
Spezifikation XTA Service Profile

*Modul des Standards XTA 2
Grobentwurf / Konzept - Version 2.0.0*

Fassung: 02.09.2026

Herausgeber: Koordinierungsstelle für IT-Standards

Bezugsort: www.xoev.de

Inhaltsverzeichnis

1 Einführung	1
1.1 Grundlegende Nutzung	1
1.2 Offene Punkte	6
2 Voraussetzungen	7
2.1 Konformität	7
3 Datenmodell	8
3.1 Hauptprofil und Basisdatentypen	8
3.2 Unterprofil Gewährleistungsziele	12
3.3 Unterprofil Fachdienst	20
3.4 Unterprofil Transportinfrastruktur	23
3.5 Unterprofil Kryptografie	32
3.6 Unterprofil Automatisierung	33
3.7 Nachweisbarkeit der Servicequalitäten	43
A Anhänge	47
A.1 Eingebundene externe Modelle	47
A.2 Übersicht Code-Datentypen	47
A.3 Codes	48
A.4 Codelisten	55
A.5 Versionshistorie	56
A.6 Mitwirkende	56

1 Einführung



Der vorliegende Grobentwurf / Konzept dient als konzeptionelle Grundlage für die weitere Ausarbeitung des Moduls *XTA Service Profile*. Der Standard XTA einschließlich seiner Module und Erweiterungen wird im Auftrag des IT-Planungsrates in den Gremien *Sicherer Transport* betrieben und fortentwickelt. Sämtliche fachlichen und technischen Details werden im zuständigen Expertengremium erarbeitet. Eine Mitwirkung an der Weiterentwicklung ist über die Mitgliedschaft in den Gremien oder durch die offizielle Einreichung eines Change Requests (CR) möglich. Weitere Informationen zu Gremienstruktur und Beteiligungsmöglichkeiten enthält das Betriebskonzept unter www.xoev.de/sicherertransport/betriebskonzept.

1.1 Grundlegende Nutzung

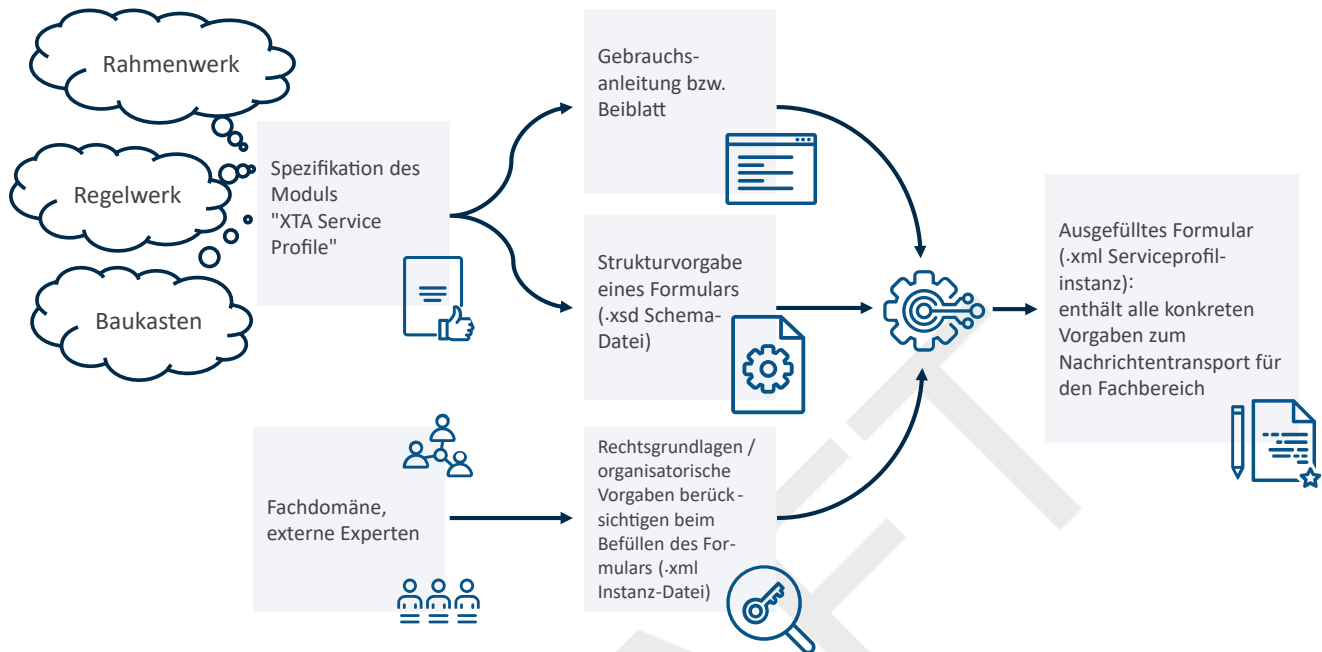
In diesem Abschnitt wird die Entstehung, die Struktur und die Verwendung einer Serviceprofilinstanz entsprechend dem Modul XTA Service Profile erläutert. Es wird ein grundlegendes Verständnis für die übergreifende Bedeutung von Serviceprofilinstanzen im Kontext des Transports von Fachnachrichten bzw. der Datenübermittlungen in und außerhalb der öffentlichen Verwaltung vermittelt.

Das Modul XTA Service Profile trägt XTA im Namen, da es im Kontext von XTA entwickelt wurde. Seine Verwendbarkeit ist gänzlich unabhängig vom konkret genutzten Technologien, Standards, Produkten und Infrastrukturen. Folglich ist ebenfalls die Verwendung des Moduls XTA Webservice möglich, jedoch nicht zwingend erforderlich (vgl. [Abbildung 1.4](#)).

Für den sicheren Transport von elektronischen Fachnachrichten in der öffentlichen Verwaltung gibt es Vorgaben auf unterschiedlicher Ebene: fachliche, technische, kryptografische sowie datenschutzrechtliche. Das Modul XTA Service Profile ermöglicht mit dessen einheitlichen Datenstrukturen die Festlegung von konkreten Vorgaben in Form von Unterprofilen (UP). Die Vorgaben liegen sodann in der maschinenlesbaren Form, womit unter anderem eine systemübergreifende Steuerung der Prozesse innerhalb der Softwaresysteme realisiert werden kann.

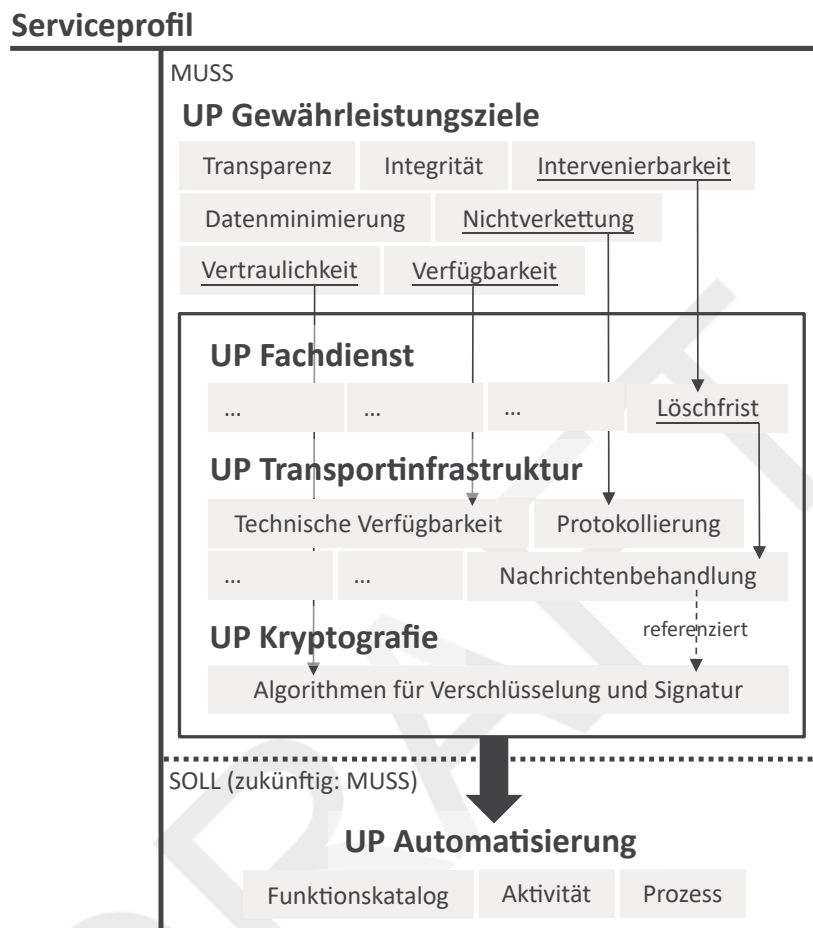
Die jeweilige Fachlichkeit befüllt ein Serviceprofil (Hauptprofil) mit den, für sie geltenden, Vorgaben und erstellt damit eine konkrete Serviceprofilinstanz (vgl. [Abbildung 1.1](#) und [Abbildung 1.3](#)). Ausgangspunkt sind die Vorgaben zu den Gewährleistungszielen des Datenschutzes. So bedingen die Vorgaben im Gewährleistungsziel des Intervenierbarkeit eine fachspezifische Vorgabe zur Löschfrist. Anhand des festgelegten Niveaus für die Löschfrist werden konkrete technischen Werte für die Nachrichtenbehandlung auf der operativen Ebene abgeleitet (vgl. [Abbildung 1.2](#)). Mit dem Unterprofil Automatisierung können alle bisherigen Vorgaben in eine Aktivitäts-/Prozessmodellierung überführt werden. Das Ergebnis soll für eine vollständig automatisierte Abwicklung des Nachrichtentransports und sogar die Verarbeitung des Fachnachrichten außerhalb des Nachrichtentransports auf der technischen Ebene mit Hilfe von Regelwerken genutzt werden können (Folgen: maximale Prozessagilität, niedriger ggf. kein Softwareentwicklungsaufwand bei geänderten Rahmenbedingungen, Stärkung der digitalen Governance, bundesweit einheitliche Bausteine/Bibliotheken, *...to be continued*).

Abbildung 1.1. Prozesssicht zur Entstehung einer Serviceprofilinstanz als schematische Darstellung



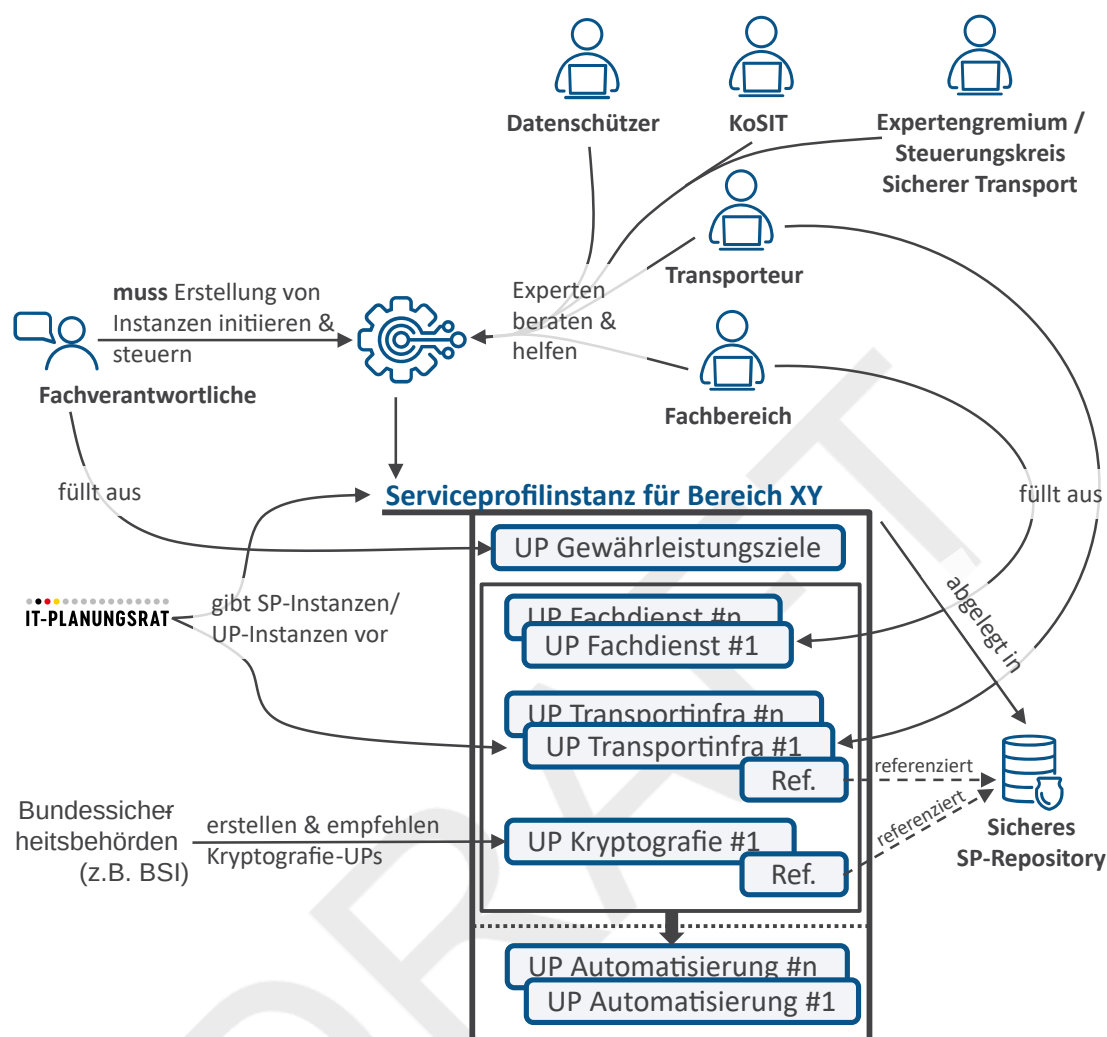
Die Spezifikation ist mit einem Formularbündel und einem Beiblatt vergleichbar. Einige Formulare sind obligatorisch, andere können für wiederkehrende ggf. ähnliche Sachverhalte mehrfach verwendet werden. Auf technischer Ebene werden dafür Schemata bereitgestellt, die gemäß der Spezifikation die konkrete fachliche Ausprägung in Form einer XML-Instanz ermöglichen. Alle Festlegungen müssen mit den jeweils gültigen rechtlichen, organisatorischen und technischen Rahmenbedingungen konform sein. Die resultierende Serviceprofilinstanz wird für den Nachrichtentransport als verbindlich erklärt und ist auf operativer Ebene einzuhalten. Struktur und Verantwortlichkeiten orientieren sich am im Abschnitt *XTA Rollenmodell* der [XTA Rahmenbedingungen](#) beschriebenen Rollenbild, den Vorgaben und Abläufen.

Abbildung 1.2. Schematische Darstellung des Zusammenwirkens der Unterprofile (UP) im Serviceprofil anhand ausgewählter Elemente



Eine Serviceprofilinstanz besteht aus mehreren Unterprofilen mit jeweils spezifischem Fokus. Das Unterprofil *Gewährleistungsziele* definiert die abstrakten Anforderungen und dient als Leitlinie für die Ausgestaltung der weiteren Unterprofile. Für die praktische Anwendung einer Serviceprofilinstanz sind insbesondere die Unterprofile *Fachdienst*, *Transportinfrastruktur* und *Kryptografie* maßgeblich. Sobald die grundsätzliche Anwendbarkeit sichergestellt ist, kann zusätzlich das Unterprofil *Automatisierung* erstellt werden, mit dem vollautomatisierte Systeme mit neuen oder geänderten Prozessen versorgt werden können („Automaten für Nachrichtentransporte“).

Abbildung 1.3. Prozessbeteiligte bei Erstellung einer Serviceprofilinstanz

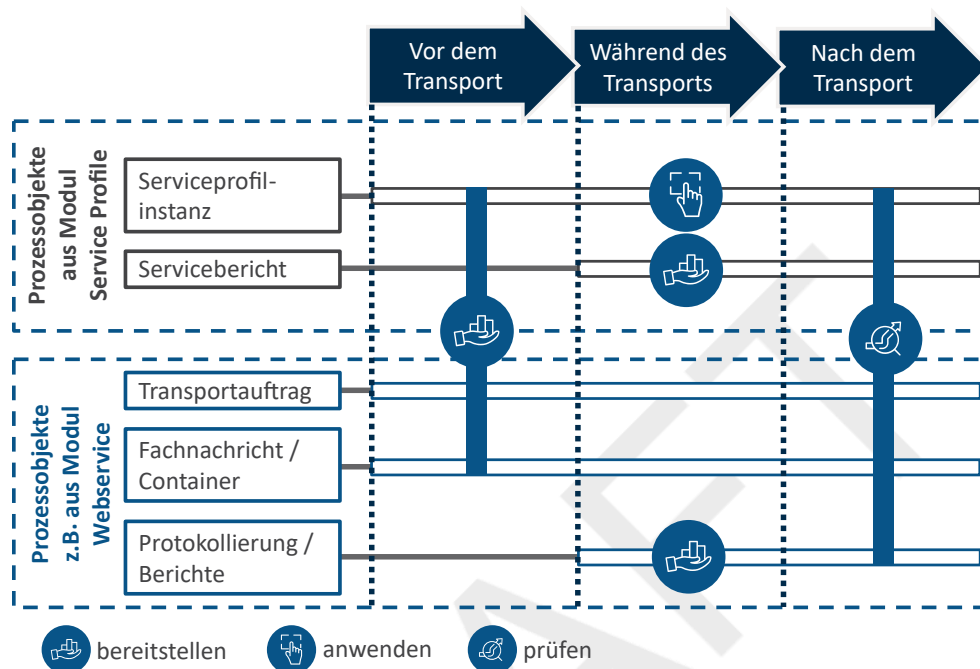


Die Fachverantwortlichen initiieren und steuern die Erstellung der Serviceprofilinstanzen (SP-Instanz) für ihren jeweiligen Fachbereich. Hierbei werden mindestens das UP *Gewährleistungsziele* und das UP *Fachdienst* sowie bei Bedarf weitere Unterprofile befüllt. Fachliche und technische Expertise können u. a. durch Datenschutzbeauftragte, das Expertengremium bzw. den Steuerungskreis *Sicherer Transport*, die KoSIT, Transporteure sowie weitere Fachvertreter eingebracht werden. Transporteure und Interessensvertreter der Fachbereiche können zudem beauftragt werden, das UP *Transportinfrastruktur* bzw. UP *Fachdienst* eigenständig auszugestalten. Soweit erforderlich, können mehrere Unterprofile parallel definiert werden. Unterprofile und gesamte Serviceprofilinstanzen können in einem sicheren Serviceprofil-Repository abgelegt und von dort per Referenz (Ref.) bezogen werden.

Aufgrund häufig übereinstimmender Anforderungen können Unterprofile oder ganze Serviceprofilinstanzen auf einer Governance-Ebene zur verpflichtenden Nutzung veröffentlicht werden. Hierzu initiiert ein Akteur (z. B. ein Bundesland) den entsprechenden Vorgang beim IT-Planungsrat als dem zentralen politischen Steuerungsgremium für die Digitalisierung der öffentlichen Verwaltung in Deutschland. Vertrauenswürdige Organisationen mit besonderer Fachkompetenz können ausgewählte Unterprofile zur Nachnutzung bereitstellen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cybersicherheitsbehörde des Bundes und zentraler Akteur für eine sichere Digitalisierung in Deutschland. Die

Bereitstellung mehrerer geeigneter Kryptografie-Unterprofilinstanzen könnte daher durch das BSI erfolgen.

Abbildung 1.4. Verwendung von XTA Service Profile im Gesamtprozess



Das Modul *XTA Service Profile* unterstützt mit seinen Prozessobjekten eine normative, regelbasierte Steuerung sowie die revisionssichere Nachweisbarkeit und Überprüfung der festgelegten Vorgaben. Damit wird die Operationalisierung rechtlicher, organisatorischer und technischer Anforderungen im Nachrichtentransport ermöglicht. Im Fokus stehen drei Prozessphasen, die in jedem Nachrichtentransport-Szenario durchlaufen und durch das Modul gestärkt werden:

- **Vor dem Transport** legt der Fachverantwortliche die geforderten Gewährleistungsziele und weiteren Vorgaben mittels einer Serviceprofilinstanz fest. Diese wird zusammen mit Transportauftrag und Fachnachricht vom Fachverfahren an das Transportverfahren übergeben. Beispielsweise mit dem Modul *XTA Webservice* gestaltet sich dieser Übergang zur nächsten Phase mit dem Aufruf der Methode `sendMessage` oder `sendMessageSync`. Mit der Übergabe des Transportauftrags `MessageMetadata` (MMD) und der Fachnachricht im `ContentContainer` (CoCo) beginnt der Transport.
- **Während des Transports** sind die in der Serviceprofilinstanz spezifizierten Servicequalitäten bei der Ausführung des Nachrichtentransports einzuhalten. Parallel werden ein Servicebericht sowie ergänzende Protokolle und weitere standardisierte Berichte erzeugt, in denen alle relevanten Ereignisse zur Nachweisführung erfasst werden. Beispielsweise mit dem Modul *XTA Webservice* wird ein Transportbericht `TransportReport` bis zur Vollendung des Transports fortgeschrieben und gesiegelt.
- **Nach dem Transport** werden sämtliche Prozessobjekte gebündelt und im Rahmen von Stichprobenprüfungen oder Audits ausgewertet. Zentral ist der Abgleich zwischen den festgelegten Servicequalitäten und den im Servicebericht dokumentierten Werten. Transportauftrag und Fachnachricht fließen in diese Gesamtprüfung ein. Für detaillierte Analysen zu spezifischen Fragestellungen können weitere Protokollierungsdaten und Berichte aus dem konkreten Nachrichtentransport herangezogen werden. Bei Nichteinhaltung von Vorgaben oder geforderten Servicequalitäten sind Eskalationsmechanismen zu nutzen und angemessene Maßnahmen einzuleiten. Beispielsweise mit dem Modul *XTA Webservice*.

vice wird der Transportbericht `TransportReport` mit weiteren Protokollen / Berichten mittels der Methode `getTransportReport` für die Prüfungen bereitgestellt.

Im Nachrichtentransport können standardisierte, teilstandardisierte und proprietäre Lösungen auf unterschiedlichen Infrastrukturebenen eingesetzt werden. Im jeweils konkreten Fall muss evaluiert werden, wie umfänglich und für welche Teilstrecke eine Prüfung erfolgen soll. Beispielsweise beim Einsatz des Moduls *XTA Webservice* erstellen Sender und Empfänger zum selben Transportauftrag jeweils einen eigenen Transportbericht `TransportReport` mit Einträgen und Ereignissen im jeweiligen Verantwortungsbereich. Für eine vollständige Prüfung des Transports von Autor bis Leser innerhalb eines Audits sind beide Transportberichte zusammen zu führen.

1.2 Offene Punkte

Einige Punkte, Ideen und Diskussionsansätze sind noch offen. Um die Transparenz zu erhöhen und die Interessengemeinschaft zu vergrößern, werden nachfolgend einige dieser offenen Arbeitspunkte aufgeführt. Zusätzlich sind diese im Abschnitt zum Datenmodell mit einem Pylonen-Symbol  markiert.

-  Übergreifende Themen
 - Bessere Differenzierung zwischen Löschfrist und Aufbewahrungsfrist (Durchwirkung der Gewährleistungsziele auf die technische Ebene) sowie detailliertere Ausgestaltung der Löschfrist je nach Kontext (Versand, Empfang, Verarbeitung).
 - Konkretisierung von Datentypen, besonders bei Platzhalter `ToBeSpecifiedType`.
 - Abstimmung mit Expertinnen und Experten zur offenen Diskussionspunkten unter " TODO" in Abschnitt zum Datenmodell.
 - Schematron-Regeln einführen z.B. mindestens `protectionGoal` oder `Reference`
-  Profilkopf
 - Wird hier noch ein Prüfintervall benötigt (z.B. Datentyp `xs:gMonth`)?
-  Unterprofil Fachdienst
 - Werden zusätzliche oder alternative Parameter/Angaben zu der Dienstbezeichnung `serviceUri` benötigt?
 - Vorgaben bei Zustellversuchen: Machen wir Vorgaben zur Anzahl der Zustellversuche? Versuchsintervall? Geltungsbereich?
-  Unterprofil Transportinfrastruktur
 - Werden spezielle Anforderungen je `ContentContainer` / `Container` / `Message` / ... benötigt?
-  Unterprofil Automatisierung
 - Frage, wann welcher „Prozess“ von wem aufgerufen wird, muss noch aufgenommen werden, ggf. muss diese Information nicht Teil der Automatisierung sein.
 - In welchem Detailgrad müssen „Prozesse“ in der Automatisierung?
 - Gestaltung der `SequenzOfCommands` innerhalb der Aktivität weiter ausarbeiten.
 - Passen die vorgesehen Datentypen der Elemente unter Automatisierung?
 - Simple Beispielinstanzen zur Veranschaulichung erstellen.
-  Unterprofil Kryptografie
 - Schutzniveau formulieren
-  Nachweisbarkeit der Servicequalitäten
 - Übernahme von `ServiceReport` aus der Spezifikation der Erweiterung `Service Reporting` mit geeigneten Anpassungen.
 - Übernahme von `EreignisType` aus der Spezifikation XTA 2 mit geeigneten Anpassungen.

2 Voraussetzungen



Die Fachverfahren beauftragen die Transportverfahren mit der Abwicklung eines Nachrichtentransports. Mit dem Modul *XTA Service Profile* können die Fachverfahren die erwarteten Servicequalitäten für den Betrieb bestimmen. Die Transportverfahren sind damit verpflichtet, den Betrieb stets ordnungsgemäß durchzuführen. Um die Überprüfbarkeit der gesamten Transportstrecke (vom Autor bis zum Leser) gewährleisten zu können, muss die Serviceprofilierung und die Berichterstattung von allen Rollen bzw. beteiligten Software-Produkten implementiert werden.

Für die einwandfreie Prüfung des Nachrichtentransports müssen alle Zeitstempel in einem UTC Format inkl. Zeitzone gesetzt werden. Ein Beispiel des [W3-Konsortiums](#) für eine in UTC definierte Zeitangabe ist: 1994-11-05T13:15:30Z

2.1 Konformität

Gegenstand der Konformitätsbewertung ist ein Software-Produkt, welches das Modul Service Profile für die Anwendungsebene oder für die Transportebene implementiert. Eine Implementierung für die Anwendungs-/Transportebene ist genau dann „konform zur Spezifikation *XTA Modul Service Profile*“, wenn alle Vorgaben aus der Spezifikation an die umgesetzte Rolle erfüllt wurden. Die Konformitätserklärung der Produktherstellerin erfolgt freiwillig und muss mindestens über die folgenden Informationen verfügen:

- Eindeutige Kennzeichnung als Selbsterklärung zur XTA-Konformität
- Eindeutiger Verweis auf die XTA-Spezifikation mit Angabe von Version und Datum, die umgesetzt wurde
 - Verweis auf die Quelle der Spezifikation (Link zur offiziellen Seite)
 - Es kann stets nur auf die XTA-Spezifikation verwiesen werden, nicht auf die Hilfsmittel, die zusammen mit der XTA-Spezifikation veröffentlicht werden (z.B. einzelne Schema- oder WSDL-Dateien)
- Eindeutige Identifikation des Produktes, insbesondere die Produktbezeichnung einschließlich Versionsangabe
 - Angabe, welche Rollen umgesetzt worden sind
- Eindeutige Angabe der Herstellerin einschließlich gültiger Kontaktinformationen
- Datum, Ort und Unterschrift einer vertretenden Person des Herstellers bzw. der Herstellerin

3 Datenmodell

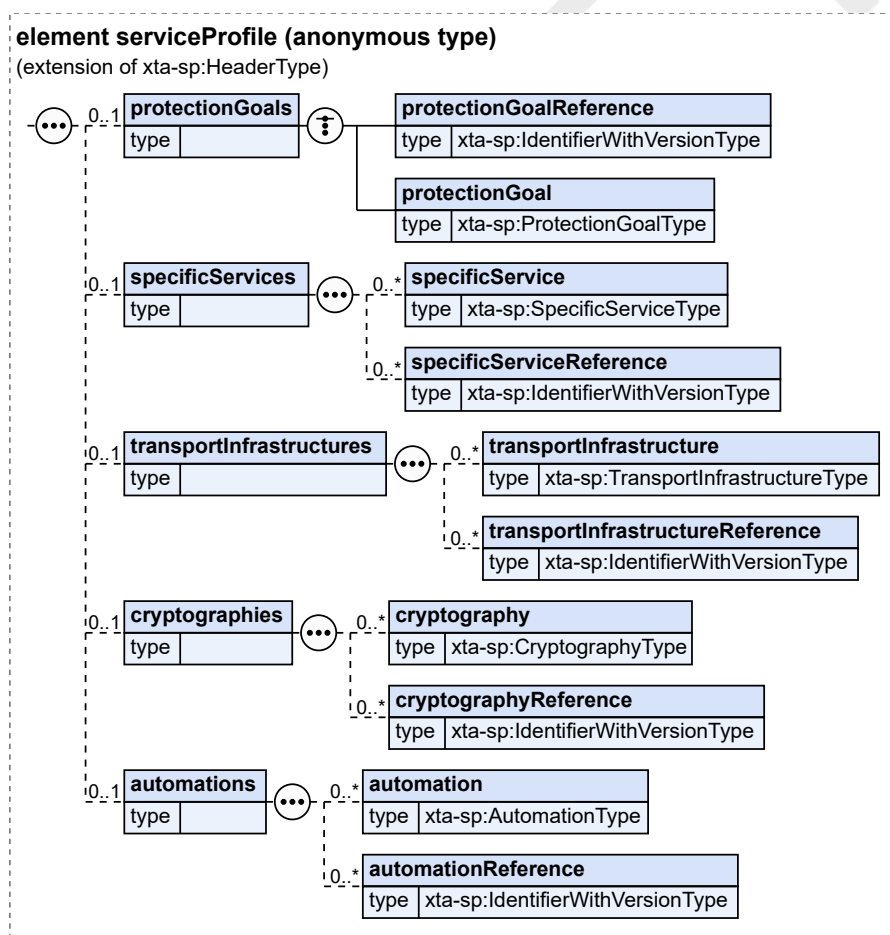


3.1 Hauptprofil und Basisdatentypen

3.1.1 serviceProfile

Nachricht: **serviceProfile**

Abbildung 3.1. serviceProfile



Diese Nachricht ist eine Erweiterung des Basistyps **HeaderType** (siehe [Abschnitt 3.1.2 auf Seite 10](#)).

Tabelle 3.1. Struktur von serviceProfile

serviceProfile ^{ooo} 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
protectionGoals ^{ooo} 1		0..1			
Im Unterprofilbereich Gewährleistungsziele sind alle Gewährleistungsziele des Datenschutzes oder eine Referenzen auf alle Gewährleistungsziele des Datenschutzes erfasst.					
protectionGoalReference	IdentifierWithVersionType 	1	3.1.3	11	
Eindeutiger Identifikator der referenzierten Profilinstanz.					
protectionGoal	ProtectionGoalType 	1	3.2.2	12	
Direkte Einbindung einer Unterprofilinstanz.					
specificServices ^{ooo} 1		0..1			
Im Unterprofilbereich Fachdienste sind einzelne Fachdienste, Referenzen auf Fachdienste oder eine Mischung aus beidem erfasst.					
specificService	SpecificServiceType 	0..n	3.3.2	20	
Direkte Einbindung einer Unterprofilinstanz.					
specificServiceReference	IdentifierWithVersionType 	0..n	3.1.3	11	
Eindeutiger Identifikator der referenzierten Profilinstanz.					
transportInfrastructures ^{ooo} 1		0..1			
Im Unterprofilbereich Transportinfrastruktur sind einzelne Transportinfrastrukturen, Referenzen auf Transportinfrastrukturen oder eine Mischung aus beidem erfasst. Jede einzelne Transportinfrastruktur soll gesiegelt / signiert werden sowie extern referenzierbar sein.					
transportInfrastructure	TransportInfrastructureType 	0..n	3.4.2	23	
Direkte Einbindung einer Unterprofilinstanz.					
transportInfrastructureReference	IdentifierWithVersionType 	0..n	3.1.3	11	
Eindeutiger Identifikator der referenzierten Profilinstanz.					
cryptographies ^{ooo} 1		0..1			
Im Unterprofilbereich Kryptografie sind einzelne Unterprofile Kryptografie, Referenzen auf Unterprofile Kryptografie oder eine Mischung aus beidem erfasst. Jedes einzelne Unterprofil Kryptografie soll gesiegelt / signiert und kann extern referenziert werden.					
cryptography	CryptographyType 	0..n	3.5.2	32	
Direkte Einbindung einer Unterprofilinstanz.					
cryptographyReference	IdentifierWithVersionType 	0..n	3.1.3	11	
Eindeutiger Identifikator der referenzierten Profilinstanz.					
automations ^{ooo} 1		0..1			
Im Unterprofilbereich Automatisierung sind einzelne Automatisierungen, Referenzen auf Automatisierungen oder eine Mischung aus beidem erfasst.					
automation	AutomationType 	0..n	3.6.2	33	
Direkte Einbindung einer Unterprofilinstanz.					
automationReference	IdentifierWithVersionType 	0..n	3.1.3	11	
Eindeutiger Identifikator der referenzierten Profilinstanz.					

3.1.2 HeaderType

Typ: **HeaderType**

Der Profilkopf ist ein eigener Datentyp für die Profile mit eindeutiger Kennung (mit Version), Ausstellungsdatum, Gültigkeit, Herausgeber und Verwendungskontext.

Abbildung 3.2. HeaderType

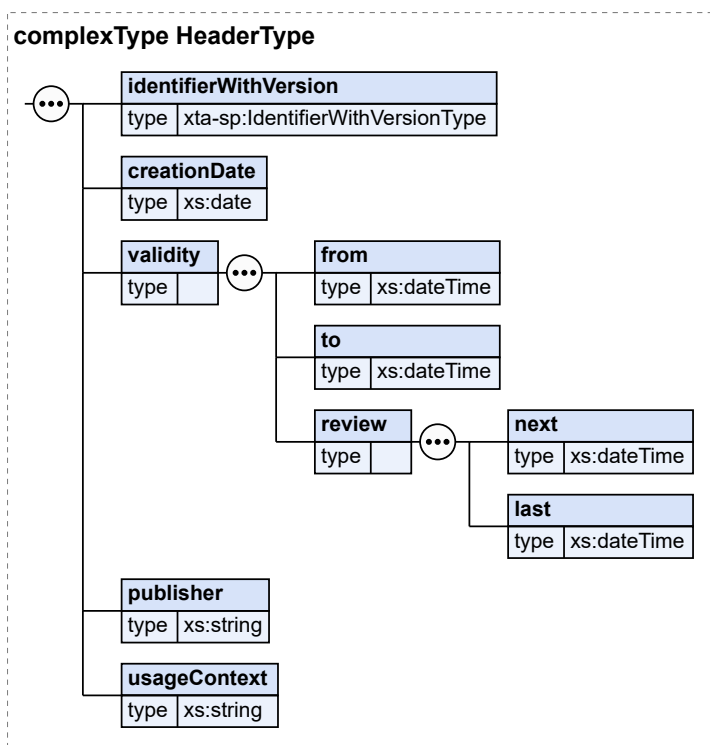


Tabelle 3.2. Struktur von HeaderType

HeaderType ^{...} 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
identifierWithVersion	IdentifizierWithVersionType	1	3.1.3	11	
Eindeutiger Identifikator der Serviceprofilinstanz mit Kennung und Version.					
creationDate	xs:date	1			
Tagesdatum zu dem diesen Version des Profils (bzw. Unterprofils) erstellt wurde.					
validity ^{...} 1		1			
Gültigkeit des Profils (von / bis) mit Angabe der nächste bzw. letzten Prüfung der Aktualität.					
from	xs:dateTime	1			
Beginn der Gültigkeit des Profils als Tagesdatum.					
to	xs:dateTime	1			
Ende der Gültigkeit des Profils als Tagesdatum.					
review ^{...} 1		1			
Angabe der nächste bzw. letzten Prüfung der Aktualität.					

HeaderType ^{...} 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
next	xs:dateTime	□	1		
Tagesdatum der nächsten Prüfung der Aktualität.					
last	xs:dateTime	□	1		
Tagesdatum der letzten Prüfung der Aktualität.					
publisher	xs:string	□	1		
Herausgebende Organisation des Profils.					
usageContext	xs:string	□	1		
Beschreibung des Kontexts der Verwendung. Hier können auch Versionsänderungen deutlich gemacht werden. Der Zweck und die Grundlagen der Verarbeitung müssen angegeben werden. Im Falle der Verwendung des Profilskopfs für Kryptografie kann hier auf Vorgaben des BSI verwiesen werden.					

3.1.2.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [cryptography](#), [protectionGoal](#), [serviceProfile](#), [specificService](#), [transportInfrastructure](#)

Von diesem Typ leiten ab: [serviceProfile](#)

3.1.3 IdentifierWithVersionType

Typ: **IdentifierWithVersionType**

Eindeutiger Identifikator der Serviceprofilinstanz mit Kennung und Version getrennt durch einen Unterstrich (z.B. urn:xoev-de:kosit:standard:xinneres.xta.serviceprofile.gewaehrleistungsziele_0.1.0).

Abbildung 3.3. IdentifierWithVersionType

complexType IdentifierWithVersionType
(restriction of xs:anyURI)

Dieser Datentyp ist eine Erweiterung des Basistyps xs:anyURI.

Tabelle 3.3. Struktur von IdentifierWithVersionType

IdentifierWithVersionType ^{...} 1				
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
@ identifier	xs:anyURI	□	1	
Kennung (z.B.urn:xoev-de:kosit:standard:xinneres.xta.serviceprofile.gewaehrleistungsziele).				
@ version	xs:normalizedString	□	1	
Version (z.B. 0.1.0).				

3.1.3.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [cryptography](#), [protectionGoal](#), [serviceProfile](#), [specificService](#), [transportInfrastructure](#)

3.1.4 Weekdays

Typ: **Weekdays**

Dieser Datentyp ist eine Einschränkung des Basistyps **xs:string**.

Die Werte müssen dem Muster 'mondays|tuesdays|wednesdays|thursdays|fridays|saturdays|sundays' entsprechen.

3.1.4.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [serviceProfile](#), [transportInfrastructure](#)

3.1.5 ToBeSpecifiedType

Typ: **ToBeSpecifiedType**

 **ToDo:** Dieser Datentyp dient als Platzhalter für weitere Ausarbeitung der Spezifikation. Es leitet vom Datentyp **xs:string** und ermöglicht somit eine freie Befüllung einer Serviceprofilinstanz in der Erpo-bungs-/Konzeptionsphase.

Dieser Datentyp ist eine Einschränkung des Basistyps **xs:string**.

3.1.5.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#), [specificService](#), [transportInfrastructure](#)

3.1.6 EmptyType

Typ: **EmptyType**

Keine gesonderte Befüllung erforderlich.

Dieser Datentyp ist eine Einschränkung des Basistyps **xs:string**.

Beschränkungen (XML-Schema-Facetten): length:0

3.1.6.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

3.2 Unterprofil Gewährleistungsziele

3.2.1 protectionGoal

Nachricht: **protectionGoal**

Globale Elementdefinition zur Nachnutzung und externen Ablagemöglichkeit.

Diese Nachricht ist eine Erweiterung des Basistyps **ProtectionGoalType** (siehe [Abschnitt 3.2.2 auf Seite 12](#)).

3.2.2 ProtectionGoalType

Typ: **ProtectionGoalType**

Dieser Unterprofilbereich benennt die Gewährleistungsziele des Datenschutzes in der Detaillierung, wie sie für den sicheren Transport von Fachnachrichten und ihren Anhängen von Relevanz ist.

Das Unterprofil "Gewährleistungsziele" ist bewusst abstrakt gehalten, um es in verschiedenen Fachkon-texten innerhalb einer gesamten Fachdomäne verwenden zu können. Es kann direkt aus einem Ser-viceprofil referenziert werden.

Die Qualitäten der Kategorien des Unterprofils Gewährleistungsziele stehen in direktem Zusammenhang mit Kategorien in anderen Unterprofilen:

- Die Vertraulichkeit im Unterprofil "Gewährleistungsziele" beeinflusst beispielsweise die Vorgaben zur Datenhaltung im Unterprofil "Transportinfrastruktur", die wiederum auf Unterprofil "Kryptografie" verweisen.
- Die protokollbasierte Nachvollziehbarkeit im Gewährleistungsziel "Transparenz" führt zu spezifischen Anforderungen an die Protokollierung im Unterprofil "Transportinfrastruktur".

Die konkrete Umsetzung der Gewährleistungsziele in den anderen Unterprofilen hängt vom jeweiligen Fachkontext ab. Beispielsweise können die Aufbewahrungs- und Löschrufen für Fachdaten im Personenstandswesen von denen im Meldewesen abweichen, obwohl beide zur Fachdomäne "Wesen des Inneren" gehören. Daher ist eine fachkontextspezifische Interpretation der Qualitätsanforderungen aus dem Unterprofil "Gewährleistungsziele" erforderlich. Diese Zuordnung zu konkreten Werten kann in Form einer Tabelle in der Spezifikation des jeweiligen Serviceprofils oder als Codeliste bereitgestellt werden.

Konkrete Angaben zu "Löschrufen" finden sich sowohl im Unterprofil Fachdienste als auch im Unterprofil Transportinfrastruktur. Die Anforderung zum Löschen von Daten leitet sich direkt aus dem Gewährleistungsziel der Vertraulichkeit ab.

Ein Unterprofil "Gewährleistungsziele" kann gesiegelt / signiert und referenziert werden.

Abbildung 3.4. ProtectionGoalType

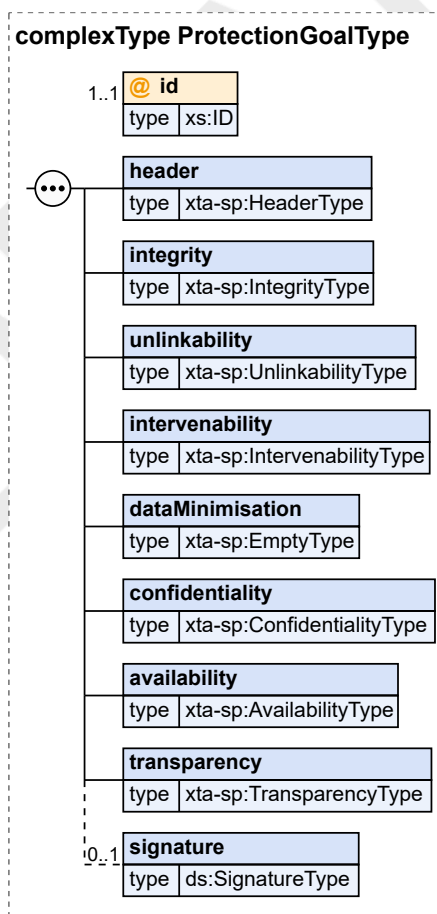


Tabelle 3.4. Struktur von ProtectionGoalType

ProtectionGoalType 1					
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
@ id	xs:ID	1			
XML-ID zur eindeutigen Adressierung der Datenstruktur, primär für die Erstellung von XML Signaturen.					
header	HeaderType	1	3.1.2	10	
integrity	IntegrityType	1	3.2.5	16	
"Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben." [SDM, 2025] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf					
unlinkability	UnlinkabilityType	1	3.2.8	19	
"Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden dürfen. Eine Zusammenführung darf nur dann erfolgen, wenn die in Art. 5 Abs. 1 lit. b DS-GVO normierte Anforderung beachtet wird, dass Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden." [SDM, 2025] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf					
intervenability	IntervenabilityType	1	3.2.6	17	
"Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Dazu müssen die für die Verarbeitungsprozesse verantwortlichen Stellen jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen." [SDM, 2025] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf					
dataMinimisation	EmptyType	1	3.1.6	12	
Das Gewährleistungsziel Datenminimierung zielt im Kontext des Datenaustauschs der Verwaltung auf den Umfang der Fachdaten ab. Ein Service Profil beschreibt den sicheren Transport dieser Fachdaten. Die dabei entstehenden transportbezogenen Protokollierungen sind bereits auf ein Minimum reduziert. [SDM, 2025] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf					
confidentiality	ConfidentialityType	1	3.2.4	15	
"Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen kann." [SDM, 2025] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf					
availability	AvailabilityType	1	3.2.3	15	
Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass eine Nachrichtenübermittlung verfügbar ist. [SDM, 2025] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf					
transparency	TransparencyType	1	3.2.7	18	
Das Gewährleistungsziel Transparenz ist für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung bis zu ihrer Löschung erforderlich und eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in diese, soweit erforderlich, von Betroffenen informiert eingewilligt werden kann. [SDM, 2025] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V31a.pdf					
signature	ds:SignatureType	0..1	A.1.4	47	

ProtectionGoalType ^{...} 1				
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
Signatur des Unterprofils zur Prüfung der Authentizität/Integrität.				

3.2.2.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

Von diesem Typ leiten ab: [protectionGoal](#)

3.2.3 AvailabilityType

Typ: **AvailabilityType**

Abbildung 3.5. AvailabilityType

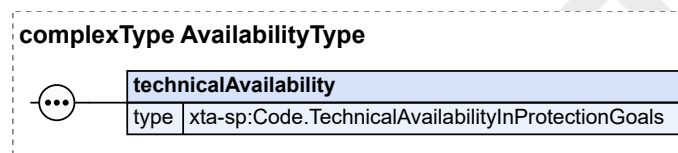


Tabelle 3.5. Struktur von AvailabilityType

AvailabilityType 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
technicalAvailability	Code.TechnicalAvailability-InProtectionGoals	1	A.3.21	54	
Technische Verfügbarkeit der Systeme. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen.					
Beispiele zur groben Orientierung:					
niedrig: unklare Antwortzeit / Zeit bis Transport abgeschlossen					
mittel: mittlere Antwortzeit / mittlere Zeit bis Transport abgeschlossen					
hoch: kurze Antwortzeit / Zeit bis Transport abgeschlossen					

3.2.3.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

3.2.4 ConfidentialityType

Typ: **ConfidentialityType**

Abbildung 3.6. ConfidentialityType

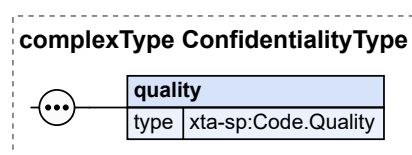


Tabelle 3.6. Struktur von ConfidentialityType

ConfidentialityType ^{...} 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
quality	Code.Quality 	1	A.3.18	53
Qualität der Vertraulichkeit. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: öffentlich: keine Vertraulichkeit normal: normale Vertraulichkeit hoch: hohe Vertraulichkeit				

3.2.4.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

3.2.5 IntegrityType

Typ: **IntegrityType**

Abbildung 3.7. IntegrityType

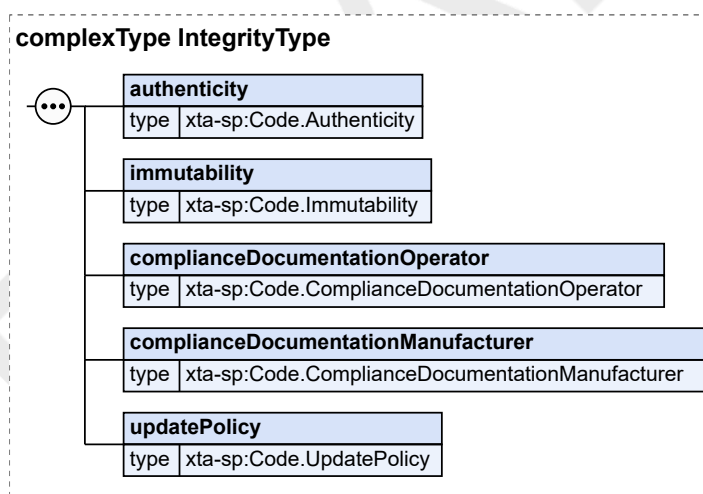


Tabelle 3.7. Struktur von IntegrityType

IntegrityType ^{...} 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
authenticity	Code.Authenticity 	1	A.3.2	49
Authentizität. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: niedrig: öffentliche, unverbindliche Informationen				

IntegrityType *** 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
normal: nur Gruppenauthentizität hoch: Systeme sind eindeutig (1:1) identifiziert				
immutability	Code.Immutability 	1	A.3.11	51
Unveränderbarkeit. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: niedrig: optional (z.B. ohne Signaturen oder einfacher Hashwert) normal: Systeminterne Mittel (z.B. Signaturen) hoch: zusätzliche Schutzmaßnahmen (z.B. qualifizierte Signaturen)				
complianceDocumentationOperator	Code.ComplianceDocumentationOperator 	1	A.3.5	50
Konformitätsdokumentation der Betreiber. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: normal: durch Eigenerklärung/Dokumentation - als Nachweis zählt eine Betreiber- oder Herstellererklärung mit einem entsprechenden Vertrag. Die Erklärung ist an einem definierten Ort hinterlegt. hoch: durch anerkannte Fremdzertifizierung - als Nachweis wird eine Zertifizierung gefordert. Der Betreiber oder Hersteller durchläuft erfolgreich einen Zertifizierungsprozess und hinterlegt den Zertifizierungsnachweis an einem definierten Ort.				
complianceDocumentationManufacturer	Code.ComplianceDocumentationManufacturer 	1	A.3.4	49
Konformitätsdokumentation der Hersteller. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: normal: durch Eigenerklärung/Dokumentation - als Nachweis zählt eine Betreiber- oder Herstellererklärung mit einem entsprechenden Vertrag. Die Erklärung ist an einem definierten Ort hinterlegt hoch: durch anerkannte Fremdzertifizierung - als Nachweis wird eine Zertifizierung gefordert. Der Betreiber oder Hersteller durchläuft erfolgreich einen Zertifizierungsprozess und hinterlegt den Zertifizierungsnachweis an einem definierten Ort.				
updatePolicy	Code.UpdatePolicy 	1	A.3.23	55
Update-Regelung. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: niedrig: optional (z.B. ohne Signaturen oder einfacher Hashwert) normal: Änderung bei Update auf nächste Version sind vereinbart hoch: keine Änderung ohne CR				

3.2.5.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

3.2.6 IntervenabilityType

Typ: **IntervenabilityType**

Abbildung 3.8. IntervenabilityType

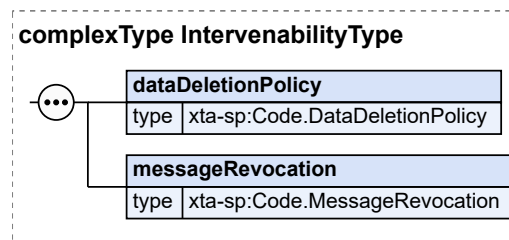


Tabelle 3.8. Struktur von IntervenabilityType

IntervenabilityType ∞ 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
dataDeletionPolicy	Code.DataDeletionPolicy 	1	A.3.8	50	
Löschkonzept. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: normal: einfaches Löschen hoch: sicheres Löschen					
messageRevocation	Code.MessageRevocation 	1	A.3.16	53	
Rückruf von Fehlnachrichten. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: normal: Bestätigung von Fehlnachrichten hoch: definierter Prozess, Transparenz des Status					

3.2.6.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

3.2.7 TransparencyType

Typ: **TransparencyType**

Abbildung 3.9. TransparencyType

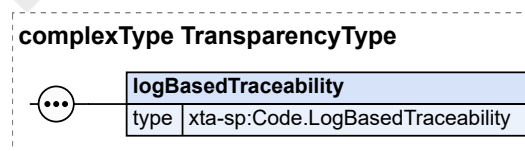


Tabelle 3.9. Struktur von TransparencyType

TransparencyType ... 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
logBasedTraceability	Code.LogBasedTraceability 	1	A.3.14	52	

TransparencyType *** 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
Protokollbasierte Nachvollziehbarkeit. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: Die Protokollbasierte Nachvollziehbarkeit hat die Funktion sicherzustellen, dass die Vorgaben der anderen Gewährleistungsziele, u.a. der Nichtverketzung, eingehalten wurden. mittel: zu Nutzen bei Daten mit geringerem Protokollierungsbedarf hoch: zu Nutzen bei Daten zu einzelnen Personen (u.a. medizinische Daten) sehr hoch: zu Nutzen für geheime Daten, z.B. für Infrastruktur die für den Schutz der BR Deutschland ist				

3.2.7.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

3.2.8 UnlinkabilityType

Typ: **UnlinkabilityType**

Abbildung 3.10. UnlinkabilityType

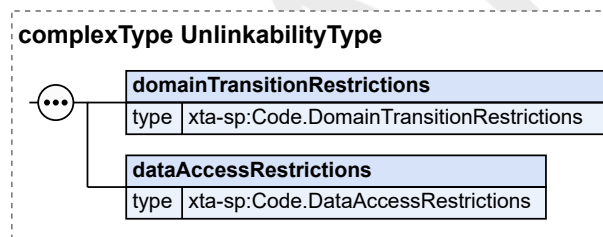


Tabelle 3.10. Struktur von UnlinkabilityType

UnlinkabilityType 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
domainTransitionRestrictions	Code.DomainTransitionRestrictions	1	A.3.10	51	
Beschränkung für Domänenübertritte. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen. Beispiele zur groben Orientierung: normal: Abrufe finden ohne Beschränkungen innerhalb der gesetzlich definierten Domäne statt mittel: nicht erlaubte Domänenübertritte erzeugen eine WARNUNG hoch: nicht erlaubte Domänenübertritte sind möglich, erzeugen aber einen ALARM sehr hoch: nicht erlaubte Domänenübertritte KÖNNEN NICHT passieren					
dataAccessRestrictions	Code.DataAccessRestrictions	1	A.3.7	50	
Beschränkung für (Daten-)Zugriffe. Angabe erfolgt mittels einer Codeliste mit dokumentierten Niveaus/Qualitätsanforderungen.					

UnlinkabilityType *** 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
⚠️ TODO: Beispiele definieren Definition des Schutzes erfolgt im eigenen Rollen- & Berechtigungskonzept. Darüber wird z.B. festgelegt wer lesen/schreiben/löschen DARF und/oder MUSS. Es werden Daten auf der Fach- und Transportebene wie z.B. Reportdaten, technische Protokollierung, standardisierte Transportberichte adressiert.				

3.2.8.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [protectionGoal](#), [serviceProfile](#)

3.3 Unterprofil Fachdienst

3.3.1 specificService

Nachricht: **specificService**

Globale Elementdefinition zur Nachnutzung und externen Ablagemöglichkeit.

Diese Nachricht ist eine Erweiterung des Basistyps **SpecificServiceType** (siehe [Abschnitt 3.3.2 auf Seite 20](#)).

3.3.2 SpecificServiceType

Typ: **SpecificServiceType**

Im Unterprofil Fachdienste sind einzelne Fachdienste, Referenzen auf Fachdienste oder eine Mischung aus beidem erfasst. Jeder einzelne Fachdienst soll gesiegelt / signiert und kann extern referenziert werden.

Abbildung 3.11. SpecificServiceType

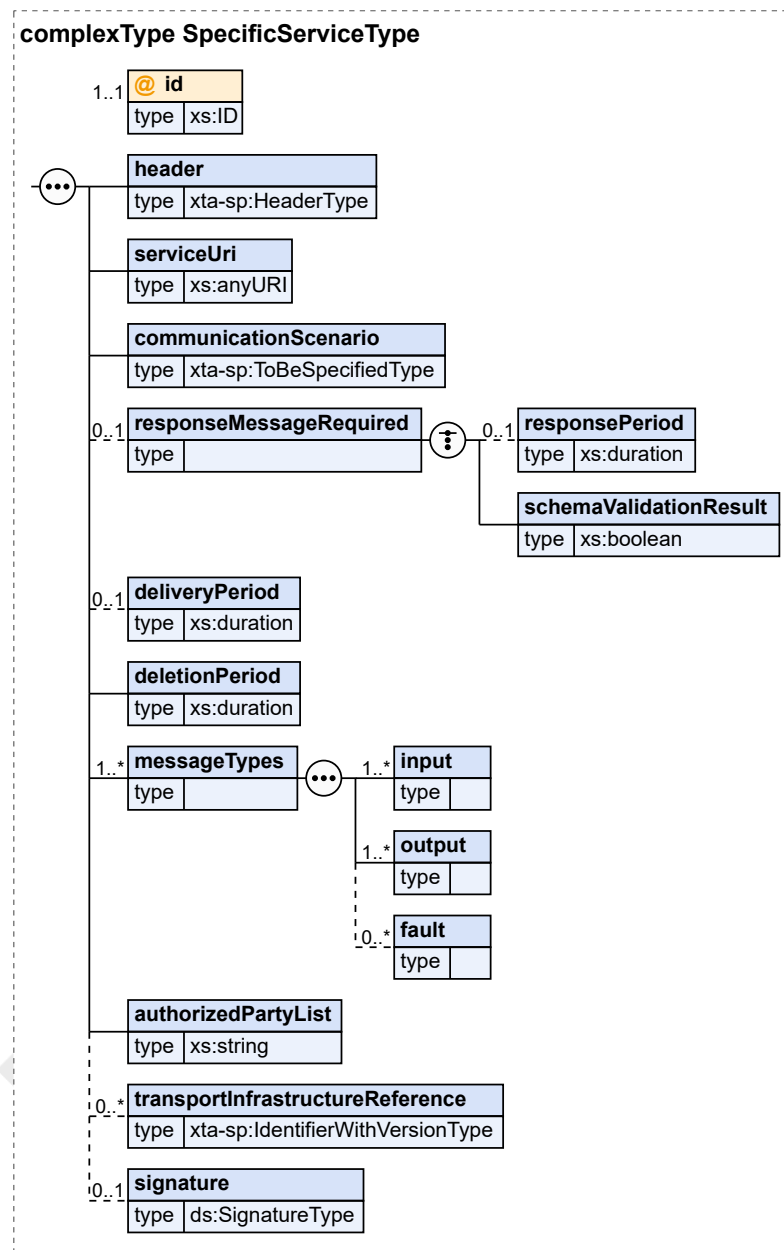


Tabelle 3.11. Struktur von SpecificServiceType

SpecificServiceType ^{***} 1					
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
@ id	xs:ID ☐	1			
XML-ID zur eindeutigen Adressierung der Datenstruktur, primär für die Erstellung von XML Signaturen.					
header	HeaderType ☐	1	3.1.2		10
serviceUri	xs:anyURI ☐	1			

SpecificServiceType 1					
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
Die Dienstbezeichnung ist eine eindeutige Ressourcenkennung (URI nach RFC 3986) des Dienstes, der durch den Transportauftrag in Anspruch genommen werden soll. Für Fachstandards mit DVDV-Bezug entspricht diese Dienstbezeichnung der Dienstbezeichnung im DVDV.					
communicationScenario	ToBeSpecifiedType	1	3.1.5	12	
Kommunikationsszenario auf Anwendungsebene (Autor - Leser) - synchron oder asynchron.					
TODO: Werteliste enum mit 2 Einträgen					
responseMessageRequired 1		0..1			
Erforderlichkeit der fachlichen Beantwortung einer Nachrichtenübermittlung. Falls sie erforderlich ist, muss eine Frist angegeben werden in derer die Beantwortung erfolgen muss.					
responsePeriod	xs:duration	0..1			
Angabe einer sekundengenauen Zeitspanne für die Beantwortung der fachlichen Angelegenheit gültig ab dem Zeitpunkt des Versands der Nachricht durch die Rolle Autor.					
schemaValidationResult	xs:boolean	1			
Es gibt Sonderfälle bei der synchronen Kommunikation (z.B. Bundesdruckerei, die eine asynchrone Return-ToSender-Nachricht vorsehen, falls Schemakonformität nicht gegeben ist). In diesen Fällen ist die Angabe für ein fachliches Schemaprüfungsergebnis positiv.					
deliveryPeriod	xs:duration	0..1			
Angabe einer sekundengenauen Zeitspanne beginnend ab dem Zeitpunkt der Erteilung des Transportauftrags als Frist für die Zustellung von Fachnachrichten und des Abschlusses der damit über diesen Dienst erteilten Transportaufträge.					
deletionPeriod	xs:duration	1			
Angabe einer Zeitspanne beginnend ab dem Zeitpunkt der Erteilung des Transportauftrags als Frist für die unwiderrufliche Löschung von Fachnachrichten.					
messageTypes 1		1..n			
Eine Aufzählung der fachlichen Nachrichtentypen die diesem Fachdiensten zugeordnet werden. Sie werden je nach fachlichem Geschäftsfall gebündelt.					
input 1	xs:string	1..n			
z.B. anmeldung.datenanforderung.0300					
Der Typ dieses Elements ist eine Erweiterung des Basistyps string.					
@ schema	xs:anyURI	1			
z.B. http://www.osci.de/xmeld2605					
output 1	xs:string	1..n			
z.B. anmeldung.datenbereitstellung.0301					
Der Typ dieses Elements ist eine Erweiterung des Basistyps string.					
@ schema	xs:anyURI	1			
z.B. http://www.osci.de/xmeld2605					
fault 1	xs:string	0..n			
z.B. administration.returntosender.0900					
Der Typ dieses Elements ist eine Erweiterung des Basistyps string.					
@ schema	xs:anyURI	1			
z.B. http://www.osci.de/xmeld2605					

SpecificServiceType *** 1				
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
authorizedPartyList	xs:string ☐	1		
Liste von berechtigten Kommunikationsteilnehmenden, kategorisiert nach Rolle Autor und Rolle Leser. Kommunikationsteilnehmenden (xs: string) können hier mittels ihrer Behördenkategorien identifiziert werden.				
transportInfrastructureReference	IdentifierWithVersionType ☐	0..n	3.1.3	11
Eindeutige Referenz auf Transportinfrastruktur. Sie kann per xs:ID gesetzt sein oder auf eine Webressource verlinken.  TODO: Referenzoptionen zu Ende diskutieren (Webressource?).				
signature	ds:SignatureType ☐	0..1	A.1.4	47
Signatur des Unterprofils zur Prüfung der Authentizität/Integrität.				

3.3.2.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [serviceProfile](#), [specificService](#)

Von diesem Typ leiten ab: [specificService](#)

3.4 Unterprofil Transportinfrastruktur

3.4.1 transportInfrastructure

Nachricht: **transportInfrastructure**

Globale Elementdefinition zur Nachnutzung und externen Ablagemöglichkeit.

Diese Nachricht ist eine Erweiterung des Basistyps **TransportInfrastructureType** (siehe [Abschnitt 3.4.2 auf Seite 23](#)).

3.4.2 TransportInfrastructureType

Typ: **TransportInfrastructureType**

Abbildung 3.12. TransportInfrastructureType

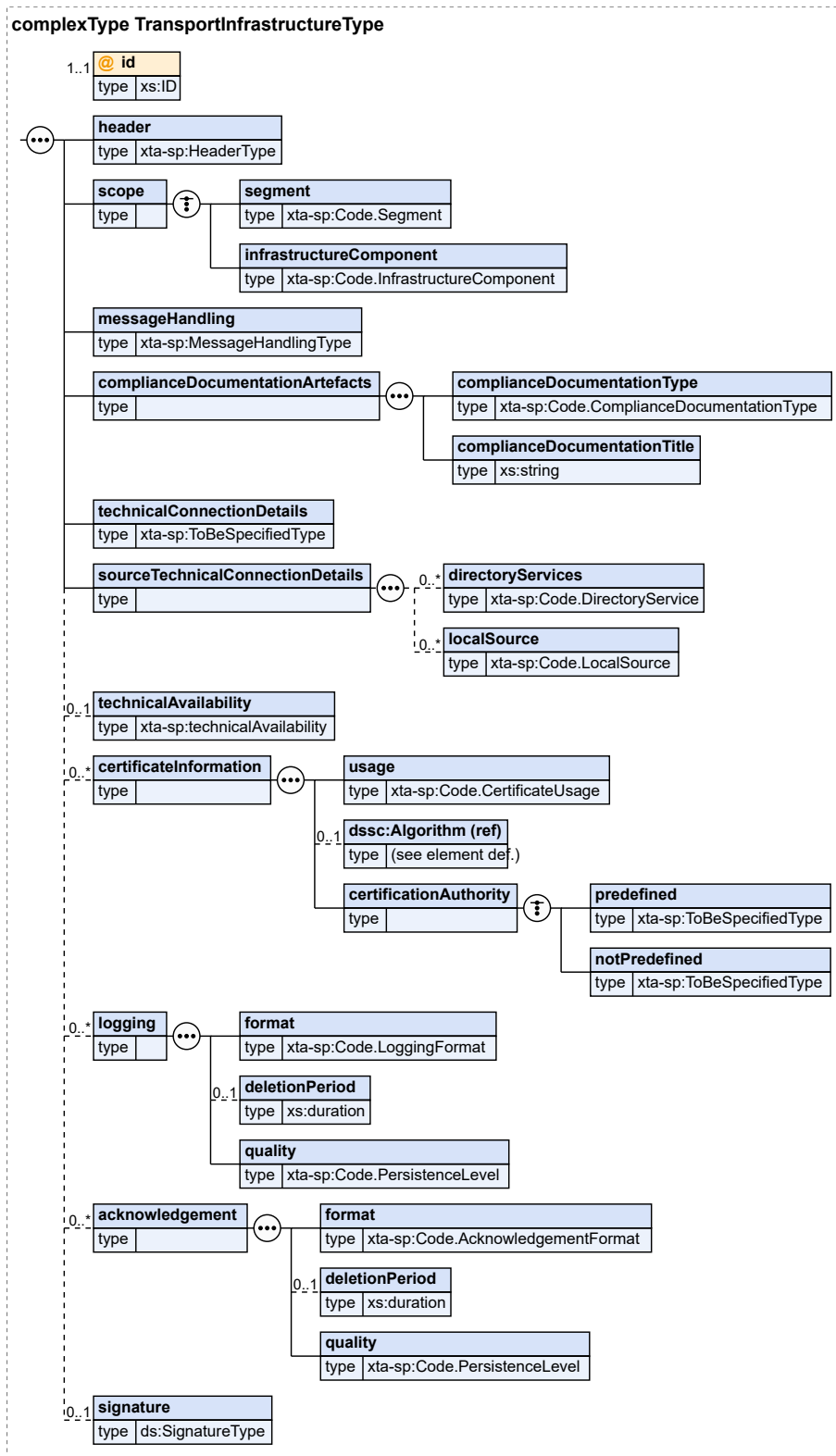


Tabelle 3.12. Struktur von TransportInfrastructureType

TransportInfrastructureType 1					
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
@ id	xs:ID ☐	1			
XML-ID zur eindeutigen Adressierung der Datenstruktur, primär für die Erstellung von XML Signaturen.					
header	HeaderType ☐	1	3.1.2	10	
scope 1		1			
Die Anwendbarkeit des Unterprofils Transportinfrastruktur kann entweder als Strecke (z.B. Sender/Empfänger, Codeliste) oder als Infrastrukturkomponente (z.B: OSCI-Intermediär) angegeben werden.					
segment	Code.Segment ☐	1	A.3.19	54	
Angabe der Kommunikationsstrecken für den Geltungsbereich der Übermittlungsvorgaben erfolgt mittels einer Codeliste. Beispiele zur groben Orientierung: lang: Autor bis Leser links: Autor bis Sender rechts: Empfänger bis Leser mitte: Sender bis Empfänger ...					
infrastructureComponent	Code.InfrastructureComponent ☐	1	A.3.12	52	
Angabe einer Infrastrukturkomponente erfolgt mittels einer Codeliste. Beispiele zur groben Orientierung: Intermediäres System XY Rechenzentrum XY NAT XY ...					
messageHandling	MessageHandlingType ☐	1	3.4.3	28	
complianceDocumentationArtefacts 1		1			
Unter Voraussetzungen sind die technische Bezeichnung aller organisatorischen Nachweise erfasst, die im Rahmen des Nachrichtentransports vorgehalten werden müssen.					
complianceDocumentationType	Code.ComplianceDocumentationType ☐	1	A.3.6	50	
Angabe des Typs erfolgt mittels einer Codeliste. Beispiele zur groben Orientierung: conformity: Konformität certification: Zertifizierung					
complianceDocumentationTitle	xs:string ☐	1			
z.B. XTA-Konformatitätserklärung oder ISO:27001-Zertifizierung.					
technicalConnectionDetails	ToBeSpecifiedType ☐	1	3.1.5	12	
Angaben zur technischen Nachrichtenübermittlung. z.B.: Protokoll ist HTTP, Port ist 30401, Netz ist Internet. Der Port sollte in jedem Fall optional sein oder entfallen.					

TransportInfrastructureType ^{ooo} 1				
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
 TODO Anforderungen sammeln und Struktur spezifizieren.				
sourceTechnicalConnectionDetails ^{ooo} 1		1		
Angabe der Bezugsquelle von Verbindungsinformationen, z.B. ein Verzeichnisdienst (Codeliste) oder eine lokale Bezugsquelle (interne Datenbank; xs:string). Angegeben wird zudem der Kontext, für den die jeweilige Bezugsquelle Daten liefert (Identität, Adressierung, Metadaten).				
directoryServices	Code.DirectoryService 	0..n	A.3.9	51
Bezeichnung des Verzeichnisdienstes, der für jeden Teilnehmer der Nachrichtenübermittlung die Parameter für die technische Adressierung von Teilnehmern bereitstellt. Angabe des Typs erfolgt mittels einer Codeliste. Aus dem Codelisteneintrag soll die Art der Nutzung hervorgehen (Identität, Adressierung, Metadaten). Beispiele zur groben Orientierung: DVDV SAFE				
localSource	Code.LocalSource 	0..n	A.3.13	52
Benennung einer lokalen Bezugsquelle, die für jeden Teilnehmer der Nachrichtenübermittlung die Parameter für die technische Adressierung von Teilnehmern bereitstellt. Angabe des Typs erfolgt mittels einer Codeliste. Aus dem Codelisteneintrag soll die Art der Nutzung hervorgehen (Identität, Adressierung, Metadaten). Beispiele zur groben Orientierung: SecretLDAP CentralDB				
technicalAvailability	technicalAvailability 	0..1	3.4.5	30
Angaben zur technischen Verfügbarkeit des Systems, vordefiniert (Codeliste) oder hier mit den Qualitäten maximale Ausfallzeit (xs:duration), minimal erwartete Verfügbarkeit (prozentual) und Betriebszeit (Wochentage, xs:time) angegeben.				
certificateInformation ^{ooo} 1		0..n		
Für diese Transportinfrastruktur zu nutzendes Zertifikat. Es wird in Bezug auf ein Unterprofil Kryptografie angegeben, hat einer Zertifizierungsstelle und dient einem Zweck.				
usage	Code.CertificateUsage 	1	A.3.3	49
Nutzungskriterium. Angabe des Typs erfolgt mittels einer Codeliste. Beispiele zur groben Orientierung: signature encryption Die bestehende Codeliste urn:xoev-de:kosit:codeliste:xta.core.certificate-usage darf nachgenutzt werden.				
	dssc:Algorithm 	0..1	A.1.2	47
Referenz auf Unterprofil Kryptografie mit Kennung, Version, Namen der Algorithmen				
certificationAuthority ^{ooo} 1		1		
Angabe der Zertifizierungsstelle, entweder als Verweis auf eine vordefinierte Liste oder direkt mit dem technischen Namen aus den Zertifikaten.				

TransportInfrastructureType ^{ooo} 1					
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
Beispiel für eine vordefinierte Liste könnte die EU/EEA Trusted List sein (https://eid.ec.europa.eu/efda/trust-services/browse/eidas/tls).					
predefined	ToBeSpecifiedType ☐	1	3.1.5	12	
Liste von offiziellen Zertifizierungsstellen. Die Liste wird extern zur Verfügung gestellt z.B. EU/EEA Trusted List. Beispielweise im eIDAS-Umfeld werden Trust Service Provider in einem Katalog aufgeführt (siehe Trust List Backbone unter Europa.eu).					
⚠️ TODO: Angabe von SchemeTerritory und einer Referenz auf einen Trust Service Provider ermöglichen.					
notPredefined	ToBeSpecifiedType ☐	1	3.1.5	12	
Liste der Zertifizierungsstellen liegt in direkten Einflussbereich der Organisation, die die konkrete Instanz des Service Profils erstellt.					
logging ^{ooo} 1		0..n			
Vorgaben zur Protokollierung mit Angabe des Formats (Codeliste), Protokollierungsart (Codeliste) und Löschrfrist (xs:duration).					
format	Code.LoggingFormat	1	A.3.15	52	
Format der Protokolle (z.B. OSCI-ProcessCardBundle, AS/4-SignalMessage oder XTA-TransportReport) angegeben über Codeliste und ⚠️ TODO: Version.					
deletionPeriod	xs:duration ☐	0..1			
Löschrfrist nach Vollendung oder Abbruch des Transports					
quality	Code.PersistenceLevel	1	A.3.17	53	
Angabe der Protokollierungsgüte erfolgt mittels einer Codeliste.					
Beispiele zur groben Orientierung:					
keine					
verpflichtend					
revisionssicher					
acknowledgement ^{ooo} 1		0..n			
Vorgaben zu Quittungen mit Angabe des Formats (Codeliste), Protokollierungsart (Codeliste) und Löschrfrist (xs:duration).					
format	Code.AcknowledgementFormat	1	A.3.1	48	
Format der Quittung angegeben über Codeliste und ⚠️ TODO: Version.					
deletionPeriod	xs:duration ☐	0..1			
Löschrfrist nach Vollendung oder Abbruch des Transports					
quality	Code.PersistenceLevel	1	A.3.17	53	
Angabe der Quittierungsgüte erfolgt mittels einer Codeliste.					
Beispiele zur groben Orientierung:					
keine					
verpflichtend					
revisionssicher					
signature	ds:SignatureType	0..1	A.1.4	47	
Signatur des Unterprofils zur Prüfung der Authentizität/Integrität.					

3.4.2.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [serviceProfile](#), [transportInfrastructure](#)

Von diesem Typ leiten ab: [transportInfrastructure](#)

3.4.3 MessageHandlingType

Typ: **MessageHandlingType**

Über die Nachrichtenbehandlung werden der Transportstandard (Codeliste), Pfade zum Ablageort der Fachnachricht und ihren Anhängen (xs:string), maximal erlaubte Größe der Fachnachricht inkl. aller Anhänge (xs:positiveInteger) sowie Löschfrist (xs:duration) und Vorgaben zur Datenhaltung (als Referenz auf Kryptografie, xs:ID) der Transportnachricht angegeben.

Abbildung 3.13. MessageHandlingType

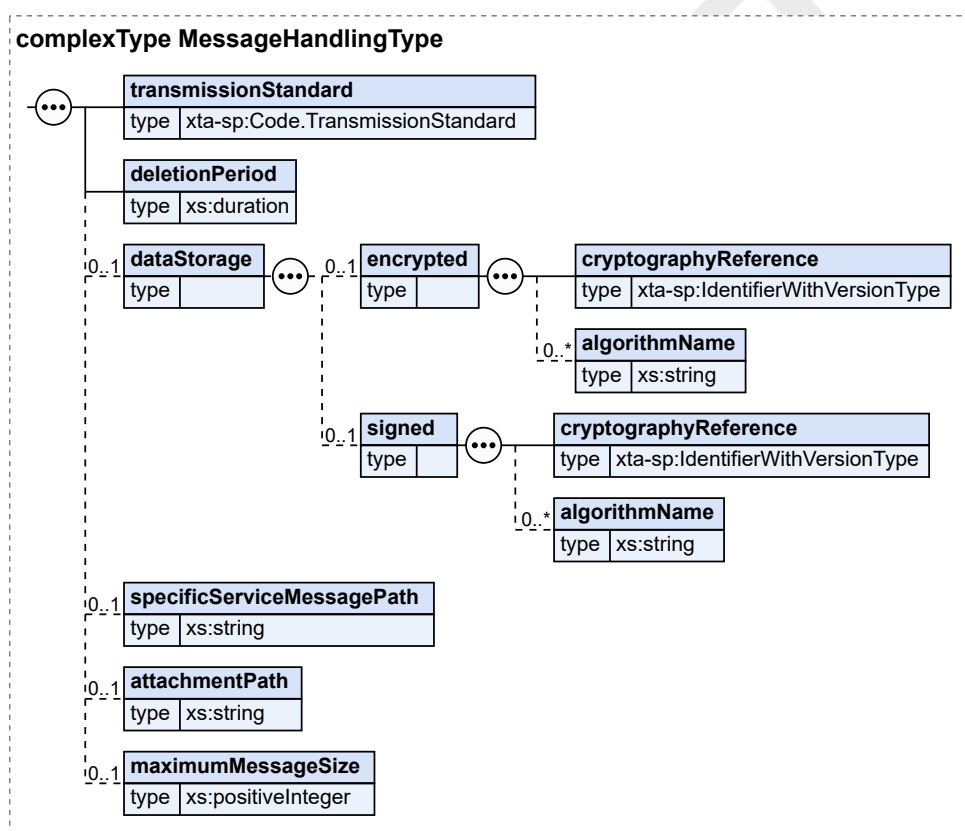


Tabelle 3.13. Struktur von MessageHandlingType

MessageHandlingType ... 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
transmissionStandard	Code.TransmissionStandard 	1	A.3.22	54	
Format und Version der Transportnachricht (z.B. OSCI, AS/4 - Peppol oder XTA).					
Angabe erfolgt mittels einer Codeliste.					

MessageHandlingType 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
⚠ TODO: Version.					
deletionPeriod	xs:duration	1			
Angabe einer Zeitspanne beginnend ab dem Zeitpunkt der Erteilung des Transportauftrags als Frist für die unwiderrufliche Löschung von Transportnachrichten.					
dataStorage 1		0..1			
Vorgaben für die Datenhaltung der Transportnachrichten, getrennt nach Vorgaben zur Verschlüsselung und Signierung/Siegelung. Sie werden als Referenz auf ein definiertes Unterprofil Kryptografie umgesetzt.					
encrypted 1		0..1			
cryptographyReference	IdentifierWithVersionType	1	3.1.3	11	
Kennung eines Kryptografieprofils.					
algorithmName	xs:string	0..n			
Weitere Einschränkung auf ein spezifisches Algorithmus.					
signed 1		0..1			
cryptographyReference	IdentifierWithVersionType	1	3.1.3	11	
Kennung eines Kryptografieprofils.					
algorithmName	xs:string	0..n			
Weitere Einschränkung auf ein spezifisches Algorithmus.					
specificServiceMessagePath	xs:string	0..1			
Generischer Pfad zur Angabe des Ablageortes für Fachnachrichten innerhalb des Transportformats					
attachmentPath	xs:string	0..1			
Generischer Pfad zur Angabe des Ablageortes für Anhänge innerhalb des Transportformats					
maximumMessageSize	xs:positiveInteger	0..1			
Maximale Größe der Fachnachricht inklusive aller Anlagen nach Encoding in Bytes					

3.4.3.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [serviceProfile](#), [transportInfrastructure](#)

3.4.4 OperatingTimeType

Typ: **OperatingTimeType**

Betriebszeit je Wochentag

Abbildung 3.14. OperatingTimeType

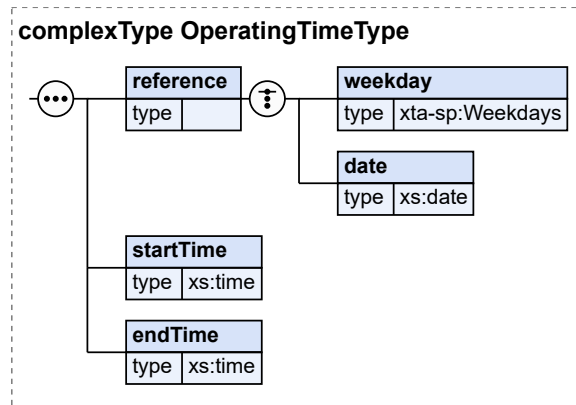


Tabelle 3.14. Struktur von OperatingTimeType

OperatingTimeType ... 1						
Kindelement		Typ / Basistyp / Referenz		Anz.	Ref.	Seite
	reference 1			1		
	weekday	Weekdays	☐	1	3.1.4	12
	Wochentag, für den eine Betriebszeit angegeben werden soll					
	date	xs:date	☐	1		
	Datum, für das eine Betriebszeit angegeben werden soll (z.B. Feiertag)					
	startTime	xs:time	☐	1		
	Beginn der Betriebszeit					
	endTime	xs:time	☐	1		
Ende der Betriebszeit						

3.4.4.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [serviceProfile](#), [transportInfrastructure](#)

3.4.5 technicalAvailability

Typ: **technicalAvailability**

Abbildung 3.15. technicalAvailability

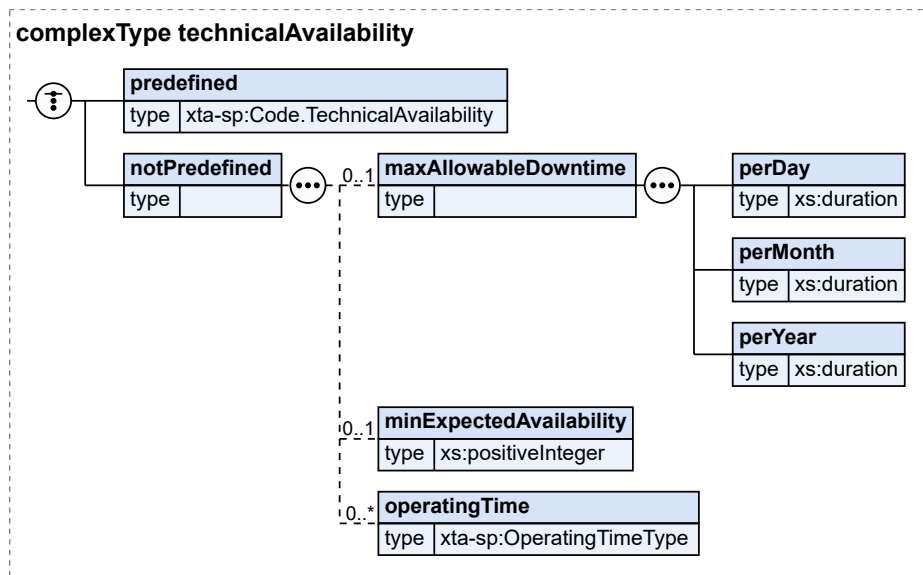


Tabelle 3.15. Struktur von technicalAvailability

technicalAvailability 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
predefined	Code.TechnicalAvailability	1	A.3.20	54	
Nutzung vordefinierter Codeliste					
notPredefined 1		1			
Nutzung eigener Vorgaben					
maxAllowableDowntime 1		0..1			
maximal erlaubte Ausfallzeit					
perDay	xs:duration	1			
pro Tag					
perMonth	xs:duration	1			
pro Monat					
perYear	xs:duration	1			
pro Jahr					
minExpectedAvailability	xs:positiveInteger	0..1			
min. erwartete Verfügbarkeit in Prozent					
operatingTime	OperatingTimeType	0..n	3.4.4	29	
Betriebszeit, für jeden Wochentag anzugeben (Mo. bis So.), für jeden Wochentag können so auch mehrere Betriebszeiträume angegeben werden; zusätzliche Angabemöglichkeit für konkrete Tage mit geplant abweichender Betriebszeit (mittels Datumsangabe)					

3.4.5.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [serviceProfile](#), [transportInfrastructure](#)

3.5 Unterprofil Kryptografie

3.5.1 cryptography

Nachricht: **cryptography**

Globale Elementdefinition zur Nachnutzung und externen Ablagemöglichkeit.

Diese Nachricht ist eine Erweiterung des Basistyps **CryptographyType** (siehe [Abschnitt 3.5.2 auf Seite 32](#)).

3.5.2 CryptographyType

Typ: **CryptographyType**

Definitionen der zu verwendenden kryptographischen Mittel. Sie ist eine Zusammenstellung von kryptographischen Mitteln (Algorithmen und Schlüssellängen), jeweils zugeordnet einem bestimmten Schutzniveau einer kryptographisch abzusichernden Kommunikation. Um die Interoperabilität zwischen Systemen sicherzustellen, werden Erzeugnisse der internationalen Gremien von IETF und europäischen Gremien von ETSI nachgenutzt. Die SecuritySuitabilityPolicy aus RFC 5698 findet in der ETSI TS 119 322 Anwendung und dient als Grundlage der Struktur des Unterprofils Kryptografie. Zusätzlich werden Ergänzungen aus ESTI wiederverwendet.

Abbildung 3.16. CryptographyType

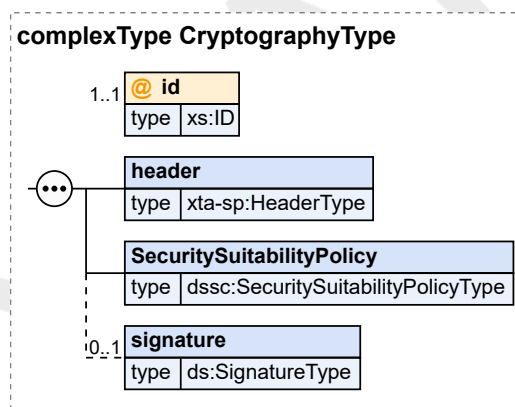


Tabelle 3.16. Struktur von CryptographyType

CryptographyType *** 1					
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
@ <i>id</i>	xs:ID ☐	1			
XML-ID zur eindeutigen Adressierung der Datenstruktur, primär für die Erstellung von XML Signaturen.					
header	HeaderType 	1	3.1.2	10	
SecuritySuitabilityPolicy	dssc:SecuritySuitabilityPolicyType 	1	A.1.2	47	
Struktur entspricht der SecuritySuitabilityPolicy nach RFC 5698.					
Die Erweiterung MoreDetails (Section A.1.3 on page 47) für SecuritySuitabilityPolicy (RFC 5698) aus ETSI TS 119 322 muss unterstützt werden. Diese muss unter /SecuritySuitabilityPolicy/Algo-					

CryptographyType ^{ooo} 1				
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
rithm/Evaluation/ als Kindelement anstelle von ##other hinterlegt werden. Ein Algorithmus mit der Angabe L in Recommendation ist nicht für neue Nachrichtentransporte empfohlen.				
signature	ds:SignatureType	0..1	A.1.4	47
Signatur des Unterprofils zur Prüfung der Authentizität/Integrität.				

3.5.2.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [cryptography](#), [serviceProfile](#)

Von diesem Typ leiten ab: [cryptography](#)

3.6 Unterprofil Automatisierung

3.6.1 automation

Nachricht: **automation**

Globale Elementdefinition zur Nachnutzung und externen Ablagemöglichkeit.

Diese Nachricht ist eine Erweiterung des Basistyps **AutomationType** (siehe [Abschnitt 3.6.2 auf Seite 33](#)).

3.6.2 AutomationType

Typ: **AutomationType**

Die Notation im Unterprofil Automatisierung dient primär der Überführung der fachlichen Vorgaben in die technische Aktivitäts-/Prozessbeschreibung für die operationale Ebene (Systeme / Software). Die Reihenfolge der Aktivitäten für einen Nachrichtentransport lässt sich präzise formulieren, gemäß den Vorgaben der Fachlichkeit. Gleichwohl ist die Notation auch auf der Ebene der jeweiligen Fachlichkeit anwendbar. So kann z.B. der gesamte fachliche Nachrichtenprozess modelliert und spezifiziert werden. Hierbei ergeben sich vor dem Hintergrund der Diskussion um „RegisterClouds“, also um die einheitliche Spezifikation der Datenbanken inkl. Tabellen und Felder, enorme Möglichkeiten. Wenn also von einer spezifizierten Datenhaltung ausgehen, wie eben beschrieben, dann kann die mit dieser Notation erstellte Spezifikation verwendet werden, um sie in allen diesen Registern unmittelbar anzuwenden. Damit dient die Notation nicht mehr nur zu Notation, sondern vielmehr zu Implementierung der normativen Vorgaben. Jede einzelne Automatisierung im Unterprofilbereich Automatisierung kann gesiegelt / signiert und referenziert werden.

Abbildung 3.17. AutomationType

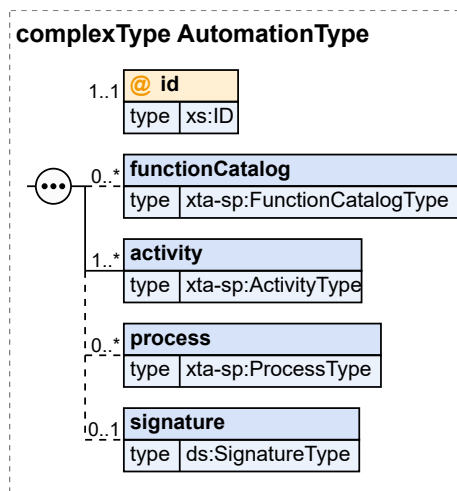


Tabelle 3.17. Struktur von AutomationType

AutomationType ^{0..1}				
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
@ <i>id</i>	xs:ID	1		
XML-ID zur eindeutigen Adressierung der Datenstruktur, primär für die Erstellung von XML Signaturen.				
functionCatalog	FunctionCatalogType	0..n	3.6.3	35
In einem Funktionskatalog werden Funktionen gebündelt. Funktionen werden als "atomare Einheit" von Funktionalität betrachtet und können Eingabe-, Rückgabewerte (Name, Type) sowie Fehlerausgabe (Type, ErrorCode) umfassen. Funktionen haben eine Kennung, die in Kombination mit der Kennung des Funktionskatalogs eine eindeutige Zuordnung / Aufruf ermöglicht. Der Funktionskatalog besitzt neben der Kennung auch eine Version und ggf. einen Namensraum.				
TODO: Simple Beispielinstanzen erstellen.				
activity	ActivityType	1..n	3.6.5	36
Aktivität ist eine Erweiterung einer Funktion um die Möglichkeit, eine Sequenz von Funktions- / Aktivitäts- / Prozessaufrufen zu definieren. Wie Funktionen verfügen Aktivitäten ebenfalls über Eingabe-, Rückgabewerte (Name, Type) sowie Fehlerausgabe. Zusätzlich können (lokale) Variablen und Konstanten definiert werden. Für eine Aktivität kann eine Gültigkeit (von / bis) angegeben werden und jede Aktivität hat eine Kennung, die eine Referenzierung innerhalb eines Profils ermöglicht.				
TODO: Simple Beispielinstanzen erstellen.				
process	ProcessType	0..n	3.6.9	40
Prozess ermöglicht die Beschreibung von Abläufen, entlang derer sich Daten zwischen (Eingabe-, Ausgabe-, lokalen) Stellen oder zwischen Aktivitäten bewegen.				
TODO: Simple Beispielinstanzen erstellen.				
signature	ds:SignatureType	0..1	A.1.4	47
Signatur des Unterprofils zur Prüfung der Authentizität/Integrität.				

3.6.2.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

Von diesem Typ leiten ab: [automation](#)

3.6.3 FunctionCatalogType

Typ: **FunctionCatalogType**

Abbildung 3.18. FunctionCatalogType

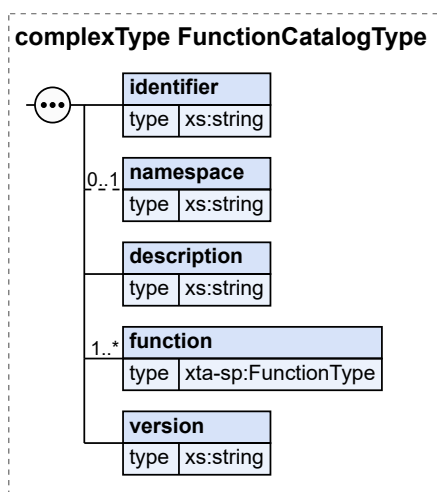


Tabelle 3.18. Struktur von FunctionCatalogType

FunctionCatalogType ∞ 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
identifier	xs:string	□ 1		
Eindeutige Kennung z.B. XTA-WS				
namespace	xs:string	□ 0..1		
Beispiel: https://xoev.de/transport/xta/core/3.1.1				
description	xs:string	□ 1		
Beschreibung des Kontextes inkl. fachlich-technischer Zuordnung der Funktionen, die in Produkten/Rechenzentren/Softwareartefakten/Systembibliotheken implementiert und eindeutig referenzierbar/aufrufbar sind.				
function	FunctionType	□ 1..n	3.6.4	35
Funktionen werden als "atomare Einheit" von Funktionalität betrachtet und können Eingabe-, Rückgabewerte (Name, Type) sowie Fehlerausgabe (Type, ErrorCode) umfassen. Funktionen haben eine Kennung, die in Kombination mit der Kennung des Funktionskatalogs eine eindeutige Zuordnung / Aufruf ermöglicht.				
version	xs:string	□ 1		
Version z.B. 3.1.1				

3.6.3.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

3.6.4 FunctionType

Typ: **FunctionType**

Abbildung 3.19. FunctionType

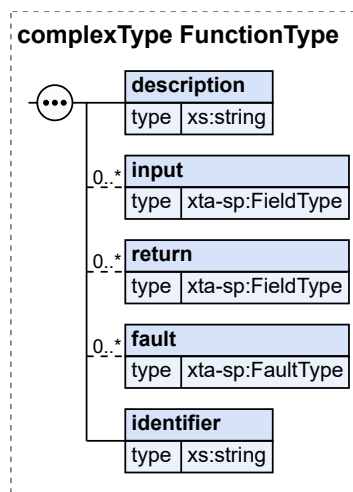


Tabelle 3.19. Struktur von FunctionType

FunctionType ^{0..1}					
Kindelement	Typ / Basistyp / Referenz		Anz.	Ref.	Seite
description	xs:string	□	1		
Erfüllungszweck					
input	FieldType	☐	0..n	3.6.6	38
Eingabeparameter/Argument z.B. mmd : MessageMetaData.					
return	FieldType	☐	0..n	3.6.6	38
Ausgabeparameter/Rückgabe z.B. cocore : ContentContainerReply.					
fault	FaultType	☐	0..n	3.6.8	39
Möglicher Ausnahmeereignis z.B. MessageVirusDetectionException mit Code 9060					
identifier	xs:string	□	1		
Eindeutige Kennung z.B. sendMessageSync					

3.6.4.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

3.6.5 ActivityType

Typ: **ActivityType**

Abbildung 3.20. ActivityType

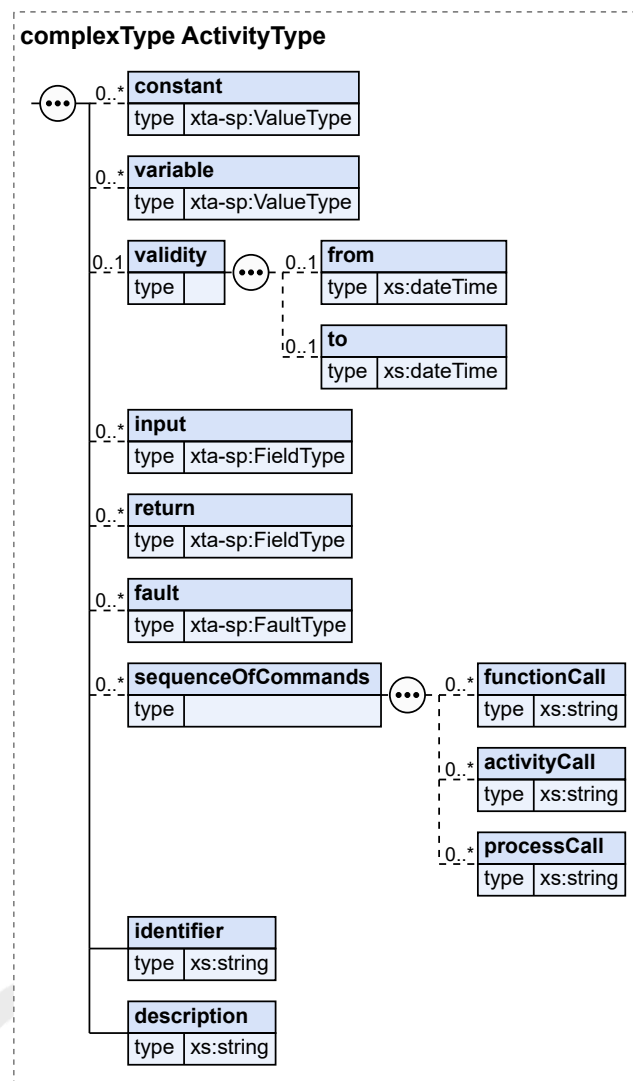


Tabelle 3.20. Struktur von ActivityType

ActivityType ^{0..1}				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
constant	ValueType	0..n	3.6.7	39
Enthält einen unveränderlichen Wert				
variable	ValueType	0..n	3.6.7	39
Enthält einen veränderlichen Wert				
validity ^{0..1}		0..1		
Angabemöglichkeit zum Verwendungszeitraum/Gültigkeit der Aktivität				
from	xs:dateTime	0..1		
Von				

ActivityType ^{...} 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
to	xs:dateTime	☐	0..1		
Bis					
input	FieldType	☐	0..n	3.6.6	38
Eingabeparameter/Argument z.B. mmd : MessageMetaData.					
return	FieldType	☐	0..n	3.6.6	38
Ausgabeparameter/Rückgabe z.B. cocore : ContentContainerReply.					
fault	FaultType	☐	0..n	3.6.8	39
Möglicher Ausnahmeereignis z.B. MessageVirusDetectionException mit Code 9060					
sequenceOfCommands ^{...} 1			0..n		
Angabe einer Sequenz von Funktionen / Aktivitäten / Prozessen, die von dieser Aktivität nacheinander aufgerufen wird.					
🚧 TODO: Gestaltung weiter ausarbeiten.					
functionCall	xs:string	☐	0..n		
Aufruf einer Funktion inkl. Angabe des Katalogs					
activityCall	xs:string	☐	0..n		
Aufruf einer Aktivität					
processCall	xs:string	☐	0..n		
Aufruf eines Prozesses					
identifizier	xs:string	☐	1		
Eindeutige Kennung					
description	xs:string	☐	1		
Beschreibung der durch die Aktivität abgedeckten Vorgänge.					

3.6.5.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

3.6.6 FieldType

Typ: **FieldType**

Technische Definition eines Feldes auf der jeweiligen Datenebene.

Abbildung 3.21. FieldType

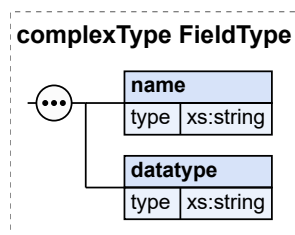


Tabelle 3.21. Struktur von FieldType

FieldType ^{...} 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
name	xs:string ☐	1		
Technischer Name des Feldes auf der jeweiligen Datenebene.				
datatype	xs:string ☐	1		
Technischer Typ des Feldes auf der jeweiligen Datenebene.				

3.6.6.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

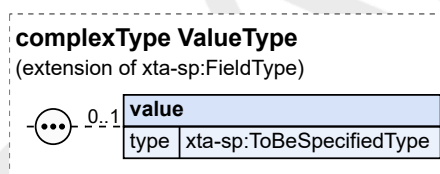
Von diesem Typ leiten ab: [ValueType](#)

3.6.7 ValueType

Typ: **ValueType**

Technische Definition eines Datenfeldes mit Wert.

Abbildung 3.22. ValueType



Dieser Datentyp ist eine Erweiterung des Basistyps **FieldType** (siehe [Abschnitt 3.6.6 auf Seite 38](#)).

Tabelle 3.22. Struktur von ValueType

ValueType ^{...} 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
value	ToBeSpecifiedType ☐	0..1	3.1.5	12
Wert. Typ eventuell any*				

3.6.7.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

3.6.8 FaultType

Typ: **FaultType**

Abbildung 3.23. FaultType

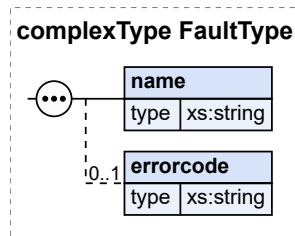


Tabelle 3.23. Struktur von FaultType

FaultType ^{...} 1					
Kindelement	Typ / Basistyp / Referenz		Anz.	Ref.	Seite
name	xs:string	☐	1		
Name des Fehlertyps z.B. VirusDetectedException					
errorcode	xs:string	☐	0..1		
Spezifischer Code zur weiteren Eingrenzung des Fehlers					

3.6.8.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

3.6.9 ProcessType

Typ: **ProcessType**

Abbildung 3.24. ProcessType

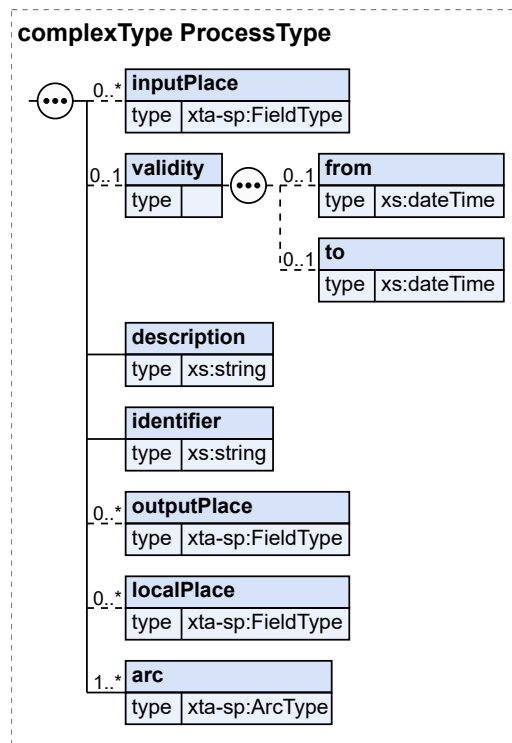


Tabelle 3.24. Struktur von ProcessType

ProcessType ... 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
inputPlace	FieldType	0..n	3.6.6	38
Eingangsstelle.				
validity ... 1		0..1		
Angabemöglichkeit zum Verwendungszeitraum/Gültigkeit des Prozesses				
from	xs:dateTime	0..1		
Von				
to	xs:dateTime	0..1		
Bis				
description	xs:string	1		
Beschreibung der durch die Aktivität abgedeckten Vorgänge.				
identifier	xs:string	1		
Eindeutige Kennung				
outputPlace	FieldType	0..n	3.6.6	38
Ausgabestelle.				
localPlace	FieldType	0..n	3.6.6	38
Stelle zur Verwendung innerhalb des Prozesses.				

ProcessType ... 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
arc	ArcType	1..n	3.6.10	42
Kante				

3.6.9.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

3.6.10 ArcType

Typ: **ArcType**

Abbildung 3.25. ArcType

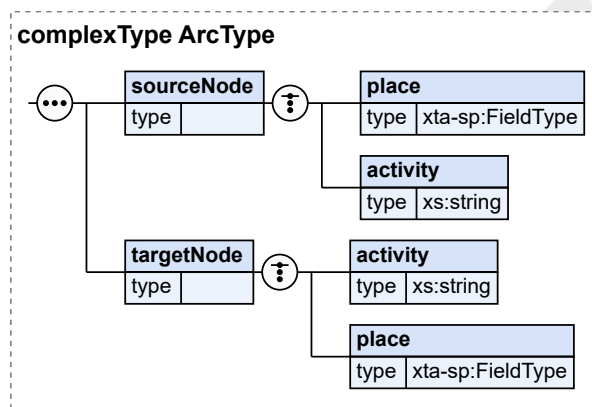


Tabelle 3.25. Struktur von ArcType

ArcType ... 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
sourceNode ... 1		1		
SourceNode entsprechend Definition Petri-Netz Modell				
place	FieldType	1	3.6.6	38
Eingehende Stelle				
activity	xs:string	1		
identifizier der Aktivität				
targetNode ... 1		1		
TargetNode entsprechend Definition Petri-Netz Modell				
activity	xs:string	1		
identifizier der Aktivität				
place	FieldType	1	3.6.6	38
Ausgehende Stelle				

3.6.10.1 Nutzung des Datentyps

Dieser Typ kann in den folgenden Nachrichten übermittelt werden: [automation](#), [serviceProfile](#)

3.7 Nachweisbarkeit der Servicequalitäten

 In diesem Kapitel werden alle Elemente der Berichterstattung zwecks Nachweises und Überprüfung der erbrachten Servicequalitäten definiert. Hierfür müssen der Bericht vom Typ **ServiceReportType** und alle Ereignisse vom Typ **EventType** in diese Spezifikation integriert werden. Dementsprechend werden sich die Hauptspezifikation (XTA-WS) und die Spezifikation der Erweiterung Service Reporting verändern.

Die Einhaltung der Servicequalitäten während der technischen Abarbeitung eines Transportauftrages ist anhand eines Serviceberichts zu prüfen. Der Bericht wird von Autoren und Lesern dazu verwendet, die Einhaltung des Transportauftrags bzw. der Servicequalitäten zu kontrollieren. Entsprechend können Sender und Empfänger mittels eines **serviceReport** nachweisen, dass der Transportauftrag eingehalten wurde. Sender erstellen einen ServiceReport für Autoren, Empfänger einen ServiceReport für Leser. Stehen für einen Transportauftrag sowohl der ServiceReport des Senders als auch des Empfängers zur Verfügung, kann die Einhaltung des Transportauftrags vom Versand bis zum Empfang nachgewiesen bzw. kontrolliert werden.

Mit dem ServiceReport soll insbesondere auch die rechtskonforme Funktionsweise der den Transport durchführenden Infrastruktur nachvollzogen werden können. Der ServiceReport ermöglicht Aussagen über die Einhaltung gesetzlicher Anforderungen und die Erfüllung von Vorgaben aus Serviceprofilen. Er dient ferner als zusätzliches Mittel zur Fehlerverfolgung in Transportprozessen.

3.7.1 serviceReport

Globale Eigenschaft: **serviceReport**

Diese globale Eigenschaft ist eine Erweiterung des Basistyps **ServiceReportType** (siehe [Abschnitt 3.7.3 auf Seite 44](#)).

3.7.2 signedServiceReport

Globale Eigenschaft: **signedServiceReport**

Datentyp für einen signierten ServiceReportType

Abbildung 3.26. signedServiceReport

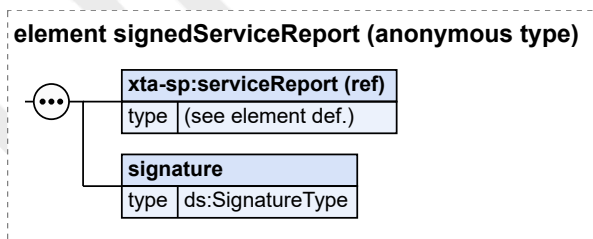


Tabelle 3.26. Struktur von signedServiceReport

signedServiceReport 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
	serviceReport 	1	3.7.1	43

Signatur des Serviceberichts zur Prüfung der Authentizität/Integrität.

Der Typ dieses Elements ist eine Erweiterung des Basistyps **ServiceReportType** (siehe [Abschnitt 3.7.3 auf Seite 44](#)).

signedServiceReport ... 1					
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
signature	ds:SignatureType 	1	A.1.4	47	
Signatur des Serviceberichts zur Prüfung der Authentizität/Integrität.					

3.7.3 ServiceReportType

Typ: **ServiceReportType**

Struktur eines Berichts über die Einhaltung der Servicequalitäten während der technischen Abarbeitung eines Transportauftrages.

Abbildung 3.27. ServiceReportType

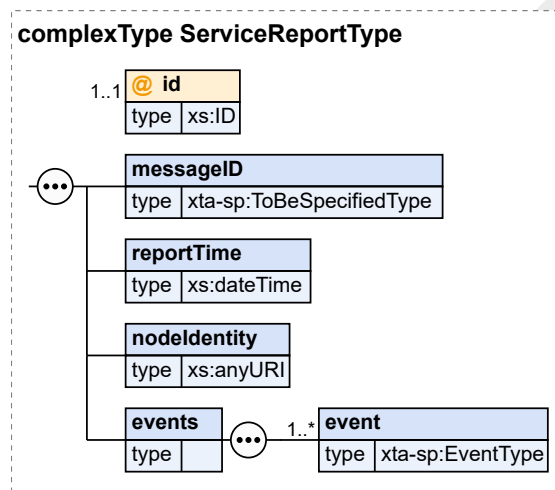


Tabelle 3.27. Struktur von ServiceReportType

ServiceReportType ... 1					
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite	
@ <i>id</i>	xs:ID ☐	1			
Hier muss die ID zur eindeutigen Referenzierung des XML-Elements eingetragen werden. Primär wird die Referenz für die Erstellung der Signatur im SelectionResult benötigt.					
messageID	ToBeSpecifiedType ☐	1	3.1.5		12
Der eindeutige Identifikator des Transportauftrags. Er ist über die gesamte Datenübermittlung die eindeutige Referenz des Transportauftrages. Der Autor lässt den Identifikator vor der Beauftragung des Transports durch den Sender erstellen, um ihn dann für den Transport dem Sender zu übergeben. In Verbindung mit dem Modul XTA Webservice muss die XTAMessageID als Identifikator eingetragen werden.					
 Sollten hier noch weitere Identifier eingefügt werden können? z.B. wie AdditionalIdentifier aus XTA-WS					
reportTime	xs:dateTime ☐	1			
Zeitpunkt der letzten Aktualisierung des Protokolls. Ist bei Fortschreibung des Protokolls zu überschreiben.					
nodeIdentity	xs:anyURI ☐	1			
Hier wird die Identität des Beteiligten des Transports bzw. seine Softwareinstanz angegeben. Im Aufbau der URI soll erkennbar sein, welcher Organisation der Ersteller angehört.					

ServiceReportType ... 1				
Kindelement/Attribut	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
⚠ Soll zusätzlich noch PartyType als weitere Identitätszuordnung eingetragen werden können?				
events ... 1		1		
Liste der Ereignisse.				
event	EventType	1..n	3.7.4	45
Hier werden Ereignisse eingetragen.				

3.7.3.1 Nutzung des Datentyps

Von diesem Typ leiten ab: [serviceReport](#)

3.7.4 EventType

Typ: **EventType** (abstrakt)

Die Grundstruktur für alle Ereignisse. Als Grundbestandteil wird der EreignisType nie direkt verwendet. An seiner Stelle wird immer ein daraus abgeleiteter, konkreter Nachweis definiert.

⚠ Konkrete Ereignisse passend zu Haupt- und Unterprofilen sind zu erarbeiten.

Die Ereignisse im ServiceReport werden vom Sender und Empfänger während der Abarbeitung von Transportaufträgen protokolliert. Aus diesen Ereignissen erstellen Sender und Empfänger den ServiceReport, wenn dieser durch den Autor oder den Leser angefordert wird. Autor oder Leser bestimmen beim Abruf, zu welchen Transportaufträgen die jeweiligen Serviceberichte geliefert werden sollen.

Abbildung 3.28. EventType

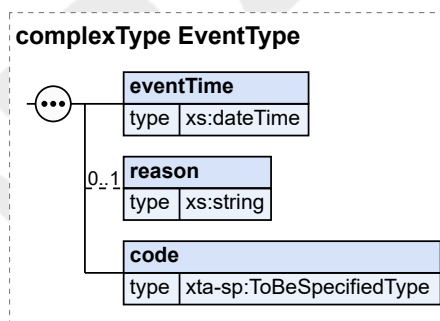


Tabelle 3.28. Struktur von EventType

EventType ... 1				
Kindelement	Typ / Basistyp / Referenz	Anz.	Ref.	Seite
eventTime	xs:dateTime	1		
Der Zeitpunkt, an dem das Ereignis protokolliert wird.				
reason	xs:string	0..1		
Hier wird zur weiteren Erläuterung der Grund der Meldung als Freitext eingetragen.				
code	ToBeSpecifiedType	1	3.1.5	12
Eindeutiger Identifikator des Ereignisses, das durch den Protokolleintrag dokumentiert wird z.B. aus der Codeliste, die das Ereignis beschreibt.				

3.7.4.1 Nutzung des Datentyps

Dieser Typ wird in diesem Modell nicht verwendet.

DRAFT

A Anhänge



A.1 Eingebundene externe Modelle

Folgende externe Modelle werden in diesem Standard verwendet und sind auf den XÖV-Webseiten (siehe <https://docs.xoev.de/>) oder im XRepository (siehe <http://www.xrepository.de>) veröffentlicht:

A.1.1 XÖV-Bibliothek

Kennung: urn:xoev-de:kosit:xoev:bibliothek:xoevbibliothek; Fassung: 2025-11-14

Folgende Inhalte aus dem externen Modell werden in diesem Standard verwendet:

Name	Namensraum
xoev-code:Code	http://xoev.de/schemata/code/1_0

A.1.2 DSSC (RFC 5698)

Kennung: urn:xoev-de:etsi:standard:rfc-5698; Version: 1.0

Folgende Inhalte aus dem externen Modell werden in diesem Standard verwendet:

Name	Namensraum
dssc:Algorithm	urn:ietf:params:xml:ns:dssc
dssc:SecuritySuitabilityPolicyType	urn:ietf:params:xml:ns:dssc

A.1.3 ETSI TS 119 322

Kennung: urn:xoev-de:etsi:standard:ts-119-322; Version: 1.1.1

Folgende Inhalte aus dem externen Modell werden in diesem Standard verwendet:

Name	Namensraum
etsi-19322:MoreDetails	http://uri.etsi.org/19322/v1.1.1#

A.1.4 XML Signature

Kennung: urn:xoev-de:w3c:standard:xmldsig_09-2000; Version: 1.1

Folgende Inhalte aus dem externen Modell werden in diesem Standard verwendet:

Name	Namensraum
ds:SignatureType	http://www.w3.org/2000/09/xmldsig#

A.2 Übersicht Code-Datentypen

In diesem Abschnitt sind die in XTA 2 SP verwendeten Code-Datentypen in der Übersicht dargestellt.

A.2.1 Code-Typ 1, 2 und 4

In der nachstehenden Tabelle werden die folgenden Informationen dargestellt:

Code-Datentyp

Alle in XTA 2 SP definierten Code-Datentypen des Typs 1, 2 und 4 in alphabetischer Reihenfolge.

Codeliste

Der Name (kurz)¹ der im jeweiligen Code-Datentyp genutzten Codeliste.

Version

Die Version der im jeweiligen Code-Datentyp genutzten Codeliste (Attribut listVersionID).

Typ

Art der Codelistennutzung, wie im Codelisten-Handbuch beschrieben.

Code-Datentyp	Codeliste	Version	Typ
Code.AcknowledgementFormat	--	--	4
Code.Authenticity	--	--	4
Code.CertificateUsage	--	--	4
Code.ComplianceDocumentationManufacturer	--	--	4
Code.ComplianceDocumentationOperator	--	--	4
Code.ComplianceDocumentationType	--	--	4
Code.DataAccessRestrictions	--	--	4
Code.DataDeletionPolicy	--	--	4
Code.DirectoryService	--	--	4
Code.DomainTransitionRestrictions	--	--	4
Code.Immutability	--	--	4
Code.InfrastructureComponent	--	--	4
Code.LocalSource	--	--	4
Code.LogBasedTraceability	--	--	4
Code.LoggingFormat	--	--	4
Code.MessageRevocation	--	--	4
Code.PersistenceLevel	Level of Persistence	0.1	1
Code.Quality	--	--	4
Code.Segment	--	--	4
Code.TechnicalAvailability	--	--	4
Code.TechnicalAvailabilityInProtectionGoals	--	--	4
Code.TransmissionStandard	--	--	4
Code.UpdatePolicy	--	--	4

A.3 Codes

A.3.1 Code.AcknowledgementFormat

Codelisten	
-beschreibung	unbestimmt

¹Weitere Informationen zu den Metadaten einer Codeliste sind im aktuellen Codelisten-Handbuch beschrieben.

Codelisten	
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.2 Code.Authenticity

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.3 Code.CertificateUsage

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.4 Code.ComplianceDocumentationManufacturer

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.5 Code.ComplianceDocumentationOperator

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.6 Code.ComplianceDocumentationType

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.7 Code.DataAccessRestrictions

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.8 Code.DataDeletionPolicy

Codelisten	
-beschreibung	unbestimmt

Codelisten	
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.9 Code.DirectoryService

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.10 Code.DomainTransitionRestrictions

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.11 Code.Immutability

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.12 Code.InfrastructureComponent

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.13 Code.LocalSource

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.14 Code.LogBasedTraceability

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.15 Code.LoggingFormat

Codelisten	
-beschreibung	unbestimmt

Codelisten	
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.16 Code.MessageRevocation

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.17 Code.PersistenceLevel

Codelisten	
-beschreibung	Die Codeliste klassifiziert die Güte der Datenpersistierung.
-nutzung	Typ: 1, Inhalte der Codeliste siehe Seite 56
-kennung	urn:xoev-de:kosit:codeliste:xta.serviceprofile.persistence.level
-version	0.1

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	keineNutzung
Umsetzung der Codelistenversion als benannter Datentyp	true

A.3.18 Code.Quality

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.19 Code.Segment

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.20 Code.TechnicalAvailability

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.21 Code.TechnicalAvailabilityInProtectionGoals

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.22 Code.TransmissionStandard

Codelisten	
-beschreibung	unbestimmt

Codelisten	
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.3.23 Code.UpdatePolicy

Codelisten	
-beschreibung	unbestimmt
-nutzung	Typ: 4, siehe Beschreibung des Code-Datentyps
-kennung	unbestimmt
-version	unbestimmt

Konfiguration des Codedatentyps (soweit angegeben und von XÖV-Default-Einstellung abweichend):

Eigenschaft	Wert
Nutzung des name -Elements	optional

A.4 Codelisten

In diesem Abschnitt sind die in XTA 2 SP verwendeten Codelisten und ihre Inhalte aufgeführt.

A.4.1 Übersicht Codelistenversionen (Typ 1 und 2)

In der nachstehenden Tabelle werden die folgenden Informationen dargestellt:

Codeliste

Alle in XTA 2 SP genutzten Codelistenversionen in alphabetischer Reihenfolge, die in mindestens einem Code-Datentyp genutzt werden (Typ der Codelistennutzung 1 bis 2).²

Version

Die Version der Codeliste.

Code-Datentyp(en)

Die die jeweilige Codeliste nutzenden Code-Datentypen.²

Die Namen der Code-Datentypen und der Codelisten stellen Links zu den jeweiligen Detail-Abschnitten dar.

Codeliste	Version	Code-Datentyp(en)
Persistence Level	0.1	Code.PersistenceLevel

²Sofern in der Spalte „Code-Datentyp(en)“ kein Eintrag vorhanden ist, bedeutet dies, dass der Standard die jeweilige Codeliste verwendet und dokumentieren möchte. Der die Codeliste nutzende Code-Datentyp ist jedoch nicht im Standard selbst spezifiziert, sondern in einem externen Modell.

A.4.2 Details

A.4.2.1 Persistence Level

A.4.2.1.1 Metadaten

Metadatenelement	Wert
Name (lang)	Level of Persistence
Name (kurz)	Persistence Level
Kennung	urn:xoev-de:kosit:codelist:xta.serviceprofile.persistence.level
Beschreibung der Codeliste	Die Codeliste klassifiziert die Güte der Datenpersistierung.
Beschreibung der Codelistenversion	Initiale Version der Codeliste.
Herausgeber	Koordinierungsstelle für IT-Standards (KoSIT)
Version	0.1

A.4.2.1.2 Daten

code	name
audit	Daten werden bei jeder Änderung revisioniert abgelegt und jede Revision ist abrufbar.
mandatory	Daten werden immer erfasst und aktuell gehalten.
none	keine Datenerfassung erforderlich

A.5 Versionshistorie

A.5.1 Grobentwurf / Konzept Version 2.0.0 (12.06.2026)

Grobentwurf / Konzept - Version 2.0.0 der Spezifikation XTA Service Profile zur Veröffentlichung und Erkundung nach neuen Stakeholdern zwecks einer Mitwirkung in der weiteren Gestaltung/Entwicklung.

A.6 Mitwirkende

Name	Organisation
Martin Rost	Unabhängige Landeszentrum für Datenschutz AöR (ULD)
Marc Behrens	Zweckverband Kommunale Datenverarbeitung Oldenburg KöR (KDO)
Frank Grubert	ekom21
Pascal Pult	Jinit[AG i.A. Landesbetrieb Rheinland-Pfalz Daten und Information (LDI-RP)
Andreas Körnig	Procilon GmbH
Andre Peiffer	SEVEN PRINCIPLES AG
Dennis Knipper	SEVEN PRINCIPLES AG
Birger Streckel	Dataport AöR i.A. IT-Servicezentrum der bayerischen Justiz (Jus-IT BY)
Klaus Lüttich	Governikus GmbH & Co. KG (teils als Dienstleister der KoSIT)
Ralf Lindemann	Governikus GmbH & Co. KG (teils als Dienstleister der KoSIT)
Christin Tabrizi	Governikus GmbH & Co. KG

Name	Organisation
Daniel Frehse-Aufderheide	Governikus GmbH & Co. KG
Andrea Westphal	HSH Soft- und Hardware Vertriebs GmbH
Carsten Reimann	HSH Soft- und Hardware Vertriebs GmbH
Helge Hauschild	Dataport AöR
Eric Seipp	Nortal AG (teils Dienstleister der KoSIT)
Karen Lahmann	LAVA Unternehmensberatung eGbR (teils Dienstleister der KoSIT)
Julius Bauer	jinit[AG (teils Dienstleister der KoSIT)
Oliver Budke	jinit[AG (teils Dienstleister der KoSIT)
Jörg Schneider	Koordinierungsstelle für IT-Standards (KoSIT)
Thomas Dodenhoff	Koordinierungsstelle für IT-Standards (KoSIT)

Hinweis: Die aktuelle Liste ist bisher noch unvollständig auf Grund von ausstehenden Einwilligungen zur Eintragung (organisationsinterne Freigabeprozesse).