



## Informationstag "Elektronische Signatur"

Gemeinsame Veranstaltung von TeleTrust und VOI

Berlin, 18.09.2014

# eIDAS as a Service – Gibt es die starke Authentisierung und die elektronische Signatur bald aus der Cloud?

Dr. Detlef Hühnlein

ecsec GmbH

# Agenda

---

- Einleitung
- eIDAS as a Service
- Zusammenfassung

# Agenda

## ■ Einleitung

### □ Cloud Computing

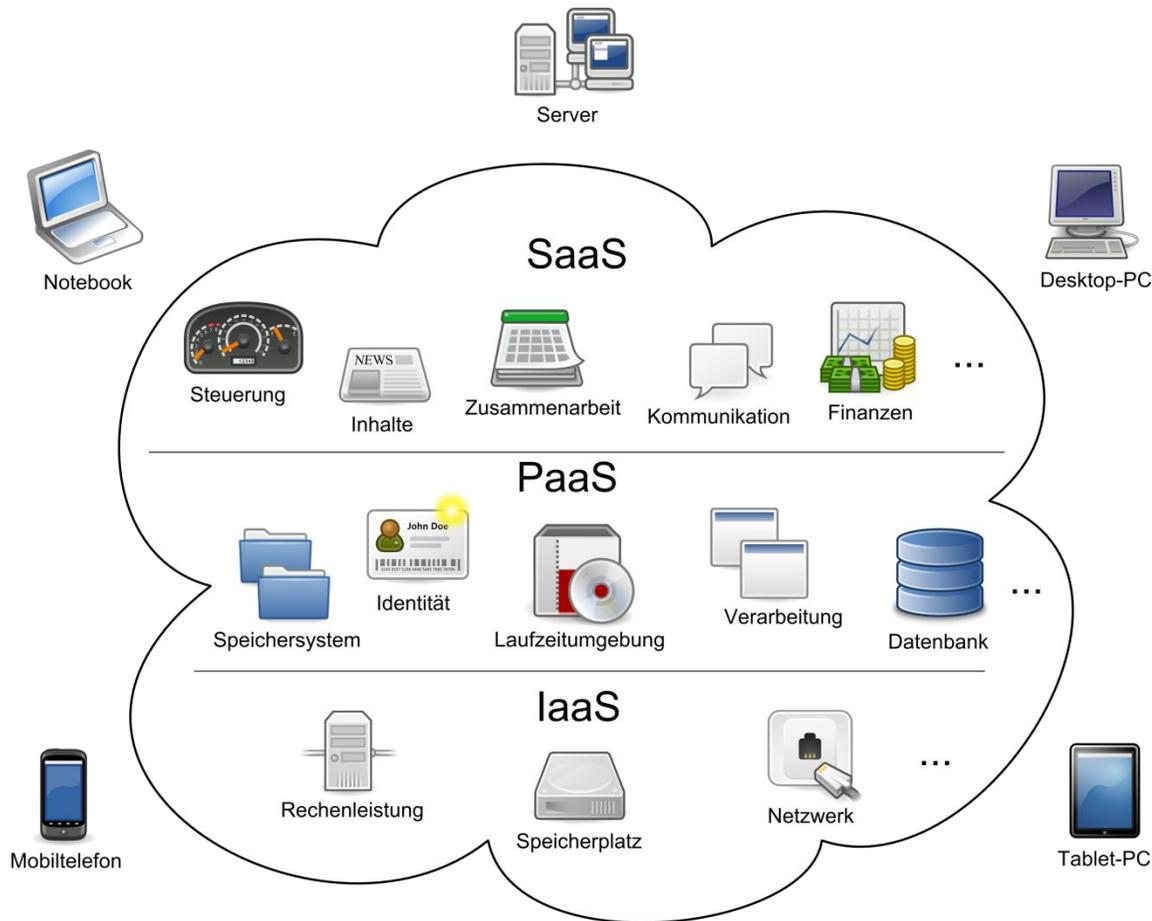
□ eIDAS-Verordnung (2014/910/EU)

□ Auf dem Weg zum IT-Sicherheitsgesetz

## ■ eIDAS as a Service

## ■ Zusammenfassung

# Cloud Computing

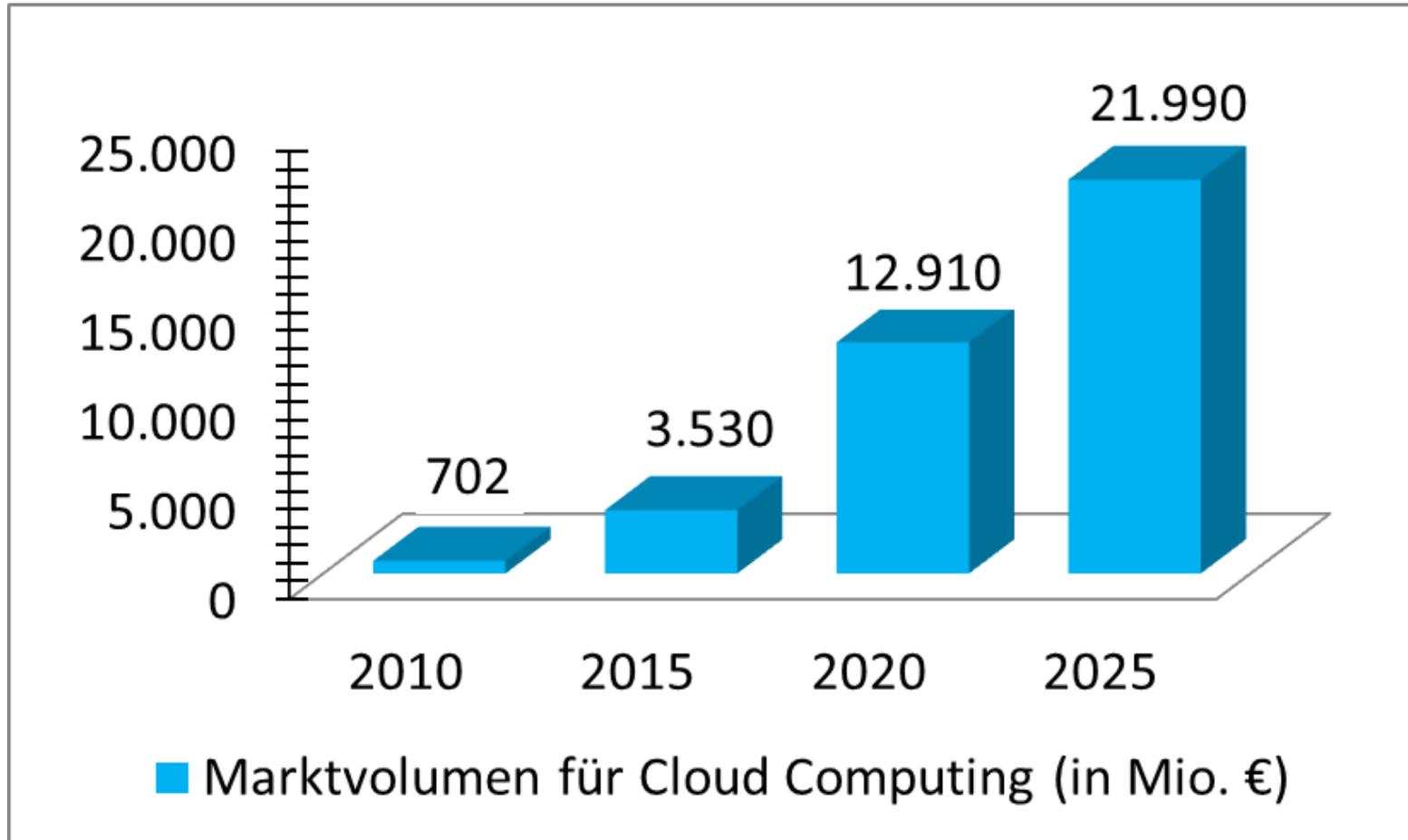


- **Bedarfsorientierung**
- **Selbstbedienung**
- **Netzwerkzugriff**
- **Ressourcenbündelung**
- **Elastische Leistung**
- **Messbare Dienste**

Quelle: <http://de.wikipedia.org/wiki/Cloud-Computing>

Quelle: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

# Cloud Computing – Wachstumsmarkt



Quelle: *Das wirtschaftliche Potenzial des Internet der Dienste*, Studie im Auftrag des BMWi,  
[http://ftp.zew.de/pub/zew-docs/gutachten/IDD\\_Endbericht\\_Nov2010.pdf](http://ftp.zew.de/pub/zew-docs/gutachten/IDD_Endbericht_Nov2010.pdf)

# Sicherheitsempfehlungen des BSI für Cloud Computing Anbieter



ID- und Rechtemanagement	Private ⇔			Public ↗		
	B	C+	A+	B	C+	A+
Starke Authentisierung (Zwei-Faktor-Authentisierung) für Administratoren des CSP	✓			✓		
Rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte	✓			✓		
Least Privilege Model (Nutzer bzw. CSP-Administratoren sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen)	✓			✓		
Vier-Augen-Prinzip für kritische Administrations-tätigkeiten		✓	✓		✓	✓
Starke Authentisierung (z. B. Zwei-Faktor-Authentisierung) für Cloud-Kunden		✓			✓	

# Agenda

- **Einleitung**
  - Cloud Computing
  - **eIDAS-Verordnung (2014/910/EU)**
  - Auf dem Weg zum IT-Sicherheitsgesetz
- eIDAS as a Service
- Zusammenfassung

## eIDAS-Verordnung (2014/910/EU)

- I. Allgemeine Bestimmungen (Artikel 1-5)
- II. Elektronische Identifizierung (Artikel 6-12)
- III. Vertrauensdienste
  - 1. Allgemeine Bestimmungen (Artikel 13-16)
  - 2. Aufsicht (Artikel 17-19)
  - 3. Qualifizierte Vertrauensdienste (Artikel 20-24)
  - 4. Elektronische Signaturen (Artikel 25-34)
  - 5. Elektronische Siegel (Artikel 35-40)
  - 6. Elektronische Zeitstempel (Artikel 41-42)
  - 7. Dienste für die Zustellung elektronischer Einschreiben (Artikel 43-44)
  - 8. Website-Authentifizierung (Artikel 45)
- IV. Elektronische Dokumente (Artikel 46)
- V. Befugnisübertragungen und Durchführungsbestimmungen (Artikel 47-48)
- VI. Schlussbestimmungen (Artikel 49-52)

# Agenda

## ■ Einleitung

- Cloud Computing
- eIDAS-Verordnung (2014/910/EU)

## □ **Auf dem Weg zum IT-Sicherheitsgesetz**

- eIDAS as a Service
- Zusammenfassung

# 16 Millionen Identitäten gestohlen (21.01.2014)

## Millionenfacher Identitätsdiebstahl: BSI bietet Sicherheitstest für E-Mail-Adressen

16 Millionen Digitale Identitäten betroffen

Bonn, 21.01.2014.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat angesichts eines Falles von großflächigem Identitätsdiebstahl unter <https://www.sicherheitstest.bsi.de> eine Webseite eingerichtet, auf der Bürgerinnen und Bürger überprüfen können, ob sie von diesem Identitätsdiebstahl betroffen sind. Im Rahmen der Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden wurden rund 16 Millionen kompromittierte Benutzerkonten entdeckt. Diese bestehen in der Regel aus einem Benutzernamen in Form einer E-Mail-Adresse und einem Passwort. Viele Internetnutzer verwenden diese Login-Daten nicht nur für das eigene Mail-Account, sondern auch für Benutzerkonten bei Internetdiensten, Online-Shops oder Sozialen Netzwerken. Die E-Mail-Adressen wurden dem BSI übergeben, damit Betroffene informiert werden und erforderliche Schutzmaßnahmen treffen können.

Auf der Webseite <https://www.sicherheitstest.bsi.de>, die das BSI mit Unterstützung der Deutschen Telekom eingerichtet hat, können Internetnutzer ihre E-Mail-Adresse eingeben, um zu überprüfen, ob sie von dem Identitätsdiebstahl betroffen sind. Die eingegebene Adresse wird dann in einem technischen Verfahren vom BSI mit den Daten aus den Botnetzen abgeglichen. Ist die Adresse und damit auch die Digitale Identität des Nutzers betroffen, so erhält dieser eine entsprechende Information per E-Mail an die angegebene Adresse. Diese Antwort-Mail enthält auch Empfehlungen zu erforderlichen Schutzmaßnahmen. Ist die eingegebene E-Mail-Adresse nicht betroffen, so erhält der Nutzer keine Benachrichtigung.

# 18 Millionen Identitäten gestohlen (07.04.2014)

## Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene

Bonn, 07.04.2014.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert angesichts eines erneuten Falles von großflächigem Identitätsdiebstahl betroffene Bürgerinnen und Bürger in Deutschland. Die Staatsanwaltschaft Verden (Aller) hat dem BSI einen Datensatz mit rund 21 Millionen E-Mail-Adressen und Passwörtern zur Verfügung gestellt. Nach technischer Analyse und Bereinigung durch das BSI verblieben rund 18 Millionen von Identitätsdiebstahl betroffene E-Mail-Adressen, darunter rund 3 Millionen deutsche E-Mail-Adressen. Die Inhaber der E-Mail-Adressen werden vom BSI in Zusammenarbeit mit den Online-Dienstleistern Deutsche Telekom, Freenet, gmx.de, Kabel Deutschland, Vodafone und web.de informiert. Zudem stellt das BSI wieder einen webbasierten Sicherheitstest zur Verfügung.

Die digitalen Identitäten sind im Rahmen eines laufenden Ermittlungsverfahrens gefunden worden. Mit den E-Mail-Adressen und den zugehörigen Passwörtern versuchen Kriminelle mithilfe eines Botnetzes, sich in E-Mail-Accounts einzuloggen und diese für den Versand von SPAM-Mails zu missbrauchen. Das Botnetz ist noch in Betrieb, die gestohlenen Identitäten werden aktiv ausgenutzt. Es ist davon auszugehen, dass es sich bei den gefundenen Adressen und Passwörtern sowohl um Zugangsdaten zu E-Mail-Konten als auch um Zugangsdaten zu anderen Online-Accounts wie Online-Shops, Internet-Foren oder Sozialen Netzwerken handelt.

# Milliardenfacher Identitätsdiebstahl: Stellungnahme des BSI (06.08.2014)

## Milliardenfacher Identitätsdiebstahl: Stellungnahme des BSI

BSI ruft Online-Anbieter auf, mehr für IT-Sicherheit und den Schutz von Kundendaten zu tun

Bonn, 06.08.2014.

Die "New York Times" berichtet in ihrer Ausgabe vom 6. August 2014 über die Aufdeckung eines Datendiebstahls, bei dem von Online-Kriminellen rund 1,2 Milliarden digitale Identitäten in Form von Kombinationen von Benutzernamen und Passwörtern sowie mehr als 500 Millionen E-Mail-Adressen gestohlen wurden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) prüft derzeit mit Hochdruck zusammen mit den zuständigen deutschen und amerikanischen Behörden, ob deutsche Internetnutzer und Online-Anbieter von dem Vorfall betroffen sind. Sollte die Zahl von 1,2 Milliarden gestohlener digitaler Identitäten zutreffen, so ist mit hoher Wahrscheinlichkeit davon auszugehen, dass sich auch deutsche Internetnutzer darunter befinden. Derzeit gibt es für Privatanwender keine Möglichkeit festzustellen, ob sie von dem Vorfall betroffen sind. Internetnutzer, die die [Empfehlungen des BSI zum sicheren Internetsurfen](#) berücksichtigen, haben ihrerseits das Bestmögliche getan, um ihre digitalen Identitäten zu sichern.

## Online-Anbieter müssen mehr für die IT-Sicherheit ihrer Systeme tun

Den Berichten zufolge ist der Hauptansatzpunkt der Angreifer nicht der Rechner des privaten Internetnutzers, sondern liegt offenbar im Bereich der Webseiten und Datenbanken von Online-Anbietern. Das BSI ruft angesichts dieses erneuten Falles die Anbieter von Online-Diensten auf, mehr für die Sicherheit ihrer Systeme und die Sicherheit der Daten zu tun, die ihnen ihre Kunden anvertrauen. Beispielsweise sollten Daten und Datenbanken durchgängig verschlüsselt vorgehalten werden. Bekannt gewordene Schwachstellen in IT-Systemen und Software müssen rasch geschlossen werden. Darüber hinaus sollten den Nutzern sicherere Authentisierungsmöglichkeiten angeboten werden, beispielsweise eine Zwei-Faktor-Authentisierung, die über die Standard-Anmeldung per Benutzernamen und Passwort hinausgeht. Das BSI hat bereits 2011 [ein Eckpunktepapier mit Mindestanforderungen zur Informationssicherheit bei eCommerce-Systemen](#) veröffentlicht.

# IT-Sicherheitsgesetz (Entwurf vom 18.08.2014)

## Artikel 2

### Änderung des Telemediengesetzes

Das Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, wird wie folgt geändert:

1. § 13 wird wie folgt geändert:

a. Nach Absatz 6 wird folgender Absatz 7 eingefügt:

„(7) Diensteanbieter im Sinne von § 7 Absatz 1 und § 10 Absatz 1 haben, soweit dies technisch möglich und zumutbar ist, für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien durch die erforderlichen technischen und organisatorischen Vorkehrungen sicherzustellen, dass ein Zugriff auf die Telekommunikations- und Datenverarbeitungssysteme nur für Berechtigte möglich ist. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Bei personalisierten Telemediendiensten ist den Nutzern die Anwendung eines sicheren und dem Schutzbedarf angemessenen Authentifizierungsverfahrens anzubieten.“

b. Der bisherige Absatz 7 wird Absatz 8.

# Agenda

- Einleitung
- **eIDAS as a Service**
- Zusammenfassung

## eIDAS-Verordnung (2014/910/EU)

I. Allgemeine Bestimmungen (Artikel 1-5)

**II. Elektronische Identifizierung (Artikel 6-12)**

eIDAS

III. Vertrauensdienste

1. Allgemeine Bestimmungen (Artikel 13-16)

2. Aufsicht (Artikel 17-19)

3. Qualifizierte Vertrauensdienste (Artikel 20-24)

**4. Elektronische Signaturen (Artikel 25-34)**

**5. Elektronische Siegel (Artikel 35-40)**

**6. Elektronische Zeitstempel (Artikel 41-42)**

**7. Dienste für die Zustellung elektronischer Einschreiben (Artikel 43-44)**

**8. Website-Authentifizierung (Artikel 45)**

eIDAS

IV. Elektronische Dokumente (Artikel 46)

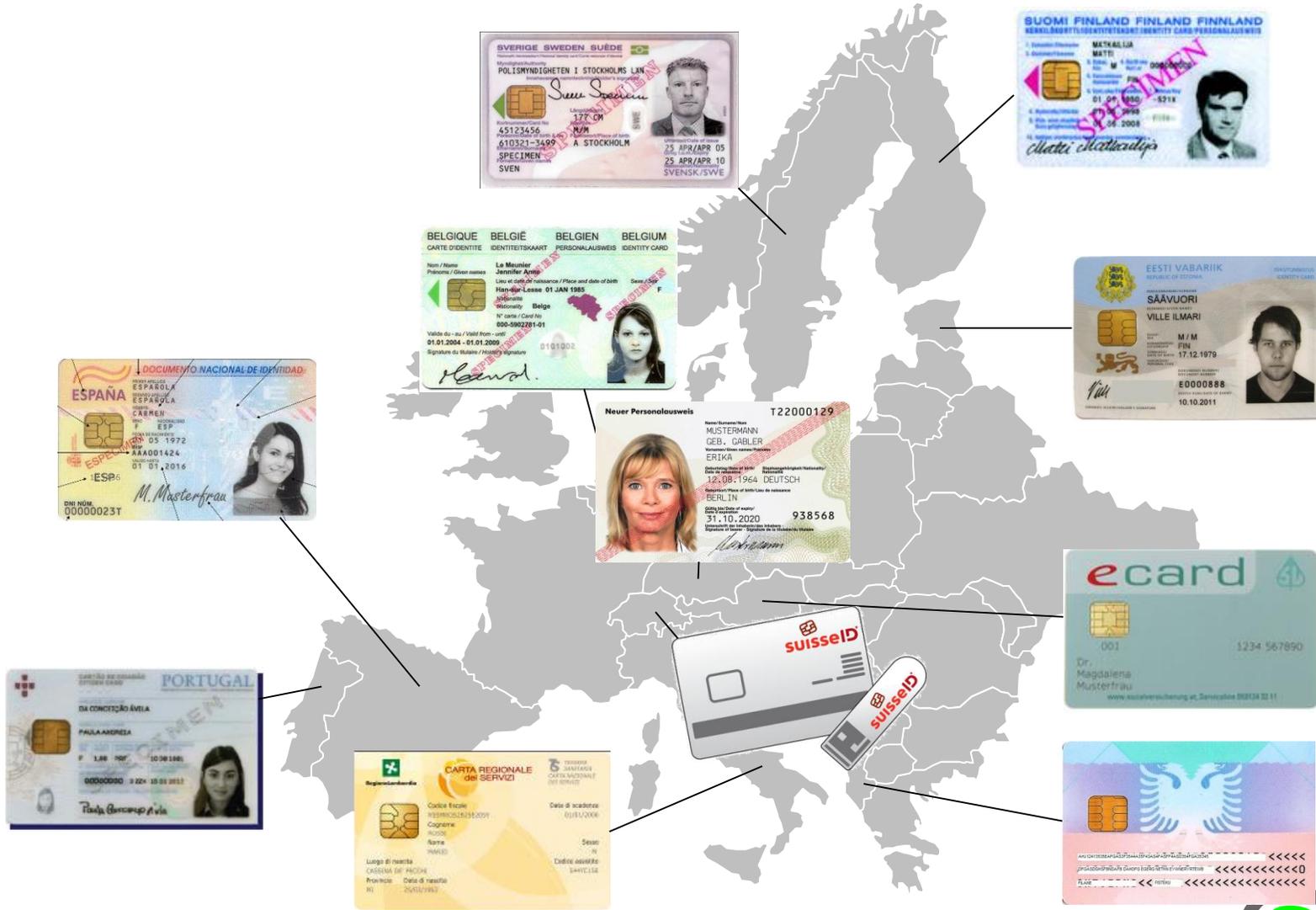
V. Befugnisübertragungen und Durchführungsbestimmungen  
(Artikel 47-48)

VI. Schlussbestimmungen (Artikel 49-52)

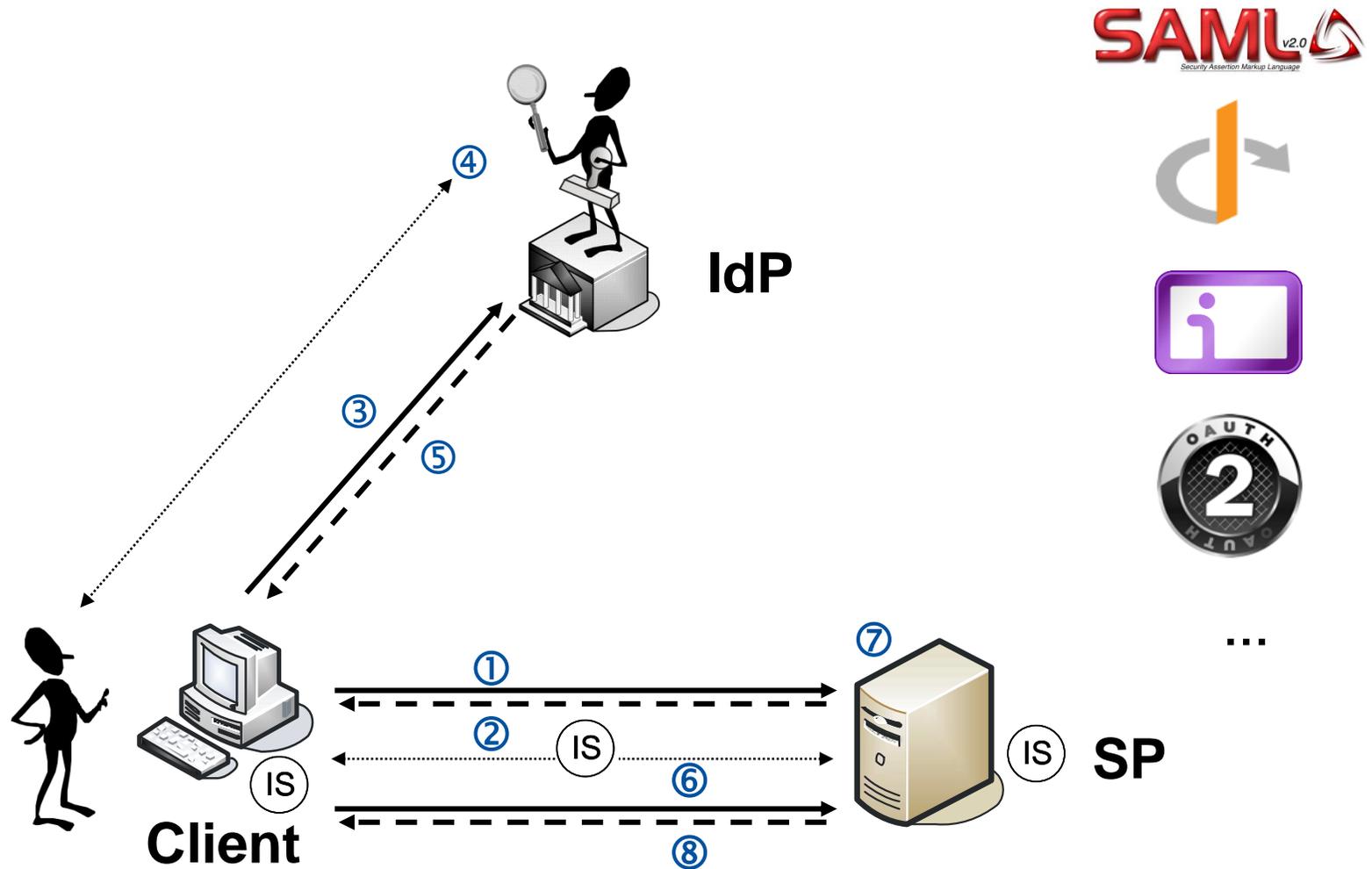
## II. Elektronische Identifizierung

- eID-Mechanismen im Verantwortungsbereich der Mitgliedstaaten können notifiziert (Art. 9) und dadurch gegenseitig anerkannt werden (Art. 6)
- eID-Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ (Art. 8) (Durchführungsrechtsakte (DRA) bis zum 18.09.2015)
- Der notifizierende Mitgliedstaat stellt Verfügbarkeit eines grenzüberschreitenden Authentifizierungsdienstes sicher (Art. 7).  
„Die grenzüberschreitende Authentifizierung sollte gebührenfrei sein, wenn sie in Bezug auf einen Online-Dienst erfolgt, der von einer öffentlichen Stelle erbracht wird.“
- Umgehende Meldung von Sicherheitsverletzungen, Behebung spätestens nach 3 Monaten (Art. 10)
- Der notifizierende Mitgliedstaat haftet für etwaige Schäden (Art. 11)
- Es wird ein eID-Interoperabilitätsrahmen geschaffen in dem die Mitgliedstaaten zusammenarbeiten (DRA bis 18.09.2015 bzw. 18.03.2015)

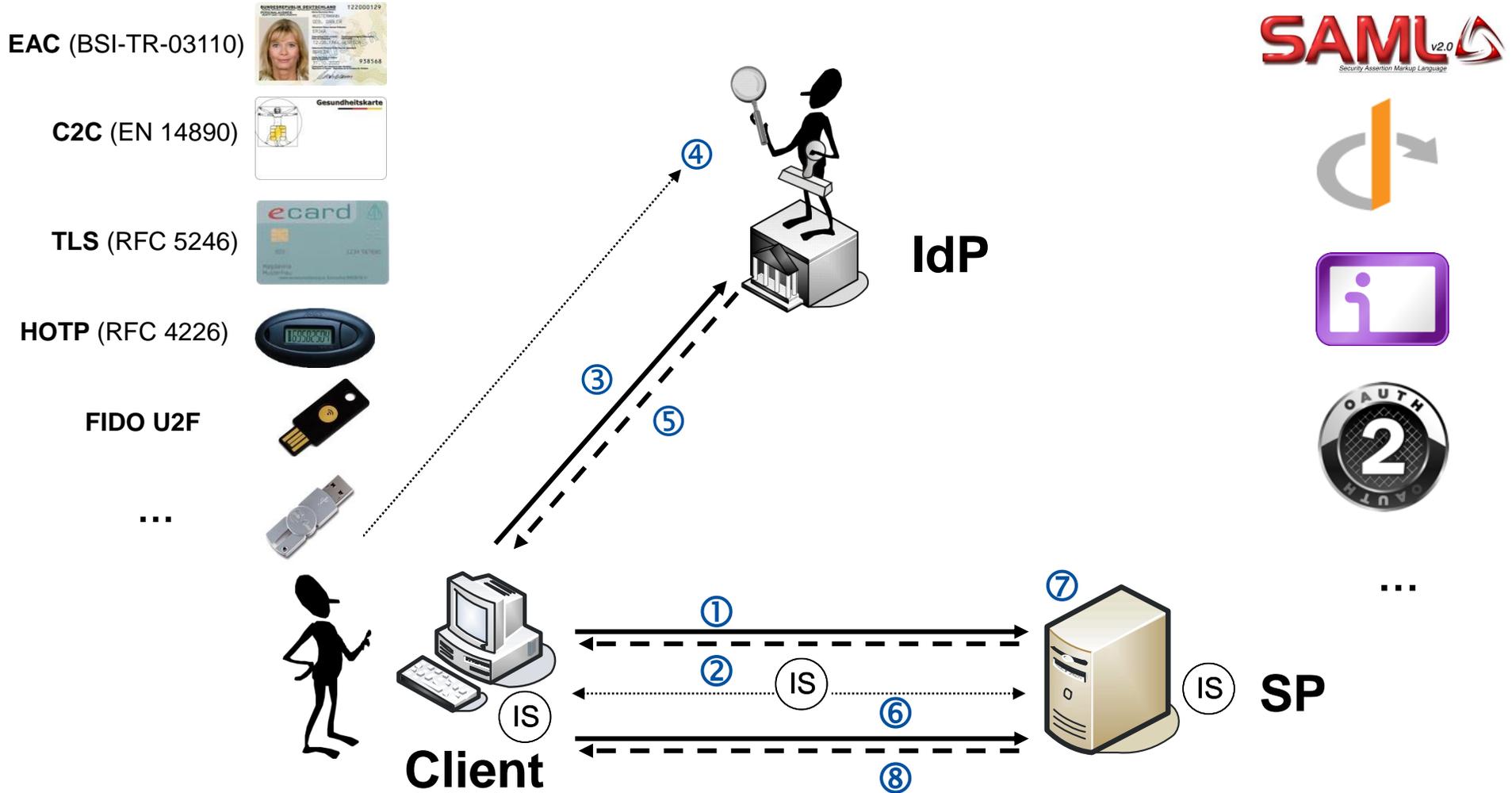
# Elektronische Ausweise in Europa



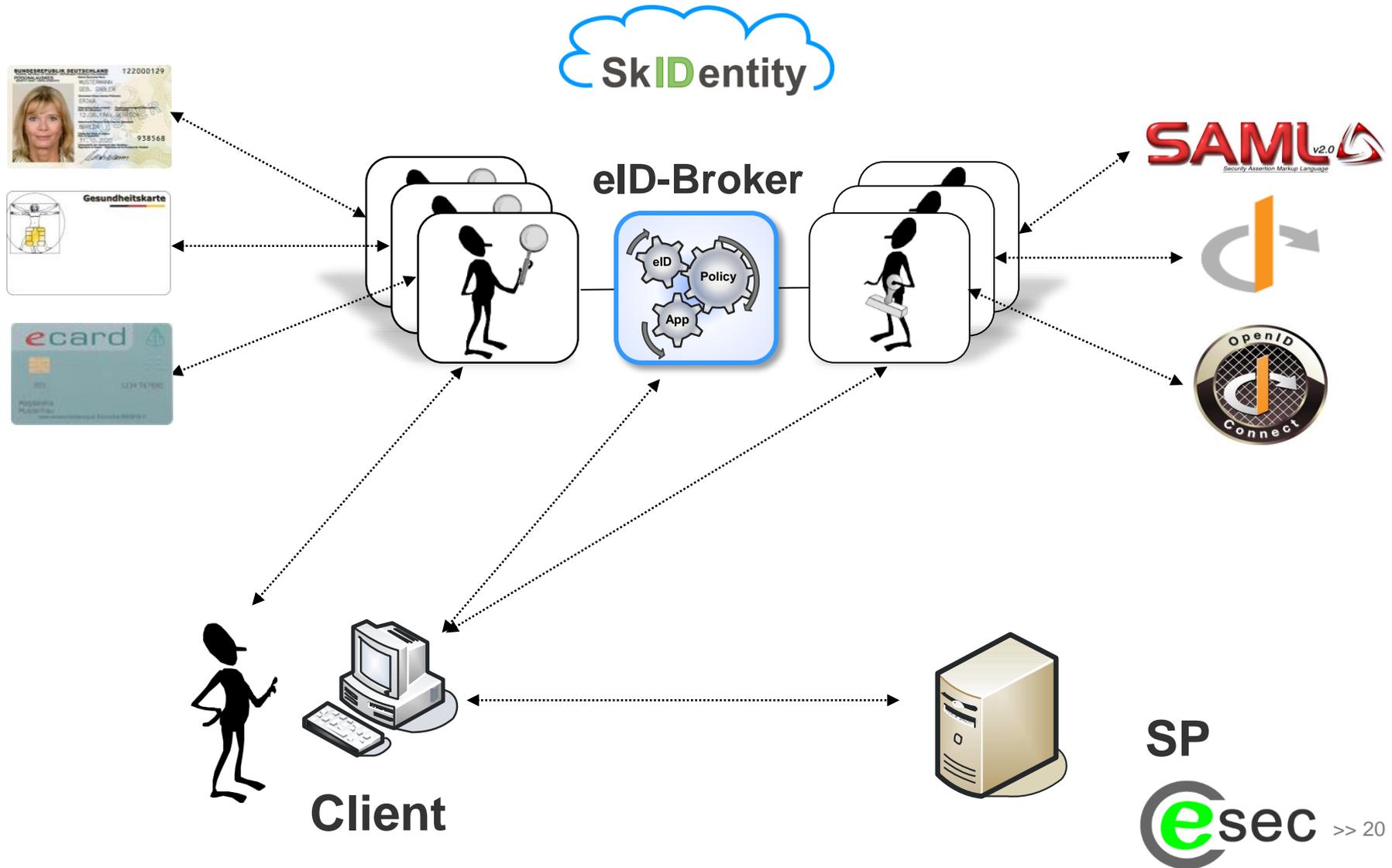
# Authentisierung in der Cloud



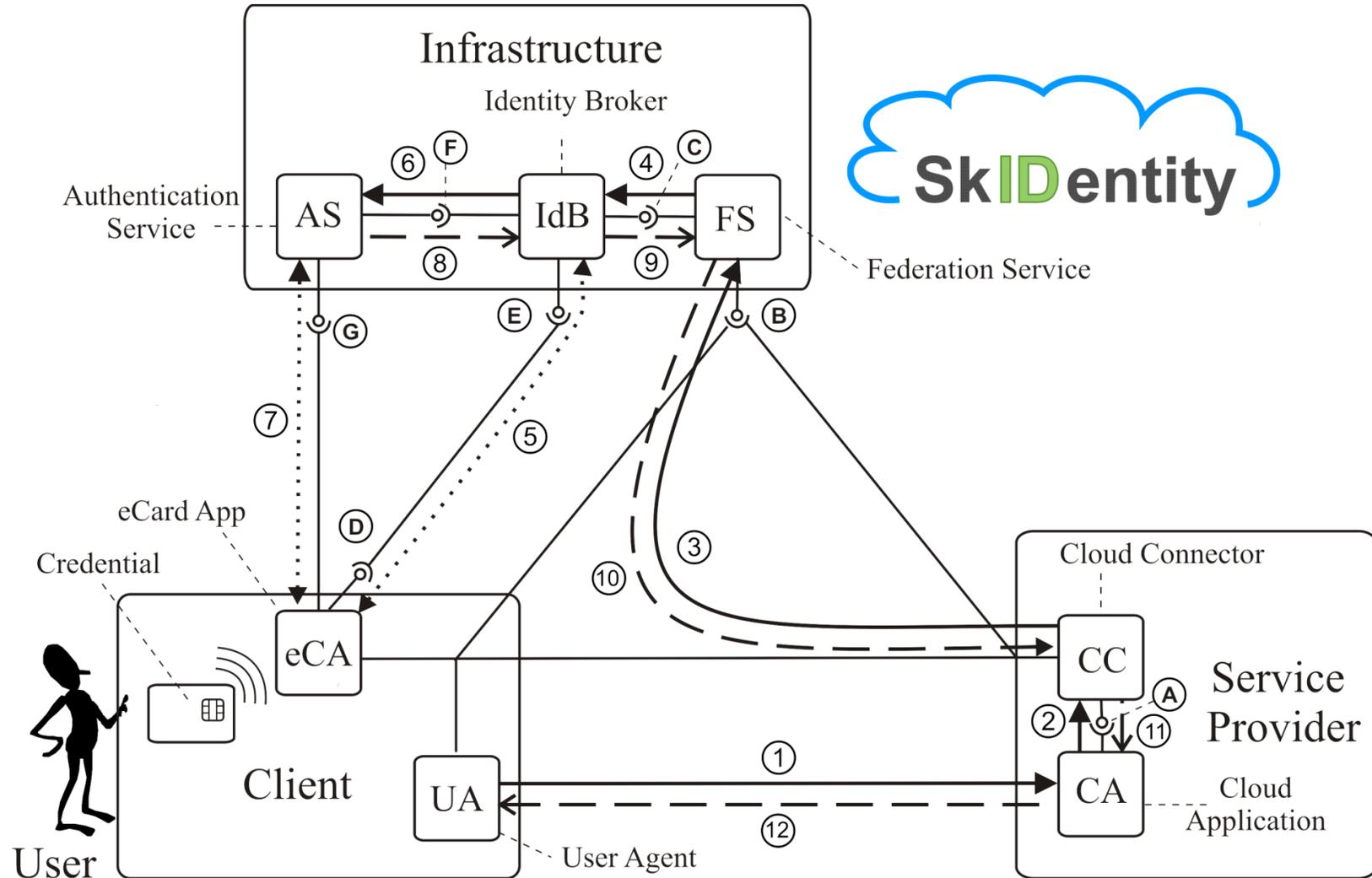
# Elektronische Ausweise in der Cloud



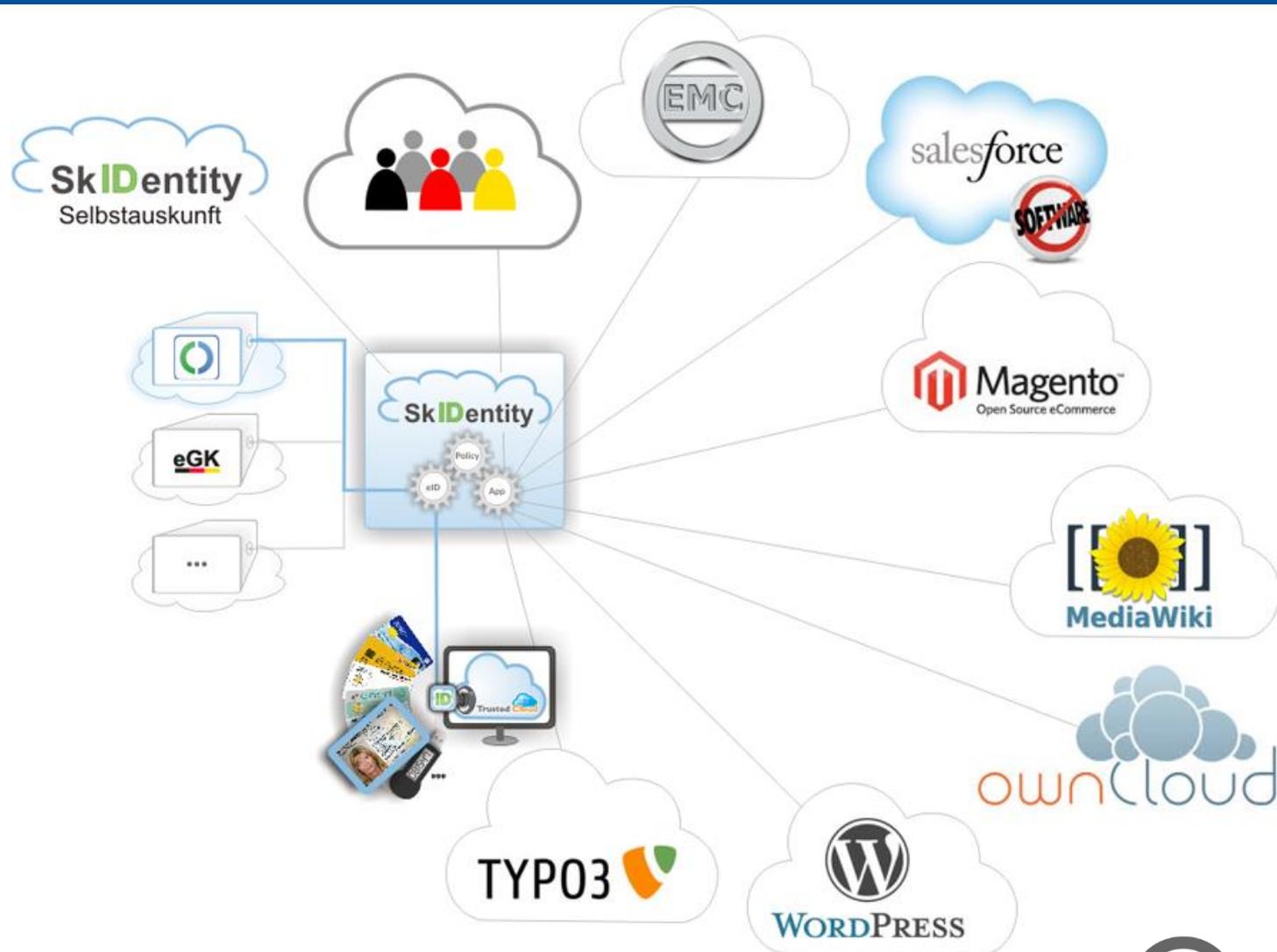
# SkIDentity – Lösungsansatz



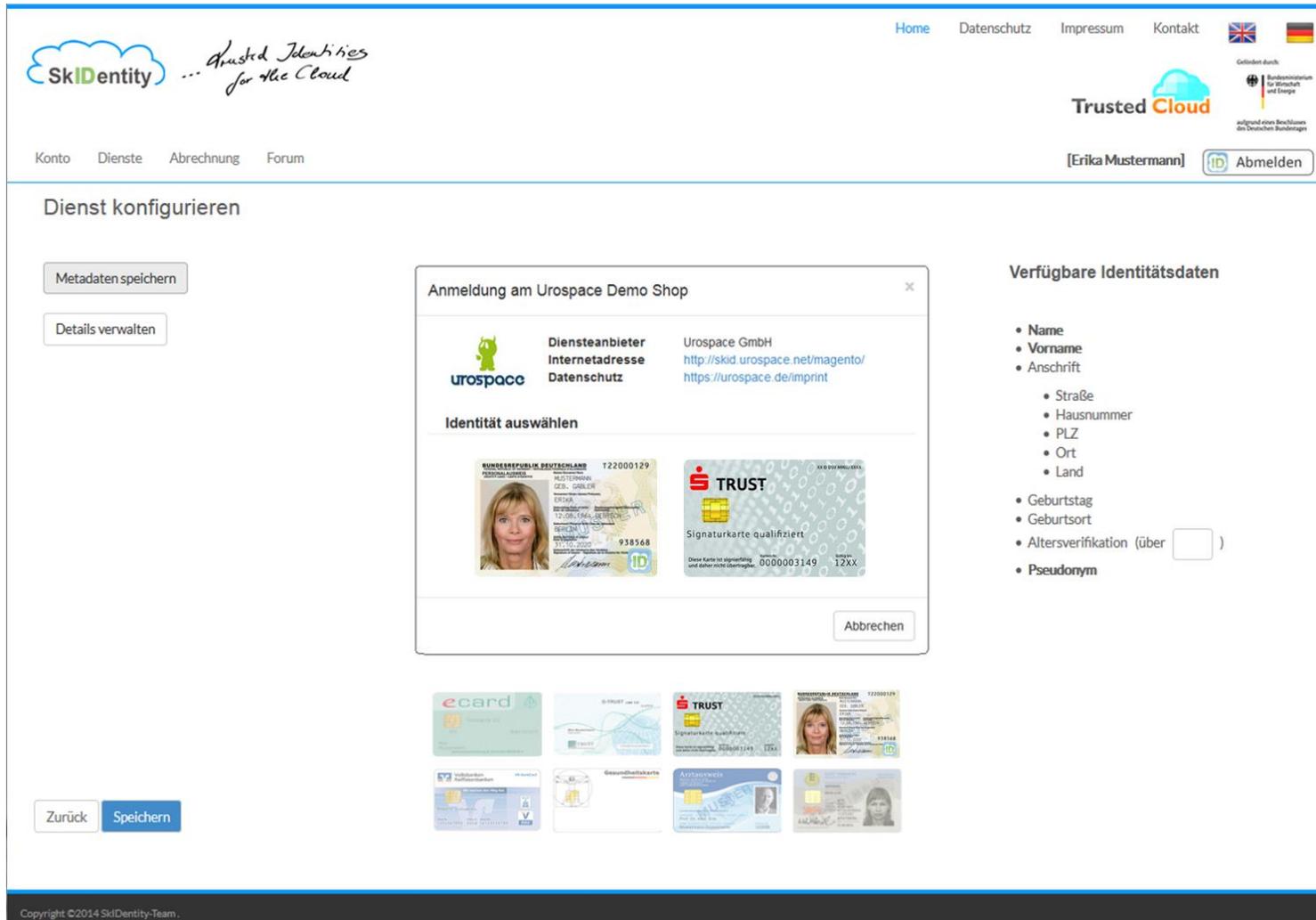
# SkIDentity – Referenzarchitektur



# SkIDentity – Demo-Anwendungen



# SkIDentity – Management-Service



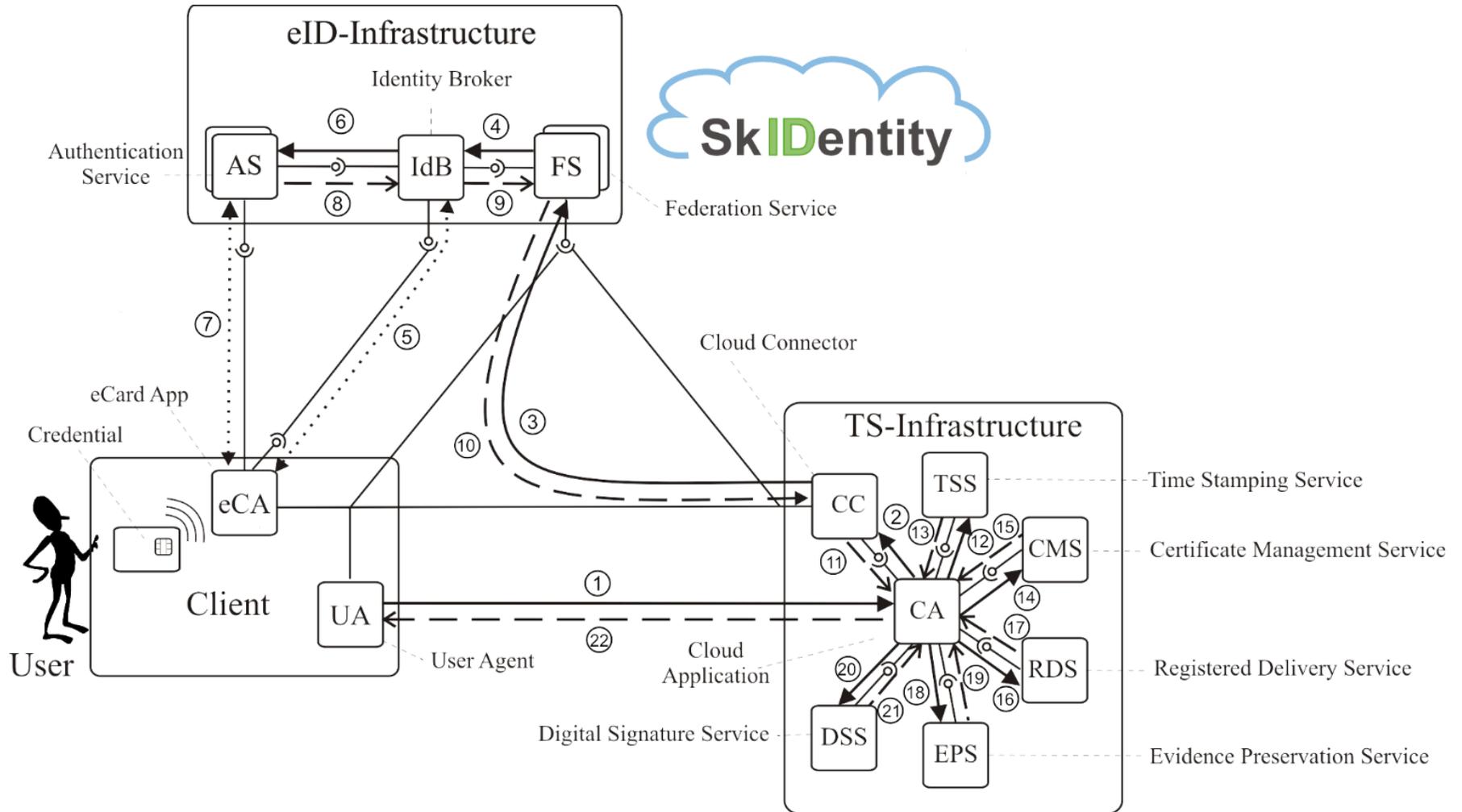
The screenshot shows the SkIDentity Management-Service interface. At the top, there is a navigation bar with links for Home, Datenschutz, Impressum, and Kontakt. The main header includes the SkIDentity logo and the slogan "Trusted Identities for the Cloud". Below the header, there are navigation links for Konto, Dienste, Abrechnung, and Forum. A user profile section shows the name [Erika Mustermann] and a button to Abmelden.

The main content area is titled "Dienst konfigurieren" (Configure Service). On the left, there are buttons for "Metadaten speichern" (Save Metadata) and "Details verwalten" (Manage Details). The central part of the page displays a configuration window for "Anmeldung am Uroospace Demo Shop". This window shows the service provider "Uroospace GmbH" with their internet address and data protection policy. Below this, there is a section "Identität auswählen" (Select Identity) with two options: a German ID card and a TRUST signature card. At the bottom of the configuration window is an "Abbrechen" (Cancel) button.

On the right side, there is a section "Verfügbare Identitätsdaten" (Available Identity Data) with a list of data points: Name, Vorname, Anschrift (with sub-items: Straße, Hausnummer, PLZ, Ort, Land), Geburtstag, Geburtsort, Altersverifikation (über ) and Pseudonym.

At the bottom of the main content area, there is a grid of various digital identity cards, including eCard, TRUST, and others. At the very bottom of the interface, there are "Zurück" (Back) and "Speichern" (Save) buttons.

# eIDAS as a Service auf Basis von SkIDentity



# Agenda

- Einleitung
- eIDAS as a Service
- **Zusammenfassung**

## Zusammenfassung

- Cloud Computing ist vielversprechender Wachstumsmarkt
  - eIDAS-Verordnung ebnet den Weg für Europäischen Markt für eID- und Trust-Services
  - IT-Sicherheitsgesetz wird starke Authentisierung fordern
  - Bereitstellung von eIDAS-Diensten als Cloud Service möglich und naheliegend
  - SkIDentity bietet starke Authentisierung und vertrauenswürdige Identitäten aus der Cloud
- 
- **Wir freuen uns darauf, auch Ihre Online-Dienste sicher machen zu dürfen!**

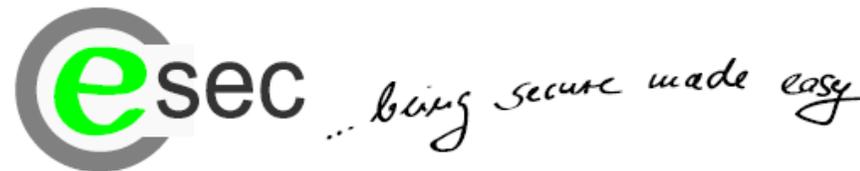


# Herzlichen Dank für Ihre Aufmerksamkeit!

Deutschland  
Land der Ideen



Ausgezeichneter Ort 2013/14



**ecsec GmbH**

Sudetenstr. 16  
96247 Michelau, Germany  
Telefon + 49 9571 896479  
Mobil + 49 171 9754980  
detlef.huehnlein@ecsec.de  
<http://www.ecsec.de>

Dipl.-Inform. (FH)  
**Dr. Detlef Hühnlein**  
Geschäftsführer