Änderung in gemF_Highspeed-Konnektor

1.1.1.1 _ 5.2.1.2 HSM

[...]

A_21987 - Zugriff auf d~~as~~ie HSM~~VAU~~ nur durch den Hersteller

~~Die VAU des~~ Der Highspeed-Konnektor~~s~~ MUSS ~~Eingriffe in das System durch andere als den Hersteller unterbinden. Das betrifft im Besonderen~~ administrative Zugriffe auf das HSM, die Kopplung ~~des~~ mit dem HSM und die Kopplung mit dem SZZP durch andere als den Hersteller unterbinden. <=

[...]

1.1.1.2 _ 5.2.1.3 Vertrauenswürdige Ausführungsumgebung

Die Vertrauenswürdigen Ausführungsumgebung (VAU) dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Klartextdaten ~~(Aktenschlüssel und Kontextschlüssel des Aktenkontos eines Versicherten)~~ innerhalb des HSK~~FM ePA~~.

Die VAU ist die Gesamtheit aus der für eine Klartextverarbeitung erforderlichen Software, dem für eine Klartextverarbeitung genutzten physikalischen System sowie den für die Integrität einer Klartextverarbeitung erforderlichen organisatorischen und physischen Rahmenbedingungen~~bildet den Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung (VAU)~~.

~~Zur Vertrauenswürdigen Ausführungsumgebung gehören neben den Verarbeitungskontexten alle für ihre Erreichbarkeit und betriebliche Steuerung erforderlichen Komponenten.~~

Die VAU~~Der Verarbeitungskontext~~ grenzt sich von allen weiteren, im betrieblichen Kontext bei einem Anbieter, der den HSK betreibt, ~~KTR-Consumer~~ vorhandenen Systemen und Prozessen dadurch ab, dass die sensiblen Klartextdaten von Komponenten innerhalb der VAU~~des Verarbeitungskontextes~~ aus erreichbar sind oder sein können, während sie dies von außerhalb der VAU~~des Verarbeitungskontextes~~ nicht sind. Sensible Daten verlassen die VAU~~den Verarbeitungskontext~~ ausschließlich gemäß wohldefinierten (Zugriffs-)Regeln und in verschlüsselter Form.

Die schützenswerten sensiblen Daten sind alle Versichertendaten (personenbezogene Daten und Schlüssel), die im HSK verarbeitet werden~~der Akten- und Kontextschlüssel der Aktenkonten, für die der KTR zugriffsberechtigt ist~~.

~~Die Mehrzahl Verarbeitungskontexte ergibt sich aus der softwaretechnischen Trennung verschiedener Sitzungen. Somit wird jede Akte in Ihrem eigenen Verarbeitungskontext genutzt. Physische Maßnahmen bspw. zum Zutrittsschutz sind hingegen nur einmalig für die gesamte VAU erforderlich, also für jeden Verarbeitungskontext identisch.~~

Die VAU muss einen Schutz dieser Daten leisten, der gerade auch gegen Innentätern beim Anbieter/Betreiber wirkt.

Dieser Schutz vor unberechtigtem Zugriff auf schützenswerte Klartextdaten kann auf unterschiedliche Art und Weise erreicht werden. Dabei können technische Maßnahmen in Software (im Code des Produkts oder hardwarenahe Mechanismen), Maßnahmen zum physischen Schutz und organisatorische Maßnahmen genutzt bzw. kombiniert werden. Ein ausschließlich organisatorischer Schutz ist jedoch nie ausreichend, denn es muss wie

o.g. stets der Innentäter, der am Betrieb des Produkts beteiligt ist betrachtet werden, der an der Durchsetzung von organisatorischen Maßnahmen beteiligt ist und diese somit ggf. umgehen kann und Zugriff direkt auf die Hardware bekäme.

Auch wenn der Schutz der Daten vorrangig ist, muss dennoch ebenso die Betreibbarkeit der Lösungen mit betrachtet werden. Daher sollen Lösungen ermöglicht werden, bei denen der Betreiber einfache Wartungsarbeiten durchführen kann, ohne dass dafür jedes Mal Ausfallzeiten für das Produkt anfallen. Der dadurch grundsätzlich gegebene Zugriff des Betreibers auf die Hardware, muss für die Auswahl der Schutzmaßnahmen berücksichtigt werden.

Die Anforderungen im Folgenden sollen Herstellern und Anbietern eine gewisse Freiheit bei der Wahl der Maßnahmen geben, jedoch für bestimmte Szenarien detailliertere Vorgaben machen unter denen diese Szenarien dann realisierbar sind. Dies sind dann Anforderungen konkret im Kontext des Highspeed-Konnektors sowie auch dessen Betrieb innerhalb des TI-Gateways.

A_17346-01 - HSK: VAU - Zwingende Verwendung~~arbeitungskontext~~ der VAU

Der ~~Verarbeitungskontext des~~ Highspeed-Konnektors MUSS ~~sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen, deren Sicherheitseigenschaften sich auf den Schutz der~~ Schlüssel und Medizinischen Daten eines Versicherten ausschließlich innerhalb der VAU verarbeiten und sie so vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext schützen~~auswirken können~~. <=

A_17347-01 - HSK: ~~Verarbeitungskontext der~~ VAU - Keine persistente Speicherung von Versichertendaten

Der ~~Verarbeitungskontext des~~ Highspeed-Konnektors DARF Schlüssel und medizinische Daten eines Versicherten NICHT persistent speichern, auch nicht verschlüsselt.<=

A_17348-01 - HSK: ~~Verarbeitungskontext der~~ VAU - Schutz ePA-Akten- und Kontextschlüssel~~verlassen VAU nie~~

Der ~~Verarbeitungskontext des~~ Highspeed-Konnektors MUSS sicherstellen, dass die Akten- und Kontextschlüssel der Versicherten die VAU nur verlassen (unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind), wenn sie ans ePA-Aktensystem übermittelt werden und die Übermittlung zum ePA-Aktensystem in einem sicheren Kanal erfolgt.<=

Zwischenüberschrift entfernen, da alles zum Thema VAU gehört

~~5.2.1.4 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld~~

A_17350-01 - HSK: VAU - Isolation ~~der VAU~~ von anderen Datenverarbeitungsprozessen des Anbieters

Der ~~ie VAU des~~ Highspeed-Konnektors MUSS die in der VAU~~im Verarbeitungskontext~~ ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters/Betreibers trennen und damit gewährleisten, dass der Anbieter/Betreiber vom Zugriff auf die in der VAU verarbeiteten, schützenswerten Daten ausgeschlossen ist.<=

A_17351-01 - HSK: VAU - Ausschluss von Manipulationen an der Software~~der VAU~~

Die VAU des Highspeed-Konnektors MUSS die Integrität der eingesetzten Software schützen und damit insbesondere unbemerkte Manipulationen an der Software durch den Anbieter/Betreiber ausschließen.<=

A_17352-01 - HSK: VAU - Ausschluss von Manipulationen an der Hardware~~der VAU~~

Die VAU des Highspeed-Konnektors MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere unberechtigten physischen Zugriff auf die VAU-Hardware und unbemerkte Manipulationen an der VAU-Hardware - auch durch den Anbieter/Betreiber- ausschließen.<=

A_17353-01 - HSK: VAU - Kontinuierliche Wirksamkeit des Manipulationsschutzes~~der VAU~~

Die VAU des Highspeed-Konnektors MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter/Betreiber mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.<=

A_17354-01 - HSK: VAU - ~~Kein p~~Physischer Zugang ~~des Anbieters zu Systemen der VAU~~

Die VAU des Highspeed-Konnektors MUSS mit technischen Mitteln sicherstellen, dass kein unberechtigter Zugriff auf die Hardware der VAU möglich ist und dass

a. niemand- berechtigt oder unberechtigt und auch nicht der Anbieter/Betreiber~~,~~ - während der Verarbeitung personenbezogener medizinischer Daten physischen Zugriff auf ~~physische Schnittstellen~~ die Hardware der Systeme erlangen kann, auf denen eine VAU ausgeführt wird
   und / oder
b. auf dem System durch Verschlüsselung auf CPU-Level keine Klartextdaten verarbeitet werden, so dass auch bei physischem Zugriff auf die Hardware
   i. kein Zugriff auf verarbeitete personenbezogenen medizinischen Daten im Klartext möglich ist,
   ii. keine Deaktivierung der Maßnahmen, die vor Zugriff auf Klartextdaten schützen, möglich ist.

Durch die Umsetzung von Punkt b werden berechtigte Zugriffe auf die Systeme durch den Anbieter entsprechend A_24294

möglich.

<=

A_17355-01 - HSK: VAU - Extraktion Klartextdaten bei ~~Nutzdatenbereinigung vor~~ physischem Zugangunterbinden ~~zu Systemen der VAU~~

Die VAU des Highspeed-Konnektors MUSS mit technischen Mitteln sicherstellen, dass ein physischer Zugang zu Hardware-Komponenten der VAU~~Verarbeitungskontexte~~ nur erfolgen kann, ~~nachdem~~wenn gewährleistet ist, dass aus ihnen keine Nutzdaten im Klartext extrahiert werden können. Dies kann erfüllt werden, indem bei physischem Zugang automatisch sämtliche sensiblen Daten sicher aus dem Speicher gelöscht werden oder gar keine Klartextdaten auf dem System verarbeitet werden und dies auch durch physischen Zugang nicht umgangen oder deaktiviert werden kann.<=

A_17356-02 - HSK: VAU - Löschen aller Daten beim Beenden von ~~des~~ Verarbeitungsvorgängen~~kontextes~~

Die VAU des Highspeed-Konnektors MUSS beim Beenden von ~~eines~~ Verarbeitungsvorgängen~~kontextes~~ sämtliche Daten dieses

Verarbeitungsvorgangs~~kontextes sicher~~ löschen, sobald diese Daten nicht mehr benötigt werden. Insbesondere müssen beim Beenden einer virtuellen HSK-Instanz sämtliche transienten Daten dieser Instanz gelöscht werden. Löschen bedeutet, dass auch keine sensiblen Daten mehr im flüchtigen Speicher gehalten werden. Ein Persistieren von sensiblen Daten ist entsprechend A_17347* zu keinem Zeitpunkt zulässig.<=

Die folgende AFO A_21990 ist vor dem Hintergrund, dass USB-Kartenleser bereits aus der Spezifikation gestrichen wurden und die Zugriffe aufs HSM bereits durch A_21987 geregelt sind obsolet.

~~**A_21990 - Kein Zugriff auf SM-B Identitäten und Kopplungs-Geheimnis durch Betreiber**~~

~~Der Highspeed-Konnektor MUSS den Betreiber vom vollen Zugriff auf SM-B-Identitäten ausschließen. Im Fall einer SMC-B darf der Betreiber nicht sowohl Zugriff auf die Karte als auch Wissen der PIN haben. Im Fall einer Speicherung von SM-B-Identitäten in einem HSM darf der Betreiber nicht das HSK-HSM-Kopplungsgeheimnis kennen.<=~~

A_23495 - HSK: VAU - Protokollierung bei physischem Zugang zu Systemen der VAU

Der Highspeed-Konnektor~~HSK~~ MUSS sämtliche Zugriffe auf die Hardware der VAU protokollieren - sei es die vorgesehene berechtigte Öffnungen oder das Auslösen der Sensoren/Alarme ~~zum~~des physischen Zugangsschutz (vgl. A_17352*, A_17354*, A_17355*)~~vor dem Herunterfahren protokollieren~~.<=

Folgende AFOs werden neu aufgenommen.

A_24294 - HSK: VAU - Physischer Zugang bei laufender Verarbeitung

Der Hersteller des Highspeed-Konnektors MUSS, wenn sein HSK-Produkt physischen Zugang zur Hardware bei laufender Datenverarbeitung durch berechtigte Mitarbeiter des Anbieters entsprechend A_17354* Punkt b zulässt, folgendes umsetzen:

- Dieser Zugang des Anbieters MUSS im Sicherheitskonzept des Herstellers berücksichtigt werden, wobei dies auch Innentäter beim Anbieter einbeziehen muss.
- In den Nutzungsbedingungen für Anbieter (bspw. "Secure User Guidance") MÜSSEN
  - die zulässigen Wartungsarbeiten, die der Anbieter durchführen darf, inkl. Maximaldauer benannt werden (diese sind auch konkret im Produktgutachten aufzuführen),
  - die für berechtigte physische Zugriffe des Anbieters notwendigen zusätzlichen organisatorischen Maßnahmen definiert werden und
  - auf die zwingende Prüfung der Umsetzung dieser zusätzlichen Maßnahmen entsprechend GS-A_4984-01 und A_24295 hingewiesen werden.

Produktgutachten HSK <=

Änderung in gemF_TI-Gateway

Folgende AFO wird neu aufgenommen für den Anbieter TI-Gateway.

A_24295 - Zusätzliche Betreiber-Rolle bei physischem Zugang bei laufender Verarbeitung

Der Anbieter TI-Gateway MUSS, wenn ein von ihm verwendetes HSK-Produkt physischen Zugang zur Hardware bei laufender Datenverarbeitung durch berechtigte Mitarbeiter des Anbieters entsprechend A_17354* Punkt b zulässt, eine Rollentrennung zwischen dem Personal, dass den HSK administriert und wartet ("HSK-Betreiber"), und dem Personal, dass das Rechenzentrum betreibt ("RZ-Betreiber"), umsetzen, so dass

- der HSK-Betreiber keinen Zutritt zum HSK hat, ohne den RZ-Betreiber,
- der RZ-Betreiber keinen Zugang zur Hardware des HSK hat, ohne den HSK-Betreiber,
- der RZ-Betreiber die Wartungsarbeiten des HSK-Betreibers überwacht und durchsetzt, dass sich diese auf die in den Vorgaben des Herstellers (bspw. "Secure User Guidance") definierten Wartungsarbeiten und deren Maximaldauer beschränken (siehe A_24294).

Der Anbieter MUSS entsprechende Prozesse definieren und etablieren, die dies dauerhaft gewährleisten und eine regelmäßige Validierung der Umsetzung durchsetzen. Die Umsetzung des Rollenausschluss MUSS die Weisungsbefugnis von Vorgesetzten berücksichtigen. Das heißt, dass keine Person direkter Vorgesetzter sowohl von Personal der Rolle HSK-Betreiber als auch von Personal der Rolle RZ-Betreiber sein darf.

Der Anbieter TI-Gateway SOLL weitere Schutz- / Überwachungsmaßnahmen, die unberechtigte Zugriffe/Manipulationen der HW erkennbar machen und durch den RZ-Betreiber durchgesetzt werden, umsetzen, wie bspw. Video-Überwachung. Werden keine zusätzlichen Maßnahmen umgesetzt ist dies durch den Gutachter im Sicherheitsgutachten zu begründen.

Sicherheitsgutachten Anbieter HSK <=