Schlüsselkataster – Aufbau und Pflege

Zweck

Ein Schlüsselkataster ist ein Verzeichnis kryptografischer Schlüssel, Zertifikate und zugehöriger Verwaltungsinformationen. Es unterstützt Übersicht, Schlüsselwechsel, Sicherheitsprüfungen und Wiederherstellung. Ein Kataster ist **kein Schlüsselspeicher**.

Empfohlene Felder

Feld	Beschreibung
Kennung	Eindeutige interne Schlüssel-ID
Verfahren	Beispielsweise OpenSSH, OpenPGP, WireGuard, TLS, Borg oder LUKS
Typ	Schlüsselpaar, symmetrischer Schlüssel, Zertifikat oder Recovery-Information
Zweck	Authentifizierung, Verschlüsselung, Signatur oder Schlüsselvereinbarung
Verantwortlichkeit	Zuständige Rolle oder Organisationseinheit
Einsatzort	System oder Dienst, möglichst ohne sensible Zugangsdaten
Öffentliche Kennung	Fingerprint oder Zertifikatsseriennummer, falls sinnvoll
Erstellung	Erstellungsdatum
Ablauf / Prüfung	Gültigkeit und nächster Prüftermin
Status	Geplant, aktiv, abgelöst, widerrufen, archiviert
Sicherung	Verweis auf ein **geschütztes** Recovery-Verfahren, ohne Geheimnisse offenzulegen
Wechselhistorie	Referenz auf Vorgänger/Nachfolger und Änderungsdatum

Was nicht hineingehört

- Private Schlüssel und symmetrische Schlüssel
- Passphrasen, Wiederherstellungscodes oder geheime Token
- Unverschlüsselte Keyfiles oder Repository-Recovery-Dateien
- Zugangsdaten zu Backup- und Administrationssystemen

Beispiel eines abstrakten Eintrags

Feld	Beispiel
Kennung	SSH-SYSTEM-A-001
Verfahren	OpenSSH / Ed25519
Zweck	Administrativer Zugang
Einsatzort	Beispielsystem A
Fingerprint	In geschützter Bestandsdokumentation hinterlegt
Status	Aktiv

Feld	Beispiel
Nächste Prüfung	Jährlich

Unterschiedliche Verfahren

Für TLS-Zertifikate sind Domainnamen, Aussteller und Ablaufdaten wichtig. Bei Borg sind Repository, Verschlüsselungsmodus und Recovery-Verfahren entscheidend. Bei OpenPGP können Hauptschlüssel, Unterschlüssel und Widerruf getrennt dokumentiert werden. Ein einziges starres Schema ist daher oft weniger sinnvoll als gemeinsame Pflichtfelder und verfahrensspezifische Ergänzungen.

Betriebsprozess

1. Schlüssel vor Ausgabe im Kataster erfassen.
1. Verantwortlichkeit und Zweck dokumentieren.
1. Ausgabe und Berechtigungen prüfen.
1. Sicherung und Wiederherstellung nachweisen.
1. Änderungen und Widerrufe protokollieren.
1. Einträge regelmäßig überprüfen und stillgelegte Schlüssel kennzeichnen.

Öffentlich oder intern?

Die **Beschreibung des Katasters** kann öffentlich sein. Ein tatsächlich geführtes Kataster sollte abhängig von seinen Metadaten zugriffsbeschränkt sein: Auch ohne private Schlüssel können Systemnamen, Zugangswege und Verantwortlichkeiten sensible Informationen darstellen.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:schluesselkataster

Last update: **2026/11/15 16:36**