End to end Security Management

Provide security mechanism to secure data at various points on complex IoT ecosystems

In complex and heterogeneous IoT infrastructure, **End-to-end security functional group** provides a fully interoperable security backend that enables **authentication** of parties, **encryption** of data, **attestation** of devices and **anonymization** of data sources. It helps to enable cyber resilience to provided escalated reactions upon various situations.

FEATURES

- **Identity federation** to benefit interoperable authentication using OAuth2, OpenID and regular directory services such as LDAP
- **Asymmetric encryption** support with an embedded Public Key Infrastructure bound to identities
- **Remote attestation** of IoT devices based on Trusted Computing Group (TCG) specifications and component such as Trusted Platform Module (TPM)
- **Anonymization** support with Direct Anonymous Attestation (ECDAA) to comply with privacy matters

KEY BENEFITS

Easy to integrate

Compliant with TCG's specifications

All-in-one security management

High scalability with clustering

Remediation examples included

Collaborative

SYSTEM REQUIREMENTS

For IoT devices:

- an hardware, firmware or software TPM2 compliant device
- measured boot
- IMA and EVL module in Linux Kernel

For Edge/Network:

- Radius or LDAP authentication capabilities

For applications:

SASL, OAuth2 and OpenID

DID YOU KNOW?

Misconfiguration and misalignment of security standard and procedure in complex system makes room for vulnerabilities. Our End-to-end solution provides a common backend to make sure various entity can benefit from a single interoperable security platform. It provides secured framework for devices, edge components, application's backend and frontend using well-known, tested and trustful components such as OpenSSL, TPM2, LDAP and PKCS standards.

End-to-end Security Managers provides unique features for cyber-resilience with automated remediation upon incident. The whole system is actively monitored and audited making security manageable during its lifecycle.