
C_12149_Anlage

1 Änderung in gemSpec_Krypt

Es wird wie folgt ein neuer Abschnitt "3.16 Anomalie-Erkennung" in gemSpec_Krypt eingefügt. Auf die Gelbmarkierung wird verzichtet, weil in Gänze neuer Text.

1.1 3.16 Anomalie-Erkennung

A_27332 - ePA-Aktensystem - Pseudonymisieren der gematik-Logdaten

Das ePA-Aktensystem MUSS die in A_27331-* für die Pseudonymisierung gekennzeichneten Informationen der Logdaten mittels AES/CBC mit dem Schlüssel key_pn_log und dem festen Initialisierungsvektor IV=0...0 (16 Null-Bytes) verschlüsseln.

Bei einer Verschlüsselung im CBC-Modus muss der zu verschlüsselnde Klartext gleich einem Vielfachen der Blocklänge der Blockchiffre sein. Dies ist bei den zu pseudonymisierenden Daten (DTBP) selten der Fall. Deshalb MUSS eine Kodierung der DTBP vor der Verschlüsselung wie folgt stattfinden:

Name	Länge	Erläuterung / Vorgaben
Längenfeld	8 Bytes	In diesem 64-Bit großen Längenfeld wird die Länge der DTBP in Network-Byte-Order (Byte-Order Big) kodiert.
DTBP	variabel	Die zu pseudonymisierenden Daten (DTBP) werden hier aufgeführt (Byte-Strom) der Länge "Längenfeld"
Padding	variabel	Das Padding besteht als Leerzeichen (chr(32)) und zwar so vielen, dass die Länge der Konkatenation <Längenfeld> <DTBP> <Padding> ein Vielfaches der AES-Blocklänge (128 Bit = 16 Byte) ist. Damit kann es zwischen 0 und 15 Padding-Leerzeichen abhängig von der Länge der DTBP geben.
Leer-Block	16 Bytes	16 Leerzeichen (chr(32))

Diese Kodierung wird Klartext (DTBE) genannt. Der Klartext wird per AES/CBC mit dem key_pn_log und dem festen Initialisierungsvektor IV=0...0 (16 Null-Bytes) verschlüsselt und man erhält damit ein Chifftrat. Dieses Chifftrat MUSS base64 kodiert werden. Das Ergebnis (diese Kodierung) ist das Pseudonym von DTBP.

[<=, Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten]

Für die betreiberübergreifende Anomalie-Erkennung werden in der VAU bestimmte Attribute (vgl. A_22496-*) pseudonymisiert aus der VAU exportiert (vgl. [gemSpec_Aktensystem_PAfueralle#"Logging und Monitoring]). Das Cyber-Defense-Center der TI kann bei der Feststellung von Anomalien, die einen Angriff als Ursache dringend vermuten lassen, die Pseudonyme depseudonymisieren, um weitere Maßnahmen zum Schutz der medizinischen Daten gezielt durchführen zu können.

Erläuterung zu A_27332-*:

Durch die Verwendung eines konstanten Initialisierungsvektors (IV) ist die Verschlüsselung eine deterministische Verschlüsselung.

Im Normalfall haben die zu pseudonymisierenden Daten (DTBP) eine Länge von kleiner 256 Bytes. Um an dieser Stelle aber auf der sicheren Seite zu sein (weil bspw. in einer späteren Ausbaustufe einige DTBP länger sein könnten), wurde ein 64-Bit-Wert als Längenfeld definiert, so dass man physikalisch dieses Limit nicht erreichen kann.

Der Leer-Block am Ende dient als (in seiner Leistungsfähigkeit sicher beschränkter) Integritäts- und Authentitätsschutz. Damit kann ein Depseudonymisierer ermitteln ob ein Pseudonym gültig ist. Ein umfassenderer Integritäts- und Authentitätsschutz macht fachlich genau an dieser Stelle wenig Sinn, der Schutz muss über die Log-Daten in Ihrer Gesamtheit erfolgen.

Auf die explizierte Anführung einer Versionskennung des verwendeten Pseudonymisierungsschlüssel wurde verzichtet.

Die gematik stellt Beispiel-Code für die Erstellung von Pseudonymen nach A_27332-* bereit.

A_27392 - ePA-Aktensystem - Import eines Pseudonymisierungsschlüssels

Ein ePA-Aktensystem MUSS von der gematik für die entsprechende ePA-VAU verschlüsselte Pseudonymisierungsschlüssel importieren können. Dabei wird ein Export-Paket analog zu A_27276-* verwendet mit den gleichen kryptographischen Vorgaben (A_27275-*). Die JSON-Struktur für den Import hat folgende Struktur:

```
{
  "Schlüsseltyp": "Pseudonymisierungsschlüssel CDC",
  "version": "<eine natürliche Zahl als String hier aufgeführt>",
  "iat": "<YYYY-MM-DD>",
  "encrypted_key":
    "01b07b90f7379b06fd4e3b406fafce16c73c8e95abfd4e60219e779bb7d76cf802a75f9f7d
    fac99e8f998b27f876dc5af910b685261f2ce38004fe638f25c5451f1b028c2b7c3d707c1e5
    dad3ed8b34bd4406284a43a15654f677b6ed7c7041cf7eaec59fa2093fc51de71dd4ad461dd
    4a2d8e1f5d611a25bd99ac1129"
}
```

Der Import eines neuen Pseudonymisierungsschlüssels überschreibt/ersetzt den älteren/vorhergehenden Pseudonymisierungsschlüssel in der VAU. D. h., nach dem Import wird also der neue Pseudonymisierungsschlüssel sofort für eine dem erfolgreichen Import folgende Pseudonymisierung verwendet.

Die Zeit in iat MUSS keine Konsequenz im VAU-HSM haben -- das Attribut dient nur zu organisatorischen Zwecken beim Import/Export-Prozess.

[<=, ,]

2 Änderung in gemSpec_Aktensystem_ePAfueralle

In Abschnitt 3.5.1.5 "Logging und Monitoring" werden folgende Abschnitte ergänzt.

2.1 gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik

A_27333 - ePA-Aktensystem - Geheimer Schlüssel für Pseudonymisierung der gematik-Logdaten nur in VAU

Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigte geheime Schlüssel key_pn_log im Klartext ausschließlich innerhalb einer VAU-Instanz verarbeitet wird.

[<=, Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten]

Hinweis zu A_27336-*: Der geheime Schlüssel für die Pseudonymisierung muss nicht im VAU-HSM gespeichert werden.

A_27336 - ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung im 4-Augen-Prinzip

Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigte geheime Schlüssel key_pn_log ausschließlich im 4-Augen-Prinzip ins ePA-Aktensystem eingebracht werden kann.

[<=, Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten]

A_27334 - ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung der gematik-Logdaten im 4-Augen-Prinzip

Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigten geheimen Schlüssel key_pn_log ausschließlich im 4-Augen-Prinzip mit der gematik ins ePA-Aktensystem einbringen.

[<=, Anb_Aktensystem_ePA, Sich.techn. Eignung: Gutachten (Anbieter)]

A_27335 - ePA-Aktensystem - Wechsel des Schlüssels für Pseudonymisierung der gematik-Logdaten

Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigten geheimen Schlüssel key_pn_log spätestens nach 1 Jahr wechseln.[<=, Anb_Aktensystem_ePA, Sich.techn. Eignung: Gutachten (Anbieter)]

3 Änderung in gemSpec_Perf

Änderung in Tabelle 57 in Kapitel 3.18.2 Betriebsdatenerfassung v2 Spezifika ePA-Aktensystem

Tabelle 1 : Tab_gemSpec_Perf_Berichtsformat_ePA

Usecase / Anwendungsfall-ID		Duration	Message-Block
EPA.UC_1	Login Versicherter	Beginnt mit VAU-Hello und endet mit dem Abschluss des Aufbaus der VAU. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	{ "cid": "\$clientId", "cv" : "\$version" }
EPA.UC_B1.1	Dokument hochladen Versicherter	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response.	{ "cid": "\$clientId", "cv" : "\$version", "size": \$size }
EPA.UC_B4.x	Verbergen von Dokumenten / Kategorien	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	{ "cid": "\$clientId", "cv" : "\$version" }
EPA.UC_A2.2	Befugnis ablegen Versicherter	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	{ "cid": "\$clientId", "cv" : "\$version" }
EPA.UC_A2.5	Befugnis ablegen Vertreter	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	{ "cid": "\$clientId", "cv" : "\$version" }
EPA.UC_2	Login PS	Beginn mit VAU-Hello und	{ "cid": "\$clientId",

		endet mit dem Abschluss des Aufbaus der VAU. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	"cv" : "\$version", "profOID": "\$professionOID", "tid" : "\$pn_telematikID", "ip" : "\$pn_ipaddress" }
EPA.UC_2x	Aktenkontext öffnen PS	Beginnt mit dem (ggf. impliziten) Request zum Öffnen eines bestimmten Health Record Contextes und endet mit Abschluss des Absendens der Response.	{ "cid": "\$clientID", "cv" : "\$version", "profOID": "\$professionOID", "tid" : "\$pn_telematikID", "ip" : "\$pn_ipaddress" }
EPA.UC_B1.2	Dokument hochladen PS	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response.	{ "cid": "\$clientID", "cv" : "\$version", "size": \$size, "profOID": "\$professionOID", "cat": "\$category", "tid" : "\$pn_telematikID", "ip" : "\$pn_ipaddress" }
EPA.UC_A3.9	Abfragen von Widersprüchen PS	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	{ "cid": "\$clientID", "cv" : "\$version" }
EPA.UC_6.1y	Medikationsliste abrufen PS	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	{ "cid": "\$clientID", "cv" : "\$version", "size": \$size, "tid" : "\$pn_telematikID", "ip" : "\$pn_ipaddress" }
EPA.UC_A2.1	Befugnis ablegen PS	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response. Während ggf. notwendigem Request an externen Komponenten pausiert die Messung.	{ "cid": "\$clientID", "cv" : "\$version", "tid" : "\$pn_telematikID", "ip" : "\$pn_ipaddress", "ciss" : "\$pn_certissuer", "csn" : "\$pn_ipaddress" }

			"\$pn_certserialnumber" }
EPA.UC_C6.1	Verordnungen einstellen eRP-FD	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response.	{ }
EPA.UC_C6.1x	Dispensierung einstellen eRP-FD	Beginnt mit dem Erhalt des Requests und endet mit Abschluss des Absendens der Response.	{ }
EPA.UC_C4.1x	Übermittlung VST	Beginnt mit dem Start des Versands der Lieferpseudonyme an die Vertrauensstelle und endet mit dem Abschluss des Versands.	{ }
EPA.UC_C4.1y	Übermittlung FDZ	Beginnt mit dem Erhalt der Empfangsbereitschaft vom Forschungsdatenzentrum und endet mit dem Abschluss des Versands des FDZ-Packages.	{ "size": \$size }

Ablösung A_22469-01 durch neue Afo A_22469-02

A_22469-02 - Performance - Betriebsdatenlieferung v2 - Spezifika ePA-Aktensystem - Message

Der Produkttyp Aktensystem_ePA MUSS bei Betriebsdatenlieferungen bzgl. des Feldes "message" folgende spezifischen Festlegungen hinsichtlich des Formates und der Inhalte berücksichtigen.

```
{ "cid": "$clientID", "cv": "$version", "size": $size, "profOID": "$professionOID", "cat":
"$category", "tid": "$pn_telematikID", "ip": "$pn_ipaddress", "ciss": "$pn_certissuer",
"csn": "$pn_certserialnumber" }
```

- \$clientID: ClientID-Parameter aus dem HTTP-Header-Feld gemäß Anforderungslage für Clientsysteme aus [gemSpec_Aktensystem_ePAfuerAlle#A_22470-04] (erster Teil des Useragent-Parameters), Datentyp String
- \$version: Versionsnummer-Parameter aus dem HTTP-Header-Feld gemäß Anforderungslage für Clientsysteme aus [gemSpec_Aktensystem_ePAfuerAlle#A_22470-04] (zweiter Teil des Useragent-Parameters), Datentyp String
- \$size: Größe des Requests in kilobyte, Datentyp Integer
- \$professionOID: professionOID gemäß [gemSpec_Aktensystem_ePAfuerAlle#A_23941], Datentyp String
- \$category: Dokumentenkategorie gemäß der Spalte "technischer Identifier" in [gemSpec_Aktensystem_ePAfuerAlle#A_19303-*], Datentyp String

- `$pn_telematikID`: Telematik-ID des angemeldeten Nutzers, verschlüsselt gemäß A_27332-*, Datentyp String
- `$pn_ipaddress`: IP-Adresse des angemeldeten Nutzers, verschlüsselt gemäß A_27332-*, Datentyp String
- `$pn_certissuer`: issuer-Parameter aus C.HCI.AUT, verschlüsselt gemäß A_27332-*, Datentyp String
- `$pn_certserialnumber`: serialNumber-Parameter aus C.HCI.AUT, verschlüsselt gemäß A_27332-*, Datentyp String

Für die jeweilige Operation sind dabei nur die in der Spalte "Message" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_ePA angegebenen Key-Value Paare zu übermitteln. Bei der Erstellung des message-Feldes ist darauf zu achten, dass weder Whitespaces noch Newlines zwischen JSON-Elementen enthalten sind (kein Indenting) und Vorgaben nach [RFC7493] eingehalten werden. [<= , ,]