ID PKI – Deployments & Use Cases

Mathieu Cherouvrier, CIO Digital ID

Jean-Joseph Herpin, Business&Solution Manager

Mindshare 2023

September 19th/20th

EVIDEN
an atos business

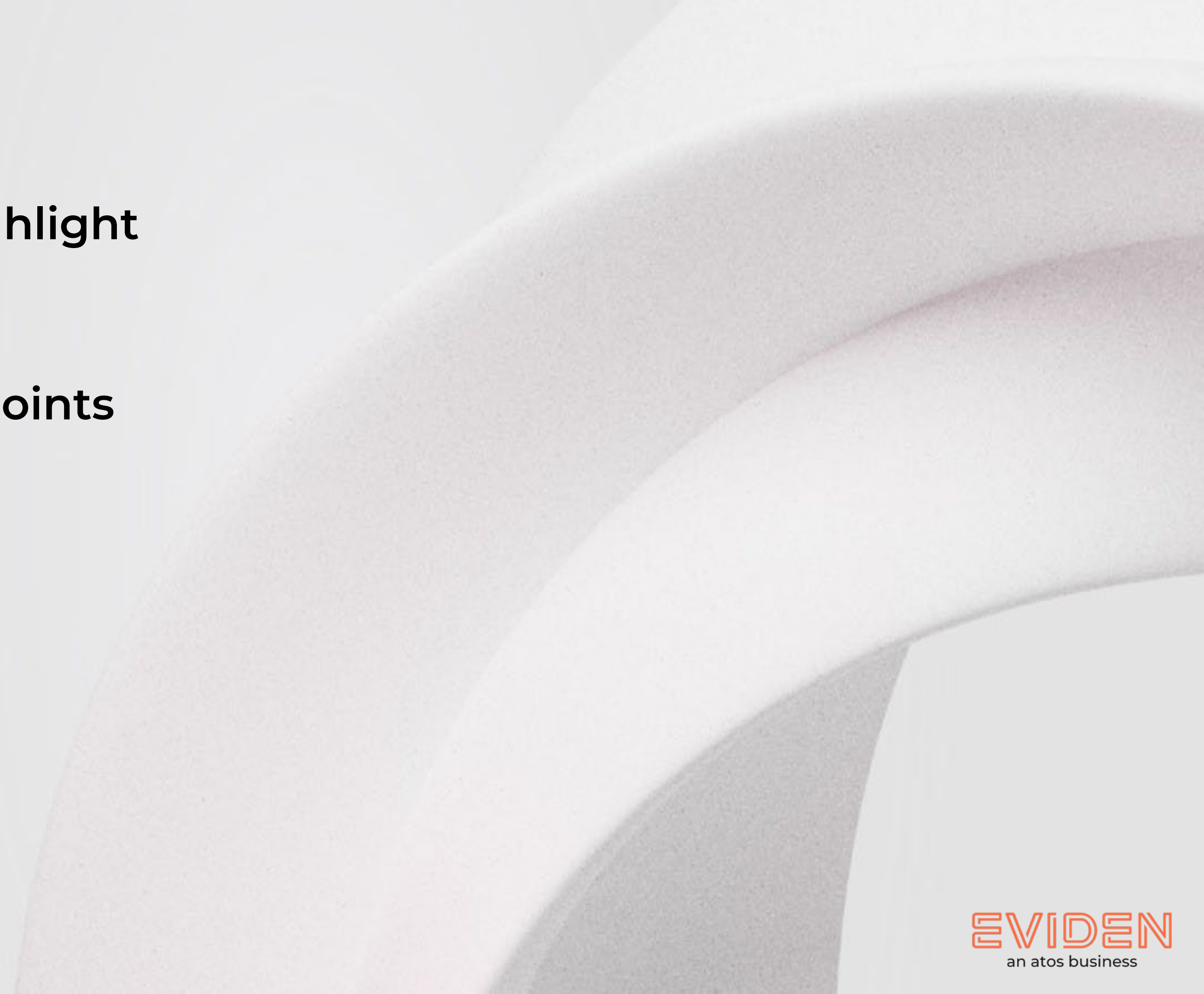
Agenda

1 **Digital ID Highlight**

2 **IDPKI – Key points**

3 **SaaS offering**

4 **Use Case**



Digital ID - Highlights

1

Digital ID portfolio

Business fields, use cases & solutions

Corporate Security

Organizations’ operational needs

- PKI – CMS – CLM – OCSP & TSP – Digital signature – Smart Cards - Middleware
    - All business verticals

IoT & IIoT Security

Remote ID & OTA management

- PKI – CLM – Code signing – OCSP & TSP – Secure elements
    - IoT users/operators
    - IoT manufacturers

Connected Cars

V2X communication security

- C-ITS PKI
    - Road operators
    - Car manufacturers
    - Tier 1, 2 providers

Government

Citizen ID & eGov services

- Interior ministries
- Civil registration authority
- Migration agency

Portfolio

Solution's ecosystem for digital certificates

ID PKI
Secure SaaS or on premise

CONNECTORS
ID management & automation

DIGITAL CERTIFICATES
Unique trustful IDs

DIGITAL SIGNATURE
Advanced signature & code signing

OCSP & TSP
Online digital certificate status validation & timestamping

CLM – CERTIFICATE LIFECYCLE MANAGEMENT
Allround trust supervision & management

Digital ID solutions

Highlights

PKI – Trusted Identities

ID CA - Certification Authority
Secure CA hierarchy management
Trusted Digital IDs production
Multi-tenant EAL4+

ID RA - Registration Authority
Management of machine IDs
Certificate lifecycle automation

CMS - Credential Management System
Management of user IDs
Workflow orchestrator of IDs distribution

CLM – Certificate Lifecycle Management
Inventory, supervision, audit, compliance...

OCSP
Online validation of certificate status

Services & expertise

PKI as a Service
Managed PKI
Dedicated CA on mutualized platform
Ready2Go PKI
Disaster Recovery site

Customer service
Professional services
Migration
Key ceremony
CP & CPS
Safe key deposit box
Training

Ecosystem Tools

IDnomic Sign
Digital signature
Code signing

Timestamping
Certified date & time seal

Cryptographic hardware
HSMs
Secure elements
Middleware for multiple

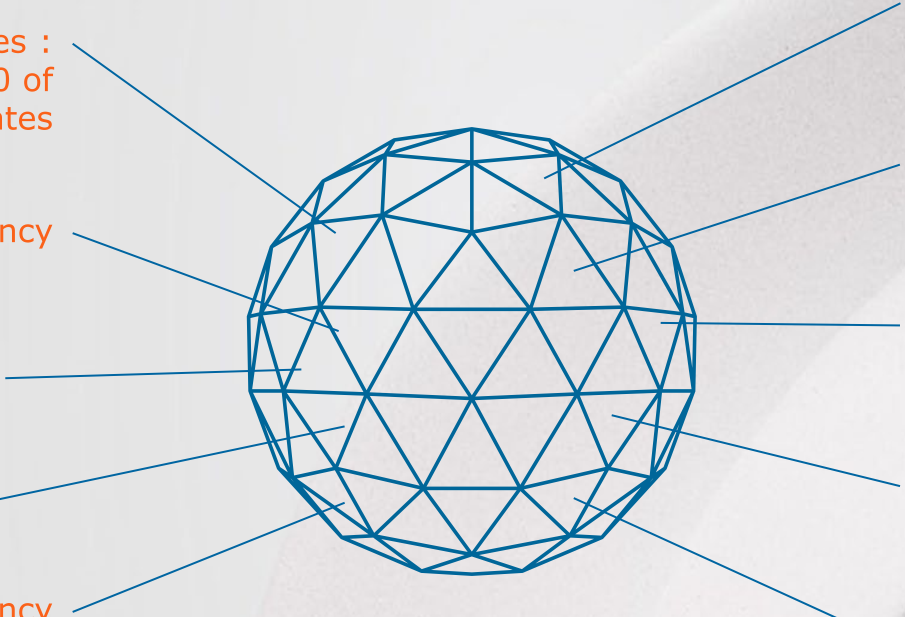
Identity & Access Management
Certificate-based access control

ID PKI suite and beyond !

2

ID PKI

Key points



High Volume capabalities : can support up to 100 of millions of certificates

Multitenancy

API REST

PQC

Certificate transparency

Web interface , easy to use

Support of multiple HSM vendors

Large choice of automated connectors EST, ACME,

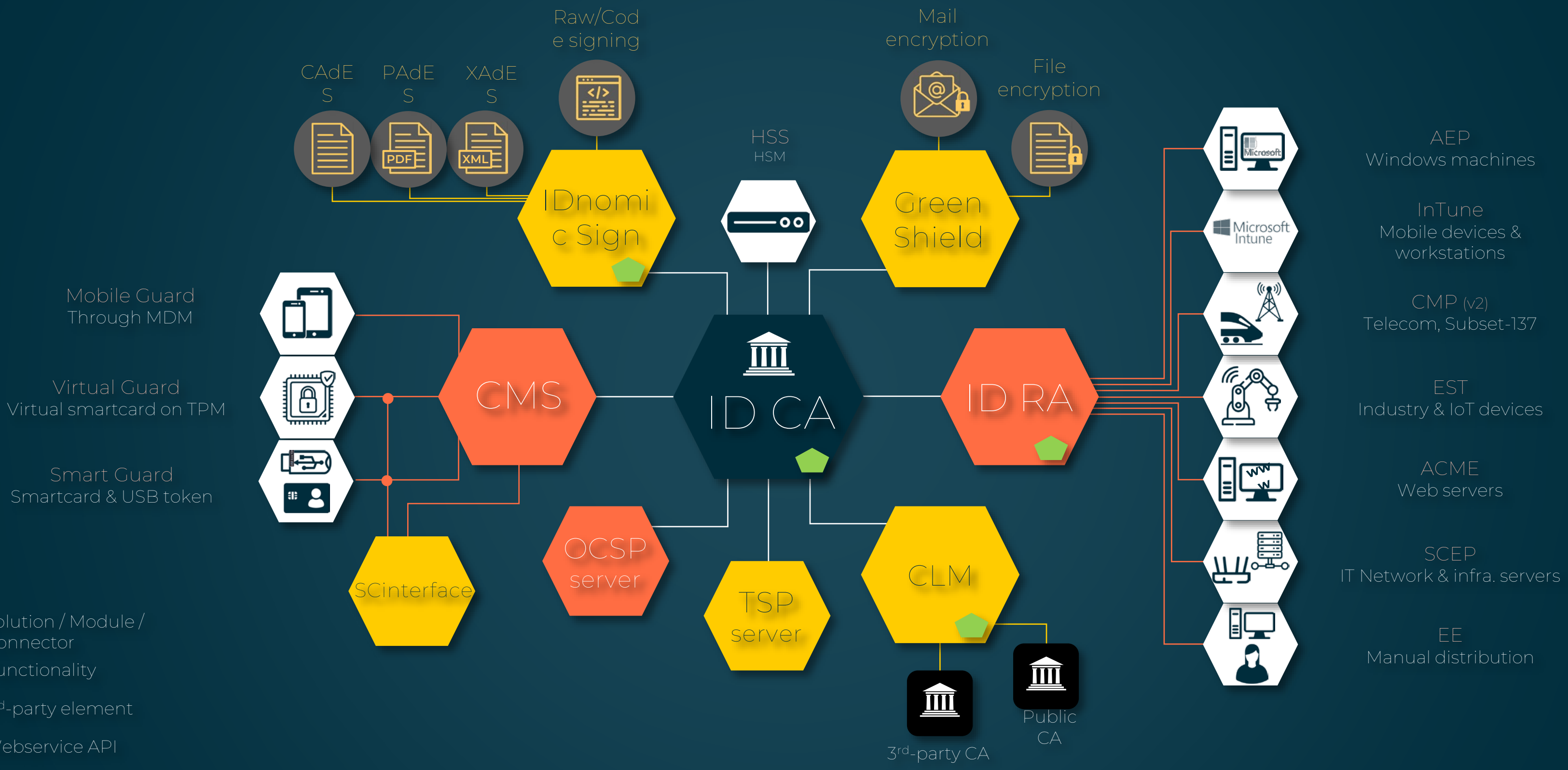
CMP, AEP(WCCE), SCEP, INTUNE

Certificate validation service (CRL, OCSP)

EAL4+ certification for the core Product (IDCA)

Software map

Global view



⬡ Solution / Module / Connector

● Functionality

■ 3rd-party element

⬟ Webservice API

3

Saas offering

First selection, mutiple options

- IDnomic Sign
- IDPKI
- CMS
- OCSP / TSP
- CLM

- **Multitenant**
  - **Or single tenant**
- **Pre defined – Ready 2GO**
  - **Or custom configuration**
- **Configuration by our teams**
  - **Or open to your teams**

Datacenters

Comprehensive management

EIDAS & RGS
for specific services
- Regular Audits

- HMS
  - Key management
  - Backup in safe
  - Secret sharing
- Segregation of duties
- 24/7 monitoring
- DR Site
- High-Availability
- Vulnerability tests
- Pentest

Use Case

4

Why do we need electronic certificates ?

Trusted Digital Certificates enable strong authentication

Confidentiality

Secure transmission of information

Encrypt data (logs, documents, etc.)

Integrity

Guarantee data hasn’t been modified during transmission

Digital signature & code signing

Certificated based authentication (CBA)

Verify the identity of users and machines

Accessing networks & e-services

Non-repudiation

Prevent entities from denying that they are at the origin of a digital event

Digital Signature

Use cases – Financial Organization

Access control to sensitive resources

- Corporate HQ and branch offices
  - Access to business systems and resources (IT, banking application, banking cards CMS etc.)
- Non console access
  - WIFI and VPN remote connection to sensitive business resources

Data exchange

- Secure mobile channel for bank employees and partners
- Secure data transiting trough the network
- In some cases, customers requiring an extra level of security for identity authentication
  - Online banking for high value transactions

Transactions

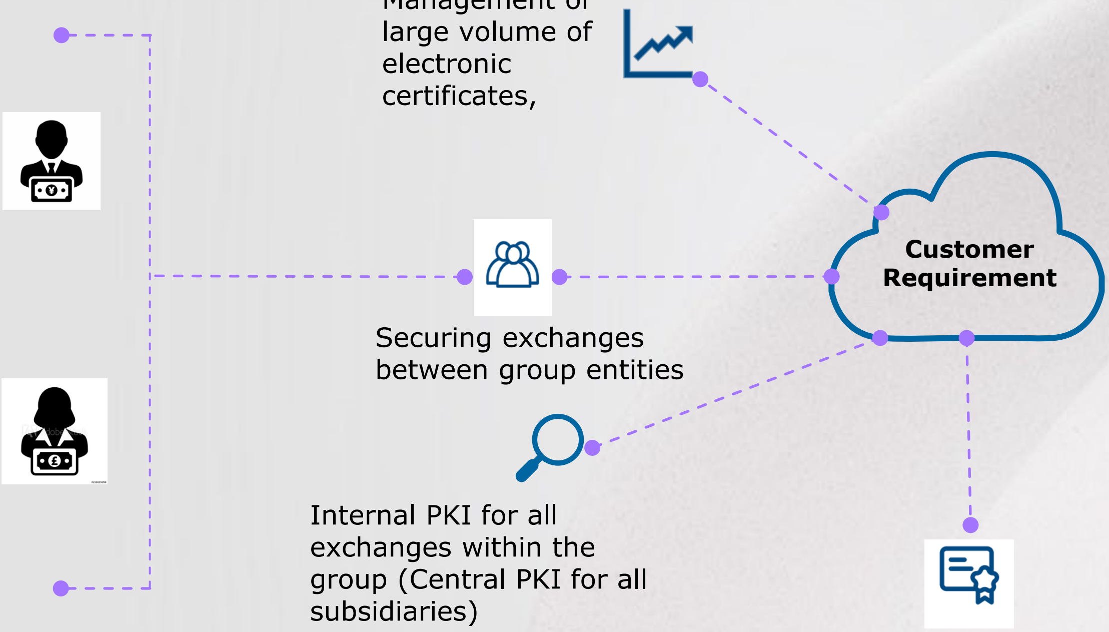
- Timestamp payments, contracts or documents when strong legal evidence is needed
- Electronic signature for loans and retail financing transactions
- Secure channel with Third Party Providers (TPP)
  - Mandatory to encrypt communication and sign requests

Kiosk, ATM & POS

- Establish an end-to-end secure environment with network access control and secure data exchange
  - Communication with peripherals
- Enforce strict authentication to configure ATMs and access firmware (Sign firmware updates)
- For the acquiring business, secure POS authentication with the network

Private International Bank (FR)

Corporate PKI – Private cloud



Management of large volume of electronic certificates,

Securing exchanges between group entities

Internal PKI for all exchanges within the group (Central PKI for all subsidiaries)

Issuance of certificates for servers, service, users, ...

Idnomic Solution based on PKI with connectors (WCCE, ACME, SCEP,)

CMS
for enrolling certificates on smart cards and mobiles (MDM,mobileIron, Blackberry)

Managing large volume of
Certificates 900,000

SaaS Solution based on Idnomic Private cloud

Experience

IDnomic in the Financial & Services sector

A complete solution

A set of products to secure IT resources and access to data by employees, subsidiaries and partners. (ID PKI, CMS, OCSP and TimeStamp)

Cloud services

A cloud-based PKI solution that provides centralized access while eliminating the cost of running on-premise software

Flexibility

Solutions adapted to the business context, which can be easily integrated into the existing environment in a reliable and fast way. (Connectors, web services and APIs)

Long term vision

Solutions that evolve with the business needs to create more value. (interface with Mobile device management solutions, PQC readyness)

Large private banks, national banks

Questions

Our business impact:

Digital Transformation

Design and deploy a unified and future-proof solution to manage identities and crypto-supports for users

What we are doing for a World-class Bank

Design and deploy a CMS to manage digital identities for users

The provided solution is:

- Designed and deployed on site with the required modules to cover the central management of all operational functionalities, including biometric access control
- Managing around 50.000 smart-cards and identities of employees, affiliates and partners
- Allowing the production certificates in badge-office mode and the production of pre-personalized badges ready to be activated with a security code