



UniCERT | Registration Authority Components

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

Registration Authority (RA) – The RA acts as a router between RA Operators (WebRAOs), Protocol handlers and the CA. RAs divide the PKI into operational domains. Each operational domain is a separate structure linked to the CA. Intra-domain confidentiality is maintained at all times. The RA obeys its own operational policy, which is maintained centrally.

WebRAO – The WebRAO's can authorize certification and revocation requests that have been sent by the Protocol Handlers, or via other WebRAOs. They can also handle face to face registrations. The WebRAOs belong to one or a number of Authorization Groups, and can only process requests associated with specific registration policies that have been assigned to their Authorization Groups by the CAOs.

Protocol Handlers – The Protocol Handlers are an extensible set of request handlers, that handle certification requests using such protocols as Web, e-mail, Cisco SCEP and PKIX CMP. The Protocol Handlers, handle the complexities of each protocol, and pass the registration (or revocation) requests into the RA for onward processing. They also return the resulting certificates.

(1) UniCERT Registration Authority

The Registration Authority (RA) acts as a router between RA Operators (WebRAOs), Protocol handlers and the CA.

Responsibilities

- The RA communicates approved end-user certificate and revocation requests received from the WebRAOs and Protocol Handlers, to the CA. It receives certificates and confirmational messages from the CA and makes them available to the WebRAOs and Protocol Handlers.
- The RA communicates certificate and revocation requests received from the Protocol Handlers to WebRAOs for authorization, and sends certificates and informational messages back to the Protocol Handlers.
- The RA is responsible for initiating end-user certificate rollover, when an end-user's certificate is about to expire and the associated registration policy dictates that a new certificate is to be issued.
- Message Signing – all messages sent by the RA are digitally signed. All messages received by the RA are also verified to ensure integrity and authenticity.
- Data Archival – all data and audit logs are archived in the RA's database. All information archived is digitally signed by the RA. Each entry has a unique tracking number.

▪ (2) UniCERT WebRAO

The WebRAO's can authorize certification and revocation requests that have been sent by the Protocol Handlers, or via other WebRAOs. They can also handle face to face registrations. . The WebRAOs belong to one or a number of Authorization Groups, and can only process requests associated with specific registration policies that have been assigned to their Authorization Groups by the CAOs.





Responsibilities

- The WebRAO can register and authorize certificate requests using Registration Policies, that have been defined by the CAOs, for their Authorization Group. Under the control of the Registration Policies, the WebRAO can register and authorize a face to face certification request, including optionally generating end user keys on a token or in software.
- Under the control of the Registration Policies, the WebRAO can authorize or reject a certification request received from the Protocol Handlers. The WebRAO can also provide additional authorization for certification request received from other WebRAOs or ARM. It can also authorize revocation of a certificate issued against a Registration Policies that have been defined by the CAOs, for their Authorization Group.
- Message Signing – all messages sent by the WebRAO are digitally signed. All messages received by the WebRAO are also verified to ensure integrity and authenticity. All data and audit logs are archived in the RA's database. All information archived is digitally signed by the WebRAO. Each entry has a unique tracking number.

(3) UniCERT Protocol Handlers (PH)

Protocol Handlers - The Protocol Handlers are an extensible set of request handlers, that handle certification requests using such protocols as Web, e-mail, Cisco SCEP and PKIX CMP.

Responsibilities

- The Protocol Handlers, handle the complexities of the various certificate management protocols, and pass the registration (or revocation) requests into the RA using a common internal format. Each request is automatically associated with a registration policy (which is then used to control its authorization path etc.)
- If allowed by the registration policy, the Protocol Handlers receive the certificates back from the RA and communicates them to the end user according to the methods allowed by the protocol handler.
- The email PH retrieves certificates requests in PKCS#10 or PEM format from a POP3 store. The email PH sends back certificates in PKCS#7 (certificate chain), X.509 (binary) or PEM format via a SMTP server. The email PH also distributes email notices, where these have been set up in a registration policy. Email notices can be configured to be sent out for any of the following status:
 - Pending - certificate request has been received into system,
 - Rejection - certificate request has been rejected,
 - Pickup - send out a URL where the certificate can be retrieved,
 - Renewal - warns that a certificate is about to expire,
 - Certificate - which includes a certificate in response to a certificate request (which may have been requested by another registration method), or from auto renewal via the system.
- The Web PH provides registration pages, which are dynamically built from the registration policies. Via these request pages customers may request certificates via the major browsers (Netscape and Microsoft IE) and via PKI-aware applications capable of generating PKCS#10 certificate requests (e.g. Web servers). The Web PH is able to distribute certificates that have been requested via the Web PH, or where web distribution has been configured in a registration policy.
- Where allowed by the registration policy, the Web PH supports end-user revocation by providing revocation specific web pages. End users may revoke or suspend their own certificate and must supply a password in order to perform this function. The Web PH, also enables users to query the status of the certificate, and to download CRLs.
- The SCEP PH receives Simple Certificate Enrolment Protocol (SCEP) requests directly by sockets and returns the certificate in the same manner. SCEP is the certificate request and retrieval method used by Cisco and other VPN vendor devices and software.
- The PKIX CMP PH handles registration and revocation requests and responses in accordance with the PKIX CMP protocol. This PH is typically used with remote registration/authorization applications written using the Baltimore PKIX CMP client.

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

