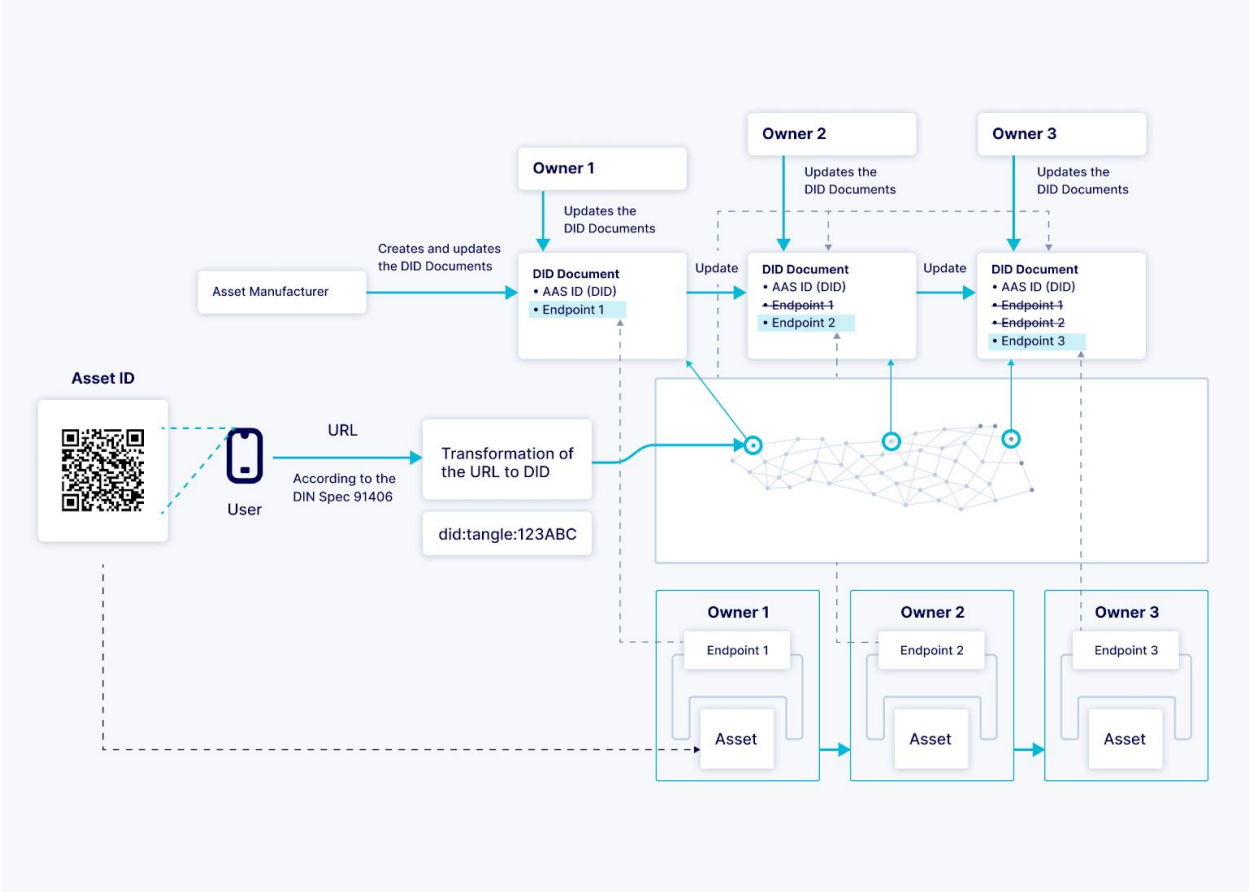

Figure 9: After the first registration, the manufacturer transfers the right to maintain data of the DID to the respective owner and the ownership respectively. Further management of the DID document and AAS's ownership is handled by the new asset owners

Value added

- Complete and chronologically traceable history of all asset owners
- Current owner always is able to update the service entries within the DID document
- No dependence on the central registry, or on the provider of the central registry service. The distributed registry belongs to everyone and nobody at the same time
- No central point of failure. In case of misuse of a central register, the ownerships could no longer be traced. This is prevented with the distributed registry.

Use case 4 - Decentralized Identity and Access Management

Especially for Internet-based services (also called smart services), identity and access management (IAM) is of great importance for companies to protect their own IT system from

unauthorized access by third parties. In order to ensure a secure way of exchanging information, it is necessary to clearly identify and authenticate all participating entities (e.g. persons, machines) as well as processes, and to verify their special characteristics. Secure identities [20] are the prerequisite for many other protective measures and support confidentiality, data integrity and reliability. An IAM system manages precisely these processes and applications, controls the life cycles of identities and manages access rights in a network. The necessary steps to verify an identity and granting access rights are authentication and authorization, i.e. determining the identity of an entity and the associated access rights that this entity has on the network and in the applications. An IAM system for AAS based on DIDs and Verifiable Credentials ensures more security and reliability, without using a central authority. This way authentication and authorization can be achieved for all participants involved in the value chain without an identity provider or certification authority. This opens up new digital business models. Furthermore, Verifiable Credentials [9] enable ABAC [21] in a decentralized system.

Diagram

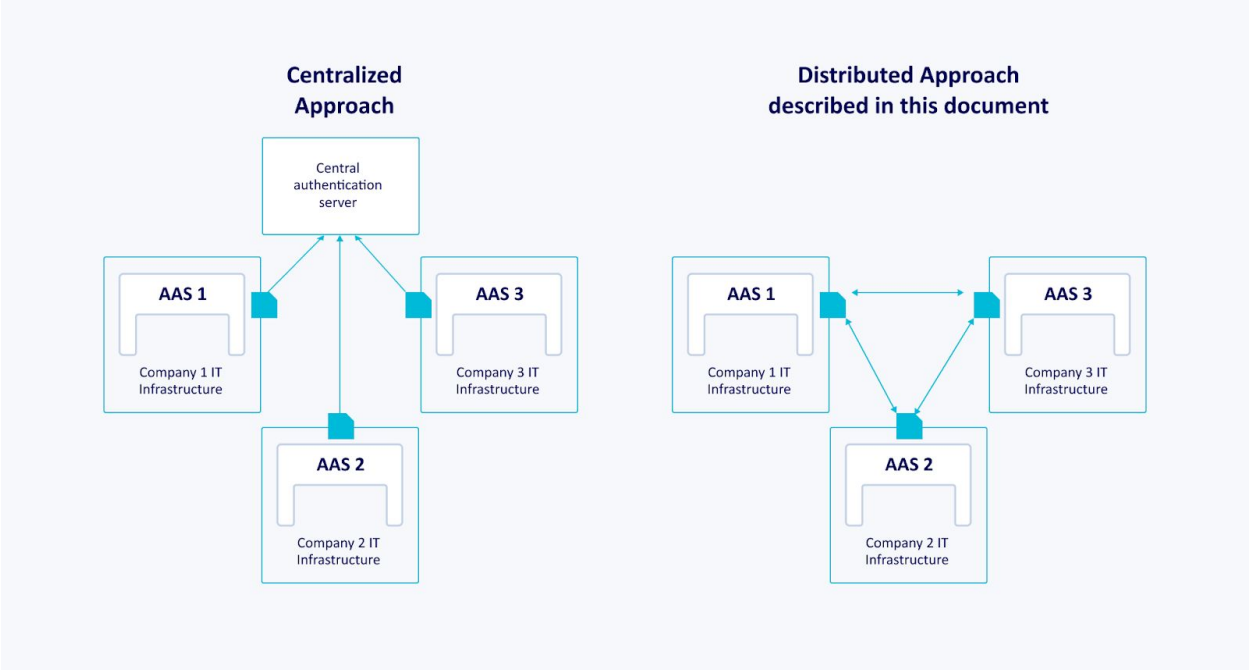

Figure 10: Centralized vs. decentralized Identity and Access Management

Key aspects

Key aspect is the use of a decentralized IAM system to authenticate and authorize entities in a decentralized context e.g. IOTA-based industry marketplace [22]. The authorization is based on

attribute-based access control (ABAC). Processes are integrated into the interaction protocol "bidding process" of the I4.0 language (Figure 11).

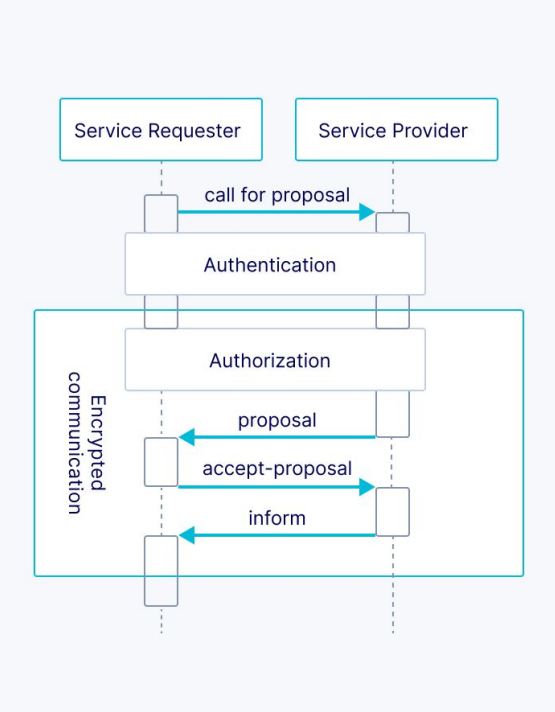

Figure 11: Extension of the in VDI/VDE 2193-2 "I4.0 language" defined semantic interaction protocol "bidding process" through direct (p2p) Authentication and Authorization processes

In this use case, ECLASS is mainly used to clearly describe the Verifiable Credentials. These are digital attribute certificates in the context of DIDs.

Note: The solution presented here is one option for authentication and authorization. Authentication and authorization using X.509 certificate chains as described in [19] is an alternative solution.

Value added

- Authentication and authorization independent from central authorities (such as PKI)
- No monopoly position of individual companies
- Fine-grained access management
- Processes are located above the application layer of the OSI reference model.
- Further application possibilities for using verifiable credentials are:
    - Issuing of licenses, e.g. temporary use of specified ECLASS IRDIs
    - Certification of an executed service, e.g. maintenance on a machine

Use case 5 - Qualification of an asset administration shell

Most recently, a growing number of asset manufacturers have started to provide standardized AAS with their manufactured assets. They take this effort because it is one possibility to provide their customers easy access to all information associated with an asset. For a customer to be able to use this information, it is crucial that the information is trustworthy and provided in a standard-conformant form. To ensure compatibility between different providers and consumers of this information, the associated AAS or the information contained in AAS need to be compliant with the standards. Unless this can be made sure by the customer, they cannot be sure their business processes, which rely on the information in the AAS, can be executed smoothly. The provider needs to prove that the consumer is able to use the information without any compatibility issues. This proof can be furnished by a qualification of the provided AAS.

Diagram

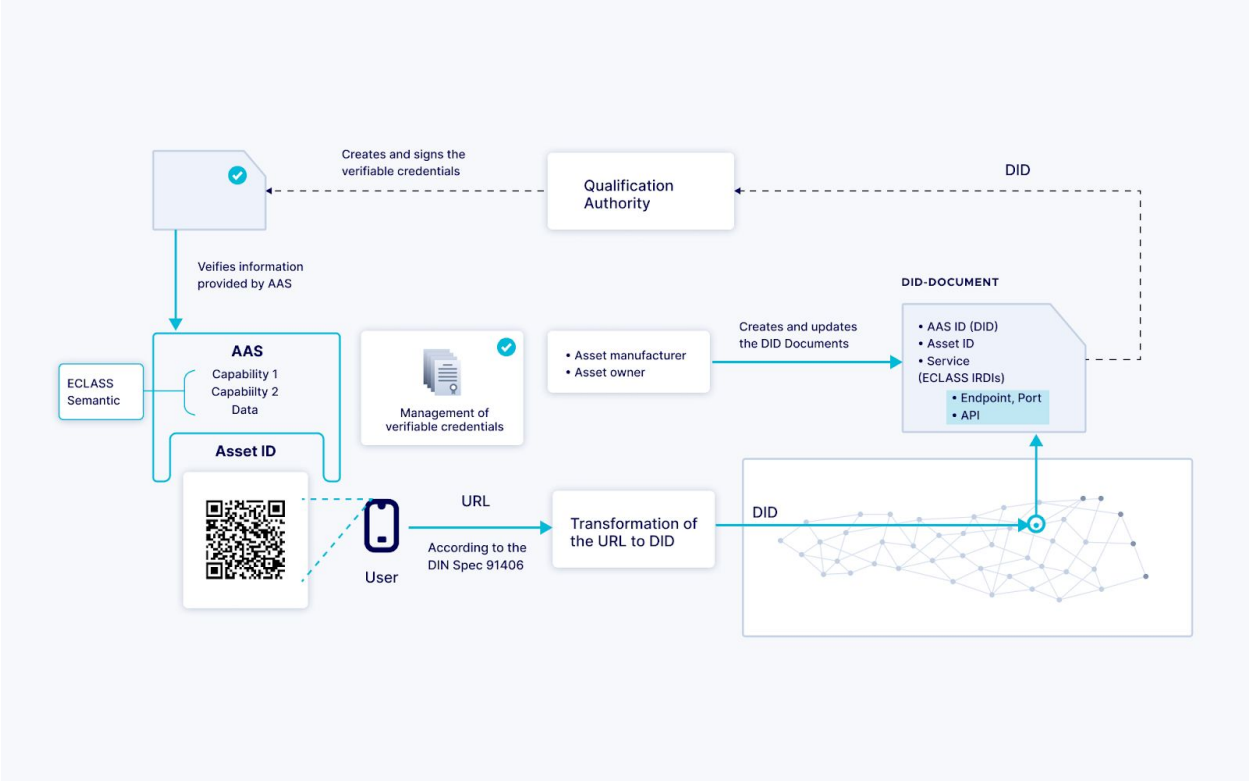

Figure 12: A Qualification Authority verifies information provided by the AAS and signs the DID document. Thus, the trustworthiness of the information provided by the AAS is confirmed

Key aspects

This use case describes the process of how the issuer of an AAS can get a verifiable credential from a qualification authority which states that the AAS or relevant information provided therein is fully compliant with certain relevant standards and regulations. It also describes how the user of the AAS can verify the compliance before accessing the data.

The process of qualification comprises the following steps:

1. Creation of an AAS
2. Registration of the AAS within a decentralized registry
3. Filing of a request for qualification of the issuer of the AAS at a qualification authority
4. Verification of the AAS by ensuring that the information provided complies with the relevant standards
5. Issuing a credential which states that the AAS referenced within the registry is compliant to relevant standards and which can be used by the value chain partners to prove to a consumer that this AAS is compliant with such standard.
6. Verification of the credential by the consumer of the AAS before accessing it.

In this use case, ECLASS properties are used to describe the qualification in a way that clarifies i.e. to which standards the compliance has been qualified and how long the qualification is valid for.

Value added

Having this use case in place has positive effects on the automated exchange of data between several entities. It:

- Guarantees that the information provided can be consumed by the consumer without any compatibility issues
- ensures business continuity as there will be no risk of malfunction when accessing the Data, as structure, semantics and data types are correct

Conclusion

In this white paper, we demonstrated that it is possible to build a decentralized registry based on I4.0 components, with concrete examples that show in detail how this can be achieved.

We also concluded that this kind of digital support can be useful not only for one specific time in the lifetime of an I4.0 component, but also to be used throughout the entire lifespan, ensuring continuity in scenarios like ownership change as seen in use case 3 and qualification of AAS in use case 5. The future proof assurance of accessibility of digital services can be realized with the authentication and authorization mechanisms, as described in use case 4.

We strongly recommend the adoption of the approaches referred to in this white paper, mainly in tandem between the decentralized registry and the decentralized identity management, because they clearly complement each other and provide an evident leverage into a wide adaptation of I4.0 for the entities that use them. The concepts described represent an extension to the centralized registries currently discussed, which themselves are an important step towards a fully decentralized I4.0 architecture.

Finally, we would like to define as next steps the implementation of a demonstrator that can effectively present to the community how these use cases can be implemented. Furthermore, we want to use the chance to discuss the findings with established expert groups and use the technical findings during this implementation phase as a guide for future improvements and implementations.

References

[1] DIN SPEC 91406 (2019). Automatic identification of physical objects and information on physical objects in IT systems, particularly IoT systems. Berlin: Beuth Verlag.

[2] ISO. (2005). ISO 19119: 2005–Geographic information–Services.

[3] Plattform Industrie 4.0 (2020). Specification: Details of the Asset Administration Shell. Part 2 - Interoperability at Runtime - Exchange information via Application Programming Interfaces (Version 1.0RC01). Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[4] Plattform Industrie 4.0 (2016). AG Forschung und Innovation: Ergebnispapier - Aspekte der Forschungsroadmap in den Anwendungsprozessen. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[5] Plattform Industrie 4.0 (2016). AG Forschung und Innovation: Ergebnispapier - Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[6] Plattform Industrie 4.0 (2020). Specification: Details of the Asset Administration Shell. Part 1 - The exchange of information between partners in the value chain of Industrie 4.0 (Version 3.0RC01). Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[7] DIN SPEC 91345 (2016). Referenzarchitekturmodell Industrie 4.0 (RAMI4.0). Berlin: Beuth Verlag.

[8] Lewin, M., Dogan, A., Schwarz, J., & Fay, A. (2019). Distributed-Ledger-Technologien und Industrie 4.0-Eine Untersuchung der Relevanz für Industrie 4.0. Informatik Spektrum: Vol. 42, No. 3.

[9] DIN SPEC 3103 (2019). Blockchain und Distributed Ledger Technologien in Anwendungsszenarien für Industrie 4.0. Berlin: Beuth Verlag.

[10] Bundesministerium für Wirtschaft und Energie (BMWi). Die volkswirtschaftliche Bedeutung von digitalen B2B-Plattformen im Verarbeitenden Gewerbe. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[11] Dogan, A., Zhang, Y., & Fay, A. (2019). Das vereinheitlichte digitale Typenschild. atp

magazin, 61(11-12), 92-101.

[12] Berners-Lee, T., Fielding, R., & Masinter, L. (1998). Uniform resource identifiers (URI): Generic syntax.

[13] Plattform Industrie 4.0 (2019). Leitbild 2030 für Industrie 4.0. Digitale Ökosysteme global gestalten. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[14] W3C (2020). Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations. Available at: https://www.w3.org/TR/did-core/

[15] W3C (2019). Verifiable Credentials Data Model 1.0. Expressing verifiable information on the Web. Available at: https://www.w3.org/TR/vc-data-model/

[16] Popov, S. (2018). The Tangle. Available at: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[17] Dogan, A. & Fay, A. (2020). DID-basiertes Identitätsmanagement für Industrie-4.0-Komponenten in dezentralen Systemen. Tagung „Entwurf komplexer Automatisierungssysteme“ (EKA). Magdeburg.

[18] Berners-Lee, T., Masinter, L., & McCahill, M. (1994). Uniform resource locators (URL). Available at: https://tools.ietf.org/html/rfc1738

[19] Orzelski, A. (2020). Industrie 4.0 Security with AASX Server. Available at: http://admin-shell-io.com/screencasts/security/Industrie_40_Security_with_AASX_Server.mp4

[20] Plattform Industrie 4.0 (2016). Technical Overview: Secure Identities. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[21] Plattform Industrie 4.0 (2018). Zugriffssteuerung für Industrie 4.0-Komponenten zur Anwendung von Herstellern, Betreibern und Integratoren. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

[22] Belyaev, A., Diedrich, C., Köther, H. & Dogan, A. (2020). Dezentraler IOTA-basierter Industrie-Marktplatz. Industrie 4.0 Management 2/20, S. 36–40.