

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter

Version:	2.0.0 CC
Revision:	1099523
Stand:	14.01.2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_DS_Anbieter_neu

Dokumentinformationen

Änderungen zur Vorversion

Komplette Überarbeitung in Kombination mit dem neu erstellten TI Security Standard.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
	10.07.2024		Komplettüberarbeitung zum Review	gematik
	03.11.2024		Einarbeitung Industriekommentare	gematik
2.0.0 CC	14.01.2025		Kommentierung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	4
1.1 Zielsetzung.....	4
1.2 Geltungsbereich.....	4
1.3 Abgrenzung des Dokuments.....	4
1.4 Methodik.....	5
2 Zusammenwirken von Spezifikation und TI Security Standard... 	6
2.1 Methodik zur Anpassung und Umsetzung des TI Security Standards.....	6
2.1.1 Bedarfsfeststellung.....	7
2.1.2 Formulieren neuer Controls.....	7
2.1.3 Abstimmung von Controls, Kritikalität und Komplexität.....	7
2.1.4 Finalisierung und Veröffentlichung.....	7
2.1.5 Änderungsbescheid zur Zulassung mit Auflagen.....	7
2.1.6 Umsetzung durch Industrie.....	8
2.1.7 Überwachung der Einhaltung der Controls.....	8
3 Sicherheitsanforderungen.....	9
4 Anhang A - Verzeichnisse.....	11
4.1 A1 - Abkürzungen.....	11
4.2 A2 - Tabellenverzeichnis.....	11
4.3 A3 - Abbildungsverzeichnis.....	11
4.4 Referenzierte Dokumente.....	11
4.4.1 Dokumente der gematik.....	11
4.4.2 Weitere Dokumente.....	12

1 Einordnung des Dokuments

1.1 Zielsetzung

Dieses Dokument definiert übergreifende Sicherheits- und Datenschutzanforderungen für Anbieter, die auf Basis einer Beauftragung der gematik GmbH (im Folgenden nur gematik genannt), einer Zulassung oder einer Bestätigung Dienste der Telematikinfrastruktur (TI) operativ betreiben und somit verantworten.

Diese Sicherheits- und Datenschutzanforderungen bilden somit die Basis für die Security Governance der gematik auf Basis ihres gesetzlichen Auftrages.

1.2 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. gemPTV_ATV_Festlegungen, 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.

1.3 Abgrenzung des Dokuments

Die in dieser Spezifikation enthaltenen Anforderungen sind bewusst allgemein beschrieben und konzentrieren sich darauf, die allgemeinen Pflichten des Anbieters - also „was ist zu erfüllen“- zu beschreiben. Die konkrete Umsetzung – „wie und in welcher Güte ist es zu erfüllen und gegenüber der gematik nachzuweisen“- wird im **begleitenden „TI Security Standard“ [gemTI_SEC_Standard]** beschrieben, der in regelmäßigen Abständen durch die gematik veröffentlicht wird.

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

Dieses Dokument enthält keine Anforderungen an Hersteller von Produkten der Telematikinfrastruktur. Diese sind in [gemSpec_DS_Hersteller] festgelegt.

1.4 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 innerhalb der Textmarken angeführten Inhalte.

2 Zusammenwirken von Spezifikation und TI Security Standard

Diese Spezifikation [gemSpec_DS_Anbieter_neu] dient dazu, grundsätzliche Anforderungen zur Informationssicherheit und zum Datenschutz vorzugeben. Wie unter 1.3- Abgrenzung des Dokuments ausgeführt, erfolgt die weitere Ausgestaltung im TI Security Standard [gemTI_SEC_Standard], wobei sowohl die Spezifikation als auch der TI Security Standard verbindliche Vorgaben für beauftragte, zugelassene sowie bestätigte Anbieter von Diensten der TI machen.

Im Rahmen der Spezifikation [gemSpec_DS_Anbieter_neu] werden (wie in allen Spezifikationen der gematik üblich) Anforderungen erhoben, die über den Zulassungsprozess bzw. bei Beauftragungen geprüft und abgenommen werden. Im Rahmen des TI Security Standards wird zur sprachlichen Abgrenzung bewusst von Controls gesprochen, da diese nicht in den Produkt- und Anbietertypsteckbriefen verankert sind und im Rahmen der Zulassung nur indirekt überprüft bzw. bei Beauftragungen abgenommen werden.

2.1 Methodik zur Anpassung und Umsetzung des TI Security Standards

Die Spezifikation folgt den grundsätzlichen Zulassungsprozessen der gematik und bildet den generellen Rahmen. Ziel ist es, eine hohe Konstanz der Spezifikationen zu erreichen, wohingegen der TI Security Standard regelmäßig (jährlich) sowie bei kurzfristigen erkannten Bedarfen überarbeitet, um neue Controls ergänzt und in einer neuen Version veröffentlicht wird. Hierdurch sollen eine hohe Flexibilität und schnelle Reaktion auf Basis von Erkenntnissen im operativen Betrieb der Telematikinfrastruktur sichergestellt werden. Auf der anderen Seite ist auch dem Wunsch der Industriepartner Rechnung zu tragen, die sich Planbarkeit hinsichtlich zukünftiger Aufwände durch die Umsetzung neuer Sicherheitsanforderungen wünschen.

Aus diesem Grund wird der nachfolgend beschriebene Prozess etabliert, der eine enge partnerschaftliche Zusammenarbeit bei der Integration neuer Controls im TI Security Standard vorsieht.

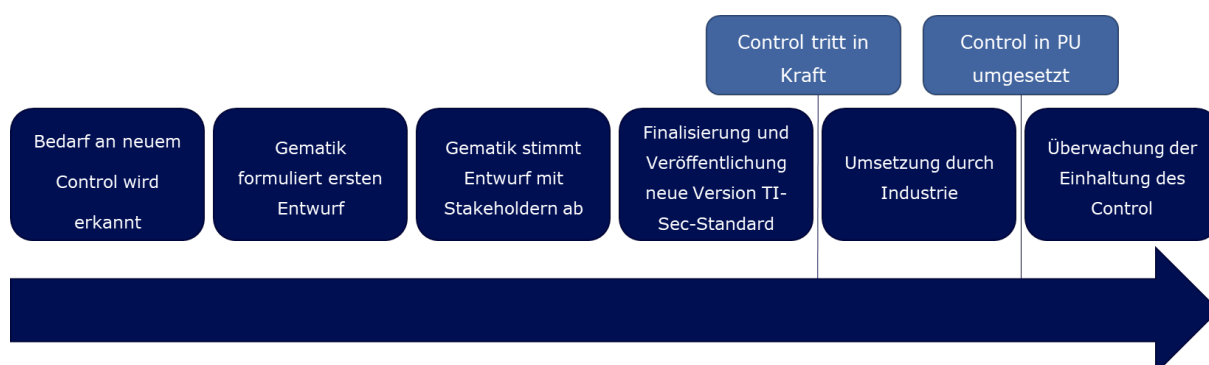


Abbildung 1: Integration neuer Controls

2.1.1 Bedarfsfeststellung

In der ersten Phase wird der Bedarf an einem neuen Control erkannt. Diese kann z. B. auf Basis von Erkenntnissen in der operativen Zusammenarbeit (z. B. Findings aus Audits oder Sicherheitsanalysen) oder neuer Bedrohungen und Angriffsvektoren ermittelt werden. In dieser Phase kann bereits ein erstes Feedback der Industriepartner einbezogen werden.

2.1.2 Formulieren neuer Controls

Auf Basis des Bedarfs und ggf. des Feedbacks von Industriepartnern wird ein erster Entwurf des neuen Controls formuliert. Neben dem Control-Text werden im TI Security Standard auch weitere Metadaten initial hinzugefügt.

2.1.3 Abstimmung von Controls, Kritikalität und Komplexität

Die gematik stimmt diesen Entwurf mit Industriepartnern ab. Dies kann entweder schriftlich per E-Mail im Umlaufverfahren, im Rahmen von persönlichen Gesprächen (Sec-Calls) oder im Rahmen des Arbeitskreises Datenschutz und Informationssicherheit (AK DIS) erfolgen. Industriepartner erhalten von der gematik eine Frist zur Stellungnahme. Neben dem Wortlaut des Controls wird auch ein Feedback zu Komplexität und Kritikalität der Umsetzung erwartet.

2.1.4 Finalisierung und Veröffentlichung

Im Anschluss wertet die gematik die Stellungnahmen der Anbieter aus und finalisiert auf Basis des Feedbacks den Control-Text sowie den Umsetzungszeitpunkt. Die Veröffentlichung erfolgt im Rahmen einer neuen Version des TI Security Standards, die anschließend durch die gematik veröffentlicht wird. Die gematik informiert alle Industriepartner über die Veröffentlichung der neuen Version. Im Regelfall sollte zwischen der Aufforderung zur Abstimmung eines neuen Controls und der Finalisierung und Veröffentlichung des Controls ein Zeitraum von nicht mehr als 6 Monaten vergehen.

2.1.5 Änderungsbescheid zur Zulassung mit Auflagen

Nach der Finalisierung und Veröffentlichung der finalen Version werden die Industriepartner im Rahmen der Anbieterzulassung über eine Auflage oder eine Vertragsänderung im Rahmen des Zulassungsvertrages verpflichtet, die aktuellen Vorgaben des TI Security Standards innerhalb einer zu definierenden, angemessenen Frist umzusetzen. Zur Berechnung der Frist wird die nachfolgende Matrix angewandt:

Komplexität	Sehr hoch	3	4	5	5	Umsetzungszeitraum
	Hoch	3	4	4	5	
	Mittel	2	2	4	4	
	Gering	1	2	3	3	
		Sehr hoch	hoch	mittel	niedrig	
Kritikalität						

1	1 Monat
2	1 Quartal
3	1 Halbjahr
4	1 Jahr
5	2 Jahre

Abbildung 2: Berechnung Umsetzungszeitraum

2.1.6 Umsetzung durch Industrie

Im Anschluss setzt die Industrie die neu hinzugekommenen oder veränderten Controls in Abhängigkeit der definierten Umsetzungsfrist um.

2.1.7 Überwachung der Einhaltung der Controls

Anbieter sind verpflichtet, die Umsetzung der Controls in der Produktivumgebung der TI gegenüber der gematik anzuzeigen. Die Anzeige kann u. a. durch die initiale Übermittlung eines geforderten Nachweises erfolgen. Viele der Controls sind so gestellt, dass sie regelmäßig wiederkehrende Nachweise gegenüber der gematik erfordern. Die Nachweise sind unaufgefordert der gematik fristgerecht bereitzustellen. Eine fehlende, unzureichende oder zeitlich verzögerte Zulieferung wirkt sich negativ auf die Bewertung der Sicherheitsleistung des Anbieters aus.

3 Sicherheitsanforderungen

GS-A_5554 - Aufrechterhaltung der Informationssicherheit

Der Anbieter MUSS Prozesse zur Gewährleistung der Informationssicherheit aufbauen und kontinuierlich verbessern. [≤]

GS-A_4980-02 - Umsetzung der Norm ISO/IEC 27001

Der Anbieter MUSS für mindestens genau die Umgebungen, in denen die Dienste der TI betrieben werden, die internationale Norm ISO/IEC 27001 umsetzen.

[≤]

GS-A_4981-01 - Erreichen der Ziele der Norm ISO/IEC 27001 Annex A

Der Anbieter MUSS für mindestens genau die Umgebungen, in denen die Dienste der TI, RZ-Consumer, der Fachdienste VSDM bzw. die weiteren Anwendungen 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_4982-01 - Umsetzung der Maßnahmen der Norm ISO/IEC 27002

Der Anbieter SOLL für mindestens genau die Umgebungen, in denen die Dienste der TI, RZ-Consumer, der Fachdienste VSDM bzw. die weiteren Anwendungen betrieben werden, beim Ergreifen 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_4983-01 - Umsetzung der Maßnahmen aus dem BSI-Grundschrift

Der Anbieter SOLL für mindestens genau die Umgebungen, in denen die Dienste der TI, der RZ-Consumer, die Fachdienste VSDM bzw. die weiteren Anwendungen betrieben werden, bei der Umsetzung der internationalen Normen ISO/IEC 27001 und ISO/IEC 27002 die anwendbaren Anforderungen des BSI-Grundschriftkompendiums oder entsprechende Maßnahmen, die ein vergleichbares Sicherheitsniveau gewährleisten, umsetzen. [≤]

Hinweis:

Der Anbieter muss aufgrund der Anforderung GS-A_4983-01 neben der nativen ISO 27001-Vorgehensweise nicht die Grundschriftvorgehensweise (BSI Standard 200-X) umsetzen. Eine zusätzliche Dokumentation ist aufgrund der Anforderung nicht erforderlich. Das BSI-Grundschriftkompendium beschreibt zu erreichende Sicherheitsanforderungen detaillierter als die Normen ISO 27001 und ISO 27002. Hierdurch soll eine gemeinsame Baseline anhand des BSI-Grundschriftkompendiums über das erforderliche Sicherheitsniveau und die Angemessenheit von Maßnahmen erlangt werden. Beispielsweise wird es einem Sicherheitsgutachter hierdurch erleichtert, die Angemessenheit von getroffenen Sicherheitsmaßnahmen besser einzuschätzen.

GS-A_2076-01 - kDSM: Datenschutzmanagement nach BSI

Der Anbieter MUSS ein Datenschutzmanagement nach Baustein CON.2 des IT-Grundschriftkompendiums umsetzen. [≤]

GS-A_5626 - kDSM: Auftragsverarbeitung

Falls ein Anbieter als Auftragsverarbeiter i. S. des Art. 4 Nr. 8 DSGVO tätig ist, MUSS dieser mit dem Auftraggeber als Verantwortlichen i. S. des Art. 4 Nr. 7 DSGVO verbindlich

regeln, wie die Pflichten des Anbieters gegenüber der gematik, die sich aus den Sicherheits- und Datenschutzanforderungen der gematik ergeben, erfüllt werden. [≤]

Hinweis: Die Ausgestaltung der Regelung obliegt den Vertragsparteien der Auftragsverarbeitung.

A_27098 - Verpflichtung zur Umsetzung des TI Security Standards

Der Anbieter MUSS die im TI Security Standard festgelegten betrieblichen Pflichten in Abhängigkeit der ihm zugewiesenen Security Governance Stufe umsetzen.

[≤]

A_27099 - Audits und Sicherheitsanalysen

Der Anbieter MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt ist, Audits und Sicherheitsanalysen (z. B. Penetrationstests) nach vorheriger Ankündigung durchzuführen und diese aktiv zu unterstützen.

[≤]

GS-A_5551-01 - Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR oder der Schweiz

Der Anbieter MUSS sicherstellen, dass die Verarbeitung personenbezogener sowie personenbezogener medizinischer Daten in einer von ihm angebotenen Komponente bzw. einem von ihm angebotenen Dienst der TI ausschließlich im Inland, in einem Mitgliedstaat der EU bzw. des EWR oder der Schweiz erfolgt. [≤]

4 Anhang A - Verzeichnisse

4.1 A1 - Abkürzungen

Kürzel	Erläuterung
DS	Datenschutz
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
kDSM	koordinierendes Datenschutzmanagementsystem
TI	Telematikinfrastruktur

4.2 A2 - Tabellenverzeichnis

Abbildung 1: Integration neuer Controls.....	6
Abbildung 2: Berechnung Umsetzungszeitraum	8

4.3 A3 - Abbildungsverzeichnis

Abbildung 1: Integration neuer Controls.....	6
Abbildung 2: Berechnung Umsetzungszeitraum	8

4.4 Referenzierte Dokumente

4.4.1 Dokumente der gematik

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemTI_SEC_Standard]	TI Security Standard - Mitwirkungspflichten für Anbieter

4.4.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO/IEC 27001]	ISO/IEC Third edition 2022-10 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[ISO/IEC 27002]	ISO/IEC 2022 Third edition 2022-02 Information security, cybersecurity and privacy protection — Information security controls