

Case Study

Controller of Certifying Authorities (CCA)



█ Promoting the growth of eCommerce and eGovernance through the widespread use of digital signatures. The CCA at the root of the trust chain in India's national PKI.

The trust root of India's national PKI relies on Nexus technology

The governmental organisation Controller of Certifying Authorities (CCA) aims at promoting the growth of eCommerce and eGovernance through the wide use of digital signatures in India. To enable the mutual recognition of digital signatures among various organisations in industry and government, a nation-wide PKI has been planned with a national root Certificate Authority at CCA. Nexus Origo Certificate Manager has been chosen by CCA to be the trusted platform of the Root Certifying Authority of India (RCAI). The product's advanced security, standard compliance and flexibility have played major roles in the decision.

IT Act, 2000 - Promoting "eGrowth" with trust

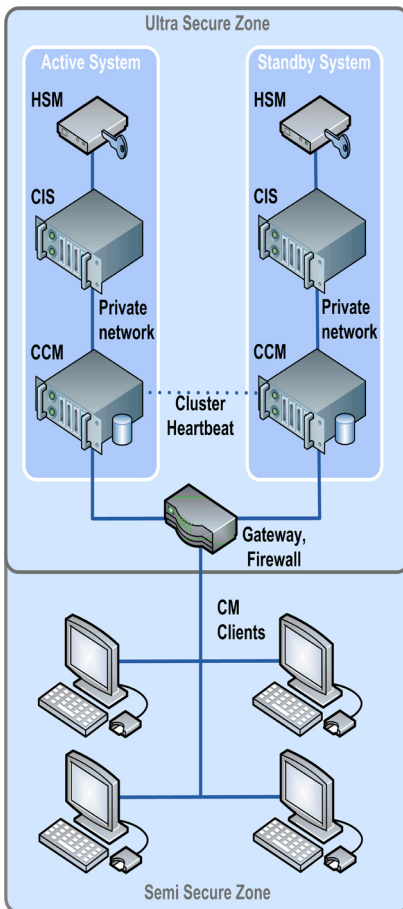
Controller of Certifying Authorities (CCA) is a governmental organisation located in New Delhi, India. CCA has been appointed by the Central Government under section 17 of the IT Act, 2000 and came into existence on 1st November 2000. CCA aims at promoting the growth of eCommerce and eGovernance through the wide use of digital signatures. Their mission is to create trust in the electronic environment through the development of necessary policy instruments and an interoperable infrastructure under the various provisions of the IT Act, 2000. The Act provides the regulations and guidelines for the issuing and usage of digital certificates, the necessary means for digital signatures. For this reason CCA set up the Root Certifying Authority of India (RCAI). Organisations and end users willing to create electronic signatures, shall receive their certificates from licensed CAs, while the licensed CAs receive their certificates from the RCAI. In this way the RCAI serves as trusted root for the validation of electronic signatures. The RCAI is furthermore responsible for providing revocation status information (CRLs) of the licensed CAs.

Certificate management platform

CCA was looking for a solution that provides a trustworthy, standard-based and open system for the production and management of electronic certificates. Nexus Origo Certificate Manager has been chosen for its flexible design, strong security framework and compliance to PKI standards. The platform is flexible, multi-CA capable and covers GUI-based support for various processes such as:

- management of CA keys and policies
- management of CA users (security administrators and operators)
- user key management, registration, certificate production, CRL production, token/card management, PIN letter printing, certificate publication and distribution, emailing
- secure creation and storage of Root CA keys
- cross-certification for licensed CAs





The production site, illustrated above, is deployed in New Delhi in a highly secure facility. Data is constantly replicated to the disaster recovery site located in Bangalore.

System overview

The production site is installed in a high security facility and consists of two Origo systems in an active/passive mode in order to ensure high availability. The two systems are constantly mirrored to keep data consistent at all times. Either of the two systems can be active without any difference in functionality. HSMs supporting the security level FIPS 140-2 create and store securely the root CA's private keys. A second location in Bangalore accommodates a disaster recovery site, which can immediately take over the production in case of an event that sets the production site out of order. The recovery site is the production site's exact replica.

Realisation in close cooperation

The project was carried out together with a local partner, who led the project locally according to a multi-stage project plan. Nexus was the responsible supplier of the CA software and provider of expertise within the PKI area. Emphasis has been put on transferring knowledge to the local partner as well as to the team of CCA. A consultant from Nexus was on site in New Delhi on a number of occasions to install and configure the software. Nexus' role was also to advise in technical and organisational issues as well as to help setting up proper processes to maintain safe CA operation. A comprehensive training program was carried out on site to ensure that CCA's personnel would be able to operate and maintain the entire system on its own. The system now operates in an ultra secure facility with no access for non-authorized staff. Over the years the system has been upgraded several times to up-to-date versions of the Origo software.

Results and prospects

The successful project of CCA has enabled more PKI related projects in the large and growing Indian IT market. With the extensive use of digital signatures the need for signature validation services grows. While the validation function has usually been implemented within the relying software, it is reasonable to externalise this complex and sensible function to a central server. CCA is investigating the possibility to set up a standard-based trusted validation service within the RCAI's framework.

