IDnomic Root CA Appliance

Manage the top of the trust chain for a PKI

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 Root of trust

Root certificates are at the heart of secure connections and digital exchanges to validate encryption operations within a public key infrastructure (PKI). Root Certificates Authorities (CA) ensures that only official and trusted root certificates are issued to maintain secure exchanges. By verifying the identity credentials of the online users, devices or services, trusted CAs bind their identity to cryptographic keys. This helps to eliminate the threat of malicious interceptions or identity usurpations, such as man-in-the middle attacks.

A Root CA must be trustworthy as certificates signed with the issued root certificate's private key will be automatically trusted by the browsers as long as it is valid. It means that if this root is compromised, this will impact the whole trust hierarchy. That is why the Root CA will be heavily secured, kept offline and only be used to issue subordinate CAs. In a trusted certificate chain, these subordinate CAs will act as an extra layer of security as the root CA will not be required to issue certificates directly to end-users or devices.

Protect your exchanges with an appliance

Root CA Appliance enables the deployment of a trusted CA hierarchy and the safe delivery of Subordinate CAs certificates quickly and cost-effectively. Its certificate is self-signed. The private key is kept inside the state-of-the-art Trustway Proteccio Hardware Security Module (HSM) where the Root CA appliance is running. It is used to create Subordinate CA certificates and is usable by PKI's operators.

Root CA is configured for the delivery of Subordinate CAs to build a trusted CA hierarchy. The CA certificate profiles are created from defined models and can be associated with RSA or ECDSA keys. The production of CA certificates complies with the certification policy defined by the customer and is compliant with supervisory body requirements. Typical usages include creation of new requested delegated CA and production of Certificate Revocation Lists (CRLs).

Root CA Appliance helps organizations 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...).

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 **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.

A high-availability model is also available for the other trust infrastructure appliances.

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.

Root CA appliance supports the following functional modules

- Generation of Root CA and management of its life cycle during Key Ceremony,
- Generation of the initial Subordinate CA certificates,
- Renewal of Delegate CA (DCA) Certificates,
- Generation of Certificate Revocation List (CRL).

Root CA appliance defines different certificate profiles for

- Production of Root CA certificate: The key pair is generated during a key ceremony in the HSM appliance.
- Production of the different subordinate CA: The key pair is generated by the PKI where the CA is hosted (DCA PKI). A Certificate signing request (CSR) is produced by the DCA PKI and transmitted to the Root CA operator to produce the corresponding certificate signed by the Root CA through GUI.

Root CA 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

Root 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

For more information: atos.net/trust-infrastructure-appliances