Providing an HSM-based Factory Certificate Authority

For reliable IoT Device Integrity and Communication

About Nexus

Nexus, a part of the French IN Groupe, is a European leader and innovative identity management company. They secure society by enabling trusted identities for people and things.

For more information, visit **nexusgroup.com**

Challenge: Secure onboarding of a device to an IoT service / application

Securing IoT device communication against counterfeiting, fraud, and illegal use of service

Be compliant with upcoming EU regulations such as the Cyber Resilience Act (CRA)

Enable secure firmware "over the air" updates

Ensuring a proof of ownership for devices

Man in the middle attacks observing provisioning or impersonating the device or service

Secure, powerful and fit-for-purpose Factory CA solution

Utimaco and Nexus provide a secure, powerful and fit-for-purpose Factory Certificate Authority (CA) solution, relying on Utimaco's u.trust General Purpose HSM Se-Series and Nexus PKI Certificate Manager™ software. The solution includes operation of one or multiple CA instances: self-signed or signed by another CA. Main functions include:

- **Production of factory certificates ('birth certificates')** in response to a Certificate Signing Request (CSR)
- **Support for industry-standard CA key and signing algorithms** (e.g. Secp256r, ECDSA with SHA256)
- **CA key is securely stored in the HSM** (FIPS 140-2 Level 3)
- **Automatic provisioning of factory and CA certificates** to the provisioning equipment via REST API or standard certificate enrolment protocols
- **Export capabilities for** produced **factory certificates**
- **Import capabilities of** produced **certificates** in an Operational CA for certificate lifecycle management

Benefits

- Secure birth identity provisioning
- Simple installation and configuration
- IoT device authentication
- No Internet connectivity requirement
- Secure IoT communication

Enhanced Visibility and Control

- **Secure birth identity provisioning**

  The certificate is signed with the private key that stays protected in the HSM.

- **IoT device authentication**

  Reliable identification of IoT devices in supply chain and operational environment.

- **Secure IoT communication**

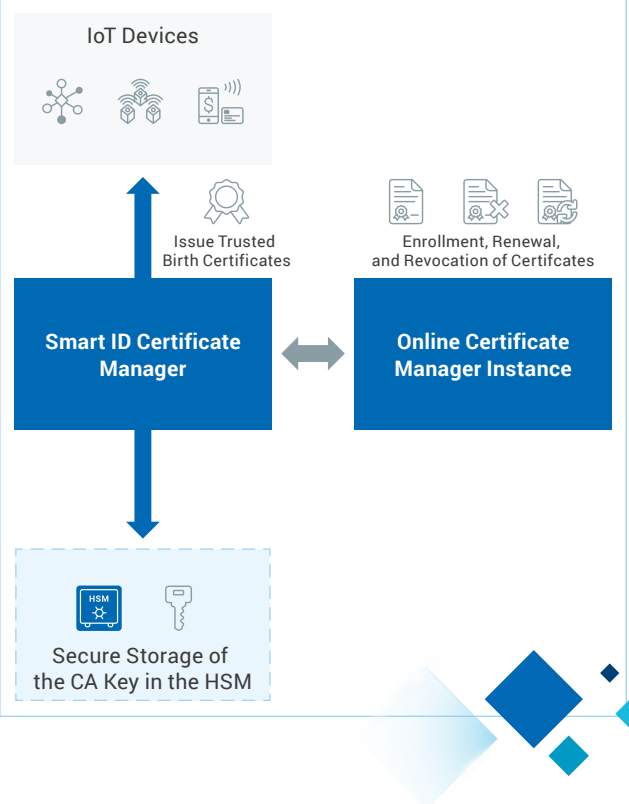
  Ensure secure communication between devices even over unsecure networks.

- **Simple installation and configuration**

  The Factory CA and HSM are integrated and can be easily installed and configured.

- **No Internet connectivity requirement**

  The solution works offline, no constant Internet connection required.



NEXUS Smart ID Certificate Manager (CM)

Smart ID Certificate Manager (CM) is a flexible, scalable, and high-security certificate authority (CA) software. CM supports a wide range of certificate enrollment protocols, that enables you to issue trusted birth certificates for devices in a Factory certificate authority (CA) setup. The Factory CA can work together with an online CM instance, which can provide auto-enrolment of operational certificates, certificate renewal and revocation services. Additionally, CM can establish Signing Authorities (SA), with HSM based key and trusted signing certificate, allowing clients using the CM REST API to request signing of data by the SA, e.g. for firmware code signing.

Free, fully functional HSM simulator

Test development and integration capabilities of the u.trust General Purpose HSM Se-Series in your environment – no purchase, delivery, or installation needed.

https://utimaco.com/resources/simulators-and-sdks/securityserver-simulator

u.trust General Purpose HSM PCIe Card and Network Appliance

EMEA

Utimaco IS GmbH

Germanusstrasse 4
52080 Aachen,
Germany

+49 241 1696 200
info@utimaco.com

Americas

Utimaco Inc.

900 E Hamilton Ave,
Suite 400
Campbell, CA 95008,
USA

+1 844 UTIMACO
info@utimaco.com

APAC

Utimaco IS Pte Limited

6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

+65 6993 8918
info@utimaco.com

utimaco.com