Course code: **J/KRYPT**

Course title: **Java platform-based cryptography in practice**

Days: 3

Description:

Course intended for:

The training is intended for programmers developing applications in the Java environment, in which it is necessary to use encryption mechanisms.

Course objective:

The participants will be able to use properly the encryption mechanisms in the Java environment, in particular, the additional functions provided by the Bouncy Castle library. The trainer will discuss the individual areas of application of cryptography, such as confidentiality, integrity, message authentication codes, encryption with a password, the electronic signature algorithms, infrastructure of the public key, protocols for safe e-mail and secure communication. For each of the topics listed, its implementation on a Java platform will be discussed, using examples practiced by the participants in form of short programming tasks. The participants are to prepare, among others, applications for management of keys and certificates in the public key infrastructure and a server and client program, communicating using the SSL protocol.

In particular: By performing practical tasks, the participants will get familiar with the issues of development and implementation of secure applications using the available encrypting mechanisms in Java.

Requirements:

The training participants are required to have the Java programming skills (to be learned at the course J/JP) and basic knowledge regarding objectives of use of specific encryption mechanisms. It is possible to conduct an extended training, during which the Users will also get familiar with encryption techniques aimed at data protection.

Course parameters:

3*8 hours (3*7 net hours) of lectures and workshops (with a visible emphasis on workshops).

5*8 hours (5*7 net hours) – an extended training – an additional detailed explanation of the principles and use of encryption techniques used.

Group size: no more than 8-10 participants.

Course curriculum:

1. Training curriculum JCA and JCE - basic architecture, suppliers, protection policies
2. Installation and configuration of the Bouncy Castle library
3. Symmetric algorithms – use of block and stream ciphers
4. Hash functions – establishing of message hashes
5. PBE (Password Based Encryption)
6. MAC (Message Authentication Code), HMAC (Keyed-Hash Message Authentication Code) – Authentication of data sources
7. ASN.1 notation – designation, encryption modes, cryptographic object storage
8. Asymmetric algorithms - RSA, Diffie-Helman
    I. Use of algorithms for electronic signatures (RSA, El Gamal, DSA) – key generation, signing operation, validation
    II. Use of algorithms for message encryption (RSA) – key generation, encryption, decryption
9. Elliptic curve algorithms – key generation, signature, signature validation, encrypting, decrypting
10. Public key infrastructure - X.509 certificates
    I. Generating and storage of certificates
    II. Validation and invalidation of certificates
    III. Use of CRL lists and the OCSP protocol
11. Management of keys and certificates – use of key repositories
12. CMS and S/MIME protocols – preparation of data securing applications, electronic message exchange applications
13. SSL and TLS protocols – preparation of applications for secure communication

14. Access to cryptographic equipment through the PKCS #11 interface
15. Java Card cryptographic card applications

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