Roundtable Digitale Identitäten & Banking – smart, secure, usable

DIGITALE IDENTITÄTEN / AUTHENTISIERUNGSMITTEL IM NATIONALEN UND INTERNATIONALEN UMFELD

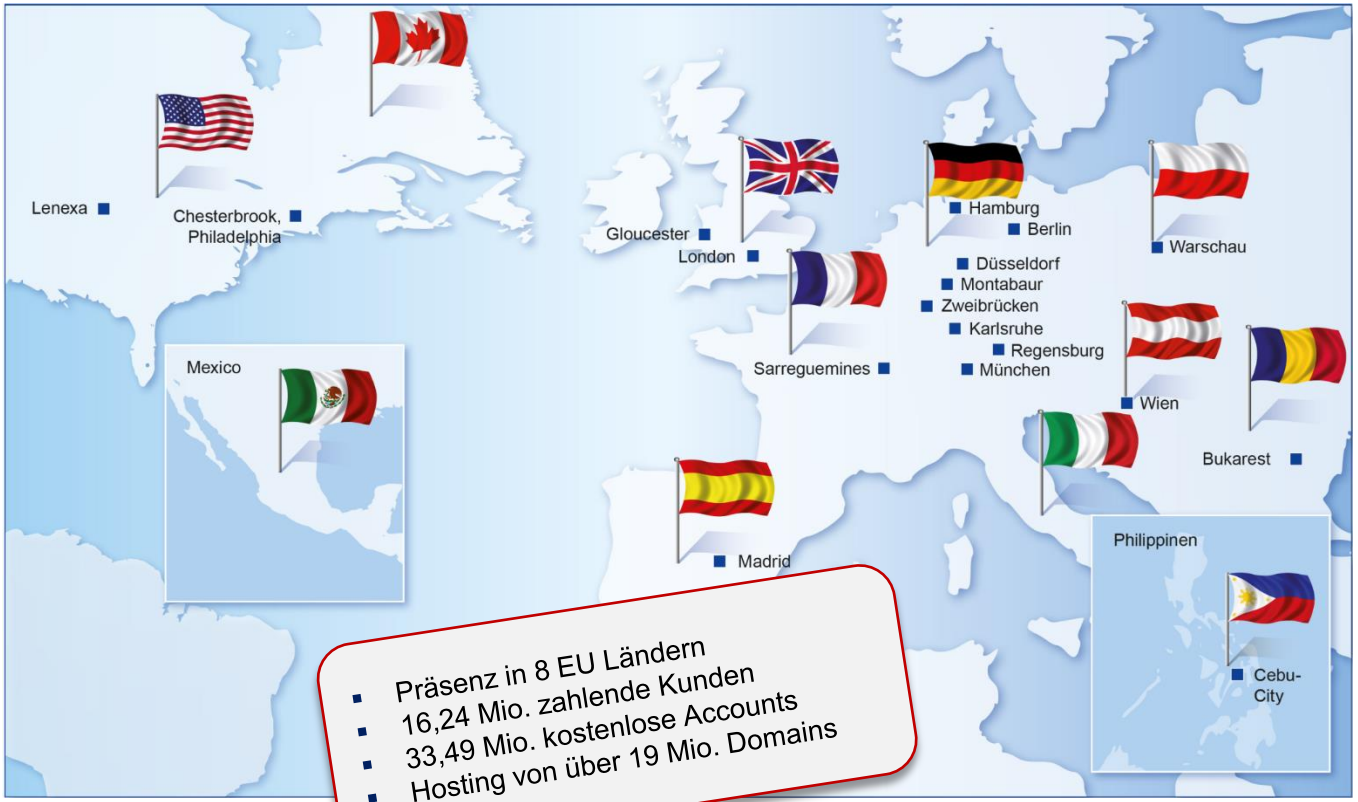
Sven Gelzhäuser
Head of Professional Services De-Mail & Trust Services
1&1 De-Mail GmbH – Member of United Internet

Agenda

- [x] 1&1 – Member of United Internet
- [x] Identifizierung
- [ ] Regularien & Verfahren national / international
- [ ] LOA4 vs. LOA3
- [ ] Exkurs Vertrauensdienstegesetz
- [ ] Chancen ohne Risiken?
- [ ] Risiken
- [ ] So klappt es!
- [x] Authentisierung
- [x] Fazit

1&1 - Member of United Internet AG (1/2)

1&1 - Member of United Internet AG (2/2)



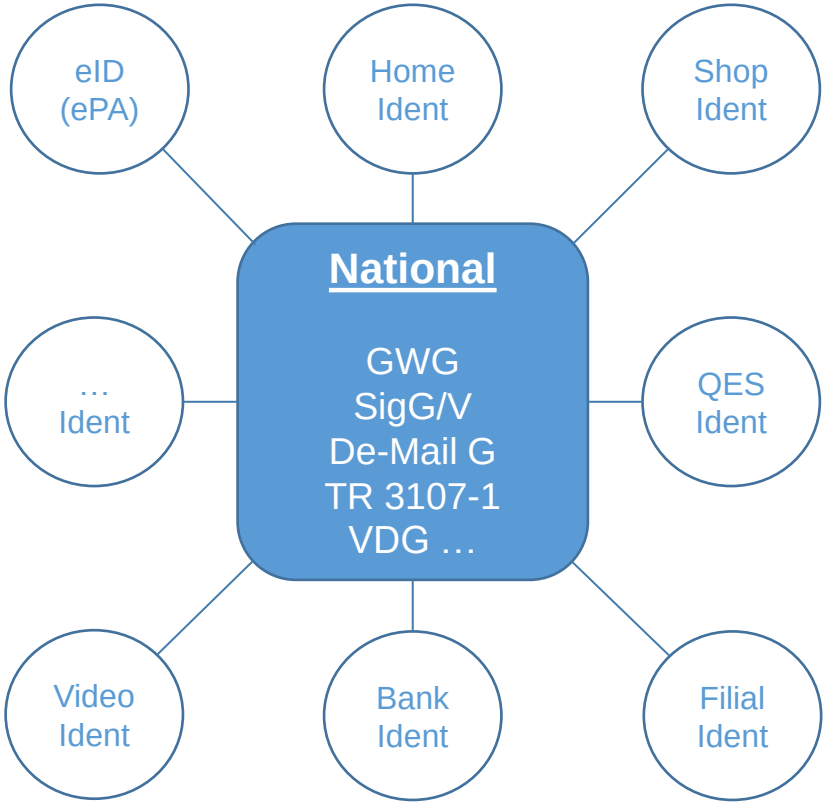
- Präsenz in 8 EU Ländern
- 16,24 Mio. zahlende Kunden
- 33,49 Mio. kostenlose Accounts
- Hosting von über 19 Mio. Domains

Identifizierung?

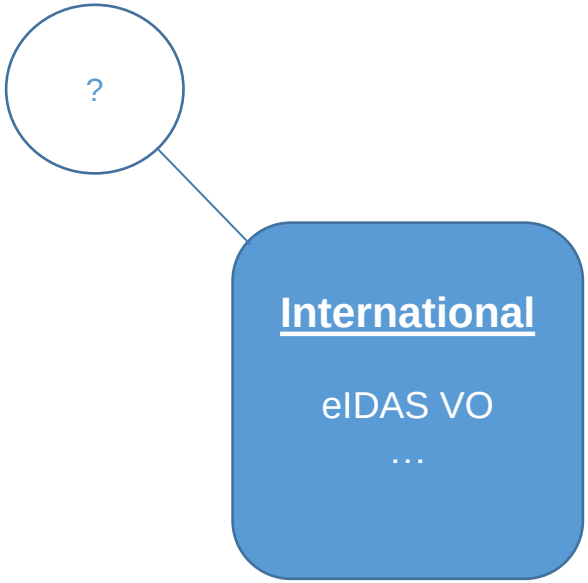
These

- Kurz- und mittelfristig werden **digitale Identitäten** immer wichtiger um vielfältige UseCases online ausführen zu können
- Bürger, Unternehmen der Privatwirtschaft und öffentliche Verwaltung **benötigen digitale Identitäten**
- Es gibt heute **unterschiedliche digitale Identitäten** auf **unterschiedliche Niveaus** (niedrig, substantiell und hoch) bspw. Facebook vs. De-Mail
- **eID Funktion** des ePA kann (noch) ausgeklammert werden, solange **keine signifikante** Durchdringung erzielt werden kann

Regularien & Verfahren zur Identifizierung (national)



Regularien & Verfahren zur Identifizierung (international)



Art. 24 eIDAS VO

1. **Persönliche Anwesenheit**
2. **Elektronische Identifizierungsmittel** auf Basis persönlicher Anwesenheit (ePA)
3. Zertifikat einer **qualifizierten Signatur/Siegel**
4. **Sonstige Identifizierungsmethoden,** die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit bieten

Regularien & Verfahren zur Identifizierung (Europa)

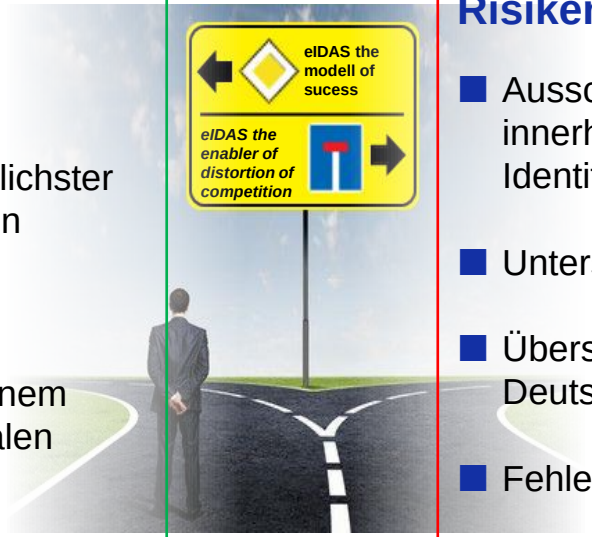
Art. 24 eIDAS VO

1. Persönliche Anwesenheit
2. Elektronische Identifizierungsmittel auf Basis persönlicher Anwesenheit (ePA)
3. Zertifikat einer qualifizierten Signatur/Siegel
4. Sonstige Identifizierungsmethoden, die auf nationaler Ebene anerkannt sind und gleichwertige Sicherheit bieten

Chancen ohne Risiko?

Chancen

- EU-weite Standardisierung
- Harmonisierung unterschiedlichster Lösungen der Mitgliedstaaten
- Einheitliche Anforderungen
- Einheitliches Spielfeld auf einem einzigen europäischen digitalen Markt



Risiken

- Ausschließlich abstrakte Regeln innerhalb der eIDAS VO zur Identifizierung
- Unterschiedliche Interpretation
- Überspitzte Anforderungen in Deutschland LOA4
- Fehlende UseCases

Gefahr der unterschiedlichen Auslegung der Verordnung durch die Mitgliedstaaten sowie der Unternehmen

§ 10 Identitätsprüfung Vertrauensdienstegesetz (1/2)

(1) Die **Bundesnetzagentur legt** nach Anhörung der betroffenen Kreise und **im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik** durch Verfügung im Amtsblatt fest, welche **sonstigen Identifizierungsmethoden** im Sinne des Artikels 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 **anerkannt sind** und **welche Mindestanforderungen** dafür jeweils gelten.

(2) Die Bundesnetzagentur überprüft die Verfügung nach Absatz 1 regelmäßig im Abstand von vier Jahren sowie

1. bei der begründeten Annahme, dass Methoden nicht mehr hinreichend sicher sind, oder
2. auf Ersuchen des Bundesamtes für Sicherheit in der Informationstechnik.

§ 10 Identitätsprüfung Vertrauensdienstegesetz (2/2)

(3) **Innovative Identifizierungsmethoden**, die noch nicht durch Verfügung im Amtsblatt anerkannt sind, **können von der Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik** und nach Anhörung **der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit** für einen Zeitraum von bis zu zwei Jahren **vorläufig anerkannt werden**, sofern eine **Konformitätsbewertungsstelle** die **gleichwertige Sicherheit** der Identifizierungsmethode im Sinne des Artikels 24 Absatz 1 Unterabsatz 2 Buchstabe d der Verordnung (EU) Nr. 910/2014 **bestätigt** hat. (…)

(4) Der **qualifizierte Vertrauensdiensteanbieter darf** nach Maßgabe der datenschutzrechtlichen Bestimmungen **personenbezogene Daten nutzen**, die zu **einem früheren Zeitpunkt** im Rahmen einer **ordnungsgemäßen Identitätsprüfung erhoben wurden**, sofern und soweit diese Daten zum Zeitpunkt der Antragstellung die zuverlässige Identitätsfeststellung des Antragstellers gewährleisten.

Risiken

- **Die Interpretationsbedürftigkeit der eIDAS VO / VDG führt zu**
  - **unterschiedliche Anforderungen** an die Konformität mit **unterschiedlichem Maßstab LOA3 vs. LOA4**
  - unterschiedliche **Marktzutrittsbarrieren** für **TSPs**
  - unterschiedliche **Barrieren** für **Produkte**
  - **Überspitzung** der Anfordergen: Harmonisierungsversuch auf das höchste Level, das nicht nutzbar ist, während in anderen Mitgliedstaaten geringere Anforderungen ausreichen

- **Konsequenzen**
  - **Marktverzerrung** und Unsicherheit auf Nutzerseite
  - **Niedrigstes Zugangslevel** wird immer der **preiswerteste** Anbieter sein
  - Die **Sicherheitslage** in der EU wird sich insgesamt **verschlechtern**

⇨ Der Markt bleibt so heterogen (und unsicher) wie heute, aber auf einer einheitlichen europäischen rechtlichen Grundlage

So funktioniert es!

- **Einheitliches Spielfeld**
  - Nationale Harmonisierung der Anforderungen an Identifizierung auf Basis LOA3
  - Gegebenenfalls sinnvoll in besonderen Ausnahmen (bspw. De-Mail) höhere Anforderungen zu stellen
- **Förderung einer schnellen Verbreitung in allen Zielgruppen**
  - Sichtbares und verbindliches Angebot durch die öffentliche Verwaltung/Sektor
  - Sichtbarkeit für den Endnutzer
  - Beteiligung von Einrichtungen, die alle notwendigen Informationen verbreiten
- **Verbesserung der Nutzungsmöglichkeiten und Schaffung von Anreizen**
  - Reduzierung von Einstiegshürden
  - Subventionierung der Nutzung

Authentisierung?

Grundsatz: Gleiche Anforderung wie an Identifizierung = LOA3

Etablierte Verfahren

- mTAN
- PushTAN
- Flickr
- OTP-Generatoren
- ePA
- ….

müssen **weiterhin** unter der Voraussetzung der gleichwertigen Sicherheit sowie Stand der Technik ihre **Existenzberechtigung** haben.

Zukünftige Verfahren

- De-Mail Identitäten
- De-Mail Altersverifikation
- SSO via De-Mail
- …

müssen ihre Chance bekommen eine **gleichwertige Sicherheit nachweisen** zu können.

Fazit: Identifizierung & Authentisierung

- Diskussionen um die zwingende Einführung von LOA4 bei Identifizierung und Authentisierung bringen **weder UseCases** noch eine **Akzeptanz** bei Nutzerschaft

- Harmonisierung der Identifizierung und Authentisierung nebst Verfahren auf LOA 3 Ebene zwingend erforderlich

- Deutsche **Sonderbetrachtungsweisen** führen nur dazu, dass sich der komplette Markt ins Ausland verschiebt wird

- **Gleiche Regelungen** / Akzeptanz für alle Identverfahren auf **nationaler Ebene** bspw. bei VideoIdent und BankIdent

Fragen?

Kontakt

Sven Gelzhäuser
Head of Professional Services

1&1 De-Mail GmbH

Ernst-Frey-Straße 10
76135 Karlsruhe
Germany

Phone +49 721 91374-4647
sven.gelzhaeuser@1und1.de
sven.gelzhaeuser@1und1.de-mail.de
www.1und1.de

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!