Bundesamt
für Sicherheit in der
Informationstechnik

eIDAS – die Basics

Jens Bender & Felix Bleckmann
BSI

Die eIDAS-Verordnung

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

und zur Aufhebung der Richtlinie 1999/93/EG

Inhalte

- Kapitel I: Allgemeine Bestimmungen
- Kapitel II: Elektronische Identifizierung
- Kapitel III: Vertrauensdienste
  - Allgemeine Bestimmungen
  - (Q|F) Signatur
  - (Q|F) Siegel
  - (Q|F) Zeitstempel
  - (Q|nQ) Zustelldienst
  - Q Webseitenzertifikate
- Kapitel IV: Elektronische Dokumente
- Kapitel V: Schlussbestimmungen
- Anhänge

European Commission

Website authentication: check if the website you enter is really linked to the seller

eID: identify (or authenticate) yourself using, for instance, an eID means

Creation of the document

E-signature: the buyer may need to agree on the transaction

E-seals: ensures the authenticity of the selling document as well as that they are from the company selling the goods

Time stamp: Proof of the date and time of the transaction

E-registered delivery: communications with and from the seller may need to be securely delivered

Preservation: Electronic storage of the submitted documents and acknowledgment of receipt

Preservation - Storage

Bundesamt für Sicherheit in der Informationstechnik

Regelungshierarchie

- eIDAS-Verordnung
  - Unmittelbar geltendes Recht in allen Msen
  - Keine Umsetzung wie bei einer Richtlinie

- Enthält Ermächtigungen für
  - 1 Delegierter Rechtsakt (Zertifizierungsstellen für QSCDs)
  - 28 Implementierungsrechtsakte
    - Davon 4 bei eID, der Rest bei Vertrauensdiensten

- Dritte Ebene: Standardisierung
  - Hauptsächlich relevant für Vertrauensdienste

Ein langer Weg …

- 04.06.2012: Vorlage des Entwurfs durch die KOM

… lange Verhandlungen in EP und Rat …

- 28.08.2014: Veröffentlichung im Official Journal
- 17.09.2014: Verordnung tritt in Kraft

… lange Diskussionen in der „Expert Group“ …

- 18.09.2015:
  - Durchführungsrechtsakte für eID müssen erlassen sein
  - Freiwillige Anerkennung der eIDs
- 01.07.2016: Regelungen zu Vertrauensdiensten wirksam
- 18.09.2018: Verpflichtende Anerkennung von eIDs

Die eIDAS-Verordnung

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

und zur Aufhebung der Richtlinie 1999/93/EG

eID nach eIDAS

eID als Basistechnologie
für eGov und eBusiness

Interoperabilität und Anerkennung
nationaler eID-Systeme
nicht
Harmonisierung

Notifizierung

- Mitgliedstaaten können ihre eID-System notifizieren

- Voraussetzungen: die Identifizierungsmittel ...
  - (a) … werden durch den MS ausgestellt / in seinem Auftrag ausgestellt / vom MS anerkannt
  - (b) … können im notifizierenden MS für den Zugang zu mindestens einem (öffentlichen) Dienst verwendet werden
  - (c) … erfüllen die Anforderungen eines der Vertrauensniveaus
  - (d) … enthält die richtigen (eindeutigen) Personenidentifizierungs-daten, garantiert durch den MS
  - (e) … werden an die richtige Person ausgegeben
  - (f) … der notifizierende MS stell sicher, dass eine Möglichkeit zur Online-Authentifisierung für den öffentlichen Sektor kostenfrei zur Verfügung steht
  - (g) [prozeduraler Kleinkram]
  - (h) … erfüllen die Interoperabilitätsanforderungen

Gegenseitige Anerkennung – Langform

(1) Ist für den Zugang zu einem von einer öffentlichen Stelle in einem Mitgliedstaat erbrachten Online-Dienst nach nationalem Recht oder aufgrund der Verwaltungspraxis eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel und mit einer Authentifizierung erforderlich, so wird ein in einem anderen Mitgliedstaat ausgestelltes elektronisches Identifizierungsmittel im ersten Mitgliedstaat für die Zwecke der grenzüberschreitenden Authentifizierung für diesen Online-Dienst anerkannt, sofern folgende Bedingungen erfüllt sind:

a) Das betreffende elektronische Identifizierungsmittel [ist notifiziert].

b) Das Sicherheitsniveau des betreffenden elektronischen Identifizierungsmittels entspricht einem Sicherheitsniveau, das so hoch wie oder höher als das von der einschlägigen öffentlichen Stelle für den Zugang zu diesem Online-Dienst geforderte Sicherheitsniveau ist [...].

c) Die betreffende öffentliche Stelle verwendet für den Zugang zu diesem Online-Dienst das Sicherheitsniveau „substanziell“ oder „hoch“.

Gegenseitige Anerkennung – Kurzform

Online-Services öffentlicher Stellen,
die eine elektronische Identifizierung mit einer eID benötigen,
müssen alle notifizierten eIDs akzeptieren,
die mindestens das Vertrauensniveau haben,
das für den Service notwendig ist.

Also ...

- Notifizierung von nationalen eID-Systemen
  - Keine „EU-eID“, sondern gegenseitig anerkannte nationale eIDs
  - „Interoperabilität“ statt „Harmonisierung“
- Die Notifizierung ist an bestimmte Voraussetzungen an das eID-System geknüpft
  - Vertrauensniveaus, Interoperabilität, Haftung
- Die Notifizierung ist nicht verpflichtend
  - … zumindest rechtlich
- Die Anerkennung notifizierter eIDs ist verpflichtend
  - Unabhängig davon, ob der MS selbst eine eID notifiziert hat
  - Verpflichtung für Anwendungen des öffentlichen Sektor, freiwillige Anerkennung durch den privaten Sektor

Gremien

The eIDAS Legal Framework

	Legal Act	Reference	Adoption date	Entry into force
	eIDAS Regulation	910/2014	23.07.2014	17.09.2014 (1.07.2016 - application provisions on TS)
eID	ID on procedural arrangements for MS cooperation on eID (art. 12.7)	2015/296	24.02.2015	17.03.2015
	IR on interoperability framework (art. 12.8) *Corrigendum C(2015) 8550 of 4.02.2016*	2015/1501	8.09.2015	29.09.2015
	IR assurance levels for electronic identification means (art. 8.3)	2015/1502	8.09.2015	29.09.2015
	ID on circumstances, formats and procedures of notification (art. 9.5)	2015/1984	3.11.2015	5.11.2015 (notified to Ms)

Formelle Gremien

- eIDAS Kommittee
  - Eingerichtet durch Artikel 48 eIDAS-VO
  - „Meinung“ zu KOM-Entwürfen für Durchführungsrechtsakte
  - DE: BMI (für eID) / BMWi (für Vertrauensdienste)
  - Unterstützung durch BSI / BnetzA

- Kooperationsnetzwerk
  - Eingerichtet durch CID (EU) 2015/296
  - Kooperation der Mitgliedstaaten im Bereich eID
  - Peer Review im Rahmen der Notifizierung
  - „Meinung“ zu technischen Spezifikationen
  - DE: BMI/BSI

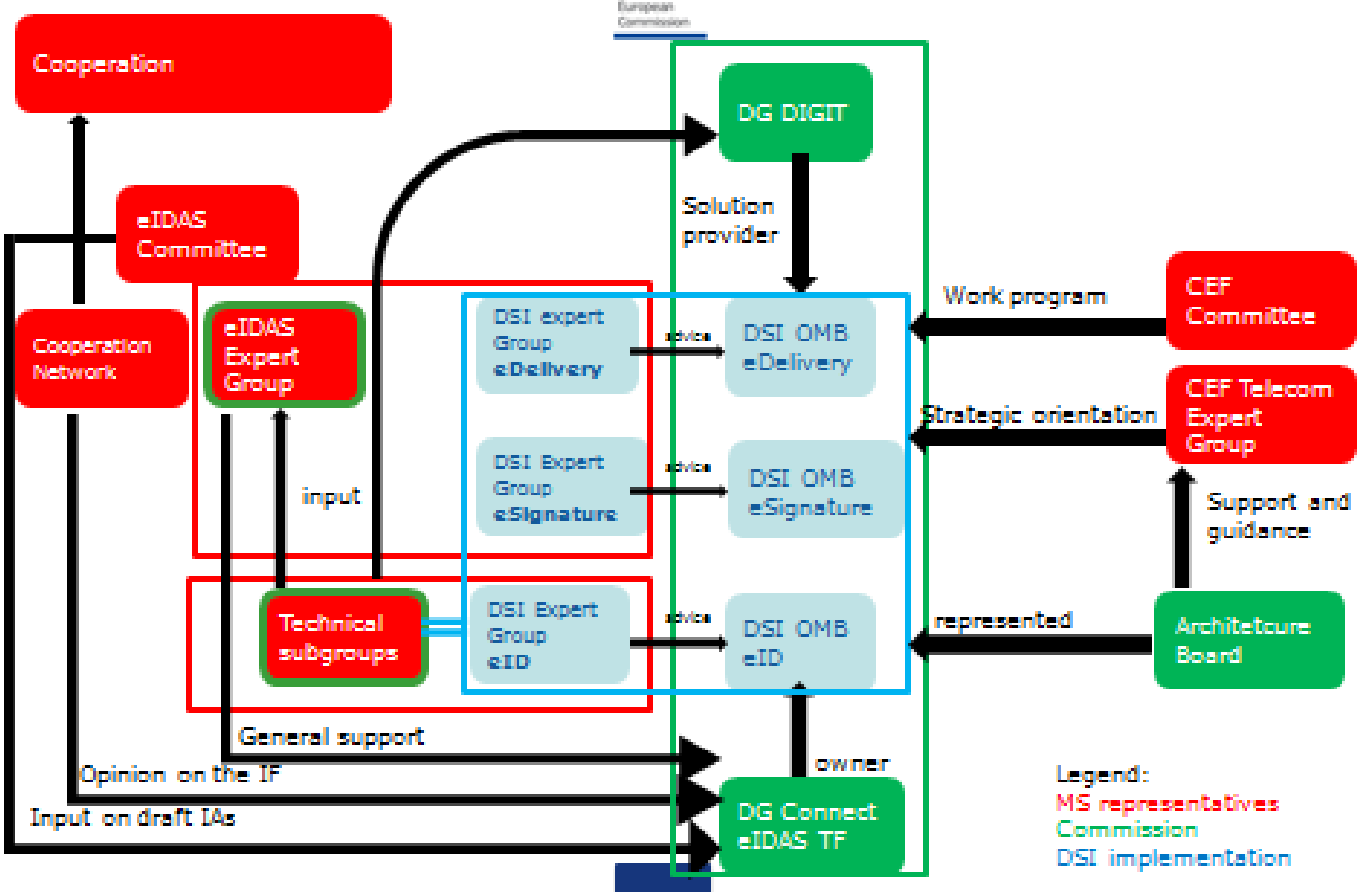
Informelle Gremien

- eIDAS Expert Group (KOM + Msen)
  - Unterstützt KOM bei der Erstellung der Durchführungsrechtsakte
  - DE: BSI und z.T. BnetzA

- Technical Subgroups der Expert Group (KOM + Msen)
  - Untergruppen für technische Fragen
  - DE: eID → BSI, Trusted List → BNetzA

- CEF Digital Service Infrastructure Expert Groups
  - Technische Umsetzung
  - DE: eID, Zustelldienste → BSI

Interrelationships between CEF and eIDAS groups



Vertrauensniveaus

Was sind Vertrauensniveaus?

- eIDAS definiert drei *Vertrauensniveaus*: niedrig, substantiell, hoch

- Vertrauensniveaus als Grundlage für gegenseitige Anerkennung
  - Ein Dienst muss nur eIDs anerkennen, die mindestens das für diesen Dienst notwendig Vertrauensniveau erreichen
    → Online-Dienste müssen Mindestniveau festlegen

- Niedrig: Ein-Faktor-Authentisierung “Passwörter”
- Substantiell: Zwei-Faktor-Authentisierung
- Hoch: Zwei-Faktor-Authentisierung mit Schutz gegen Kopie/Veränderung

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

eIDAS Regulation

Implementing Act Level of Assurance

Guidance of the Cooperation Network

TR-03107-1

- Die eIDAS Verordnung ist “technologieneutral”
  - Definition der Vertrauensniveaus abstrakt, nicht konkret

- Niedrig → “**begrenztes Maß an Vertrauen** in die beanspruchte oder behauptete Identität”, “**Minderung** der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung;”
- Substantiell → “**substantielles Maß an Vertrauen** in die beanspruchte oder behauptete Identität”, “**substantielle Minderung** der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung;”
- Hoch → “**höheres Maß an Vertrauen** in die beanspruchte oder behauptete Identität”, “**Verhinderung** des Identitätsmissbrauchs oder der Identitätsveränderung;”

eIDAS Regulation

Implementing Act Level of Assurance

Guidance of the Cooperation Network

TR-03107-1

9.9.2015 EN Official Journal of the European Union L 235/7

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

of 8 September 2015

on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

(Text with EEA relevance)

- Details werden in einem **Durchführungsrechtsakt** definiert
  - Immer noch mehr oder minder “technologieneutral”

- Anforderungen an
  - Enrolment
    - u.a. Registrierung, Identitätsprüfung
  - Elektronische Identifizierungsmittel
    - u.a. Ausgabe, Rückruf, Suspendierung
  - Authentisierung
    - u.a. ein oder zwei Faktoren, Angriffsresistenz
  - Management und Organisation
    - u.a. Sicherheitsmanagement aller beteiligter Stellen

eIDAS Regulation

Implementing Act Level of Assurance

Guidance of the Cooperation Network

TR-03107-1

- Das Kooperationsnetzwerk hat **“Guidance”** als Auslegungshilfe zu den Vertrauensniveaus erstellt
  - Auslegungshilfe, aber nicht normativ
  - Konkrete (mehr oder minder) Beispiele
- Weitere Konkretisierung im peer review-Verfahren
  - Nutzung vorhergehender peer reviews als Vergleich

eIDAS Regulation

Implementing Act Level of Assurance

Guidance of the Cooperation Network

TR-03107-1

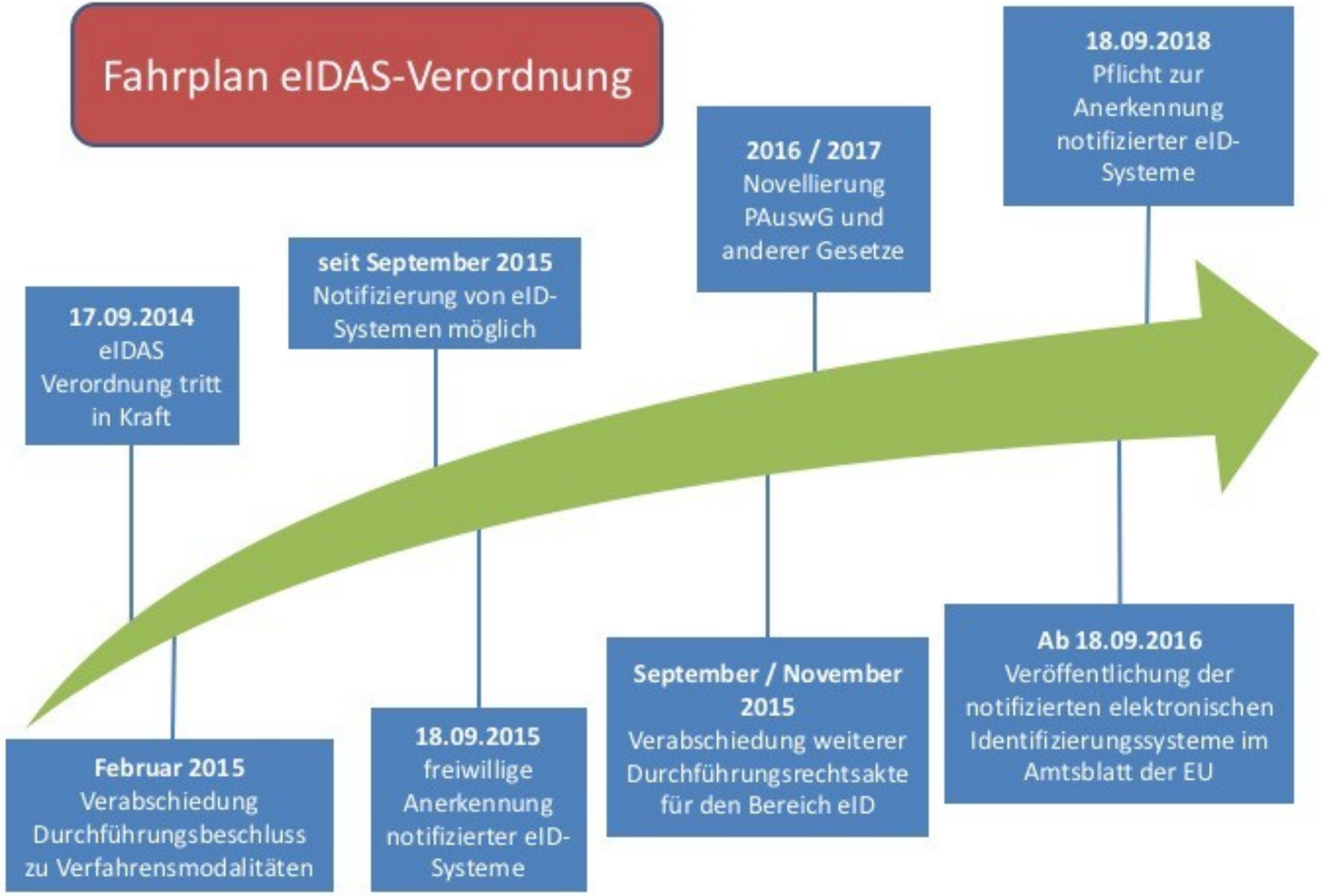
- Technische Richtlinie TR-03107-1
  “Elektronische Identitäten und Vertrauensdienste im E-Government”

- Interpretiert die eIDAS Anforderungen für den deutschen Markt
- Beispiele für Einstufung konkreter Mechanismen

- Für eine Notifizierung übernimmt not. MS die Haftung für die korrekte Einordnung in Vertrauensniveau
  - Daher konkretere Vorgaben / Nachweisverfahren

- Angenommen vom IT-Planungsrat
  - Grundlage für die Kategorisierung von eID-Verfahren für eGov (Nutzerkonten)

Fahrplan eIDAS-Verordnung



Der Notifizierungsprozess

Am Beispiel der Online Ausweisfunktion

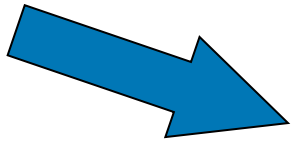
1. Prä-Notifizierung (am 20.02.2017)

- **Notification Template**
- German eID – **Overview**: Überblick über deutsche eID und eIDAS-Integration
- German eID – **LoA mapping**: Erfüllung von Vertrauensniveau “Hoch”
- German eID – **IF mapping**: Erfüllung Interoperabilitätsanforderungen
- German eID – **Supporting Documentation**: Liste der relevanten Gesetze, Verordnungen, TRs, …

Die gesamte Dokumentation ist erhältlich unter https://www.bsi.bund.de/eIDAS-Notifizierung.

2. Peer Review (ab 03.04.2017)

- **Koordinator:** NL
- **Rapporteure:** BE, FR, AT, SE
- **Active Members** aus weiteren MS
- **Observer**



Max. 3 Monate

Bewertung des eID-Schemas anhand von

- Unterlagen der Prä-Notifizierung
- Fragerunden auf Basis der Unterlagen
- Vor-Ort-Termin

3. Die Opinion des Cooperation Networks (am 22.08.2017)

"Based on the examination of the pre-notification documents [...] the Cooperation Network is of the opinion that the pre-notification documents and additional information provided by the Federal Republic of Germany ***demonstrate sufficiently*** *how the German eID scheme to be notified meets the requirements of Article 7, Articles 8(1)-(2) for assurance level* ***"high"*** *[...]."*

(https://ec.europa.eu/cefdigital/wiki/x/kw3oAg)

→4. Notifizierung durch den MS!

5. Veröffentlichung der Notifizierung (am 26.09.2017)

Nach Artikel 9 Absatz 1 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [1] notifizierte elektronische Identifizierungssysteme

(2017/C 319/03)

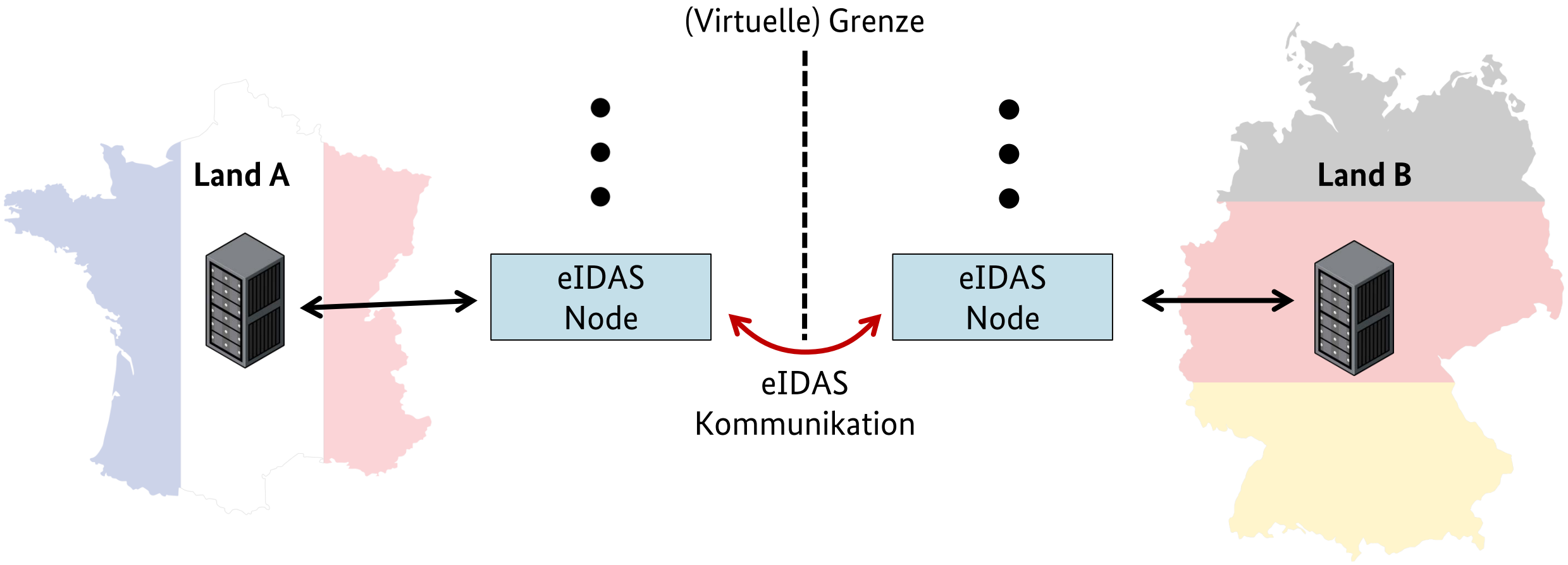
Name des Systems	eID-Mittel im Rahmen des notifizierten Systems	Notifizierender Mitgliedstaat	Sicherheitsniveau	Für das System zuständige Stelle
Online-Ausweisfunktion basierend auf *Extended Access Control* (elektronischer Identitätsnachweis — eID)	Nationaler Personalausweis Elektronischer Aufenthaltstitel (eAT)	Bundesrepublik Deutschland	Hoch	Bundesministerium des Innern Alt-Moabit 140 10557 Berlin Deutschland ITI4@bmi.bund.de +49 30186810

→6. Die Anerkennungsverpflichtung begann am 29.09.2018!

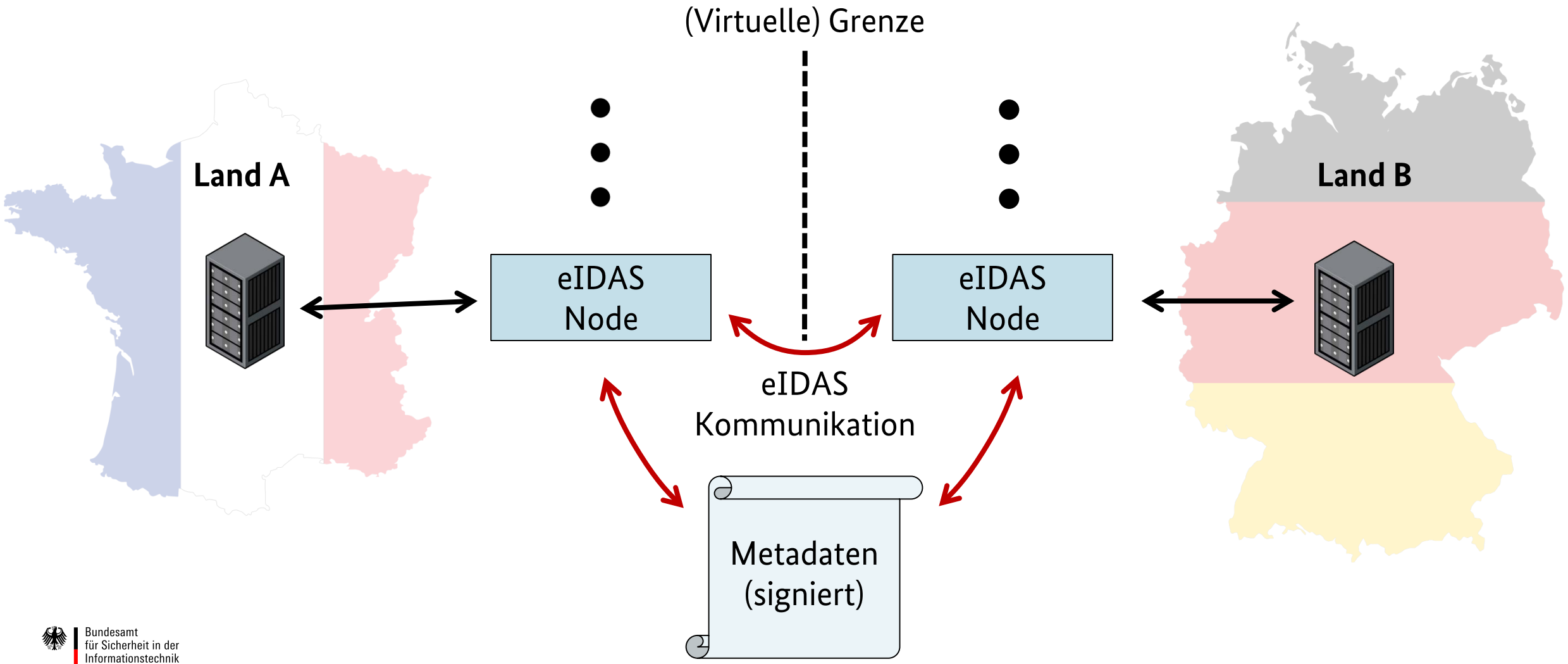
Interoperabilität

Wie ist das gedacht?

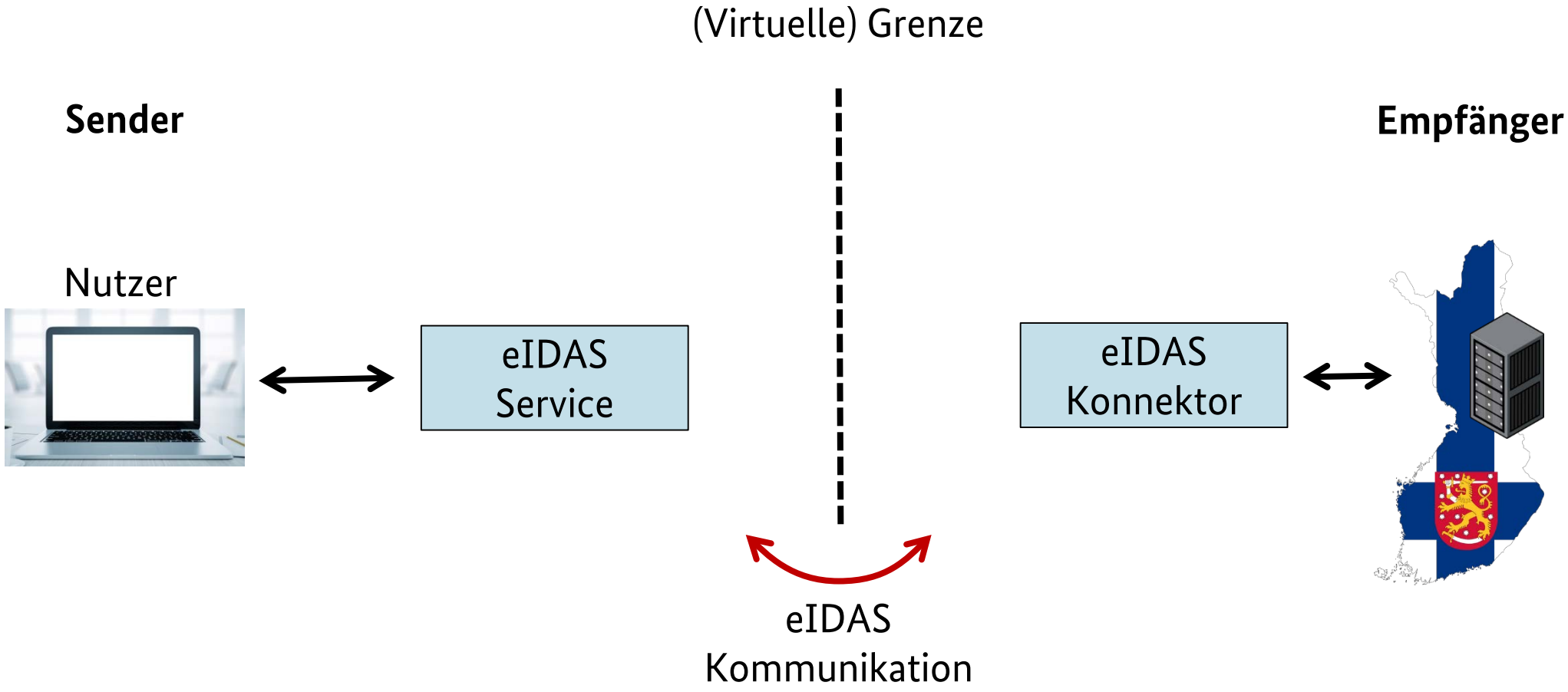
Interoperabilität- Das eIDAS Netzwerk



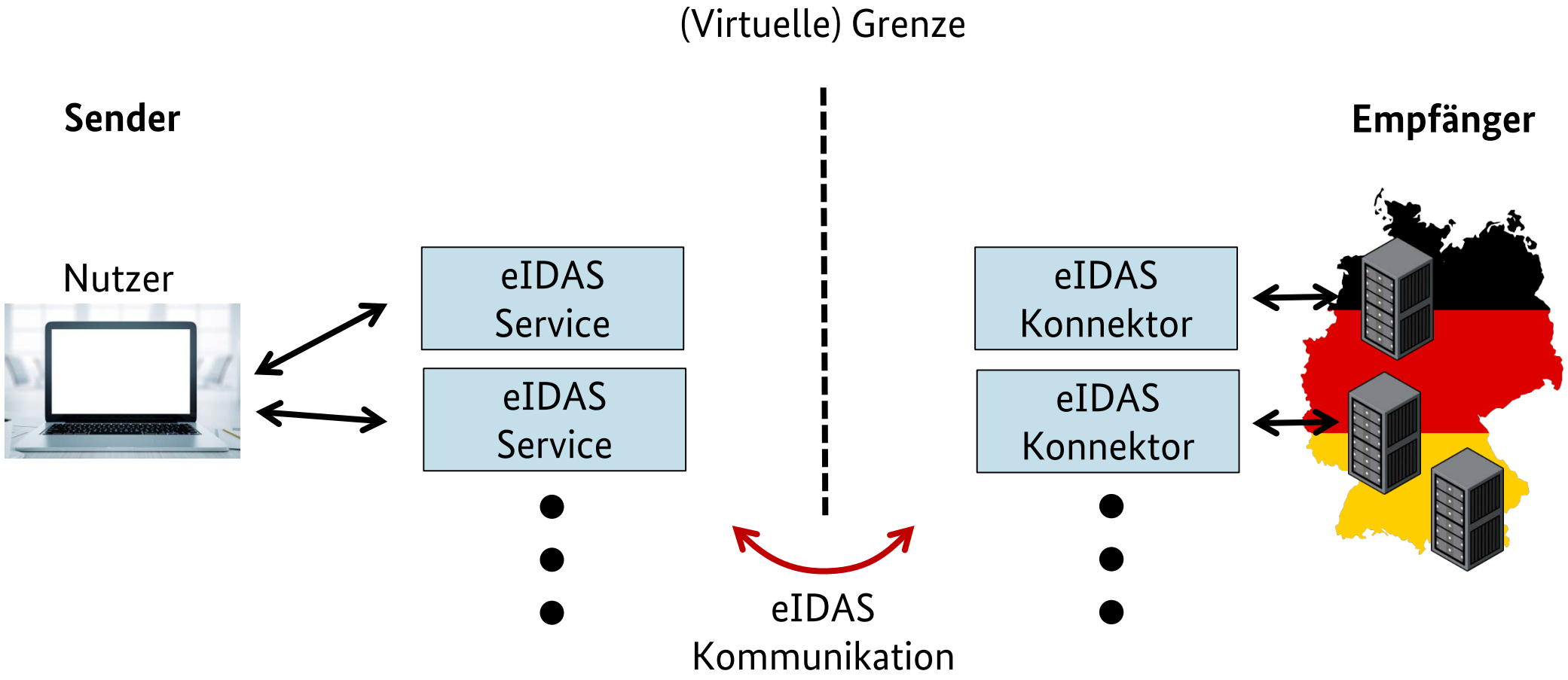
Interoperabilität- Das eIDAS Netzwerk



Interoperabilität- Die Varianten I



Interoperabilität- Die Varianten II

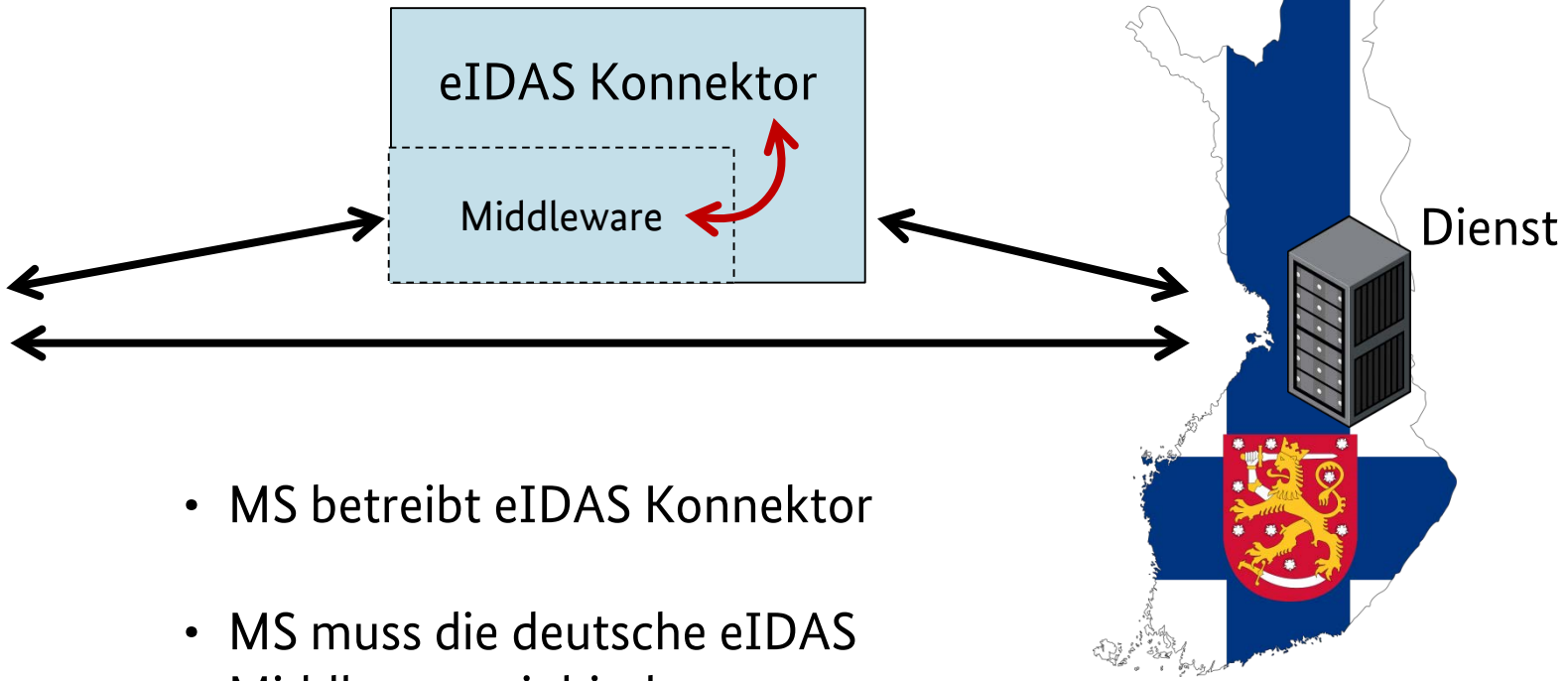


Nutzung der Online Ausweisfunktion im Ausland

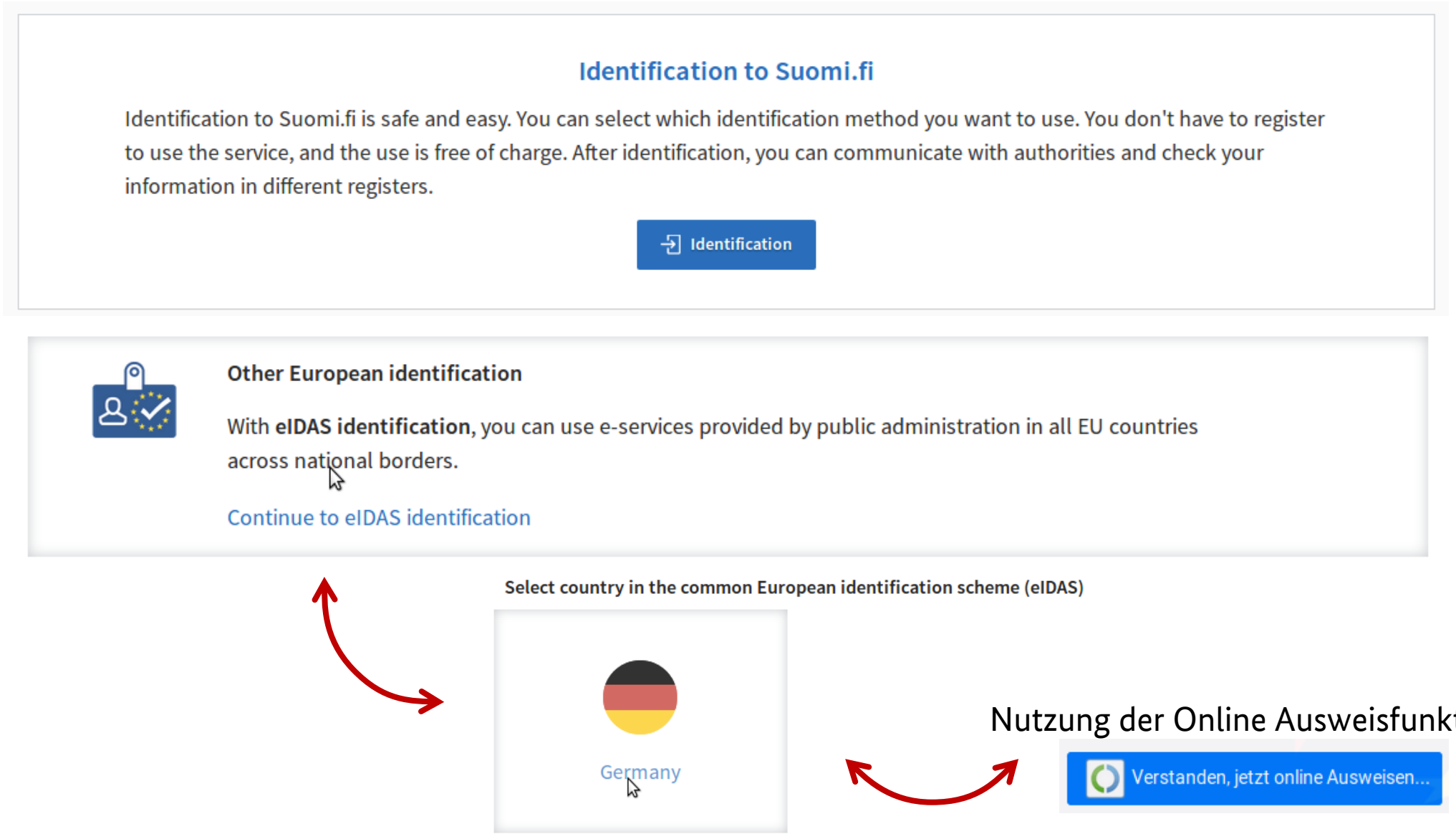
Wie geht das?
Wo ist es schon möglich?

Anbindung der Online Ausweisfunktion

Nutzer:



- MS betreibt eIDAS Konnektor
- MS muss die deutsche eIDAS Middleware einbinden



Nutzung der Online Ausweisfunktion:

Aktueller Status

Die deutsche eIDAS Middleware wurde von den folgenden 18 MS eingebunden und ist **produktiv**:

NL, LU, FI, AT, CZ, UK, MT, SK, BE, GR, EE, DK, ES, SI, LT, LV, IT, SE, KOM

→ Zugang zu eGovernment mit PA / eAT:

... zumindest im Prinzip – “Portalzugang”

... nicht notwendigerweise alle Anwendungen ...

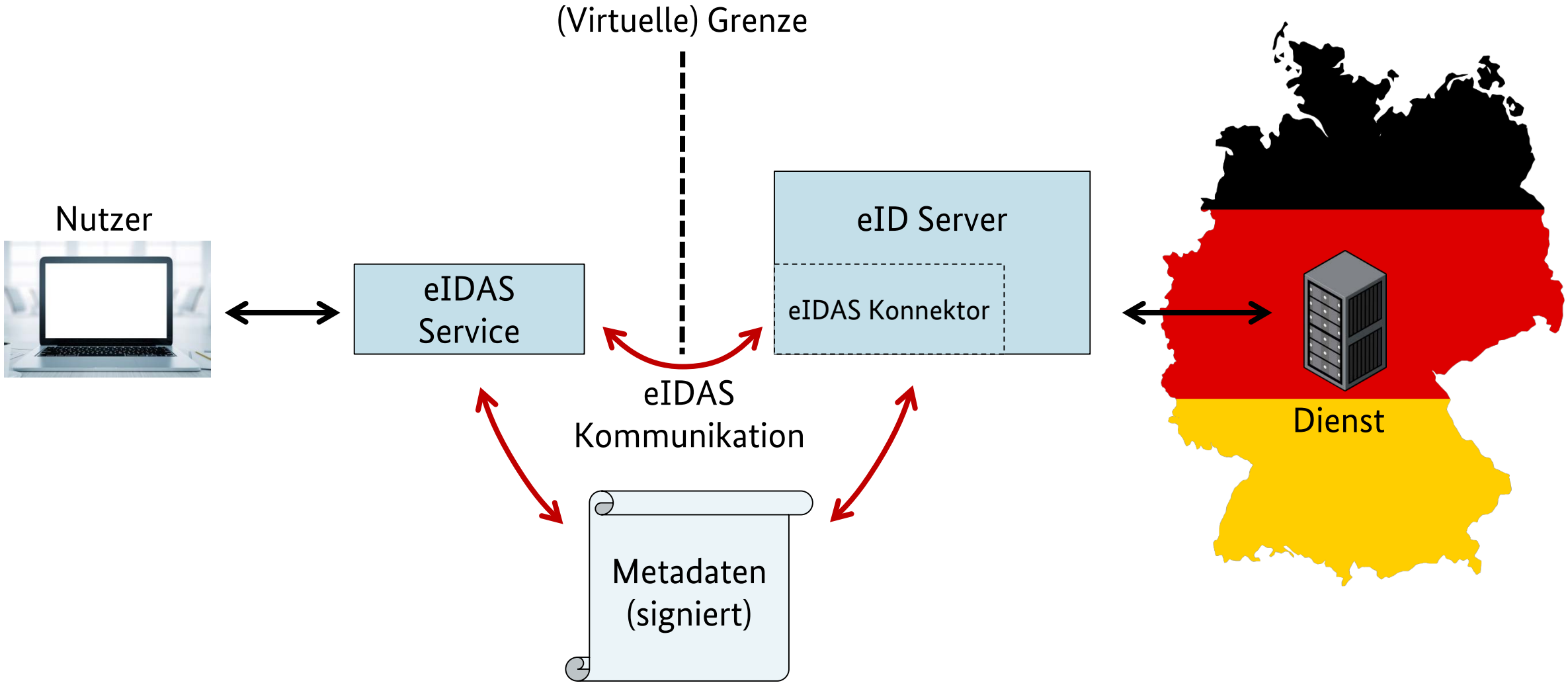
Darüber hinaus **testen** derzeit die folgenden MS die Einbindung:

BG, CY, HR, NO, PL, PT, FR, IE

Nutzung von europäischen eIDs in Deutschland

Was ist zu beachten?

Anbindung europäischer eIDs



Was muss ein Diensteanbieter also beachten?

- Der Diensteanbieter benötigt ein Berechtigungszertifikat
- Der eID Server muss um den eIDAS Konnektor erweitert werden
- Die Metadaten Root Zertifikate etc. der MS müssen importiert werden

→**Weitere FAQs auch unter**:
https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_verordnung_haeufige_fragen/eIDAS_verordnung_haeufige_fragen_node.html

Land	Titel	Status	LoA	Datum
DE	Online-Ausweisfunktion (nPA und eAT)	Not.	High	26.09.2017
IT	SPID – Public System of Digital Identity	Not.	Low/Subst./High	10.09.2018
EE	ID card, RP card, Digi-ID, und weitere …	Not.	High	07.11.2018
ES	Documento Nacional Identidad electrónico (DNIe)	Not.	High	07.11.2018
HR	NIAS and Personal Identity Card (eOI)	Not.	High	07.11.2018
LU	Luxemburg national identity card	Not.	High	07.11.2018
BE	Belgian eID Scheme FAS/eCards	Not.	High	27.12.2018
PT	Cartão de Cidadão	Not.	High	28.02.2019
UK	GOV.UK Verify	Not.	Low/Subst.	02.05.2019
CZ	National identification scheme of the Czech Republic	Not.	High	13.09.2019
NL	Trust Framework for Electronic Identification	Not.	Subst./High	13.09.2019
IT	Italian eID based on National ID card (CIE)	Not.	High	13.09.2019
BE	Belgian eID Scheme FAS / Itsme	Not.	High	18.12.2019
SK	National identity scheme of the Slovak Republic	Not.	High	18.12.2019

Übertragene Daten

	Feldtyp	PT	BE	EE	ES	HR	IT	LU	UK
Verpflichtend:	Nachname	✓	✓	✓	✓	✓	✓	✓	✓
	Vorname	✓	✓	✓	✓	✓	✓	✓	✓
	Geburtsdatum	✓	✓	✓	✓	✓	✓	✓	✓
	Personenkennziffer	✓	✓	✓	✓	✓	✓	✓	✓
Optional:	Geburtsname	✓				✓			
	Geburtsvorname								
	Geburtsort	✓	✓			✓		✓	
	Aktuelle Adresse	✓				✓	✓	✓	
	Geschlecht	✓	✓			✓		✓	
Weitere:		✓							

Was muss ein Diensteanbieter also beachten?

- Der Diensteanbieter benötigt ein Berechtigungszertifikat
- Der eID Server muss um den eIDAS Konnektor erweitert werden
- Die Metadaten Root Zertifikate der MS müssen importiert werden
- Die Liste der europäischen eIDs wächst stetig
- Die übermittelten Datenfelder hängen vom Herkunftsland ab (z.B.: Geburtsname, Adresse)
- Eine eIDAS basierte Authentifizierung macht es nötig den gesamten Datensatz zu verwenden

→**Weitere FAQs auch unter**:
https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_verordnung_haeufige_fragen/eIDAS_verordnung_haeufige_fragen_node.html

eIDAS ist und bleibt ein großes Abenteuer…

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Dr. Jens Bender und Dr. Felix Bleckmann
Referat „Technische Anforderungen an eID-Komponenten und hoheitliche Dokumente“

felix.bleckmann@bsi.bund.de
Tel. +49 (0) 228 9582 6372
Fax +49 (0) 228 10 9582 6372

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik