IDnomic Technical Subordinate CA Appliance

Secure your devices with electronic certificates

For transparent and operational digital exchanges, communication stakeholders, such as browsers or web servers, rely on certificate authorities and digital certificates issued from them.

It enables the protection and reliability of billions of exchanges every day.

Your devices' identity

Electronic certificates are at the heart of secure connections and digital. They ensure the digital identity of third parties for trustful exchanges. They also enable the encryption of data exchanged.

Thus, the 3 fundamental principles in IT security are respected: integrity, confidentiality and authenticity. Certificates are issued by trusted certificate authorities (CAs) that are pyramidally deployed: a root CA at the top of the pyramid and subordinate CAs linked to it.

Technical Subordinate CA appliance complements the root CA that issues subordinate authorities' certificates and ensures the lifecycle of the CAs linked to it.

Technical subordinate CAs issue certificates for devices. These certificates can have different functions (authentication, signature, encryption...).

Protect your infrastructure with an appliance

The Technical Subordinate Certificate Authority appliance enables the deployment of one or more subordinate Certificates Authorities (CAs) to securely issue certificates for devices or people quickly and cost-efficiently.

The certificate of the subordinate CA may be issued by a root CA (Root CA Appliance for example) or by the appliance's CA itself (self-signed certificate). The private key is stored in the state-of-the-art Trustway Proteccio Hardware Security Module (HSM), where the Subordinate CA Appliance is running. It is used to create certificates for devices.

The Technical Subordinate CA appliance is configured to issue certificates for end holders such as devices and servers (technical Delegated CA).

Certificate profiles are created from defined templates and can be associated with RSA or ECDSA keys. The certificates' production complies with the customer-defined certification policy and the requirements of supervisory bodies.

Typical use cases include the deployment of authentication certificates to ensure the identity of devices through an automatic enrollment process (SCEP or CMP) that facilitates the lifecycle management of certificates such as self-enrollment.

The Technical Subordinate CA appliance helps organizations to deliver their project quickly and cost-efficiently as:

- A pre-defined configuration is implemented: the appliance model is delivered with a standard configuration that can be used in most use cases, with **no extra time** in specifications or integration,
- Product is delivered in a **unique hardware** with **pre-configured features** and **database**,
- Minimal configuration is done at first run to make the appliance **ready to use**.

The system maintenance and support are simplified as the appliance is an all-in-one solution facilitating the tasks that can be complex and time-consuming in a classic implementation due to tailored configurations (VM, Servers, HSM...).

Get a greater control over the security of the information system and independence from “as-a-service” solutions with a certified hardware solution, ease and speed of implementation.

A model tailored to your needs

Atos provides a wide range of trust infrastructure appliances (PKI, digital signature, user explicit consent, time stamping, blockchain) and offers different appliance models according to the needs of the infrastructure:

- A **basic model** with only one service embedded in a HSM. This simple model is autonomous and does not require management of high volume of data. It can be deployed in a short time because it does not depend on the infrastructure. As an example, this model is fully adapted for the Root CA appliance.
- A **high-availability model** deploying several appliances to guarantee high availability by ensuring business continuity with a centralized database.
- A **multi-services model** with several services embedded in a HSM. In this way, it is possible to combine many services such as electronic signature or timestamping together with PKI..

Technical Subordinate CA appliance supports the following functional modules:

- Generation of the Certificate Signing Request (CSR) to attach to a root CA or generate a self-signed certificate,
- Generation of initial certificates with an automatic enrollment process (SCEP, CMP...),
- Lifecycle management of the certificates (revocation, renewal, suspension...),
- Generation of Certificate Revocation List (CRL).

Technical Subordinate CA appliance defines different certificates profiles for:

- Root Authority Attachment: The key pair is generated by the subordinate CA infrastructure. A Certificate Signing Request (CSR) is generated and delivered to the root certification authority operator to produce the corresponding certificate signed by the root CA.
- Production of certificates for devices: A CSR is sent to the subordinate CA (either by the device or by the infrastructure manager). If the device supports automatic registration protocols (SCEP, CMP), an automatic certificate deployment can be implemented to facilitate the certificate lifecycle's management.

Technical Subordinate CA appliance includes strong internal security mechanisms:

- Access to all functional modules is controlled. Operators and administrators must be authenticated using strong authentication (with smart card or USB token).
- All actions related to the management of certificates are recorded in a database accessible only by authorized operators. All events are logged.
- Communications between functional modules and information stored in the database are all protected. Sensitive information is enciphered.
- Private keys are protected using Hardware Security Modules (HSM).

Standards and technical specifications

HSM Certifications

- Common Criteria EAL4+ compliant with CWA 14167-2-PP
- NATO SECRET
- Compliant with eIDAS
- «Qualification Renforcée» (the highest qualification from the ANSSI)
- FIPS 140-2 level 3 (in progress)

Administration

- Cryptographic profiles definition
- Secure updates of embedded software
- Load balancing capability

Physical Interfaces

- 2 Ethernet 10/100/1000BASE-T ports
- 4 USB2 ports
- 1 VGA port
- Integrated keyboard and chip card reader
- Redundant electrical supply
- Restart button on the front
- Secure RPC over SSL to Windows, Linux and AIX 32/64 servers

Technical Subordinate CA appliance

- Certificate compliance with ITU-T X.509v3, RFC 5280 and RFC 3739
- Revocation information compliance with ITU-T X.509v2 CRL
- Certification request format: PKCS#10
- Algorithms: RSA 4096 and ECDSA named curves secp224r1, secp384r1, frp256v1
- Support for SCEP and CMP automatic enrollment protocols (V1.1, V1.2)

For more information:
atos.net/en/solutions/cyber-security-products/digital-identities/trust-infrastructure-appliances

CT-201105-AS-J3515-IDnomic-Secureyou