

Der neue Personalausweis und was nun ?



Agenda

- ✓ Über OpenLimit
- ✓ Warum „Digitale Identitätslösungen“ für Online Prozesse -Prozesse wichtig werden.
- ✓ Was ist truedentity?
- ✓ Welche Herausforderungen
- ✓ Welche Vorteile
- ✓ Wie bekommt man eine schnelle und automatisierte Erstidentifizierung zu Stande

Über OpenLimit – Unternehmen

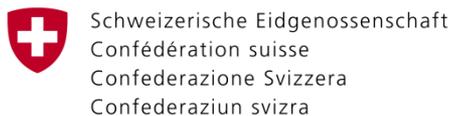
- ✓ Gründung 2002 – börsennotierte AG
- ✓ Hauptsitz in Baar, Kanton Zug (CH)
- ✓ Niederlassung in Berlin (D)
- ✓ 65 Mitarbeiter
- ✓ BSI-zertifizierte Technologien nach international höchsten Sicherheitsstandards, Common Criteria EAL 4+

Zertifizierter Softwareanbieter für:

- ✓ Digitalen Identitäten
- ✓ Elektronische Signaturen
- ✓ Beweiswerterhaltende Langzeitarchivierung



Über OpenLimit – Referenzen (Auszug)



Über OpenLimit – Technologiekompetenz eID

- ✓ Exklusiver Lieferant von Siemens/ATOS Worldline für die AusweisApp, der Anwendersoftware für den neuen Personalausweis in Deutschland
- ✓ zertifizierte Technologien nach dem international höchsten Sicherheitsstandard für Software-Produkte – Common Criteria EAL 4+
- ✓ hochsichere und praxiserprobte eID-Servertechnologien gemäß BSI-Richtlinien (eCard-API-Framework)
- ✓ eID-Kompetenzausbau durch Projektbeteiligungen:
[SkIDentity](#) - Ziel: Sichere Identitäten für Cloud-Computing-Infrastrukturen
[STORK](#) - Ziel: Interoperabilität von europäischen Ausweisdokumenten
- ✓ Entwicklung einer eID-kompatiblen Technologie, die alternative Zugänge bspw. über Soft-Token ohne Einsatz eines Kartenlesers oder Zusatzsoftware zulässt → [truedentity](#)



Partnerschaften



TimeProof GmbH



Bonität

&

Identität

Definition für digitale Identität

Eine **digitale Identität** ist eine Identität, die von einem Rechner verstanden und verarbeitet werden kann.

Die digitale Identität entsteht, indem Attribute einer natürlichen Person oder eines Objektes in einem Rechner in elektronischer Form **sicher** registriert werden.



Die Bedrohung nimmt zu; Internetaktivitäten und unsere Identitäten müssen geschützt werden



- ! 2 Millionen Kundendaten von Vodafone-Kunden wurden abgeschöpft
- ! Eine hohe sechsstellige Zahl von elektronischen Gesundheitsakten wurde 2013 zwei Krankenhäusern in Baden Württemberg gestohlen
- ! 100.000 Kundendaten wurden einer Bausparkasse in Deutschland gestohlen und beim bisherigen Inhaber komplett gelöscht
- ! 2013 im ersten Quartal 250.000 elektronische Identitäten gestohlen

Herausforderung: sichere Identitäten für sichere Online-Prozesse



- ✓ Die Zahl **der** Onlineprozesse nimmt stetig zu
- ✓ Cloud-Angebote versprechen neue IT-Dienstleistungen
- ✓ **ABER:** datenschutz- und datensicherheitstechnische Fragen sind noch nicht gelöst
- ✓ Grundsatzfrage: Wer nimmt berechtigten Zugriff auf Daten?
- ✓ **nPA kommt nur langsam in Fahrt**

> 20 Mio nPA

< 8 Mio mit elektronischer Funktionalität

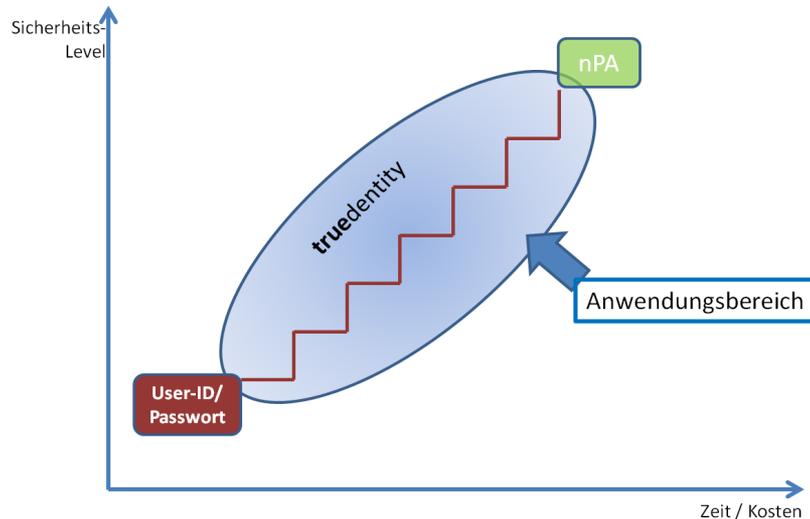
< 50.000 Kartenleser daheim



Bis auf wenige Aktivitäten auf NFC-Basis geht das
Ganze momentan nur stationär

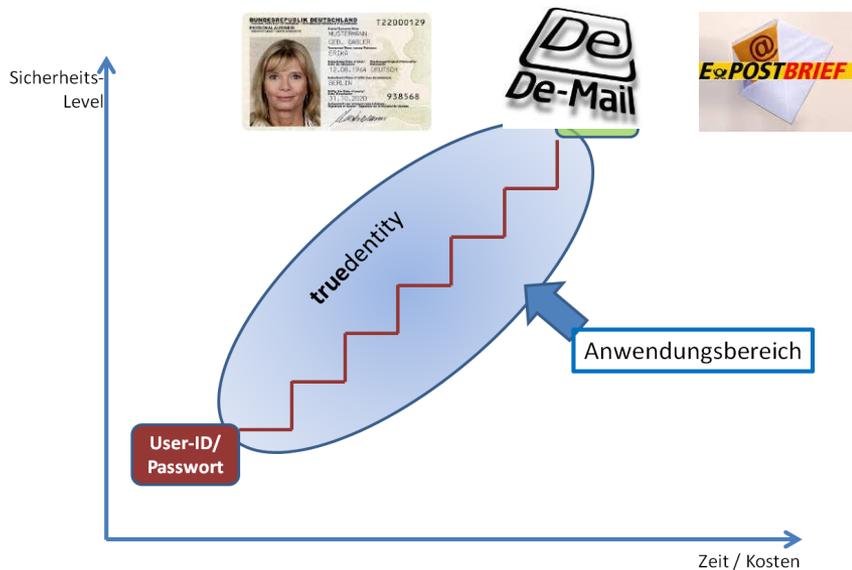


Herausforderung: Eindeutige Identitäten (ID) ist Fundament für neue Cloud-Prozesse



- ✓ Bisherige Authentisierungsverfahren halten den datenschutztechnischen Sicherheitsanforderungen nicht stand
- ✓ Wachsender ID-Technologieschub durch nPA, eGK, HBA usw.
- ✓ **Ziel: ein einheitliches Identitätsverfahren für unterschiedliche Identitätsformate!**

Herausforderung: Eindeutige Identitäten (ID) ist Fundament für neue Cloud-Prozesse



Identifizierungsverfahren für den hoheitlichen Ansatz:

- nPA
- DE-MAIL
- E-POST-Brief

für den wirtschaftlichen Ansatz:

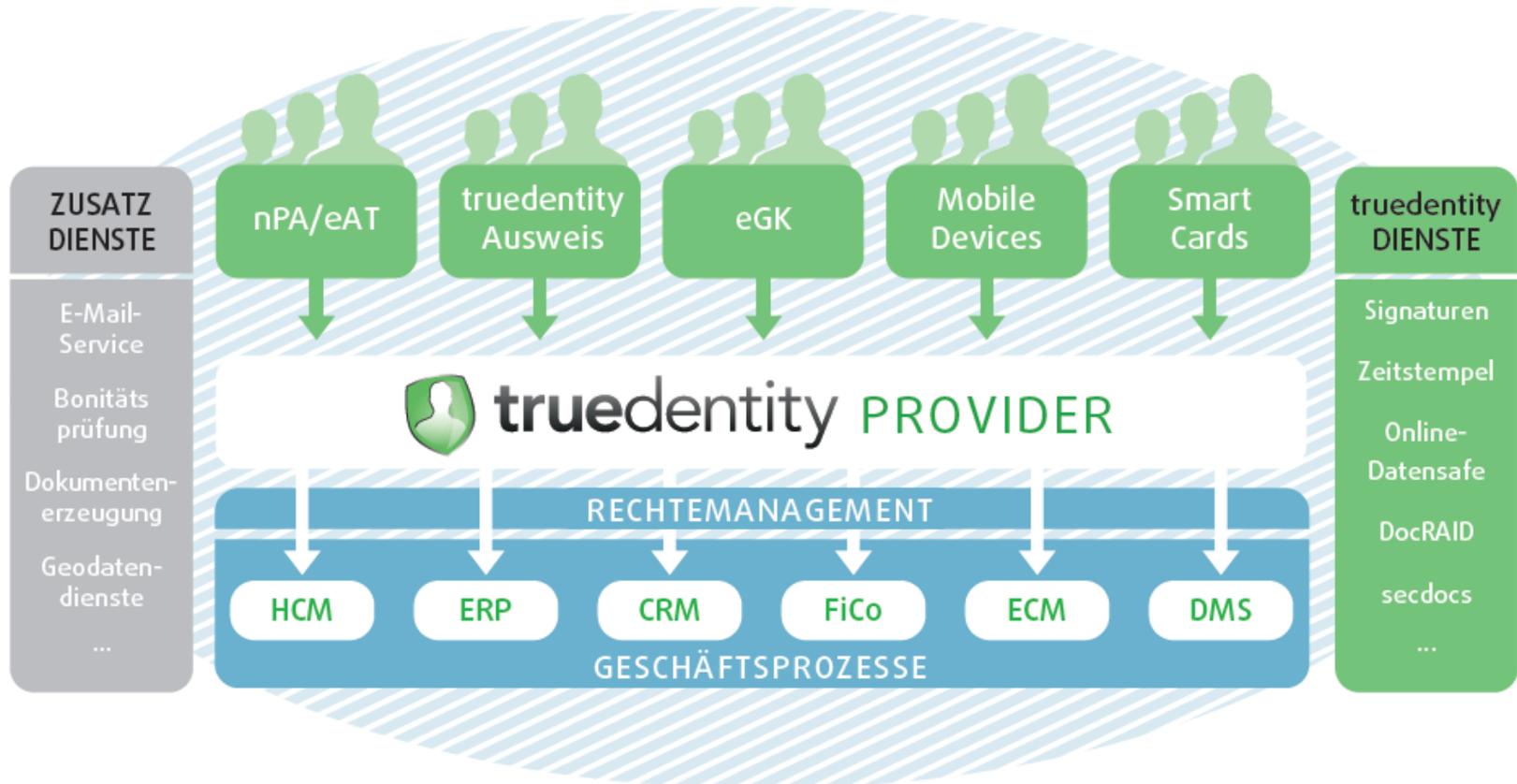
- nPA (zum Teil- wenig Angebote)
- User-ID / Passwort
- Token
- RSA-Token
- Smart Cards
-

Lösungsansatz – OpenLimit truedentity

- ✓ **truedentity** ist eine skalierbare 2-Faktor-Authentisierungslösung, die sich an der Technologie des neuen Personalausweises und den zugrundeliegenden Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) orientiert.
- ✓ Je nach Anforderungen unterstützt **truedentity** verschiedenste Identitätsformate und kann auf verschiedenen Sicherheitsebenen eingesetzt werden.
- ✓ Truedentity kann zu einer 3-Faktor-Authentisierungslösung erweitert werden- unterschiedliche biometrische Merkmale können genutzt werden



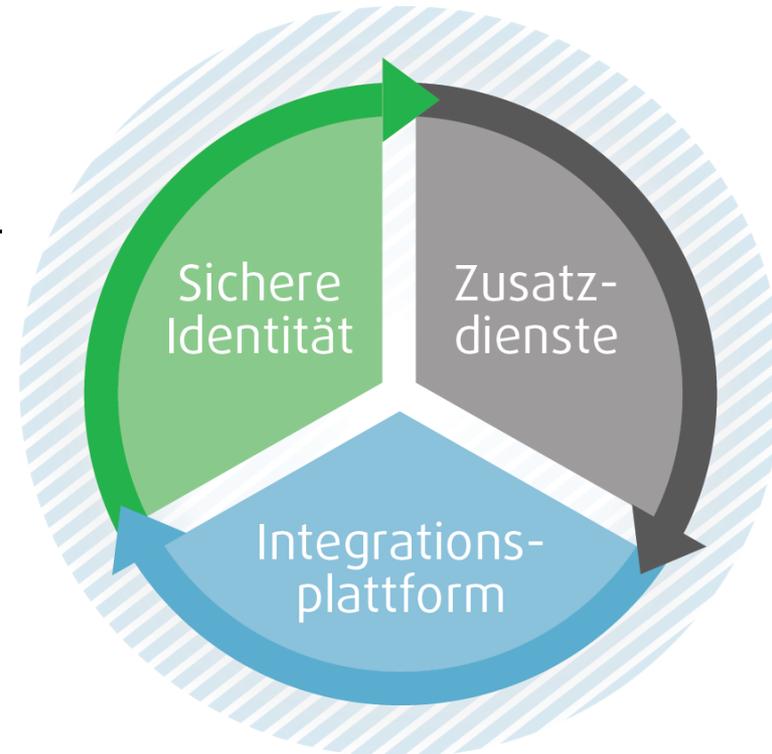
truedentity im Überblick (1)



truedentity im Überblick (2)



- ✓ Online-Ausweis für Mitarbeiter, Zulieferer, Kunden, etc.
- ✓ Integrations-Schnittstelle für verschiedene Authentisierungs-Lösungen, z. B. Dienstausweise, Personalausweis, Ausländer-Aufenthaltstitel, Signaturkarten, Mobile Devices und weitere
- ✓ Zusatzfunktionen und –dienste wie Signaturen, Cloud- und Langzeitspeicherung zur Prozessoptimierung und Mehrwertanreicherung



Welche Vorteile bietet truedentity? (1)



- ✓ Verlässliche Identitätsfeststellung als Baustein für Ihren Business Prozess
- ✓ Sichere Identifizierung von Anspruchsgruppen, die auf Ihre Infrastruktur zugreifen
- ✓ Revisionssichere, medienbruchfreie und beweissichere Geschäftsprozesse mit externen Anspruchsgruppen
- ✓ Erhöhte Zugangssicherheit auf Ihre Cloud-Services und Applikationen
- ✓ Imagegewinn durch höheres Vertrauen Ihrer Kunden gegenüber Ihren Services

Welche Vorteile bietet truedentity? (2)



- ✓ Persönliche Kundenansprache durch eindeutige Wiedererkennung
- ✓ Sicherung des Zugriffs auf Content mit sensiblen, persönlichen Daten über das Internet
- ✓ Erweiterung Ihrer Kundenkarten, Mitgliederausweise, Dienstaussweise, etc.
- ✓ Unmittelbare Sperrung von Identitäten bzw. Zugangsberechtigungen bei Verlust oder Diebstahl
- ✓ Vorbereitung auf Nutzung des Personalausweises als Identifizierungsverfahren durch gemeinsame Schnittstellen

Welche Vorteile bietet truedentity ?



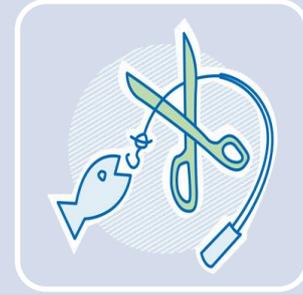
Ohne Kartenleser/
Softwareinstallation

Kann auf USB-Stick,
Smartphone, Tablet-
oder Desktop-PC
laufen



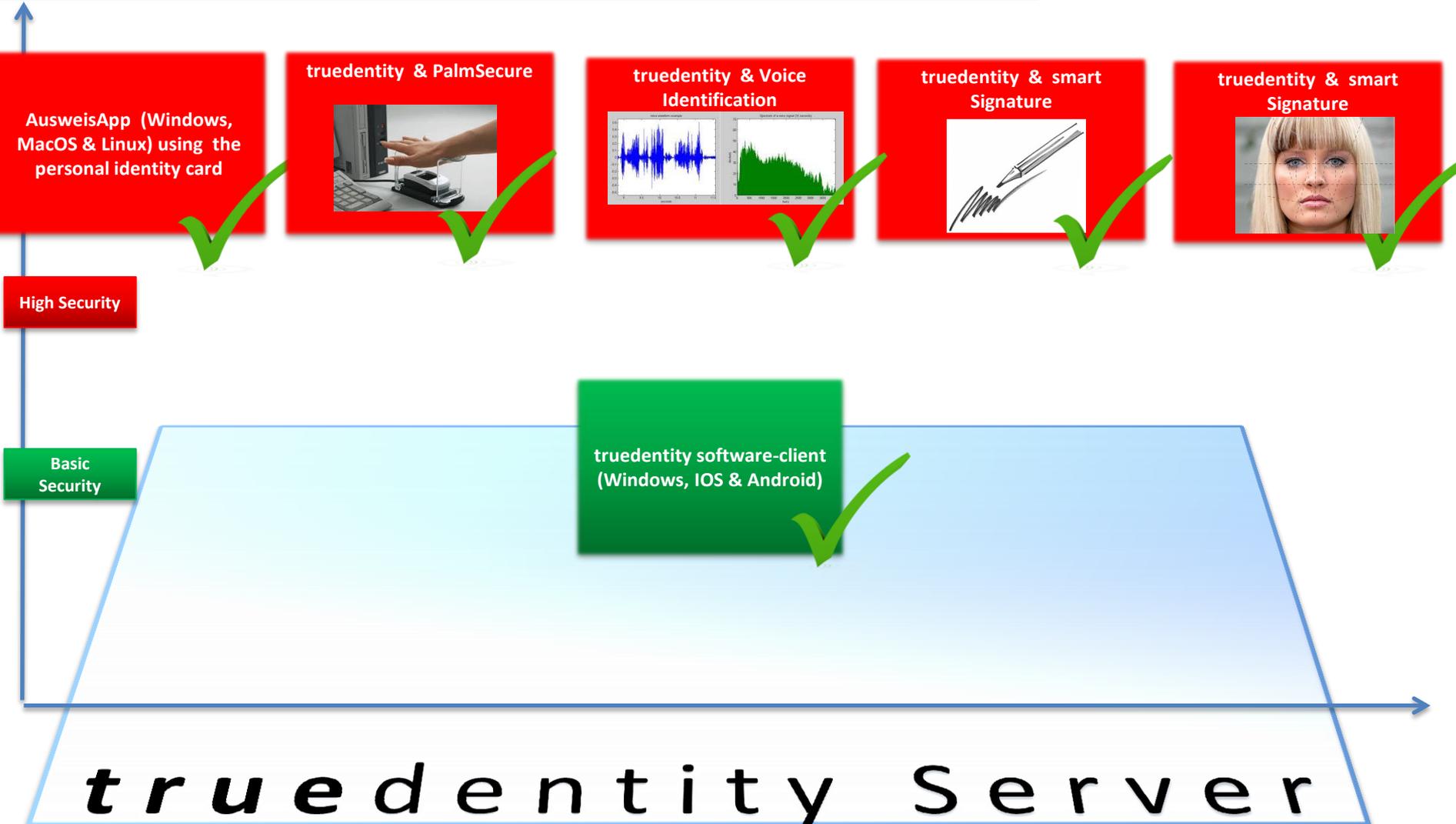
Kontrolle über
persönliche Daten

Abruf von Content
mit sensiblen,
persönlichen Daten
über das Internet



Sperrung bei Verlust
oder Diebstahl

Schutz vor Phishing-
Attacken und Daten-
/Identitätsdiebstahl



Agenda



TimeProof GmbH

Facesign

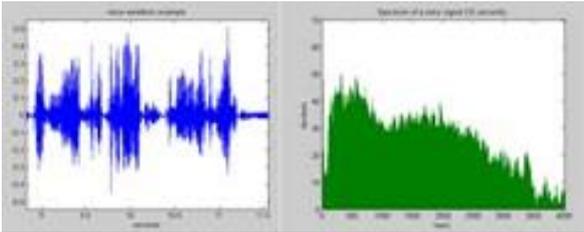
Für die vollelektronische Erstidentifizierung mittels
Mobile Device



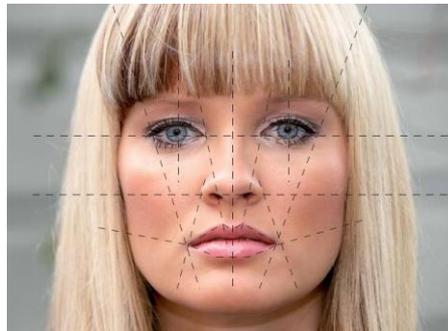
Smart Phone und Container ?



Smart Phone und Container ?



Smart Phone und Container ?



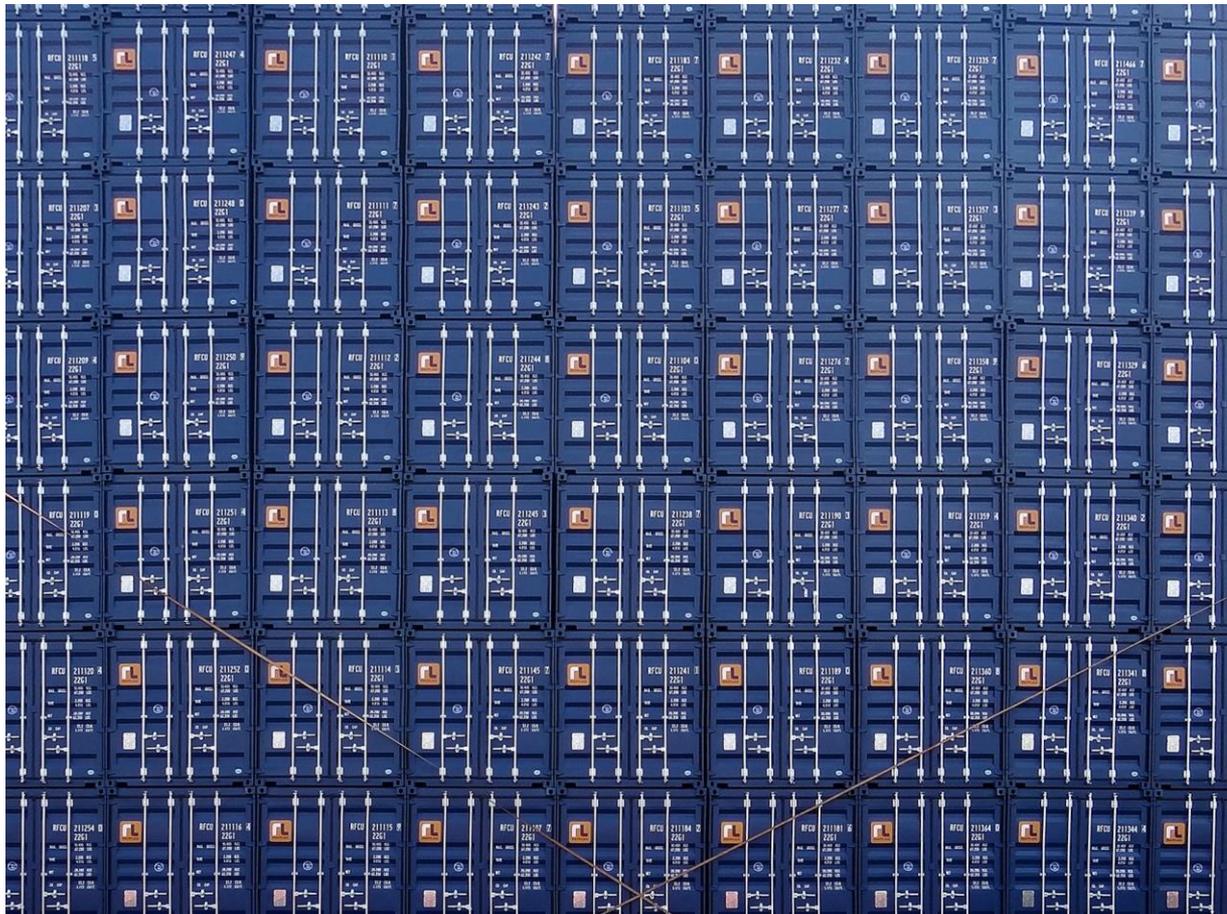
Smart Phone und Container ?



Containerlager unserer Identitäten



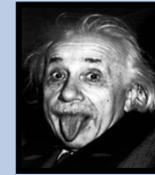
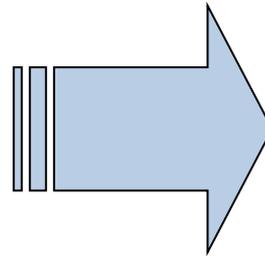
Anonyme Container mit anonymen Inhalten



Facesign Prozess



Anwender



Zusatzinformation(en):

- ✓ Zeit
- ✓ Umgebungsinformation
- ✓ Geräteinformation

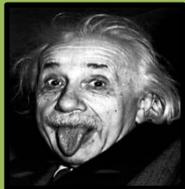
AnwenderSignatur

ApplikationsSignatur



Facesign Prozess

- ✓ W5: Wer hat wann, was, wo, womit aufgenommen?
- ✓ Automatisches Copyright
- ✓ Gerichtsfest, da manipulationsresistent
- ✓ Zusatzinformationen werden geschützt eingebettet



Zusatzinformation(en):

- ✓ Zeit
- ✓ Umgebungsinformation
- ✓ Geräteinformation
- ✓ Voice
- ✓ Unterschrift

AnwenderSignatur

ApplikationsSignatur

facesign ready



Facesign Prozess



Basisregistrierung im eSignPortal mit USER/PASSWORD war erfolgreich, Ergebnis ist **eSignID** verknüpft mit **MobileNR (+49-160-xxxxxx)** der zu identifizierenden Person



Smartphone mit Front-/Back-Side-Cam mit **IMEI** und **SmartCardID** der Telco



PA – Personalausweis (neuer, alter) mit personenbezogenen Daten **PAset** zur Identifikation



FaceSignApp – manipulationsresistente App



eSignPortal – Identifikationsportal Dienstleister



Facesign Prozess

aufnehmen

Foto von PA mit FaceSignApp mit Back-Side-Cam des Smartphones mit Autofokus auf PA. Erfassung der kompletten Vorder- und Rückseite des PA. ①

+

Gleichzeitig wird mit Front-Side-Cam **Fotoserie** oder **Video** von aufnehmender Person aufgenommen. Dauer max. 30 Sekunden. ②

Facesign Prozess

aufnehmen

versiegeln

Foto von PA mit FaceSignApp mit Back-Side-Cam des Smartphones mit Autofokus auf PA. Erfassung der kompletten Vorder- und Rückseite des PA. ①

+

Gleichzeitig wird mit Front-Side-Cam **Fotoserie** oder **Video** von aufnehmender Person aufgenommen. Dauer max. 30 Sekunden. ②

Versiegelung der erfassten Daten und Metadaten aus ① und ② mittels Patenten (SecDoc, SecStream) für eSignID im eSignPortal per Webservices oder SMS-DATA-Service im Hintergrund. Das geschieht unmittelbar nach ① und ② in einem sehr begrenzten Zeitfenster maximal 1 Minute. ③

Facesign Prozess

aufnehmen

versiegeln

extrahieren

Foto von PA mit FaceSignApp mit Back-Side-Cam des Smartphones mit Autofokus auf PA. Erfassung der kompletten Vorder- und Rückseite des PA. ①

+

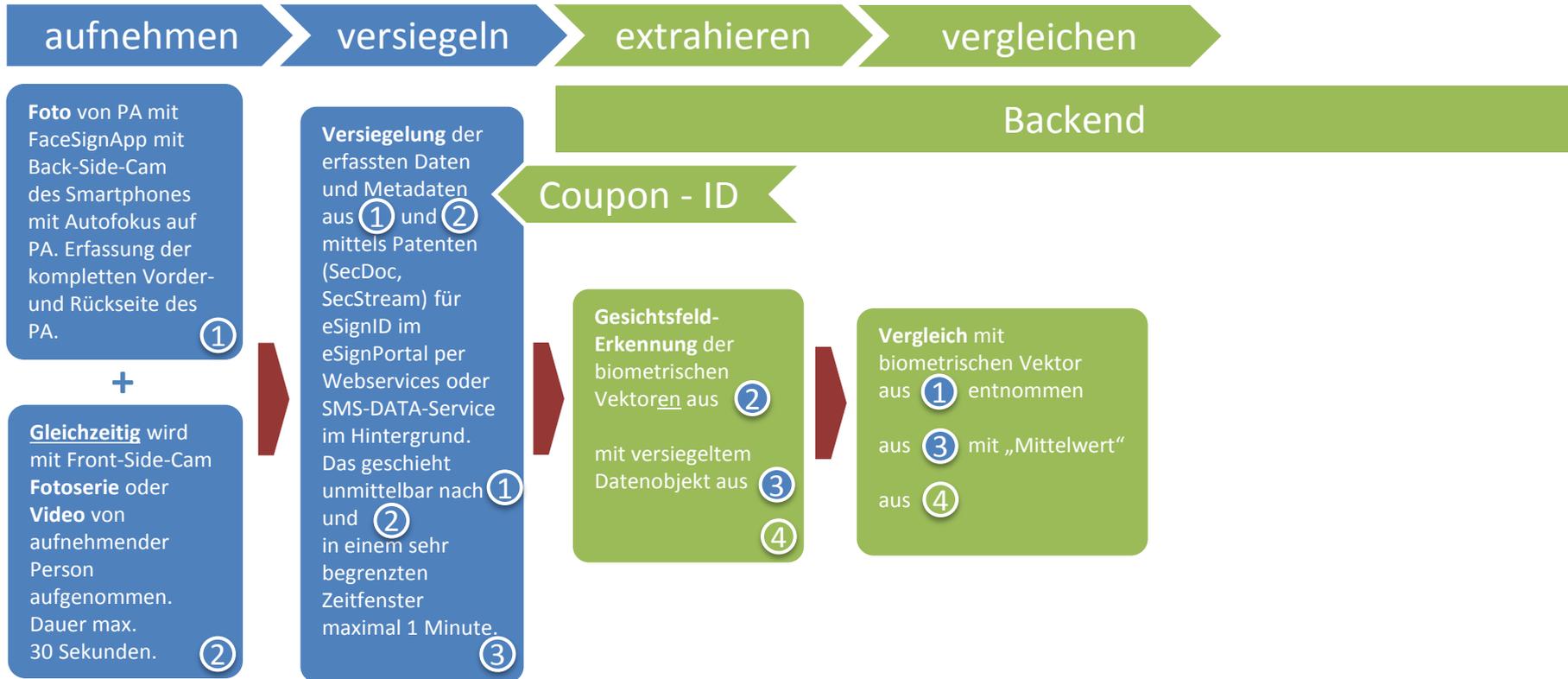
Gleichzeitig wird mit Front-Side-Cam **Fotoserie** oder **Video** von aufnehmender Person aufgenommen. Dauer max. 30 Sekunden. ②

Versiegelung der erfassten Daten und Metadaten aus ① und ② mittels Patenten (SecDoc, SecStream) für eSignID im eSignPortal per Webservices oder SMS-DATA-Service im Hintergrund. Das geschieht unmittelbar nach ① und ② in einem sehr begrenzten Zeitfenster maximal 1 Minute. ③

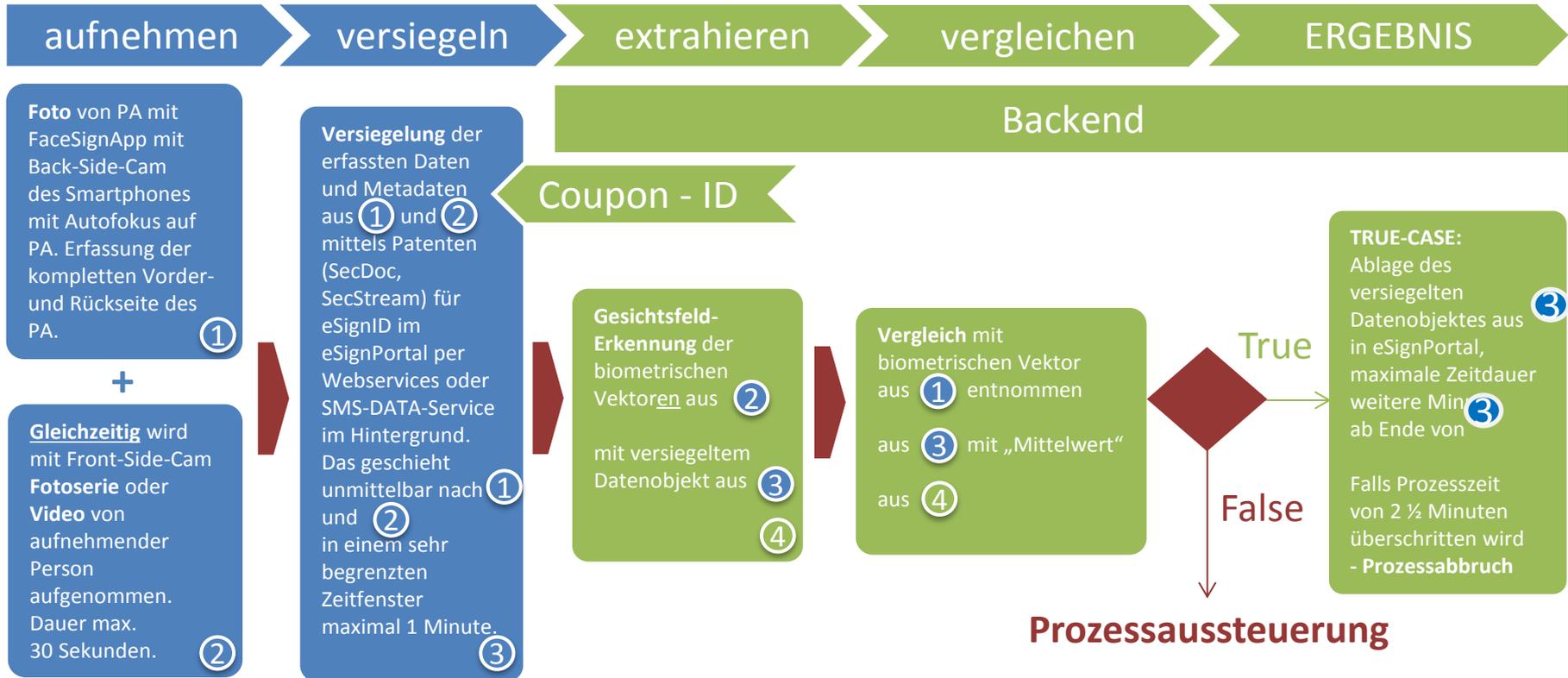
Gesichtsfeld-Erkennung der biometrischen Vektoren aus ② mit versiegeltem Datenobjekt aus ③ ④

Backend

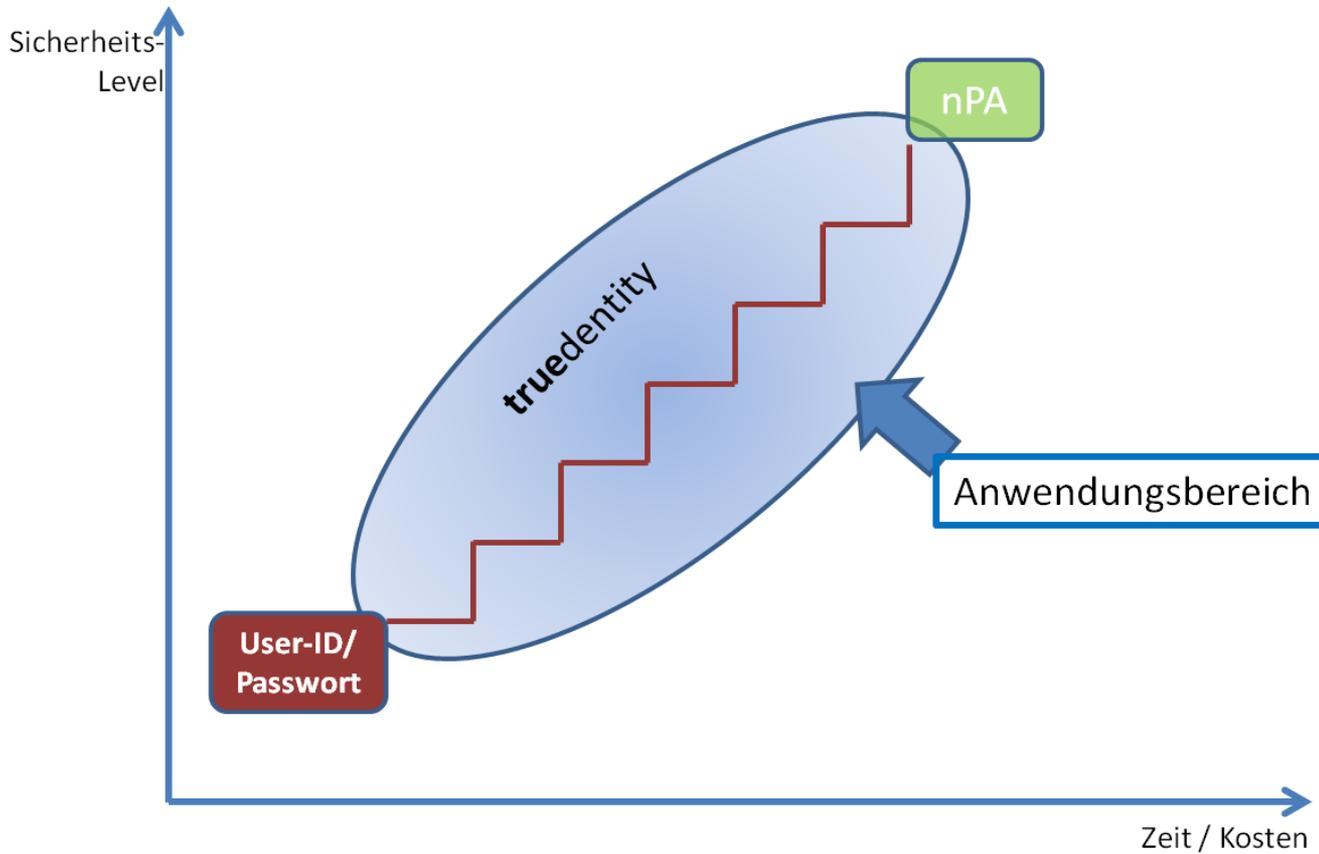
Facesign Prozess



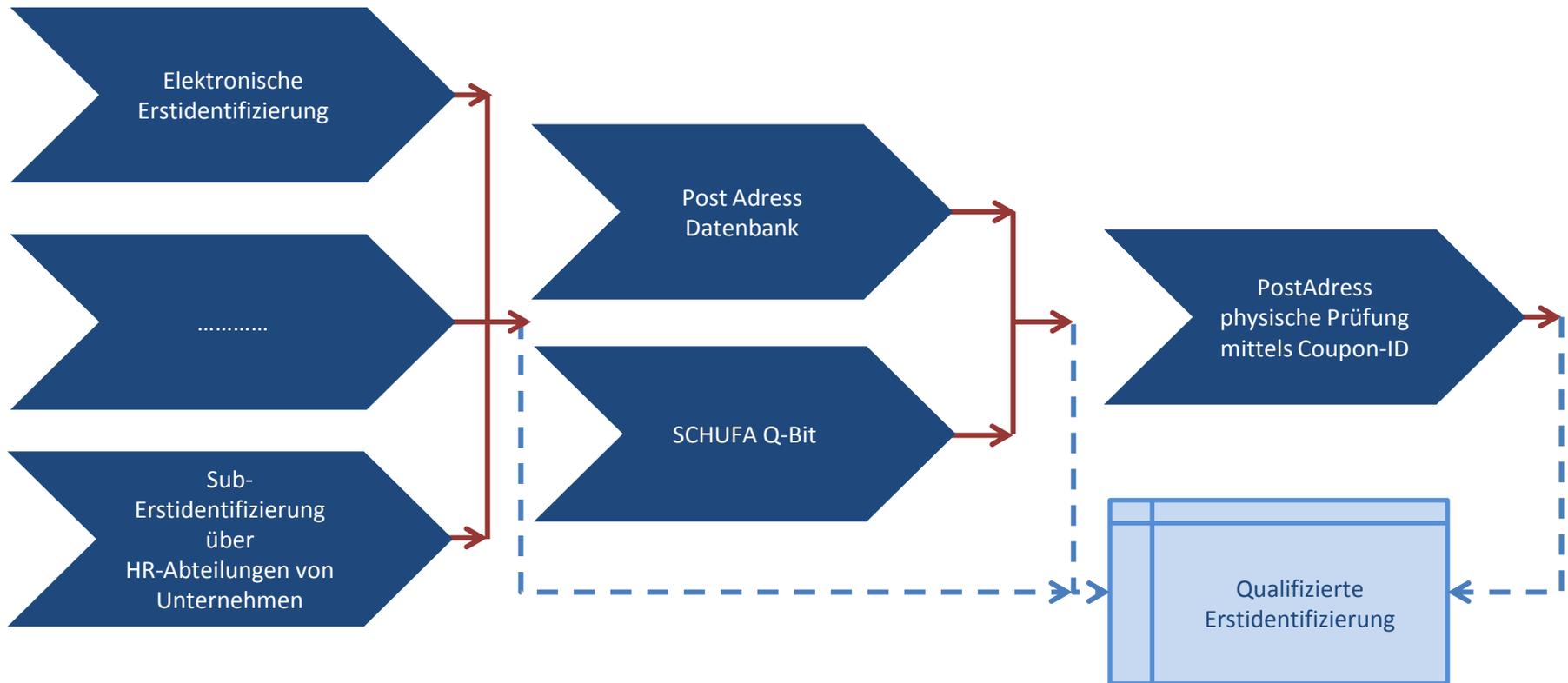
Facesign Prozess



Facesign Prozess



Facesign Prozess



Facesign Prozess

Co-Registrierungen zur Steigerung der Erstidentifizierungsstärke oder schneller Reichweitenerhöhung:

- ✓ SCHUFA
- ✓ Diverse Informationsdienste
- ✓ Mobilfunkverträge
- ✓ Verträge Customer mit Stadtwerken
- ✓ Coupon ID für Verifizierung von Adressdaten
- ✓ Personalabteilungen von Großkonzernen

Übergabe an GwG-Prozess

