ODYSSEY
cryptic by intent

Odyssey Certrix FAQs

Odyssey Technologies Ltd

1. What is Certrix?

Odyssey Certrix is a Certification Authority (CA) Server that issues and manages digital certificates. Managing certificates includes activities like revocation, renewal, suspension, and re-activation. Certrix uses PKI for issuing certificates in a secure and trust-worthy manner.

Odyssey Certrix suite of products provides a comprehensive solution that enables any organization or Trusted Third Party to run their own Certification Authority.

Certrix Suite:

Extended Registration Authority (ERA) server

The ERA server provides the interface between a user and the Certification Authority. It is a single monolithic web-enabled server to enable registration of subscribers over extended geographic areas.

Certification Authority (CA) server:

The CA server issues different classes of digital certificates. Subsequent certificate management activities like revocation, renewal, suspension and reactivation are also carried out in this server.

Signing server:

The Signing server carries out CA signing operations for issuing digital certificates. The signing server securely stores the signing key(private key). This server is capable of isolating itself automatically from other components to protect the signing key against possible attacks.

2. How does it benefit my business?

- Certrix suite of products is comprehensive and provides a turnkey software solution to meet certification needs of enterprises as well as trusted third parties.
- The ERA server provides a cost-effective solution for registering certificates across a wide geographical area. Instead of running multiple RA servers and enforcing identical configuration on all of them, the certrix suite uses a single web enabled Registration Authority server.
- The cost of training and coordinating the Registration Authority operators is greatly reduced due to the intuitive web enabled RA interface.

- For enterprises, running a certification authority inhouse reduces the cost of buying certificates from Trusted Third Parties like Verisign, TCS, etc.
- Certrix administrators are themselves authenticated into the system using digital certificates. Certrix ensures admin accountability by enabling all admin activities to be signed and logged.
- The entire communication process between ERA , CA server and signing server is carried out through SSL channel, therefore ensuring secure communication.
- Certrix ensures accountability through its comprehensive logging and reporting features like:

  - *Admin Activity Report:-*

    Contains detailed administrator activity report. The report contains details of the admin activity type, action type, status, action time and IP address from where the activity was carried out.

  - *Certificate Request Report:-*

    Contains detailed report about every registration, renewal or revocation request.

- Certrix also has a mailing component for enabling businesses to intimate and update clients.

  - *Certificate Readiness Intimation Mail:-*

    Once the certificate is ready and available in ERA server for the subscriber to download, an intimation mail will be sent to the subscriber along with the certificate download link.

  - *Certificate Expiry Intimation Mail:-*

    Option for sending expiry intimation mail is provided in ERA server for the subscriber to initiate the renewal request.

3. How does ERA work?

The ERA Server provides the interface between the subscriber and the CA. It is a single monolithic web-enabled server to enable registration of subscribers over extended geographic areas. Users of this system are known as agents. The system can support one single RA to thousands of RA agents. These Registration Agents hold access rights for configuration changes like importing policy class and adding virtual RAs.

An agent can register for certificate application. To make this process secure and reliable, the agent is authenticated using his digital certificate.

Depending on his registration rights, the agent would be able to access the pages from the ERA server.

The Agent then enters the applicant's details including photographs and fingerprints if required by policy. The Agent adds the user's CSR to the form and digitally signs the entire form with his own certificate and finally sends the form to the CA server.

4. How does the subscriber registration process work in ERA?

Face to Face registration with CSR

The agent collects the application form, verifies the document and uploads the CSR submitted by the subscriber to ERA server. The subscriber is mapped to this agent and the certificate quota will be appropriately reduced from this agent.

Face to Face registration without CSR

The agent collects the application form, verifies the document and uploads the details to the ERA server. The subscriber submits the CSR through the subscriber interface.

Face to Face application form collection

The Agent provides the application form and also the registration number assigned for that subscriber. The subscriber provides the registration details and CSR through subscriber interface with the registration number provided by the agent.

Subscriber submits the request without binding them to an agent

The subscriber submits the request in a virtual RA. Agent with rights for approving this type of request can verify and acknowledge the document.

5. Does the CA have options for manual intervention?

Yes. The CA operates in both manual and automatic mode.

Manual Mode:

The CA operators have to login and verify each request and then accept / reject them.

Automatic Mode:

The Certrix CA Server signs all the requests without any manual intervention.

6. How does the signing server work?

Certrix supports a separate signing server for signing the certificates.The signing key will reside only in this signing server to ensure absolute protection. For every policy class, a different signing server can be configured.

The signing server is capable of automatically detaching itself from the rest of the network when signing a certificate. This is to protect the signing key from potential attacks. The signing key is protected in HSM format.

7. On what platform does Certrix run?

The Certrix Server runs on Linux platform. Supported databases include Oracle and MySQL.

8. How long does it take to deploy Certrix?

We have successfully deployed Certrix within two weeks!

9. What is CerTrust?

Odyssey CerTrust

Odyssey CerTrust is a comprehensive validation solution for managing digital certificates, including an OCSP (online certificate status protocol) Responder for providing real-time certificate status, a messenger for downloading and posting revocation information, and APIs for integration with custom applications.

The OCSP server responds to the relying party about certificate status:

Good - States that the certificate is not revoked.

Revoked- States the time and reason of revocation.

Unknown- States that the CA of the certificate is unknown.

Certrust runs on 64-bit Linux with Kernel 2.6.

10. What is ClockTix?

Odyssey ClockTix server is a fully scalable, standards compliant time stamping server that responds to RFC 3161 requests with time-stamp tokens. The server supports requests in multiple transport mechanisms including Email, HTTP, and TCP and could keep time accurately by relying on any of the established time sources such as GPS, NTP or atomic clocks.

ODYSSEY TECHNOLOGIES LTD.
5th Floor, Dowlath Towers, 63,Taylors Road, Kilpauk, Chennai – 600 010
Telephone : +91 44 26450082, 26450083, 43084070, 43084080
e-mail : info@odysseytec.com