



CORISECIO - XKMS Service

Security Automation across the SOA Lifecycle

Service Oriented Architectures (SOA) are based on open standards. Compatibility and interoperability have to be met as basic requirement as well as further developments and adjustments to new functionalities and applications. Public Key Infrastructures (PKI) are the basis of the system security in Service Oriented Architectures. Only by implementing a PKI on basis of certificates objectives like authenticity, confidentiality, integrity and liability of different services may be achieved.

KEY MANAGEMENT IN DISTRIBUTED ARCHITECTURES

A PKI is no easy task, especially the design of technical and organizational processes regarding the key and certificate management in heterogeneous environments is a challenge. From user registration via issue and distribution of certificates up to provision of validation functionality methods have to be provided, which meet the high requirements to availability and interoperability.

CORISECIO – XKMS SERVICE

With the XKMS Service CORISECIO provides an XKMS implementation within the securityRunTime. The protocol XML Key Management Specification (XKMS) published by the W3C represents an interface description for administration and validation of certificates and keys within a PKI.

The CORISECIO securityRunTime there acts as an independent XKMS Service Provider. Without programming efforts the methods for key information are provided XKMS compliant via Web Service. So the question regarding the public key is as reliably answered as the validation check of the certificate – standard compliant as a valid SOAP message. Thus the XKMS Service is compatible with all systems and may be implemented in all leading SOA environments.

The XMKS Service is seamlessly integrated in the CORISECIO infrastructure and available at modeling and configuring Web Service Security. The service so is the ideal extension of the CORISECIO Basic Security Services.

USER ADMINISTRATION, PKI, CERTIFICATE AUTHORITY

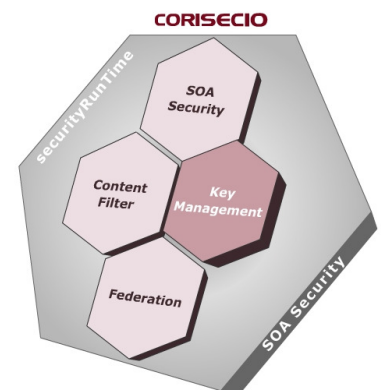
An integrated user administration with automatic PKI service belongs to the basic functionalities the CORISECIO securityRunTime. At the click of the mouse the administrator creates new user and issues or renews

FACTS

- Automatic Key Management for SOA
- Standard compliant XKMS Provider
- Certificate localization and validation
- Use of existing certificates in SOA

BENEFITS

- Maximum interoperability
- Low migration and license costs
- Future proofness
- Decreasing costs for maintenance and operations





certificates of the own Certificate Authority (CA). Import- and integration functionality enables the use of existing Meta Directories and directory services. So existing user, certificates and keys may easily be imported from established solutions and administrated centrally. The distribution as well as the certificate management is done automated, so that certificate and validation requests may be answered always up-to-date.

SOA SECURITY INFRASTRUCTURE

The CORISECIO securityRunTime provides a Security Basis for SOA infrastructures. Security Standards, implementation, administration and automation are the basis. The solution may easily be enhanced with security mechanisms due to the flexible adapter concept.

KEY FEATURES

■ CORISECIO securityRunTime

System and platform independent run time environment for security applications.

(see Factsheet - securityRunTime)

■ CORISECIO - XKMS Adapter

- *XKMS-Service for SOA*
- *W3C Standard-compliant*
- *XML Key Information Service (XKISS)*
 - *Validate Request*
 - *Locate Request*
- *Web Service and SOAP based*

