Digital Signature Training Programme

A *Strategic Planning*

B *Roadmap to Success*

C *Achieving Success*

Achieving Interoperability of Digital Signatures

Our Digital Signature Training Programme consists of three independent workshops. The workshops are designed for IT professionals, technology decision makers, information security experts and managers as well as decision makers responsible for strategic planning. The workshops have separate focus areas for all interested parties to choose from the best corresponding agendas and objectives.

The training programme gives a comprehensive overview on the nature and operation of digital signatures, it establishes a good understanding of different standards and their practical implementations and it gives a practical approach to all the functional features that are enabled by different digital signature systems. The programme gives tools to understand the legal and technical requirements that relate to digital signature acceptance and interoperability, and maps these requirements to business needs. You will get a good understanding of what requirements and objectives should be set for evaluating digital signature systems when purchasing systems, conducting security audits, calculating total-cost-of-ownership and planning system lifecycle management.

Workshop 1: Interoperability, Digital Signature Practices and Standards

The objective of this workshop is to give a comprehensive overview on the nature and operation of digital signatures. It will explain the different standards and their practical implementations. The workshop answers the questions: what are digital signatures; how are they used; what do they enable and how do they integrate with internet applications.

Agenda:

1. **Jump-start to PKI and the concept of non-repudiation**
2. **Governing signature principals**
   - 2.1. The hand-written signature
   - 2.2. The electronic signature
3. **Electronic and digital signatures**
   - 3.1. Features
   - 3.2. Usability and comparative advantages
   - 3.3. Signature types and applicability with different workflow-processes
4. **Digital signature technologies**
   - 4.1. Different signature formats
   - 4.2. Effects of different formats on technologies and processes
   - 4.3. Commercial considerations
5. **Relationship between European ETSI signature format standards and international Internet standards**
   - 5.1. ETSI and IETF RFC
   - 5.2. ETSI and W3C
   - 5.3. ETSI and OASIS
   - 5.4. ETSI and HL7 with IHE

Workshop 2: Digital Signature Systems

This workshop is intended for IT professionals dealing with IT security, Identity Management and legal compliance issues. The workshop is split in two focus areas: part A and part B. The objective of the Workshops 2A and 2B is to give a comprehensive overview of the different technologies, solutions and systems used for implementing, creating, validating and managing digital signatures.

Workshop 2A: Signature Types

Objective: The workshop concentrates on the various signature implementations and requirements governing the application of digital signatures. The workshop gives a good understanding of all the functional features that are enabled by different digital signature systems.

RegioPKI®

Workshop Agenda:

1. Jump-start to digital signature standards and technologies

2. Standard digital signature formats: what and why?

2.1. PKCS#7, CMS, XMDLSig and XAdES signatures
2.2. S/MIME and e-mail signing
2.3. Requirements for a legally binding signature (EU Directive)
2.4. Long term validity
2.5. Signature validation and signature renewal

3. Signature types

3.1. Enveloped signatures
3.2. Enveloping signatures
3.3. Detached signatures

4. Signature models

4.1. Simple-Single signature
4.2. Select-Single signature
4.3. Simple-Multiple signatures
4.4. Select-Multiple signatures
4.5. Simple-Hierarchy signatures
4.6. Multiple-Parallel signatures
4.7. Modify-Multiple signatures

5. Signature methods

5.1. Decentralised client-based signature solutions
5.2. Centralises signing solutions
5.3. Mass / batch process signing solutions
5.4. Centralised system signing solutions
5.4.1. System certificate signing
5.4.2. Timestamps

Workshop 2B: Interoperability and Integration with Business Applications

The objective of this workshop is to explain the legal and technical requirements that relate to digital signature acceptance and interoperability, and how these requirements are mapped to business needs. The workshop gives a good understanding of what requirements and objectives should be set when evaluating digital signature systems for acquisition, security audits, total-cost-of-ownership calculations and system lifecycle management planning. Workshop Agenda:

1. Interoperability

1.1. Interoperability of digital signatures
1.1.1. Technical and legal interoperability
1.1.2. European and national requirements
1.1.3. Sector specific requirements: case healthcare
1.1.4. Requirements for validation services
1.2. Digital signature object interoperability
1.2.1. Signature types
1.2.2. Platform independence
1.2.3. Use of integration profiles (case healthcare: IHE)

6. Digital signature profiles

1.3. OASIS profiles
1.4. OSCI profile (case Germany)

7. Requirements for a digital signature system

1.5. Compliance with standards
1.6. Usability and functionality
1.7. Platform independence
1.8. Visual representation and information security
1.9. Integration with Workflow-processes
1.10. Modularity

Training Organisation

Target groups: IT professionals, technology decision makers, information security experts and managers, decision makers responsible for strategic planning.

Training location: *At customer's location and premises. No travel fees are charged in Brussels and Helsinki areas. Ask also for in-house training options.*

Group size: 5 - 20 persons

Duration: Each workshop is designed for 1 training day. The workshop 2 training sessions can be stretched to three full days with practical exercises. Please ask for further details on the exercises.

All training attendees will receive a participation diploma.

Your IT Security Partner

EuroConseils Sprl offers highly skilled consultancy and advisory services and solutions for public and private organisations in the strategic area of trust, security and identity management. We offer only solutions based on the most innovative, advanced and proven best practices and standards with highest conceptual and technological security levels to protect any valuable asset, data and user privacy.

These training sessions are carried out in close collaboration with our technical service partner XCure Solutions Ltd., which is an expert organisation formed by highly qualified and experienced IT security professionals. Together our professionals offer a wide range of expert services in fields of IT security management, security audit and design, security application development and integration, and system implementation. Our team brings together a wealth of experience in complex IT Security services. All our professionals are CISA and, or CISSP certified.

The RegioPKI® Platform

RegioPKI®

The RegioPKI® platform service gives a comprehensive approach to regionally developed, initiated and completed eServices. It enables a bottom-up development process for eGovernment and paperless process by providing all necessary tools and knowledge in order to achieve highly interoperable and locally manageable eServices based on trust and security.

RegioPKI®

Finland:
Conseils Oy
Hämeentie 153 B, FI-00560 Helsinki
Tel : +358 50 379 5343
teemu.rissanen@regiopki.com
www.regiopki.com

Belgium:
EuroConseils Sprl.
Avenue Colonel Daumerie 5, BE-1150 Brussels
Tel :+32 2 779 0503
tapio.rissanen@regiopki.com
www.regiopki.com