



Bundesministerium
des Innern
und für Heimat



Umstellung der Verschlüsselungs- und Signiervverfahren

Information und Anleitung

26. November 2024



Überblick über das Dokument

Name des Dokuments	BundID_Umstellung auf neue Verfahren Information und Anleitung
Dokument-Version	1.0
Herausgebende Stelle	Bundesministerium des Innern und für Heimat DVI5
Stand	26.11.2024

Nachdruck, auch auszugsweise, ist genehmigungspflichtig.

Versionshistorie

Version	Beschreibung	Datum
1.0	Erstmalige Erstellung	26.11.2024

Inhaltsverzeichnis

Versionshistorie	3
1 Information zur Umstellung auf neue Verfahren im IDP der BundID	5
2 Anleitung zur Anpassung im BundID SSP	7
3 Hinweis zur Nutzung von Keycloak	10

1 Information zur Umstellung auf neue Verfahren im IDP der BundID

Aufgrund der Vorgaben des BSI in der TR 03116-4 sind folgende zwei **Änderungen in der SAML-Kommunikation mit dem IDP der BundID** zwingend erforderlich:

1. Das **Verschlüsselungsverfahren** (EncryptionMethod) wird von "aes128-cbc" auf "**aes128-gcm**" (AES-GCM Mode) umgestellt.
2. Das **Signierverfahren** (SigningMethod) wird von "rsa-sha256" auf "**sha256-rsa-mgf1**" (RSASSA-PSS) umgestellt.

Abweichung	Verwendung maximal bis	Empfehlung
Signatur		
RSASSA-PKCS1-v1_5	2023	Migration auf RSASSA-PSS bzw. ECDSA
Content Encryption		
AES CBC-Mode	2020	Migration auf AES GCM-Mode

Tabelle 17: Übergangsregelungen für XML Security

Quelle: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/>

TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=5, Seite 17

Der BundID IDP unterstützt die neuen Verfahren bereits. Entsprechend empfehlen wir die schnellstmögliche Umstellung Ihrer Anbindung, da zu den bisher genutzten Verfahren ein bekannter Angriffsvektor existiert, sodass eine Kompromittierung möglich ist.

Zusätzlich empfehlen wir folgendes Vorgehen:

1. Die Anpassung in Ihrer Anbindung vorab mit Hilfe der Integrationsumgebung der BundID zu testen, bevor die produktive Umstellung Ihrerseits stattfindet.
Hinweis: Im BundID Self Service Portal (BundID SSP) können Sie die Metadaten Ihrer Anbindung für die BundID Integrationsumgebung gesondert von der BundID Produktionsumgebung ändern.

2. Die technische Unterstützung der alten Verfahren in Ihrer Anbindung aufrecht zu erhalten, bis die neuen Verfahren erfolgreich etabliert sind.

Hinweis: So kann ein reibungsloser Übergang ohne Downtime gewährleistet werden.

3. Die technische Unterstützung der alten Verfahren in Ihrer Anbindung im Anschluss zurückzubauen.

Hinweis: Dies dient der Absicherung Ihrer Anbindung gegen die potentielle Ausnutzung der Sicherheitslücken in den alten Verfahren.

Bis zum 30.06.2025 ist die Umstellung für alle Anbindungen verpflichtend. Die Unterstützung der veralteten Verfahren durch die BundID wird zu diesem Zeitpunkt deaktiviert.

Bitte stellen Sie sicher, dass Ihre Anbindung diese Änderungen in der SAML-Kommunikation unterstützt und aktualisieren Sie Ihre Metadaten im BundID SSP. Das BundID SSP erreichen Sie unter folgender URL: <https://ssp.id.bund.de/>.

Im Folgenden finden Sie eine Erläuterung zur Einstellung im BundID SSP, die ab Dezember 2024 möglich sein wird.

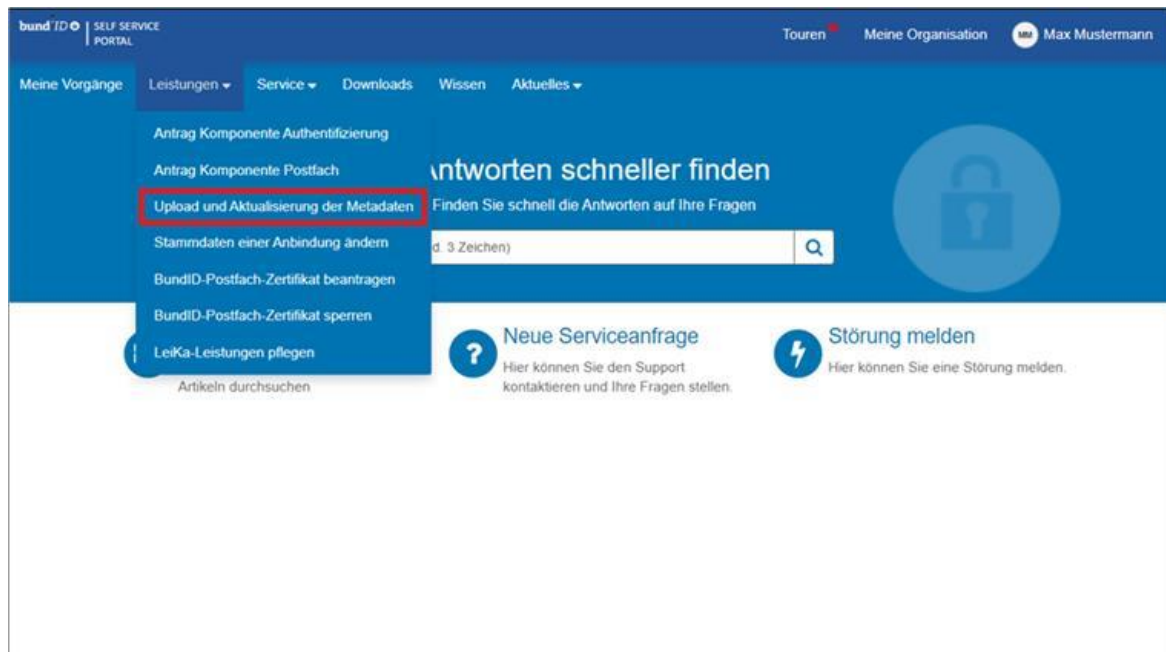
2 Anleitung zur Anpassung im BundID SSP

Nachdem durch Ihre Anbindung die technische Unterstützung der neuen Verfahren gewährleistet ist, müssen Sie im BundID SSP Ihre Metadaten anpassen.

Für das Vorgehen finden Sie unten eine Kurzanleitung mit entsprechenden Screenshots. Außerdem steht das Video „SSP_Metadaten_zu_Anbindung_pfleger.mp4“ im Downloadbereich des BundID SSP zur Verfügung: <https://ssp.id.bund.de/ip?id=downloads>.

Neben der Eingabe Ihrer anbindungsspezifischen Informationen, müssen Sie nun in den Metadaten das Signierv Verfahren sowie das Verschlüsselungsverfahren angeben. (Hinweis: Zur Eingabe von Metadaten muss Ihr Anbindungsvorhaben für die jeweilige Umgebung (Integrations- oder Produktivumgebung) bereits freigegeben sein.) Ihre eingegebenen Metadaten werden anschließend für die Anbindung an die Integrationsumgebung am nachfolgenden Dienstag und für die Anbindung an die Produktivumgebung am nachfolgenden Donnerstag auf die entsprechenden Systeme der BundID eingespielt. Nach erfolgter Einspielung erhalten Sie eine Benachrichtigung per E-Mail.

1. Melden Sie sich im BundID SSP (<https://ssp.id.bund.de/>) an und wählen Sie unter dem Menüpunkt „Leistungen“ den Punkt „Upload und Aktualisierung der Metadaten“ aus.



2. Wählen Sie „Hochladen“ bzw. „Aktualisieren“ von Metadaten aus.

Hinweis: Metadaten, die vor der Einführung vom BundID SSP (09/2024) bereits eingespielt wurden, sind nicht im BundID SSP hinterlegt. Sie müssen somit bei der erstmaligen Eingabe von Metadaten hier „Hochladen“ auswählen. Metadaten, die schon im BundID SSP erfasst wurden, können über die Auswahl „Aktualisieren“ bearbeitet werden.

The screenshot shows the 'bund ID SELF SERVICE PORTAL' interface. The user is logged in as 'Max Mustermann'. The navigation bar includes 'Meine Vorgänge', 'Leistungen', 'Service', 'Downloads', 'Wissen', and 'Aktuelles'. The breadcrumb trail is 'Startseite > Integrationsleistungen > Leistungen'. A search bar is present. The main heading is 'Upload und Aktualisierung der Metadaten'. Under the 'Erforderlich' section, the dropdown 'Ich möchte Metadaten...' is highlighted with a red box and shows 'Hochladen'. Below it are fields for 'BMI ID' and 'EntityID'.

3. Das Formular wird folgendermaßen angepasst werden. Unter der Eingabe Ihrer anbindungsspezifischen Angaben finden Sie die Dropdowns für die Angabe des Signiervfahrens und für das Verschlüsselungsverfahren.

The screenshot shows the updated 'bund ID SELF SERVICE PORTAL' interface. The user is still logged in as 'Max Mustermann'. The navigation bar and breadcrumb trail are the same. The main heading is 'Upload und Aktualisierung der Metadaten'. Under the 'Erforderlich' section, the 'Ich möchte Metadaten...' dropdown is still 'Hochladen'. Below it are fields for 'BMI ID' (set to 'Serviceportal ABC') and 'EntityID' (set to 'https://example-serviceportal-abc.de'). To the right, there is a new section 'Umgebung' with a dropdown set to 'Integration'. Below these, two dropdowns are highlighted with red boxes: 'Welches Signiervfahren (SigningMethod) nutzen Sie?' (set to 'Keine') and 'Welches Verschlüsselungsverfahren (EncryptionMethod) nutzen Sie?' (set to 'Keine'). At the bottom, there is a field for 'Primäres X.509 Zertifikat (signing) Base64 codiert'.

4. Wählen Sie unter dem Dropdown für das Signiervverfahren nun „**sha256-rsa-mgf1**“ und für das Verschlüsselungsverfahren „**aes128-gcm**“:

* Welches Signiervverfahren (SigningMethod) nutzen Sie? ⓘ

-- Keine --

http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1

* Welches Verschlüsselungsverfahren (EncryptionMethod) nutzen Sie? ⓘ

-- Keine --

http://www.w3.org/2001/04/xmlenc#aes128-cbc

http://www.w3.org/2009/xmlenc11#aes128-gcm

Standardized XML Encryption (signing) and Encryption

3 Hinweis zur Nutzung von Keycloak

Mittels manueller Tests konnte erfolgreich validiert werden, dass Keycloak mindestens seit V16.0.0 (veröffentlicht am 17.12.2021) die erforderlichen neuen Verfahren unterstützt.

