SPIK 2016

Kantonspolizei Zürich

abraxas

Platform as a Service für Forensik und eDiscovery

Beat Kirchhofer *Chef IT-Betrieb, Kantonspolizei Zürich*

Anton Brauchli *Solution Architekt, Abraxas Informatik AG*

Stade de Suisse, Bern
17.03.16

Agenda

Einleitung

Service Ziele

Service Details

Architektur Übersicht

Wissenstransfer

Zusammenarbeit

Vorteile

Roadmap

Einleitung

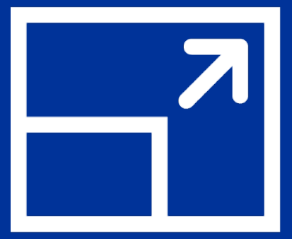
- Beweggründe
- Herausforderungen
  - Kosten/Budget
  - Know-how
  - Flexibilität
  - Beschaffung/Einsatz
  - Ressourcen

Service Ziele

Einfacher Zugriff

Sicherheit

Skalierbarkeit

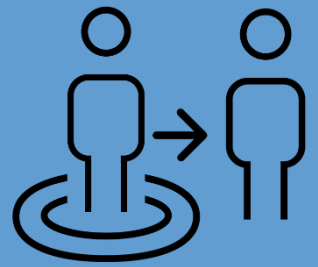


Nachvollziehbar

Tiefe Investitionen

Flexibilität

Wissenstransfer



Kapazität nach Bedarf

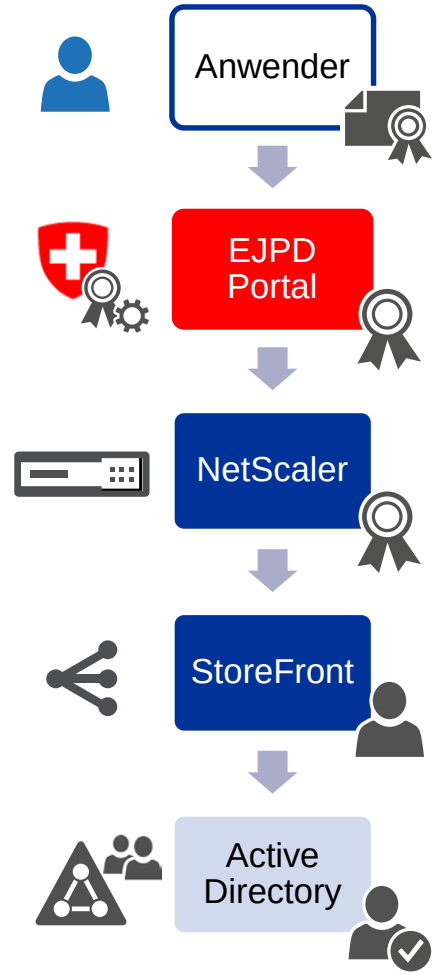
abraxas

Service Details

Authentisierung & Autorisierung

Zugriff auf den Service

- SmartCard & PIN Authentisierung
- EJPD Portal als Identity Provider -> SAML Token
- Citrix NetScaler
- Citrix StoreFront
- Active Directory «Shadow Accounts»



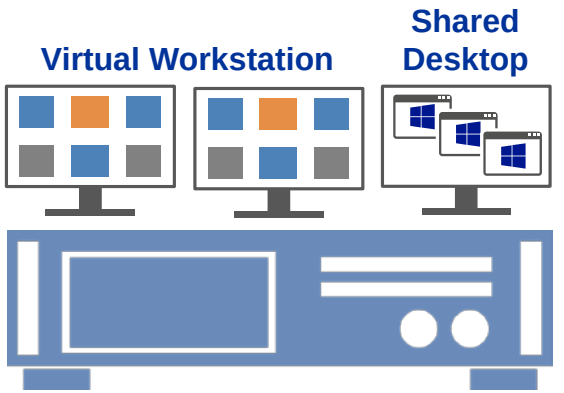
Präsentationsschicht

Arbeitsplatz für Forensische Analysen

- Persönliche virtuelle Forensik Workstation (VDI)
- Individuelle SW Installationen pro Benutzer
- Dedizierte VDI Hardware pro Korps

Arbeitsplatz für Review Tätigkeiten

- Shared Desktop für «Light» Benutzer
- Standard Tools Set



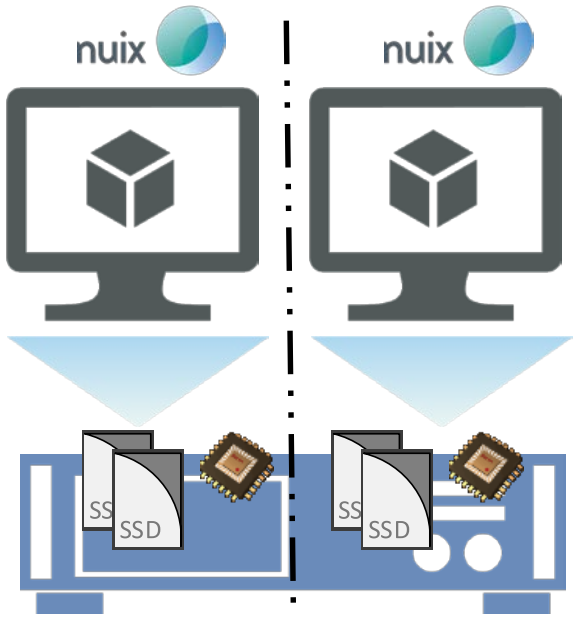
Anwendungsschicht

Forensik Daten Aufbereitung mit «NUIX»

- Datenbearbeitung zu 100% im Datacenter
- Dedizierte HW pro VM *(CPU & SSD)*
- Skalierbare Architektur
- Zentraler Lizenz Server

Weitere Services geplant

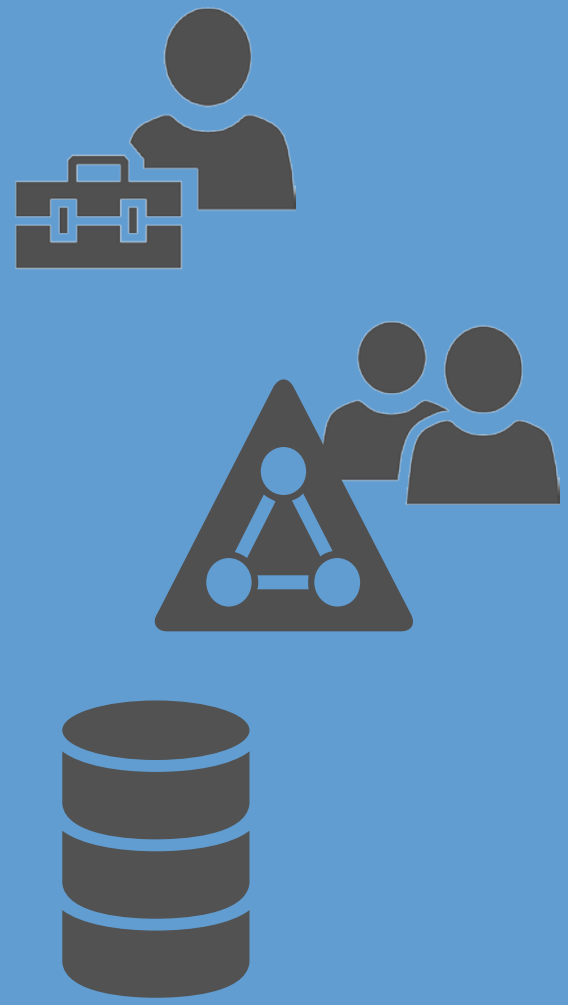
- Relativity eDiscovery
- Text und Content Analyse
- Video und Bild Auswertung



Management

Kapo ZH verwaltet die Ressourcen

- Zuteilung der «NUIX» Systeme
- Storage as a Service
- Anwenden des Berechtigungskonzepts
- «NUIX» Lizenzierung & Betrieb
- Benutzer Verwaltung für Datentransfer



Transparenz und Nachvollziehbarkeit

Kantonspolizei Zürich

observe it People audit

Kapo ZH auditiert die Zugriffe

- Separation of Duties
- Administrator & Anwender Überwachung
- Alerting für sicherheitsrelevante Aktionen
- Video Aufzeichnung
- Dual-Passwort für Video Review
- DBA Aktivitätsauditierung
- Anwendungsauditierung

Threat Detection Dashboard

Betrieb und Administration

Abraxas betreibt die Basis Infrastruktur

- Betriebssysteme & Datenbanken
- Datensicherung & Monitoring
- Security Systeme
- Vmware & Citrix
- Server & Storage
- Datacenter
- Microsoft & Citrix Lizenzierung

abraxas

Schweiz

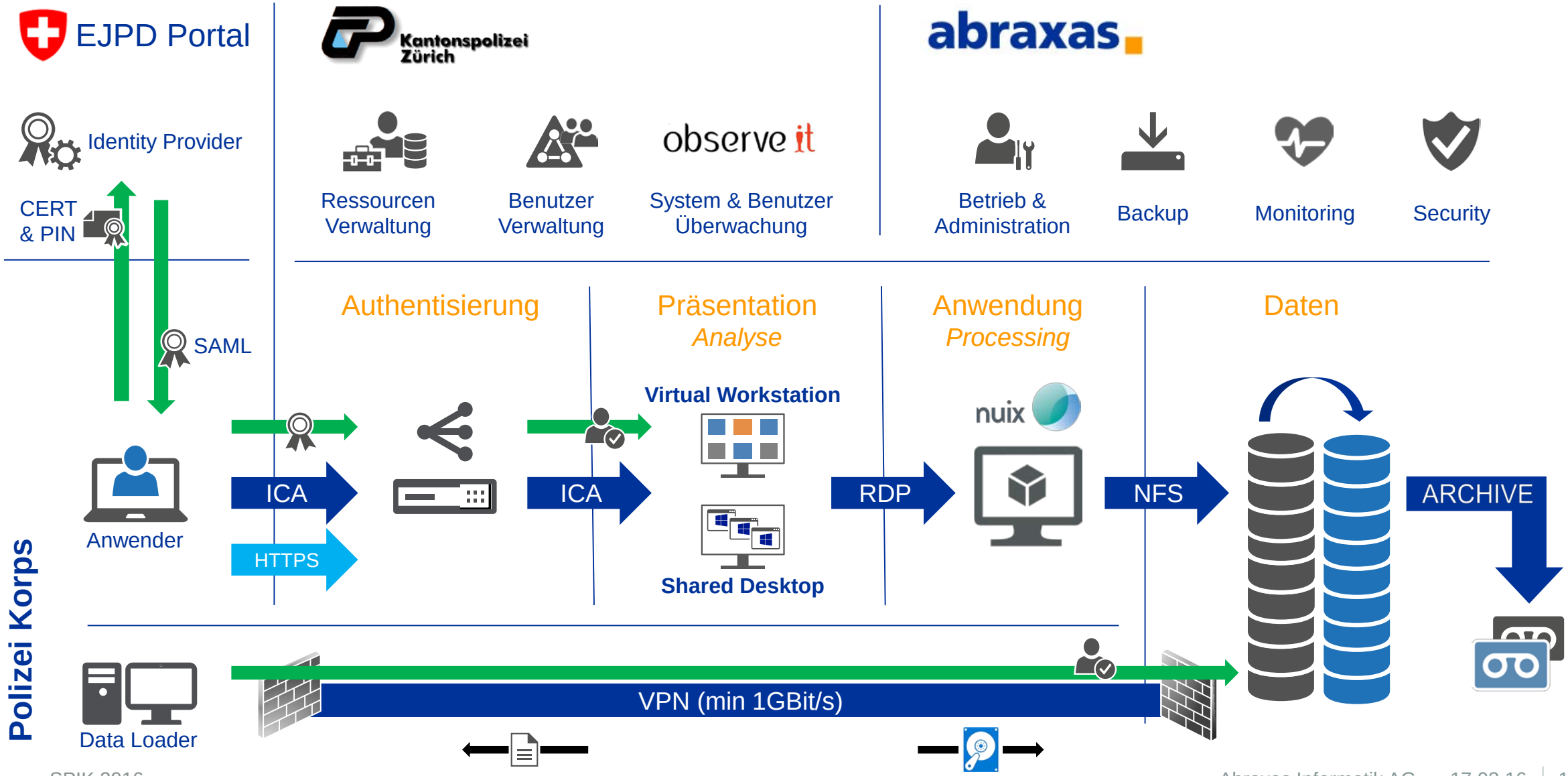
Sicherheit

Kundennähe

abraxas

Architektur Übersicht

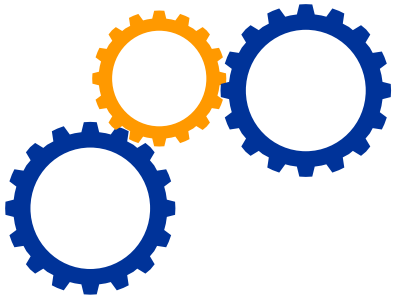
Architektur



Anforderungen

Was sind die Anforderungen auf Kundenseite?

- Anschluss am KOMBV-KTV
- 1GBit/s Link zum Kapo ZH Datacenter
- Housing der Firewall auf Kundenseite
- Mitarbeit bei der Netzwerk Integration
- Microsoft EA (VDA Lizenzierung)



Kantonspolizei Zürich

Wissenstransfer

Zusammenarbeit

Vorteile

Roadmap

Wissenstransfer

Kantonspolizei Zürich

Digital Forensics

- Breites Wissen aufgebaut / wird vermittelt
- Scripts für Automatisierung vorhanden
- Weiterentwicklung Tools, Scripts etc. gewährleistet
- Plattform FAQ wird breit bewirtschaftet
- Neue Technologien gemeinsam evaluieren und zentral zur Verfügung stellen

Zusammenarbeit / Vorteile

Kantonspolizei Zürich

Zusammenarbeit

- Wissenstransfer national/international
- Einmaliger Aufbau der Infrastruktur
- Übersicht der Kosten gewährt / Budget

Vorteile

- Forensics Tools sind bekannt / Support gewährt
- Services verfügbar wenn benötigt
- Anwendung bewährter Methoden

Zusammenfassung

- Einfacher Zugang zum Service mit bewährten Methoden
- Abdeckung von Lastspitzen dank Ressourcen Sharing
- Persönliche Forensik Workstations erlauben individuelle SW Installationen
- Wissenstransfer und Synergien durch Zusammenarbeit
- Ermöglich den Zugang zu weiteren forensischen Anwendungen
- «Storage aaS» als Speichermodell
- Der Service ist gesichert und Audit fähig

Roadmap

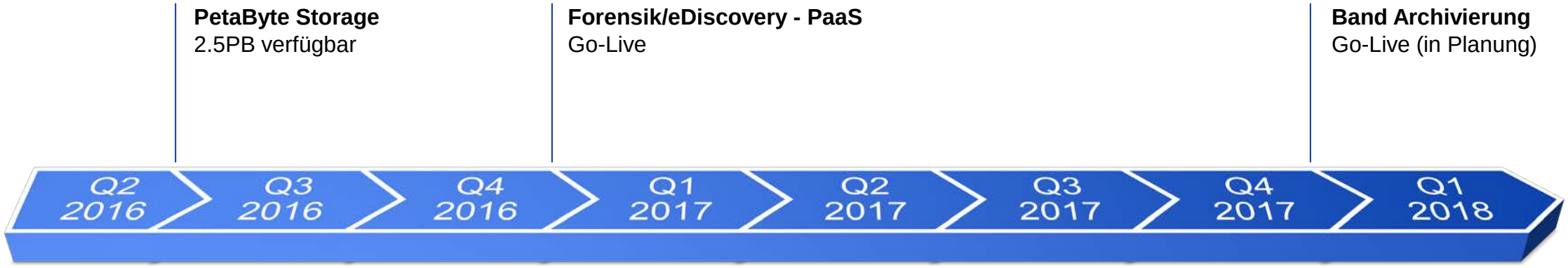
Kantonspolizei Zürich

Nächste Schritte

Ausbau des PetaByte Storage Systems (2.5PB verfügbar)

Go-Live des Forensik/eDiscovery Services

Go-Live der Band Archivierung (in Planung)



Kantonspolizei Zürich

abraxas

Besten Dank für Ihre Aufmerksamkeit

Abraxas Informatik
AGWaltersbachstrasse
5CH-8006 Zürich

www.abraxas.ch