

	DIN EN IEC 63173-2 (VDE 0878-173-2)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 47.020.70

Einsprüche bis 2020-12-09

Entwurf

**Navigations- und Funkkommunikationsgeräte und -systeme für die Seeschifffahrt –
Digitale Schnittstellen –
Teil 2: Sicherer Austausch und Kommunikation von S-100-basierten Produkten (SECOM)
(IEC 80/956/CD:2020);
Text Deutsch und Englisch**

Maritime navigation and radiocommunication equipment and systems –
Data interface –

Part 2: Secure exchange and communication of S-100 based products (SECOM)
(IEC 80/956/CD:2020);
Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-10-09 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 164 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Nationales Vorwort

Das internationale Dokument IEC 80/956/CD:2020-02 "Maritime navigation and radiocommunication equipment and systems – Data interface – Part 2: Secure exchange and communication of S-100 based products (SECOM)" (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom IEC/TC 80 "Maritime navigation and radiocommunication equipment and systems" der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und unterliegt dem Copyright der IEC . Das Dokument wurde den nationalen Komitees zur Stellungnahme vorgelegt.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf FprEN nur 6 Wochen beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine "JA/NEIN"-Entscheidung möglich ist, wobei eine "NEIN"-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/K 738 "Elektronische Navigationsinstrumente" der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Inhalt

Seite

EINLEITUNG	8
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe und Abkürzungen	9
3.1 Begriffe	10
3.2 Abkürzungen	12
4 Allgemeine Beschreibung	12
5 SECOM-Dienstschnittstelle	15
5.1 Allgemeines	15
5.2 Dienstdefinitionsmodell	15
5.3 Diensttechnologie	16
5.4 Definition der Dienstschnittstellen	16
5.4.1 Allgemeines	16
5.4.2 Paginierung	17
5.4.3 Filterung	17
5.4.4 Dienstschnittstelle – Upload (Hochladen)	17
5.4.5 Dienstschnittstelle – Upload Link (Verknüpfung hochladen)	21
5.4.6 Dienstschnittstelle – Acknowledgement (Quittierung)	23
5.4.7 Dienstschnittstelle – Get (Anfordern)	26
5.4.8 Dienstschnittstelle – Get Summary (Zusammenfassung anfordern)	29
5.4.9 Dienstschnittstelle – Subscription (Subskription)	33
5.4.10 Dienstschnittstelle – Remove Subscription (Subskription entfernen)	35
5.4.11 Dienstschnittstelle – Get Subscription List (Subskriptionsliste anfordern)	37
5.4.12 Dienstschnittstelle – Subscription Notification (Subskriptionsbenachrichtigung)	38
5.4.13 Dienstschnittstelle – Request Access (Zugriff anfordern)	40
5.4.14 Dienstschnittstelle – Access Notification (Zugriffsbenachrichtigung)	42
5.4.15 Dienstschnittstelle – Capability (Funktionalität)	44
5.4.16 Dienstschnittstelle – Description (Beschreibung)	46
5.4.17 Dienstschnittstelle – Status	48
5.4.18 Dienstschnittstelle – EncryptionKey (kryptografischer Schlüssel)	49
6 SECOM-Kommunikationskanalsicherheit	51
6.1 Allgemeines	51
6.2 Sichere Übertragung	51
6.2.1 Sicherer Kommunikationskanal	51
6.2.2 Authentifizierungsverfahren	52
7 SECOM-Datenschutz	52
7.1 Allgemeines	52
7.2 Teilnehmer am Schutzkonzept	52
7.3 Datenkompression und -paketierung	53
7.4 SECOM-PKI	53
7.4.1 Allgemeines	53
7.4.2 Management von öffentlichen und privaten Schlüsseln	53
7.4.3 Zertifikatsstatusprüfung	53
7.5 Datenauthentifizierung und -signierung	54
7.5.1 Datenformate und Standards für digitale Signaturen, Schlüssel und Zertifikate	54
7.5.2 Prüfmethode und erwartetes Ergebnis	54

7.6	Datenverschlüsselung	54
7.6.1	Allgemeines	54
7.6.2	Verschlüsselungsalgorithmus.....	55
7.6.3	Erstellung und Übertragung des geheimen Schlüssels	55
7.6.4	Prüfmethode und erwartetes Ergebnis.....	57
8	SECOM-Service Discoverability	57
8.1	Allgemeines	57
8.2	Dienst auffinden.....	57
8.2.1	Allgemeines	57
8.2.2	Suchparameter	57
8.2.3	Content im Ergebnis	57
8.2.4	Dienstschnittstelle – Dienst suchen.....	57
	Anhang A (normativ) REST-Dienst-Swagger	61
A.1	Zweck	61
A.2	SECOM-Dienstschnittstelle mit spezifischem Datentyp verknüpfen	61
A.3	Dienstkombination	61
A.4	Technische Auslegung des Dienstes S-421 nach REST	61
	Anhang B (informativ) Anwendungsfälle und Anforderungen	62
B.1	Zweck	62
B.2	Anwendungsfälle und Dienstschnittstellenprofile	62
B.2.1	UC-1 Schiff teilt Routenplan mit Dienst, der erweiterte Überwachung anbietet	62
B.2.2	UC-2 Erweiterter Überwachungsdienst fordert Routenplan vom/für das Schiff zur Überwachung an	63
B.2.3	UC-3 Dienst ohne Zugriffsberechtigung auf Daten	64
B.2.4	UC-4 Abfrage von Dienstfunktionalitäten über die Konsumentenschnittstelle.....	65
	Anhang C (informativ) Nachverfolgbarkeit des S-100-Dienstmodells	66
C.1	Zweck	66
C.2	Spezifikation der Dienstschnittstelle	66
C.3	Technische Auslegung des Dienstes nach REST	66
	Anhang D (informativ) Austauschmuster für Nachrichten	67
D.1	Zweck	67
D.2	Austauschmuster für Nachrichten	67
D.2.1.1	Austauschmuster für Nachrichten	67
D.2.1.2	Dienstorchestrierung	70
	Anhang E (informativ) Implementierungsleitfaden.....	72
E.1	Zweck	72
E.2	Schiffsseite	73
E.3	Landseite	74
	Anhang F (informativ) Verwendung der Positivliste.....	75
F.1	Zweck	75
F.2	Positivliste.....	75
Bilder		
Bild 1	— Beziehung zwischen den Spezifikationen von Maritimen Diensten, Technischen Diensten und Datenmodellen in e-Navigation	13
Bild 2	— Übersicht über SECOM.....	13
Bild 3	— „Upload“-Schnittstelle in UML	18
Bild 4	21	
Bild 5	— REST-Schnittstelle „Acknowledgement“	24

Bild 6 — REST-Schnittstelle „Get“	27
Bild 7 30	
Bild 8 — REST-Schnittstelle „Subscribe“	33
Bild 9 — REST-Schnittstelle „Remove Subscription“	35
Bild 10 — REST-Schnittstelle „Get Subscription List“	37
Bild 11 — REST-Schnittstelle „Subscription Notification“	39
Bild 12 — REST-Schnittstelle „Request Access“	41
Bild 13 — REST-Schnittstelle „Access Notification“	43
Bild 14 — REST-Schnittstelle „Capability“	45
Bild 15 — REST-Schnittstelle „Description“	47
Bild 16 48	
Bild 17 50	
Bild 18 — Prinzip der gegenseitigen Authentifizierung	52
Bild 19 — Interaktionsbeispiel für den Austausch klassifizierter Daten	56
Bild A.1 — Zwei Beispiele für Dienstkompositionen	61
Bild D.20 — Austauschmuster für Nachrichten - ONE_WAY	67
Bild D.21 — Austauschmuster für Nachrichten - REQUEST_CALLBACK	68
Bild D.22 — Austauschmuster für Nachrichten - REQUEST_RESPONSE	68
Bild D.23 — Austauschmuster für Nachrichten - PUBLISH_SUBSCRIBE (Benennung durch den Produzenten)	69
Bild D.24 — Austauschmuster für Nachrichten - PUBLISH_SUBSCRIBE (Anforderung durch den Konsumenten)	70
Bild D.25 — PUBLISH_SUBSCRIBE unter Verwendung von Informationen zur Anforderung	71
Bild E.1 — Überblick über SECOM	72
Bild E.2 — Überblick über die Zertifikatsverwendung	73
Bild E.3 — Deployment-Beispiel für SECOM auf dem Schiff	74
Bild E.4 — Deployment-Beispiel für SECOM an Land	74

Tabellen

Tabelle 1 — Überblick über die Dienstschnittstellen	16
Tabelle 2 — Informationsaustausch für die „Upload“-Schnittstelle	18
Tabelle 3 — REST-Implementierung der „Upload“-Schnittstelle	19
Tabelle 4 — Datenaustauschmodell für die REST-Implementierung der „Upload“-Schnittstelle	19
Tabelle 5 — HTTP-Antwortcodes und Nachricht im Antwort-Objekt	20
Tabelle 6 — Informationsaustausch für die „Upload Link“-Schnittstelle	21
Tabelle 7 — REST-Implementierung der „Upload Link“-Schnittstelle	22
Tabelle 8 — Datenaustauschmodell für die REST-Implementierung der „Upload Link“-Schnittstelle	22
Tabelle 9 — HTTP-Antwortcodes und Nachricht im Antwort-Objekt	23
Tabelle 10 — Informationsaustausch für die „Quittierung“-Schnittstelle	24
Tabelle 11 — REST-Implementierung der „Acknowledgement“-Schnittstelle	25
Tabelle 12 — Datenaustauschmodell für die REST-Operation „Acknowledgement“	25
Tabelle 13 — HTTP-Antwortcodes und Antwortnachricht	25
Tabelle 14 — Informationsaustausch für die „Get“-Schnittstelle	26
Tabelle 15 — REST-Implementierung der „Get“-Schnittstelle	27
Tabelle 16 — Aufzählung für AreaName	28
Tabelle 17 — Datenaustauschmodell für die REST-Operation „Get“	29
Tabelle 18 — HTTP-Antwortcodes	29
Tabelle 19 — Informationsaustausch für die „Get Summary“-Schnittstelle	30
Tabelle 20 — REST-Implementierung der „Get Summary“-Schnittstelle	31

Tabelle 21 — Datenaustauschmodell für die REST-Operation „Get Summary“	32
Tabelle 22 — HTTP-Antwortcodes und Nachrichten.....	32
Tabelle 23 — Informationsaustausch für die „Subscription“-Schnittstelle	33
Tabelle 24 — REST-Implementierung der „Subscription“-Schnittstelle	34
Tabelle 25 — Datenaustauschmodell für die REST-Operation „Subscription“	34
Tabelle 26 — HTTP-Antwortcodes und Nachrichten.....	35
Tabelle 27 — Parameterbindung für „Remove Subscription“	35
Tabelle 28 — REST-Implementierung der „Remove Subscription“-Schnittstelle	36
Tabelle 29 — Datenaustauschmodell für die REST-Operation „Delete Subscription“	36
Tabelle 30 — HTTP-Antwortcodes und Nachrichten.....	36
Tabelle 31 — Informationsaustausch für die „Get Subscription List“-Schnittstelle	37
Tabelle 32 — REST-Implementierung der „Get Subscription List“-Schnittstelle	38
Tabelle 33 — Datenaustauschmodell für die REST-Operation „Get Subscription List“	38
Tabelle 34 — HTTP-Antwortcodes	38
Tabelle 35 — Informationsaustausch für die „Subscription Notification“-Schnittstelle	39
Tabelle 36 — Operation – POST <Datentyp>/subscription/notification	39
Tabelle 37 — Datenaustauschmodell für die REST-Operation „Subscription Notification“	40
Tabelle 38 — HTTP-Antwortcodes	40
Tabelle 39 — Informationsaustausch für die „Request Access“-Schnittstelle	40
Tabelle 40 — Parameterbindung für die Operation	41
Tabelle 41 — Datenaustauschmodell für die REST-Operation „Request Access“	42
Tabelle 42 — HTTP-Antwortcodes	42
Tabelle 43 — Informationsaustausch für die „Access Notification“-Schnittstelle	42
Tabelle 44 — Parameterbindung für die Operation	43
Tabelle 45 — Datenaustauschmodell für die REST-Operation „Access Notification“	44
Tabelle 46 — HTTP-Antwortcodes	44
Tabelle 47 — Informationsaustausch für die „Capability“-Schnittstelle	44
Tabelle 48 — REST-Implementierung der „Capability“-Schnittstelle	45
Tabelle 49 — Datenaustauschmodell für die REST-Operation „Capability“	46
Tabelle 50 — HTTP-Antwortcodes und Nachrichten.....	46
Tabelle 51 — Informationsaustausch für die „Description“-Schnittstelle	47
Tabelle 52 — REST-Implementierung der „Description“-Schnittstelle	47
Tabelle 53 — Datenaustauschmodell für die REST-Operation „Description“	48
Tabelle 54 — HTTP-Antwortcodes	48
Tabelle 55 — Informationsaustausch für die „Status“-Schnittstelle.....	48
Tabelle 56 — REST-Implementierung der „Status“-Schnittstelle	49
Tabelle 57 — Datenaustauschmodell für die REST-Operation „Description“	49
Tabelle 58 — HTTP-Antwortcodes	49
Tabelle 59 — Informationsaustausch für die „EncryptionKey“-Schnittstelle.....	50
Tabelle 60 — REST-Implementierung der „EncryptionKey“-Schnittstelle	50
Tabelle 61 — Datenaustauschmodell für die REST- Implementierung der „EncryptionKey“- Schnittstelle	50
Tabelle 62 — HTTP-Antwortcodes	51
Tabelle 63 — Erstellung von Schlüsselpaaren aus öffentlichem und privatem Schlüssel – grundlegende Befehle	53
Tabelle 64 — Beispiel für Befehle	57
Tabelle 65 — Parameterbindung für die Operation „Dienst suchen“	58
Tabelle 66 — Parameterbindung für die REST-Operation „Get Service“	58

Tabelle 67 — Datenaustauschmodell für die REST-Operation.....	58
Tabelle 68 — Suchparameter.....	59
Tabelle 69 — HTTP-Antwortcodes.....	60
Tabelle A.1 — Datentypen in REST-Operationen.....	61
Tabelle B.1 — Erforderliche Dienstschnittstellen in UC-1.....	63
Tabelle B.2 — Erforderliche Dienstschnittstellen in UC-2.....	64
Tabelle B.3 — Erforderliche Dienstschnittstellen in UC-3.....	64
Tabelle B.4 — Erforderliche Dienstschnittstellen in UC-4.....	65

EINLEITUNG

Die Internationale Seeschiffahrtsorganisation (en: International Maritime Organization, IMO) hat zur harmonisierten Bereitstellung elektronischer Informationen die Initiative „E-Navigation“ ins Leben gerufen, die den Einsatz festgelegter maritimer Dienste vorsieht. Im Strategischen Implementierungsplan (SIP) der IMO zur E-Navigation-Initiative wird die Erwartung an die IEC formuliert, die im SIP umrissenen Einzelheiten umzusetzen.

Bei den maritimen Diensten handelt es sich um operationelle Dienste sowohl für landseitige als auch für bordseitige Akteure, welche wiederum auf technische Dienste angewiesen sind, die digitalisierte Informationen bereitstellen. Die Datenformate sind typischerweise in Datenmodellspezifikationen genormt, und viele Organisationen sind mit der Erarbeitung neuer Normen beschäftigt, z. B. innerhalb des Rahmenwerks S-100 der Internationalen Hydrografischen Organisation (International Hydrographic Organization, IHO) auf Grundlage des universellen hydrografischen Datenmodells (en: Universal Hydrographic Data Model, UHDM).

Eine Spezifikationsvorlage für technische Dienste ist in den Richtlinien zur Dokumentation von Diensten (en: Service Documentation Guidelines) des Internationalen Verbands der Seezeichenverwaltungen (en: Association of Marine Aids to Navigation and Lighthouse Authorities, IALA) enthalten (IALA G1128) sowie ein Bestandteil des S-100, Ed. 4, Part 14 der IHO. Dieses IEC-Dokument legt eine Dienstschnittstelle fest, die auf die Nutzung genormter Datenformate und die Implementierung der Vorlagen und Richtlinien von IALA und IHO für Informationsdienste abzielt. Die Standardisierung einer gemeinsamen Dienstschnittstelle für den Austausch S-100-basierter Produkte wird eine breitere technische Interoperabilität ermöglichen, bei der dieselbe Dienstschnittstelle für den Informationsaustausch ungeachtet der operationellen Verwendung genutzt werden kann.

Dementsprechend besteht der Zweck des Dokuments darin:

- den genormten Informationsaustausch des S-100-basierten Teils von maritimen Diensten, z. B. Routenpläne, Seekarten-Aktualisierungen und nautische Warnmeldungen, zu erleichtern;
- die Interoperabilität zwischen maritimen IT-Systemen zu erleichtern;
- die Notwendigkeit der Unterstützung unterschiedlicher (proprietärer) Dienstausslegungen zu verringern;
- die Vorteile der serviceorientierten Architektur zu nutzen, z. B. um es Schiffssystemen zu ermöglichen, beim ersten Ruf in einen bestimmten Hafen mit den Hafensystemen zu interagieren.

Navigations- und Funkkommunikationsgeräte und -systeme für die Seeschifffahrt — Digitale Schnittstellen — Teil 2: Sicherer Austausch und Kommunikation von S-100-basierten Produkten (SECOM)

1 Anwendungsbereich

Der Anwendungsbereich von SECOM umfasst Dienstschnittstellen für den Datenaustausch und Datenschutz, um die sichere Kommunikation von hauptsächlich S-100-basierten Produkten zu ermöglichen, und eine Schnittstelle für die Auffindbarkeit von Diensten (Service Discoverability). Dieses Dokument ergänzt S-100 zur Erreichung der technischen Interoperabilität bis zu der Ebene, auf der Informationen sicher online ausgetauscht werden können.

Die SECOM-Dienstschnittstelle besteht aus Spezifikationen und Definitionen einer Reihe von Schnittstellen, d. h. APIs. Die Dienstschnittstelle schließt die öffentliche Seite mit Zugang zum Internet ein. Die Verknüpfungen der „letzten Meile“ zwischen der SECOM-Dienstinstanz und der Endbenutzeranwendung sind in einem informativen [Anhang B](#) beschrieben. Dies ermöglicht unterschiedliche Lösungen zwischen dem Dienst und dem System/den Anwendungen an Land bzw. an Bord.

Der SECOM-Datenschutz enthält ein Schutzkonzept für den Informationsaustausch in Sinne von S-100 der IHO. Der Anwendungsbereich des Datenschutzes bezieht sich auf die Kommunikation zwischen Endbenutzern.

Die Service-Discoverability-Schnittstelle beinhaltet Methoden zur Auffindbarkeit/Erkennbarkeit von Diensten und unterstützt die dynamische Nutzung der lose gekoppelten Dienste.

SECOM ist hauptsächlich auf IP-basierte, sitzungslose (en: session-less) interaktive Webdienste für den Informationsaustausch anwendbar. Andere mögliche Arten des Datenaustauschs, z. B. die allgemeine Verteilung von Dateien, ist nicht eingeschlossen. SECOM ist nicht für die Festlegung vorgesehen, von welcher physikalischen Schicht der Transport durchgeführt wird, solange IP-Kommunikation unterstützt werden kann. Dieses Dokument ist sowohl auf öffentliche (staatliche) als auch auf private (geschäftliche) Dienste anwendbar.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

S-100, *IHO Universal Hydrographic Data Model*

RFC-2246, *TLS version 1.0 (1999)*

RFC-4346, *TLS version 1.1 (2006)*

RFC-5246, *TLS version 1.2 (2008)*

RFC-8446, *TLS version 1.3 (2018)*

RFC-2818, *HTTP Over TLS (2000)*

RFC-5280, *Profile of X.509*

RFC-2459, *Internet X.509 Public-key infrastructure and attribute certificate frameworks*

RFC-7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1 Begriffe

3.1.1

Akteur

die Rolle, die von einem mit dem Subjekt interagierenden Anwender oder einem anderen System eingenommen wird.

[QUELLE: einheitliche Modellierungssprache (en: Unified Modeling Language, UML)]

3.1.2

Authentifizierungsdaten

Informationen, die zur Überprüfung der behaupteten Identität einer Instanz, wie z. B. eines Individuums, einer definierten Rolle, eines Unternehmens oder einer Institution, verwendet werden

[QUELLE: ISO 21188:2018]

3.1.3

Zertifikat

öffentlicher Schlüssel und Identität einer Instanz (Authentifizierungsdaten (3.1.2)), die zusammen mit weiteren Informationen fälschungssicher wiedergegeben werden. Dazu werden die Zertifikatsinformationen mit dem privaten Schlüssel der den öffentlichen Schlüssel ausstellenden Zertifizierungsstelle signiert

[QUELLE: ISO 21188:2018]

3.1.4

Zertifizierungsstelle (en: Certificate Authority)

CA

von mindestens einer Instanz als vertrauenswürdig anerkannte Instanz (3.1.9) für Erstellung, Zuweisung und Widerruf von Zertifikaten des öffentlichen Schlüssels

[QUELLE: ISO 21188:2018]

3.1.5

Zertifikatanforderung

Übermittlung einer validierten Registrierung durch eine RA (3.1.17), deren Beauftragten oder ein Subjekt einer CA (3.1.4) zur Registrierung der Übernahme des öffentlichen Schlüssels eines Subjekts in ein Zertifikat (3.1.3)

[QUELLE: ISO 21188:2018]

3.1.6

Cross-Zertifizierung

gegenseitige Zertifizierung der öffentlichen Schlüssel zweier CAs (3.1.4) untereinander

Anmerkung 1 zum Begriff: Dieser Prozess kann, muss aber nicht automatisiert ablaufen.

[QUELLE: ISO 21188:2018]

3.1.7

digitale Signatur

an eine Dateneinheit angefügte Daten oder eine kryptografische Transformation einer Dateneinheit, mit der ein Empfänger der Dateneinheit die Möglichkeit der Überprüfung der Quelle und Integrität der Dateneinheit erhält und die einen Schutz gegen Fälschung, z. B. durch den Empfänger, bietet

[QUELLE: ISO 7498-2]

3.1.8

End-Entität

Zertifikatsinhaber, der seinen privaten Schlüssel für andere Zwecke als das Signieren von Zertifikaten nutzt

[QUELLE: ISO 21188:2018]

3.1.9

Instanz

Person, Partnerschaft, Organisation oder Unternehmen mit einer rechtlichen und einzeln identifizierbaren Existenz

Eine gesetzliche Instanz oder eine individuelle End-Entität (3.1.8), wie z. B. eine Zertifizierungsstelle (3.1.4), eine Registrierungsstelle (3.1.17) oder End-Entität (3.1.8)

[QUELLE: ISO 21188:2018]

3.1.10

Merkmal (en: Feature)

Abstraktion eines Phänomens der realen Welt. Ein Merkmal kann als Typ oder Instanz auftreten. Ein Merkmalstyp oder eine Merkmalsinstanz sollte verwendet werden, wenn nur eine gemeint ist.

[QUELLE: IHO S-100]

3.1.11

Merkmalskatalog (en: Feature Catalogue)

Katalog mit Definitionen und Beschreibungen des Merkmalstyps, der Merkmalsattribute und der Merkmalsverknüpfungen, die in einem oder mehreren geographischen Datensätzen auftreten

[QUELLE: IHO S-100]

3.1.12

Hash-Code

Bitfolge als Ausgabe einer Hash-Funktion

Anmerkung 1 zum Begriff: Die Literatur zu diesem Thema enthält eine Vielzahl von Begriffen, die dieselbe oder eine ähnliche Bedeutung wie Hash-Code haben. „Modification Detection Code“, „Manipulation Detection Code“, „Digest“, „Hash-Ergebnis“, „Hash-Wert“ und „Imprint“ sind einige Beispiele.

Anmerkung 2 zum Begriff: In NIST SP 800-63B wird dafür der Begriff „message digest“ verwendet.

[QUELLE: ISO/IEC 10118-1]

3.1.13

Hash-Funktion

Funktion zur Abbildung von Bitfolgen variabler (aber üblicherweise nach oben begrenzter) Länge auf Bitfolgen fester Länge, die die folgenden zwei Eigenschaften erfüllen:

- für einen gegebenen Ausgabewert ist es mathematisch unmöglich, auf dessen ursprünglichen Eingabewert zurückzuschließen;
- für einen gegebenen Eingabewert ist es mathematisch unmöglich, einen zweiten Eingabewert zu finden, der denselben Ausgabewert ergibt.

Verwendet im Rahmen von Datenauthentifizierung, Integritätsprüfung und Nicht-Abstreitbarkeit.

[QUELLE: ISO/IEC 10118-1]

3.1.14

privater Schlüssel

kryptografischer Schlüssel des asymmetrischen Schlüsselpaars einer Instanz, der nur von dieser Instanz verwendet werden kann

[QUELLE: ISO/IEC 11770-3]

3.1.15

öffentlicher Schlüssel

kryptografischer Schlüssel des asymmetrischen Schlüsselpaars einer Instanz, der öffentlich gemacht werden kann

[QUELLE: ISO/IEC 11770-3]

3.1.16

Infrastruktur des öffentlichen Schlüssels (en: Public key infrastructure)

PKI

Struktur aus Hardware, Software, Menschen, Prozessen und Richtlinien, die die Technologie der digitalen Signatur nutzt, um eine überprüfbare Zuordnung zwischen der öffentlichen Komponente eines asymmetrischen Schlüsselpaars und einem bestimmten Teilnehmer zu erleichtern, der den entsprechenden privaten Schlüssel besitzt

Anmerkung 1 zum Begriff: Der öffentliche Schlüssel kann zur Überprüfung der digitalen Signatur, zur Authentifizierung des Subjekts in Kommunikationsdialogen und/oder für den Schlüsselaustausch oder die Schlüsselaushandlung bei der Nachrichtenverschlüsselung verwendet werden

[QUELLE: ISO 21188:2018]

3.1.17

Registrierungsstelle (en: Registration Authority)

RA

Instanz, deren primäre funktionale Rolle und Verantwortlichkeiten die Identitätsvalidierung des Subjekts zwecks Genehmigung von Zertifikatanforderungen (3.1.17) beinhaltet, die von einer CA (3.1.4) gestellt werden

Anmerkung 1 zum Begriff: Eine RA kann im Anforderungsprozess und/oder im Widerrufsprozess für ein Zertifikat assistieren. Die RA muss keine eigenständige Stelle sein, sondern es kann sich um einen Teil der CA handeln.

[QUELLE: ISO 21188:2018]

3.1.18

REpresentational State Transfer (REST)

Art von Softwarearchitektur, die eine Reihe von Einschränkungen definiert, die bei der Erstellung von Webdiensten anzuwenden sind. Webdienste, die der REST-Softwarearchitektur entsprechen, werden als „RESTful Web Services (RWS) bezeichnet und bieten Interoperabilität zwischen Computersystemen im Internet.

[QUELLE: Roy Fielding - Representational State Transfer (REST)]

3.1.19

geheimer Schlüssel

mit symmetrischen Verschlüsselungsverfahren verwendeter kryptografischer Schlüssel, der nur von einer bestimmten Anzahl von Instanzen einsetzbar ist

Anmerkung 1 zum Begriff: Angepasst aus ISO/IEC 11770-3:1999, 3.35.

[QUELLE: ISO/IEC 11770-3]

3.1.20

Dienst

Mechanismus zur Ermöglichung des Zugriffs auf eine oder mehrere Funktionalitäten, wobei der Zugriff mittels einer wohldefinierten Schnittstelle erfolgt und unter Berücksichtigung der Einschränkungen und Richtlinien, welche in der Dienstbeschreibung festgelegt sind

[QUELLE: OASIS Reference Model for Service Oriented Architecture 1.0]

3.1.21

Unterzeichner

Instanz, die eine digitale Signatur generiert

[QUELLE: ISO/IEC 13888-1]

3.2 Abkürzungen

API Anwendungsprogramm-Schnittstelle (en: Application Program Interface)

CA Zertifizierungsstelle (en: Certification Authority)

ENC Elektronische Seekarte (en: Electronic Navigational Chart)

IALA Internationaler Verband der Seezeichenverwaltungen (en: International Association of Marine Aids to Navigation and Lighthouse Authorities)

IHO Internationale Hydrografische Organisation (en: International Hydrographic Organization)

IMO Internationale Seeschiffahrtsorganisation (en: International Maritime Organization)

ISO Internationale Organisation für Normung (en: International Organization for Standardization)

PKI Infrastruktur des öffentlichen Schlüssels (en: Public Key Infrastructure)

REST REpresentational State Transfer

4 Allgemeine Beschreibung

Bei den maritimen Diensten handelt es sich um operationelle Dienste sowohl für landseitige als auch für bordseitige Akteure, welche wiederum auf technische Dienste angewiesen sind, die digitalisierte Informationen bereitstellen, siehe [Bild 1](#), abgeleitet aus der eNav-Beschreibung ENAV23-12.1.4 der IALA. Die Datenformate sind typischerweise in Datenmodellspezifikationen genormt, und viele Organisationen sind mit der Erarbeitung neuer Normen beschäftigt, z. B. innerhalb des Rahmenwerks S-100 der IHO auf Grundlage des universellen hydrografischen Datenmodells (UHDM).

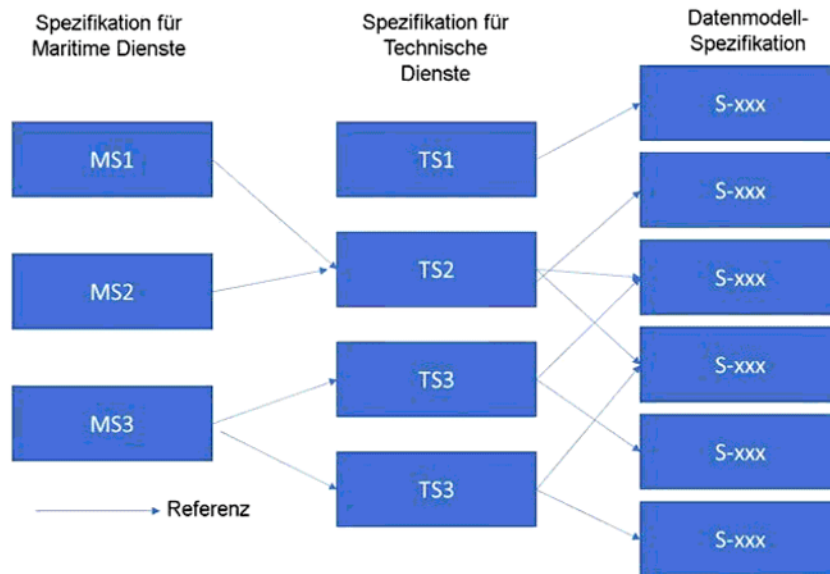


Bild 1 — Beziehung zwischen den Spezifikationen von Maritimen Diensten, Technischen Diensten und Datenmodellen in e-Navigation

Dieses Dokument legt eine Reihe von Dienstschnittstellen (d. h. APIs) fest, die für den Informationsaustausch auf Grundlage des universellen hydrografischen Datenmodells IHO S-100 verwendet werden. Außerdem enthält es ein Schutzkonzept für den Kommunikationskanal, Authentifizierungsverfahren für Webdienste und Service Discoverability. Der Datenschutz bezieht sich auf das Datenschutzkonzept der IHO (IHO S-100, Ed. 4, Part 15). Bild 2 gibt den Anwendungsbereich und die Beziehung zu bestehenden IHO-Normen wieder. Die Kommunikation erfolgt bi-direktional, d. h. sowohl das Schiff/die Reederei als auch die Behörden an Land und private Dienstanbieter können die Kommunikation initiieren und als Informationsanbieter fungieren. Ein Implementierungsleitfaden ist in [Anhang E](#) enthalten.

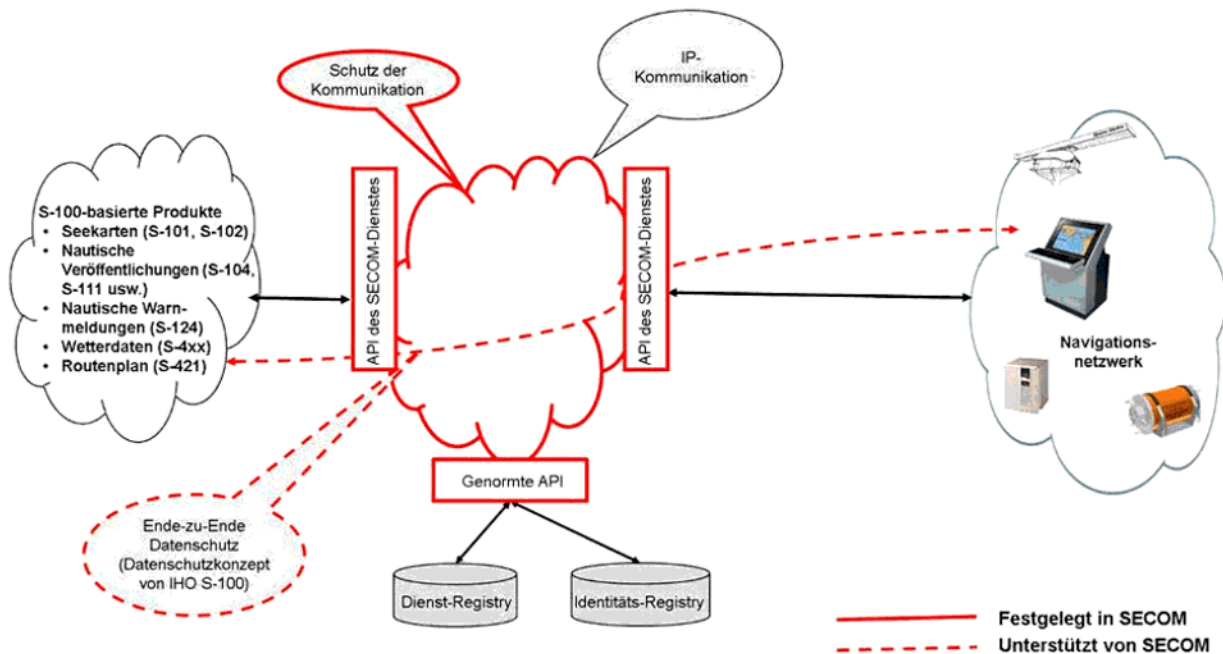


Bild 2 — Übersicht über SECOM

Die Standardisierung einer gemeinsamen Dienstschnittstelle für den Austausch S-100-basierter Informationen ermöglicht eine breitere technische Interoperabilität, bei der dieselbe Dienstschnittstelle für den Informationsaustausch ungeachtet der operationellen Verwendung genutzt wird. Dies ermöglicht es einem Anwender, der die Standard-Dienstschnittstelle z. B. für den Austausch des Routenplans S-421 implementiert hat, eine Reihe operationeller Dienste zu nutzen, die einen unterschiedlichen Zweck erfüllen, aber alle auf dem

Austausch (Push) des S-421-Routenplans beruhen. Die Standard-Dienstschnittstelle enthält außerdem Schnittstellen für Subskription, Zugriffsanforderung, Abruf und dynamische Anforderung von Funktionalitäten, Status und Beschreibung der Instanz.

Die Implementierung einer genormten Schnittstelle für ein bestimmtes Produkt anstelle der erzwungenen Implementierung einer riesigen Anzahl unterschiedlicher Schnittstellen zur Anpassung an proprietäre Schnittstellen verschiedener Dienstanbieter und Konsumenten bietet erhebliche Vorteile für ein Schiff. Die Schwerpunktsetzung auf die Dienstschnittstelle (Informationsdienst) für den Austausch von Informationsprodukten wird es Schiffen und ECDIS-Anbietern erleichtern, eine Zulassung ihrer Ausrüstung für bestimmte Informationsprodukte zu erhalten. Allerdings ist die Nutzung dieser Dienste aus operationeller Perspektive dynamisch, dem Anwender überlassen und wird höchstwahrscheinlich zu weniger bordseitigen Änderungsanforderungen bei der Einführung neuer Dienste führen.

Dienstanbieter werden ähnliche Vorteile bei der Erstellung von Diensten basierend auf dem Austausch genormter Informationsprodukte wahrnehmen können und dabei technische Interoperabilität mit allen Schiffen hinzugewinnen, die die Standard-Dienstschnittstelle implementiert haben.

Die Normung des Kommunikationsschutzkonzepts ermöglicht technische Interoperabilität für den sicheren Online-Transfer, und Service Discoverability ermöglicht die Suche nach dem Dienst, der genutzt werden soll.

Dieses Dokument ergänzt S-100 zur Erreichung der technischen Interoperabilität bis zu der Ebene, auf der Informationen zwischen Diensten sicher online ausgetauscht werden können.

SECOM enthält mehrere Schritte zur Sicherstellung des sicheren Informationsaustauschs. Der erste Schritt besteht darin, die Unterstützung für die Signierung von Informationen mit einem privaten Schlüssel vor dem Absenden zu ermöglichen. Die digitale Signatur enthält die Prüfsumme zur Integritätsüberprüfung der empfangenen Daten als auch der behaupteten Identität zum Zweck der Datenauthentifizierung. Die Verifizierung der Signatur beinhaltet den Zugang zu einer gemeinsamen Infrastruktur des öffentlichen Schlüssels (PKI), aus der der öffentliche Schlüssel für die behauptete Identität heruntergeladen werden kann. Bei jedem Datenaustausch muss die digitale Signatur stets beigefügt und in größtmöglicher Nähe zum Endbenutzer überprüft werden. Auf diese Weise wird der grundlegende Ende-zu-Ende-Datenschutz realisiert.

Außerdem unterstützt SECOM die Verschlüsselung von Daten nach unterschiedlichen Schutzkonzepten. Das bestehende Schutzkonzept für ENC-Daten, wie z. B. PRIMAR, kann zusammen mit der SECOM-Dienstschnittstelle verwendet werden. SECOM beinhaltet außerdem ein eigenes Schutzkonzept, das speziell für einen dynamischeren Datenaustausch von Schiff zu Land und von Land zu Schiff sowie den Routenplan-Austausch ausgelegt ist. Im SECOM-Datenschutzkonzept erstellt der Sender klassifizierter Daten einen temporären geheimen Schlüssel, der auf sicherem Wege übertragen wird, bevor die Übertragung der verschlüsselten Daten erfolgt. Die temporäre geheime Schlüssel wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt – demselben Schlüssel, der auch für die Authentifizierung verwendet wird – und kann somit ausschließlich von dem Akteur entschlüsselt werden, der den passenden privaten Schlüssel besitzt. Dies erfordert ein starkes Schlüsselpaar, das über einen ausreichend langen Schlüssel zur Ver- und Entschlüsselung des geheimen Schlüssels verfügt.

Das SECOM-Datenschutzkonzept stützt sich auf die SECOM-Infrastruktur des öffentlichen Schlüssels (SECOM-PKI) und dessen Management für öffentliche und private Schlüssel unter Verwendung von X.509-Zertifikaten für den Schlüsselaustausch. Der private Schlüssel wird durch den Akteur generiert und intern gespeichert, während der öffentliche Schlüssel in die SECOM-PKI hochgeladen und mit der Identität verknüpft wird.

In SECOM ist außerdem die SECOM-Dienstschnittstelle für den – offenen und signierten oder verschlüsselten und signierten – Austausch von S-100-basierten Produkten definiert. Die SECOM-Dienstschnittstelle ist zwar für S-100-basierte Produkte ausgelegt, enthält jedoch auch eine Schnittstelle für beliebige Nutzdaten, aber unter Verwendung des SECOM-Datenschutzkonzepts für den Austausch. Die SECOM-Dienstschnittstelle gestattet sowohl Push- und Pull-Daten, asynchrone Quittierung, Subskription und die Anforderung des Datenzugriffs auf sichere Weise. Bei der Nutzung der SECOM-Dienste muss die Internetübertragung mit TLS und gültigen Zertifikaten von einer vertrauenswürdigen Partei geschützt sein.

Zur Unterstützung der dynamischen Nutzung von lose gekoppelten Diensten wurde in SECOM eine Service-Discoverability-Schnittstelle definiert. SECOM Service Discoverability enthält gemeinsame Schnittstellen für die Suche nach Diensten.

Die folgenden Abschnitte sind in SECOM enthalten:

Abschnitt 5	SECOM-Dienstschnittstelle
-------------	---------------------------

Abschnitt 6	SECOM-Kommunikationskanalsicherheit
Abschnitt 7	SECOM-Datenschutz
Abschnitt 8	SECOM-Service Discoverability

5 SECOM-Dienstschnittstelle

5.1 Allgemeines

In diesem Abschnitt wird die SECOM-Dienstschnittstelle für den Austausch von S-Produkten beschrieben. Die SECOM-Dienstschnittstelle muss digitale Signaturen und die optionale Datenverschlüsselung unterstützen.

Die Definition enthält eine Zusammenstellung mehrerer Dienstschnittstellen, die gemeinsam die SECOM-Dienstschnittstelle darstellen.

In der folgenden Definition bezieht sich die Bezeichnung „Konsument“ auf den Datenclient, und „Produzent“ bezieht sich auf den Datenserver.

Zwei der Dienstschnittstellen werden für den eigentlichen Datenaustausch verwendet: „Upload“ (Hochladen) und „Get“ (Anfordern). Die Dienstschnittstelle „Upload“ wird von Produzenten von Informationen verwendet, um Daten an einen Konsumenten zu senden. Dies deckt die primäre Anforderung an den Datenaustausch ab. Die Dienstschnittstelle „Get“ wird verwendet, wenn ein Konsument Daten vom Produzenten anfordert. Für größere Datenmengen, bei denen „Upload“ nicht verwendet werden kann, wird die Schnittstelle „Upload Link“ (Verknüpfung hochladen) verwendet, um eine Verknüpfung (Kennung) zu den Daten zu senden, und im Anschluss daran können die Daten mit der „Get“-Schnittstelle abgerufen werden.

Die Dienstschnittstelle „Get Summary“ (Zusammenfassung anfordern) wird verwendet, um eine Kurzzusammenfassung der verfügbaren Daten zu erhalten, aus der der Anwender eines oder mehrere Elemente für den Abruf über die „Get“-Schnittstelle auswählen kann.

Die Dienstschnittstelle „Subscription“ (Subskription) wird verwendet, wenn ein Konsument eine Subskription von Daten des Produzenten erstellen möchte. Der Produzent übermittelt dann die Daten über die Dienstschnittstelle „Upload“ an den Konsumenten. Der Konsument verwendet die Schnittstelle „Get Subscription List“ (Subskriptionsliste anfordern), um eine Liste der aktiven Subskriptionen zu erhalten und nutzt die Schnittstelle „Remove Subscription“ (Subskription entfernen), um Subskriptionen zu löschen. Der Produzent kann einen Konsumenten außerdem intern „benennen“, indem er die Subskription intern für ihn erstellt. Anschließend verwendet er die Dienstschnittstelle „Subscription Notification“ (Subskriptionsbenachrichtigung), um den Konsumenten darüber zu informieren, dass er nunmehr über eine aktive Subskription verfügt. Der Produzent kann eine Subskription auch intern löschen und verwendet dann die Dienstschnittstelle „Subscription Notification“, um den Konsumenten davon in Kenntnis zu setzen.

Wenn ein Konsument keinen Zugriff auf bestimmte Daten besitzt, z. B. weil er nicht über die entsprechende Berechtigung verfügt, verwendet er die Schnittstelle „Request Access“ (Zugriff anfordern), um diese vom Produzenten zu erhalten. Der Produzent teilt dem Konsumenten daraufhin über die Schnittstelle „Access Notification“ (Zugriffsbenachrichtigung) seine Entscheidung (Zustimmung oder Ablehnung) mit.

Sowohl der Produzent als auch der Konsument nutzen die Schnittstelle „Capability“ (Funktionalität), um Informationen bezüglich der zugänglichen Schnittstellen und Datentypen abzurufen. Dies ermöglicht es Funktionen z. B. abzufragen, welche Version der S-Produkt-Spezifikation ein Produzent oder Konsument akzeptiert sowie nur die für einen bestimmten Dienst zugängliche Schnittstellen anzuzeigen, um eine nicht ordnungsgemäße Nutzung des Dienstes zu verhindern.

Die Schnittstelle „Description“ (Beschreibung) muss verwendet werden, wenn eine ausführlichere Beschreibung zur Nutzung des Dienstes gewünscht ist.

Die Schnittstelle „Status“ muss verwendet werden, um den technischen Status des Dienstes zu prüfen.

5.2 Dienstdefinitionsmodell

Die Dienstschnittstelle wird nach dem Dienstdefinitionsmodell in S-100, Ed.4.0.0, Kapitel 14 „Online Data Exchange“ (Online-Datenaustausch) beschrieben. Siehe [Anhang C](#) mit Einzelheiten bezüglich der Verwendung des Dienstdefinitionsmodells in SECOM.

5.3 Diensttechnologie

Die gewählte Technologie (der Architekturtyp) ist REST (REpresentational State Transfer) auf HTTP/1.1 (RFC-7231).

Die Definition der einzelnen Operationen beinhaltet die Festlegung zusätzlicher Fehlermeldungen, mit denen die Operation zusätzlich zu den durch HTTP/1.1 (RFC-7231) definierten Antwortcodes antworten muss.

5.4 Definition der Dienstschnittstellen

5.4.1 Allgemeines

Unterabschnitt 5.4 enthält ausführliche Definitionen der einzelnen Dienstschnittstellen. Zuerst wird eine technologieunabhängige Spezifikation der Dienstschnittstelle angegeben, gefolgt von einer Definition der Dienstschnittstelle mit REST-Technologie. Jede Dienstschnittstelle beinhaltet außerdem Prüfmethode und erwartete Ergebnisse.

Tabelle 1 gibt einen Überblick über die Dienstschnittstellen, aus denen die SECOM-Dienstschnittstelle besteht.

Tabelle 1 — Überblick über die Dienstschnittstellen

Dienstschnittstelle	Austauschmuster	Definition
Upload (Hochladen)	ONE_WAY (einseitig)	Schnittstelle zum Senden (Push) von Informationen an den Konsumenten
Upload Link (Verknüpfung hochladen)	ONE_WAY (einseitig)	Schnittstelle zum Senden (Push) einer Verknüpfung zu Informationen, die ein Konsument herunterladen kann
Acknowledgement (Quittierung)	ONE_WAY (einseitig)	Schnittstelle zum Senden einer Quittierung zu hochgeladenen Informationen.
Get (Anfordern)	REQUEST_RESPONSE (Anforderung und Antwort)	Schnittstelle zur Anforderung (Pull) von Informationen vom Produzenten
Get Summary (Zusammenfassung anfordern)	REQUEST_RESPONSE (Anforderung und Antwort)	Schnittstelle zur Anforderung (Pull) einer Liste von Informationen vom Produzenten
Subscription (Subskription)	PUBLISH_SUBSCRIBE (Veröffentlichen und abonnieren)	Schnittstelle zur Erstellung einer Subskription von Informationen Konsumentenschnittstelle (ConsumerInterface): SubscriptionNotification (Subskriptionsbenachrichtigung) Upload (Hochladen)
Remove Subscription (Subskription entfernen)	ONE_WAY (einseitig)	Schnittstelle zum Entfernen einer Subskription
Get Subscription List (Subskriptionsliste anfordern)	REQUEST_RESPONSE (Anforderung und Antwort)	Schnittstelle für den Abruf einer Liste aktiver Subskriptionen
Subscription Notification (Subskriptionsbenachrichtigung)	ONE_WAY (einseitig)	Schnittstelle zur Benachrichtigung über Subskriptionsereignisse
Request Access (Zugriff anfordern)	REQUEST_CALLBACK (Anforderung und Rückmeldung)	Schnittstelle zur Anforderung des Zugriffs auf Informationen Konsumentenschnittstelle (ConsumerInterface): AccessNotification (Zugriffsbenachrichtigung)
Access Notification (Zugriffsbenachrichtigung)	ONE_WAY (einseitig)	Schnittstelle zur Mitteilung der Entscheidung bezüglich einer Zugriffsanforderung
Capability (Funktionalität)	REQUEST_RESPONSE (Anforderung und Antwort)	Schnittstelle zur Abfrage der Schnittstellenfunktionalitäten
Description (Beschreibung)	REQUEST_RESPONSE (Anforderung und Antwort)	Schnittstelle zur Anforderung einer Kurzbeschreibung des Dienstes

Dienstschnittstelle	Austauschmuster	Definition
Status	REQUEST_RESPONSE (Anforderung und Antwort)	Schnittstelle zur Überprüfung des Status an der Schnittstelle
EncryptionKey (kryptografischer Schlüssel)	REQUEST_RESPONSE (Anforderung und Antwort)	Schnittstelle für den sicheren Versand eines symmetrischen Schlüssel zur Datenverschlüsselung

5.4.2 Paginierung

Die Dienstschnittstellen „Get“ und „Get List“ (Liste anfordern) können mehr als ein Ergebnis zurückgeben. Um die Größe der Antworten zu begrenzen, unterstützen diese Schnittstellen Paginierung.

Bei Anforderungen an diese Dienste darf der Client die optionalen Parameter „Page“ (Seite) und „pageSize“ (Seitengröße) angeben. Diese ermöglichen es dem Client festzulegen, wie viele Elemente zurückgegeben werden und mit welchem Element begonnen werden soll. Wenn eine bestimmte Anforderung z. B. zu einem aus 30 Elementen bestehenden Ergebnis führen würde, würden mit den Einstellungen „page = 1“ und „pageSize = 20“ die verbleibenden zwanzig Elemente und mit „page = 2“ und „pageSize = 20“ die verbleibenden zehn Elemente zurückgegeben.

Unabhängig davon, ob „page“ oder „pageSize“ angegeben werden, gibt der Server immer die Gesamtzahl der Elemente im Attribut „totalItems“ und die maximale Anzahl der Elemente je Seite im Attribut „maxItemsPerPage“ zurück.

Fehler werden vom Server zurückgegeben, wenn entweder eine ungültige Seite oder zu viele Elemente gleichzeitig angefordert werden.

Wird der Parameter „page“ nicht angegeben, gibt der Server die erste Seite mit Ergebnissen zurück.

Wird der Parameter „pageSize“ nicht angegeben, gibt der Server die maximal unterstützte Anzahl von Elementen je Seite zurück.

Wird der Parameter „page“ auf 0 gesetzt, gibt der Server gar keine Elemente zurück, sondern den Wert von „maxItemsPerPage“. Dieser Wert muss bei jeder Serverabfrage konstant sein (so dass der Client dies nur einmal abfragen muss).

5.4.3 Filterung

Noch festzulegen

5.4.4 Dienstschnittstelle – Upload (Hochladen)

5.4.4.1 Spezifikation

Der Zweck dieser Schnittstelle besteht darin, Informationen an den Konsumenten hochzuladen (Push). Daher muss ein Konsument diese Schnittstelle implementieren, um Informationen zu empfangen.

Diese Operation wird sowohl zum vereinzelt Hochladen als auch zum Hochladen im Rahmen einer Subskription verwendet. Bei „Upload“-Vorgängen innerhalb einer Subskription zeigt der Parameter <FromSubscription> „true“ (wahr) an, außerhalb davon „false“ (falsch).

Beim Hochladen der Nachricht kann eine Quittierung angefordert werden, die empfangen werden soll, wenn die hochgeladene Nachricht an das Endsystem zugestellt wurde (technische Quittierung), und zusätzlich, sofern dies unterstützt wird, eine Quittierung, die empfangen wird, wenn die Nachricht vom Endbenutzer geöffnet (gelesen) wird (operationelle Quittierung).

[Tabelle 2](#) beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 2 — Informationsaustausch für die „Upload“-Schnittstelle

Informationen (Eingang)	Mult.	Definition
Data	1	Die Nutzdaten, offen oder verschlüsselt, XML oder binär
Exchange Metadata	1	Die Austausch-Metadaten enthalten Informationen bezüglich Schutzkonzept, Komprimierung, Signatur und behauptete Identität.
FromSubscription	0..1	Flag, das anzeigt, ob die Daten innerhalb einer aktiven Subskription hochgeladen wurden oder nicht.
AckRequest	0..1	Flag, das anzeigt, dass die Rücksendung einer Quittierung erwartet wird
Informationen (Ausgang)	Mult.	
Ergebnis aus Operation	1	Referenz für Quittierung

5.4.4.2 REST-Auslegung

5.4.4.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 3 als UML-Modell definiert. Das Datenaustauschmodell ist ebenfalls dort definiert. SECOM_ServiceExchangeMetadata ist ein generisches Objekt, das allen Schnittstellen beigelegt ist, an denen ein Signaturaustausch erforderlich ist.

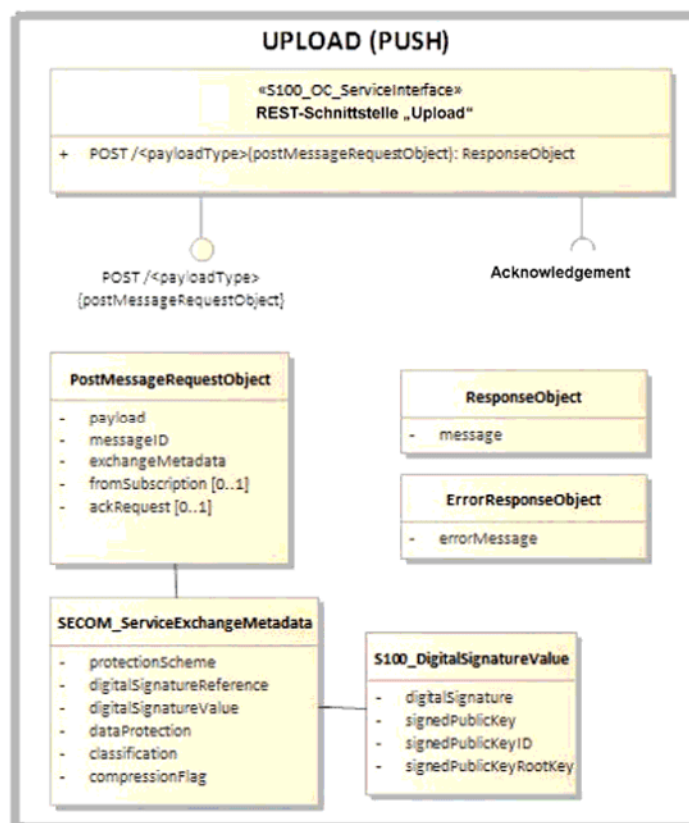


Bild 3 — „Upload“-Schnittstelle in UML

ExchangePattern (Austauschmuster)

- ONE_WAY (einseitig) oder REQUEST_CALLBACK (Anforderung und Rückmeldung)

ConsumerInterface (Konsumentenschnittstelle)

- Nimmt Dienstschnittstelle „Acknowledgement“ (Quittierung) in Anspruch, wenn Quittierung angefordert wird.

5.4.4.2.2 Operation – POST <Datentyp>

Die REST-Operation POST <Datentyp>, wobei <Datentyp> bei S-Produkten durch die S-Produktnummer ersetzt werden muss, z. B. s421. Die Schnittstelle muss für das Hochladen (Push) von Daten an einen Konsumenten verwendet werden. Die Operation erwartet ein einzelnes Datenobjekt und dessen Metadaten. Die Einzelheiten sind in Tabelle 3 beschrieben.

Tabelle 3 — REST-Implementierung der „Upload“-Schnittstelle

REST-Operation				
POST <Datentyp>				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
–				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
PostMessageRequestObject	string	application/json	1	Das (Nutz-)Datenpaket mit dessen Metadaten
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
ResponseObject ErrorResponseObject	string	application/json	1	Bestätigung des Hochladens oder Fehlermeldung, einschließlich Beschreibung der fehlerhaften oder fehlenden Werte in den Nutzdaten für den jeweiligen Dienst.

5.4.4.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 4 beschrieben.

Tabelle 4 — Datenaustauschmodell für die REST-Implementierung der „Upload“-Schnittstelle

PostMessageRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
data	json.string	Base64	1	Die Daten dürfen in XML (z. B. S100_ExchangeSet), verschlüsselt binär oder (ZIP-)komprimiert binär vorliegen.
exchangeMetadata	json.string	ExchangeMetadataObject	1	Austausch-Metadaten des Dienstes mit Signatur, ID usw.
fromSubscription	json.boolean	nicht verfügbar	0..1	Flag, das anzeigt, ob die Nutzdaten innerhalb einer aktiven Subskription hochgeladen wurden oder nicht
ackRequest	json.boolean	nicht verfügbar	0..1	Flag, das anzeigt, dass eine Quittierung erwartet wird.
ExchangeMetadataObject				
Attribut	Typ	Kodierung	Mult.	Definition
messageIdentifier	json.string	UUID MRN TIMESTAMP oder Kombination daraus	1	Nachrichtenkennung muss bei der Quittierung verwendet werden
dataProtection	json.boolean	nicht verfügbar	1	(S-100) Zeigt an, ob die Daten verschlüsselt sind. 0 bedeutet, dass die Daten unverschlüsselt sind 1 bedeutet, dass die Daten verschlüsselt sind
protectionScheme	json.string	nicht verfügbar	1	(S-100) Für den Datenschutz verwendete Spezifikation oder Methode z. B. S-63, SECOM

PostMessageRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
digitalSignatureReference	json.string	nicht verfügbar	1	(S-100) Legt den zur Berechnung von digitalSignatureValue verwendeten Algorithmus fest z. B. „dsa“
digitalSignatureValue	json.string	digitalSignatureValueObject	1	(S-100) Signierter öffentlicher Schlüssel plus digitale Signatur
classification	json.integer	nicht verfügbar	0..1	(S-100) Zeigt die Sicherheitsklassifizierung der Daten an 1 = nicht klassifiziert noch zu bestätigen
compressionFlag	json.boolean	nicht verfügbar	0..1	(S-100) Zeigt an, ob die Daten komprimiert sind. 0 bedeutet unkomprimiert 1 bedeutet komprimiert
DigitalSignatureValueObject				
Attribut	Typ	Kodierung	Mult.	Definition
signedPublicKeyID	json.string	nicht verfügbar	1	(S-100) Behauptete Identität des Unterzeichners
signedPublicKeyRootKey	json.string	nicht verfügbar	1	(S-100) Behaupteter Rootschlüssel in Bezug auf das gewählte Schutzkonzept
signedPublicKey	json.string	nicht verfügbar	1	(S-100) Öffentlicher Schlüssel für die behauptete Identität
digitalSignature	json.string	hex	1	(S-100) Die digitale Signatur im Hexadezimal-Format
ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	json.string	nicht verfügbar	1	Nachricht über erfolgreiche Antwort

5.4.4.2.4 Antwort des Dienstes

Der Dienst muss mit HTTP-Codes und einer Nachricht nach Tabelle 5 antworten.

Tabelle 5 — HTTP-Antwortcodes und Nachricht im Antwort-Objekt

HTTP-Code	Nachricht
200	Nachricht <messageldentifizier> erfolgreich hochgeladen
403	Keine Berechtigung zum Hochladen
500	Attribut <x> fehlt in <messageldentifizier>
500	Attribut <x> in <messageldentifizier> ist falsch

5.4.4.2.5 Dynamisches Verhalten

<Sequenzdiagramm für die Dienstschnittstelle einfügen>

5.4.4.3 Prüfmethode und erwartetes Ergebnis

Prüfung anhand des Dokuments

- Verfahren zur Prüfung von Anwendbarkeit, Konsistenz, Vollständigkeit und Korrektheit des Dokuments

Prüfung des Arbeitsobjekts anhand des Dokuments

- Verfahren zur Prüfung von X anhand des Dokuments, um die Frage zu beantworten: „Entspricht mein Arbeitsobjekt den Vorgaben des Dokuments?“
- Datenprüfung

5.4.5 Dienstschnittstelle – Upload Link (Verknüpfung hochladen)

5.4.5.1 Spezifikation

Der Zweck dieser Schnittstelle besteht darin, eine Verknüpfung an einen Konsumenten hochzuladen (Push). Daher muss ein Konsument diese Schnittstelle implementieren, um eine Verknüpfung zu den Informationen zu empfangen, die abgerufen werden können.

Diese Schnittstelle muss verwendet werden, wenn große Datenmengen ausgetauscht werden müssen. Der Produzent der Informationen lädt dann eine Verknüpfung (messagelidentifiziert) für einen Konsumenten hoch, und der Konsument nutzt anschließend die „Get“-Schnittstelle, um die Daten vom Produzenten abzurufen.

Tabelle 6 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 6 — Informationsaustausch für die „Upload Link“-Schnittstelle

Informationen (Eingang)	Mult.	Definition
Message Identifier	1	Die Nutzdaten, offen oder verschlüsselt, XML oder binär
Exchange Metadata	1	Die Austausch-Metadaten enthalten Informationen bezüglich Schutzkonzept, Komprimierung, Signatur und behauptete Identität.
Informationen (Ausgang)	Mult.	
Ergebnis aus Operation	1	Referenz für Quittierung

5.4.5.2 REST-Auslegung

5.4.5.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 4 als UML-Modell definiert. Das Datenaustauschmodell ist ebenfalls dort definiert. SECOM_ServiceExchangeMetadata ist ein generisches Objekt, das allen Schnittstellen beigelegt ist, an denen ein Signaturaustausch erforderlich ist.

Noch festzulegen

Fehler! Es wurde kein Dateiname angegeben.

Bild 4

ExchangePattern (Austauschmuster)

- REQUEST_CALLBACK (Anforderung und Rückmeldung)

ConsumerInterface (Konsumentenschnittstelle)

- „Get“-Schnittstelle

5.4.5.2.2 Operation – POST <Datentyp>\link

Die REST-Operation POST <Datentyp>, wobei <Datentyp> bei S-Produkten durch die S-Produktnummer ersetzt werden muss, z. B. s421. Die Schnittstelle muss für das Hochladen (Push) von Daten an einen Konsumenten verwendet werden. Die Operation erwartet ein einzelnes Datenobjekt und dessen Metadaten. Die Einzelheiten sind in [Tabelle 7](#) beschrieben.

Tabelle 7 — REST-Implementierung der „Upload Link“-Schnittstelle

REST-Operation				
POST <Datentyp>\link				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
–				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
PostMessageRequestObject	string	application/json	1	Die Nachrichtenverknüpfung mit deren Metadaten
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
ResponseObject	string	application/json	1	Bestätigung des Hochladens oder Fehlermeldung

5.4.5.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 8 beschrieben.

Tabelle 8 — Datenaustauschmodell für die REST-Implementierung der „Upload Link“-Schnittstelle

PostMessageRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
exchangeMetadata	json.string	ExchangeMetadataObject	1	Austausch-Metadaten des Dienstes mit Signatur, ID usw.
ExchangeMetadataObject				
Attribut	Typ	Kodierung	Mult.	Definition
messageIdentifier	json.string	UUID MRN TIMESTAMP oder Kombination daraus	1	Nachrichtenennung muss bei der Quittierung verwendet werden
dataProtection	json.boolean	nicht verfügbar	1	(S-100) Zeigt an, ob die Daten verschlüsselt sind. 0 bedeutet, dass die Daten unverschlüsselt sind 1 bedeutet, dass die Daten verschlüsselt sind
protectionScheme	json.string	nicht verfügbar	1	(S-100) Für den Datenschutz verwendete Spezifikation oder Methode z. B. S-63, SECOM
digitalSignatureReference	json.string	nicht verfügbar	1	(S-100) Legt den zur Berechnung von digitalSignatureValue verwendeten Algorithmus fest z. B. „dsa“
digitalSignatureValue	json.string	digitalSignatureValueObject	1	(S-100) Signierter öffentlicher Schlüssel plus digitale Signatur
classification	json.integer	nicht verfügbar	0..1	(S-100) Zeigt die Sicherheitsklassifizierung der Daten an 1 = nicht klassifiziert noch zu bestätigen
compressionFlag	json.boolean	nicht verfügbar	0..1	(S-100) Zeigt an, ob die Daten komprimiert sind. 0 bedeutet unkomprimiert 1 bedeutet komprimiert
DigitalSignatureValueObject				
Attribut	Typ	Kodierung	Mult.	Definition

PostMessageRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
signedPublicKeyID	json.string	nicht verfügbar	1	(S-100) Behauptete Identität des Unterzeichners
signedPublicKeyRootKey	json.string	nicht verfügbar	1	(S-100) Behaupteter Rootschlüssel in Bezug auf das gewählte Schutzkonzept
signedPublicKey	json.string	nicht verfügbar	1	(S-100) Öffentlicher Schlüssel für die behauptete Identität
digitalSignature	json.string	hex	1	(S-100) Die digitale Signatur im Hexadezimal-Format

ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	json.string	nicht verfügbar	1	Nachricht über erfolgreiche Antwort

5.4.5.2.4 Antwort des Dienstes

Der Dienst muss mit HTTP-Codes und einer Nachricht nach Tabelle 9 antworten.

Tabelle 9 — HTTP-Antwortcodes und Nachricht im Antwort-Objekt

HTTP-Code	Nachricht
200	Nachricht <messagelidentifizier> erfolgreich hochgeladen
403	Keine Berechtigung zum Hochladen
500	Attribut <x> fehlt in <messagelidentifizier>
500	Attribut <x> in <messagelidentifizier> ist falsch

5.4.5.2.5 Dynamisches Verhalten

<Sequenzdiagramm für die Dienstschnittstelle einfügen>

5.4.5.3 Prüfmethode und erwartetes Ergebnis

Prüfung anhand des Dokuments

- Verfahren zur Prüfung von Anwendbarkeit, Konsistenz, Vollständigkeit und Korrektheit des Dokuments

Prüfung des Arbeitsobjekts anhand des Dokuments

- Verfahren zur Prüfung von X anhand des Dokuments, um die Frage zu beantworten: „Entspricht mein Arbeitsobjekt den Vorgaben des Dokuments?“
- Datenprüfung

5.4.6 Dienstschnittstelle – Acknowledgement (Quittierung)

5.4.6.1 Spezifikation

Beim Hochladen von Informationen kann eine Quittierung angefordert werden, die zurückgesendet wird, sobald die Informationen vom Konsumentensystem an das Endsystem zugestellt wurden. Die Quittierung enthält eine Referenz auf das zugestellte Informationsprodukt.

[Tabelle 10](#) beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 10 — Informationsaustausch für die „Quittierung“-Schnittstelle

Informationen (Eingang)	Mult.	Definition
Message Identifier	1	Referenz auf das quittierte Objekt
Time	1	Uhrzeit der Zustellung oder des Öffnens
AcknowledgementType	1	Art der Quittierung (Quittierung der technischen Zustellung oder operationelle Quittierung, dass Nachricht geöffnet wurde)
AcknowledgementMessage	1	Bestätigungsmeldung
Informationen (Ausgang)	Mult.	Definition
Ergebnis aus Operation	1	

5.4.6.2 REST-Auslegung

5.4.6.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 5 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

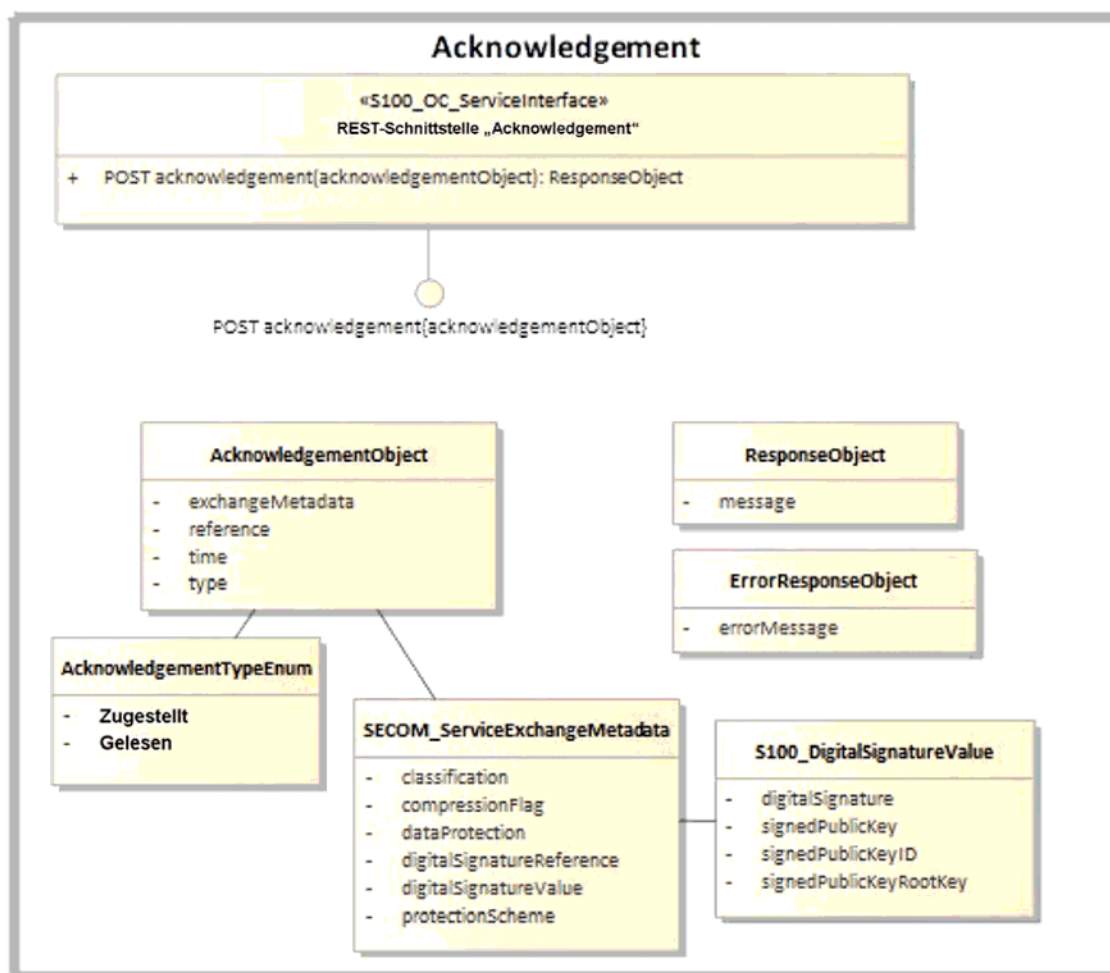


Bild 5 — REST-Schnittstelle „Acknowledgement“

ExchangePattern (Austauschmuster)

- ONE_WAY (einseitig)

ConsumerInterface (Konsumentenschnittstelle)

- Keine Schnittstelle in Anspruch genommen.

5.4.6.2.2 Operation – POST acknowledgement

Die Einzelheiten für die Operation „Acknowledgement“ in der Schnittstelle sind in Tabelle 11 beschrieben.

Tabelle 11 — REST-Implementierung der „Acknowledgement“-Schnittstelle

REST-Operation				
POST acknowledgement				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
–				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
AcknowledgementObject	string	application/json	1	Objekt mit Referenz auf Informationen und Zustellungszeitpunkt
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
ResponseObject ErrorResponseObject	string	application/json	1	Bestätigung oder Fehlermeldung

5.4.6.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 12 beschrieben.

Tabelle 12 — Datenaustauschmodell für die REST-Operation „Acknowledgement“

AcknowledgementObject				
Attribut	Typ	Kodierung	Mult.	Definition
messagelidentifizier	json.string	UUID	1	Beim Hochladen vergebene Referenzkennung
time	json.string	dateTime	1	Erstellungszeitpunkt der Quittierung
Typ	json.string	enumType	1	Quittierungstyp
ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	string		1	Antwortnachricht
enumType				
Enum	Typ	Kodierung		Definition
technicalACK	string			Technische Quittierung wie z. B. „zugestellt an Endsystem“.
operationalACK	string			Operationelle Quittierung, wenn z. B. vom Endbenutzer geöffnet/gelesen.

5.4.6.2.4 Antwort des Dienstes

Der Dienst muss mit HTTP-Codes und einer Nachricht nach Tabelle 13 antworten.

Tabelle 13 — HTTP-Antwortcodes und Antwortnachricht

HTTP-Code	Nachricht
200	Quittierung für <reference> erfolgreich empfangen
403	Keine Berechtigung zum Hochladen der Quittierung
404	Nachricht <reference> nicht gefunden

5.4.6.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.6.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.7 Dienstschnittstelle – Get (Anfordern)

5.4.7.1 Spezifikation

Die „Get“-Schnittstelle wird zur Anforderung von Informationen von einem Dienstanbieter (Produzenten) verwendet. Der Eigentümer der Informationen (Produzent) ist für das Autorisierungsverfahren verantwortlich, das durchlaufen wird, bevor Informationen zurückgegeben werden.

Der Konsument kann Informationen anhand von deren Referenz, Kennung, Status, Geometrie und Zeitstempel abfragen.

Diese Schnittstelle gibt möglicherweise eine große Anzahl von Informationsobjekten zurück und unterstützt die in 5.4.2 beschriebene Paginierung. Werden keine Parameter angegeben, werden als Ergebnis alle Nachrichten für die erste Seite zurückgegeben.

Tabelle 14 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 14 — Informationsaustausch für die „Get“-Schnittstelle

Informationen (Eingang)	Mult.	Definition
Reference	0..1	Referenz auf Informationsobjekt, z. B. aus „Get List“ (Liste anfordern)
InformationIdentifier	0..1	Kennung des Informationsobjekts, z. B. aus „Get List“
Status	0..1	Status im Informationsobjekt, z. B. aus „Get List“
Geometry	0..1	Geometrische Beschaffenheit bei Informationsobjekten mit Geolokalisierung
AreaName	0..1	Bezeichnung des festgelegten Bereichs
UN/LOCODE	0..1	Code des definierten Objekts
TimePeriod	0..1	Zeit in Bezug auf die Gültigkeit von Informationsobjekten
Pagination Information	0..1	Angeforderte Paginierung
Informationen (Ausgang)	Mult.	Definition
Liste der Informationsobjekte	0..*	Zurückgegebene(s) Informationsobjekt(e)

5.4.7.2 REST-Auslegung

5.4.7.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 6 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

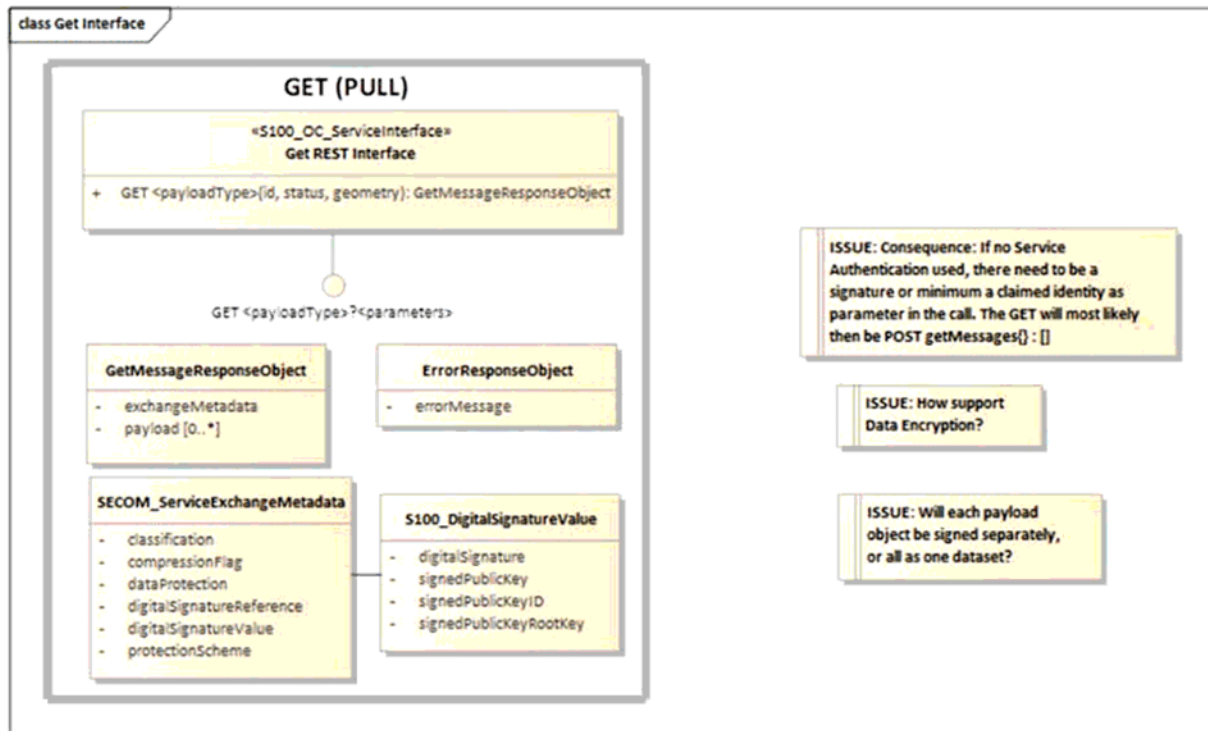


Bild 6 — REST-Schnittstelle „Get“

ExchangePattern (Austauschmuster)

- REQUEST_RESPONSE (Anforderung und Antwort)

ConsumerInterface (Konsumentenschnittstelle)

- Keine Schnittstelle in Anspruch genommen.

5.4.7.2.2 Operation – GET <Datentyp>

Diese Operation wird zur Anforderung von Informationen verwendet. Bei bestehender Berechtigung werden die Daten in der Antwort zurückgesendet. Es obliegt dem Dienst, ein relevantes Autorisierungsverfahren anzuwenden und den Informationszugriff zu kontrollieren.

Tabelle 15 beschreibt die logischen Parameter, die die Schnittstelle bereitstellt.

Tabelle 15 — REST-Implementierung der „Get“-Schnittstelle

REST-Operation				
GET <Datentyp>				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
informationIdentifier	json.string		0..1	Als Suchkriterium angegebene Informationskennung. Als Liste der Kennungen kann über die „Get List“-Schnittstelle abgerufen werden.
messageIdentifier	json.string	UUID	0..1	Informationen, die durch Verwendung der in „Get List“ oder „Upload Link“ bereitgestellten Referenz abgerufen werden
query	json.string	key:value Aufzählung von Schlüsseln mit den jeweils zugehörigen Werten	0..1	Abfrage anhand der Aufzählungen im betreffenden S-Produkt

REST-Operation				
geometry	json.string	S-100-Geometrie (Fläche, Kurve)	0..1	Geometrie als Suchparameter im S-100-Format.
areaName	json.string	Liste von AreaNameEnum	0..1	Durch Komma getrennte Liste der Aufzählungswerte (z. B. „1,2,3“). Siehe Tabelle 16
unlocode	json.string	nicht verfügbar	0..1	Siehe <UN-Website>
fromTime	json.string	dateTime	0..1	Zeit in Bezug auf den Beginn der Gültigkeit des Informationsobjekts
toTime	json.string	dateTime	0..1	Zeit in Bezug auf das Ende der Gültigkeit des Informationsobjekts
page	json.integer	nicht verfügbar	0..1	Paginierungsinformationen
pageSize	json.integer	nicht verfügbar	0..1	Paginierungsinformationen
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
-				
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
GetMessageResponseObject ErrorResponseObject	json.string	application/json	1	Paket mit einer Reihe von Nachrichten mit Metadaten oder einer Fehlermeldung

Tabelle 16 — Aufzählung für AreaName

AreaNameEnum	Aufzählungswert	AreaNameEnum	Aufzählungswert
0	METAREA I	22	NAVAREA I
1	METAREA II	23	NAVAREA II
2	METAREA III	23	NAVAREA III
3	METAREA IV	25	NAVAREA IV
4	METAREA V	26	NAVAREA V
5	METAREA VI	27	NAVAREA VI
6	METAREA VII	28	NAVAREA VII
7	METAREA VIII_N	29	NAVAREA VIII
8	METAREA VIII_S	30	NAVAREA IX
9	METAREA IX	31	NAVAREA X
10	METAREA X	32	NAVAREA XI
11	METAREA XI	33	NAVAREA XII
12	METAREA XII	34	NAVAREA XIII
13	METAREA XIII	35	NAVAREA XIV
14	METAREA XIV	36	NAVAREA XV
15	METAREA XV	37	NAVAREA XVI
16	METAREA XVI	38	NAVAREA XVII
17	METAREA XVII	39	NAVAREA XVIII
18	METAREA XVIII	40	NAVAREA XIX
19	METAREA XIX	41	NAVAREA XX

AreaNameEnum	Aufzählungswert	AreaNameEnum	Aufzählungswert
20	METAREA XX	42	NAVAREA XXI
21	METAREA XXI		

5.4.7.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 17 beschrieben.

Tabelle 17 — Datenaustauschmodell für die REST-Operation „Get“

GetMessageResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
payload	string	nicht verfügbar	1	Die Daten nach Produktspezifikation, eingebettet in JSON. Die Daten dürfen verschlüsselt und signiert sein.
exchangeMetadata	string	ExchangeMetadataObject	1	Austausch-Metadaten des Dienstes mit Signatur, ID usw.
Paginierung	string	PaginationObject	1	Paginierungsinformationen
PaginationObject				
Attribut	Typ	Kodierung	Mult.	Definition
totalItems	integer	nicht verfügbar	0..1	Gesamtzahl der Elemente, die der Abfrage entsprechen. Diese wird immer zurückgegeben, sofern nicht Seite 0 angefordert wird.
maxItemsPerPage	integer	nicht verfügbar	1	Die maximale Anzahl der Elemente, die der Dienst je Seite zurückgibt.
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	string	string	1	Nachricht über Antwort mit Fehlermeldung

5.4.7.2.4 Antwort des Dienstes

Tabelle 18 beschreibt die Antwort des Dienstes.

Tabelle 18 — HTTP-Antwortcodes

HTTP-Code	Nachricht
200	GetMessageResponseObject
403	Keine Zugriffsberechtigung für angeforderte Informationen
404	Information mit <informationIdentifier> nicht gefunden
404	Information mit <reference> nicht gefunden
500	Parameterstatus=<status> nicht korrekt
500	Format der Parameter-ID=<id> nicht korrekt

5.4.7.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.7.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.8 Dienstschnittstelle – Get Summary (Zusammenfassung anfordern)

5.4.8.1 Spezifikation

Diese Schnittstelle gibt eine Liste mit Informationen zurück. Die Liste enthält Identität, Status und Kurzbeschreibung jedes Informationsobjekts. Die eigentlichen Informationsobjekte können über die „Get“-Schnittstelle abgerufen werden.

Diese Schnittstelle gibt möglicherweise eine große Anzahl von Informationsobjekten zurück und unterstützt die in 5.4.2 beschriebene Paginierung. Wird kein Parameter angegeben, ist das Standardergebnis eine leere Liste.

Tabelle 19 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 19 — Informationsaustausch für die „Get Summary“-Schnittstelle

Informationen (Eingang)	Mult.	Definition
Geometry	0..1	Geometrie in Bezug auf Informationsobjekte
AreaName	0..1	Bezeichnung des festgelegten Bereichs
UN/LOCODE	0..1	Code des definierten Objekts
TimePeriod	0..1	Zeit in Bezug auf die Gültigkeit von Informationsobjekten
Pagination information	0..1	Angeforderte Paginierungsinformationen
Informationen (Ausgang)	Mult.	Definition
Für jedes Objekt: Reference Information Identifier Status Beschreibung des Informationsobjekts	0..*	

5.4.8.2 REST-Auslegung

5.4.8.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 7 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

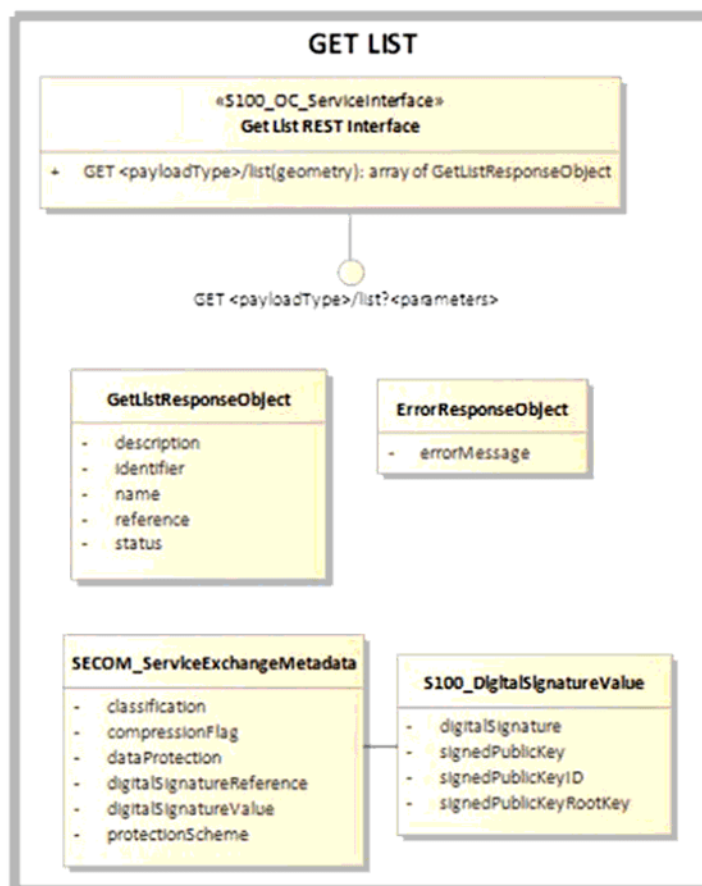


Bild 7

ExchangePattern (Austauschmuster)

- REQUEST_RESPONSE (Anforderung und Antwort)

ConsumerInterface (Konsumentenschnittstelle)

- Keine Abhängigkeit.

5.4.8.2.2 Operation – GET <Datentyp>/summary

Diese Operation wird zur Anforderung einer Zusammenfassung verfügbarer Informationen verwendet. Die Antwort enthält eine Zusammenfassung der Informationen, für die die anfordernde Person eine Autorisierung besitzt. Die eigentlichen Informationen können über eine „Subscription“-Anforderung oder eine „Get“-Anforderung abgerufen werden.

Tabelle 20 beschreibt die REST-Dienstschnittstelle.

Tabelle 20 — REST-Implementierung der „Get Summary“-Schnittstelle

REST-Operation				
GET <Datentyp>/summary				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Beschreibung
query	json.string	"key:pair"	0..1	Abfrage anhand der Aufzählungen im betreffenden S-Produkt
geometry	json.string	S-100-Geometrie (Fläche, Kurve)	0..1	Geometrie als Suchparameter im S-100-Format
areaName	json.string	codelist	0..1	Liste gültiger Namen
unlocode	json.string	char[5]	0..1	Referenz auf UN/LOCODE
fromTime	json.string	dateTime	0..1	Zeit in Bezug auf den Beginn der Gültigkeit des Informationsobjekts
toTime	json.string	dateTime	0..1	Zeit in Bezug auf den Beginn der Gültigkeit des Informationsobjekts
page	json.integer	nicht verfügbar	0..1	Angeforderte Seitenanzahl
pageSize	json.integer	nicht verfügbar	0..1	Angeforderte Seitengröße
REST-Body (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Beschreibung
GetSummaryResponseObject ErrorResponseObject	json.string	application/json	1	Liste verfügbarer Informationsobjekte (mit Zugriffsautorisierung), ermittelt nach Identität, Status und Kurzbeschreibung oder eine Fehlermeldung

5.4.8.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in [Tabelle 21](#) beschrieben.

Tabelle 21 — Datenaustauschmodell für die REST-Operation „Get Summary“

GetSummaryResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
informationSummaryObject	json.string	InformationSummaryObject	0..*	Beschreibung des Informationsobjekts
pagination	json.string	PaginationObject	1	Paginierungsinformationen
InformationSummaryObject				
Attribut	Typ	Kodierung	Mult.	Definition
messageIdentifier	json.string	UUID MRN Zeitstempel oder Kombination daraus	1	Referenz auf Daten
identifier	json.string	abhängig von der Informationsproduktspezifikation	1	Kennung des Informationsobjekts
name	json.string	nicht verfügbar	1	Bezeichnung des Informationsobjekts
statusEnum	json.string	abhängig von der Informationsproduktspezifikation	0..1	Status des Informationsobjekts
description	json.string	nicht verfügbar	1	Beschreibung des Informationsobjekts
PaginationObject				
Attribut	Typ	Kodierung	Mult.	Definition
totalItems	json.integer	nicht verfügbar	0..1	Gesamtzahl der Elemente, die der Abfrage entsprechen. Diese wird immer zurückgegeben, sofern nicht Seite 0 angefordert wird.
maxItemsPerPage	json.integer	nicht verfügbar	1	Die maximale Anzahl der Elemente, die der Dienst je Seite zurückgibt.
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	json.string	nicht verfügbar	1	Nachricht über Antwort mit Fehlermeldung

5.4.8.2.4 Antwort des Dienstes

Tabelle 22 beschreibt die Antwort des Dienstes.

Tabelle 22 — HTTP-Antwortcodes und Nachrichten

HTTP-Code	Nachricht
200	GetSummaryResponseObject
403	Keine Zugriffsberechtigung für angeforderte Informationen
404	Informationen nicht gefunden

5.4.8.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.8.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.9 Dienstschnittstelle – Subscription (Subscription)

5.4.9.1 Spezifikation

Der Zweck der Schnittstelle besteht darin, eine Subskription von Informationen anzufordern. Dabei kann es sich um spezifische Informationen entsprechend bestimmter Parameter handeln oder um Informationen, die aufgrund einer Entscheidung des Informationsanbieters zugänglich sind.

Tabelle 23 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 23 — Informationsaustausch für die „Subscription“-Schnittstelle

Informationen (Eingang)	Mult.	Definition
Information Identifier	0..1	Kennung des Informationsobjekts
Status	0..1	Status des Informationsobjekts
Geometry	0..1	Geometrische Beschaffenheit bei Informationsobjekten mit Geolokalisierung
AreaName	0..1	Bezeichnung des festgelegten Bereichs
UN/LOCODE	0..1	Code des definierten Objekts
Informationen (Ausgang)	Mult.	Definition
Subscription Identifier	0..1	Kennung für die erstellte Subskription, sofern Autorisierung besteht. Für die Entfernung von Subskriptionen („Remove Subscription“-Schnittstelle) zu verwenden. Wenn die Subskriptionsanforderung mehr als einem Informationsobjekt entspricht, sind alle diese Informationsobjekte Teil einer Subskription.

5.4.9.2 REST-Auslegung

5.4.9.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 8 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

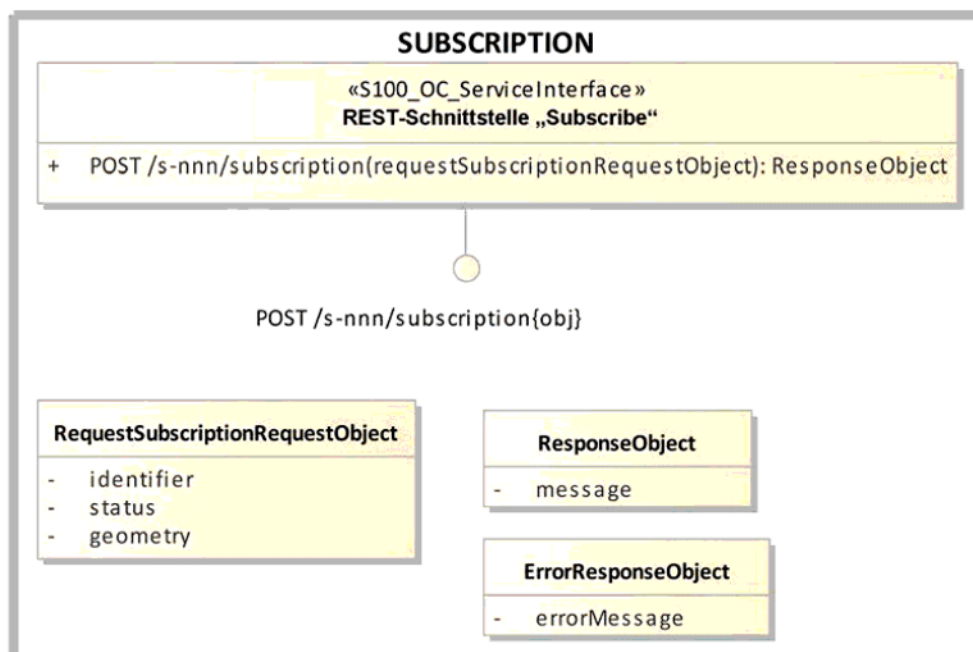


Bild 8 — REST-Schnittstelle „Subscribe“

ExchangePattern (Austauschmuster)

- PUBLISH_SUBSCRIBE (Veröffentlichen und abonnieren)

ConsumerInterface (Konsumentenschnittstelle)

- Dienstschnittstelle „Upload“
- Dienstschnittstelle „Subscription Notification“

5.4.9.2.2 Operation – POST <Datentyp>/subscription

Diese Operation wird zur Anforderung von Subskriptionen verwendet. Besitzt die anfordernde Person die erforderliche Autorisierung, wird eine Subskription erstellt und die neueste Nachricht wird gesendet.

Tabelle 24 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 24 — REST-Implementierung der „Subscription“-Schnittstelle

REST-Operation				
POST <Datentyp>/subscription				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
RequestSubscriptionRequestObject	string	application/json	0..1	Spezifische ID des Informationsobjekts, für die eine Subskription angefordert wird Spezifischer Status der Information Spezifischer Interessenbereich
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
ResponseObject ErrorResponseObject	string	application/json	1	Bestätigung oder Fehlermeldung Wenn in Ordnung, wird SubscriptionIdentifier zurückgegeben.

5.4.9.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 25 beschrieben.

Tabelle 25 — Datenaustauschmodell für die REST-Operation „Subscription“

RequestSubscriptionRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
identifier	string	abhängig von der Informationsproduktspezifikation	0..1	Kennung des Informationsobjekts
statusEnum	string	abhängig von der Produktspezifikation	0..1	Status im Informationsobjekt
geometry	json.string	S-100-Geometrie (Fläche, Kurve)	0..1	Geometrie als Kriterium im S-100-Format.
areaName	json.string	AreaNameList	0..1	Codeliste
unlocode	json.string	char [5]	0..1	Nach UN/LOCODE
ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	json.string	nicht verfügbar	1	Antwortnachricht
subscriptionIdentifier	json.string	UUID	0..1	SubscriptionIdentifier, wenn erfolgreich

5.4.9.2.4 Antwort des Dienstes

Tabelle 26 beschreibt die Antwort des Dienstes.

Tabelle 26 — HTTP-Antwortcodes und Nachrichten

HTTP-Code	Nachricht
200	Subskription erfolgreich erstellt
403	Keine Zugriffsberechtigung für angeforderte Informationen
404	Informationen nicht gefunden

5.4.9.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.9.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.10 Dienstschnittstelle – Remove Subscription (Subskription entfernen)

5.4.10.1 Allgemeines

Subskriptionen können entweder intern durch den Informationseigner oder extern auf Anforderung durch den Konsumenten entfernt werden. Diese Schnittstelle wird vom Konsumenten verwendet, um die Entfernung einer Subskription anzufordern.

Tabelle 27 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 27 — Parameterbindung für „Remove Subscription“

Informationen (Eingang)	Mult.	Definition
Subscription Identifier	0..1	Kennung der Subskription. Bei der Erstellung der Subskription abgerufen
Informationen (Ausgang)	Mult.	Definition
Ergebnis aus Operation	1	

5.4.10.2 REST-Auslegung

5.4.10.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 9 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

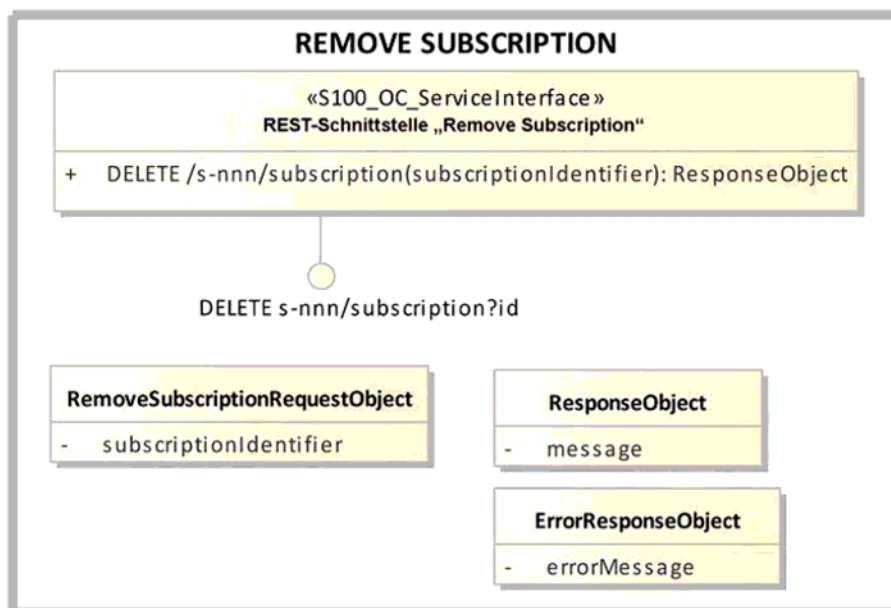


Bild 9 — REST-Schnittstelle „Remove Subscription“

ExchangePattern (Austauschmuster)

- ONE_WAY (einseitig)

ConsumerInterface (Konsumentenschnittstelle)

- Dienstschnittstelle „Subscription Notification“

5.4.10.2.2 Operation – DELETE <Datentyp>/subscription

Diese Operation wird zum Löschen von Subskriptionen verwendet.

Tabelle 28 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 28 — REST-Implementierung der „Remove Subscription“-Schnittstelle

REST-Operation				
DELETE <Datentyp>/subscription				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Beschreibung
RemoveSubscriptionRequestObject	json.string	application/json	0..1	Spezifische Identität des Informationsobjekts, dessen Subskription gelöscht werden soll. Wird keine ID (Identität) angegeben, werden alle Subskriptionen der anfordernden Person entfernt
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Beschreibung
ResponseObject	json.string	application/json	1	Bestätigung oder Fehlermeldung

5.4.10.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 29 beschrieben.

Tabelle 29 — Datenaustauschmodell für die REST-Operation „Delete Subscription“

RemoveSubscriptionRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
subscriptionIdentifier	string	UUID	1	Kennung der Subskription, die entfernt werden soll. Empfangen bei Subskriptionsanforderung oder Subskriptionsbenachrichtigung.
ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	string		1	Antwortnachricht

5.4.10.2.4 Antwort des Dienstes

Tabelle 30 beschreibt die Antwort des Dienstes.

Tabelle 30 — HTTP-Antwortcodes und Nachrichten

HTTP-Code	Nachricht
200	Subskription <identifier> entfernt
403	Keine Berechtigung für Entfernung der Subskription
404	Subskriptionskennung nicht gefunden

5.4.10.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.10.3 Prüfmethoden und erwartetes Ergebnis

Noch festzulegen

5.4.11 Dienstschnittstelle – Get Subscription List (Subskriptionsliste anfordern)

5.4.11.1 Spezifikation

Über diese Schnittstelle wird eine Liste der aktiven Subskriptionen abgerufen.

Tabelle 31 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 31 — Informationsaustausch für die „Get Subscription List“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
-		
ReturnType (Ausgang)	Mult.	Definition
Subscription Identifier	0..*	Kennung der Subskription.
Subscription Parameters	0..*	Bei der Erstellung der Subskription verwendete Parameter.

5.4.11.2 REST-Auslegung

5.4.11.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 10 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

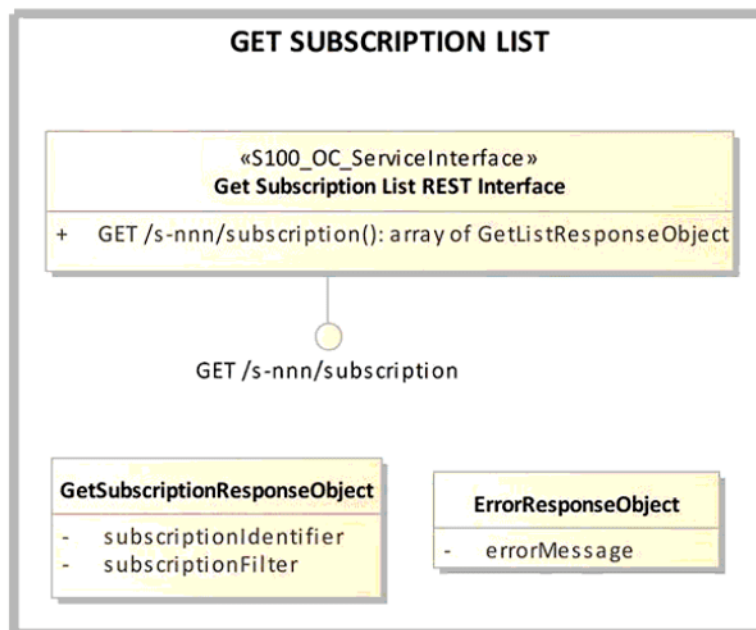


Bild 10 — REST-Schnittstelle „Get Subscription List“

ExchangePattern (Austauschmuster)

- REQUEST_RESPONSE (Anforderung und Antwort)

ConsumerInterface (Konsumentenschnittstelle)

- Keine Abhängigkeit.

5.4.11.2.2 Operation – GET <Datentyp>/subscription

Diese Operation wird zur Anforderung einer Liste der aktiven Subskriptionen der anfordernden Person verwendet. Die Antwort enthält alle aktiven Subskriptionen der anfordernden Person.

[Tabelle 32](#) beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 32 — REST-Implementierung der „Get Subscription List“-Schnittstelle

REST-Operation				
POST <Datentyp>/subscription				
REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
-				
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
Feld von GetListResponseObject ErrorResponseObject	character string	application/json	1	Liste von Identitäten oder Fehlermeldung

5.4.11.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 33 beschrieben.

Tabelle 33 — Datenaustauschmodell für die REST-Operation „Get Subscription List“

GetListResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
subscriptionIdentifizier	string	UUID	1	Subskriptionskennung. Kann bei Entfernung der Subskription verwendet werden.
subscriptionFilter	string	SubscriptionFilter	0..*	Beschreibung der Subskriptionsfilter-Parameter
SubscriptionFilter				
Attribut	Typ	Kodierung	Mult.	Definition
Schlüssel	string		1	Filterparameter-Schlüssel
value	string		1	Filterparameter-Wert
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	string	string	1	Nachricht über Antwort mit Fehlermeldung

5.4.11.2.4 Antwort des Dienstes

Der Dienst muss mit HTTP-Codes und einer Nachricht nach Tabelle 34 antworten.

Tabelle 34 — HTTP-Antwortcodes

HTTP-Code	Nachricht
200	Feld von GetListResponseObject
403	Keine Zugriffsberechtigung für angeforderte Informationen

5.4.11.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.11.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.12 Dienstschnittstelle – Subscription Notification (Subskriptionsbenachrichtigung)

5.4.12.1 Spezifikation

Die Schnittstelle dient zum Erhalt einer Benachrichtigung, wenn eine Subskription durch den Informationsproduzenten erstellt oder entfernt wird.

[Tabelle 35](#) beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 35 — Informationsaustausch für die „Subscription Notification“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
Subscription Identifier	1	Kennung der Subskription.
Ereignis	1	Ereignistyp: Erstellen, Löschen
ReturnType (Ausgang)	Mult.	Definition
Ergebnis aus Operation	1	

5.4.12.2 REST-Auslegung

5.4.12.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 11 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

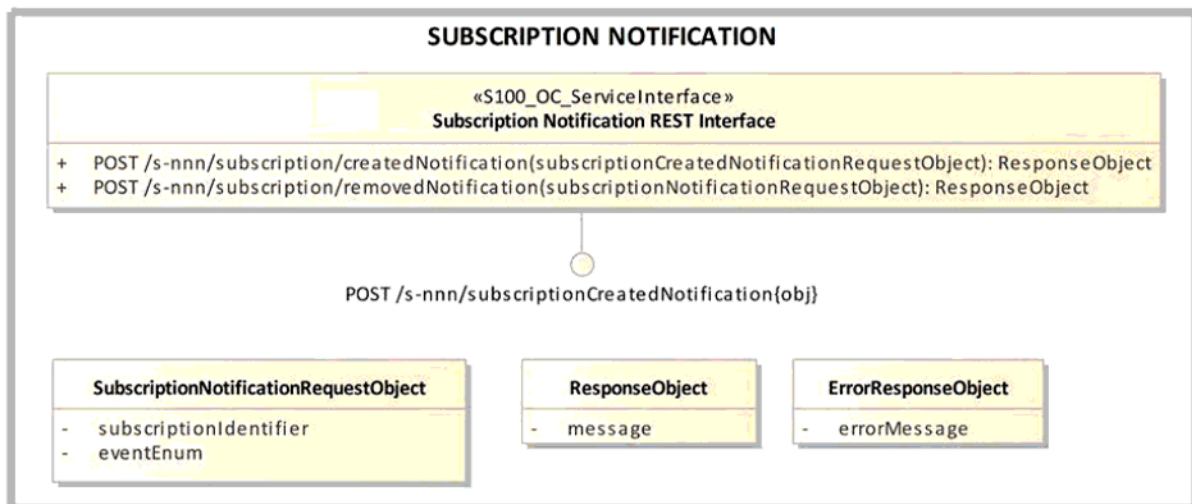


Bild 11 — REST-Schnittstelle „Subscription Notification“

ExchangePattern (Austauschmuster)

- ONE_WAY (einseitig)

ConsumerInterface (Konsumentenschnittstelle)

- Keine Abhängigkeit.

5.4.12.2.2 Operation – POST <Datentyp>/subscription/notification

Diese Operation dient zum Erhalt einer Benachrichtigung, wenn eine Subskription – intern durch den Informationsproduzenten oder extern auf Anforderung durch den Konsumenten – erstellt wird.

Tabelle 36 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 36 — Operation – POST <Datentyp>/subscription/notification

REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Beschreibung
SubscriptionNotificationRequestObject	string	application/json		Enthält die Identität des betreffenden Informationsobjekts und Ereignistyps (Erstellen oder Löschen)
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Beschreibung
ResponseObject	string	application/json		Bestätigung oder Fehlermeldung

5.4.12.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 37 beschrieben.

Tabelle 37 — Datenaustauschmodell für die REST-Operation „Subscription Notification“

SubscriptionNotificationRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
subscriptionIdentifier	string		1	
eventEnum	string	EnumEvent	1	
ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	string		1	Nachricht über erfolgreiche Antwort
EnumEvent				
Enum	Typ	Kodierung		Definition
Create	string			„Erstellen“-Ereignis
Delete	string			„Löschen“-Ereignis

5.4.12.2.4 Antwort des Dienstes

Der Dienst muss mit HTTP-Codes und einer Nachricht nach Tabelle 38 antworten.

Tabelle 38 — HTTP-Antwortcodes

HTTP-Code	Nachricht
200	noch festzulegen
403	Keine Zugriffsberechtigung für angeforderte Informationen

5.4.12.2.5 Dynamisches Verhalten

5.4.12.3 Prüfmethode und erwartetes Ergebnis

5.4.13 Dienstschnittstelle – Request Access (Zugriff anfordern)

5.4.13.1 Spezifikation

Der Zugriff auf Informationen kann über die „Request Access“-Schnittstelle angefordert werden. Das Ergebnis wird asynchron über die „Access Notification“-Schnittstelle gesendet.

Tabelle 39 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 39 — Informationsaustausch für die „Request Access“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
Reason	1	Visuell lesbarer Grund für die Informationsanforderung
ReasonEnum	1	Maschinenlesbar
Status		z. B. routeStatus überwacht
ReturnType (Ausgang)	Mult.	Definition
Ergebnis aus Operation	1	

5.4.13.2 REST-Auslegung

5.4.13.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in [Bild 12](#) als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

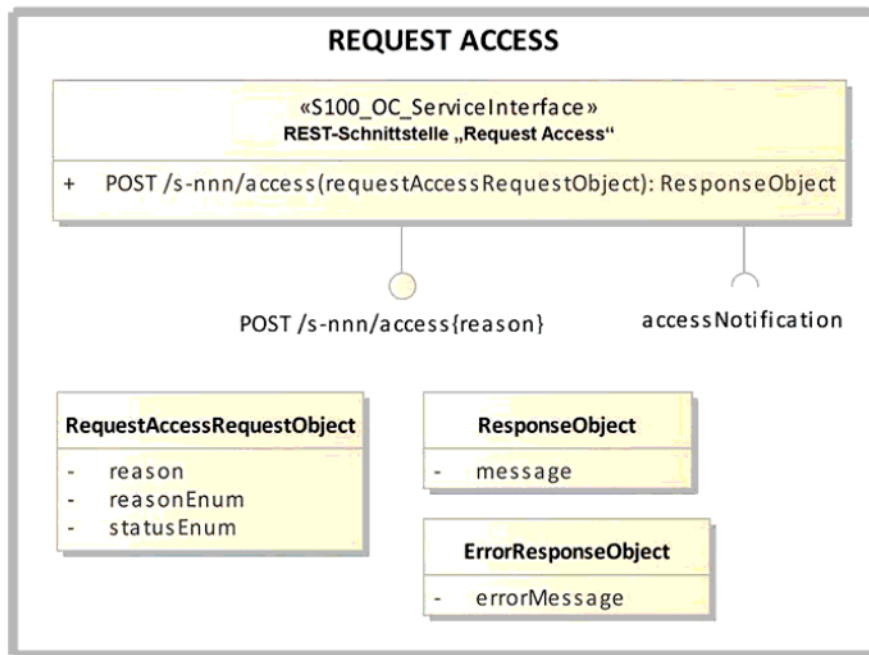


Bild 12 — REST-Schnittstelle „Request Access“

ExchangePattern (Austauschmuster)

- REQUEST_CALLBACK (Anforderung und Rückmeldung)

ConsumerInterface (Konsumentenschnittstelle)

- Dienstschnittstelle „Access Notification“

5.4.13.2.2 Operation – POST <Datentyp>/access/request

Diese Operation wird zur Zugriffsanforderung durch einen Konsumenten verwendet. Das Ergebnis wird asynchron gesendet.

Tabelle 40 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 40 — Parameterbindung für die Operation

REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
RequestAccessRequestObject	character string	application/json	1	Beschreibung des Grundes für die Informationsanforderung
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
ResponseObject ErrorResponseObject	character string	application/json	1	Bestätigung oder Fehlermeldung. Das Ergebnis der Anforderung wird asynchron über die „Access Notification“-Schnittstelle gesendet.

5.4.13.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in [Tabelle 41](#) beschrieben.

Tabelle 41 — Datenaustauschmodell für die REST-Operation „Request Access“

RequestAccessRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
reason	string		1	Visuell lesbarer Grund für die Informationsanforderung
reasonEnum	string	enumReason	1	Maschinenlesbarer Grund für die Informationsanforderung
statusEnum	string	EnumStatus	0..1	Status des Informationsobjekts, für das der Zugriff angefordert wird
ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	string		1	Nachricht über erfolgreiche Antwort
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	string		1	Nachricht über Antwort mit Fehlermeldung
EnumReason				
Enum	Typ	Kodierung	Mult.	Definition
Noch festzulegen				
EnumStatus				
Enum	Typ	Kodierung	Mult.	Definition
Noch festzulegen				<Abhängig von der Informationsproduktspezifikation>

5.4.13.2.4 Antwort des Dienstes

Tabelle 42 beschreibt die Antwort des Dienstes.

Tabelle 42 — HTTP-Antwortcodes

HTTP-Code	Nachricht
200	noch festzulegen
403	Keine Zugriffsberechtigung für angeforderte Informationen

5.4.13.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.13.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.14 Dienstschnittstelle – Access Notification (Zugriffsbenachrichtigung)

5.4.14.1 Spezifikation

Das Ergebnis der Zugriffsanforderung wird asynchron über diese Schnittstelle gesendet.

Tabelle 43 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 43 — Informationsaustausch für die „Access Notification“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
Decision	1	Entscheidung
Reason	1	Visuell lesbarer Grund für die Entscheidung
ReasonEnum	1	Maschinenlesbarer Grund für die Entscheidung
ReturnType (Ausgang)	Mult.	Definition

Parameter (Eingang)	Mult.	Definition
Ergebnis aus Operation	1	

5.4.14.2 REST-Auslegung

5.4.14.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 13 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

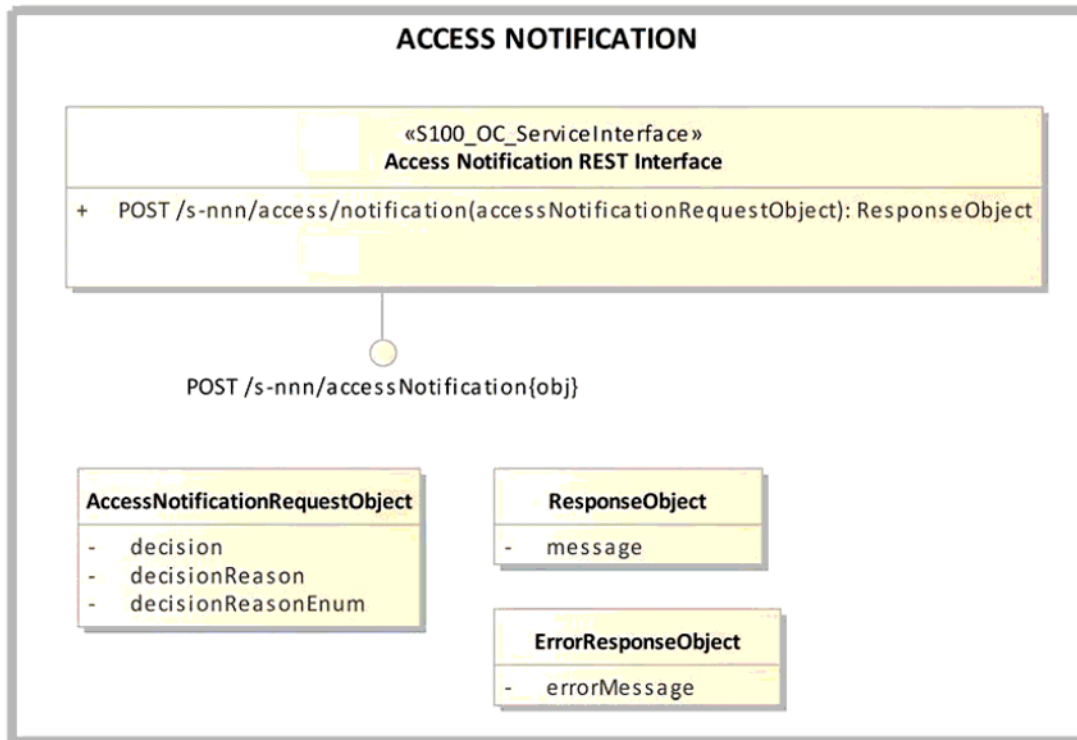


Bild 13 — REST-Schnittstelle „Access Notification“

ExchangePattern (Austauschmuster)

- ONE_WAY (einseitig)

ConsumerInterface (Konsumentenschnittstelle)

- Keine Abhängigkeit.

5.4.14.2.2 Operation – POST <Datentyp>/access/notification

Diese Operation wird zur Abfrage des Ergebnisses einer Zugriffsanforderung verwendet.

Tabelle 44 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 44 — Parameterbindung für die Operation

REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
AccessNotificationRequestObject	characterString	application/json		Ergebnis der Zugriffsanforderung: True oder False
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
ResponseObject ErrorResponseObject	character string	application/json	1	Bestätigung oder Fehlermeldung

5.4.14.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 45 beschrieben.

Tabelle 45 — Datenaustauschmodell für die REST-Operation „Access Notification“

AccessNotificationRequestObject				
Attribut	Typ	Kodierung	Mult.	Definition
decision	boolean		1	Entscheidung über Anforderung: ja oder nein
decisionReason	string		1	Visuell lesbarer Grund für die Entscheidung
decisionReasonEnum	string	DecisionReasonEnum	1	Maschinenlesbarer Grund für die Entscheidung
ResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
message	string		1	Nachricht über erfolgreiche Antwort
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	string		1	Nachricht über Antwort mit Fehlermeldung
DecisionReasonEnum				
Enum	Typ	Kodierung		Definition
Noch festzulegen				

5.4.14.2.4 Antwort des Dienstes

Tabelle 46 beschreibt die Antwort des Dienstes.

Tabelle 46 — HTTP-Antwortcodes

HTTP-Code	Nachricht
200	noch festzulegen
403	Keine Zugriffsberechtigung für angeforderte Informationen

5.4.14.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.14.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.15 Dienstschnittstelle – Capability (Funktionalität)

5.4.15.1 Spezifikation

Der Zweck der Schnittstelle besteht darin, ein dynamisches Verfahren bereitzustellen, um über eine Dienstinstanz während der Laufzeit abzufragen, auf welche Schnittstellen zugegriffen werden kann und welche Nutzdatenformate und Version gültig sind.

Tabelle 47 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 47 — Informationsaustausch für die „Capability“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
-		
ReturnType (Ausgang)	Mult.	Definition
Capability	1	Beschreibung der Dienstschnittstelle „Capability“.

Parameter (Eingang)	Mult.	Definition
		Die Dienstschnittstelle „Capability“ beinhaltet Flags, die anzeigen, mit welchen Schnittstellen und mit welchen Informationsprodukten der Dienst umgehen kann

5.4.15.2 REST-Auslegung

5.4.15.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 14 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

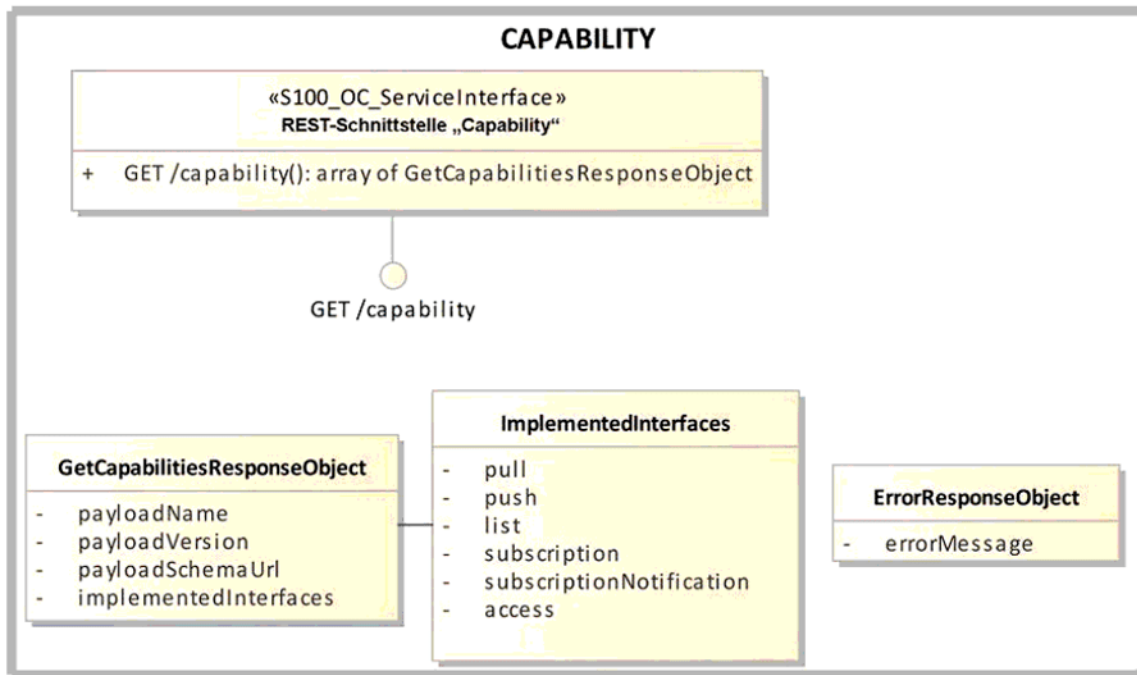


Bild 14 — REST-Schnittstelle „Capability“

ExchangePattern (Austauschmuster)

- REQUEST_RESPONSE (Anforderung und Antwort)

ConsumerInterface (Konsumentenschnittstelle)

- Keine Abhängigkeit.

5.4.15.2.2 Operation – GET capability

Diese Operation wird zur Abfrage der Funktionalitäten einer Dienstschnittstelle verwendet. Das Ergebnis enthält die von der Dienstinstanz bereitgestellten Schnittstellen und den behandelten Informationsprodukttyp.

Tabelle 48 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 48 — REST-Implementierung der „Capability“-Schnittstelle

REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Definition
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Definition
-				
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Definition
Feld von GetCapabilitiesResponseObject	character string	application/json	1..*	Beschreibung der Dienstfähigkeiten; gültige Schnittstellen für die jeweilige Dienstinstanz,

ErrorResponseObject				zulässiges Nutzdatenformat und Version, spezifische Anforderungen in den Nutzdaten usw.
---------------------	--	--	--	---

5.4.15.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 49 beschrieben.

Tabelle 49 — Datenaustauschmodell für die REST-Operation „Capability“

GetCapabilitiesResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
payloadName	string		1	
payloadVersion	string		1	
payloadSchemaUrl	string	URL	1	
implementedInterfaces	ImplementedInterfaces (implementierte Schnittstellen)		1	
ImplementedInterfaces				
Attribut	Typ	Kodierung	Mult.	Definition
upload	boolean		1	
get	boolean		1	
getSummary	boolean		1	
subscription	boolean		1	
access	boolean		1	
description	boolean		1	
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	string		1	Nachricht über Antwort mit Fehlermeldung

5.4.15.2.4 Antwort des Dienstes

Tabelle 50 beschreibt die Antwort des Dienstes.

Tabelle 50 — HTTP-Antwortcodes und Nachrichten

HTTP-Code	Nachricht
200	GetCapabilityResponseObject
403	Keine Zugriffsberechtigung für angeforderte Informationen

5.4.15.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.15.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.16 Dienstschnittstelle – Description (Beschreibung)

5.4.16.1 Spezifikation

Der Zweck der Schnittstelle besteht darin, ein dynamisches Verfahren zur Abfrage einer operationellen/benutzerbezogenen Beschreibung der jeweiligen Dienstinstanz bereitzustellen.

Die Antwort des Dienstes enthält Informationen, wie die Dienstinstanz zu nutzen/in Anspruch zu nehmen ist, sowie die erwarteten Eingangs- und Ausgangsdaten der Dienstinstanz.

Tabelle 51 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 51 — Informationsaustausch für die „Description“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
-		
ReturnType (Ausgang)	Mult.	Definition
Description	1	Während der Laufzeit von der Dienstinstanz gemeldete Beschreibung des Dienstes

5.4.16.2 REST-Auslegung

5.4.16.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 15 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

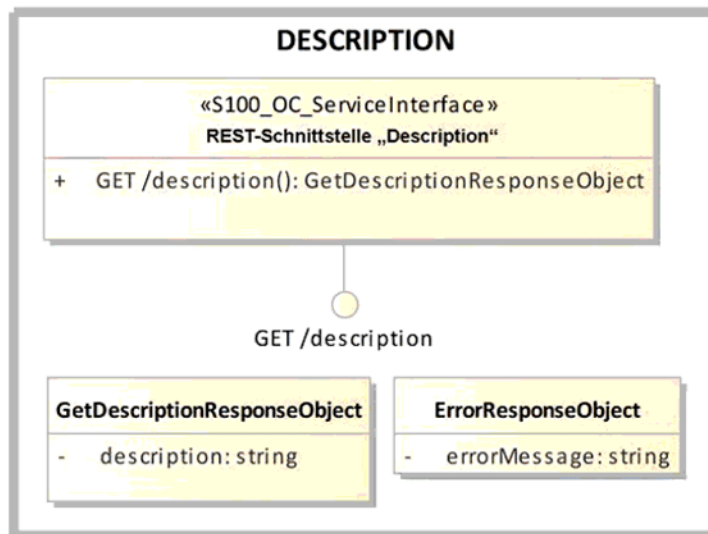


Bild 15 — REST-Schnittstelle „Description“

ExchangePattern (Austauschmuster)

- REQUEST_RESPONSE (Anforderung und Antwort)
- ConsumerInterface (Konsumentenschnittstelle)
Keine Abhängigkeit.

5.4.16.2.2 Operation – GET description

Diese Operation wird zur Anforderung der Beschreibung einer Dienstinstanz verwendet.

Tabelle 52 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 52 — REST-Implementierung der „Description“-Schnittstelle

REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Beschreibung
GetDescriptionResponseObject ErrorResponseObject	character string	application/json	1	Beschreibung der Dienstschnittstelle.

5.4.16.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 53 beschrieben.

Tabelle 53 — Datenaustauschmodell für die REST-Operation „Description“

GetDescriptionResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
description	string	Noch festzulegen?	1	Operationelle Kurzbeschreibung der Dienstinstanz
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	string		1	Nachricht über Antwort mit Fehlermeldung

5.4.16.2.4 Antwort des Dienstes

Tabelle 54 beschreibt die Antwort des Dienstes.

Tabelle 54 — HTTP-Antwortcodes

HTTP-Code	Nachricht
200	GetDescriptionResponseObject
403	Keine Zugriffsberechtigung für angeforderte Informationen

5.4.16.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.16.3 Prüfmethoden und erwartetes Ergebnis

Noch festzulegen

5.4.17 Dienstschnittstelle – Status

5.4.17.1 Spezifikation

Der Zweck der Schnittstelle besteht darin, ein dynamisches Verfahren zur Abfrage des technischen Status der jeweiligen Dienstinstanz bereitzustellen.

Tabelle 55 beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 55 — Informationsaustausch für die „Status“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
-		
ReturnType (Ausgang)	Mult.	Definition
Description	1	Während der Laufzeit von der Dienstinstanz gemeldeter Status des Dienstes

5.4.17.2 REST-Auslegung

5.4.17.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 16 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

Noch festzulegen

Bild 16

ExchangePattern (Austauschmuster)

- REQUEST_RESPONSE (Anforderung und Antwort)
- ConsumerInterface (Konsumentenschnittstelle)
Keine Abhängigkeit.

5.4.17.2.2 Operation – GET status

Diese Operation wird zur Statusabfrage einer Dienstinstantz verwendet.

Tabelle 56 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 56 — REST-Implementierung der „Status“-Schnittstelle

REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Beschreibung
GetStatusResponseObject	Typ	application/json	1	Status der Dienstschnittstelle

5.4.17.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 57 beschrieben.

Tabelle 57 — Datenaustauschmodell für die REST-Operation „Description“

GetStatusResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
status	string	Noch festzulegen	1	Operationelle Kurzbeschreibung der Dienstinstantz
ErrorResponseObject				
Attribut	Typ	Kodierung	Mult.	Definition
errorMessage	string		1	Nachricht über Antwort mit Fehlermeldung

5.4.17.2.4 Antwort des Dienstes

Tabelle 58 beschreibt die Antwort des Dienstes.

Tabelle 58 — HTTP-Antwortcodes

HTTP-Code	Nachricht
200	GetDescriptionResponseObject
403	Keine Zugriffsberechtigung für angeforderte Informationen

5.4.17.2.5 Dynamisches Verhalten

Noch festzulegen

5.4.17.3 Prüfmethode und erwartetes Ergebnis

Noch festzulegen

5.4.18 Dienstschnittstelle – EncryptionKey (kryptografischer Schlüssel)

5.4.18.1 Spezifikation

Der Zweck dieser Schnittstelle besteht im Austausch eines temporären geheimen Schlüssels.

[Tabelle 59](#) beschreibt die in der Schnittstelle ausgetauschten Daten.

Tabelle 59 — Informationsaustausch für die „EncryptionKey“-Schnittstelle

Parameter (Eingang)	Mult.	Definition
Encrypted Key	1	
Signature	1	
ReturnType (Ausgang)	Mult.	Definition
ResponseObject	1	Antwort des Dienstes

5.4.18.2 REST-Auslegung

5.4.18.2.1 Allgemeines

Die Dienstschnittstelle entsprechend der REST-Technologie ist in Bild 17 als UML-Modell definiert. Die Informationsaustauschobjekte sind ebenfalls dort definiert.

Noch festzulegen

Bild 17

ExchangePattern (Austauschmuster)

- ONE_WAY (einseitig)
- ConsumerInterface (Konsumentenschnittstelle)
- Keine Abhängigkeit.

5.4.18.2.2 Operation – POST key

Diese Operation dient zum Versand eines geheimen kryptografischen Schlüssels an einen Konsumenten.

Tabelle 60 beschreibt die logischen Parameter in der Schnittstelle.

Tabelle 60 — REST-Implementierung der „EncryptionKey“-Schnittstelle

REST-Parameter (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
REST-Body (Eingang)	Typ	Kodierung	Mult.	Beschreibung
-				
Rückgabe (Ausgang)	Typ	Kodierung	Mult.	Beschreibung
ResponseObject	character string	application/json	1	Antwort des Dienstes

5.4.18.2.3 Datenaustauschmodell

Die ausgetauschten Daten in der Dienstschnittstelle sind ausführlich in Tabelle 61 beschrieben.

Tabelle 61 — Datenaustauschmodell für die REST- Implementierung der „EncryptionKey“-Schnittstelle

Noch festzulegen				
Attribut	Typ	Kodierung	Mult.	Definition
DigitalSignatureValueObject				
Attribut	Typ	Kodierung	Mult.	Definition
signedPublicKeyID	string		1	(S-100) Behauptete Identität des Unterzeichners
signedPublicKeyRootKey	string		1	(S-100) Behaupteter Rootschlüssel in Bezug auf das gewählte Schutzkonzept
signedPublicKey	string		1	(S-100) Öffentlicher Schlüssel für die behauptete Identität