Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller

Version:	1.2.0
Revision:	246940
Stand:	30.06.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_DS_Hersteller

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	14.05.18		freigegeben	gematik
1.1.0	15.05.19		Änderungsliste P18.1	gematik
1.2.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments 4
1.1 Zielsetzung 4
1.2 Zielgruppe 4
1.3 Geltungsbereich 4
1.4 Abgrenzungen 4
1.5 Methodik 5
2 Anforderungen der Informationssicherheit an Hersteller 6
2.1 Basis-Anforderungen 6
2.2 Sicherer Softwareentwicklungsprozess 8
2.3 Unterstützung von Audits 10
3 Anhang A – Verzeichnisse 12
3.1 Abkürzungen 12
3.2 Abbildungsverzeichnis 12
3.3 Referenzierte Dokumente 12
3.3.1 Dokumente der gematik 12
3.3.2 Weitere Dokumente 13

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 TI (vgl. [gemKPT_Arch_TIP]). Bei Smartcards (z.B. eGK) sind die Anforderungen nur dem COS zugeordnet, nicht dem Objektsystem.

2.1 Basis-Anforderungen

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.

2.2 Sicherer Softwareentwicklungsprozess

A_19148 - Sicherheits- und Datenschutzkonzept
Der Hersteller eines Produktes MUSS die Sicherheits- und Datenschutzmaßnahmen für sein Produkt in einem Sicherheits- und Datenschutzkonzept dokumentieren und auf Verlangen der gematik zur Verfügung stellen.**[**<=**]**

Hinweis: Das Sicherheitskonzept muss die folgenden Punkte umfassen:

- Beschreibung des Produkts bzgl. allgemeiner Informationssicherheitsaspekte,
- Sicherheitsanforderungen der gematik,
- Schutzbedarfsfeststellung,
- Bedrohungsanalyse,
- Sicherheitsanalyse (Verifikation der Wirksamkeit der Sicherheitsmaßnahmen),
- Erstellung einer Restrisikoabschätzung.

Hinweis: Das Datenschutzkonzept muss die folgenden Punkte umfassen:

- Beschreibung des Produkts bzgl. Datenschutzaspekten,
- Identifikation der Rahmenbedingungen des Datenschutzes,
- Identifikation der personenbezogenen Daten und Anwendungsprozesse,
- Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten - Datenschutz-Risiken und Datenschutz-Hinweise.

A_19147 - Sicherheitstestplan
Der Hersteller eines Produktes MUSS einen Testplan für Sicherheitstests erstellen und auf Verlangen der gematik zur Verfügung stellen.**[**<=**]**

Hinweis: Der Testplan umfasst alle Sicherheitstests während der Phasen der Produktentwicklung sowie regelmäßige Sicherheitsprüfungen (Pentest) durch unabhängige Sicherheitsexperten. Der Umfang des Testplans hängt von der Zielplattform sowie den Funktionalitäten des Produktes ab und muss zwingend das Testvorgehen zu den Sicherheitsvorgaben der gematik beinhalten.

Orientierungen zu den Inhalten eines Testplanes sind z.B. imOWASP Mobile Security Testing Guide [MSTG] und im OWASP Mobile Application Security Verification Standard [MASVS] beschrieben. Der Testplan muss einen ähnlichen Detaillierungsgrad haben wie in den beiden OWASP-Referenzen.

A_19150 - Umsetzung Sicherheitstestplan
Der Hersteller eines Produktes MUSS seinen Testplan für Sicherheitstests umsetzen und der gematik bei jeder Veröffentlichung einer neuen Produktversion einen Testbericht zur Verfügung stellen.**[**<=**]**

A_19151 - Implementierungsspezifische Sicherheitsanforderungen
Der Hersteller eines Produktes MUSS während der Entwicklung des Produktes implementierungsspezifische Sicherheitsanforderungen dokumentieren und umsetzen.**[**<=**]**

Hinweis: Der Testbericht muss zwingend Testauswertungen zu den Sicherheitsvorgaben der gematik beinhalten.

A_19152 - Verwendung eines sicheren Produktlebenszyklus

Der Hersteller eines Produktes MUSS innerhalb des Produktlebenszyklus (Entwicklung, Betrieb, Außerbetriebnahme) seines Produktes Sicherheitsaktivitäten integrieren und anwenden, d. h. in einschlägigen Fachkreisen anerkannte, erprobte und bewährte Regeln anwenden.**[<=]**

Hinweis: Ein Beispiel für Sicherheitsaktivitäten in einem Produktlebenszyklus ist der Microsoft Security Development Lifecycle. Für weitere Informationen siehe [OWASP SAMM Project] oder den durch das BSI bereitgestellten "Leitfaden zur Entwicklung sicherer Webanwendungen - Empfehlungen und Anforderungen an die Auftragnehmer" (insbesondere Kapitel 4).

A_19153 - Sicherheitsrelevanter Softwarearchitektur-Review
Der Hersteller eines Produktes MUSS einen sicherheitsrelevanten Softwarearchitektur-Review durchführen und identifizierte Architekturschwachstellen beheben.**[<=]**

A_19154 - Durchführung einer Bedrohungsanalyse
Der Hersteller eines Produktes MUSS eine Bedrohungsanalyse durchführen und Maßnahmen gegen die identifizierten Bedrohungen implementieren.**[<=]**

A_19155 - Durchführung sicherheitsrelevanter Quellcode-Reviews
Der Hersteller eines Produktes MUSS während der Entwicklung des Produktes sicherheitsrelevante Quellcode-Reviews oder automatisierte sicherheitsrelevante Quellcode-Scans durchführen.**[<=]**

A_19156 - Durchführung automatisierter Sicherheitstests
Der Hersteller eines Produkts MUSS während der Entwicklung des Produktes automatisierte Sicherheitstests durchführen.**[<=]**

A_19157 - Dokumentierter Plan zur Sicherheitsschulung für Entwickler
Der Hersteller eines Produktes MUSS einen Schulungsplan zur regelmäßigen Schulung von Entwicklern in sicherer Entwicklung und Secure-Coding-Techniken dokumentieren und umsetzen.**[<=]**

A_19158 - Sicherheitsschulung für Entwickler
Der Hersteller eines Produktes MUSS alle Entwickler des Produktes in sicherer Entwicklung und Secure-Coding-Techniken schulen.**[<=]**

A_19159 - Dokumentation des sicheren Produktlebenszyklus
Der Hersteller eines Produktes MUSS den verwendeten sicheren Produktlebenszyklus und dessen Teilprozesse dokumentieren und auf Nachfrage der gematik zur Verfügung stellen. Die Dokumentation soll mindestens die folgenden Sicherheitsaktivitäten beschreiben:

- Erfassen und Umsetzen von implementierungsspezifischen Sicherheitsanforderungen für das Produkt und von Best-Practice-Sicherheitsanforderungen,
- Durchführen von sicherheitsrelevanten Architektur- und Design-Reviews,
- Durchführen von Bedrohungsanalysen,
- Durchführen von sicherheitsrelevanten Quellcode-Reviews,
- Durchführen von Sicherheitstests während der Qualitätssicherungsphase,
- Etablieren von Quality Gates, die eine Veröffentlichung des Produkts mit 'Mittel' oder 'Hoch' bewerteten Sicherheitsfehlern verhindern,
- Änderungs- und Konfigurationsmanagement,
- Schwachstellen-Management.

[<=]

A_19160 - Änderungs- und Konfigurationsmanagementprozess
Der Hersteller eines Produktes MUSS während der Entwicklung des Produktes einen Änderungs- und Konfigurationsmanagementprozess verwenden. Das Änderungsmanagement umfasst mindestens den Entscheidungsprozess über vorgeschlagene Änderungen und die Autorisierung der Änderungen. Das Konfigurationsmanagement liefert mindestens zu jedem Zeitpunkt die eindeutige Zusammensetzung des Produktes bezüglich seiner eindeutigen Komponenten (Dritt-Software wie Bibliotheken, Frameworks) und den vorgenommenen Änderungen an eigenen Komponenten.**[<=]**

A_19161 - Verifizierung der Einhaltung sicherheitstechnische Eignung durch Datenschutzbeauftragten
Der Hersteller eines Produktes MUSS bei Veröffentlichung einer neuen Produktversion des Produktes die Einhaltung der Herstellererklärung "sicherheitstechnische Eignung" durch seinen Datenschutzbeauftragten verifizieren lassen.**[<=]**

Hinweis: Falls es keinen Datenschutzbeauftragten beim Hersteller gibt, kann eine alternative Rolle die sicherheitstechnische Eignung verifizieren, z.B. der Sicherheitsbeauftragte. Diese Rolle darf nicht an der Entwicklung des Produktes teilnehmen und muss direkt an die Geschäftsführung des Herstellers berichten.

A_19162 - Informationspflicht bei Veröffentlichung neue Produktversion
Der Hersteller eines Produktes MUSS die gematik bei Veröffentlichung einer neuen Produktversion informieren.**[<=]**

2.3 Unterstützung von Audits

A_19163 - Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes
Der Hersteller eines Produktes MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind,

- Sicherheitsprüfungen (z.B. Whitebox oder Blackbox Pentest) seines Produktes durchzuführen (hiervon unbenommen ist das Recht der gematik, eine anlasslose Sicherheitsprüfung durchzuführen),
- im Rahmen einer Sicherheitsprüfung die konkrete Umsetzung der an das Produkt gestellten Anforderungen zu überprüfen.

Der Hersteller MUSS dies im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Hersteller durch diese Mitwirkungspflichten entstehen, trägt der Hersteller selbst.**[<=]**

A_19164 - Mitwirkungspflicht bei Sicherheitsprüfung
Der Hersteller eines Produktes MUSS Sicherheitsprüfungen (z.B. Pentest) der gematik unterstützen.**[<=]**

Hinweis: Unterstützen bedeutet beispielsweise das Bereitstellen einer Release- oder Beta-Version des Produkts, das Bereitstellen eines Testsystems inkl. Test-Accounts, kleine Anpassungen des Produktes, die eine Beschleunigung des Tests ermöglichen (z.B. Entfernung von Certificate Pinning, Code Obfuscation) und Unterstützung bei Rückfragen.

A_19165 - Auditrechte der gematik zur Prüfung der Herstellerbestätigung

Der Hersteller eines Produktes MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind,

- Audits durchzuführen (hiervon unbenommen ist das Recht der gematik, anlasslose Audits durchzuführen),
- im Rahmen eines Audits beim Hersteller die konkrete Umsetzung der an den Hersteller gestellten Anforderungen zu überprüfen,
- im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Herstellers zu betreten,
- im Rahmen eines Audits alle für das Audit benötigten Informationen zur Verfügung gestellt zu bekommen und insbesondere die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu erhalten.

Der Hersteller MUSS dies im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Hersteller durch diese Mitwirkungspflichten entstehen, trägt der Hersteller selbst.**[**<=**]**

3 Anhang A – Verzeichnisse

3.1 Abkürzungen

Kürzel	Erläuterung
ISM	Informationssicherheitsmanagement
SGB V	Sozialgesetzbuch
TI	Telematikinfrastruktur

3.2 Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

3.3 Referenzierte Dokumente

3.3.1 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

3.3.2 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)