
C_12555_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_Krypt.....	3
3 Änderungen in Steckbriefen.....	5
3.1 Änderungen in gemProdT_..._PTVx.y.z-n.....	5

1 Änderungsbeschreibung

Beim PoPP-Service sollen analog wie bei ePA und E-Rezept die Telematik-IDs bei den Telemetriedaten pseudonymisiert werden.

Dafür gibt es eine Ergänzung in gemSpec_Krypt.

2 Änderung in gemSpec_Krypt

Ergänzung in gemSpec_Krypt am Ende von Abschnitt „3.16 Anomalie-Erkennung“

Folgender Text wird hinzugeführt. Auf die Gelbfärbung wird der besseren Lesbarkeit willen verzichtet (gesamter Text ist neu).

Bei ePA und E-Rezept wird die Pseudonymisierung von Daten (Telemetriedaten / Anomalie-Erkennung) nach den zuvor in diesem Abschnitt aufgeführten Vorgaben durchgeführt. Für alle anderen Anwendungen wird für die Pseudonymisierung ein hybrides Verschlüsselungsverfahren (ECIES mit AES/GCM) eingesetzt. Dieses ist zwar weniger performant als das Verfahren aus A_27332-*, aber dafür kann auf die Verteilung der geheimen Pseudonymisierungsschlüssel (vgl. A_27392-*) verzichtet werden.

A_28578 - PoPP-Service - Pseudonymisierung bei den Telemetriedaten (Anomalie-Erkennung)

Der PoPP-Service MUSS bei der Pseudonymisierung von Daten im Kontext von A_26532-* folgende Vorgaben umsetzen:

1. Der PoPP-Service MUSS ein von der gematik/CDC bereitgestelltes Verschlüsselungszertifikat, integritäts- und authentitätsgeschützt in der VAU einpflegen (Initialisierung des Fachdienstes). (Hinweis: Das Verschlüsselungszertifikat ist ECC-basiert, d. h. auch der EE-Schlüssel ist ein ECC-Schlüssel.)
2. Der PoPP-Service MUSS auf Anweisung der gematik/CDC dieses Verschlüsselungszertifikat innerhalb von 5 Werktagen wechseln können. (Kontext: Regelmäßiger Wechsel des Verschlüsselungszertifikats)
3. Sei P die zu pseudonymisierende Zeichenkette. Der PoPP-Service MUSS am Ende von P solange Leerzeichen anfügen bis die Länge der somit erzeugten Zeichenkette ein Vielfaches von 32 ist. Sei Padding-Länge die Anzahl der hinzugefügten Leerzeichen. Diese Padding-Länge wird als Byte kodiert (Beispiel: Padding-Länge 0 würde als \x00 Byte kodiert) und der erzeugten Zeichenkette vorangestellt. Das Ergebnis wird als Plaintext bezeichnet.
4. Er MUSS diesen Plaintext mittels ECIES (AES/GCM) unter Verwendung des öffentlichen Verschlüsselungsschlüssels aus dem Verschlüsselungszertifikat aus Punkt 1 (bzw. 2) verschlüsseln.
 - a. Dabei MUSS der PoPP-Service ein ephemeres ECDH-Schlüsselpaar zufällig erzeugen und mit diesem und dem öffentlichen Schlüssel aus dem Verschlüsselungszertifikat ein ECDH gemäß [NIST-800-56-A] durchführen. Das somit erzeugte gemeinsame Geheimnis ist Grundlage für die folgende Schlüsselableitung.
 - b. Als Schlüsselableitungsfunktion MUSS er die HKDF nach [RFC-5869] auf Basis von SHA-256 verwenden.
 - c. Dabei MUSS er den Ableitungsvektor "ecies-cdc-p17" verwenden, d. h. in der Formulierung von [RFC-5869] info="ecies-cdc-p17".
 - d. Er MUSS mit dieser Schlüsselableitung einen AES-128-Bit Content-Encryption-Key (CEK) für die Verwendung von AES/GCM ableiten.
 - e. Er MUSS für die Verschlüsselung mittels AES/GCM einen 96 Bit langen Null-Vektor (0...0) als Initialisierungsvektor (IV) verwenden.

- f. Er MUSS mit dem CEK und dem IV mittels AES/GCM den Plaintext verschlüsseln, wobei dabei ein 128 Bit langer Authentication-Tag zu verwenden ist.
 - g. Aus dem Verschlüsselungszertifikat MUSS er den SubjectKeyIdentifier (SKI) entnehmen und die ersten 16 Bit als „gekürzter SKI“ im folgenden Schritt verwenden.
 - h. Er MUSS das Ergebnis wie folgt kodieren: `chr(0x02) || <gekürzter SKI> || <32 Byte X-Koordinate des öffentlichen Schlüssels aus (a) > || <AES-GCM-Chifftrat> || <16 Byte AuthenticationTag>`. (Hinweis: es fehlt absichtlich die Y-Koordinate und der IV).
 - i. Die X-Koordinate ist (wie üblich) vorne mit `chr(0)` zu paden solange bis sie eine Kodierungslänge von 32 Byte erreicht. Die Byte-Order MUSS Network-Byte-Order (= Big) sein.
 - j. Das so kodierte Ergebnis wird als erweitertes Chifftrat bezeichnet.
5. Der PoPP-Service MUSS das erweiterte Chifftrat mittels Base64 kodieren. Das Ergebnis ist ein Pseudonym von P (vgl. Punkt 3).

[zur Kommentierung freigegeben,<=]

Hinweise zu A_28578-:*

1. *Die gematik stellt Beispiel-Code für die Pseudonymisierung von Daten nach A_28578-* bereit.*
2. *Aufgrund der zufälligen Erzeugung der ephemeren Schlüssel in A_28578-* Punkt 4 a) erzeugt jede Pseudonymisierung gemäß A_28578-* ein neues (anderes) Pseudonym.*

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_..._PTVx.y.z-n

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

Tabelle 1: Anforderungen zur Anforderungszuordnung

Afo-ID	Afo-Zuweisung
A_28578	PoPP-Service: Sicherheitstechnische Eignung, Produktgutachten