sages

Course code: **PKI**

Course title: **The Public Key Infrastructure (PKI)**

Days: 3

Description:

Course intended for:

The training is intended for persons wishing to get familiar with the issues of the Public Key Infrastructure. It is particularly recommended for programmers, administrators and security officers, who will be dealing with digital signatures and other services based on PKI.

Course objective:

The participants will get familiar with the basic information protection services and the modes of use of these for the purpose of development of the Public Key Infrastructure. The trainers will discuss the cryptographic mechanisms and their designation and present the legal aspects, associated with PKI services in Poland and in the European Union. During the training, the participants will configure and launch their own certification center, which will be used for handling of certification submissions for the purpose of issue of certificates for public keys using RSA, DSA, ECDSA algorithms of various designations. They will also get familiar with practical aspects of services associated with PKI, such as digital signature, authentication in the SSL/TLS protocol, the certificate status verification server (OCSP), time stamping server (TSA).

In particular, in the practical tasks, the participants will get familiar with the basic cryptographic mechanisms and the entire process associated with the public key certificate life cycle and the associated services (OCSP, TSA server). The workshop will be based on the OpenSSL library.

Requirements:

The training participants are required to have some computer handling skills, using Windows or Linux.

Course parameters:

3*8 hours (3*7 net hours)

The training consists of lectures and workshops.

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: office@sages.io web: www.sages.io

sages

Course curriculum:

1. Information protection services

    I. Basic information protection services – integrity, confidentiality, authentication and non-repudiation

    II. Shortcut functions

    III. confidentiality

        Symmetric algorithms

        Asymmetric algorithms

    IV. Storage of cryptographic data

        ASN.1

        DER and PEM encoding

    V. Digital signature

        Legal aspects in Poland and the European Union

        Key generation

        Signature development

        Signature verification

    VI. The problem of safe storage of a private key

        Key repositories

        Intelligent cards

        Hardware security modules (HSM)

        Access to cryptographic equipment (PKCS #11 libraries, CSP)

    VII. Key authenticity problem

    VIII. A trusted third party (TTP)

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: office@sages.io web: www.sages.io

A list of trusted suppliers (TSL)

IX. Current recommendations for cryptographic mechanisms used in PKI (algorithms, key lengths)

2. Public Key Infrastructure components

I. PKI Architecture

Registration Authority (RA)

Certification Authority (CA)

Repository

II. PKI services in the context of information protection services

III. Generating of keys and certification submissions

IV. X.509 certificates

Basic certificate fields (distinguishing name, validity dates)

Certificate extensions

Right certificates

Extended validation certificates

Certification policy

Certificate life cycle

Certification path

V. Certificate revocation

List of revoked certificates (CRL, delta CRL)

Certificate status verification protocol (OCSP)

VI. Time stamping service (TSA)

3. Practical use of the PKI infrastructure

I. Signing of documents

II. Safe mail

III. Signing of applications (e.g. Java applets)

IV. Server and client authentication in the SSL/TLS protocol