

synrion-xbind-readiness-checklist-de

SYNRION x.ID readiness checkliste

Info

Letzte freigegebene PDF-Version:

[synrion-xid-readiness-checklist-de_v1.0.pdf](#)

(Pfad: de/synrion/xid/_media/synrion-xid-readiness-checklist-de_v1.0.pdf)

Inhaltsverzeichnis

- [SYNRION x.ID readiness checkliste](#)
 - [Inhaltsverzeichnis](#)
 - [Änderungsverlauf](#)
- [Readiness Checkliste SYNRION x.ID](#)
 - [Zertifikatsbasiertes Identity Management fuer YubiKey, PIV-Token und hardwaregebundene Identitaeten](#)
 - [Fuer hoch segmentierte, regulierte und komplexe Infrastrukturen](#)
 - [Fuer kompakte, pragmatische und sicherheitsbewusste Setups](#)
 - [Sicherheitsanspruch auch auf der Serverseite](#)
 - [Warum das Thema kritisch ist](#)
 - [Zweck](#)
 - [Was Sie am Ende haben](#)
 - [Fuer wen lohnt sich SYNRION x.ID](#)
 - [ROI und Einstiegsschwelle](#)
 - [Minimalanforderungen \(einfaches Setup\)](#)
 - [Maximalsetup \(hoch segmentiert, reguliert, HA\)](#)
 - [x.ID Features](#)
 - [🔒 Beyond Enrollment - Die drei Enforcements](#)
 - [🔒 Policy Enforced](#)
 - [🔑 HSM Enforced](#)
 - [📅 PKI Lifecycle Enforced](#)
 - [Typische Einsatzszenarien](#)
 - [👤 Multi-Identity Support](#)
 - [Warum x.ID](#)
 - [Vollstaendiger X.509-Lifecycle](#)
 - [Flexibles Betriebsmodell: agentless oder agent-based](#)
 - [Multi-Identity Support](#)
 - [Ein YubiKey - mehrere Identitaeten](#)
 - [Policy-Enforcement](#)
 - [HSM-Enforced](#)

- [PKI Lifecycle Enforced](#)
- [AD- und Entra-Readiness als Teil der Erstintegration](#)
- [Security endet nicht am Produkt](#)
- [Was zertifikatsbasiertes Identity Management wirklich umfasst](#)
- [Offene Fragen, die vor einer Kaufentscheidung geklärt werden sollten](#)
 - [Architektur und Segmentierung](#)
 - [Token, Endpunkte und Deployment](#)
 - [PKI, CA und Protokolle](#)
 - [HSM, Schlüsselschutz und Schutzbedarf](#)
 - [AD, Entra und Domain Controller](#)
 - [Betrieb, Rollen, Rechte und Prozesse](#)
 - [Evidence, Audit und Compliance](#)
- [Abschnitt 1: Quick Pass \(10 Fragen\)](#)
 - [Quick Interpretation](#)
- [Abschnitt 2: x.ID Core Use-Cases \(Was wird automatisiert und kontrolliert?\)](#)
 - [Kurzbewertung \(Abschnitt 2\)](#)
- [Abschnitt 3: Voraussetzungen und Architekturfragen \(Was brauchen wir dafür?\)](#)
 - [Kurzbewertung \(Abschnitt 3\)](#)
- [Abschnitt 4: Sichtbarkeit, Evidence, Audit \(Was bekommen wir heraus?\)](#)
 - [Kurzbewertung \(Abschnitt 4\)](#)
- [Abschnitt 5: Pilot Worksheet \(Scope, Erfolgskriterien, Deliverables\)](#)
 - [5.1 Pilot Scope](#)
 - [5.2 Erfolgskriterien \(Messbar\)](#)
 - [5.3 Deliverables \(Was liefern wir im Pilot?\)](#)
- [Abschnitt 6: Auswertung \(Scoring und Interpretation\)](#)
- [Abschnitt 7: Minimal Evidence Set \(was im Audit wirklich zählt\)](#)
- [Abschnitt 8: Pilot Output Paket \(was ein Pilot liefern muss\)](#)
- [Kontakt](#)

Änderungsverlauf

- v1.0 – Initialer Entwurf

Readiness Checkliste SYNRIION x.ID



Zertifikatsbasiertes Identity Management fuer YubiKey, PIV-Token und hardwaregebundene Identitaeten

Note

Claim: Alle PKI-Prozesse. Automatisiert. Nachvollziehbar. Policy-enforced.

SYNRION x.ID ist die zentrale Plattform fuer die sichere Verwaltung, Durchsetzung und Automatisierung PIV-basierter Identitaeten in Enterprise-, Behoerden- und KRITIS-Umgebungen (IT/OT). Die Loesung verbindet Token-Management, X.509-Lifecycle, Policy-Enforcement, HSM-gestuetzten Schluesselschutz und revisionsfaehige Nachvollziehbarkeit in einem durchgaengigen System.

Fuer hoch segmentierte, regulierte und komplexe Infrastrukturen

Seine besondere Staerke entfaltet SYNRION x.ID in hoch segmentierten, regulierten und sicherheitskritischen Infrastrukturen. Genau dort geraten viele Loesungen an ihre Grenzen: weil Netzsegmente getrennt sind, Rollen strikt voneinander abgegrenzt werden muessen, Dienste nicht beliebig miteinander kommunizieren duerfen und dennoch ein konsistenter, auditfaehiger Betrieb erwartet wird. SYNRION x.ID wurde fuer genau diese Realitaet entwickelt.

Die Plattform unterstuetzt kontrollierte Kommunikationspfade, klare Rollentrennung, segmentierungsgerechte Service-Architekturen sowie nachvollziehbare Prozesse ueber den gesamten Lebenszyklus digitaler Identitaeten hinweg. Dazu gehoeren auch komplexe Verzeichnis- und Betriebsmodelle, etwa Multi-Domain-Umgebungen, Multi-Forest-Strukturen ohne direkte Trusts sowie On-Prem-, Hybrid- und Cloud-native Bereitstellungsmodelle.

Damit eignet sich x.ID besonders fuer grosse Unternehmen, Behoerden, KRITIS-Organisationen und alle Umgebungen, in denen Identitaet, Zertifikat und Hardware-Token nicht nur verwaltet, sondern ueber unterschiedliche Sicherheitszonen, Verzeichnissgrenzen und Betriebsmodelle hinweg sicher, stabil und revisionsfaehig betrieben werden muessen.

Fuer kompakte, pragmatische und sicherheitsbewusste Setups

Gerade fuer kleinere Organisationen oder klar umrissene Einsatzszenarien ist das ein entscheidender Vorteil: hohe Sicherheit, saubere Architektur und kontrollierte Prozesse, ohne dass von Beginn an eine grosse Zielinfrastruktur vorausgesetzt wird. x.ID waechst

damit entlang der Anforderungen - vom fokussierten Einstieg bis zur umfassenden Enterprise-Architektur.

Sicherheitsanspruch auch auf der Serverseite

Für den Schutz serverseitiger Schlüssel verfolgt SYNRIION x.ID einen klaren Sicherheitsansatz: **HSM statt ungeschützter Schlüsselspeicherung**. Denn es ist schwer vermittelbar, wenn Benutzeridentitäten konsequent in Hardware-Token geschützt werden, während die privaten Schlüssel ausstellender, prüfender oder vermittelnder Dienste im Dateisystem oder im lokalen Zertifikatsstore liegen.

SYNRIION x.ID unterstützt dabei nicht nur klassische Enterprise-HSMs, sondern auch wirtschaftliche Einstiegsmodelle. Neben grossen Plattformen wie Thales oder Utimaco lassen sich auch kompakte und kosteneffiziente Alternativen sinnvoll integrieren, beispielsweise YubiHSM-basierte Designs in redundanter Auslegung. Das senkt die Einstiegshürde deutlich und schafft dennoch ein Schutzniveau, das softwarebasierte Schlüsselspeicherung klar übertrifft.

SYNRIION x.ID skaliert damit entlang Ihrer Realität: von einem einzelnen Server bis zur hoch segmentierten Sicherheitsarchitektur, von pragmatischen Einstiegsmodellen bis zum durchgehend HSM-gestützten Betriebsmodell.

Warum das Thema kritisch ist

Zertifikatsbasierte Authentifizierung gilt zu Recht als deutlich stärker als passwort- oder OTP-basierte Modelle. In der Praxis entsteht diese Sicherheit jedoch nicht durch das Zertifikat allein, sondern erst durch das korrekte Zusammenspiel von Hardware-Token, PKI, Active Directory, Microsoft Entra, Domain Controllern, Smartcard-Policies, Certificate Mapping, Revocation-Verhalten und sauber abgesicherten Service-Endpunkten.

Genau hier liegt heute die eigentliche Herausforderung: Viele Organisationen wollen phishing-resistente, hardwaregebundene Identitäten einführen, unterschätzen aber den operativen und architektonischen Aufwand. Starke zertifikatsbasierte Authentifizierung ist weder in Entra noch im lokalen Active Directory einfach out of the box sicher. Ohne Hardening, Baselines, nachvollziehbare Lifecycle-Prozesse und kontrollierte Richtliniendurchsetzung entstehen unsaubere Zuordnungen, verwaiste Zertifikatszustände, Medienbrüche und später teure Audit- oder Betriebsprobleme.

Hinzu kommt: Wer Endanwenderidentitäten konsequent auf Hardware absichert, muss denselben Sicherheitsanspruch auch auf der Serverseite, im Lifecycle und in den angrenzenden Verzeichnis- und CA-Diensten durchhalten. Genau hier setzt SYNRIION x.ID an: nicht nur bei der Ausstellung, sondern beim sicheren, kontrollierten und nachweisbaren Gesamtbetrieb digitaler Identitäten.

Zweck

Diese Checkliste klärt in 10-15 Minuten die wichtigsten Fragen vor einer Einführung von SYNRIION x.ID:

- Welche Anforderungen adressiert x.ID in Ihrer Umgebung konkret?

- Welche Betriebsmodelle sind sinnvoll - kompakt, segmentiert, agentless, agent-based oder HSM-gestuetzt?
- Welche technischen und organisatorischen Voraussetzungen muessen fuer starke zertifikatsbasierte Authentifizierung geschaffen werden?
- Welche Mehrwerte entstehen fuer Sicherheit, Betrieb, Audit und Compliance?
- Wie laesst sich ein sinnvoller Pilotumfang definieren?

Der Fokus liegt bewusst nicht nur auf Token-Ausgabe oder Enrollment, sondern auf dem gesamten Sicherheits- und Betriebsmodell: von der Initialisierung ueber Policy-Pruefung, Lifecycle und AD-/Entra-Readiness bis hin zu Evidence, Audit und kontrolliertem Betrieb.

Was Sie am Ende haben

Am Ende dieser Checkliste haben Sie:

- eine kurze Standortbestimmung, ob und wo SYNRIION x.ID in Ihrer Umgebung unmittelbaren Mehrwert schafft
- einen strukturierten Ueberblick ueber technische, organisatorische und sicherheitsrelevante Voraussetzungen
- eine klare Sicht auf moegliche Betriebsmodelle - vom Single-Server-Setup bis zur segmentierten Enterprise-Architektur
- eine Liste offener Architektur-, Security- und Integrationsfragen fuer die Kaufentscheidung
- einen belastbaren Ausgangspunkt fuer einen Pilot mit klaren Erfolgskriterien

Fuer wen lohnt sich SYNRIION x.ID

Note

Sichere Identitaeten sind keine Groessenfrage.

Nicht die Unternehmensgroesse entscheidet ueber den Schutzbedarf, sondern der Anspruch, Zugaenge, Rollen und digitale Identitaeten wirklich sicher zu betreiben. SYNRIION x.ID ist deshalb nicht nur fuer hochkomplexe Enterprise- und KRITIS-Umgebungen geeignet, sondern ebenso fuer kompakte und sicherheitsbewusste Organisationen.

SYNRIION x.ID lohnt sich fuer alle Organisationen, die zertifikatsbasierte Identitaeten nicht nur ausstellen, sondern kontrolliert, nachvollziehbar und sicher betreiben wollen. Die Plattform adressiert komplexe, segmentierte und regulierte Zielbilder ebenso wie kompakte Umgebungen mit hohem Sicherheitsanspruch.

Besonders relevant ist x.ID typischerweise fuer:

- Unternehmen und Behoerden mit YubiKey-, PIV- oder Smartcard-basierten Login- und Admin-Szenarien
- regulierte oder sicherheitskritische Umgebungen mit hohen Anforderungen an Rollen, Nachvollziehbarkeit und Hardening

- Organisationen mit AD-, Entra- oder hybriden Identitätslandschaften, in denen Strong Authentication technisch belastbar umgesetzt werden muss
- Umgebungen mit mehreren CA-Strukturen, segmentierten Netzen, HSM-Vorgaben oder besonderen Anforderungen an Break-Glass-, Betriebs- und Admin-Identitäten
- Teams, bei denen manuelle Enrollment-, Revocation-, Replacement- oder Token-Prozesse zu hohem Aufwand, Fehlern oder Auditproblemen führen

Kurz gesagt: SYNRIION x.ID lohnt sich dort, wo Hardware-Token und Zertifikate nicht nur ausgegeben, sondern als Teil eines belastbaren Sicherheits- und Betriebsmodells eingeführt werden sollen - unabhängig davon, ob die Umgebung kompakt, mittelgross oder hochkomplex ist.

ROI und Einstiegsschwelle

Der wirtschaftliche Nutzen von SYNRIION x.ID beginnt dort, wo digitale Identitäten nicht mehr als Einzelfall, sondern als kontrollierter und sicherheitskritischer Betriebsprozess behandelt werden müssen. In der Praxis ist das häufig bereits ab etwa 50 Identitäten der Fall - insbesondere dann, wenn privilegierte Rollen, Hardware-Token, auditierbare Prozesse oder hohe Sicherheitsanforderungen ins Spiel kommen.

Mit wachsender Anzahl an Identitäten, Token, Rollen und organisatorischen Anforderungen steigt der Nutzen überproportional. Der Hebel entsteht nicht allein durch die Ausgabe von Zertifikaten, sondern vor allem durch die Reduktion manueller Betriebsanteile, Medienbrüche und sicherheitsrelevanter Risiken, insbesondere bei:

- Enrollment, Replacement und Re-Issuance
- PIN-/PUK- und tokenbezogenen Betriebsprozessen
- Revocation, Cleanup und Publishing in AD, LDAP und Entra
- Multi-Identity- und Rollenmodellen auf Hardware-Token
- Audit- und Evidence-Anforderungen
- Hardening, Baseline-Einführung und kontrolliertem Rollout

Je höher Schutzbedarf, Segmentierung, Anzahl der Identitäten oder regulatorischer Druck sind, desto schneller wird x.ID zu einem klaren Betriebs-, Sicherheits- und Effizienzvorteil.

Minimalanforderungen (einfaches Setup)

SYNRIION x.ID kann in einem kompakten Basisszenario bereits mit überschaubarem Infrastrukturaufwand betrieben werden.

Typisches Minimalsetup:

- 1x Windows Server für x.ID Core, Services und Portal
- 1x SQL Datenbank für Konfiguration, Status, Events, Audit und Lifecycle-Daten
- 1x angebundene CA bzw. PKI
- 1x angebundene Zielumgebung, typischerweise Active Directory, optional zusätzlich Microsoft Entra
- optional HSM-Anbindung für serverseitigen Schlüsselschutz, dringend empfohlen

Hinweise:

- Ein kompaktes Setup kann auf einem einzigen Host betrieben werden.
- Auch in kleinen Setups bleiben Dienste und Service-Identitäten logisch getrennt.
- Agentless-Modelle sind möglich und für viele Einstiegs- oder Verwaltungsszenarien sinnvoll.
- Der Einsatz eines HSM ist auch in kompakten Setups fachlich empfehlenswert.

Maximalsetup (hoch segmentiert, reguliert, HA)

Für hoch segmentierte, regulierte und sicherheitskritische Umgebungen kann SYNRIION x.ID als verteilte und hochverfügbare Architektur betrieben werden.

Typisches Zielbild:

- x.ID Core, Portal und zentrale Services als hochverfügbare Komponenten
- SQL Datenbank hochverfügbar, je nach Plattformstandard
- Outpost Services für Policy Enforcement, LDAP/Entra-Anbindung und CA Connectoren je nach Segment, Zone oder Sicherheitsanforderung
- Anbindung mehrerer Certification Authorities innerhalb einer gemeinsamen Architektur
- HSM-gestützte Service-Schlüssel für zentrale und sicherheitskritische Komponenten
- getrennte Betriebswege für Admin-, User-, Betriebs- oder Break-Glass-Identitäten
- agentless und/oder agent-based, je nach Schutzbedarf und Zielarchitektur

Ergebnis:

- kontrollierte und firewall-freundliche Kommunikationspfade
- saubere Trennung von Endidentitäten, Verzeichnisdiensten und Certification Authorities
- konsistente Richtlinienprüfung auch in stark segmentierten Umgebungen
- nachvollziehbare Lifecycle- und Audit-Prozesse über mehrere Zonen und Vertrauensräume hinweg
- eine Architektur, die sowohl hohe Sicherheit als auch skalierbaren Betrieb ermöglicht

SYNRION x.ID skaliert damit entlang Ihrer Realität: von einem einzelnen Server bis zur hoch segmentierten Sicherheitsarchitektur, von pragmatischen Einstiegsmodellen bis zum durchgehend HSM-gestützten Betriebsmodell.

x.ID Features



Beyond Enrollment - Die drei Enforcements



Policy Enforced

- **Technisch erzwungene Richtlinienreue:** Zertifikatsanfragen werden nicht nur formal angenommen, sondern unmittelbar vor Ausstellung bzw. Signatur gegen definierte Richtlinien und autoritative Quellen geprüft.

- **Mehr-Augen-Prinzip durch neutrale Instanzen:** Outpost Services validieren Requests unabhaengig gegen LDAP, Entra ID oder andere Quellsysteme und schaffen damit ein technisch erzwungenes, nachvollziehbares Kontrollmodell.
- **Geeignet fuer segmentierte und Multi-CA-Architekturen:** Outposts koennen in Reihe oder parallel betrieben werden, bauen firewall-freundliche Kommunikationspfade auf und ermoeglichen die saubere Trennung von Endidentitaeten, Vertrauenszonen und Certification Authorities.



HSM Enforced

- **Konsistenter Schlüsselschutz:** Wenn Endidentitaeten hardwarebasiert auf YubiKey oder PIV-Token geschuetzt werden, sollten auch die privaten Schlüssell der x.ID-Services nicht softwarebasiert abgelegt werden, sondern im HSM bleiben.
- **Sichere Service-Architektur:** SYNRIION x.ID nutzt Zertifikate selbst als Sicherheitsgrundlage - fuer mTLS zwischen Diensten, geschuetzte Service-Endpunkte, Signaturprozesse und sensible Kommunikationspfade.
- **Hohe Sicherheit auch wirtschaftlich umsetzbar:** Neben klassischen Enterprise-HSMs unterstuetzt x.ID auch kosteneffiziente Modelle, zum Beispiel zwei redundant betriebene YubiHSM-Module fuer Ausfallsicherheit und Backup.



PKI Lifecycle Enforced

- **Durchgaengige Lifecycle-Kontrolle:** Ausstellung, Renewal, Revocation, Rollover, Re-Issuance und Cleanup werden nicht als isolierte Einzelaktionen behandelt, sondern als kontrollierter Gesamtprozess.
- **Saubere Bereinigung in Verzeichnis- und Zielsystemen:** Zertifikatswechsel und Widerrufe werden nicht nur in der CA sichtbar, sondern auch in LDAP, Entra und weiteren Zielsystemen nachvollziehbar nachgezogen.
- **Mehr Sicherheit und weniger Betriebsrisiko:** x.ID reduziert Medienbrueche, Altlasten, verwaiste Zuweisungen und unsaubere Restzustaende, die in der Praxis haeufig zu Stoerungen, Fehlsuordnungen oder Audit-Findings fuehren.

Typische Einsatzszenarien

- _Rollout und Betrieb von YubiKey- und PIV-basierten Logon-Identitaeten in Tier- und Multi-Forest-Architekturen.
- _Self-Service- und on-behalf-of-Prozesse fuer Onboarding, Replacement, PIN-Management und Wiederanlauf.
- _PIV-Attestation, kontrollierte Zertifikatsausstellung und policy-konforme CSRs auch fuer heterogene CA-Landschaften.
- _Publishing und Cleanup in Active Directory (LDAP) und Entra ID inklusive Strong Authentication und Strong Certificate Binding.
- _Trennung mehrerer Rollen und Identitaeten auf einem Token, inklusive Admin-, Betriebs- und Break-Glass-Kontexten.



Multi-Identity Support



Note

Ein YubiKey - mehrere Identitäten (1:n)

x.ID ermöglicht strikt getrennte **Mehrfach-Identitäten** auf **einem** YubiKey ueber zusätzliche PIV-Key-Container und, wo technisch zulaessig, Retired Slots. Damit lassen sich beispielsweise Admin-, Betriebs- und Break-Glass-Rollen auf einem Token sauber getrennt abbilden - explizit freigegeben, policy-gesteuert und vollstaendig auditierbar.

Hinweis: Diese Betriebsform ist technisch mit YubiKey-PIV moeglich, aber nicht Bestandteil des klassischen Standard-PIV-Profiles und daher nur nach expliziter Freigabe sinnvoll.

Warum x.ID

Vollstaendiger X.509-Lifecycle

Initialisierung, Enrollment, Re-Enrollment, Revocation, Replacement und Deprovisionierung in einem durchgaengigen, kontrollierten Prozess.

Flexibles Betriebsmodell: agentless oder agent-based

SYNRION x.ID ist nicht auf ein einziges Betriebsmodell festgelegt. Die Plattform kann **agentless** ohne lokale Client-Installation betrieben werden und eignet sich damit hervorragend fuer Umgebungen, in denen eine schlanke Architektur, geringe AngriffsOberflaeche und hohe Kompatibilitaet im Vordergrund stehen. In diesem Modell erfolgt die Steuerung zentral ueber freigegebene Verwaltungswege.

Ebenso kann x.ID **agent-based** ausgerollt werden. Dieses Modell ist besonders fuer hochkritische Clients relevant, wenn zu jeder Zeit nachvollziehbar sein muss, welcher Hardware-Token an welchem System eingesteckt ist oder wenn bereits ein unerlaubter Token als Sicherheitsverstoss bewertet wird. Auch in stark automatisierten Umgebungen kann dieser Ansatz gezielt Vorteile bieten.

Note

SYNRION x.ID passt sich damit dem Schutzbedarf an: **agentless** fuer einen schlanken, zentralen Betrieb; **agent-based** fuer maximale Endpunkttransparenz und tiefere Automatisierung.

Multi-Identity Support

Ein YubiKey - mehrere Identitäten

Im klassischen PIV-Betrieb ist die nutzbare Identitätsabbildung in der Praxis eng am Standardprofil ausgerichtet: 9A fuer Authentisierung, 9C fuer Signatur, 9D fuer Key Management und 9E fuer Card Authentication. Der YubiKey stellt zusaetzlich weitere PIV-Slots bereit, darunter die Retired-Key-Management-Slots 82 bis 95.

docs.yubico.com

docs.yubico.com

Note

Ein Mensch - mehrere Identitäten - ein YubiKey.

SYNRION x.ID macht ein kontrolliertes, policy-gesteuertes und auditierbares Multi-Identity-Modell auf einem einzelnen Hardware-Token praktikabel.

Die Besonderheit von SYNRION x.ID liegt darin, dass diese technischen Möglichkeiten in Verbindung mit dem YubiKey erstmals als **kontrolliertes Multi-Identity-Betriebsmodell** nutzbar werden. Dadurch kann eine einzelne Person mehrere strikt getrennte digitale Identitäten auf einem einzigen Token führen - zum Beispiel für Standard-User, Administration, Betrieb oder Break-Glass-Szenarien.

Diese Mehrfachnutzung erfolgt nicht beliebig, sondern nur explizit freigegeben, policy-gesteuert und vollständig auditierbar. So verbindet SYNRION x.ID die Hardware-Sicherheit des YubiKey mit einem Identitätsmodell, das in der Praxis deutlich flexibler ist als das klassische Standard-PIV-Profil.

Multi-Identity Support bedeutet damit: **ein Mensch, mehrere Identitäten, ein Hardware-Token - sauber getrennt, kontrolliert und nachvollziehbar.**

Policy-Enforcement

SYNRION x.ID prüft Zertifikatsanfragen nicht nur formal, sondern **setzt Richtlinien technisch durch** - unmittelbar vor Ausstellung bzw. Signatur. Dazu können sogenannte Outpost Services flexibel in Reihe oder parallel aufgebaut werden. Jeder Outpost arbeitet eigenständig, bewertet den Request neutral und validiert die angefragten Inhalte direkt gegen die jeweils massgebliche Quelle, zum Beispiel LDAP, Entra ID oder andere autoritative Systeme.

Genau diese Neutralität ist entscheidend: Die Prüfung erfolgt nicht ausschliesslich dort, wo der Antrag entsteht oder verarbeitet wird, sondern wird über eine oder mehrere unabhängige Instanzen technisch nachvollzogen. So entsteht ein **technisch erzwungenes Mehr-Augen-Prinzip**, das nicht nur organisatorisch beschrieben, sondern systemseitig umgesetzt wird.

Outpost Services haben dabei noch einen zweiten wesentlichen Vorteil: Sie schaffen in stark segmentierten Infrastrukturen **klar definierte, kontrollierbare Kommunikationspfade**. Dadurch lassen sich die eigentlichen Kronjuwelen der PKI - insbesondere die Certification Authorities - sauber von den Endidentitäten und anfordernden Systemen trennen. Requests müssen nicht direkt (z.B. über RPC Kommunikation) bis an die CA gelangen, sondern werden über definierte Prüf- und Vermittlungsinstanzen geführt.

Die Architektur ist dabei bewusst firewall-freundlich ausgelegt. Outpost Services bauen Verbindungen grundsätzlich von innen nach aussen auf. Dadurch entstehen keine

unkontrollierten Rückkanäle oder schwer vermittelbaren Netzfreigaben. Das erleichtert Betrieb, Segmentierung und Freigabe durch Netzwerk- und Security-Teams erheblich.

Je nach Anwendungsfall können unterschiedliche Outpost-Typen eingesetzt und kombiniert werden, zum Beispiel:

- **CA Connector** für die kontrollierte Anbindung von Zertifizierungsstellen
- **LDAP Connector** für die Validierung gegen Verzeichnisdienste
- **Policy Enforcement** für Richtlinienprüfung und Freigabelogik und Signatur

Von jedem dieser Outpost-Typen können mehrere Instanzen betrieben werden - aus Gründen der Segmentierung, Hochverfügbarkeit, Lastverteilung oder zur Durchsetzung unterschiedlicher Sicherheitszonen. Das macht die Architektur besonders geeignet für komplexe Enterprise- und KRITIS-Umgebungen.

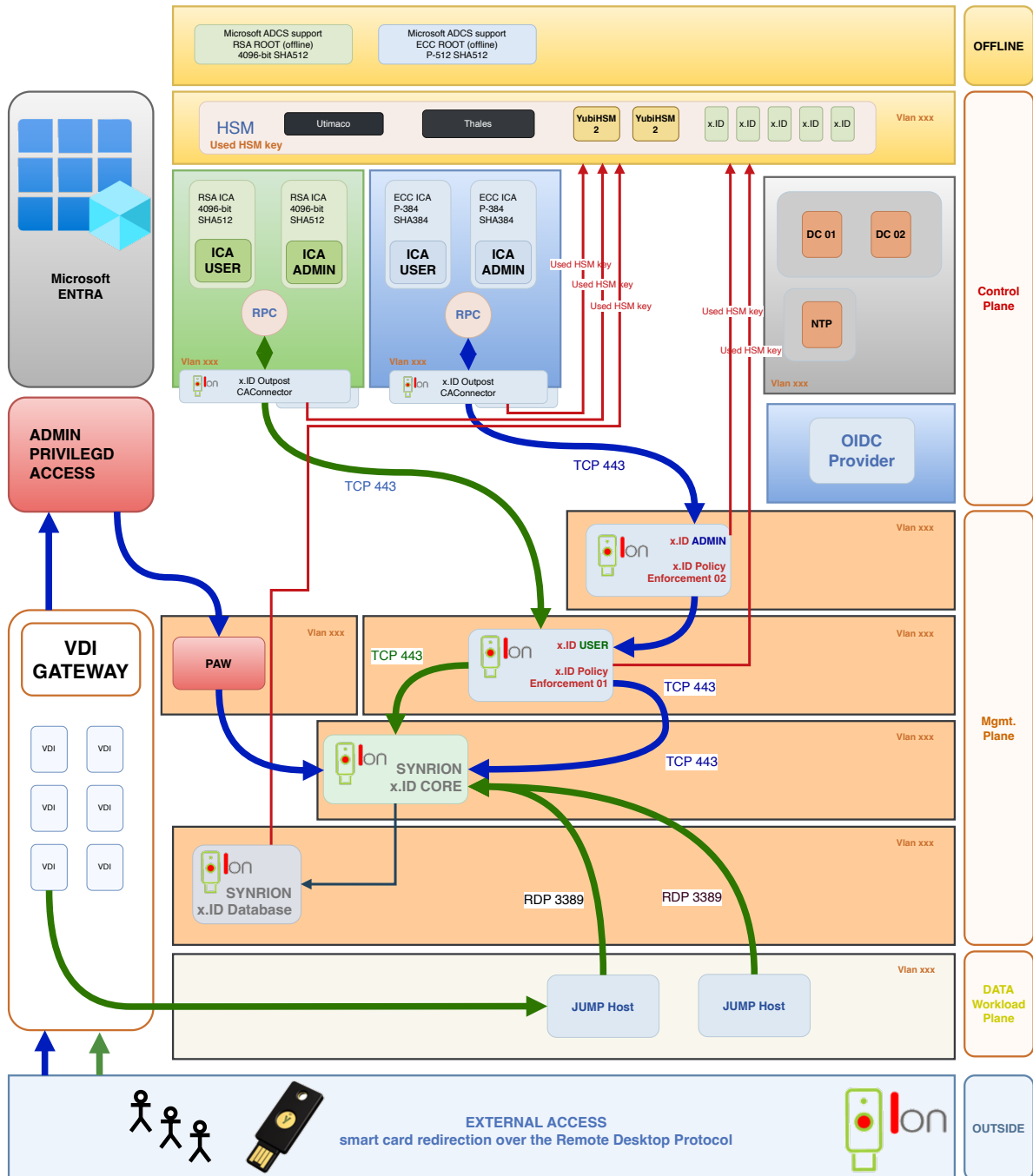
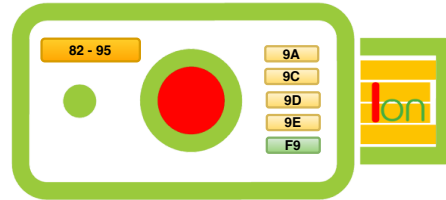
Ein weiterer Mehrwert liegt in der gezielten Trennung unterschiedlicher Identitäts- und Vertrauensmodelle. **SYNRION x.ID ist multi-CA-fähig** und ermöglicht den parallelen, kontrollierten Betrieb **mehrerer Zertifizierungsstellen innerhalb einer gemeinsamen Architektur**. Dadurch kann technisch erzwungen werden, dass administrative Identitäten ausschließlich aus einer definierten CA stammen, während Benutzerzertifikate über eine andere CA ausgestellt werden. Auf diese Weise lassen sich getrennte PKI-Welten, verschiedene Schutzbedarfe und unterschiedliche Vertrauenszonen sauber, nachvollziehbar und technisch belastbar abbilden.

Policy-Enforcement in SYNRION x.ID bedeutet damit mehr als nur Regelprüfung: Es ist die technische Durchsetzung von Sicherheitsvorgaben, die saubere Trennung von Rollen und Vertrauenszonen sowie die kontrollierte Vermittlung zwischen Endidentitäten, Verzeichnisdiensten und Certification Authorities.

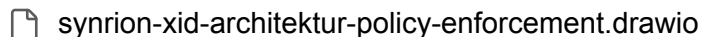
SYNRION x.ID - Referenzarchitektur für Policy-Enforcement, HSM und Multi-CA in segmentierten Infrastrukturen (Beispiel)

SYNRION

powered by **keyONE**



Direkt in draw.io bearbeiten:



HSM-Enforced

SYNRION x.ID ist konsequent auf Sicherheit ausgelegt. Deshalb empfehlen wir nachdruecklich, die privaten Schluesel aller sicherheitsrelevanten x.ID-Services nicht im Dateisystem und auch nicht ungeschuetzt im lokalen Windows-Zertifikatsstore abzulegen, sondern in Hardware-Sicherheitsmodulen zu erzeugen, zu speichern und zu verwenden.

Der Grund ist einfach: Es waere sicherheitlich kaum konsistent, wenn sich Endidentitaeten mit hardwaregebundenen Schlueseln auf YubiKeys oder anderen PIV-Token authentisieren, waehrend die serverseitigen Schluesel der dahinterliegenden Dienste nur softwarebasiert geschuetzt waeren. Wer hardwaregebundene Identitaeten ernst nimmt, sollte denselben Schutzanspruch auch fuer die Schluesel der ausstellenden, pruefenden und vermittelnden Dienste verfolgen.

SYNRION x.ID kann zwar auch mit dem Windows-Zertifikatsstore arbeiten. In klar abgegrenzten Sonderfaellen kann das ausreichend sein, zum Beispiel bei stark isolierten Appliances, die ausschliesslich einen einzelnen Dienst bereitstellen und betriebsseitig weitgehend abgeschottet sind. Fuer den regulaeren Einsatz in Enterprise-, Behoerden- und KRITIS-Umgebungen empfehlen wir jedoch dringend den Einsatz von HSMs.

Das gilt insbesondere deshalb, weil saemtliche Kernservices von SYNRION x.ID ausschliesslich zertifikatsbasiert arbeiten. Die Plattform nutzt Zertifikate nicht nur fuer die eigentliche Ausstellung und den Lifecycle von Identitaeten, sondern auch fuer die Absicherung der Servicekommunikation selbst. Dazu gehoeren insbesondere:

- **mTLS** zur gegenseitigen Authentisierung zwischen Diensten
- **Service Endpoint Protection** ueber zertifikatsbasierte Absicherung
- **App Data Protection** zur Verschluesselung sensibler Anwendungsdaten und abgelegter Credentials
- **Signatur- und Ausstellungsprozesse** mit kontrollierter kryptographischer Schluesselnutzung

Damit wird klar: x.ID schuetzt nicht nur Zertifikate fuer Benutzer, sondern verwendet Zertifikate selbst als tragendes Sicherheitselement der gesamten Plattform. Umso wichtiger ist es, dass die zugrunde liegenden privaten Schluesel nicht exportierbar, nicht unkontrolliert kopierbar und revisionsfaehig nutzbar sind.

Genau hier setzt HSM-Enforcement an. Private Keys koennen HSM-basiert erzeugt, geschuetzt und verwendet werden, ohne dass sie die Hardware im Klartext verlassen. Zugriffe und kryptographische Operationen werden kontrollierbar, nachvollziehbar und auditierbar. Das reduziert die Gefahr von Schluesselabfluss, Missbrauch und stillen Sicherheitsverlusten erheblich.

Dabei muss HSM-Einsatz nicht automatisch gross, komplex oder kostenintensiv sein. Neben klassischen Enterprise-HSM-Plattformen koennen auch wirtschaftliche und servicefreundliche Modelle sinnvoll sein. Fuer viele Einsatzszenarien empfehlen wir eine redundante Auslegung mit zwei YubiHSM-Modulen, kontrolliert in die Architektur eingebunden, beispielsweise zur Ausfallsicherheit und als Backup-Konzept. So laesst sich

ein deutlich hoeheres Schutzniveau erreichen, ohne die Einstiegshuerde grosser HSM-Infrastrukturen vorauszusetzen.

HSM-Enforced bedeutet in SYNRIION x.ID damit mehr als nur geschuetzte Schluesselspeicherung: Es ist die konsequente Fortsetzung einer hardwarebasierten Sicherheitsarchitektur - vom Endnutzer-Token bis zum serverseitigen Vertrauensanker.

PKI Lifecycle Enforced

SYNRION x.ID betrachtet Zertifikate nicht als einmalig ausgestellte Objekte, sondern als Teil eines vollstaendig kontrollierten Lifecycle. Dazu gehoeren Ausstellung, Verlaengerung, Erneuerung, Revocation, Rollover, Re-Issuance sowie die nachvollziehbare Bereinigung von Altzustaenden in den angeschlossenen Zielsystemen.

Gerade in sicherheitskritischen Umgebungen reicht es nicht aus, ein neues Zertifikat auszustellen oder ein altes zu widerrufen. Entscheidend ist, dass alle zugehoerigen Folgeaktionen kontrolliert, vollstaendig und nachvollziehbar ausgefuehrt werden. Dazu zaehlen insbesondere Publishing, Update und Cleanup in LDAP, Microsoft Entra und weiteren angebundenen Verzeichnis- oder Zielsystemen.

Ohne diese durchgaengige Lifecycle-Kontrolle entstehen in der Praxis genau die Probleme, die spaeter teuer werden: veraltete Zertifikatsreferenzen, unsaubere Zuordnungen, stehengebliebene Altzustaende, unvollstaendige Widerrufsfolgen oder Inkonsistenzen zwischen CA, Verzeichnisdienst und tatsaechlich genutzter Identitaet. Das ist nicht nur ein Betriebsrisiko, sondern oft auch ein Audit- und Sicherheitsproblem.

SYNRION x.ID fuehrt diese Schritte in einem nachvollziehbaren Gesamtprozess zusammen. Aenderungen werden kontrolliert ausgeloeset, protokolliert und revisionsfaehig dokumentiert. Dadurch wird aus einer Reihe einzelner PKI-Aktionen ein steuerbarer, belastbarer und auditierbarer Lifecycle-Prozess.

PKI-Lifecycle-Enforced bedeutet in SYNRIION x.ID damit mehr als Renewal oder Revocation allein: Es ist die konsequente technische Kontrolle ueber den gesamten Lebenszyklus einer digitalen Identitaet - von der Ausstellung bis zur sauberen Ruecknahme und Bereinigung aller abhaengigen Systeme.

AD- und Entra-Readiness als Teil der Erstintegration

Zertifikatsbasierte Authentifizierung ist nicht automatisch sicher, nur weil Zertifikate verwendet werden. Ihre Sicherheitswirkung entsteht erst dann, wenn auch die Zielumgebung - insbesondere Microsoft Entra ID, Active Directory, Domain Controller, Trust Stores, Certificate Mapping, Revocation-Pruefung, Smartcard-Policies und der eingesetzte Minidriver-Stack - korrekt vorbereitet, gehaertet und auf die Zielarchitektur abgestimmt sind.

Gerade hier unterschaelten viele Projekte den Aufwand. Starke zertifikatsbasierte Authentifizierung ist weder in Entra noch im lokalen Active Directory einfach "out of the box" aktiv. Sie setzt technische Vorarbeiten, gezielte Richtlinienanpassungen, belastbare Zertifikatszuordnung, saubere Trust- und Revocation-Pfade sowie kontrollierte Betriebs- und Logging-Konzepte voraus. Microsoft Entra Authentication Strengths definieren zwar, welche Authentisierungsmethoden fuer einen Zugriff zugelassen sind; die eigentliche Sicherheit der zertifikatsbasierten Methode haengt aber weiterhin an der korrekten PKI-,

AD- und Endpoint-Umsetzung. Gleiches gilt fuer Windows-Domaenencontroller: Mit dem Hardening gem. KB5014754 werden unsichere oder uneindeutige Zertifikatszuordnungen nicht mehr stillschweigend toleriert, sondern muessen sauber vorbereitet und nachvollziehbar betrieben werden.

[Microsoft Learn concept-authentication-strengths](#)

[Microsoft Learn certificate-based-authentication](#)

Deshalb ist die Erstintegration von SYNRIION x.ID bewusst mehr als eine reine Produktinstallation. Die initiale Inbetriebnahme erfolgt durch die Experten der keyONE GmbH und umfasst immer auch ein strukturiertes PKI-, AD- und Entra-Assessment. Ziel ist es, die Zielumgebung nicht nur technisch anzubinden, sondern sie so vorzubereiten, dass starke zertifikatsbasierte Authentifizierung tatsaechlich sicher, stabil und auditierbar betrieben werden kann.

Im Rahmen dieser Erstintegration werden unter anderem folgende Themen bewertet und abgestimmt:

- Readiness und Hardening von Active Directory und Domain Controllern
- Strong Certificate Binding und Certificate Mapping gem. KB5014754
- Certificate Path Validation, Trust Stores, AIA-, CRL- und OCSP-Verhalten
- Smartcard-, Kerberos-, Schannel- und CAPI2-Logging fuer Betrieb und Audit
- Smartcard-GPOs, Registry-Baselines und Rollenkonzepte fuer Clients, Server, RDS und Tier-0
- Minidriver- und Endpoint-Baselines fuer YubiKey/PIV, inklusive kontrollierter Rollout- und Evidenzmechanismen
- Abstimmung auf die konkrete Zielarchitektur, inklusive Segmentierung, Betriebsmodell und Schutzbedarf

Fuer diese Arbeiten hat keyONE eigene, projekterprobte Baseline- und Assessment-Dokumente entwickelt. Dazu gehoeren sowohl die AD-/Windows-Hardening- und Logging-Baseline fuer x.ID als auch die Rollout- und Registry-Baseline fuer den YubiKey Smart Card Minidriver. Diese Unterlagen bilden die Grundlage fuer eine strukturierte Erstintegration, fuer reproduzierbare Soll-/Ist-Abnahmen und fuer revisionsfaehige Evidenz im laufenden Betrieb.

[x.ID Security Baseline yk-minidriver-registry-settings][yk-minidriver-registry-settings_v1.0.pdf]

[x.ID Security Baseline sc-gpo-registry-settings][sc-gpo-registry-settings_v1.0.pdf]

Wichtig ist dabei: Diese Massnahmen sind sicherheitskritisch und immer individuell auf die Zielarchitektur abzustimmen. Pauschale Standardrezepte reichen hier nicht aus. Aenderungen an Domain Controllern, Smartcard-Logon, Certificate Mapping, Revocation-Verhalten oder Minidriver-Baselines sollten deshalb nur gemeinsam mit erfahrenen Spezialisten geplant und umgesetzt werden.

SYNRION x.ID liefert damit nicht nur Lifecycle-Management fuer Zertifikate und Hardware-Token, sondern schafft bereits in der Erstintegration die notwendige technische und organisatorische Grundlage dafuer, dass zertifikatsbasierte Authentifizierung im Zusammenspiel mit AD und Entra wirklich stark ist - und nicht nur auf dem Papier.

Security endet nicht am Produkt

SYNRION x.ID liefert nicht nur sicheres Zertifikats- und Token-Management, sondern auch die notwendige Sicherheitsintegration in die Zielumgebung. Denn starke zertifikatsbasierte Authentifizierung entsteht nicht allein durch das Zertifikat, sondern erst durch korrekt gehaertete und abgestimmte AD-, Entra-, ADCS- und Endpoint-Komponenten.

Deshalb ist die Security-Baseline-Integration Teil der Erstintegration. Gemeinsam mit dem AD-, Entra- und PKI-Assessment werden Trust- und Revocation-Pfade, Smartcard- und Zertifikatsrichtlinien, Logging, Domain-Controller-Konfigurationen sowie die relevanten Service-Endpunkte auf die Zielarchitektur abgestimmt. Grundlage dafuer sind eigens von keyONE entwickelte Baseline- und Assessment-Dokumente fuer Smartcard-/Minidriver-Rollout, Registry- und GPO-Settings sowie AD-/Windows-Readiness.

[x.ID Security Baseline yk-minidriver-registry-settings] [yk-minidriver-registry-settings_v1.0.pdf](#)

[x.ID Security Baseline sc-gpo-registry-settings] [sc-gpo-registry-settings_v1.0.pdf](#)

Ergaenzend unterstuetzt keyONE mit spezialisierten Modulen und Services, etwa fuer revisionsfaehige Audit-Trails und Benachrichtigungen bei kritischen Aktivitaeten in ADCS, Active Directory und Microsoft Entra. Microsoft stellt dafuer sowohl AD-CS-Auditing fuer sicherheitsrelevante CA-Vorgaenge als auch umfassende Entra-Audit-Logs fuer Tenant-Aenderungen bereit. Ebenso werden sichere Web-Service-Endpunkte fuer kontrollierte Renewal- und Zertifikatsprozesse unterstuetzt.

[Microsoft Learn audit-certification-services](#)

Kurz gesagt: keyONE liefert Security nicht nur im Produkt, sondern vollumfaenglich auch in und bei der Integration - damit zertifikatsbasierte Authentifizierung nicht nur vorhanden, sondern wirklich sicher ist.

Note

Das Zertifikat allein bringt keine Sicherheit.

Wirklich starke zertifikatsbasierte Authentifizierung entsteht erst dann, wenn Produkt, AD, Entra, ADCS, Service-Endpunkte, Audit-Trails und Sicherheitsbaselines sauber integriert, gehaertet und nachvollziehbar betrieben werden.

Was zertifikatsbasiertes Identity Management wirklich umfasst

Zertifikatsbasiertes Identity Management ist mehr als Token-Ausgabe oder Enrollment. In der Praxis umfasst es immer den kompletten Betriebs- und Sicherheitskontext einer digitalen Identitaet:

- Initialisierung und kontrollierte Personalisierung von YubiKey-, PIV- oder Smartcard-basierten Identitaeten
- sichere Schluesselerzeugung, Schluesselschutz und Token-Lifecycle
- CSR-, Enrollment-, Re-Enrollment- und Signaturprozesse
- Richtlinienpruefung vor Ausstellung bzw. Signatur
- Publishing, Cleanup und Aktualisierung in Active Directory, LDAP und Microsoft Entra
- PIN-/PUK-, Reset-, Replacement- und Wiederanlaufprozesse

- Revocation, Rollover, Re-Issuance und nachvollziehbare Ruecknahme von Identitaeten
- AD-, Entra-, Domain-Controller- und Endpoint-Readiness fuer starke zertifikatsbasierte Authentifizierung
- Audit-Trails, Evidence, Rollenmodell und revisionsfaehige Nachvollziehbarkeit
- optional agentless oder agent-based, kompakt oder hoch segmentiert, softwarebasiert oder HSM-gestuetzt

Kurz gesagt:

- Das Zertifikat allein schafft noch keine starke Identitaet.
- Erst der kontrollierte Gesamtprozess aus Token, PKI, Richtlinie, Verzeichnis, Zielsystem und Audit macht aus einer ausgestellten Identitaet eine sicher betreibbare Identitaet.

Offene Fragen, die vor einer Kaufentscheidung geklaert werden sollten

Diese Fragen sind bewusst enthalten, weil sie in der Praxis ueber Erfolg, Sicherheit und Betriebskosten entscheiden.

Architektur und Segmentierung

- Soll x.ID zentral, segmentiert oder hybrid betrieben werden?
- Reicht ein kompaktes Single-Server-Setup, oder werden getrennte Zonen und Outposts benoetigt?
- Welche Netzwege sind zwischen Core, Outposts, CAs, Verzeichnisdiensten und Endpunkten notwendig?
- Gibt es Multi-Domain-, Multi-Forest- oder Hybrid-Szenarien ohne direkte Trusts?
- Muessen On-Prem-, Hybrid- und Cloud-native Zielbilder gleichzeitig unterstuetzt werden?
- Gibt es HA-, Cluster- oder georedundante Anforderungen?

Token, Endpunkte und Deployment

- Welche Token-Typen und Betriebsmodelle sind im Scope (YubiKey PIV, Smartcard, andere PIV-Token)?
- Soll agentless, agent-based oder kombiniert gearbeitet werden?
- Welche Endpunkte muessen unterstuetzt werden (Clients, Admin-Workstations, RDS, VDIs, Jump Hosts)?
- Gibt es Anforderungen an Multi-Identity auf einem Token?
- Wie werden Replacement, Verlust, Reset und Break-Glass betriebsseitig behandelt?

PKI, CA und Protokolle

- Welche CAs muessen angebunden werden (ADCS, Public CA, interne SubCAs, mehrere PKIs)?

- Gibt es unterschiedliche CAs fuer unterschiedliche Rollen oder Identitaetstypen?
- Welche Enrollment-Wege sind relevant?
- Muessen bestehende Templates, Policies, Kryptovorgaben oder Ausstellungsprozesse angepasst werden?
- Gibt es Parallelbetrieb oder geplante CA-Wechsel?

HSM, Schluesselschutz und Schutzbedarf

- Welche x.ID-Services muessen zwingend HSM-gestuetzt arbeiten?
- Reicht in Teilbereichen Software Key Storage, oder ist durchgaengig HSM-backed erforderlich?
- Welche HSMs oder HSM-nahen Modelle kommen in Frage (z. B. YubiHSM, Thales, Utimaco)?
- Wie werden serverseitige Private Keys erzeugt, gespeichert und genutzt (KMS)?
- Welche Rollen, Systeme oder Prozesse haben Zugriff auf kryptographische Operationen?

AD, Entra und Domain Controller

- Ist die Zielumgebung fuer starke zertifikatsbasierte Authentifizierung bereits vorbereitet?
- Sind Strong Certificate Binding und Certificate Mapping gem. KB5014754 adressiert?
- Sind Trust Stores, Revocation-Pfade, AIA-, CRL- und OCSP-Verhalten sauber definiert?
- Welche Smartcard-, Kerberos-, Schannel- und CAPI2-Policies sind notwendig?
- Wie werden Entra Authentication Strengths, Conditional Access und hybride Trust-Modelle eingebunden?

Betrieb, Rollen, Rechte und Prozesse

- Welche Rollen gibt es (Owner, Operator, Auditor, Helpdesk, Security)?
- Wie werden Vier-Augen-Prinzip, Freigaben und Aenderungsprozesse technisch umgesetzt?
- Welche Rechte benoetigen x.ID, Outposts und Operatoren?
- Wie werden Lifecycle-Aenderungen freigegeben und dokumentiert?
- Wie sehen Prozesse fuer Wiederanlauf, Tokenverlust, Revocation und Rollentausch aus?

Evidence, Audit und Compliance

- Welche Nachweise werden im Audit konkret benoetigt?
- Wie schnell muessen Reports und Exporte bereitstehen?
- Welche Events muessen revisionsfaehig protokolliert werden?
- Welche KPIs sind fuer Management, Betrieb und Revision relevant?
- Wo liegen heute die groessten Risiken: Mapping, Revocation, Tokenverlust, manuelle Prozesse, fehlende Baselines?

Abschnitt 1: Quick Pass (10 Fragen)

Ziel: In 5 Minuten klaeren, ob SYNRIION x.ID in Ihrer Umgebung sofort Mehrwert liefert und welche Grundvoraussetzungen bzw. offenen Punkte vor einem Pilot zu pruefen sind.

Antworten: Ja / Teilweise / Nein

Notizen: 1 Satz pro Zeile (optional)

#	Frage (kauf- und betriebsrelevant)	Ja	Teilweise	Nein	Notizen
1	Sind Ihre zertifikatsbasierten Identitaeten heute ueber den gesamten Lifecycle hinweg nachvollziehbar und kontrolliert?				
2	Gibt es heute bereits hardwaregebundene Identitaeten fuer kritische oder privilegierte Rollen?				
3	Sind AD, Entra, Domain Controller und Endpoint-Baselines fuer starke zertifikatsbasierte Authentifizierung technisch vorbereitet?				
4	Koennen Sie Revocation, Replacement, Re-Issuance und Cleanup heute kontrolliert und revisionsfaehig durchfuehren?				
5	Gibt es mehrere Rollen oder Identitaetskontexte pro Person (z. B. User, Admin, Betrieb, Break-Glass), die sauber getrennt werden muessen?				
6	Sind HSM-gestuetzte Service-Schluesel heute bereits umgesetzt oder zumindest geplant?				
7	Gibt es segmentierte, hybride oder Multi-Forest-/Multi-Domain-Szenarien, die eine kontrollierte Architektur verlangen?				
8	Muessen Sie im Audit belastbare Nachweise zu Identitaeten, Rollen, Lifecycle-Ereignissen und Sicherheitsrichtlinien liefern?				
9	Verursachen manuelle Token-, PIN-/PUK-, Enrollment- oder Replacement-Prozesse heute Aufwand, Fehler oder Sicherheitsrisiken?				

#	Frage (kauf- und betriebsrelevant)	Ja	Teilweise	Nein	Notizen
10	Können Sie für einen Pilot 20-50 Identitäten, 1-2 Rollenkonzepte und die vorgesehenen Einsatzkontexte klar benennen (z. B. User-Logon, Admin-Logon, AD, Entra, Break-Glass)?				

Quick Interpretation

- Wenn bei #1, #3, #4 oder #8 mindestens ein "Nein" steht, besteht typischerweise unmittelbarer Nutzen durch x.ID.
- Wenn #5, #6 oder #7 "Ja/Teilweise" sind, müssen Architektur, Rollenmodell und Schlüsselschutz früh geklärt werden.
- Wenn #10 "Nein" ist, fehlt meist nicht Technik, sondern ein belastbarer Startscope für einen Pilot.

Abschnitt 2: x.ID Core Use-Cases (Was wird automatisiert und kontrolliert?)

Ziel: Klären, welche Identity-, Token- und Lifecycle-Use-Cases x.ID in Ihrer Umgebung abdecken soll und wo heute manueller Aufwand, Sicherheitsrisiko oder fehlende Nachvollziehbarkeit entsteht.

Antworten: Ja / Teilweise / Nein

Notizen: kurz und konkret (Rolle, Identität, Zielsystem nennen)

#	Use-Case / Aussage	Ja	Teilweise	Nein	Notizen
1	YubiKey-/PIV-Token kontrolliert initialisieren, personalisieren und ausgeben				
2	Enrollment und Re-Enrollment für Benutzer- und Rollenidentitäten standardisiert durchführen				
3	CSR-Prüfung und Policy-Enforcement unmittelbar vor Ausstellung bzw. Signatur technisch durchsetzen				
4	Mehrere Identitäten bzw. Rollenkontexte auf einem Hardware-Token kontrolliert abbilden				

#	Use-Case / Aussage	Ja	Teilweise	Nein	Notizen
5	PIN-/PUK-, Reset-, Replacement- und Wiederanlaufprozesse reproduzierbar und nachvollziehbar betreiben				
6	Revocation, Re-Issuance, Rollover und Cleanup in AD, LDAP und Entra kontrolliert durchfuehren				
7	Strong Authentication in AD, Entra oder hybriden Umgebungen technisch belastbar unterstuetzen				
8	Agentless und/oder agent-based je nach Schutzbedarf einsetzen				
9	Mehrere CAs bzw. getrennte Vertrauensmodelle parallel in einer Architektur betreiben				
10	Serverseitige Service-Schluesel HSM-gestuetzt erzeugen, verwenden und auditieren				
11	Readiness- und Hardening-Massnahmen fuer AD, Entra, Domain Controller und Endpunkte strukturiert einfuehren				
12	Evidence, Audit-Trails und nachvollziehbare Lifecycle-Nachweise zentral erzeugen				

Kurzbewertung (Abschnitt 2)

- Wenn #1, #2, #5 oder #6 "Teilweise/Nein" sind, ist der operative Nutzen oft sofort sichtbar.
- Wenn #3, #9 oder #10 "Ja/Teilweise" sind, sollten Policy, Multi-CA und HSM frueh in den Pilot aufgenommen werden.
- Wenn #11 oder #12 "Nein" sind, fehlt oft die Grundlage fuer belastbare, auditierbare starke Authentifizierung.

Abschnitt 3: Voraussetzungen und Architekturfragen (Was brauchen wir dafuer?)

Ziel: Klare technische und organisatorische Voraussetzungen fuer einen sicheren Betrieb von x.ID.

Antworten: Ja / Teilweise / Nein

Notizen: konkrete Zonen, Accounts, Rollen, Zielsysteme

#	Voraussetzung / Frage	Ja	Teilweise	Nein	Notizen
1	Gibt es ein klares Zielbild fuer Deployment, Segmentierung und Betriebsmodell?				
2	Sind benoetigte Netzwege zwischen x.ID, Outposts, CAs, Verzeichnisdiensten und Endpunkten moeglich?				
3	Sind Service-Identitaeten, gMSAs und Rollen fuer x.ID sauber definierbar?				
4	Sind AD-, Entra- und Domain-Controller-Baselines grundsatzlich adressierbar?				
5	Sind Smartcard-/Minidriver-, Policy- und Endpoint-Baselines organisatorisch und technisch einfuehrbar?				
6	Koennen Lifecycle-Aenderungen und sicherheitsrelevante Aktionen in ein Freigabe- bzw. Betriebsmodell eingebettet werden?				
7	Ist geklaert, ob HSM-Pflicht, HSM-Empfehlung oder Software Key Storage in Teilbereichen gilt?				
8	Existiert ein Rollenmodell fuer Owner, Operator, Helpdesk, Auditor und Security?				
9	Sind Logging, SIEM, Alarmierung und revisionsfaehige Ablage grundsatzlich vorgesehen?				
10	Gibt es ein belastbares Pilotzielbild inklusive Zielsystemen, Rollen und Verantwortlichen?				

Kurzbewertung (Abschnitt 3)

- Wenn #2, #3 oder #4 "Nein" sind, muss zuerst die Betriebsfaehigkeit geklaert werden.
- Wenn #5, #6 oder #9 "Nein" sind, ist x.ID zwar moeglich, aber noch nicht auditfest und betrieblich stabil.
- Wenn #7 unklar ist, sollte der Schluesselschutz frueh als Architekturentscheidung behandelt werden.

Abschnitt 4: Sichtbarkeit, Evidence, Audit (Was bekommen wir heraus?)

Ziel: Klaeren, ob x.ID die benoetigten Nachweise, Steuerungsdaten und Auditinformationen liefert und wie schnell diese bereitstehen muessen.

Antworten: Ja / Teilweise / Nein

Notizen: Audit-Anforderungen, Report-Formate, SLA

#	Evidence / Frage	Ja	Teilweise	Nein	Notizen
1	Gibt es heute eine zentrale Sicht auf ausgegebene Token, Identitaeten, Rollen und Lifecycle-Status?				
2	Koennen Sie nachvollziehen, wer wann welche Identitaet erhalten, geaendert, ersetzt oder widerrufen hat?				
3	Gibt es KPIs fuer Rollout-Status, Abdeckung, Lifecycle-Ereignisse und Sicherheitskonformitaet?				
4	Koennen Reports und Exporte fuer Audit, Revision oder Security innerhalb von Stunden bereitgestellt werden?				
5	Werden Revocation-, Cleanup-, Mapping- und Baseline-Abweichungen sichtbar und nachvollziehbar?				
6	Gibt es nachvollziehbare Audit-Trails fuer Policy-Entscheidungen, Rollen, Token und Lifecycle-Aenderungen?				
7	Sind sicherheitsrelevante Ereignisse aus AD, Entra, ADCS und x.ID technisch korrelierbar?				
8	Gibt es eine klare Zuordnung von Identitaeten, Rollen, Verantwortlichen und Betriebsprozessen?				

Kurzbewertung (Abschnitt 4)

- Wenn #2 oder #4 "Nein" ist, ist Audit-Readiness typischerweise teuer und langsam.
- Wenn #5, #6 oder #7 "Teilweise/Nein" sind, fehlt oft die belastbare Grundlage fuer starke und nachweisbare zertifikatsbasierte Authentifizierung.

Abschnitt 5: Pilot Worksheet (Scope, Erfolgskriterien, Deliverables)

Ziel: In 10 Minuten einen Pilot definieren, der belastbare Ergebnisse fuer x.ID liefert.

5.1 Pilot Scope

Ziel:

- 10-30 Identitaeten
- 1-2 Rollenmodelle
- 1-2 Zielsysteme oder Zielumgebungen
- optional 1 HSM- und 1 Multi-Identity-Use-Case

Feld	Eintrag
Pilot Owner (Business)	
Pilot Owner (Technical)	
Identitaeten (Anzahl + Typen)	
Rollenmodelle im Scope	
Token / Hardware im Scope	
AD / Entra / Zielumgebungen	
CA / PKI im Scope	
HSM / Schluesselschutz im Scope	

5.2 Erfolgskriterien (Messbar)

KPI / Kriterium	Zielwert	Messmethode
Rollout-/Lifecycle-Abdeckung		Dashboard/Report
Evidence Export Time		Zeitmessung
Zeit fuer Enrollment / Replacement		Vorher-Nachher-Vergleich
Revocation / Cleanup Vollstaendigkeit		Events/Report
Baseline- und Readiness-Status		Assessment / Report

5.3 Deliverables (Was liefern wir im Pilot?)

- Pilot-Inventory fuer Identitaeten, Rollen, Token und Zielsysteme
- Readiness- und Gap-Sicht fuer AD, Entra, Domain Controller und Endpunkte
- Lifecycle-Nachweise fuer Enrollment, Replacement, Revocation oder Re-Issuance
- Evidence-Paket fuer Audit, Security und Revision
- Empfehlung fuer Rollout, Rollenmodell, Segmentierung und Betriebsuebergang

Abschnitt 6: Auswertung (Scoring und Interpretation)

Ziel: Aus Ja / Teilweise / Nein eine klare Aussage ableiten, ohne lange Diskussion.

Scoring:

- Ja = 2
- Teilweise = 1
- Nein = 0

Interpretation:

- 0-20 Punkte: Hoher Handlungsdruck
- 21-35 Punkte: Mittel
- 36-50 Punkte: Gut
- 51+ Punkte: Sehr gut

Gate-Fragen (Quick Pass):

- #1, #3, #4 und #8 sind Gate-Fragen. Ein "Nein" dort ist fast immer ein Pilot-Kandidat.

Bereich	Punkte	Kommentar
Abschnitt 1: Quick Pass (10 Fragen)		
Abschnitt 2: Core Use-Cases (12 Aussagen)		
Abschnitt 3: Voraussetzungen (10 Fragen)		
Abschnitt 4: Evidence (8 Fragen)		
Gesamt		

Abschnitt 7: Minimal Evidence Set (was im Audit wirklich zaehlt)

Ziel: Klar machen, was auditfaehig im Umfeld von x.ID in der Praxis bedeutet.

Minimal Evidence:

- zentrale Sicht auf Identitaeten, Rollen, Token und Lifecycle-Status
- Nachweis von Enrollment-, Replacement-, Revocation- und Re-Issuance-Ereignissen
- Audit-Trail fuer Policy-Entscheidungen, Rollenfreigaben und kritische Aktionen
- Cleanup-/Publishing-Nachweise in AD, LDAP und Entra
- Baseline- und Readiness-Nachweise fuer AD, Domain Controller, Endpunkte und Minidriver
- Report zu sicherheitsrelevanten Abweichungen und offenen Risiken

Optional (wenn benoetigt):

- ADCS-, AD- und Entra-Korrelation fuer sicherheitsrelevante Events
- Export als CSV/Report, bei Bedarf PDF

Abschnitt 8: Pilot Output Paket (was ein Pilot liefern muss)

Ziel: Der Pilot muss messbar sein und ein Ergebnis liefern, das intern weitergegeben und entschieden werden kann.

Pilot Outputs (Minimum):

1. Inventory Snapshot

- Liste der Pilot-Identitaeten
- Rollen, Token und Zielsysteme im Scope
- Lifecycle-Status je Identitaet

2. Risiken und Abweichungen

- Top-Risiken in AD-/Entra-Readiness
- Baseline- und Mapping-Abweichungen
- offene Lifecycle- oder Rollenprobleme
- HSM-/Schluesselschutz-Findings

3. Evidence Paket

- Export relevanter Lifecycle-Events
- Nachweise fuer mindestens einen kontrollierten Enrollment-/Replacement-/Revocation-Prozess
- dokumentierte Policy- und Readiness-Ergebnisse

4. Betriebsempfehlung

- Rollen und Rechte
- Segmentierung und Zielarchitektur
- Zielbild fuer Rollout und Betriebsuebergang
- naechste Ausbaustufe fuer 100 / 500 / 5000 Identitaeten

Erfolg = wenn 3 Dinge nachweislich besser sind:

- Evidence Export Time sinkt
- Lifecycle-Prozesse laufen kontrollierter und nachvollziehbarer
- Baseline- und Readiness-Luecken werden sichtbar und gezielt schliessbar

Kontakt

- Christian Schorr
- Mail: c.schorr@keyONE.one
- Phone: +49 174 3443815
- Produktseite: <https://keyone.de/synrion>