C_12872_Anlage - gID 2.0 - Maintenance sektorale IDP 2026 - Laufzeit Gerätebindung

Inhaltsverzeichnis

1 Änderungsbeschreibung....2
2 Änderung in gemSpec_IDP_Sek....3
3 Änderungen in Steckbriefen....6
3.1 Änderungen in gemProdT_IDP-Sek_PTV....6

1 Änderungsbeschreibung

Die Anforderung zur begrenzten Laufzeit der Gerätebindung wurde mit Release IDP 26.1 auf den 02.01.2026 begrenzt, mit der Aussicht in Release 26.2

- entweder die Afo zu entfernen
  - Berücksichtigen: Desktop-Anwendung (RISE) hat aktuell 24h (Software Keystore). Diese Anforderung muss bleiben.
- oder den Zeitraum der Befristung zu verlängern
- oder die Anforderung durch eine oder mehrere alternative Anforderungen zu ersetzen.

Es wurde entschieden, dass die Laufzeit der Gerätebindung für Geräte mit Hardware Key-Store 24 Monate beträgt. die Anforderung A_22750 wird entsprechend neu formuliert.

2 Änderung in gemSpec_IDP_Sek

Es wird in Kapitel "4.4.2 Authentifizierungsverfahren" geändert:

Alt:

A_22750-02 - Gerätebindung und Authentisierung für "gematik-ehealth-loa-high" und "gematik-ehealth-loa-substantial" (befristet bis 02.01.2027)

Abhängig von der Geräteausstattung des Nutzers ist eine Gerätebindung für einen festgelegten Zeitraum ohne Erneuerung gültig. Der Anbieter des sektoralen IDP MUSS, wenn er eine Gerätebindung im Rahmen eines Authentisierungsverfahren nutzt, die Zeitrahmen der Gültigkeit für die Gerätebindung gemäß Tabelle "Übersicht Gerätebindung" berücksichtigen.
Beim Zugriff auf Daten mit hohem Schutzbedarf gelten die Zeiträume der maximalen Gerätebindung`gematik-ehealth-loa-high` in der Tabelle. Nach Einwilligung des Nutzers gemäß A_23103* gelten beim Zugriff auf Daten mit hohem Schutzbedarf, unter Verwendung von Authentisierungsverfahrens `gematik-ehealth-loa-substantial` die Zeiträume der maximalen Gerätebindung`gematik-ehealth-loa-substantial` in Tabelle "Übersicht Gerätebindung".
Die Gerätebindung MUSS durch den Nutzer nach Ablauf dieser Frist dementsprechend erneuert werden.
Der Anbieter des sektoralen IDP MUSS mit den zur Verfügung stehenden Plattformmechanismen, einen kryptographischen Nachweis der Gerätebindung auf dem Endgerät erzeugen und auf Serverseite prüfen (z.B. Android: Key & ID Attestation; iOS: DCAppAttestService).
Die Gerätebindung kann:

1. durch Identifikation, welche dem Niveau `gematik-ehealth-loa-high` entspricht oder
2. mit einer 2FA, welche dem Niveau `gematik-ehealth-loa-high` entspricht,

angelegt werden.

Tabelle 1: Übersicht Gerätebindung

Schlüsselspeicher	Gültigkeit der Gerätebindung
ohne Hardware Keystore	Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden: • 24h auf dem Niveau "gematik-ehealth-loa-high" • 48h auf dem Niveau "gematik-ehealth-loa-substantial"
mit Hardware Keystore	Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden: • 6 Monate auf dem Niveau "gematik-ehealth-loa-high" • 12 Monate auf dem Niveau "gematik-ehealth-loa-substantial"
mit zertifiziertem Secure Element	Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden:

	• unbegrenzt auf dem Niveau "gematik-ehealth-loa-high" • unbegrenzt auf dem Niveau "gematik-ehealth-loa-substantial"

Neu:

A_22750-03 - Gerätebindung und Authentisierung ~~für "gematik-ehealth-loa-high" und "gematik-ehealth-loa-substantial" (befristet bis 02.01.2027)~~

Abhängig von der Geräteausstattung des Nutzers ist eine Gerätebindung für einen festgelegten Zeitraum ohne Erneuerung gültig. Der Anbieter des sektoralen IDP MUSS, wenn er eine Gerätebindung im Rahmen eines Authentisierungsverfahren nutzt, die Zeitrahmen der Gültigkeit für die Gerätebindung gemäß Tabelle "Übersicht Gerätebindung" berücksichtigen.
~~Beim Zugriff auf Daten mit hohem Schutzbedarf gelten die Zeiträume der maximalen Gerätebindung~~`~~gematik-ehealth-loa-high~~`~~ ~~in der Tabelle. Nach Einwilligung des Nutzers gemäß A_23103* gelten beim Zugriff auf Daten mit hohem Schutzbedarf, unter Verwendung von Authentisierungsverfahrens~~ `~~gematik-ehealth-loa-substantial~~` ~~die Zeiträume der maximalen Gerätebindung~~`~~gematik-ehealth-loa-substantial~~` ~~in Tabelle "Übersicht Gerätebindung".~~
Die Gerätebindung MUSS durch den Nutzer nach Ablauf dieser Frist dementsprechend erneuert werden.
Der Anbieter des sektoralen IDP MUSS mit den zur Verfügung stehenden Plattformmechanismen, einen kryptographischen Nachweis der Gerätebindung auf dem Endgerät erzeugen und auf Serverseite prüfen (z.B. Android: Key & ID Attestation; iOS: DCAppAttestService).
Die Gerätebindung kann:

1. durch Identifikation, welche dem Niveau `gematik-ehealth-loa-high` entspricht oder
2. mit einer 2FA, welche dem Niveau `gematik-ehealth-loa-high` entspricht,

angelegt werden.

Tabelle 2: Übersicht Gerätebindung

Schlüsselspeicher	Gültigkeit der Gerätebindung
ohne Hardware Keystore	Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen ode Inhärenz 24h genutzt werden. • ~~24h auf dem Niveau "gematik-ehealth-loa-high"~~ • ~~48h auf dem Niveau "gematik-ehealth-loa-substantial"~~
mit Hardware Keystore	Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen ode Inhärenz 24 Monate genutzt werden. • ~~6 Monate auf dem Niveau "gematik-ehealth-loa-high"~~ • ~~12 Monate auf dem Niveau "gematik-ehealth-loa-substantial"~~
mit zertifiziertem Secure Element	Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen ode Inhärenz unbegrenzt genutzt werden. • ~~unbegrenzt auf dem Niveau "gematik-ehealth-loa-high"~~

	• ~~unbegrenzt auf dem Niveau "gematik-ehealth-loa-substantial~~

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_IDP-Sek_PTV

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_IDP-Sek_PTV]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 3: Anforderungen zur sicherheitstechnischen Eignung "Produktgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_22750-02~~	Gerätebindung und Authentisierung für "gematik-ehealth-loa-high" und "gematik-ehealth-loa-substantial" (befristet bis 02.01.2027)	gemSpec_IDP_Sek
A_22750-03	Gerätebindung und Authentisierung	gemSpec_IDP_Sek