

Elektronische Gesundheitskarte und Telematikinfrastruktur

Signaturrichtlinie QES

Notfalldaten-Management (NFDM)

Version: 1.4.0
Revision:
Stand: 28.06.2019
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemRL_QES_NFDM

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
1.1.0	02.08.17		freigegeben	gematik
1.2.0	26.10.18		Einarbeitung P15.9	gematik
1.3.0	15.05.19		Einarbeitung P18.1, Disclaimer entfernt, VDG ist bereits in Kraft	gematik
			Einarbeitung Änderungsliste P19.1	
1.4.0	28.06.19		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen	2
Inhaltsverzeichnis	3
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 Überblick	6
3 Signaturrichtlinie SR_DF_NFDM_NOTFALLDATEN	7
3.1 Gültigkeitsbereich	7
3.2 Typkonformität	7
3.3 Profilierung der Schnittstelle SignDocument	8
3.4 Profilierung der Schnittstelle VerifyDocument	9
Anhang A – Verzeichnisse	11
A1 – Abkürzungen	11
A2 – Glossar	11
A3 – Tabellenverzeichnis	11
A4 – Referenzierte Dokumente	11
A4.1 – Dokumente der gematik	11

1 Einordnung des Dokuments

1.1 Zielsetzung

Die vorliegende Signaturrichtlinie definiert normative Regeln zur Signaturerstellung und Signaturprüfung für Notfalldatensätze. Zudem werden Parameter festgelegt, die für die Signaturerstellung bzw. für die Signaturprüfung notwendig sind, insoweit diese Festlegungen nicht schon in der Konnektorspezifikation oder in XML-Schema-Dateien des Notfalldaten-Managements (NFDM) getroffen werden.

1.2 Zielgruppe

Das Dokument ist für die Anbieter und Hersteller des Konnektors des Vorhabens „Online-Rollout (Stufe 2)“ relevant.

1.3 Geltungsbereich

Die durch die Signaturrichtlinie getroffenen Festlegungen werden durch Referenzierung aus normativen Anforderungen (des Konnektors) normativ. Auf diesem Weg entstehen Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens für den Online-Rollout (Stufe 2). 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

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Erstellen und Überprüfen von qualifizierten elektronischen Signaturen auf NFD, die bereits in der Konnektor-Spezifikation getroffen werden.

1.5 Methodik

Dieses Dokument enthält keine Anforderungen. Normativ wird sein Inhalt durch Referenzierung aus Anforderungen des Konnektors.

Hinweise zur Nomenklatur:

Schnittstellen-, Operations-, Parameter- und Dateinamen, Extensible-Markup-Language(XML)-Elemente oder -Attribute, Namen der referenzierten Technischen Use Cases (TUCs) des Konnektors sowie Bezeichner von Signaturrichtlinien, Dokumentenformaten, XML-Namensräumen und Uniform Resource Identifier (URI) werden in diesem Dokument in nicht-proportionaler Schriftart gesetzt.

2 Überblick

Der Konnektor ermöglicht die Erstellung und Prüfung qualifizierter elektronischer Signaturen (QES).

[gemSpec_Kon] beschreibt die Anforderungen der Signaturerstellung und -Prüfung auf dem Konnektor abschließend und legt dabei fest, dass bestimmte Dokumentenformate sicher gemäß speziell für diese Dokumentenformate festgeschriebener Signaturrichtlinien verarbeitet werden.

Das Dokumentenformat, dessen Signaturerstellung und -prüfung durch diese Signaturrichtlinie festgelegt wird, ist das XML-Dokumentenformat des Notfalldatensatzes, welches in [gemSpec_InfoNFDM#3.3] spezifiziert wird. Es wird hier mit dem Bezeichner: `DF_NFDM_NOTFALLDATEN` referenziert. Die zugehörige Signaturrichtlinie wird im folgenden Kapitel definiert und ist unter dem Bezeichner `SR_DF_NFDM_NOTFALLDATEN` referenzierbar. Über diese Referenz wird sie in Anforderungen in [gemSpec_FM_NFDM] normativ verankert.

Die Signaturrichtlinie `SR_DF_NFDM_NOTFALLDATEN` führt aus, unter welchen Eingangsbedingungen der Konnektor eine QES für einen Notfalldatensatz erzeugt, sicher anzeigt und prüft. Dabei werden fachanwendungsspezifische Anforderungen des NFDM gezielt für Notfalldatensätze in der SAK umgesetzt.

Die Festlegungen der Signaturrichtlinie `SR_DF_NFDM_NOTFALLDATEN` zum Aufruf der Operationen `SignDocument` und `VerifyDocument` sind von aufrufenden Systemen zusätzlich zu den allgemeinen Festlegungen der Schnittstellen in [gemSpec_Kon] zu beachten.

3 Signaturrichtlinie SR_DF_NFDM_NOTFALLDATEN

Die Signaturrichtlinie SR_DF_NFDM_NOTFALLDATEN zum Dokumentenformat DF_NFDM_NOTFALLDATEN wird im Folgenden definiert.

3.1 Gültigkeitsbereich

Die Signaturrichtlinie SR_DF_NFDM_NOTFALLDATEN wird für Aufrufe der Operation `SignDocument` bei den in Tabelle 1 angegebenen Parametern im Kontext einer QES-Signatur wirksam. Für `VerifyDocument` oder beim Aufruf von TUC_KON_151 „QES Dokumentensignatur prüfen“ wird sie wirksam, wenn in der Signatur die in Tabelle 1 angegebene URI eingebettet ist. Die Signaturrichtlinie erlaubt eine detached XAdES-Signatur, die innerhalb des Dokuments eingebettet ist.

Tabelle 1: TAB_01_SR_DF_NFDM_NOTFALLDATEN - Elemente zur Steuerung der Signaturrichtlinie

XML-Element oder XML-Attribut	URI Signaturrichtlinie
<p>für <code>SignDocument</code>:</p> <p><code>/SIG:SignDocument/SIG:SignRequest/SIG:OptionalInputs/sp:GenerateUnderSignaturePolicy/sp:SignaturePolicyIdentifier</code></p> <p>für <code>VerifyDocument</code>:</p> <p><code>ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SignaturePolicyIdentifier/xades:SignaturePolicyIdentifier/xades:SigPolicyId/xades:Identifier</code></p>	<p><code>urn:gematik:fa:sak:nfdm:rl:v1</code></p>

3.2 Typkonformität

Das Dokument muss XML-Schema-valide zum Schema in Tabelle 2 sein.

Tabelle 2: TAB_02_SR_DF_NFDM_NOTFALLDATEN - XML-Schemata

Datei (Pfad und Name)	targetNamespace
<code>/fa/nfds/NFD_Document.xsd</code>	<code>http://ws.gematik.de/fa/nfds/NFD_Document/v1.3</code>

Die erlaubten Root-Elemente des Dokuments sind durch Tabelle 3 definiert.

Tabelle 3: TAB_03_SR_DF_NFDm_NOTFALLDATEN - Erlaubte Root-Elemente

URI Signaturrichtlinie	Namespace	Element
urn:gematik:fa:sak:nfdm:rl:v2	http://ws.gematik.de/fa/nfds/NFD_Document/v1.3	NFD_Document

3.3 Profilierung der Schnittstelle SignDocument

Der Konnektor muss bei Aufrufen der Operation `SignDocument` eine Parameterprüfung durchführen, in der die Konformität der Parameter gemäß Tabelle 4 geprüft wird. Bei der Prüfung wird auf abweichende Werte sowie auf fehlende Elemente mit einem Fehler reagiert. Im Schnittstellenaufbau vorhandene optionale Elemente, die nicht in der Tabelle aufgeführt sind, werden ignoriert, d. h., bei der Bearbeitung des Aufrufs so behandelt, als ob sie im Aufruf nicht gesetzt wären.

Tabelle 4: TAB_06_SR_DF_NFDm_NOTFALLDATEN – Constraints SignDocument

XML-Element oder –Attribut (XPath)	Wert	Kardinalität
/SIG:SignDocument/SIG:Crypt	Keine Einschränkung	0
/SIG:SignDocument/SIG:SignRequest/SIG:Document/@ID	Platzhalter für Dokumentbezeichner NFD_DOC_ID	1
/SIG:SignDocument/SIG:SignRequest/SIG:Document/@RefURI	Der Wert muss übereinstimmen mit dem Wert des Attributes ID des Elementes NFD:Notfalldaten	1
/SIG:SignDocument/SIG:SignRequest/SIG:Document/@ShortText	keine Einschränkung	1
/SIG:SignDocument/SIG:SignRequest/SIG:Document/dss:Base64XML	keine Einschränkung	1
/SIG:SignDocument/SIG:SignRequest/SIG:OptionalInputs		1
/SIG:SignDocument/SIG:SignRequest/SIG:OptionalInputs/SIG:SignatureType	"urn:ietf:rfc:3275"	1
/SIG:SignDocument/SIG:SignRequest/SIG:OptionalInputs/dss:SignaturePlacement		1
/SIG:SignDocument/SIG:SignRequest/SIG:OptionalInputs/dss:SignaturePlacement/@WhichDocument	NFD_DOC_ID	1
/SIG:SignDocument/SIG:SignRequest/SIG:OptionalInputs/dss:SignaturePlacement/@CreateEnvelopedSignature	false	1
/SIG:SignDocument/SIG:SignRequest		1

XML-Element oder –Attribut (XPath)	Wert	Kardinalität
/SIG:OptionalInputs/dss:SignaturePlacement /XPathFirstChildOf	"/*[local-name()='NFD_Document']/*[local-name()='SignatureArzt']"	
/SIG:SignDocument/SIG:SignRequest /SIG:OptionalInputs/ sp:GenerateUnderSignaturePolicy/sp:SignaturePolicyIdentifier	"urn:gematik:fa:sak:nfdm:r1:v1"	1
/SIG:SignDocument/SIG:SignRequest /SIG:IncludeRevocationInfo	true	1
/SIG:SignDocument/SIG:TxMode	keine Einschränkung Der Parameter wird im Konnektor nicht ausgewertet.	1
/SIG:SignDocument/SIG:JobNumber	Keine Einschränkung	1

3.4 Profilierung der Schnittstelle VerifyDocument

Der Konnektor muss bei Aufrufen der Operation VerifyDocument eine Parameterprüfung durchführen, in der die Konformität der Parameter gemäß Tabelle 5 geprüft wird. Bei der Prüfung wird auf abweichende Werte sowie auf fehlende Elemente mit einem Fehler reagiert. Im Schnittstellenaufbau vorhandene optionale Elemente, die nicht in der Tabelle aufgeführt sind, werden ignoriert d. h. bei der Bearbeitung des Aufrufs so behandelt, als ob sie im Aufruf nicht gesetzt wären.

Tabelle 5: TAB_07_SR_DF_NFDm_NOTFALLDATEN – Constraints VerifyDocument

XML-Element oder –Attribut (XPath)	Wert	Kardinalität
/SIG:VerifyDocument/SIG:Document		1
/SIG:VerifyDocument/SIG:Document /@ID	Platzhalter für Dokumentbezeichner NFD_DOC_ID	1
/SIG:VerifyDocument/SIG:Document/CON N:Base64XML	keine Einschränkung	1
/SIG:VerifyDocument/SIG:Document/@ShortText	keine Einschränkung	1
/SIG:VerifyDocument/dss:SignatureObject/ds:SignaturePtr		1

/SIG:VerifyDocument/dss:SignatureObject/ds:SignaturePtr/@WhichDocument	NFD_DOC_ID	1
/SIG:VerifyDocument/dss:SignatureObject/ds:SignaturePtr/@XPath	"/*[local-name()='NFD_Document']/*[local-name()='SignatureArzt']/*[local-name()='Signature']"	1
/SIG:VerifyDocument/SIG:OptionalInputs/vr:ReturnVerificationReport	keine Einschränkung	0-1
/SIG:VerifyDocument/SIG:OptionalInputs/SIG:UseVerificationTime	keine Einschränkung	0-1
/SIG:VerifyDocument/SIG:TvMode	keine Einschränkung Der Parameter wird im Konnektor nicht ausgewertet.	1

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
NFD	Notfalldatensatz
NFDM	Notfalldaten-Management
QES	Qualifizierte elektronische Signatur
SAK	Signaturanwendungskomponente
TUC	Technischer Use Case
URI	Uniform Resource Identifier
XML	Extensible Markup Language

A2 – Glossar

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

A3 – Tabellenverzeichnis

Tabelle 1: TAB_01_SR_DF_NFDM_NOTFALLDATEN - Elemente zur Steuerung der Signaturrichtlinie.....	7
Tabelle 2: TAB_02_SR_DF_NFDM_NOTFALLDATEN - XML-Schemata	7
Tabelle 3: TAB_03_SR_DF_NFDM_NOTFALLDATEN - Erlaubte Root-Elemente.....	8
Tabelle 4: TAB_06_SR_DF_NFDM_NOTFALLDATEN – Constraints SignDocument	8
Tabelle 5: TAB_07_SR_DF_NFDM_NOTFALLDATEN – Constraints VerifyDocument	9

A4 – Referenzierte Dokumente

A4.1 – 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
[gemSpec_InfoNFDM]	gematik: Informationsmodell Notfalldaten-Management (NFDM)
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_FM_NFDM]	gematik: Spezifikation Fachmodul NFDM