FH-Anlage 3

Selbsteinschätzung Hersteller betreffend eigener Lösungsansätze zur Erfüllung der softwarespezifischen Anforderungen des Dokumentes REA 6-A (März 2017)

Anleitung zur Verwendung

Die roten Spalten (2-4) sind Original-Text aus dem REA-Dokument 6-A. Bitte tragen Sie in die blauen Spalte 5 ein, wie Sie aus Ihrer Sicht mit Ihrem Produkt (TOE) diese Anforderungen erfüllen. In der Zeile geben Sie dazu bitte die Textstellen in Ihren Original-Dokumenten an, die Ihre Aussage zu Erfüllung der Anforderung begründen. Die Fundstellen bitte mit Dokumentname, Kapitel-Nr. und Seitenzahl angeben. Am der Eintragungen in die Zellen bitte immer das Datum angeben (TT.MM.JJJJ)

Der Verfahrensbetreuer in der PTB wird Ihre Aussagen prüfen und bewerten und einen Kommentar dazu in Spalte 6 abgeben. Z.B. „akzeptiert“ oder „es fehlen noch folgende Informationen …“ usw. Die Liste wird bei Bedarf mehrfach zwischen Hersteller und PTB hin- und gesandt, bis die vollständige Erfüllung aller Anforderungen festgestellt werden kann. Bitte niemals Text aus der Tabelle löschen. Die gesamte Chronologie der Abstimmung soll nachvollziehbar bleiben.

1 Nr.	2 Kürzel	3 Titel	4 Akzeptable Beispiellösung gemäß Beispiel zur Verdeutlichung eines angemessenen Schutzniveaus	5 Beschreibung des Lösungsansatz des Herstellers mit Fundstellen-Angabe in der Hersteller-Doku.	6 Kommentar Konformitätsbewertungsstelle
1	AU1	Schnittstelle für Kundenidentifikation	PIN-Pad zur Eingabe einer Kunden-ID und eines Passworts oder RFID-Schnittstelle		
2	AU2	Kundenidentifikation für den Geschäftsvorgang	EMAID, UID oder RFID		
3	ID1	Softwareidentifikation	Prüfung eines SHA2-Hashes über die gesamte Software beim Systemstart		
4	IN1	Einflussnahme über die Benutzerschnittstelle	Eingeschränkter Befehlssatz, der nur Lesebefehle für Identifikatoren, gespeicherte Messergebnisse und das Logbuch erlaubt sowie die Eingabe einer Kundenidentifikation		
5	IN2	Einflussnahme über die Kommunikationsschnittstelle	Ein rechtlich relevantes Softwaremodul prüft alle eingehenden Befehle auf ihre Zulässigkeit hin und blockiert unzulässige Befehle.		
6	MA1	Unbeabsichtigte Veränderung rechtlich relevanter Software und gerätespezifischer Parameter	Prüfung eines SHA2-Hashes über die gesamte Software beim Systemstart		
7	MA2	Absichtliche Veränderung rechtlich relevanter Software und von Messdaten	Prüfung eines SHA2-Hashes über die gesamte Software beim Systemstart		
8/9	MA3 MA4	Absichtliche Veränderung gerätespezifischer Parameter Nachweis eines Eingriffs	Prüfung eines SHA2-Hashes über die gerätespezifischen Parameter; jede Änderung der Parameter wird mit Zeitstempel in einem Logbuch hinterlegt.		
10	MA5	Verfügbarkeit des Nachweises eines Eingriffs	Rechtlich relevante Software kann nur neue Einträge zum Logbuch hinzufügen und keine alten löschen.		
11	AN1	Existenz und Vollständigkeit der Anzeige	Integrierte Anzeige in der Ladestation mit Darstellung der Maßeinheit		
12/3	AN2 AN3	Softwareauthentizität und Darstellung der Ergebnisse Gemischte Anzeige	Eine akzeptable Lösung für Softwaretrennung wäre: Die Anzeige der rechtlich nicht relevanten Software wird von der rechtlich relevanten Software kontrolliert und als rechtlich nicht relevant gekennzeichnet.		

14	ER1	Ergonomie	Die Benutzerschnittstelle genügt den Ergonomieanforderungen der EN ISO 9241-110.		
15	LS1	Vollständigkeit der gespeicherten Messdaten	Die Daten eines Messergebnisses werden vollständig inklusive ihrer jeweiligen Einheiten gespeichert.		
16	LS2	Zufällige oder unbeabsichtigte Änderung gespeicherter Messdaten	Der übertragene Datensatz wird mit einer CRC-32-Checksumme versehen. Alternativ kann auch die Signatur gemäß DK3 genutzt werden.		
17/8	LS3 LS4	Integrität gespeicherter Messdaten Authentizität gespeicherter Messdaten	Die übertragenen Daten werden von einer kryptographischen Signatur (bspw. ECDSA mit 256 Bit Schlüssellänge gemäß BSI TR-03116-3) begleitet, die die Überprüfung der Datenintegrität und -authentizität ermöglicht.		
19	LS5	Umgang mit kryptographischem Material	Der private Schlüssel zum Erstellen der Signatur aus LS3 und LS4 ist nach Zerstörung einer eichtechnischen Sicherung auslese- oder änderbar.		
20	LS6	Abrufen gespeicherter Messdaten	Die gespeicherten Messergebnisse können über die Nutzerschnittstelle dargestellt werden.		
21	LS7	Automatisches Speichern	Die rechtlich relevante Software speichert das Messergebnis automatisch nach Abschluss der Messung ab.		
22	LS8	Speicherkapazität und -dauer	Der Speicher ist so dimensioniert, dass alle während der Eichgültigkeit der Ladestation erzeugten relevanten Daten dauerhaft aufgezeichnet werden können.		
23	DK1	Vollständigkeit übertragener Daten	Das Übertragungsprotokoll gewährleistet die Vollständigkeit der übertragenen Daten.		
24	DK2	Zufällige oder unbeabsichtigte Änderung übertragener Daten	Der übertragene Datensatz wird mit einer CRC-32-Checksumme versehen. Alternativ kann auch die Signatur gemäß DK3 genutzt werden.		
25/6	DK3 DK4	Beabsichtigte Änderung übertragener Daten Authentizität übertragener Daten	Die übertragenen Daten werden von einer kryptographischen Signatur (bspw. ECDSA mit 256 Bit Schlüssellänge gemäß BSI TR-03116-3) begleitet, die die Überprüfung der Datenintegrität und -authentizität ermöglicht.		
27	DK5	Umgang mit kryptographischem Material	Der private Schlüssel zum Erstellen der Signatur aus DK3 und DK4 ist nach Zerstörung einer eichtechnischen Sicherung auslese- oder änderbar.		
28/9	DK6 DK7	Umgang mit beschädigten übertragenen Daten Umgang mit Übertragungsverzögerungen	Verwendung von TCP zum Übertragen der Daten.		
30	DK8	Verfügbarkeit von Übertragungsdiensten	Eine Übertragung von Daten wird nur angestoßen, wenn eine Kommunikationsverbindung aufgebaut werden kann, andernfalls werden die Daten bis zur Übertragung zwischengespeichert.		
31	DK9	Empfängerseitige Prüfung von Integrität und Authentizität übertragener Daten	Die Empfänger der übertragenen Daten prüft Integrität und Authentizität der übertragenen Daten durch Verifikation der kryptographischen Signatur aus DK3.		
32	ST1	Umsetzung der Softwaretrennung	Eine akzeptable Lösung wäre:		

			Ein Teil der Software, der eindeutig von anderen Softwareteilen getrennt ist, umfasst die rechtlich relevante Software und Parameter.		
33	ST2	Rückwirkungsfreie Softwareschnittstelle	Eine akzeptable Lösung für Softwaretrennung wäre: Die Datenübergabe von der rechtlich nicht relevanten Software zur rechtlich relevanten Software erfolgt über eine rückwirkungsfreie Schnittstelle.		
34	ST3	Vollständigkeit der rückwirkungsfreien Softwareschnittstelle	Eine akzeptable Lösung für Softwaretrennung wäre: Jegliche rechtlich nicht relevante Software läuft in einer virtuellen Maschine, die von der rechtlich relevanten Software kontrolliert und überwacht wird.		
35	SD1	Download-Mechanismus	Zum Zweck einer Softwareaktualisierung existiert in der rechtlich relevanten Software ein Hilfsprogramm, das: - sich mit dem Sender synchronisiert und die Genehmigung überprüft, - automatisch das Messen während der Übertragung und Installation sperrt, - automatisch die rechtlich relevante Software auf einen sicheren Zwischenspeicher herunterlädt, - automatisch die nach SD2 bis SD4 erforderlichen Überprüfungen ausführt, - automatisch die Software an der richtigen Stelle installiert, - sich um die Verwaltung kümmert, z.B. überflüssige Dateien löscht usw., - dafür sorgt, dass jeder Schutz, der zur Erleichterung von Übertragung und Installation entfernt wurde, nach Abschluss automatisch auf das erforderliche Niveau erneuert wird, die entsprechenden Fehlerbehandlungsprozeduren einleitet, wenn ein Fehler auftritt.		
36/7	SD2 SD3	Authentifizierung der heruntergeladenen Software Integrität der heruntergeladenen Software	Die heruntergeladene Software ist kryptographisch signiert (bspw. ECDSA mit 256 Bit Schlüssellänge gemäß BSI TR-03116-3). Die Überprüfung der Signatur der heruntergeladenen Software erfolgt mittels eines Schlüssels, der im rechtlich relevanten Softwareteil des Geräts gespeichert ist. Der Abgleich der Signatur erfolgt automatisch. Der Schlüssel kann nur durch Brechen eines Siegels ausgetauscht werden.		
38	SD4	Rückverfolgbarkeit des Downloads rechtlich relevanter Software	Im Logbuch wird zumindest Datum und Zeitpunkt des Downloads, der Identifikator der heruntergeladenen rechtlich relevanten Software, der Identifikator der herunterladenden Stelle und ein Erfolgseintrag aufzeichnet. Für jeden Downloadversuch, unabhängig davon, ob dieser erfolgreich war oder nicht, wird ein Eintrag erzeugt.		