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

Endgeräte

Inhalte

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

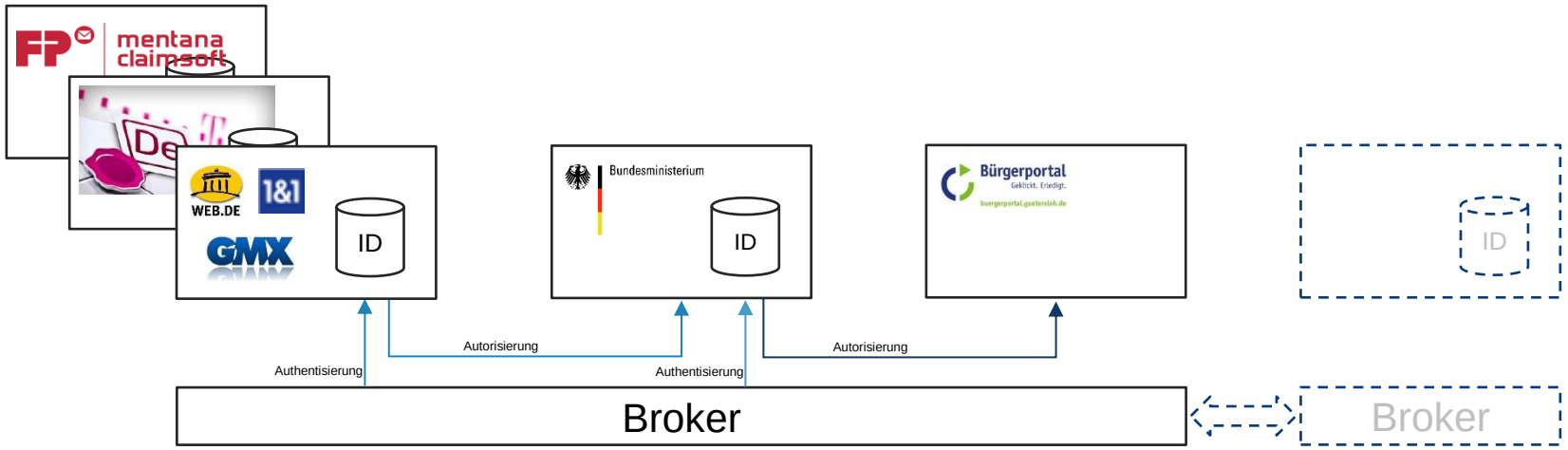
Leistungsfähige Netz-Infrastruktur

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

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

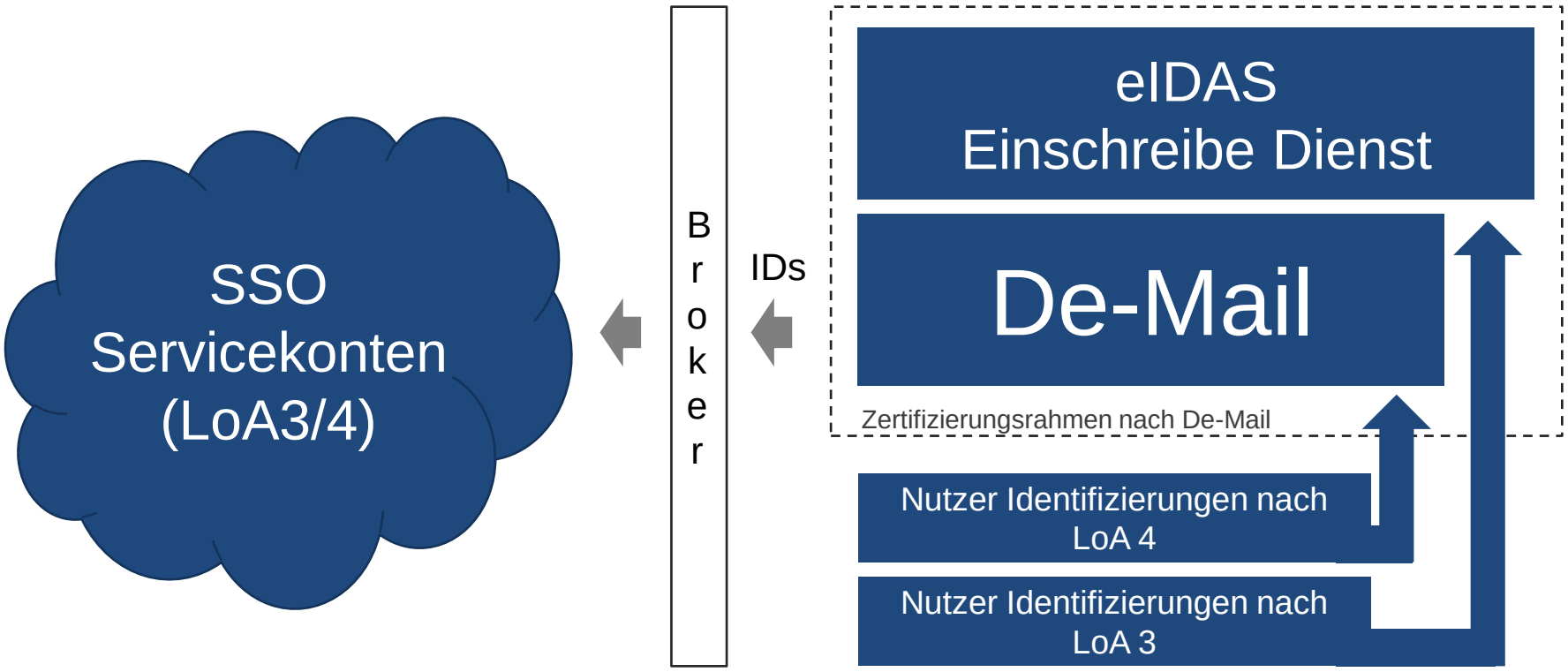
De-Mail

1. SSO mit „De-Mail Verifikation“



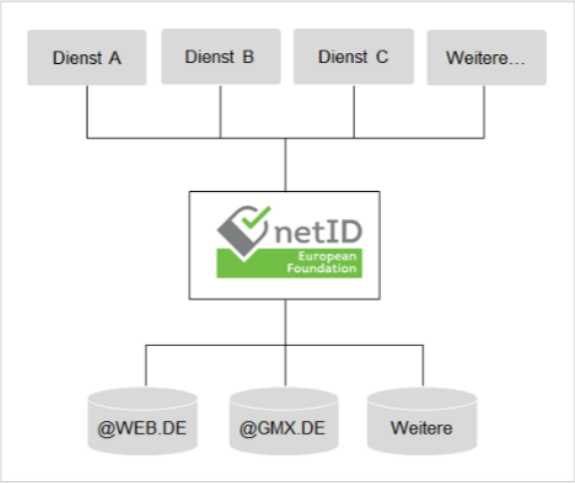
- Technische Basis bildet OpenID-Connect mit OAuth2.
- Notwendiges eineindeutiges Merkmal ist die De-Mail oder E-Mail Adresse
- Offenes föderales System für alle De-Mail-Diensteanbieter
  - Erweiterung auf andere Anbieter gleichen Sicherheitsniveaus möglich (z.B. Servicekontenprovider)
- Der Broker kann 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



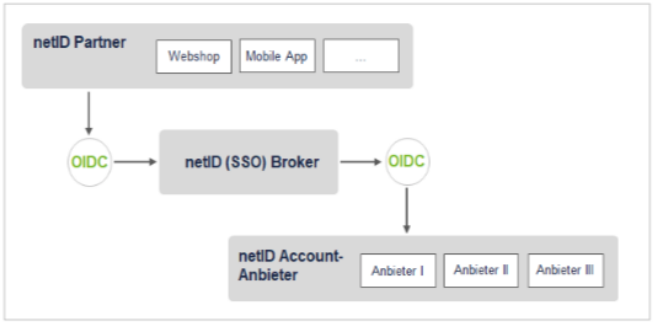
- netID **offen** für alle[1] Dienste
- **Entgeltfreie** (nicht-exklusive) netID Einbindung
- **Dezentrale Nutzerdatenhaltung** der Services

- Setzten 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 Nutzereinwilligung

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)

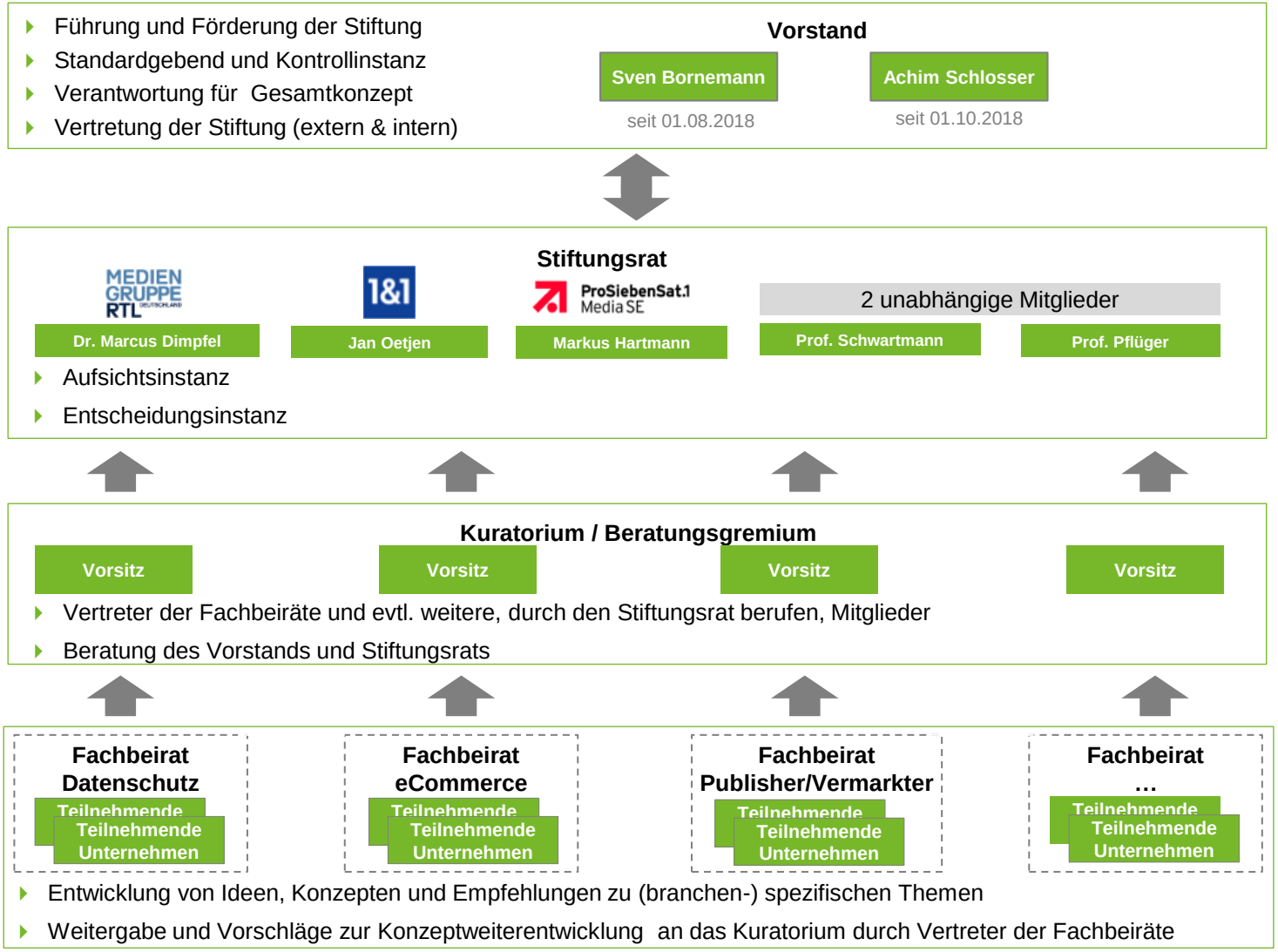
3. „European netID Foundation“

ÜBERBLICK

Initiatoren

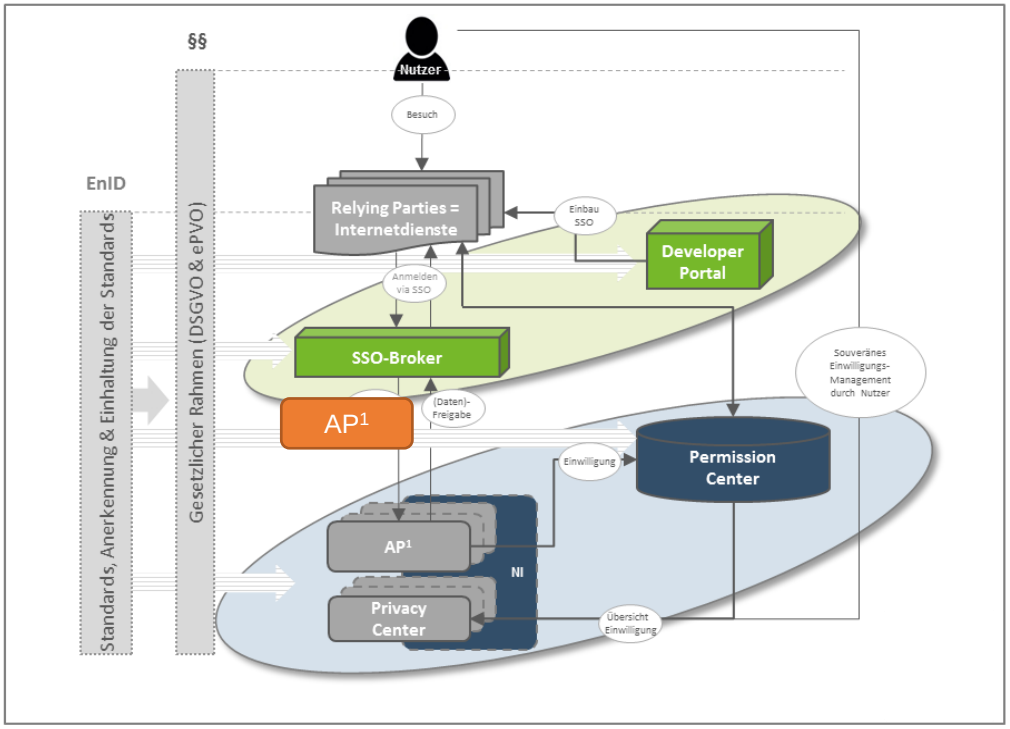
Partner / Unterstützer

3. „ European netID Foundation“



3. „ European netID Foundation“

Technische Komponenten



1 Mit Sitz des Unternehmens in der EU und im EFTA Raum

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

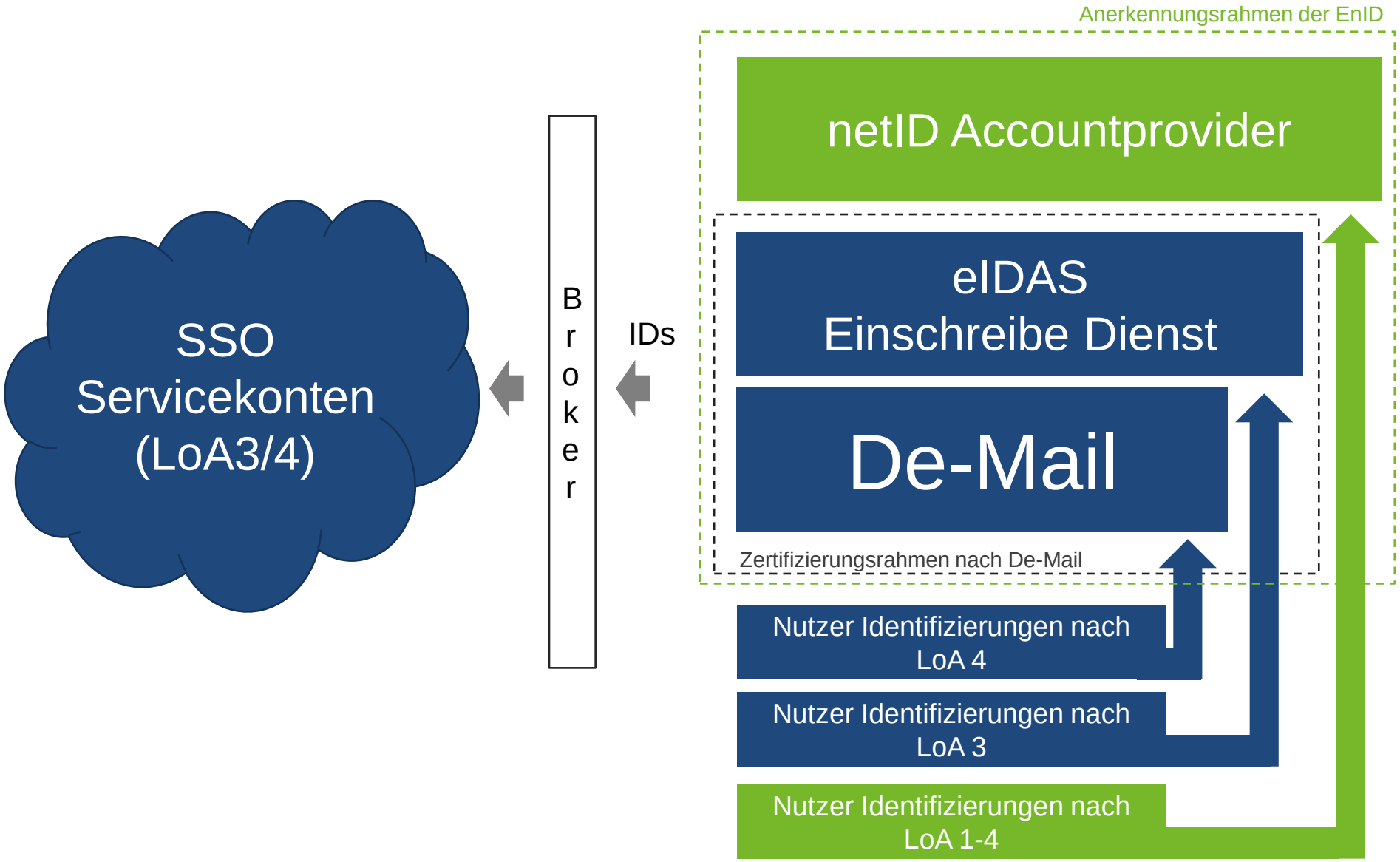
Komponenten außerhalb der Stiftung

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

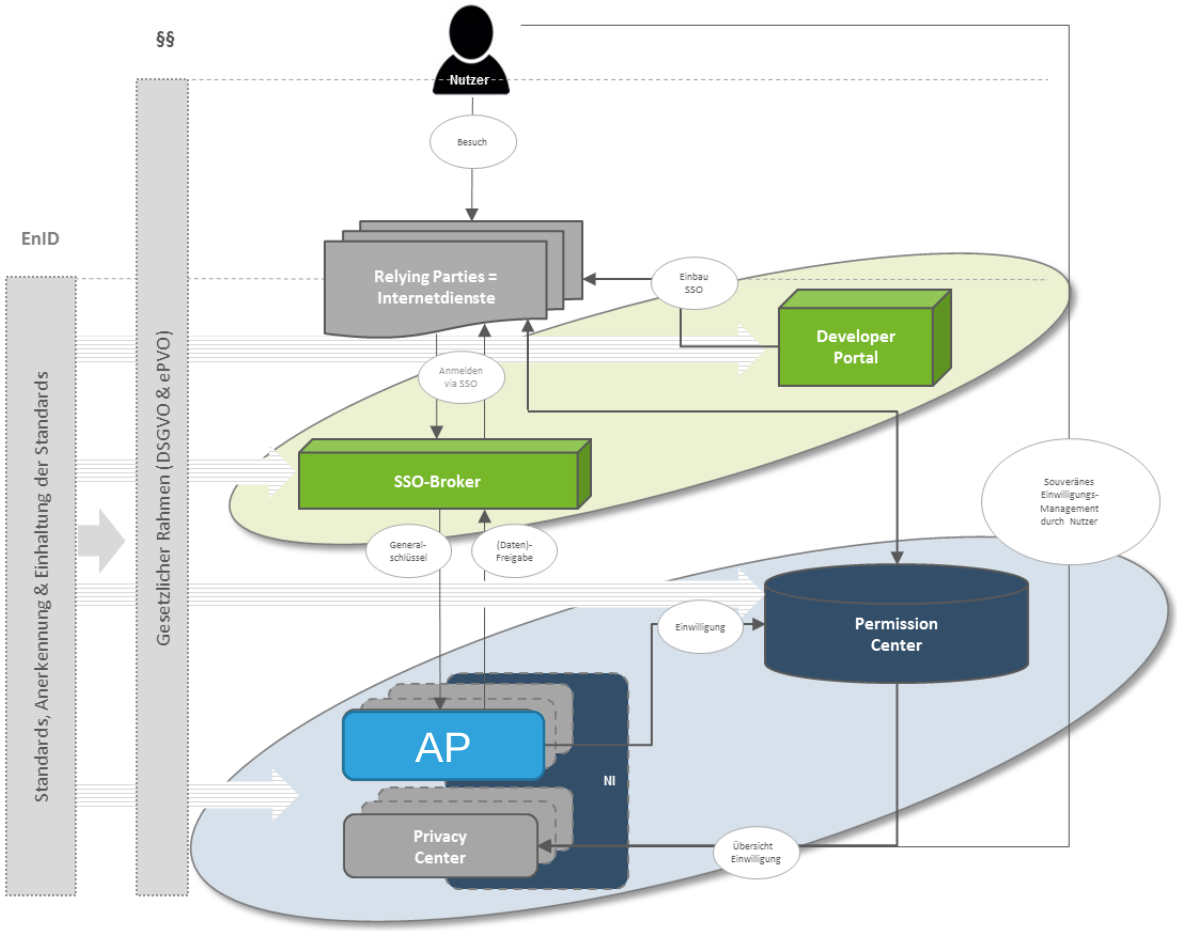
Die zentrale Vertrauensinstanz ist der Account Provider.
Über Anerkennungen und Zertifizierungen durch die European netID Foundation und ISO 27001 wird dies sichergestellt

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

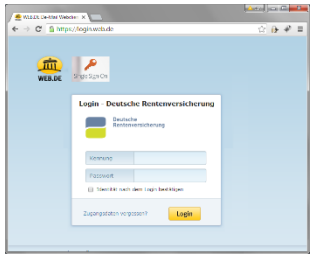


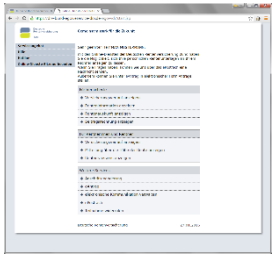
VIELEN DANK

BACKUP // EXKURS

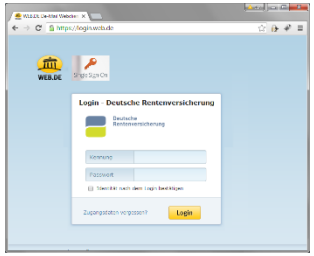

§§
Nutzer
Besuch
EnID
Relying Parties = Internetdienste
Einbau SSO
Developer Portal
Anmelden via SSO
SSO-Broker
Souveränes Einwilligungs-Management durch Nutzer
General-schlüssel
(Daten)-Freigabe
Einwilligung
Permission Center
AP
NI
Privacy Center
Übersicht Einwilligung
Standards, Anerkennung & Einhaltung der Standards
Gesetzlicher Rahmen (DSGVO & ePVO)

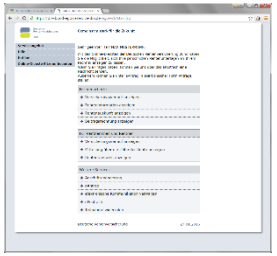
Praxisbeispiel De-Mail ID/SSO

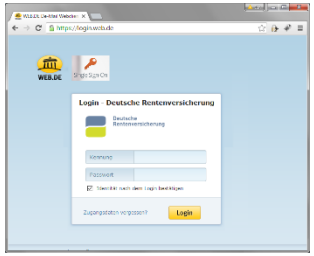


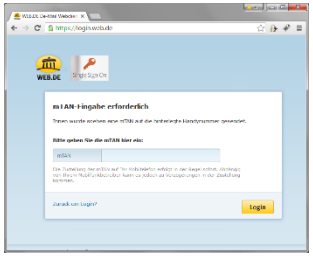
Erster Login

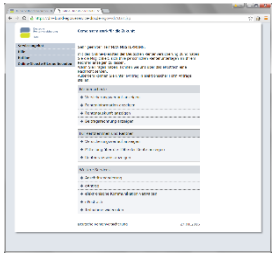





Folge Login





Login mit mTAN Token

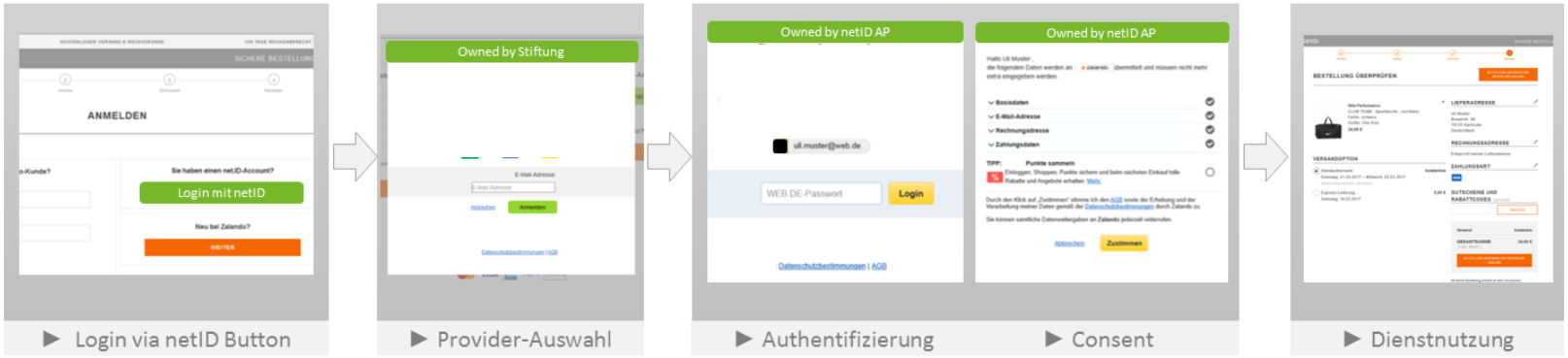
USER JOURNEY SINGLE SIGN-ON

PROZESS IM ÜBERBLICK DER KOMPONENTEN

Netid User Journey 1

netID Erstnutzung

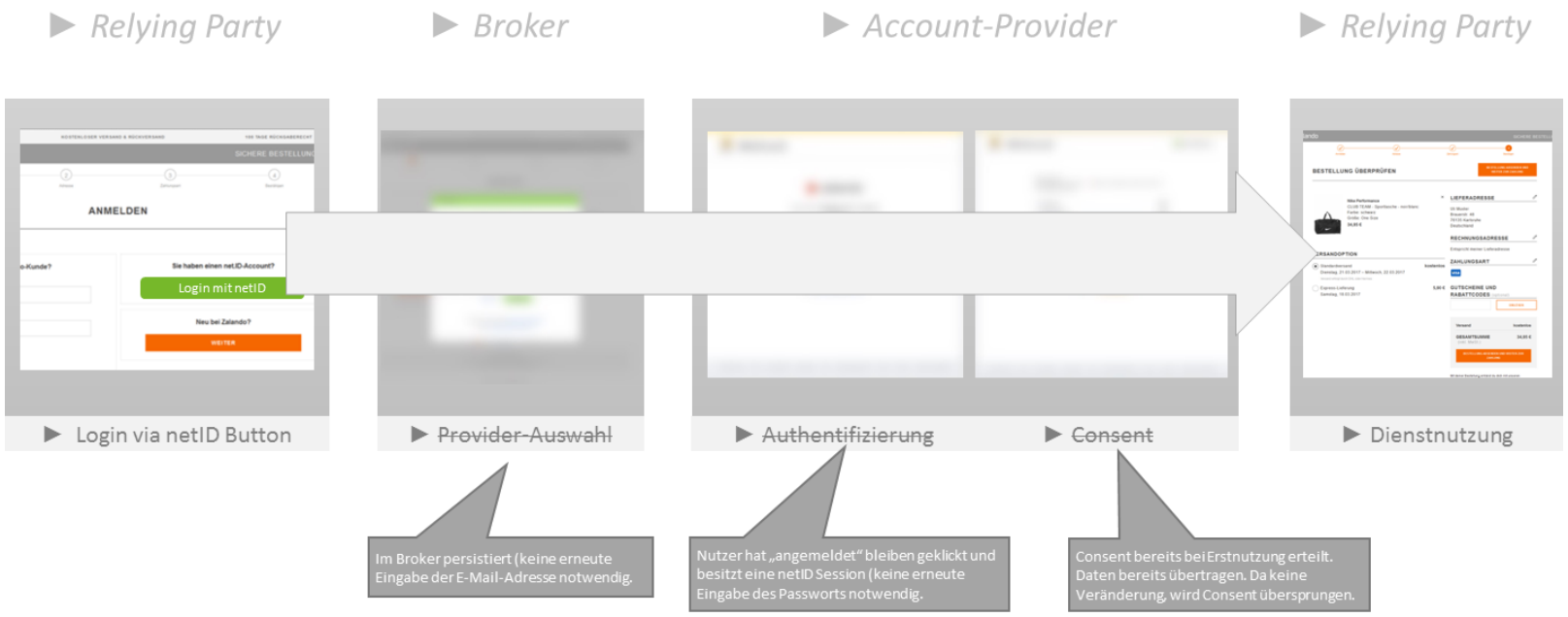
▶ *Relying Party* ▶ *Broker* ▶ *Account-Provider* ▶ *Relying Party*



▶ Login via netID Button ▶ Provider-Auswahl ▶ Authentifizierung ▶ Consent ▶ Dienstnutzung

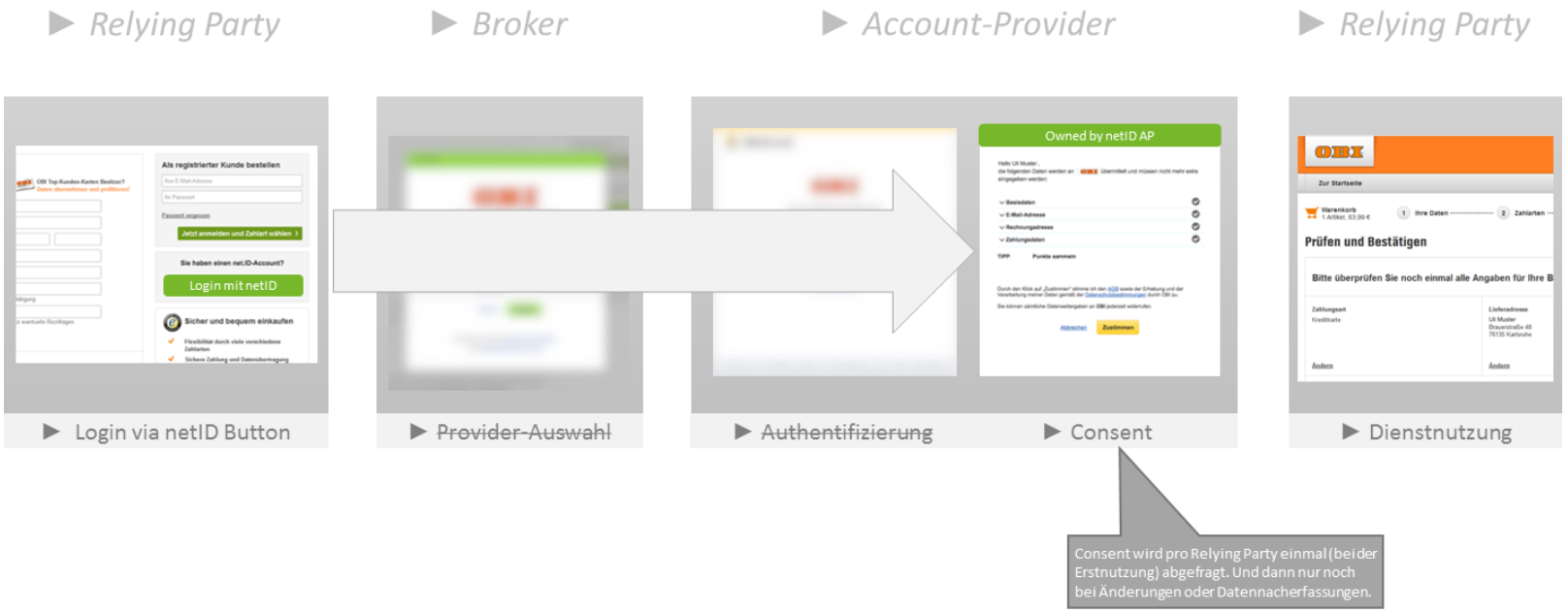
Netid User Journey 2

netID Folgenutzung einer Relying Party mit erteiltem Consent



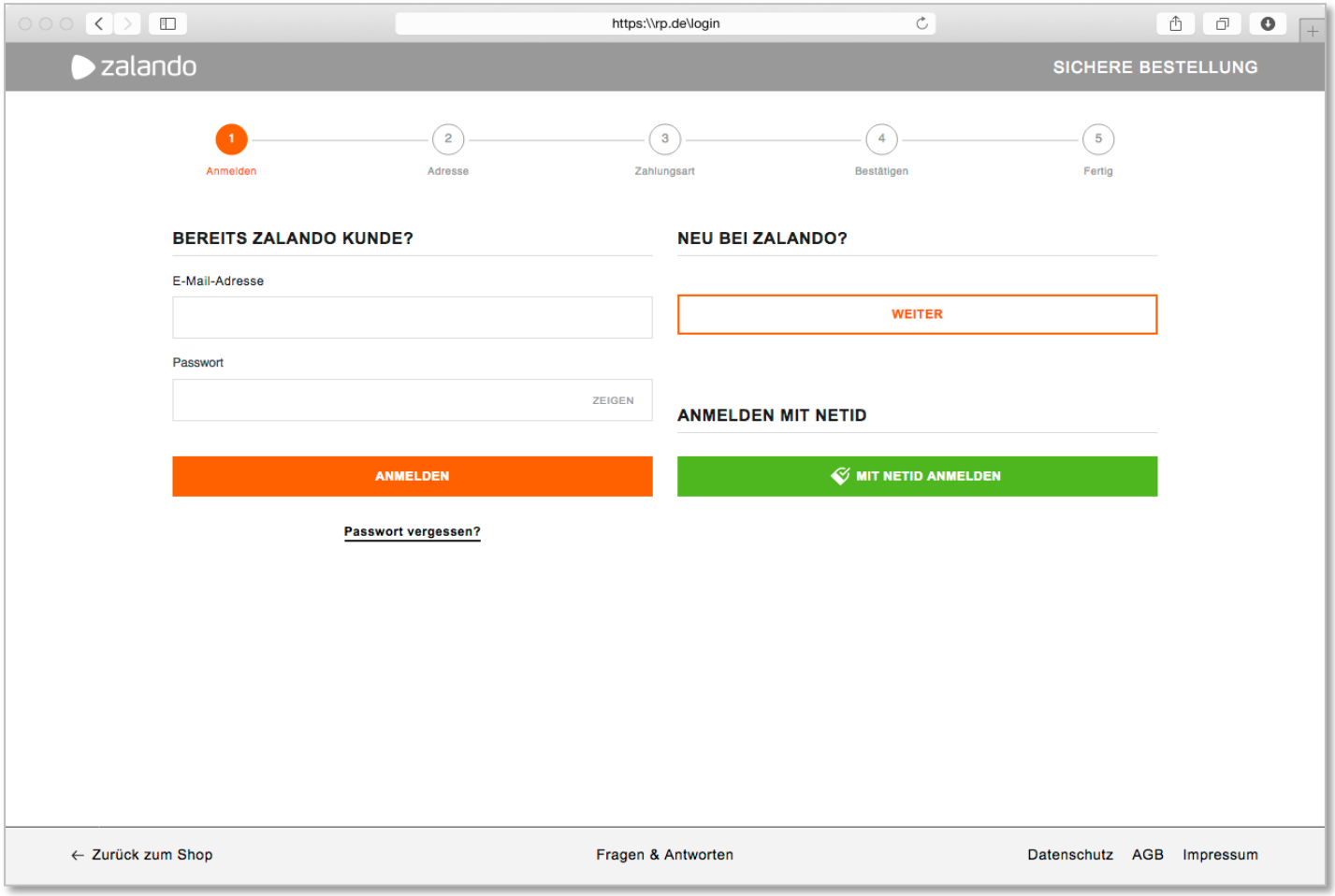
Netid User Journey 3

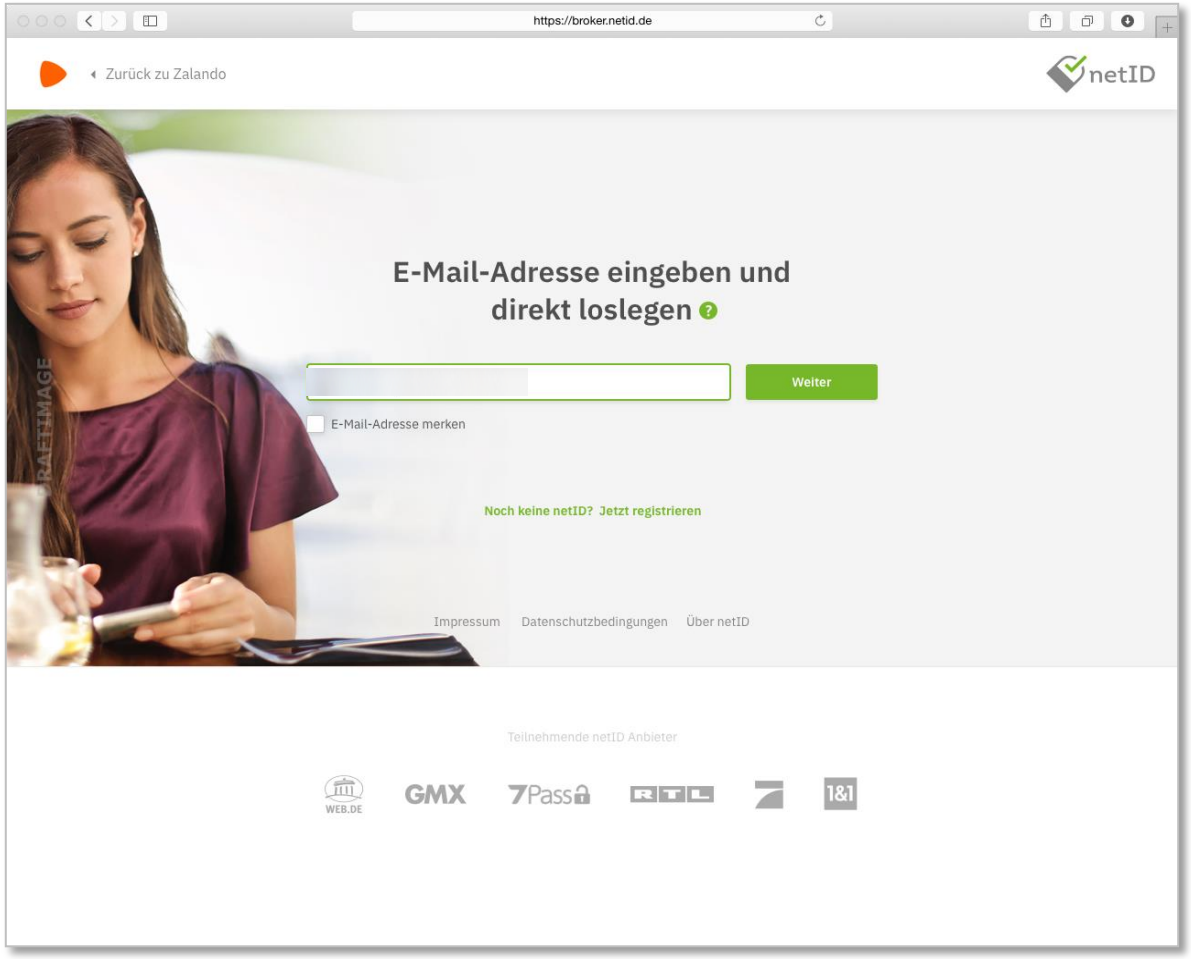
netID Folgenutzung einer weiteren Relying Party noch ohne Consent

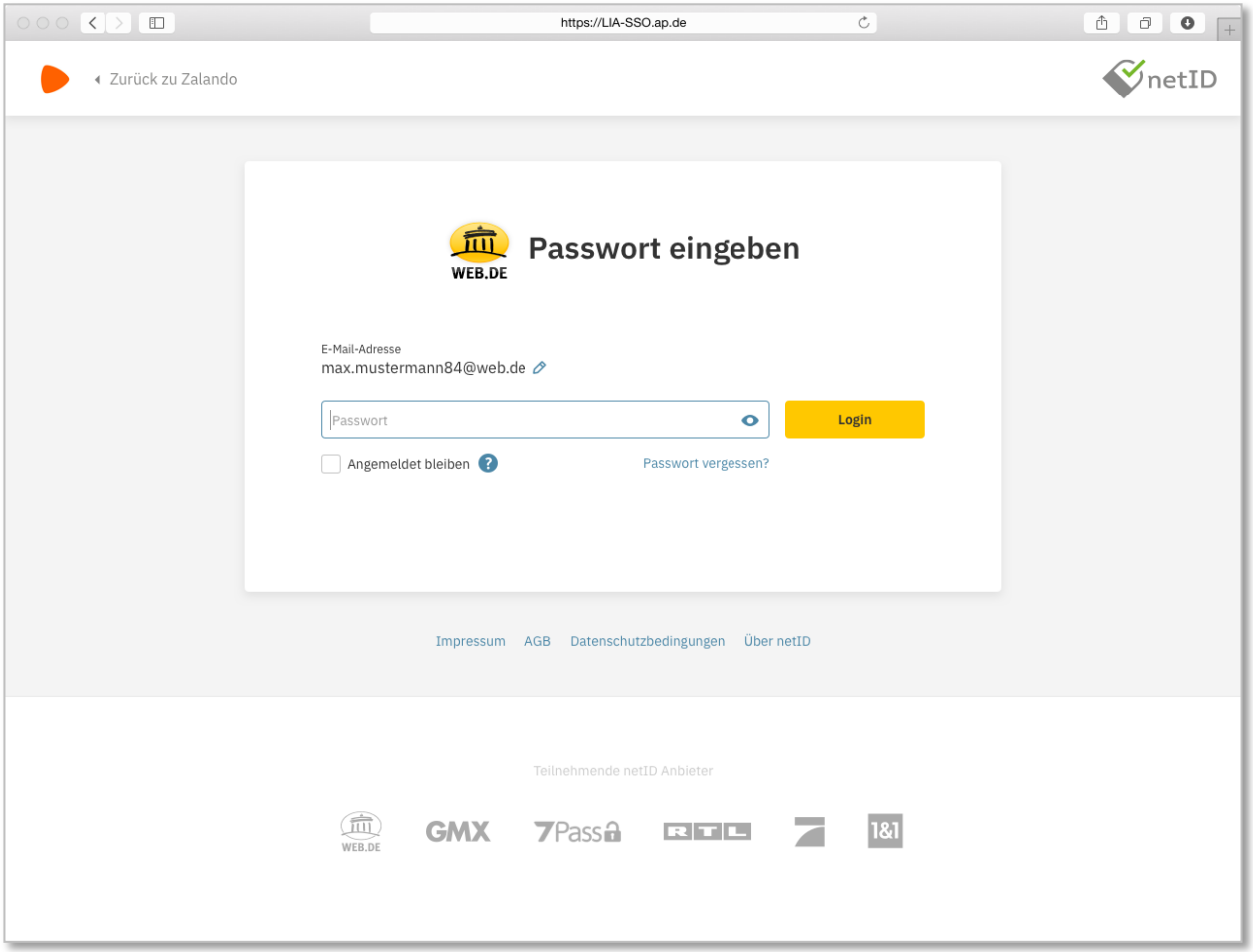


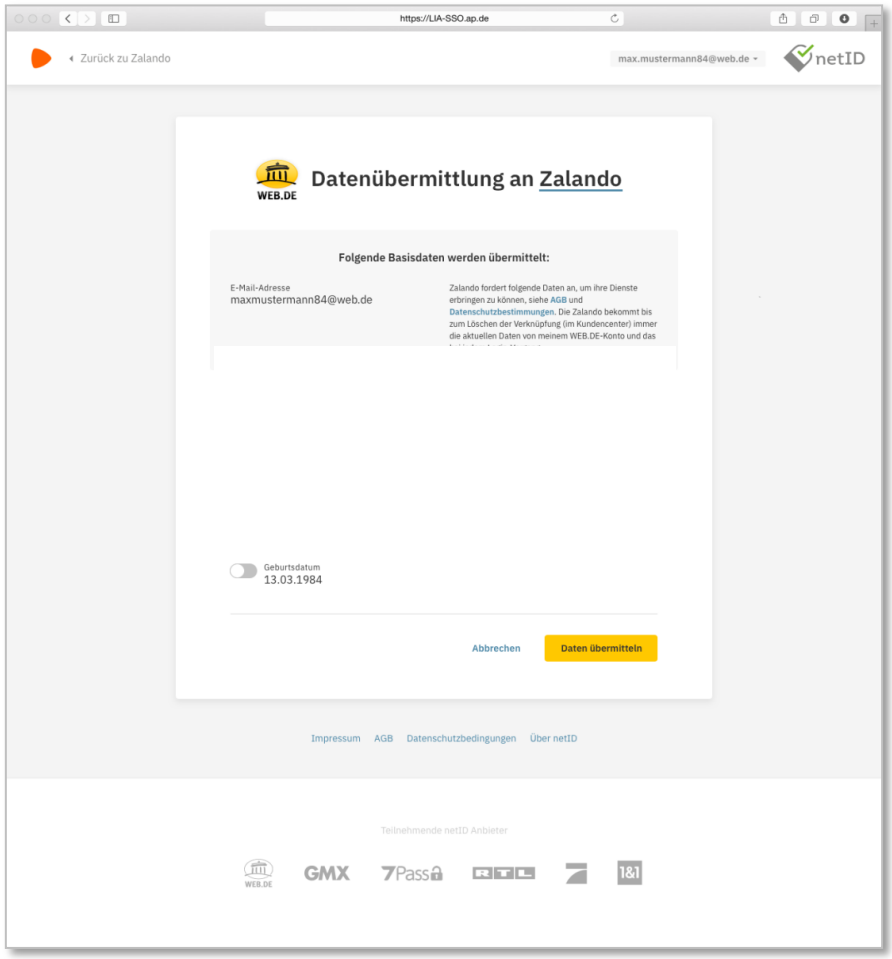
USER FLOW SINGLE SIGN-ON

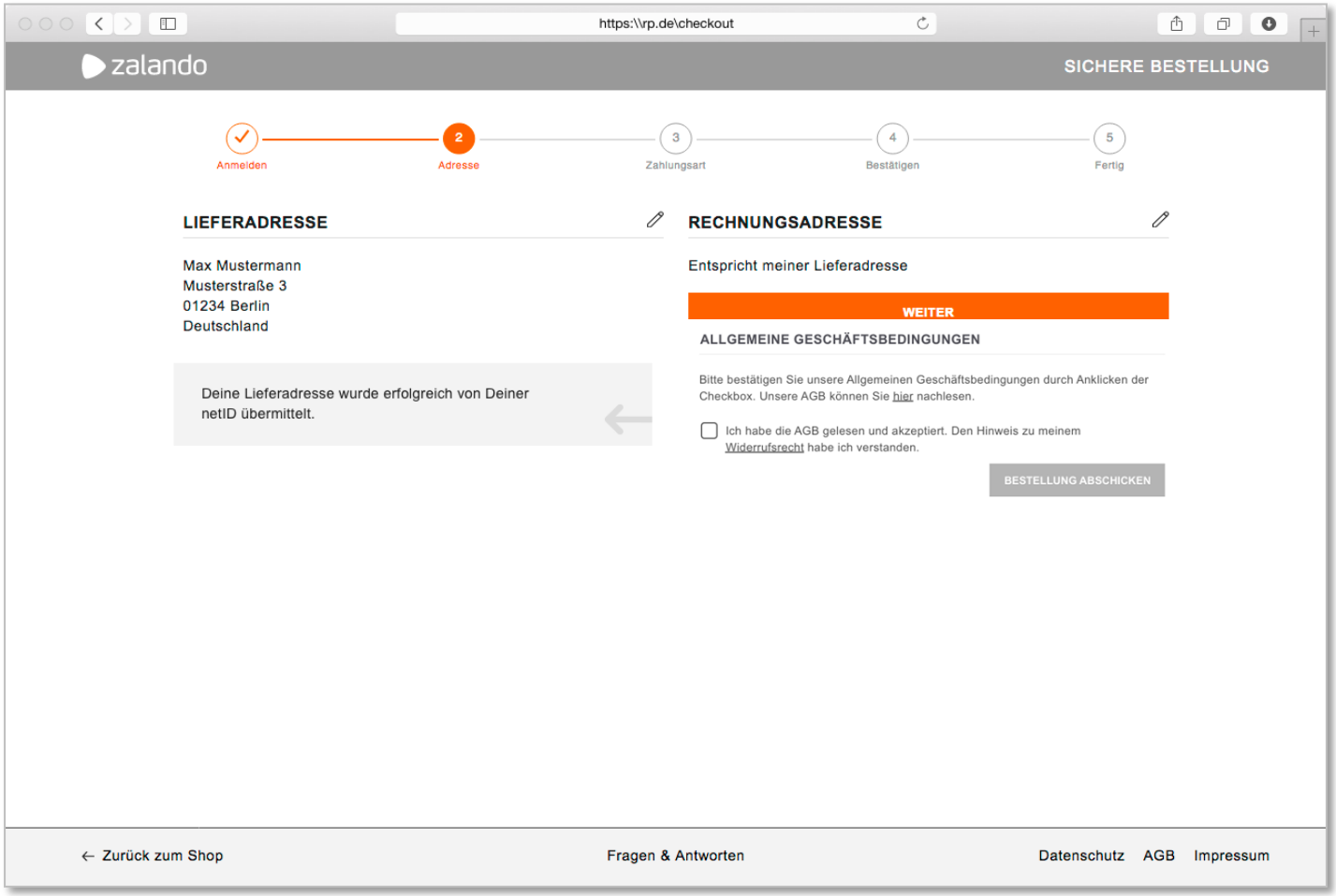
AM BEISPIEL ZALANDO

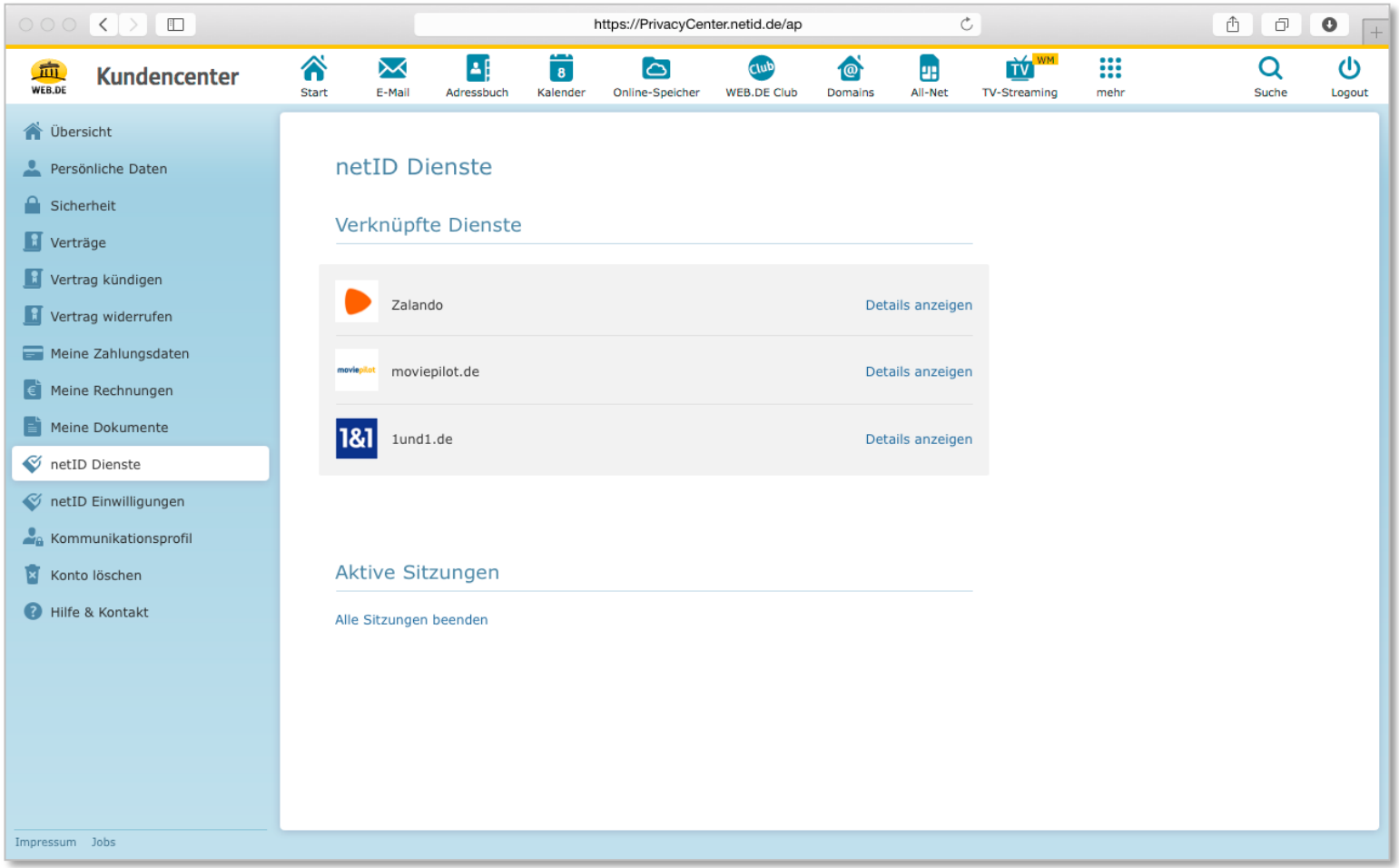

https:\\rp.de\login
zalando
SICHERE BESTELLUNG
1
Anmelden
2
Adresse
3
Zahlungsart
4
Bestätigen
5
Fertig
BEREITS ZALANDO KUNDE?
E-Mail-Adresse
Passwort
ZEIGEN
ANMELDEN
Passwort vergessen?
NEU BEI ZALANDO?
WEITER
ANMELDEN MIT NETID
MIT NETID ANMELDEN
← Zurück zum Shop
Fragen & Antworten
Datenschutz
AGB
Impressum

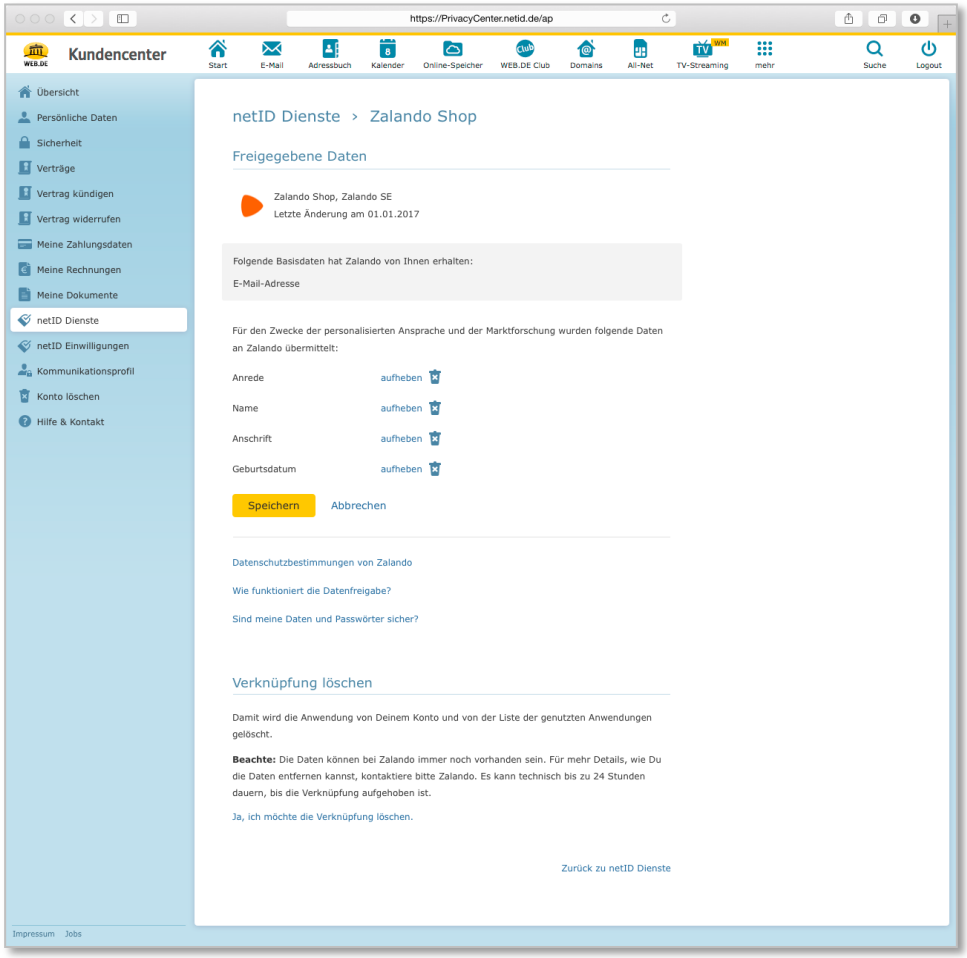

https://broker.netid.de
Zurück zu Zalando
netID
E-Mail-Adresse eingeben und direkt loslegen
Weiter
E-Mail-Adresse merken
Noch keine netID? Jetzt registrieren
Impressum
Datenschutzbedingungen
Über netID
Teilnehmende netID Anbieter
WEB.DE
GMX
7Pass
RTL
1&1


https://LIA-SSO.ap.de
Zurück zu Zalando
netID
WEB.DE
Passwort eingeben
E-Mail-Adresse
max.mustermann84@web.de
Passwort
Login
Angemeldet bleiben
Passwort vergessen?
Impressum
AGB
Datenschutzbedingungen
Über netID
Teilnehmende netID Anbieter
WEB.DE
GMX
7Pass
RTL
1&1


https://LIA-SSO.ap.de
Zurück zu Zalando
max.mustermann84@web.de
netID
WEB.DE
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
WEB.DE
GMX
7Pass
RTL
1&1

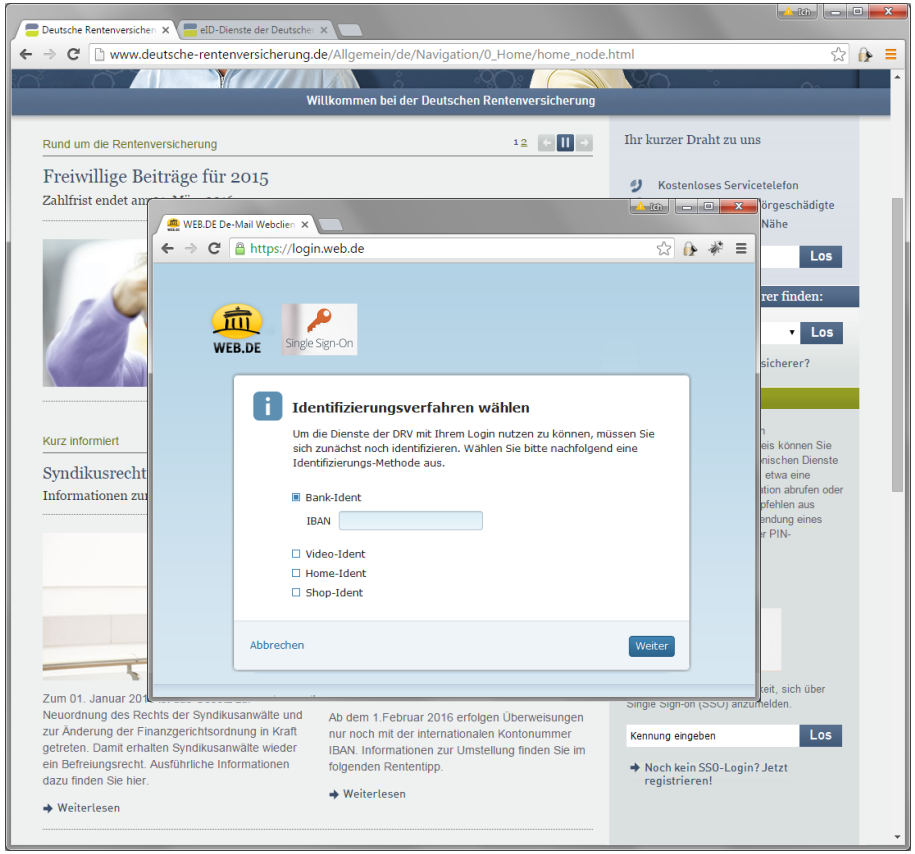

https:\\rp.de\checkout
zalando
SICHERE BESTELLUNG
Anmelden
2
Adresse
3
Zahlungsart
4
Bestätigen
5
Fertig
LIEFERADRESSE
Max Mustermann
Musterstraße 3
01234 Berlin
Deutschland
Deine Lieferadresse wurde erfolgreich von Deiner netID übermittelt.
RECHNUNGSADRESSE
Entspricht meiner Lieferadresse
WEITER
ALLGEMEINE 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
← Zurück zum Shop
Fragen & Antworten
Datenschutz
AGB
Impressum


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
Impressum
Jobs
netID Dienste
Verknüpfte Dienste
Zalando
Details anzeigen
moviepilot.de
Details anzeigen
1und1.de
Details anzeigen
Aktive Sitzungen
Alle Sitzungen beenden

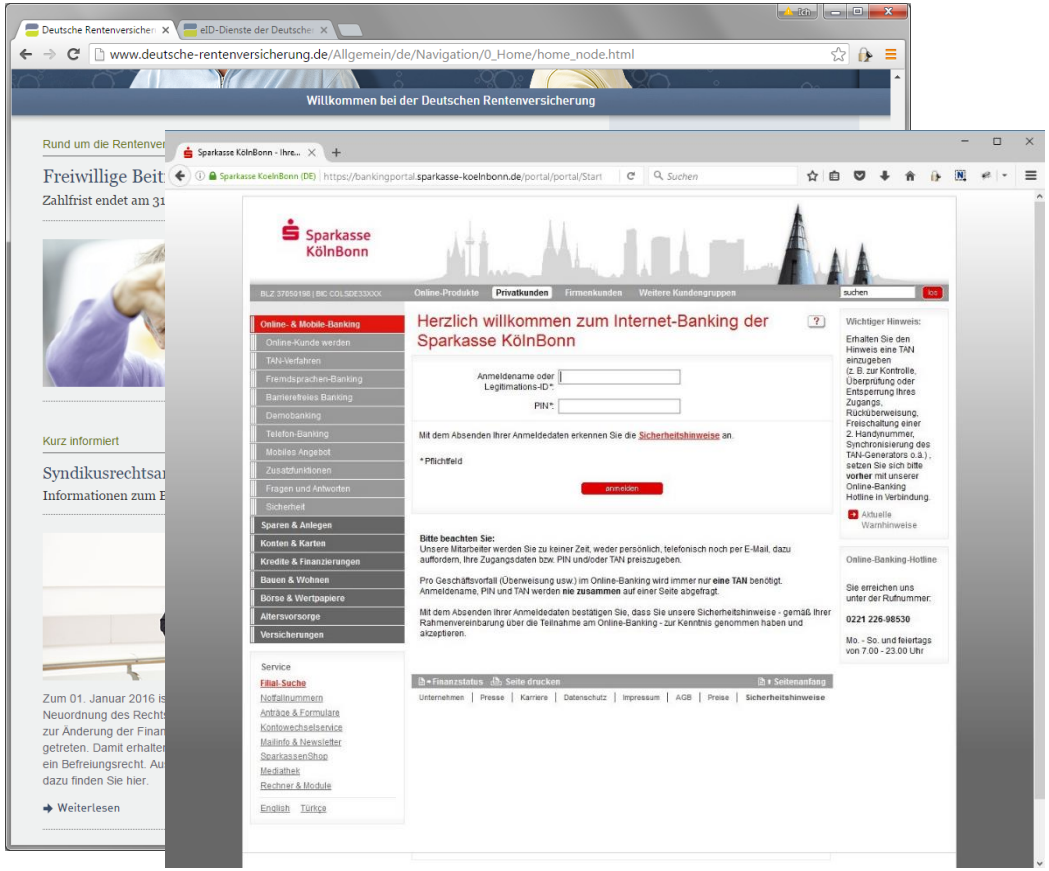

https://PrivacyCenter.netid.de/ap
Kundencenter
Start
E-Mail
Adressbuch
Kalender
Online-Speicher
WEB.DE Club
Domains
All-Net
TV-Streaming
mehr
Suche
Logout
Übersicht
Persönliche Daten
Sicherheit
Verträge
Vertrag kündigen
Vertrag widerrufen
Meine Zahlungsdaten
Meine Rechnungen
Meine Dokumente
netID Dienste
netID Einwilligungen
Kommunikationsprofil
Konto löschen
Hilfe & Kontakt
Impressum
Jobs
netID Dienste › Zalando Shop
Freigegebene Daten
Zalando Shop, Zalando SE
Letzte Änderung am 01.01.2017
Folgende Basisdaten hat Zalando von Ihnen erhalten:
E-Mail-Adresse
Für den Zwecke der personalisierten Ansprache und der Marktforschung wurden folgende Daten an Zalando übermittelt:
Anrede aufheben
Name aufheben
Anschrift aufheben
Geburtsdatum aufheben
Speichern
Abbrechen
Datenschutzbestimmungen von Zalando
Wie funktioniert die Datenfreigabe?
Sind meine Daten und Passwörter sicher?
Verknüpfung löschen
Damit wird die Anwendung von Deinem Konto und von der Liste der genutzten Anwendungen gelöscht.
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.
Ja, ich möchte die Verknüpfung löschen.
Zurück zu netID Dienste

SSO-NUTZER: UNZUREICHENDES IDENTITÄTSLEVEL

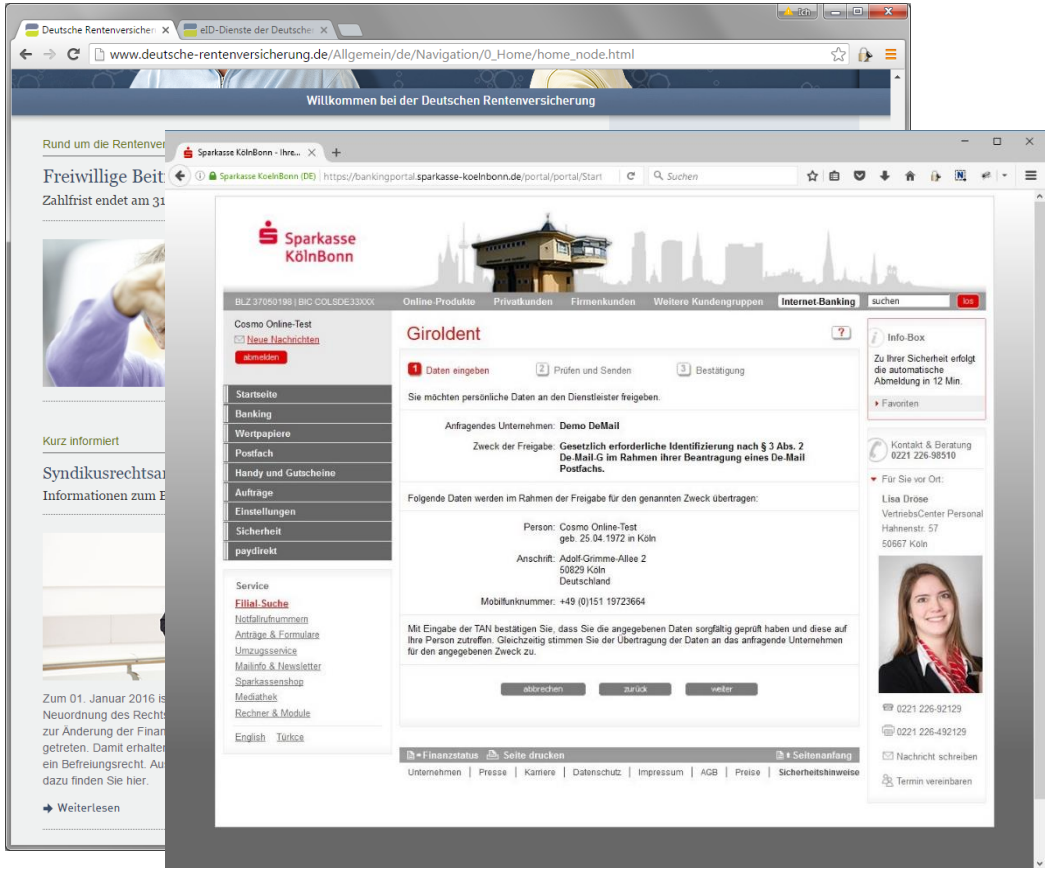
Praxisbeispiel



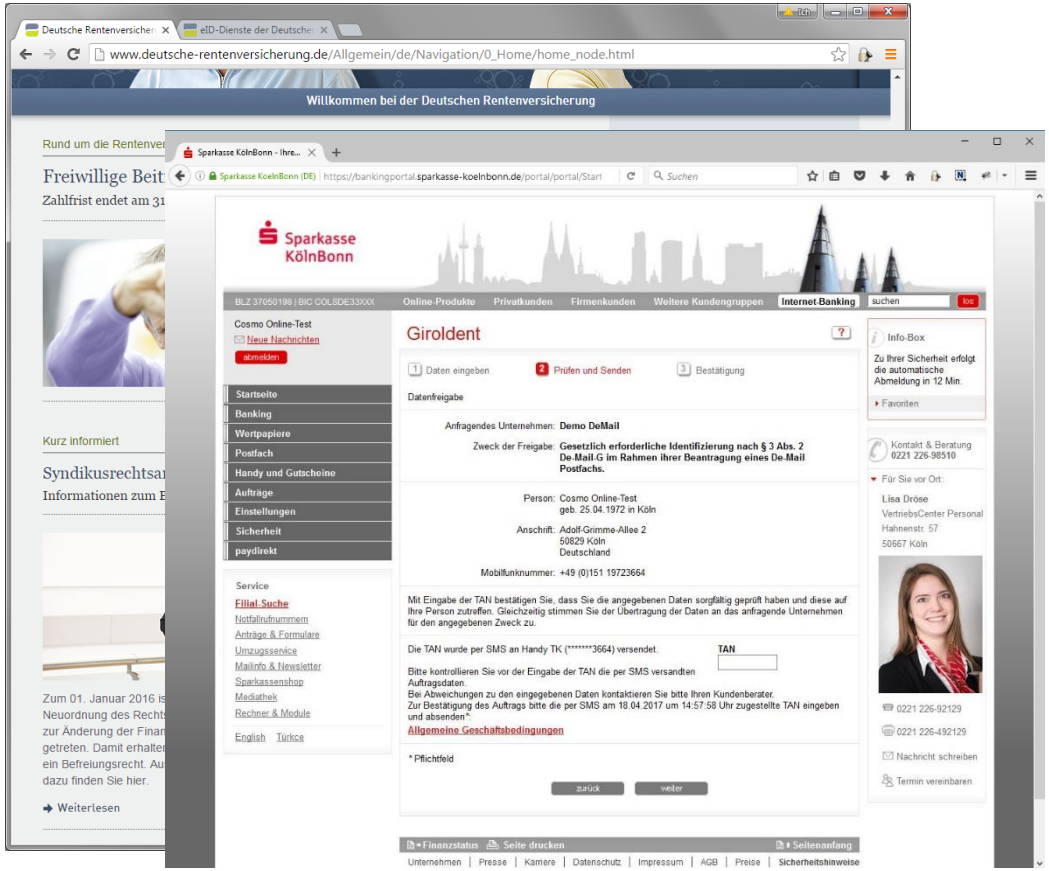
Praxisbeispiel



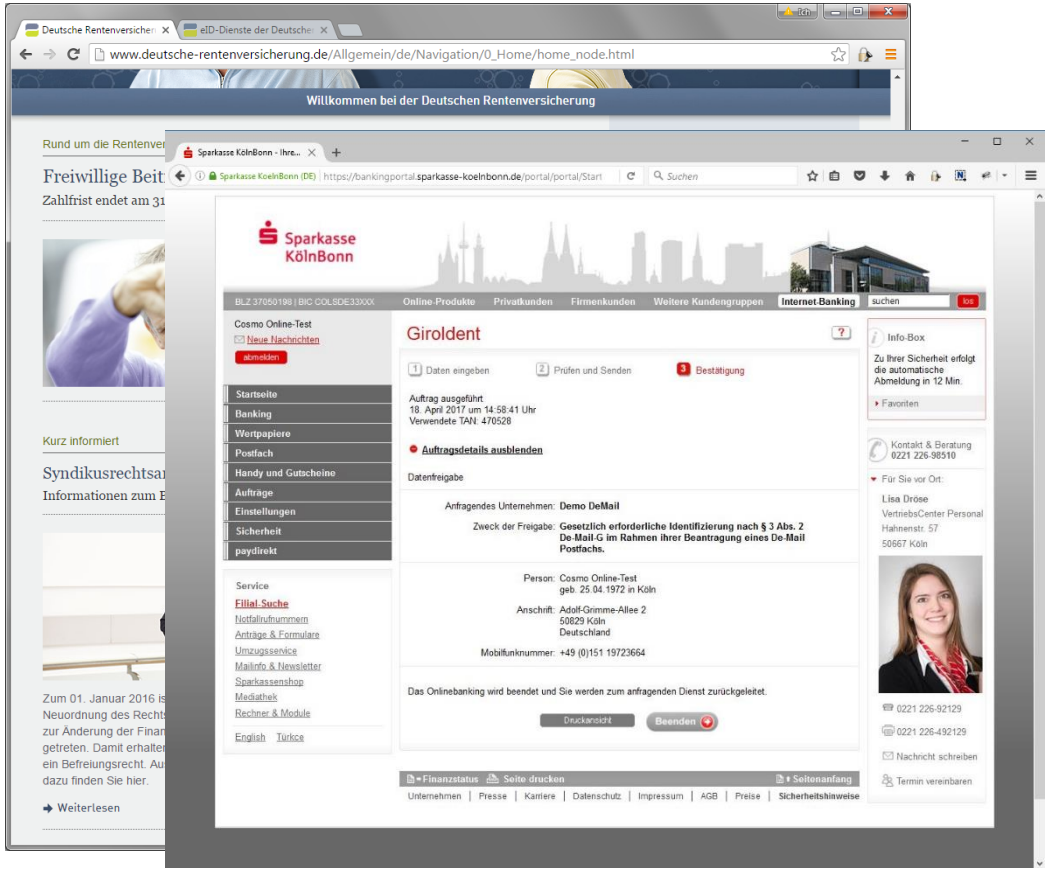
Praxisbeispiel



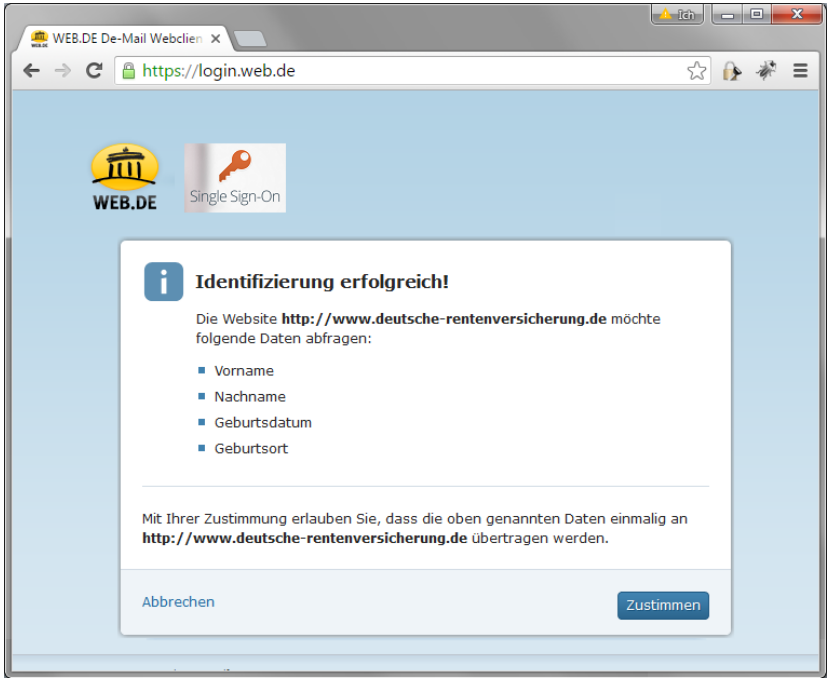
Praxisbeispiel



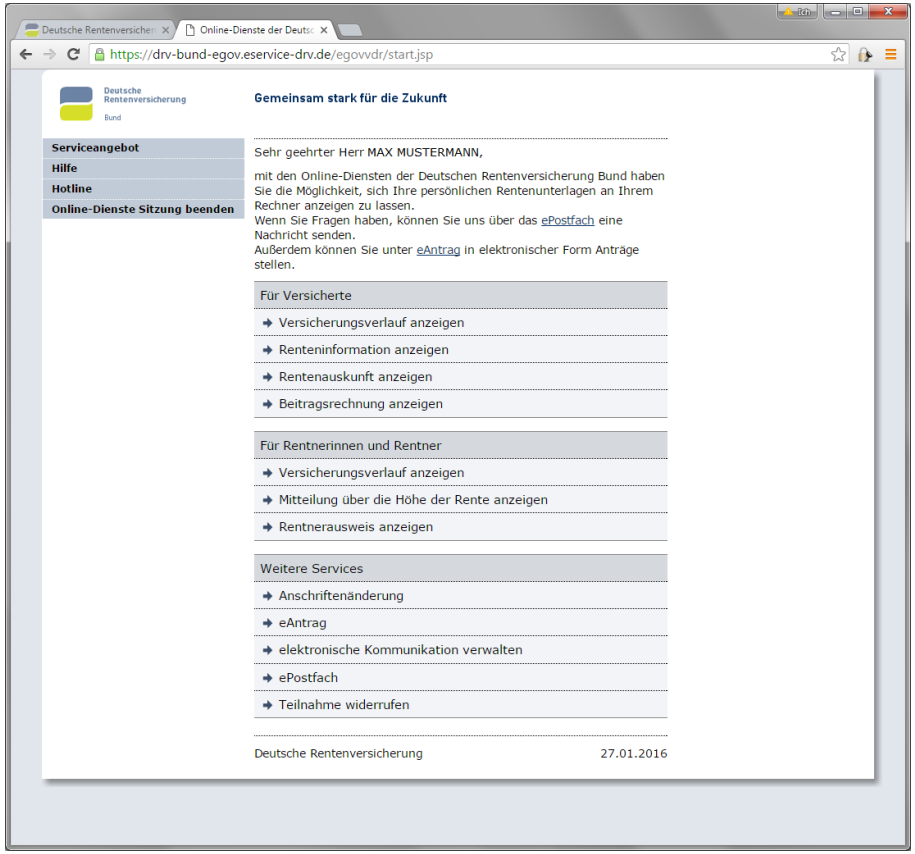
Praxisbeispiel



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	Inter-operabilität	Kryptografie	Integrität	IT-Sicherheit	Datenschutz
national	BSI TR-3107-1 DIN ISO/IEC 27001 Nativ (A9, A11) /IT-Grundschutz	BSI TR-3107-1 DIN ISO/IEC Nativ/IT-Grundschutz (A9.2)	BSI TR-01201 Teil 1.4 DIN ISO/IEC Nativ/IT-Grundschutz (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 Vorschriften: 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-Grundschutz (B1.5) De-Mail Prüfkriterienkatalog Vorschriften: 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 Vorschriften: eIDAS-VO	ETSI EN 319 401 ETSI GS ISI 001 Part 1	ETSI EN 319 401 CWA 16113 Vorschriften: 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	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	-/-

Nachweis Sicherheit / Prozess

Nachweis Sicherheit IT