Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller

Version:	1.1.0
Revision:	109011
Stand:	15.05.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_DS_Hersteller

Dokumentinformationen

Änderungen zur Vorversion

Die Änderung zur Vorversion ist gelb markiert.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	14.05.18		freigegeben	gematik
			Änderungsliste P18.1	
1.1.0	15.05.2019		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Das vorliegende Dokument definiert übergreifende Sicherheits- und Datenschutzanforderungen für Hersteller von Produkten der Telematikinfrastruktur (TI), für die eine Produktzulassung vorgesehen ist.

1.2 Zielgruppe

Das vorliegende Dokument richtet sich an Hersteller von Produkten der Telematikinfrastruktur, für die eine Produktzulassung vorgesehen ist.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Wichtiger Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Die Anforderungen dieses Dokumentes richten sich nicht an Anbieter betrieblicher Leistungen von Produkten der TI oder weiterer Anwendungen.

Spezifische Datenschutz- und Sicherheitsanforderungen für einzelne Produkttypen sind in den jeweiligen Spezifikationen des Produkttyps festgelegt.

Übergreifende Anforderungen an die Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur sind in [gemSpec_Krypt] festgelegt.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke angeführten Inhalte.

2 Anforderungen der Informationssicherheit an Hersteller

Dieses Dokument enthält Sicherheitsanforderungen an Produkttypen der dezentralen Zone der TI-Plattform (vgl. [gemKPT_Arch_TIP]). Bei Smartcards (z.B. eGK) sind die Anforderungen nur dem COS zugeordnet, nicht dem Objektsystem.

GS-A_2524-01 - Produktunterstützung: Nutzung des Problem-Management-Prozesses
Hersteller von dezentralen Produkten der TI MÜSSEN im Rahmen der Produktunterstützung den in den „Übergreifenden Richtlinien zum Betrieb der TI“ [gemRL_Betr_TI] fest-ge-legten Problem-Management-Prozess nutzen, um Schwachstellen an die gematik zu melden.**[<=]**

GS-A_2330-02 - Hersteller: Schwachstellen-Management
Hersteller von dezentralen Produkten der TI MÜSSEN präventive Maßnahmen zur Erkennung und Analyse von technischen Hard- oder Softwareschwachstellen („vulnerabilities“) ihres Produktes wie auch zur Bewertung und Implementierung von Sicherheitsupdates durchführen. Hierzu gehört insbesondere auch, dass sich der Hersteller aktiv und kontinuierlich über Schwachstellen in eingesetzten Hard- und Softwarekomponenten von Dritten informiert. Dies ist auch für Anteile des Produktes sicherzustellen, die von Drittherstellern stammen.**[<=]**

GS-A_2525-01 - Hersteller: Schließen von Schwachstellen
Hersteller von dezentralen Produkten der TI MÜSSEN die gematik direkt und unverzüglich über neu gemeldete Software- oder Hardware-Schwachstellen in ihren Produkten informieren und das weitere Vorgehen mit der gematik abstimmen, um die Auswirkungen unverzüglich auf das mögliche Minimum zu reduzieren und die Schwachstelle schnellstmöglich komplett zu schließen.
[<=]

GS-A_2354-01 - Produktunterstützung mit geeigneten Sicherheitstechnologien
Hersteller von dezentralen Produkten der TI MÜSSEN eine vom koordinierenden ISM freigegebene Technologie zur Wahrung der Integrität, Authentizität und (wo nötig) Vertraulichkeit der Informationen zur Produktunterstützung und Schwachstellenmeldung einsetzen.
[<=]

GS-A_2350-01 - Produktunterstützung der Hersteller
Hersteller von dezentralen Produkten der TI MÜSSEN der gematik Supportinformationen sowie Informationen zu Softwareupdates als Produktunterstützung für von ihnen entwickelte Produkte der TI zur Konsolidierung und Weiterleitung an die ISM der Beteiligten zur Verfügung stellen.
[<=]

GS-A_4944-01 - Produktentwicklung: Behebung von Sicherheitsmängeln
Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen Produkte der TI gewährleisten, dass technisch-organisatorische Verfahren zur Behebung von Sicherheitsmängeln in den Produkten während der Zeit des Einsatzes in der TI vorgehalten werden. Dies beinhaltet das kontinuierliche Aufspüren (bug tracking) und Nachbessern (bug fixing) von Sicherheitsmängeln (security bugs) und das zur Verfügung stellen von Updates (security updates).**[<=]**

Hinweis: In Anforderung GS-A_4944-01 bezeichnet die „Zeit des Einsatzes in der TI“ die Zeitspanne, für die das Produkt für die TI zugelassen ist.

GS-A_4945-01 - Produktentwicklung: Qualitätssicherung
Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen Produkte der TI gewährleisten, dass bei der Entwicklung der Produkte technisch-organisatorische Verfahren der Qualitätssicherung angewendet werden (bspw. fuzz (robustness) testing bzw. penetration testing und source code review).**[<=]**

GS-A_4946-01 - Produktentwicklung: sichere Programmierung
Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen Produkte der TI gewährleisten, dass bei der Entwicklung der Produkte Secure Coding Guidelines angewendet werden; d. h., in einschlägigen Fachkreisen anerkannte, erprobte und bewährte Regeln sicherer Programmierung befolgt wurden.**[<=]**

GS-A_4947-01 - Produktentwicklung: Schutz der Vertraulichkeit und Integrität
Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen Produkte der TI gewährleisten, dass sie in einer Entwicklungsumgebung entwickelt werden, für die technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit und Integrität der Produkte getroffen werden.**[<=]**

A_17178 - Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken
Hersteller von dezentralen Produkten der TI MÜSSEN für die von ihnen angebotenen Produkte der TI gewährleisten, dass das Produkt resistent bezüglich der im aktuellen und den beiden vorherigen OWASP Top 10 Report(s) ausgewiesenen Risiken ist.**[<=]**

Hinweis: Die Nichtanwendbarkeit eines Risikos für das Produkt ist zu begründen. Für Informationen zum Umgang mit den OWASP Top 10 Risiken wird auf den aktuellen [OWASP Top 10 Report] und die darin enthaltenen Vorgehensweisen für z. B. Entwickler und Tester verwiesen.

A_17179 - Auslieferung aktueller zusätzlicher Softwarekomponenten
Hersteller von dezentralen Produkten der TI, die zu ihrem Produkt ein Installationspaket mit zusätzlichen Softwarekomponenten ausliefern, MÜSSEN im Falle von Sicherheitsaktualisierungen dieser zusätzlichen Softwarekomponenten unverzüglich die gepatchten Softwareversionen als Aktualisierung an die Nutzer des Produktes ausliefern. **[<=]**

Hinweis: Hierunter fallen Softwarekomponenten von Dritten, die nicht von der gematik zugelassen werden und somit auch nicht Teil des Sicherheitsnachweises im Rahmen der Zulassung sind, bspw. Bibliotheken zur Laufzeitumgebung (Java-Bibliotheken etc.). Im Kontext dieser Anforderung beinhaltet „unverzüglich“ auch, dass der Hersteller sein Produkt im Zusammenhang mit den neuen Versionen der zusätzlichen Softwarekomponenten testet, bevor er diese an die Nutzer ausliefert. Ansonsten gilt, dass er die zusätzlichen Softwarekomponenten ohne schuldhaftes Zögern so schnell als möglich ausliefert. Sollte der Hersteller feststellen, dass die Sicherheitseigenschaften seines Produkts von der Aktualisierungen der zusätzlichen Softwarekomponenten beeinträchtigt sind, so muss er das Produkt erneut bei der gematik zur Zulassung einreichen – unabhängig davon, ob er sein Produkt verändert hat oder nicht.

3 Anhang A – Verzeichnisse

3.1 Abkürzungen

Kürzel	Erläuterung
ISM	Informationssicherheitsmanagement
SGB V	Sozialgesetzbuch
TI	Telematikinfrastruktur

3.2 Referenzierte Dokumente

3.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

3.2.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[OWASP Top 10 Report]	OWASP Foundation, OWASP Top Ten Project: “OWASP Top 10 The Ten Most Critical Web Application Security Risks“, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (üblicherweise im PDF Format)