ICSNC 2023, November 13-17, 2023 - Valencia, Spain

Using Attribute Certificates to Support Cryptographic Algorithm Flexibility

Steffen Fries, Dr. Rainer Falk,
Siemens AG, Technology

Authors' background: Applied industrial research at Siemens Technology

Cyber Security 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 Technology

Steffen Fries
Principal Key Expert
Siemens Technology

SIEMENS

Security must be (continuously) adopted 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

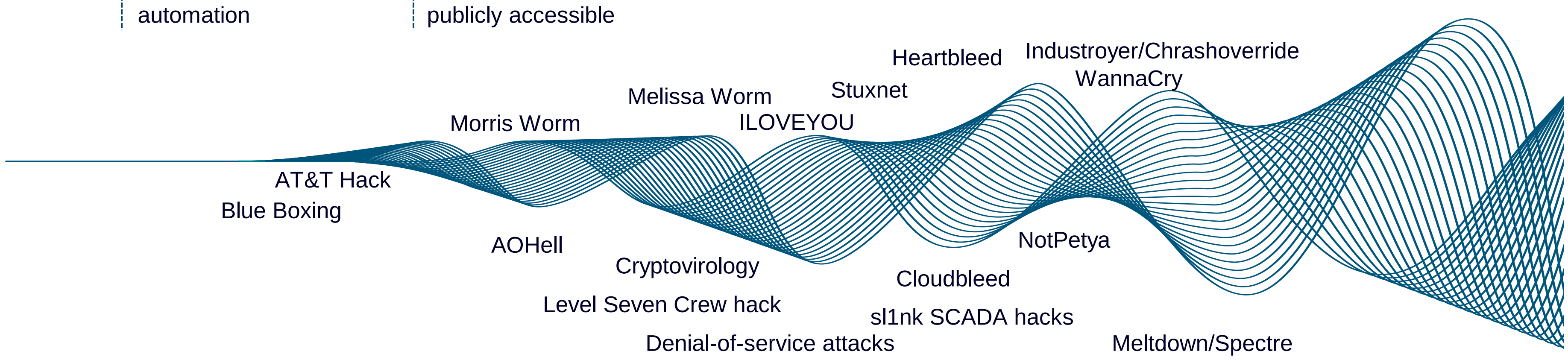
1970s
Home computer is introduced

1990s
Digital enhancement of electrification and automation

1991
The World Wide Web becomes publicly accessible

2000s
Mobile flexibility

2020s
Industry 4.0



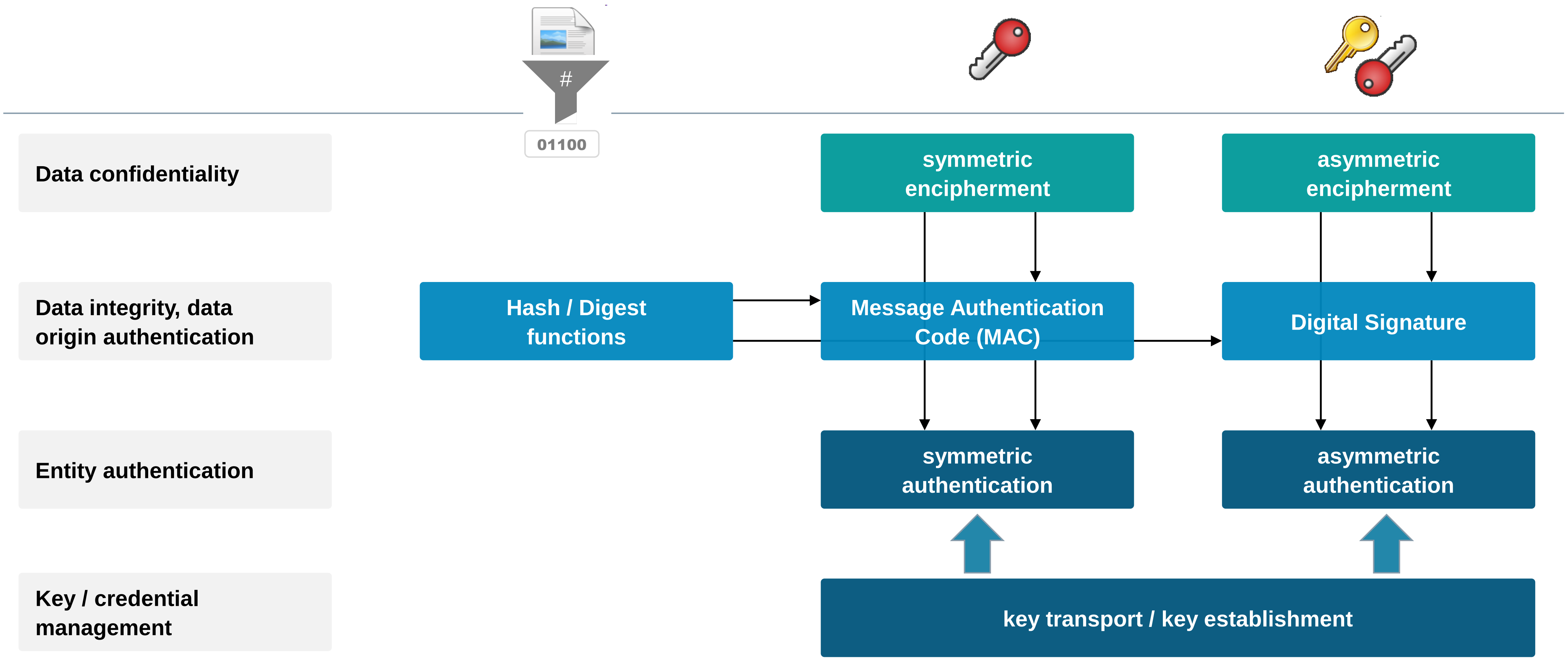
SIEMENS

Advances in cryptography demand for crypto agility

- Recommendations on strong cryptographic algorithms are updated over time (e.g., NIST, BSI, ANSSI)
- Examples from the past show that advances in breaking cryptography rendered certain cryptographic algorithms weak. Therefore they need to be replaced. Examples are RC4, DES, MD5, SHA1.
- Recent development in the area of quantum computers will endanger today’s utilizes cryptographic algorithms. Quantum computers could become very efficient to solve certain mathematical problems that are the basis of common today’s crypto algorithms:

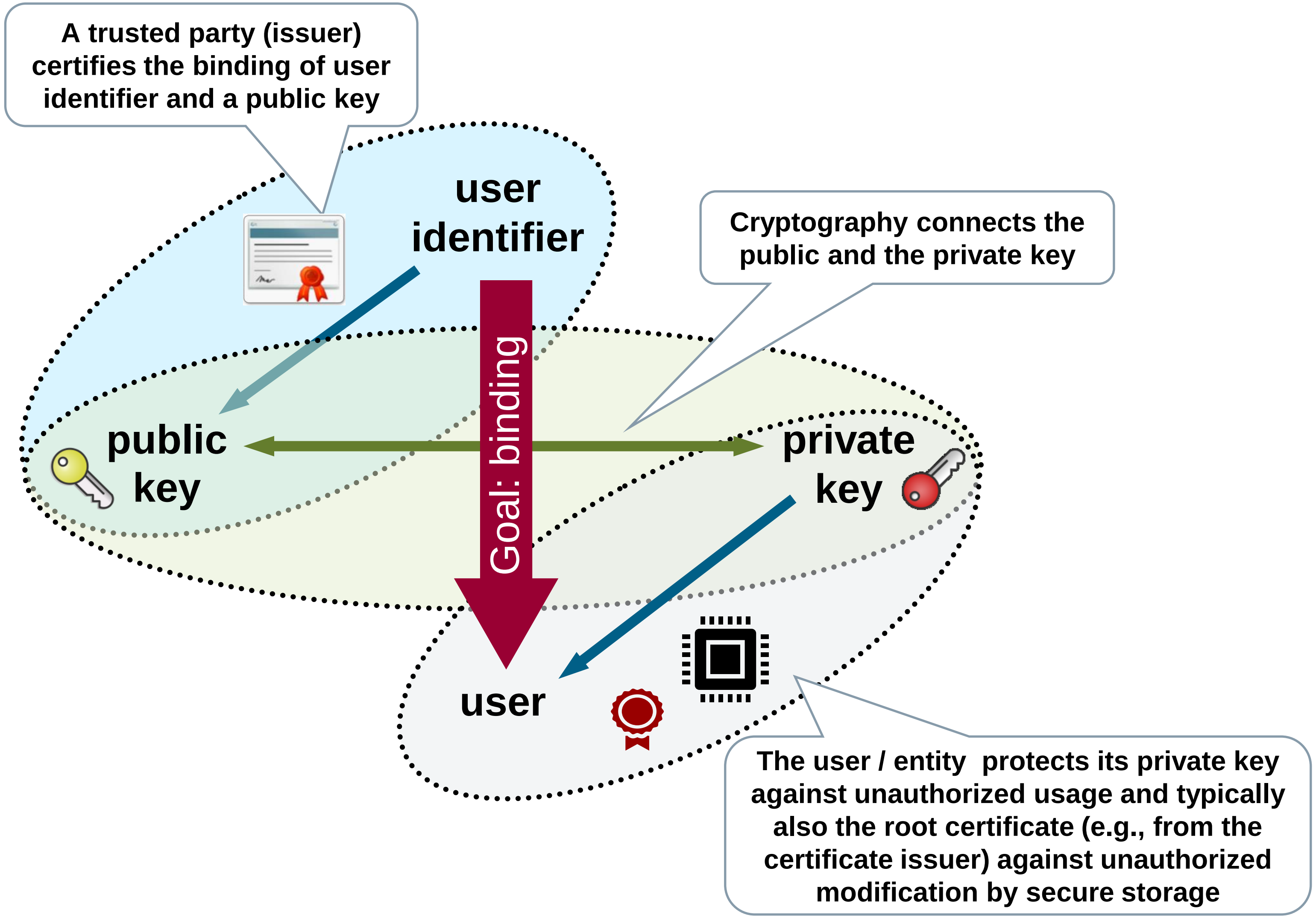
  - Asymmetric cryptographic algorithms like RSA (Rivest, Shamir, Adleman) or ECDSA (Elliptic Curve Digital Signature Algorithm), and also key agreement schemes like Diffie Hellman through effective factorization and solving discrete logarithm problems leveraging Shor’s algorithm
  - Symmetric cryptographic algorithms like AES by applying can also be attacked using Grover’s algorithm
- While the solution for symmetric cryptographic algorithms is to double the key length, asymmetric cryptographic algorithms need to be replaced.

Application of cryptographic techniques to protect data at rest and data in transit



SIEMENS

Certificates bind user identities and cryptographic keys

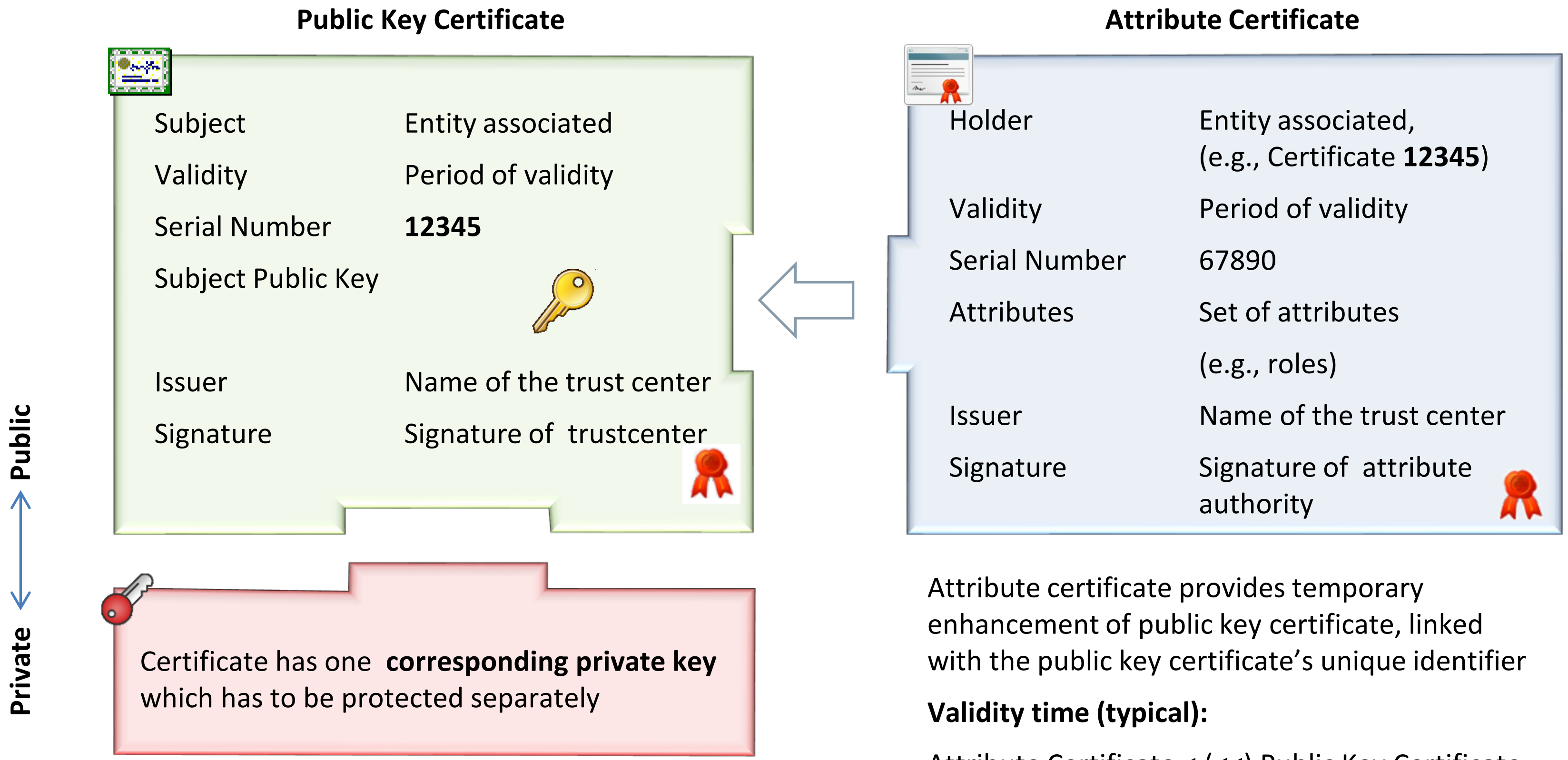


- A public key certificate binds the identity of the owner (user) to a public key. The owner also possesses the corresponding private key. The certificate is issued by a trusted third party allowing validation of the certificate.
- Such a certificate has typically a restricted lifetime, and it may be 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 in X.509 | ISO/IEC 9594-8.
- An internet profile for X.509 was published by the IETF as RFC 5280.

SIEMENS

Public Key Certificates and Attribute Certificates are data structures standardized 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.



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 migration of asymmetric cryptographic algorithms in certificates using X.509 extensions

- ITU-T X.509 defines the ASN.1 structures for public key certificates and attribute certificates
- Both types of certificates are extendable, which allows to convey additional information
- X.509 already defines additional extensions to support alternative cryptographic algorithms for public key certificates and attribute certificates:
  - `subjectAltPublicKeyInfo` – contains an alternative public key
  - `altSignatureAlgorithm` – contains an alternative signature algorithm (used to sign the public key certificate) and
  - `altSignatureValue` – contains the actual alternative signature value.
- Note that the usage of the `subjectAltPublicKeyInfo` extension is not foreseen in attribute certificates

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 -- } )
```

X.509 Public attribute certificate – ASN.1 definition

```
AttributeCertificate ::= SIGNED{TBSAttributeCertificate}

TBSAttributeCertificate ::= SEQUENCE {
  version                 AttCertVersion, -- version is v2
  holder                  Holder,
  issuer                  AttCertIssuer,
  signature               AlgorithmIdentifier{{SupportedAlgorithms}},
  serialNumber            CertificateSerialNumber,
  attrCertValidityPeriod  AttCertValidityPeriod,
  attributes              SEQUENCE OF Attribute{{SupportedAttributes}},
  issuerUniqueID          UniqueIdentifier OPTIONAL,
  ...,

  extensions              OPTIONAL }
```


SIEMENS

Proposal 1:
Extend X.509 attribute certificates to transmit subject public key information

- Proposed is the usage of the already defined X.509 extensions to convey also the alternative subject public key together with the alternative cryptographic algorithms also in the context of attribute certificates
  - **`subjectAltPublicKeyInfo`**
  - `altSignatureAlgorithm`
  - `altSignatureValue`

X.509 Public attribute certificate – ASN.1 definition

```
AttributeCertificate ::= SIGNED{TBSAttributeCertificate}

TBSAttributeCertificate ::= SEQUENCE {
  version                 AttCertVersion, -- version is v2
  holder                  Holder,
  issuer                  AttCertIssuer,
  signature               AlgorithmIdentifier{{SupportedAlgorithms}},
  serialNumber            CertificateSerialNumber,
  attrCertValidityPeriod  AttCertValidityPeriod,
  attributes              SEQUENCE OF Attribute{{SupportedAttributes}},
  issuerUniqueID          UniqueIdentifier OPTIONAL,
  ...,
  ...,
  extensions              OPTIONAL }
```

- Benefits
  - Conveying the alternative public key in an attribute certificate easily allows to extend an already existing public key certificate with a new public key for the owner without issuing a new public key certificate. Based on the holder information, the connection to the original public key certificate can be done.
  - While this approach may be unusual, as the alternative public key is treated as attribute, it may ease the handling in the migration period to alternative cryptographic algorithms without the necessity to re-issue certificates immediately.

SIEMENS

Proposal 2:
Extend X.509 certificates to transmit key usage (transition) policy

- Migration to alternative cryptographic algorithms like post-quantum algorithms requires a transition policy as part of the overall security policy.
- It defines the transition from one cryptographic algorithm to an alternative cryptographic algorithm and may define the verification of
  - only one signature,
  - both signatures (classic and alternative), and

  may also provide a weight on the verification result, e.g., by the order of operations.
- The security policy is typically configured per relying party and may be part of the engineering data of devices.
- Alternative proposal
  - Specify transition policies as part of an additional extension of public key certificates or attribute certificates conveying alternative cryptographic algorithm information.
  - The transition policy extension `altCryptoPolicy` can be evaluated by the relying party and processed accordingly.

Proposed new extension – ASN.1 definition

```
altCryptoPolicy ::= SEQUENCE {
  combAND      [0] boolean OPTIONAL,
  combOR       [1] boolean OPTIONAL,
  weightOnAlt  [2] boolean OPTIONAL
}
```


SIEMENS

Summary & Outlook

- Transition from currently used classical cryptographic algorithms to new, alternative cryptographic algorithms is needed.
- Enhancements to existing X.509 certificates to support the transition towards alternative cryptographic algorithms.
  - Include public key information in an attribute certificate to ease the handling for adding new public keys for an user having already a public certificate.
  - Provide a transition policy that defines which public key or which combination of public keys is acceptable
- This approach allows to extend support for additional cryptographic algorithms by issuing further attribute certificates containing alternative public keys and associated security policy.
- Upcoming requirements to support post-quantum cryptographic algorithms can be addressed.
- Future work is a proof-of-concept implementation of the proposed approach.

SIEMENS

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

Contact

Steffen Fries
Principal Key Expert

E-mail steffen.fries@siemens.com

T CST
Otto-Hahn-Ring 6
81739 Munich
Germany

Siemens Cyber Security

Dr. Rainer Falk
Principal Key Expert

E-mail rainer.falk@siemens.com

T CST
Otto-Hahn-Ring 6
81739 Munich
Germany

Siemens Cyber Security

SIEMENS

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

SIEMENS