EVIDEN

Flexibility in Digital ID:

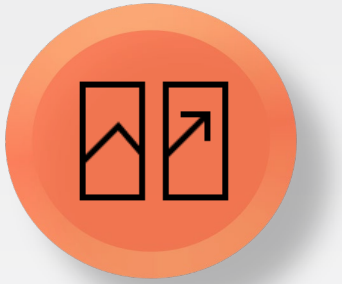
Virtual, mobile and smart card management & integration

Jean-Joseph Herpin
Julia Zimmermann
19.09.2023

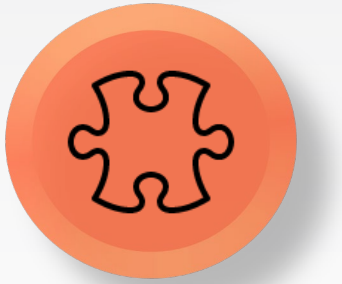
EVIDEN

#1 Why Digital ID?

Why Digital ID?



Invaluable flexibility and the freedom of a modular portfolio.



Digital sovereignty on all levels.

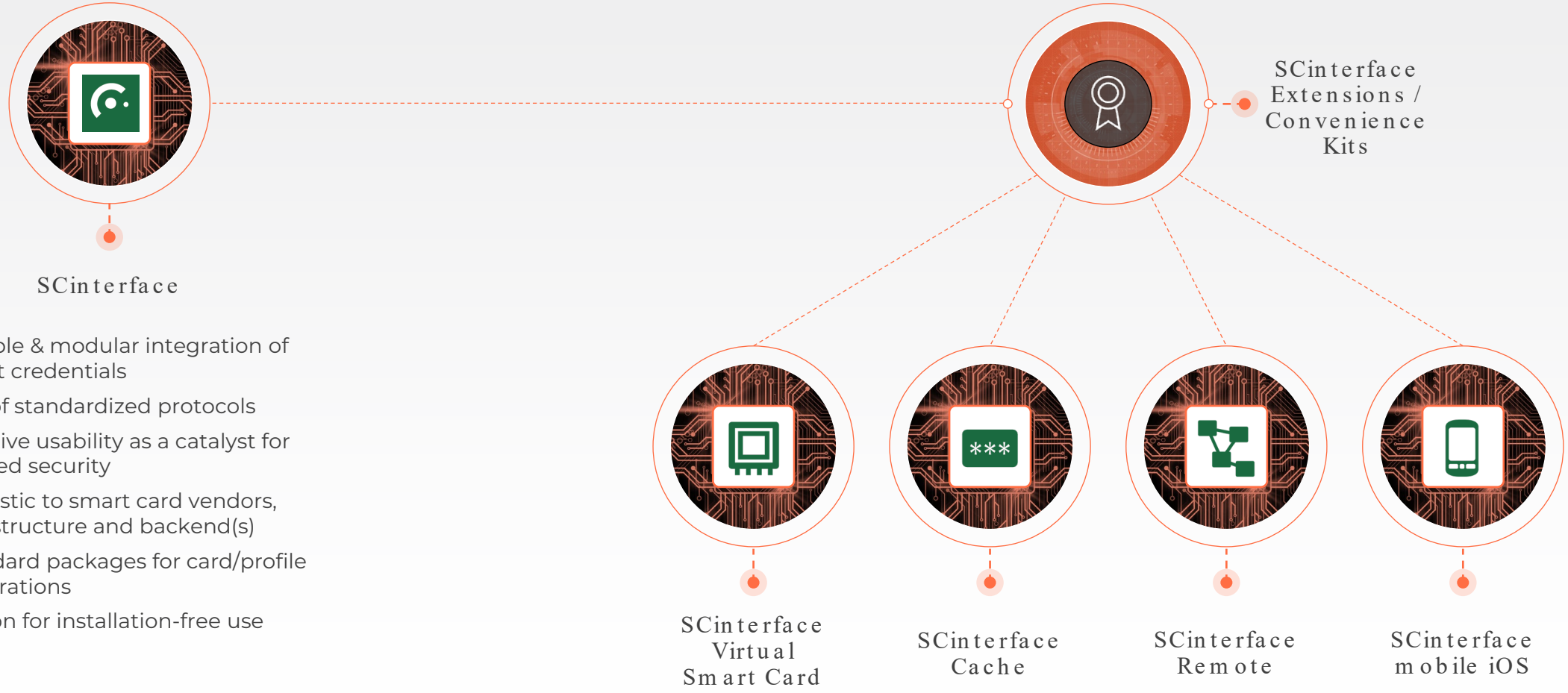
Usability as the ultimate catalyst for applied security.

EVIDEN

#2 What‘s new?

SCinterface

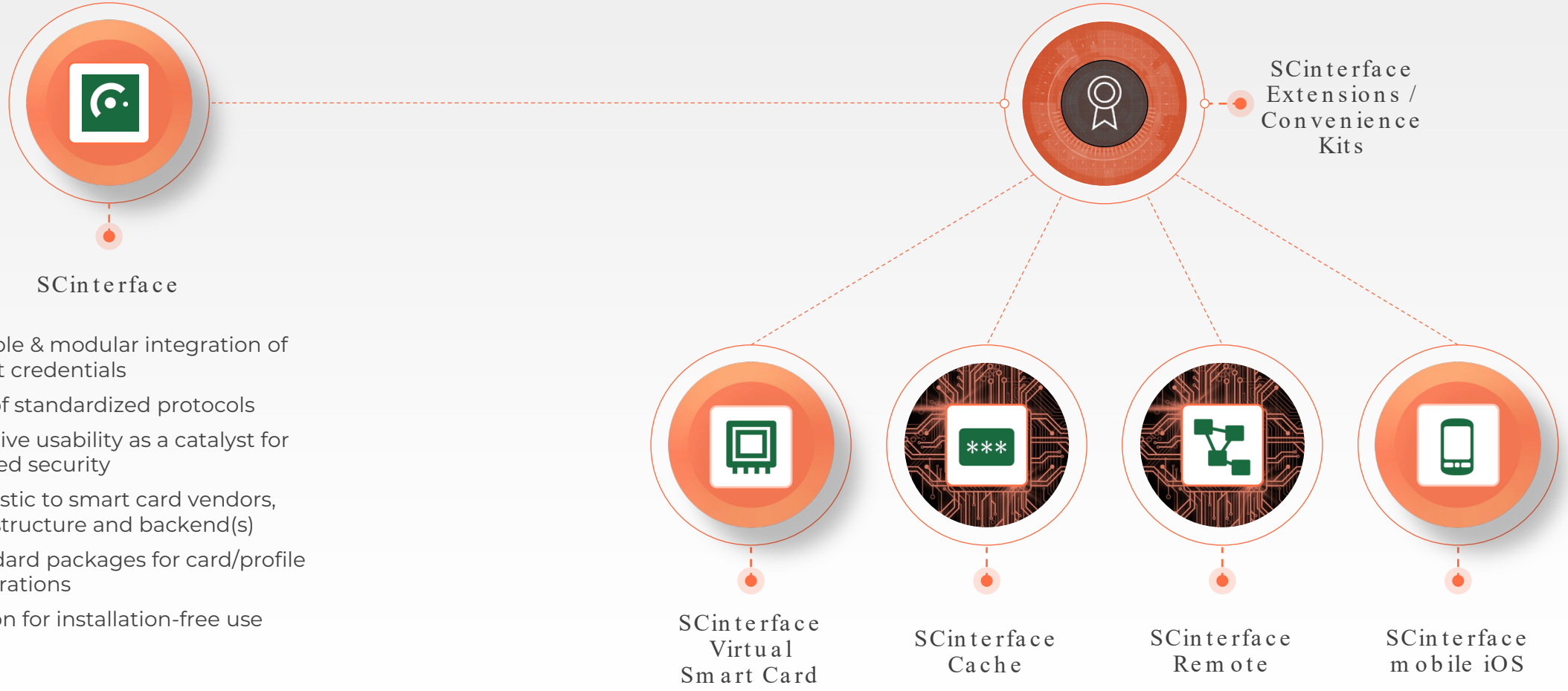
Established security with extended capabilities



- Flexible & modular integration of smart credentials
- Use of standardized protocols
- Intuitive usability as a catalyst for applied security
- Agnostic to smart card vendors, infrastructure and backend(s)
- Standard packages for card/profile integrations
- Option for installation-free use

SCinterface

Established security with extended capabilities



- Flexible & modular integration of smart credentials
- Use of standardized protocols
- Intuitive usability as a catalyst for applied security
- Agnostic to smart card vendors, infrastructure and backend(s)
- Standard packages for card/profile integrations
- Option for installation-free use

SCinterface Virtual Smart Card

Sovereign USABILITY

- Handling like a physical smart card
- Supports all use cases incl. smart card log-on
- Multi-instance support
- Parallel use with MS VSC* and physical tokens
- Available for Windows

FLEXIBLE backend technology

- Key storage on TPM 2.0
- TPM-encrypted software tokens
- VDI and CMS integration
- Compatible with PKCS#11, Minidriver, ...

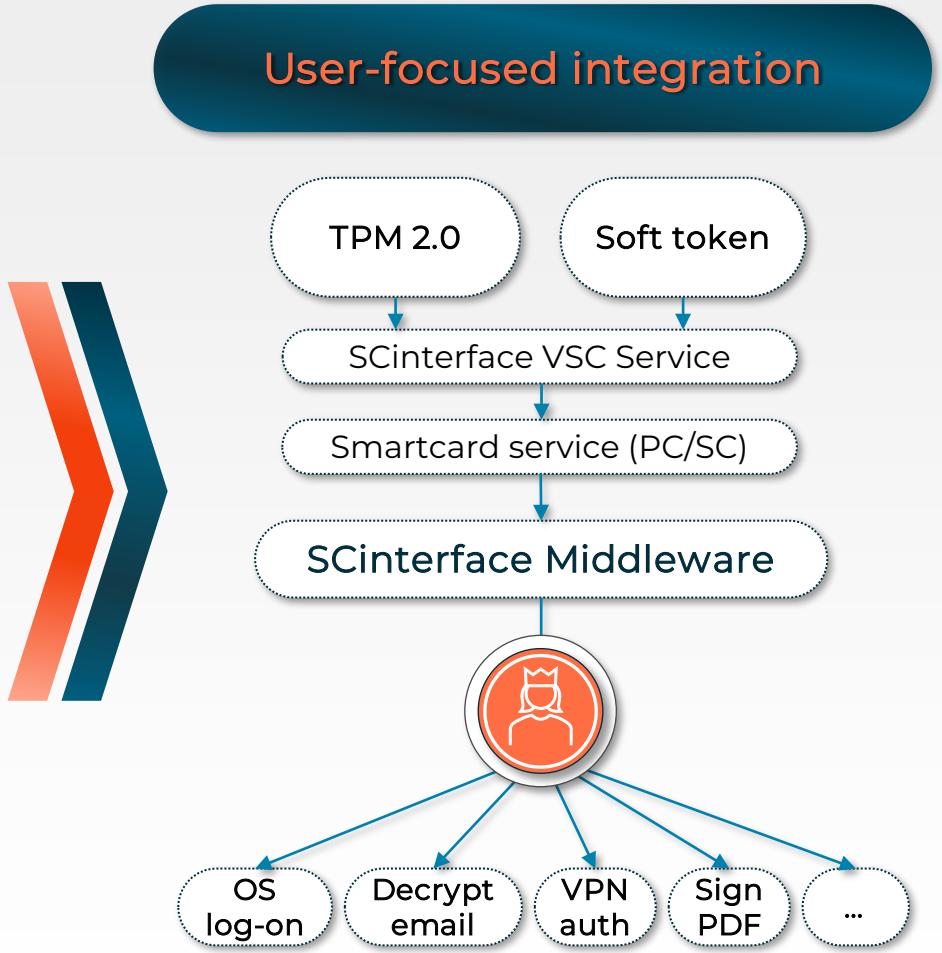
Reliable SECURITY

- ISO 7816 compliant; PKCS#15 profile
- RSA and ECC (NIST) support
- Use of Botan crypto library

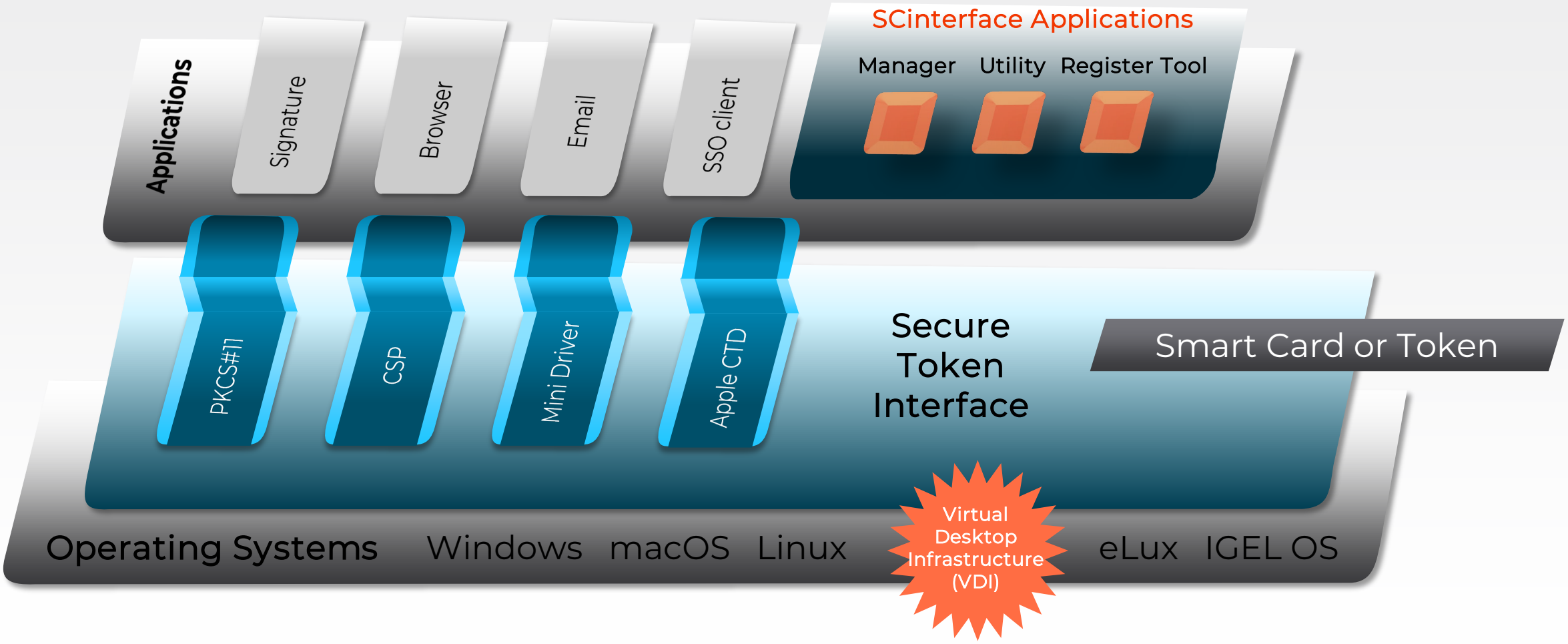
FUTURE outlook

- Availability for Linux

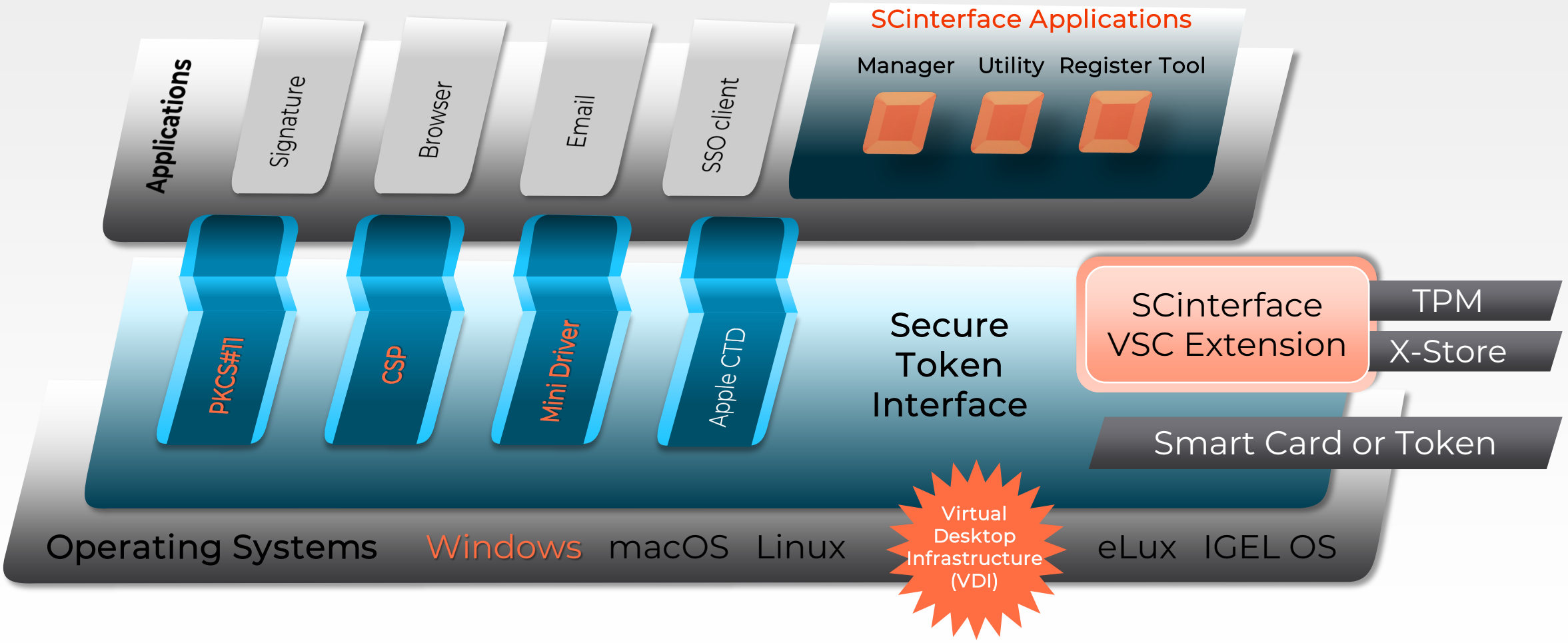
*deprecated by MS

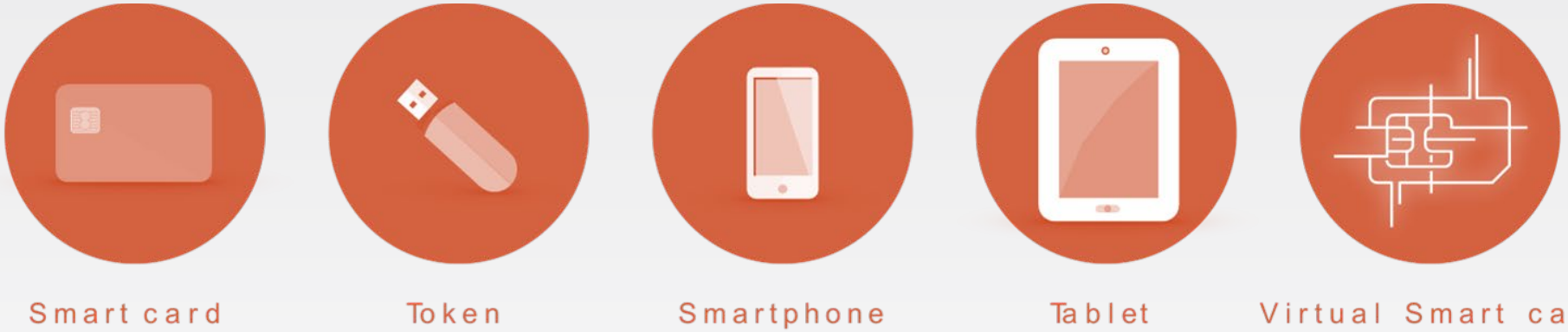


SCinterface: Architecture



SCinterface: Architecture





Credential Management System (CMS)

CMS acts as a Registration Authority and manages the lifecycle of Cryptographic devices for business users

- Can be integrated with ID-CA, OT-PKI, EJBCA/PrimeKey, Dogtag, among others
- Smartcards, USB tokens, Virtual Smart Cards, Mobile Devices, etc
- It manages the entire lifecycle of certificates issued (active, revoked, suspended)

Compliant with security standards:

- RFC 5280, RFC 8399, X.509, 7816 CVC

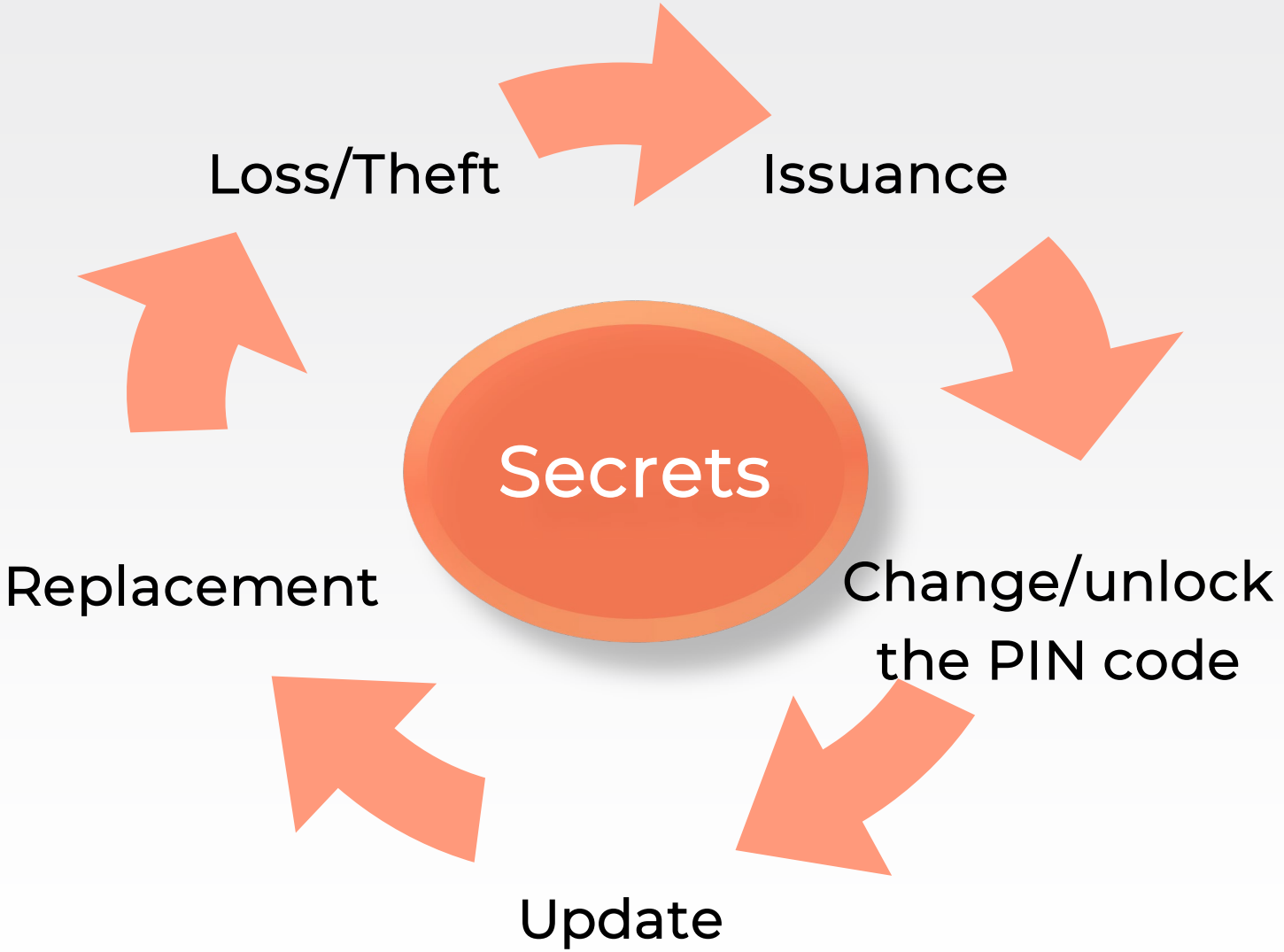
CMS - Capabilities

Management of Smart Cards and Tokens

- Logical and physical personalization
- Issuance
- Activation
- Update
- Revocation
- Recycling, Disposal

User Support

- Temporary Cards
- Key-Pair Recovery
- Unblocking the card offline or online



SCinterface: Mobile on iOS

Sovereign
USABILITY

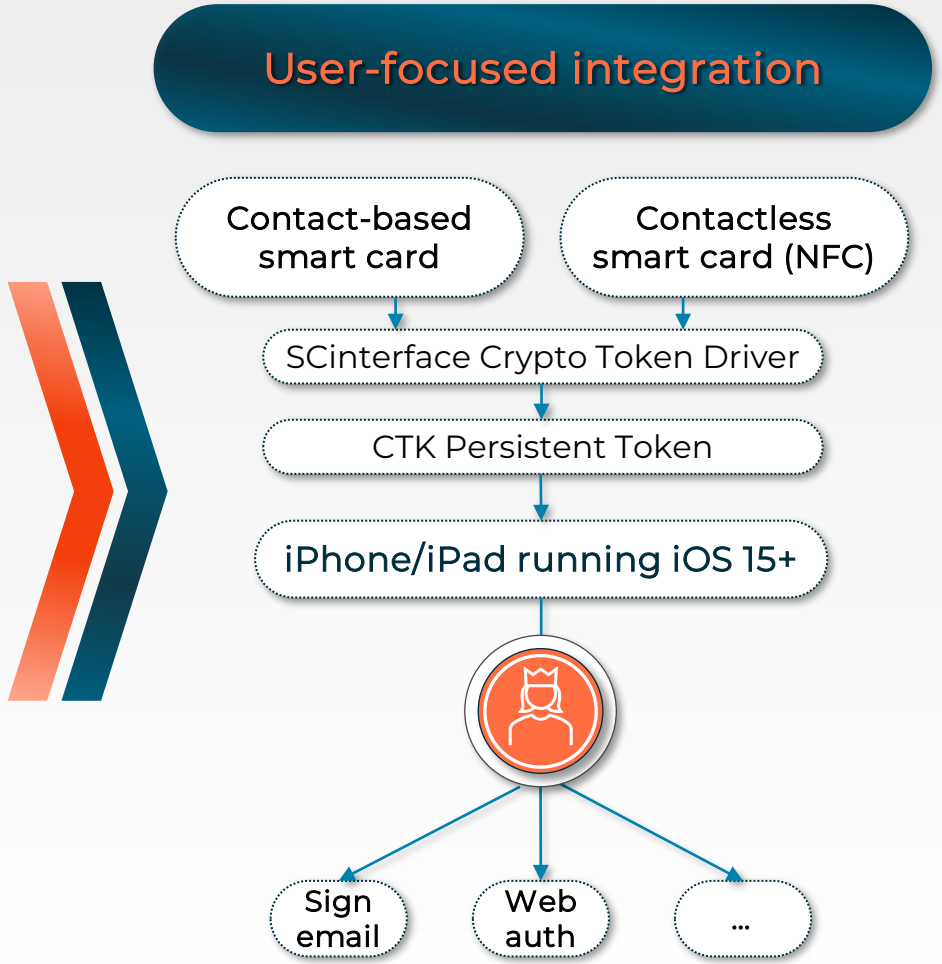
- User interaction is kept to a minimum
- Intuitive user interface
- NFC on iPhone
- External readers on iPhone & iPad
- Low administrative effort required

Well
established
SECURITY

- 20 years holistic middleware experience
- SCi PKCS#11 module forms part of VS-NfD approved configuration of GreenShield
- Track record of supporting cards used in PS
- Constant addition of new cards

FUTURE
outlook

- Decryption of emails
- Usability with VS-NfD on iNDIGO



IDnomic Sign

The army knife of Digital signature

Remote & Local Signature

Full API REST & Multitenant architecture

Signature creation & Verification of signature

Seal

Signature (legal entities)

&

Personal Signature (Natural Person)

PADES
Pdf signature

XADES
XLS document

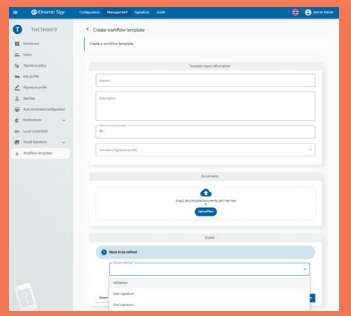
Code Signing
RAW Signature

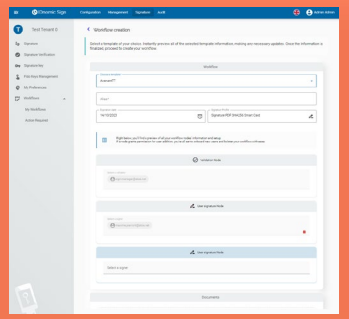
IDnomic Sign

What's new in the version 10.4

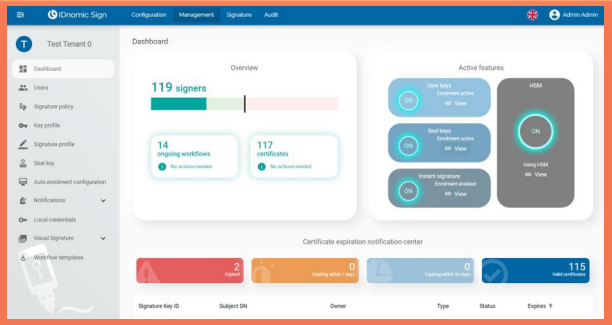
New visual signature management

New Signature Workflow management

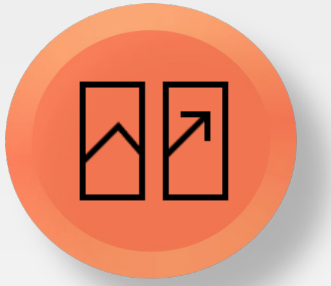




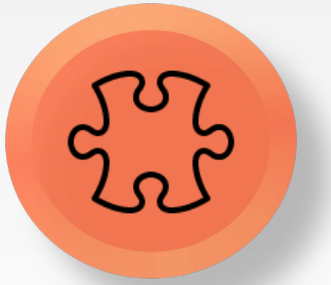
Reporting & Dashboarding



Why Digital ID?



Invaluable flexibility and the freedom of a modular portfolio.



Digital sovereignty on all levels.

Usability as the ultimate catalyst for applied security.

EVIDEN

Questions

EVIDEN

Thank you!

For more information please contact:

jean-joseph.herpin@eviden.com
julia.zimmermann@eviden.com

SCinterface: credential integration beyond smart cards

Atos CardOS
AustriaCard ACOS
AustriaCard JCOP
Bayern PKI Legacy Card
cv Company ID
D-TRUST Card (Siegelkarte)
ePasslet-Suite
G&D Sm@rtCafé Expert
G&D StarCOS
Gemalto Classic V3
GemXpresso
GoID Card
HID Crescendo
Identity Device (Microsoft Generic Profile)
Infineon SECORA⌀ ID S
Infineon SECORA⌀ ID X
NXP JCOP
MS VSC
MTCOS
Oberthur Cosmo
Philips ISO Creditcard
Siemens CardOS
SwissSign suisseID
TCOS 3 & 4
UniCard TU Dortmund (SECCOS)
Uniper Card
...
SCinterface Extension: SCi Remote
SCinterface Extension: Virtual Smart Card

PKCS#11

CSP

Minidriver

Crypto Token Driver

cryptovision SCinterface

System login

WWW login

VPN login

Disc encryption

Secure email

SSO

Digital signature

Virtual desktop

Others

SCinterface Extension: Remote Smart Card

Sovereign
USABILITY

- Handling like a physical smart card
- Supports all use cases (except OS log-on)
- Parallel use with other extensions & cards

FLEXIBLE
key access

- Remote credentials on key server
- Access to shared keys via group policies
- Compatible with PKCS#11, Minidriver, ...

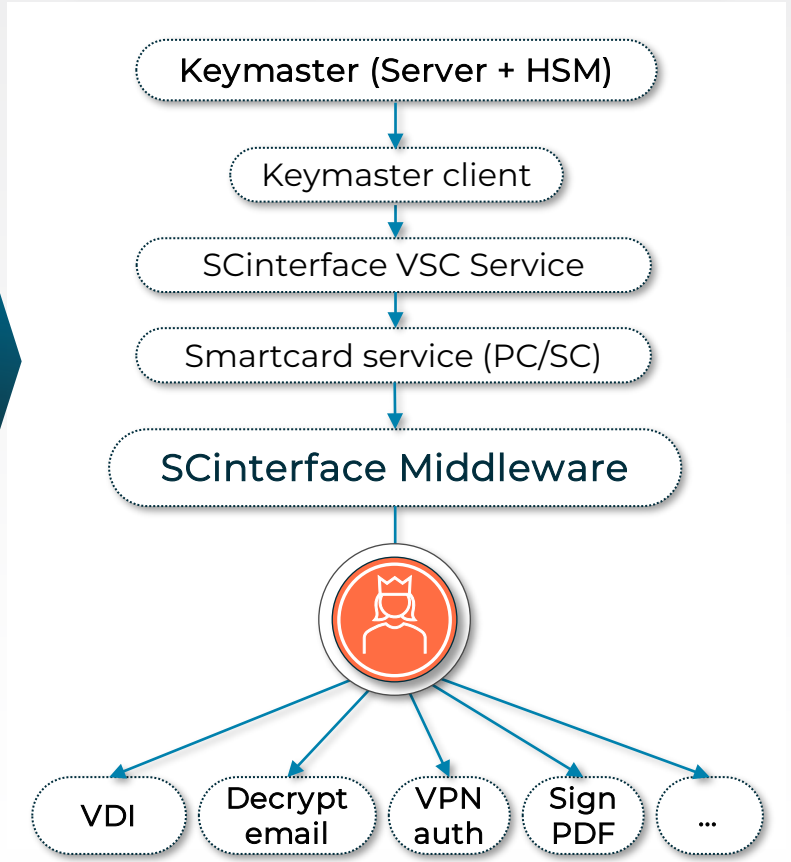
Reliable
SECURITY

- ISO 7816 compliant; PKCS#15 profile
- RSA and ECC support

FUTURE
outlook

- Standalone solution in development for Windows and macOS
- Backend extension: mobile devices

User-focused integration



CMS - Main Features

- Management of Challenge/Response Security Data

- Enrollment Workflows
  - Self-enrollment: authentication using LDAP Directory
  - Badge Office: face-to-face with a security officer
  - Central Office: (pre-)personalization by security officer, possibly in batch

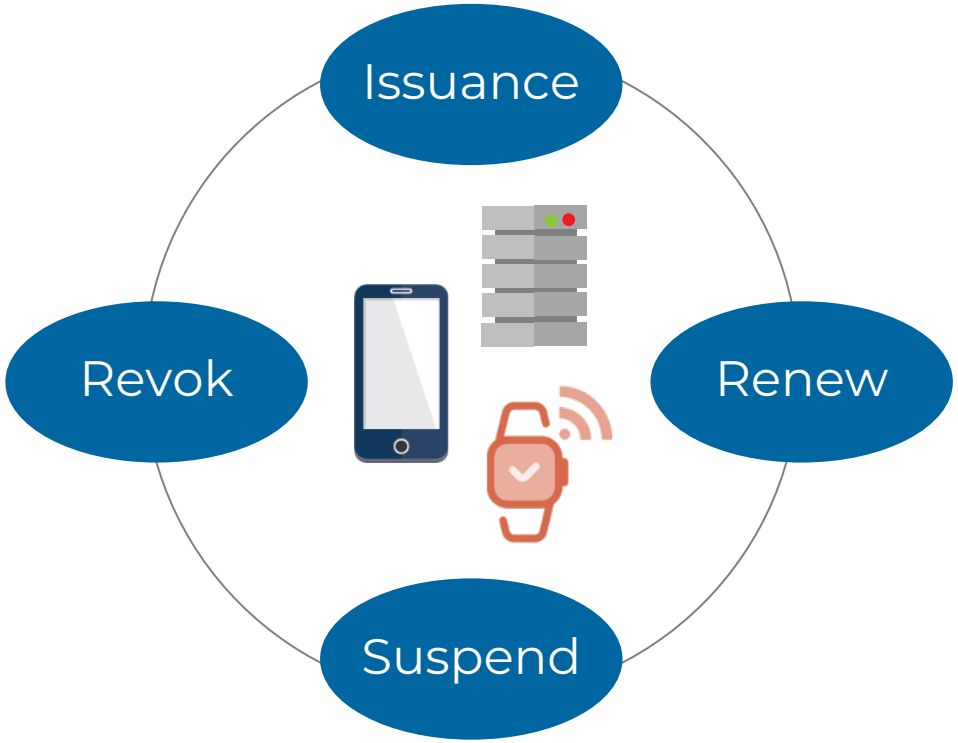
- Unblocking Methods
  - Via Help Desk, online or offline
  - Via Badge Office
  - Self-unlock via CMS Client or Self-Care Web Portal

- Intuitive Web Interface
  - Card Profiles: Configuration of the enrollment process and card unlocking. Select smart card type and stored credentials
  - Data Sources: Detailed configuration of the directory-fetched data
  - Credentials: Configuration of the different credentials during the enrollment for PKI, SSO, OTP

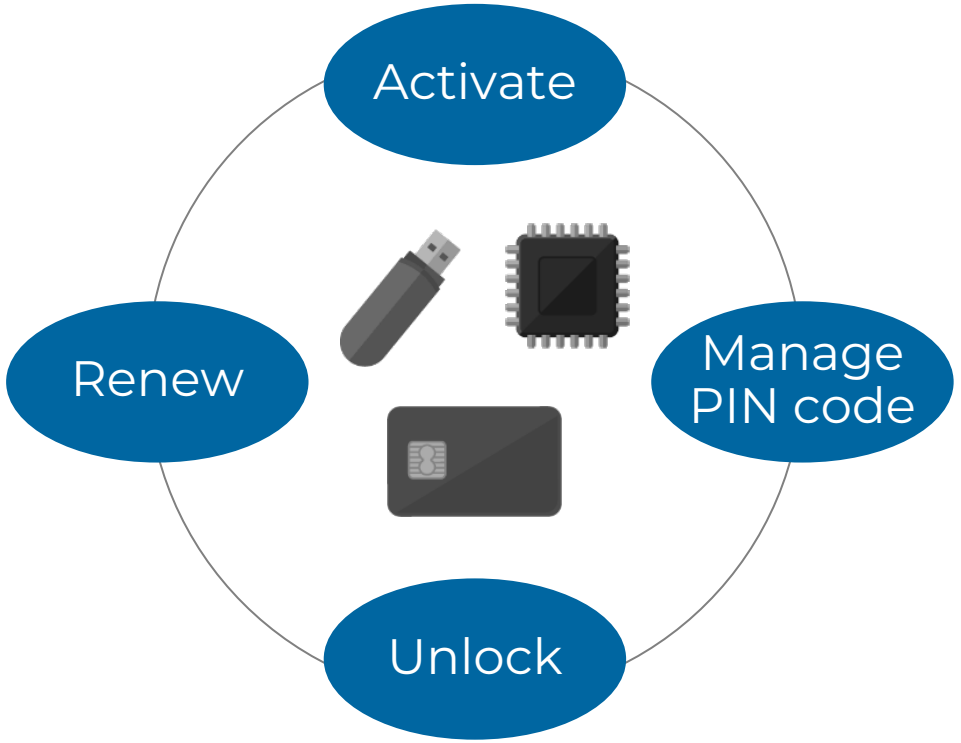
- Common Technical Framework with PKI for logs, rights management, SOAP Connectors

Lifecycle management

A single environment to manage identities on all cryptographic devices

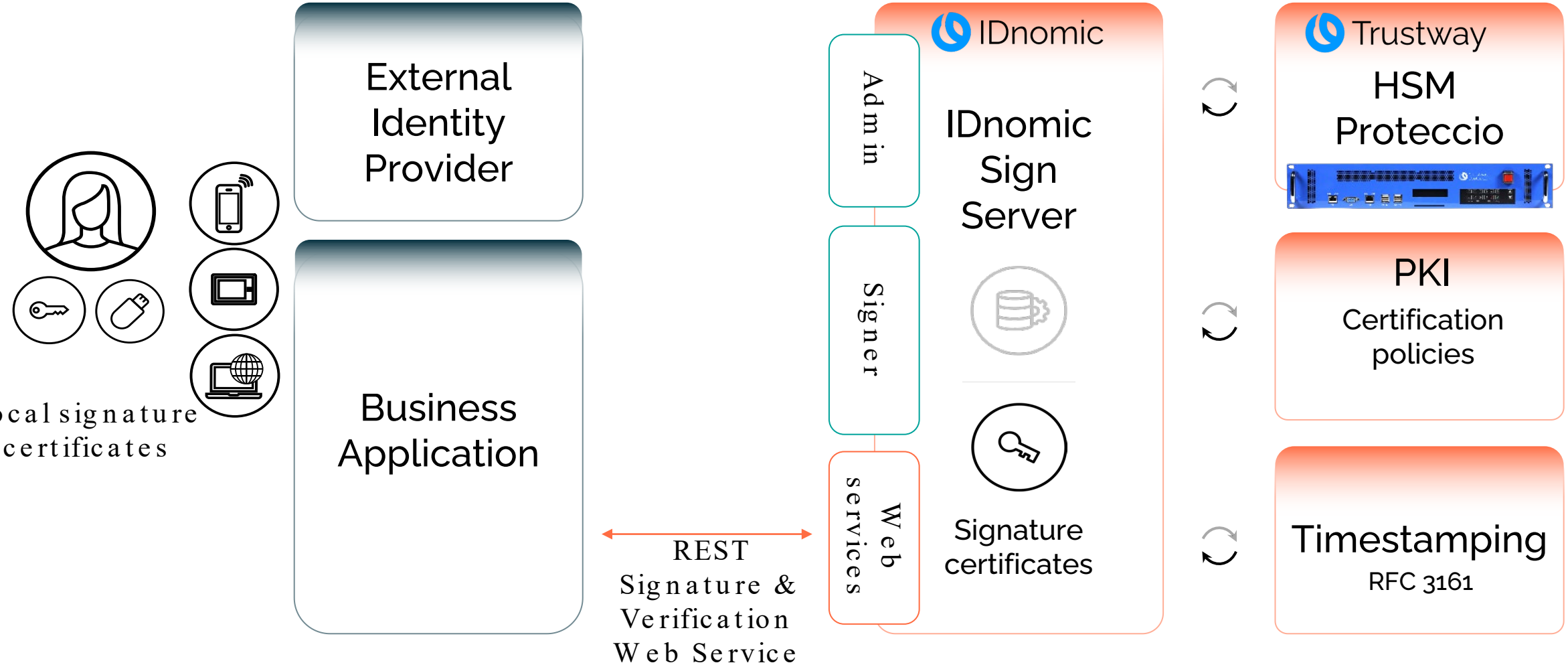


Certificate management



Cryptographic media management

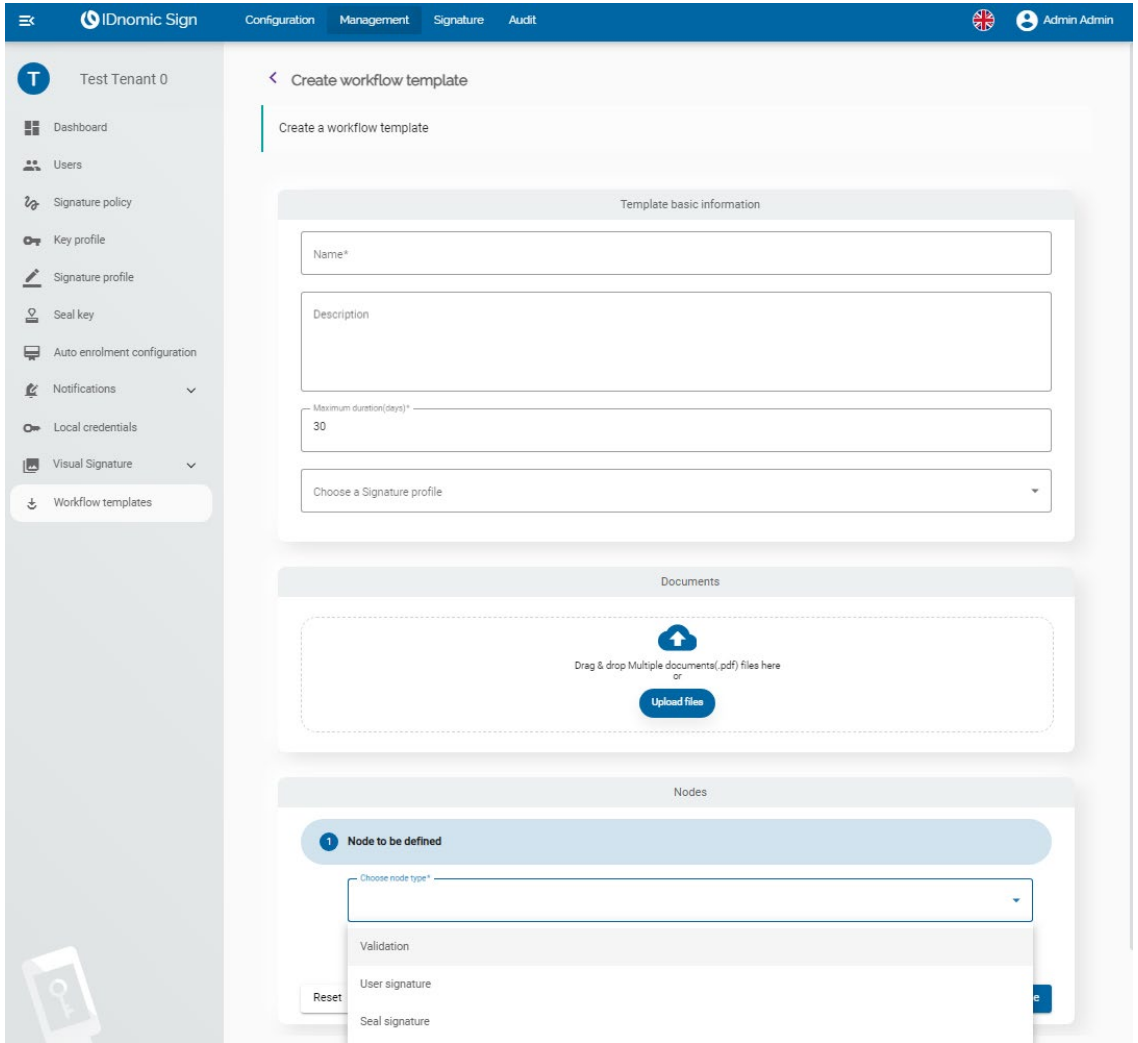
IDnomic Sign Server
Functional architecture



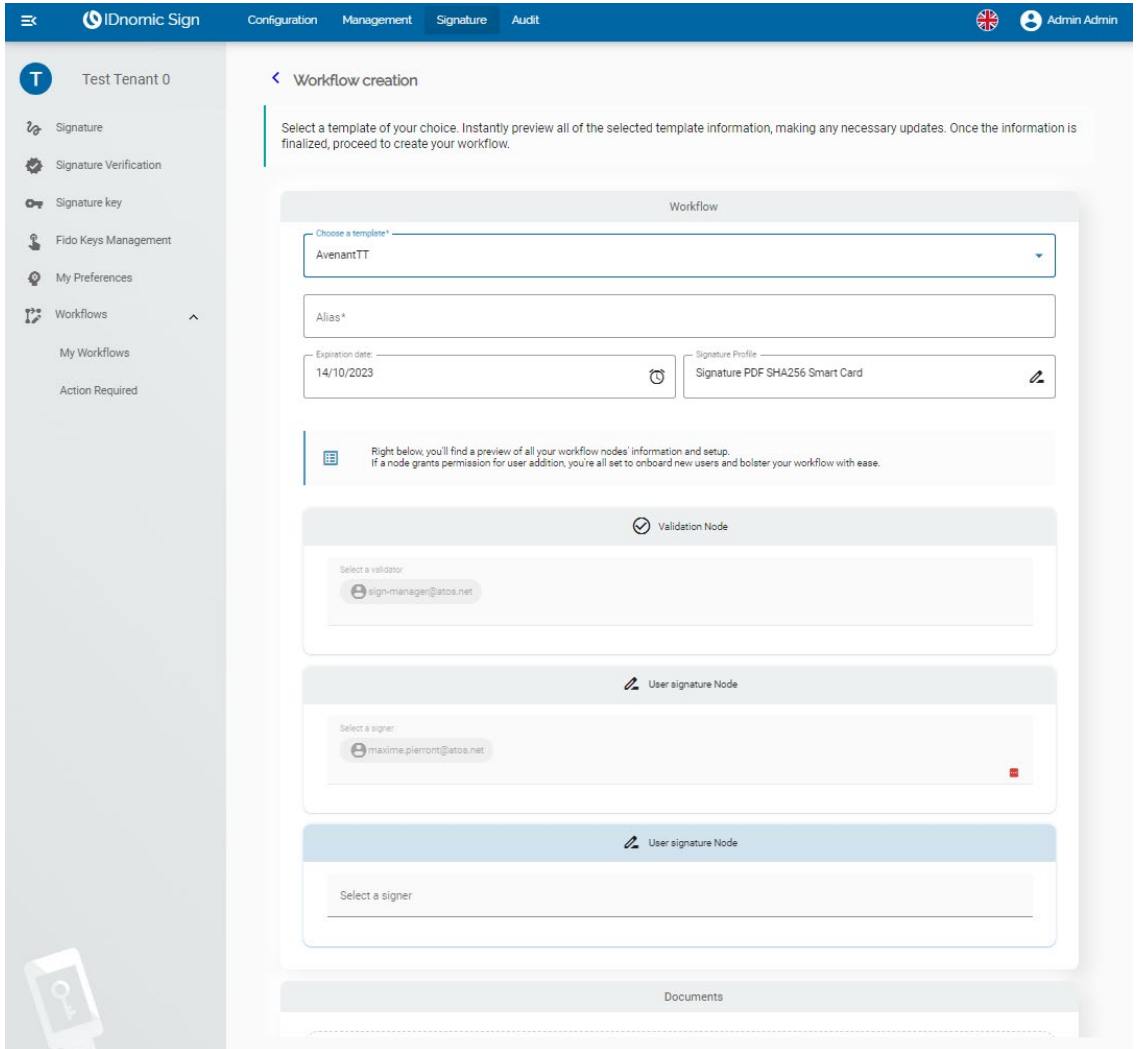
Workflows

Capability to run a sequence of steps

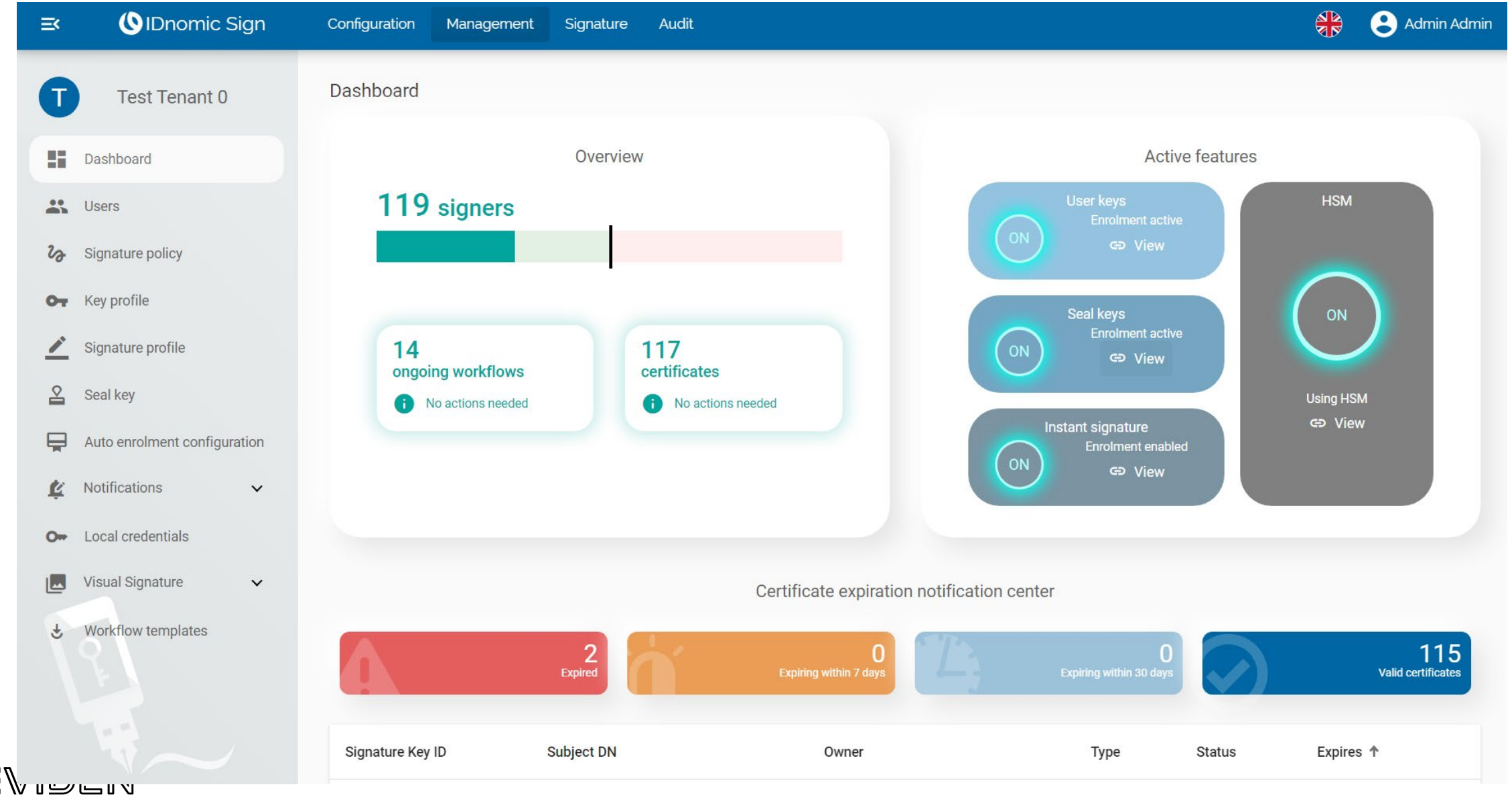
- As an administrator I can create a template to ease the execution of workflows



- As a user I can run customize a template for my purpose and run it.



Dashboard


IDnomic Sign
Configuration
Management
Signature
Audit
Admin Admin
Test Tenant 0
Dashboard
Users
Signature policy
Key profile
Signature profile
Seal key
Auto enrolment configuration
Notifications
Local credentials
Visual Signature
Workflow templates
Dashboard
Overview
119 signers
14
ongoing workflows
No actions needed
117
certificates
No actions needed
Active features
User keys
Enrolment active
View
ON
Seal keys
Enrolment active
View
ON
Instant signature
Enrolment enabled
View
ON
HSM
ON
Using HSM
View
Certificate expiration notification center
2
Expired
0
Expiring within 7 days
0
Expiring within 30 days
115
Valid certificates
Signature Key ID
Subject DN
Owner
Type
Status
Expires