Treinamento

Certificação Digital + Criptografia

O Treinamento de Certificação Digital e Criptografia da e-Sec é focado nas equipes das organizações e abrange fundamentos, operação, administração e desenvolvimento de soluções que utilizem certificação digital e/ou criptografia. Os treinamentos são elaborados de acordo com as demandas específicas de cada organização, adaptando-se conforme as necessidades dos clientes.

Programação em Certificação Digital – EVO-SDK

Este curso abordará o uso da Biblioteca EVO-SDK de Certificação Digital no desenvolvimento de aplicações Java de forma fácil e segura. O EVO-SDK provê um conjunto de componentes que facilitam a integração da certificação digital em Aplicações Web, bem como simplifica um conjunto de procedimentos, tais como validação de certificados, gerenciamento de certificados confiáveis e Lista de Certificados Revogados.

Outro ponto forte deste curso é o uso do suporte aos padrões de assinatura digital CAdES e XAdES conforme definidos pela ICP-Brasil, incluindo o uso de Políticas de Assinatura e LPA (Lista de Políticas Aprovadas).

Pré-requisitos: Programação em Certificação Digital – Java

Carga horária: 30h

- Entendendo o EVO-SDK
  - O que é o EVO-SDK
  - Principais Módulos
  - Principais Funcionalidades
  - Integração JCA/JCE
    - Provider "J128"
    - Provider PKCS#11
  - Instalação e Configuração do EVO-SDK
- Manipulação de Certificados Digitais
  - Leitura e Geração de Certificados Digitais X.509
  - Acessando as extensões de um Certificado
  - Acesso aos dados específicos da ICP-Brasil
  - Gerenciamento de Certificados Confiáveis
- Manipulação de LCRs (Lista de Certificados Digitais)
  - Leitura e Geração de LCRs

- Verificação de revogação de certificados
- Gerenciamento Automático de LCRs

- Cadeias de Certificados
  - Validação de Certificados Digitais
  - Construção de Cadeias de Certificados
- Selos Temporais
  - Entendendo o Protocolo TSP (TimeStamping Protocol)
  - Geração de uma Solicitação de Selo Temporal
  - Persistência de um Selo Temporal
  - Validação de um Selo Temporal
- Repositórios de Chaves e Certificados
  - Utilização dos CryptoDevices
    - PKCS#12 (Arquivo)
    - MSCAPI (Windows)
    - PKCS#11 (Hardware)
  - Recuperando chaves e certificados de diferentes repositórios
- Padrões de Assinatura Digital
  - O Padrão PKCS#7 (CMS)
    - Assinatura de Arquivos
    - Envelopes Digitais
  - O Padrão XMLDSig
    - Assinatura de arquivos
- Assinaturas de Longa Duração
  - Suporte ao CAdES
    - Recordando as Políticas de Assinatura
    - Assinatura baseada em Políticas
    - Políticas de Assinatura na ICP-Brasil
      - LPA
  - Suporte ao XAdES
    - Assinatura baseada em Políticas XAdES
- Integrando Certificação Digital em Ambiente WEB
  - O módulo SDK-WEB
    - Principais Funcionalidades
  - Autenticação baseada em Desafio/Resposta
  - Autenticação baseada em HTTPS
  - Assinatura de Arquivos via WEB
    - Entendendo as Principais Configurações
    - Escolha do Modo de Operação
      - Com ou sem Interface Gráfica
      - Upload ou Download do documento sendo assinado
      - Padrão de assinatura: PKCS#7, XMLDSig ou CadES
  - Gestão de Dispositivos Criptográficos