SECURWARE 2024, November 03-07, 2024 – Nice, France

Device Onboarding Transparency – Supporting Initial Trust Establishment

Steffen Fries, Dr. Rainer Falk

Siemens AG, Foundational Technologies

SIEMENS

Authors' background:
Applied industrial research at Siemens Foundational Technologies

Cybersecurity for Industrial Systems

- Industrial systems need a security design that address the relevant security objectives and respect side conditions for the specific environment (e.g., lifetime, real-time, functional safety, usability).
- The industrial security standard IEC 62443 as "what" standard is applied in different verticals. The responsibilities of the different roles (system operator, integrator, component manufacturer) are distinguished.
- Based on that, "how" standards can be developed to enable interoperable integration of product or system features.

Dr. Rainer Falk
Principal Key Expert
Siemens
Foundational
Technologies

Steffen Fries
Principal Key Expert
Siemens
Foundational
Technologies

Security must be (continuously) adapted to the changing threat and vulnerability landscape

1950s – 1960s
Military, governments and other organizations implement computer systems

1980s
Computers make their way into schools, homes, business and industry

1999
The globe is connected by the internet

2010s
Cloud computing enters the mainstream

2020s
Internet of Things, Smart and autonomous systems, Artificial Intelligence, Big Data

Digital Information Processing

Digital Connectivity

Digital Automation and Artificial Intelligence

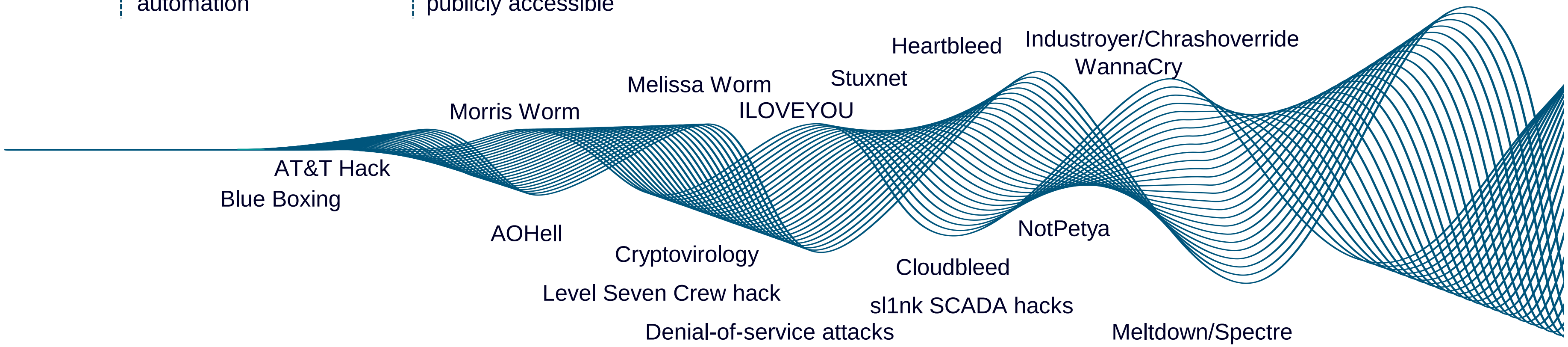
1970s
Home computer is introduced

1990s
Digital enhancement of electrification and automation

1991
The World Wide Web becomes publicly accessible

2000s
Mobile flexibility

2020s
Industry 4.0



Adherence to regulative and standard requirements need oversight on the system security state

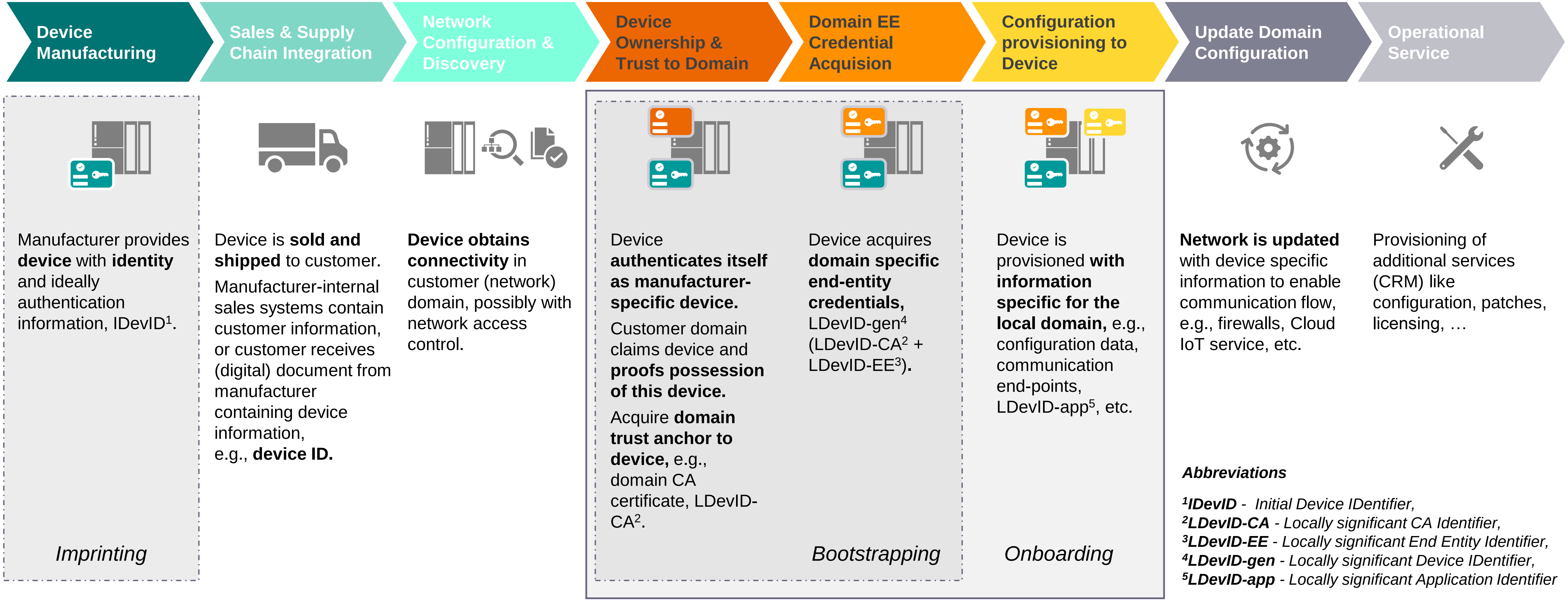
- Regulative requirements like the NIS2 Directive for operators, or the upcoming EU CRA for manufacturers require security measures to ensure operation of services and (critical) infrastructures.
- Security requirements, ranging from the product development process incl. security functionality of components and further to the overall system integration and operation, are specified in the standard IEC 62443.
- Monitoring and evaluating system security state during operation enables the identification of potentially weak points in a system and helps identifying root causes after an attack.
- Information that supports adherence to an operator's security policy and forensic analysis in the aftermath of a security event typically comprise operational (security) data.

⚠ The system security state depends also on how components were provisioned and onboarded into the operational environment.

- The proposed provisioning extension enhances manufacturer-provided certificates to support an optimized onboarding, including the registration of the provisioning into an onboarding transparency log.

Zero-Touch Onboarding of IoT/OT Components

Automated mutual trust establishment in customer site networks starts in production


Device Manufacturing
Sales & Supply Chain Integration
Network Configuration & Discovery
Device Ownership & Trust to Domain
Domain EE Credential Acquision
Configuration provisioning to Device
Update Domain Configuration
Operational Service
Imprinting
Bootstrapping
Onboarding

Device Manufacturing: Manufacturer provides **device** with **identity** and ideally authentication information, IDevID[1].

Sales & Supply Chain Integration: Device is **sold and shipped** to customer.

Manufacturer-internal sales systems contain customer information, or customer receives (digital) document from manufacturer containing device information, e.g., **device ID.**

Network Configuration & Discovery: **Device obtains connectivity** in customer (network) domain, possibly with network access control.

Device Ownership & Trust to Domain: Device **authenticates itself as manufacturer-specific device.**

Customer domain claims device and **proofs possession of this device.**

Acquire **domain trust anchor to device,** e.g., domain CA certificate, LDevID-CA[2].

Domain EE Credential Acquision: Device acquires **domain specific end-entity credentials,** LDevID-gen[4] (LDevID-CA[2] + LDevID-EE[3]).

Configuration provisioning to Device: Device is provisioned **with information specific for the local domain,** e.g., configuration data, communication end-points, LDevID-app[5], etc.

Update Domain Configuration: **Network is updated** with device specific information to enable communication flow, e.g., firewalls, Cloud IoT service, etc.

Operational Service: Provisioning of additional services (CRM) like configuration, patches, licensing, …

Imprinting | *Bootstrapping* | *Onboarding*

Analogy

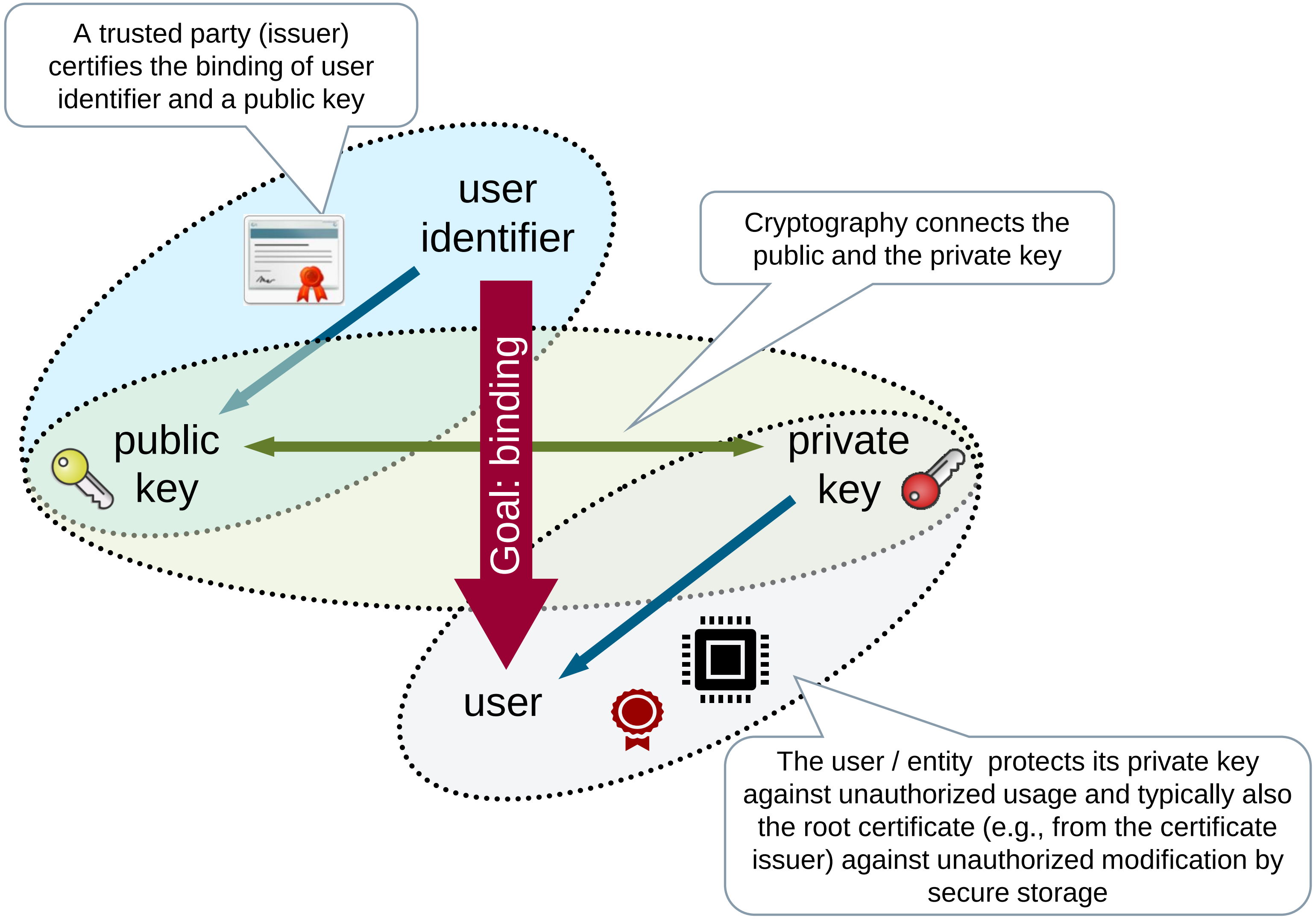
“Birth Record” | “Passport Request” | “Passport” | “Drivers License”

Abbreviations

[1] ***IDevID*** - *Initial Device IDentifier,*
[2] ***LDevID-CA*** - *Locally significant CA Identifier,*
[3] ***LDevID-EE*** - *Locally significant End Entity Identifier,*
[4] ***LDevID-gen*** - *Locally significant Device IDentifier,*
[5] ***LDevID-app*** - *Locally significant Application Identifier*

X.509 Certificates bind user identities and cryptographic keys

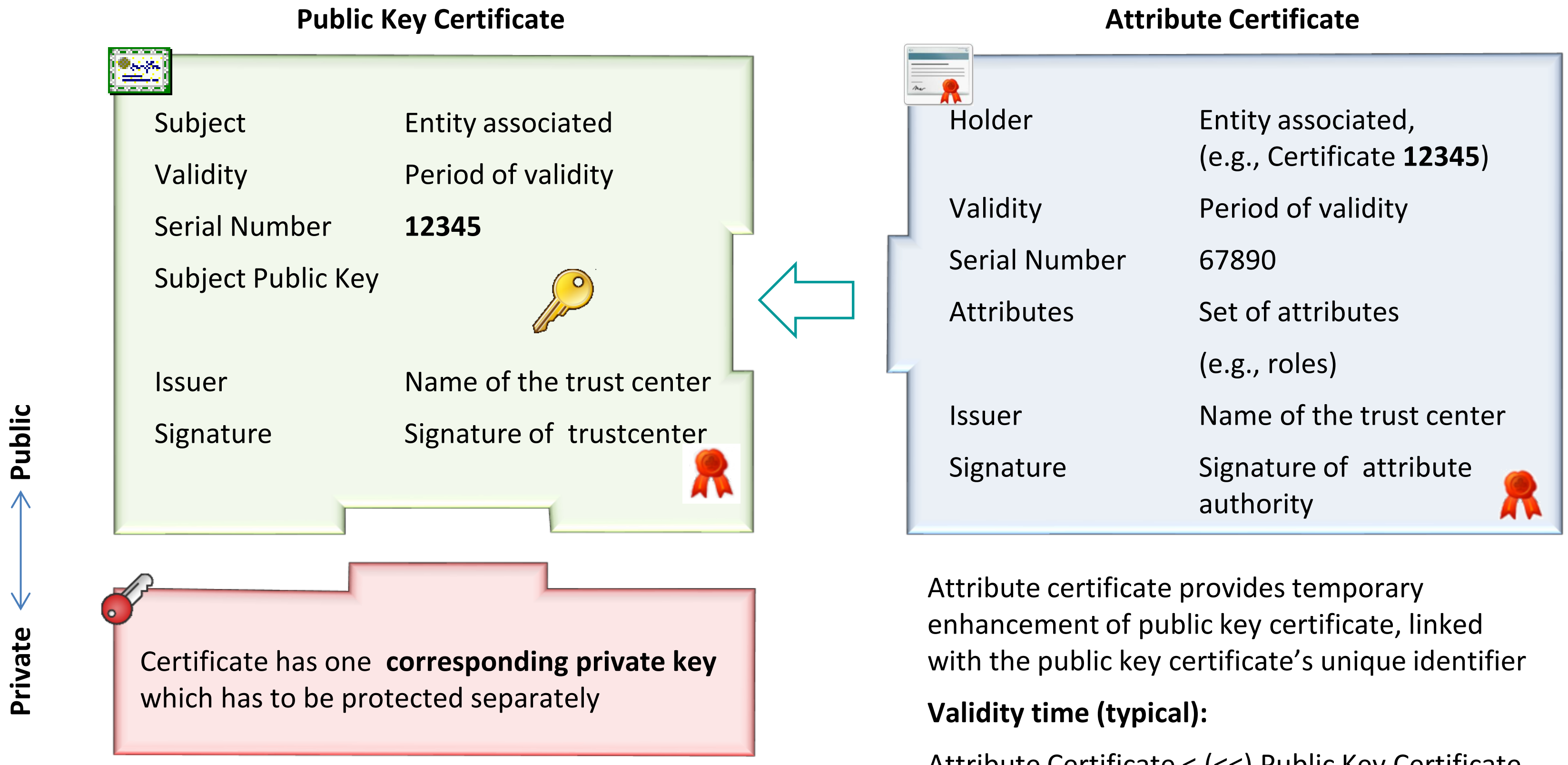
Support of user and device authentication


A trusted party (issuer) certifies the binding of user identifier and a public key
user identifier
Cryptography connects the public and the private key
public key
private key
Goal: binding
user
The user / entity protects its private key against unauthorized usage and typically also the root certificate (e.g., from the certificate issuer) against unauthorized modification by secure storage

- A public key certificate binds the identity of the subject (user, device) to a public key. The subject possesses also the corresponding private key. The certificate is issued by a trusted third party, allowing validation of the certificate.
- Such a certificate has typically a restricted lifetime, and it may be revoked by the issuer during that time, e.g., in case of key compromise.
- Credentials in terms of certificates and corresponding private keys, as well as the managing infrastructure are standardized in ITU-T X.509 | ISO/IEC 9594-8.
- An internet profile for X.509 was defined by the IETF as RFC 5280.

Public Key Certificates and Attribute Certificates
Standardized data structures in ITU-T X.509

- A **Public Key Certificate** may be compared to an ID card, enabling to authenticate to another person or entity.
- An **Attribute Certificate** may be seen as temporary enhancement of a public key certificate, and may be compared to a visa, for which the possession of the ID card is necessary to show that the visa can be used legitimately.



Public Key Certificate

Subject	Entity associated
Validity	Period of validity
Serial Number	**12345**
Subject Public Key	
Issuer	Name of the trust center
Signature	Signature of trustcenter

Certificate has one **corresponding private key** which has to be protected separately

Attribute Certificate

Holder	Entity associated, (e.g., Certificate **12345**)
Validity	Period of validity
Serial Number	67890
Attributes	Set of attributes (e.g., roles)
Issuer	Name of the trust center
Signature	Signature of attribute authority

Attribute certificate provides temporary enhancement of public key certificate, linked with the public key certificate’s unique identifier

Validity time (typical):

Attribute Certificate < (<<) Public Key Certificate

SIEMENS

Supporting onboarding transparency in certificates using X.509 extensions
Proposed transparency extension

- ITU-T X.509 defines ASN.1 structures for public key certificates and attribute certificates
- Both types of certificates are extendable, which allows to convey additional information
- An extension to convey the supported provisioning or onboarding methods for a device certificate can be defined as:

Transparency Extension

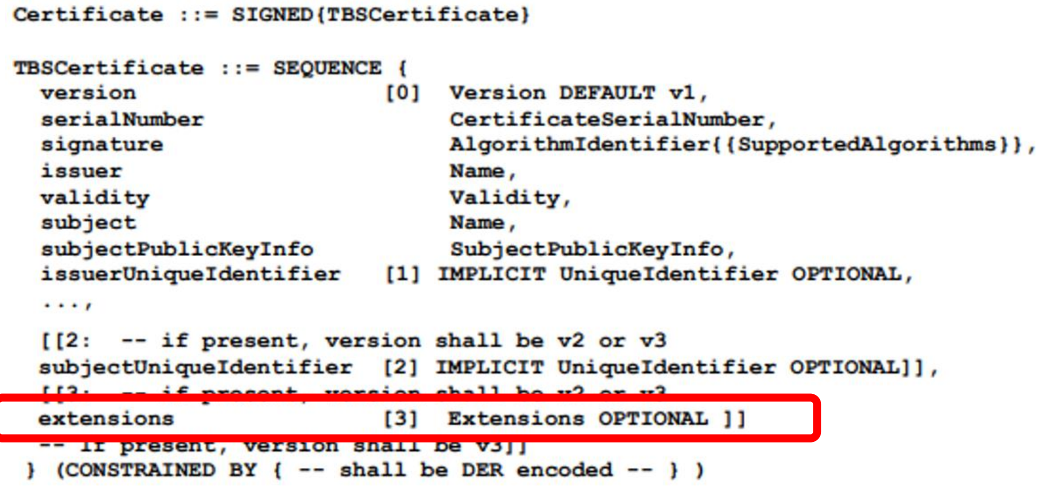
```
supportedProvisioningMethods EXTENSION ::= {
  SYNTAX SupportedProvisioningMethods
  IDENTIFIED BY id-ce-SupportedProvisioningMethods }

SupportedProvisioningMethods ::= ProvisioningDescription {{ ProvisioningMethod }}

ProvisioningMethod::= SEQUENCE {
  provisioningMethod     Name,
  provisiningId          OBJECT IDENTIFIER OPTIONAL,
  provisioningVersion    integer OPTIONAL
}

ProvisioningMethod ::= {
  CMP, SCEP, EST, CMC, ACME, FDO, OMA-DM, OPC-UA-P21,BRSKI, SZTP, …}
```

X.509 Public key certificate – ASN.1 definition



```
Certificate ::= SIGNED{TBSCertificate}

TBSCertificate ::= SEQUENCE {
  version                    [0]  Version DEFAULT v1,
  serialNumber                    CertificateSerialNumber,
  signature                       AlgorithmIdentifier{{SupportedAlgorithms}},
  issuer                          Name,
  validity                        Validity,
  subject                         Name,
  subjectPublicKeyInfo            SubjectPublicKeyInfo,
  issuerUniqueIdentifier     [1] IMPLICIT UniqueIdentifier OPTIONAL,
  ...,
  [[2:  -- if present, version shall be v2 or v3
  subjectUniqueIdentifier   [2] IMPLICIT UniqueIdentifier OPTIONAL]],
  [[3:  -- if present, version shall be v2 or v3
  extensions                 [3]  Extensions OPTIONAL ]]
  -- if present, version shall be v3]]
 } (CONSTRAINED BY { -- shall be DER encoded -- } )
```

Contained information allows to state supported provisioning methods of a device, e.g.:

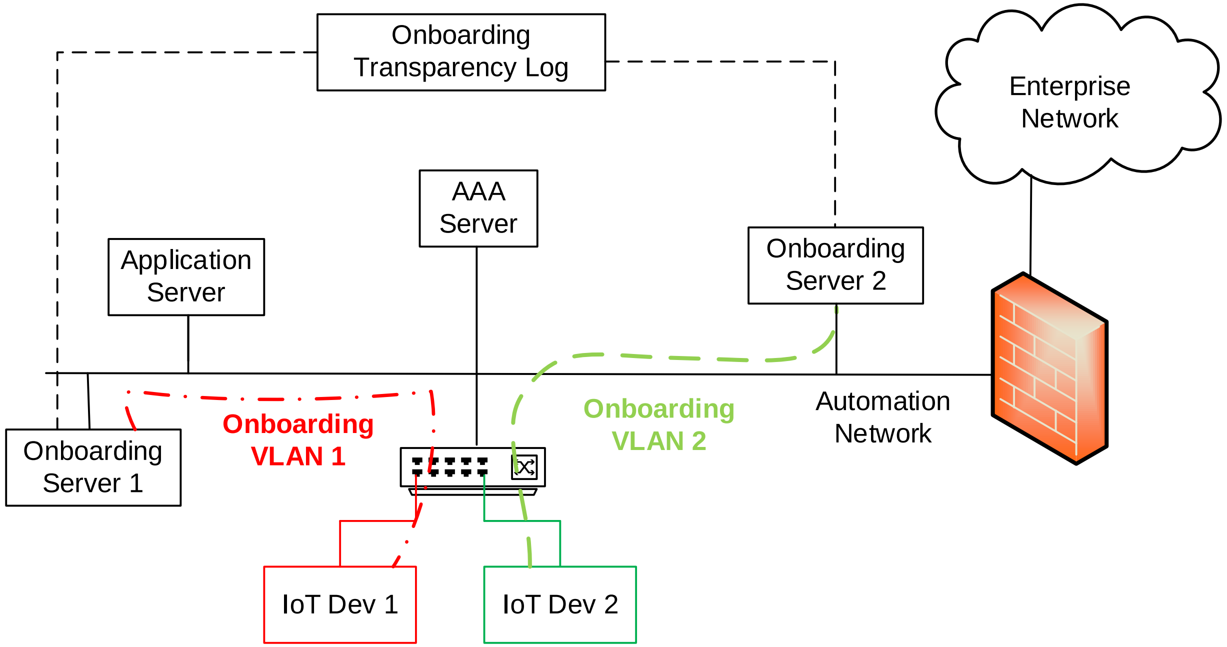
`ProvisioningMethod ::= {EST, BRSKI}`

Meaning: Device supports BRSKI for onboarding and EST for certificate management.

Supporting onboarding transparency in certificates using X.509 extensions

Usage of transparency extension during onboarding

- Initial manufacturer-provided X.509 certificate (IDevID) carries information about supported provisioning methods
- The supported provisioning method in the device IDevID certificate support selection of the appropriate infrastructure component and communication path may during device onboarding in the operational environment.
- Logging the used provisioning method in an onboarding transparency log supports root cause analysis in the aftermath of a security event.



As a side note: Security has to be suitable for the addressed environment

Awareness and Acceptance

Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along easily with this system wide functionality.

The proposed migration approach targets this incorporation already in existing structures.

In addition, it needs, especially for automation environments, actions for:

- awareness trainings
- help people to understand security measures and processes
- provide user-friendly interfaces and processes

SIEMENS

Summary & Outlook

- Cybersecurity includes preventing, detecting, and reacting to cyber-security attacks.
- Cybersecurity is addressed by regulation and standards
- Introducing new components into an operational environment is the first step to be monitored
- Proposed enhancements to X.509 certificates allow to
  - provide support for the selection of an appropriate provisioning methods, and to
  - support monitoring of onboarding using an onboarding transparency log.
- This approach improves the onboarding and forensic analysis in case of a security event
- Future work includes a proof-of-concept implementation of the proposed approach.

Contact

Steffen Fries
Principal Key Expert

E-mail steffen.fries@siemens.com

FT RPD CST
Otto-Hahn-Ring 6
81739 Munich
Germany

Siemens Cyber Security

Dr. Rainer Falk
Principal Key Expert

E-mail rainer.falk@siemens.com

FT RPD CST
Otto-Hahn-Ring 6
81739 Munich
Germany

Siemens Cyber Security

Information

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Security note

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic Industrial Security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art Industrial Security concept. Third-party products that may be in use should also be considered. For more information on Industrial Security, visit:

siemens.com/industrial-security

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit

support.automation.siemens.com