

# IoT SECURITY COMPLIANCE

Achieve cost effective & quick compliance to major IoT Standard with SEALSQ



U.S. CYBER TRUST MARK



## One-Stop-Shop

Unique security partner delivers fully integrated solution from Root of Trust to chip.



## Cost Effective

No intermediates in the value chain. Reduced integration and certification costs.



## Fast-time-to-market

Simplify and accelerate development and certification processes.



## Convenient

Easy PKI as-a-Service online interface to manage certificates.



## Flexible

Full range of pre-provisioning options (Factory, OTA, Zero Touch...).



## Highest Security

State-of-The-Art tamper resistant hardware & trust services.

## ETSI EN 303 645 (CE Label) vs NIST IR 8425 (US Cyber Trust Mark) Requirements

ETSI EN 303 645 Requirement	NIST IR 8425 "Cybersecurity Capabilities"
No universal default passwords	Access Control
Keep software updated	Software Update
Securely store sensitive security parameters	Data Protection
Communicate Securely	Data Protection
Minimize exposed attack surfaces	Access Control
Ensure software integrity	Software Update
Ensure that personal data is secure	Data Protection
Make systems resilient to outages	Access Control
Examine system telemetry data	Cybersecurity State Awareness
Delete user data and reset are easy	Data Protection
Installation and Maintenance are easy	Access Control
Validate input data	Data Protection

### Industry "Best Practices" Baseline Requirements Combined and consolidated "Implied Requirements" from NIST IR 8425 and ETSI EN 303 645:

Best Practices Requirement	Description	SEALSQ Solution
Securely Store Credentials & Certificates	This applies to both the Birth (or factory) Certificate (IDEVID) and Operational Certificates (LDEVIDs) along with their associated public private key pairs.	✓
Credential based authentication	IDEVID (birth certificate) and LDEVIDs (application certificates)	✓
Unique password	Factory defined passwords must be unique	✓
Specialized User Roles	Roles for administration, operation, etc.	✓
Secure Storage and Update of data	Applies to configuration, user, and application data	✓
Secure Communication	Includes communication on the bus, and communication to other IoT ecosystem nodes	✓
Secure Software Update	Verify software package when downloading	✓
Secure Boot	Verify software package in bootloader	✓
Device Intent	Configuration to only intended Functionality of IoT device	✓



Visit [sealsq.com](https://www.sealsq.com)



Download white paper