BLACKFORT TECHNOLOGY

Blackfort
Certificate Intelligence

Volle Transparenz über Ihre Zertifikatslage – rein lesend, nicht invasiv, DORA-tauglich

Juni 2026 · Blackfort Technology · blackfort-tec.de

MANAGEMENT SUMMARY

Die Kernbotschaft

Warum dieses Inventar jetzt relevant ist

- Zertifikate sind ICT-Assets – DORA verlangt deren Identifikation und Klassifikation.
- Die meisten Organisationen kennen ihre Zertifikatslage nicht vollständig.
- Abgelaufene, verwaiste oder schwache Zertifikate verursachen Ausfälle und Audit-Findings.
- Unsere Antwort: ein zentrales, rein lesendes Inventar ohne Eingriff in den Betrieb.
- Aktuell in Pilotphase – 60 Tage kostenlos und mit vollem Funktionsumfang testbar.

> *Sie können nur schützen, was Sie kennen – wir machen Ihre Zertifikatslage sichtbar, ohne sie anzufassen.*

WARUM JETZT

DORA macht Krypto-Transparenz zur Pflicht

Verordnung (EU) 2022/2554 – anwendbar seit 17.01.2025

03

DORA KONKRET

Zertifikate sind ICT-Assets – das Mapping

Anforderung trifft Zertifikatslage

Art. 8 – Asset-Identifikation

- Identifikation und Klassifikation aller ICT-Assets
- Zuordnung zu kritischen und wichtigen Funktionen
- Inventar liefert genau diese Bestandsaufnahme für Zertifikate

Art. 9 – Schutz und Prävention

- RTS verlangen Richtlinien zu Kryptografie und Verschlüsselung
- Schlüssel- und Zertifikats-Lebenszyklus muss beherrscht sein
- Inventar liefert Nachweise über Algorithmen, Laufzeiten, Hygiene

Art. 28–30 – Drittparteienrisiko

- CA- und Cloud-KMS-Abhängigkeiten sichtbar machen
- Konzentrationsrisiko bei Ausstellern erkennen
- Belastbare Daten für das Informationsregister

Das Inventar adressiert Art. 8, 9 und 28–30 – es liefert Nachweise, es garantiert keine Konformität.

DER STATUS QUO

Der blinde Fleck in fast jeder Organisation

05

Niemand kennt alle Zertifikate – bis eines ausfällt

DAS PROBLEM

Was unsichtbare Zertifikate kosten

Von der Störung bis zum Audit-Finding

- Abgelaufene Zertifikate auf kritischen Funktionen verursachen ungeplante Ausfälle.
- Verwaiste Zertifikate ohne Owner – niemand fühlt sich zuständig.
- Schwache Kryptografie (RSA<2048, SHA-1) bleibt unbemerkt im Bestand.
- Widerrufene, aber weiter aktive Zertifikate untergraben das Vertrauen.
- Tabellen und Tickets veralten sofort – keine belastbare Datengrundlage fürs Audit.

> *Ein abgelaufenes oder widerrufenes Zertifikat auf einer kritischen Funktion ist potenziell ein IKT-Vorfall nach Art. 17.*

UNSER ANSATZ

Die Lösung: ein zentrales, rein lesendes Inventar

Transparenz ohne Eingriff in Produktionssysteme

07

ÜBERBLICK

Inventar, kein Key-Store

Die Positionierung auf einen Blick

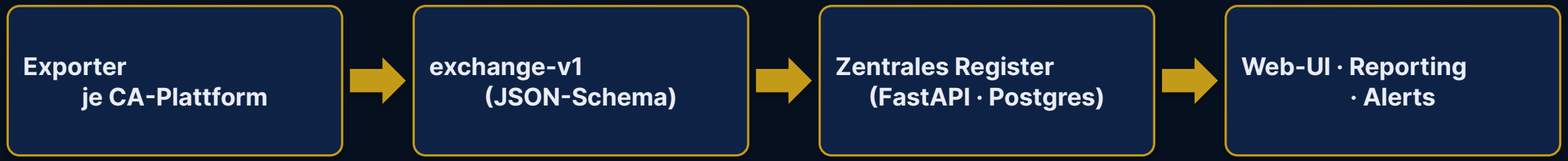
- Rein lesend und nicht invasiv – kein Eingriff in laufende Systeme.
- Niemals private Schlüssel – nur öffentliche Zertifikatsteile und Metadaten.
- Ein zentrales Web-Register als Single Source of Truth.
- Manuell gepflegte Governance-Felder überleben jeden Re-Import (Upsert, nie Replace).
- Kein OpenBao beim Kunden nötig – schlanke Inbetriebnahme.

> *Wir inventarisieren Zertifikate – wir verwalten keine Schlüssel. Das ist bewusst die sichere Grenze.*

ARCHITEKTUR

Exporter → exchange-v1 → Register

Logik im Zentrum, nicht an der Quelle



- Dumme, minimale Exporter pro CA-Plattform – rein lesend, einzeln auditierbar.
- Stabiles, versioniertes Austauschformat (JSON-Schema, exchange-v1).
- Gesamte Logik lebt im zentralen Register, nicht in den Exportern.
- Register: FastAPI + Postgres + HTMX + Tabulator – Air-Gap-tauglich, kein CDN.
- Primärschlüssel = SHA-256-Fingerprint; Import = Upsert/Merge, niemals Replace.
- Auslieferung als Container (Docker Compose, docker save) und VM-Appliance (OVA).

Minimale, auditierbare Exporter an der Quelle – die Intelligenz lebt zentral und versioniert.

DISCOVERY-BREITE

Vielfältige Quellen, ein Inventar

Am PKI-Testlab validiert

5 CA-Connectoren

- Microsoft ADCS
- EJBCA
- HashiCorp Vault PKI
- smallstep step-ca
- Azure Key Vault

Aktive Erkennung

- Eigener schlanker TLS-Scanner (Go, statisch, rein lesend)
- Nur Zertifikatsabruf je host:port, kein Cipher-Probing
- Portrange und Concurrency konfigurierbar

Extern und Offline

- CT-Log-Monitoring (certspotter) für öffentlich vertraute Zertifikate
- Klar getrennt als extern dargestellt (origin_class)
- Air-Gap-Datei-Import für isolierte Segmente

Managed, extern oder air-gapped – jede Quelle wird sauber als origin_class managed/external/mixed gekennzeichnet.

DAS REGISTER

Drei Feldklassen – sauber getrennt

Technik immutable, Governance editierbar, Provenienz nachvollziehbar

Technisch (read-only)

- Fingerprint, Seriennummer, Subject/CN, SAN, Issuer
- Laufzeit, Public-Key-Algo/Länge, Signaturalgo, SPKI-Hash
- KeyUsage/EKU, BasicConstraints, Typ (Leaf/Intermediate/Root)
- AKI/SKI für Kettenverknüpfung, CDP-/AIA-/OCSP-URLs

Governance (editierbar)

- Unterstützt kritische / wichtige Funktion (Ja/Nein)
- Aktiv in Nutzung, verantwortlicher Kontakt
- Funktion/Anwendung/Prozess als Freitext
- Verwaist (manuell, scan-informiert), freie Custom-Spalten

Provenienz/Beobachtung

- Zuletzt/erstmals importiert (aus CA-Export/Datei)
- Getrennt von zuletzt/erstmals gesehen (aus Netz-Scan)
- Quell-Connector und Beobachtungsorte
- Vollständige Herkunftsnachvollziehbarkeit

Technische Wahrheit bleibt unveränderbar – Ihre Governance-Arbeit bleibt geschützt und auditierbar.

COMPLIANCE-INTELLIGENZ

Abgeleitete Spalten, die Risiken sichtbar machen

Aus Rohdaten werden Entscheidungen

- Tage-bis-Ablauf mit Eskalation nach Service-Klasse (Schwellen z. B. 30/90 Tage).
- Renewal-Methode erkannt: ACME, SCEP, EST oder manuell.
- Schwach-Krypto-Flags: RSA<2048, SHA-1-Signatur, self-signed auf kritischer Funktion.
- Key-Reuse über geteilten SPKI-Hash, Wildcard-Erkennung.
- Waisen: kein Owner / ausgestellt-aber-nie-gesehen / gesehen-aber-nicht-im-Export.
- Sperrstatus rein lesend über CRL (CDP) und OCSP (AIA) – Spalte widerrufen-aber-aktiv.
- Ketten- und Trust-Auflösung über AKI/SKI; append-only Audit-Trail der Governance-Felder.

> *Das Register denkt mit: es flaggt schwache Krypto, Waisen und widerrufene-aber-aktive Zertifikate automatisch.*

NUTZEN PRO ROLLE

Wert je Zielgruppe

Vom IT-Admin bis zum Vorstand – jede Rolle profitiert anders

WERTMATRIX

Eine Plattform – sechs Perspektiven

Rolle, DORA-Bezug, Schmerzpunkt, Nutzen

Rolle	DORA	Schmerzpunkt	Nutzen
IT-Admin	**Art. 8/9**	Überraschende Abläufe, manuelle Listen veralten	Früh-Warnung bei Ablauf, alle Zertifikate an einem Ort
Leitung IT	**Art. 8/9**	Kein Gesamtbild, Ausfälle ohne Vorwarnung	Belastbare Bestandszahlen, planbare Erneuerungen
CISO	**Art. 9/17**	Schwache Krypto und Waisen unsichtbar, Vorfallrisiko	Krypto-Hygiene messbar, Risiken priorisierbar
IKT/Drittparteien	**Art. 28–30**	CA-Abhängigkeiten und Konzentrationsrisiko unklar	Aussteller-Transparenz, Daten für Informationsregister
Risikokontrollfunktion	**Art. 5/9**	Keine unabhängige Datengrundlage für 2nd Line	Prüfbare Kennzahlen, Audit-Trail, DORA-Views
Vorstand	**Art. 5**	Letztverantwortung ohne belastbaren Überblick	Verdichteter Status als Nachweis der Steuerung

Ein Datenbestand, sechs Sichten – jede Rolle bekommt genau die Filter, die sie braucht.

CISO UND RISIKO VERTIEFT

Krypto-Hygiene, Nachweis und Drittparteienrisiko

Was die zweite und dritte Verteidigungslinie gewinnt

Krypto-Hygiene und Vorfälle

- Schwache Algorithmen und self-signed auf kritischen Funktionen sichtbar
- Widerrufen-aber-aktiv als potenzieller IKT-Vorfall (Art. 17)
- Key-Reuse über geteilten SPKI erkannt

Nachweis und kritische Funktionen

- Zuordnung kritische/wichtige Funktion direkt am Asset
- Append-only Audit-Trail als prüfbarer Nachweis
- DORA-Views als wiederholbare Berichtsgrundlage

Konzentrations- und Drittparteienrisiko

- Verteilung über Aussteller und CAs auswertbar
- Cloud-KMS- und CA-Abhängigkeiten transparent (Art. 28–30)
- Datenbasis für das Informationsregister

Die Risikofunktion bekommt eine unabhängige, prüfbare Datengrundlage – nicht die Eigenauskunft des Betriebs.

SICHERHEIT UND VERTRAUEN

Warum dieses Inventar sicher betreibbar ist

Vertrauen by Design

- Rein lesend und nicht invasiv – kein Eingriff in Produktionssysteme.
- Niemals private Schlüssel – ausschließlich öffentliche Zertifikatsteile und Metadaten.
- Auslieferung als Container (docker save) oder VM-Appliance (OVA).
- Air-Gap-tauglich: Datei-Export/-Import für isolierte Segmente, kein externer Cron.
- Agenten zentral verwaltbar: Token erzeugen, sperren, rotieren, last_seen.
- Web-Login mit RBAC (admin schreibt, viewer liest) und append-only Audit-Trail.

> *Kein Private Key, kein Cipher-Probing, kein CDN – das System ist bewusst auf minimale Angriffsfläche ausgelegt.*

Aus Daten werden Berichte und Benachrichtigungen

Im Alltag und im Audit nutzbar

- DORA-Auswertungs-Views mit Schnellfiltern für wiederkehrende Fragen.
- Export als XLSX und CSV für Audit, Reporting und Weiterverarbeitung.
- Teams-Benachrichtigungen pro Kunde konfigurierbar: Schwellen und Toggles.
- Toggles für schwache Krypto, Waisen und self-signed-kritisch.
- Tages-Digest als Adaptive Card – ohne externen Cron.
- Zertifikate archivieren: Soft-Archiv, reversibel und auditiert statt hartem Löschen.

> *Compliance-gerecht statt destruktiv: archiviert wird reversibel und auditiert, nie hart gelöscht.*

ROADMAP

Was als Nächstes kommt

Geplante Ausbaustufen

Weitere Quellen

- DigiCert-Integration
- AWS Certificate Manager
- Google Cloud Certificate Manager
- Kubernetes-Secret-Discovery

Workflow und Monitoring

- Jira-Integration
- Erweitertes CT-Log-Monitoring
- Tiefere Einbindung in bestehende Prozesse

Spätere Ausbaustufe

- mTLS-Hardened-Mode
- Weitere Vertiefung der Drittparteien-Sicht

Die Plattform wächst entlang der realen Quellen unserer Kunden – Cloud, CI/CD und Kubernetes.

EINSTIEG

Einfach starten – ohne Risiko

Pilotphase, Self-Install, faire Skalierung

- 60 Tage kostenlos testen – mit vollem Funktionsumfang.
- Self-Install: Sie installieren Container oder OVA selbst, in Ihrer Umgebung.
- Kein OpenBao und keine externe Cloud-Abhängigkeit nötig.
- Skalierung ausschließlich nach Anzahl der Zertifikate – transparent und planbar.
- Optionaler Installationssupport nach Aufwand, wenn gewünscht.

> *Voller Funktionsumfang, 60 Tage kostenlos, in Ihrer eigenen Umgebung – ohne Daten aus der Hand zu geben.*

NÄCHSTER SCHRITT

Machen Sie Ihre Zertifikatslage sichtbar

Starten Sie Ihren 60-Tage-Pilot mit Blackfort Certificate Intelligence

- Gemeinsam einen Pilot in Ihrer Umgebung aufsetzen.
- Erste DORA-Auswertung Ihrer realen Zertifikatslage.
- Blackfort Technology · info@blackfort-tec.de

> *Reden wir über Ihren blinden Fleck – bevor das nächste Zertifikat ihn für Sie sichtbar macht.*