Der Elektronische Identitätsnachweis (E-ID)

& aktuelle Entwicklungen zu eIDAS / SSI

arne.tauber@egiz.gv.at
Arne Tauber

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

TU Graz

EGIZ
E-Government Innovationszentrum

E-Government: panta rhei!

Akzeptiert

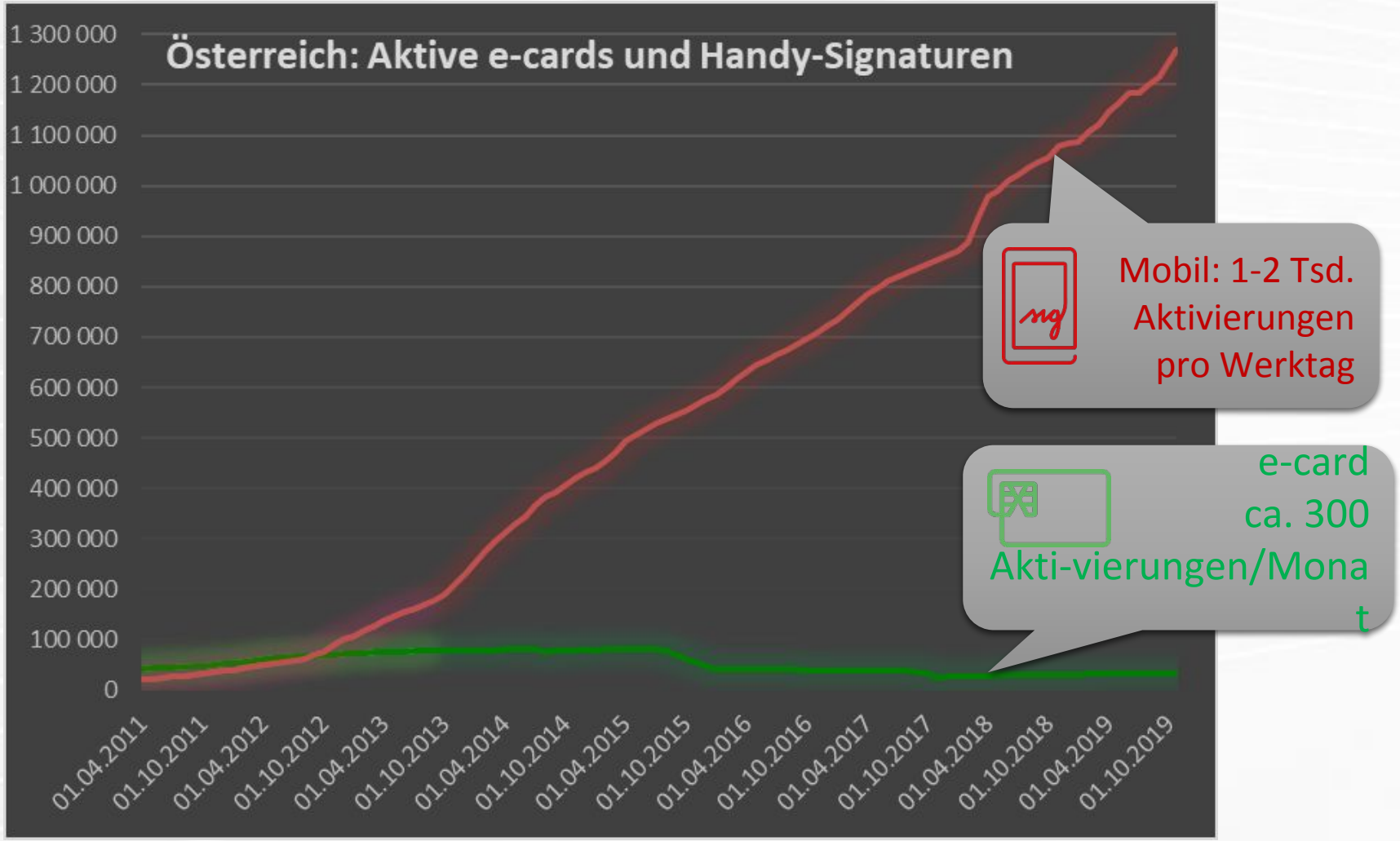
- Digital by default
- Data Once Only
- Data (as open as possible)
- GDPR

eIDAS

In Entwicklung

- Mobile First
- Security by Design
- Data Protection by Default
- Dienste □APPs
- Internet der Dinge

Remote-Signatur – Die Richtige Entscheidung



M-Government: Technologieunterschiede

WEB >>>
APP

Ähnliche Userexperience – deutliche Technologieunterschiede (Session, Sicherheit, …..)

Herausforderungen

- Mobile Anwendungen anders denken
  - Formulare vermeiden, Once-Only umsetzen
- Mobil folgt anderen Paradigmen
  - Transaktionsorientiert, nicht Session-basiert
  - Strategie Halten vs. Re-Authentifizierung
  - Integration App Dritter, App-App Kommunikation
- Mobil bringt auch Sicherheitsvorteile
  - Hochpersönliches Gerät
  - Sandboxing, SE/TEE, App-Berechtigungen, …

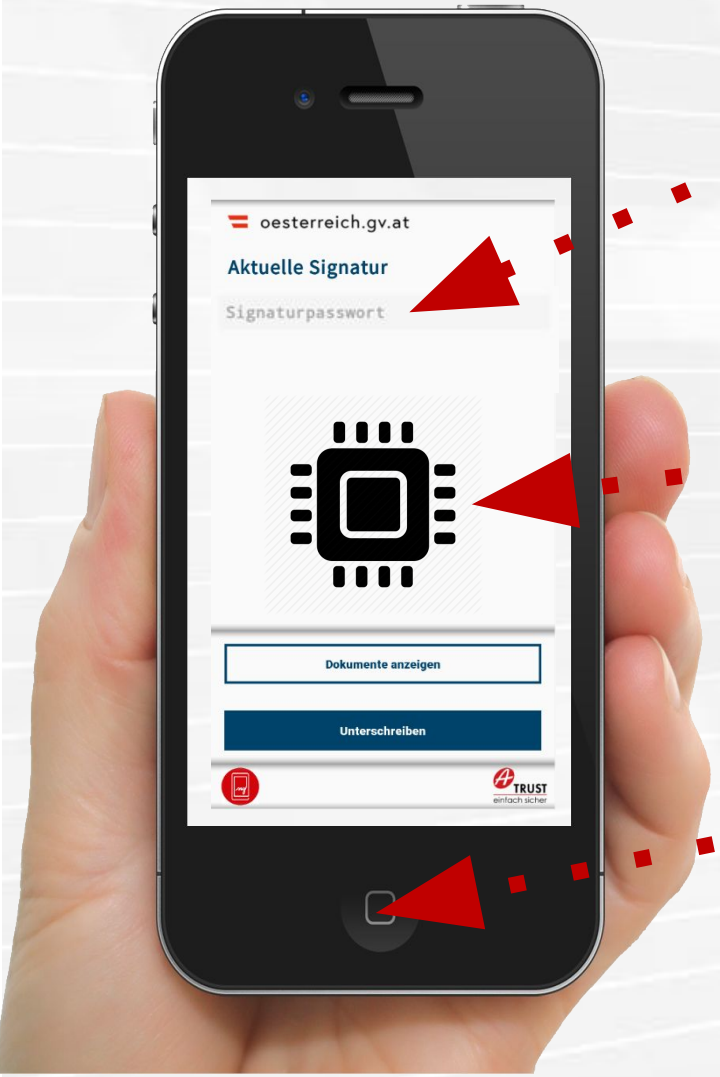
Mobil ist anders

- ALWAYS ON:
  von der Sitzung zur Transaktion

- wann identifiziere ich mich?
- wie identifiziere ich mit?
- wie wird „Wissen“ verwendet?

- Qualität der Identifikation und
  Qualität der Bindung müssen
  gleich stark sein

Handy-Signatur Neu - Sicherheitstechnologien



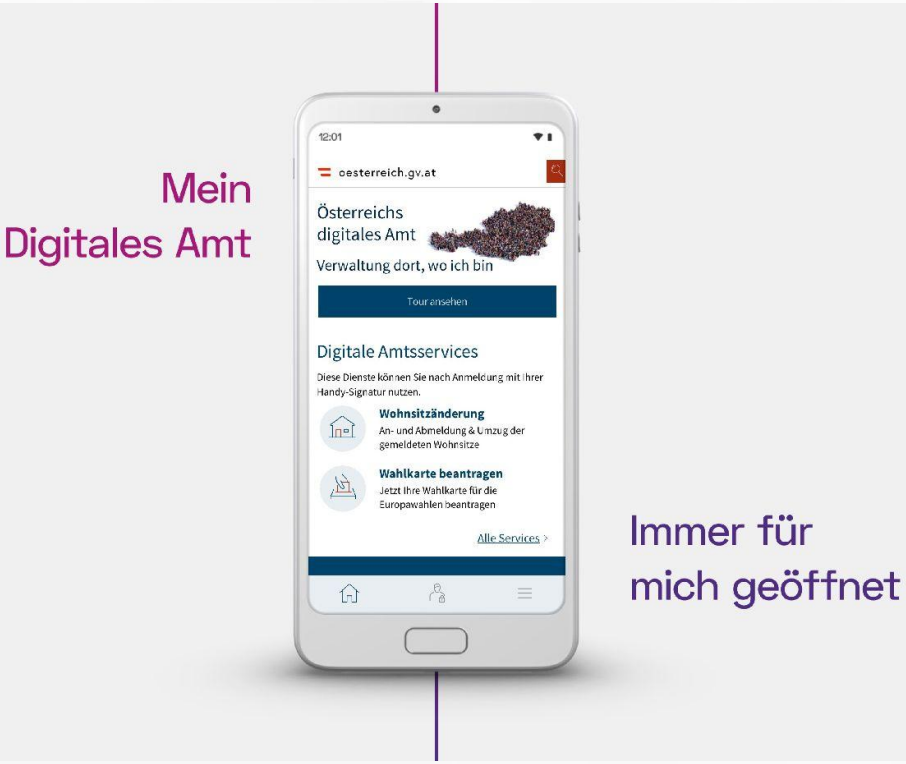
Faktor Wissen: Passwort

Faktor Besitz: Sicherheits-Chip im Mobilgerät

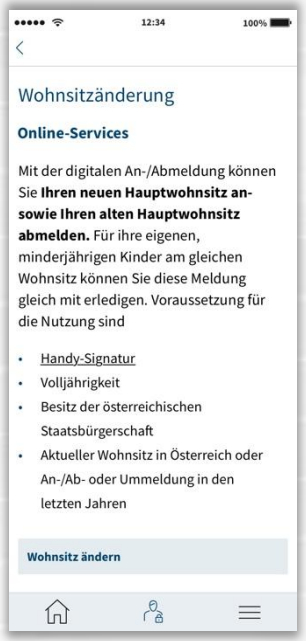
Faktor Sein: Biometrie (Fingerabdruck, Face-ID)

M-Government – Digitales Amt

- eGov/mGov App oesterreich.gv.at
  - Digital Single-Point of Contact
  - Desktop oder Smartphone
  - Mobile-First Ansatz
  - Handy-Signatur Integration



Beispiel: Wohnsitzänderung mobil



- Einbindung des Zentralen Melderegisters und des Adressregisters
- Abmeldung des bisherigen und Anmeldung neuen Hauptwohnsitzes
- Bestätigung nach Abschluss

Plattform oesterreich.gv.at / Digitales Amt

Bereitstellen einer Grundstruktur (Framework) = Fahrgestell

Unterschiedliche Player setzen darauf unterschiedliche Applikationen auf

MOBILE FIRST

EMBEDDED	EMBEDDED	WEBAPP	EXTERN APP
SIGN-IN	WEITER	WEITER	WEITER

AUS EINEM GUSS □ nahtloses miteinander von integrierten, externen und Web-Applikationen

Der E-ID

„Bürgerkarte Neu“

„Bürgerkarte neu“ durch E-GovG-Novelle

- Änderung von Begrifflichkeiten
  - „**Elektronischer Identitätsnachweis (E-ID)**“ statt „Bürgerkarte“

- **Weiterentwicklung** des österreichischen elektronischen Identifizierungssystems (bislang Bürgerkarte)
  - Schaffung eines behördlichen Prozesses für die Registrierung eines E-ID
  - „Weiterverwendung“ mittels eines sicherheitstechnisch gleichwertigen Vorgangs, der an eine frühere qualifizierte elektronische Signatur des E-ID-Inhabers gebunden ist (Bindungsservice SSO)
  - Erweiterung des Funktionsumfangs des E-ID, insbesondere durch die Einfügung weiterer Merkmale in die Personenbindung (variabel je nach Anwendungsfall)

Online Personenbindung – § 4 Abs. 5

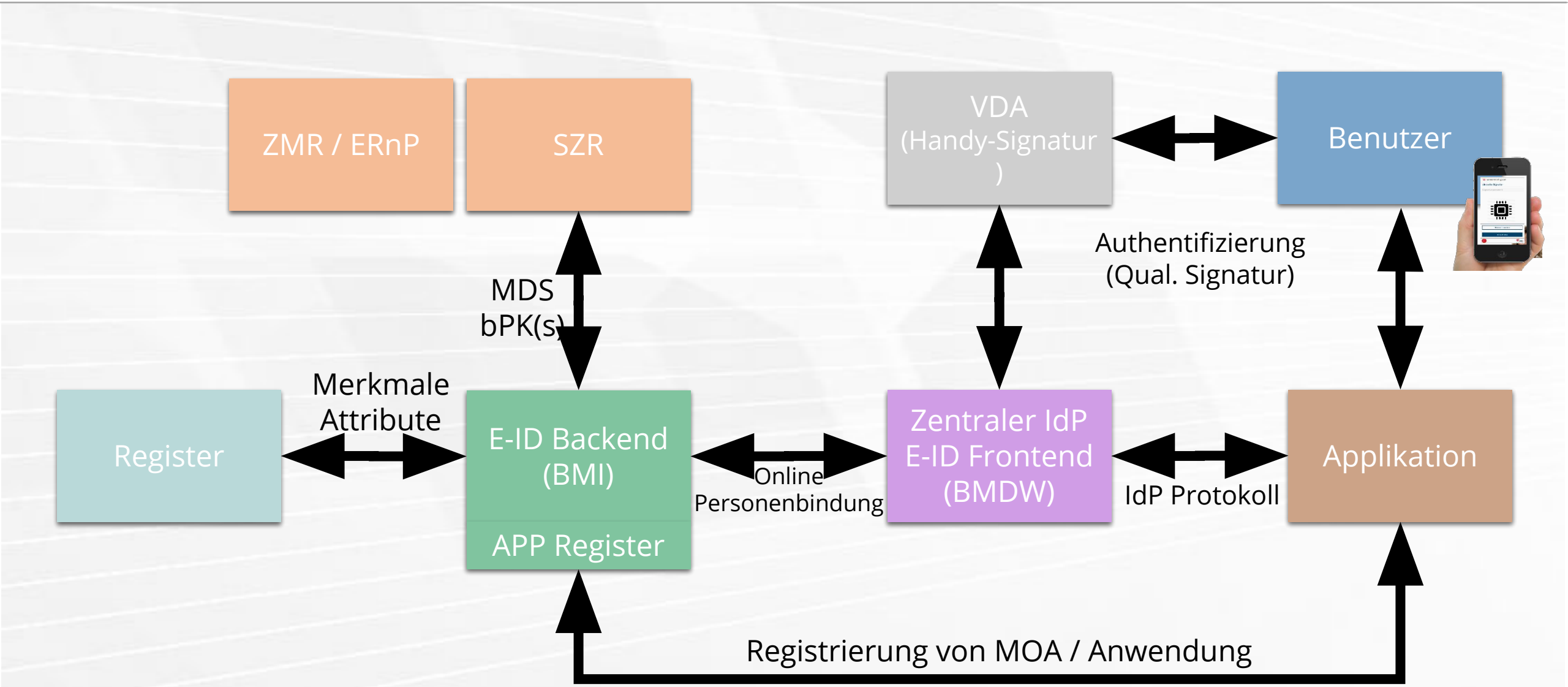
- Wird bei jeder Verwendung des E-ID „neu“ gebildet und von der Stammzahlenregisterbehörde signiert/besiegelt
- Unterschiedlicher Inhalt je nach Art der Verwendung:
  - öffentlicher Bereich § 4 Abs. 5: ein/mehrere bPK, Mindestdatensatz (MDS=Vorname, Nachname, Geburtsdatum),
    optional: weitere Merkmale
  - privater Bereich § 14 Abs. 3: ein bPK
    optional: MDS, weitere Merkmale
  - Ausland § 14a Abs. 2: ein bPK, MDS
    optional: weitere Merkmale
- Prüfbarkeit im eIDAS Kontext damit sichergestellt, da auch Anwendungen im privaten Bereich und im Ausland eine behördlich signierte/besiegelte Personenbindung erhalten

Weitere Merkmale

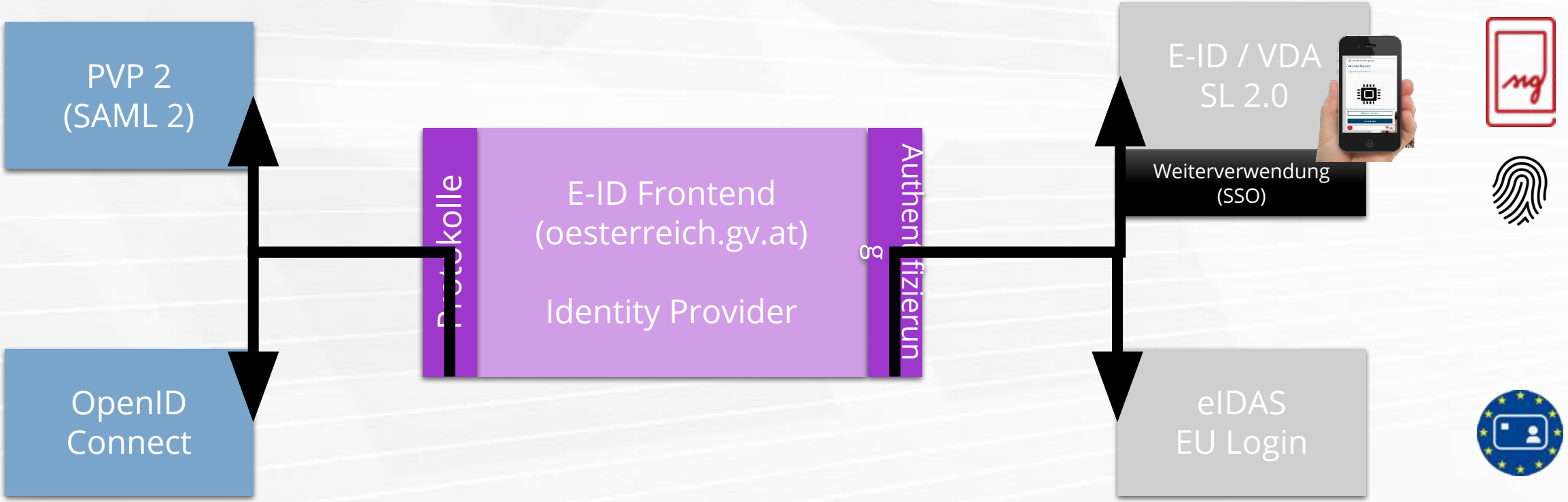
- Nachweis von Daten aus Registern von Auftraggebern des öffentlichen Bereichs (etwa Personenstands-, Melde- oder Staatsbürgerschaftsdaten)
- Werden nach Maßgabe der technischen Möglichkeit (etwa Anbindung des jeweiligen Registers) bei Verwendung des E-ID in die Personenbindung eingefügt und behördlich signiert/ besiegelt
  - Zugriff auf derartige Merkmale nur mit Zustimmung und Wissen des Betroffenen
  - Im privaten Bereich hätte der Betroffene die Möglichkeit, bloß Informationen über das Alter oder das Geburtsdatum, jedoch nicht seine Identität preiszugeben (vgl. § 14 Abs. 3)

Architektur

E-ID: Block-Architektur



Identity Provider - Funktionen



Neuer E-ID: Grundkonzepte / Zusammenfassung

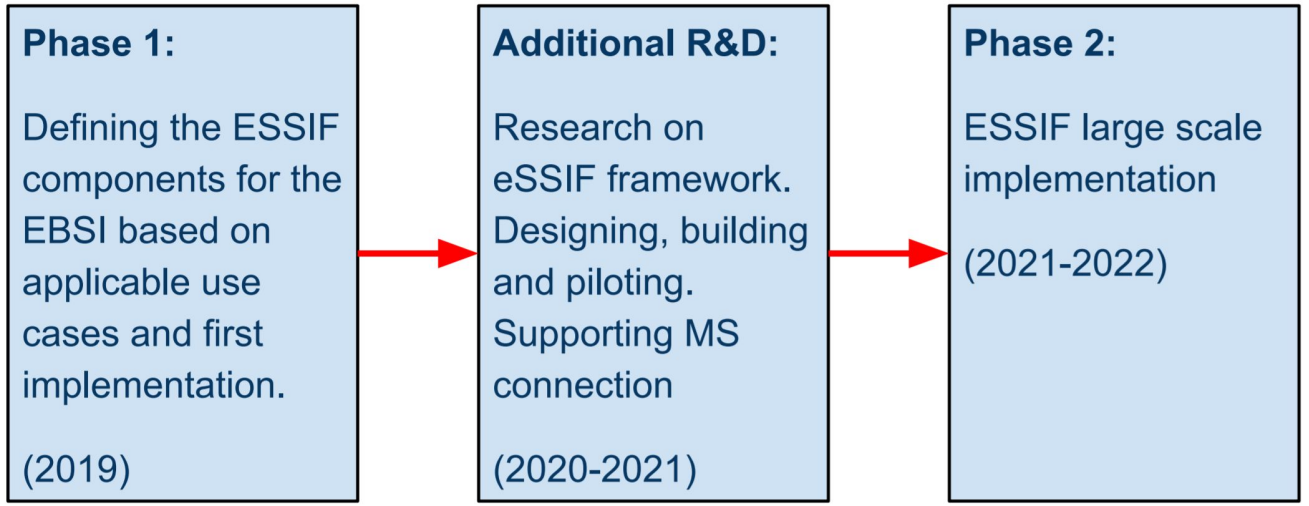
- Wird Ende 2020 starten
- Erfahrungen seit 2005 berücksichtigt
- Fernsignatur-basiert *(vgl. kaum Chipkarten-Nutzung)*
- Ermöglicht **single-device** Nutzung *(mit SE/ TEE)*
- Entkopplen von IdP und QVDA
  - BMDW / BMI betreiben IdP Schnittstelle
  - Leiten an Signatur-Dienst weiter
- (künftig) Integration weiterer Attribute
- Anwendungen ohne Spezialsoftware
  - SAML2 oder OIDC als Standard-Schnittstellen
- Anwendungsregister
- User Consent

eIDAS & SSI

Aktuelle Entwicklungen

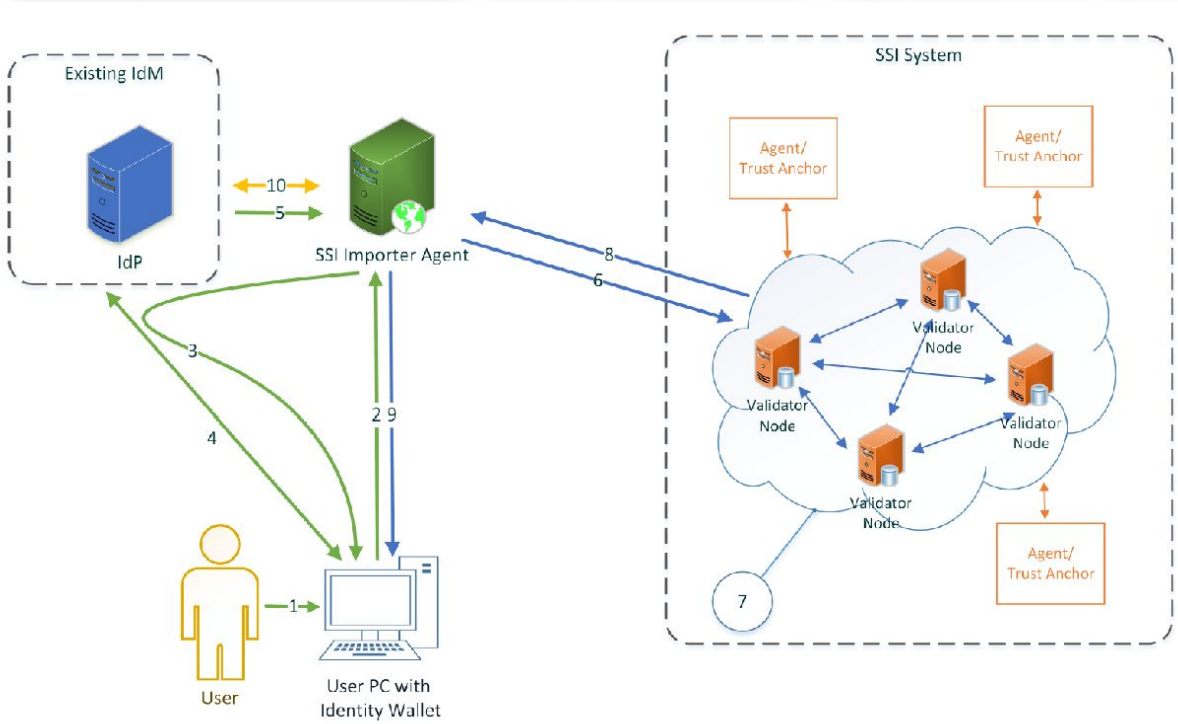
EBSI/ESSIF

- European Blockchain Service Infrastructure (EBSI)
  - Eine use-case Gruppe: European Self-Sovereign Identity Framework (ESSIF)
  - https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
- Cross-border SSI / Interoperabilität
- Aktuell nur LoA low
- Langzeit-Fokus
  - LoA substantial und high
- Verknüpfen von IDs zu qual. Zertifikaten (eIDAS certificates
  - Bridge zwischen eIDAS and ESSIF



eIDAS & SSI – Konzept EGIZ

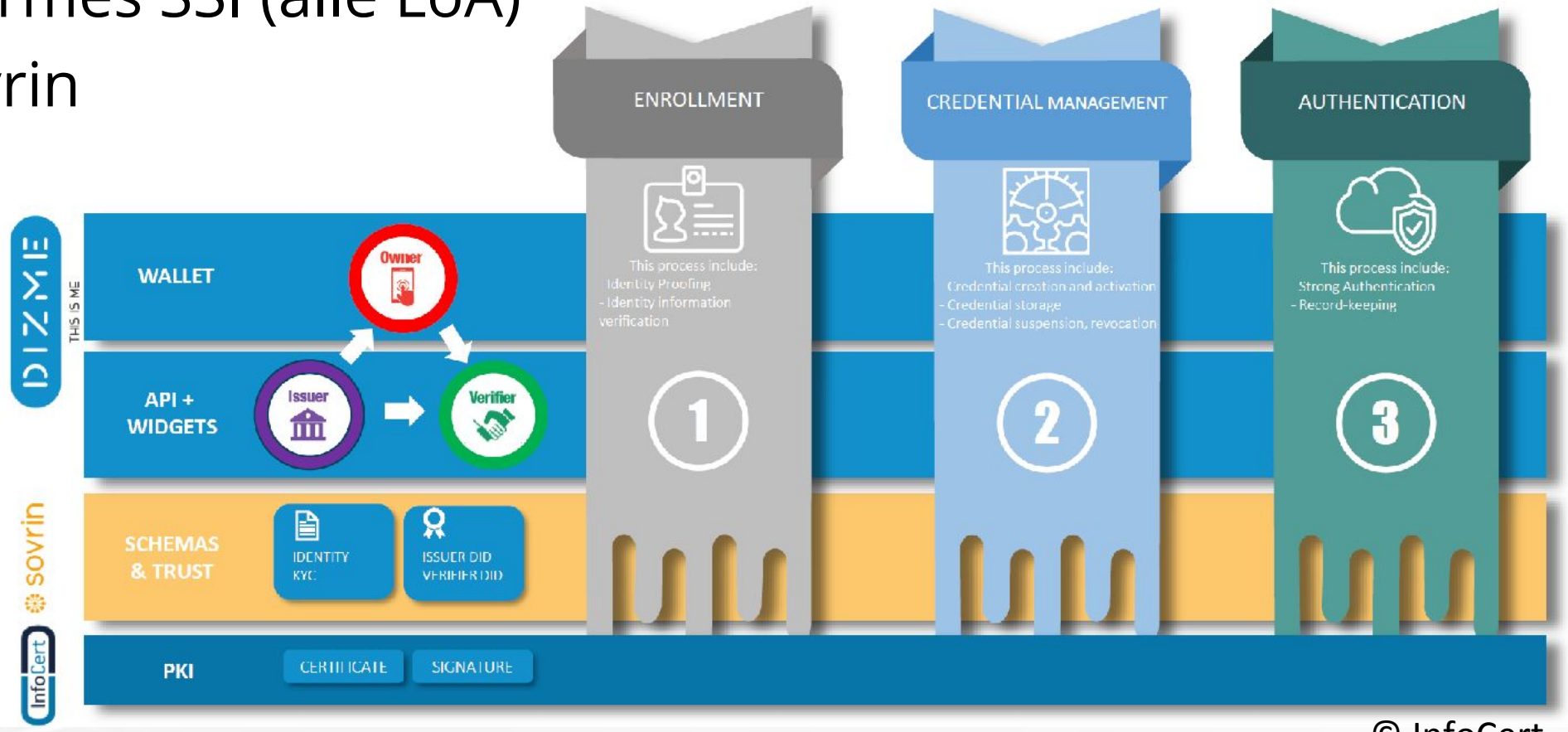
- Forschung im Bereich SSI
- eID Derivation von eIDAS zu SSI
  - Basis Sovrin SSI Netzwerk
- Direkte Anbindung eIDAS Netzwerk an SSI Netzwerk
- Transformation der eIDAS Assertion auf SSI Format
- Privacy-preserving
  - Non-interactive ZKP (NIZP)
- Korrektheit der Transformation wird überprüft



- http://importdemo.iaik.tugraz.at/SP/populateIndexPage

DIZME (This is me)

- Projekt des ital. QVDA InfoCert
- eIDAS-konformes SSI (alle LoA)
- Baut auf Sovrin



EU Projekt KRAKEN

- EU Horizon 2020 Project
  - TU Graz Partner eines internationalen Konsortiums
- Brokerage and Market platform for personal data
- Forschungsthemen
  - SSI Erweiterungen (eIDAS Konformität)
  - Sichere Cloud Wallet (Ablage und Weitergabe)
  - Datenverschlüsselung / Datenanalyse auf verschl. Daten
  - Proxy Re-encryption
- ESSIF Compliance
- Marktplatz für SSI Daten
  - Piloten im Bereich Gesundheit / Universitäten

Dr. Arne Tauber
arne.tauber@egiz.gv.at

Fragen? eid@egiz.gv.at

E-Government Innovationszentrum (EGIZ)
Inffeldgasse 16a
A-8010 Graz