Integrated Lifecycle Management of Smart Cards, USB Tokens & User Credentials
Agenda

• Introduction
  - IT Security: Too many challenges…
  - A strong need for “Trusted Identities”
  - “Trusted Users” Key Benefits
  - A strong need for Integrated Badge & Credential Management (CMS)

• OpenTrust SCM Overview
  - OpenTrust SCM Key Benefits
  - A Simple and Full Featured Enterprise CMS
  - Making “Trusted Users” a reality
  - OpenTrust SCM Architecture and Ecosystem
  - Worldwide References & related business cases

• Use Cases: eBanking, IAM Integration
IT Security: too many challenges ...

How to allow IS access to roaming users, third parties and remote application services without compromising IT security?

How to secure access control to business applications, while authentication schemes rely (mostly) on shareable/spoofable logins and passwords?

How to (safely) provide enough IS flexibility to adapt to:

► Evolving business workflow requirements?
► Organization and regulations changes?
► Heterogeneous connection means and devices?

How to warrant Enterprise data privacy and integrity in order to protect mission critical assets, with respect to existing regulations (SOX, PCI, BAII, SAFE, etc.)?

How to take advantage of electronic transactions to leverage business processes and to increase global productivity?

How to get better protected against internal threats & frauds?

e tc…

e tc…
The widespread use of Digital Identities securely granted to any user and IS component establishes the basis of new and powerful security policy enforcement paradigms:

- "Trusted Networks"
- "Trusted Users"
- "Trusted Transactions"

At OpenTrust, we believe that implementing a global Trust Infrastructure is the only foundation to address upcoming IT security challenges all in one, with respect to:

- Security standards
- Ease of use
- Productivity requirements (TCO, ROI)

Certification Authority
Bridge Provider (PKI)
OTP Server
SSO Server
Application Portal
Archiving System
Corporate User
Authorized Employee
Customer
External User
Key benefits of “Trusted Users” (1/2)

Prevent user security credentials disclosure using a single, safe and personal cryptographic support

► Enabling IS-wide “two factor” strong authentication, regardless of connection means and user types
► Confining multiple user “secrets” (OTP, SSO, Key pairs…) in a single support that can be fully managed locally and remotely at any time
► Providing a suitable mean of convergence for logical (certificate, key pairs…) and physical (contactless, biometrics…) access control credentials… one step toward unified Corporate Badging

Allow a simple, cost effective and deep integration of asymmetric cryptography standards in the IT environment

► Already supported by most of the IT (infrastructure: routers, switches… & software components: web servers, email clients, SSO, Windows Logon…)
► Enabling easy user (or server) based data encryption and regulation compliant digital signature
Key benefits of “Trusted Users” (2/2)

Establish a user friendly “state of the art” security model
► No more passwords (goal : not even a few)
► Simple and secure handling of personal authentication means
► Enhanced user capabilities and asset protection (encryption, digital signature)
► Empowered user productivity (focus on core business rather than getting lost with multiple access control schemes)

Provide secure and integrated credential lifecycle management to existing X.509 Certificate (PKI), SSO, OTP & IAM solutions
► Allowing them to rely on secure digital identities that can be trusted far beyond logins and passwords… and that belong to a global, consistent and business effective security policy
► Lowering TCO : multiple (i.e. per solution) credential management tasks are automated and handled from a focal point : the Card Management System (CMS)
Widespread use of Digital Identities stored on personal cryptographic supports is a very attractive approach of user security

But it requires strong and complete management capabilities to become a reality across the Enterprise

Multiple Holders
- Employees
- Externals
- Partners
- Customers (B2B, B2C)
- Etc…

Multiple Lifecycle Operations
- Distribution & Enrollement
- Revocation
- Credential renewal
- Badge recycling
- Self care (unlocking, PIN change, replacement, etc.)

Multiple Supports
- Multi vendors
- Smart Cards & Tokens (and related drivers, middlewares…)

Multiple Holders
- Employees,
- Externals,
- Partners,
- Customers (B2B, B2C),
- Etc…
OpenTrust SCM is a comprehensive answer that provides enterprise wide “Trusted Users” management capabilities, while remaining:

- **Highly secure** (communications, access control, operations, auditing…)
- **Simple** and user friendly (easy endorsement, enhanced productivity)
- **Open** to third party solutions (SSO, OTP, IAM…) and through standard interfaces (Web Services, LDAP, PKCS#7…)
- **Flexible and complete** (multiple smart card & token support, many operator and user profiles, heterogeneous issuance and lifecycle operations…)
- **Cost effective**: providing an outstanding security level, while lowering user credential management costs (automation, centralization, homogeneity)
- Modeling tools: datasources & profiles (users, cards, certificates…)

- Integrated Enrolment & Issuance processes
  - “Self Enrolment” by the badge holder (end user)
  - Issuance through the “Badge Office”
  - Badge “Pre Personalization” process

- Card & Token Lifecycle Management processes
  - Issuance of replacement/temporary badges
  - Badge loss/theft statement
  - Replacement and renewal of cryptographic contents
  - Badge recycling
  - Card & Token remote unlocking

- Badge holder Self Care operations
  - Certificate renewal
  - Auto recovery of old encryption certificates
  - PIN Code change
  - Badge unlocking (on line, off line)

- Common Platform Services
  - Logging, notification, publication, auditing…
  - Strong Authentication and Access Control
  - Dynamic application skinning and multi lingual support
  - Platform clustering and HA management
Making “Trusted Users” a reality...

- Enterprise AD / LDAP User Directory
- Hardware Security Module
- PKI Server
- OTP Server
- SSO Server

Help Desk Operator
Security Officer
Card Holder
Employee, External, Partner, etc.

Credential Generation Requests (SOAP)

User Authentication

Automated Card Initialization process

Entire Support
OpenTrust SCM Architecture

OpenTrust SCM Server
Smartcard & Credentials Lifecycle Management

- Card profile Authentication
- Card profile Signature
- Card profile encryption

Third-party Applications (IAM)

OpenTrust PKI
WS/SOAP

OpenTrust OTP
WS/SOAP

Smartcard Initialization & Selfcare Operations

Third-party Applications

HSM
A large and complete Ecosystem

Certificate Providers
- Sun Microsystems
- Oracle
- Evidian

SSO & IAM Providers
- Tivoli
- OpenTrust
- OpenTrust

OTP Solutions
- OpenTrust
- Gemalto

Microsoft PKI

PKI Vendors
- SafeNet
- Ultimaco
- NCipher

HSM Vendors
- Bull

OT Solutions
- Passlogix

PKI Vendors
- Microsoft PKI

Certificate Providers
- Keynectis PKI
- OpenTrust PKI
ALSTOM Transport

Multiservice Smart Card security project for both physical and logical access control (integration with SSO from Evidian and with IAM from Sun Microsystems) - 6 weeks deployment, 30,000 enrolled supports

Usage: Physical (HQ) & logical access control
Strong authentication (WIFI, VPN, Windows), Data encryption
"Self Enrolment" by the Badge Holder

- **Enterprise AD/LDAP User Directory**
- **Auth. Scheme**
- **User's Card Profile**
- **Card Serial Numbers Registration**
- **Auto Discovery**
- **Card Shipping Process**
- **Registered User**
- **Central Security Officer**

**Steps:**

1. **a** - Enterprise AD/LDAP User Directory
2. **b** - Card Shipping Process
3. **c** - Auth. Scheme
4. **d** - User's Card Profile

**Note:**
- **Auto**
- **Discovery**
- **Registered**
- **User**
- **Central**
- **Security**
- **Officer**

**Explanation:**

- The process starts with the Central Security Officer who initiates the enrollment process.
- The Enterprise AD/LDAP User Directory is accessed for user information.
- Authentication scheme is used to verify the user's identity.
- The user's card profile is registered and serial numbers are recorded.
- The registration process ends with the shipping of the card to the user.
Badge Enrollement through the « Badge Office »

1. Enrolling User
2. Badge Office
3. Badge Operator
4. Personal Q&A for Off Line Identification
5. Formal Authentication

Enterprise AD/LDAP User Directory

Enrolled Support

User's Card Profile

+ « PIN »
Badge “Pre Personalization” process
Recording, Shipping and Assignment

Enterprise AD/LDAP User Directory

Card Serial Numbers (CSV file)

Central Security Officer

Card Shipping Process

Card Activation Code & Instructions

Card Delivery Operator

Enrolling User
“Pre Perso” Process

Stage 2 – Final Badge Activation by the Holder

Enrolled User

Enterprise AD/LDAP User Directory

« Activation Code »

« PIN Code »

Server
“Pre Perso” Process

**Stage 1 – Badge recording & “face to face” Issuance**

- **a** Enrolling User
- **b** Badge Operator
- **c** Enterprise AD/LDAP User Directory

**Diagram Notes:**
- Enrolling User interacts with Badge Operator.
- Badge Operator accesses Enterprise AD/LDAP User Directory.
- «Activation Code» transmission.
Use Case: “Trusted Users” in eBanking

1. Security Officer
   - Token Serial Numbers Registration

2. Production Environment
   - Token’s Central Enrolment
   - Activation Codes

3. Mailing Process
   - Token Shipping Process
   - B2C eBanking Infrastructure

4. Secure Auth
   - Secure Transactions

Customer
- Personal Token Activation Code

Server
- Use Case: "Trusted Users" in eBanking
- Security Officer
- Personal Token Activation Code
Use Case: Tight Coupling with the IAM

Security Credentials

Authentication: WIFI, VPN, SSO, Windows...
Encryption: Certificates & Private Keys
Digital Signature: Signing Certificates for Business Applications

Help Desk Operator

Enterprise Portal / IAM

Card Holder
Employee, External, Partner, etc.

Security Credentials

PKI Server

Enterpise AD / LDAP User Directory

OTP Server

SSO Server

LDAP / SOAP Infrastructure

« User Properties & Identities »
OpenTrust SCM Sample Card Profile

Card Profile

- Access Control
- Workflows & Options
- Security Profile
- Operators
- Smart Cards (Gemalto, Obertur, Aladdin)
- X.509 Certificate Profiles
- SSO App.
OpenTrust Project Méthodology

1. Project Launch
2. Training & Skills Transfert
3. Solution’s Architecture & Parameters specification
   - Qualification Platform’s Acceptance Testing
   - Server infrastructure Installation & Configuration
   - Production Platform Setup & Config. Phase
   - Formal Reception & Sign Off
   - Roll out & Operations Maintenance & support from OpenTrust