

BITKOM - eIDAS Summit 2019

Von Berlin nach Brüssel und zurück ...

De-Mail, eIDAS und die European netID Foundation

13.06.2019 – Leslie Romeo

1&1: Internet-Services der United Internet AG



Access

Applications

Netze

Inhalte

Endgeräte

Standard-Software

Motiviertes Team

- Rund 9.100 Mitarbeiter, davon 3.000 in Produkt-Management, Entwicklung und Rechenzentren

Vertriebskraft

- Über 5 Mio. Verträge p. a.
- Täglich 50.000 Registrierungen für Free-Dienste

Operational Excellence

- 61 Mio. Accounts in 12 Ländern

10 Rechenzentren

- 90.000 Server in Europa und USA

Leistungsfähige Netz-Infrastruktur

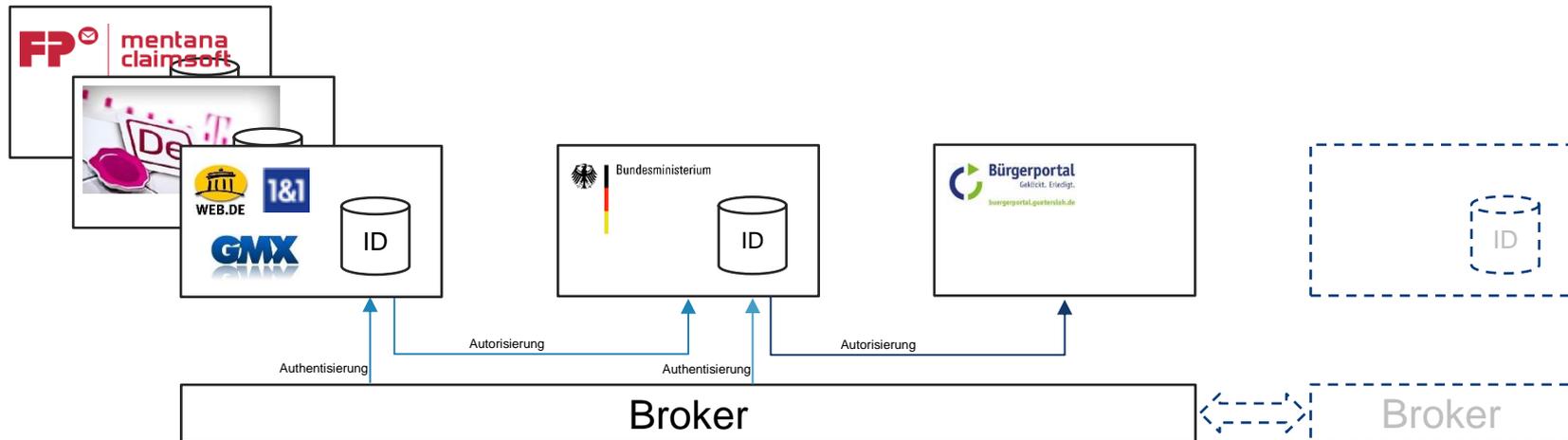
- Rund 47.000 km Glasfaser-Netz
- Bis zu 30% der Mobilfunkkapazitäten von Telefónica

■ Zertifizierter De-Mail Provider seit 03.03.2013
 ■ Qualifizierter De-Mail Dienst für die Zustellung elektronischer Einschreiben seit 01.07.2016



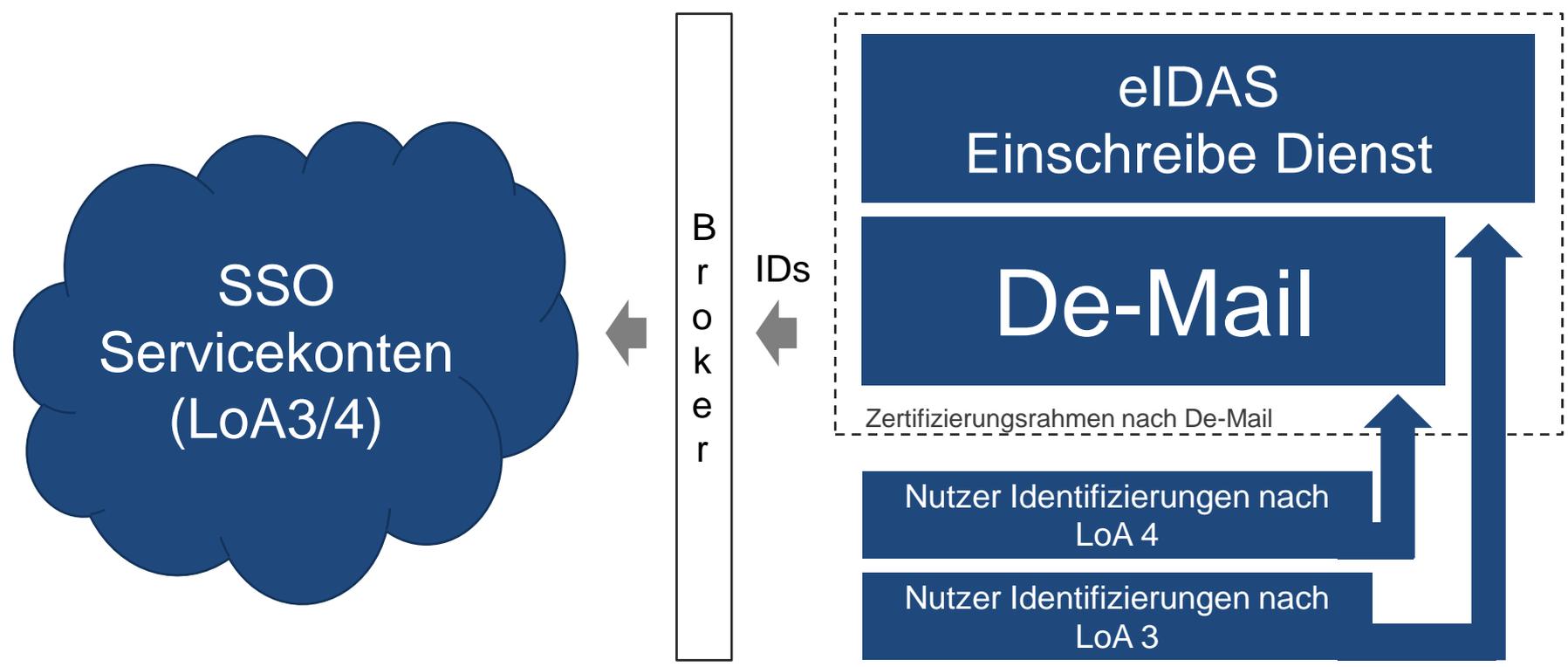


1. SSO mit „De-Mail Verifikation“



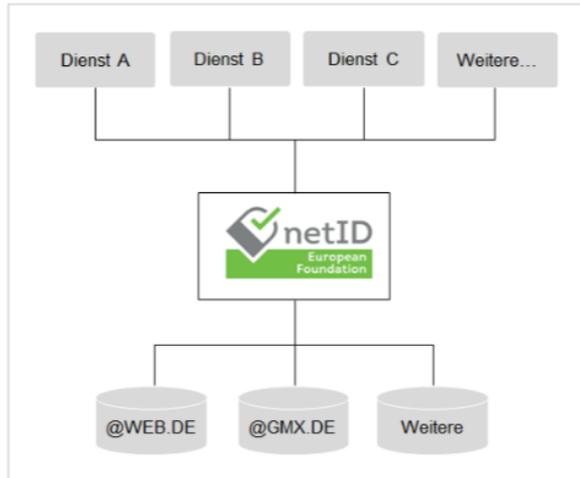
- Technische Basis bildet OpenID-Connect mit OAuth2.
- Notwendiges eindeutiges Merkmal ist die De-Mail oder E-Mail Adresse
- Offenes föderales System für alle De-Mail-Diensteanbieter
 - Erweiterung auf andere Anbieter gleichen Sicherheitsniveaus möglich (z.B. Servicekontenprovider)
- Der Broker kann sowohl zentral als auch de-zentrale sowie als föderale Instanz betrieben werden. Aus Performance und Latenz Gründen sollte die Anzahl der Broker möglichst gering gehalten werden.

2. „De-Mail Verifikation & eIDAS“



3. „European netID Foundation“

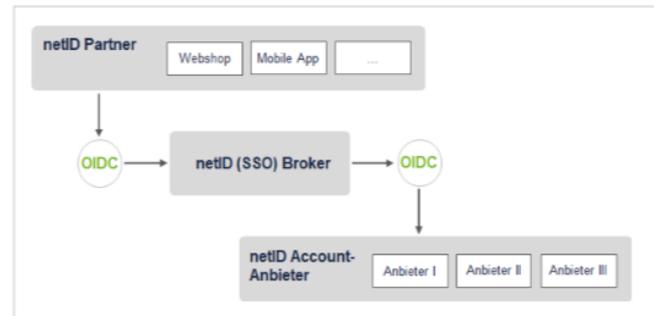
NETID KONZEPT: UNABHÄNGIGE STIFTUNG ALS ZENTRALE INSTANZ & STANDARDTECHNOLOGIE



- netID **offen** für alle¹ Dienste
 - **Entgeltfreie** (nicht-exklusive) netID Einbindung
 - **Dezentrale Nutzerdatenhaltung** der Services
-
- Setzen von **Standards** und Richtlinien
 - **Verwaltung netID**
 - **Kein Daten-Pooling**, keine Daten bei der Stiftung
-
- **Verwaltung** von **Nutzer-Accounts**
 - **Authentifizierung** der Nutzer
 - **Übertragung** von **Nutzerstammdaten** an Dienste bei Nutzereinstimmung

Technologie

- netID unterstützt die Funktionalitäten des **OpenID Connect Core 1.0** Protocols, es handelt sich dabei um eine **Standardtechnologie**
- **Weitere Rolle** im netID Kontext: Der netID (SSO) **Broker**
- Der netID (SSO) Broker erlaubt es dem netID Partner mit **mehreren netID Account-Anbietern** Nutzerdaten auszutauschen.



Weitere Details zur Anbindung finden sich im Whitepaper netID Partner (Relying Party)

3. „European netID Foundation“

ÜBERBLICK

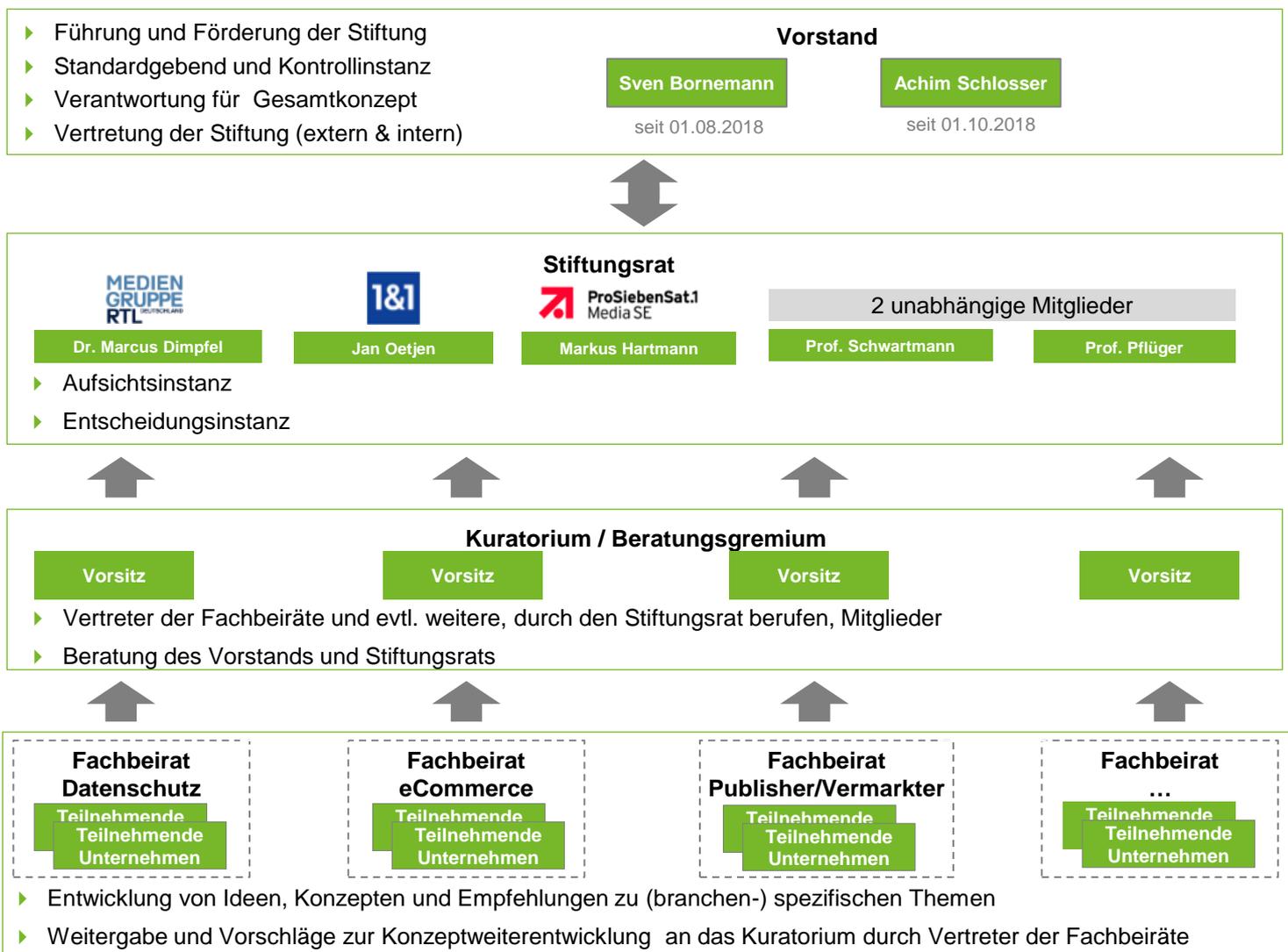


Initiatoren

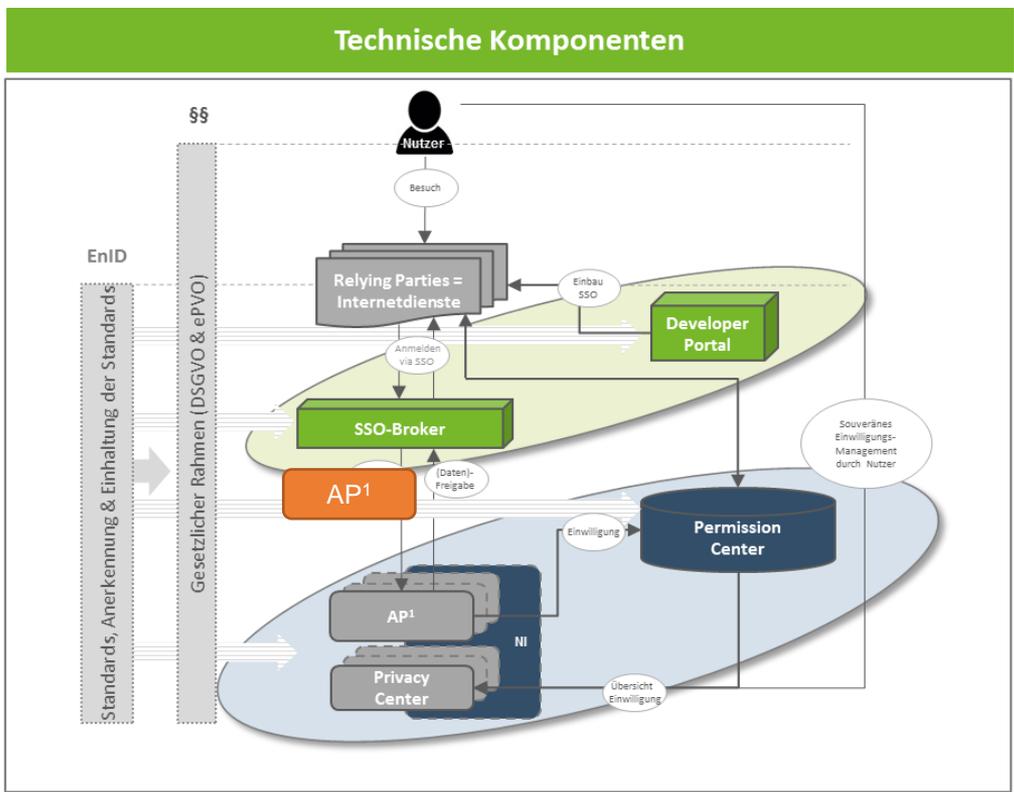
Partner / Unterstützer

Mit netID anmelden

3. „European netID Foundation“



3. „European netID Foundation“



Komponenten der Stiftung

Wesentliche technische Komponenten zur Erfüllung des Stiftungszwecks für eine „schlanke“ Stiftung

- ➔ **SSO Broker:** Zentrale Verteilungsinstanz für alle netID Nutzer und Vermittler zw. den Relying Parties und den Account Providern
- ➔ **Developer Portal:** Zentrale Anlauf- und Integrationsplattform für die Relying Parties, welche den SSO-Dienst einbinden möchten

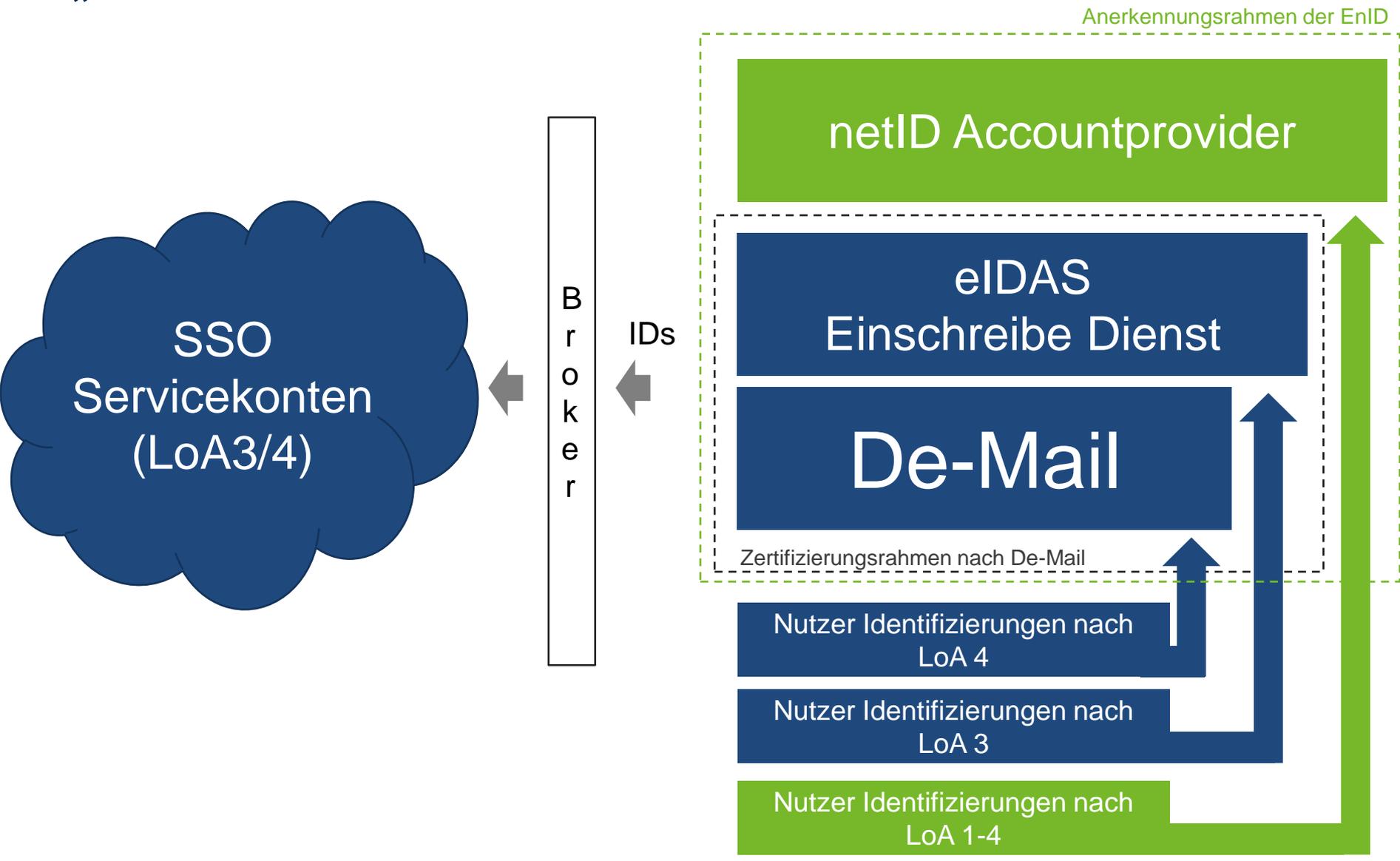
Komponenten außerhalb der Stiftung

Harmonisierung des Konstrukts durch Definition von Standards und Anerkennung technischer Dienstleister durch die Stiftung

- ➔ **Permission Center:** System zur zentralen datenschutzkonformen Speicherung und Verwaltung von Einwilligungen der Nutzer
- ➔ **Neutrale Instanz:** Technische Lösung für Account Provider zur Nutzer-Authentifizierung mit eigenem IAM System

Die zentrale Vertrauensinstanz ist der Account Provider.
 Über Anerkennungen und Zertifizierungen durch die European netID Foundation und ISO 27001 wird dies sichergestellt

4. „De-Mail Verifikation & eIDAS“ mit netID



VIELEN DANK



GMX

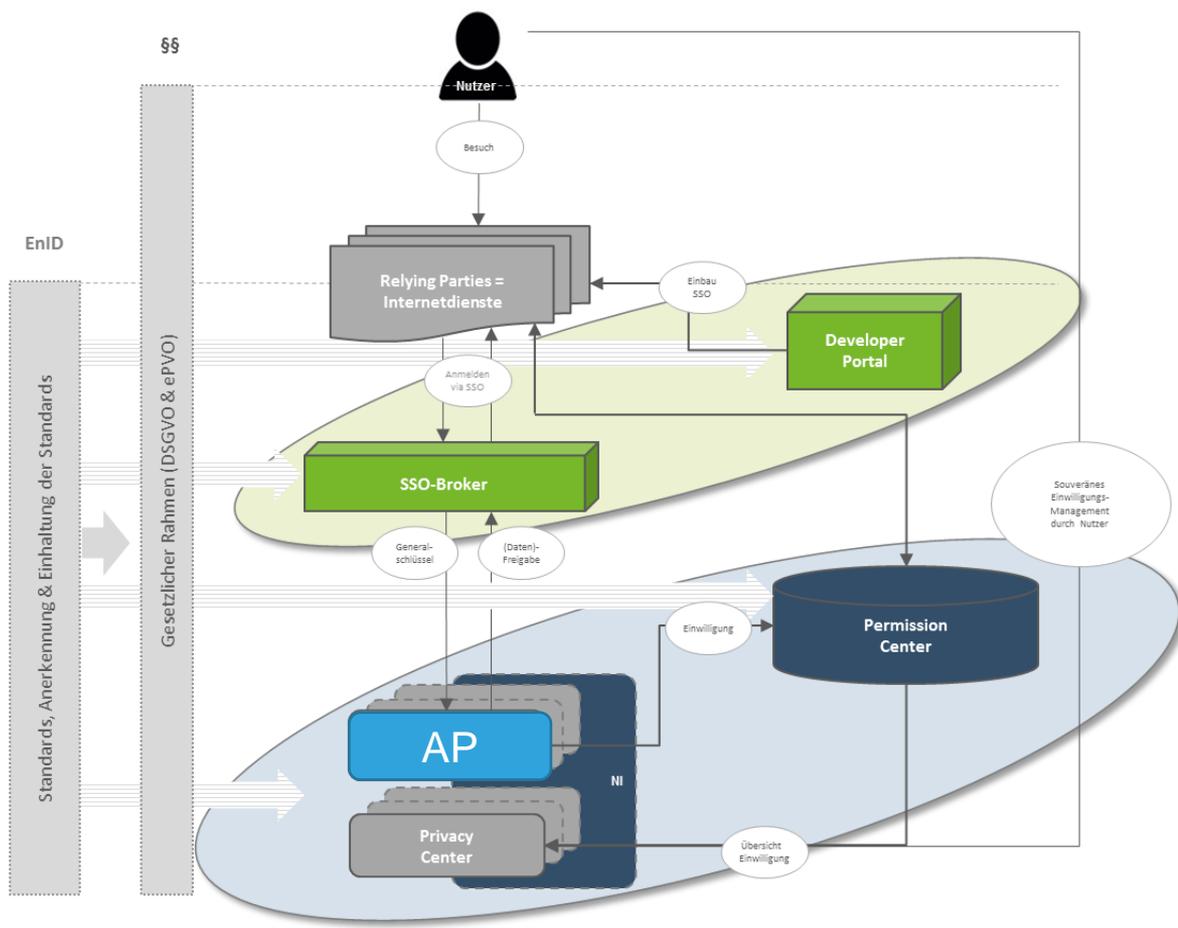


1&1

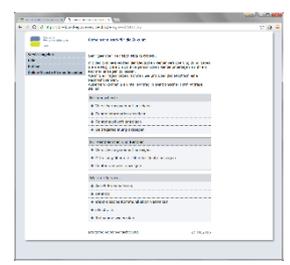
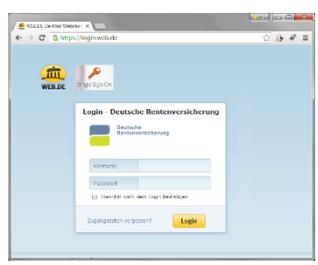


WEB.DE

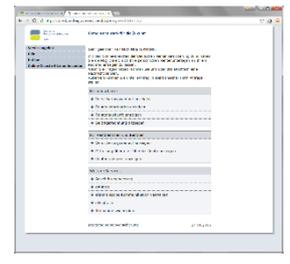
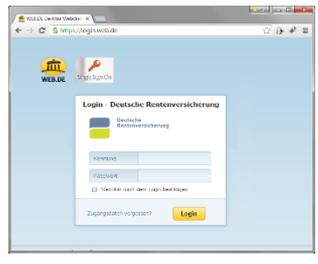
BACKUP // EXKURS



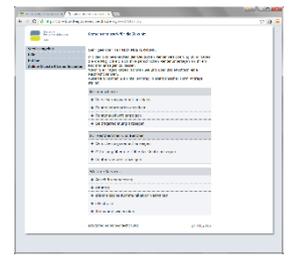
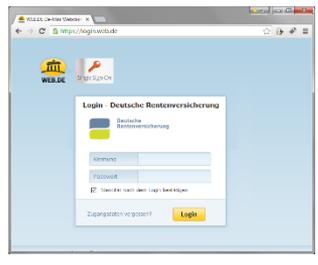
Praxisbeispiel De-Mail ID/SSO



Erster Login



Folge Login



Login mit mTAN Token

USER JOURNEY SINGLE SIGN-ON PROZESS IM ÜBERBLICK DER KOMPONENTEN

Netid User Journey 1

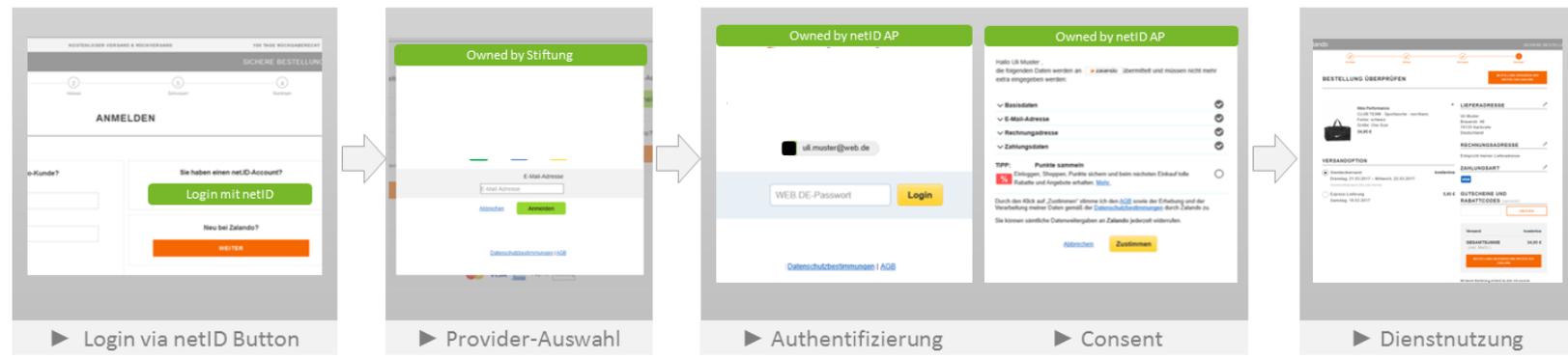
netID Erstnutzung

► Relying Party

► Broker

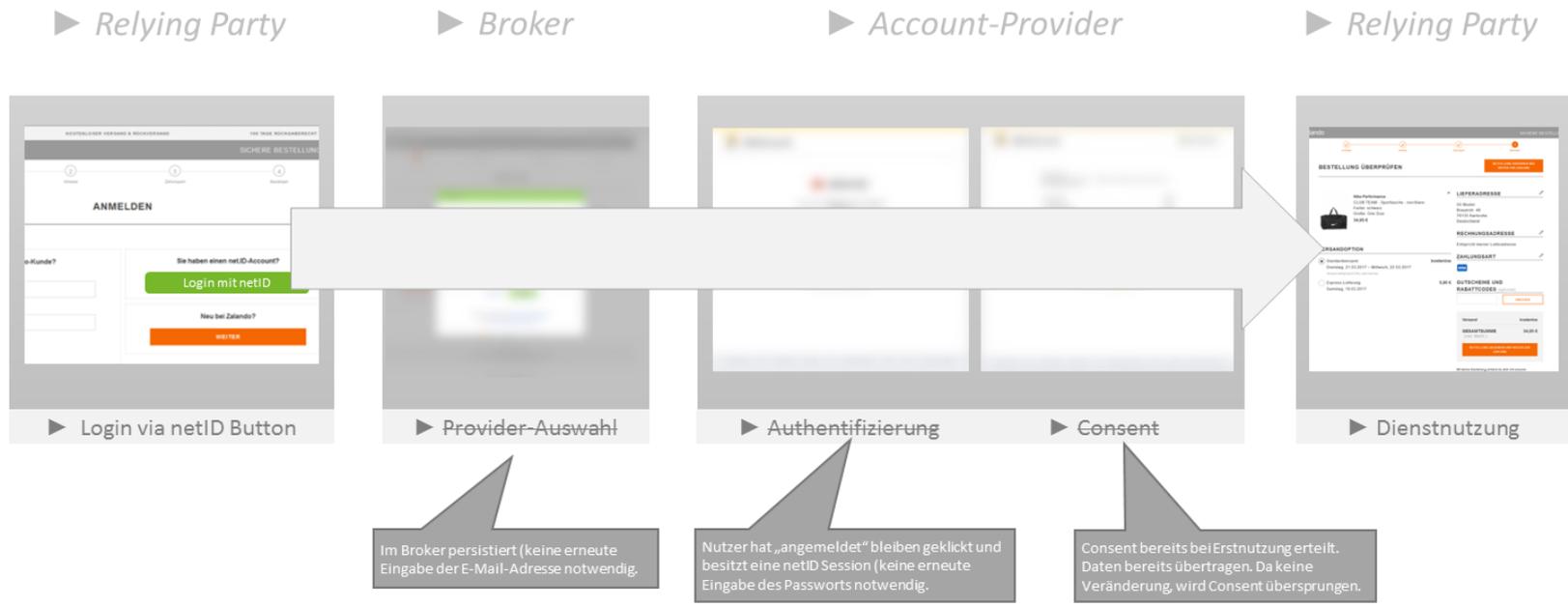
► Account-Provider

► Relying Party



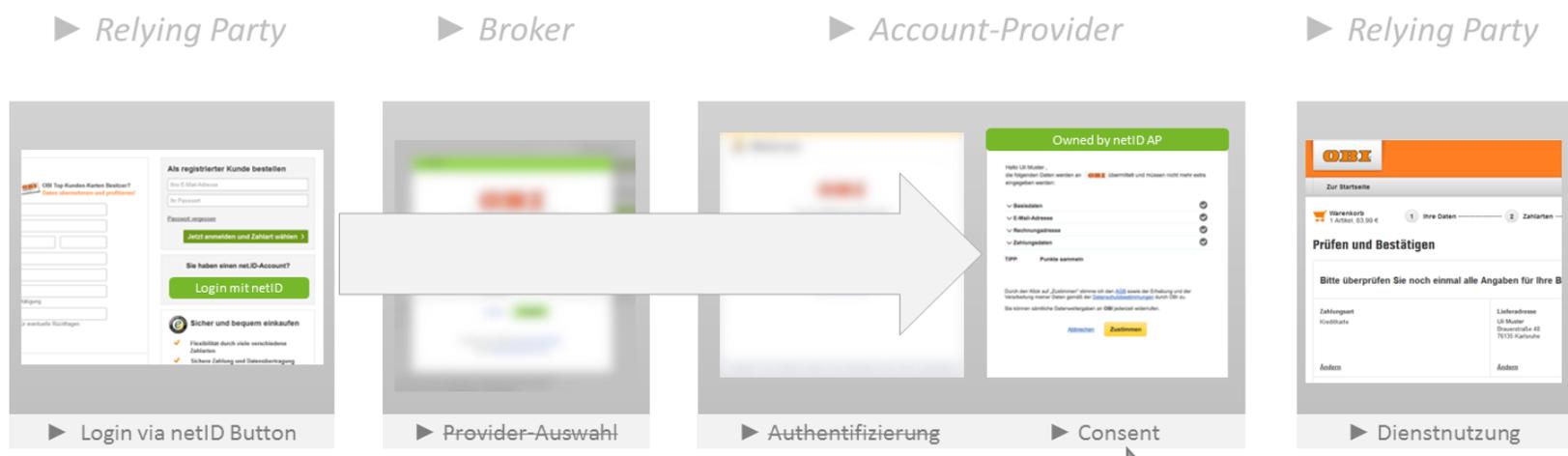
Netid User Journey 2

netID Folgenutzung einer Relying Party mit erteiltem Consent



Netid User Journey 3

netID Folgenutzung einer weiteren Relying Party noch ohne Consent



Consent wird pro Relying Party einmal (bei der Erstnutzung) abgefragt. Und dann nur noch bei Änderungen oder Datennacherfassungen.

USER FLOW SINGLE SIGN-ON

AM BEISPIEL ZALANDO

zalando SICHERE BESTELLUNG

1 Anmelden — 2 Adresse — 3 Zahlungsart — 4 Bestätigen — 5 Fertig

BEREITS ZALANDO KUNDE?

E-Mail-Adresse

Passwort

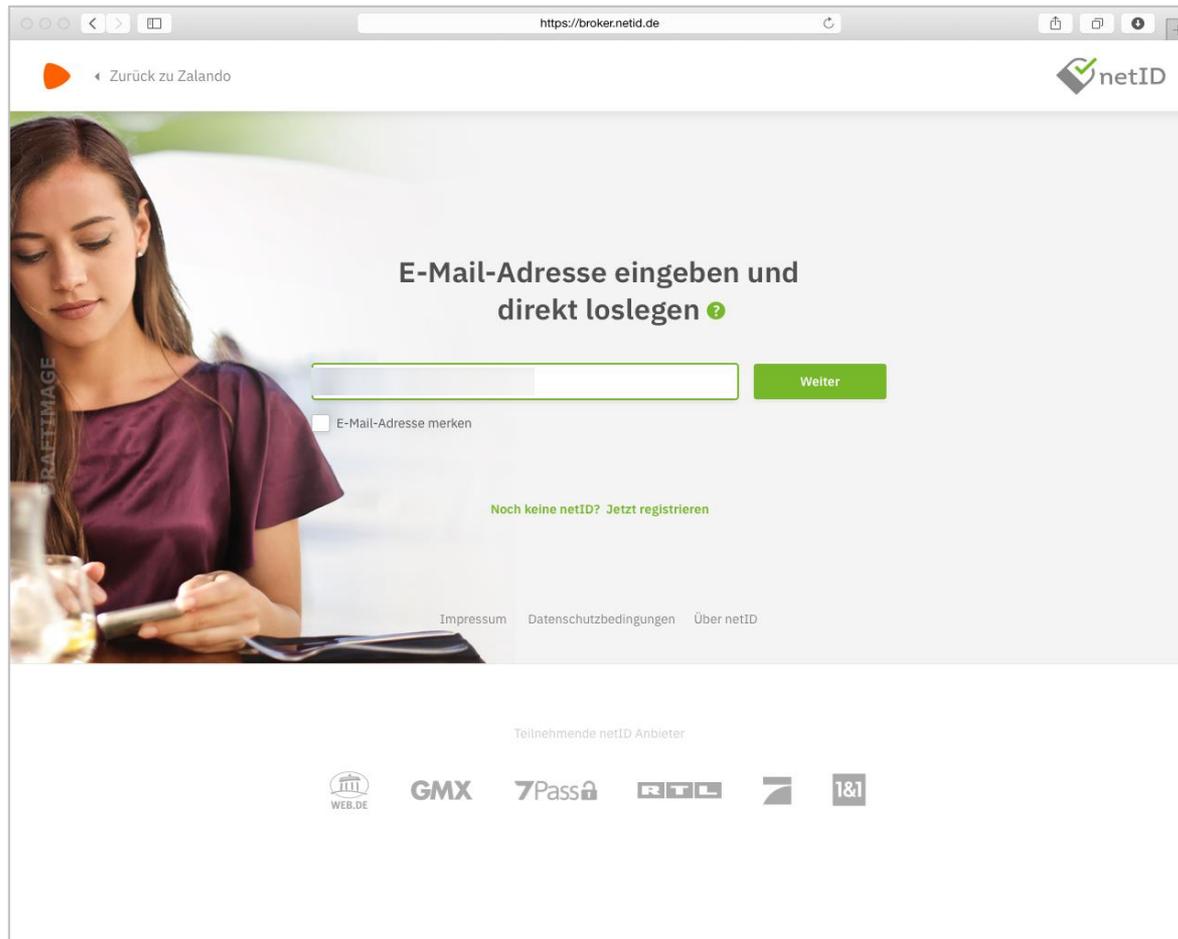
ZEIGEN

NEU BEI ZALANDO?

 WEITER

[Passwort vergessen?](#)

[← Zurück zum Shop](#) [Fragen & Antworten](#) [Datenschutz](#) [AGB](#) [Impressum](#)



https://LIA-SSO.ap.de

Zurück zu Zalando netID

Passwort eingeben

WEB.DE

E-Mail-Adresse
max.mustermann84@web.de

Passwort

Angemeldet bleiben [?](#) [Passwort vergessen?](#)

[Impressum](#) [AGB](#) [Datenschutzbedingungen](#) [Über netID](#)

Teilnehmende netID Anbieter

https://LIA-SSO.ap.de

Zurück zu Zalando max.mustermann84@web.de netID

Datenübermittlung an Zalando

Folgende Basisdaten werden übermittelt:

E-Mail-Adresse
maxmustermann84@web.de

Zalando fordert folgende Daten an, um ihre Dienste erbringen zu können, siehe AGB und [Datenschutzbestimmungen](#). Die Zalando bekommt bis zum Löschen der Verknüpfung (im Kundencenter) immer die aktuellen Daten von meinem WEB.DE-Konto und das

Geburtsdatum
13.03.1984

[Abbrechen](#) [Daten übermitteln](#)

[Impressum](#) [AGB](#) [Datenschutzbedingungen](#) [Über netID](#)

Teilnehmende netID Anbieter

zalando SICHERE BESTELLUNG

1 ✓ Anmelden —
 2 **Adresse** —
 3 Zahlungsart —
 4 Bestätigen —
 5 Fertig

LIEFERADRESSE ✎

Max Mustermann
Musterstraße 3
01234 Berlin
Deutschland

Deine Lieferadresse wurde erfolgreich von Deiner netID übermittelt. ←

RECHNUNGSADRESSE ✎

Entspricht meiner Lieferadresse

WEITER

ALLGEMEINE GESCHÄFTSBEDINGUNGEN

Bitte bestätigen Sie unsere Allgemeinen Geschäftsbedingungen durch Anklicken der Checkbox. Unsere AGB können Sie [hier](#) nachlesen.

Ich habe die AGB gelesen und akzeptiert. Den Hinweis zu meinem Widerrufsrecht habe ich verstanden.

BESTELLUNG ABSCHICKEN

Browser address bar: <https://PrivacyCenter.netid.de/ap>

Kundencenter | Start | E-Mail | Adressbuch | Kalender | Online-Speicher | WEB.DE Club | Domains | All-Net | TV-Streaming | mehr | Suche | Logout

- Übersicht
- Persönliche Daten
- Sicherheit
- Verträge
- Vertrag kündigen
- Vertrag widerrufen
- Meine Zahlungsdaten
- Meine Rechnungen
- Meine Dokumente
- netID Dienste**
- netID Einwilligungen
- Kommunikationsprofil
- Konto löschen
- Hilfe & Kontakt

netID Dienste

Verknüpfte Dienste

	Zalando	Details anzeigen
	moviepilot.de	Details anzeigen
	1und1.de	Details anzeigen

Aktive Sitzungen

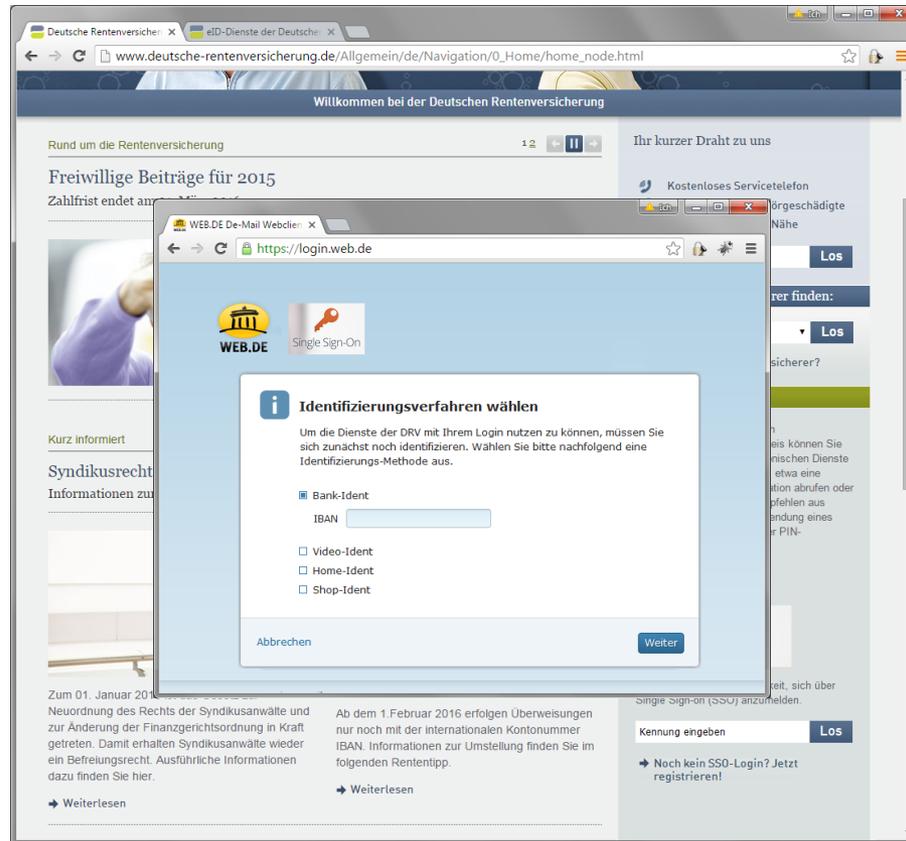
[Alle Sitzungen beenden](#)

Impressum | Jobs

The screenshot shows a web browser window with the URL <https://PrivacyCenter.netid.de/ap>. The page title is "netID Dienste > Zalando Shop". The left sidebar contains a navigation menu with items: Übersicht, Persönliche Daten, Sicherheit, Verträge, Vertrag kündigen, Vertrag widerrufen, Meine Zahlungsdaten, Meine Rechnungen, Meine Dokumente, netID Dienste (selected), netID Einwilligungen, Kommunikationsprofil, Konto löschen, and Hilfe & Kontakt. The main content area is titled "Freigegebene Daten" and shows a card for "Zalando Shop, Zalando SE" with the last update on 01.01.2017. Below this, a grey box states: "Folgende Basisdaten hat Zalando von Ihnen erhalten: E-Mail-Adresse". A paragraph explains: "Für den Zwecke der personalisierten Ansprache und der Marktforschung wurden folgende Daten an Zalando übermittelt:". A table lists the data points: Anrede, Name, Anschrift, and Geburtsdatum, each with an "aufheben" button and a trash icon. At the bottom of this section are "Speichern" and "Abbrechen" buttons. The next section is "Datenschutzbestimmungen von Zalando" with sub-headers "Wie funktioniert die Datenfreigabe?" and "Sind meine Daten und Passwörter sicher?". The final section is "Verknüpfung löschen", which includes a warning: "Damit wird die Anwendung von Deinem Konto und von der Liste der genutzten Anwendungen gelöscht." and a note: "Beachte: Die Daten können bei Zalando immer noch vorhanden sein. Für mehr Details, wie Du die Daten entfernen kannst, kontaktiere bitte Zalando. Es kann technisch bis zu 24 Stunden dauern, bis die Verknüpfung aufgehoben ist." A checkbox "Ja, ich möchte die Verknüpfung löschen." is present. A "Zurück zu netID Dienste" link is at the bottom right. The footer contains "Impressum" and "Jobs".

SSO-NUTZER: UNZUREICHENDES IDENTITÄTSLEVEL

Praxisbeispiel



Praxisbeispiel

The screenshot displays a web browser window with two tabs. The active tab is titled 'www.deutsche-rentenversicherung.de/Allgemein/de/Navigation/0_Home/home_node.html'. Below the browser window, a second window shows the Sparkasse KölnBonn internet banking login page. The page features a navigation menu on the left with categories like 'Online- & Mobile Banking', 'Konten & Karten', and 'Service'. The main content area is titled 'Herzlich willkommen zum Internet-Banking der Sparkasse KölnBonn' and contains a login form with fields for 'Anmeldename oder Legitimations-ID*' and 'PIN*'. A red 'Anmelden' button is positioned below the fields. To the right of the login form, there are several informational sections, including a 'Wichtiger Hinweis' about TAN security and a 'Warnhinweise' section. At the bottom of the page, there are links for 'Finanzstatus', 'Seite drucken', and 'Seitenanfang'.

Praxisbeispiel

The screenshot shows a web browser window with two tabs. The active tab is titled "Sparkasse KölnBonn - Ihre..." and displays the online banking interface for a "Girolent" account. The browser's address bar shows the URL "https://bankingportal.sparkasse-koelnbonn.de/portal/portal/Start".

The page header includes the Sparkasse KölnBonn logo and navigation links: "Online-Produkte", "Privatkunden", "Firmenkunden", "Weitere Kundengruppen", and "Internet Banking". A search bar is located on the right side of the header.

The main content area is titled "Girolent" and displays the following information:

- Account Details:**
 - Anfragendes Unternehmen: **Demo DeMail**
 - Zweck der Freigabe: **Gesetzlich erforderliche Identifizierung nach § 3 Abs. 2 De-Mail-G im Rahmen ihrer Beantragung eines De-Mail Postfachs.**
- Person Information:**
 - Person: **Cosmo Online-Test**
 - geb. 25.04.1972 in Köln
 - Anschrift: **Adolf-Grimme-Allee 2**
 - 50829 Köln, Deutschland
 - Mobilfunknummer: +49 (0)151 19723664

Below the account details, there is a section titled "Folgende Daten werden im Rahmen der Freigabe für den genannten Zweck übertragen:" followed by the person's contact information. At the bottom of the main content area, there are buttons for "abrechnen", "zurück", and "weiter".

The page also features a sidebar on the left with a navigation menu and a "Service" section with links such as "Filial-Suche", "Notfallnummern", and "Arbeits- & Formulare". On the right side, there is an "Info-Box" with a security warning and contact information for Lisa Dröse.

Praxisbeispiel

The screenshot shows a web browser window with two tabs. The active tab is the Sparkasse KölnBonn portal. The address bar shows the URL: <https://bankingportal.sparkasse-koelnbonn.de/portal/portal/Start>. The page title is "Willkommen bei der Deutschen Rentenversicherung".

The main content area is titled "Girolent" and contains a form for data entry. The form steps are: 1. Daten eingeben, 2. Prüfen und Senden, 3. Bestätigung. The form fields include:

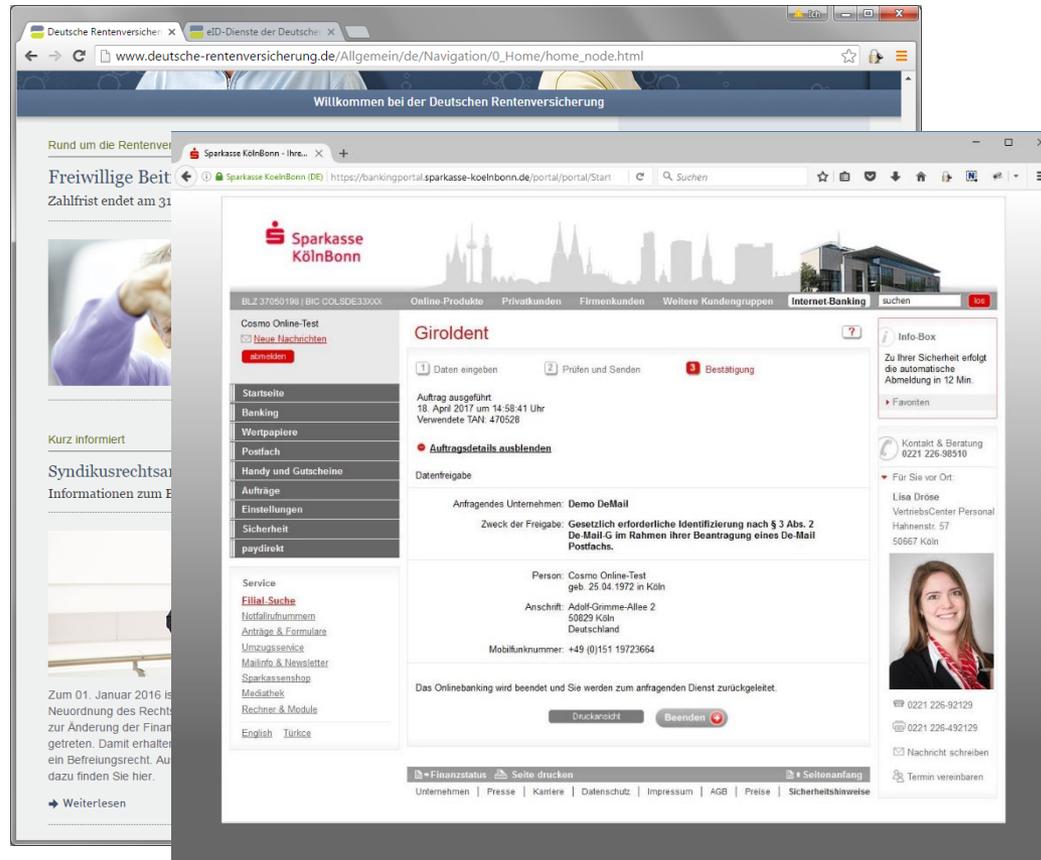
- Antragendes Unternehmen:** Demo DeMail
- Zweck der Freigabe:** Gesetzlich erforderliche Identifizierung nach § 3 Abs. 2 De-Mail-G im Rahmen ihrer Beantragung eines De-Mail Postfachs.
- Person:** Cosmo Online-Test, geb. 25.04.1972 in Köln
- Anschrift:** Adolf-Grimme-Allee 2, 50829 Köln, Deutschland
- Mobilfunknummer:** +49 (0)151 19723664

Below the form, there is a section for TAN verification: "Die TAN wurde per SMS an Handy TK (*****3664) versendet." and a field for entering the TAN. A note states: "Bitte kontrollieren Sie vor der Eingabe der TAN die per SMS versandten Auftragsdaten. Bei Abweichungen zu den eingegebenen Daten kontaktieren Sie bitte Ihren Kundenberater. Zur Bestätigung des Auftrags bitte die per SMS am 18.04.2017 um 14:57:58 Uhr zugestellte TAN eingeben und absenden".

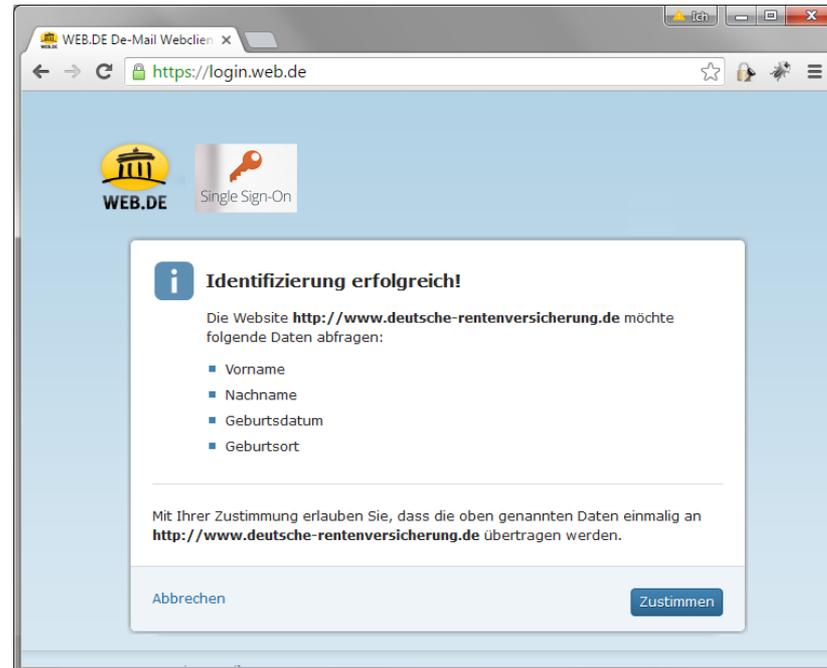
The sidebar on the left contains a navigation menu with items like "Startseite", "Banking", "Wortpapiere", "Postfach", "Handy und Gutscheine", "Aufträge", "Einstellungen", "Sicherheit", "paydirekt", and "Service". The "Service" section includes links for "Filial-Suche", "Notfallnummern", "Anträge & Formulare", "Umsorgungsservice", "MailInfo & Newsletter", "Sparkassenshop", "Mediathek", "Rechner & Module", and "Englisch / Türkce".

The right sidebar contains an "Info-Box" with contact information for Lisa Dröse, including phone numbers (0221 226-92129) and a "Nachricht schreiben" button.

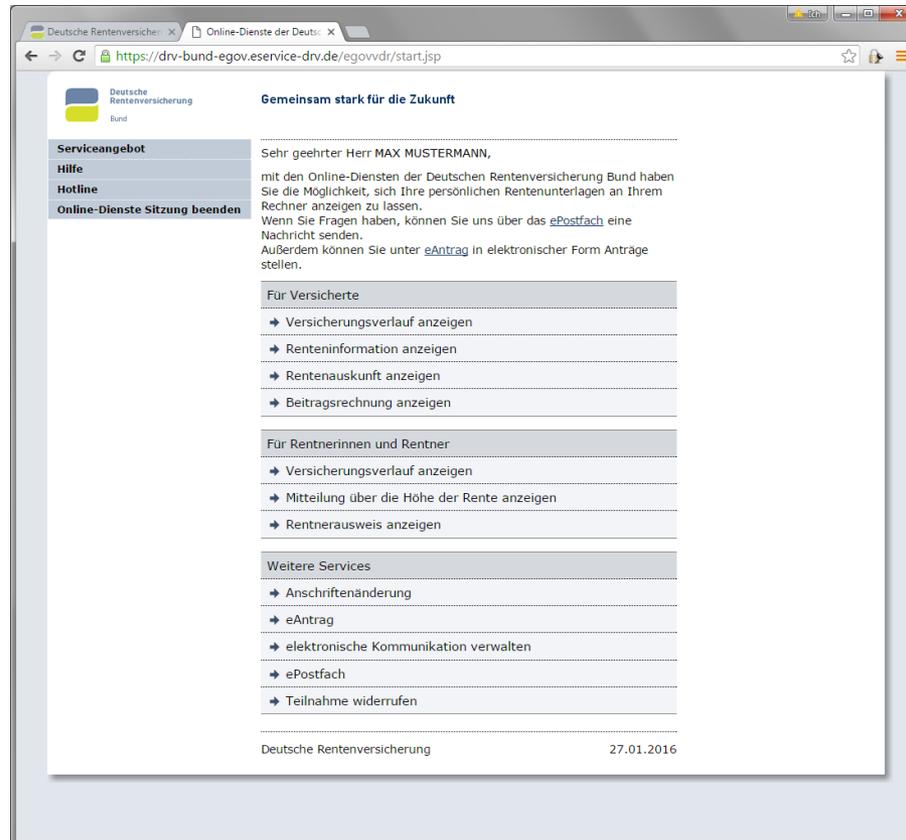
Praxisbeispiel



Praxisbeispiel



Praxisbeispiel



Anforderungen Mitgliedschaft

Alle Mitglieder müssen ein Mindestmaß an

- Authentisierung
- Identifizierung
- Interoperabilität
- Kryptografie
- Integrität
- Datenschutz
- IT-Sicherheit

einhalten und diese **Einhaltung** gegenüber einer **unabhängigen dritten Stelle**, bspw. im Rahmen einer Akkreditierung und/oder Zertifizierung – nachhaltig und dauerhaft **nachgewiesen** haben.

Nationale/Internationale Standards

	Authentisierung	Identifizierung	Interoperabilität	Kryptografie	Integrität	IT-Sicherheit	Datenschutz
national	BSI TR-3107-1 DIN ISO/IEC 27001 Nativ (A9, A11) /IT-Grundschatz	BSI TR-3107-1 DIN ISO/IEC Nativ/IT-Grundschatz (A9.2)	BSI TR-01201 Teil 1.4 DIN ISO/IEC Nativ/IT-Grundschatz (A9.2)	BSI TR-02102-x BSI TR-03116 DIN ISO/IEC 27001 (A 10) und 27002 (10)	BSI TR-03125 DIN ISO/IEC 27001 elektr.. Signaturen: DIN 31644 <u>Vorschriften:</u> SigG / SigV	BSI TR-03108 BSI TR 01201 Teil 1.3 BSI TR 01201 Teil 6.1 BSI-100-x DIN ISO/IEC 27001	BSI BS 10012 DIN ISO/IEC 27001 Nativ (A18) /IT-Grundschatz (B1.5) De-Mail Prüfkriterienkatalog <u>Vorschriften:</u> BDSG
europäisch	ETSI EN 319411-1 ETSI EN 319411-2	ETSI EN 319411-1 ETSI EN 319411-2	-/-	-/-	ETSI EN 319 102-1 ETSI EN 319 122 ETSI EN 319 132 ETSI EN 319 142 ETSI EN 319 162 CWA14167-x CWA14169 Zertifikate: ETSI EN 319 412-x <u>Vorschriften:</u> eIDAS-VO	ETSI EN 319 401 ETSI GS ISI 001 Part 1	ETSI EN 319 401 CWA 16113 <u>Vorschriften:</u> EU-DSGVO
inter-national	ISO/IEC 29115 ISO 27001 nativ (A9, A11)	ISO/ICE 29115 ISO 27001 nativ	ISO 27001 nativ	ISO 27001 nativ (A10)	ISO 27001 nativ Signaturen: ISO 14721 (OAIS) ISO 14533 ({C,X,P}AdES)	ISO 27001 nativ ISO/IEC 15408 (CC)	ISO 27001 nativ (A18) ISO/IEC 27018 ISO/IEC 29100 ISO/IEC 29101

Nachweise zu Standards

	Authentisierung	Identifizierung	Inter-operabilität	Kryptografie	Integrität	IT-Sicherheit	Datenschutz
national	BSI TR-01201 De-Mail Akkreditierung	BSI TR-01201 De-Mail Akkreditierung	BSI TR-01201 De-Mail Akkreditierung	BSI TR-01201 De-Mail Akkreditierung DIN ISO/IEC 27001 Zertifikat IT-Grundschutz	BSI TR-01201 De-Mail Akkreditierung DIN ISO/IEC 27001 Zertifikat IT-Grundschutz	BSI TR-03108 Sicherer E-Mail- Transport Akkreditierung DIN ISO/IEC 27001 Zertifikat IT-Grundschutz <u>Großbritannien:</u> BS 7799 Zertifikat ISMS	De-Mail Datenschutz- zertifikat
europäisch	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	-/-	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	-/-
inter- national	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	-/-

Fazit: Nachweise zu Standards

	Authentisierung	Identifizierung	Interoperabilität	Kryptografie	Integrität	IT-Sicherheit	Datenschutz
national	BSI TR-01201 De-Mail Akkreditierung	BSI TR-01201 De-Mail Akkreditierung	BSI TR-01201 De-Mail Akkreditierung	BSI TR-01201 De-Mail Akkreditierung DIN ISO/IEC 27001 Zertifikat IT-Grundschutz	BSI TR-01201 De-Mail Akkreditierung DIN ISO/IEC 27001 Zertifikat IT-Grundschutz	BSI TR-03108 Sicherer E-Mail-Transport Akkreditierung DIN ISO/IEC 27001 Zertifikat IT-Grundschutz <u>Großbritannien:</u> BS 7799 Zertifikat ISMS	De-Mail Datenschutz-zertifikat
europäisch	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	-/-	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	VO (EU) Nr. 910/2014 (eIDAS) Akkreditierung als qualifizierter TSP	-/-
inter-national	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	ISO 27001 nativ Zertifikat	-/-

Nachweis
Sicherheit / Prozess

Nachweis
Sicherheit IT