SRQ - Specification Related Question

SRQ-ID: 1158

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Erweiterung "Sicherheitsvorfälle und Notfallmaßnahmen"
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh F 6., 6.4

Stichwort: Erweiterung "Sicherheitsvorfälle und Notfallmaßnahmen"

Frage:

Welche Basisrollout - relevanten Erweiterungen im Kapitel F6 "Sicherheitsvorfälle und Notfallmaßnahmen" gibt es von der Version 2.2.0 zur Version 2.4.0 ?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

1) Das Kapitel F6 „Sicherheitsvorfälle und Notfallmaßnahmen“ wird wie folgt erweitert.

F6 - Sicherheitsvorfälle und Notfallmaßnahmen

Dieses Kapitel beschreibt eine abgestufte Hierarchie der Sicherheitsvorfälle, die Anforderung an Notfallmaßnahmen wie Schlüssellöschung, Sperrung von Zertifikaten, event-getriebener Tausch von Schlüsseln, Umstieg auf vorgesehene Ausweichverfahren.

Das BSI empfiehlt den Betreibern von kryptographischen Komponenten auf Notfälle so vorbereitet zu sein, dass im Ernstfall Maßnahmen sofort ergriffen werden können, was zu kürzeren Ausfallzeiten eines Systems führt.

Hinweis: Das BSI hält die neuen Seitenkanalangriffe für die realistischste Bedrohung von Komponenten mit langer Einsatzzeit.

Beim Einsatz des RSA-Verfahrens ist es aus wissenschaftlicher Sicht viel wahrscheinlicher, dass bestimmte, zurzeit noch nicht bekannte, RSA-Module Schwächen zeigen, als dass das Verfahren komplett gebrochen wird. Daher ist eine wirklich zufällige Wahl der RSA-Module wichtig.

Auch beim Einsatz von elliptische Kurven ist es viel wahrscheinlicher, dass bestimmte, zurzeit noch nicht bekannte, Klassen von Kurven Schwächen zeigen, als dass die Verfahren komplett gebrochen werden. Daher ist eine zufällige Wahl der Kurven mit Prüfung der Kurven und die Möglichkeit des Wechsels der Kurven wichtig.

… weiter im Text mit Abschnitt F6.1 etc. …

2) Das Kapitel F6.4 „Vorgaben zur Alarmierung bei kryptographischen Problemen“ wird erweitert und komplett ersetzt mit:

F6.4 - Vorgaben zur Alarmierung bei kryptographischen Problemen

Da immer mit Angriffen zu rechnen ist, MUSS eine wichtige Sicherheitsfunktion zumindest das Erkennen von Angriffen und Angriffsversuchen unterstützen. Mit Hilfe dieser Funktion wird die Analyse der Angriffe erleichtert. Entsprechend notwendige Alarmbehandlungen und Schadensabwehrmaßnahmen können durchgeführt werden.

Beim Auftreten bestimmter, durch die Beweissicherung erfasster Ereignisse MUSS unverzüglich Sicherheitsalarm ausgelöst und ein bestimmter Benutzer / eine bestimmte Rolle benachrichtigt werden.

Es MUSS im Sicherheitskonzept des Betreibers festgelegt sein, welche Situationen zu Alarmen führen. Für alle definierten Alarme MUSS folgendes gelten:

- Es MUSS festgelegt sein, wer für die Bearbeitung des Alarms zuständig ist.
- Es MÜSSEN Verfahren existieren um festzustellen, welcher Schaden angerichtet worden ist. Die dazu notwendigen Informationen müssen gesammelt und bereitgestellt werden.
- Es MUSS festgelegt sein, welche Notfallprozeduren und Abwehrstrategien ablaufen sollen. Insbesondere müssen die maximalen Reaktionszeiten, die Informations- und Entscheidungsprozesse festgelegt sein.
- Es MUSS mindestens dann ein Alarm ausgelöst werden, wenn Schlüssel oder PINs bei der Erzeugung, Verteilung, Speicherung oder im Betrieb kompromittiert wurden. Die gematik MUSS unverzüglich informiert werden [A_03234].

Neben den Hinweisen auf eine mögliche Kompromittierung von Schlüsseln sind alle Unregelmäßigkeiten entsprechend der Tabelle unten zu klassifizieren.
Unregelmäßigkeiten in diesem Sinne sind u. a.:

- Benutzung von nicht gültigen Schlüsseln/Zertifikaten. (D.h. der Gültigkeitsnachweis scheitert aus mindestens einem Grund)

- Häufige Benutzung von nicht gültigen Schlüsseln/Zertifikaten.
- Kryptographische Autorisierungsprotokolle scheitern
- Kryptographische Autorisierungsprotokolle scheitern häufig
- Auftauchen einer nicht plausiblen Uhrzeit/Datums
- Auftauchen von nicht verifizierbaren Signaturen
- Auftauchen von nicht entschlüsselbaren verschlüsselten Dokumenten
- Ein benutztes Kryptoverfahren ist aufgrund des zeitlichen Ablaufs nicht mehr geeignet
- Ein benutztes Kryptoverfahren ist aufgrund einer Warnung nicht mehr geeignet

Tabelle AnhF-6.4: Stufen eines Sicherheitsalarms

Security Alarm	Bezeichnung	Reaktion
0	Geringe Bedeutung	Keine Meldung, lokal lösen
1	Mitzuteilen	Meldung im Rahmen des Berichtswesens, lokal lösen.
2	Sofort mitzuteilen	Sofortige Meldung, lokal lösen.
3	Sofort mitzuteilen, Betrieb anhalten	Sofortige Meldung, lokal lösen, Wiederaufnahme erst nach Rücksprache (und ggf. weiteren Maßnahmen).
4	Sofort mitzuteilen, Betrieb anhalten, Eingriff nur nach Rücksprache	Sofortige Meldung, lokal lösen Wiederaufnahme erst nach Rücksprache, Wiederaufnahme erst nach Wiederfreigabe, ggf. Sperrung von Zertifikaten.
5	Betrieb einstellen	Sofortige Meldung, Betreib einstellen, alle Zulassungen und Zertifikate sperren