TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Konferenz

Berlin, 26.06.2026

DNA - Passwort-freie Zero-Access-Sicherung privater Schlüssel

Nick London, PNL Technology

Über uns

PNL Technology

Gruppe 2013 als Projektberatung gegründet
Idee zur sicheren Schlüsselwiederherstellung 2022
Erstes Patent 2024
Operative Gesellschaft 2025 gegründet
Mitglied seit 2026
Ansässig in Bremen

Unsere Philosophie:
Nur Schlüsselsouveränität bring echte Datensouveränität

Kontext: Asymmetrische Kryptografie

Privater Schlüssel Öffentlicher Schlüssel

Beispiele von Anwendungsfällen

E-Mail-Verschlüsselung (S/MIME, PGP)

Datenaustausch

Elektronische Signatur

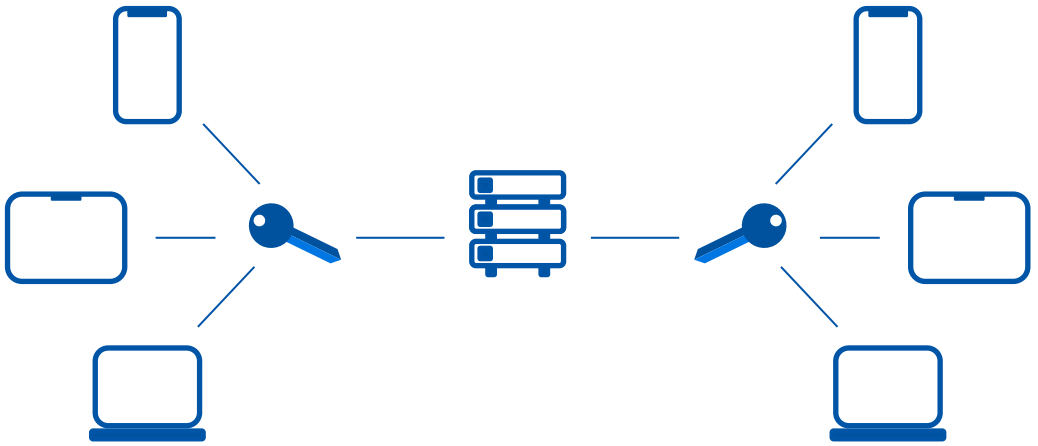
Echtzeitkommunikation (Chat, Telefonie)

Softwaresignatur

Und vieles mehr

Problemstellung

Herausforderungen bei der Umsetzung von Ende-zu-Ende Verschlüsselung in (Cloud-)Unternehmensanwendungen



- Schlüsselverlust
- Notwendigkeit von Master-Passwörtern
- Fehlende Einbindung in das Unternehmens-IAM
- Komplexe Schlüsselverteilungsverfahren
- Erfüllbarkeit von Aufbewahrungs- und Nachweispflichten
- Unverschlüsselte Schlüsselweitergabe
- CLOUD Act u.ä. Gesetzgebungen
- u.v.m.

Herausforderung: Schlüsselaufbewahrung

Privater Schlüssel Öffentlicher Schlüssel

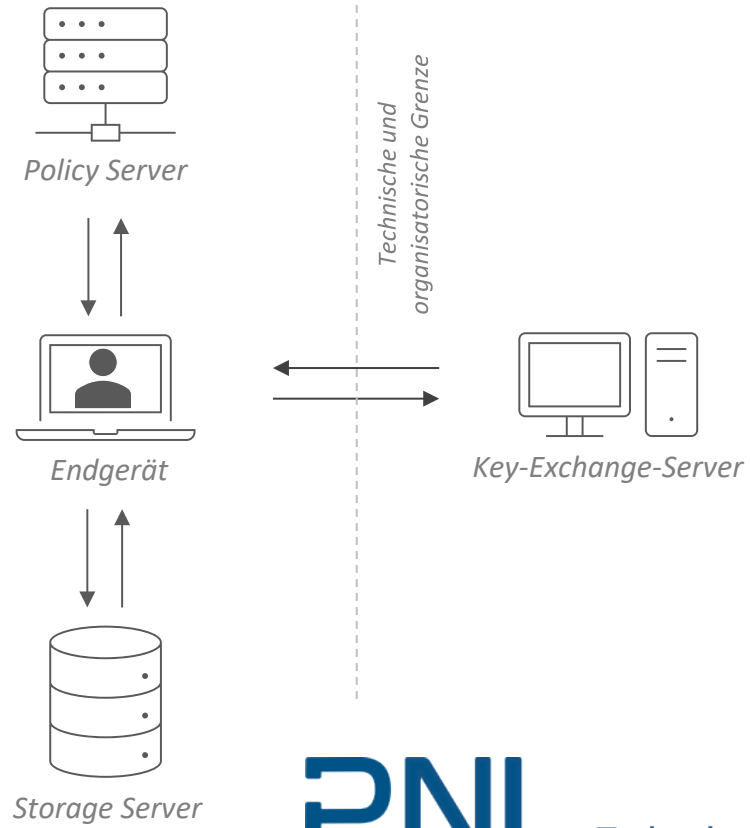
Anforderungen:

- ✓ Vertraulichkeit
  - ➢ Wer darf zugreifen?
  - ➢ Wer kann zugreifen?
  - ➢ Wo könnte der Schlüssel ggf. abgegriffen werden?
- ✓ Verfügbarkeit
  - ➢ Was sind die Voraussetzungen (Wissen, Haben) für einen Zugriff?
  - ➢ Welche Ausfallszenarien werden unterstützt?

Schlüsselwiederherstellung

- DNA bietet als Verfahren die Möglichkeit, Geheimnisse (wie private Schlüssel) zu sichern und wiederherzustellen.
- DNA wird dabei direkt in die Client-Anwendung integriert.
- Mit DNA liegt das unverschlüsselte Geheimnis ausschließlich auf dem Client.
- DNA verteilt die notwendigen Informationen auf zumindest zwei getrennte administrative Domänen.

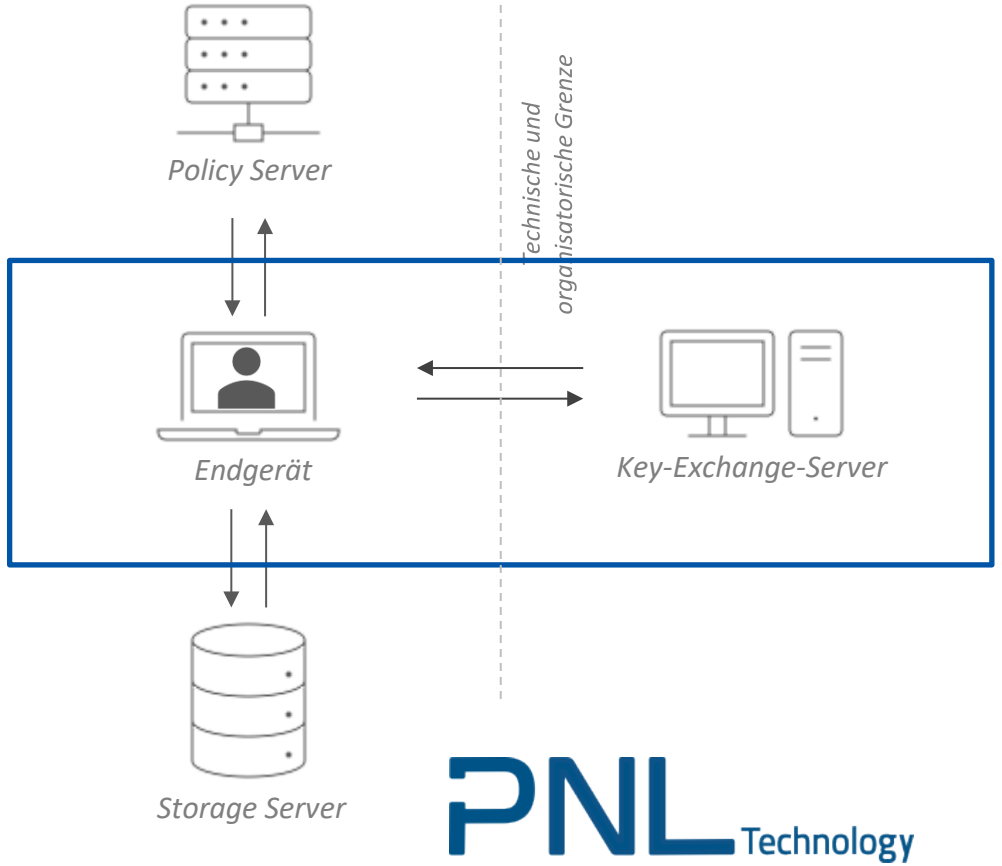
Beispielaufbau



Schlüsselsicherung (1/3)

- Partieller Schlüsselaustausch
  - DH, ECDH, ML-KEM
- Key-Exchange-Server kennt nur seinen eigenes Schlüsselpaar
- Client hat Pre-Key (K_0)

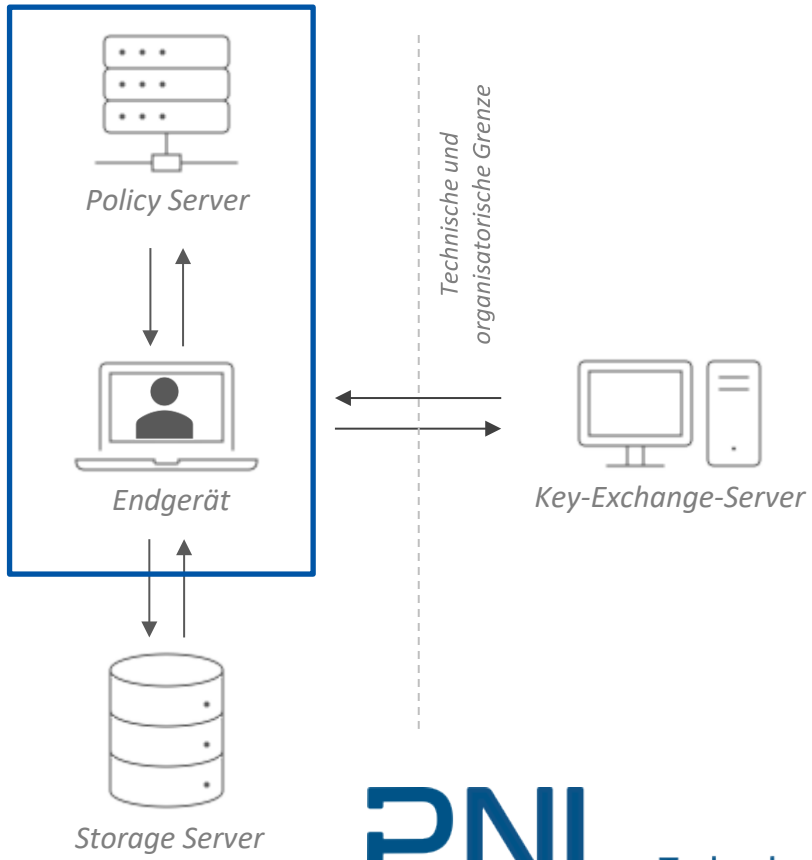
Beispielaufbau



Schlüsselsicherung (2/3)

- OPRF mit Policy Server
  - RFC 9497
  - Sobald standardisiert auch PQ-Verfahren, wie LeOPaRd
- Policy Server hält eigenen Schlüssel (S)
- Client leitet aus Pre-Key (K_{n-1}) neuen Schlüssel (K_n) ab, ohne etwas über S zu lernen
- Policy Server lernt nichts über K_{n-1} oder K_n
- Kann verkettet werden

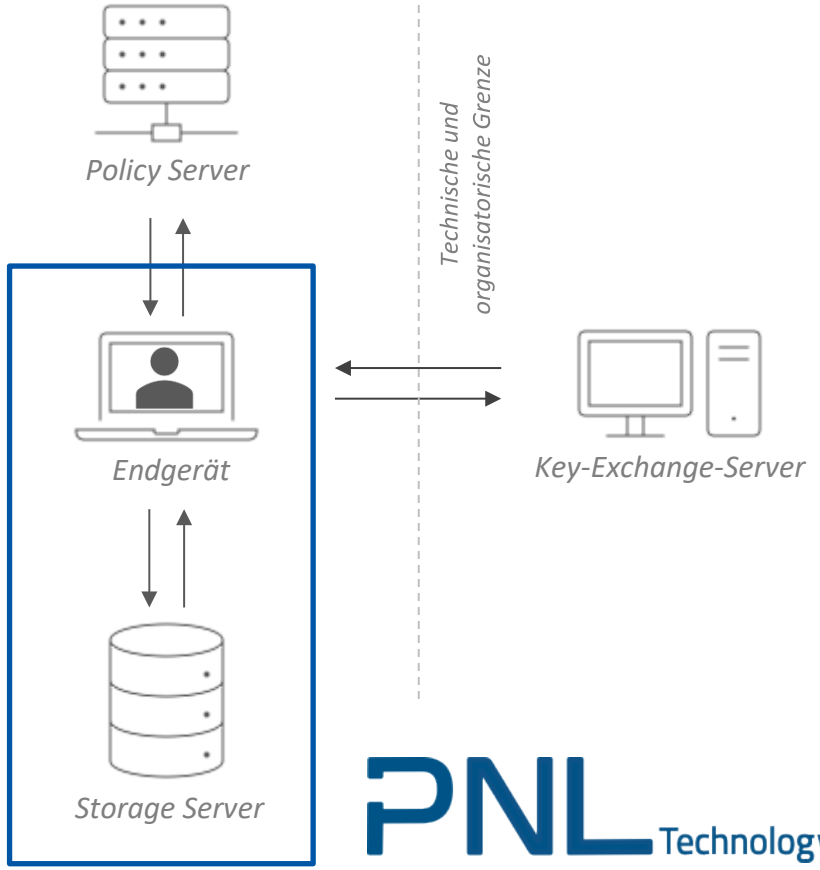
Beispielaufbau



Schlüsselsicherung (3/3)

- Client verschlüsselt Geheimnis (privaten Schlüssel) mit K_n
  - AES
  - ChaCha
- Storage Server speichert verschlüsseltes Geheimnis plus den öffentlichen Schlüssel des Client zum Schlüsselaustausch

Beispielaufbau



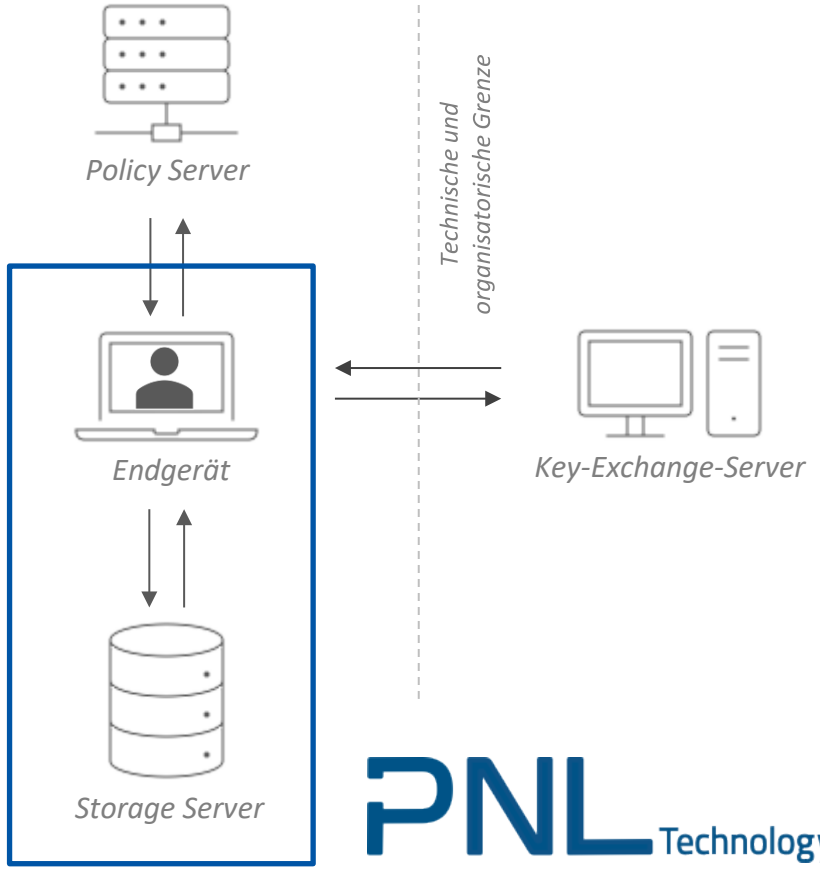
Zeitsprung

- Der Schlüssel ist nun gesichert.
- Wenn ein Client Zugriff auf den Schlüssel benötigt, kann dieser jederzeit wiederhergestellt werden.
- Zur Wiederherstellung sind alle Server von der Berechtigung des Client zu überzeugen.

Schlüsselwiederherstellung (1/4)

- Client ruft öffentlichen Schlüssel des Client zum Schlüsselaustausch ab
  - DH, ECDH, ML-KEM

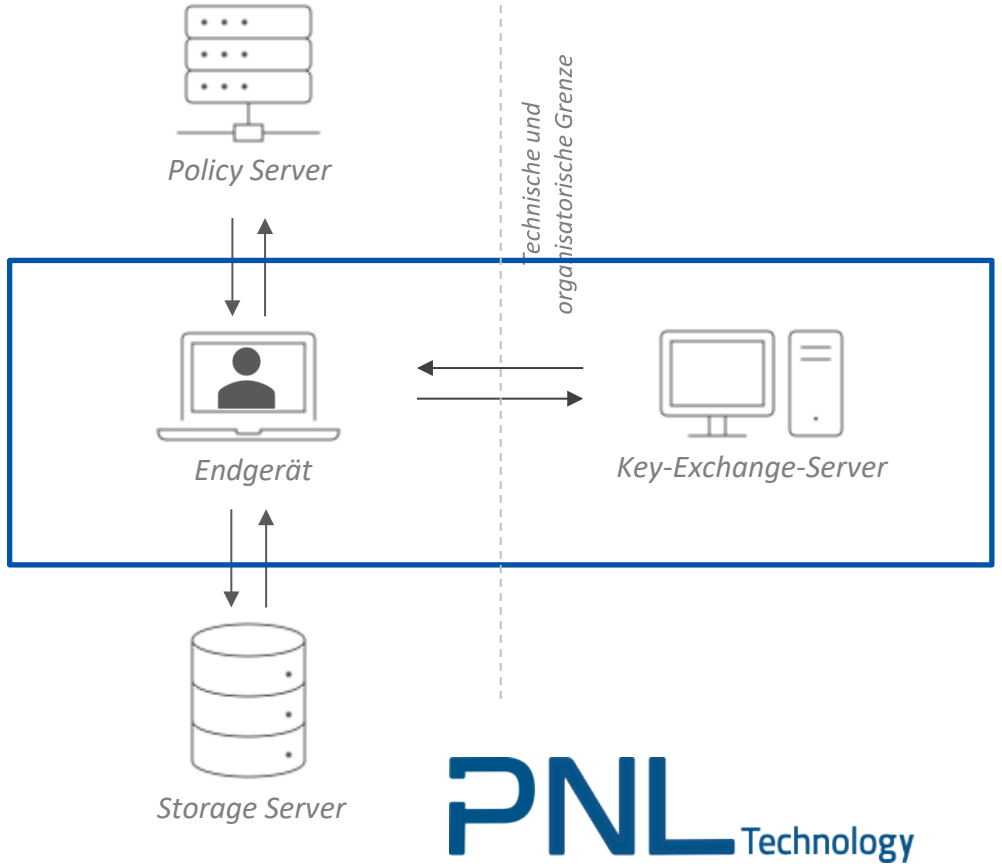
Beispielaufbau



Schlüsselwiederherstellung (2/4)

- Partieller Schlüsselaustausch wird vervollständigt
  - DH, ECDH, ML-KEM
- Key-Exchange Server lernt K_0

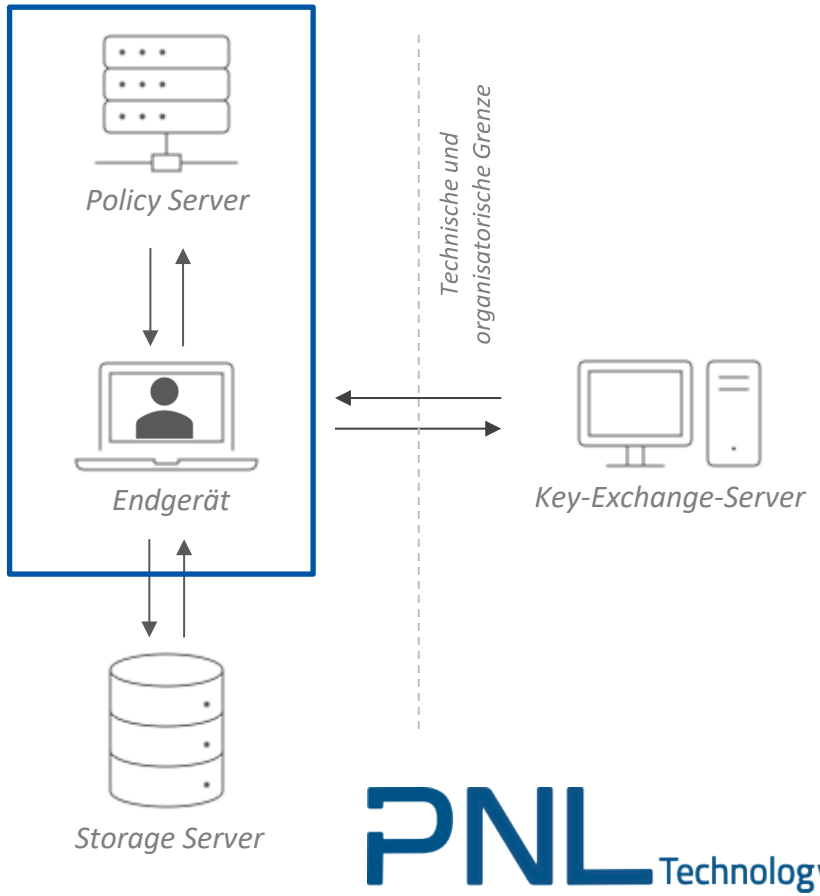
Beispielaufbau



Schlüsselwiederherstellung (3/4)

- Client führt OPRF mit den selben Policy Servern in der selben Reihenfolge, wie zur Sicherung durch.
- Client leitet aus Pre-Key (K_{n-1}) neuen Schlüssel (K_n) ab, ohne etwas über S zu lernen
- Policy Server lernt nichts über K_{n-1} oder K_n

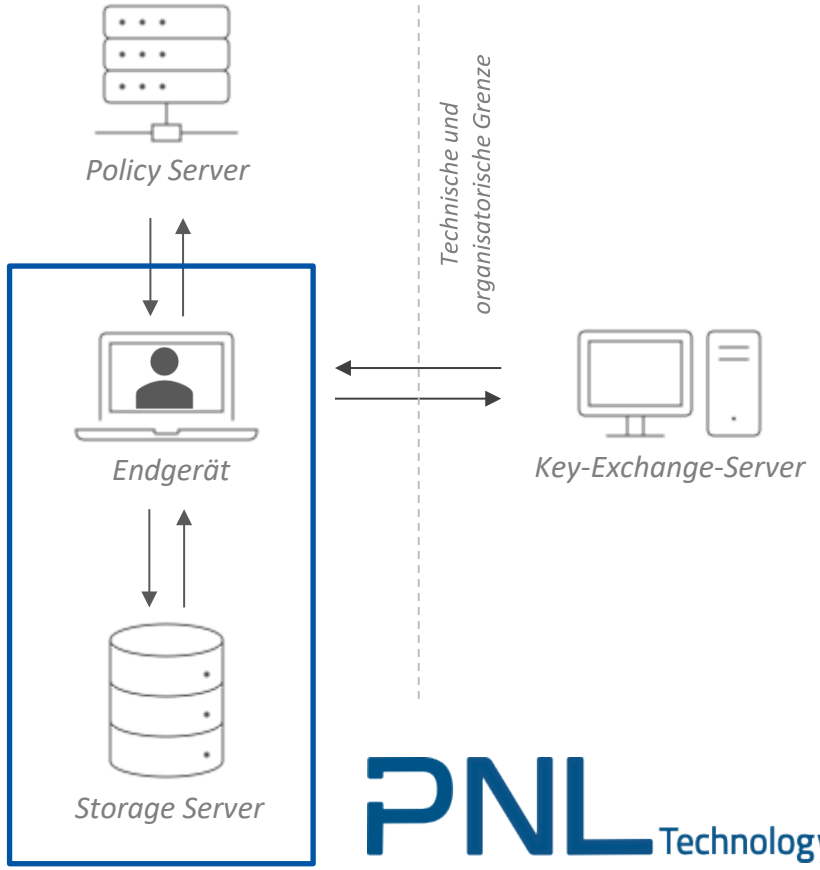
Beispielaufbau



Schlüsselwiederherstellung (4/4)

- Client Client ruft verschlüsseltes Geheimnis vom Storage Server ab
- Client entschlüsselt Geheimnis mit K_n

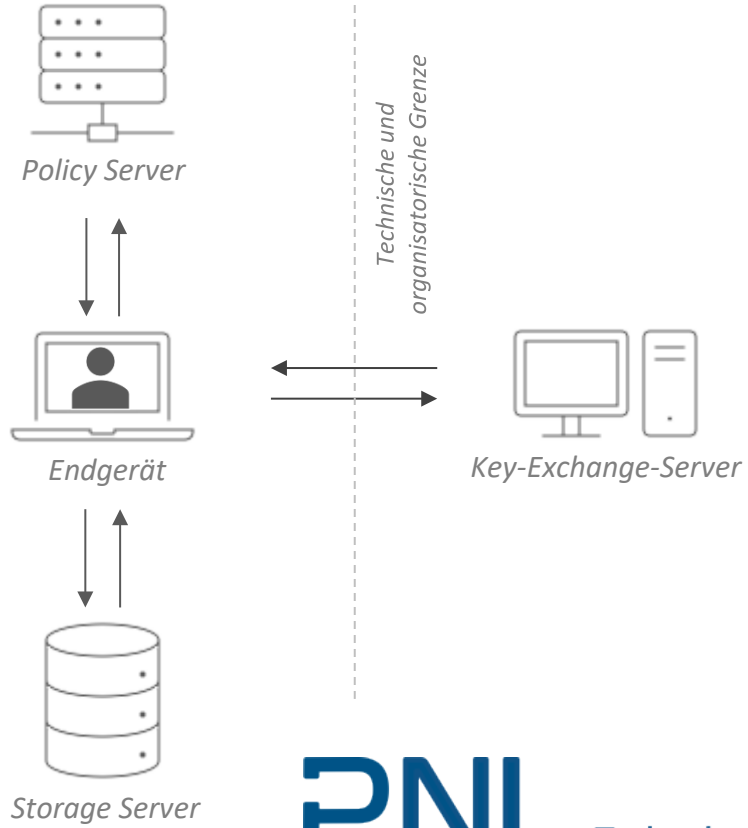
Beispielaufbau



Schlüsselwiederherstellung

- Zero Access Schlüsselwiederherstellungsverfahren
- Passwortfrei
- Identitäts- und berechtigungsbasiert
- Kann problemfrei mit OIDC, SAML2.0 o.ä. verwendet werden
- Ermöglicht Integration eigener Policy Server für beliebige Zwecke
- Keine „eigene Krypto“
- Post-Quantum-Ready
- Horizontal skalierbar

Beispielaufbau



Kontaktinformationen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

DNA

Vielen Dank für Ihre Aufmerksamkeit!

PNL Technology

dna@pnl-technology.eu
+49 421 33 11 42 - 10