PQC Transition Considerations for Power System Automation in IEC 62351

Steffen Fries, FT RPD CST, Siemens, steffen.fries@siemens.com

Fourth ITU-T X.509 Day, September 09, 2025

SIEMENS

Regulative and standard requirements demand state-of-the-art cryptography support (examples)

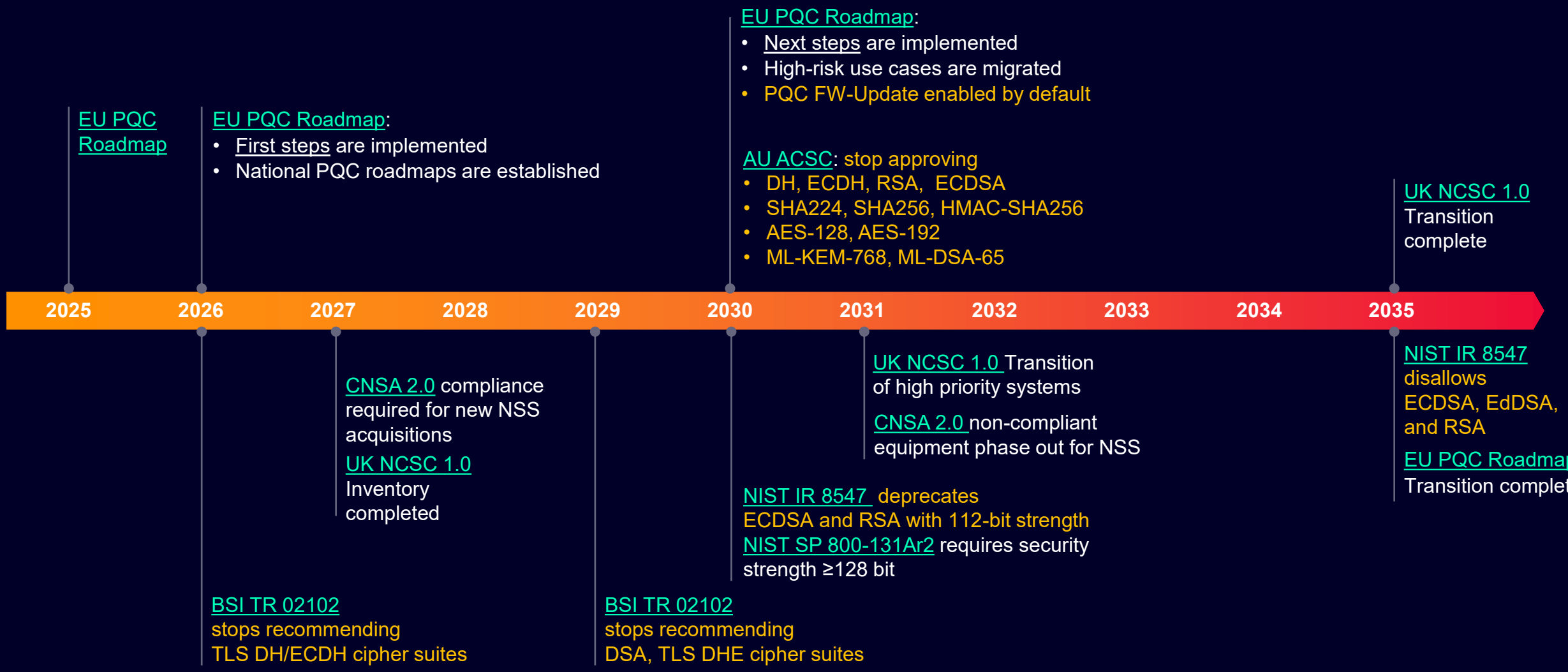
- **EU CRA**
  - ANNEX I: Essential Cybersecurity Requirements Part I, (2).e: "*protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by **state of the art mechanisms**, and by using other technical means*"

- **hEN18031** (harmonized framework to address Radio Equipment Directive (RED-DA) cybersecurity requirements)
  - [CRY-1] Best practice cryptography: "*The equipment **shall use best practice for cryptography** that is used for the protection of the security assets or network assets, …*"

- **IEC 62443-4-2**
  - CR 4.3 – Use of cryptography: "*If cryptography is required, the component shall use cryptographic security mechanisms **according to internationally recognized and proven security practices and recommendations**.*"

State-of-the-art cryptography is a moving target: Transition to PQC defined

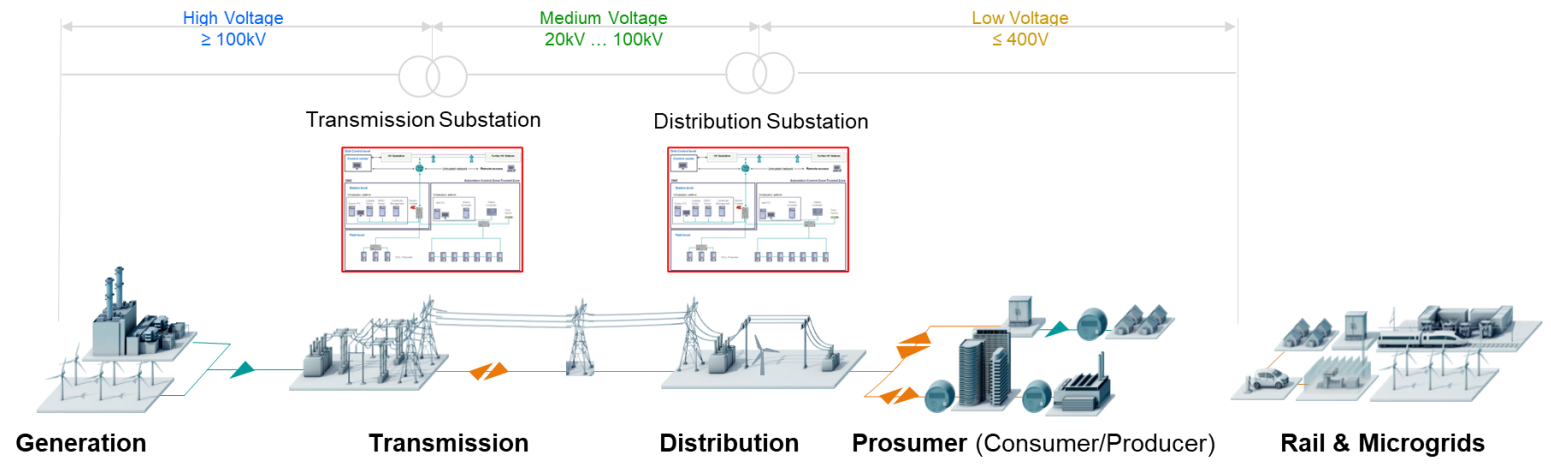
Recommendations of transition timelines for several regions (examples: EU, US, AU, UK, DE)



SIEMENS

Digital Power Grid – a critical infrastructure in need of protection

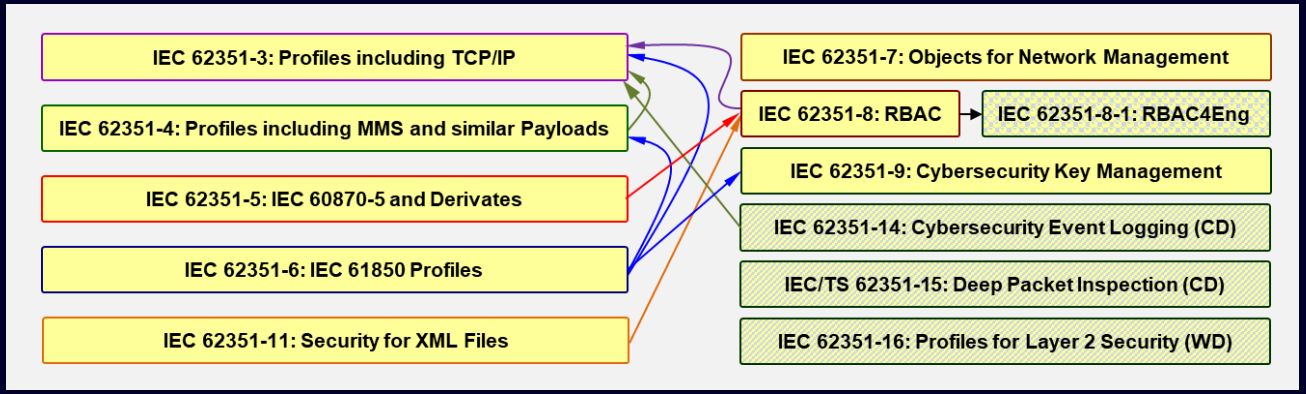
Standards exist to address power system value chain security requirements



Related (example) use cases

- Power Quality Monitoring
- Substation Automation
- Inter Control Center Communication
- Remote Maintenance and Service
- DER Integration (Metering & Control)
- Electric Vehicles Charging

- IEC TC57 defines power system management reference architecture (IEC 62357). It incorporates security to protect related communication protocols, specifically IEC 60870-5 and IEC 60870-6 series, and the IEC 61850 family.
- Security measures are defined in IEC 62351 series, e.g.,
  - Authentication and authorization (RBAC)
  - Secure IP- based and serial communication
  - Secure application-level exchanges
  - Security monitoring and event logging
- Authentication, key agreement, and digital signature applications rely on X.509 certificates



SIEMENS

Next steps in advancing security in power automation systems
IEC 62351 Considerations regarding PQC transition

- IEC 62351 relies on symmetric and asymmetric cryptographic algorithms to protect communication. While symmetric cryptographic algorithms may be handled by increasing the key length, asymmetric algorithms need to be migrated. A cryptographic inventory of IEC 62351 has been compiled to better prioritize further development of the series.
- Several parts of IEC 62351 utilize standard protocols and mechanisms and profile them (e.g., TLS). For these PQC transition can likely be handled by updating defined profiles to take PQC into account.
- Still, some IEC 62351 parts, define own security solutions or rely on protocols, which are likely not updated to PQC. Utilized cryptographic mechanisms for security context establishment rely on digital signatures (RSA, ECDSA) and Diffie Hellman for key agreement. These need to be addressed specifically and the effort is ongoing in IEC TC57.
- IEC 62351-90-4 “Migration support to stronger cryptographic algorithms” provides guidance on migrating to stronger cryptographic algorithms relying on ITU-T X.509 and ITU-T X.510. It allows migrating from a currently used (native) cryptographic algorithm to a new (alternative) target cryptographic algorithm.
- PQC transition is also discussed in further standardization bodies, specifically in IETF, from which several security standards (e.g., TLS, syslog) are applied in power systems. They must be considered to provide a sound system approach.

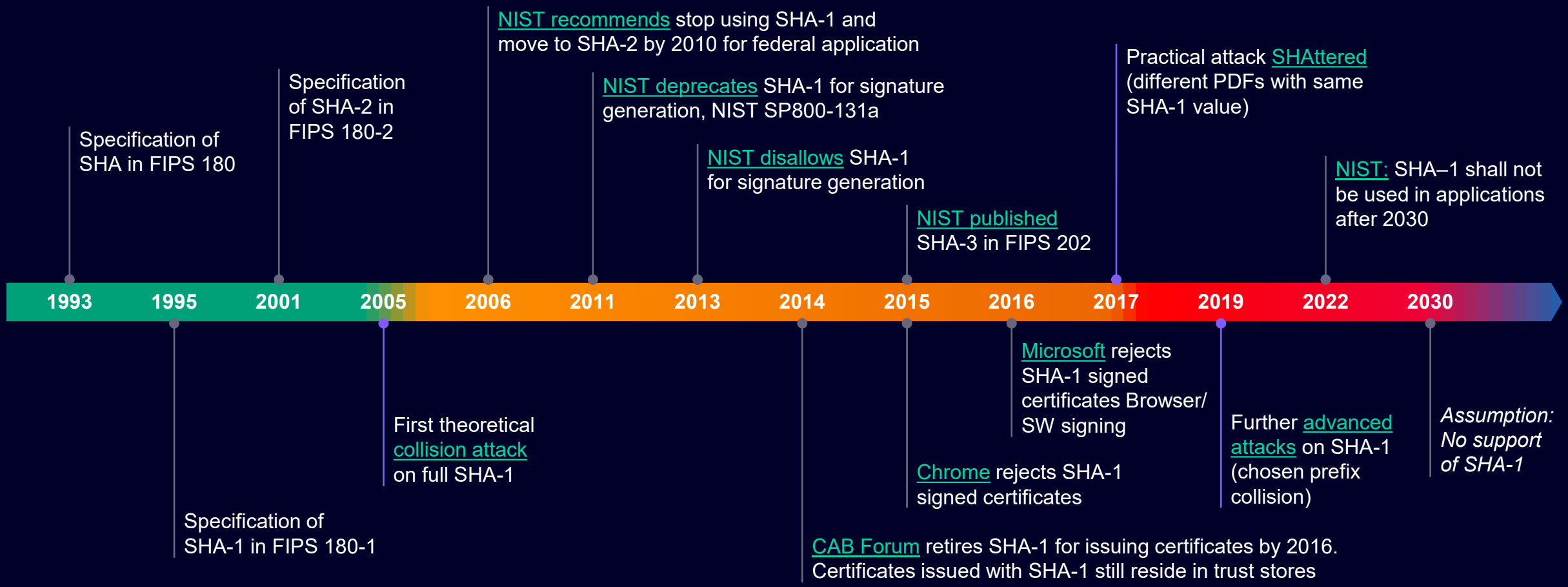
Summary

- PQC transition for IEC 62351 has started, but further refinements are necessary.
- Deviating approaches for PQC transition will influence market acceptance and likely increase system complexity.

SIEMENS

Experiences from ongoing cryptographic algorithm transition underline the necessity to act

The rise and fall of SHA–1 (hash function)



Migration towards new cryptographic algorithm support takes its time. Disallowing application of outdated cryptographic algorithm may take even longer.

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

Siemens Grid 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