Digitaler Nachlass

Gedanken zu einer technischen Lösung

L//P

Zürich, 10. Oktober 2019

Inhalt

1. Beispiele
2. Problemstellung
3. Architektur
4. Sicherheitskonzept
5. Flow-Chart
6. Defintionen
7. Verschlüsselungskonzept
8. Angriff Vektoren
9. Verbesserungspotenzial

Notfallplan

Digitale, finanzielle und persönliche Hilfe

Die Zurich Versicherung springt ein, wenn der Unternehmer oder die Unternehmerin ausfällt, sodass aus einer persönlichen Krise, einem Unfall oder Todesfall kein Konkurs wird und mit dem Wissen und der Erfahrung auch noch unnötig Arbeitsplätze verloren gehen. Das Angebot besteht aus den Komponenten:

- Digitaler Notfallplan
- Persönliche Unterstützung durch Krisenspezialisten
- Versicherbare Kapitalleistungen zur Überbrückung

Dadurch bleibt das Unternehmen jederzeit handlungsfähig, ein kleiner Unfall kann nicht mehr zur Zerstörung ganzer Firmen führen.

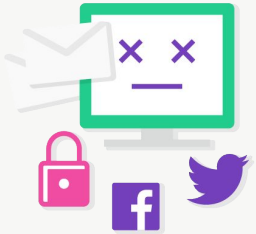
Tooyoo in Kürze

Unterstützen Sie Ihre Liebsten auch bis nach Ihrem Tod

Der Tod eines Angehörigen ist oft mit einer grossen Hilflosigkeit verbunden. Zur Trauer gesellen sich zahlreiche administrative Herausforderungen. Tooyoo ist eine digitale Plattform zur sicheren

Aufbewahrung der letzten Wünsche von verstorbenen Angehörigen.

Schritt für Schritt ermöglicht die Plattform die Abwicklung administrativer und organisatorischer Aufgaben nach einem Todesfall – beruhigend, einfach und intuitiv.

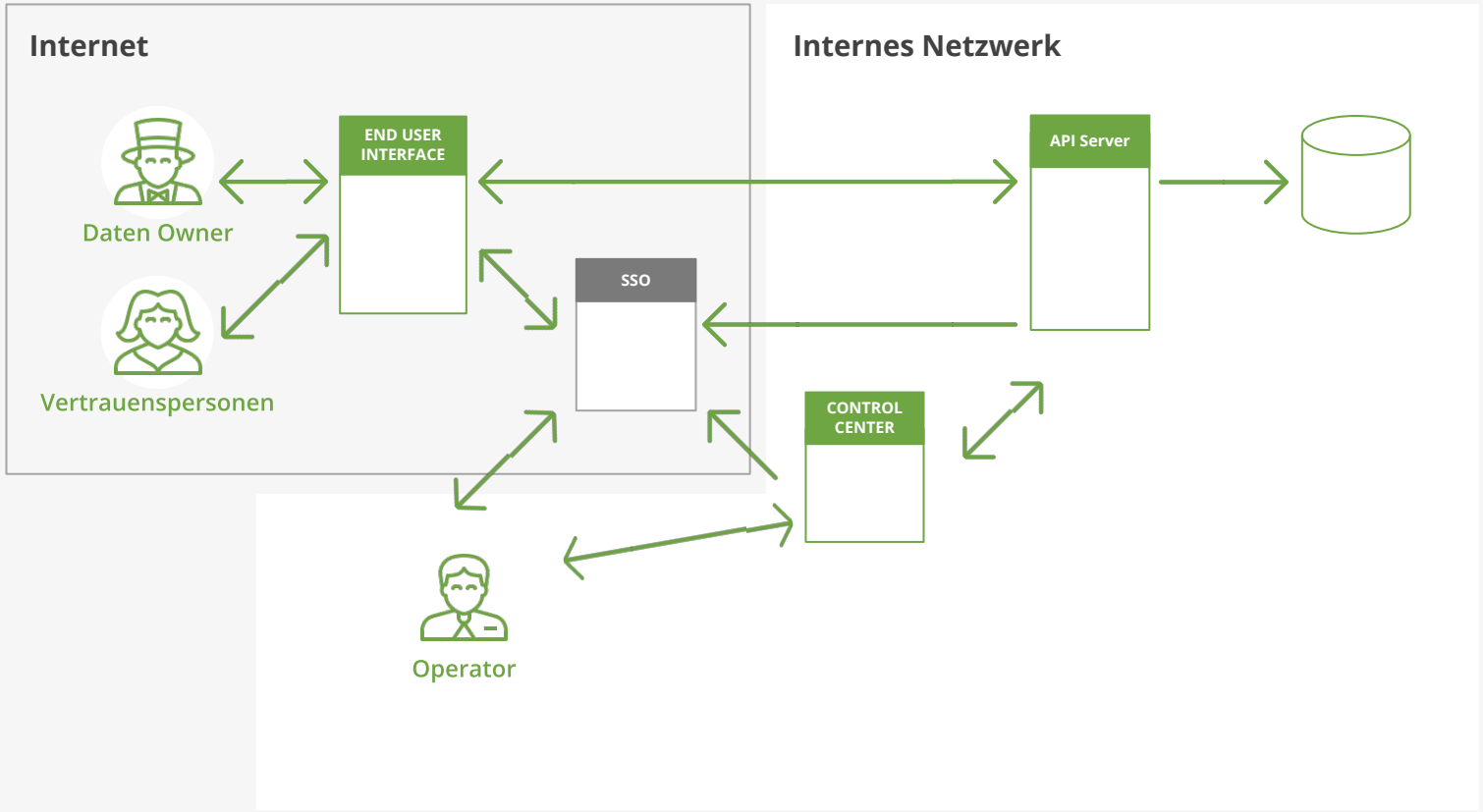


Problemstellung

Datenbereitstellung an Vertrauenspersonen bei spezifischen Szenarien.

- Daten Owner will bei Eintreten bestimmter Szenarien Datenpakete Vertrauenspersonen zugänglich machen
- Szenarien sind in der Regel solche, wo der Daten Owner nicht mehr selber fähig ist, das Datenpaket weiter zu geben (Unfall, Tot ..)
- Operator ist zustaendig das Eintreten des Szenario zu überprüfen und den Zugriff auf das Datenpaket für die Vertrauensperson freizuschalten
- Vertrauensperson bekommt also erst wenn das Szenario eingetreten ist Zugriff auf die Daten
- Die Herausforderung: Wie können die Daten abgesichert werden?

Architektur



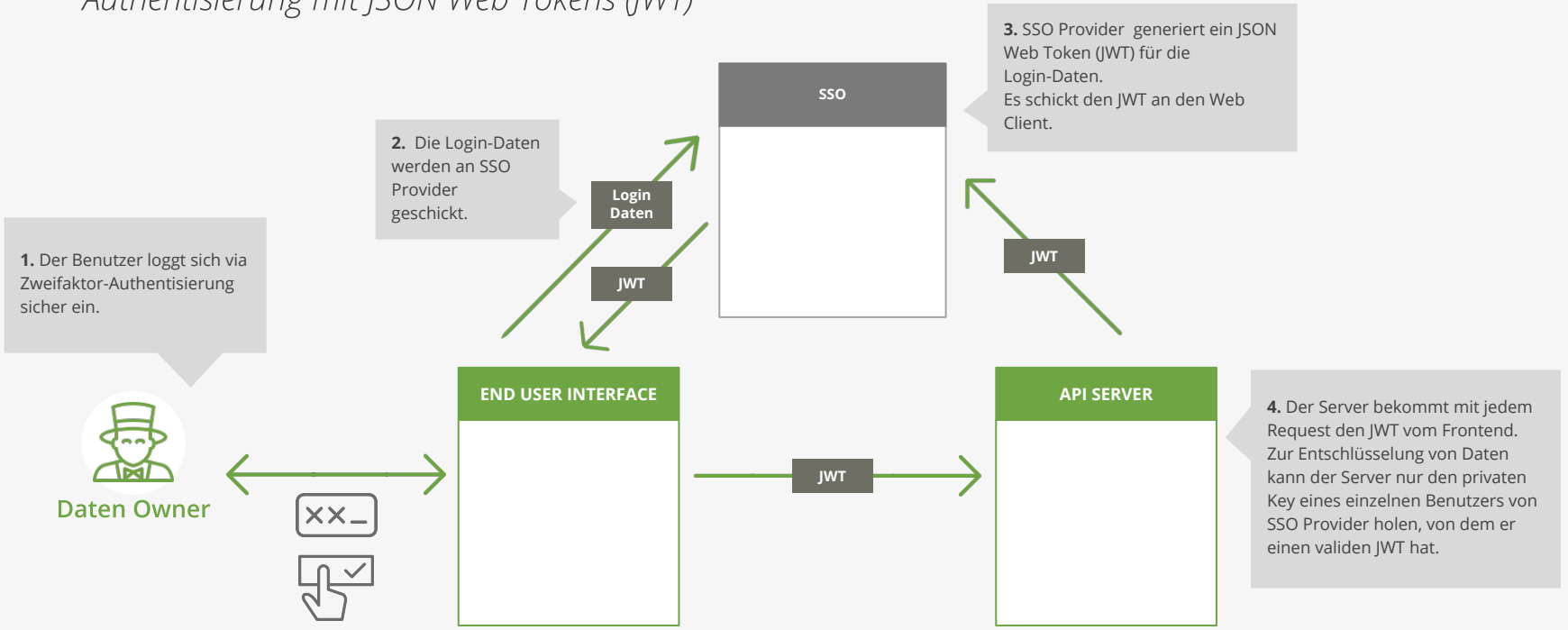
Sicherheit

Höchste Sicherheit ohne Usability-Abstriche

- Sichere Authenthisierung dank JSON Web Tokens
- Kombination aus asymmetrischer und symmetrischer Verschlüsselung sämtlicher Daten (RSA + AES)
- Private Schlüssel werden vom System verwaltet, damit die Benutzer sie nicht selber weitergeben müssen
- Zweifaktor-Authentifizierung mit SSO (SMS etc)
- 100% HTTPS, auch im internen Verkehr

Flow-Chart

Authentisierung mit JSON Web Tokens (JWT)



Definitionen

Symmetrische Schlüssel

- Bei symmetrischen Verschlüsselungsverfahren gibt es nur einen einzigen Schlüssel.
- Dieser Schlüssel ist für die Verschlüsselung, als auch für die Entschlüsselung zuständig.
- Da Schlüsselübergabe umständlich ist, bedient man sich in der Praxis häufig dem Prinzip der Hybridverschlüsselung, bei der man neben der symmetrischen Verschlüsselung auf die asymmetrischen Verschlüsselung zurückgreift.
- Beispiele: VPN nach Aufbau der Verbindung

Definitionen

Asymmetrische Schlüssel

- Bei einem Asymmetrischen Verschlüsselungsverfahren (auch Public-Key-Verfahren genannt), gibt es zwei Schlüssel.
- Dieses sogenannte Schlüsselpaar setzt sich aus einem privaten Schlüssel (Privater Schlüssel -> Private Key) und einem öffentlichen Schlüssel (nicht geheim -> Public Key) zusammen.
- Mit dem privaten Schlüssel, werden Daten Entschlüsselt oder eine digitale Signatur erzeugt.
- Mit dem öffentlichen Schlüssel kann man Daten verschlüsseln und erzeugte Signaturen auf ihre Authentizität überprüfen.
- Beispiele: PGP / SSH / SSL

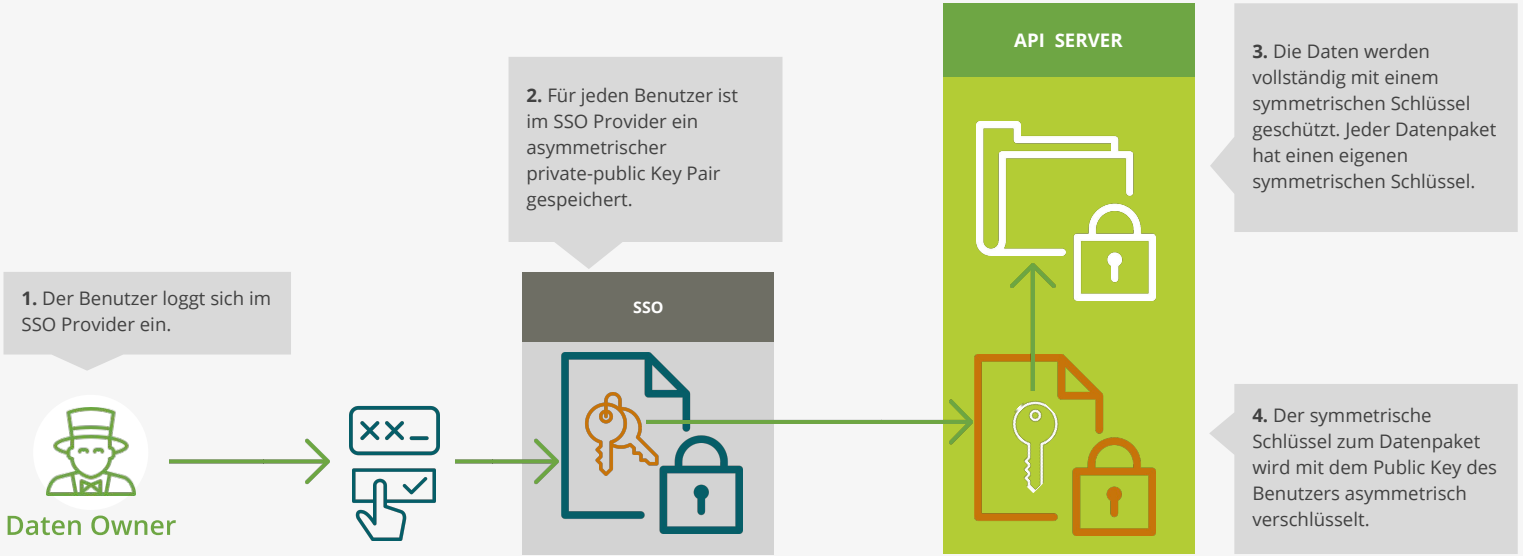
Definitionen

Two-Factor Authentication / 2FA, Multi-Factor Authentication / MFA

- Bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier (oder mehr) unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren)
- Beispiele: Geldautomaten (Karte + PIN), TAN Verfahren

Verschlüsselungskonzept

Asymmetrische und symmetrische Verschlüsselung kombiniert (RSA + AES)



Angriff Vektoren

Private Key auf dem Server

- Private Key jeder aktiven Session ist im Memory auf dem Server
- Operator hat Zugriff auf alle Private Keys im SSO Provider

Vorteil:

- Operator kann Daten Recovery bei Passwortverlust ausführen
- Datenzugriff bei Behördenanfragen möglich

Nachteil:

- Daten auch für andere Personen als Daten Owner und Vertrauensperson möglich

Verbesserungspotenzial

Entschlüsseln der Daten im Browser

- Private Key bleibt im Besitz des Daten Owner bzw. Vertrauensperson
- Kopien der Symmetrischen Schlüssel werden direkt bei Definition der Vertrauensperson mit dem jeweiligen Public Key erstellt

Vorteil:

- Operator hat keinen Zugriff auf die Daten

Nachteil:

- Daten Owner bzw. Vertrauensperson eventuell mit Verwaltung des Private Key überfordert
- Gefahr von Datenverlust wenn Private Keys verloren sind

Fragen

Sicherheit vs. Ease of Use?

- Darf Sicherheit reduziert werden um die Benutzung zu vereinfachen?
- Muss Sicherheit reduziert werden um Benutzerfehler zu verhindern?
- Werden sich die Antworten auf diese Fragen ändern mit steigender Medienkompetenz der Gesellschaft?

Danke für Ihre Aufmerksamkeit

Ihr Kontakt:

Lukas Kahwe Smith
@lsmith
lukas.smith@liip.ch