

PKI Digital Certification

General Description

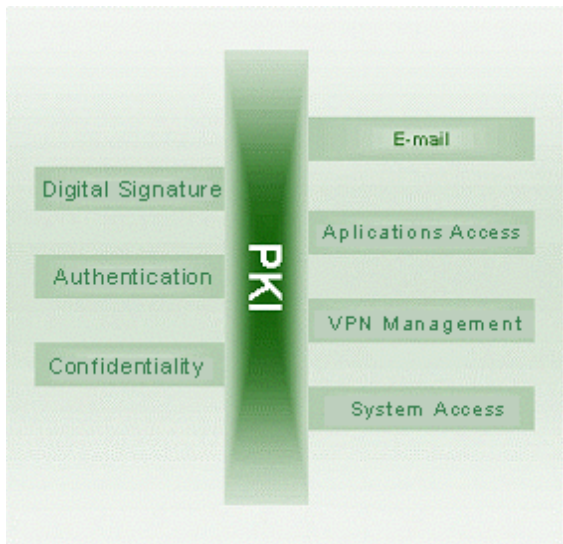
Realsec's PKI family of products provide complete solutions to generate digital certificates with recognition from any public or private service provider, with the choice of most suitable combination for each enterprise.

It also provides a toolkit that will allow any customer application to operate and manage the containers where the certificates are securely stored and insert these certificates into all customers applications that require additional security services based on digital certificates.

The use of digital certificates into current applications will add important security values like:

- Confidentiality.
- Digital signature of message content.
- Strong Authentication.

The security and custody of the Keys is guaranteed by the use of our HSM Cptosec both for CA's and RA's.



OpenSecure CA

Technical Features:

- Root and intermediary CA including Hierarchy support .
- Generation of x509 v3 & CRLs v2 certificates.
- 512, 1024 & 2048 RSA Key generation.
- Support of PKCS#10, for certification requests generation (PEM or DER format).
- Graphic user interface for configuration and management tasks.
- Connection capabilities CA->RA by using standard protocol PKIX.
- Support of private certification extension capabilities.
- Publication of certificates and CRLs in any directory following LDAP standards.
- Information Logs generation of transactions, CA status and global management functions performed.
- Remote RA administration by using HTTPS.



OpenSecure RA

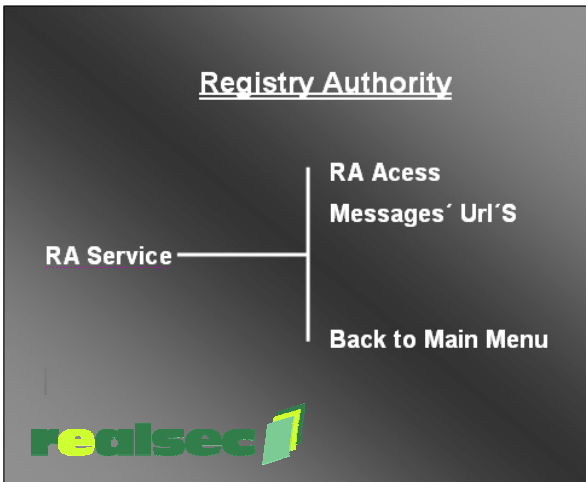
The Registry Authority is conceptually divided into the following components:

✦ **RA Service (dispatcher).**- In charge of managing user's and RA's operator's requests (certifications, repeals, renovations, etc...).

✦ **Administration Pages.**- ASP pages in charge of all the administration tasks associated with the RA, policy management, prevalidations, reports and so on...

✦ **User Pages.**- This group is composed by the ASP pages of certificate request and they are the RA interface with the public.

✦ **Dispatcher configuration Tool.**- It is in charge of configuring the required data for the RA dispatcher.



Technical Features:

✦ The Registry Authority acts like an intermediate entity between the customer and the Certification Authority.

✦ It provides a robust and friendly management of certificates (x509/v3), transactions, user's certification policy, server's certification policy, repeals, management of distributed policies, access control and user's authentication, etc... through a web interface.

✦ Remote administration provided by a secured web interface.

✦ Operations Hierarchy.

✦ Fullfilment of standard certificates X509/v3.

✦ Certification's Policies that will allow for different certificates generations, based on its use (web server certificates, certificates for digital signature and encryption of messages S/MIME, etc..)

✦ Different certification Policies for several CA's with communication capabilities among them.

✦ Reports generation and management about:

- Online Certification Requests Registry.
- Administration of generated certificates.
- Key generation and cryptographic services based on our FIPS 140-2 Level 3 Certified HSM, Cryptosec.



Realia Technologies, S.L.

info@realsec.com

www.realsec.com