trust yourself.

P3KI Core Framework

Überblick

Version
Juni 2024

Inhaltsverzeichnis

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

1 Einleitung

Die Produkte der P3KI GmbH (“P3KI”) optimieren Prozesse, reduzieren Risiko und schaffen Sichtbarkeit für Systeme der Kritischen Infrastruktur, welche den höchsten Anforderungen an Resilienz unterliegen. Unsere Berechtigungs- und Vollmachtlösung *P3KI Core* macht Konzepte aus Self-sovereign Identity (SSI) und *personalisiert delegierbaren Verifiable Credentials* (pdVC) feldtauglich und ermöglicht die Umsetzung von *Zero-Trust Architecture* (ZTA), auch ohne zentrale Orchestrierung sowie ohne Blockchain/DLT.

Die von P3KI entwickelte Autorisationslösung eignet sich im Speziellen zur Abbildung stark föderierter Strukturen mit flexiblen Hierarchien innerhalb verteilter und stark partitionierter Systemarchitekturen. Ein Alleinstellungsmerkmal von P3KI Core ist die Möglichkeit Berechtigungsprozesse in Offlineszenarien und ohne Hinzunahme Dritter oder zentraler Infrastruktur verlässlich umzusetzen.

Darüber hinaus bietet die P3KI auf die Kernlösung zugeschnittene sowie generelle Beratungsdienstleistungen in den Bereichen IT-Sicherheit und Rechtemanagementsysteme an.

Die P3KI bedient Kunden aus den Feldern Industrie, kritische Infrastrukturen und Verteidigung.

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2 P3KI Core Framework

2.1 Kernfähigkeiten

Business Enabler Fähigkeiten

- Prozessoptimierung und -einsparung durch Wegfall der Notwendigkeit immer verfügbarer zentraler Instanzen zur Orchestrierung und Automatisierung
- Reduzierter Personalaufwand für zentrale Berechtigungsverwaltung durch kontrollierte, föderierte Berechtigungsverwaltung
- Risikominimierung durch präzise, kontextabhängige, personalisierte Berechtigungen
- Risikominimierung durch kontextualisierte Vertrauensanker
- Auditierbarkeit durch vollständig personalisierte Berechtigungsketten
- Umgebungsagnostische Architektur anwendbar auf alle Netzwerkmodelle bis hin zu air-gapped

Technische Fähigkeiten

- Erstellung und Verwaltung von *Self-sovereign Identities* (SSI, nativ oder PKI-basiert)
- Berechtigungs- und Vollmachtausstellung in Form von *personalisiert delegierbaren Verifiable Credentials* (pdVC) (personalisierte Berechtigungen, IEC 62443)
- Kontrollierte und nachvollziehbare, personalisierte Berechtigungsweitergabe (Autorisierung)
- Hochflexibles hybrides Mehrparteien-Vertrauensmodell basierend auf *Lattice-Based Access Control* (LBAC), kombinierbar mit parallelen Konzepten aus RBAC, PBAC, ReBAC
- Hochpräzise Definition beliebiger Berechtigungsanforderungen und/oder Berechtigungsgruppen und -hierarchien
- Interoperabel mit PKI- / zertifikatbasierten Identitäten, auch über PKI Hierarchiegrenzen hinweg
- Berechtigungsverifikation vollständig offlinetauglich
- Berechtigungsausstellung & -weitergabe im Offlinekontext möglich
- Gesicherte, verschlüsselte Kommunikation durch autorisierte und authentifizierte Kanäle
- Dynamische, mathematisch bewiesene Policysprache erlaubt parallelen Betrieb mehrerer Anwendungsfälle
- Datenaustauschebene auf Wunsch in Ausprägung *High Availability* (HA)

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.2 Anwendungsfallspezifische Umsetzungen

Das P3KI Core Framework kann in unterschiedlichsten Umgebungen zum Einsatz gebracht werden, um Berechtigungsverwaltung und Zugriffskontrolle hoch resilient umzusetzen. Die folgenden Passagen beschreiben konkrete Anwendungsfälle, welche durch das P3KI Core Framework möglich gemacht wurden.

2.2.1 IIoT Feldgeräte Lifecycle & Berechtigungssystem

Dieses auf einer Nordic nRF5340 Plattform (ARM Cortex M33, Zephyr RTOS) umgesetzte System erlaubt die Abbildung folgender Arbeitsabläufe für Feldgeräte:

- Kontrollierter Besitzübergang des Feldgeräts an den Kunden inkl. Rechteaufgabe des Herstellers
- Optionaler Vorbehalt von Teilberechtigungen durch den Hersteller (z.B. Wartungsberechtigungen oder Sonderfunktionen)
- Nachvollziehbarer Zugriff für Betriebs- und Wartungspersonal
- Passwortlose, operationsspezifische Berechtigungsverwaltung ohne Benutzeraccounts
- Dynamische, nachvollziehbare Berechtigungsweitergabe
- Unabhängig von zentralen Managementlösungen, vollständig offlinefähig
- Optionale Fähigkeit: Gerät-zu-Gerät Berechtigung zur automatischen Konfigurationsverteilung in Mesh-Netzwerken

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.2.2 Cross-Airgap Self-Service Accounts

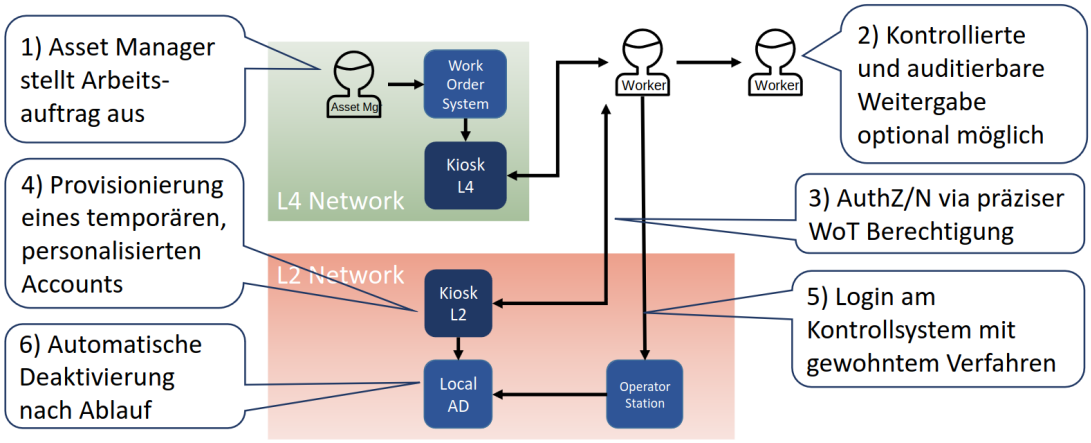

Abbildung 1: High-level Konzept der Cross-Airgap Lösung

Diese Lösung zielt auf den Einsatz in industriellen Kontrollnetzwerken (SCADA/ICS) ab. Diese sind üblicherweise dadurch gekennzeichnet, dass eine starke und deutliche Trennung zwischen der Netzwerkumgebung des Kontrollsystems (Purdue Network Layer L2) einer spezifischen Anlage und dem weiteren Office Netzwerk (Purdue Network Layer L4) vorherrscht. Dies macht die zentrale Verwaltung von personalisierten Zugriffsrechten und Accounts schwierig bis unmöglich, was wiederum in Konflikt mit regulatorischen Anforderungen zur Nachvollziehbarkeit (z.B. IEC 62443, GMP, NIS2, etc.) steht.

- Berechtigungsausstellung direkt durch Anlagenmanager
- Übermittlung personalisierter Berechtigungen an Mitarbeiter über Kiosksysteme im L4 Netzwerk
- Transport der personalisierten Berechtigungen via Mobile App Wallet
- Ausstellung temporärer und personalisierter Benutzeraccounts in der L2 Umgebung basierend auf diesen Berechtigungen
- Dynamische und kontrollierte Weitergabe der Berechtigungen direkt von Mitarbeiter zu Mitarbeiter
- Integration und Optimierung von Identitätsverifikationsschritten durch die Abteilung Anlagensicherheit
- Möglichkeit der Auslagerung der Identitätsverifikationsschritte an vertrauenswürdige Dritte
- Erweiterung des Nutzerkreises auf externe Dienstleister
- Erweiterungsmöglichkeit durch Integration von Zutrittskontrollsystemen

P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.2.3 Protokoll zur Message Autorisierung innerhalb Message Bus Architekturen

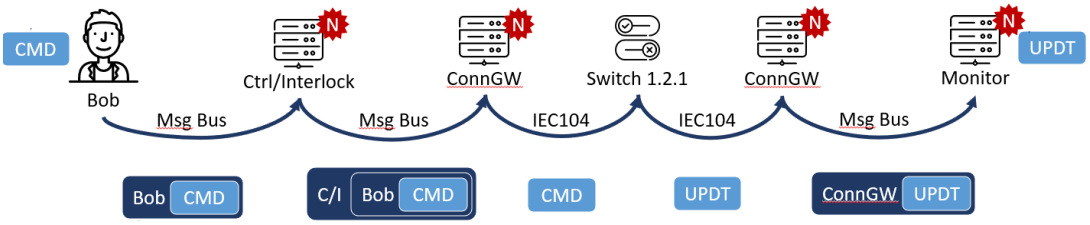

Abbildung 2: Schematischer Aufbau der Message Bus Autorisierung

Diese Protokollschicht stellt eine Anwendung von *P3KI Core* für die flexible und sichere Autorisierung von Nachrichten im Kontext einer Message Bus Architektur (z.B. Apache Kafka, MQTT, etc) dar.

Durch das eigens entworfene Protokoll wird die flexible Autorisierung und Authentifizierung basierend auf *P3KI Core* für Einwegprotokolle ohne aktive Interaktion zwischen anfragender und berechtigender Partei möglich. Alle Vertrauensmodelle (direkt, Multi-Anker / Multi-Path) sind anwendbar.

Eine dynamische Skalierung einzelner Dienste der Prozesskette mit ad-hoc generierten personalisierten Identitäten für selbige ist möglich. Hierdurch wird eine Ende zu Ende nachvollziehbare und auditierbare Informations- und Berechtigungskette sichergestellt.

- Mehrparteien Unterzeichnung
- Identitäten müssen nicht vorab benannt sein
- Replay-Schutz Informationen integriert
- Funktionalität über Netzwerkzonen hinweg möglich
- Unterstützt dynamische Skalierung einzelner Dienste innerhalb der Prozesskette

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.2.4 Konzept: Cross-PKI Berechtigung und Interaktion

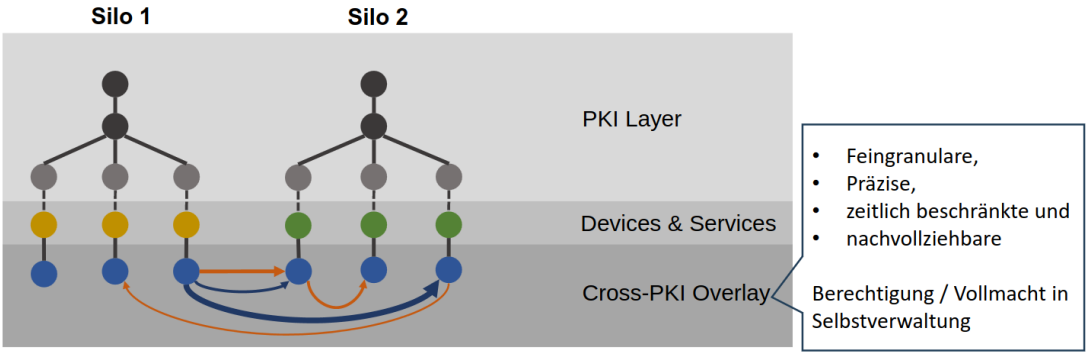

Abbildung 3: High-level Konzept der Cross-PKI Lösung

Dieses im Rahmen des TeleTrusT-EBCA “PKI-Workshop” 2023 unter dem Titel “Cross-PKI Web-of-Trust als Enabler für Zusammenarbeit” vorgestellte Konzept ermöglicht erstmals die technische Zusammenarbeit über die Grenzen einer einzelnen PKI Hierarchie hinweg. Kernfähigkeiten des Konzepts sind:

- Kein Cross-Signing notwendig
- Kein Ausstellen neuer Zertifikate notwendig
- Präzise, fein-granulare kontext- und fallbezogene, zeitlich beschränkte Berechtigungen

P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.3 Komponenten der Kernlösung

Die folgenden Passagen beschreiben die Kernelemente des P3KI Core Frameworks. Diese dienen als Bausteine zur Umsetzung individueller Berechtigungslösungen, welche über die oben genannten Anwendungsfälle hinaus gehen.

2.3.1 Berechtigungsweitergabe mit feinstgranularer Policysprache zur Modellierung von Berechtigungen und Rollen

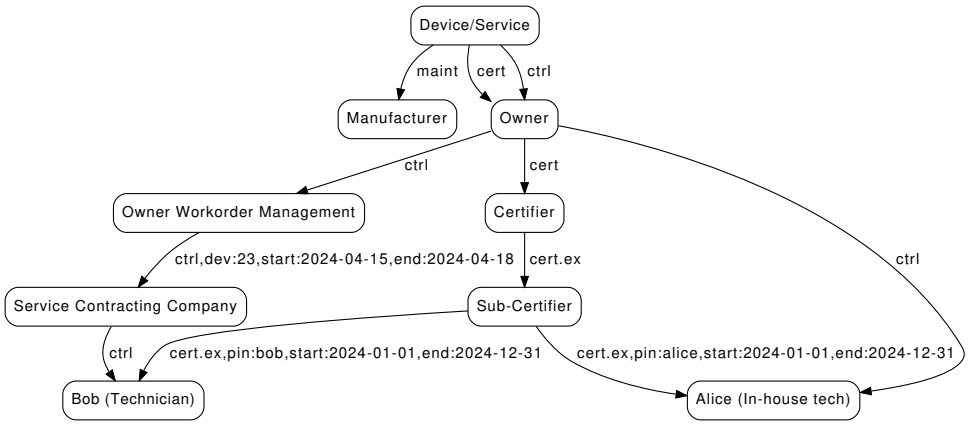

Abbildung 4: Einfaches Beispiel eines Multi-Pfad Berechtigungsmodells

Berechtigungsweitergabe stellt ein fundamentales Konzept in P3KI Core dar. Es ist in allen Ausprägungen der Software enthalten.

Eine vollständige oder teilweise Einschränkung der Fähigkeit Berechtigungen weiterzugeben ist möglich.

Eine Einschränkung der Weitergabefähigkeit ist prinzipiell auf folgende Arten möglich:

- Berechtigungs-Pinning an eine konkrete Identität (“you and only you”)
- Zeitlich beschränkte Berechtigungen mit automatischem Verfall
- Multi-Anker / Multi-Pfad Berechtigung durch Aufspaltung der Berechtigung in mehrere Sub-Policies im Rahmen eines Rollenkonzepts (“is operator for X area (approved by company, pinned) AND scheduled to work today (by shift lead, pinned) AND allowed to control SCADA in area X (part of workorder, delegable”)

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.3.2 Microservice Integration & Identitätsverwaltung Managed (trinityd)

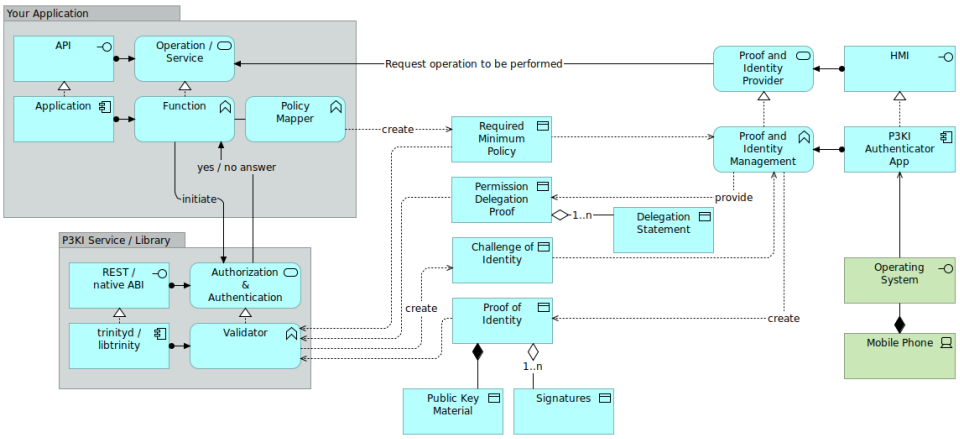

Abbildung 5: Authorization mit trinityd beispielhafte Architektur

Trinityd ist die Basis zur schnellen Integration in Microservice-Architekturen. Diese Komponente bietet einen "one-stop shop" für viele übliche Anwendungsfälle und erlaubt es schnell und agil, verteilte Berechtigungssysteme umzusetzen.

Seinen primären Einsatz findet *trinityd* im Backend von microservice-basierten Anwendungen im Cloud und On-Prem Kontext.

- Identitätsbasis ad-hoc/nativ oder x.509 Zertifikat möglich
- REST Schnittstelle
- OpenAPI 3.0 / Swagger Schnittstellendefinition liegt bei

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.3.3 Berechtigungsverwaltung und AuthN/Z via Mobile App (P3KI Authenticator)

P3KI Authenticator für Android Betriebssysteme ist unsere Basislösung für personalisierte, ortsbewegliche Identitäten und Berechtigungen. Die Schlüsselablage erfolgt im Secure Element des Mobiltelefons. Die Authentifizierung erfolgt biometrisch gesichert mittels Fingerabdruck.

Eine kontrollierte und personalisiert nachvollziehbare Berechtigungsweitergabe ist direkt am Mobiltelefon möglich. Datenaustausch kann über Netzwerk, Bluetooth, NFC oder beliebige Transportwege wie Instant Message und Email erfolgen. An den Datenaustauschkanal werden keine gesonderten Sicherheitsanforderungen gestellt.

Für das Identitätsmanagement sind folgende, untereinander prinzipiell interoperable, Modelle vorgesehen:

- Durch autorisierten Dienst bestätigte Identität (via *P3KI Proven ID* Dienst)
- Aus X.509 Zertifikat abgeleitete Identität (Beta)
- Auf Smartphone erstellte lokale Identität

Für die Mobile App sind mehrere Benutzungsmodelle vorgesehen:

- Verwendung der Anwendung “as-is” für Basis Use-Cases
- Whitelabel Lösung mit angepasstem Branding und Workflows
- Optionale Offenlegung des Quellcodes als Basis zur Eigenentwicklung durch den Kunden
- Android Smartphone Basis
- Apple iOS technisch möglich (PoC)
- Üblicher Einsatz in Kombination mit
  - Delegationsspeicher
  - trinity-device
  - trinityd
  - P3KI Proven ID

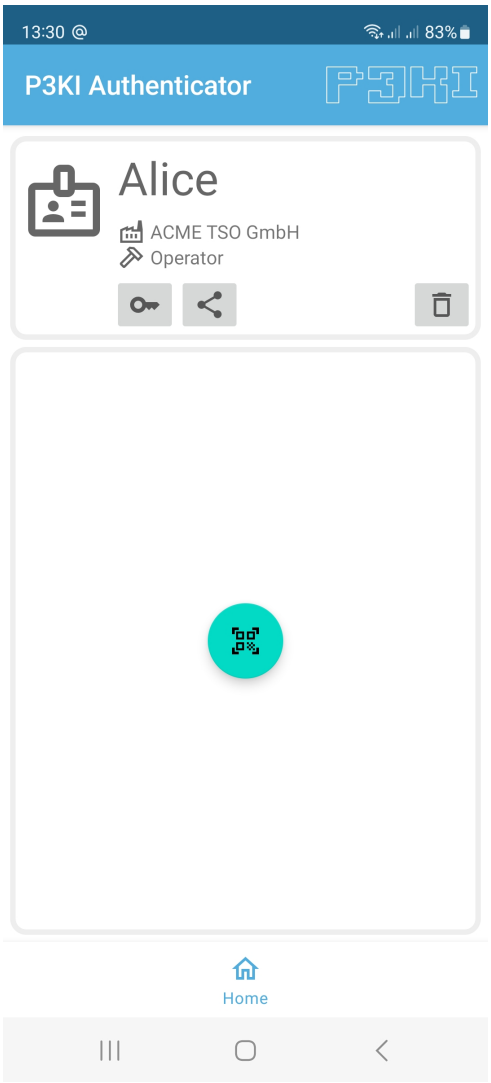

Abbildung 6: P3KI Authenticator App (Android)

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.3.4 Delegationsspeicher

Der *Delegationsspeicher* dient als schneller Kommunikationsmultiplikator und Plattform zur Informationsverteilung. Über ihn können neue Berechtigungen oder Änderungen an bestehenden Berechtigungen schnell mit einer großen Anzahl Personen und Diensten ausgetauscht werden.

Überdies dient er im föderierten Betrieb als lokaler Zwischenspeicher zur Erhöhung der Systemresilienz, da auch bei vorübergehender Unerreichbarkeit zentraler Instanzen, weiterhin effektiv und effizient der Betrieb sichergestellt wird.

Der Delegationsspeicher erlaubt es lokale, föderierte oder, je nach Konzept, auch zentrale Datenablageorte für Berechtigungsdaten zu definieren.

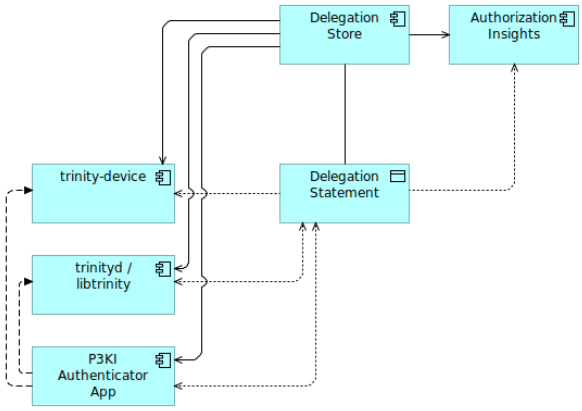

Abbildung 7: Delegationsspeicher High-level Architektur

Ideal ist das Zusammenspiel mit *groved* zur Sammlung von Audit-Trails und *Authorization Insights* zur Visualisierung der im Delegationsspeicher gesammelten Berechtigungen als Vertrauensnetzwerk.

- Kompaktversion bereits integriert in trinityd
- Erweiterbar auf *High Availability (HA)* mit alternativen Datenbank Backend
- Üblicher Einsatz in Kombination mit
  - trinityd
  - trinity-device
  - Authenticator App
  - groved
  - Authorization Insights

P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.4 Erweiterungskomponenten

Neben den für die Funktion des P3KI Core Framework notwendigen Kernkomponenten, bieten wir darüber hinausgehende Fähigkeiten in separaten Komponenten an. Diese dienen zur schnellen Entwicklung, vereinfachen den Betrieb und ermöglichen lückenlose Nachweisführung.

2.4.1 Funktionsproxy (trinity-device)

Mit *trinity-device* bieten wir einen einfachen und schnellen Weg Operationen individuell und sicher zu exponieren und Berechtigungen zum Zugriff auf selbige delegierbar zu machen.

Trinity-device bietet die komplette Anwendungslogik zur schnellen Entwicklung von Prototypen.

Unterstützt werden folgende Operationen:

- Aufruf von CLI Anwendungen
- API Aufrufe (z.B. REST Schnittstelle)

Die Konfiguration von trinity-device erfolgt über eine Konfigurationsdatei - Config - Service - Authz - Interact

- Java CLI Anwendung
- Mehrkanal-Interaktion mit Authenticator App
  - Netzwerk
  - Bluetooth
  - NFC
- Üblicher Einsatz in Kombination mit
  - Delegationsspeicher
  - Authenticator App
  - groved

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.4.2 P3KI Proven ID Dienst

P3KI Proven ID ist eine kompakte on-boarding Lösung, um durch Benutzer in der *P3KI Authenticator* Mobile App erstellte Identitäten im Corporate Kontext einzupflegen. Dieser Dienst stellt das Verbindungsglied zwischen der Corporate Identity Governance und dem Bring-you-own-key (BYOK) Prinzip von *P3KI Core* dar.

- Üblicher Einsatz in Kombination mit
  - Authenticator App

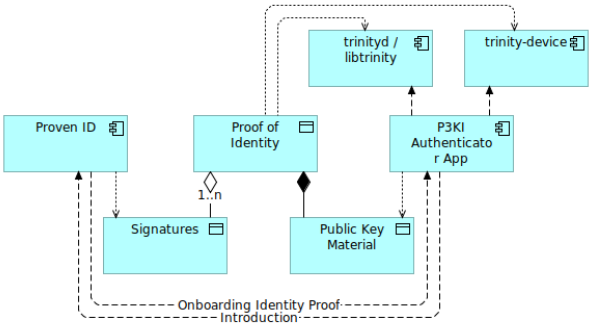

Abbildung 8: Proven ID High-level Architektur

2.4.3 Ad-hoc Peering über Zweitkanal

Diese Erweiterung dient dem ad-hoc Peering von bislang einander nicht bekannten Kommunikationspartnern im Feld unter anderweitigen Offlinebedingungen (keine erreichbare 3rd Party). Hierzu werden zwei getrennte Kommunikationskanäle etabliert, welche beide von seiten des P3KI Core Frameworks agnostisch betrachtet werden, sprich die konkrete Ausprägung ist für die korrekte Funktion unerheblich.

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.4.4 Datenaggregation zur Auditierung und Überwachung (groved und groves, aktuell in Entwicklung)

Groved ist eine Audit-Erweiterung zu *trinityd* und *trinity-device* um die dortig bereits generierten Auditdaten effektiv und effizient zu extrahieren und zu aggregieren.

Die Erweiterung sammelt zu jedem angestoßenen Berechtigungsvorgang kryptografisch signierte Beweisdaten. Diese enthalten, u.A. Informationen zur Berechtigten als auch Berechtigenden Partei, die Zusammenstellung des Autorisierungsbeweises und Informationen über den Erfolg oder Misserfolg des Berechtigungsvorgangs.

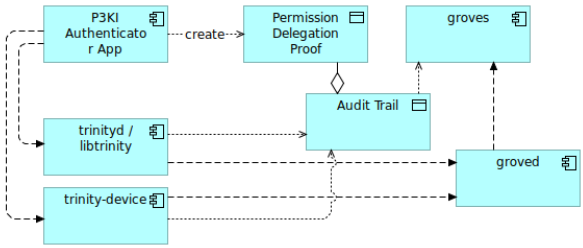

Abbildung 9: Groved und groves High-level Architektur

Gesammelte Informationen werden direkt oder indirekt an *groved* Aggregatoren übermittelt und zur späteren Auswertung vorgehalten.

- Audit-Erweiterung zu *trinityd* und *trinity-device*
- Erfasst audit-relevante Daten
- Kryptografisch signierte Datenablage
- Lokale, föderierte oder zentrale Sammlung
- Üblicher Einsatz in Kombination mit
  - trinityd
  - trinity-device
  - groves

Groves ist ein automatisches, regelbasiertes Werkzeug zur laufenden Auditierung von Berechtigungsvorgängen.

- Enumeration aktiver Identitäten
- Überwachung der Aktualität im Vertrauensnetzwerk verwendeter Berechtigungsbeweise
- Erkennung von Datenpropagationsprobleme
- Erkennung der Verwendung veralteter Berechtigungsdaten
- Erkennung von Berechtigungsfehlern / potentiellen Angriffen
- Regelbasiertes Alarming bei Anomalien
- Üblicher Einsatz in Kombination mit
  - groved
  - Authorization Insights Visualisierung

P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.4.5 Authorization Insights Visualisierung

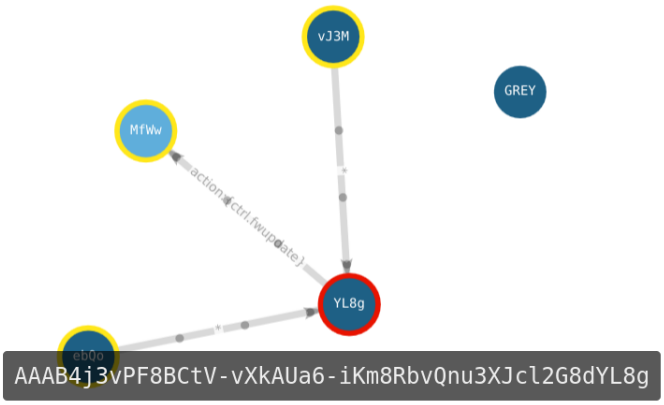

Abbildung 10: Beispiel einer browser-basierten Graphvisualisierung von Berechtigungsbeziehungen

Authorization Insights ist eine browser-basierte Graphenvisualisierung zur Darstellung von Berechtigungsbeziehungen. Die Komponente ist flexibel einsetzbar auf lokalen und zentralen Delegationsspeichern sowie zur Darstellung einzelner Berechtigungsbeweise.

- Browser-basiert
- In eigene Web-Apps integrierbar
- Üblicher Einsatz in Kombination mit
  - groves
  - Delegationsspeicher
  - trinityd
  - trinity-device

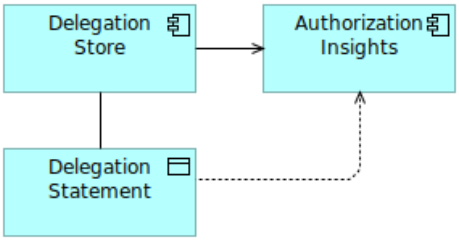

Abbildung 11: Authorization Insights High-level Architektur

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

2.4.6 OpenTelemetry

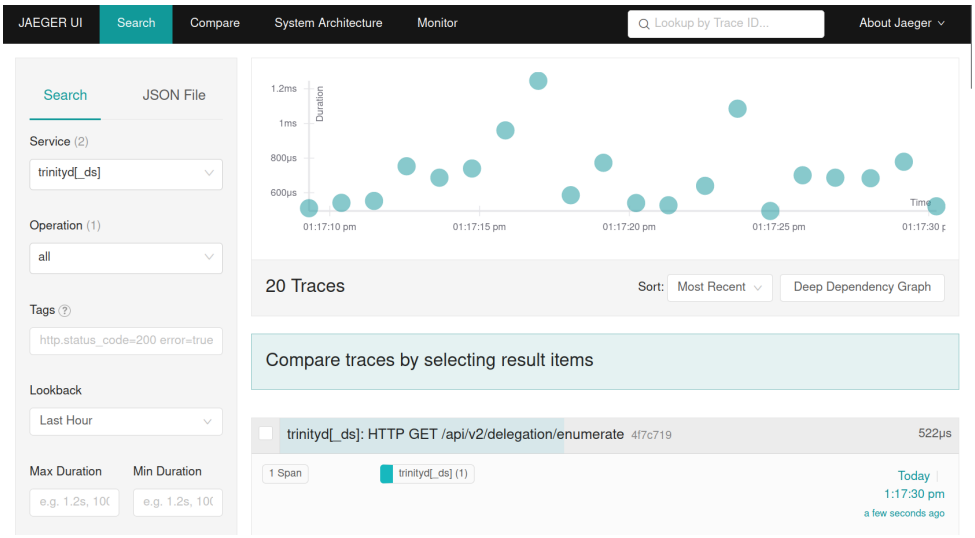

Abbildung 12: OpenTelemetry Visualisierung mit Jaeger

Trinityd bietet die Möglichkeit detaillierte Trace-Informationen im OpenTelemetry Format zu exportieren. Hierdurch wird in Echtzeit die Interaktion zwischen mehreren *trinityd* Instanzen visualisiert nachvollziehbar.

Ein wertvolles Werkzeug sowohl für die Entwicklungsphase als auch den gesicherten Betrieb.

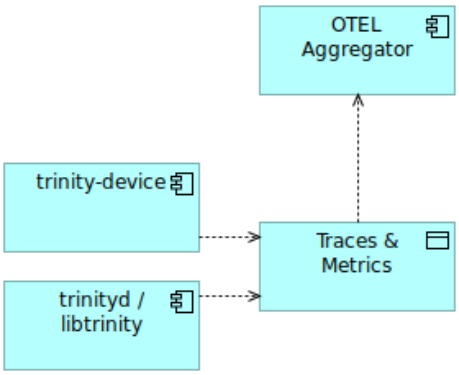

Abbildung 13: OpenTelemetry Integration High-level Architektur

2.5 Integration und Plattformunterstützung

P3KI Core Framework ist auf einer Vielzahl von Plattformen einsetzbar:

- Intel x86 und kompatible (Server, Desktop, Laptop Computer)
- ARM (u.A. ARM11, Cortex A53, Cortex M33. z.B. Raspberry Pi, Nordic nRF5340)
- Xtensa LX6 (experimentell, z.B. Espressif ESP32)

Daneben kann das P3KI Core Framework in verschiedensten Laufzeitumgebungen zum Einsatz gebracht werden:

- Linux
- Microsoft Windows
- Zephyr RTOS
- Google Android
- Apple iOS (experimentell)
- WASM (experimentell)

Version , Juni 2024,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com