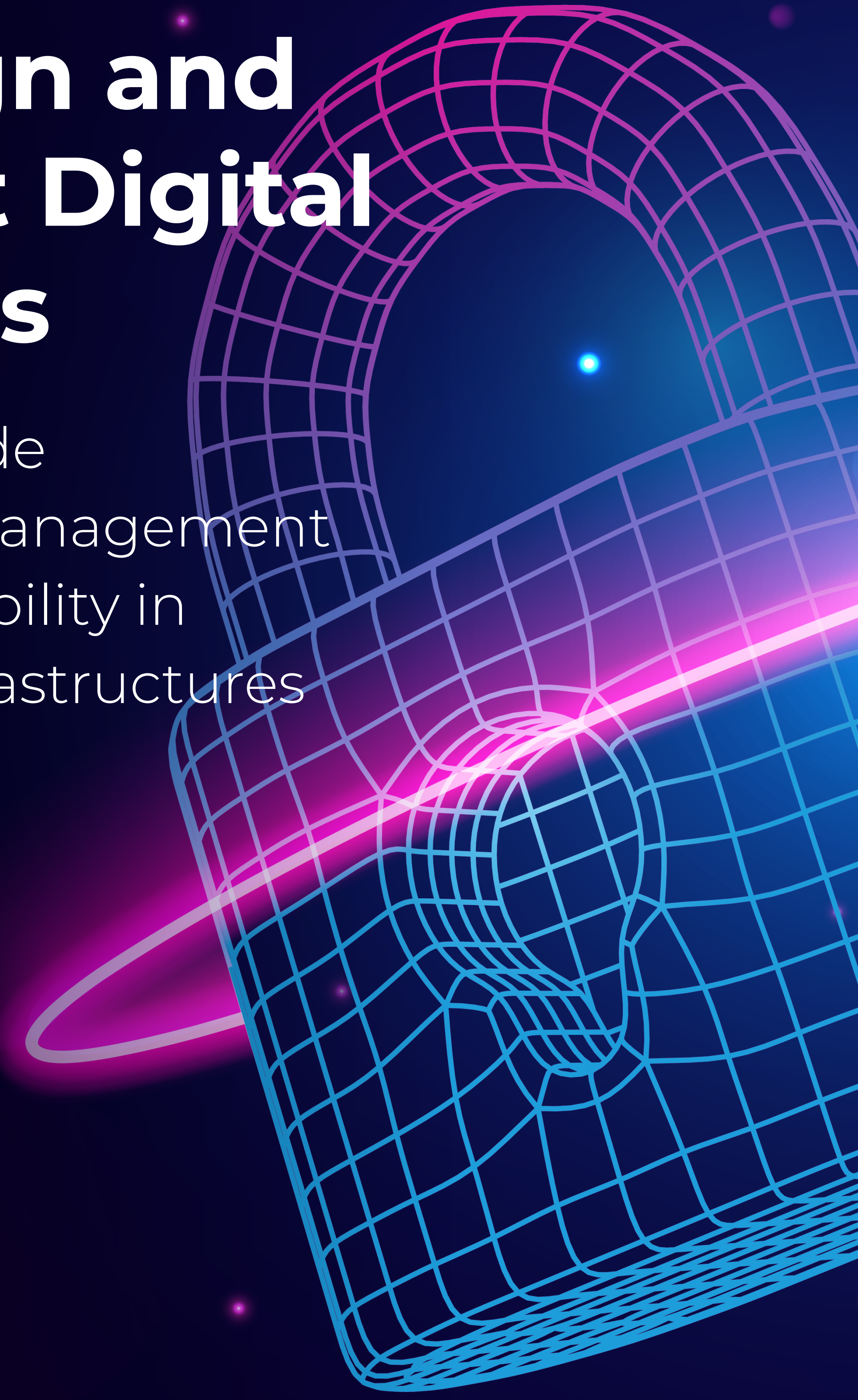
EVIDEN

Sovereign and Resilient Digital Identities

A strategic guide to certificate management and interoperability in complex IT infrastructures



Digitalization poses new challenges for companies and institutions. In addition to efficiency and scalability, the issue of digital sovereignty is increasingly coming to the fore. Digital identities play a central role in this context: they enable secure communication, controlled access, traceability, and trustworthiness. They thus form the foundation for protected digital processes in sensitive areas.

This guide provides a structured overview of requirements, implementation criteria, and proven solutions for resilient digital identities in complex environments with high protection needs—with a focus on standards, interoperability, and avoiding vendor dependencies.

Fundamentals and areas of application of digital identities

Digital identities are ubiquitous: they represent people, systems, or organizational units in digital processes. Protecting them is essential for the integrity, traceability, and confidentiality of communications and transactions. This is achieved through authentication, encryption, and digital signatures based on trusted certificates and secure key material.

Typical usage scenarios

Authentication
for users,
services, and devices

Encryption
of emails, files,
communication

Digital signature
qualified &
automated

Code signing
for secure
software distribution

Access control
for sensible
resources

Special features

Classified information
requires improved
protection

Real-time permission provisioning
instead of static key

Dynamic team compositions
with changing roles

Audit-proof security efficient
and auditable

Security-critical environments

One specific application area is the protection of particularly sensitive information, such as when communicating classified content. Scenarios of this kind require special products enabling high-level cryptographic procedures, approved by the German Federal Office for Information Security (BSI) or a similar authority. The interoperability of these solutions with existing infrastructures and compliance with open standards are crucial to ensuring sustainable and scalable integration.

Requirements and implementation criteria for secure digital identities

Dynamic access management

Flexible rights and access management are essential. Cross-group use of resources, such as access to group or function keys, requires dynamic solutions. Static models, in which cryptographic keys are permanently stored on physical smart cards and issued to individual employees, are only of limited practical use in these scenarios. In the event of personnel changes or changing responsibilities, these keys would have to be manually revoked—a process that is not only prone to errors but also involves a great deal of organizational effort.

Permissions can be granted or revoked in real time

A client-server model with centrally stored private keys offers decisive advantages here: the keys are used temporarily, in a controlled manner, and without leaving the protected storage. Rights can be granted or revoked in real time.

Typical application scenarios with variable access permissions

- **Project groups**
  (e.g., departments or divisions) with changing compositions and dynamic needs for access to data, email accounts, or network segments
- **Role based mailboxes**
  (e.g., “division manager,” “department manager”), which are used on a role basis rather than on a personal basis
- **Mobile technicians,**
  whose access rights change depending on the location and task at hand

Governance and traceability

In security-conscious organizations, technical safeguards alone are not enough. Critical security-related processes—in particular the assignment of keys or the issuance of new certificates—are therefore subject to strict organizational requirements. In particularly sensitive cases, a dual control principle is established, whereby security-critical decisions must always be made and documented jointly by at least two authorized persons. This applies, for example, to the release of decryption keys or the allocation of new qualified signature certificates for sensitive information.

Safety-related processes are subject to strict organizational requirements.

In addition, comprehensive logging is required. All security-related activities must be documented in a traceable manner so that an audit can be guaranteed if necessary—an essential element for both internal compliance requirements and external audit and supervisory processes.

Automation as the basis for scaling and acceptance

User-friendliness is a key success factor for security-related processes. This is because procedures that are perceived as too time-consuming, complex, or incomprehensible are often circumvented in practice—with corresponding risks for the overall architecture. To counteract this, security-critical processes must be as automated, traceable, and transparent to users as possible.

One example is automated onboarding: Once an approval workflow has been completed, access to a group mailbox is automatically set up. The necessary certificates are requested, issued, and integrated in the background—without any active involvement on the part of the users. All that is required is a one-time PIN assignment. Even security-related processes such as resetting forgotten PINs can be implemented reliably and conveniently in this way.

Modern certificate management systems independently recognize expiring certificates and automatically initiate their renewal—differentiated according to the use case and taking into account the respective certification authority. This reduces sources of error and lowers administrative costs in the long term.

Only what is simple will be used reliably.

Approaches to resilient digital identities

Complexity in practice

Organizations often face the challenge of historically grown, heterogeneous IT infrastructures. These bring with them a multitude of technical and organizational peculiarities:

- **The use of specific smart cards, including proprietary middleware, often leads to vendor lock-in.**
- **Outdated or no longer supported smart cards and software components**
- **Lack of interoperability between different platforms, services, or security solutions**
- **A wide variety of device types, operating systems, security domains, and user groups with widely diverging requirements**

This structural and technological fragmentation poses a significant obstacle to consistent, uniform, scalable, and secure certificate management.

Openness, standardization, and interoperability as success factors

A key objective of modern identity infrastructures should be to avoid lock-in effects.

Proprietary solutions that tie organizations to individual providers or technologies stand in the way of long-term flexibility.

Eviden therefore focuses specifically on universal standards, modular architectures, and interoperability. The use of internal, external, and public certification authorities, as well as their combination, is a central principle.

This openness makes it possible to continue using existing components, seamlessly integrate new solutions, and respond flexibly and appropriately to future requirements—such as regulatory changes or technological advances like post-quantum cryptography. At the same time, this ensures a high level of resilience to technological dependencies.

Recommendations for CISOs and IT decision-makers

Analysis
Identify existing dependencies and isolated solutions

Architecture check
Evaluate PKI applications based on standards and scalability

Future planing
Consider post-quantum-readiness in strategy

User focus
Consider user-friendliness as a safety factor

Souvereignty
Prefer European, standardized solutions

Integration
Integrating certificate management into ITSM processes

Conclusion

The secure and confident management of digital identities is one of the key challenges facing modern IT architectures. This involves not only the technical implementation of cryptographic procedures, but also the interplay between architecture, processes, automation, interoperability, and user-friendliness.

Well-designed and future-proof certificate management can be a decisive lever for organizations: it reduces operational complexity, increases security, and facilitates the integration of new areas of application—such as digital signatures, secure email communication, or bring your own device (BYOD) scenarios. It also lays the groundwork for preparing for future challenges such as post-quantum technology.

Organizations that want to modernize their existing PKI structures, streamline their administrative processes, or reliably meet regulatory requirements benefit from a holistic strategy—especially if it is based on standards, modular design, and high interoperability.

Eviden offers a comprehensive portfolio of tried-and-tested solutions for this purpose: from zero-touch onboarding and scalable PKI services to role-based key management. Eviden also offers BSI-approved solutions that ensure the secure transmission and processing of classified information up to the VS-NfD confidentiality level. Particular emphasis is placed on technological sovereignty.

Technological sovereignty requires standards-based, modular architectures.

More Information:
www.cryptovision.com

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Germany
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

About Eviden

Eviden is the Atos Group brand for hardware and software products with c. € 1 billion in revenue, operating in 36 countries and comprising four business units: advanced computing, cybersecurity products, mission-critical systems and vision AI. As a next-generation technology leader, Eviden offers a unique combination of hardware and software technologies for businesses, public sector and defense organizations and research institutions, helping them to create value out of their data. Bringing together more than 4,500 world-class talents and holding more than 2,100 patents, Eviden provides a strong portfolio of innovative and eco-efficient solutions in AI, computing, security, data and applications.

Connect with us

eviden.com