



## UniCERT | Certification Authority Components

---

There are a number of modules that together perform the overall CA functionality within UniCERT. These components are the:

**(1) Certification Authority (CA)** – Generates and signs certificates and Certificate Revocation Lists (CRLs). The CA operates according to its own flexible operational policy, which is controlled by the Certification Authority Operator (CAO).

**(2) Certification Authority Operator (CAO)** – The CAO module is the Security Officer of the PKI. The CAO controls all of the administration functions and grants privileges to other UniCERT modules and operators. There can be several CAOs, with reduced rights if required.

**(3) Publisher**– the Publisher handles all the publishing requirements of the CA, including the ability to publish to a wide range of different directories (including Microsoft's Active directory) and OCSP responders, and to be able to publish to multiple directories. It supports flexible publishing schemas, and has the ability to only publish certain types of certificates.

---

### **(1) UniCERT Certificate Authority**

The Certificate Authority (CA) module is the nucleus of a PKI. All trust within the infrastructure depends upon the CA's signature. The CA operates according to its own flexible operational policy, which is controlled by the Certificate Authority Operator (CAO).

#### ***Responsibilities***

- The CA receives approved certificate and revocation requests from Registration Authorities (RAs) and CAOs, and returns certificates and confirmational messages. If selected in the registration policy, the CA sends end users' private encryption keys that are marked to be archived to the Key Archive Server (KAS).
- Certificate Signing – the CA is responsible for signing infrastructural and end-user certificates. The CA also signs certificates for both subordinate (sub) CAs and other CAs in the case of cross certification. The CA signs all revocation information in the form of CRLs, partial CRLs (CDPs) and ARLs. Optional publication of CRLs and ARLs to disk to provide an easily customisable publication mechanism.
- Message Signing – all messages sent by the CA are digitally signed. The CA verifies all messages it receives to ensure integrity and authenticity.
- Data Archival – all data and audit logs are archived in the CA's database. All information archived is digitally signed by the CA. Each entry has a unique tracking number.
- Generation of Key Pairs – the CA generates its own key pair(s).
- Unique distinguished name (Dname) and public key check – the CA can optionally check that all certificates being certified have a unique Dname and/or public key.





## **(2) UniCERT Certificate Authority Operator**

The Certificate Authority Operator (CAO) module is the Security Officer of the PKI. The CAO controls all of the administration functions and grants privileges to other UniCERT modules and operators. There can be multiple CAOs each with diminished rights if distributed control is required.

### ***Responsibilities***

- Registration Policy Creation – the CAO is responsible for the creation and maintenance of registration policies for the issuance of certificates.
- Operational Policies - the CAO is responsible for maintaining the operational policies of all the PKI modules e.g. CA, RA etc. The operational policies control how these modules operate.
- Authorization Group Maintenance – The CAO is responsible for assigning Registration Offices (WebRAOs) to Authorization Groups, and to controlling which Registration Policies can be used by a specific Authorization Group.
- PKI Design – the CAO can add new modules to the PKI e.g. new RAs, a sub CA etc.
- Certification of PKI Entities – the CAO can authorize the certification of other PKI entities, such as other CAOs, sub CAs, RAs etc. This can include generation of key for the entity if necessary.
- Revocation – Any certificate can be revoked by the CAO. The CAO can view certificates that have been issued, and can view the audit logs. The CAO communicates approved certificate requests directly with the CA; revocation requests are placed in the CA's database.
- Message Signing – all messages sent by the CAO are digitally signed. All messages received by the CAO are verified to ensure integrity and authenticity. Data Archival – all data and audit logs are archived in the CA's database. All information archived is digitally signed.

## **(3) UniCERT Publisher**

The Publisher handles all the publishing requirements of the CA.

### ***Responsibilities***

- Publication of CA certificates – the Publisher optionally publishes its CA certificates to one or more LDAP connected directories.
- Publication of CRLs and ARLs – the Publisher optionally publishes CRLs and ARLs to one or more LDAP connected directories.
- Publication of End Entity certificates – the Publisher optionally publishes end entity certificates to one or more LDAP connected directories. Control of whether end entities certificates are published, is done via configurable filters.
- Publication of CRLs to OCSP responder – the Publisher optionally publishes CRLs to Online Certification Status Protocol (OCSP) servers.

**\* For more comprehensive information, please review the UniCERT v5 Product Overview \***

