gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI

Version:	1.4.0
Revision:	\main\rel_online\rel_ors1\rel_opb1\8
Stand:	24.08.2016
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_SiBetrUmg]

Dokumentinformationen

Änderungen zur Vorversion

Überarbeitung der Dokumente für den Online-Produktivbetrieb (Stufe 1), als Grundlage für Produktivzulassungen und den bundesweiten Rollout.

Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
	05.09.08		Vorversion Anhang G des übergreifenden Sicherheitskonzeptes (Version 2.4.0)	gematik
	17.11.09	3.3.2	Umsetzung SRQ 1044	gematik
	20.02.10		Auflösen der Tabellen und Einarbeitung neuer Afo-Id für bestehende (und noch nicht gemeldete) Anforderungen; Auflösen von Stapel-Anforderungen; Übernahme neuer Anforderungen für die spezifischen Sicherheits-Konzepte	gematik
	01.03.12	C	Übernahme Kap. 7.6 aus üSiKo v2.4.0	gematik
0.9.0	15.05.12		Einarbeitung der Kommentare	gematik
0.10.0	07.09.12		Anpassungen und Aktualisierungen	gematik
1.0.0	15.10.12		freigegeben	gematik
1.1.0	12.11.12		Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	gematik
1.1.9	22.04.13		zur Abstimmung freigegeben	gematik
1.2.0	06.06.13		Einarbeitung Kommentare LA	gematik
1.3.0	21.02.14		Losübergreifende Synchronisation	gematik
1.3.9	18.12.15		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
1.4.0	24.08.16		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung und Einordnung des Dokuments

Die vorliegende übergreifende Spezifikation definiert Anforderungen für den Themenbereich Sicherheitsanforderungen an die Betriebsumgebung von Anbietern von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten, die bei der Realisierung (bzw. dem Betrieb) von Produkttypen der TI zu beachten sind. Diese Anforderungen sind als übergreifende Regelungen relevant für Interoperabilität und Verfahrenssicherheit.

1.2 Zielgruppe

Das Dokument richtet sich an Anbieter von Produkten der TI.

1.3 Geltungsbereich

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

Die vorliegende *Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI* [gemSpec_SiBetrUmg] ist insbesondere für Test, Zulassung und Betrieb von zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten relevant.

Für Zertifizierungsdiensteanbieter (ZDAs) gelten die hier gestellten Anforderungen nur, sofern sie Dienstleistungen für die TI erbringen, die nicht unter das deutsche Signaturgesetz fallen. Das gilt auch, wenn sich aus der Schnittstelle zur TI besondere Anforderungen an die Sicherheit ergeben, die von den Aufsichtsmaßnahmen der Bundesnetzagentur nicht erfasst sind.

Schutzrechts-/Patentrechtshinweis:

Das vorliegende Sicherheitskonzept 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 übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzung

Nicht Bestandteil des vorliegenden Dokumentes ist die Dokumentation der Implementierung der Sicherheitsanforderungen dieses Dokuments. Dies erfolgt in betreiberspezifischen Sicherheitskonzepten, die gemäß Anhang B durch die verantwortlichen Anbieter zu erstellen sind.

1.5 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:

⌦ **GS-A_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Sicherheitsanforderungen Betrieb

Für Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten wird davon ausgegangen, dass diese ihre Betriebsumgebung so ausgestalten, dass Informationsobjekte und Anwendungsprozesse mit einem Schutzbedarf von „mittel" ohne zusätzliche Sicherheitsmaßnahmen verarbeitet werden können. Grundlage dieser Annahme ist ein Betrieb, in dem

- die in dieser Spezifikation [gemSpec_SiBetrUmg] getroffenen Anforderungen und
- die an das „ISM der Beteiligten“ gestellten Anforderungen aus [gemSpec_ISM] und [gemSpec_Sich_DS]

erfüllt sind.

GS-A_4980 Umsetzung der Norm ISO/IEC 27001

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN für genau die Umgebungen, in denen diese Produkte betrieben werden, die internationale Norm ISO/IEC 27001 umsetzen.

GS-A_4981 Erreichen der Ziele der Norm ISO/IEC 27001 Annex A

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN für genau die Umgebungen, in denen diese Produkte betrieben werden, zu allen gemäß der Erklärung der Anwendbarkeit (engl. „Statement of Applicability“) anwendbaren Maßnahmen (engl. „controls“) der internationalen Norm ISO/IEC 27001 ergreifen und die dort angegebenen Ziele (engl. „objectives“) erreichen.

GS-A_4982 Umsetzung der Maßnahmen der Norm ISO/IEC 27002

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten SOLLEN für genau die Umgebungen, in denen diese Produkte betrieben werden, bei Ergreifung der Maßnahmen (engl. „controls“) aus der internationalen Norm ISO/IEC 27002 die dort angegebene „Anleitung zur Umsetzung“ (engl. „implementation guidance“) und die dort angegebenen "Weiteren Informationen" (engl. „other information“) befolgen.

GS-A_4983 Umsetzung der Maßnahmen aus dem BSI-Grundschutz

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten SOLLEN für genau die Umgebungen, in denen diese Produkte betrieben werden, bei der Umsetzung der internationalen Normen ISO/IEC 27001 und ISO/IEC 27002 die zugehörigen Maßnahmen des BSI-Grundschutzkatalogs umsetzen (vgl. Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz des BSI).

GS-A_4984 Befolgen von herstellerspezifischen Vorgaben

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten SOLLEN für genau die Umgebungen, in denen diese Produkte betrieben werden, herstellerspezifische Sicherheitsvorgaben und -empfehlungen befolgen.⌫

GS-A_3784 Nachweis durch ISO27001 Zertifikat

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten KÖNNEN zum Nachweis der Umsetzung der Anforderungen an die Betriebsumgebung ihre Dienste und das ISM der Beteiligten eine ISO 27001-Zertifizierung mit einem Geltungsbereich, der den betriebenen Dienst und die unterstützenden Systeme umfasst, durchführen. ⌫

Für die Umsetzung dieser Anforderungen ist der Anbieter des jeweiligen Dienstes verantwortlich. Dabei wird nicht unterschieden, ob diese Umsetzung durch einen zugelassenen oder durch die gematik beauftragten Anbieter erfolgt.

Der Nachweis über die Umsetzung dieser Anforderungen erfolgt durch Erstellung eines betreiberspezifischen Sicherheitskonzeptes (siehe Anhang B).

GS-A_3719 Vorgaben an das Sicherheitskonzept des Betreibers

Der Anbieter MUSS zur Einhaltung der organisatorischen Sicherheitsanforderungen die Vorgaben der gematik an das betreiberspezifische Sicherheitskonzept erfüllen. ⌫

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
ISO	International Organization for Standardization
TI	Telematikinfrastruktur
VMM	Virtual Machine Monitor
VPN	Virtual Private Network

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

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 entnehmen Sie bitte der aktuellsten, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemSpec_ISM]	gematik: Koordinierendes Informationssicherheitsmanagement der Telematikinfrastruktur
[gemSpec_Sich_DS]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen
[gemMeth_Bedr]	gematik: Einheitliche Methoden der Informationssicherheit – Bedrohungs- und Schwachstellenanalyse in der Telematikinfrastruktur
[gemMeth_Risk]	gematik: Methode zur Risikoanalyse

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemMeth_Schlüssel]	gematik: Methode zur Schlüsseldokumentation
[gemMeth_Schutzbed]	gematik: Methode der Schutzbedarfsfeststellung
[gemMeth_SichAnalyse]	gematik: Methode der Sicherheitsanalyse

A3.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI 100-4]	BSI-Standardreihe zur Informationssicherheit: 100-4 Notfallmanagement Version 1.0 (2008) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf
[ISO/IEC27001]	ISO/IEC 27001:2005 Specification for an Information Security Management System, ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
[ISO/IEC27002]	ISO/IEC 27002:2005 Code of Practice for Information Security Management ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt

Anhang B – Betreiberspezifische Sicherheitskonzepte

B1 - Vorgaben für betreiberspezifische Sicherheitskonzepte

B1.1 – Abgrenzung

Unter dem „Betreiberspezifischen Sicherheitskonzept“ wird das Sicherheitskonzept des zugelassenen oder durch die gematik beauftragten Anbieters eines zentralen Dienstes oder eines fachanwendungsspezifischen Dienste der Telematikinfrastruktur verstanden.

Die Vorgaben gelten nur für Anbieter, die von der gematik beauftragt und geprüft oder von der gematik zugelassen werden (siehe auch Kapitel B3).

B1.2 - Inhaltsübersicht

⌦ **GS-A_3737 Spezifisches Sicherheitskonzept: Mindestumfang des spezifischen Sicherheitskonzeptes..**

Der Anbieter MUSS ein betreiberspezifisches Sicherheitskonzept erstellen, das die folgenden Inhalte umfasst:

- Beschreibung des Dienstes
- Schutzbedarf der Daten (gemäß [gemMeth_Schutzbed] oder äquivalente Methode)
- Bedrohungsanalyse (gemäß [gemMeth_Bedr] oder äquivalente Methode)
- Dokumentation der Erfüllung der Sicherheitsanforderungen der gematik
- Besondere technische Komponenten
- Schlüssel- und Zertifikatsmanagement (gemäß [gemMeth_Schlüssel] oder äquivalente Methode)
- Wirksamkeit der Sicherheitsmaßnahmen (gemäß [gemMeth_SichAnalyse] oder äquivalente Methode)
- Erstellung einer Restrisikoabschätzung (gemäß [gemMeth_Risk] oder äquivalente Methode)
- Erstellung eines Notfallkonzepts.⌫

Konkrete Anforderungen zu einzelnen Inhalten werden in den nachfolgenden Abschnitten erläutert.

Dem Anbieter ist es freigestellt, das Sicherheitskonzept um weitere Inhalte zu ergänzen, sofern er dies für seinen Betrieb als vorteilhaft ansieht. Der Anbieter muss dieses Sicherheitskonzept fortschreiben.

Der Anbieter muss den RFC 2119 (Begriffsbestimmungen zu MUSS, DARF, SOLL, KANN, etc.) berücksichtigen.

B1.3 - Schutzbedarf der Daten

Neben den durch die gematik vordefinierten Informationsobjekten müssen dienstspezifisch weitere Informationsobjekte identifiziert werden, die in dem betreiberspezifischen Sicherheitskonzept zu berücksichtigen sind.

B1.4 - Sicherheitsanforderungen der gematik

Für Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten wird davon ausgegangen, dass diese ihre Betriebsumgebung so ausgestalten, dass Informationsobjekte und Anwendungsprozesse mit einem Schutzbedarf von „mittel" verarbeitet werden können. Grundlage dieser Annahme ist ein Betrieb, in dem

- die in dieser Spezifikation [gemSpec_SiBetrUmg] getroffenen Anforderungen und
- die an das „ISM der Beteiligten“ gestellten Anforderungen [gemSpec_ISM] [gemSpec_Sich_DS]

erfüllt sind.

Innerhalb der spezifischen Sicherheitskonzepte der Fachanwendungen und der TI-Plattform wurde eine Bedrohungs- und Risikoanalyse für die Telematikinfrastruktur vorgenommen. Ausgehend von dieser Bedrohungs- und Risikoanalyse wurden weitere Sicherheitsanforderungen abgeleitet, die durch den Anbieter einzuhalten sind. Diese Sicherheitsanforderungen sind in den jeweiligen Spezifikationen der Fachanwendungen bzw. der TI-Plattform enthalten.

B1.5 - Besondere technische Komponenten

Für ausgewählte Aufgaben muss der Anbieter technische Komponenten einsetzen, deren Sicherheit überprüft wurde. Im Einzelnen handelt es sich dabei beispielsweise um

- die VPN-Konzentratoren,
- die Firewalls,
- die Hardware-Sicherheitsmodule zum Schutz kryptographischer Schlüssel,
- die technischen Komponenten, die besonders sicherheitsrelevante Vorgänge der einzelnen Dienste umsetzen (z. B. die Signaturprüfung und Anonymisierung durch einen fachanwendungsspezifischen Intermediär).

Die Anforderungen an die VPN-Konzentratoren und an die technischen Komponenten, die besonders sicherheitsrelevante Vorgänge der einzelnen Dienste umsetzen, sind in den Sicherheitsanforderungen der entsprechenden Dienste bzw. Netze enthalten.

⌦ **GS-A_3747 Technische_Komponenten: Dokumentation der technischen Komponenten und der geforderten Sicherheitsfunktionalität.**

Der Anbieter MUSS bei der Beschreibung der technischen Komponenten die folgenden Punkte behandeln:

- Übersicht über die eingesetzten Produkte, welche die oben genannte Sicherheitsfunktionalität umsetzen
- Nachweis der Sicherheitsüberprüfungen dieser Produkte gemäß den Anforderungen der gematik.

Sofern die Sicherheitsbegutachtungen, z. B. Evaluierung nach Common Criteria (CC), besondere Anforderungen an die Einsatzumgebungen stellen, hat der Anbieter zu erläutern, wie er diese Anforderungen umgesetzt hat. ⌫

B1.6 - Erstellung eines Notfallkonzepts

⌦ **GS-A_3753 Notfallkonzept: Der Dienstanbieter muss ein Notfallkonzept erstellen**

Der Anbieter MUSS ein Notfallkonzept erstellen. Das Notfallkonzept MUSS mindestens die folgenden Punkte umfassen:

- Übergeordnete Notfallstrategie
- Gesetzliche und vertragliche Anforderungen
- Rollen und Verantwortliche in Bezug auf das Notfall-Management
- Dokumentation zur Notfallvorsorge
- Verhalten in Notfällen
- Spezielle Notfälle wie Brand, Einbruch, Wasser, Stromausfall, etc.
- Nachbereitung von Notfällen
- Prävention und Vorbeugung, insbesondere Fachkunde und Schulungen ⌫

⌦ **GS-A_3772 Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen**

Der Anbieter SOLL für sein Notfallkonzept der Gliederung und den inhaltlichen Vorgaben des Dokuments BSI-Standard 100-4 „Notfallmanagement" [BSI 100-4] folgen. ⌫

B2 - Dokumentation der Implementierungen von Maßnahmen durch den Anbieter

⌦ **GS-A_3756 Umsetzung_Maßnahmen_spezifisches_Siko: Umsetzung und Prüfbarkeit von Maßnahmen**

Der Anbieter MUSS eine detaillierte, korrekte, prüfbare und aktuelle Dokumentation der Implementierungen der Maßnahmen des betreiberspezifischen Sicherheitskonzeptes erstellen. ⌫

B3 - Sicherheitsgutachten zu Betreiberkonzepten

GS-A_3760 Gutachten zur Einhaltung der Sicherheitsanforderungen für Dienstbetreiber

Anbieter, deren betreiberspezifisches Sicherheitskonzept nicht von der gematik geprüft wird, MÜSSEN ein von einem bestellten Dritten erstelltes Gutachten vorlegen, das die Einhaltung der Vorgaben für betreiberspezifische Sicherheitskonzepte durch den Anbieter bestätigt.