

SRQ-ID: 1160

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Anwendungssicherheit
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh G 9.1, 9.3

Stichwort: Anwendungssicherheit

Frage:

Die Anforderungen [A_03506 bis A_03509] sehen einen Genehmigungsprozess der gematik für Schutzmaßnahmen an Anwendungssassets vor. Zusätzlich müssen diese im Sicherheitskonzept des Betreibers dargelegt werden. Wann muss der Genehmigungsprozess genutzt werden und wann reichen die Darstellungen im Sicherheitskonzept?

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:			
Herstellerebefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	<input checked="" type="checkbox"/> erfasst <input checked="" type="checkbox"/> intern abgestimmt <input type="checkbox"/> extern abgestimmt <input type="checkbox"/> zurückgezogen <input checked="" type="checkbox"/> freigegeben <input type="checkbox"/> eingearbeitet in Folgeversion		

Antwort:

Durch detaillierte Angaben zur Anwendungssicherheit im Sicherheitskonzept des Betreibers und dem spezifischen Sicherheitskonzept des Dienstes, welche auf den Anforderungen des übergreifenden Sicherheitskonzepts beruhen, entfallen die Forderungen nach einem separaten Genehmigungsprozess für Schutzmaßnahmen an Anwendungssassets.

G9.1 - Anwendungssicherheit

Entsprechende Anforderung gemäß ISO/IEC 27002:2005

Diese Ziffer entspricht Ziffer 12.1 Security requirements of information systems (Sicherheitsanforderungen für IT-Systeme), Ziffer 12.2 Correct processing in applications (Ordnungsgemäße Verarbeitung innerhalb von Anwendungen) und Ziffer 12.4.3 Access control to program source (Zugriffskontrolle zur Programmquelle).

Die Sicherheit der verwendeten Programme MUSS gewährleistet und die Daten der eingesetzten Anwendungen MÜSSEN gegen den nicht autorisierten Zugriff und die nicht autorisierte Verwendung geschützt werden [A_03506] [A_54419]. ~~Hierzu MÜSSEN die folgenden Angaben der Anwendung bei der gematik erfragt werden:~~

- ~~• Informationen zum öffentlichen Zugriff für die Programme und Daten~~
- ~~• Liste der Benutzer, die zusätzlich Zugriff auf die Programme und Daten benötigen~~
- ~~• Prüfvoraussetzungen für die Programme und Daten~~

~~Ohne Einhaltung des festgelegten Genehmigungsprozesses der gematik werden keine Änderungen an den Schutzmaßnahmen für die Programme oder Daten vorgenommen [A_03507].~~

Die notwendigen Vorgaben ergeben sich aus dem Sicherheitskonzept des Betreibers, dem spezifischen Sicherheitskonzept des Dienstes und dem übergreifenden Sicherheitskonzept.

Anwendungssicherheit		
Optionale Aufgabenbereiche Verantwortungen (P = Performt, A = Assistiert)	Dienstbetreiber	gematik
Vorgabe von Sicherheitsanforderungen für Anwendungsassets, die vom Dienstanbieter übernommen werden soll [A_54421]		P
Definieren der Sicherheitsanforderungen für Anwendungsassets [A_03508] [A_54420]	P A	P
Implementieren der Sicherheitsanforderungen für Anwendungsassets mit Hilfe der Zugriffskontrollsoftware [A_03509]	P	

G9.3 – Zusammenfassung der Ausgangsanforderungen

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_03506 Ersetzt durch A_54419		S	Anwendungs_Endnutzer_Sicherheit_01: Die Sicherheit der verwendeten Programme MUSS gewährleistet sein.	<p>Die Sicherheit der verwendeten Programme MUSS gewährleistet und die Daten der eingesetzten Anwendungen MÜSSEN gegen den nicht autorisierten Zugriff und die nicht autorisierte Verwendung geschützt werden. Hierzu MÜSSEN die folgenden Angaben der Anwendung bei der gematik erfragt werden:</p> <ul style="list-style-type: none"> • Informationen zum öffentlichen Zugriff für die Programme und Daten • Liste der Benutzer, die zusätzlich Zugriff auf die Programme und Daten benötigen • Prüfvoraussetzungen für die Programme und Daten 		Anhang G 9
A_54419		S		Der Betreiber MUSS die Sicherheit der verwendeten Programme gewährleisten und die Daten der eingesetzten Anwendungen gegen nicht autorisierten Zugriff und nicht autorisierte Verwendung schützen.		Anhang G 9
A_03507		S	Anwendungs_Endnutzer_Sicherheit_02: Genehmigungsprozesses.	Ohne Einhaltung des festgelegten Genehmigungsprozesses der gematik DÜRFEN KEINE Änderungen an den Schutzmaßnahmen für die Programme oder Daten vorgenommen werden.		Anhang G 9
A_03508 Ersetzt durch		S	Anwendungs_Endnutzer_Sicherheit_03: Definieren der Sicherheitsanforderungen für	Optionaler Aufgabenbereich (Dienstbetreiber: assistiert, gematik: performt):		Anhang G 9

Afo-ID	Anfo	Art	Titel	Beschreibung	Rel.	Quelle
A_54420 A_54421			Anwendungsassets	Definieren der Sicherheitsanforderungen für Anwendungsassets		
A_54420		S		Der Anbieter MUSS die Sicherheitsanforderungen für Anwendungsassets definieren.		Anhang G 9
A_54421		S		Eine von der gematik vorgegebene Definition von Sicherheitsanforderungen für Anwendungsassets SOLL vom Dienstanbieter übernommen werden		Anhang G 9