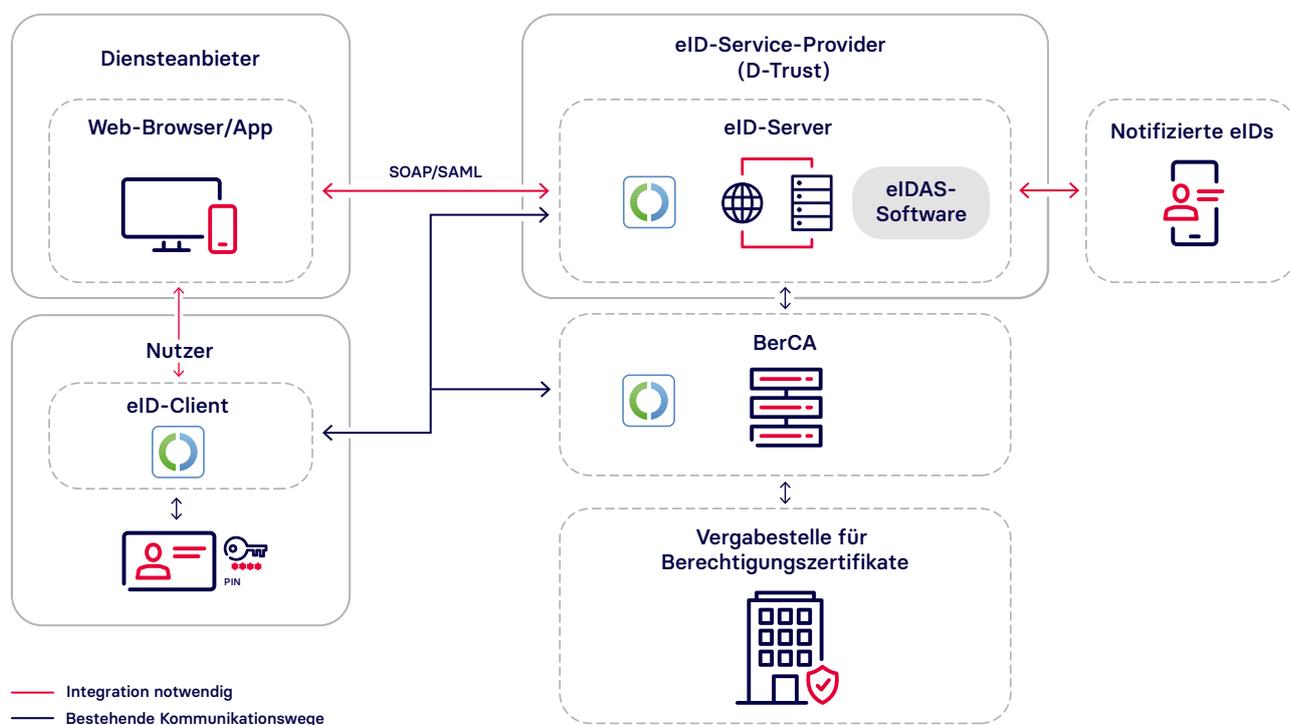


FACTSHEET

Integration des D-Trust eID-Service

Technische Einordnung des D-Trust eID-Service:
Einbindung des Online-Ausweises in Ihre Anwendung
als Diensteanbieter



Die eID-Infrastruktur

Unter eID-Infrastruktur wird die für die Online-Ausweisfunktion notwendige Architektur zwischen Ausweisinhaber und Diensteanbieter verstanden. Diese Architektur besteht aus folgenden Komponenten:

Nutzerumgebung

Der Nutzer benötigt ein digitales Endgerät (PC, Tablet, Smartphone etc.) sowie einen installierten eID-Client auf einem Smartphone oder einen USB-Kartenleser.

eID-Client

Der eID-Client ist die Schnittstelle zwischen der Ausweiskarte, dem Diensteanbieter sowie dem Nutzer. Der am häufigsten genutzte eID-Client ist die AusweisApp (AA), die kostenlos vom Bund zur Verfügung gestellt wird. Die AA kann über das angebotene Software Development Kit (SDK) in die eigene Anwendung integriert werden und ist für iOS sowie Android verfügbar. Die Entwicklerdokumentation steht auf der Website der AA zur Verfügung. Auf der Website ist ebenfalls eine Übersicht über geeignete Smartphones und Kartenlesegeräte zu finden.

Ein alternativer eID-Client ist beispielsweise Open eCard.

eID-Server

Mit dem nach TR-03130 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zertifizierten eID-Service der D-Trust können Diensteanbieter nicht nur im Internet ihre Kunden identifizieren, sondern auch am Point of Service (POS) Ausweisdaten elektronisch auslesen oder als Ident-Dienstleister für Dritte auftreten.

Über einen sicheren Kanal kommuniziert der eID-Server mit dem eID-Client. Dabei überprüft der eID-Server nicht nur die Identität des Ausweisinhabers, sondern zudem Echtheit und Sperrstatus des Ausweisdokuments. Die bei der Authentifizierung ausgelesenen Ausweisdaten werden entsprechend der Vorgaben technischer Richtlinien und Gesetze verschlüsselt und signiert bereitgestellt.

Der eID-Service kann über eine SOAP- oder eine SAML-Schnittstelle bereitgestellt werden. Die Anbindung an den eID-Service erfolgt in drei Schritten:

1. Berechtigung bei der Vergabestelle für Berechtigungszertifikate (VfB) des Bundesverwaltungsamts beantragen
2. Berechtigungszertifikat und eID-Service-Anbindung bei der D-Trust erwerben
3. Implementierung mittels SAML oder SOAP in die Anwendung des Diensteanbieters

Unser Support-Team steht bei Fragen per E-Mail sowie Telefon zur Verfügung. Zudem findet sich auf der D-Trust Webseite und im Service-Portal eine FAQ-Rubrik.

Da der eID-Service ein zertifiziertes Produkt ist, ist die Software relativ statisch und es sind nur selten Software-updates notwendig. Die geplanten Wartungsfenster für den D-Trust eID-Service sind dienstags von 6:30 bis 8:00 Uhr sowie donnerstags von 18:00 bis 22:00 Uhr.

BerCA

Für die Anbindung an den eID-Service ist ein gültiges Berechtigungszertifikat des Diensteanbieters notwendig. Im Berechtigungszertifikat wird festgelegt, welche Daten der Diensteanbieter aus dem Ausweis auslesen darf.

Berechtigungszertifikate werden bei der Vergabestelle für Berechtigungszertifikate (VfB) des Bundesverwaltungsamtes beantragt. Mit dem VfB-Bescheid kann dann das technische Berechtigungszertifikat bei der D-Trust BerCA erworben werden.

eIDAS-Software

Über die eIDAS-Software auf dem eID-Server wird die Identifizierung mit notifizierten eID-Mitteln anderer EU-Mitgliedstaaten ermöglicht. Eine Übersicht sämtlicher notifizierter eID-Mittel ist auf der Website der Europäischen Kommission abrufbar. Dort lassen sich ebenfalls die länderspezifischen „Terms of Access“ nachlesen, die insbesondere für Dienste aus der Privatwirtschaft zu beachten sind.

Wissenswerte Fakten & Links

D-Trust eID-Service & BerCA

Testsystem	<ul style="list-style-type: none">▪ Kostengünstige Referenzumgebung▪ Kostengünstige Test-Berechtigungszertifikate
-------------------	--

Voraussetzungen zum Testen	<ul style="list-style-type: none">▪ Ausweissimulator PersoSim oder Testausweise des BSI
-----------------------------------	---

Integrationskomponenten (SDKs, Beispiel-Code)	SDK der eingesetzten eID-Service-Software des Herstellers Governikus
--	--

Handbücher	<ul style="list-style-type: none">▪ D-Trust eID-Service-Integrationshandbuch▪ im Service-Portal nach Erhalt der Login-Daten
-------------------	--

SAML-Integration	<ul style="list-style-type: none">▪ Profile und Messages in Teil 1 der BSI – Technische Richtlinie BSI TR-03130 (bund.de)▪ Allgemeine Informationen: docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
-------------------------	---

SOAP-Integration	<ul style="list-style-type: none">▪ WSDL-Schemadateien als Download: BSI – Technische Richtlinie BSI TR-03130 (bund.de)▪ Allgemeine Informationen: Simple Object Access Protocol (SOAP) 1.1 (w3.org)
-------------------------	---

Support und FAQs	<ul style="list-style-type: none">▪ Im Service-Portal nach Erhalt der Login-Daten
-------------------------	---

eID-Client

AusweisApp SDK	Entwicklerdokumentation steht auf der Website der AA zur Verfügung (AusweisApp: Software Development Kit [SDK] [bund.de])
-----------------------	---

AusweisApp Kartenleser	<ul style="list-style-type: none">▪ Smartphones und Tablets▪ USB-Kartenleser
-------------------------------	---

Open eCard App	Open eCard
-----------------------	----------------------------

eIDAS

Notifizierte eID-Mittel	<ul style="list-style-type: none">▪ Overview of pre-notified and notified eID schemes under eIDAS – eID User Community – (europa.eu)▪ Terms of access to notified eID schemes for non-public sector – Identification of relying parties
--------------------------------	--