AMT FÜR INFORMATIK
FÜRSTENTUM LIECHTENSTEIN

Sicheres IAM für Bürger & Juristische Personen

Christine Wohlwend / externe Projektleiterin im Auftrag des Amt für Informatik (AI)
Liechtensteinische Landesverwaltung
15. Februar 2024

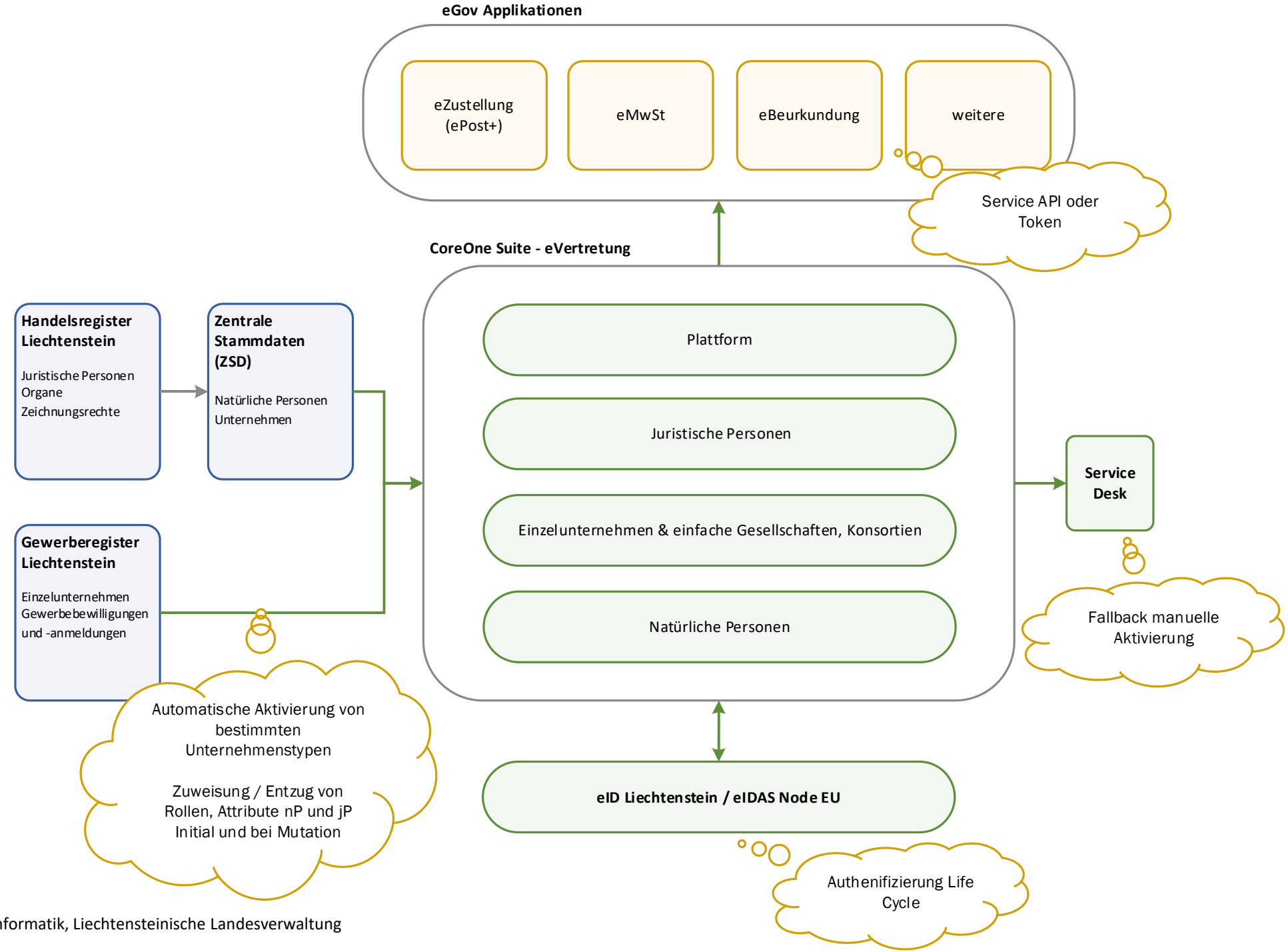
Was ist ein sicheres IAM?

- Die «**technische**» Sicherheit wird von den Stakeholdern **vorausgesetzt**!

- **Authentifizierungsmechanismen:** Verwendung starker Authentifizierungsverfahren (z.B. Multi-Faktor-Authentifizierung) zur Sicherstellung, dass nur **autorisierte Benutzer** auf das System zugreifen können.

  eID Liechtenstein

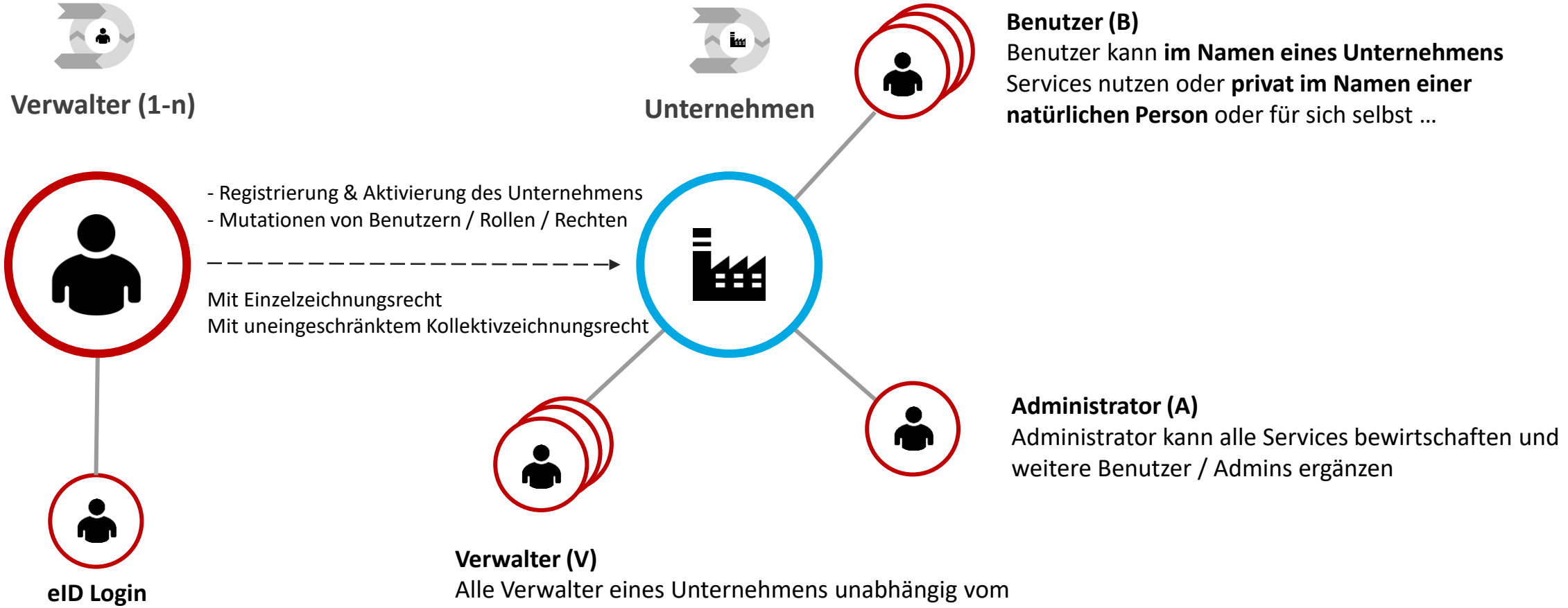
- **Autorisierungs- und Zugriffskontrollen:** Feingranulare Zugriffskontrollmechanismen, die sicherstellen, dass Benutzer nur auf die Daten und Funktionen zugreifen können, für die **sie berechtigt sind**, basierend auf ihrer Identität, Rolle und den geltenden Richtlinien.
- **Management des Identitätslebenszyklus:** Prozesse und Werkzeuge zur Verwaltung des gesamten **Lebenszyklus** einer Identität, von der Erstellung über die Aktualisierung bis hin zur Deaktivierung oder Löschung, um sicherzustellen, dass die Daten zu jeder Zeit aktuell und korrekt sind.
- **Integration und Synchronisation mit Umsystemen:** Mechanismen zur Integration und Synchronisation mit anderen Systemen und Datenquellen, um einerseits Daten zentral ins IAM einzuspeisen und Berechtigungen / Rollen i.S. Compliance zentral vom IAM an Umsysteme bereitzustellen.


eGov Applikationen
eZustellung (ePost+)
eMwSt
eBeurkundung
weitere
Service API oder Token
CoreOne Suite - eVertretung
Handelsregister Liechtenstein
Juristische Personen
Organe
Zeichnungsrechte
Zentrale Stammdaten (ZSD)
Natürliche Personen
Unternehmen
Gewerberegister Liechtenstein
Einzelunternehmen
Gewerbebewilligungen und -anmeldungen
Plattform
Juristische Personen
Einzelunternehmen & einfache Gesellschaften, Konsortien
Natürliche Personen
Service Desk
Fallback manuelle Aktivierung
Automatische Aktivierung von bestimmten Unternehmenstypen
Zuweisung / Entzug von Rollen, Attribute nP und jP Initial und bei Mutation
eID Liechtenstein / eIDAS Node EU
Authenifizierung Life Cycle

Autorisierung- und Zugriffskontrollen

- **Wer ist befugt, Benutzern eine Identität und eine Rolle zuzuweisen?**
  - (A) Uneingeschränkt von Gesetzes wegen: Die Organe einer juristischen Person: z.B. Verwaltungsrat, Geschäftsleitung, der Vertreter einer Einzelunternehmung / einfachen Gesellschaft: Inhaber bzw. Einzelunternehmer, Gesellschafter der einfachen Gesellschaft.
    - Übersetzt ins «IAM»: Verwalter, die «digitale Vollmachten» ausstellen dürfen, Rollen und Berechtigungen erteilen und entziehen dürfen, sowie «Generalbevollmächtigte» i.S. von Administratoren ernennen dürfen.
  - (B) Eingeschränkt durch die obigen Vertreter bezeichnete Personen: Prokuristen, Bevollmächtigte.
    - Übersetzt ins «IAM»: Administratoren, die bevollmächtigt werden, Rollen und Berechtigungen zu erteilen sowie Benutzer, die für bestimmte Services befugt sind.

Aktivierung und Bewirtschaftung

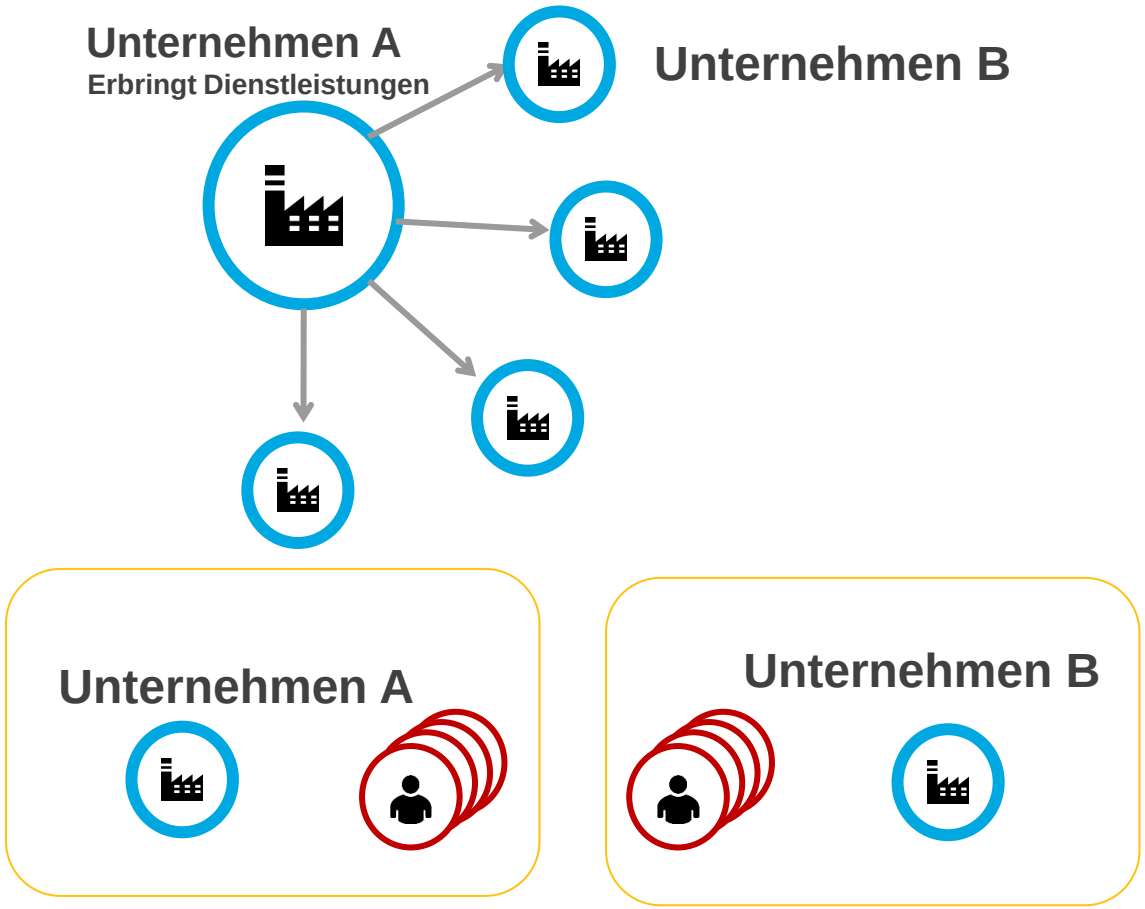


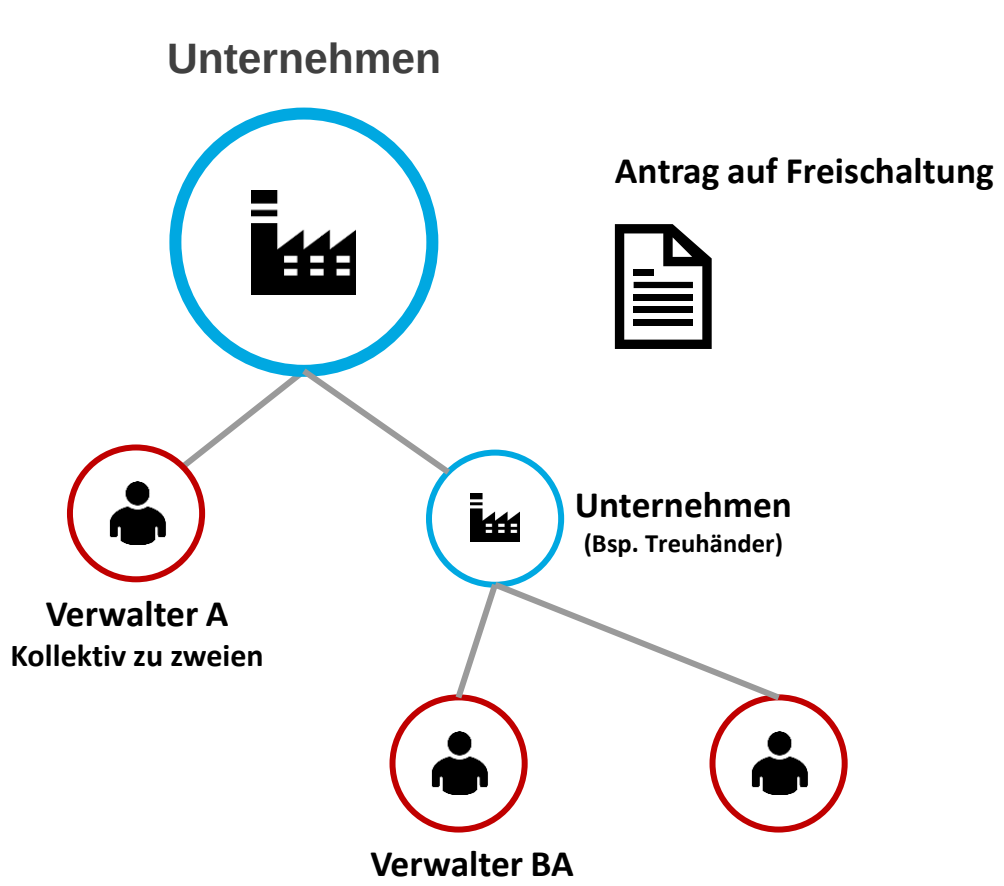
Benutzer (B)
Benutzer kann **im Namen eines Unternehmens** Services nutzen oder **privat im Namen einer natürlichen Person** oder für sich selbst …

Administrator (A)
Administrator kann alle Services bewirtschaften und weitere Benutzer / Admins ergänzen

Verwalter (V)
Alle Verwalter eines Unternehmens unabhängig vom Zeichnungsrecht nach der Aktivierung
Mutation von Benutzern / Rollen / Rechten

Edge Cases – was wird unterstützt?





Management des Identitätslebenszyklus

- **Des Unternehmens**
  - Eintragung im Handelsregister, Mutationen und Austragung / Löschung erfolgt zentral mit Übergabe an das IAM.
    - Automatischer Abgleich von : Unternehmens-Identifikator (PEID), Name, Rechtsform
    - Je nach Status des Unternehmens werden unterschiedliche Prozesse im IAM angestossen (Aktualisierung der Vertreter, Löschung, Archivierung)

- **Des Verwalters / Organs eines Unternehmens**
  - Eintragung, Mutationen und Austragung / Löschung erfolgt zentral mit Übergabe an das IAM.
    - Automatischer Abgleich von: Personen-Identifikator (PEID), Name, Organfunktion inkl. Zeichnungsrecht
    - Prozesse bei «ist gelöscht» werden im IAM angestossen zur Entfernung der Person im IAM

- **Des Administrators / Benutzers**
  - Regelmässige Überprüfung der Rollen / Berechtigungen wird erzwungen
  - Bei Wegfall einer eID (Tod, Deaktivierung und Abmeldung): Bereinigung des Benutzers im IAM

Identitätslebenszyklus – Edge Cases

- **Des Unternehmens**
  - Massenaktivierungen vs. Self-Service Portal (z.B. Treuhänder)
  - «in Gründung» – bis zu «gegründet»: Ohne Gründung keine zentrale Verwaltung

- **Des Verwalters / Organs eines Unternehmens**
  - Keine Verwalter verfügbar (Demissionierung, Tod)
    - Was passiert mit dem Unternehmen?
    - Was passiert mit den Serviceberechtigungen der Mitarbeiter?

- **Und viele mehr …**

Integration von Umsystemen – die Services

- **Welche Möglichkeiten gibt es?**
  - Es wurden verschiedene Anbindungsvarianten erarbeitet und bewertet
- **Welche wollen wir?**
  - Von den Anbindungsvarianten wurden **zwei** als Standardvarianten definiert (API, Token-basiert über COS/eID.li)
  - Welche Anbindungsvariante eines Services jeweils umgesetzt wird entscheidet das AI je Projekt einer frühen Konzeptphase
  - Der Entscheid zur Anbindung führt zur Auslieferung von Standard-Onboarding-Informationen
- **Das Onboarding**
  - Integration **Guide eVertretung** für die Lieferanten / Beschreibung der Lösung sowie Anbindung generisch
  - Je nach Variante eine vollständige **Postman-Collection** zum Testen der Anbindung / technisch
  - Ein Standardset an **Testdaten** inkl. Fragenkatalog zum Onboarding
  - Welche Rollen und Rechte gibt es überhaupt? Soll eine bestimmte Gruppe von Benutzern eine Rolle systemseitig zugewiesen bekommen? Soll der Service nur für bestimmte Benutzertypen sichtbar sein?)

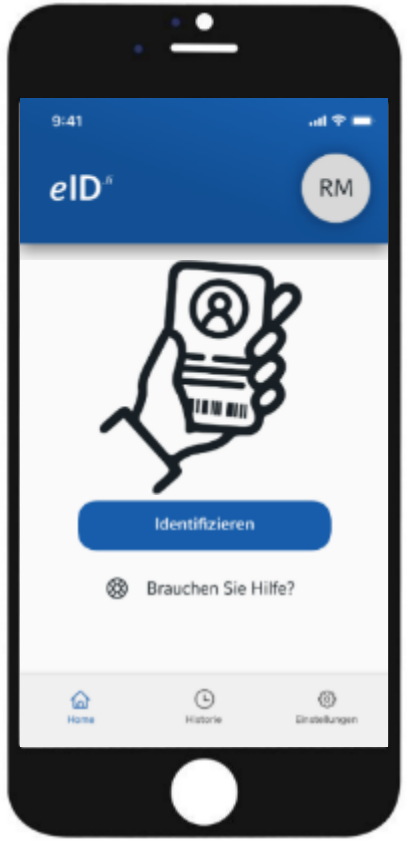
- COS Postman TEST
  - Authentication (Token Endpunkt)
    - POST Service Account Permission API
    - POST eID
  - Person
    - GET Suchen der Person anhand der PEID
    - GET Laden der Unternehmungsverbindungen einer Person
  - Unternehmen
    - GET Suchen eines Unternhemen andhand der PEID
    - GET Alle aktiven Unternehmen
    - GET Alle gelöschten Unternehmen
    - GET Laden der Unternehmungsverbindungen eines Unternehmen
  - Permission API
    - GET Wer repräsentiert den Angegebenen Benutzer in der Applikation
    - GET Wer repräsentiert die angegebene Organisationseinheit
    - GET Wer wird vom angegebenen Benutzer repräsentiert
  - User
    - GET Suchen eines Benutzers anhand der PEID
    - GET Suchen der PEID anhand der Benutzer-ID

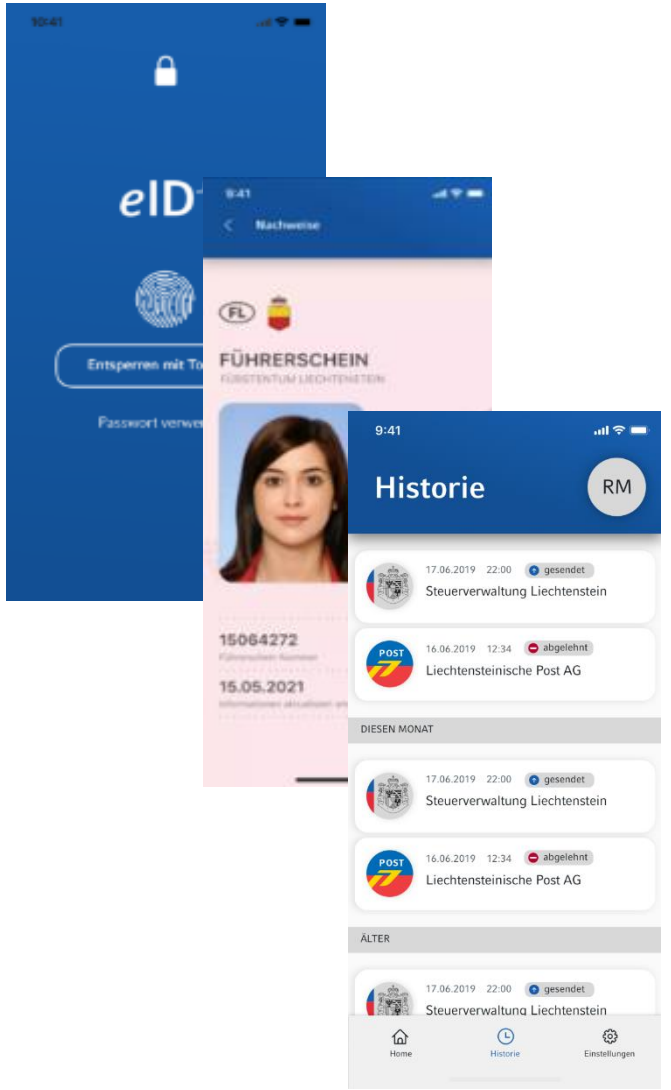

```
{
    "$type": "iTsense.CoreLogin2.Server.API.Models
    "userName": "1800889",
    "userId": 82,
    "userEmail": "romy.frommelt@llv.li",
    "role": "Stellvertreter",
    "application": "ezustellung",
    "contextType": "OrganizationUnit",
    "contextObjectIdentifier": "1890"
},
{
    "$type": "iTsense.CoreLogin2.Server.API.Models
    "userName": "1800891",
    "userId": 84,
    "userEmail": "katharina.kaiser@llv.li",
    "role": "Stellvertreter",
    "application": "ezustellung",
    "contextType": "OrganizationUnit",
    "contextObjectIdentifier": "1890"
},
{
    "$type": "iTsense.CoreLogin2.Server.API.Models
```

Unsere Authentifizierung: eID.li

Kerninformationen

- Download über App-Store
- Aktivierbar über persönliches Erscheinen (Ausländer- und Passamt-Schalter) oder Videoidentifikation
- Übersichtlich und aufgeräumt
- Historie über getätigte Logins und Weitergaben von Personendaten
- Verwaltung über die Liechtensteinische Landesverwaltung
- eIDAS notifiziert





Demo