**Glossar**

Instances

|  |  |
| --- | --- |
| Issuers | Die Instanz die die Daten ausstellt |
| Holders | Die Instanz die die Daten besitzt |
| Verifiers | Die Instanz die die Daten anfordert |

[More](https://w3c.github.io/vc-data-model/#ecosystem-overview)

**Fragen**

* Wie kann ich mein “Recht auf vergessen werden” ausüben der Verbindung zwischen publicKey und meiner Identität

**Projektideen**

* Trusted Web mit DIDs
* Implementierung eines Agents und eines Wallets
* E-Mail Client der SSI Authentifizierung beinhaltet

**Praktische Probleme mit SSI:**

* Wie geht man mit Schlüsselverlust um? Wie kann ich mich authentifizieren wenn mein Schlüssel verloren gegangen ist? E-Mail Authentifizierung?
* Wenn ich meine publicKeys bekomme indem ich nach der DID suche... Soll man dann alle DIDs durchsuchen? Entweder man gibt den DIDs eine Regel um sie schneller zu durchsuchen ODER man übergibt immer direkt publicKeys

**Konzeptnotizen:**

PKE = Private key encrypted

Verbindung von Server und lokaler Identität. Anstatt den gesamten privateKey auf dem eigenen Rechner zu speichern könnte ein Teil von PKE auf einem Server gespeichert werden (dieser kann mit dem Teilschlüssel alleine nichts anfangen). Dieser kann dann zusammen mit dem lokal gespeicherten Teil entschlüsselt und für die Signatur verwendet werden. => Nur im Moment des Verschlüsselns ist der key jemals komplett „sichtbar“. Es wird nie vom Benutzer eingesehen oder eingegeben. (Gegen Phishing)  
  
Insgesamt sollte dadurch selbst bei einer Komprimierung des lokalen Rechners oder des Servers die Schlüssel weiterhin sicher sein.

Logischerweise sollte man seinen Schlüssel daraufhin verändern. => Instanz die diese Schlüsselveränderungen verifiziert und aufzeichnet sodass andere Instanzen den alten Schlüssel verwerfen und nur noch den neuen akzeptieren.

Agent beinhaltet dadurch sowohl Aufgabe des schützen des Wallets als auch die Kommunikation mit dem remote-Teil des Schlüssels

**Problem: Wie authentifiziert man sich beim Server???**

Dieser Server könnte durch Passwort geschützt werden?

**Signaturen in der Mail:**Signatur der Uni bestätigt, dass PublicKey des Absenders Teil der Universität bzw. eines bestimmten Uniteilbereichs ist.

Signatur des Absenders bestätigt, dass die Mail vom PrivateKey welcher zum von der Universität verifizierten PublicKey signiert wurde

Mail selbst wurde mit dem PublicKey des Empfängers verschlüsselt und kann nur mit dessen privateKey entschlüsselt werden

**Beim Senden einer Mail muss der publicKey des Empfängers bei der Uni angefragt werden!**

Der Benutzer sollte vielleicht in der Lage sein, das Schlüsselpaar zu Beginn einmalig selbst zu generiern. Daraufhin würde er den publicKey an die Universität senden. Dadurch könnte man sicherstellen, dass der privateKey nie an eine Instanz weiter gegeben wird.

Jeder Student/Mitarbeiter/Mensch m bekommt eine DID zugeordnet. m bekommt ein VC von der Universität aus gestellt. Mit diesem kann jede andere Instanz die Rolle von m verifizieren.

Den publicKey kann man online einsehen. Kollektive Seite aller Unis für publicKeys

Alternativ zum bestehnden Vorgang die emailAdressen in VC einzubinden könnte man auch DIDs erzeugen und der Uni einen Service hinzufügen, welcher einem zu jeder Mail-Adresse eine DID zurückgibt. (Nachteil: Uni wäre bottle neck)