PLATTFORM INDUSTRIE 4.0

WORKING PAPER

# Technical Overview: Secure Identities

# Imprint

**Published by**
Federal Ministry for Economic Affairs and Energy (BMWi)
Public Relations
10119 Berlin
www.bmwi.de

**Text and editing**
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

**Design and production**
PRpetuum GmbH, Munich

**Status**
April 2016

**Illustrations**
Maxsim – Fotolia (Title); Petrovich12 – Fotolia (p. 8);
kebox – Fotolia (p. 10); tatomm – Fotolia (p. 14);
Sergey Nivens – Fotolia (p. 17)

This brochure is published as part of the public relations work of the Federal Ministry for Economic Affairs and Energy. It is distributed free of charge and is not intended for sale. The distribution of this brochure at campaign events or at information stands run by political parties is prohibited, and political party-related information or advertising shall not be inserted in, printed on, or affixed to this publication.

The Federal Ministry for Economic Affairs and Energy was awarded the audit berufundfamilie® for its family-friendly staff policy. The certificate is granted by berufundfamilie gGmbH, an initiative of the Hertie Foundation.

**This publication as well as further publications can be obtained from:**
Federal Ministry for Economic Affairs
and Energy (BMWi)
Public Relations
E-mail: publikationen@bundesregierung.de
www.bmwi.de

**Central procurement service:**
Tel.: +49 30 182722721
Fax: +49 30 18102722721

# Content

**List of Tables**

**List of Figures**

# 1. Introduction

The aim of this paper is to provide an overview of the security challenges, requirements and approaches for secure identities in Industrie 4.0 environments. This document outlines the additional efforts that will be necessary to ensure the use of sufficiently secure identity features for Industrie 4.0.

The content of this paper is presented in general terms in order to ensure good transferability. This approach was chosen because a detailed examination of security would have to be an examination of individual cases so that the underlying conditions that play a crucial role in the particular case can be taken into account. Consequently this paper does not describe specific projects or implementations.

This document is directed at decision-makers and users in the Industrie 4.0 context. Examples of the framework conditions to be complied with, secure identities, guiding principles, and knowledge and insights that have been gained regarding security are outlined here for this target group.

## Why “secure identities”?

As already explained in “Implementation Strategy Industrie 4.0”, the summary report issued by the Industrie 4.0 Platform in April 2015, the secure exchange of information throughout the entire value creation network is essential to Industrie 4.0. A secure exchange of information requires the unambiguous, unique identification and authentication of individuals, machines and processes and the verification of certain properties. The need for different security levels was also established.[1]

Secure identities are the starting point for security chains that protect data capture, transport and processing at the hardware, software and process levels. They are a prerequisite for many other protection measures. When an attacker succeeds in assuming an identity on an unauthorised basis, all other constructive measures, such as access protection, make no sense. The primary aim of secure identities is to start a chain of trust in automated communication. Secure identities support the well-known protection objectives:

- Confidentiality
- Integrity
- Availability

To use an example from everyday life, this could be compared to a doorkeeper’s control of access to a building. A doorkeeper checks, on the basis of, for example, a company ID, the individual’s authorisation to enter a building. The doorkeeper checks the authenticity and validity of the company ID and cross-checks the holder with a blacklist. He then verifies whether the ID and the ID holder match the information on file (passport photo, height, eye colour and, where applicable, biometric features). In the digital world it is likewise necessary to verify who has been granted access to data or has placed an order and whether this person is authorised to do so. In both worlds these are fundamental processes that provide the basis for successful operations and must be conducted with due care.

Secure identities are also important for legal and commercial processes. In principle they increase the transparency of processes. This is easier to understand, who, how, when and with what rights someone communicates and possibly decides. In general it can be said that: The more reliable, trustworthy and traceable identities are, the more conceivable the transfer of (automated) execution and decision-making authority for persons, machines and components is. In this way secure identities can enable efficiency gains.

## Starting situation for secure identities in Industrie 3.0

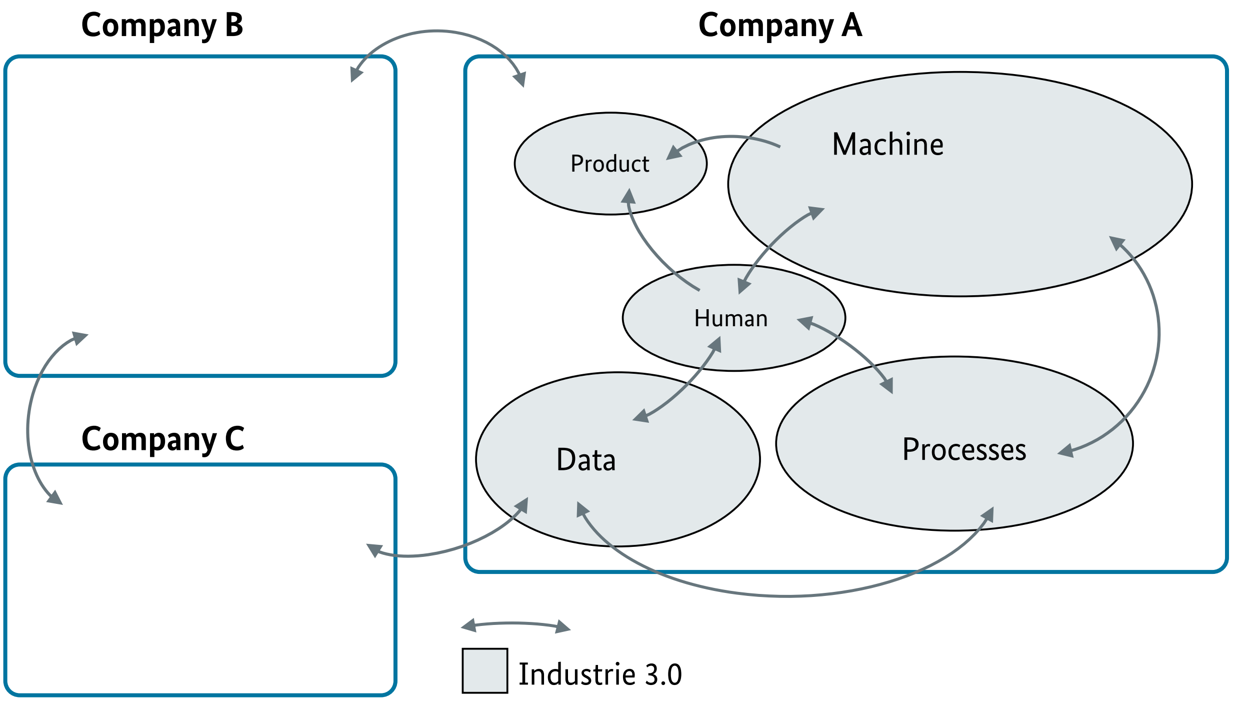
Industrie 3.0 primarily involves the interactions illustrated in the following diagram:

- People, data, processes and machines interact within an organisation. The product itself plays a passive role here. It is simply produced.
- Organisations interact with one another via traditional, defined channels in which data, processes and machines seldom interact beyond the respective organisation’s boundaries. Instead, there is perimeter protection between organisations which deliberately hampers and prevents direct interaction.

In Industrie 3.0 the individuals, machines, processes and companies are known to all and relationships and classifications are established.

[1] Cf. “Final Report 2015”, p. 53 ff.

**Figure 1: Communication and trust-based relationships in Industrie 3.0**



Source: Plattform Industrie 4.0

Today, security in the automation environment focuses on protecting internal company networks against external threats.

Today, secure identities are generally not integral to the respective system, but rather supplemental to it, taking the form of add-ons in special security products (dongles, hardware tokens, software tokens). At present, authority is seldom coordinated between the office area – often called information technology (IT) – and the production level – also called operations technology (OT) – on a comprehensive basis to enable experience and information to be shared in appropriate ways. The same applies to security by design in products and machines.

Secure identities are currently used primarily at user level, for example to access remote maintenance, for licensing mechanisms and in the office domain for encrypting e-mail. In addition, cryptography-based identification mechanisms (such as authentication chips) are often used to support cloning protection for hardware and software components.

There is no established security infrastructure to support secure identities across company boundaries (security domains).

Small and medium-sized enterprises have much catching up to do with regard to security in general and secure identities in particular. A low level of methodological expertise in assessing and evaluating security risks plus a lack of standards and generally accepted guidelines often hinder the implementation of concrete controls.

Overall, many companies do not even have a running security infrastructure and there is a lack of organisational processes – such as a public key infrastructure (PKI) – for implementing the security management system necessary for secure identities.

## What does the situation look like in the case of Industrie 4.0?

In contrast, interaction between a company's business units and with parts of different companies across their corporate boundaries is much denser in the case of Industrie 4.0 as a result of the development of value creation networks and increased flexibility.

In the case of Industrie 4.0, the interaction between persons, software processes and machines that already takes place is now joined by interaction with the following players:

- Machine components that are replaceable / interchangeable and therefore initially unknown
- Digital images (asset administration shells[2]) of machines, components or products

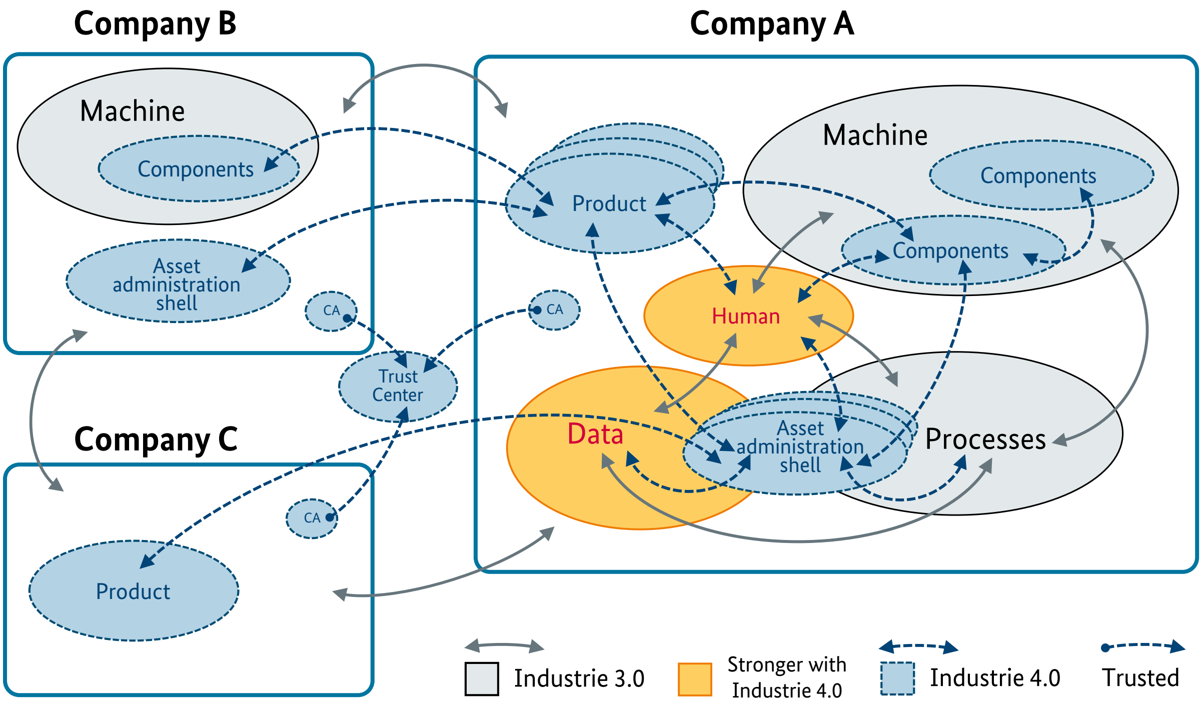
Identities are the requisite starting point – especially for legal reasons – for nearly all business processes, particularly when a company wants to make its processes more flexible. It would be virtually impossible to increase flexibility in Industrie 4.0 without them. What previously applied to Industrie 3.0 has become an absolutely essential tenet for Industrie 4.0: Only those (persons or machines) who trust one another should communicate with one another. As a consequence, identities are of key importance for the entire process.

Industrie 4.0 also envisages executing legally relevant communication, such as in connection with ordering and logistics processes. For this reason, the following protection objectives must also be taken into account in this examination:

- Authenticity
- Non-repudiation
- Accountability

Thus business dealings are conducted on an electronic basis and machines increasingly communicate directly with one another. This requires customary checks from the physical world to be carried over to the electronic world. In the case

**Figure 2: Communication and trust-based relationships in Industrie 4.0**



Source: Plattform Industrie 4.0

[2] Cf. footnote 1 on page 4

of contract negotiations, for example, it is important to not only have secure identification, but also to receive additional information such as regarding credit standing. The situation is similar with communication between machines and components. Here too, it must be ensured that access is allowed only when there is a legitimate interest, that information comes from a specific sensor and that data is only transmitted to specific machines.

## Common uses of identities

For manufacturers, integrators and asset owners, instances when identities are necessary include:

- Checking and verifying the system integrity of components and machines,
- Controllability of processes, access and rights with regard to time, place and domain,
- Authentication of components and spare parts,
- Conducting remote maintenance or predictive maintenance,
- Quality assurance in the production process (e.g. process locking),
- Inventory of products,
- Fulfilling compliance and documentation requirements, and
- Meeting traceability requirements.

Identities have exemplary uses in the application scenarios of the Industrie 4.0 Platform:[3]

- M2M contract negotiations or attribution of self-descriptions (Scenario 1)
- Traceability of components or replacement parts that have been delivered or the activation of features (components and features must be identifiable) (Scenario 4)
- Identification of production modules, their functionality and compatibility with other modules (Scenario 5)

These examples show that identities are widely used and have a variety of objectives. The range extends from type designations all the way to identities associated with business transactions. In some cases, a simple label in the form of, for example, a barcode is enough. In other scenarios a secure and manipulation-proof identity is required. Table 1 contains an overview of identities.

The question of which objects need an identity and which type of identity the respective type of object needs must be answered with the help of a security analysis and risk assessment. This document provides information regarding different types of identities and the relevant requirements. Pointers are provided that should help with the decision whether an identity is secure, trustworthy and suitable for the particular purpose.

[3] Plattform Industrie 4.0: Aspects of the Research Roadmap in Application Scenarios

# 2. Brief list of definitions

The following section defines basic identity management terminology as used in this document (based on [ISO 24760-1] and [BSI TR 3107-1], sections 2.1 and 2.2):

- An entity is a specific or abstract object, including associations between objects [DIN 4002-4:2013-09].
  - **Note 1:** Concrete objects can be persons, machines, products and organisations (companies/parties to a contract).
  - **Note 2:** Abstract objects can be digital data sets, files and patents.
- An attribute or a date is a characteristic or property of an entity.
  - **Note:** Name and date of birth are examples of a person's attributes and dates. Attributes of machines include the designation of the particular machine and its functions. Examples for products include date of production, article number, weight and colour.
- An identity (ID) is a property of an entity and is characterised by a set of attributes. An entity may have several identities, just as several entities may have the same identity.
  - **Note:** This is comparable to the case of a street address for a building. The building has a clear identity that applies to several occupants. When they are identified using only the house number, the occupants do not have a unique identity. An identity is therefore usually not unique as a rule but may be unique in a particular context.
- A unique identity (UID) is a specified set of attributes which clearly represents the corresponding entity in a certain application context.
  - **Note:** Unique identities are assigned to just one entity or entity class. An entity may have several unique identities, such as through the passage of ownership in different companies.

- A secure identity (SID) is a unique identity with additional security properties for the robust, trustworthy authentication of the entity (e.g. with suitable controls to prevent the assumption of a false identity).
  - **Note:** In technical terms, it is possible to fulfil the security requirements for a target system in different ways (see the examples in Table 1). In order to be able to comply with stringent security requirements, it is advisable to link identity information with a physical property, in other words, with a second factor. This property must be such that it cannot be copied or deliberately modified or can be copied or modified only through a disproportionate amount of effort (for the attacker).
  - **Note:** In the case of IT-linked systems, a high level of security can be achieved by means of hardware-based cryptographic authentication functions. Using a cryptographic certificate, the identity information is coupled with a securely stored, secret key whose local use serves as proof of identity.
- **Authenticity:** Property of an attribute. An attribute is authentic when it actually corresponds to a statement; in other words, when the actual property corresponds to the claimed property.
  - **Note:** A sent message is designated authentic in terms of its origin when the actual sender is identical with the sender specified in the metadata (e.g. sender address).
- **Authentication:** Determination of authenticity. Input variables: Attribute of a sender and the received message or attributes of an accessing party and an access request. Output variable: Is authentic [yes/no].
  - **Example:** A typical M2M authentication consists of suitable controls such as challenge-response authentication or PKI-based authentication using established cryptographic functions. The sender or accessing party proves his authenticity by successfully executing a specific cryptographic process which requires knowing the necessary cryptographic key(s).
- **Trust:** Explicitly tested and confirmed suitability of the security measures used to meet the security requirements. A combination of checks, audits and evaluations is used here. Together they establish a trust level. A security policy specifies which trust level is considered to be adequate. Security controls that pass such tests are then considered within the scope of the policy as being trustworthy in terms of fulfilling their security function. The policy is updated as necessary. It additionally contains time requirements such as the permissible period of validity between two checks. For further information see the detailed description in Annex A3.
- **Credential carrier:** Examples of credential carriers include physical objects (RFID and QR code stickers) and electronic components (TPM modules) that supply the entity’s identity; see Table 3 for further information.

# 3. Types of identities

*Table 1 classifies the term "identities" using examples for the three types: identity (ID); unique identity (UID) and secure identity (SID). This typing differentiates identities on the basis of the level of the security requirements that the target system must fulfil. The SID is presented in greater detail in Annex 2.*

## Properties of identities

The fundamental characteristics of identities are examined in the following section:

- **Level of identity uniqueness (simple, unique, secure)**
- **Owner of the identity: Person, machine, product, etc.**
- **The credential carrier's tie to the owner**
    - In terms of time (one-off vs reusable)
    - Robustness of the link
- **Limitation of the validity** of the identity:
    - Spatial: Company premises vs global
    - Time: One hour vs permanent

Of fundamental importance is the question of the need for a specific type of identity based on the respective protection objectives. When, for example, products are furnished with a simple identity, this may be sufficient for ensuring that only this particular product class is used. In such cases several entities have the same identity. In other cases a company wants to unambiguously establish which machine performed a task at a specified time. This requires a unique identity. If on the other hand protection against forgery, theft and/or misuse is required, a secure identity should be chosen.

The factor "time" also has an influence on identities. Due to this factor, identity attributes can change. When a person changes the company this usually results in a new identity. (This will be examined in greater detail in the section on life cycles.) In the production area it can also be necessary to be able to use an identity to access certain resources for just a limited period of time or to exclude an identity entirely from further activities. This pertains primarily to authentication processes.

**Table 1: Types of identities broken down by security characteristics, with examples of corresponding technologies**

| | | Identity (ID) | Unique identity (UID) | Secure identity (SID) |
|---|---|---|---|---|
| **Security characteristics** | **Depth of identification; Aim/Objective** | Identification of articles, manufacturers and persons (classes of entities) | Identification of individual entities | Identification and authentication of individual entities |
| | **Identification** | X[1] | X | X |
| | **Differentiation within a class** | – | X | X |
| | **Integrity** | – | X | X |
| | **Forgery resistance** | – | (X) | X |
| | **Offline identification** | X | (X) | (X) |
| | **Authentication** | – | –[2] | X |
| | **Offline authentication** | – | – | (X) |
| **Examples of current technologies** | **Digital ID** | Software that is signed with a public key | IP address, MAC[3] address, GUID | TPM[4] (containing a security anchor or certificate) |
| | **RFID[5]** | RFID tag with stored class information (e.g. article number) | RFID tag with stored, fixed UID | Secure microprocessor (various solutions) |
| | **DMC (data matrix code)** | DMC with GTIN[6] | DMC with SGTIN | – (possible only with a second factor) |
| | **QR code** | QR code | QR code with serial number | – (possible only with a second factor) |
| | **Pattern recognition (graphic)** | Visual recognition (contours, dimensions) | Additional factors (e.g. duration and pressure when signing) | – |
| | **Toll vignette** | Vignette | Vignette with serial number | Toll system – OBU (on board unit) |
| | **OVD (optical variable devices)** | Hologram, security colour, security materials and the like | Hologram or security print with serial number | – (only possible with a second factor) |
| | **Biometrics (patterns in cell structure, blood vessels, skin, iris, …)** | Seat occupancy (low-resolution camera, scale) | Facial image, fingerprint, hand vein pattern, iris scan | – (only possible with a second factor) |
| | **1D code (barcode)** | EAN/GTIN, GS1[7] DataBar | (GSI DataBar in a closed domain) | – |
| | **PUF[9] (physical unclonable function)** | E.g. foils with controls to prevent their removal | Extraction of an optical fingerprint from the surface texture | Electronic PUF in microprocessor |
| | **Examples of common techniques/methods** | Proof of origin, EAN[8] barcode, figurative mark, "Made in Germany" | Reserved seat tickets in cinemas, serial numbers, business cards, chassis numbers | Electronic identity cards, electronic health insurance cards, banknotes |
| | **Examples from the industrial production sector** | Part numbers (type numbers) on machine parts … referenced to IEC 62443 | Licence keys for software installation … referenced to IEC 62443 | Smart meter … with Industrie 4.0 |

[1] Explanations for those parts of the table that are highlighted in grey
X = Is possible with this type of identity; (X) = Is possible only to a limited extent with this type of identity; – = Is not possible with this type of identity

[2] Since a secure identity (SID) can be produced by combining a unique identity with additional mechanisms for providing proof, the unique identity cannot be authenticated without additional checks.

[3] Media Access Control – the hardware address of a network adapter, often with reference to Ethernet in accordance with IEEE802.3

[4] Trusted Platform Module, alternatively software / hardware implementation

[5] Radio Frequency Identification is a system for contactless communication between an electronic reader and a (security) chip that is affixed to an object.

[6] Global Trade Item Number or SGTIN = Serialized Global Trade Item Number

[7] Global Standards One, issuer of GTINs as an issuing agency pursuant to ISO/IEC 15459-2

[8] European Article Number, superseded by GTIN in 2009

[9] PUF (physical unclonable functions): A function module that provides a unique identity based on its individual physical properties, proves its authenticity and cannot be reproduced within the framework of given security requirements

In any event, it is necessary to be prepared for the possibility that an entity's identity can change over time or that the technology and equipment being used must also be changed because cryptographic processes in use are possibly no longer appropriate.

Cross-company use of identities will increase in connection with communication in the value creation networks of Industrie 4.0. This will require trust in the issuing authority and the communication partner.

## Life cycle of an identity (identity management)

The life cycle of an identity is briefly described here to facilitate understanding of the use of identities. An identity life cycle is comprised of four phases. The different roles of the component manufacturer, the machine manufacturer or integrator and the asset owner of the equipment are to be taken into account.

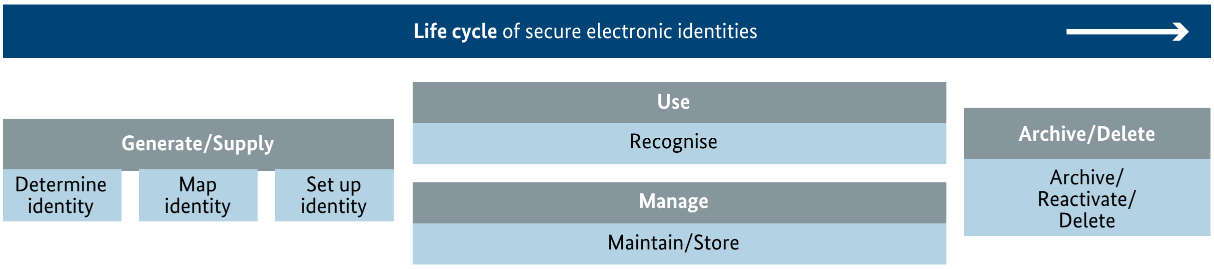
When an **identity is generated** the respective entity's identity attributes are recorded and assigned to the identity. In the case of a secure identity, a digital certificate and a signature are generated by the issuing authority. Another example is the generation of a barcode on the basis of a serial number with the necessary information. The component manufacturer thus establishes the initial prerequisite for a component's use. In the case of a machine manufacturer or integrator, components that have been assigned an identity are combined to build up a machine. The identity generated in this case applies to the machine as a product. Here it can take the form of a digital certificate that serves as the secure identity of the machine or a serial number for the machine. In the case of the asset owner, the generated identity, e.g. a digital certificate, is to be viewed as a secure identity of the particular machine within the context of the company or as an inventory number. Identification that is based on the job the machine does or on the machine's location[4] is also conceivable.

**Use and management** take place at the same time. During use the identity is used. For example, a machine authenticates itself vis-à-via another machine on the basis of a secure identity. Management is understood as the maintenance of identity attributes, in other words, their updating and augmentation, their storage in central or decentral systems, and adjustments to the rights of an identity. Information that is generated when the identity is used can be utilised, for example, for tracing a component and determining its current location.

The process is concluded with the **archiving and deletion** of the identity. In the case of archiving, certain contents can be retained in order to be able to refer at a later date to parameters that arose during production. This point also includes blocking an identity when, for instance, a token is lost or stolen. When this is done, the identity can no longer be used and a new secure identity must be generated. Existing information can also be used for this.

In many cases an identity has a limited life time. Physical properties are subject to ageing. General technical progress can reduce the robustness of cryptographic methods (e.g. as a result of the increasing availability of computing capacity for brute-force attacks). Such aspects must particularly be taken into account in industrial application scenarios in the case that the identity of a component has to be verified over the entire life cycle of the particular machine or plant.

**Figure 3: Life cycle of a secure identity (based on ISO 29115)**



Source: Plattform Industrie 4.0

[4] This is common in the area of IT infrastructures and is implemented using, for example, the SysLocation SNMP object.

An identity reflects an entity's placement in its environment. An entity can therefore have several identities at the same time or successively which correspond to the entity's respective role. Each of these identities goes through the life cycle of generation/application, management/archiving and deletion. Therefore an identity management system is necessary.

The special challenge for secure identities can be illustrated using the example of the above-mentioned machine and roles: When the machine is commissioned at the asset owner, a secure identity in the form of a certificate is generated and must be updated any time there is a change in the machine's intended purpose. In the event that the machine is de-commissioned, it must be ensured that the secure identity that identifies this particular machine as one of the asset owner's machines is handled appropriately. One example of this is the deletion of this identity.

## Secure identities and system integrity

In addition to an entity's secure identities, steps must be taken to ensure that the functions provided are indeed the functions that the user expects from the entity. It must for example be ensured that entities do not contain viruses or Trojans that compromise the respective entity's functional integrity. Therefore, although protecting the respective identity is necessary, it is not enough to ensure security.

The preservation of integrity is an undertaking that spans all value creation networks, starting from design and extending to production all the way to the operation of the entity. Preserving integrity is therefore a question of appropriate processes plus controls that are used to preserve security in the processes of all players in the value creation network.

Integrity is not a static property, but rather can change over the life of the entity. Integrity can change as a result of, for instance, security gaps that lead to attacks of a kind that were not known at the time the machine was delivered. For the asset owner of an automation plant, this raises the question of verifying and preserving the integrity status of his plant. In addition, corresponding measures must be brought into line with the priority assigned to the plant's availability.

# 4. Requirements for identities in Industrie 4.0

## Comparison with the current state of affairs

IEC 62443, an international series of standards for the IT security of industrial automation and control systems (IACS), defines four security levels (SL1 to SL4) based on technical security capabilities. These security levels are oriented to the level of attack power. Level 1 additionally takes unintentional operating errors into account. The higher the security level, the higher the achievable security level (see Table 2 in Annex A2).

The type of identity needed is determined by an assessment of the relationship between the entities and the identification and authentication this calls for. An authenticator (e.g. user name as identification and a password for authentication) is needed for authentication.

ISO/IEC JTC 1/SC 27 develops standards for protecting information and communication, with a focus on security and data protection. This includes cryptographic mechanisms and security aspects of biometrics, data protection and identity management. In the area of identity management the following activities are being pursued:

- A framework for identity management (ISO/IEC 24760); Parts 1 and 2 have been adopted ("Terminology and concepts", "Reference architecture and requirements"). Part 3 ("Practice") is currently in preparation.

- Entity authentication assurance framework (ISO/IEC 29115, adopted). High-level and technology-agnostic overview of fundamental aspects of authentication. Contains definitions for four levels of assurance for authentication plus threats and countermeasures during the authentication process.

- Authentication under increased data protection requirements: Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, adopted); Attribute-based credentials (study)

- Access management framework (ISO/IEC 29146, in process), identity proofing (ISO/IEC 29003, in preparation)

ISO/IEC 24760, ISO/IEC 29115, ISO/IEC 29146 and ISO/IEC 29003 expressly concern the authentication of entities which can be persons or non-person entities (NPEs). By contrast, activities that pertain to data protection usually concern the identity of persons or groups of persons and not things.

ISO 29115 Information technology – Security techniques – Entity authentication assurance framework: This standard describes a framework for the management of identities. It describes different levels of assurance for the authenticity of identifies and defines corresponding requirements. This document can provide guidance for establishing requirements.

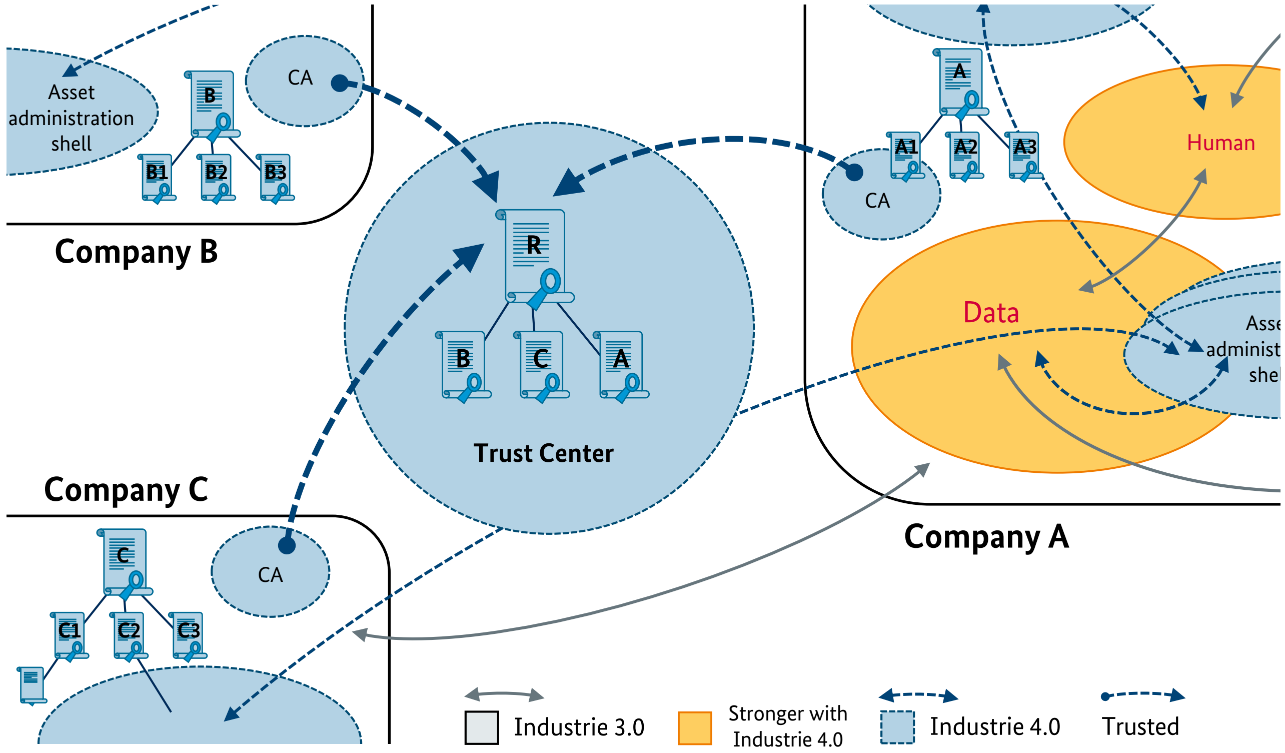
## Requirements for implementing secure identities

Security requirements are based on protection objectives, a risk assessment and a threat analysis for the use case (or also, more generally, for a field of use cases).

Typical protection objectives which have an influence of the requirements of the level of the secure authentification:

- Know-how protection for manufacturers, integrators and asset owners

Figure 4: Trustworthy “neutral” instance (Trust Center)



Source: Plattform Industrie 4.0

- Integrity of the product and system functions
- Confidentiality of (communicated) data
- Securing safety mechanisms (against intentional disruptions)

The necessary security level of the respective identity (with for example PKI support, hardware controls) is determined by the risk assessment, taking the accruing costs into account.

Actually identities are assigned within a security domain (within a company). Mechanisms and rules ensure that only authenticated entities take part in the communication.

A **trustworthy authority** (certification authority, **CA**) is needed as an instance for administering the identities of all entities in a particular security domain. From today’s standpoint, a PKI appears to be viable as a possible solution. Consequently the term “certification authority” will be used in the following section; see also Figure 2: Communication and trust-based relationships in Industrie 4.0

Today it is common practice in the office domain to place a time limit on the validity of identities. This procedure (use of limited validity periods) must be evaluated to ensure the protection objective of availability in production and in the product. Depending on the use case, the identity’s period of validity can be linked to its life cycle or specified by the user.

Making use of the advantages of Industrie 4.0 requires secure value creation networks. Consequently, entities in cross-company Industrie 4.0 value creation networks need, as a necessary and essential feature, a secure identity that can be used across security domains.

The figure here shows a central certification authority (Trust Center) as a trustworthy instance (centre of diagram) for the subscription of certificates in security domains.

It must be possible to verify identities across different security domains. The issue and revocation of rights must be controlled by the respective domain.

**Standards and processes for the trustworthy linking of the certification authorities (CAs)** of the respective security domains are needed. There has been no suitable model for this today. The design and implementation could be based on the identity management systems and the roaming agreements of mobile communications providers. Companies (security domains) must trust other companies (other security domains).

In order to be able to use a documented level of assurance on a cross-organisation basis, **guidelines and verification requirements must be incorporated into an overarching security context for all companies involved**.

Identity management must support the protection of intellectual property at all levels. This includes using access control mechanisms to limit the number of products manufactured on the basis of provided product and production models. An accepted and practicable digital rights management system is an important prerequisite for this

## Requirements for secure identities in the product development phase (security by design)

The security of the identity information also plays an important role in connection with security by design. The aim of security by design is to realise security functions as an integral part of a product or solution. In addition to clearly anchoring security in the respective standards - right from the start - this has consequences for manufacturers and asset owners of plants and equipment. Existing processes must undergo extensive supplementation that also concerns the requirements placed on the security of the identities and the choice of possible solutions.

Additional security features are linked to the system's security anchor during the security by design process.
In this connection, the security level of the security anchor will particularly determine the security level of functions related to confidentiality and integrity in future.

In addition to the implementation of a secure identity in the physical production process, Industrie 4.0 requires a corresponding digital/virtual presentation (**asset administration shell**[5]).

Security by design must also take into account various aspects of the integration of the secure identity into the target architecture: In many cases infrastructures for keys and their certificates are also needed in order to be able to use secure identities. These infrastructures must be taken into account and provided for in the design. The rule that the overall security level of a system chain is not greater than the security of the weakest link in the chain particularly applies here as well.

Security by design also pertains to the trustworthiness of the implementation and the processes. It must be ensured that the security of an identity is not compromised by weaknesses in its implementation or in the supporting processes. There must be no way to retrieve security anchor-dependent system secrets through side channels or backdoors on an unauthorised basis.

[5] Cf. http://www.zvei.org/Downloads/Automation/Industrie%204.0_Komponente_Download.pdf

# 5. Recommendations for action

The implementation of an identities concept will always be the responsibility of the respective company. It knows its processes and needs best. The political sector is however responsible for establishing – together with industry – the conditions necessary for a targeted, interoperable and efficient international infrastructure. In particular, the allocation of roles between government, PPP and private-sector models must be jointly discussed.

VDI/VDE Guideline 2182 "IT security for industrial automation" describes a general model with several process steps. The roles of the component manufacturer, the machine manufacturer or integrator and the asset owners are taken into account and interlinked. The asset owner plays a **key role with regard to risk assessment and threat analysis** that involves the identification and evaluation of risks pertaining to IT security. He determines the measures needed to reduce risk and the consequential requirements for the machine manufacturer/integrator. **Analyses and evaluations** must be repeated on a **regular basis**. The machine manufacturer/integrator is called upon to implement the requirements that the asset owner considers necessary. The prerequisites for implementation are passed on as requirements to the component manufacturers.

This model provides the basis for differentiated recommendations for action for these roles (manufacturer, machine manufacturer/integrator, asset owner including SMEs) and the political sector.

## Companies as asset owners

The asset owner is called upon to develop, manage and regularly update a security concept for its domain. An **identities concept from the asset owner's perspective** must be developed for the value creation networks; the necessary security level of the identities must be ascertained. The requirements arising from this are to be passed on to the suppliers of the machines and plants.

The asset owner's infrastructure must meet the requirements arising from the identities concept, such as the establishment of a trustworthy certification authority (CA) as the administrative instance in the particular security domain for issuing and managing secure identities for all entities in the production level (OT), taking into account concepts from the office domain (IT).

## Machine manufacturer/Integrator

An identities concept for the respective machine is to be developed from the vantage point of the machine manufacturer and on the basis of the security protection objectives it has prioritised. Where are secure identities needed in the machine in order, for example, to protect company know-how? The identities of the integrated components are to be verified on the basis of the concept. The identity assigned to the machine should be linked to the identities of the integrated components. This provides the basis for the requirements placed on the components used and consequently on the manufacturer of the components.

Further, the asset owner requirements regarding the required security level of the identities are to be taken into account. For example, the provision of hardware support to ensure the secure management of an identity.

The asset owner's infrastructure must meet the requirements arising from the identities concept for the machine, such as the establishment of a trustworthy certification authority (CA) as the administrative instance for integrating key material into the machine/into the components built into it.

In the manufacture of machines, the recommendations for action for a company as the asset owner are also to be taken into account (suppler requirements).

## Component manufacturers

Manufacturers should provide their components with a suitable identity. The level (ID, UID or SID) and the robustness of the protection are determined by the possible use of the components in the system. Machine manufacturers/integrators should be in a position to verify the authenticity of the components when they incorporate them into a system. For this reason, the component manufacturer should offer a suitable method that the machine manufacturer/integrator can use to conduct this type of check.

When manufacturing a product, the recommendations for action that apply to companies in their capacity as the asset owner are also to be taken into account.

## The political sector

Using laws and regulations, the political sector establishes the legal framework in which players such as asset owners, integrators and component manufacturers operate. The identity concepts necessary for Industrie 4.0 must be practicable within this legal framework. To ensure this, the political sector should take these concepts into account in the legislative process. Relevant areas include data protection and contract law. National rules should be viewed in an international context.

Technical solutions with a high level of trustworthiness could become a trademark for Germany and Europe. Germany is already home to many highly specialised providers of solutions for cyber and ICT-security. The development of trustworthy IT infrastructures must be systematically pushed forward as a contribution to Europe's digital sovereignty. This must however be supported by corresponding political initiatives. The aim is to strengthen the security competence and trustworthiness of German and European companies as a crucial competitive factor.

## Open issues:

Methods and processes that are suitable for automatically verifiable trust between entities across company boundaries must be described. Suitable models for this do not yet exist due to the challenge of establishing corresponding robustness, independence and technical uniformity. The experience gathered in setting up certification authorities must be taken into account for a number of reasons, such as preventing any compromising of individual certification authorities from becoming a problem for all of the entities.

The successful methods and processes used by mobile communication providers for identity management and roaming appear to be viable for use as models for a new concept.

The questions arise whether processes and products that are necessary for cross-company cooperation must satisfy security criteria that are determined by the players in the value creation network and whether they should be correspondingly audited and classified. This classification could greatly facilitate the asset owner's and machine manufacturer's procurement activities.

# 6. Annex

## A-1 Examples for identity concepts

### Electronic components as credential carriers, Part 1: RFID tags as carriers of a unique identity (UID)

RFID tags are components consisting of an integrated circuit (a microchip) and an antenna. The energy is supplied from the electromagnetic field of the reader. Depending on the communication standard, the distance between the RFID tag and the reader can be up to 10 cm, one metre or several metres. RFID tags record small amounts of data (a few hundred bytes) and have limited security functions. They typically have a unique serial number (unique identifier - UID) which the chip manufacturer entered in the memory during production. The UID assigned by the chip manufacturer is applicable in the chip production context. In the context of the chip's use, this UID can also be regarded as an UID as defined by Table 1; however this does not automatically have to be the case. This type of RFID tag is assigned to the tagged object based on the assignment undertaken in the assets administration shell. The data contained in the memory of the RFID tag can only be read when the tag is within range of a reader. Typically this is the case only during brief periods of time. The design of the RFID tag has an influence on its use as a credentials carrier:

- A **glued-on or screwed-on RFID tag** is separable from the tagged object in such a way that it is possible to remove it. It is suitable for use as a credentials carrier (ID), for logistics information and to simplify and speed up inventory processes. It must be determined on a case-by-case basis if this type of RFID tag is still attached to the object to which it was originally assigned.

- An **RFID tag that is permanently bonded** to the tagged object cannot be removed. Removing the tag from the object using heat or chemical or mechanical means would also destroy it. Consequently the assignment to a specific object is permanent and trustworthy. As a result, this type of RFID tag is suitable for use as a carrier of a unique identity (UID).

### Electronic components as credential carriers, Part 2: Secure microprocessor

Secure microprocessors can be found in forms that resemble RFID tags. Some types of secure microprocessors can likewise get their energy from the electromagnetic field of the reader. However the range within which this is possible is always less than 10 cm. In contrast to RFID tags, secure microprocessors are complex chips with an extensive array of security functions. They have an embedded operating system and application software that determines the range of their functions. They can store up to several hundred kilobytes of data. They calculate complex cryptographic algorithms and are capable of strongly encrypted communication. Their memory content and all calculations are encrypted and hardened against numerous types of attacks. Their use as a credential carrier is also connected with the respective design used:

- A **secure microprocessor in a chip card** is suitable for use as a carrier of a unique identity (UID) for people. Identities of this type are protected against being copied and the data on the card is protected against unauthorised access. The chip card's assignment to its legal provider must be verified separately in the system if necessary.

- A **glued-on or screwed-on secure microprocessor** resembles a glued-on/screwed-on RFID tag in its use and can look the same as an RFID tag. However, in contrast to an RFID tag, a secure microprocessor can store larger amounts of data, offers significantly more robust protection for the data stored on it and provides encrypted communication with the reader. Since it enables integrity verification, forgery resistance, and authentication, a secure microprocessor is suitable for use as a secure identity (SID) carrier in the context of the respective application. The fact that it can be separated from the assigned object is a limitation that the system must take into account.

- In contrast to the aforementioned examples, a **secure microprocessor that is permanently built into the electronics assembly of a machine** does not require a separate reader because it is directly connected with the machine's electronic assembly. It makes it possible to operate the security processes in the system online. In addition to providing a secure identity (SID) that is firmly connected to the respective machine, a secure microprocessor of this type is also suited for authenticating, encrypting and verifying the integrity of communication in the system. When using this type of microprocessor as a security anchor or credentials carrier it must be remembered that the surrounding electronics and the transmission paths in the system are not automatically secure. End-to-end encryption and integrity checks may be necessary in order to ensure trust at system level.

## Trust anchors and secure identities

The term "trust anchor" plays an important role in the definition and assessment of a system's security architecture.

On the one hand the term "trust anchor" is often used to designate the root CA in the certificate hierarchy of a public key infrastructure.[6]

On the other hand, the term "trust anchor of an entity" designates the implementation (=secure anchoring) of the sensitive security parameters for this entity (e.g. integrity check sums and secret key material).[7]

In any event, the security level of the trust anchor is key to the security of the entire system: A trust anchor with software implementations that hackers can more or less easily access evidently justify a lower security level in comparison to embedding the security parameters in closed security hardware which, when correctly integrated, cannot be compromised from the outside by software-based attacks.

Thus the security level of the authentication function of a secure identity is ultimately based on the quality of the security anchors involved in the system and entity. Secure identities with corresponding security anchors will particularly be needed for participating in Industrie 4.0 communication across several networks. Otherwise, a partner in the communications network can become a security risk because, for example, the signature it generated can be counterfeited or keys for cryptographic algorithms can be copied on an unauthorised basis.

Hardware-supported trust anchors can significantly improve the security of IT-based systems. However it is not enough to use protected hardware to run security parameters and cryptographic functions that are used for authentication and other purposes. Following the principles of security by design, the way the security hardware is embedded in the system must be correspondingly secure in order to avoid additional vulnerabilities.

Hardware components that primarily serve to process security functions are also called hardware security modules or secure elements. Such components can store keys securely (for example, in such a way that they cannot be copied) and securely use them (for example, in such a way that they cannot be eavesdropped). They can also prove to communication partners with the help of cryptography (remote attestation) that the system is in a trustworthy state.

One example of a standardised security module is the Trusted Platform Module (TPM) of the Trusted Computing Group (TCG). A TPM can be realised as a special security IC, as a function in a standard IC or in firmware. TPMs are used in the area of personal computers, mobile devices (tablets, smartphones) and servers. However, these devices are designed to have a service life of significantly less than ten years. This is not suited to the life cycles of industrial components. As part of the IUNO national reference project which is being funded by the Federal Ministry of Education and Research, concepts for security hardware with a longer service life are to be examined and then implemented in demonstrators on a targeted basis by the year 2018. In addition to this there are many kinds of hardware-based security modules that are used in ICT components, in payment terminals and credit card systems, in mobile communications systems, in toll systems, in connection with EU tachographs in the on-board units in heavy goods vehicles, and in the card reader units at the family physician's office.

[6] http://tools.ietf.org/html/rfc5280, http://tools.ietf.org/html/rfc5914

[7] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5955006&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5955006,
http://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trust-anchor-technologies-ds-45-734230.pdf

## Trustworthy instance and its integration; mobile communications standards

According to the requirements set forth in the standard, the International Mobile Station Equipment Identity (IMEI), a 15-digit serial number for a GSM or UTMS terminal, should be unique worldwide. In the case of many devices however, security and uniqueness is not guaranteed. The SIM card serves to identify the user. The IMSI serves to unambiguously identify network participants. An IMSI is issued by the mobile communications provider worldwide once per SIM and is stored on the SIM card. IMSIs are issued nationally (in Germany by the Bundesnetzagentur).

In the area of mobile communications, the mobile phone subscriber's authenticity is verified vis-à-vis the provider for the purpose of ensuring correct billing by the provider.

A mobile communications provider is an example of a trustworthy authority (certification authority, CA) and an administrative authority for all entities in a security domain. In the case of Industrie 4.0, SIMs with an IMSI represent the identity of an Industrie 4.0 entity. All entities whose identity is assigned by this type of CA can, with the help of the CA, check the authenticity of the identity of the desired partner in a security domain.

The roaming agreements of mobile communications providers allow communication across networks. In the case of Industrie 4.0, roaming agreements are agreements between CAs and thus enable communication and trust relationships across security domains.

## A-2 Requirements for secure identities

### Based on IEC 62443-3-3

IEC 62443 is an international series of standards for the IT security of industrial automation and control systems (IACS). It defines four security levels (SL1 to SL4) based on technical security capabilities. These security levels are oriented to the level of attack power. Level 1 additionally takes unintentional operating errors into account. The higher the security level, the higher the achievable level of security.

**Table 2: Requirements for secure identities based on IEC 62443-3-3**

| | SL1 | SL2 | SL3 | SL4 |
|---|---|---|---|---|
| Human user identification and authentication | Requirement … to identify and authenticate all human users. This capability must enforce the identification and authentication on all interfaces that provide human user access to the automation system … | SL1 +<br>Unique identification and authentication | SL2 +<br>Multifactor authentication for untrusted networks | SL3 +<br>Multifactor authentication for all networks |
| Software process and device identification and authentication | | Requirement … to identify and authenticate all software processes and devices. This capability must implement this type of identification and authentication at all interfaces that permit access to automation systems … | SL2 +<br>Unique identification and authentication | SL2 +<br>Unique identification and authentication |
| Authenticator management | Capability … to protect all authenticators against an unauthorised disclosure and modification during storage and transmission. | SL1 | SL1 +<br>Hardware security for software process identity credentials | SL1 +<br>Hardware security for software process identity credentials |

→

Table 2: Requirements for secure identities based on IEC 62443-3-3 (Continued)

| | SL1 | SL2 | SL3 | SL4 |
|---|---|---|---|---|
| Password strength | Capability ... to enforce ... a configurable strength for passwords. | SL1 | SL1 +<br>Password generation and lifetime restrictions for human users | SL3 +<br>Password lifetime restrictions for all users |
| PKI certificates | | Support PKI | SL2 | SL2 |
| Strength of public key authentication | | ... check the validity of public and private keys | SL2 +<br>Hardware security | SL2 +<br>Hardware security |
| Derived identity type (cf. Table 1) | ID | SID | SID+ | SID++ |

## A-3 Definition of trust

Trust is a concept for modelling the conviction that a property is valid even if the validity cannot be proven in the individual case (it is therefore a belief that deduces and generalizes from the observable by means of fundamental trust). As a rule it would be too risky in the Industrie 4.0 context to blindly extrapolate trust in this form. Here, trust is to be achieved explicitly and on a fine-grained basis through a conviction arising from the successful verification that an individual security property (e.g. authenticity of a sender) is valid at a specific point in time. This trust must be motivated by knowledge of the selection and use of the technical/organisational protection measures and of the proofs of the quality of these measures.

Since it is not possible to verify all aspects of a security concept for each and every technical operation, a distinction must continue to be made between all relevant surrounding security features of the system and the individual local security feature. An explicit basis for trust is necessary for both categories. Examples of the first include environmental security (system) features such as overall security concepts with mode of operation and selection of technologies and countermeasures, taking standards, best practices, authorisations, etc. into account. In this case, everything - from process level to engineering, design and commissioning – is to be verified by means of an audit or evaluation.

The local security feature is the individual security feature that can be verified on an automated basis whenever a technical function or action is executed. This verification is conducted in, for example, the message receiver via the cryptographic verification of a signature which, when positive, confirms the integrity of the sender address and provides semantic proof for the authenticity of the message.

The proofs of quality and/or the checks measure current values and compare them with reference values. The required reference values for “good enough” are defined by a security guideline that also takes the time aspect (from what point on is a proof “out of date”?) into account. Today the reference values for “good enough” and “out of date” are usually specified on a company-specific basis. In order for it to be possible to repeatedly use a documented assurance level on a cross-organisation basis, the guideline has to be incorporated and verification requirements must be established in an overarching security context.

In the example here, the combination of integrated and local assessment means that the measures used are suitable in principle and have been implemented with sufficient quality, in other words, comply with the guideline (e.g. PKI signature with private keys that are always managed in hardware security modules). Based on this, it means that the recipient uses signature verification to cryptographically check the authenticity of the sender data of every message. Coupling this with the message content via a hash function makes it possible to check the authenticity and integrity of the entire message.

This local check thus implicitly trusts many other security features of the overall system, such as the confidentiality of the private key; in other words, it trusts that the private key is available only to the authorised user/system component/sender for generating the signature. Only the local property can be automatically checked using cryptographic signature verification. When however there are no suitable controls (e.g. lack of a four-eyes procedure when keys are generated), the private key for generating signatures is compromised (e.g. insider attack). In this case an attacker could generate on an unauthorised basis formally correct signatures that would pass the local signature verification. This breach of security cannot be recognised locally. The local check therefore requires as a foundation the verified confidence in the surrounding security properties.

In the multi-level process outlined here, trust in the security property/properties ultimately expresses on the basis of the trust in the surrounding security properties the reasonable expectation that all attacks on the protected security property which were taken into account in the security design would entail so much effort that a successful attack would be unlikely.

Looking at PKI structures which are often used to manage identities, the Technical Guideline BSI-TR-03145 for certification authorities with the security level 'high' describes the appropriate (organisational and technical) measures (also with regard to documentation) that are needed for ensuring an adequate level of trust.

## A-4 Literature regarding relevant standards and norms

In addition to the ISO standards

- Identity management framework (ISO/IEC 24760),
- Entity authentication assurance framework (ISO/IEC 29115),
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191),
- Access management framework (ISO/IEC 29146, in progress),
- Identity proofing (ISO/IEC 29003, in progress), referred to in this paper, there are further publications, a few of which should be mentioned here. The document "Kompass der IT-Sicherheit"[8] from DIN and Bitkom offers a much more extensive compilation.

### BSI TR-03126 Secure RFID use[9]

The use of RFID technologies is examined in different scenarios. The documents can serve as guidance for asset owners, manufacturers and integrators in order to ensure surefooted implementation.

### Privacy Impact Assessment Guideline for RFID Applications[10]

Observations are made concerning the secure use of RFID which is in compliance with data protection law. The documents can serve as guidance for asset owners, manufacturers and integrators in order to ensure surefooted implementation.

### DIN SPEC 16599 (prestandard) Information technology – Automatic identification and data capture techniques – Traceability

Traceability is very important in connection with strategic decisions that have an influence on product and process developments in companies. The recommendations in this prestandard point out ways for implementing tracking and tracing systems on the basis of existing standard modules and thereby close a gap between technology and application. It describes the unique identification for applications for the local and overarching traceability of objects (e.g. raw materials, products, containers) over entire life cycles.

[8] https://www.bitkom.org/Publikationen/2014/Leitfaden/Kompass-IT-Sicherheitsstandards/140311-Kompass-der-IT-Sicherheitsstandards.pdf

[9] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03126/index_htm.html

[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1

### DIN SPEC 16589 (prestandard) Information Technology — Automatic Identification and Data Capture – Product to Internet Communication – Pointer to Process

Developed through the INS funding project Innovation with Norms and Standards, DIN SPEC 16589 opens up a simplified solution for automatically linking a product or object with the internet or an intranet. The Pointer to Process (P2P) solution links the unambiguous identification which is needed for logistics with processes that are triggered or executed over networks. For this purpose, an ISO-standardised data carrier is used as an optical Data Matrix or RFID transponder, such as an electronic identification plate as defined by DIN 66277. The object ID of the identification plate leads to a source via the internet at the same time. This can trigger automatic processes along the lines of the Internet of Things autonomously and without any external services. This constitutes an element of Industrie 4.0 since it is possible for an object to communicate directly via the data carrier with control systems. DIN SPEC 16589 “P2P” can thus be used for automated maintenance and fault clearance services where the P2P object code connects via a smart phone to the computer on which worker management processes and information and documentation processes are executed. The automatic communication which is initiated during automatic and manual scans enables very precise documentation, control and tracing of processes and operations.

**AUTHORS OF THE WORKING GROUP ON THE SECURITY OF NETWORKED SYSTEMS:**

Dr. Lutz Jänicke, PHOENIX CONTACT Cyber Security AG | Michael Jochem (Leitung), Bosch Rexroth AG | Hartmut Kaiser, secunet Security Networks AG | Dr. Wolfgang Klasen, Siemens AG | Martin Klimke, Infineon Technologies AG | Dr. Bernd Kosch, Fujitsu Technology Solutions GmbH | Lukas Linke, ZVEI e.V. | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Torsten Nitschke, PHOENIX CONTACT Software GmbH | Michael Sandner, Volkswagen AG | Mario Stoltz, NXP Semiconductors Germany GmbH | Thomas Walloschke, Fujitsu Technology Solutions GmbH | Steffen Zimmermann, VDMA e.V.

This publication is a result of the work of the Working Group on the Security of Networked Systems (Industrie 4.0 Platform).

www.plattform-i40.de