Odyssey

ERA Server

Odyssey ERA Server

Trustworthy registration practices from the backbone of any dependable Public Key Infrastructure. Good registration practices are easily implemented at a small enterprise level where all the users are likely to be in specific geographic locales. But for the truly disbursed set of users like the customers of a large bank or the citizens under an e-Governance initiative, registration of users can turn into a logistic nightmare with traditional Registration Authority software. Apart from the cost of setting up and maintaining a large number of geographically disbursed registration facilities, the sheer cost of training and coordinating the Registration Authority operators can quickly outweigh the cost benefits of the PKI itself.

Odyssey Extended Registration Authority Server (ERA) offers a secure and cost effective solution to all your registration logistics or problems. Instead of keeping multiple RA servers and enforcing identical configuration on all of them, this product uses a single web enabled Registration Authority Server working to offer the most flexible and trustworthy solution.

ERA Server– Functional Architecture

Odyssey ERA server sits atop a standard web server and has simple HTML based configuration interface that lets the administrator configure the registration details that need to be obtained from each applicant. Where used with Odyssey Certrix CA , it will also import the configuration information from the CA directly.

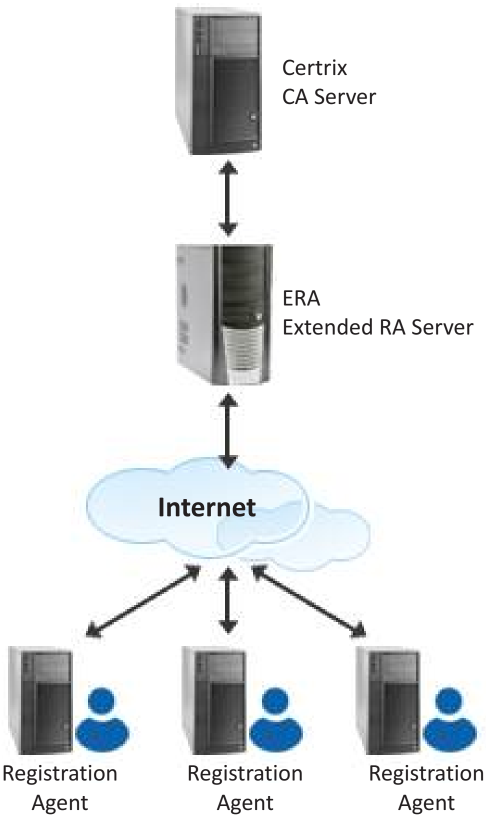
The users of this system are called Registration Agents. The system can support from a single Registration Agent to thousands of such agents. The rights of the Agents in the system are again classified as delegatable or terminal. While both the class of users can register prospective applicants for issue of certificates, the delegatable agents can create other delegatable or terminal agents.

When a prospective certificate applicant approaches an agent for registration, he can do so with his key pair already generated in his own secure system or it may be generated in the Agent's system itself. The Agent logs on to the ERA server over a secure SSL channel. The agent is also authenticated using his digital certificate. Depending on his registration rights, he would be able to access the pages from the ERA server.

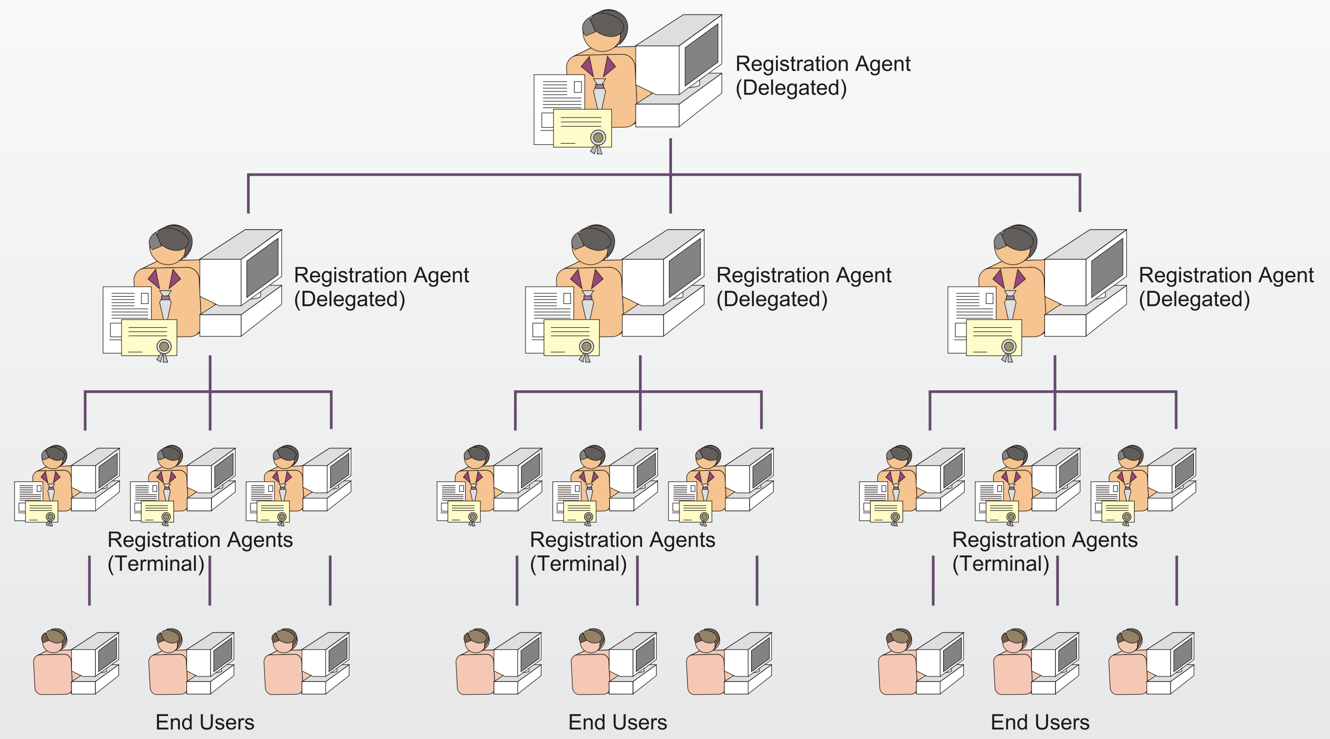
The Agent then enters the appropriate details of the applicant user including photographs and finger prints if required by the policy. He then adds the user's CSR to the form and digitally signs the entire form with his own certificate.

The ERA server then updates its databases and passes on the request to the CA for certification. Since all the certificate requests are archived along with the Registration Agent’s signature, a clear audit trail is available at any time to establish non-repudiation by the Agent.

Extended RA server Model



Registration Agents – Hierarchial Model


Registration Agent (Delegated)
Registration Agent (Delegated)
Registration Agent (Delegated)
Registration Agent (Delegated)
Registration Agents (Terminal)
Registration Agents (Terminal)
Registration Agents (Terminal)
End Users
End Users
End Users

How Registration Agents are created?

A prospective Registration Agent should already posses a digital certificate issued by the system. He approaches an existing Registration Agent with delegatable powers. This agent logs on the appropriate page in the ERA server and registers the new Agent's certificate and any additional details that may be required. As simple as that!

Where can ERA be used?

Take the case of a large Bank with hundreds of branches across the country. In the normal scenario, RA systems would have to be deployed in each of the branches to register the customers there with ERA server; the highest official of the bank registers the Regional Manager and makes the Registration Agents as well. They in turn register the Branch managers who are again made Registration Agents. Now these managers can proceed to register the actual customers of the bank.

With this cascading model, a Bank with a few thousand branches will be able to deploy a complete PKI in a matter of weeks. Contrast this with the wholly unsatisfactory deployments that take two to three years!

And think of all the cost savings that arise out of operating a single facility!!

Security of ERA

Since the deployment of PKI itself is PKI enabled here, it ranks the highest in security.

The ERA server, by itself takes care of authentication, signature verification and CRL checking for any agent.

ODYSSEY
Cryptic by intent

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