



Gerenciamento de Certificados Digitais EVO

Principais Módulos

EVO® CA

- Responsável pela geração de certificados a partir das requisições de certificações originadas pelo EVO® RA.
- O modelo implementado está baseado no conceito de lote, isto é, processa lotes de entrada contendo requisições de certificação ou revogação e gera lotes de saída contendo certificados ou listas de revogação.
- Um lote de entrada é uma seqüência de requisições de certificação e/ou revogação de um certificado previamente emitido.
- Um lote de saída é uma seqüência de certificados associados um a um com as requisições de certificação e/ou lista de certificados revogados.
- Pode emitir certificados para diversas políticas de certificação diferentes de acordo com as necessidades da solução.
- Permite geração de chaves RSA de até 4096 bits.

EVO® RA

- Responsável pelo gerenciamento do registro dos usuários e suas requisições. É o componente do sistema de certificação que tem contato direto com os usuários, e gerencia o ciclo de vida de um certificado.
- Permite aos operadores solicitar emissão, renovação e revogação de certificados, com todas as ações registradas.

EVO® Off-line

- Módulo integrado com o EVO® RA, que permite recepção de requisições de certificação e entrega de certificados em processo de lote. Desta forma, é possível operar a Autoridade Certificadora sem que esteja on-line, elevando a segurança por prevenir ataques remotos.

EVO® Gateway

- Módulo que gerencia a comunicação das diversas RAs com a CA;
- Suporta múltiplas RAs simultaneamente;
- Publicação em LDAP através de conexão segura SSL;
- Efetua publicação de Certificados em repositório LDAP;
- Efetua publicação de LCR em repositório LDAP;
- Efetua notificação por e-mail de:
- Emissão de Certificado;
- Renovação de Certificado;
- Revogação de Certificado;
- Efetua autenticação de usuário via smart-card;

- *Suporta os principais HSMs do mercado;*
- *Suporta sincronismo de base de dados com a CA;*
- *Efetua comunicação com CA através de canal Seguro SSL (Modo Online);*
- *Efetua comunicação com CA através de arquivos de Lote (Modo Offline);*
-

Requisitos de Hardware e Software

O equipamento mínimo sugerido é um Pentium IV 1 GHz, ou equivalente, com 512 Mb RAM. O EVO® é facilmente instalado em diversos sistemas operacionais (NT, 2000, Windows 95/98, Linux, Solares, etc).

Requisitos de Comunicação

Protocolo TCP/IP.

Padrões Implementados

X.509 v3, CRL v2, PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#11, PKCS#12, CMP, OCSP, LDAP

Algoritmos Suportados

3DES, IDEA, RC4, RSA, DSA, Diffie-Hellman, MD5, MD2, SHA-1

Arquitetura do EVO

CA Engine - Módulo responsável pela geração e revogação de certificados, emissão de lista de certificados revogados e administração das chaves da CA.

CA Offline - Módulo responsável pela comunicação offline (arquivos batch) do gateway com a CA.

Gateway - Módulo responsável por intermediar a comunicação da Autoridade de Registro com a Autoridade Certificadora.

RAO - Operador da Autoridade de Registro. Solicita emissão, revogação de certificados.

X.500 Repository - Repositório público onde fica disponível relação de certificados emitidos e revogados.

