# Security in Power System Automation

## Application of ITU-T X.509

Second X.509 Day

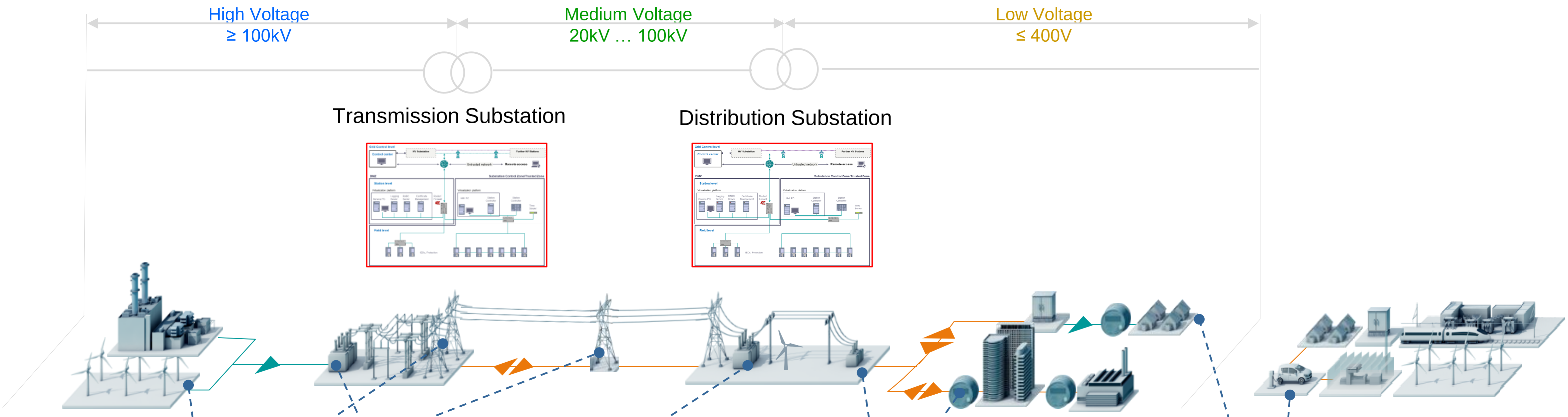
Steffen Fries, Siemens, T CST

May 09, 2023

SIEMENS

# Digital Grid – a Critical Infrastructure in Need of Protection

## Power system value chain and use case examples



**Generation**

**Transmission**

**Distribution**

**Prosumer Consumer / Producer**

**Rail & Microgrids**

- Power Quality Monitoring
- Network Optimization

- Substation Automation
- Inter Control Center Communication
- Remote Maintenance and Service

- DER Integration (Metering & Control)
- Remote Services

- Connecting Electric Vehicles to the Charging Infrastructure

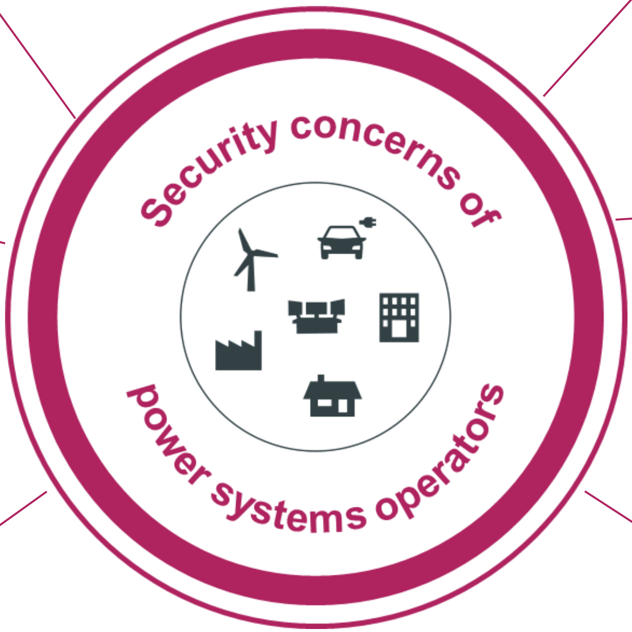
# Cybersecurity supported by IEC 62351

## A security kit to address security requirements in Power System Automation

Who/What are the entities in my digital grid?
(relates to identification of personal and assets)

Which entities have access to my OT and under which conditions?
(relates to roles and attributes used for access control decisions, e.g., may differ based on location)

Can I trust my OT network?
(relates to monitor changes in the OT network)



Can I trust the software and firmware running in my OT and specifically, can I trust updates received during operation?
(relates to device integrity)

Can I depend on my process data to control the actions ?
(relates to data integrity)

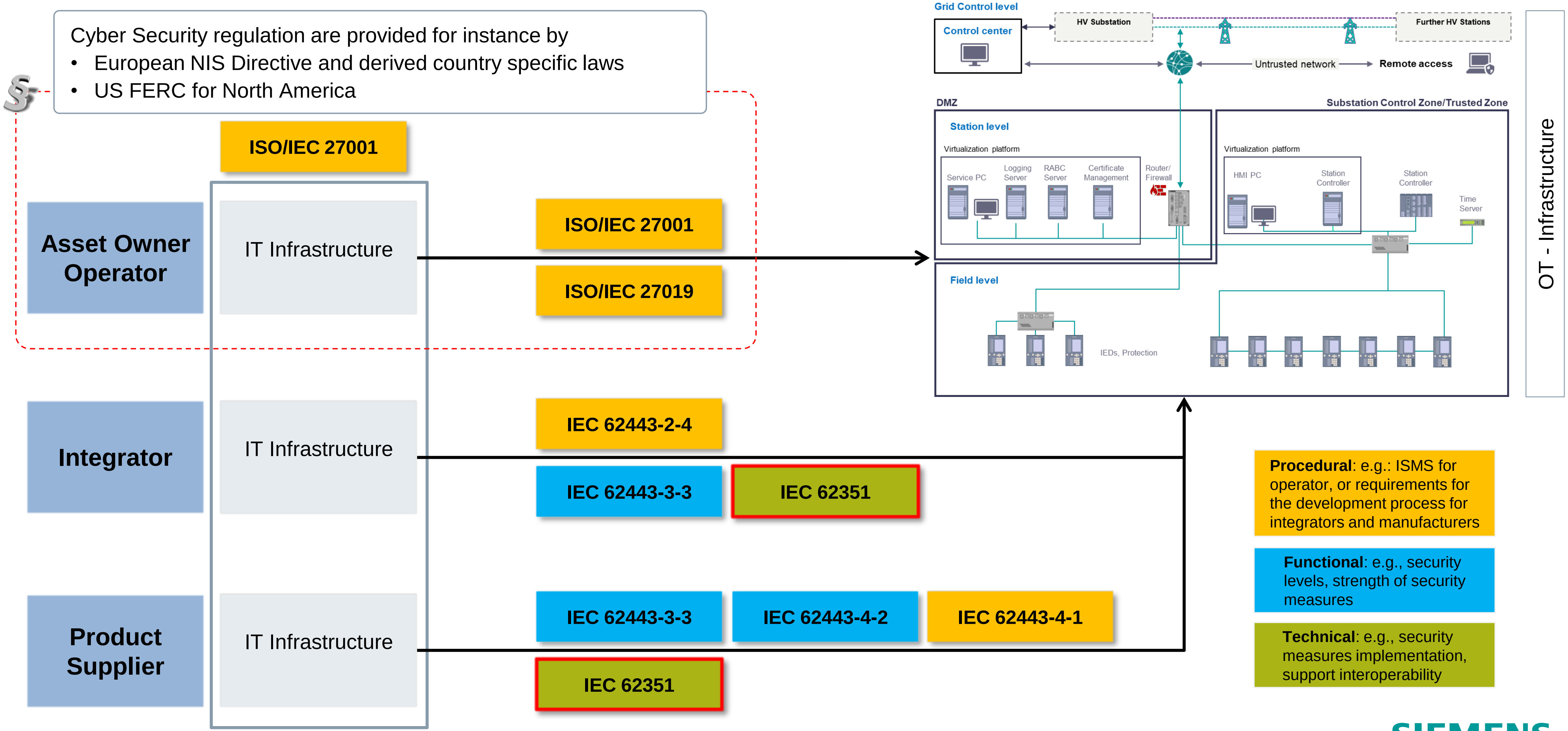
Are my critical operational settings intact?
(relates to data integrity)

# Cybersecurity for Power System Automation

## Interplay of ISO/IEC 27001 / IEC 62443 / IEC 62351

Cyber Security regulation are provided for instance by

- European NIS Directive and derived country specific laws
- US FERC for North America



§

ISO/IEC 27001

Asset Owner Operator — IT Infrastructure — ISO/IEC 27001, ISO/IEC 27019

Integrator — IT Infrastructure — IEC 62443-2-4, IEC 62443-3-3, IEC 62351

Product Supplier — IT Infrastructure — IEC 62443-3-3, IEC 62443-4-2, IEC 62443-4-1, IEC 62351

**Procedural**: e.g.: ISMS for operator, or requirements for the development process for integrators and manufacturers

**Functional**: e.g., security levels, strength of security measures

**Technical**: e.g., security measures implementation, support interoperability

SIEMENS

# Cybersecurity supported by IEC 62351 (defined in IEC TC57 WG15)

## A security kit to address security requirements in Power System Automation

### Identity and Access Management

Identification, Authentication, Authorization (RBAC) of Users/Devices

**Focus:** Usage of X.509 certificates

### Secure Communication

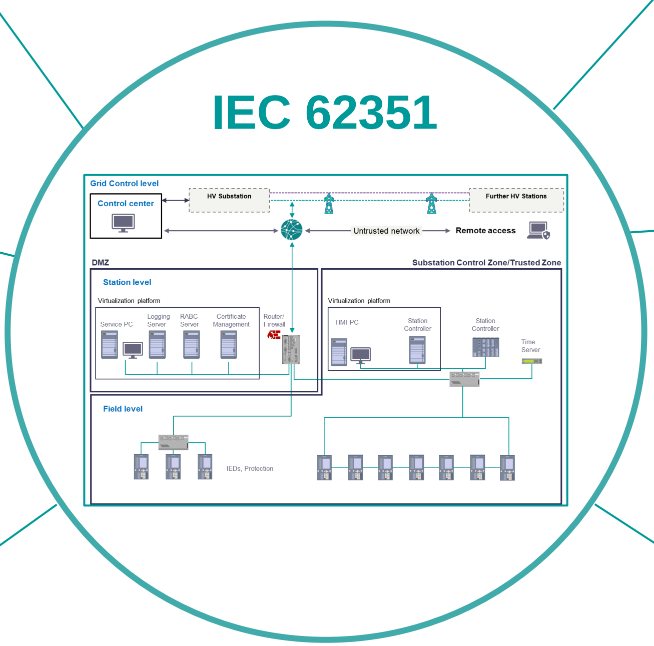
Between different actors on different layers (Ethernet, IP, serial)

**Focus:** Profiling of existing standards (e.g., TLS) and definition of security enhancements if necessary

### Monitoring and Audit

Logging and processing of security relevant events

**Focus:** Application of established standards like syslog and SNMP



### Key Management

Management of long term and session keys

**Focus:** Application of established certificate management (EST, SCEP) and key management (GDOI) protocols

### Conformity Tests

Test case description for specified security measures in the different parts of IEC 62351 based on PICS statements

**Focus:** Specification of conformity test cases

### Guidelines

Guidance and support for securing power system

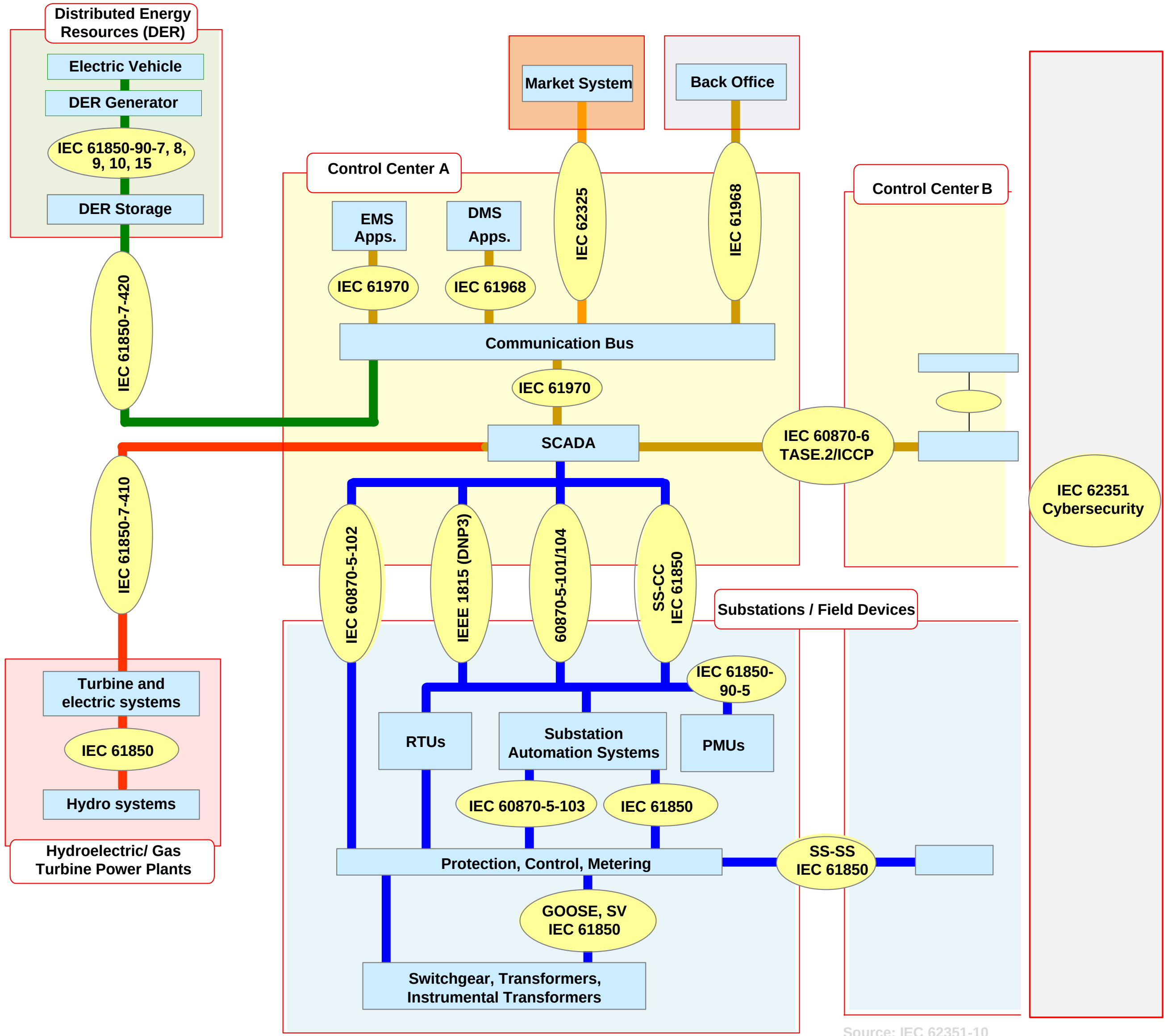
**Focus:** Examples for architectures, RBAC, monitoring, …

# Core Communication Standards for Digital Grids

## IEC TC57 defines the reference architecture with domain-specific cybersecurity

### IEC TC57 WG15 Scope

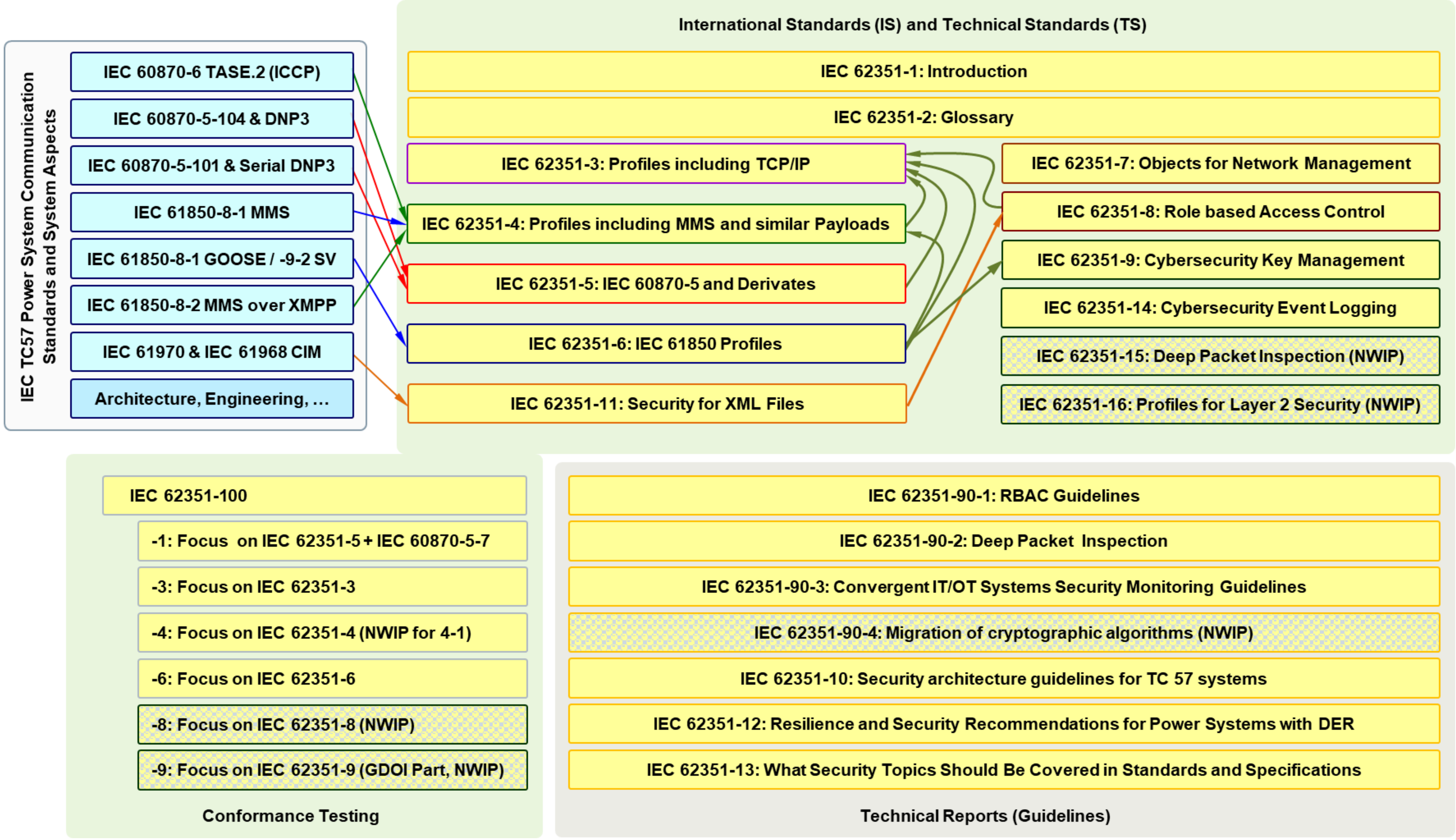
- Development of IEC 62351 to secure communication protocols defined by IEC TC 57, specifically
  - IEC 60870-5 and IEC 60870-6 series,
  - IEC 61850 series,
  - IEC 61968 & IEC 61970 series.
- Focus on end-to-end security to ensure that data exchanged between a source (sender) and a sink (receiver) is protected from unauthorized access and/or modifications.
- Further parts address architecture and system aspects and support engineering and operation.
- Addressed in currently 18+ parts of IEC 62351 of different status



Source: IEC 62351-10

# Cybersecurity in Digital Grids as defined in IEC TC57 WG15

## IEC 62351 provides technical security measures and guidelines



IEC TC57 Power System Communication Standards and System Aspects

- IEC 60870-6 TASE.2 (ICCP)
- IEC 60870-5-104 & DNP3
- IEC 60870-5-101 & Serial DNP3
- IEC 61850-8-1 MMS
- IEC 61850-8-1 GOOSE / -9-2 SV
- IEC 61850-8-2 MMS over XMPP
- IEC 61970 & IEC 61968 CIM
- Architecture, Engineering, …

International Standards (IS) and Technical Standards (TS)

- IEC 62351-1: Introduction
- IEC 62351-2: Glossary
- IEC 62351-3: Profiles including TCP/IP
- IEC 62351-4: Profiles including MMS and similar Payloads
- IEC 62351-5: IEC 60870-5 and Derivates
- IEC 62351-6: IEC 61850 Profiles
- IEC 62351-11: Security for XML Files
- IEC 62351-7: Objects for Network Management
- IEC 62351-8: Role based Access Control
- IEC 62351-9: Cybersecurity Key Management
- IEC 62351-14: Cybersecurity Event Logging
- IEC 62351-15: Deep Packet Inspection (NWIP)
- IEC 62351-16: Profiles for Layer 2 Security (NWIP)

Conformance Testing

- IEC 62351-100
  - -1: Focus on IEC 62351-5 + IEC 60870-5-7
  - -3: Focus on IEC 62351-3
  - -4: Focus on IEC 62351-4 (NWIP for 4-1)
  - -6: Focus on IEC 62351-6
  - -8: Focus on IEC 62351-8 (NWIP)
  - -9: Focus on IEC 62351-9 (GDOI Part, NWIP)

Technical Reports (Guidelines)

- IEC 62351-90-1: RBAC Guidelines
- IEC 62351-90-2: Deep Packet Inspection
- IEC 62351-90-3: Convergent IT/OT Systems Security Monitoring Guidelines
- IEC 62351-90-4: Migration of cryptographic algorithms (NWIP)
- IEC 62351-10: Security architecture guidelines for TC 57 systems
- IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER
- IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications

**Security means defined for**

- Authentication and authorization (RBAC)
- Secure IP-based and serial communication
- Secure application level exchanges
- Security monitoring and event logging
- Test case definition
- Guidelines for applying specific security measures in power system architectures

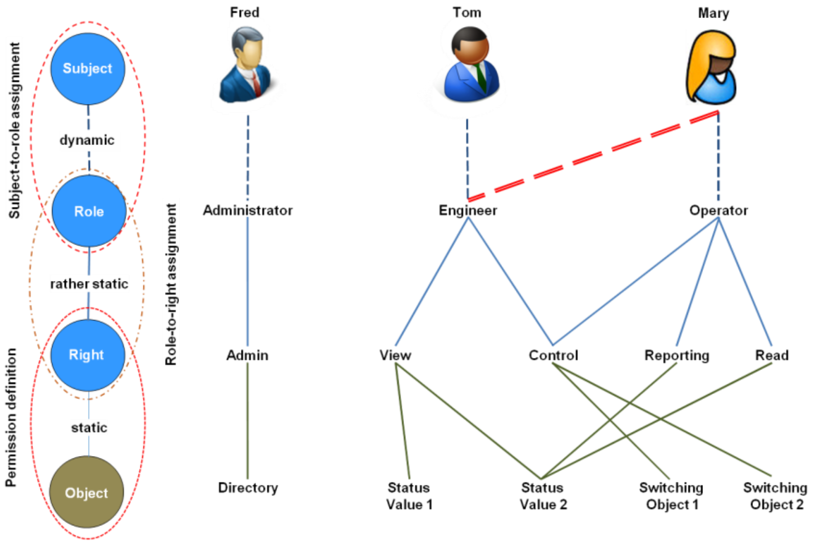
**by utilizing or profiling**

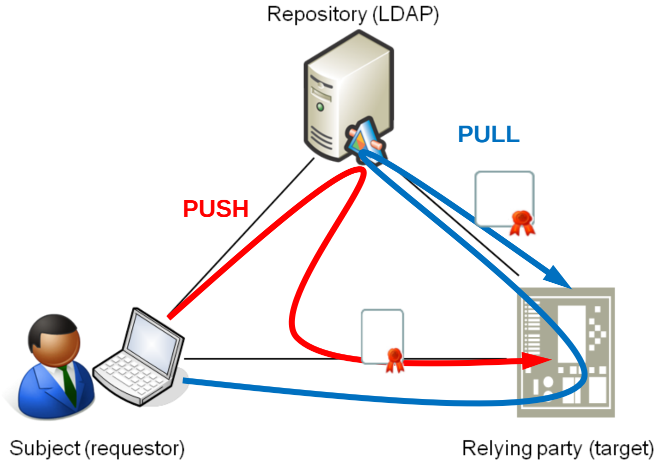
- existing standards and recommendations

# IEC 62351-8 Role-based Access Control

## Support of fine-grained authorization supported by X.509 certificates

- Roles are intended to ease access control configuration and decisions
- Base RBAC model shall support distinction of
  - subjects and roles; subjects = {humans; devices; SW processes}
  - roles and associated permissions; permission = right on data object
- IEC 62351-8 defines
  - 4 profiles for distributing RBAC information as an access token (X.509 public key certificate, X.509 attribute certificate, JSON Web Token, RADIUS)
  - 7 standardized roles (IEC 61850 scope)
  - role-to-permission assignment for custom defined roles using XACML
  - PULL or PUSH approach for provisioning of access tokens
- Gap regarding missing LDAP scheme for X.509 attribute certificates is addressed in a liaison of ITU-T SG 17 and IEC TC57 WG15 resulting in an update of X.509

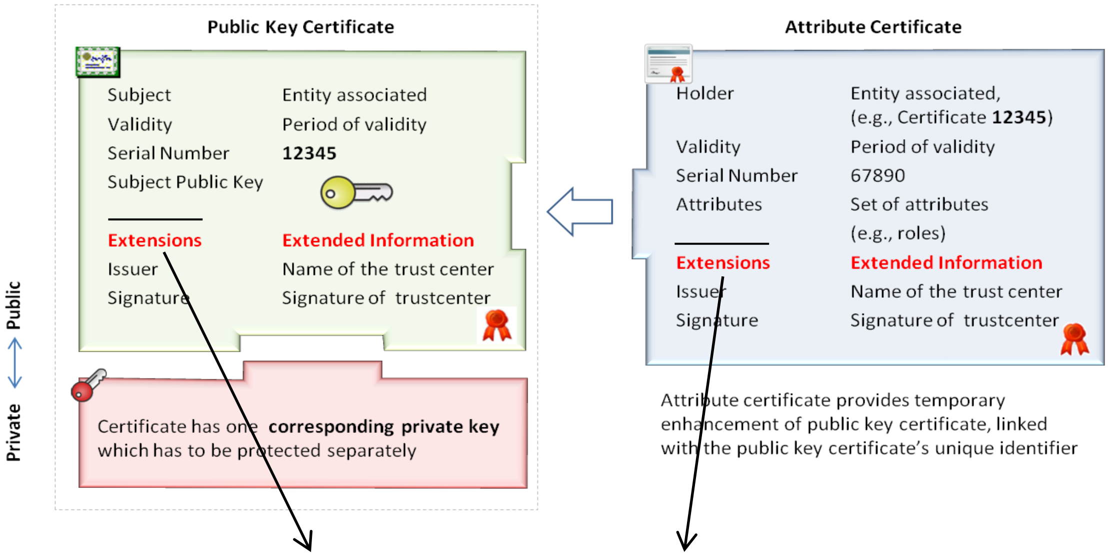




# IEC 62351 Role-based Access Control

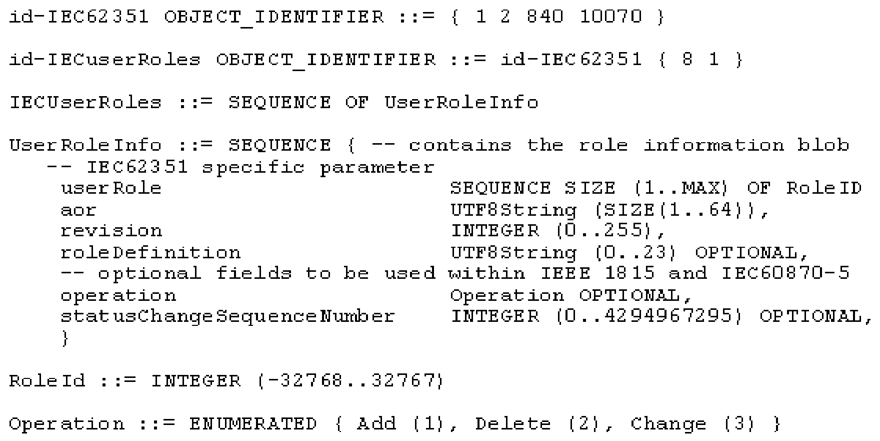
## RBAC extension defined for application in X.509 public key and attribute certificate

### IEC 62351-8 access token (here: Profile A and Profile B)



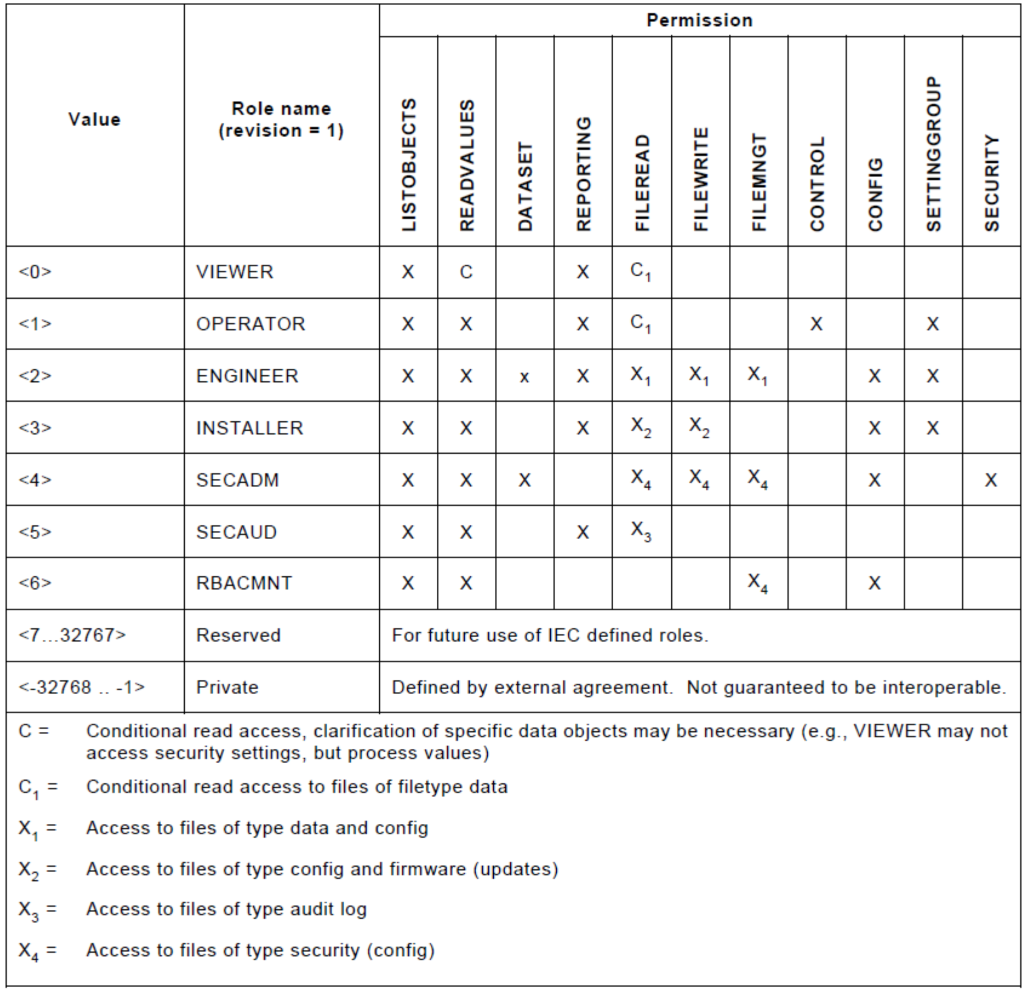
Certificate has one **corresponding private key** which has to be protected separately

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



```
id-IEC62351 OBJECT_IDENTIFIER ::= { 1 2 840 10070 }

id-IECuserRoles OBJECT_IDENTIFIER ::= id-IEC62351 { 8 1 }

IECUserRoles ::= SEQUENCE OF UserRoleInfo

UserRoleInfo ::= SEQUENCE { -- contains the role information blob
   -- IEC62351 specific parameter
    userRole                          SEQUENCE SIZE (1..MAX) OF RoleID
    aor                               UTF8String (SIZE(1..64)),
    revision                          INTEGER (0..255),
    roleDefinition                    UTF8String (0..23) OPTIONAL,
    -- optional fields to be used within IEEE 1815 and IEC60870-5
    operation                         Operation OPTIONAL,
    statusChangeSequenceNumber        INTEGER (0..4294967295) OPTIONAL,
    }

RoleId ::= INTEGER (-32768..32767)

Operation ::= ENUMERATED { Add (1), Delete (2), Change (3) }
```

### IEC 62351-8 pre-defined roles



| Value | Role name (revision = 1) | Permission | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | LISTOBJECTS | READVALUES | DATASET | REPORTING | FILEREAD | FILEWRITE | FILEMNGT | CONTROL | CONFIG | SETTINGGROUP | SECURITY |
| <0> | VIEWER | X | C | | X | $C_1$ | | | | | | |
| <1> | OPERATOR | X | X | | X | $C_1$ | | | X | | X | |
| <2> | ENGINEER | X | X | x | X | $X_1$ | $X_1$ | $X_1$ | | X | X | |
| <3> | INSTALLER | X | X | | X | $X_2$ | $X_2$ | | | X | X | |
| <4> | SECADM | X | X | X | | $X_4$ | $X_4$ | $X_4$ | | X | | X |
| <5> | SECAUD | X | X | | X | $X_3$ | | | | | | |
| <6> | RBACMNT | X | X | | | | | $X_4$ | | X | | |
| <7…32767> | Reserved | For future use of IEC defined roles. | | | | | | | | | | |
| <-32768 .. -1> | Private | Defined by external agreement. Not guaranteed to be interoperable. | | | | | | | | | | |

C = Conditional read access, clarification of specific data objects may be necessary (e.g., VIEWER may not access security settings, but process values)

$C_1$ = Conditional read access to files of filetype data

$X_1$ = Access to files of type data and config

$X_2$ = Access to files of type config and firmware (updates)

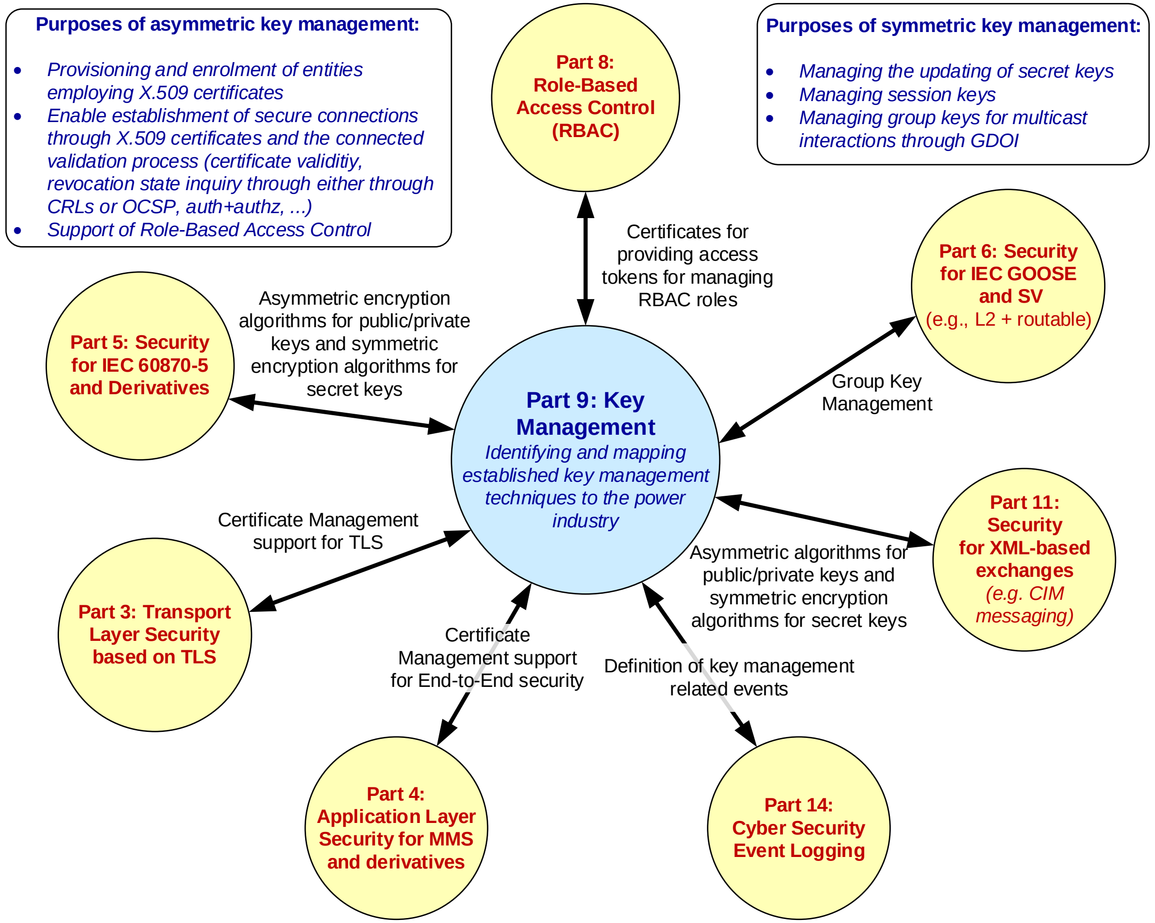
$X_3$ = Access to files of type audit log

$X_4$ = Access to files of type security (config)

# IEC 62351-9 – Cyber security key management for power system equipment

## Handling the prerequisite: symmetric and asymmetric keys

- X.509 certificates are a pre-requisite for most IEC 62351 security means
- IEC 62351-9 defines the management of certificates and corresponding private keys as well as group keys and security policies, specifically:
  - Management of Certificates (PKI)
    - Enrollment support : SCEP, EST (both mandatory for infrastructure, only one mandatory for the client)
    - Detail certificate verification rules for public-key certificates and attribute certificates, including revocation status checking using CRLs and/or optional OCSP
    - Optional trust anchor management support using TAMP
  - Management of group keys based on GDOI
    - Group key distribution is bound to peer authentication based on X.509 certificates
    - Defines enhancements for group key and group security policy for GOOSE and SV and PTP (in Edition2)
- IEC 62351-3 Edition 9 targeted for 06/2023 (FDIS passed)



**Purposes of asymmetric key management:**

- *Provisioning and enrolment of entities employing X.509 certificates*
- *Enable establishment of secure connections through X.509 certificates and the connected validation process (certificate validitiy, revocation state inquiry through either through CRLs or OCSP, auth+authz, ...)*
- *Support of Role-Based Access Control*

**Purposes of symmetric key management:**

- *Managing the updating of secret keys*
- *Managing session keys*
- *Managing group keys for multicast interactions through GDOI*

**Part 9: Key Management**
*Identifying and mapping established key management techniques to the power industry*

**Part 8: Role-Based Access Control (RBAC)** – Certificates for providing access tokens for managing RBAC roles

**Part 6: Security for IEC GOOSE and SV** (e.g., L2 + routable) – Group Key Management

**Part 11: Security for XML-based exchanges** *(e.g. CIM messaging)* – Asymmetric algorithms for public/private keys and symmetric encryption algorithms for secret keys

**Part 14: Cyber Security Event Logging** – Definition of key management related events

**Part 4: Application Layer Security for MMS and derivatives** – Certificate Management support for End-to-End security

**Part 3: Transport Layer Security based on TLS** – Certificate Management support for TLS

**Part 5: Security for IEC 60870-5 and Derivatives** – Asymmetric encryption algorithms for public/private keys and symmetric encryption algorithms for secret keys

PKI – Public Key Infrastructure
EST – Enrollment over Secure Transport
OCSP – Online Certificate Status Protocol
GDOI – Group Domain of Interpretation

SCEP – Simple Certificate Enrollment Protocol
CRL – Certificate Revocation List
TAMP – Trust Anchor Management Protocol

# Summary & Outlook

## There are still Security Challenges in Power System Automation

- IEC 62351 supporting the security in power system automation bases on the application of X.509 certificates.
- Liaison with ITU-T SG17 enhancements to allow for a better application of attribute certificates are targeted.
    - Support of **Crypto Agility** to enable migration to stronger cryptographic algorithms.
        - Specific options in X.509 allow using alternative cryptographic algorithms (hybrid approaches).
        - In addition X.510 allows to wrap existing protocols, which may not support crypto algorithm agility in the future. This will be addressed in a new part IEC 62351-90-4
- **Bootstrapping of security credentials** typically increases the effort for service technicians during installation. Automated bootstrapping targets to make this step transparent to the technician.
    - Zero-touch onboarding approaches currently defined in the IETF leverages the existence of device certificates and utilizes a *provisional* accept of X.509 certificates to establish trust.
    - Zero-touch onboarding approaches are already referred to in IEC 62351 but not normatively required.

# Contact

**Steffen Fries**
Principal Key Expert

T CST
Otto-Hahn-Ring 6
81739 Munich
Germany

E-mail steffen.fries@siemens.com

Siemens Grid Security

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

SIEMENS