ASEBA SxS

ASEBA SxS

Single Point of Authentication Service

Consumer security concerns have a big impact on online banking, with 20% of survey respondents worried about security, saying they stopped or won't start transferring money between accounts. The percentage doubled among fraud victims. („2008 Data Breaches and Financial Crimes Scare Consumers Away", Gartner)

HIGHLIGHTS

Wide range of authentication methods and standards
Hardware tokens (ActivIdentity, Vasco, RSA), EMV CAP/DPA card based authentication, Mobile token authentication - J2ME application for mobile phones, SMS OTP, OATH, RADIUS. Easy adaption of new authentication methods.

Prevention of client side attacks
Use of two factor user & transaction authentication prevents Trojan horse attack, Phishing, Man in the middle, Inside attack (Man in the browser)

Fully centralized lifecycle management
User credentials management (ID, PIN), physical device management (token, card reader), mobile application management from a single place

Multiple service channels
Web, IVR, ATM using a single authentication platform

Easy to integrate & maintain
Service Oriented Architecture integration to 3rd party applications and modular system administration

ASEBA Authentication Server (SxS) is a two-factor authentication server specifically designed to meet the business and regulatory requirements of multi-channel organizations (financial institutions, managed service providers, and other organizations). ASEBA SxS enables simultaneous use of different types of end-user devices and OTP standards, simplifies user experience, increases security, and reduces cost by enabling organizations to apply consistent strong authentication and authorization over multiple service channels, including web and phone.

Key Business Benefits

Prevents potential damage to the organization – providing high security standards (Two-Factor Authentication solutions based on One-Time Passwords, Challenge/Response and Electronic Signature) eliminates targeted attacks on organizations

Leveraging on current technology investment – EMV chip migration

Independent from mobile operator – Mobile token client application doesn't require any special support from telecom operators, SIM change does not affect application in any way

Prepared to meet demands of millions of online users – solution modularity, high availability and scalability allow meeting of demands of millions of online users (e.g. retail banking)

System configurability – the system is completely configurable and allows you to combine different authentication schemes with different devices for authentication

Easy user adoption – relying on mechanisms familiar to the customers across all channels, now and tomorrow meaning less investment in coaching campaigns, registration and help desk support

Return of investment – single point of authentication service consolidated across separate business units into single solution supporting multiple OTP devices of different types is cost-effective solution from operational level.

Compliance with financial standards – including OATH, ensures lower deployment costs

ASEBA SxS

PRODUCT COMPONENTS

SxS Engine - Authentication service
- Validates authentication requests (OTP, C/R, MAC, MDS)
- Digitally signs and stores authentication Audit Log
- Attack Notification (OTP Brute-Force Attack, User Behaviour Monitoring)

SxS Admin - Administration web application
- Authentication properties configuration (Authentication types, HSM configuration, Key management, Authentication parameters)
- Authentication devices management (Initialization, Enrolment, Status tracking / Blocking, Unlocking, Synchronizing)
- Users management (Enrolment, Authentication device assigning, Initial PIN printing, Status tracking/Blocking)
- Administrators management (Roles, Access rights)
- Statistics & Reporting

SxS Integration API
- XML/SOAP
- C/C++
- Java

SxS Provisioning
- mobile token (LOMAAP): application distribution (OTA), activation code generation, application validation
- hardware tokens: token initialization, token personalization (user registration credentials generation, initial PIN/Activation Code Generation and delivery)

ASSECO SEE d.o.o.
Ulica grada Vukovara 269d
Zagreb, CROATIA
Tel.: +385 1 30 30 000
Fax.: +385 1 30 30 010
e-mail: info@asseco-see.hr
www.asseco-see.com

asseco SOUTH EASTERN EUROPE

Key technical advantages

Black box concept – solution acts as "black box" towards 3rd party applications enabling smooth integration and limiting modifications on 3rd party systems in the environment

Authentication methods - Synchronous and Asynchronous One Time Passwords, Challenge/Response (CR), Message Authentication Codes (MAC), Multiple Data Signature (MDS) for tokens and Mode1, Mode2, Mode2 with TDS and Mode3 for MasterCard CAP (Chip Authentication Program) and VISA DPA (Dynamic Passcode Authentication) support

Support for latest MasterCard's AA4C (Advanced Authentication for Chip) specification

Multi-Token support – support for VASCO, ActivIdentity and RSA tokens

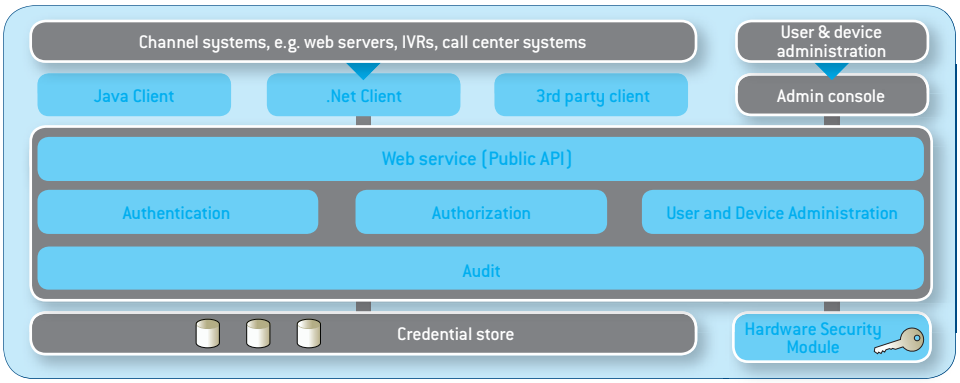
Mobile token support – support for J2ME MIDP 2.0 and iPhone phones

Administration – rich-featured administration enables easy personalization and monitoring, as well as card profile setups, HSM keys management, detailed transaction history, ATC synchronization, etc.

Auditing – all transactions are logged, both authentication requests and results and administrators activities; and each log is tamper-proved, digitally signed and time stamped

High availability – solution architecture enables clustering and load-balancing, resulting in high reliability and authentication requests workloads

Platform independency – Java development toolkits provide support for multiple Server platforms and Operating Systems



Technical details

Operating systems:
- Redhat Enterprise Linux 5
- Windows 2003 Server
- IBM AIX
- Sun Solaris

Hardware Security Module:
- nCipher (nShield and pay Shield)
- Thales WebSentry

Application Server:
- IBM WebSphere Application Server v.6.2
- Jakarta Tomcat 5.5

Databases
- Oracle
- DB/2
- MS SQL

Devices:
- Vasco digipass tokens
- ActivIdentity OTP Tokens
- RSA Secure ID
- Logos mobile token
- ActivIdentity Solo Reader
- Xiring CAP reader
- CAP/DPA compliant EMV smart card

Mobile Phones Requirements
- MIDP 2.0
- CLDC 1.1
- Supported vendors: Nokia, Sony Ericsson, Samsung, Windows Mobile (HP, HTC, MDA VARIO, QTEK, etc.), Motorola, LG, etc.
- iPhone

Mobile Tokens Provisioning
- SMPP
- ParlayX
- GSM modem

Authentication schemes:
- One-time passwords (OTP)
  - ActivIdentity one-time passwords
  - Vasco one-time passwords
  - OATH one-time passwords
  - SMS OTP
- EMV authentication compatible with the following algorithms
  - MasterCard CAP/PLA
  - Visa DPA

Authentication framework is extendable to support:
- Other token vendors
- ODBC/JDBC data stores
- Remote RADIUS servers

Administration features
- Device management
  - Synchronise
  - Unlock
  - Assign/unassign
  - Import
- Credential management
  - Status (enable/disable)
  - Usage statistics
- User and permission management
  - User management
  - Role management
- Secure audit
  - Digitally signed tamper-evident log
  - Audit log queries
  - Archive and purge