Cyber Security

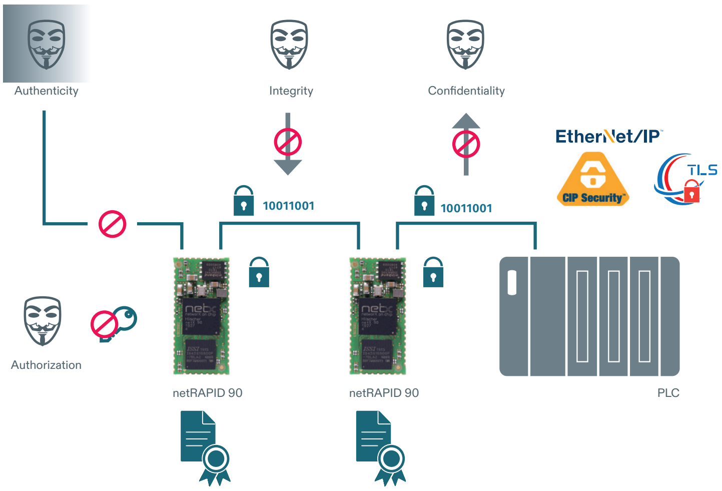
Secure Field Level

- → **Integrity: Protection against data manipulation**
  IO-Data signature supported by EtherNet/IP CIP Security Firmware
- → **Authenticity: Ensures communication establishment to trustful devices only**
  EtherNet/IP CIP Security Firmware supports device identity verification by Device Identity Certificate and Webserver Certificate
- → **Authorization: Only authorized users get device and data access**
  netX 90 supports Secure Boot
  User Management integrated into EtherNet/IP CIP Security Firmware
- → **Confidentiality: Prevent unauthorized data reading, keep data secret**
  IO-Data encryption supported by EtherNet/IP CIP Security Firmware with Confidentiality Profile

Cyber Security Support in Hilscher Products

With growing relevance of IIoT and the related OT/IT convergence, cyber security becomes more and more important on field level. To ensure robustness and availability of a system, four cyber security goals must be met: Integrity, Authenticity, Authorization and Confidentiality.

Hilscher products address these goals. Our hardware and software offers features to meet IEEE 62443 requirements and significantly improve cyber security on field level.



→ QR Code Link: Cyber Security
Service-Hotline: +49 (0) 6190 9907-90
www.hilscher.com

empowering communication

Secure Field Level – Cyber Security

Secure Boot

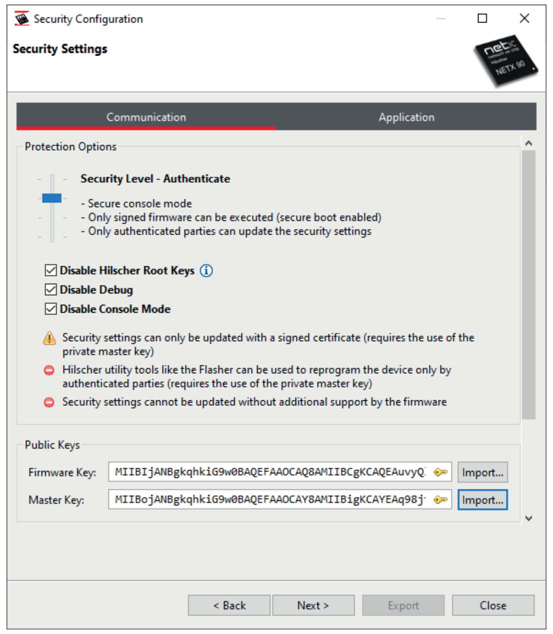
Secure Boot is a “close to hardware” functionality since it is active during the start-up phase of the device. It ensures that only intended, original firmware without manipulations is started and executed on the device.

The firmware signing, public key installation and secure boot configuration is performed with the netX Studio IDE. Command line tools are available for production environments.

Four Security Levels and several additional options can be configured with increasing protection level:

- **Disabled**
  Open system
- **Development**
  Firmware verification active, but security configuration can be modified without restrictions
- **Authenticate**
  Firmware verification active, private key required to modify security configuration
- **Immutable**
  Security configuration cannot be modified anymore

JTAG and console interfaces are lockable.



Security Settings

Protection Options

Security Level - Authenticate

- Secure console mode
- Only signed firmware can be executed (secure boot enabled)
- Only authenticated parties can update the security settings

☑ **Disable Hilscher Root Keys** ⓘ
☑ **Disable Debug**
☑ **Disable Console Mode**

⚠ Security settings can only be updated with a signed certificate (requires the use of the private master key)

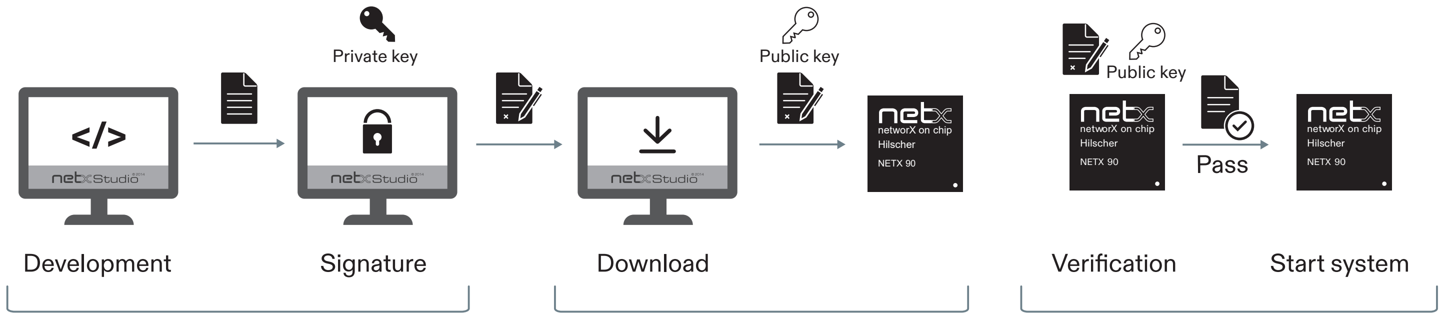
⊖ Hilscher utility tools like the Flasher can be used to reprogram the device only by authenticated parties (requires the use of the private master key)

⊖ Security settings cannot be updated without additional support by the firmware

Public Keys

Firmware Key: MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuvyQ

Master Key: MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAq98j



1 Develop firmware and sign it with private key

2 Download signed firmware and public key to the device

3 Firmware verification with public key during start-up phase of netX 90

Secure Communication

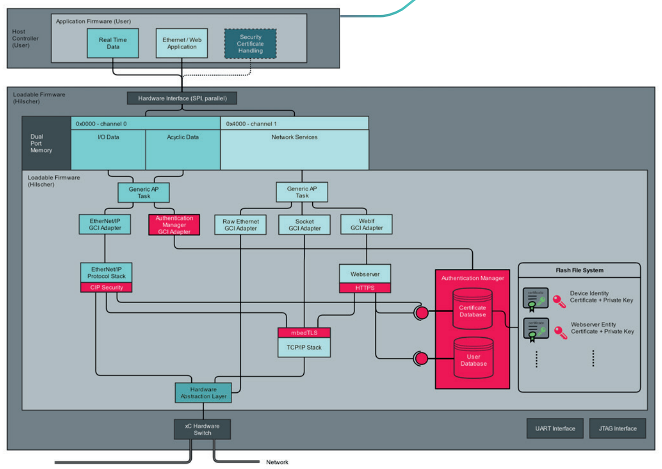
The Hilscher EtherNet/IP protocol firmware with CIP Security for netX 90 supports the “EtherNet/IP Confidentiality Profile”, which covers the aspects integrity, authenticity and even confidentiality.

Most secure communication functions are based on the TLS – Transport Layer Security – stack, on top of the TCP/IP stack and the netX 90 crypto accelerator in hardware.

HTTPS protocol support ensures secure Webserver accesss.

The implemented user database allows the definition of user groups, roles and related data access rights.

Security Functionality is encapsulated in the Hilscher Firmware. Low effort on the application side guarantees fast time to market.



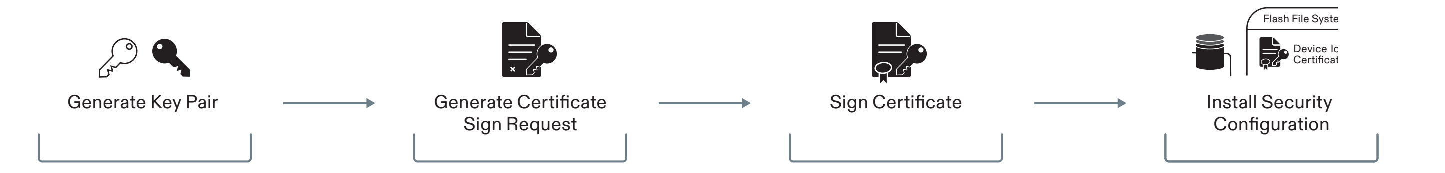
Certificate Deployment

Hilscher security firmware offers a great flexibility in generating and deploying security certificates, with or without a PKI – public key infrastructure.

Two main methods:

- Security configuration by application, using an API over the Dual-Port-Memory interface
- Protocol specific methods and tools, like the Rockwell FactoryTalk® Policy Manager for EtherNet/IP CIP Security

Security configuration by application consists of 4 steps.



1 The application triggers on-chip key generation

or

downloads a prepared key pair (DER or PEM)

2 The application triggers on-chip certificate signing request (CSR) generation

or

the CSR can be uploaded to the application

3 The application triggers on-chip certificate signature

or

downloads an externally signed certificate (X.509)

4 User application activates the security configuration by installation command

→ QR Code Link: Cyber Security
Service-Hotline: +49 (0) 6190 9907-90
www.hilscher.com

empowering communication

Product Information

Technical Data

Technical Data

Endpoint authentication
X.509v3 Certificate (PEM/DER format), Pre-Shared Key (PSK)

Cryptographic techniques
Symmetric: AES (128, 256 bit),
Asymmetric: ECC, RSA (2048, 3072, 4096 bit)

Supported elliptic curves
secp256r1, secp384r1

Hash functions
SHA-1, SHA-256, SHA-384

EtherNet/IP over (D)TLS port number
TCP/UDP: 2221

HTTPS port number
TCP: 443

Number HTTPS connection
1

TLS version
1.2

Supported security profiles
EtherNet/IP Confidentiality Profile

Certificate options
Self-signed certificate, Vendor-signed certificate

Software compatibility
Compatible with Rockwell FactoryTalk® Policy Manager Version 6.20.00

Technical Data

EtherNet/IP supported (D)TLS cipher suites
ECDHE-ECDSA with SHA-1 (no encryption)
ECDHE-ECDSA with AES-128 bit CBC mode and SHA-256
ECDHE-ECDSA with AES-128 bit GCM mode and SHA-256
ECDHE-ECDSA with AES-256 bit CBC mode and SHA-384
RSA with SHA-256 (no encryption)
RSA with AES-128 bit CBC mode and SHA-256
RSA with AES-256 bit CBC mode and SHA-256
ECDHE-PSK with SHA-256 (no encryption)
ECDHE-PSK with AES-128 bit CBC mode and SHA-256
ECDHE-PSK with AES-128 bit GCM mode and SHA-256
ECDHE-PSK with ChaCha20 Poly1305 mode and SHA-256

Predefined standard objects
File Object (0×37)
CIP Security Object (0×5D)
EtherNet/IP Security Object (0×5E)
Certificate Management Object (0×5F)
TCP/IP Interface Object (0xF5)
Ingress Egress Object (0×3AC) (from Rockwell)

Supported features
Secure I/O communication (Class 0/1)
Secure Explicit Messaging (Class3 and UCMM)
Certificate provisioning via Push Model
Default Security Configuration via DPM services

Note: All technical data may be changed without further notice.