

Anschluss an die BundID

Erfahrungen und Fallstricke

Links & Support

HIS-Dokumentation: Integration Nutzerkonto Bund-HISinOne

https://wiki.his.de/mediawiki/index.php/Integration_Nutzerkonto_Bund-HISinOne

BundID-Zugriffspunkte

Integrationsumgebung: <https://int.id.bund.de/>

Produktionsumgebung: <https://id.bund.de/>

ITZ-Bund

<https://www.itzbund.de/>

SSP-BundID

<https://ssp.id.bund.de/>

<https://ssp.id.bund.de/ip?id=downloads> (Leitfaden zur Anbindung & sonstige Hinweise)

BMDS (Zuständigkeit BundID - ehemals BMI)

<https://www.digitale-verwaltung.de/Webs/DV/DE/digitale-identitaeten/bundid/bundid-node.html>

Supportkanäle

SSP-Kontaktformular unter: <https://ssp.id.bund.de/> → Service → Serviceanfrage

Alternativ (eher ungewünscht, manchmal aber gut zu haben) → bundID@bmi.bund.de

Integration BundID in HISinOne

1. Zertifikate und Schlüsselpaar erstellen bzw. importieren
2. Identity Provider erstellen und konfigurieren
3. Globale Konfiguration vorbereiten
4. Metadaten zu BundID hochladen

1. Zertifikate und Schlüsselpaar

Funktion (Admin) --> Zertifikatsspeicher verwalten

1. Zertifikatsspeicher anlegen
2. Schlüsselpaar erzeugen
 - Schlüsselalgorithmus RSA
 - Daten ergänzen
3. BundID Zertifikat anhängen
 - Umspeichern notwendig!

Sie sind hier: Startseite > Administration > System-Administration > Zertifikatsspeicher verwalten

Zertifikatsspeicher




[+ Zertifikatsspeicher erstellen](#) [Zertifikatsspeicherdatei \(keystoreMerge.dat\) aktualisieren](#)

Name	Technischer Bezeichner
Datei: keystoreMerge.dat	keystoreMerge.dat
BundID Schlüsselpaar	bundKey

Zertifikatsspeicher

UOS

[+ Konfiguration hinzufügen](#) [Konfiguration entfernen](#) [Tabelle anpassen](#)

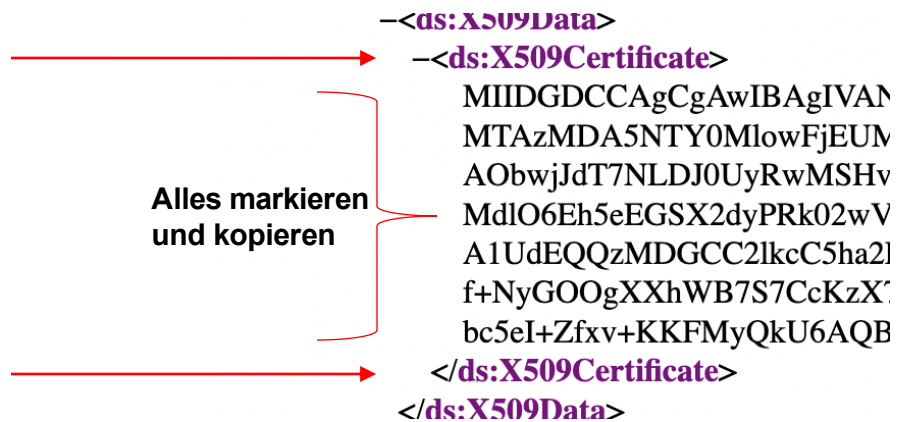
Eintrag	Verwenden von	Verwenden bis	Aktionen
BundID Schlüsselpaar			   
<ul style="list-style-type: none">  bundKeyRSA bundkeysa ← Schlüsselpaar Hochschule  bundKeyRSA 	01.04.2025	31.12.2100	   
<ul style="list-style-type: none">  idp.akdb.de idp.akdb.de ← Zertifikat ITZ-Bund  entry 	31.10.2012	29.10.2032	   

Achtung: Kleine Hürde

Folgende Schritte sind notwendig:

Abruf der benötigten Metadaten von <https://int.id.bund.de/idp> (Testserver)
bzw. <https://id.bund.de/idp> (Produktiv).

Zertifikatsschlüssel zwischen den `<ds:X509Certificate>` Tags suchen und kopieren.



```

-<ds:X509Data>
  -<ds:X509Certificate>
    MIIDGDCCAgCgAwIBAgIVAN
    MTAzMDA5NTY0MlowFjEUM
    AObwjJdT7NLDJ0UyRwMSHv
    MdlO6Eh5eEGSX2dyPRk02wV
    A1UdEQQzMDGCC2lkcC5ha2l
    f+NyGOOgXXhWB7S7CcKzX'
    bc5eI+Zfxv+KKFMyQkU6AQB
  </ds:X509Certificate>
</ds:X509Data>

```


Achtung: Kleine Hürde

Folgende Schritte sind notwendig:

Zertifikatsschlüssel incl. Header in Notepad oder beliebigen Editor in ein neues Dokument einfügen.



















Speichern mit Dateiendung *.crt

1. Zertifikate und Schlüsselpaar

Zertifikatsspeicher

UOS

Konfiguration hinzufügen Konfiguration entfernen Tabelle anpassen

Eintrag	Verwenden von	Verwenden bis	Aktionen
BundID Schlüsselpaar			     
<ul style="list-style-type: none"> bundKeyRSA ← Schlüsselpaar Hochschule bundkeysa bundKeyRSA 	01.04.2025	31.12.2100	     
<ul style="list-style-type: none"> idp.akdb.de ← Zertifikat ITZ-Bund idp.akdb_de entry 	31.10.2012	29.10.2032	     

Funktion (Admin) --> Zertifikatsspeicher verwalten

1. Zertifikatsspeicher anlegen
2. Schlüsselpaar erzeugen
 - Schlüsselalgorithmus RSA
 - Daten ergänzen
3. **BundID Zertifikat anhängen**
 - Grün markiertes Symbol im Zertifikatsspeicher
 - Erstellte *.crt Zertifikatsdatei auswählen und hinzufügen

Zertifikat importieren - X

Schritt 1: Zertifikatsdatei auswählen

* Format Zertifikatsdatei

* Zertifikatsdatei Auswählen (hier klicken oder Datei hineinziehen, nur PDF-Format)

Abbrechen
▶ Weiter

2. Identity Provider erstellen und konfigurieren

Funktion (Admin) → Identity Provider konfigurieren

1. Neue Konfiguration anlegen
2. Daten eingeben und gewünschte Services anhaken
3. Speichern → Konfiguration (Tab)
4. Daten eingeben
 - Protokolltyp SAML
5. Parameter konfigurieren

Sie sind hier: [Startseite](#) > [Administration](#) > [System-Administration](#) > [Service-Administration](#) > [Identity Provider konfigurieren](#)
 Identity Provider konfigurieren

Übersicht der Identity Provider Konfigurationen

Ein Identity Provider ist ein Anbieter, der Identitäten verwaltet und für Service Provider bereitstellt. Vor der Verwendung muss ein Identity Provider hier konfiguriert werden.

[+ Neue Konfiguration anlegen](#)

Grunddaten Konfiguration

Grunddaten

Die Grunddaten definieren neben Name, Standardtext und Beschreibung auch die Gültigkeit der Konfiguration.

* Name

* Standardtext

* Beschreibung

* Gültig von

* Gültig bis

Services:

- Login
- Selbstregistrierung
- Account-Verknüpfung
- Rückkanal
- Identitätsprüfung
- Manuelle Identitätsprüfung

2. Identity Provider erstellen und konfigurieren

Funktion (Admin) → Identity Provider konfigurieren

1. Neue Konfiguration anlegen
2. Daten eingeben und gewünschte Services anhaken
3. Speichern → Konfiguration (Tab)
4. Daten eingeben
 - Protokolltyp SAML
5. Parameter konfigurieren

Grunddaten **Konfiguration**

Konfiguration

[+ Neue Konfiguration hinzufügen](#) [📄 Konfiguration kopieren](#)
[📄 Download der Meta-Datei](#)

Für diesen Provider gibt es Konfigurationen in folgenden Konfigurationsquellen:

* Konfigurationsquelle

* Protokolltyp

Personenidentifikator

Privater Schlüssel Service Provider

Entity Id Service Provider

Login-URL Beispiel für Testserver BundID

Logout-URL

Zertifikat des IDP Benennung evtl. anders. Gemeint ist BundID Zertifikat.

Nachrichten-Template für Rückkanal An dieser Stelle noch unwichtig

[+ Neuen Parameter anlegen](#)

Aktionen	Name	Wert	Typ	Service	Merkmal der Identitätsprüfung	Aktionen
	givenName	urrcoid:2.5.4.42	mapping			
	surname	urrcoid:2.5.4.4	mapping			
	title	urrcoid:0.9.2342.19200300.100.1.40	mapping			
	gender	urrcoid:1.3.6.1.4.1.33592.1.3.5	mapping			
	birthdate	urrcoid:1.2.40.0.10.2.1.1.55	mapping			
	placeOfBirth	urrcoid:1.3.6.1.5.5.7.9.2	mapping			
	birthName	urrcoid:1.2.40.0.10.2.1.1.225566	mapping			
	nationality	urrcoid:1.2.40.0.10.2.1.1.225577	mapping			
	street	urrcoid:2.5.4.16	mapping			
	postcode	urrcoid:2.5.4.17	mapping			
	city	urrcoid:2.5.4.7	mapping			
	country	urrcoid:1.2.40.0.10.2.1.1.225599	mapping			

2. Identity Provider erstellen und konfigurieren

Funktion (Admin) → Identity Provider konfigurieren

1. Neue Konfiguration anlegen
2. Daten eingeben und gewünschte Services anhaken
3. Speichern → Konfiguration (Tab)
4. Daten eingeben
 - Protokolltyp SAML
- 5. Parameter konfigurieren**

Name	Wert	Typ	Beschreibung
givenName	urn:oid:2.5.4.42	mapping	Vorname
surname	urn:oid:2.5.4.4	mapping	Nachname
email	urn:oid:0.9.2342.19200300.100.1.3	mapping	E-Mail-Adresse
street	urn:oid:2.5.4.16	mapping	Straße der Adresse
postcode	urn:oid:2.5.4.17	mapping	Postleitzahl der Adresse
city	urn:oid:2.5.4.7	mapping	Ort der Adresse
country	urn:oid:1.2.40.0.10.2.1.1.225599	mapping	Land der Adresse
title	urn:oid:0.9.2342.19200300.100.1.40	mapping	Titel
gender	urn:oid:1.3.6.1.4.1.33592.1.3.5	mapping	Geschlecht
birthdate	urn:oid:1.2.40.0.10.2.1.1.55	mapping	Geburtsdatum
placeOfBirth	urn:oid:1.3.6.1.5.5.7.9.2	mapping	Geburtsort
birthName	urn:oid:1.2.40.0.10.2.1.1.225566	mapping	Geburtsname
nationality	urn:oid:1.2.40.0.10.2.1.1.225577	mapping	Staatsangehörigkeit
phone	urn:oid:2.5.4.20	mapping	Telefonnummer
extident	urn:oid:1.3.6.1.4.1.25484.494450.3	mapping	bpk2 (Identifizier)
postkorb-handle	urn:oid:2.5.4.18	mapping	Postkorb-Handle (Identifizier für den Postkorb)
postkorb-handle-typ	Nutzerkonto Bund Postkorb	mapping	Zuordnung des Personenidentifikators für die Speicherung des Identifizier für den Postkorb BundID
storklvl	urn:oid:1.2.40.0.10.2.1.1.261.94	mapping	Vertrauensniveau des Authentifizierungsvorgangs

Achtung: Seit August 2024 zusätzlich SAML-Extensions erforderlich!

Werden wie die anderen Parameter zum IDP (Identity Provider) hinzugefügt

Werte können unter https://wiki.his.de/mediawiki/index.php/Integration_Nutzerkonto_Bund-HISinOne#Authentifizierungsmethoden_festlegen abgerufen werden.

Anwendungsfall Account-Verknüpfung:

Typ: SAML-Extension
 Name: Verknüpfung
 Wert: siehe Wert für Account-Verknüpfung
 Service: Account-Verknüpfung

Anwendungsfall Login:

Typ: SAML-Extension
 Name: Login
 Wert: siehe Wert für Login
 Service: Login

Anwendungsfall Selbstregistrierung:

Typ: SAML-Extension
 Name: Selbstregistrierung
 Wert: siehe Wert für Selbstregistrierung
 Service: Selbstregistrierung

3.9.1 Wert für Account-Verknüpfung [\[edit \]](#) [\[edit source \]](#)

Folgende Attribute werden als erforderliche Angaben deklariert:

- der Identifier bpk2 (<urn:oid:1.3.6.1.4.1.25484.494450.3>)
- das Postkorb Handle (<urn:oid:2.5.4.18>)
- das STORK Level (<urn:oid:1.2.40.0.10.2.1.1.261.94>)

```
<akdb:AuthenticationRequest xmlns:akdb="https://www.akdb.de/request/2018/09" Version="2">
  <akdb:AuthnMethods>
    <akdb:Benutzername>
      <akdb:Enabled>true</akdb:Enabled>
    </akdb:Benutzername>
    <akdb:eID>
      <akdb:Enabled>true</akdb:Enabled>
    </akdb:eID>
    <akdb:eIDAS>
      <akdb:Enabled>true</akdb:Enabled>
    </akdb:eIDAS>
    <akdb:Diia>
      <akdb:Enabled>true</akdb:Enabled>
    </akdb:Diia>
    <akdb:Elster>
      <akdb:Enabled>true</akdb:Enabled>
    </akdb:Elster>
    <akdb:FINK>
      < akdb:Enabled>true</akdb:Enabled>
    </akdb:FINK>
  </akdb:AuthnMethods>
  <akdb:RequestedAttributes>
    <akdb:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.25484.494450.3" RequiredAttribute="true" />
    <akdb:RequestedAttribute Name="urn:oid:2.5.4.18" RequiredAttribute="true" />
    <akdb:RequestedAttribute Name="urn:oid:1.2.40.0.10.2.1.1.261.94" RequiredAttribute="true" />
  </akdb:RequestedAttributes>
</akdb:AuthenticationRequest>
```

Beispiel Werte für Account-Verknüpfung.
 Gesamten Inhalt des Codeblocks kopieren und als Wert
 in der entsprechenden Parameterkonfiguration einfügen

3. Globale Konfiguration vorbereiten

Funktion (Admin) → Globale Konfiguration bearbeiten

core.sys.domain.current_trusted_domain

-> prüfen und ggf. anpassen

core.psv.selfregistration.availableidentityproviders

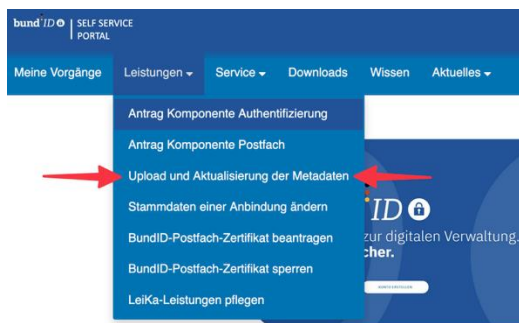
-> Identity Provider auswählen und in Konfigurationsquelle aktiv schalten

4. Metadaten im SSP ID-Bund hochladen

Im Browser auf SSP ID-Bund navigieren

<https://ssp.id.bund.de/>

1. Login (oder Registrierung)
2. Leistungen → Upload und Aktualisierung der Metadaten
3. Daten in Maske einpflegen (siehe rechts)
4. Hochschulzertifikat aus dem Zertifikatsspeicher kopieren und X.509 Zertifikat einfügen (primär signing und encryption)
5. Absenden und bis kommenden Dienstag warten



Upload und Aktualisierung der Metadaten

Auf dieser Seite können Sie Ihre Metadaten hochladen oder aktualisieren.

Sollten Sie Fragen zur Eingabe der Metadaten haben, besuchen Sie bitte zunächst unseren [Download-Bereich](#). Unter "Technische Informationen/SAML Authentifikation" finden Sie hilfreiche Dokumente. Wenn Sie sich nach der Lektüre weiterhin mit Fragen konfrontiert sehen, wenden Sie sich bitte über eine [Serviceanfrage](#) an uns.

*** Erforderlich**

*** Ich möchte Metadaten...**

*** BMI ID**

*** EntityID**

*** Umgebung**

*** Welches Signierverfahren (SigningMethod) nutzen Sie?**

*** Welches Verschlüsselungsverfahren (EncryptionMethod) nutzen Sie?**

*** Primäres X.509 Zertifikat (signing) Base64 codiert**

Sekundäres X.509 Zertifikat (signing) Base64 codiert

*** X.509 Zertifikat (encryption) Base64 codiert**

*** Attribute Consume Service Endpoint (HTTP-POST)**

Aktionen	URL
UNI URL einfügen z.B. https://cms.system.hochschule-testland.de/	Keine anzuzeigenden Daten.

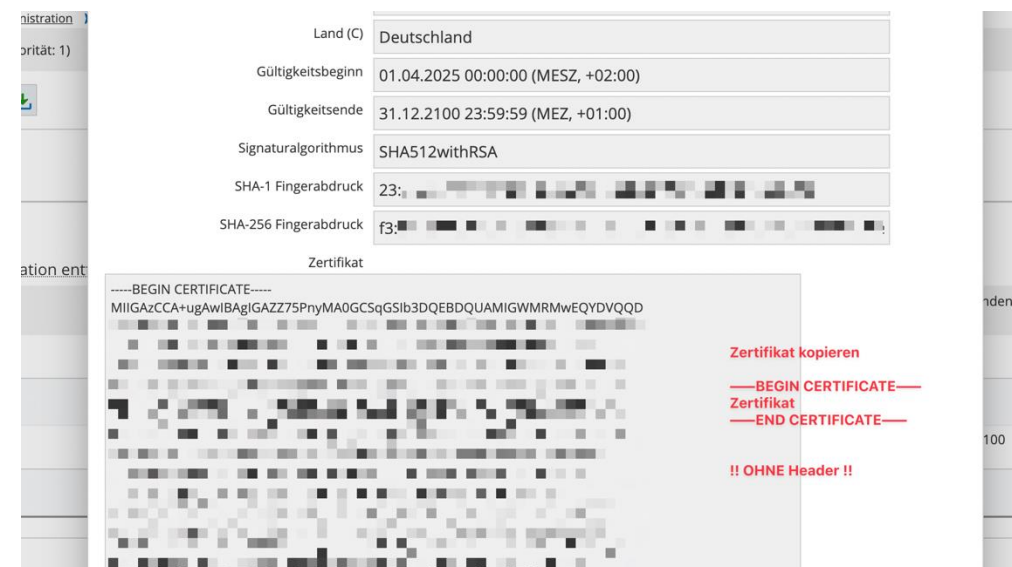
Wenn fertig, absenden.
Upload jeden Dienstag ggn. Nachmittag

4. Metadaten im SSP ID-Bund hochladen

Im Browser auf SSP ID-Bund navigieren

<https://ssp.id.bund.de/>

1. Login (oder Registrierung)
2. Leistungen → Upload und Aktualisierung der Metadaten
3. Daten in Maske einpflegen (siehe rechts)
4. **Hochschulzertifikat aus dem Zertifikatsspeicher kopieren und X.509 Zertifikat einfügen** (primär signing und encryption)
5. Absenden und bis kommenden Dienstag warten



*Primäres X.509 Zertifikat (signing) Base64 codiert ⓘ

Hier das kopierte Zertifikat aus dem Schlüsselpaar einfügen

Sekundäres X.509 Zertifikat (signing) Base64 codiert ⓘ

*X.509 Zertifikat (encryption) Base64 codiert ⓘ

Hier das kopierte Zertifikat aus dem Schlüsselpaar einfügen

Wie kann ich die Anbindung testen?

Erste Tests über Selbstregistrierung

→ Benutzername & Passwort für generelle Anbindung und niedriges Vertrauensniveau

→ Testausweis vom BMI beziehen für hohes Vertrauensniveau

→ Simulierter Testausweis in AusweisApp (Entwicklermodus notwendig)

→ PersoSim nutzen, um verschiedene Testausweise zu simulieren

→ Siehe https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Online-Ausweisfunktion/Testinfrastruktur/PersoSim/PersoSim_node.html

Exkurs Vertrauensniveaus

Als Grundlage zur Beurteilung der Vertrauensniveaus dienen die Vorgaben der europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste. Mehr Informationen finden Sie unter: [eIDAS-VO](#)

In der BundID können folgende (nicht-) Vertrauensniveaus bzw. zugehörige Authentifizierungsmittel genutzt:

- „Basisregistrierung“

Dieses Vertrauensniveau erreichen Sie mit der Benutzung der Zugangsart „Benutzername & Passwort“. Diese Zugangsart entspricht nicht den Vorgaben der eIDAS-VO, wird jedoch trotzdem aus Gründen der Benutzerfreundlichkeit in der BundID angeboten, zum Beispiel, um das eigene Konto zu verwalten oder einen Nachrichteneingang zu prüfen. Hierbei ist zu beachten, dass ausschließlich Nachrichten auf dem Vertrauensniveau „Basisregistrierung“ mit der Zugangsart „Benutzername & Passwort“ eingesehen werden können.

- Vertrauensniveau „substanziell“

Dieses Vertrauensniveau erreichen Sie mit der Benutzung der Zugangsart „ELSTER-Zertifikat“ und einzelnen „EU Identitäten“.

- Vertrauensniveau „hoch“

Dieses Vertrauensniveau erreichen Sie mit der Benutzung der Zugangsart „Online-Ausweis“ sowie einzelnen „EU Identitäten“. Unter die Kategorie „Online-Ausweis“ fallen der Personalausweis mit Onlinefunktion, die Smart-eID, der elektronische Aufenthaltstitel und die Unionsbürgerkarte.

Hinweis: Vertrauensniveau „hoch“ ggf. nicht in allen EU-Mitgliedsstaaten verfügbar.

Vielen Dank