



**Ursula von der Leyen**

Präsidentin der Europäischen Kommission



Jedes Mal, wenn eine Website uns auffordert, eine **neue digitale Identität** zu erstellen oder uns bequem über eine **große Plattform** anzumelden, haben wir in Wirklichkeit keine Ahnung, was mit unseren Daten geschieht.

Aus diesem Grund wird die Kommission demnächst eine **sichere europäische digitale Identität** vorschlagen.

Eine, der wir **vertrauen** und die Bürgerinnen und Bürger **überall in Europa nutzen** können, um vieles Denkbare digital zu erledigen, vom Steuern Zahlen bis hin zum Fahrrad Mieten.

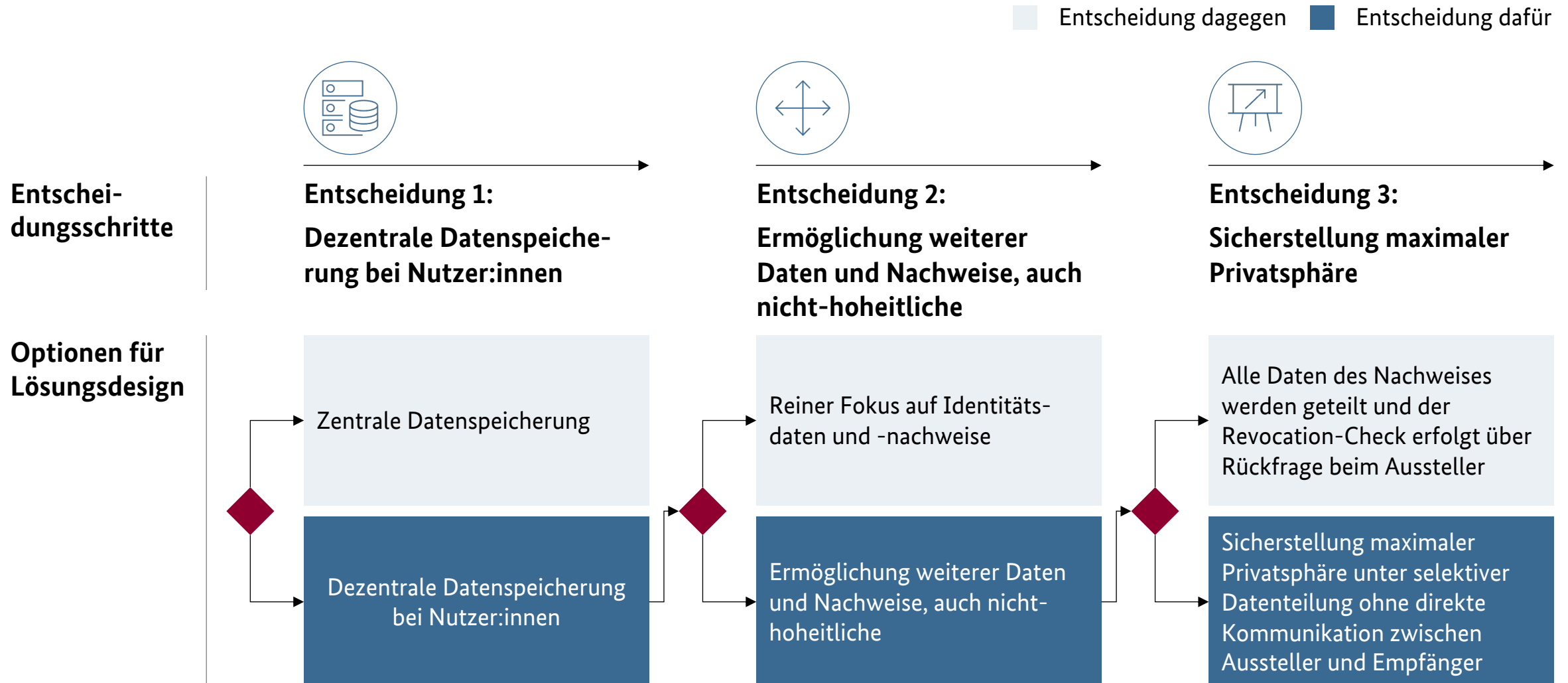
Eine Technologie, bei der wir **selbst kontrollieren können, welche Daten ausgetauscht und wie sie verwendet** werden.

# Basierend auf den Statements der EU zu digitalen Identitäten haben wir Anforderungen für unser Projekt definiert

■ Relevant für Akteur




Anforderungen	Bürger:innen	Unternehmen	Staat
① Kontrolle & Datensouveränität	■	■	■
② One-Stop-Shop für digitale Nachweise	■	■	■
③ Nutzerfreundlichkeit & Verfügbarkeit	■	■	■
④ Datensicherheit & Datensparsamkeit	■	■	■
⑤ Offene Standards & Interoperabilität	■	■	■
⑥ Europäische Skalierbarkeit	■	■	■
⑦ Vielfältige Anwendungsfälle (mit unterschiedlichem Vertrauensniveau)	■	■	■
⑧ Unabhängigkeit von großen Big Tech Playern	■	■	■

# Drei wesentliche Entscheidungsschritte haben zur Definition des Lösungsdesigns des Ökosystems geführt ...



# ... bei welchen jeweils unterschiedliche Anforderungen an das Ökosystem fokussiert betrachtet wurden

■ Anforderung betrachtet bei jeweiliger Entscheidungsfindung

Anforderungen	 <b>Entscheidung 1:</b> <b>Dezentrale Datenspeicherung bei Nutzer:innen</b>	 <b>Entscheidung 2:</b> <b>Ermöglichung weiterer Daten und Nachweise, auch nicht-hoheitliche</b>	 <b>Entscheidung 3:</b> <b>Sicherstellung maximaler Privatsphäre</b>
① Kontrolle & Datensouveränität	■		
② One-Stop-Shop für digitale Nachweise		■	
③ Nutzerfreundlichkeit & Verfügbarkeit			■
④ Datensicherheit & Datensparsamkeit			■
⑤ Offene Standards & Interoperabilität		■	■
⑥ Europäische Skalierbarkeit		■	
⑦ Vielfältige Anwendungsfälle (mit unterschiedlichem Vertrauensniveau)		■	
⑧ Unabhängigkeit von großen Big Tech Playern	■		

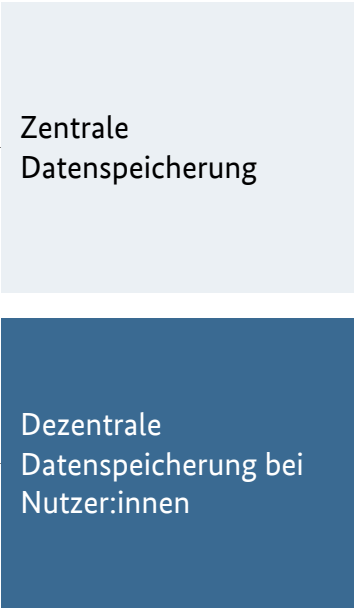
# Entscheidung 1: Dezentrale Speicherung der Bürger:innen-Daten soll ihnen maximale Kontrolle über Datenflüsse geben

Entscheidung dagegen    Entscheidung dafür



Entscheidung 1:  
Dezentrale Datenspeicherung bei Nutzer:innen

Optionen für Lösungsdesign



## Problemstellung

- Speicherort für die Bürger:innen-Daten



## Anforderungen & Erwägungsgründe

- Kontrolle & Datensouveränität für Bürger:innen
- Unabhängigkeit von einflussreichen Big Tech Playern



## Entscheidungs-begründung

- Zentrale Datenhaltung mit konzentrierter Haltung von Identitätsdaten macht diese zu einem attraktiven Angriffsziel („Honey Pot“)
- Die dezentrale Datenspeicherung bei Nutzer:innen gibt diesen de facto (nicht nur konzeptionell / de jure) die Kontrolle über die Datenflüsse
- Glaubwürdiger Gegenpol zu Machtkonzentration wie bei zentralistischen Identitätslösungen von „Big Techs“ (mit quasi-monopolistischen Zügen)

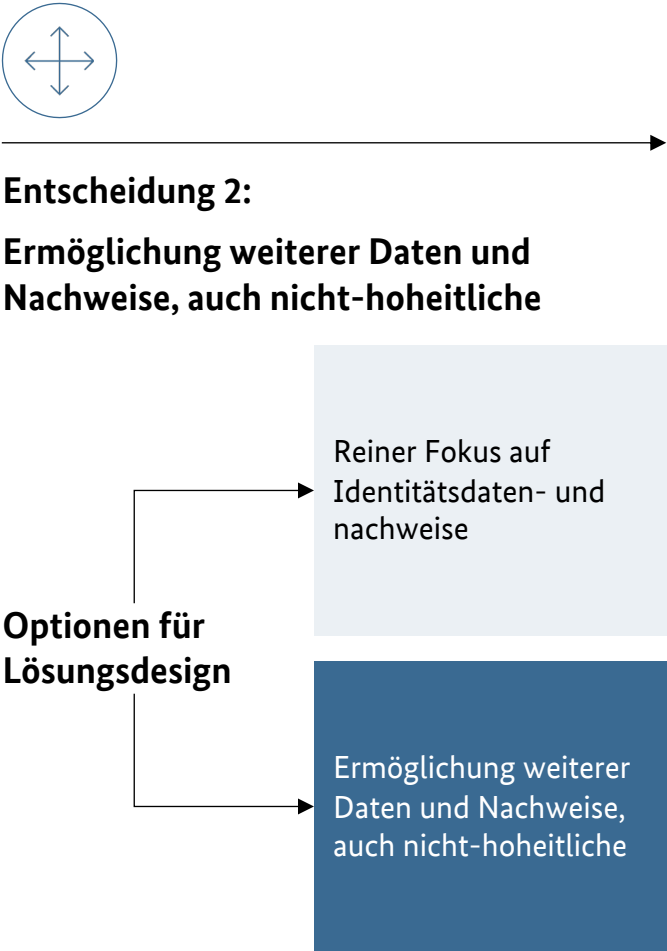
## Technischer Lösungsraum


IDP	eIDAS <sup>1</sup> -Token	PKI	SSI
✗	✓	✓	✓

1. eIDAS = Electronic identity technical specifications


# Entscheidung 2: Vielfältige Anwendungsfälle sollen über reine Identitätsnachweise hinaus ermöglicht werden

Entscheidung dagegen    Entscheidung dafür




**Problemstellung**

- Unternehmen und Staat benötigen über den Identitätsnachweis hinaus die Bereitstellung und Nutzungsmöglichkeit von Nachweisen an/durch Bürger:innen





**Anforderungen & Erwägungsgründe**

- One-Stop-Shop für digitale Nachweise
- Anwendungsfälle mit unterschiedlichem Vertrauensniveau über Unternehmen & Sektoren hinweg
- Europäische Skalierbarkeit
- Offene Standards & Interoperabilität

**Entscheidungs-begründung**

- E-ID als wenig verwendetes aber eIDAS-konformes, hochsicheres Identitätsverfahren verfügbar
- eIDAS-Token (Technologie der E-ID) praktisch nicht in Verwendung für Nachweise außer für Identität
- Es besteht ein globales Momentum für SSI für jegliche Arten von Nachweisen
- Bestehende E-ID mit beliebigen Nachweisen kombinieren (trotz nicht SSI-konformer, vom Projekt gewählter proprietärer Herangehensweise)

### Technischer Lösungsraum

IDP	eIDAS <sup>1</sup> -Token	PKI	SSI
			
	für Identität	für beliebige Nachweise	

1. eIDAS = Electronic identity technical specifications

# Entscheidung 3: Das Ökosystem soll höchste Anforderungen an Datensicherheit, Datenschutz und Datensparsamkeit erfüllen

Entscheidung dagegen    Entscheidung dafür



**Entscheidung 3:**  
**Sicherstellung maximaler Privatsphäre**

**Optionen für  
Lösungsdesign**

Alle Daten des Nachweises werden geteilt und der Revocation-Check erfolgt über Rückfrage beim Aussteller

Sicherstellung maximale Privatsphäre unter selektiver Datenteilung und ohne direkte Kommunikation zwischen Aussteller und Empfänger



## Problemstellung

- Höchste Anforderungen an Datensicherheit, -schutz, -sparsamkeit und Ermöglichung Ökosystem jenseits Ländergrenzen



## Anforderungen & Erwägungsgründe

- Datensicherheit & Datensparsamkeit
- Nutzerfreundlichkeit & Verfügbarkeit
- Offene Standards & Interoperabilität



## Entscheidungs- begründung

- Keine Eigenentwicklung, Nutzung gängiger offener Lösung
- Bürger:innen sollen nur die Daten preisgeben, die benötigt werden (Selective Disclosure)
- Invalidierung von Nachweisen soll die Privatsphäre wahren (= keine öffentlichen Sperrlisten)
- Implementiert und bereits im praktischen Einsatz durch Hyperledger Indy
- PKI ist erprobt, aber SSI als Lösung der nächsten Generation („dezentrale PKI“) hat globales Momentum
- SSI-Anerkennung in eIDAS 2.0 zu erwarten und damit Relevanz in ganz Europa
- Einfaches Onboarding für Aussteller und Verifizierer in einem Ökosystem, nicht jeweils ein eigenes PKI-Ökosystem je Aussteller

**Anmerkung:** Hyperledger Indy/Aries hat als einziges Framework die Anforderungen (u.a. Selective Disclosure) erfüllt. Die Nutzung von DLT war eine Konsequenz der Frameworkauswahl, bietet jedoch auch weitere Vorteile.

## Technischer Lösungsraum

IDP	eIDAS <sup>1</sup> -Token	PKI	SSI
	für Identität	für beliebige Nachweise	

1. eIDAS = Electronic identity technical specifications

# Identifizierte Problemstellungen der Architektur erfordern Lösungsvorschläge, die abgestimmt werden müssen

Architekturbacklog

## Identifizierte Problemstellungen



## Empfohlene Lösungsvorschläge



Notwendigkeit für Identitätsnachweis mit Vertrauensniveau „hoch“

Integration von **Smart eID** in die ID Wallet

Limitierte Adoption aufgrund bestehender, konkurrierende PKI Lösungen

Integration von **PKI-Zertifikaten** in die ID Wallet

Begrenzte Möglichkeit einer „Man-in-the-Middle“ Attacke („Man weiß nicht wem ggü man sich verifiziert“)

Verbesserte **Validierung der Verifizierer** durch qualifizierte Zertifikate

Ableitung von Vertrauen durch Zertifikathierarchie (Delegation) nicht abgebildet
















**Trust Registries** für **erwünschte Aussteller** konzipiert, Umsetzung ausstehend

Limitation der Datenempfänger (Verifizierer) für definierte Credentials nicht möglich

Über **Trust Registries** könnten auch **erwünschte Verifizierer** festgelegt werden

# Getroffene Entscheidungen führten zum SSI- Ansatz ergänzt durch eIDAS- Token

Teil der Lösungsarchitektur

		Technischer Lösungsraum			
		IDP	eIDAS-Token	PKI	SSI
	Entscheidung 1: Dezentrale Datenspeicherung bei Nutzer:innen				
	Entscheidung 2: Ermöglichung weiterer Daten und Nachweise, auch nicht- hoheitliche				
	Entscheidung 3: Sicherstellung maximaler Privatsphäre		  für Identität		  für beliebige Nachweise