«VOI»

TeleTrusT
Pioneers in IT security.

Informationstag "Elektronische Signatur"

Gemeinsame Veranstaltung von TeleTrusT und VOI

Berlin, 17.09.2015

eID-Interoperabilität im Rahmen der eIDAS-VO – Aktueller Stand

Guido Frank, BSI

eIDAS-Verordnung – Ziele und Prinzipien im Bereich eID

- Ziel: Grenzüberschreitende Nutzung von eIDs innerhalb der EU
- Prinzipien:
  - Kein Eingriff in nationale Systeme

    → Interoperabilität statt Harmonisierung
  - Freiwillige Notifizierung von nationalen eID-Systemen
    - Anforderungen an notifizierte Systeme
      - Haftung, Vertrauenslevel, Interoperabilität
  - Verpflichtende Anerkennung notifizierter eIDs für Online-Dienste öffentlicher Stellen
    - Unter den Bedingungen von Art 6
    - Freiwillig für „Privatsektor“
  - Kooperation der MS im Bereich eID

Durchführungsrechtsakte eID

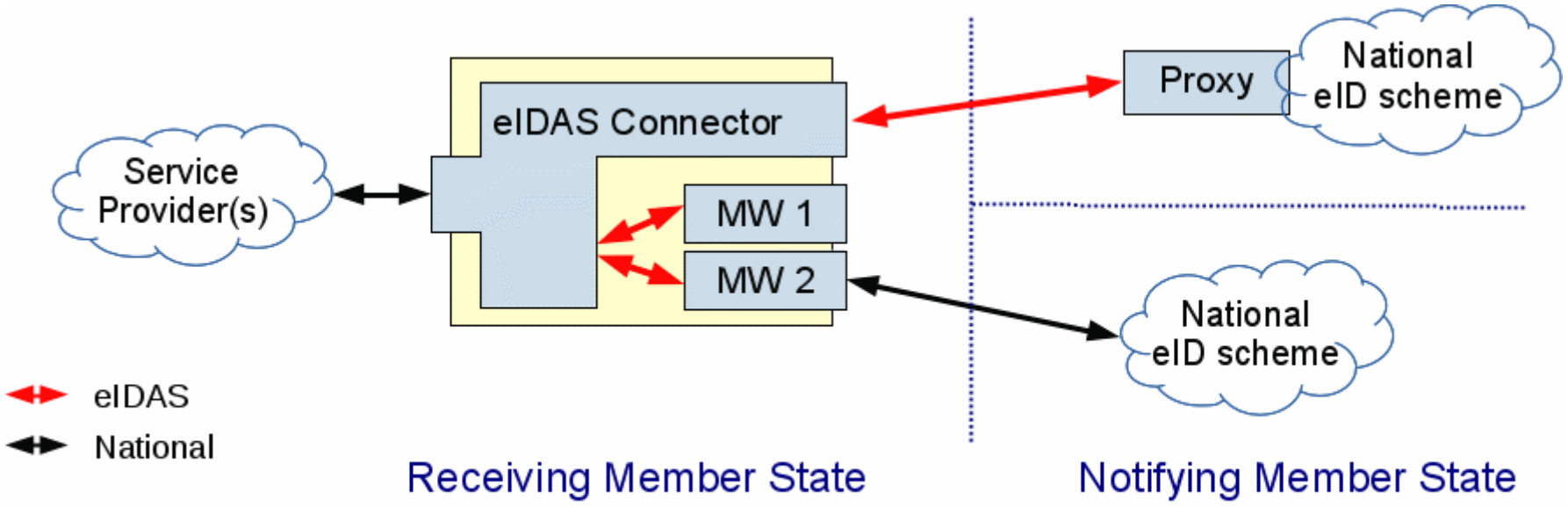
- Cooperation Network (done)
  - Kooperation der MS zum Thema eID
  - Peer Review im Rahmen der Notifizierung
- Level of Assurance (done)
  - Drei Level: „low“, „substantial“, „high“
  - Input: ISO 29115, STORK QAAL
- Interoperability Framework (done)
  - Technische Mindestanforderungen an die Interoperabilität
  - Sicherheitsanforderungen an Komponenten
  - Minimum Data Set
  - Details via technischer Spezifikationen
- Notification Procedure (almost done)
  - Einzelheiten/Formalien zum Notifizierungsverfahren

Interoperability Framework - Technische Spezifikationen

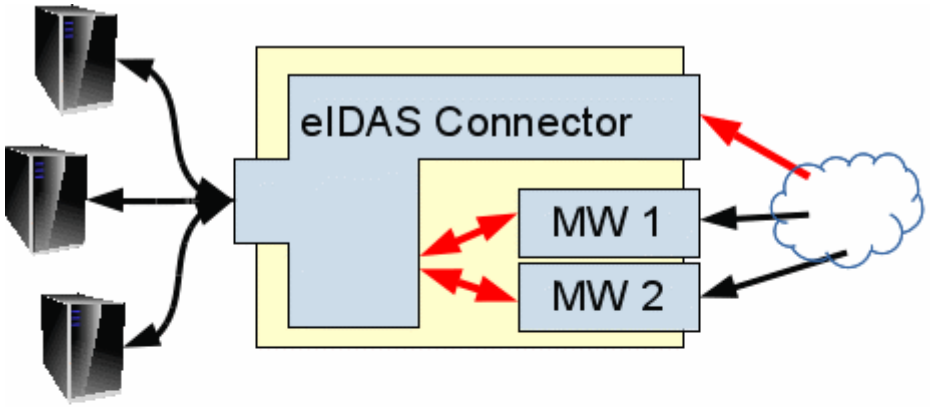
- Inhalt: Definition der Schnittstellen für grenzüberschreitende Authentisierung
  - Architektur, Trust-Management, Kommunikationsablauf, Datenformate, Krypto-Vorgaben
- eIDAS-Nodes übersetzen zwischen nationalen Systemen und eIDAS
  - eIDAS-Connector (SP ↔ eIDAS)
  - eIDAS-Service (eIDAS ↔ eID)
- Verschiedene Integrationsszenarien
  - Proxy-basiert vs. MW-basiert
  - Zentral vs. Dezentral
- Status: Stabiler Entwurf, derzeit letztes Feintuning

Integrationszenarien - Notifizierender MS (Sending MS)

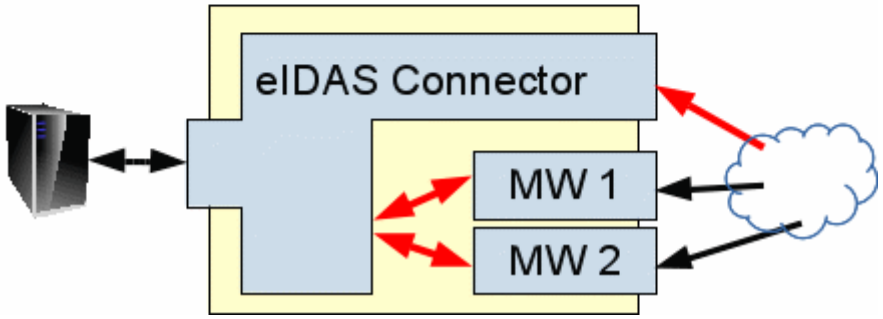
- Proxy-basiert
  - Notifizierender MS betreibt Proxy (*eIDAS-Proxy-Service*), der zwischen nationalen eIDs und eIDAS „übersetzt“.
- Middleware-basiert
  - Notifizierender MS stellt Middleware zur Verfügung, die im anerkennenden MS betrieben wird und die Vermittlung übernimmt (*eIDAS-MW-Service*)



Integrationsszenarien - Anerkennender MS (Receiving MS)



- Zentraler Betrieb
  - Zentrale Instanz betreibt eIDAS-Software (Connector + MWs) für alle Dienstanbieter eines MS

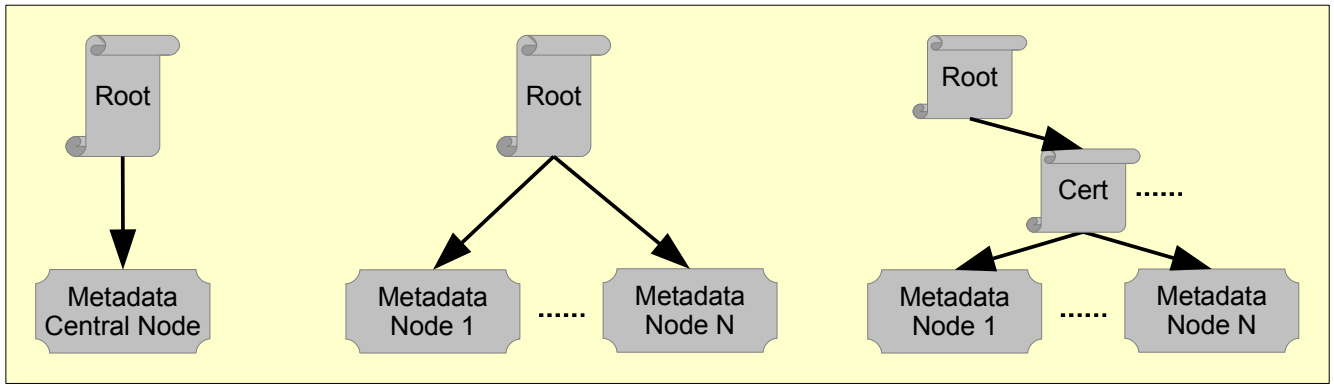


- Dezentraler Betrieb
  - Jeder Dienstanbieter eines MS betreibt eIDAS-Software (Connector + MWs) selbst

- Auch Mischformen möglich

Protokolle und Trust Management

- SAML-basierte Kommunikation
- Absicherung der Daten auf Inhalts- und Transportebene
  - Ende-zu-Ende-Sicherung auf Inhaltsebene: Signatur der SAML-Nachrichten, Verschlüsselung von SAML-Assertions zwischen Connector und Service
  - TLS zur Sicherung der lokalen Transportkanäle
- Trust-Management
  - Bilateraler Austausch von Vertrauensankern (Zertifikaten) zwischen MS
  - Signierte SAML-Metadaten zum Austausch von Zertifikaten von eIDAS-Connectors und Proxy-Services für SAML-Kommunikation
  - Metadaten von MW-Services müssen nicht signiert werden (1:1-Beziehung)



Ablauf der Authentisierung in eIDAS

- Der Dienstanbieter startet die Authentisierung und sendet Authentisierungsrequest an den eIDAS-Connector (Receiving MS)
  - Bestimmung des relevanten MS (durch Dienstanbieter oder eIDAS-Connector)
- Der eIDAS-Connector (Receiving MS) sendet signierten SAML-Request an den eIDAS-Service des ausgewählten MS
- Der eIDAS-Service (Sending MS)
  - prüft die Authentizität des Requests und angefragten LoA
  - führt die Authentisierung mit dem Nutzer gemäß dem nationalen Schema des Sending MS mit angefragtem LoA durch
  - sendet signierte SAML-Response mit verschlüsselter SAML-Assertion zum eIDAS-Connector
- Der eIDAS-Connector (Receiving MS)
  - verifiziert die Authentizität der SAML-Response, entschlüsselt die Assertion und prüft die Einhaltung des angeforderten LoA
  - leitet die Identifizierungsdaten an Dienstanbieter weiter

Minimum Data Set

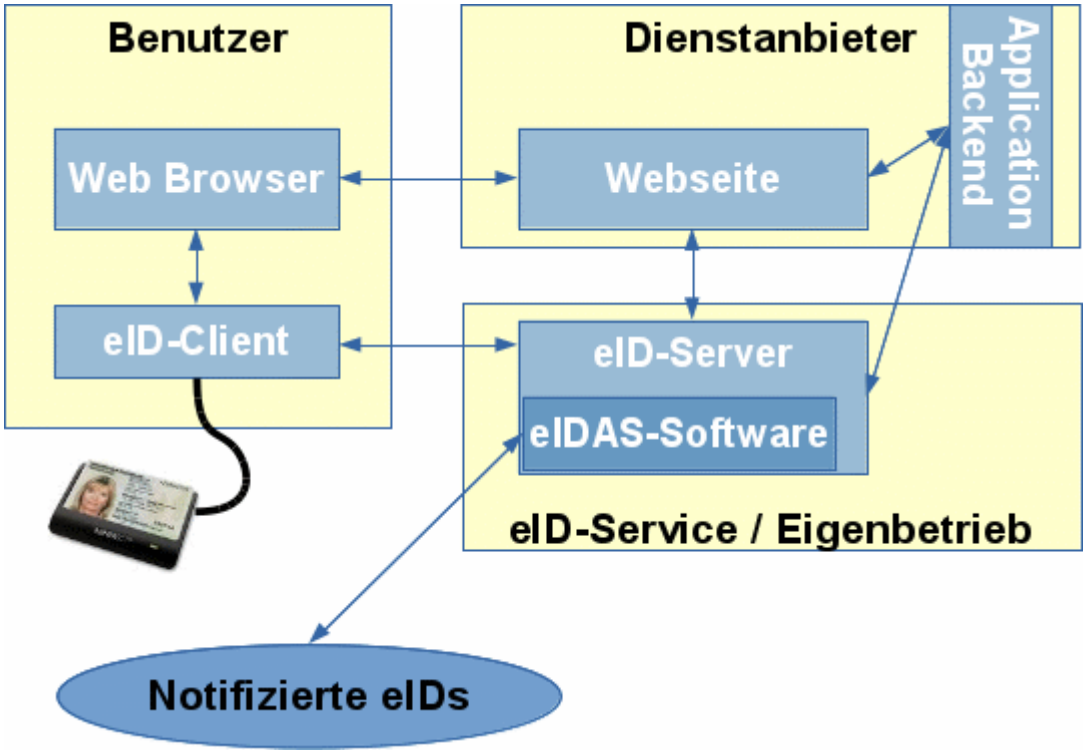
- Natural Persons
  - Mandatory: current family name(s); current first name(s); date of birth; uniqueness identifier.
  - Optional: first name(s) and family name(s) at birth; place of birth; current address; gender.
- Legal Persons
  - Mandatory: current legal name; uniqueness identifier.
  - Optional: current address; VAT registration number; tax reference number; the identifier referred to in Article 3(1) of Directive 2009/101/EC; Legal Entity Identifier (LEI); Economic Operator Registration and Identification (EORI); System for Exchange of Excise Data (SEED); Standard Industrial Classification.
- NP representing LP: Kombination beider MDS

eIDAS-Verordnung – Auswirkungen für DE

- Notifikation
  - eID-Funktion des Personalausweis kann (wie sie ist) auf Vertrauensniveau „hoch“ notifiziert werden
- Anerkennung
  - Online-Services öffentlicher Stellen, die eine elektronische Identifizierung mit eID benötigen, müssen alle notifizierten eIDs akzeptieren, die mindestens das Vertrauensniveau haben, die die „heimatliche“ eID (hier: ePA → „hoch“) hat.
  - Etwa: eGovG → (Bundes-)Behörden müssen Identifizierung mit ePA anbieten → also auch mit allen notifizierten „hoch“ eIDs!

eIDAS-Verordnung – Umsetzung

- Integration in DE
  - Keine zentrale Komponente im deutschen System
  - Integration der eIDAS-SW bei eID-Server/-Service möglich
  - Ggf. Ergänzung Vertrauensniveaus in Schnittstelle Dienst ↔ eID-Server
- KOM stellt eine Implementierung der eIDAS-SW kostenfrei und quelloffen zur Verfügung (CEF-Program)



Überblick und Ausblick

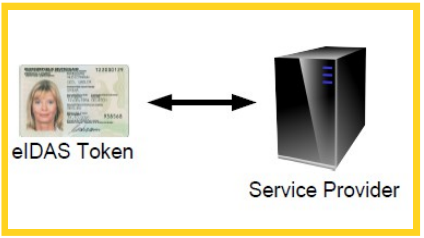
- Aktuell:
  - Jeder MS hat eigenes System
  - Interoperabilität durch „Übersetzung“ zwischen Systemen

- Erwartung: Langfristig Konvergenz von eID-Systemen
  - Entwicklung von gemeinsamer Standards für direkte Interoperabilität
  - Begrenzte Anzahl von Systemen/Varianten
  - Reduktion von Entwicklungs-/Wartungsaufwänden
  - Leichtere/Schnellere Einführung von erprobten Systemen

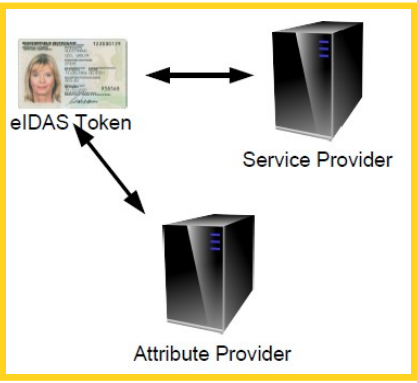
Vorschlag: eIDAS-Token

ANSSI + BSI + Europäische Industrie

- Annahme:
  - Für Vertrauensniveau „hoch“ ist ein token-basiertes, fälschungssicheres eID-System notwendig.
  - Hoher Datenschutz erfordert die volle Kontrolle des Nutzers über seine Attribute



- eIDAS Token →
  - Spezifikation von Sicherheitsmechanismen Datenstrukturen (BSI TR-03110)
  - Sichere Hardware („Besitz“) als Sicherheitsanker
  - Bewährte Passtechnologie als Basis
  - Modularer Ansatz: Ermöglicht bedarfsorientierte Entwicklung token-basierter eID-Systeme



https://www.bsi.bund.de/eIDAS

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Dr. Guido Frank
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5841
Fax: +49 (0)22899-10-9582-5841

guido.frank@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de