PROTECT

SECUREIDENT
PKI & PIM

SecureIdent is a highly secure authentication solution based on certificate-based two-factor authentication (2FA) in combination with privileged identity management (PIM). The solution was developed to meet the highest security requirements and is suitable for security-critical environments in business, government and defence.

As a provider, we support companies and public authorities in setting up a multi-level enterprise public key infrastructure (PKI), integrating YubiKey smart cards and introducing a PIM system.

KEY FEATURES

- Certificate-based authentication (PKI) with X.509 certificates
- YubiKey 5 FIPS hardware token as a smart card (FIPS 140-2 Level 2 certified)
- PIV-compatible authentication (smartcard login)
- Integrated Privileged Identity Management (PIM)

  Temporary rights assignment

  Permission-based access

  Role-based assignment

  Least Privilege Enforcement
- Central certificate management (CA integration)
- Compatible with Microsoft Entra ID (formerly Azure AD), AD FS, Linux PAM, and more
- Auditability & logging according to NIST SP 800-53

SERVICE DESCRIPTION

Our company provides comprehensive support to customers in the implementation of a highly secure, certificate-based authentication infrastructure. Our services include:

MH SERVICE
WORLD OF FORENSICS

PROTECT

SECUREIDENT
PKI & PIM

Consulting & Concept Development

- Analysis of existing IAM/PKI environments
- Security requirements & target vision definition
- Selection of suitable components (CAs, middleware, PIM systems, tokens)

PKI implementation

- Establishment of a multi-level enterprise PKI (root CA, issuing CAs)
- Documentation, governance & operating concepts (e.g. according to ETSI EN 319 411-1/2)
- Key Management & Policy Creation (CP/CPS)

YubiKey integration

- User enrolment with X.509 certificates
- Smartcard-Login & Middleware-Deployment
- Role & certificate allocation

Privileged Identity Management (PIM)

- Integration with Microsoft Entra ID PIM or other systems
- Definition of roles & guidelines
- Automation & auditing of privileged access

Rollout, support & training

- Support for pilot phases and migration projects
- Training courses for administrators and helpdesk staff
- Operating manual & maintenance contracts

MH SERVICE
WORLD OF FORENSICS

PROTECT

SECUREIDENT PKI & PIM

APPLICATION SCENARIOS

- Access to highly sensitive IT systems and administrative networks
- Authentication on Windows, Linux and web systems
- Zero Trust networks with hardware-bound identity
- Managing privileged accounts in hybrid environments

SICHERHEITSSTANDARDS & ZERTIFIZIERUNGEN

AREA	STANDARD / CERTIFICATION
• hardware token	• FIPS 140-2 Level 2 (YubiKey 5 FIPS)
• authentication	• X.509, PIV, PKCS#11, OpenPGP
• PIM architecture	• NIST SP 800-53, ISO/IEC 27001
• compatibility	• BSI TR-03107, Common Criteria Ready

TECHNICAL REQUIREMENTS

- Client support: Windows 10/11, macOS, Linux
- Smartcard middleware: Supports Microsoft MiniDriver, OpenSC, PIV middleware
- Infrastructure: Active Directory / Entra ID / OpenLDAP / SSSD
- PKI compatibility: Microsoft CA, EJBCA, other X.509-compliant CAs

MH SERVICE
WORLD OF FORENSICS

PROTECT

SECUREIDENT
PKI & PIM

WHY ‘MILITARY GRADE’?

SecureIdent is based on technologies used in security-critical government environments. The combination of:

- Hardware-based 2FA with FIPS-certified YubiKeys
- Certificate-based, tamper-proof authentication
- Compliant implementation of zero trust & least privilege
- Auditability and traceability according to NIST standards

....makes SecureIdent the ideal choice for environments with the highest security requirements.

ADDITIONAL SERVICES (OPTIONAL)

- Initial security analysis & integration
- penetration tests
- Training for administrators & helpdesk staff
- Maintenance & update contract

MH SERVICE
WORLD OF FORENSICS