Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz

E-ID-Partizipation Online-Meeting

2. Juni 2022

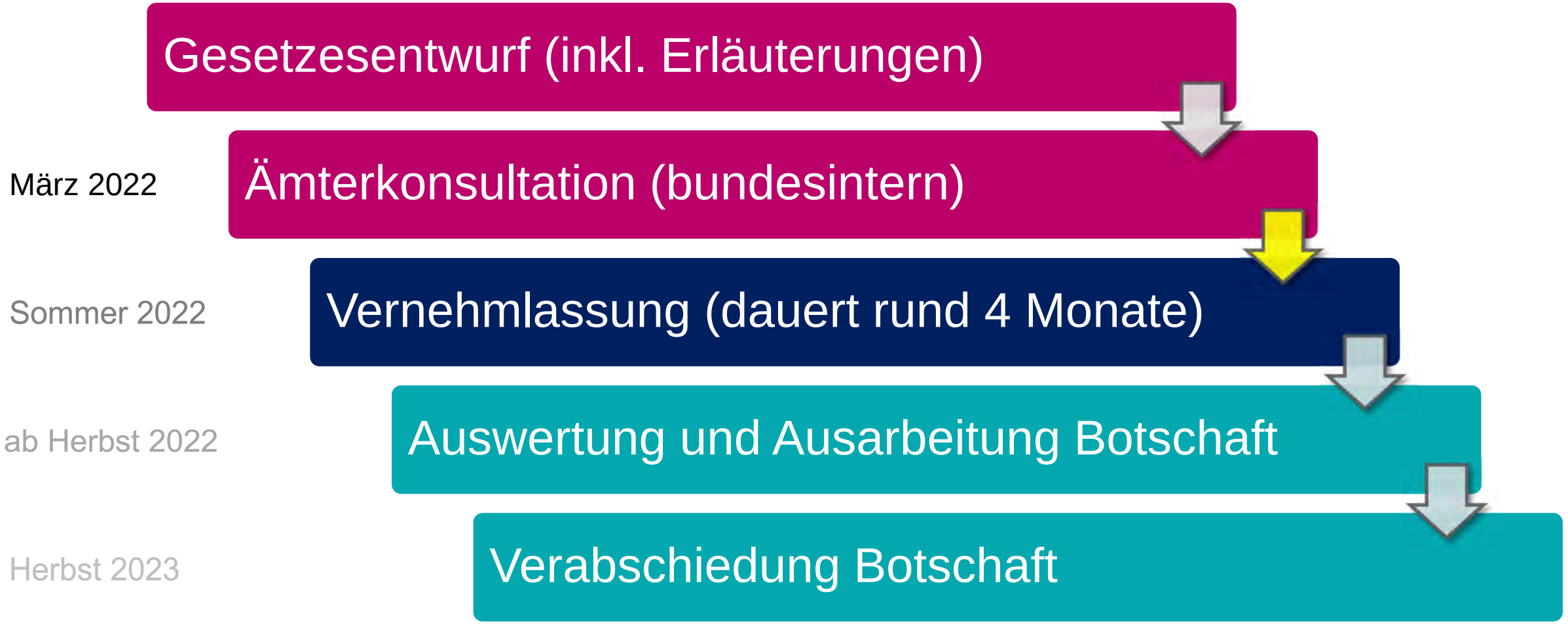
Agenda

1. Begrüssung & Ablauf
2. Informationen zur Vernehmlassung und der Rolle der GitHub-Plattform
3. Präsentation Datakeeper
4. Point de situation «GitHub»
5. Call for Entries «Business/Verifikatorinnen»
6. Varia – Inputs aus dem Plenum

Informationen zur kommenden Vernehmlassung

- Alle Beteiligten arbeiten unter Zeitdruck und sind engagiert, um den Zeitplan einzuhalten
- Alle Stellungnahmen und Hinweise aus der bundesinternen Ämterkonsultation dienen der gemeinsamen Weiterentwicklung des Vorentwurfs
- Benachrichtigung aller Adressaten der E-ID-Mailingliste nach Eröffnung der Vernehmlassung

Aktueller Stand Gesetzgebung



Rolle von GitHub bei der Vernehmlassung

GitHub

- Dient der Information und Diskussion für
- Fragen stellen möglich, Antworten vom E-ID-Team
- Inputs werden wahrgenommen, haben aber keine formale Wirkung

Vernehmlassung

- Formale Stellungnahme, Wirkung hängt vom politischen Gewicht der Verfasserin ab
- Systematische Auswertung

Weder Beiträge auf GitHub noch formale Stellungnahmen bedeuten ein Recht auf Umsetzung der Forderungen im Gesetzesentwurf

Was ist eine Vernehmlassung?

- Die Vernehmlassung ist ein **formal geregelter Prozess**
- Eine Vernehmlassung dient dazu, interessierte Kreise **vor** der parlamentarischen Debatte an der Formulierung des Gesetzesentwurfs zu beteiligen
- Es gibt **keine Einschränkung** hinsichtlich des Kreises, der an der Vernehmlassung teilnehmen kann
- Alle eingereichten Vernehmlassungen werden durch den Bund **publiziert**
- Auf Basis der eingereichten Vernehmlassungen wird ein **Bericht** zuhanden des Bundesrats verfasst, auch dieser wird veröffentlicht
- Ein **Recht** auf die Umsetzung von Forderungen, die via Vernehmlassung gemacht werden, **besteht nicht**

Welche Rolle spielt GitHub bei der Vernehmlassung?

- GitHub dient – wie bis anhin – als **Informations- und Diskussionsplattform** der E-ID-Community
- Es können **alle E-ID-relevanten Fragen** auf GitHub diskutiert werden, auch Fragen rund um den Vorentwurf des neuen Gesetzes
- Das **E-ID-Projektteam** nimmt – wie bis anhin – alle GitHub-Beiträge zur Kenntnis und wird wenn möglich auf diese auf GitHub reagieren
- Aber: **Einträge auf GitHub gelten nicht als Vernehmlassungen**
- Community kann eine gemeinsame Stellungnahme einreichen – natürlich können auch individuelle Stellungsnahmen formuliert werden

Rolle von GitHub bei der Vernehmlassung

GitHub

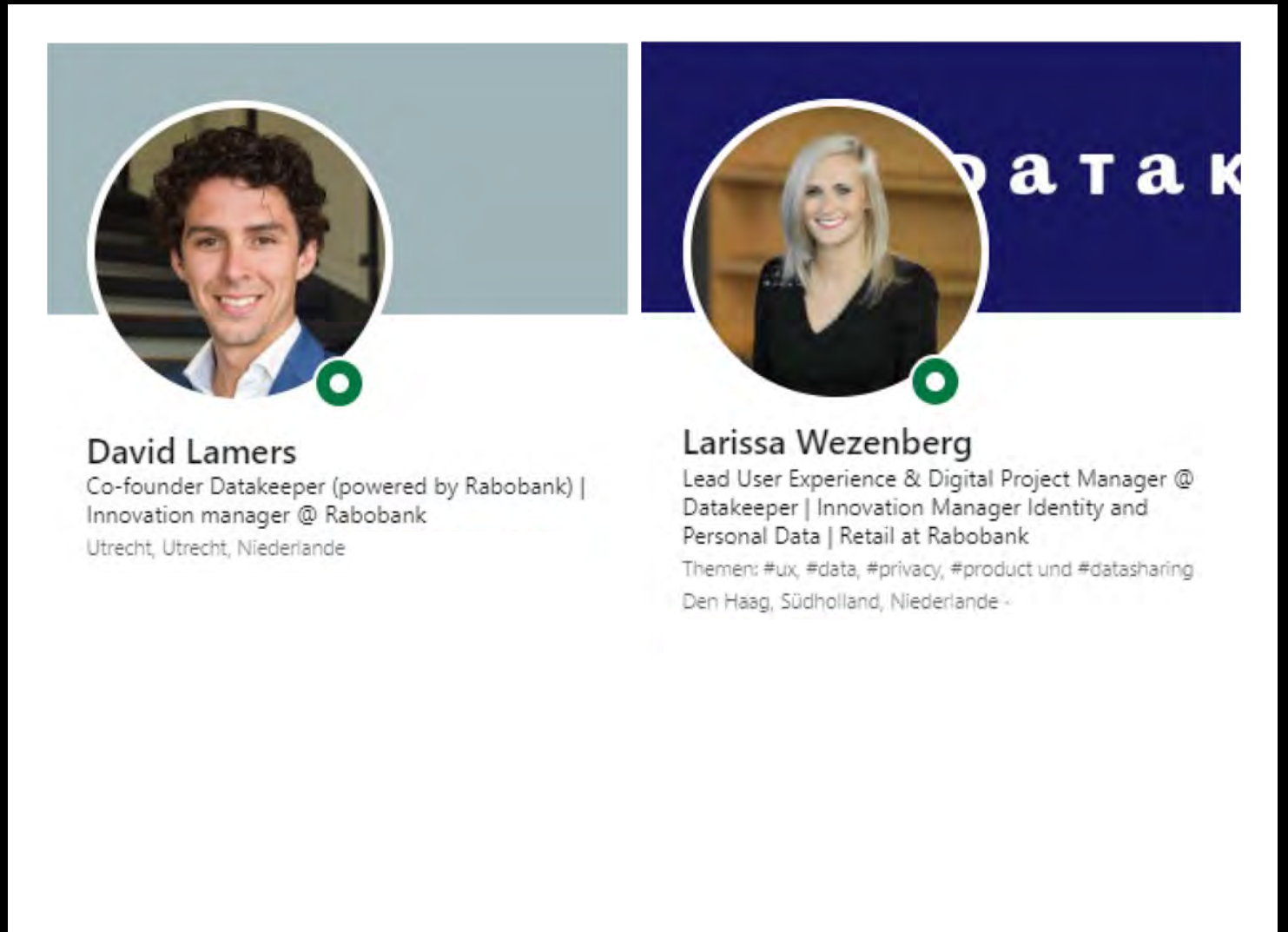
- Dient der Information und Diskussion für
- Fragen stellen möglich, Antworten vom E-ID-Team
- Inputs werden wahrgenommen, haben aber keine formale Wirkung

Vernehmlassung

- Formale Stellungnahme, Wirkung hängt vom politischen Gewicht der Verfasserin ab
- Systematische Auswertung

Weder Beiträge auf GitHub noch formale Stellungnahmen bedeuten ein Recht auf Umsetzung der Forderungen im Gesetzesentwurf

Input-Referat: Datakeeper (NL)



Point de situation «GitHub»

Was ist die E-ID?

- **Die E-ID ist der staatliche, digitale Ausweis der Schweiz**, mit welchem die eigene Identität nachgewiesen werden kann – sowohl in der analogen wie auch in der digitalen Welt
- **Die E-ID wird weder ID-Karte noch Pass ersetzen**, im Gegenteil: Ausweisdokumente bilden die Basis zur Ausstellung und dem Erhalt einer E-ID
- **Login?** Anwendung der E-ID als Zugangsmittel möglich!
- **Verknüpfung** mit allen anderen digitalen Nachweisen?
  Digitale Nachweise *können* logische oder technische Verknüpfungen untereinander haben, genauso aber alleinstehend in einer Wallet geführt werden

Vorbehalte zur SSI-Stossrichtung

- Technologieneutrale Gesetzgebung,
  gewisse Architekturvorstellung sind aber unumgänglich

- Faktor Zeit: Lösung für morgen, nicht heute
- Synchron mit Entwicklungen in der EU
- Konzentration auf Stossrichtung SSI im Sinne von Maximallösung und zum Ausloten des technisch Machbaren

Sicherheitsaspekte

- Sicherheit des Wallets
  - Secure elements (SE, TEE, Hardware-Krypto-Elemente)
  - Sicherheit vs. Portabilität/Backup
- Sicherheit bei Übermittlung und Überprüfungen
  - Man-in-the-Middle-Angriffe
  - Phishing-Angriffe

Wie sicher ist sicher genug?

- Sicherheit ↔ Benutzerfreundlichkeit
- Level of Assurance «high»: 0 Use Cases

Datenschutz

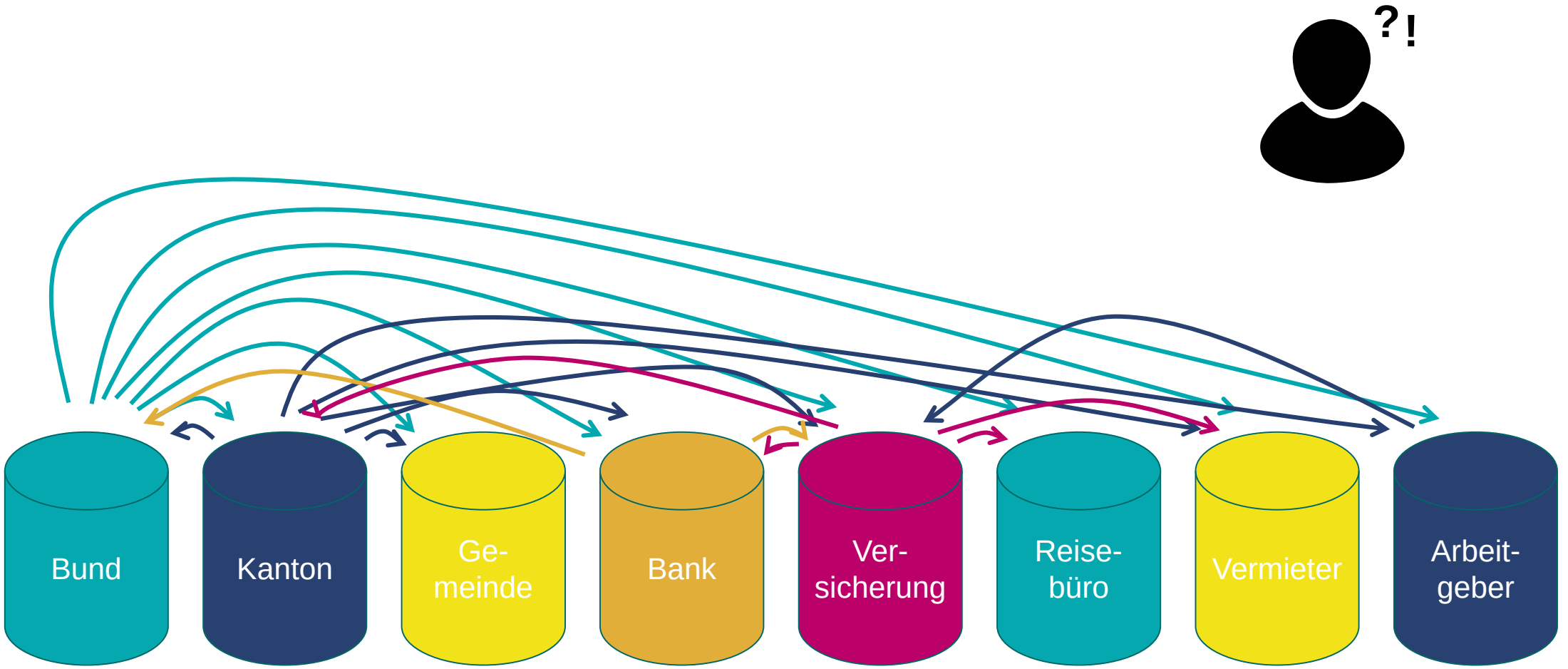
- Risiko Globaler Identifikator?
  - AHV-Nummer als Identifikator für Behörden → Gesetz erlaubt
  - AHV-Nummer für Private nicht erlaubt → Gesetz verbietet
- Datenschutzaspekten wird ein hohes Gewicht gegeben (Forderungen Motionen)
- Datenschutzgrundlage des Ökosystems: neues Datenschutzgesetz (nDSG)
- Aspekt Zertifizierung ebenfalls mittels nDSG abgedeckt
- Macht-Asymmetrie Benutzer ↔ Verifikatorin

- Zero-Knowledge-Proof und Selective Disclosure versprechen Mehrwert

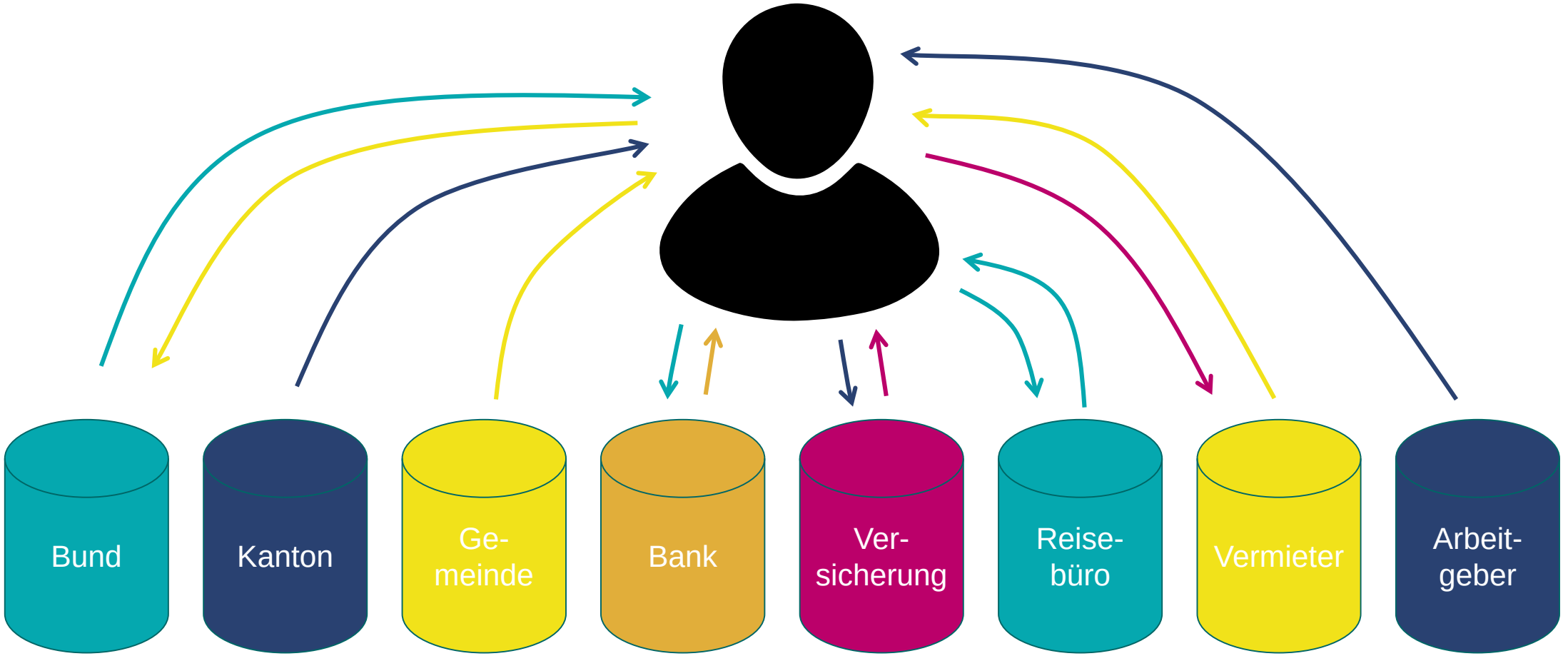
Mehrwert Ökosystem

- E-ID zum Fliegen bringen – «alltäglich nutzbare» digitale Nachweise als Treiber
- Gemeinsames «Framework zur Bewirtschaftung» digitaler Nachweise
- Vereinheitlichung von Flows und UX
- Vereinheitlichung und Standardisierung von digitalen Nachweisen: Maschinenlesbarkeit und Semantik für eine effiziente Digitalisierung und die Ermöglichung neuer Dienstleistungen im Sinne einer digitalen Transformation

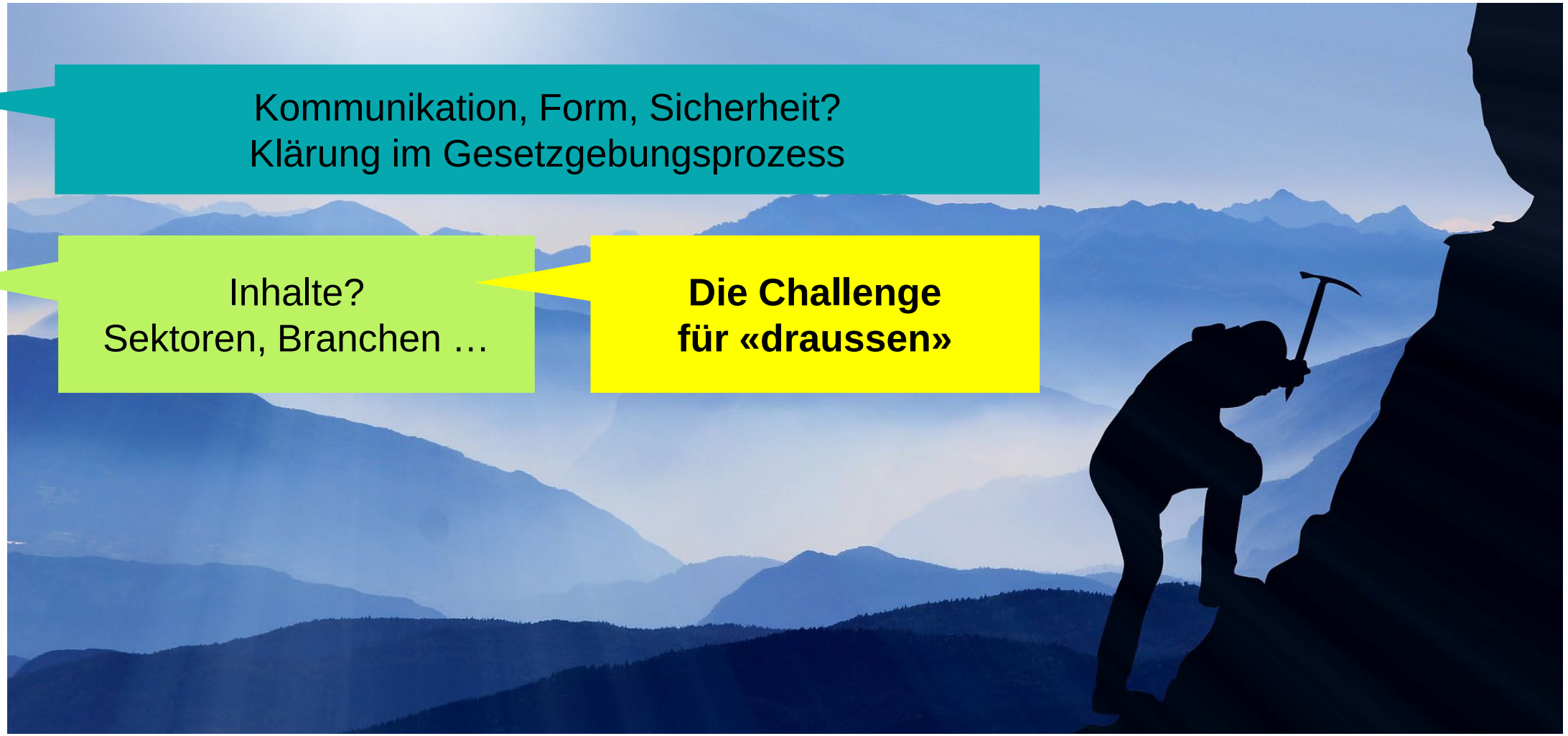
Digitale Nachweise – Heute



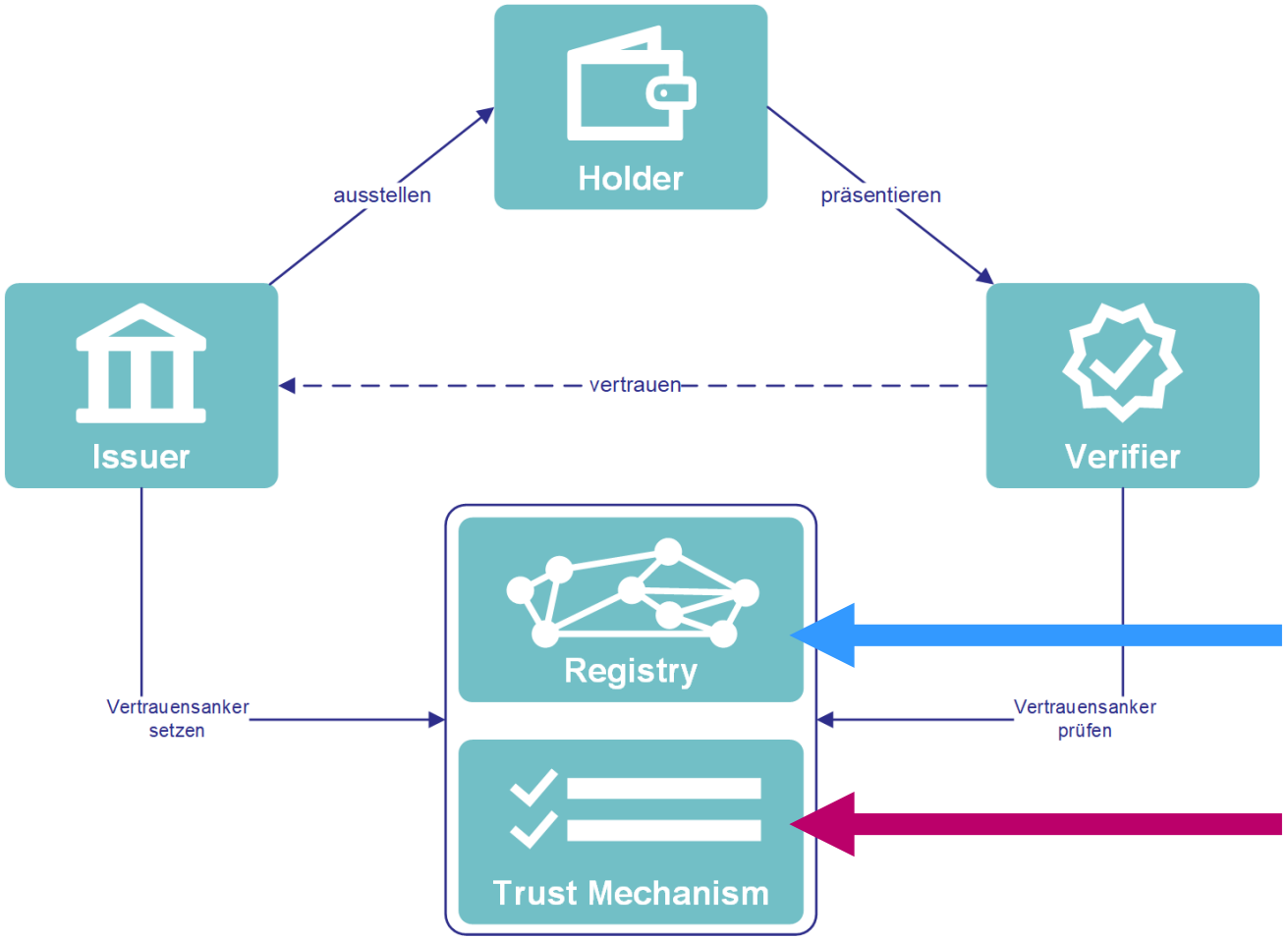
Digitale Nachweise – User als «Prozess-Owner»



Normative Vorgaben



Verifiable Data Registry und Trust Directory – zwei unterschiedliche Zwecke



Verifiable Data Registry
Technical Trust

«Trust Directory»
Human Trust

Was steckt drin?

- Schemenhafte Darstellung der **Registry** (aka Verifiable Data Registry):

Identifier	Public Key
A1	89fac8bb1722cb3e8eec231745726a
B2	65d624d5e6a56cef676df1016653cbc

kryptografisch gesichert

+ Revokations-informationen

- Schemenhafte Darstellung des **Trust Mechanism:**

Identifier	Physische, reelle Entität
B2	Staatskanzlei Zug

geprüft

Aussage *einer Autorität (z.B. Bund):* ***B2 gehört der Staatskanzlei Zug***

Dezentralität

«Dezentralität» an verschiedenen Orten, u.a.:

- Halten der Credentials beim User
- Wallet-Wahl
- Freier Zugang zum Ökosystem für Verifikatorinnen
- Diverse Autoritäten der Trust Directories
- Vertrauensanker in einer dezentralen Verifiable Data Registry

Bis zum Umsetzungsentscheid der Verifiable Data Registry bedarf es noch einigen Diskussionen, u.a. zu:

Gedankenspiele

Diskussion «Revokation durch Dritte»

- Durchgedachtes Beispiel anhand des Use-Cases «Arztrezept»
- Hilft Verständnis zu entwickeln, was eine Vertrauensinfrastruktur für digitale Nachweise leistet, und was nicht:
  - Organisationsübergreifend ohne Rückkanal: Ja
  - Organisationsintern als Nachrichtenüberbringer: Ja
  - Organisationsintern als System zur Statusverfolgung: Nein

Offene Punkte & Ausblick

- Glossar
- Vernehmlassung: GitHub als Ort zur Iteration von Gedanken und Fragestellungen
- Einbezug weiterer Kreise und Teilnehmer

Call for Entries «Business/Verifikatorinnen»

Varia – Inputs aus dem Plenum

Nächstes Online-Meeting:
Donnerstag, 7. Juli 2022 – 16.00 bis 18.00 Uhr