Einführung der Gesundheitskarte

Spezifikation Datenschutz- und Sicherheitsanforderungen an Hersteller

|  |  |
| --- | --- |
| Version: | 1.0.0 CC |
| Revision: | \main\rel\_ors2\2 |
| Stand: | 14.08.2017 |
| Status: | zur Abstimmung freigegeben |
| Klassifizierung: | vertraulich\_LA |
| Referenzierung: | gemSpec\_Datenschutz\_Sicherheit\_Hersteller |

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
| --- | --- | --- | --- | --- |
| 1.0.0 CC | 14.08.17 |  | Initiale Erstellung | gematik |
|  |  |  |  |  |
|  |  |  |  |  |

Inhaltsverzeichnis

[1 Einordnung des Dokuments 4](#_Toc501701459)

[1.1 Zielsetzung 4](#_Toc501701460)

[1.2 Zielgruppe 4](#_Toc501701461)

[1.3 Geltungsbereich 4](#_Toc501701462)

[1.4 Abgrenzungen 4](#_Toc501701463)

[1.5 Methodik 5](#_Toc501701464)

[2 Module der Informationssicherheit 6](#_Toc501701465)

[2.1 Modul „Hersteller dezentraler Produkte“ 7](#_Toc501701466)

[2.2 Modul „Referenz- und Testumgebung“ 8](#_Toc501701467)

[3 Anhang A – Verzeichnisse 10](#_Toc501701468)

[3.1 A1 – Abkürzungen 10](#_Toc501701469)

[3.2 A2 – Abbildungsverzeichnis 10](#_Toc501701470)

[3.3 A3 – Referenzierte Dokumente 10](#_Toc501701471)

[3.3.1 A3.1 – Dokumente der gematik 10](#_Toc501701472)

# Einordnung des Dokuments

## Zielsetzung

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

## Zielgruppe

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

## 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.

## 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.

## Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern 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:

**⌦ gemxxxxxx\_AFO\_0000 <Titel der Afo>**

Text/Beschreibung

**⌫**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

# 

# Module der Informationssicherheit

Dieses Dokument enthält, wie eingangs erwähnt, Datenschutz- und Sicherheitsanforderungen an Hersteller von Produkten der Telematikinfrastruktur, für die eine Produktzulassung vorgesehen ist. Diese Anforderungen sind in Module aufgeteilt. Jede Anforderung gehört somit zu genau einem Modul. Die Module werden anschließend Herstellern zugeordnet (siehe auch Abbildung 1). Ist ein Modul einem Hersteller zugeordnet, muss dieser alle Anforderungen des jeweiligen Moduls umsetzen.

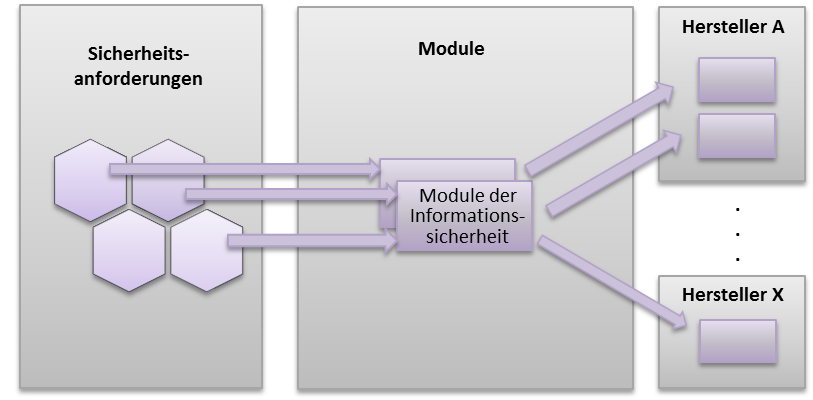


Abbildung – Anforderungen, Module und Hersteller

Abbildung 2 zeigt die Module für Hersteller im Überblick. Das Modul „Hersteller dezentraler Produkte“ ist nur für Hersteller von dezentralen Produkten der TI relevant. Das Modul „Referenz- und Testumgebung“ hingegen ist von allen Herstellen von Produkten der TI (dezentral und zentral) umzusetzen.

Die Anforderungen dieser Module sind in den Abschnitten 2.1 und 2.2 beschrieben.

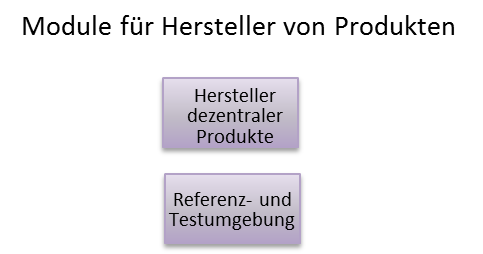


Abbildung – Modulübersicht für Herstellermodule

## Modul „Hersteller dezentraler Produkte“

Die Anforderungen dieses Moduls sind von Herstellern dezentraler Produkte der TI (z. B. Konnektoren) umzusetzen.

⌦ GS-A\_2524 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] fest­ge­legten Problem-Management-Prozess nutzen, um Schwachstellen an die gematik zu melden.

**⌫**

⌦ GS-A\_2330\_2 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 Hersteller: Schließen von Software-Schwachstellen

Hersteller von dezentralen Produkten der TI MÜSSEN die gematik direkt und unverzüglich über neu ge­mel­dete Software-Schwachstellen in ihren Produkten informieren und unverzüglich, spätestens jedoch innerhalb von 45 Tagen nach der initialen Meldung, einen Antrag auf Zulassung bzw. Erteilung einer befristeten Genehmigung gemäß § 291b Abs. 1a Satz 11 SGB V unter Beistellung der neuen Version der Software bei der Zulassungsstelle der gematik einreichen, sofern im Einzelfall keine andere Absprache mit der gematik erfolgt.

**⌫**

⌦ GS-A\_2525\_2 Hersteller: Schließen von Hardware-Schwachstellen

Hersteller von dezentralen Produkten der TI MÜSSEN die gematik direkt und unverzüglich über neu ge­mel­dete Hardware-Schwachstellen in ihren Produkten informieren und unverzüglich nach der initialen Meldung einen Antrag auf Zulassung bzw. Erteilung einer befristeten Genehmigung gemäß § 291b Abs. 1a Satz 11 SGB V unter Beistellung der neuen Version der Hardware bei der Zulassungsstelle der gematik einreichen.

**⌫**

⌦ GS-A\_2354 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 Produktunterstützung der Hersteller

Hersteller von dezentralen Produkten der TI MÜSSEN der gematik Supportinfor­mationen, Sicherheitswarnungen 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 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).

**⌫**

⌦ GS-A\_4945 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 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 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.

**⌫**

## Modul „Referenz- und Testumgebung“

Alle Produkte der TI müssen im Rahmen der Produktzulassung in der Referenz- und Testumgebung der Telematikinfrastruktur getestet werden. Dieses Modul wird daher jedem Hersteller eines Produktes der TI zugeordnet.

**⌦ GS-A\_**2157 **Keine Echtdaten in Referenz- und Testumgebungen**

Der Hersteller, der sein Produkt an die Referenz- oder Testumgebung der Telematikinfrastruktur anbindet, MUSS sicherstellen, dass im angeschlossenen Produkt keine Echtdaten verarbeitet werden.

**⌫**

**⌦ GS-A\_2162 Kryptographisches Material in Entwicklungs- und Testumgebungen**

Der Hersteller, der sein Produkt an die Referenz- oder Testumgebung der Telematikinfrastruktur anbindet, MUSS sicherstellen, dass in seinem angeschlossenem Produkt keine kryptographischen Identitäten bzw. Schlüssel der Produktivumgebung der TI (Umgebungen mit Echtdaten) genutzt werden.

**⌫**

# 

# Anhang A – Verzeichnisse

## A1 – Abkürzungen

| **Kürzel** | **Erläuterung** |
| --- | --- |
| ISM | Informationssicherheitsmanagement |
| SGB V | Sozialgesetzbuch |
| TI | Telematikinfrastruktur |

## A2 – Abbildungsverzeichnis

[Abbildung 1 – Anforderungen, Module und Hersteller 6](#_Toc490485003)

[Abbildung 2 – Modulübersicht für Herstellermodule 6](#_Toc490485004)

## A3 – Referenzierte Dokumente

### A3.1 – 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: Einführung der Gesundheitskarte -  Glossar |
| [gemRL\_Betr\_TI] | gematik: Übergreifende Richtlinien zum Betrieb der TI |
| [gemSpec\_Krypt] | gematik: Verwendung kryptographischer Algorithmen in der  Telematikinfrastruktur |