SECURWARE 2025, October 26-30, 2025 – Barcelona, Spain

Optimizing Certificate Validation in OT Environments

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

SIEMENS

Authors' background:
Applied industrial research and development at Siemens

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, like IEC 62351 for the power system industry, are developed to enable interoperability between different vendors products.

Dr. Rainer Falk
Principal Key Expert
Siemens Foundational Technologies

Steffen Fries
Principal Key Expert
Siemens Foundational Technologies

Andreas Güttinger
Senior Key Expert
Siemens Infrastructure

SIEMENS

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

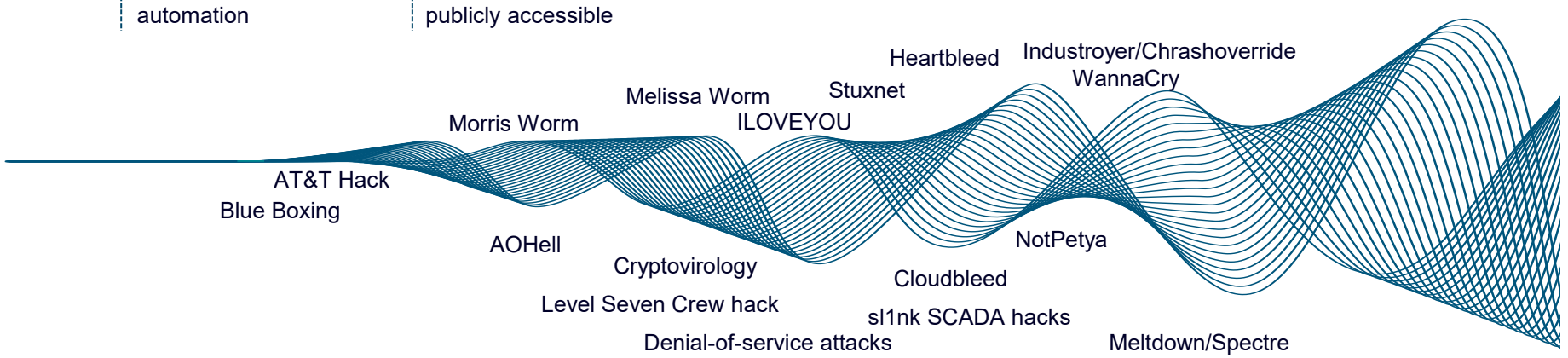
1970s
Home computer is introduced

1990s
Digital enhancement of electrification and automation

1991
The World Wide Web becomes publicly accessible

2000s
Mobile flexibility

2020s
Industry 4.0



SIEMENS

Compliance with regulative and standard requirements need oversight on the system security state, specifically considering the applied security credentials

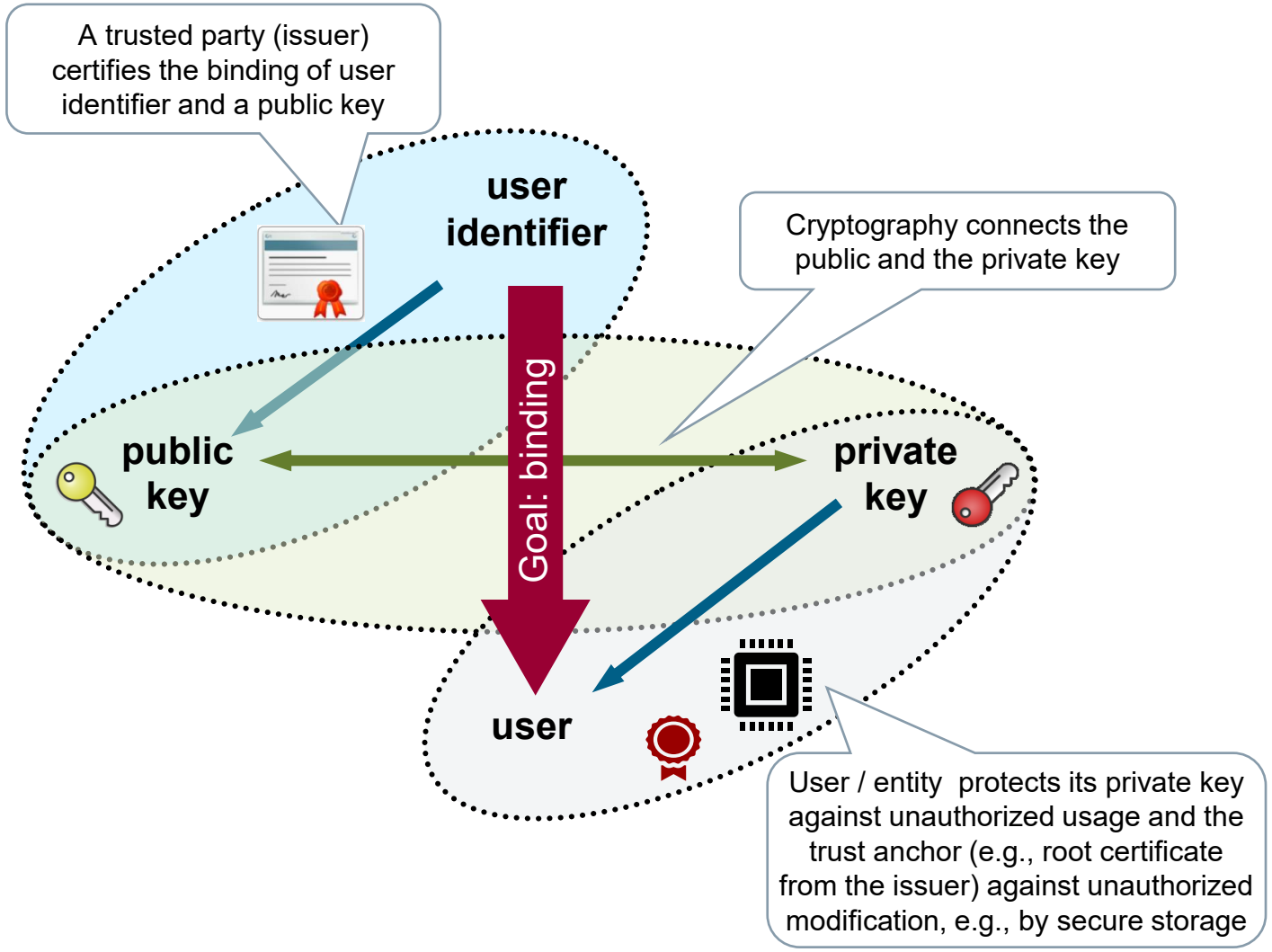
- Regulative requirements like the NIS2 Directive for operators, or the upcoming EU CRA for manufacturers / importers / distributors require security measures to ensure operation of services and (critical) infrastructures.
- Security requirements, ranging from the product development process incl. security 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 with security credentials, onboarded into the operational environment, and how the security credentials are maintained and verified during the operational lifecycle.

- A solution is necessary to take specifically constraint devices into account and to provide optimizations for the operational infrastructure. The proposed approach targets both aspects.

SIEMENS

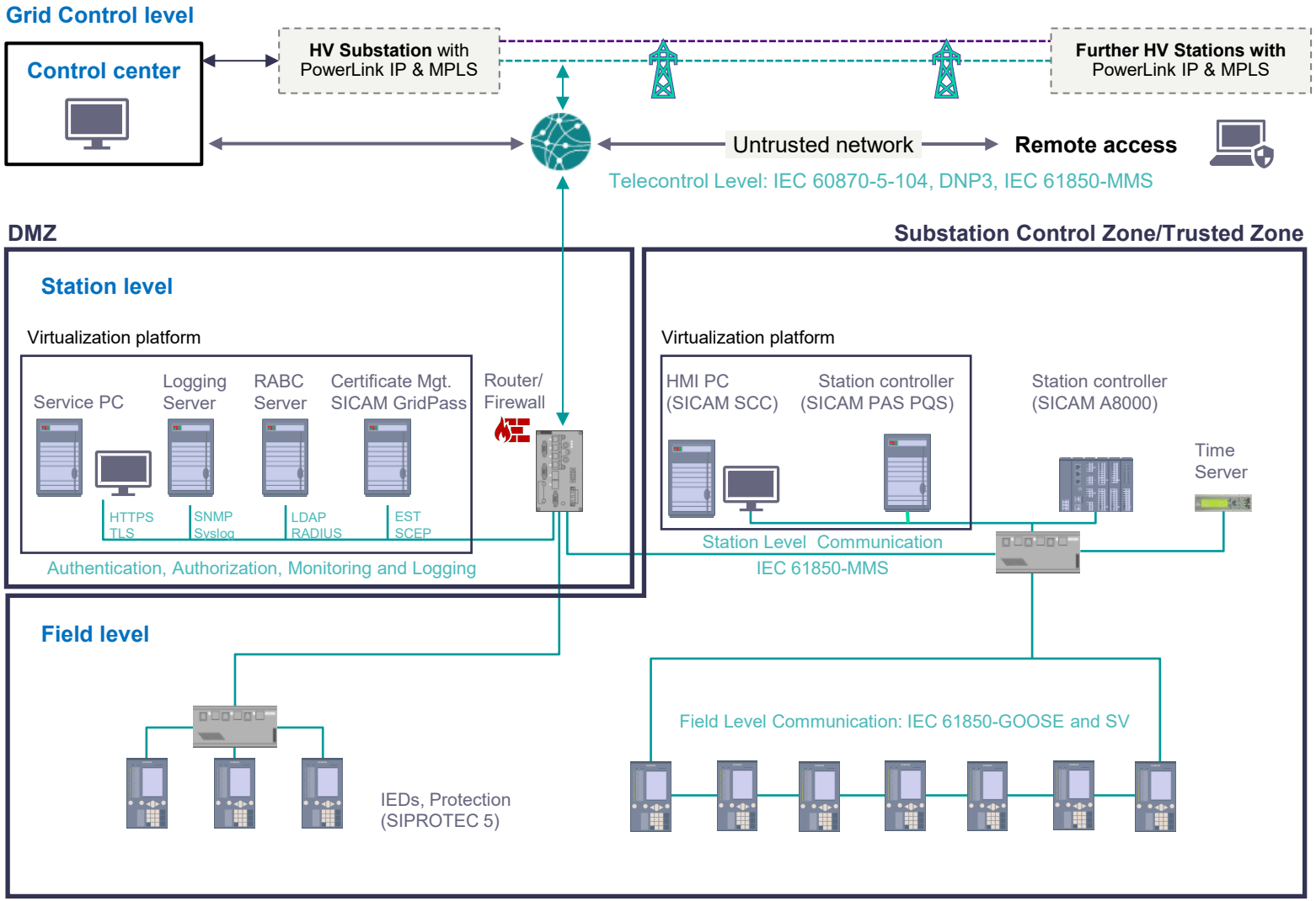
X.509 certificates bind user identities and cryptographic keys
Support of user and device authentication



- Public key certificate: binds 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 for validation using issuer information.
- Such a certificate has a restricted lifetime, and it may be revoked by the issuer during that time, e.g., in case of key compromise.
- Certificates are extensible and may be enhanced with further information.
- Certificates and requirements to the managing infrastructure are standardized in ITU-T X.509 | ISO/IEC 9594-8 and profiled, e.g., by the internet profile defined in IETF RFC 5280.

SIEMENS

Use case example: Cybersecurity in the power grid
Securing energy automation systems

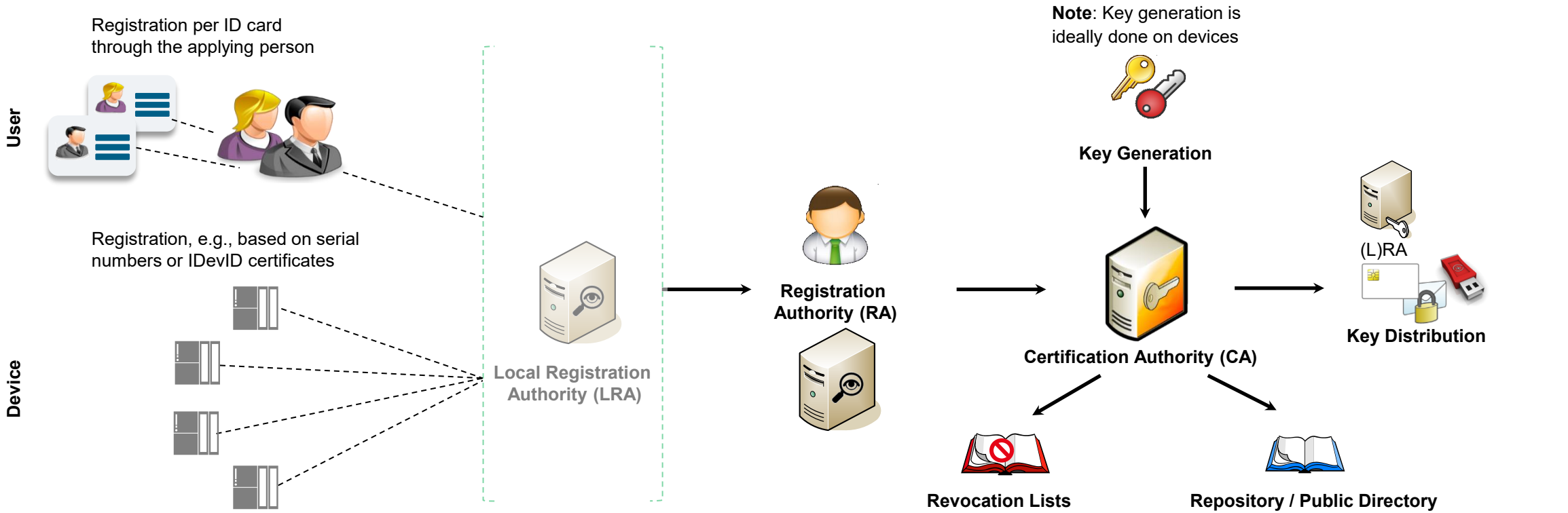


X.509 certificates are used in power system automation to

- Identify and authenticate logical and physical devices during communication establishment using domain specific protocols (e.g., IEC61850, IEC 60870-5-7)
- Identify and authenticate human users during local and remote system and component access
- Support role-based access control by utilizing respective extensions in X.509 certificates
- Ensure integrity of firmware or software updates.

SIEMENS

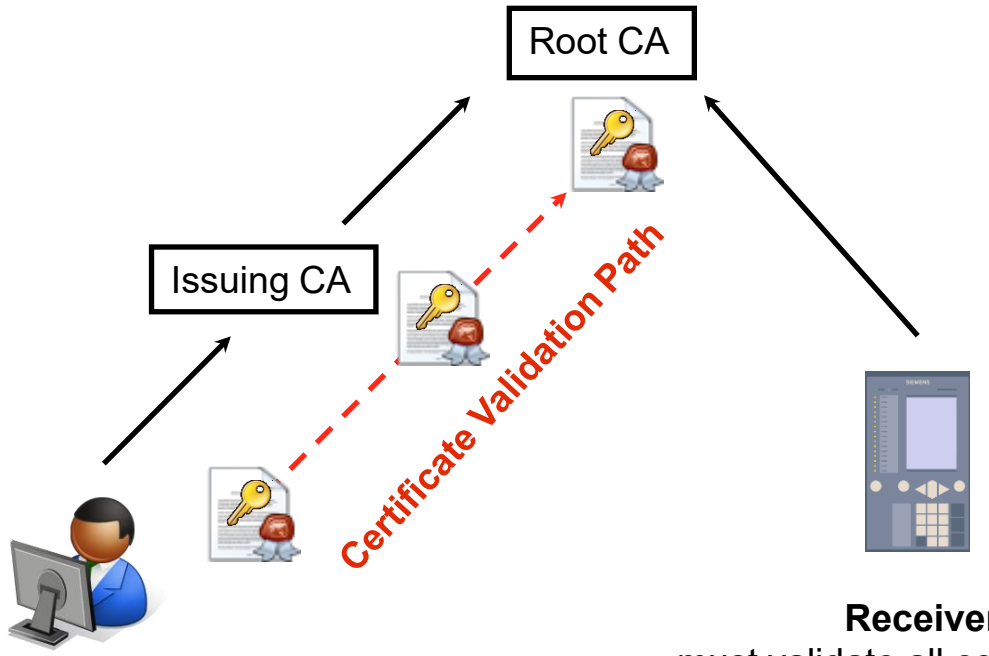
Maintenance of X.509 credentials is supported by a Public Key Infrastructure (PKI)



Realization examples	Enrollment	Revocation	Fetching
	• manual • automated (**SCEP, EST,** CMP, CMC)	• manual (CRL) • automated (**CRL, OCSP**, **SCVP**) **Focus of proposed enhancement**	• manual (configuration) • automated (LDAP, HTTP)

SIEMENS

Challenge: Handle X.509 certificate validation on constraint devices



- Validation of X.509 end entity certificate contains at least the check of the
  - Validity period (from, to)
  - Subject and subject alternative name against expected names
  - Signature of the issuer
  - Contained key usages
  - Potential further extensions contained in the certificate (e.g., authorization)
  - Revocation state of the certificate
- Validation of issuing CA certificates along the certification chain up to a common trust anchor
- Depending on the certificate chain length, this involves the validation of multiple certificates and potentially communication to retrieve revocation information.
- This may be a burden for constrained devices.

SIEMENS

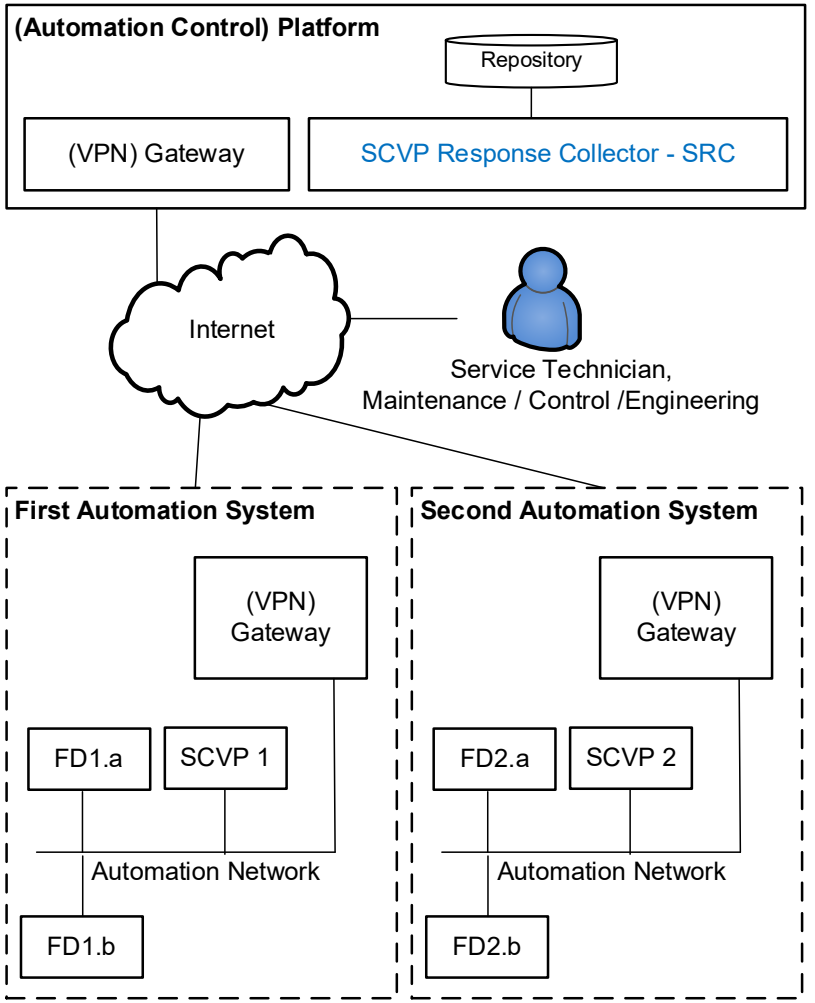
Known approaches for handling / optimizing X.509 certificate validation

Mechanism / Properties	Certificate Revocation Lists (CRL)	Caching of Revocation Information	Online Certificate Status Protocol (OCSP)	OCSP Stapling	Server Certificate Validation Protocol (SCVP)	Certificate Authorization Validation Lists (CertAVL)	DNS-based Authentication of Named Entities
Standard	ITU-T X.509, IETF RFC 5280		IETF RFC 6960	IETF RFC 6066, IETF RFC 6961	IETF RFC 5055	ITU-T X.509, IEC 62351-9	IETF RFC 6698
Overview	• Relying party queries CRL distribution point for revocation information regarding issued certificates • Distribution point contained in certificate	• Common practice to avoid fetching fresh CRLs whenever a certificate is received and validated • CRLs contain information about CRL issue time and when the next update will be provided.	• Relying party queries the revocation state of single or set of certificates from OCSP responder • Lifts handling of complete CRLs from the clients • Distribution point contained in certificate	• Known in the context of TLS • Allows peer to provide OCSP response inbound • Avoids relying party to interact with OCSP responder • Available as extension in the TLS handshake for single or multiple certificates	• Delegates the certificate validation to central authority • Includes handling of certification path including revocation states	• Constitute allow lists, which explicitly provide information about certificates considered trustworthy • Offload revocation handling to the central point creating the CertAVL	• Enables to specify keys or certificates used by TLS servers as DANE TLSA resource record. • Authoritative binding between domain name and certificate used by TLS server in that domain.
Side conditions	• Requires online connection at least once a day	• Emergency updates in CRL validity period not recognized	• Needs online connectivity to OCSP responder during query	• Limited to TLS or DTLS	• Needs online connectivity to SCVP server during query	• Managed by system operator, not by issuing CA	• Relying party trusts name and certificate information from DNS

SIEMENS

Proposed solution: SCVP response collector

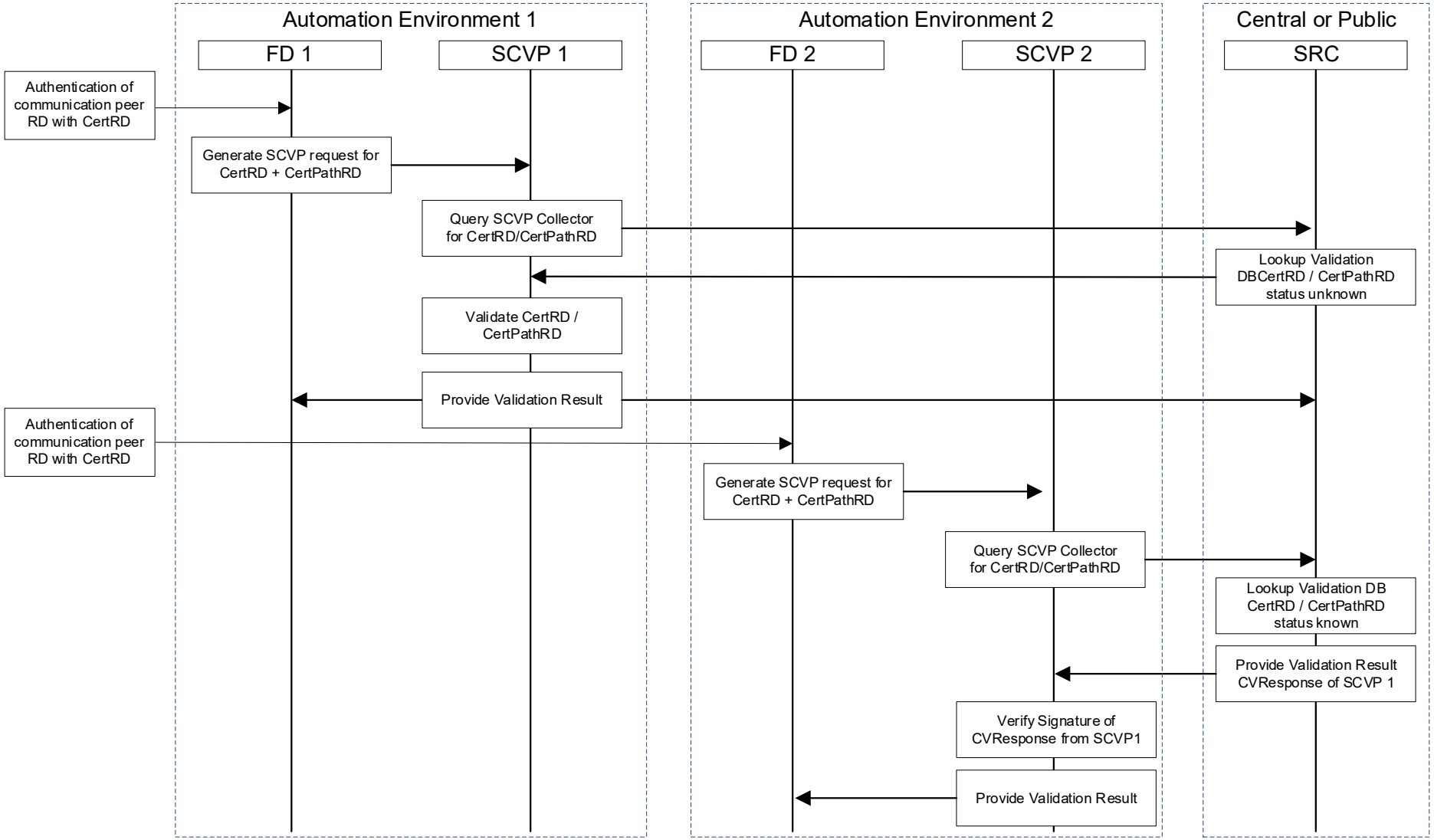
- SCVP client sends request containing the certificate to be validated including specific verifications to be done.
- Validation result will be provided to the requesting client, which verifies only the SCVP server's signed response.
- **Enhancement of SCVP server:** Result of a certificate validation or certificate chain validation is provided to SCVP Response Collector (SRC). Reduces response time for client queries for the same certificate or certificate chain.
- Publication of validation result information (certificate and/or the certificate chain) by SRC may be done, e.g., via:
  - public directory (e.g., LDAP, HTTP, FTP, ...),
  - hash chain-based ledger technology (e.g., Ethereum, Hyperledger).
- Choice of realization specifically for a chosen ledger technology may have influence on validation effort for both, infrastructure and requesting client.
- Security policy of the organization may need to consider that caching of validation results provides an optimization but also requires further consideration like the storage duration of validation results to ensure it matches freshness requirements.



SIEMENS

Proposed solution: Detailed call flow

- Interaction between
  - SCVP clients on FD
  - local SCVP server
  - central SCVP response collector.
- Case shown utilizes an available response from the SRC to forward to requesting client.
- Not shown: Depending on SCVP2 security policy, server may perform an own certificate validation, if the SRC answer is not considered fresh.



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

Summary & Outlook

- Cybersecurity is increasingly required by regulation and standards, targeting technical product features and system operation.
- Credential management is crucial, as credentials like X.509 certificates enable identification and authentication of communication peers, authorization, and support security parameter management for communication sessions.
- X.509 certificates need to be validated before trust is established, which relates to effort for the infrastructure to provide the information and for relying parties to check the information.
- Proposed enhancement for X.509 certificate validation allows to
  - Reduce computational effort and storage requirements for the relying party, which is specifically important for constrained devices.
  - Reduce computational effort and response time for the infrastructure components (SCVP server) by caching the validated information.
- Future work aims at a proof-of-concept implementation and evaluation of the proposed approach.
  Specific points comprise:
  - performance impact on client side specifically with different certificate path lengths,
  - impact on code size for client side, as communication protocol stacks for selected protocols may be omitted,
  - impact on infrastructure side, e.g., depending on the chosen approach for the publishing of validation results.

SIEMENS

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

Andreas Güttinger
Senior Key Expert

E-mail andreas.guettinger@siemens.com

SI EA R&D AR
Humboldtstr. 59
90459 Nuremburg
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