



CORISECIO - SSO Service

Security Automation across the SOA Lifecycle

The authentication at backend systems may be done very efficiently using SOA technology. Within the business processes applications and services require an authentication, to grant access to appropriate contents, services or functionalities on basis of authorization profiles. Without suitable SSO solutions this means great efforts because of multiple authentications. Therefore, many companies avoid these efforts and use a technical user for registration of integrated systems. Subsequently a high loss of security, traceability and personalization possibilities arise, which may be avoided by use of applicable SSO solutions.

SECURITY AS A SERVICE

In an SOA infrastructure it would be favorable to establish security mechanisms as services themselves. Security Services may be provided via standardized interfaces and used by all services. The functionality itself does not have to be installed in front of or in each application. Even license and operating costs may be significantly decreased with central resp. domain wide Security Services.

CORISECIO – SSO SERVICE

Based on the CORISECIO securityRunTime CORISECIO provides an authentication solution as extensive as efficient. The service is called up via standardized interfaces and delivers appropriate user information/credentials in the format required of the application. The service so takes over authentication at the application without modifying it.

Via the central administration all rights and configurations regarding authentication and transformation processes are performed. There existing user and credentials from Meta Directories may be imported/synchronized optionally. A Public Key Infrastructure (PKI) is integrated in the securityRunTime and may embed own Certificate Authority (CA) as well as external Trust Centers. A mapping of the credentials is possible with Wizard support.

MODELING & ORCHESTRATION

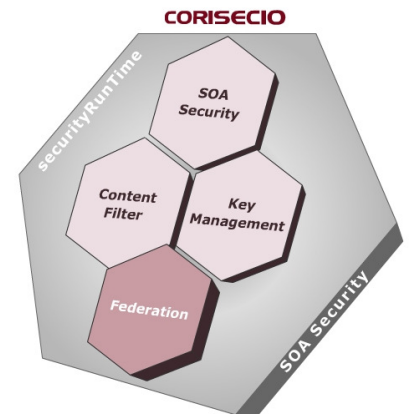
The powerful Visual Modeler enables policy modeling at the click of a mouse. Administrators define rules, which formats and credentials should be used for the login at the target system. With the transformation e. g. a registration per Session Token may be transformed into a certificate authentication at the backend system via SSL.

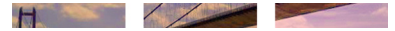
FACTS

- Single Sign On for Portals & Services
- Supports SAML, certificates, SAP and many more.
- Use of existing solutions for SOA Sign On
- Partner integration

BENEFITS

- Increased security, usability and personalization
- Protection of investment
- Future proofness
- Low implementation effort





In connection with additional Adapters the communication with Web Service Security Standards may be completely secured.

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)
- Adapter - SSO (generic)
 - *Sign-On via SAML Token*
 - *SAML authentication*
 - *SSL with X.509 certificates*
 - *Application LogIn*
 - *SAP formats (RFC/IDOC/BAPI)**
 - *MQ Series**
 - *HTTP Basic Authentication**
- Adapter - SSO Federation
 - *LogIn inkl. Captcha Support*
 - *LogIn Credential Mapping (User ID/ Password)*
 - *Intermediate Token Generation*
 - *User Authorisation check against Meta Directory*
- Adapter - SAML WebEx (Option)
 - *SSO for WebEx*
 - *SAML Authentication*
 - *WebEx One-click productivity tools*
 - *WebEx User Generation*

**optional*

