Virtuelle Poststelle des Bundes
OCSP/CRL-Relay
Schnittstellenbeschreibung

bremen online services
GmbH & Co. KG

Virtuelle Poststelle des Bundes, Release 2.2

Dokument-Version 2.2

Dokument Version 2.2 vom 31. Oktober 2005

Erstellt von:

Marc Horstmann

Hamed Tabrizi

Gregor Leander

André Jens

Dieses Dokument kann bezogen werden über:

Bundesamt für Sicherheit in der Informationstechnik
Referat I 1.1
Postfach 200363
53133 Bonn

Tel.: +49 (1888) 9582-232
Fax: +49 (1888) 9582-405
E-Mail: egov@bsi.bund.de

bremen online services GmbH & Co. KG

Matthias Intemann
Am Fallturm 9
28359 Bremen

Tel.: +49 (421) 20495-62
Fax: +49 (421) 20495-11
E-Mail: mi@bos-bremen.de

Weitere Informationen zur Virtuellen Poststelle des Bundes finden Sie unter:

http://www.bsi.de/fachthem/egov/vps.htm

Inhaltsverzeichnis

1 Einleitung

Im Rahmen der Virtuellen Poststelle – Basiskomponente Datensicherheit (VPS) des Bundes wird ein Web-Service zur Verfügung gestellt, welcher das Prüfen und Auffinden von Zertifikaten vereinfachen soll. Dieses „OCSP/CRL-Relay" nimmt der einzelnen Anwendung dabei die offline durchführbaren Zertifikatsprüfungen ab, bildet die Zertifikatsketten und stellt für die Online-Prüfungen die Verbindungen mit den Verzeichnisdiensten der Trust-Centern gemäß deren jeweiligen technischen Möglichkeiten und eingesetzten Protokollen her. Die Antworten beinhalten zudem Informationen, welche der Anwendung die Entscheidung erleichtern, ob das Zertifikat für den beabsichtigten Zweck verwendet werden darf. Zusätzlich wird eine Infrastruktur aufgebaut, welche das Lokalisieren von Zertifikaten der Kommunikationspartner erleichtert.

Das vorliegende Dokument spezifiziert die Schnittstellen des OCSP/CRL-Relays in Release 2.0 der Virtuellen Poststelle. Um die Anforderungen den Deutschen Signaturgesetztes (SigG) und die Vorgaben von ISIS-MTT[1] zu erfüllen, ist das dem OCSP/CRL-Relay zugrunde liegende XKMS[2]-Protokoll erweitert worden.

In die vorliegende Version sind Neuerungen der europäischen Standardisierungsbemühungen (ETSI-Zertifikatsprofile) sowie Ergebnisse der Harmonisierungsbemühungen im Rahmen des Signaturbündnisses[3] eingegangen.

Client-Anwendungen der Virtuellen Poststelle bedienen sich für Zertifikatsvalidierungen der Dienste des OCSP/CRL-Relay über das VPS-Kernsystem und vorgeschaltete Web-Serveranwendungen. Die korrekte Interpretation der XKMS-Responses des Relays obliegt der Verantwortung der Client-Anwendungen.

Zum Verständnis dieses Dokuments wird von der Kenntnis der im Kapitel [11.1 Referenzdokumente] aufgeführten Grundlagen ausgegangen.

An dieser Stelle noch ein Hinweis: Sofern in dem vorliegenden Dokument für Personen die männliche Form benutzt wird, geschieht dies nur der besseren Lesbarkeit wegen und hat keinen diskriminierenden Hintergrund. Selbstverständlich sind z.B. bei „Anwender" oder „Nutzer" auch immer die Anwenderin oder Nutzerin gemeint.

1 http://www.t7-isis.de/ISIS-MTT/isis-mtt.html

2 http://www.w3.org/TR/2003/WD-xkms2-20030418/

3 http://www.staat-modern.de/E-Government/-,10111/Signaturbuendnis.htm

2 Funktionsübersicht

Das OCSP/CRL-Relay deckt Anforderungen im Kontext von Public-Key Infrastrukturen (PKI) ab, welche im Zusammenhang mit der elektronischen Signatur sowie der Verschlüsselung und Authentisierung über X509-Zertifikate anfallen. Im Detail sind die Funktionaliäten beschrieben in [Releasebeschreibung des OCSP/CRL-RelaysReleasebeschreibung des OCSP/CRL-Relays].

Zusammengefasst sind dies

- die Statusüberprüfung des dem verwendeten Schlüssel zugeordneten Zertifikats,
- das Extrahieren von Zertifikats-Informationen.

Eine weitere Anforderung - das Lokalisieren von Zertifikaten in Verzeichnisdiensten über verschiedene Suchkriterien wie Name, E-Mail-Adresse etc. – wird in Release 2.2 der Virtuellen Poststelle zunächst direkt über das Kernsystem der VPS gelöst[4]. Es ist für ein späteres Release de VPS geplant, diese Funktionalität ebenfalls in das OCSP/CRL-Relay aufzunehmen.

Der Zugriff auf das OCSP/CRL-Relay erfolgt entweder per JMS oder direkt mittels http(s) Bei einem direkten Zugriff erfolgt die Kommunikation über ein Java-Servlet mittels http(s)-POST. Die Anfrage und Antworten werden auf der Grundlage des XKMS[5] Protokolls in der Version 2, welches vom W3C veröffentlicht wurde, formuliert.

XKMS-Anfragen, welche über http oder https gestellt werden, müssen das SOAP-Binding[6] unterstützen.

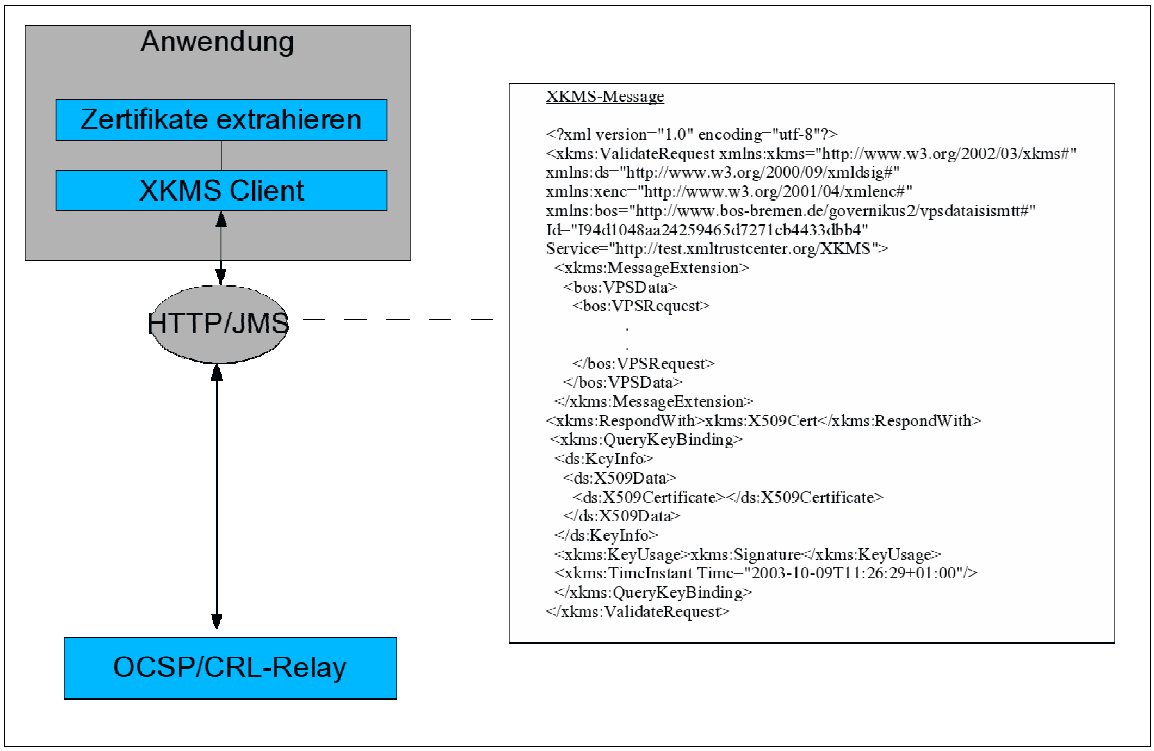


Abbildung 1: Client-Server Kommunikation

4 siehe SCHNITTKERN

5 http://www.w3.org/TR/xkms2/

6 http://www.w3.org/TR/xkms2-bindings/

3 Das XKMS2-Protokoll

Einer der wesentlichen Gründe für die Wahl von XKMS2 war die Datenstruktur. Der gesamte Informationsaustausch erfolgt auf Basis von XML-strukturierten Datenströmen. Die Technik kommt auch in den anderen Softwareeinheiten der VPS zum Einsatz. Daraus ergibt sich eine durchgängig identische Technik im gesamten System. XKMS2 ist ein Standard, der bereits viele Anforderungen abdeckt, von vielen Herstellern unterstützt wird und darüber hinaus gut erweiterbar ist, um das breite Anforderungsspektrum der Konzepte der VPS funktional umzusetzen. XKMS2 bietet von Haus aus die Möglichkeit, mehrere Zertifikate in einer einzigen Anfrage zu unterstützen, was in anderen Protokollen nicht vorgesehen ist. Zudem umfasst dieses Protokoll neben der Validierung von Zertifikaten eine Suchfunktion sowie die Key-Registrierung.

Mittels des XKMS2-Protokolls werden Dienste wie das Validieren, Lokalisieren und Registrieren von Zertifikaten zentralisiert werden. Dies bündelt den Aufwand für Administration und Kommunikation mit den Verzeichnisdiensten in ihrer bestehenden Vielfalt an zentraler Stelle. Die Inanspruchnahme der Dienste kann über eine einheitliche, stabile Schnittstelle gefahren werden und erfordert beim Endnutzer weder spezielle Kenntnisse noch die Verwaltung von Verbindungsdaten zu Verzeichnisdiensten.

Das Protokoll setzt keine konkrete unterliegende PKI voraus und wurde mit Blick auf XML-Signature [XML-SIG] und XML-Encryption [XML-ENC] entwickelt. Die Spezifikation besteht aus den beiden Teilen XML Key Information Service Specification [X-KISS] und XML Key Registration Service Specification [X-KRSS]. Das OCSP/CRL-Relay implementiert nur X-KISS und bietet dementsprechend auch keine Schnittstelle um z.B. Schlüsselregistrierungen entsprechend X-KRSS durchzuführen.

XKMS soll den Client von der Komplexität der Verarbeitung von XML-Signature <KeyInfo> Elementen befreien. Dies bedeutet aber nicht, dass das OCSP/CRL-Relay nicht z.B. von Mailanwendungen, welche mit PKCS#7-Signaturen auf der Basis von ASN.1 umgehen, eingesetzt werden kann. Solche Anwendungen müssen nur ein entsprechendes <KeyInfo> Element aufbauen.

```
<KeyInfo>
  <X509Data>
    <X509Certificate>
      Aus der PKCS#7-Struktur extrahiertes und Base64-kodiertes Zertifikat
    </X509Certificate>
  </X509Data>
</KeyInfo>
```

Listing 1: <KeyInfo> Element

Im XML-Umfeld kann das existierende Element in der Regel direkt in die XKMS-Nachricht eingestellt werden. Muss eine Anwendung mehr als ein Zertifikat prüfen - z.B. die Zertifikate für Signatur und Verschlüsselung oder weitere Attributzertifikate - können alle Anfragen zur Effizienzsteigerung in einer einzigen XKMS2-Nachricht, einem so genannten *Compound Request*[7], zusammengefasst werden.

Die Kommunikation auf der Grundlage von XKMS folgt einem Request-Response-Schema. Das bedeutet, dass das OCSP/CRL-Relay jede Anfrage mit genau *einer* Nachricht beantwortet. Dies heißt aber nicht, dass diese Antwort bereits zwingend das Ergebnis der Prüfungen beinhaltet. So kann der Server eine Anmeldung mittels des *Two Phase*

[7] http://www.w3.org/TR/xkms2/#XKMS_2_0_LC2_Section_3_4

Request Protocol[8] fordern. In diesem Fall erfolgt zunächst eine Art einfaches Challenge Response Verfahren oder aber die Verarbeitung der Nachricht erfolgt mittels Asynchronous Processing[9]. In diesem Fall reicht der Client die Anfrage beim OCSP/CRL-Relay ein und hat dann die Möglichkeit, die Antwort zu einem späteren Zeitpunkt aktiv abzuholen. Dieses Verfahren wird primär in Verbindung mit der Registrierung von Schlüsseln verwendet, da in diesem Fall unter Umständen erst eine händische Kontrolle der Daten erfolgen muss. Dieser Teil der Spezifikation ist nicht Bestandteil des OCSP/CRL-Relays, daher wird auf die Implementierung dieses Nachrichtentyps verzichtet.

Hervorzuheben ist, dass im Rahmen der Entwicklung des OCSP/CRL-Relays nur die Teile betrachtet werden, die für die Implementierung von X-KISS von Bedeutung sind. *Nicht implementiert* wurden insbesondere die Abschnitte

- Kapitel 6: Key Registration Service Overview[10]
- Kapitel 7: Key Registration Service Message Set[11]
- Kapitel 8: Cryptographic Algorithm Specific Parameters[12]

Von den drei Nachrichtentypen

1. X-KISS-Request,
2. X-KRSS-Request,
3. Compound Request

werden nur die Typen 1 und 3 unterstützt.

XKMS kennt neben dem synchronen Bearbeiten von Anfragen drei besondere Verarbeitungstypen:

1. Asynchronous Processing[13]
2. Two Phase Request Protocol[14]
3. Compound Requests and Responses[15]

Von diesen Nachrichtentypen wird nur *Compound Requests and Responses* unterstützt.

3.1 Eingangs- und Ausgangsattribute

Dieses Kapitel gibt eine Übersicht über die Eingangsparameter und möglichen Rückgabewerte des OCSP/CRL-Relays. Es werden in der tabellarischen Übersicht keine Teilbäume, sondern nur terminale Elemente und relevante Attribute beschrieben. Details sind der Schemadefinition zu entnehmen (siehe Kapitel [10]).

Die Ausprägungen der Spalte „Support" kennzeichnen, in welcher Weise Clients diese Werte zu versorgen (Request) bzw. zu interpretieren (Response) haben.

8 http://www.w3.org/TR/xkms2/#XKMS_2_0_LC2_Section_2_6

9 http://www.w3.org/2002/03/xkms#Asynchronous

10 http://www.w3.org/TR/xkms2/#XKMS_2_0_LC2_Section_6

11 http://www.w3.org/TR/xkms2/#XKMS_2_0_LC2_Section_7

12 http://www.w3.org/TR/xkms2/#XKMS_2_0_LC2_Section_8

13 http://www.w3.org/2002/03/xkms#Asynchronous

14 http://www.w3.org/2002/03/xkms#Represent

15 http://www.w3.org/2002/03/xkms#Compound

3.1.1 Eingangswerte

Wert	Erläuterung	mögliche Werte	Support
X509Certificate	ein oder mehrere Base64-codierte X509-Zertifikate, die zu prüfen sind	Base64-codiertes Zertifikat	MUST
RespondWith	erwartete Rückgabewerte des OCSP/CRL-Relays	X509Cert X509Chain OCSP	OPTIONAL
KeyUsage	Verwendungzweck, für den die Anwendung das Zertifikat benutzen möchte	Encryption Signature Exchange	OPTIONAL
AdvancedKey Usage	Erweiterung des Elements KeyUsage der XKMS-Spezifikation, um die Konformität zu ISIS-MTT sicherzustellen	NonRepudiation crlSign key-CertSign keyAgreement encipherOnly decipherOnly	CONDITIONAL
UseKeyWith	Anwendung, mit der das Zertifikat benutzt werden soll	Protocol XKMS XKMS/ profile S/MIME TLS TLS/https TLS/SMTP IPSEC PKIX	OPTIONAL
OpaqueClient Data	Feld, in dem der Client weitere Informationen übergibt, um Anfragen zu kennzeichnen. Dieses Feld wird vom OCSP/ CRL-Relay unbearbeitet zurückgegeben. Die maximale Länge ist in diesem Profil auf 256 Byte festgelegt.	base64Binary	OPTIONAL
Id	eindeutige Request-ID des Clients	Id	MUST
Response Mechanism	Response-Mechanismus, den der Client für diese Anfrage erwartet	RequestSignatureValue	OPTIONAL
TimeInstant	Zeitpunkt, für den das Zertifikat geprüft werden soll. Dieser Wert muss in der Vergangenheit liegen, ansonsten wird ein Fehler	dateTime	OPTIONAL

	zurückgegeben.		

Tabelle 1: Eingangswerte

3.1.2 Rückgabewerte

Wert	Erläuterung	mögliche Werte	Support
X509Certificate	ein oder mehrere Base64-codierte X509-Zertifikate	Base64-codiertes Zertifikat	MUST
NotOnOrAfter	Datum, ab dem das Zertifikat nicht mehr gültig ist.	DateTime	MUST
NotBefore	Datum, ab dem das Zertifikat gültig ist.	DateTime	MUST
OpaqueClient Data	Feld, in dem der Client weitere Informationen übergibt, um Anfragen zu kennzeichnen. Dieses Feld wird vom OCSP/ CRL-Relay unbearbeitet zurückgegeben. Die maximale Länge ist in diesem Profil auf 256 Byte festgelegt.	base64Binary	OPTIONAL
ResultMajor	Ergebnis des Requests. Dies ist *nicht* das Ergebnis einer Bearbeitung, sondern gibt nur an, *ob* eine Anfrage erfolgreich durchgeführt werden konnte.	Success (erfolgreich beendet) VersionMismatch (Protokoll wird nicht unterstützt) Sender (Fehler auf der Sender-Seite) Receiver (Fehler bei der Verarbeitung)	MUST
ResultMinor	weitere Erläuterungen zu dem Haupt-Ergebnis	NoMatch TooMany Responses Incomplete Failure Refused NoAuthentication MessageNot-Supported Unknown ResponseId NotSynchronous	RECOMMENDED
RequestID	RequestID des Clients	Id	MUST
Request SignatureValue	Wert des <ds:SignatureValue> Elementes in der dazugehörigen Anfrage	base64Binary	OPTIONAL

Wert	Erläuterung	mögliche Werte	Support
KeyUsage	Zulässige Verwendungsarten für das Zertifikat	Encryption Signature Exchange	CONDITIONAL
AdvancedKey Usage	Erweiterung des Elements KeyUsage der XKMS-Spezifikation, um die Konformität zu ISIS-MTT sicherzustellen	NonRepudiation crlSign key-CertSign keyAgreement encipherOnly decipherOnly	CONDITIONAL
UseKeyWith	Anwendungen-Context in dem das Zertifikat verwendet werden soll.	Protocol XKMS XKMS/profile S/MIME TLS TLS/https TLS/ SMTP IPSEC PKIX	CONDITIONAL
ValidReason	Gründe für die Gültigkeit des Zertifikats	IssuerTrust (Zertifikats-Kette bis zu einem Trusted-Anchor erfolgreich hergestellt) RevocationStatus (Prüfung gegen CRL oder OCSP) ValidityInterval (Zertifikat war bereits gültig und noch nicht abgelaufen) Signature (Signatur des Zertifikats wurde erfolgreich geprüft)	CONDITIONAL
InvalidReason	Gründe, warum das Zertifikat ungültig war	IssuerTrust (Zertifikats-Kette bis zu einem Trust-Anchor konnte nicht erfolgreich hergestellt werden) RevocationStatus (Prüfung gegen CRL oder OCSP) ValidityInterval (Zertifikat war noch nicht gültig oder bereits abgelaufen) Signature (Signatur des Zertifikats war falsch)	CONDITIONAL

Wert	Erläuterung	mögliche Werte	Support
Indeterminate Reason	Prüfungen, die nicht durchgeführt werden konnten	IssuerTrust (Zertifikats-Kette bis zu einem Trusted-Anchor konnte aus technischen Gründen nicht erfolgreich hergestellt werden) RevocationStatus (Prüfung gegen CRL oder OCSP war aus technischen Gründen nicht möglich) Signature (Signatur des Zertifikats konnte aus technischen Gründen nicht geprüft werden)	CONDITIONAL
ValidateScheme	Angabe der vorgesehenen Tests bei einer CA. Dies ist NICHT die Angabe, welche Tests erfolgreich durchgeführt wurden.	OCSP CRL CRL_LDAP LDAP LOCAL	MUST
Status	Status des Zertifikats	Valid Indeterminate Invalid	MUST
QcStatements	Reihe von Elementen, die die Verwendung des Zertifikats einschränken.	Folgende Unterelemente sind vorgesehen: QcLimitValue QcCompliance QcRetentionPeriod	CONDITIONAL
QcLimitValue	Beschränkt die monetäre Höhe der Transaktionen, die mit diesem Zertifikat durchführbar sind.		
QcCompliance	Wenn dieses Feld enthalten ist, wurde das Zertifikat in Übereinstimmung mit den EU-Richtlinien ausgestellt, einschliesslich der, in dem Land des Ausstellers, geltenden gesetzlichen Vorschriften.	TRUE / FALSE	
QcRetentionPeriod	Zertifikatsherausgeber halten Informationen über den Zertifikatsinhaber vor. Diese Informationen erlauben es, im Fall eines Rechtsstreits, eine physische Person zu identifizieren. Die Information gibt an, wie lange der Zertifikatsherausgeber die Daten vorhält.	Integer	

Wert	Erläuterung	mögliche Werte	Support
MissingAttribute Certificate	Attributzertifikat wurde nicht mit übergeben		CONDITIONAL
CertQuality	Qualität des Zertifikates	Advanced Qualified Accredited Pki1verwaltung	

Tabelle 2: Rückgabewerte

3.1.3 Beispiel-Request

```
01 <?xml version="1.0" encoding="utf-8"?>
02 <xkms:ValidateRequest
xmlns:xkms="http://www.w3.org/2002/03/xkms#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:bos="http://www.bos-bremen.de/2003/11/bosMsgExt#"
Id="I94d1048aa24259465d7271cb4433dbb4"
Service="http://test.xmltrustcenter.org/XKMS">
03   <xkms:MessageExtension>
04      <bosMsg:VPSData>
05        <bosMsg:VPSRequest>
06          <bosMsg:AdvancedRespondWithSubjectInfo>
bosMsg:SurName
   </bosMsg:AdvancedRespondWithSubjectInfo>
07          <bosMsg:AdvancedRespondWithSubjectInfo>
bosMsg:GivenName
             </bosMsg:AdvancedRespondWithSubjectInfo>
08          <bosMsg:AdvancedRespondWithIssuerInfo>
bosMsg:SurName
   </bosMsg:AdvancedRespondWithIssuerInfo>
09          <bosMsg:AdvancedRespondWithIssuerInfo>
bosMsg:GivenName
   </bosMsg:AdvancedRespondWithIssuerInfo>
10          <bosMsg:AdvancedRespondWithExtensionInfo>
bosMsg:BasicConstraints
   </bosMsg:AdvancedRespondWithExtensionInfo>
11          <bosMsg:AdvancedRespondWithExtensionInfo>
bosMsg:AdvancedKeyUsage
```

```
   </bosMsg:AdvancedRespondWithExtensionInfo>
12         </bosMsg:VPSRequest>
13       </bosMsg:VPSData>
14    </xkms:MessageExtension>
15    <xkms:RespondWith>xkms:X509Chain</xkms:RespondWith>
16      <xkms:QueryKeyBinding>
17        <ds:KeyInfo>
18          <ds:X509Data>
19            <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
20          </ds:X509Data>
21        </ds:KeyInfo>
22        <xkms:KeyUsage>xkms:Signature</xkms:KeyUsage>
23        <xkms:TimeInstant Time="2015-10-09T11:26:29+01:00"/>
24      </xkms:QueryKeyBinding>
25 </xkms:ValidateRequest>
```

Listing 2: Validate-Request

Zeile	Erläuterung
02	Dem OCSP/CRL-Relay wird mitgeteilt, dass es sich um eine Prüfanfrage handelt. Außerdem wird in dem Attribut ein für den Client eindeutiger Identifier übergeben. Dieser Identifier wird vom OCSP/CRL-Relay unbearbeitet zurückgeliefert.
03	Beginn der XKMS-Message-Extension
04	Beginn des VPS-Data-Elementes (Erweiterungen der XKMS-Message-Extension um ISIS-MTT Konformität zu erreichen)
05	Beginn der Anfrage auf der Basis von VPS-Data
06	Antwort soll den Nachnamen des Zertifikatsinhabers enthalten
07	Antwort soll den Vornamen des Zertifikatsinhabers enthalten
08	Antwort soll den Nachnamen des Zertifikatsausstellers enthalten
09	Antwort soll den Vornamen des Zertifikatsausstellers enthalten
10	Anfrage nach der „Basic-Constraints-Extension" des Zertifikats
11	Anfrage nach den erweiterten Key-Usages nach ISIS-MTT
12	Ende der VPS-Data-Erweiterungen
13	Ende des Elementes VPSData
14	Ende der XKMS-Message-Extension
15	Anforderung der kompletten Zertifikatskette in der Anwort
16 – 21	Schlüsselinformationen inkl. des X509-Zertifikats (Base64 codiert)
22	Anfrage nach dem Verwendungszweck des Zertifikats
23	Zeitpunkt, für den die Prüfung stattfinden soll

24-25	Ende der Nachricht

3.1.4 Beispiel-Result

```
01 <xkms:ValidateResult ResultMajor="xkms:Success" Reques-
tId="I94d1048aa24259465d7271cb4433dbb4" Id="Ac0eeg1069687737855Yvu" Service="http://bos-
bremen.certrelay.de/XKMS" xmlns:xkms="http://www.w3.org/2002/03/xkms#">
02  <xkms:MessageExtension>
03   <bosMsg:VPSData xmlns:bos="http://www.bos-bremen.de/2003/11/bosMsgExt#">
04       <bosMsg:VPSResult>
05         <bosMsg:MissingAttributeCertificate/>
06         <bosMsg:SubjectInfo>
07           <bosMsg:SurName>Mustermann</bosMsg:SurName>
08           <bosMsg:GivenName>Emil</bosMsg:GivenName>
09         </bosMsg:SubjectInfo>
10         <bosMsg:IssuerInfo>
11           <bosMsg:SurName>Test</bosMsg:SurName>
12           <bosMsg:GivenName>PKI</bosMsg:GivenName>
13         </bosMsg:IssuerInfo>
14         <bosMsg:ExtensionInfo>
15           <bosMsg:AdvancedKeyUsage Critical="true">
16            <bosMsg:KeyUsageContent>
bosMsg:nonRepudation</bosMsg:KeyUsageContent>
17           </bosMsg:AdvancedKeyUsage>
18           <bosMsg:BasicConstraints Critical="true">
19             <bosMsg:CA>false</bosMsg:CA>
20           </bosMsg:BasicConstraints>
21         </bosMsg:ExtensionInfo>
22         <bosMsg:accredited>false</bosMsg:accredited>
23                 <bosMsg:ValidateScheme>bosMsg:OCSP</bosMsg:ValidateScheme>
24       </bosMsg:VPSResult>
25     </bosMsg:VPSData>
26   </xkms:MessageExtension>
27   <xkms:KeyBinding>
28     <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
29       <ds:X509Data>
30         <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
31         <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
32         <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
```

```
33        </ds:X509Data>
34      </ds:KeyInfo>
35      <xkms:ValidityInterval NotOnOrAfter="2005-10-09T11:26:29+01:00" NotBefore="2002-
10-11T11:26:29+01:00"/>
36      <xkms:Status StatusValue="xkms:Valid">
37        <xkms:ValidReason>xkms:IssuerTrust</xkms:ValidReason>
38        <xkms:ValidReason>xkms:ValidityInterval</xkms:ValidReason>
39                <xkms:ValidReason>xkms:RevocationStatus</xkms:ValidReason>
40                <xkms:ValidReason>xkms:Signature</xkms:ValidReason>
41      </xkms:Status>
42    </xkms:KeyBinding>
43 </xkms:ValidateResult>
```

Listing 3: Validate-Response

Zeile	Erläuterung
01 – 04	Dem Client wird mitgeteilt, dass es sich um eine Prüfantwort handelt. Außerdem wird in dem Attribut ein für das OCSP/CRL-Relay eindeutiger Identifier übergeben. Die RequestId betrifft die Anfrage.
05	Es wird ein Stammzertifikat zur Prüfung übermittelt, zu dem ein Attributzertifikat gehört. Dieses Attributzertifikat wird nicht mitgeliefert.
06 – 13	Informationen über den Zertifikatsinhaber und Aussteller. Diese Informationen wurden in der Anfrage angefordert.
14	Beginn der erweiterten Informationen in diesem Zertifikat
15 – 17	Erweiterte Key-Usage nach ISIS-MTT. Das „Critical"-Attribut, falls vorhanden, schreibt die weitere Auswertung vor.
18 - 20	Zeigt an, ob es sich bei dem Zertifikat um ein Ausstellerzertifikat handelt.
21	Ende der erweiterten Informationen in diesem Zertifikat.
22	Gibt an, ob das Zertifikat konform zum Signaturgesetz ist.
23	Gibt an, dass das Zertifikat gegen einen OCSP-Server geprüft wurde.
24 - 25	Ende der Erweiterungen zu XKMS2.
26 – 27	Beginn der Zertifikats-Informationen nach XKMS2.
28 - 32	Liste der Zertifikate in der Kette. Dabei steht das Userzertifikat immer an erster Stelle. Das jeweils darunter stehende Zertifikat ist das Ausstellerzertifikat.
34	Gültigkeits-Zeitraum für das an erster Stelle stehende Zertifikat.
35	Zertifikat war zum Prüfzeitpunkt gültig.
36 - 39	Gründe für die Gültigkeit des Zertifikats. In diesem Beispiel sind das IssuerTrust (Zertifikatskette konnte bis zu einem Zertifikat gebildet werden, dem das OCSP/CRL-Relay vertraut), ValidityInterval (der Prüfzeitpunkt lag innerhalb des Gültigkeitszeitraums des Zertifikats), Signature (das Zertifikat war korrekt signiert) und RevocationStatus (das Zertifikat war bei einer Prüfung gegen ein Trust-Center nicht gesperrt).
38 – 40	Ende der Result-Nachricht.

3.2 Signaturen

In diesem Abschnitt geht es um eine Protokollierung der XML-Signature[16] für die Payload-Signaturen. Einschränkungen für das Element <ds:Signature>:

- Signaturen müssen Exclusive XML Canonicalization[17] verwenden.
- Signaturen dürfen keine Transformer außer Exclusive XML Canonicalization verwenden.
- Signaturen, welche die Authentizität sicherstellen sollen - also *nicht* die HMAC-Signaturen im Rahmen des Schlüsselmanagements - dürfen nur mittels des Verfahrens SHA1withRSA erzeugt werden. Die minimal akzeptierte Schlüssellänge hängt von der konkreten Konfiguration des OCSP/CRL-Relays ab. Dies ist eine Untermenge der Einschränkungen des OSCI-1.2-Protokolls.

3.3 Element <OpaqueClientData>

Der Client kann in dem Element <OpaqueClientData> beliebige Informationen an den Service senden, die von diesem an den Client zurückgesendet werden *müssen*. Die maximale Größe der in dieses Element eingestellten Daten wird auf 256 Byte begrenzt.

Wichtig! Nach dieser Spezifikation ist es dem Server also nicht freigestellt, *ob* er die Client-Daten zurücksendet. Dafür wird aber die Größe der Daten begrenzt.

3.4 Element <RespondWith>

Mit einer Liste von Elementen dieses Typs legt die anfragende Instanz fest, an welchen Informationen sie interessiert ist. Die jeweilige Information wird durch den Wert des Attributs *type* näher bestimmt. Das OCSP/CRL-Relay unterstützt folgende Attributwerte entsprechend der XKMS2-Spezifikation:

Attributwert	Element nach XML-Sig[18]	Erläuterung
KeyName	<ds:KeyName>	Ein Name, wie z.B. eine E-Mail-Adresse, über den der Schlüssel referenziert werden kann.[19]
X509Cert	<ds:X509Data>	Antwort soll das Element dieses Typs zurückliefern.[20]
X509Chain	<ds:X509Data>*	Die Antwort soll alle Zertifikate der gebildeten Kette in Form von <X509Data> Elementen beinhalten. Wenn gleichzeitig eine Zertifikatskette und das Userzertifikat angefordert werden, dann wird nur die Kette geliefert, an erster Stelle der Kette steht dann das Userzertifikat.[21]
X509CRL	<ds:X509Data>	Die Antwort soll die vollständige CRL in einem <X509Data> Element eingeschlossen zurückliefern.
OCSP	<ds:X509Data>	OCSP-Response soll - wenn eine solche Anfrage gestellt wurde - BASE64-kodiert zurückgegeben

16 http://www.w3.org/TR/xmldsig-core/

17 http://www.w3.org/TR/xml-exc-c14n/

18 Sternchen (*) bedeutet: Element kann mehrfach vorkommen.

19 Ein '>http://www.w3.org/TR/xmldsig-core/#sec-KeyName

20 Die '>http://www.w3.org/TR/xmldsig-core/#sec-X509Data

21 <X509Data>http://www.w3.org/TR/xmldsig-core/#sec-X509Data

Attributwert	Element nach XML-Sig[18]	Erläuterung
		werden.
RetrievalMethod	<ds:RetrievalMethod>	Das Element <ds:RetrievalMethod> soll, wenn verfügbar, in die Antwort eingestellt werden.[22]

Tabelle 3: Mögliche Werte für das Attribut *type*

Nicht unterstützt wird die Rückgabe folgender Elemente der XML-Signature-Spezifikation[23], welche im XKMS2 aufgelistet werden:

- KeyValue - <ds:KeyValue>
- X509CRL
- PGP - <ds:PGPData>
- PGPWeb - <ds:PGPData>*
- SPKI - <ds:SPKIData>*
- PrivateKey - kein entsprechendes Element in XML-Signature vorhanden

3.5 Element <KeyUsage>

Dieses Element beschreibt den Verwendungszweck für das vorliegende Zertifikat. Eine Erweiterung dieses Elements zur Erfüllung der ISIS-MTT-Konformität findet man in dem Unter-Element <AdvancedKeyUsage> unter <VPSData>. Die Erweiterung ist notwendig, da ISIS-MTT den Verwendungszweck von Zertifikaten, insbesondere im Umfeld der Erbringung von Signaturen nach SigG, sehr viel granularer betrachtet.

Inhalt des Elements	Erläuterung
Encryption	Der Schlüssel darf zum Verschlüsseln verwendet werden.
Signature	Der Schlüssel darf zum Signieren verwendet werden.
Exchange	Schlüsselaustausch

Tabelle 4: Mögliche Werte für das Element <KeyUsage>

3.6 Element <UseKeyWith>

Dieses Element beschreibt, mit welchen Anwendungen das Zertifikat verwendet werden kann/darf.

Protocol	Application URI	Identifier	Type
XKMS	http://www.w3.org/2002/03/x kms#	URL identifying SOAP role	URI
XKMS/profile	http://www.w3.org/2002/03/x kms#profile	URL identifying SOAP role	URI
S/MIME	urn:ietf:rfc:2633	SMTP email address of subject	RFC822 addr-spec

22 <ds:RetrievalMethod>http://www.w3.org/TR/xmldsig-core/#sec-RetrievalMethod

23 XML-Signature'>http://www.w3.org/TR/xmldsig-core/

Protocol	Application URI	Identifier	Type
TLS	urn:ietf:rfc:2246	URI identifying certificate subject	URI
TLS/http/s	urn:ietf:rfc:2818	DNS address of http server	DNS Address
TLS/SMTP	urn:ietf:rfc:2487	DNS address of mail server	DNS Address

Tabelle 5: Unterstützte Werte für das Element <UseKeyWith> aus der XKMS-Spezifikation

3.7 Element <RequestSignatureValue>

Das OCSP/CRL-Relay stellt dieses Element in die Antwortnachricht ein, wenn die geschilderten Bedingungen laut Spezifikation erfüllt sind (SHOULD wird an dieser Stelle durch MUST ersetzt).

Das Element enthält das Base64-codierte Feld <ds:SignatureValue> aus der Anfrage. Wenn die Antwort des Relays signiert wird, ist so eine kryptographische Verknüpfung zwischen Anfrage und Antwort möglich.

3.8 Element <VPSData>

Dieses Element erweitert das XKMS2-Protokoll um zusätzliche Elemente, die benötigt werden, um die Konformität des XKMS-VPS-Profils zu ISIS-MTT herzustellen.

3.8.1 Element <VPSRequest>

Hier werden alle Anfragen bezüglich Informationen des Zertifikats gebündelt, die über XKMS hinausgehen. Anfragen können sich auf Informationen über den Zertifikatsinhaber, den Zertifikatsaussteller oder auf im Zertifikat enthaltene Erweiterungen beziehen.

3.8.1.1 Element <AdvancedRespondWithSubjectInfo>

In diesem Element werden die zusätzlichen Informationen über den Zertifikatsinhaber lt. ISIS-MTT aufgenommen. In dem Request werden die Namen der Elemente als Anfrage übergeben. In dem Response werden die Antworten in dem Element <SubjectInfo> eingetragen. Die möglichen Werte sind in der folgenden Tabelle dargestellt:

Element-Name	Erläuterung
CommonName	Vor- und Nachname des Zertifikatsinhabers lt. Zertifikat
SurName	Nachname des Zertifikatsinhabers lt. Zertifikat
GivenName	Vorname des Zertifikatsinhabers lt. Zertifikat
Title	Titel des Zertifikatsinhabers lt. Zertifikat
DistinguishedNameQualifier	Eindeutiger Qualifier zur Unterscheidung ggf. identischer DistinguishedName Einträge
OrganizationName	Fimen-oder Organisationsname lt. Zertifikat
OrganizationalUnitName	Abteilung lt. Zertifikat
BusinessCategory	Geschäftsfeld
StreetAddress	Straßenname des Zertifikatsinhabers lt. Zertifikat
PostalCode	Postleitzahl des Zertifikatsinhabers lt. Zertifikat
LocalityName	Region

Element-Name	Erläuterung
StateOrProvinceName	Bundesland des Zertifikatsinhabers lt. Zertifikat
CountryName	Staat
Initials	Initialen des Zertifikatsinhabers lt. Zertifikat
GenerationQualifier	Namenszusatz (z.B. "jun." oder "sen.")
EmailAddress	E-Mail-Adresse des Zertifikatsinhabers lt. Zertifikat
DomainComponent	Teil eines Domain-Namens
PostalAddress	Adresse des Zertifikatsinhabers lt. Zertifikat
Pseudonym	Pseudonym des Zertifikatsinhabers lt. Zertifikat
DateOfBirth	Geburtsdatum des Zertifikatsinhabers lt. Zertifikat
PlaceOfBirth	Geburtsort des Zertifikatsinhabers lt. Zertifikat
Gender	Geschlecht des Zertifikatsinhabers lt. Zertifikat
CountryOfCitizenship	Staatsangehörigkeit
CountryOfResidence	Aufenthaltsland
NameAtBirth	Geburtsname des Zertifikatsinhabers lt. Zertifikat

Tabelle 6: Einzelelemente von <AdvancedRespondWithSubjectInfo>

3.8.1.2 Element <AdvancedRespondWithIssuerInfo>

In diesem Element werden die zusätzlichen Informationen über den Zertifikatsaussteller lt. ISIS-MTT aufgenommen. In dem Request werden die Namen der Elemente als Anfrage übergeben. In dem Response werden die Antworten in dem Element <IssuerInfo> eingetragen. Die möglichen Werte entsprechen denen in [**Tabelle 6:** Einzelelemente von <AdvancedRespondWithSubjectInfo>].

3.8.1.3 Element <AdvancedRespondWithExtensionInfo>

In diesem Element werden die zusätzlichen Informationen über die Erweiterungen des Zertifikats lt. ISIS-MTT aufgenommen. In dem Request werden die Namen der Elemente als Anfrage übergeben. In dem Response werden die Antworten in dem Element <ExtensionInfo> eingetragen. Die möglichen Werte entprechen den Namen der Erweiterungen, wie unter <ExtensionInfo> beschrieben.

3.8.2 Element <VPSResult>

Dieses Element enthält alle zusätzlichen Informationen zu dem Zertifikat und den Ergebnissen der Gültigkeitsprüfung, die über XKMS hinausgehen.

3.8.2.1 Element <MissingAttributeCertificate>

Dieses Element wird nur dann erzeugt, wenn ein Stammzertifikat zur Prüfung übergeben wurde, das ein dazugehöriges Attributzertifikat besitzt, welches jedoch *nicht* mit übertragen wurde. Dieses Element ist grundsätzlich leer.

3.8.2.2 Element <SubjectInfo>

Dieses Element enthält Informationen über den Inhaber des Zertifikats. Die möglichen Werte entsprechen denen in [**Tabelle 6:** Einzelelemente von <AdvancedRespondWithSubjectInfo>].

3.8.2.3 Element <IssuerInfo>

Dieses Element enthält Informationen über den Aussteller des Zertifikats. Die möglichen Werte entsprechen denen in [**Tabelle 6:** Einzelelemente von <AdvancedRespondWithSubjectInfo>].

3.8.2.4 Element <SerialNumber>

Die Seriennummer des Zertifikats.

3.8.2.5 Element <ExtensionInfo>

Hier werden die Informationen über die Erweiterungen dargestellt. Neben den Erweiterungen die angefragt wurde, werden ALLE kritischen Erweiterungen zurückgegeben. Die übergebenen Erweiterungen sind von folgenden aus ISIS-MTT und ISIS-MTT SigG-Profile übernommen Typen. Alle Elemente haben ein Attribut „critical", welches angibt, ob die Erweiterung ausgewertet werden muss oder nicht.

3.8.2.5.1 Element <AuthorityKeyIdentifier>

Eine ID, die den öffentlichen Schlüssel des Ausstellers identifiziert.

3.8.2.5.2 Element <SubjectKeyIdentifier>

Eine ID, die den öffentlichen Schlüssel des Benutzers identifiziert.

3.8.2.5.3 Element <AdvancedKeyUsage>

Eine Erweiterung des <KeyUsage>-Elements der XKMS2-Spezifikation, um die entsprechenden Werte aus ISIS-MTT zu übernehmen. Hier sind folgende Werte gültig:

Wert	Erläuterung
digitalSignature	Signatur für andere Zwecke außer nonRepudation, keyCertSign, crlSign
nonRepudation	Nichtabstreitbarkeit
keyEncipherment	Verschlüsselung von Sitzungsschlüsseln
dataEncipherment	Verschlüsselung von Daten
keyAgreement	Zertifikat zum Schlüsselaustausch
keyCertSign	Zertifikat zum Signieren von Zertifikaten, nur bei CA Zertifikaten
crlSign	Zertifikat zum Signieren von CRL's
encipherOnly	Wenn dieses Zertifikat für KeyAgreement zugelassen ist, dann ist nur die Verschlüsselung von Daten erlaubt.
decipherOnly	Wenn dieses Zertifikat für KeyAgreement zugelassen ist, dann ist nur die Entschlüsselung von Daten erlaubt.

Tabelle 7: Mögliche Werte für das Element <AdvancedKeyUsage>

3.8.2.5.4 Element <PrivateKeyUsagePeriod>

Ein Gültigkeitszeitraum für den Privaten Schlüssel, der sich von dem Gültigkeitszeitraum des Zertifikats unterscheiden kann.

3.8.2.5.5 Element <CertificatePolicies>

Beschreibt die Policy, nach welcher das Zertifikat ausgestellt wurde und für welchen Zweck es eingesetzt werden soll.

3.8.2.5.6 Element <SubjectAltNames>

Alternativer technischer Name des Zertifikatsinhabers, wie z.B. E-Mail-Adresse, IP-Adresse

3.8.2.5.7 Element <IssuerAltNames>

Alternativer technischer Name des Zertifikatsausstellers, wie z.B. E-Mail-Adresse, IP-Adresse.

3.8.2.5.8 Element <BasicConstraints>

Beschreibt, ob es sich bei diesem Zertifikat um ein CA Zertifikat handelt und legt optional die maximale Länge eines Pfades zu einem Benutzerzertifikat fest.

3.8.2.5.9 Element <NameConstraints>

Spezifiziert einen Namesraum für dieses CA Zertifikat, in dem alle weiteren Zertifikate liegen müssen.

3.8.2.5.10 Element <PolicyConstraints>

Beschreibt Einschränkungen bei der Validierung eines Zertifikatapfades.

3.8.2.5.11 Element <ExtendedKeyUsage>

Weitergehende Nutzungsmöglichkeiten für dieses Zertifikat, die über die in <AdvancedKeyUsage> beschriebenen Möglichkeiten hinausgehen.

3.8.2.5.12 Element <CRLDistributionPoints>

Beschreibt, wie die zugehörige CRL erreicht werden kann.

3.8.2.5.13 Element <AuthorityInfoAccess>

Beschreibt die Möglichkeit zur Online-Validierung und/oder Informationen über die Policy des Ausstellers.

3.8.2.5.14 Element <QcStatements>

Hier wird die rechtliche Grundlage beschrieben, auf der dieses Zertifikat gültig ist.

3.8.2.5.15 Element <OCSPNocheck>

Eine CA gibt an, dass dem Zertifikat des OCSP Responders vertraut werden kann und keine Statusinformation berücksichtigt werden muß.

3.8.2.5.16 Element <accredited>

Gibt an, dass es sich hierbei um ein nach SigG gültiges Zertifikat handelt, das von einer akkreditieren CA ausgestellt wurde. Möglich sind die Werte "true" oder "false".

3.8.2.5.17 Element <SubjectDirectoryAttributes>

Beschreibt weitere DN Attribute des Zertifikatsinhabers zur rechtlichen Identifizierung.

3.8.2.5.18 Element <QcCompliance>

Dieses Zertifikat ist konform zu der ETSI-POL Policy.

3.8.2.5.19 Element <QcLimitValue>

Neue Variante des <MonetaryLimit>. Beschreibung des Grenzwertes; beinhalten einen Wert und eine Währung.

3.8.2.5.20 Element <QcRetentionPeriod>

Zeitangabe, wie lange nach Ablauf de Zertifikats beim Zertifizierungsdiensteanbieter noch Informationen über den Besitzer dieses Zertifikats eingeholt werden können.

3.8.2.5.21 Element <LiabilityLimitationFlag>

Gibt an, dass ein Attributzertifikat existiert, welches die Verwendung des öffentlichen Schlüssels einschränkt.

3.8.2.5.22 Element <Procuration>

In diesem Element wird eine Vertretungsregelung gemäß ISIS-MTT abgebildet. Es enthält folgende Elemente:

- country - Bezeichnung des Landes, dessen Gesetze hier anzuwenden sind
- typeOfSubstitution - Art der Vertretung
- certRef - Referenz auf das Stammzertifikat

Weitere Unter-Elemente gemäß ISIS-MTT werden noch definiert.

3.8.2.5.23 Element <Admission>

Informationen über Berufsbezeichnung/ -zugehörigkeit.

3.8.2.5.24 Element <MonetaryLimit>

Eine Beschreibung über monetäre Beschränkungen. Siehe auch <QcLimitValue>.

3.8.2.5.25 Element <DeclarationOfMajority>

Enthält Informationen über das Alter und die Volljährigkeit des Zertifikatsinhabers.

- notYoungerThen - Zertifikatsinhaber ist nicht jünger als angegeben
- fullAgeAtCountry - Zertifikatsinhaber ist nach geltendem Recht des angegebenen Landes volljährig ("true/false", ISO-Code des Landes)
- dateOfBirth -Geburtsdatum des Zertifikatsinhabers (Format ISO 8601)

3.8.2.5.26 Element <Restriction>

Weitere Beschränkungen in Form eines Textes.

3.8.2.6 Element <CertificateRevocationReason>

Bei gesperrten Zertifikaten wird in diesem Feld der Sperrgrund eingetragen. Mögliche Werte sind hier:

Wert	Erläuterung
unspecified	Ein genauer Sperrgrund wurde nicht angegeben.
keyCompromised	Das Zertifikat wurde kompromittiert.

Wert	Erläuterung
caCompromised	Das Ausstellerzertifikat wurde kompromittiert.
affiliationChanged	Der Name oder eine andere Information des Zertifikatsinhabers hat sich geändert. Das Zertifikat wurde nicht kompromittiert.
superseded	Zertifikat wurde ersetzt. Das Zertifikat wurde nicht kompromittiert.
cessationOfOperation	Zertifikat wird nicht länger benötigt. Das Zertifikat wurde nicht kompromittiert.
certificateHold	Zertifikat wurde temporär zurückgezogen.
removeFromCRL	Zertifikat wurde entsperrt und kann wieder benutzt werden.

Tabelle 8: Mögliche Werte für das Element <CertificateRevocationReason>

3.8.2.7 Element <ValidateScheme>

Nimmt die möglichen Werte auf, nach denen bei einer bestimmten CA geprüft wird. Hier werden die Soll-Prüfungen und nicht die tatsächlich durchgeführten Prüfungen beschrieben.

Wert	Erläuterung
CRL	Prüfung gegen eine CRL (Negativ-Prüfung)
CRL_LDAP	Prüfung gegen eine CRL und anschließend gegen einen LDAP-Server (Positiv- und Negativ- Prüfung)
LDAP	Prüfung gegen einen LDAP-Server (Positiv-Prüfung)
OCSP	Prüfung gegen einen OCSP-Server

Tabelle 9: Mögliche Werte für das Element <ValidateScheme>

3.8.2.8 Element <ErrorExtension>

Dieses Element erweitert die Fehlermeldungen aus XKMS2. Die Fehlermeldungen werden dabei in einem Attribut mit dem Namen *reason* vom Typ String übermittelt. Folgende Einträge sind hier möglich:

Fehlermeldung	Erläuterung	ResultMajor	ResultMinor
MissingParentCertificate	Attributzertifikat wurde übergeben, das dazugehörige Hauptzertifikat fehlt jedoch.	Sender	Failure
OpaqueClientDataToLong	Die Länge des Elements Opaque-<ClientData> übersteigt die zulässigen 256 Byte.	Sender	Failure
TrustCenterNotReachable	Es ist zu einer technischen Störung gekommen, die verhindert, dass ein Zertifikat gegen das Trust-Center geprüft werden kann.	Receiver	Failure
WrongCertificateFormat	Das übergebene Zertifikat hat eine falsche Codierung oder ist auf andere Art defekt.	Sender	Failure
UnknownCA	Der Aussteller des Zertifikats ist dem OCSP/CRL-Relay nicht bekannt.	Success	Incomplete

Fehlermeldung	Erläuterung	ResultMajor	ResultMinor
WrongTimeInstant	Das Format des angegebenen Prüfzeitpunkts ist unbekannt oder dieser liegt in der Zukunft.	Sender	Failure
SignatureKeyToShort	Die Schlüssellänge des Signaturzertifikats war zu kurz.	Sender	Failure
AttributeCertificateDontMatch	Ein Attribut-Zertifikat wurde übergeben, das nicht zum Stamm-Zertifikat passt.	Sender	Failure

Tabelle 10: Mögliche Werte für das Element <errorExtension>

3.8.2.9 Element <CertQuality>

Mit diesem Element wird ein Rating abgebildet, welches Auskunft gibt über die Qualität der CA. Ist die PKI1-Verwaltung Herausgeber des Zertifikats, wird dies hier eingetragen; für andere CAs wird vermerkt, ob es sich um ein forgeschrittenes oder qualifiertes Zertifikat handelt bzw. einen Herausgeber mit Anbieterakkreditierung.

Wert	Erläuterzung
advanced	Fortgeschrittenes Zertifikat
Qualified	Zertifikat einer qualifizierten CA
Accredited	Zertifikat einer akkreditierten CA
PKI1-Verwaltung	Zertifikat der PKI1-Verwaltung

Tabelle 11: Qualität des geprüften Zertifikats

4 Zertifikate validieren

Sollen mehrere Zertifikate geprüft werden, können diese Anfragen in einer einzigen XKMS2-Nachricht vom Typ *CompoundRequest* zusammengefasst werden. Da das OCSP/CRL-Relay keine asynchrone Verarbeitung von Nachrichten unterstützt, beinhaltet die Antwort auf einen solchen Request immer die Antworten zu allen Einzelanfragen.

```
<?xml version="1.0" encoding="utf-8"?>

<xkms:CompoundRequest xmlns:xkms="http://www.w3.org/2002/03/xkms#"

         xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

         xmlns:xenc=http://www.w3.org/2001/04/xmlenc#

         Id="Ie383fac377f1e54d2b26596c072b8b7a"

         Service="http://test.xmltrustcenter.org/XKMS"

         xmlns="http://www.w3.org/2002/03/xkms#">

  <xkms:ValidateRequest xmlns:xkms="http://www.w3.org/2002/03/xkms#"

xmlns:ds=http://www.w3.org/2000/09/xmldsig#
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

xmlns:bosMsg="http://www.bos-bremen.de/2003/11/bosMsgExt#"

Id="I94d1048aa24259465d7271cb4433dbb4" Service="http://test.xmltrustcenter.org/XKMS">

    <xkms:MessageExtension>

      <bosMsg:VPSData>

         <bosMsg:VPSRequest>

           <bosMsg:MissingAttributeCertificate/>

             <bosMsg:AdvancedRespondWithSubjectInfo>

bosMsg:SurName

   </bosMsg:AdvancedRespondWithSubjectInfo>

             <bosMsg:AdvancedRespondWithSubjectInfo>

bosMsg:GivenName

   </bosMsg:AdvancedRespondWithSubjectInfo>

             <bosMsg:AdvancedRespondWithIssuerInfo>

bosMsg:SurName

   </bosMsg:AdvancedRespondWithIssuerInfo>

                    <bosMsg:AdvancedRespondWithIssuerInfo>

bosMsg:GivenName

   </bosMsg:AdvancedRespondWithIssuerInfo>

             <bosMsg:AdvancedRespondWithExtensionInfo>

bosMsg:BasicConstraints

   </bosMsg:AdvancedRespondWithExtensionInfo>
```

```
            <bosMsg:AdvancedRespondWithExtensionInfo>
bosMsg:AdvancedKeyUsage
    </bosMsg:AdvancedRespondWithExtensionInfo>
         </bosMsg:VPSRequest>
      </bosMsg:VPSData>
    </xkms:MessageExtension>
    <xkms:RespondWith>xkms:X509Cert</xkms:RespondWith>
    <xkms:QueryKeyBinding>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>Base64 codiertes Zertifikat
            </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
      <xkms:KeyUsage>xkms:Signature</xkms:KeyUsage>
      <xkms:TimeInstant Time="2000-10-09T11:26:29+01:00"/>
    </xkms:QueryKeyBinding>
   </xkms:ValidateRequest>
  <xkms:ValidateRequest xmlns:xkms="http://www.w3.org/2002/03/xkms#"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:bosMsg="http://www.bos-bremen.de/2003/11/bosMsgExt#"
Id="I94d1048aa24259465d7271cbccscsb5" Service="http://test.xmltrustcenter.org/XKMS">
    <xkms:MessageExtension>
     <bosMsg:VPSData>
       <bosMsg:VPSRequest>
            <bosMsg:MissingAttributeCertificate/>
              <bosMsg:AdvancedRespondWithSubjectInfo>
bosMsg:SurName
   </bosMsg:AdvancedRespondWithSubjectInfo>
              <bosMsg:AdvancedRespondWithSubjectInfo>
bosMsg:GivenName
   </bosMsg:AdvancedRespondWithSubjectInfo>
              <bosMsg:AdvancedRespondWithIssuerInfo>
bosMsg:SurName
   </bosMsg:AdvancedRespondWithIssuerInfo>
              <bosMsg:AdvancedRespondWithIssuerInfo>
```

```
bosMsg:GivenName

   </bosMsg:AdvancedRespondWithIssuerInfo>

            <bosMsg:AdvancedRespondWithExtensionInfo>

bosMsg:BasicConstraints

   </bosMsg:AdvancedRespondWithExtensionInfo>

            <bosMsg:AdvancedRespondWithExtensionInfo>

bosMsg:AdvancedKeyUsage

   </bosMsg:AdvancedRespondWithExtensionInfo>

</bosMsg:VPSRequest>

      </bosMsg:VPSData>

  </xkms:MessageExtension>

  <xkms:RespondWith>xkms:X509Cert</xkms:RespondWith>

  <xkms:QueryKeyBinding>

    <ds:KeyInfo>

      <ds:X509Data>

          <ds:X509Certificate>Base64 codiertes Zertifikat </ds:X509Certificate>

      </ds:X509Data>

    </ds:KeyInfo>

    <xkms:KeyUsage>xkms:Signature</xkms:KeyUsage>

    <xkms:TimeInstant Time="2003-10-09T11:26:29+01:00"/>

  </xkms:QueryKeyBinding>

 </xkms:ValidateRequest>

</xkms:CompoundRequest>
```

Listing 4: CompoundRequest

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

  <xkms:CompoundResult ResultMajor="xkms:Success"

                       RequestId="Ie383fac377f1e54d2b26596c072b8b7a"

                       Id="ifUzlc10697624810706tR"

                       Service="http://bos-bremen.certrelay.de/XKMS"

                       xmlns:xkms="http://www.w3.org/2002/03/xkms#">

         <xkms:ValidateResult ResultMajor="xkms:Success"

                         RequestId="I94d1048aa24259465d7271cb4433dbb4"

                         Id="dQHoCL1069762481070C08"

                         Service="http://bos-bremen.certrelay.de/XKMS">

      <xkms:MessageExtension>

        <bosMsg:VPSData xmlns:bosMsg="http://www.bos-bremen.de/2003/11/bosMsgExt#">
```

```
        <bosMsg:VPSResult>
          <bosMsg:MissingAttributeCertificate/>
          <bosMsg:SubjectInfo>
            <bosMsg:SurName>null</bosMsg:SurName>
            <bosMsg:GivenName>null</bosMsg:GivenName>
          </bosMsg:SubjectInfo>
          <bosMsg:IssuerInfo>
            <bosMsg:SurName>null</bosMsg:SurName>
            <bosMsg:GivenName>null</bosMsg:GivenName>
          </bosMsg:IssuerInfo>
          <bosMsg:ExtensionInfo>
            <bosMsg:AdvancedKeyUsage Critical="true">
              <bosMsg:KeyUsageContent> nonRepudation</bosMsg:KeyUsageContent>
            </bosMsg:AdvancedKeyUsage>
            <bosMsg:BasicConstraints Critical="true">
              <bosMsg:CA>false</bosMsg:CA>
            </bosMsg:BasicConstraints>
          </bosMsg:ExtensionInfo>
          <bosMsg:accredited>false</bosMsg:accredited >
        </bosMsg:VPSResult>
      </bosMsg:VPSData>
    </xkms:MessageExtension>
  <xkms:KeyBinding>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
    <xkms:ValidityInterval NotOnOrAfter="2005-10-09T11:26:29+01:00"
       NotBefore="2002-10-11T11:26:29+01:00"/>
    <xkms:Status StatusValue="xkms:Valid">
      <xkms:ValidReason>xkms:IssuerTrust</xkms:ValidReason>
      <xkms:ValidReason>xkms:ValidityInterval</xkms:ValidReason>
       <xkms:ValidReason>xkms:Signature</xkms:ValidReason>
       <xkms:ValidReason>xkms:RevocationStatus</xkms:ValidReason>
    </xkms:Status>
  </xkms:KeyBinding>
</xkms:ValidateResult>
```

```
<xkms:ValidateResult ResultMajor="xkms:Success"
                     RequestId="I94d1048aa24259465d7271cbccscsb4"
                      Id="SoUkqH1069762481070nPa"
                     Service="http://bos-bremen.certrelay.de/XKMS">
  <xkms:MessageExtension>
    <bosMsg:VPSData xmlns:bos="http://www.bos-bremen.de/2003/11/bosMsgExt##">
      <bosMsg:VPSResult>
        <bosMsg:MsgMissingAttributeCertificate/>
        <bosMsg:SubjectInfo>
          <bosMsg:SurName>null</bosMsg:SurName>
          <bosMsg:GivenName>null</bosMsg:GivenName>
        </bosMsg:SubjectInfo>
        <bosMsg:IssuerInfo>
          <bosMsg:SurName>null</bosMsg:SurName>
          <bosMsg:GivenName>null</bosMsg:GivenName>
        </bosMsg:IssuerInfo>
        <bosMsg:ExtensionInfo>
          <bosMsg:AdvancedKeyUsage Critical="true">
            <bosMsg:KeyUsageContent>nonRepudation</bosMsg:KeyUsageContent>
          </bosMsg:AdvancedKeyUsage>
          <bosMsg:BasicConstraints Critical="true">
            <bosMsg:CA>false</bosMsg:CA>
          </bosMsg:BasicConstraints>
        </bosMsg:ExtensionInfo>
        <bosMsg:accredited >false</bosMsg:accredited>
      </bosMsg:VPSResult>
    </bosMsg:VPSData>
  </xkms:MessageExtension>
  <xkms:KeyBinding>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
        <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
        <ds:X509Certificate>Base64 codiertes Zertifikat</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
    <xkms:ValidityInterval NotOnOrAfter="2005-10-09T11:26:29+01:00"
       NotBefore="2002-10-11T11:26:29+01:00"/>
```

```
      <xkms:Status StatusValue="xkms:Invalid">

        <xkms:ValidReason>xkms:IssuerTrust</xkms:ValidReason>

<xkms:ValidReason>xkms:Signature</xkms:ValidReason>

         <xkms:ValidReason>xkms:RevocationStatus</xkms:ValidReason>

        <xkms:InvalidReason>xkms:ValidityInterval</xkms:InvalidReason>

      </xkms:Status>

    </xkms:KeyBinding>

  </xkms:ValidateResult>

</xkms:CompoundResult>
```

Listing 5: CompoundResult

Die Antworten des OCSP/CRL-Relays werden mit einer XML-Signatur versehen. Hierbei werden die Algorithmen *SHA1* und *RSA* verwendet.

5 XKMS2 SOAP Message Binding

In diesem Abschnitt wird auf das Dokument *http://www.w3.org/TR/2003/WD-xkms2-bindings-20030418/* Bezug genommen. XKMS2 als solches kann über beliebige Protokolle transportiert werden. Jeder XKMS2-Service sollte mindestens die Kommunikation mittels SOAP unterstützen. Das verwendete Transportprotokoll hat entscheidenden Einfluss auf die Sicherheitsmechanismen. Hierbei geht es sowohl um die Unversehrtheit der Nachricht und die Identifikation der Kommunikationspartner als auch die Verschlüsselung der übermittelten Daten. Diese Mechanismen können entweder auf der Ebene des Payloads, also im Rahmen der XKMS2-Nachrichten sichergestellt werden oder über das verwendete Transportprotokoll.

Werden die Mechanismen im Rahmen des XKMS2-Protokolls verwendet, so spricht man von der Payload-Schicht. Hier werden zwei Verfahren unterschieden:

1. Identifier: http://www.w3.org/2002/03/xkms#payload-I - Keine Authentifikation
2. Identifier: http://www.w3.org/2002/03/xkms#payload-II - Authentifikation mittels Signatur

Darüber hinaus können die Anfragen entsprechend XML-Encryption verschlüsselt werden.

Auf der Ebene des Transports stehen die Mechanismen Secure Socket Layer and Transaction Layer (SSL/TLS) zur Auswahl (siehe XKMS2-bindings-20030418). Da diese für das OCSP/CRL-Relay transparent realisiert werden, soll an dieser Stelle auf diese Verfahren nicht weiter eingegangen werden.

Es werden folgende Protokolle unterstützt:

- *SOAP 1.2 über http:*
  Der Aufbau der Nachrichten wird in *http://www.w3.org/TR/2003/WD-xkms2-bindings-20030418/#__Section_3* beschrieben. Dieses Binding kann in Verbindung mit der Payload Authentification verwendet werden.
- *SOAP 1.2 über http/s:*
  Der Aufbau der Nachrichten wird in *http://www.w3.org/TR/2003/WD-xkms2-bindings-20030418/#__Section_3* beschrieben. Dieses Binding kann in Verbindung mit der Payload Authentification (XMKS-Elemet Request/Signature) verwendet werden.
- *JMS 1.1:*
  In diesem Fall werden die XKMS-Nachrichten nicht in einen weiteren SOAP-Umschlag verpackt. Auch bei diesem Übermittlungsverfahren können die Payload-Authentification oder die Mechanismen der JMS-Implementierung verwendet werden.

Wie die Mechanismen auf der Ebene des Transports im Detail aussehen, hängt von der Implementierung der verwendeten Schnittstellenspezifikation ab.

6 Zugriff auf das OCSP/CRL-Relay via http(s)

Die XKMS2-Anfragen müssen das SOAP-Binding[24] verwenden und können dann mittels http oder https POST an das OCSP/CRL-Relay übermittelt werden.

Die maximale Größe einer Anfrage kann als SOAP-Header übermittelt werden. Die XKMS-Nachrichten müssen entsprechend PARTII[25] der Spezifikation in einen SOAP-1.2-Umschlag verpackt werden.

```
<?xml version="1.0"?>

<env:Envelope xmlns:env="http://www.w3.org/2002/06/soap-envelope">

  <env:Body>

<?xml version="1.0" encoding="utf-8"?>

 <xkms:ValidateRequest

xmlns:xkms="http://www.w3.org/2002/03/xkms#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

         xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

         xmlns:bos="www.bos-bremen.de/2003/11/bosMsgExt#"

         Id="I94d1048aa24259465d7271cb4433dbb4"

         Service="http://test.xmltrustcenter.org/XKMS">

         .

         .

         .

</xkms:ValidateRequest>

  </env:Body>

</env:Envelope>
```

Listing 6: SoapKeyBinding Request

Das Ergebnis hat folgenden Aufbau:

```
<?xml version="1.0"?>

<env:Envelope xmlns:env="http://www.w3.org/2002/06/soap-envelope">

  <env:Body>

 <xkms:ValidateResult ResultMajor="xkms:Success" Reques-
tId="I94d1048aa24259465d7271cb4433dbb4" Id="Ac0eeg1069687737855Yvu" Service="http://bos-
bremen.certrelay.de/XKMS" xmlns:xkms="http://www.w3.org/2002/03/xkms#">

         .

         .
```

[24] http://www.w3.org/TR/xkms2-bindings/

[25] http://www.w3.org/TR/xkms2-bindings/

```
          .
</xkms:ValidateResult>
  </env:Body>
</env:Envelope>
```

Listing 7: SoapKeyBinding Response

Clients dürfen mehrere Anfragen in einem CompoundRequest zusammenfassen.

7 Zugriff auf das OCSP/CRL-Relay via JMS

Dieses Kapitel beschreibt den Zugriff auf das OCSP/CRL-Relay mittel JMS. Funktional ist die Anbindung über JMS identisch zu http und https.

7.1 Die Kommunikation über JMS 1.1

Das OCSP/CRL-Relay verwendet für die Kommunikation mit den Clients das Point-To-Point-Verfahren (PTP). Clients sollten die JMS Common Interfaces verwenden. Die Kommunikation erfolgt in der Form Request/Reply und bedient sich dazu der Informationen im *JMSReplyTo*-Nachrichten-Header. Der Einstiegspunkt des OCSP/CRL-Relays wird als Message-driven Bean entsprechend der EJB-2.0-Spezifikation realisiert.

- Die Nachrichten werden über die Queue *xkms2certrelay* entgegengenommen.
- Die Nachrichten müssen als *BytesMessage* oder *TextMessage* übermittelt werden.
- Es werden keine *transacted Messages* verwendet.
- Das OCSP/CRL-Relay informiert die aufrufende Anwendung nicht mittels *ExceptionListener* über aufgetretene Fehler. Solange das OCSP/CRL-Relay in der Lage ist, eine Anfrage zu bearbeiten, ist die Antwort immer eine XKMS2-Nachricht.
- Die Authentifikation erfolgt je nach Instanz des OCSP/CRL-Relays mittels *Payload Authentication* oder auf Grundlage der Mechanismen des verwendeten Protokolls.

JMS-Typen

- relayvalidate
- relaylocate
- relaycompound

7.2 Reaktionen im Fehlerfall

Das OCSP/CRL-Relay beantwortet alle Anfragen mit einer entsprechenden XKMS2-Nachricht. Können bestimmte Aktionen, wie z.B. die Onlineprüfung eines Zertifikats, nicht durchgeführt werden, wird eine entsprechende Nachricht auf der Ebene von XKMS2 an den Client zurückgegeben.

Wann welcher Fehlercode zurückgeliefert wird, kann der XKMS2-Spezifikation entnommen werden.

8 Begrenzung der maximalen Nachrichtengröße

Die XKMS2-Spezifikation trifft keine Aussage über die maximale Größe einer Nachricht. Diese Tatsache stellt für das OCSP/CRL-Relay eine potenzielle Gefährdung dar. Aus den nachfolgend genannten drei Gründen kann es z.B. zu unbegrenzt großen Nachrichten kommen:

- Beliebig große Zeichenfolgen können in das Element <OpaqueClientData> eingestellt werden,
- es können unbegrenzt viele Zertifikate in einem Request gesendet werden,
- im Rahmen eines Compound Requests können beliebig große Nachrichten erzeugt werden.

Das OCSP/CRL-Relay wird daher nur Nachrichten bis zu einer frei konfigurierbaren maximalen Größe annehmen. Wie diese maximale Nachrichtengröße dem Client bekannt gegeben wird, ist in XKMS2 nicht definiert und muss daher auf einer anderen Ebene gelöst werden. Normalerweise wird ein SOAP-Fault generiert:

Code: „env:Sender"; Value: „xkms:BadMesage"

Die Daten im Element <OpaqueClientData> dürfen eine Größe von 256 Byte nicht überschreiten.

9 XKMS2-Conformance des OCSP/CRL-Relays

In diesem Abschnitt erfolgt eine Zuordnung der Conformance-Anforderungen aus Kapitel 9 der XKMS2-Spezifikation.[26]

Feature	Operations	Requirement Level	Comments	
Operations Support	Locate	RECOMMENDED	Services SHOULD support retrieval of their own credential by means of the Locate operation with the XKMS protocol URI.	
	All	One Operation REQUIRED	A conforming XKMS service MUST support at least one XKMS operation, that is there MUST be at least one possible input that results in the result Success.	
	Compound	OPTIONAL	See note for Status operation support.	
	Status	RECOMMENDED	Services SHOULD support status operations if asynchronous processing and compound requests are also supported.	nicht unterstützt
Operation Response	All	REQUIRED	A conforming XKMS service MUST accept any valid XKMS request sent to it and be capable of responding to the request with a correctly formatted XKMS result. If a service does not support an operation it MUST respond to all requests for a particular operation with the result Sender.MessageNotSupported	
Response Mechanisms				
Synchronous Response	All	REQUIRED	A conforming XKMS service MUST be capable of returning an immediate response to any XKMS request.	

[26] siehe http://www.w3.org/TR/2003/WD-xkms2-20030418/#XKMS_2_0_LC2_Section_9

Feature	Operations	Requirement Level	Comments	
Asynchronous Response	Register, Reissue, Recover	RECOMMENDED	Processing of certain XKRSS operations may require manual intervention by an operator in certain circumstances. It is therefore recommended that clients support the use of asynchronous processing with these operations unless it is known that all requests will be serviced immediately.	nicht unterstützt
	Compound	RECOMMENDED	Services that support Compound Operations SHOULD support compound requests	
	Locate, Validate, Revoke	OPTIONAL	Services MAY support Asynchronous Responses be supported on these operations.	nicht unterstützt
	Pending, Status	PROHIBITED	A client MAY offer asynchronous processing of Pending and Status operations however a service MUST NOT return a pending response.	nicht unterstützt
Two-Phase Request	All	RECOMMENDED	Clients SHOULD support use of the two phase request protocol. The additional complexity of implementing the two phase protocol is not high and allows a service to provide a response even in cases where it is under a denial of service attack.	Der Server muss keine Anfragen ohne T-PR akzep tieren
Protocol Encapsulation				
http Transport	All	REQUIRED	Services MUST support the use of http transport	
SOAP 1.1 Transport	All	REQUIRED	Services MUST support the use of SOAP 1.1 encapsulation	nicht unterstützt
SOAP 1.2 Transport	All	RECOMMENDED	Services SHOULD support the use of SOAP 1.2 encapsulation	
Security Enhancements				
No Security	Locate	REQUIRED		Rel. 2.0
	[Others]	RECOMMENDED		Nicht unterstützt
Payload Authentication I	All	RECOMMENDED		unterstützt
Payload Authentication II	All	RECOMMENDED		Rel. 2.0

Feature	Operations	Requirement Level	Comments	
TLS Binding I	All	RECOMMENDED		unterstützt
TLS Binding II	All	RECOMMENDED		nicht unterstützt
TLS Binding III	All	RECOMMENDED		Rel. 2.0
Exclusive Canonicalization	All	REQUIRED	If XML Signature is used, Exclusive Canonicalization MUST be supported.	Rel. 2.0

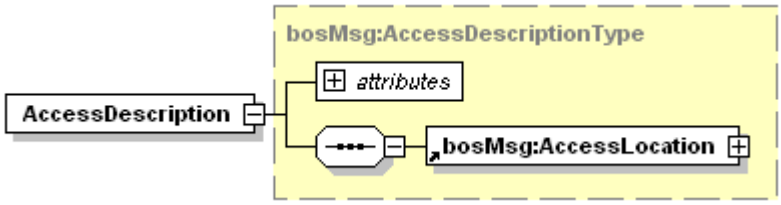
Tabelle 12: XKMS-Conformance des OCSP/CRL-Relays

10 XKMS2 Schema und Erweiterungen

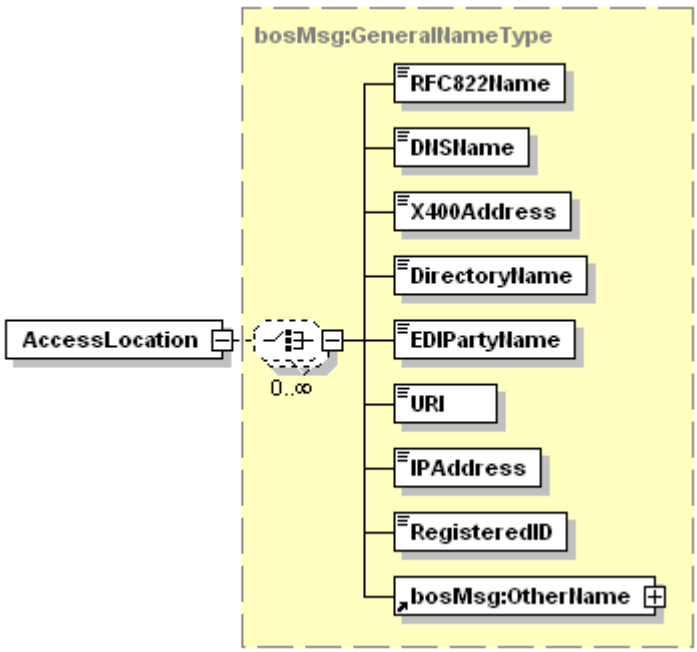
Schema xkms-bos

10.1 Elements

10.1.1 element AccessDescription

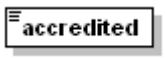
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:AccessDescriptionType**
Properties	content complex
Children	**bosMsg:AccessLocation**
used by	complexType **AuthorityInfoAccessType**
Attributes	Name Type Use Default Fixed Annotation AccessMethod **xs:string**
Source	<xs:element name="AccessDescription" type="bosMsg:AccessDescriptionType"/>

10.1.2 element AccessLocation

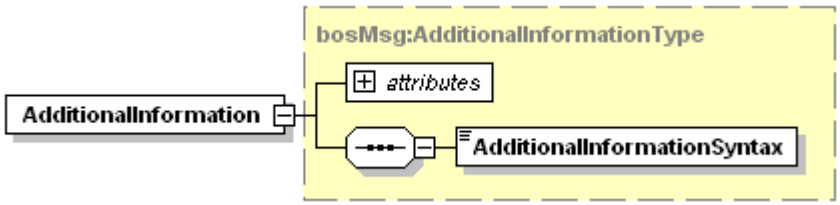
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:GeneralNameType**

Properties	content complex
children	**RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName**
used by	complexType **AccessDescriptionType**
source	<xs:element name="AccessLocation" type="bosMsg:GeneralNameType"/>

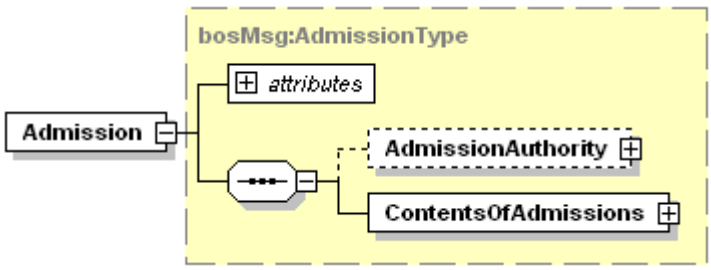
10.1.3 element accredited

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:boolean**
properties	content simple
used by	complexType **VPSResultType**
source	<xs:element name="accredited" type="xs:boolean"/>

10.1.4 element AdditionalInformation

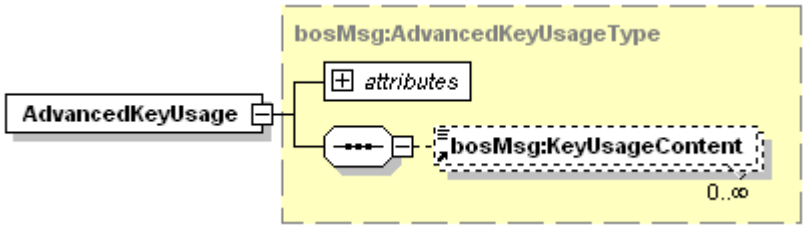
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:AdditionalInformationType**
properties	content complex
children	**AdditionalInformationSyntax**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:element name="AdditionalInformation" type="bosMsg:AdditionalInformationType"/>

10.1.5 element Admission

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:AdmissionType**
Properties	content complex

Children	**AdmissionAuthority ContentsOfAdmissions**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:element name="Admission" type="bosMsg:AdmissionType"/>

10.1.6 element AdvancedKeyUsage

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:AdvancedKeyUsageType**
properties	content complex
children	**bosMsg:KeyUsageContent**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:element name="AdvancedKeyUsage" type="bosMsg:AdvancedKeyUsageType"/>

10.1.7 element AdvancedRespondWithExtensionInfo

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:AdvancedRespondWithExtensionType**
Properties	content simple
used by	complexType **VPSRequestType**
Facets	enumeration bosMsg:BasicConstraints enumeration bosMsg:AdvancedKeyUsage enumeration bosMsg:AuthorityKeyIdentifier enumeration bosMsg:SubjectKeyIdentifier enumeration bosMsg:PrivateKeyUsagePeriod enumeration bosMsg:CertificatePolicies enumeration bosMsg:SubjectAltNames enumeration bosMsg:IssuerAltNames enumeration bosMsg:SubjectDirectoryAttributes enumeration bosMsg:CRLDistributionPoints enumeration bosMsg:AuthorityInfoAccess enumeration bosMsg:OCSPNocheck
Source	<xs:element name="AdvancedRespondWithExtensionInfo" type="bosMsg:AdvancedRespondWithExtensionType"/>

10.1.8 element AdvancedRespondWithIssuerInfo

Diagram	

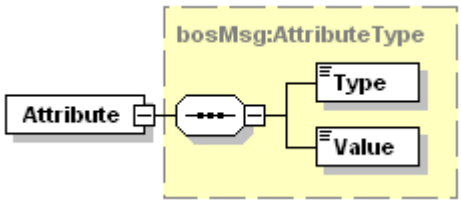
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:AdvancedRespondWithNameType**
Properties	content simple
used by	complexType **VPSRequestType**
Facets	enumeration bosMsg:SurName enumeration bosMsg:GivenName enumeration bosMsg:SerialNumber enumeration bosMsg:Title enumeration bosMsg:OrganizationName enumeration bosMsg:OrganizationalUnitName enumeration bosMsg:BusinessCategory enumeration bosMsg:StreetAddress enumeration bosMsg:PostalCode enumeration bosMsg:LocalityName enumeration bosMsg:StateOrProvinceName enumeration bosMsg:CountryName enumeration bosMsg:Initials enumeration bosMsg:GenerationQualifier enumeration bosMsg:EmailAddress enumeration bosMsg:DomainComponent enumeration bosMsg:PostalAddress enumeration bosMsg:Pseudonym enumeration bosMsg:DateOfBirth enumeration bosMsg:PlaceOfBirth enumeration bosMsg:Gender enumeration bosMsg:CountryOfCitizenship enumeration bosMsg:CountryOfResidence enumeration bosMsg:NameAtBirth enumeration bosMsg:CommonName enumeration bosMsg:DistinguishedNameQualifier
Source	<xs:element name="AdvancedRespondWithIssuerInfo" type="bosMsg:AdvancedRespondWithNameType"/>

10.1.9 element AdvancedRespondWithSubjectInfo

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:AdvancedRespondWithNameType**
Properties	content simple
used by	complexType **VPSRequestType**
Facets	enumeration bosMsg:SurName enumeration bosMsg:GivenName enumeration bosMsg:SerialNumber enumeration bosMsg:Title enumeration bosMsg:OrganizationName enumeration bosMsg:OrganizationalUnitName enumeration bosMsg:BusinessCategory enumeration bosMsg:StreetAddress enumeration bosMsg:PostalCode enumeration bosMsg:LocalityName enumeration bosMsg:StateOrProvinceName enumeration bosMsg:CountryName enumeration bosMsg:Initials enumeration bosMsg:GenerationQualifier enumeration bosMsg:EmailAddress enumeration bosMsg:DomainComponent enumeration bosMsg:PostalAddress enumeration bosMsg:Pseudonym enumeration bosMsg:DateOfBirth enumeration bosMsg:PlaceOfBirth enumeration bosMsg:Gender enumeration bosMsg:CountryOfCitizenship enumeration bosMsg:CountryOfResidence

	enumeration bosMsg:NameAtBirth enumeration bosMsg:CommonName enumeration bosMsg:DistinguishedNameQualifier
Source	<xs:element name="AdvancedRespondWithSubjectInfo" type="bosMsg:AdvancedRespondWithNameType"/>

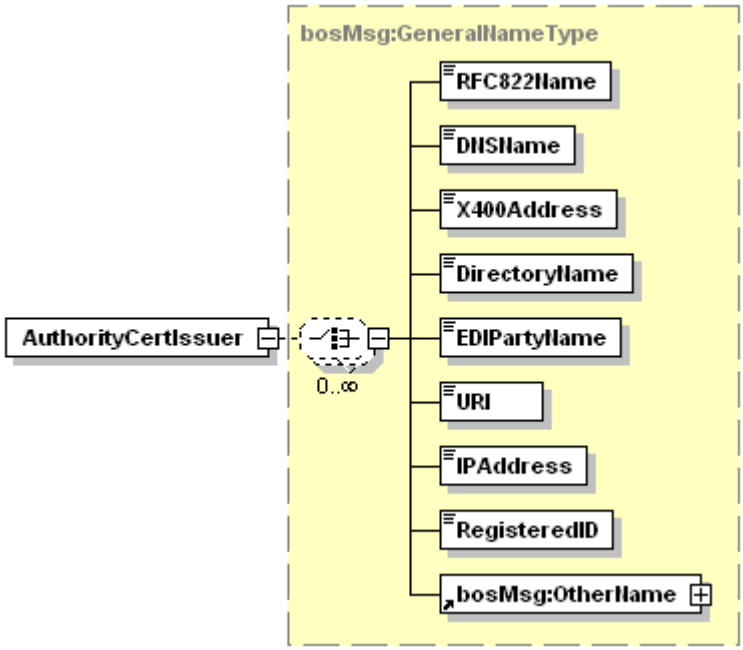
10.1.10 element Attribute

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:AttributeType**
Properties	content complex
Children	**Type Value**
used by	complexType **SubjectDirectoryAttributesType**
Source	<xs:element name="Attribute" type="bosMsg:AttributeType"/>

10.1.11 element Attributes

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
Source	<xs:element name="Attributes" type="xs:string"/>

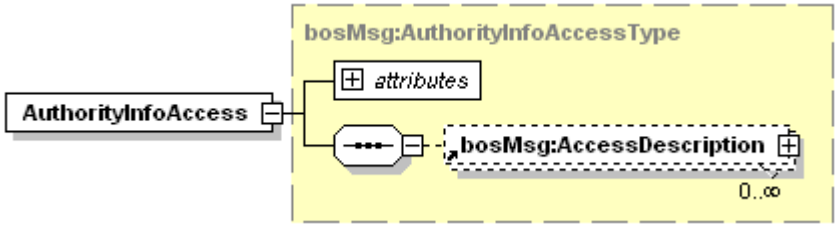
10.1.12 element AuthorityCertIssuer

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralNameType**
properties	content complex
children	**RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName**
used by	complexType **AuthorityKeyIdentifierType**
source	<xs:element name="AuthorityCertIssuer" type="bosMsg:GeneralNameType"/>

10.1.13 element AuthorityCertSerialNumber

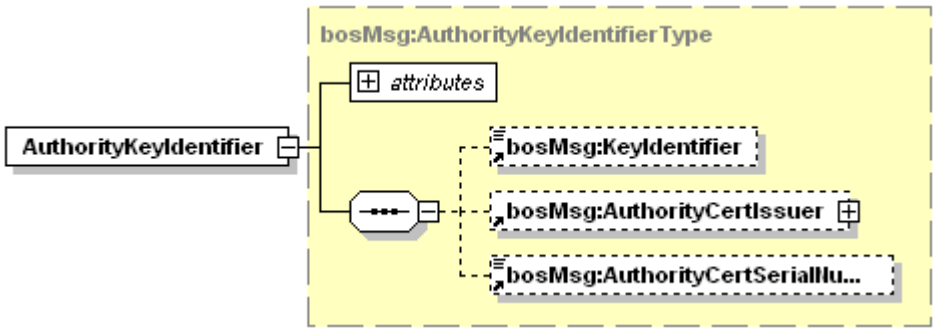
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	content simple
used by	complexType **AuthorityKeyIdentifierType**
source	<xs:element name="AuthorityCertSerialNumber" type="xs:integer"/>

10.1.14 element AuthorityInfoAccess

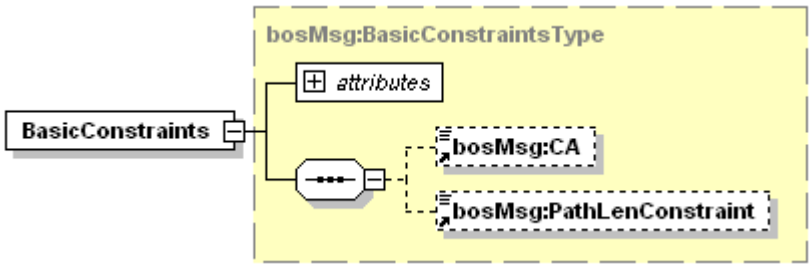
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#

type	**bosMsg:AuthorityInfoAccessType**
properties	content complex
children	**bosMsg:AccessDescription**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:element name="AuthorityInfoAccess" type="bosMsg:AuthorityInfoAccessType"/>

10.1.15 element AuthorityKeyIdentifier

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:AuthorityKeyIdentifierType**
properties	content complex
children	**bosMsg:KeyIdentifier** **bosMsg:AuthorityCertIssuer** **bosMsg:AuthorityCertSerialNumber**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:element name="AuthorityKeyIdentifier" type="bosMsg:AuthorityKeyIdentifierType"/>

10.1.16 element BasicConstraints

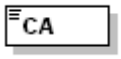
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:BasicConstraintsType**
properties	content complex
children	**bosMsg:CA** **bosMsg:PathLenConstraint**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional

source	<xs:element name="BasicConstraints" type="bosMsg:BasicConstraintsType"/>

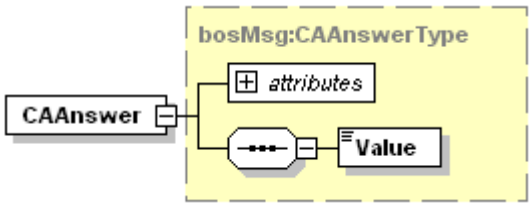
10.1.17 element BusinessCategory

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	content simple
used by	complexType **NameInfoType**
source	<xs:element name="BusinessCategory" type="xs:string"/>

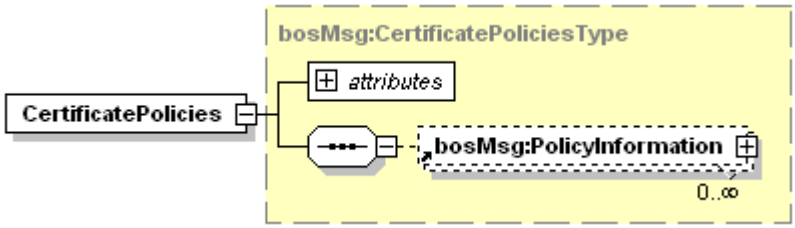
10.1.18 element CA

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:boolean**
properties	content simple
used by	complexType **BasicConstraintsType**
source	<xs:element name="CA" type="xs:boolean"/>

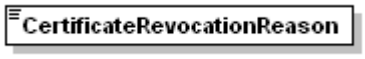
10.1.19 element CAAnswer

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:CAAnswerType**
properties	content complex
children	**Value**
attributes	Name Type Use Default Fixed Annotation Type **xs:QName** required
source	<xs:element name="CAAnswer" type="bosMsg:CAAnswerType"/>

10.1.20 element CertificatePolicies

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:CertificatePoliciesType**
properties	content complex
children	**bosMsg:PolicyInformation**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:element name="CertificatePolicies" type="bosMsg:CertificatePoliciesType"/>

10.1.21 element CertificateRevocationReason

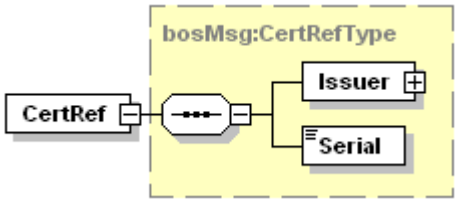
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:CertificateRevocationReasonType**
properties	content simple
used by	complexType **VPSResultType**
facets	enumeration bosMsg:Unspecified enumeration bosMsg:KeyCompromised enumeration bosMsg:CaCompromised enumeration bosMsg:AffiliationChanged enumeration bosMsg:Superseded enumeration bosMsg:CessationOfOperation enumeration bosMsg:CertificateHold enumeration bosMsg:RemoveFromCRL enumeration bosMsg:None enumeration bosMsg:PrivilegeWithdrawn enumeration bosMsg:AACompromise
source	<xs:element name="CertificateRevocationReason" type="bosMsg:CertificateRevocationReasonType"/>

10.1.22 element CertQuality

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:certQualityType**
properties	content simple
used by	complexType **VPSResultType**
facets	enumeration bosMsg:advanced enumeration bosMsg:qualified enumeration bosMsg:accredited

	enumeration bosMsg:pki1verwaltung
source	<xs:element name="CertQuality" type="bosMsg:certQualityType"/>

10.1.23 element CertRef

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:CertRefType**
properties	content complex
children	**Issuer** **Serial**
source	<xs:element name="CertRef" type="bosMsg:CertRefType"/>

10.1.24 element CommonName

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	content simple
used by	complexType **NameInfoType**
source	<xs:element name="CommonName" type="xs:string"/>

10.1.25 element CountryName

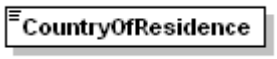
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	content simple
used by	complexType **NameInfoType**
source	<xs:element name="CountryName" type="xs:string"/>

10.1.26 element CountryOfCitizenship

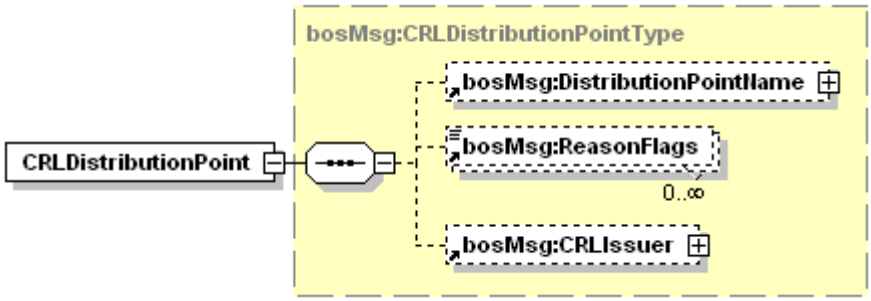
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	content simple
used by	complexType **NameInfoType**

source	<xs:element name="CountryOfCitizenship" type="xs:string"/>

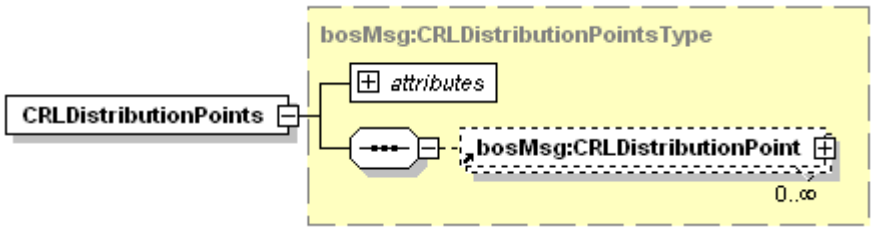
10.1.27 element CountryOfResidence

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	content simple
source	<xs:element name="CountryOfResidence" type="xs:string"/>

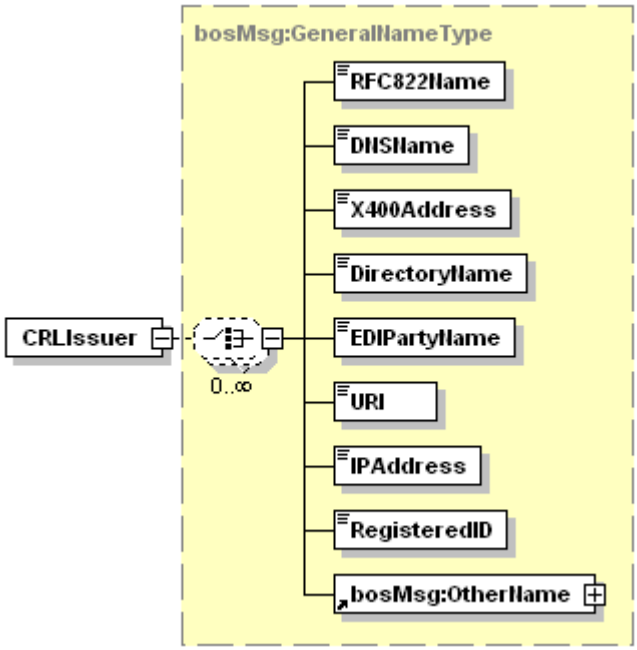
10.1.28 element CRLDistributionPoint

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:CRLDistributionPointType**
properties	content complex
children	**bosMsg:DistributionPointName** **bosMsg:ReasonFlags** **bosMsg:CRLIssuer**
used by	complexType **CRLDistributionPointsType**
source	<xs:element name="CRLDistributionPoint" type="bosMsg:CRLDistributionPointType"/>

10.1.29 element CRLDistributionPoints

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:CRLDistributionPointsType**
properties	content complex
children	**bosMsg:CRLDistributionPoint**
used by	complexType **ExtensionInfoType**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:element name="CRLDistributionPoints" type="bosMsg:CRLDistributionPointsType"/>

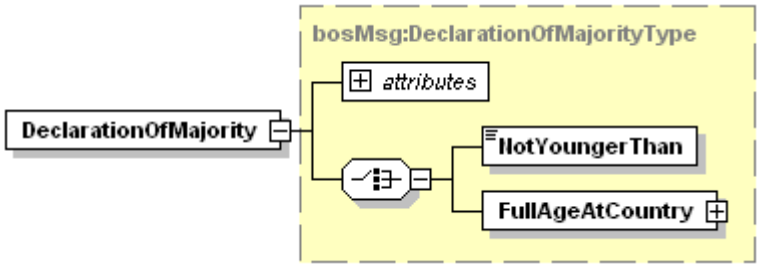
10.1.30 element CRLIssuer

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralNameType**
properties	content complex
children	**RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName**
used by	complexType **CRLDistributionPointType**
source	<xs:element name="CRLIssuer" type="bosMsg:GeneralNameType"/>

10.1.31 element DateOfBirth

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:date**
properties	content simple
used by	complexType **NameInfoType**
source	<xs:element name="DateOfBirth" type="xs:date"/>

10.1.32 element DeclarationOfMajority

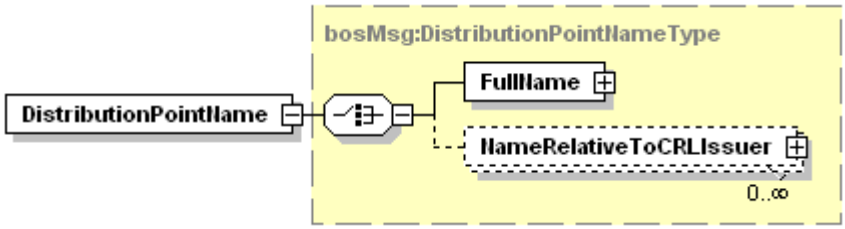
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#

Type	**bosMsg:DeclarationOfMajorityType**
Properties	content complex
Children	**NotYoungerThan** **FullAgeAtCountry**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="DeclarationOfMajority" type="bosMsg:DeclarationOfMajorityType"/>

10.1.33 element DistinguishedNameQualifier

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="DistinguishedNameQualifier" type="xs:string"/>

10.1.34 element DistributionPointName

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:DistributionPointNameType**
Properties	content complex
Children	**FullName** **NameRelativeToCRLIssuer**
used by	complexType **CRLDistributionPointType**
Source	<xs:element name="DistributionPointName" type="bosMsg:DistributionPointNameType"/>

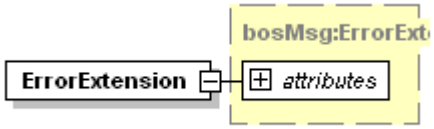
10.1.35 element DomainComponent

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="DomainComponent" type="xs:string"/>

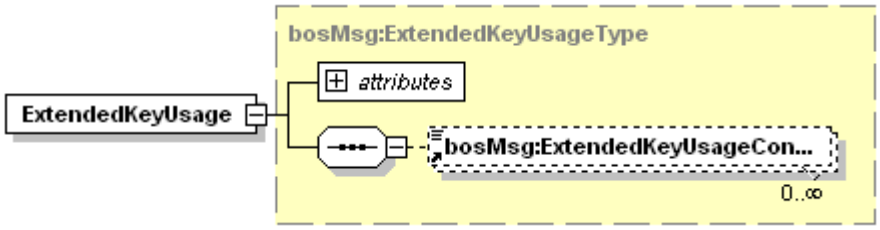
10.1.36 element EmailAddress

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="EmailAddress" type="xs:string"/>

10.1.37 element ErrorExtension

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:ErrorExtensionType**
Properties	content complex
used by	complexType **VPSResultType**
Attributes	Name: Reason; Type: **bosMsg:reasonType**; Use; Default; Fixed; Annotation
Source	<xs:element name="ErrorExtension" type="bosMsg:ErrorExtensionType"/>

10.1.38 element ExtendedKeyUsage

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:ExtendedKeyUsageType**
Properties	content complex
Children	**bosMsg:ExtendedKeyUsageContent**
used by	complexType **ExtensionInfoType**
Attributes	Name: Critical; Type: **xs:boolean**; Use: optional; Default; Fixed; Annotation
Source	<xs:element name="ExtendedKeyUsage" type="bosMsg:ExtendedKeyUsageType"/>

10.1.39 element ExtendedKeyUsageContent

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:ExtendedKeyUsageContentType**
Properties	content simple
used by	complexType **ExtendedKeyUsageType**
Facets	enumeration bosMsg:ServerAuthentication enumeration bosMsg:ClientAuthentication enumeration bosMsg:CodeSigning enumeration bosMsg:EmailProtection enumeration bosMsg:TimeStamping enumeration bosMsg:OCSPSigning
Source	<xs:element name="ExtendedKeyUsageContent" type="bosMsg:ExtendedKeyUsageContentType"/>

10.1.40 element ExtensionInfo

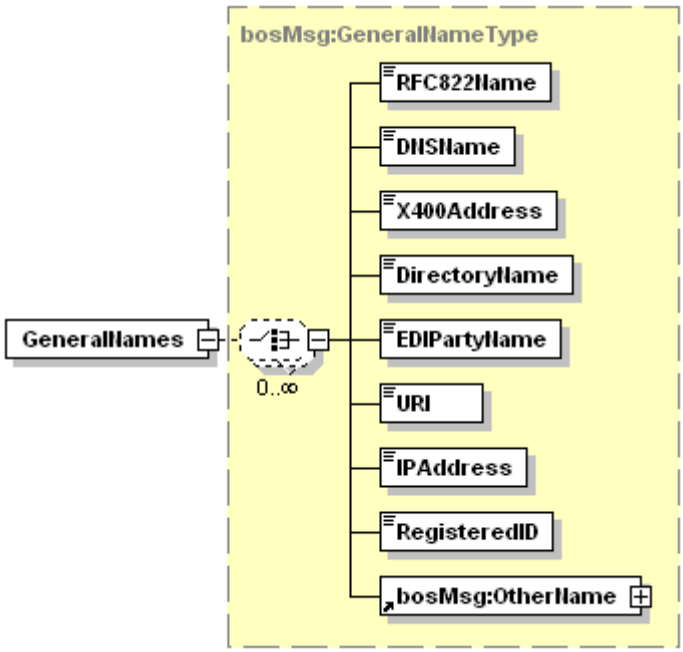
Diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	bosMsg:ExtensionInfoType
properties	content complex mixed true
children	bosMsg:AdvancedKeyUsage bosMsg:BasicConstraints bosMsg:AuthorityKeyIdentifier bosMsg:SubjectKeyIdentifier bosMsg:CertificatePolicies bosMsg:SubjectAltNames bosMsg:IssuerAltNames bosMsg:SubjectDirectoryAttributes

	bosMsg:CRLDistributionPoints bosMsg:AuthorityInfoAccess bosMsg:OCSPNocheck bosMsg:ExtendedKeyUsage bosMsg:PolicyConstraints bosMsg:NameConstraints bosMsg:LiabilityLimitationFlag bosMsg:QCStatements bosMsg:Procuration bosMsg:MonetaryLimit bosMsg:DeclarationOfMajority bosMsg:Restriction bosMsg:AdditionalInformation bosMsg:Admission bosMsg:PrivateKeyUsagePeriod
used by	complexType VPSResultType
source	<xs:element name="ExtensionInfo" type="bosMsg:ExtensionInfoType"/>

10.1.41 element Gender

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	xs:string
Properties	content simple
used by	complexType NameInfoType
Source	<xs:element name="Gender" type="xs:string"/>

10.1.42 element GeneralNames

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	bosMsg:GeneralNameType
properties	content complex
children	RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName
used by	complexTypes IssuerAltNamesType SubjectAltNamesType
source	<xs:element name="GeneralNames" type="bosMsg:GeneralNameType"/>

10.1.43 element GenerationQualifier

Diagram	

Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="GenerationQualifier" type="xs:string"/>

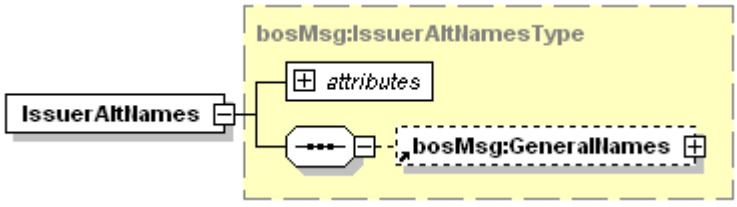
10.1.44 element GivenName

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="GivenName" type="xs:string"/>

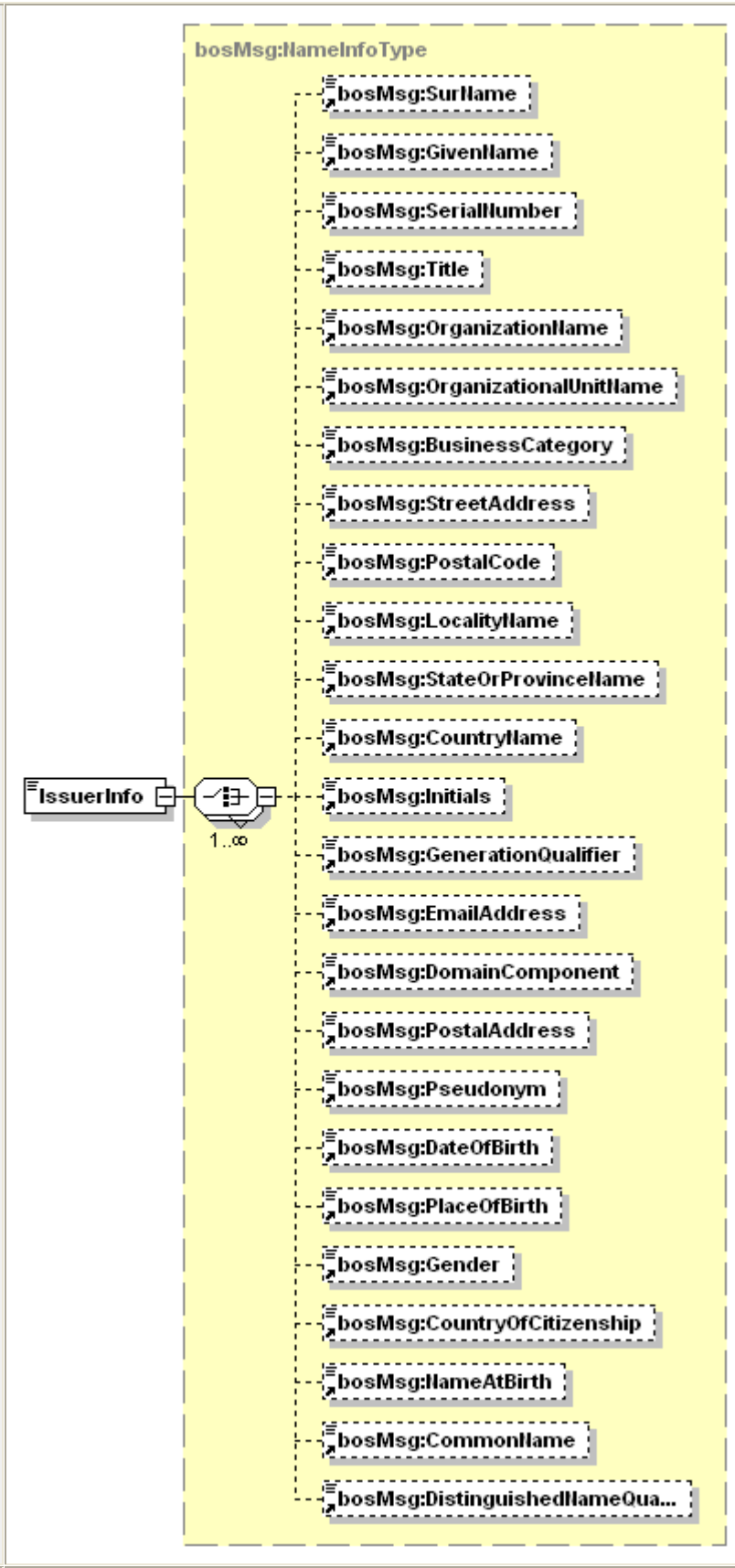
10.1.45 element Initials

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="Initials" type="xs:string"/>

10.1.46 element IssuerAltNames

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:IssuerAltNamesType**
Properties	content complex
Children	**bosMsg:GeneralNames**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="IssuerAltNames" type="bosMsg:IssuerAltNamesType"/>

10.1.47 element IssuerInfo

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	bosMsg:NameInfoType

Properties	content complex mixed true
Children	bosMsg:SurName bosMsg:GivenName bosMsg:SerialNumber bosMsg:Title bosMsg:OrganizationName bosMsg:OrganizationalUnitName bosMsg:BusinessCategory bosMsg:StreetAddress bosMsg:PostalCode bosMsg:LocalityName bosMsg:StateOrProvinceName bosMsg:CountryName bosMsg:Initials bosMsg:GenerationQualifier bosMsg:EmailAddress bosMsg:DomainComponent bosMsg:PostalAddress bosMsg:Pseudonym bosMsg:DateOfBirth bosMsg:PlaceOfBirth bosMsg:Gender bosMsg:CountryOfCitizenship bosMsg:NameAtBirth bosMsg:CommonName bosMsg:DistinguishedNameQualifier
used by	complexType VPSResultType
Source	<xs:element name="IssuerInfo" type="bosMsg:NameInfoType"/>

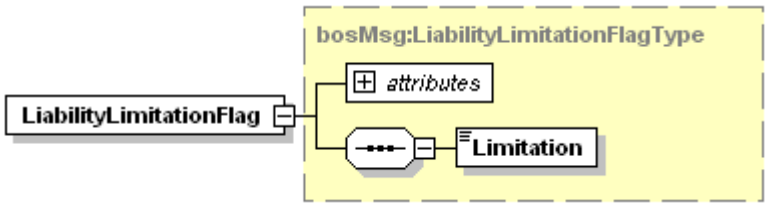
10.1.48 element KeyIdentifier

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	xs:string
Properties	content simple
used by	complexTypes AuthorityKeyIdentifierType SubjectKeyIdentifierType
Source	<xs:element name="KeyIdentifier" type="xs:string"/>

10.1.49 element KeyUsageContent

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	bosMsg:KeyUsageContentType
Properties	content simple
used by	complexType AdvancedKeyUsageType
Facets	enumeration bosMsg:DigitalSignature enumeration bosMsg:NonRepudation enumeration bosMsg:KeyEncipherment enumeration bosMsg:DataEncipherment enumeration bosMsg:KeyAgreement enumeration bosMsg:KeyCertSign enumeration bosMsg:CRLSign enumeration bosMsg:EncipherOnly enumeration bosMsg:DecipherOnly
Source	<xs:element name="KeyUsageContent" type="bosMsg:KeyUsageContentType"/>

10.1.50 element LiabilityLimitationFlag

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	bosMsg:LiabilityLimitationFlagType
Properties	content complex

Children	**Limitation**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="LiabilityLimitationFlag" type="bosMsg:LiabilityLimitationFlagType"/>

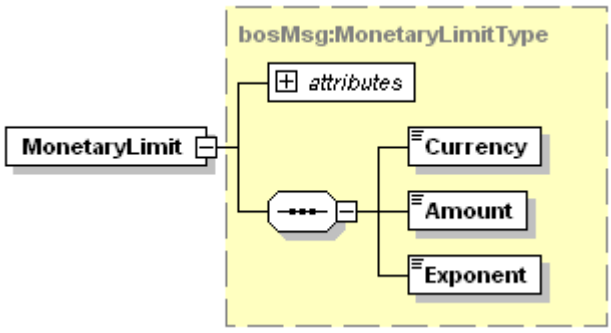
10.1.51 element LocalityName

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="LocalityName" type="xs:string"/>

10.1.52 element MissingAttributeCertificate

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **VPSMessageAbstractType**
Source	<xs:element name="MissingAttributeCertificate" type="xs:string"/>

10.1.53 element MonetaryLimit

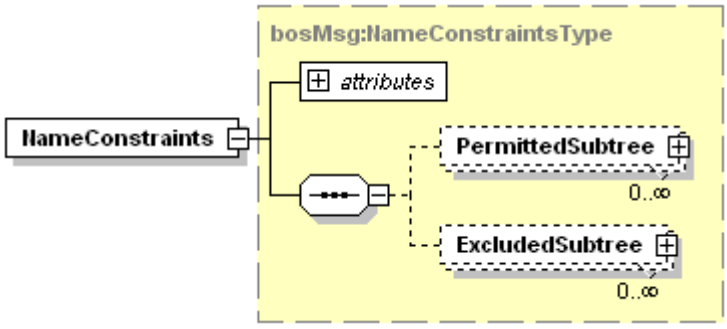
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:MonetaryLimitType**
Properties	content complex
Children	**Currency Amount Exponent**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional

Source	<xs:element name="MonetaryLimit" type="bosMsg:MonetaryLimitType"/>

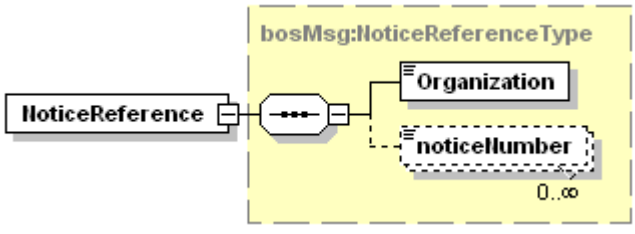
10.1.54 element NameAtBirth

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="NameAtBirth" type="xs:string"/>

10.1.55 element NameConstraints

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:NameConstraintsType**
Properties	content complex
Children	**PermittedSubtree** **ExcludedSubtree**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="NameConstraints" type="bosMsg:NameConstraintsType"/>

10.1.56 element NoticeReference

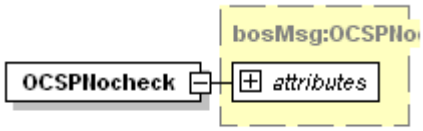
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:NoticeReferenceType**
Properties	content complex
Children	**Organization** **noticeNumber**
used by	complexType **UserNoticeType**

Source	<xs:element name="NoticeReference" type="bosMsg:NoticeReferenceType"/>

10.1.57 element OCSPNoCache

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:boolean**
Properties	content simple
used by	complexType **VPSRequestType**
Source	<xs:element name="OCSPNoCache" type="xs:boolean"/>

10.1.58 element OCSPNocheck

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:OCSPNocheckType**
Properties	content complex
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="OCSPNocheck" type="bosMsg:OCSPNocheckType"/>

10.1.59 element OrganizationalUnitName

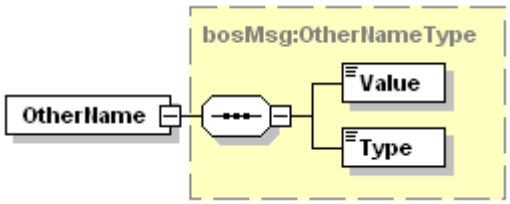
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="OrganizationalUnitName" type="xs:string"/>

10.1.60 element OrganizationName

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**

Source	<xs:element name="OrganizationName" type="xs:string"/>

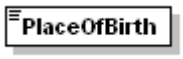
10.1.61 element OtherName

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:OtherNameType**
Properties	content complex
Children	**Value** **Type**
used by	complexType **GeneralNameType**
Source	<xs:element name="OtherName" type="bosMsg:OtherNameType"/>

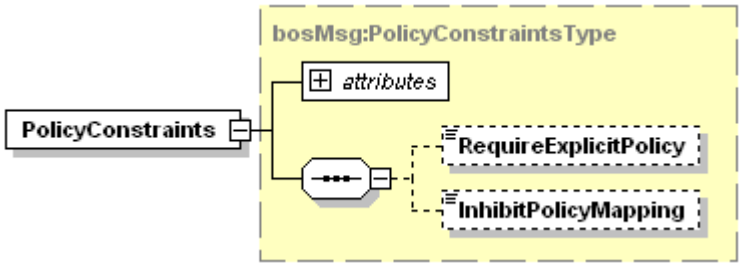
10.1.62 element PathLenConstraint

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **BasicConstraintsType**
Source	<xs:element name="PathLenConstraint" type="xs:string"/>

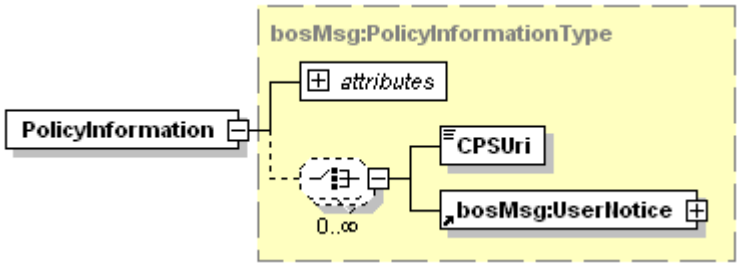
10.1.63 element PlaceOfBirth

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="PlaceOfBirth" type="xs:string"/>

10.1.64 element PolicyConstraints

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:PolicyConstraintsType**
Properties	content complex
Children	**RequireExplicitPolicy** **InhibitPolicyMapping**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="PolicyConstraints" type="bosMsg:PolicyConstraintsType"/>

10.1.65 element PolicyInformation

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:PolicyInformationType**
Properties	content complex
Children	**CPSUri** **bosMsg:UserNotice**
used by	complexType **CertificatePoliciesType**
Attributes	Name Type Use Default Fixed Annotation PolicyIdentifier **xs:string**
Source	<xs:element name="PolicyInformation" type="bosMsg:PolicyInformationType"/>

10.1.66 element PostalAddress

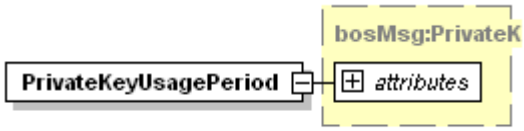
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**

Source	<xs:element name="PostalAddress" type="xs:string"/>

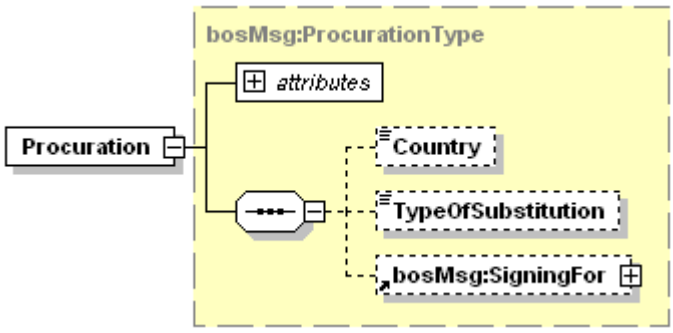
10.1.67 element PostalCode

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="PostalCode" type="xs:string"/>

10.1.68 element PrivateKeyUsagePeriod

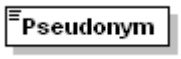
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:PrivateKeyUsagePeriodType**
Properties	content complex
used by	complexType **ExtensionInfoType**
Attributes	Name / Type / Use / Default / Fixed / Annotation Critical / **xs:boolean** / optional NotBefore / **xs:dateTime** NotAfter / **xs:dateTime**
Source	<xs:element name="PrivateKeyUsagePeriod" type="bosMsg:PrivateKeyUsagePeriodType"/>

10.1.69 element Procuration

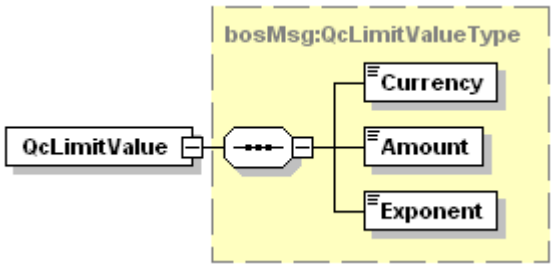
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:ProcurationType**
Properties	content complex
Children	**Country TypeOfSubstitution bosMsg:SigningFor**
used by	complexType **ExtensionInfoType**

Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="Procuration" type="bosMsg:ProcurationType"/>

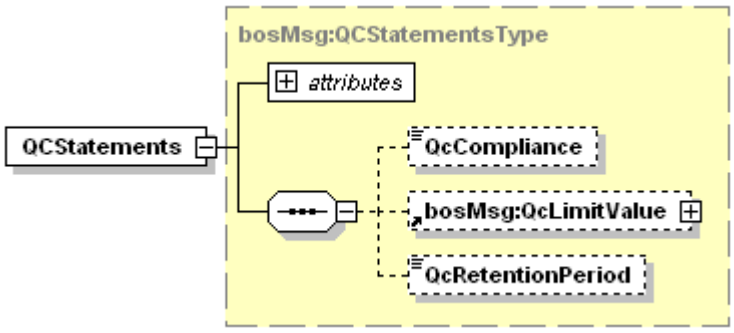
10.1.70 element Pseudonym

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="Pseudonym" type="xs:string"/>

10.1.71 element QcLimitValue

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:QcLimitValueType**
properties	content complex
children	**Currency Amount Exponent**
used by	complexType **QCStatementsType**
source	<xs:element name="QcLimitValue" type="bosMsg:QcLimitValueType"/>

10.1.72 element QCStatements

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:QCStatementsType**
Properties	content complex
Children	**QcCompliance bosMsg:QcLimitValue QcRetentionPeriod**

used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="QCStatements" type="bosMsg:QCStatementsType"/>

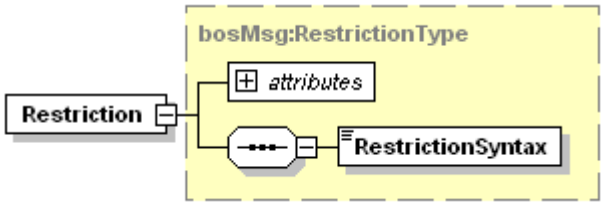
10.1.73 element ReasonFlags

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:ReasonFlagsType**
Properties	content simple
used by	complexType **CRLDistributionPointType**
Facets	enumeration bosMsg:Unused enumeration bosMsg:KeyCompromised enumeration bosMsg:CaCompromised enumeration bosMsg:AffiliationChanged enumeration bosMsg:Superseded enumeration bosMsg:CessationOfOperation enumeration bosMsg:CertificateHold
Source	<xs:element name="ReasonFlags" type="bosMsg:ReasonFlagsType"/>

10.1.74 element RelativeDistinguishedName

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:RelativeDistinguishedNameType**
Properties	content complex
Attributes	Name Type Use Default Fixed Annotation Type **xs:string** Value **xs:string**
Source	<xs:element name="RelativeDistinguishedName" type="bosMsg:RelativeDistinguishedNameType"/>

10.1.75 element Restriction

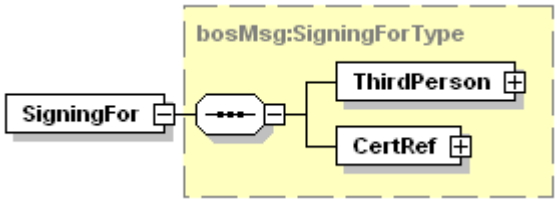
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:RestrictionType**
Properties	content complex

Children	**RestrictionSyntax**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="Restriction" type="bosMsg:RestrictionType"/>

10.1.76 element SerialNumber

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="SerialNumber" type="xs:string"/>

10.1.77 element SigningFor

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:SigningForType**
Properties	content complex
Children	**ThirdPerson** **CertRef**
used by	complexType **ProcurationType**
Source	<xs:element name="SigningFor" type="bosMsg:SigningForType"/>

10.1.78 element StateOrProvinceName

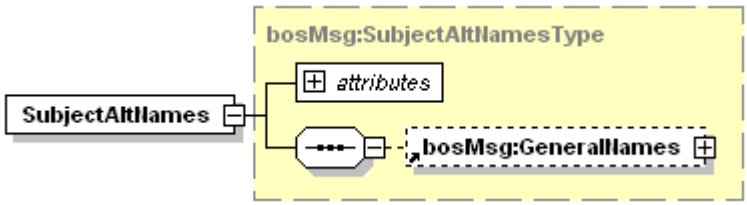
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="StateOrProvinceName" type="xs:string"/>

10.1.79 element StreetAddress

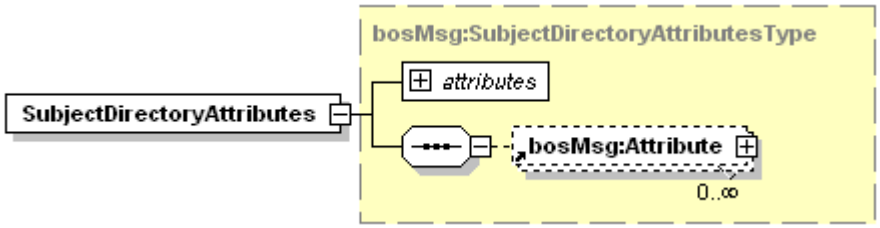
Diagram	

Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="StreetAddress" type="xs:string"/>

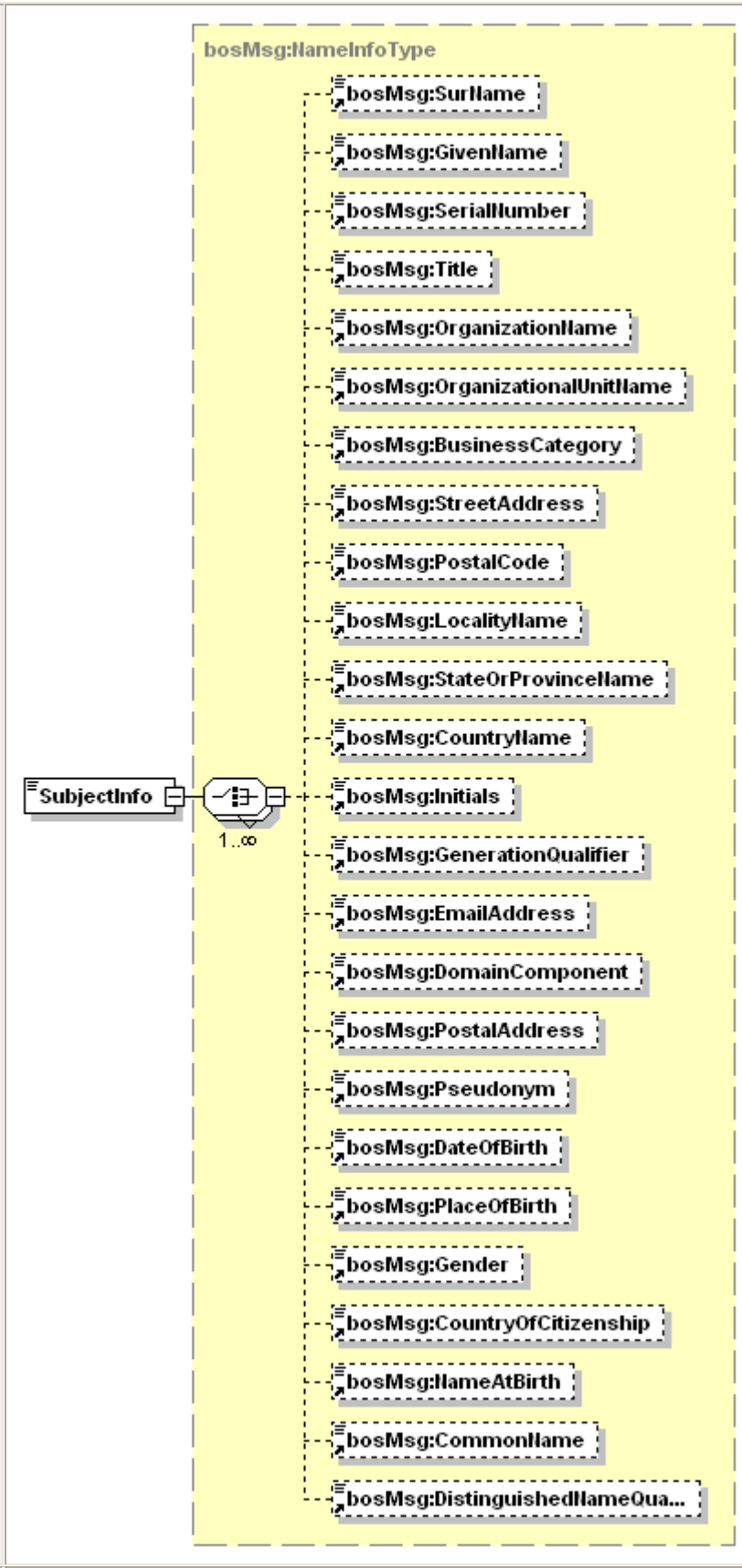
10.1.80 element SubjectAltNames

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:SubjectAltNamesType**
Properties	content complex
Children	**bosMsg:GeneralNames**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="SubjectAltNames" type="bosMsg:SubjectAltNamesType"/>

10.1.81 element SubjectDirectoryAttributes

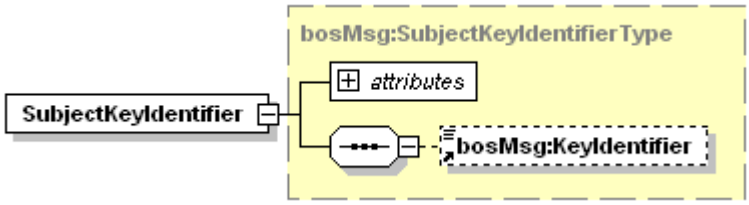
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:SubjectDirectoryAttributesType**
Properties	content complex
Children	**bosMsg:Attribute**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="SubjectDirectoryAttributes" type="bosMsg:SubjectDirectoryAttributesType"/>

10.1.82 element SubjectInfo

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	bosMsg:NameInfoType

Properties	content complex mixed true
Children	bosMsg:SurName bosMsg:GivenName bosMsg:SerialNumber bosMsg:Title bosMsg:OrganizationName bosMsg:OrganizationalUnitName bosMsg:BusinessCategory bosMsg:StreetAddress bosMsg:PostalCode bosMsg:LocalityName bosMsg:StateOrProvinceName bosMsg:CountryName bosMsg:Initials bosMsg:GenerationQualifier bosMsg:EmailAddress bosMsg:DomainComponent bosMsg:PostalAddress bosMsg:Pseudonym bosMsg:DateOfBirth bosMsg:PlaceOfBirth bosMsg:Gender bosMsg:CountryOfCitizenship bosMsg:NameAtBirth bosMsg:CommonName bosMsg:DistinguishedNameQualifier
used by	complexType **VPSResultType**
Source	<xs:element name="SubjectInfo" type="bosMsg:NameInfoType"/>

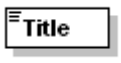
10.1.83 element SubjectKeyIdentifier

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:SubjectKeyIdentifierType**
Properties	content complex
Children	**bosMsg:KeyIdentifier**
used by	complexType **ExtensionInfoType**
Attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
Source	<xs:element name="SubjectKeyIdentifier" type="bosMsg:SubjectKeyIdentifierType"/>

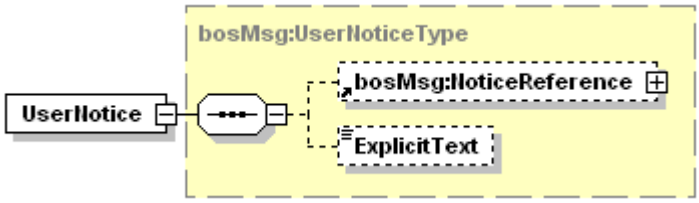
10.1.84 element SurName

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="SurName" type="xs:string"/>

10.1.85 element Title

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**xs:string**
Properties	content simple
used by	complexType **NameInfoType**
Source	<xs:element name="Title" type="xs:string"/>

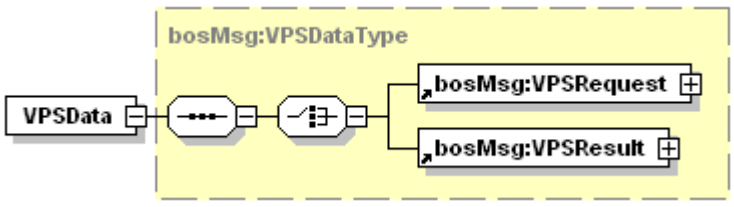
10.1.86 element UserNotice

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:UserNoticeType**
Properties	content complex
Children	**bosMsg:NoticeReference** **ExplicitText**
used by	complexType **PolicyInformationType**
Source	<xs:element name="UserNotice" type="bosMsg:UserNoticeType"/>

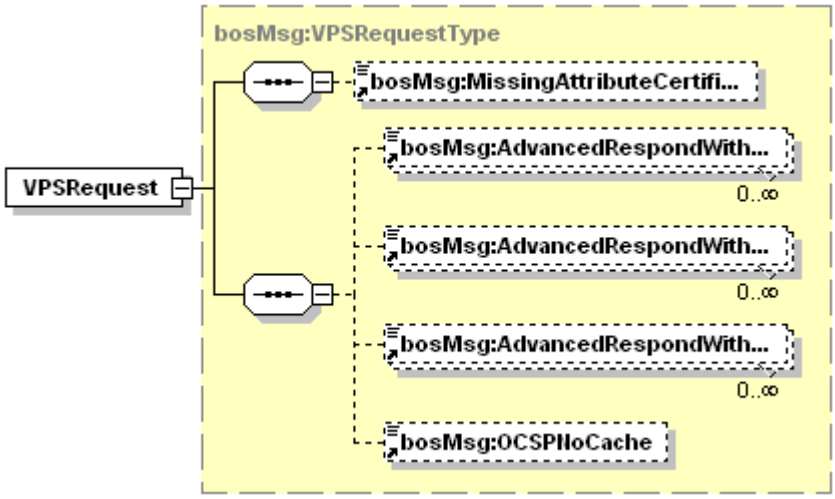
10.1.87 element ValidateScheme

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:ValidateSchemeType**
Properties	content simple
used by	complexType **VPSResultType**
Facets	enumeration bosMsg:LOCAL enumeration bosMsg:OCSP enumeration bosMsg:CRL enumeration bosMsg:CRL_LDAP enumeration bosMsg:LDAP
Source	<xs:element name="ValidateScheme" type="bosMsg:ValidateSchemeType"/>

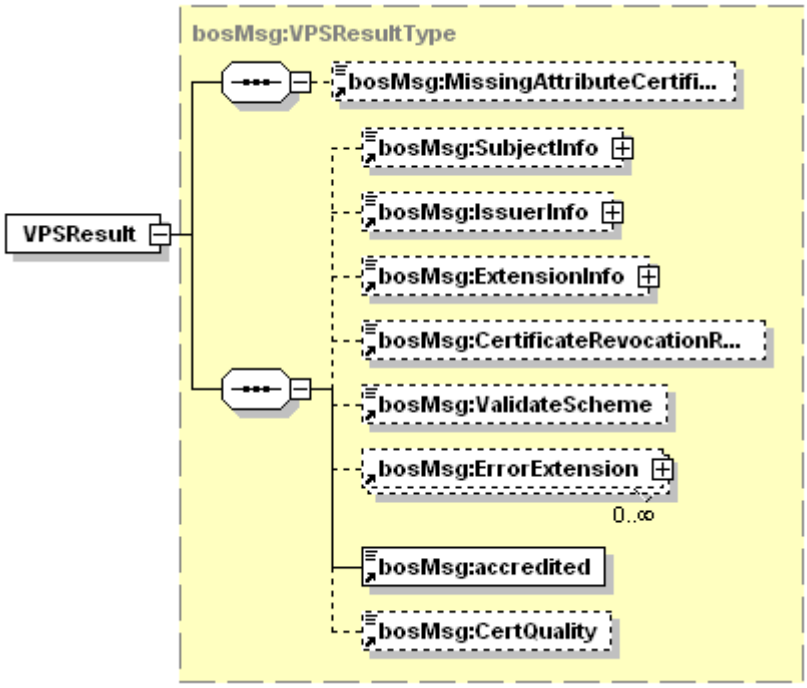
10.1.88 element VPSData

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:VPSDataType**
Properties	content complex
Children	**bosMsg:VPSRequest** **bosMsg:VPSResult**
Source	<xs:element name="VPSData" type="bosMsg:VPSDataType"/>

10.1.89 element VPSRequest

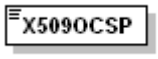
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:VPSRequestType**
Properties	content complex
Children	**bosMsg:MissingAttributeCertificate** **bosMsg:AdvancedRespondWithSubjectInfo** **bosMsg:AdvancedRespondWithIssuerInfo** **bosMsg:AdvancedRespondWithExtensionInfo** **bosMsg:OCSPNoCache**
used by	complexType **VPSDataType**
Source	<xs:element name="VPSRequest" type="bosMsg:VPSRequestType"/>

10.1.90 element VPSResult

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:VPSResultType**
Properties	content complex

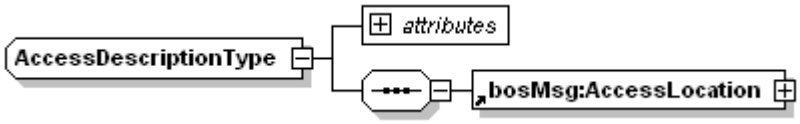
Children	bosMsg:MissingAttributeCertificate bosMsg:SubjectInfo bosMsg:IssuerInfo bosMsg:ExtensionInfo bosMsg:CertificateRevocationReason bosMsg:ValidateScheme bosMsg:ErrorExtension bosMsg:accredited bosMsg:CertQuality
used by	complexType VPSDataType
Source	<xs:element name="VPSResult" type="bosMsg:VPSResultType"/>

10.1.91 element X509OCSP

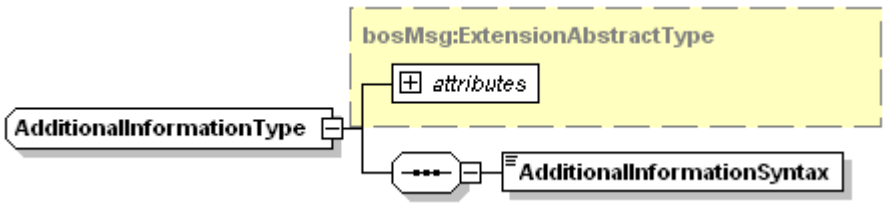
Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	xs:base64Binary
Properties	content simple
Source	<xs:element name="X509OCSP" type="xs:base64Binary"/>

10.2 Complex Types

10.2.1 complexType AccessDescriptionType

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Children	bosMsg:AccessLocation
used by	element AccessDescription
Attributes	Name Type Use Default Fixed Annotation AccessMethod xs:string
Source	<xs:complexType name="AccessDescriptionType"> <xs:sequence> <xs:element ref="bosMsg:AccessLocation"/> </xs:sequence> <xs:attribute name="AccessMethod" type="xs:string"/> </xs:complexType>

10.2.2 complexType AdditionalInformationType

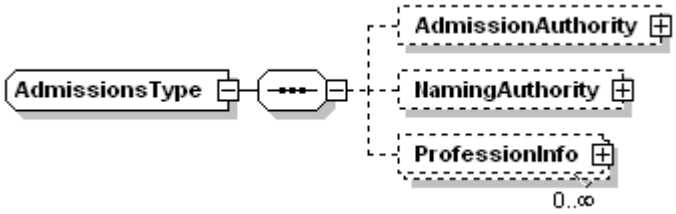
Diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of bosMsg:ExtensionAbstractType
properties	base bosMsg:ExtensionAbstractType
children	AdditionalInformationSyntax
used by	element AdditionalInformation

attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="AdditionalInformationType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="AdditionalInformationSyntax" type="xs:string"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

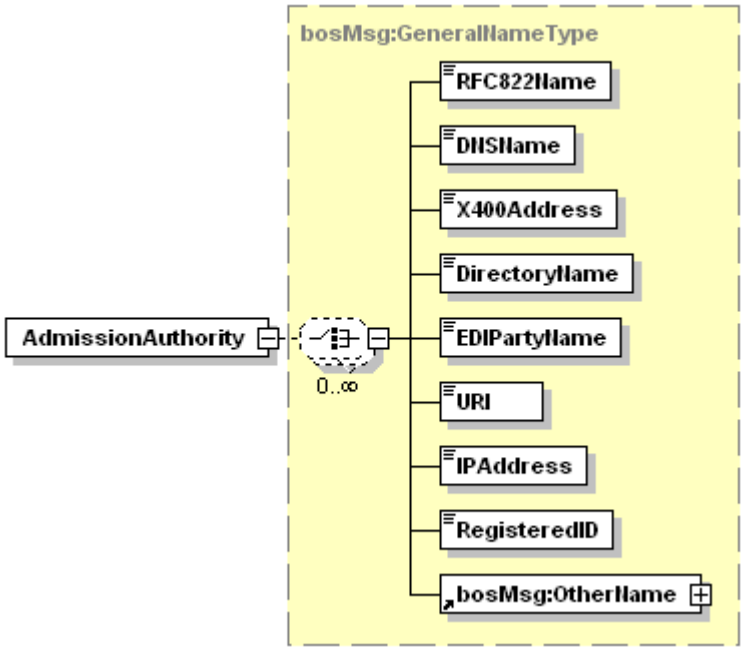
10.2.2.1 element AdditionalInformationType/AdditionalInformationSyntax

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="AdditionalInformationSyntax" type="xs:string"/>

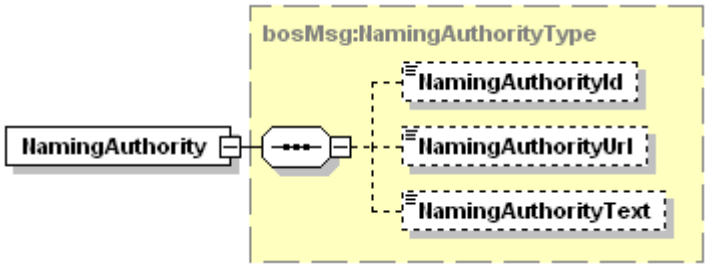
10.2.3 complexType AdmissionsType

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Children	**AdmissionAuthority** **NamingAuthority** **ProfessionInfo**
used by	element **AdmissionType/ContentsOfAdmissions**
Source	<xs:complexType name="AdmissionsType"> <xs:sequence> <xs:element name="AdmissionAuthority" type="bosMsg:GeneralNameType" minOccurs="0"/> <xs:element name="NamingAuthority" type="bosMsg:NamingAuthorityType" minOccurs="0"/> <xs:element name="ProfessionInfo" type="bosMsg:ProfessionInfoType" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:complexType>

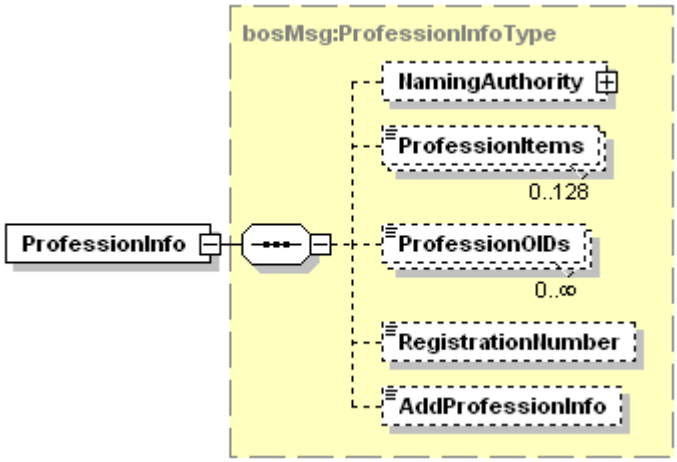
10.2.3.1 element AdmissionsType/AdmissionAuthority

Diagram	
Namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
Type	**bosMsg:GeneralNameType**
Properties	isRef 0 content complex
Children	**RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName**
Source	<xs:element name="AdmissionAuthority" type="bosMsg:GeneralNameType" minOccurs="0"/>

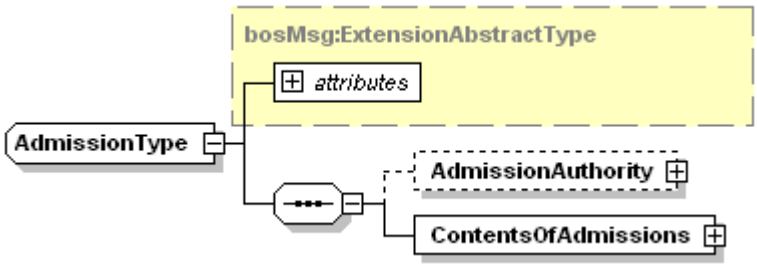
10.2.3.2 element AdmissionsType/NamingAuthority

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:NamingAuthorityType**
properties	isRef 0 content complex
children	**NamingAuthorityId NamingAuthorityUrl NamingAuthorityText**
source	<xs:element name="NamingAuthority" type="bosMsg:NamingAuthorityType" minOccurs="0"/>

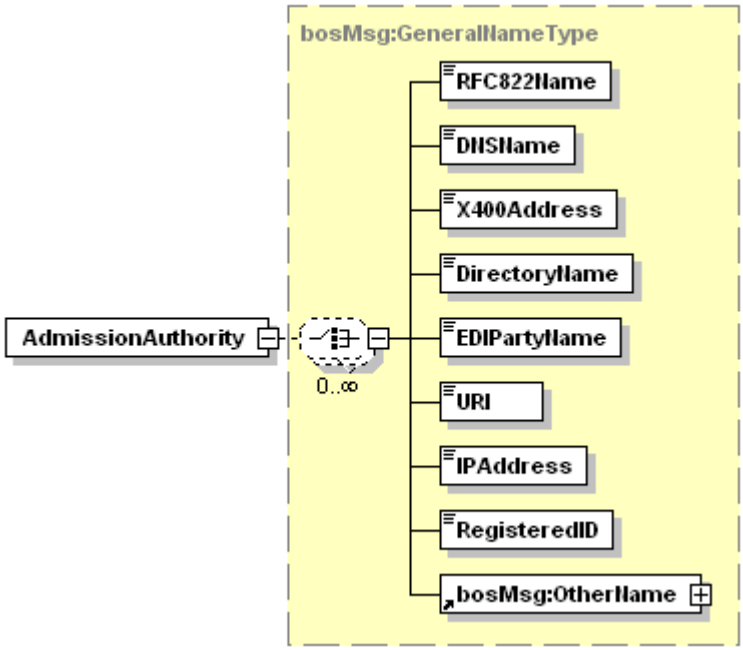
10.2.3.3 element AdmissionsType/ProfessionInfo

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:ProfessionInfoType**
properties	isRef 0 content complex
children	**NamingAuthority** **ProfessionItems** **ProfessionOIDs** **RegistrationNumber** **AddProfessionInfo**
source	<xs:element name="ProfessionInfo" type="bosMsg:ProfessionInfoType" minOccurs="0" maxOccurs="unbounded"/>

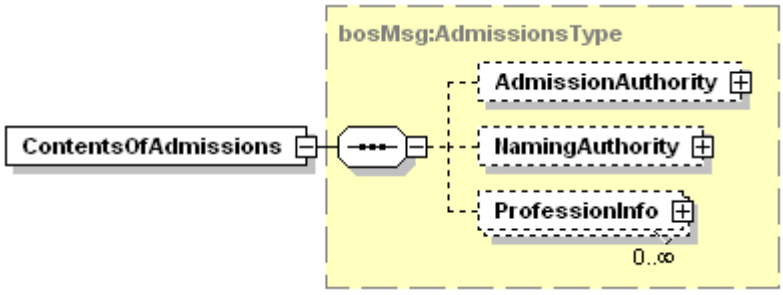
10.2.4 complexType AdmissionType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**AdmissionAuthority** **ContentsOfAdmissions**
used by	element **Admission**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="AdmissionType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="AdmissionAuthority" type="bosMsg:GeneralNameType" minOccurs="0"/> <xs:element name="ContentsOfAdmissions" type="bosMsg:AdmissionsType"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

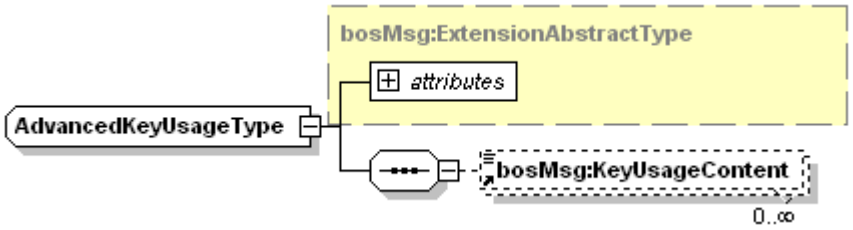
10.2.4.1 element AdmissionType/AdmissionAuthority

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralNameType**
properties	isRef 0 content complex
children	RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName
source	<xs:element name="AdmissionAuthority" type="bosMsg:GeneralNameType" minOccurs="0"/>

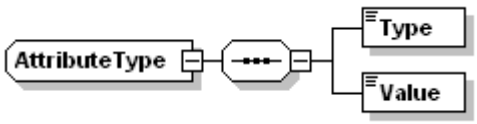
10.2.4.2 element AdmissionType/ContentsOfAdmissions

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:AdmissionsType**
properties	isRef 0 content complex
children	AdmissionAuthority NamingAuthority ProfessionInfo
source	<xs:element name="ContentsOfAdmissions" type="bosMsg:AdmissionsType"/>

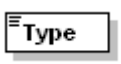
10.2.5 complexType AdvancedKeyUsageType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:KeyUsageContent**
used by	element **AdvancedKeyUsage**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="AdvancedKeyUsageType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:KeyUsageContent" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

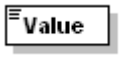
10.2.6 complexType AttributeType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**Type** **Value**
used by	element **Attribute**
source	<xs:complexType name="AttributeType"> <xs:sequence> <xs:element name="Type" type="xs:string"/> <xs:element name="Value" type="xs:string"/> </xs:sequence> </xs:complexType>

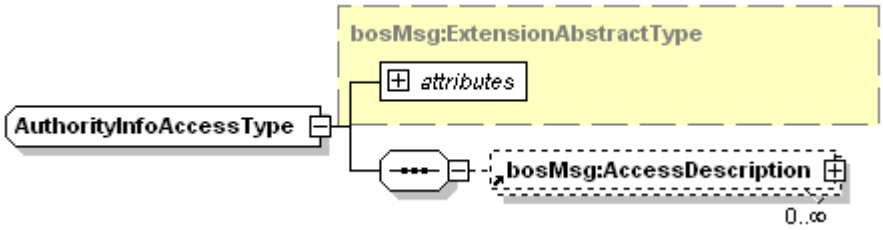
10.2.6.1 element AttributeType/Type

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="Type" type="xs:string"/>

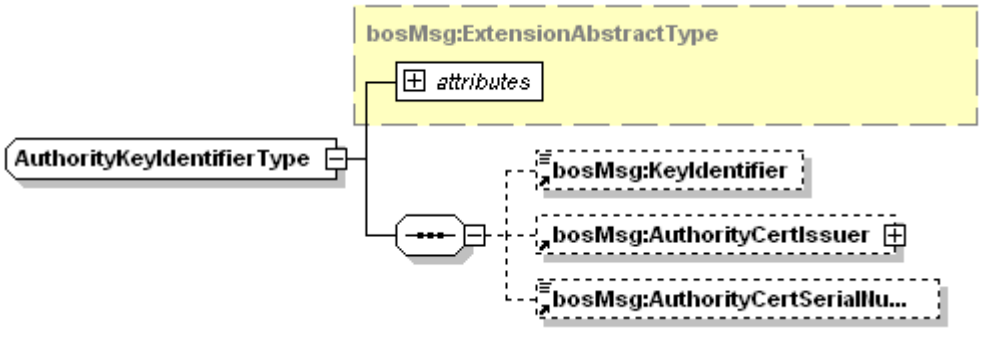
10.2.6.2 element AttributeType/Value

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="Value" type="xs:string"/>

10.2.7 complexType AuthorityInfoAccessType

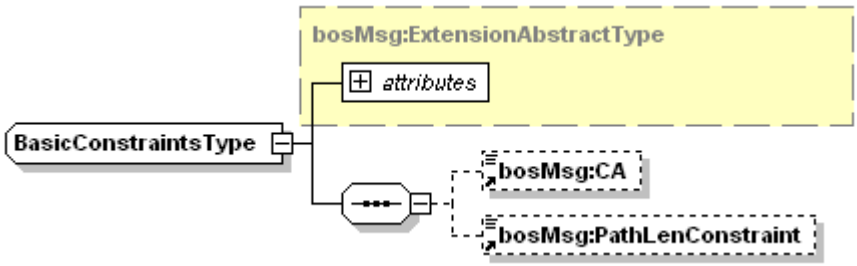
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:AccessDescription**
used by	element **AuthorityInfoAccess**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="AuthorityInfoAccessType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:AccessDescription" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.8 complexType AuthorityKeyIdentifierType

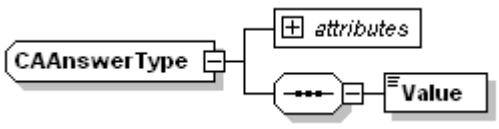
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType

children	**bosMsg:KeyIdentifier** **bosMsg:AuthorityCertIssuer** **bosMsg:AuthorityCertSerialNumber**
used by	element **AuthorityKeyIdentifier**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="AuthorityKeyIdentifierType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:KeyIdentifier" minOccurs="0"/> <xs:element ref="bosMsg:AuthorityCertIssuer" minOccurs="0"/> <xs:element ref="bosMsg:AuthorityCertSerialNumber" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.9 complexType BasicConstraintsType

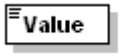
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:CA** **bosMsg:PathLenConstraint**
used by	element **BasicConstraints**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="BasicConstraintsType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:CA" minOccurs="0"/> <xs:element ref="bosMsg:PathLenConstraint" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.10 complexType CAAnswerType

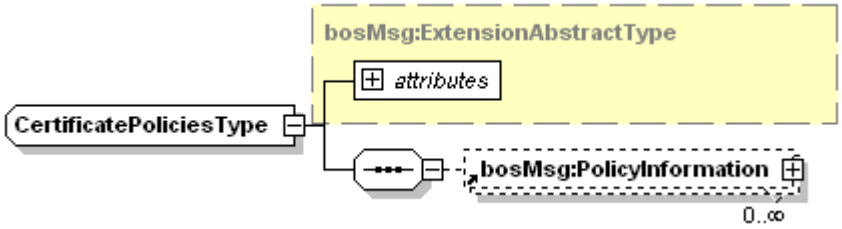
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**Value**
used by	element **CAAnswer**

attributes	Name Type Use Default Fixed Annotation Type **xs:QName** required
source	<xs:complexType name="CAAnswerType"> <xs:sequence> <xs:element name="Value" type="xs:base64Binary"/> </xs:sequence> <xs:attribute name="Type" type="xs:QName" use="required"/> </xs:complexType>

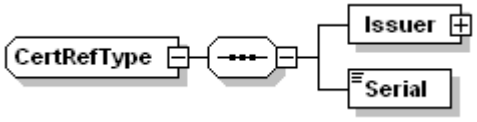
10.2.10.1 element CAAnswerType/Value

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:base64Binary**
properties	isRef 0 content simple
source	<xs:element name="Value" type="xs:base64Binary"/>

10.2.11 complexType CertificatePoliciesType

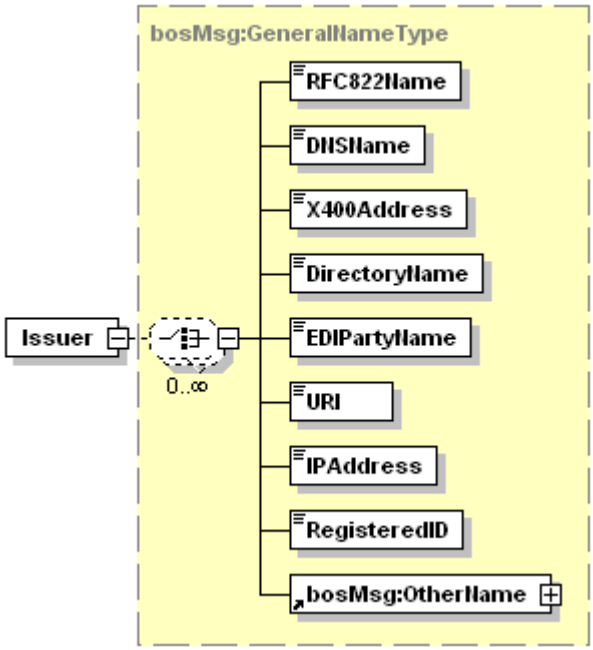
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:PolicyInformation**
used by	element **CertificatePolicies**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="CertificatePoliciesType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:PolicyInformation" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.12 complexType CertRefType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#

children	**Issuer** **Serial**
used by	elements **CertRef** **SigningForType/CertRef**
source	<xs:complexType name="CertRefType"> <xs:sequence> <xs:element name="Issuer" type="bosMsg:GeneralNameType"/> <xs:element name="Serial" type="xs:integer"/> </xs:sequence> </xs:complexType>

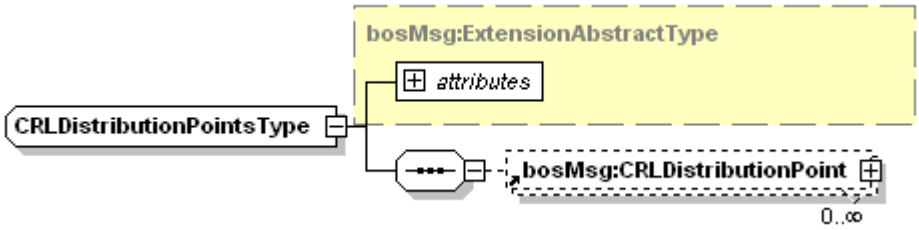
10.2.12.1 element CertRefType/Issuer

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralNameType**
properties	isRef 0 content complex
children	**RFC822Name** **DNSName** **X400Address** **DirectoryName** **EDIPartyName** **URI** **IPAddress** **RegisteredID** **bosMsg:OtherName**
source	<xs:element name="Issuer" type="bosMsg:GeneralNameType"/>

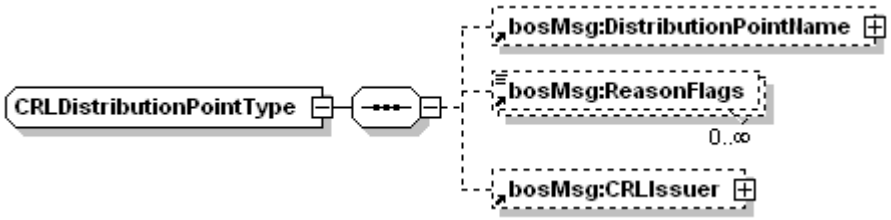
10.2.12.2 element CertRefType/Serial

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="Serial" type="xs:integer"/>

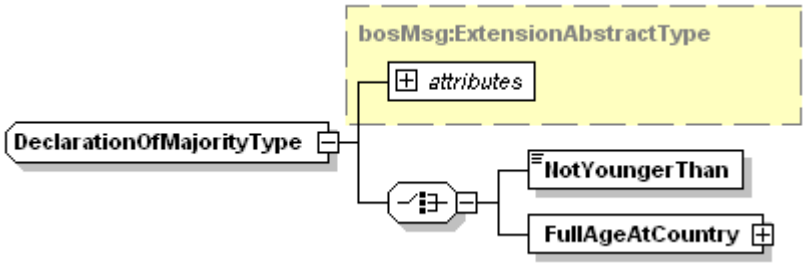
10.2.13 complexType CRLDistributionPointsType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:CRLDistributionPoint**
used by	element **CRLDistributionPoints**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="CRLDistributionPointsType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:CRLDistributionPoint" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.14 complexType CRLDistributionPointType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**bosMsg:DistributionPointName** **bosMsg:ReasonFlags** **bosMsg:CRLIssuer**
used by	element **CRLDistributionPoint**
source	<xs:complexType name="CRLDistributionPointType"> <xs:sequence> <xs:element ref="bosMsg:DistributionPointName" minOccurs="0"/> <xs:element ref="bosMsg:ReasonFlags" minOccurs="0" maxOccurs="unbounded"/> <xs:element ref="bosMsg:CRLIssuer" minOccurs="0"/> </xs:sequence> </xs:complexType>

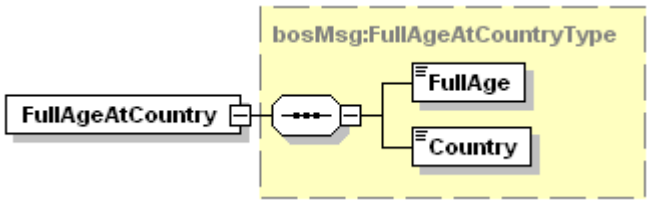
10.2.15 complexType DeclarationOfMajorityType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**NotYoungerThan** **FullAgeAtCountry**
used by	element **DeclarationOfMajority**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="DeclarationOfMajorityType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:choice> <xs:element name="NotYoungerThan" type="xs:integer"/> <xs:element name="FullAgeAtCountry" type="bosMsg:FullAgeAtCountryType"/> </xs:choice> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.15.1 element DeclarationOfMajorityType/NotYoungerThan

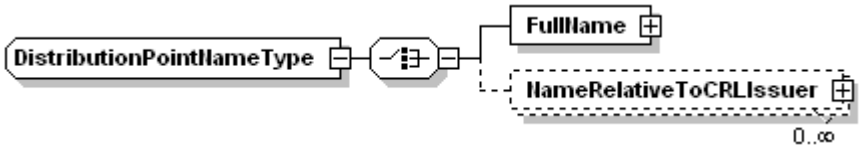
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="NotYoungerThan" type="xs:integer"/>

10.2.15.2 element DeclarationOfMajorityType/FullAgeAtCountry

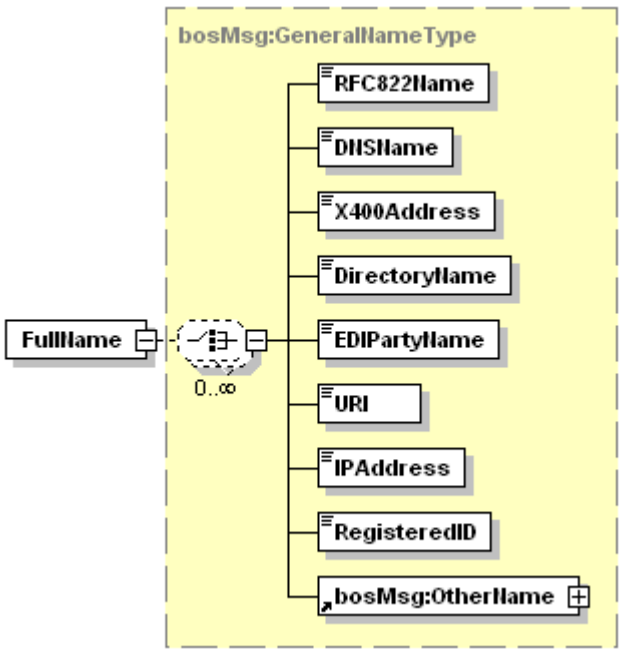
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:FullAgeAtCountryType**
properties	isRef 0 content complex

children	**FullAge Country**
source	<xs:element name="FullAgeAtCountry" type="bosMsg:FullAgeAtCountryType"/>

10.2.16 complexType DistributionPointNameType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**FullName NameRelativeToCRLIssuer**
used by	element **DistributionPointName**
source	<xs:complexType name="DistributionPointNameType"> <xs:choice> <xs:element name="FullName" type="bosMsg:GeneralNameType"/> <xs:element name="NameRelativeToCRLIssuer" type="bosMsg:RelativeDistinguishedNameType" minOccurs="0" maxOccurs="unbounded"/> <!--<xs:element name="FullName" ref="bosMsg:GeneralNames"/>--> <!--<xs:element name="NameRelativeToCRLIssuer" ref="bosMsg:RelativeDistinguishedName" minOccurs="0" maxOccurs="unbounded"/>--> </xs:choice> </xs:complexType>

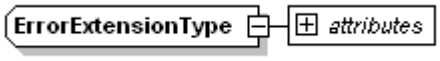
10.2.16.1 element DistributionPointNameType/FullName

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralNameType**
properties	isRef 0 content complex
children	**RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName**
source	<xs:element name="FullName" type="bosMsg:GeneralNameType"/>

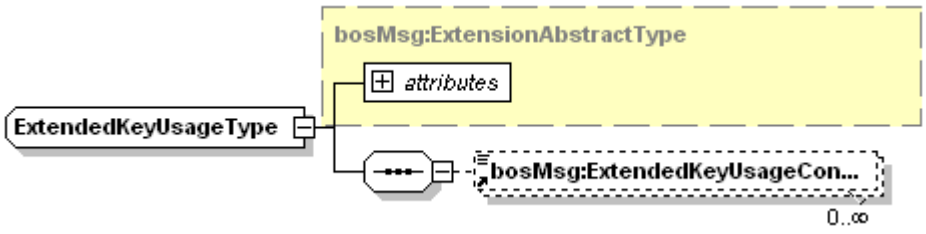
10.2.16.2 element DistributionPointNameType/NameRelativeToCRLIssuer

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:RelativeDistinguishedNameType**
properties	isRef 0 content complex
attributes	Name Type Use Default Fixed Annotation Type **xs:string** Value **xs:string**
source	<xs:element name="NameRelativeToCRLIssuer" type="bosMsg:RelativeDistinguishedNameType" minOccurs="0" maxOccurs="unbounded"/>

10.2.17 complexType ErrorExtensionType

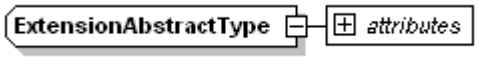
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
used by	element **ErrorExtension**
attributes	Name Type Use Default Fixed Annotation Reason **bosMsg:reasonType**
source	<xs:complexType name="ErrorExtensionType"> <xs:attribute name="Reason" type="bosMsg:reasonType"/> </xs:complexType>

10.2.18 complexType ExtendedKeyUsageType

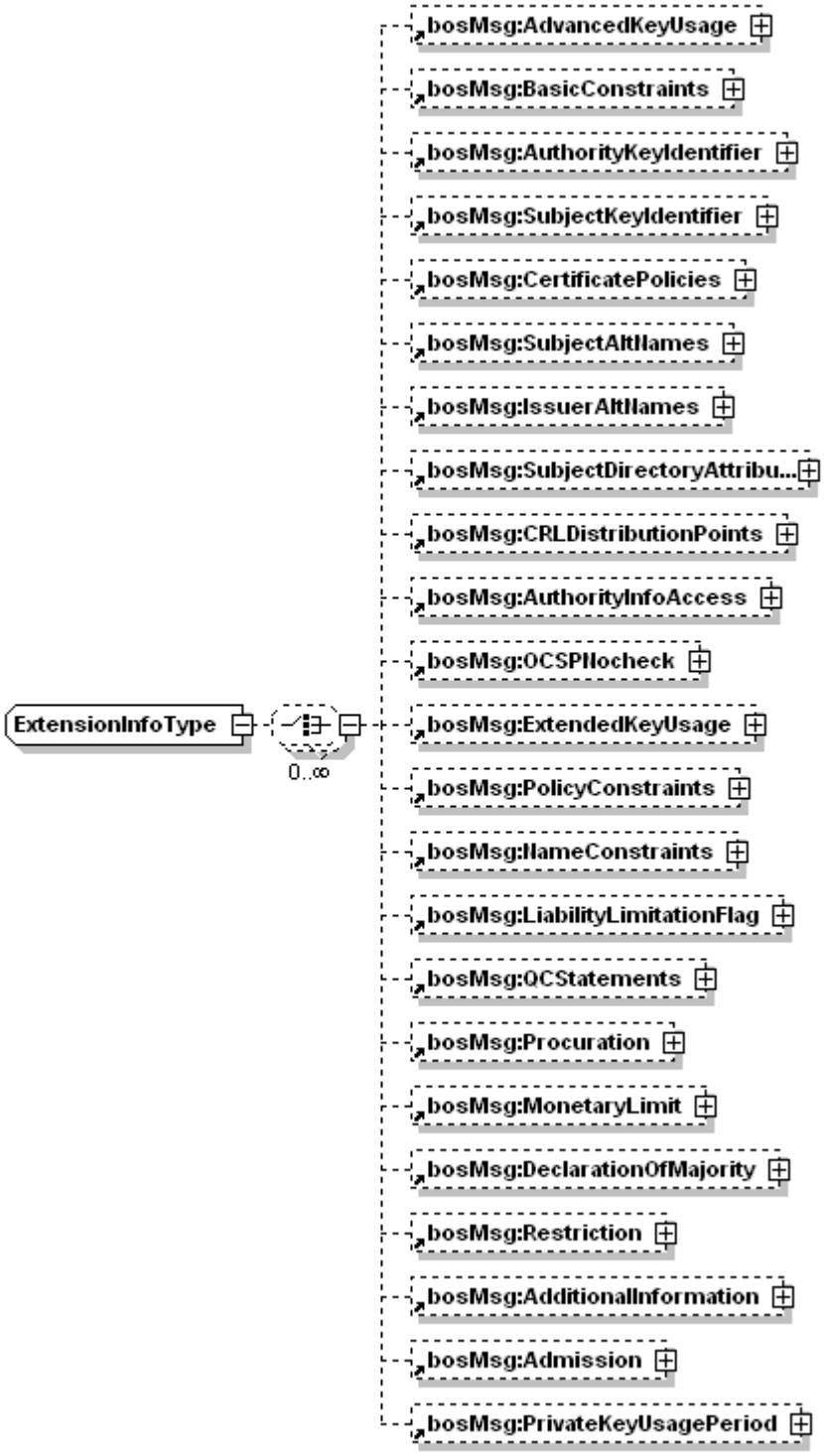
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:ExtendedKeyUsageContent**
used by	element **ExtendedKeyUsage**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="ExtendedKeyUsageType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence>

```
      <xs:element ref="bosMsg:ExtendedKeyUsageContent" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:extension>
 </xs:complexContent>
</xs:complexType>
```

10.2.19 complexType ExtensionAbstractType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
properties	abstract true
used by	complexTypes **AdditionalInformationType** **AdmissionType** **AdvancedKeyUsageType** **AuthorityInfoAccessType** **AuthorityKeyIdentifierType** **BasicConstraintsType** **CertificatePoliciesType** **CRLDistributionPointsType** **DeclarationOfMajorityType** **ExtendedKeyUsageType** **IssuerAltNamesType** **LiabilityLimitationFlagType** **MonetaryLimitType** **NameConstraintsType** **OCSPNocheckType** **PolicyConstraintsType** **PrivateKeyUsagePeriodType** **ProcurationType** **QCStatementsType** **RestrictionType** **SubjectAltNamesType** **SubjectDirectoryAttributesType** **SubjectKeyIdentifierType**
attributes	Name: Critical; Type: **xs:boolean**; Use: optional; Default: ; Fixed: ; Annotation:
source	`<xs:complexType name="ExtensionAbstractType" abstract="true"> <xs:attribute name="Critical" type="xs:boolean" use="optional"/> </xs:complexType>`

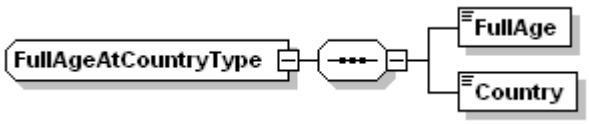
10.2.20 complexType ExtensionInfoType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
properties	mixed true
children	bosMsg:AdvancedKeyUsage bosMsg:BasicConstraints bosMsg:AuthorityKeyIdentifier bosMsg:SubjectKeyIdentifier bosMsg:CertificatePolicies bosMsg:SubjectAltNames bosMsg:IssuerAltNames bosMsg:SubjectDirectoryAttributes bosMsg:CRLDistributionPoints bosMsg:AuthorityInfoAccess bosMsg:OCSPNocheck bosMsg:ExtendedKeyUsage bosMsg:PolicyConstraints bosMsg:NameConstraints bosMsg:LiabilityLimitationFlag bosMsg:QCStatements bosMsg:Procuration bosMsg:MonetaryLimit bosMsg:DeclarationOfMajority bosMsg:Restriction bosMsg:AdditionalInformation bosMsg:Admission bosMsg:PrivateKeyUsagePeriod
used by	element ExtensionInfo

source
```
<xs:complexType name="ExtensionInfoType" mixed="true">
 <xs:choice minOccurs="0" maxOccurs="unbounded">
  <xs:element ref="bosMsg:AdvancedKeyUsage" minOccurs="0"/>
  <xs:element ref="bosMsg:BasicConstraints" minOccurs="0"/>
  <xs:element ref="bosMsg:AuthorityKeyIdentifier" minOccurs="0"/>
  <xs:element ref="bosMsg:SubjectKeyIdentifier" minOccurs="0"/>
  <xs:element ref="bosMsg:CertificatePolicies" minOccurs="0"/>
  <xs:element ref="bosMsg:SubjectAltNames" minOccurs="0"/>
  <xs:element ref="bosMsg:IssuerAltNames" minOccurs="0"/>
  <xs:element ref="bosMsg:SubjectDirectoryAttributes" minOccurs="0"/>
  <xs:element ref="bosMsg:CRLDistributionPoints" minOccurs="0"/>
  <xs:element ref="bosMsg:AuthorityInfoAccess" minOccurs="0"/>
  <xs:element ref="bosMsg:OCSPNocheck" minOccurs="0"/>
  <xs:element ref="bosMsg:ExtendedKeyUsage" minOccurs="0"/>
  <xs:element ref="bosMsg:PolicyConstraints" minOccurs="0"/>
  <xs:element ref="bosMsg:NameConstraints" minOccurs="0"/>
  <xs:element ref="bosMsg:LiabilityLimitationFlag" minOccurs="0"/>
  <xs:element ref="bosMsg:QCStatements" minOccurs="0"/>
  <xs:element ref="bosMsg:Procuration" minOccurs="0"/>
  <xs:element ref="bosMsg:MonetaryLimit" minOccurs="0"/>
  <xs:element ref="bosMsg:DeclarationOfMajority" minOccurs="0"/>
  <xs:element ref="bosMsg:Restriction" minOccurs="0"/>
  <xs:element ref="bosMsg:AdditionalInformation" minOccurs="0"/>
  <xs:element ref="bosMsg:Admission" minOccurs="0"/>
  <xs:element ref="bosMsg:PrivateKeyUsagePeriod" minOccurs="0"/>
 </xs:choice>
</xs:complexType>
```

10.2.21 complexType FullAgeAtCountryType

diagram



namespace http://www.bos-bremen.de/2003/11/bosMsgExt#

children **FullAge** **Country**

used by element **DeclarationOfMajorityType/FullAgeAtCountry**

source
```
<xs:complexType name="FullAgeAtCountryType">
 <xs:sequence>
  <xs:element name="FullAge" type="xs:boolean"/>
  <xs:element name="Country" type="xs:string"/>
 </xs:sequence>
</xs:complexType>
```

10.2.21.1 element FullAgeAtCountryType/FullAge

diagram

namespace http://www.bos-bremen.de/2003/11/bosMsgExt#

type **xs:boolean**

properties isRef 0
content simple

source
```
<xs:element name="FullAge" type="xs:boolean"/>
```

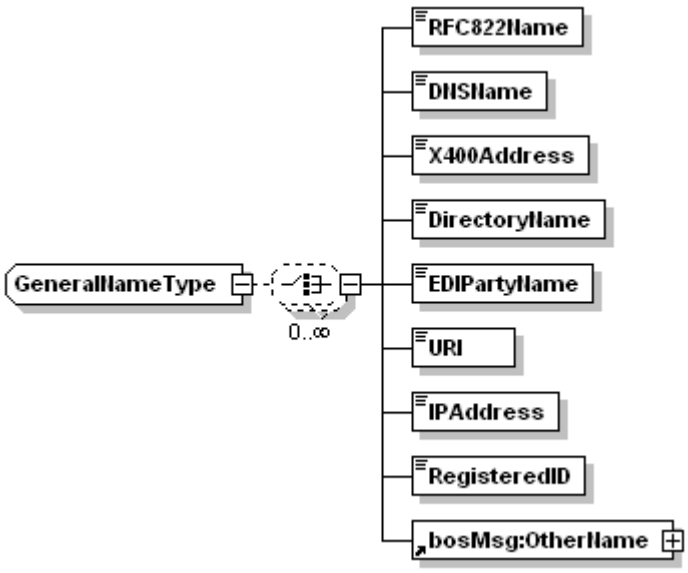
10.2.21.2 element FullAgeAtCountryType/Country

diagram

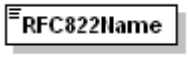
namespace http://www.bos-bremen.de/2003/11/bosMsgExt#

type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="Country" type="xs:string"/>

10.2.22 complexType GeneralNameType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName
used by	elements AccessLocation AdmissionType/AdmissionAuthority AdmissionsType/AdmissionAuthority AuthorityCertIssuer GeneralSubtreeType/base CRLIssuer DistributionPointNameType/FullName GeneralNames CertRefType/Issuer SigningForType/ThirdPerson
source	<xs:complexType name="GeneralNameType"> <xs:choice minOccurs="0" maxOccurs="unbounded"> <xs:element name="RFC822Name" type="xs:string"/> <xs:element name="DNSName" type="xs:string"/> <xs:element name="X400Address" type="xs:string"/> <xs:element name="DirectoryName" type="xs:string"/> <xs:element name="EDIPartyName" type="xs:string"/> <xs:element name="URI" type="xs:string"/> <xs:element name="IPAddress" type="xs:string"/> <xs:element name="RegisteredID" type="xs:string"/> <xs:element ref="bosMsg:OtherName"/> </xs:choice> </xs:complexType>

10.2.22.1 element GeneralNameType/RFC822Name

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="RFC822Name" type="xs:string"/>

10.2.22.2 element GeneralNameType/DNSName

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="DNSName" type="xs:string"/>

10.2.22.3 element GeneralNameType/X400Address

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="X400Address" type="xs:string"/>

10.2.22.4 element GeneralNameType/DirectoryName

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="DirectoryName" type="xs:string"/>

10.2.22.5 element GeneralNameType/EDIPartyName

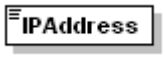
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="EDIPartyName" type="xs:string"/>

10.2.22.6 element GeneralNameType/URI

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0

	content simple
source	<xs:element name="URI" type="xs:string"/>

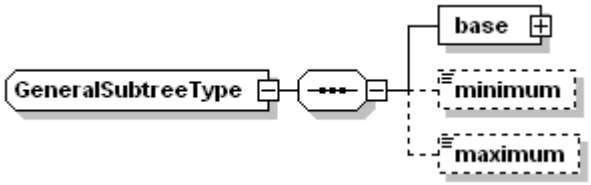
10.2.22.7 element GeneralNameType/IPAddress

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="IPAddress" type="xs:string"/>

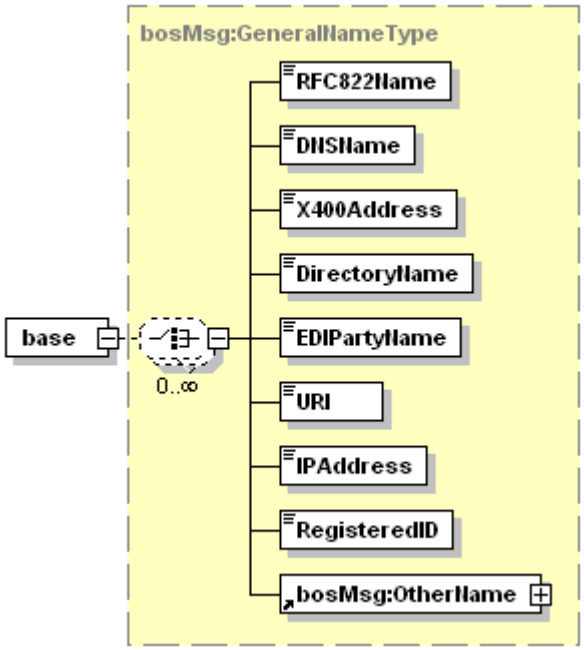
10.2.22.8 element GeneralNameType/RegisteredID

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="RegisteredID" type="xs:string"/>

10.2.23 complexType GeneralSubtreeType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**base minimum maximum**
used by	elements **NameConstraintsType/ExcludedSubtree NameConstraintsType/PermittedSubtree**
source	<xs:complexType name="GeneralSubtreeType"> <xs:sequence> <xs:element name="base" type="bosMsg:GeneralNameType"/> <xs:element name="minimum" type="xs:integer" minOccurs="0"/> <xs:element name="maximum" type="xs:integer" minOccurs="0"/> </xs:sequence> </xs:complexType>

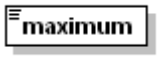
10.2.23.1 element GeneralSubtreeType/base

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralNameType**
properties	isRef 0 content complex
children	RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName
source	<xs:element name="base" type="bosMsg:GeneralNameType"/>

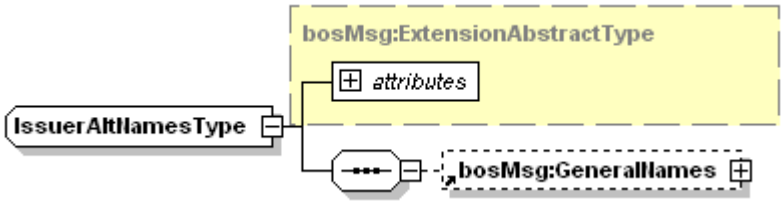
10.2.23.2 element GeneralSubtreeType/minimum

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="minimum" type="xs:integer" minOccurs="0"/>

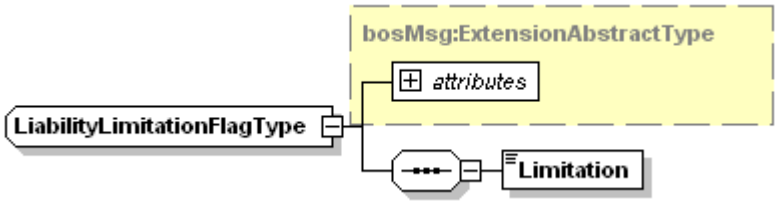
10.2.23.3 element GeneralSubtreeType/maximum

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="maximum" type="xs:integer" minOccurs="0"/>

10.2.24 complexType IssuerAltNamesType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:GeneralNames**
used by	element **IssuerAltNames**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="IssuerAltNamesType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:GeneralNames" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

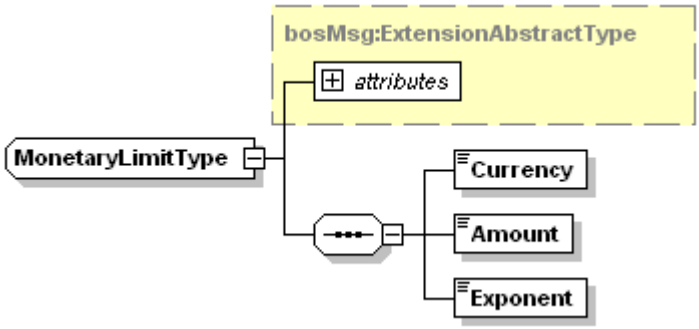
10.2.25 complexType LiabilityLimitationFlagType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**Limitation**
used by	element **LiabilityLimitationFlag**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="LiabilityLimitationFlagType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="Limitation" type="xs:boolean"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.25.1 element LiabilityLimitationFlagType/Limitation

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:boolean**
properties	isRef 0 content simple
source	<xs:element name="Limitation" type="xs:boolean"/>

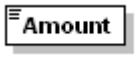
10.2.26 complexType MonetaryLimitType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**Currency Amount Exponent**
used by	element **MonetaryLimit**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="MonetaryLimitType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="Currency" type="xs:string"/> <xs:element name="Amount" type="xs:integer"/> <xs:element name="Exponent" type="xs:integer"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

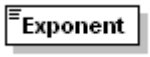
10.2.26.1 element MonetaryLimitType/Currency

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="Currency" type="xs:string"/>

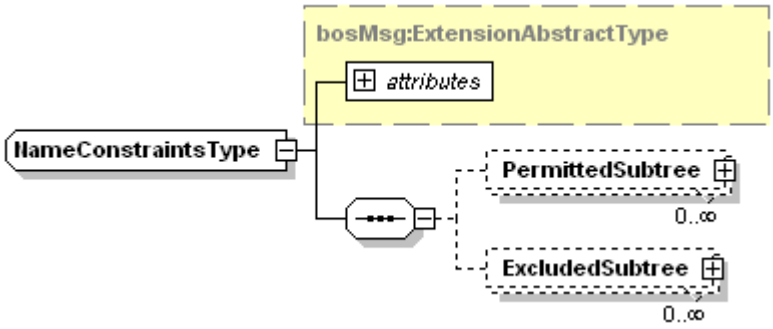
10.2.26.2 element MonetaryLimitType/Amount

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="Amount" type="xs:integer"/>

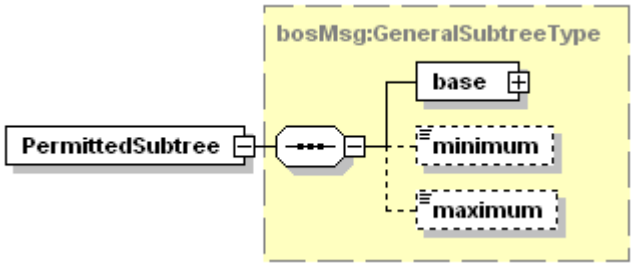
10.2.26.3 element MonetaryLimitType/Exponent

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="Exponent" type="xs:integer"/>

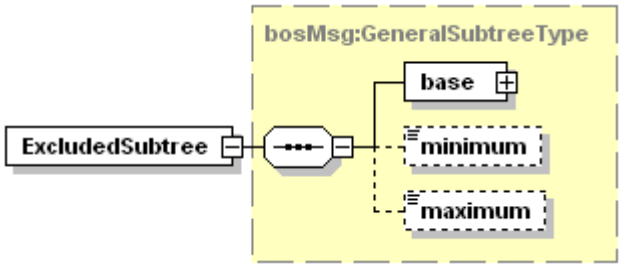
10.2.27 complexType NameConstraintsType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**PermittedSubtree** **ExcludedSubtree**
used by	element **NameConstraints**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="NameConstraintsType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="PermittedSubtree" type="bosMsg:GeneralSubtreeType" minOccurs="0" maxOccurs="unbounded"/> <xs:element name="ExcludedSubtree" type="bosMsg:GeneralSubtreeType" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

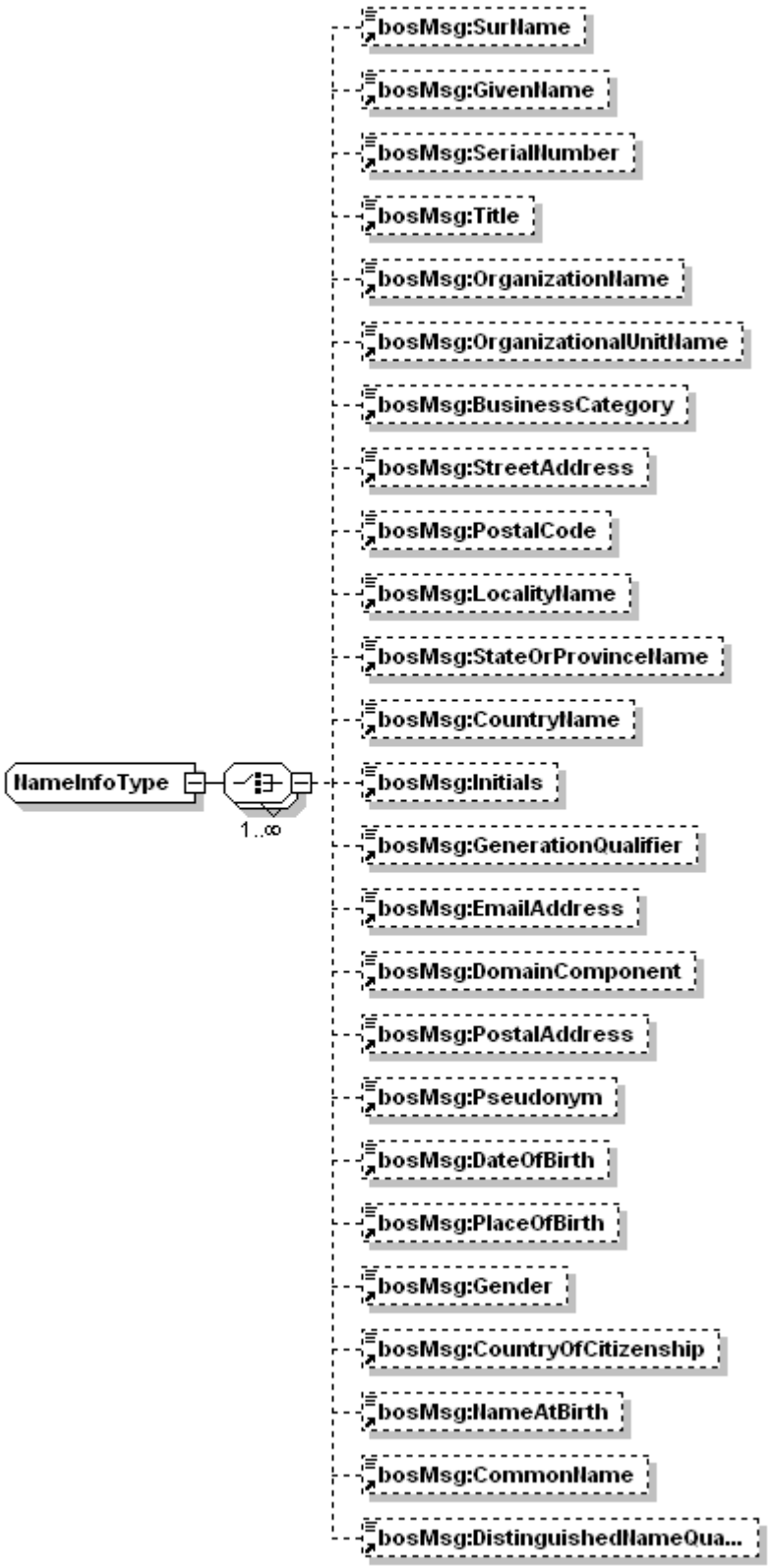
10.2.27.1 element NameConstraintsType/PermittedSubtree

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralSubtreeType**
properties	isRef 0 content complex
children	**base minimum maximum**
source	<xs:element name="PermittedSubtree" type="bosMsg:GeneralSubtreeType" minOccurs="0" maxOccurs="unbounded"/>

10.2.27.2 element NameConstraintsType/ExcludedSubtree

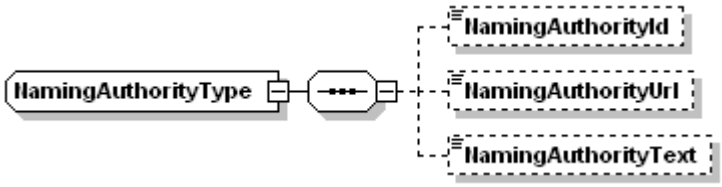
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralSubtreeType**
properties	isRef 0 content complex
children	**base minimum maximum**
source	<xs:element name="ExcludedSubtree" type="bosMsg:GeneralSubtreeType" minOccurs="0" maxOccurs="unbounded"/>

10.2.28 complexType NameInfoType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
properties	mixed true
children	bosMsg:SurName bosMsg:GivenName bosMsg:SerialNumber bosMsg:Title bosMsg:OrganizationName bosMsg:OrganizationalUnitName bosMsg:BusinessCategory bosMsg:StreetAddress bosMsg:PostalCode bosMsg:LocalityName bosMsg:StateOrProvinceName bosMsg:CountryName bosMsg:Initials bosMsg:GenerationQualifier bosMsg:EmailAddress

	bosMsg:DomainComponent bosMsg:PostalAddress bosMsg:Pseudonym bosMsg:DateOfBirth bosMsg:PlaceOfBirth bosMsg:Gender bosMsg:CountryOfCitizenship bosMsg:NameAtBirth bosMsg:CommonName bosMsg:DistinguishedNameQualifier
used by	elements **IssuerInfo SubjectInfo**
source	<xs:complexType name="NameInfoType" mixed="true"> <xs:choice maxOccurs="unbounded"> <xs:element ref="bosMsg:SurName" minOccurs="0"/> <xs:element ref="bosMsg:GivenName" minOccurs="0"/> <xs:element ref="bosMsg:SerialNumber" minOccurs="0"/> <xs:element ref="bosMsg:Title" minOccurs="0"/> <xs:element ref="bosMsg:OrganizationName" minOccurs="0"/> <xs:element ref="bosMsg:OrganizationalUnitName" minOccurs="0"/> <xs:element ref="bosMsg:BusinessCategory" minOccurs="0"/> <xs:element ref="bosMsg:StreetAddress" minOccurs="0"/> <xs:element ref="bosMsg:PostalCode" minOccurs="0"/> <xs:element ref="bosMsg:LocalityName" minOccurs="0"/> <xs:element ref="bosMsg:StateOrProvinceName" minOccurs="0"/> <xs:element ref="bosMsg:CountryName" minOccurs="0"/> <xs:element ref="bosMsg:Initials" minOccurs="0"/> <xs:element ref="bosMsg:GenerationQualifier" minOccurs="0"/> <xs:element ref="bosMsg:EmailAddress" minOccurs="0"/> <xs:element ref="bosMsg:DomainComponent" minOccurs="0"/> <xs:element ref="bosMsg:PostalAddress" minOccurs="0"/> <xs:element ref="bosMsg:Pseudonym" minOccurs="0"/> <xs:element ref="bosMsg:DateOfBirth" minOccurs="0"/> <xs:element ref="bosMsg:PlaceOfBirth" minOccurs="0"/> <xs:element ref="bosMsg:Gender" minOccurs="0"/> <xs:element ref="bosMsg:CountryOfCitizenship" minOccurs="0"/> <xs:element ref="bosMsg:NameAtBirth" minOccurs="0"/> <xs:element ref="bosMsg:CommonName" minOccurs="0"/> <xs:element ref="bosMsg:DistinguishedNameQualifier" minOccurs="0"/> <!--<xs:element ref="bosMsg:LiabilityLimitationFlag" minOccurs="0" maxOccurs="1"/>--> <!--<xs:element ref="bosMsg:DateOfCertGen" minOccurs="0" maxOccurs="1"/>--> <!--<xs:element ref="bosMsg:QcCompliance" minOccurs="0" maxOccurs="1"/>--> </xs:choice> </xs:complexType>

10.2.29 complexType NamingAuthorityType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**NamingAuthorityId NamingAuthorityUrl NamingAuthorityText**
used by	elements **AdmissionsType/NamingAuthority ProfessionInfoType/NamingAuthority**
source	<xs:complexType name="NamingAuthorityType"> <xs:sequence> <xs:element name="NamingAuthorityId" type="xs:string" minOccurs="0"/> <xs:element name="NamingAuthorityUrl" type="xs:string" minOccurs="0"/> <xs:element name="NamingAuthorityText" type="xs:string" minOccurs="0"/> </xs:sequence> </xs:complexType>

10.2.29.1 element NamingAuthorityType/NamingAuthorityId

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**

properties	isRef 0 content simple
source	<xs:element name="NamingAuthorityId" type="xs:string" minOccurs="0"/>

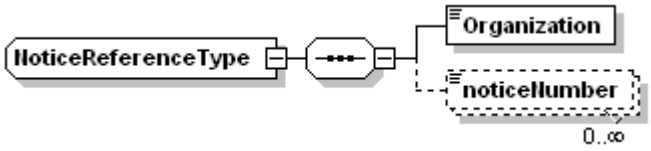
10.2.29.2 element NamingAuthorityType/NamingAuthorityUrl

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="NamingAuthorityUrl" type="xs:string" minOccurs="0"/>

10.2.29.3 element NamingAuthorityType/NamingAuthorityText

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="NamingAuthorityText" type="xs:string" minOccurs="0"/>

10.2.30 complexType NoticeReferenceType

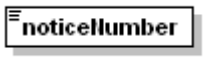
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**Organization** **noticeNumber**
used by	element **NoticeReference**
source	<xs:complexType name="NoticeReferenceType"> <xs:sequence> <xs:element name="Organization" type="xs:string"/> <xs:element name="noticeNumber" type="xs:integer" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:complexType>

10.2.30.1 element NoticeReferenceType/Organization

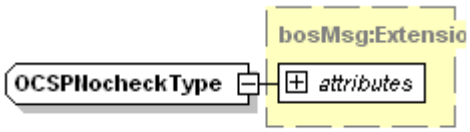
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple

source	<xs:element name="Organization" type="xs:string"/>

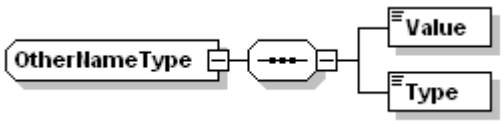
10.2.30.2 element NoticeReferenceType/noticeNumber

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="noticeNumber" type="xs:integer" minOccurs="0" maxOccurs="unbounded"/>

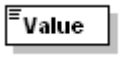
10.2.31 complexType OCSPNocheckType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
used by	element **OCSPNocheck**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="OCSPNocheckType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"/> </xs:complexContent> </xs:complexType>

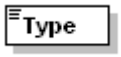
10.2.31.1 complexType OtherNameType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**Value** **Type**
used by	element **OtherName**
source	<xs:complexType name="OtherNameType"> <xs:sequence> <xs:element name="Value" type="xs:string"/> <xs:element name="Type" type="xs:string"/> </xs:sequence> </xs:complexType>

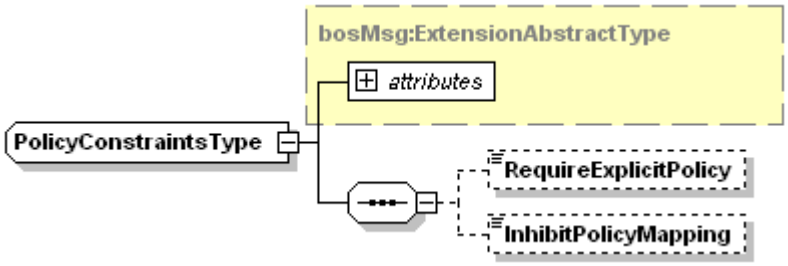
10.2.31.2 element OtherNameType/Value

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="Value" type="xs:string"/>

10.2.31.3 element OtherNameType/Type

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="Type" type="xs:string"/>

10.2.32 complexType PolicyConstraintsType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**RequireExplicitPolicy** **InhibitPolicyMapping**
used by	element **PolicyConstraints**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="PolicyConstraintsType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="RequireExplicitPolicy" type="xs:integer" minOccurs="0"/> <xs:element name="InhibitPolicyMapping" type="xs:integer" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

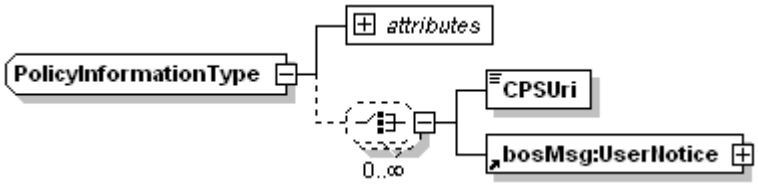
10.2.32.1 element PolicyConstraintsType/RequireExplicitPolicy

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="RequireExplicitPolicy" type="xs:integer" minOccurs="0"/>

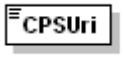
10.2.32.2 element PolicyConstraintsType/InhibitPolicyMapping

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="InhibitPolicyMapping" type="xs:integer" minOccurs="0"/>

10.2.33 complexType PolicyInformationType

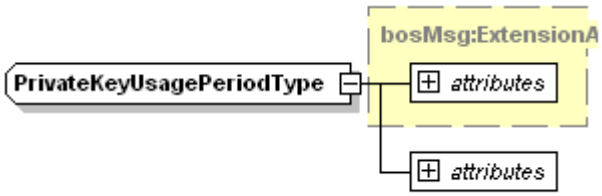
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**CPSUri** **bosMsg:UserNotice**
used by	element **PolicyInformation**
attributes	Name Type Use Default Fixed Annotation PolicyIdentifier **xs:string**
source	<xs:complexType name="PolicyInformationType"> <xs:choice minOccurs="0" maxOccurs="unbounded"> <xs:element name="CPSUri" type="xs:string"/> <xs:element ref="bosMsg:UserNotice"/> </xs:choice> <xs:attribute name="PolicyIdentifier" type="xs:string"/> </xs:complexType>

10.2.33.1 element PolicyInformationType/CPSUri

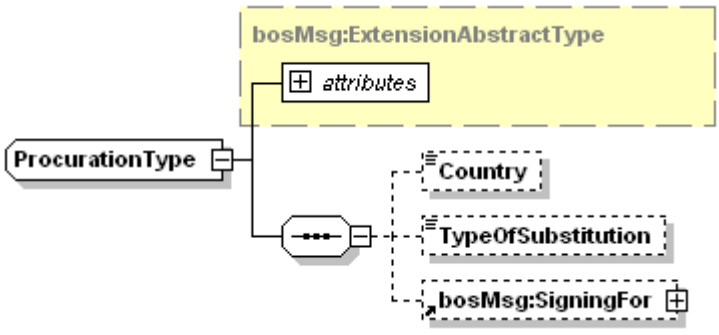
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple

source	<xs:element name="CPSUri" type="xs:string"/>

10.2.34 complexType PrivateKeyUsagePeriodType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
used by	element **PrivateKeyUsagePeriod**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional NotBefore **xs:dateTime** NotAfter **xs:dateTime**
source	<xs:complexType name="PrivateKeyUsagePeriodType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:attribute name="NotBefore" type="xs:dateTime"/> <xs:attribute name="NotAfter" type="xs:dateTime"/> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.35 complexType ProcurationType

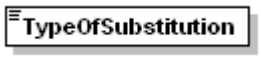
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**Country TypeOfSubstitution bosMsg:SigningFor**
used by	element **Procuration**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="ProcurationType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="Country" type="xs:string" minOccurs="0"/>

```
      <xs:element name="TypeOfSubstitution" type="xs:string" minOccurs="0"/>
      <xs:element ref="bosMsg:SigningFor" minOccurs="0"/>
    </xs:sequence>
  </xs:extension>
 </xs:complexContent>
</xs:complexType>
```

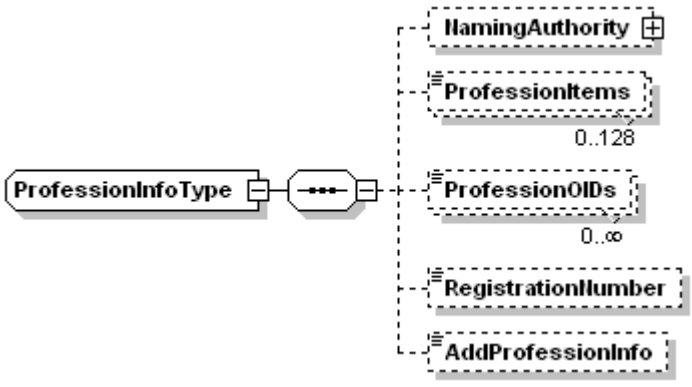
10.2.35.1 element ProcurationType/Country

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	`<xs:element name="Country" type="xs:string" minOccurs="0"/>`

10.2.35.2 element ProcurationType/TypeOfSubstitution

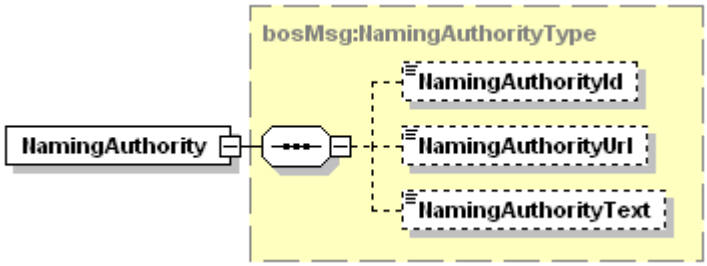
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	`<xs:element name="TypeOfSubstitution" type="xs:string" minOccurs="0"/>`

10.2.36 complexType ProfessionInfoType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**NamingAuthority ProfessionItems ProfessionOIDs RegistrationNumber AddProfessionInfo**
used by	element **AdmissionsType/ProfessionInfo**

source	`<xs:complexType name="ProfessionInfoType">`
	`<xs:sequence>`
	`<xs:element name="NamingAuthority" type="bosMsg:NamingAuthorityType" minOccurs="0"/>`
	`<xs:element name="ProfessionItems" type="xs:string" minOccurs="0" maxOccurs="128"/>`
	`<xs:element name="ProfessionOIDs" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>`
	`<xs:element name="RegistrationNumber" type="xs:string" minOccurs="0"/>`
	`<xs:element name="AddProfessionInfo" type="xs:string" minOccurs="0"/>`
	`</xs:sequence>`
	`</xs:complexType>`

10.2.36.1 element ProfessionInfoType/NamingAuthority

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:NamingAuthorityType**
properties	isRef 0 content complex
children	**NamingAuthorityId NamingAuthorityUrl NamingAuthorityText**
source	<xs:element name="NamingAuthority" type="bosMsg:NamingAuthorityType" minOccurs="0"/>

10.2.36.2 element ProfessionInfoType/ProfessionItems

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="ProfessionItems" type="xs:string" minOccurs="0" maxOccurs="128"/>

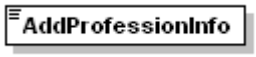
10.2.36.3 element ProfessionInfoType/ProfessionOIDs

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="ProfessionOIDs" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>

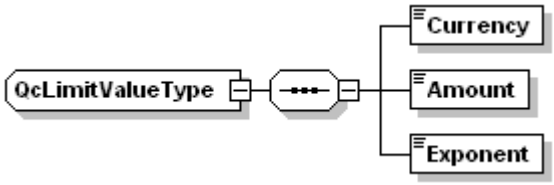
10.2.36.4 element ProfessionInfoType/RegistrationNumber

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="RegistrationNumber" type="xs:string" minOccurs="0"/>

10.2.36.5 element ProfessionInfoType/AddProfessionInfo

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="AddProfessionInfo" type="xs:string" minOccurs="0"/>

10.2.37 complexType QcLimitValueType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**Currency** **Amount** **Exponent**
used by	element **QcLimitValue**
source	<xs:complexType name="QcLimitValueType"> <xs:sequence> <xs:element name="Currency" type="xs:string"/> <xs:element name="Amount" type="xs:integer"/> <xs:element name="Exponent" type="xs:integer"/> </xs:sequence> </xs:complexType>

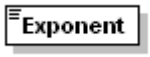
10.2.37.1 element QcLimitValueType/Currency

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="Currency" type="xs:string"/>

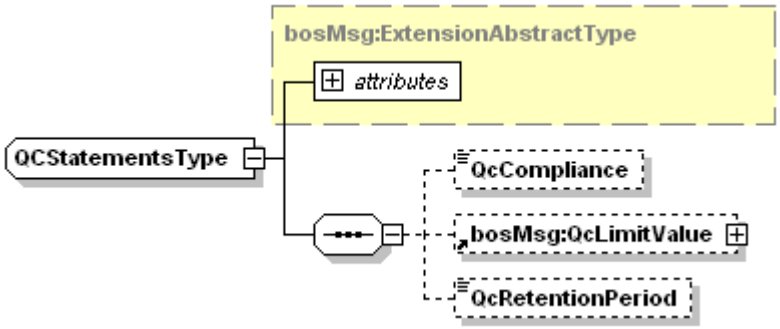
10.2.37.2 element QcLimitValueType/Amount

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="Amount" type="xs:integer"/>

10.2.37.3 element QcLimitValueType/Exponent

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="Exponent" type="xs:integer"/>

10.2.38 complexType QCStatementsType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**QcCompliance bosMsg:QcLimitValue QcRetentionPeriod**
used by	element **QCStatements**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="QCStatementsType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="QcCompliance" type="xs:boolean" minOccurs="0"/> <xs:element ref="bosMsg:QcLimitValue" minOccurs="0"/> <xs:element name="QcRetentionPeriod" type="xs:integer" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.38.1 element QCStatementsType/QcCompliance

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:boolean**
properties	isRef 0 content simple
source	<xs:element name="QcCompliance" type="xs:boolean" minOccurs="0"/>

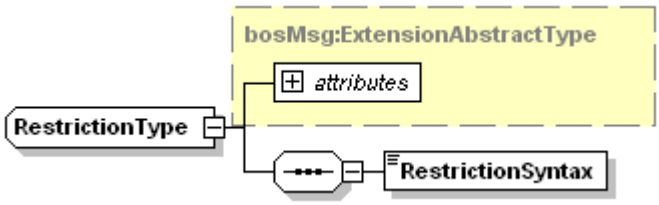
10.2.38.2 element QCStatementsType/QcRetentionPeriod

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:integer**
properties	isRef 0 content simple
source	<xs:element name="QcRetentionPeriod" type="xs:integer" minOccurs="0"/>

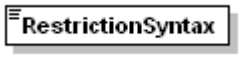
10.2.39 complexType RelativeDistinguishedNameType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
used by	elements **DistributionPointNameType/NameRelativeToCRLIssuer** **RelativeDistinguishedName**
attributes	Name Type Use Default Fixed Annotation Type **xs:string** Value **xs:string**
source	<xs:complexType name="RelativeDistinguishedNameType"> <xs:attribute name="Type" type="xs:string"/> <xs:attribute name="Value" type="xs:string"/> </xs:complexType>

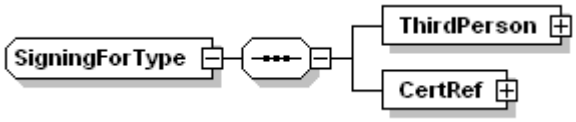
10.2.40 complexType RestrictionType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**RestrictionSyntax**
used by	element **Restriction**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="RestrictionType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element name="RestrictionSyntax" type="xs:string"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

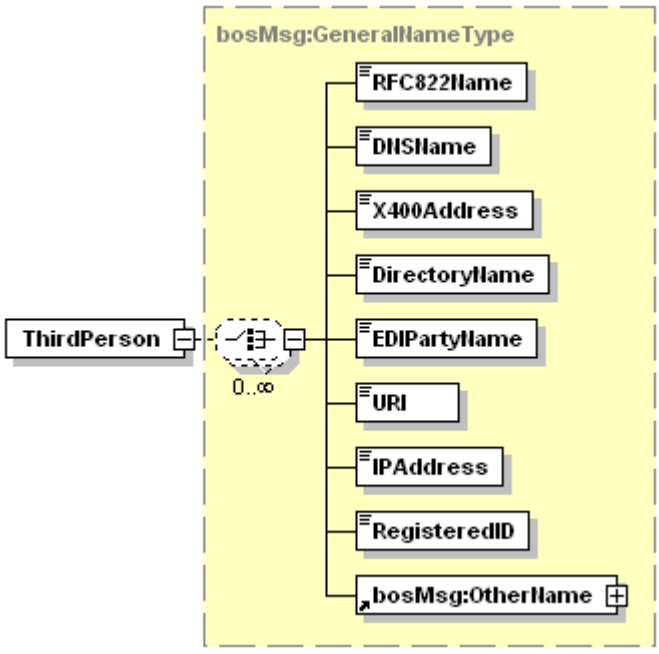
10.2.40.1 element RestrictionType/RestrictionSyntax

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="RestrictionSyntax" type="xs:string"/>

10.2.41 complexType SigningForType

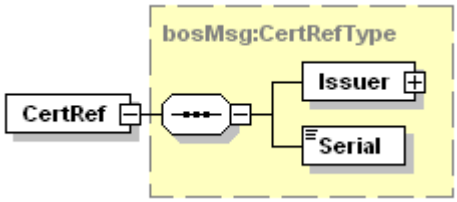
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**ThirdPerson** **CertRef**
used by	element **SigningFor**
source	<xs:complexType name="SigningForType"> <xs:sequence> <xs:element name="ThirdPerson" type="bosMsg:GeneralNameType"/> <xs:element name="CertRef" type="bosMsg:CertRefType"/> </xs:sequence> </xs:complexType>

10.2.41.1 element SigningForType/ThirdPerson

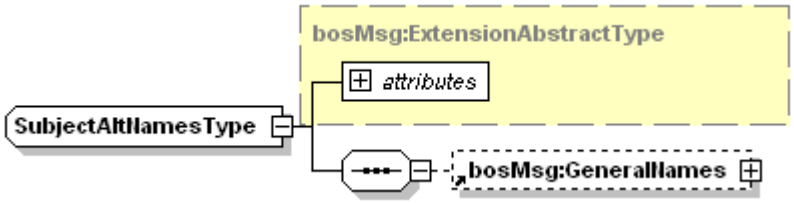
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:GeneralNameType**
properties	isRef 0 content complex

children	**RFC822Name DNSName X400Address DirectoryName EDIPartyName URI IPAddress RegisteredID bosMsg:OtherName**
source	<xs:element name="ThirdPerson" type="bosMsg:GeneralNameType"/>

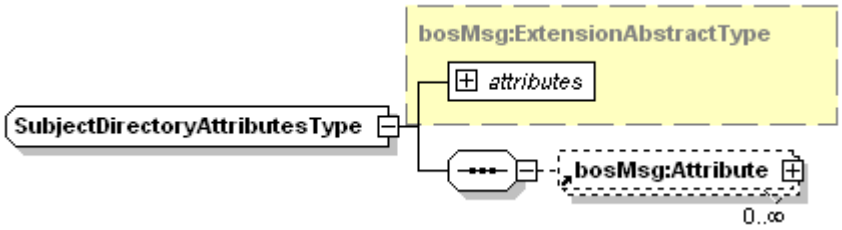
10.2.41.2 element SigningForType/CertRef

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**bosMsg:CertRefType**
properties	isRef 0 content complex
children	**Issuer Serial**
source	<xs:element name="CertRef" type="bosMsg:CertRefType"/>

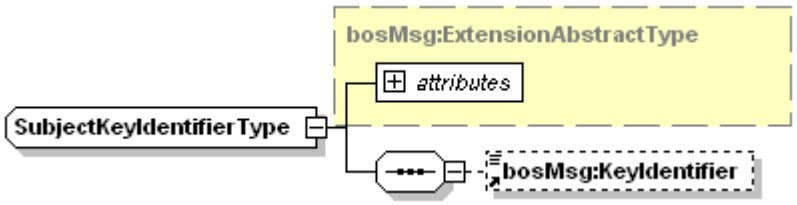
10.2.42 complexType SubjectAltNamesType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:GeneralNames**
used by	element **SubjectAltNames**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="SubjectAltNamesType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:GeneralNames" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

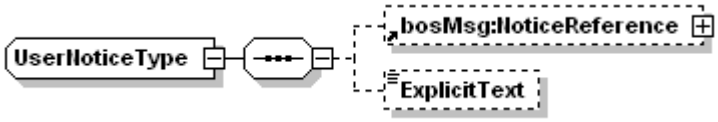
10.2.43 complexType SubjectDirectoryAttributesType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:Attribute**
used by	element **SubjectDirectoryAttributes**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="SubjectDirectoryAttributesType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:Attribute" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.44 complexType SubjectKeyIdentifierType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:ExtensionAbstractType**
properties	base bosMsg:ExtensionAbstractType
children	**bosMsg:KeyIdentifier**
used by	element **SubjectKeyIdentifier**
attributes	Name Type Use Default Fixed Annotation Critical **xs:boolean** optional
source	<xs:complexType name="SubjectKeyIdentifierType"> <xs:complexContent> <xs:extension base="bosMsg:ExtensionAbstractType"> <xs:sequence> <xs:element ref="bosMsg:KeyIdentifier" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

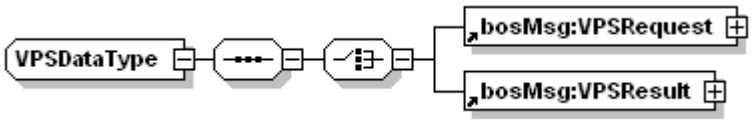
10.2.45 complexType UserNoticeType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**bosMsg:NoticeReference** **ExplicitText**
used by	element **UserNotice**
source	<xs:complexType name="UserNoticeType"> <xs:sequence> <xs:element ref="bosMsg:NoticeReference" minOccurs="0"/> <xs:element name="ExplicitText" type="xs:string" minOccurs="0"/> </xs:sequence> </xs:complexType>

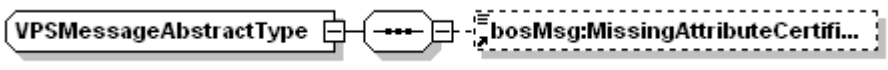
10.2.45.1 element UserNoticeType/ExplicitText

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	**xs:string**
properties	isRef 0 content simple
source	<xs:element name="ExplicitText" type="xs:string" minOccurs="0"/>

10.2.46 complexType VPSDataType

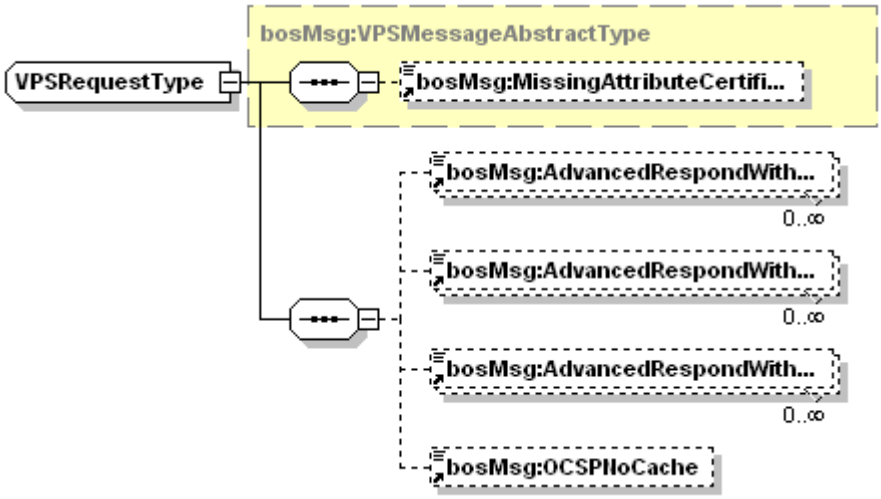
diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
children	**bosMsg:VPSRequest** **bosMsg:VPSResult**
used by	element **VPSData**
source	<xs:complexType name="VPSDataType"> <xs:sequence> <xs:choice> <xs:element ref="bosMsg:VPSRequest"/> <xs:element ref="bosMsg:VPSResult"/> </xs:choice> </xs:sequence> </xs:complexType>

10.2.47 complexType VPSMessageAbstractType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
properties	abstract true
children	**bosMsg:MissingAttributeCertificate**

used by	complexTypes **VPSRequestType** **VPSResultType**
source	<xs:complexType name="VPSMessageAbstractType" abstract="true"> <xs:sequence> <xs:element ref="bosMsg:MissingAttributeCertificate" minOccurs="0"/> </xs:sequence> </xs:complexType>

10.2.48 complexType VPSRequestType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:VPSMessageAbstractType**
properties	base bosMsg:VPSMessageAbstractType
children	**bosMsg:MissingAttributeCertificate** **bosMsg:AdvancedRespondWithSubjectInfo** **bosMsg:AdvancedRespondWithIssuerInfo** **bosMsg:AdvancedRespondWithExtensionInfo** **bosMsg:OCSPNoCache**
used by	element **VPSRequest**
source	<xs:complexType name="VPSRequestType"> <xs:complexContent> <xs:extension base="bosMsg:VPSMessageAbstractType"> <xs:sequence> <xs:element ref="bosMsg:AdvancedRespondWithSubjectInfo" minOccurs="0" maxOccurs="unbounded"/> <xs:element ref="bosMsg:AdvancedRespondWithIssuerInfo" minOccurs="0" maxOccurs="unbounded"/> <xs:element ref="bosMsg:AdvancedRespondWithExtensionInfo" minOccurs="0" maxOccurs="unbounded"/> <xs:element ref="bosMsg:OCSPNoCache" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.2.49 complexType VPSResultType

diagram	
namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	extension of **bosMsg:VPSMessageAbstractType**
properties	base bosMsg:VPSMessageAbstractType
children	**bosMsg:MissingAttributeCertificate bosMsg:SubjectInfo bosMsg:IssuerInfo bosMsg:ExtensionInfo bosMsg:CertificateRevocationReason bosMsg:ValidateScheme bosMsg:ErrorExtension bosMsg:accredited bosMsg:CertQuality**
used by	element **VPSResult**
source	<xs:complexType name="VPSResultType"> <xs:complexContent> <xs:extension base="bosMsg:VPSMessageAbstractType"> <xs:sequence> <xs:element ref="bosMsg:SubjectInfo" minOccurs="0"/> <xs:element ref="bosMsg:IssuerInfo" minOccurs="0"/> <xs:element ref="bosMsg:ExtensionInfo" minOccurs="0"/> <xs:element ref="bosMsg:CertificateRevocationReason" minOccurs="0"/> <xs:element ref="bosMsg:ValidateScheme" minOccurs="0"/> <xs:element ref="bosMsg:ErrorExtension" minOccurs="0" maxOccurs="unbounded"/> <xs:element ref="bosMsg:accredited"/> <xs:element ref="bosMsg:CertQuality" minOccurs="0"/> </xs:sequence> </xs:extension> </xs:complexContent> </xs:complexType>

10.3 Simple Types

10.3.1 simpleType AdvancedRespondWithExtensionType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	element **AdvancedRespondWithExtensionInfo**
facets	enumeration bosMsg:BasicConstraints enumeration bosMsg:AdvancedKeyUsage

	enumeration bosMsg:AuthorityKeyIdentifier enumeration bosMsg:SubjectKeyIdentifier enumeration bosMsg:PrivateKeyUsagePeriod enumeration bosMsg:CertificatePolicies enumeration bosMsg:SubjectAltNames enumeration bosMsg:IssuerAltNames enumeration bosMsg:SubjectDirectoryAttributes enumeration bosMsg:CRLDistributionPoints enumeration bosMsg:AuthorityInfoAccess enumeration bosMsg:OCSPNocheck
source	<xs:simpleType name="AdvancedRespondWithExtensionType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:BasicConstraints"/> <xs:enumeration value="bosMsg:AdvancedKeyUsage"/> <xs:enumeration value="bosMsg:AuthorityKeyIdentifier"/> <xs:enumeration value="bosMsg:SubjectKeyIdentifier"/> <xs:enumeration value="bosMsg:PrivateKeyUsagePeriod"/> <xs:enumeration value="bosMsg:CertificatePolicies"/> <xs:enumeration value="bosMsg:SubjectAltNames"/> <xs:enumeration value="bosMsg:IssuerAltNames"/> <xs:enumeration value="bosMsg:SubjectDirectoryAttributes"/> <xs:enumeration value="bosMsg:CRLDistributionPoints"/> <xs:enumeration value="bosMsg:AuthorityInfoAccess"/> <xs:enumeration value="bosMsg:OCSPNocheck"/> </xs:restriction> </xs:simpleType>

10.3.2 simpleType AdvancedRespondWithNameType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	elements **AdvancedRespondWithIssuerInfo** **AdvancedRespondWithSubjectInfo**
facets	enumeration bosMsg:SurName enumeration bosMsg:GivenName enumeration bosMsg:SerialNumber enumeration bosMsg:Title enumeration bosMsg:OrganizationName enumeration bosMsg:OrganizationalUnitName enumeration bosMsg:BusinessCategory enumeration bosMsg:StreetAddress enumeration bosMsg:PostalCode enumeration bosMsg:LocalityName enumeration bosMsg:StateOrProvinceName enumeration bosMsg:CountryName enumeration bosMsg:Initials enumeration bosMsg:GenerationQualifier enumeration bosMsg:EmailAddress enumeration bosMsg:DomainComponent enumeration bosMsg:PostalAddress enumeration bosMsg:Pseudonym enumeration bosMsg:DateOfBirth enumeration bosMsg:PlaceOfBirth enumeration bosMsg:Gender enumeration bosMsg:CountryOfCitizenship enumeration bosMsg:CountryOfResidence enumeration bosMsg:NameAtBirth enumeration bosMsg:CommonName enumeration bosMsg:DistinguishedNameQualifier
source	<xs:simpleType name="AdvancedRespondWithNameType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:SurName"/> <xs:enumeration value="bosMsg:GivenName"/> <xs:enumeration value="bosMsg:SerialNumber"/> <xs:enumeration value="bosMsg:Title"/> <xs:enumeration value="bosMsg:OrganizationName"/> <xs:enumeration value="bosMsg:OrganizationalUnitName"/> <xs:enumeration value="bosMsg:BusinessCategory"/> <xs:enumeration value="bosMsg:StreetAddress"/> <xs:enumeration value="bosMsg:PostalCode"/>

```
    <xs:enumeration value="bosMsg:LocalityName"/>
    <xs:enumeration value="bosMsg:StateOrProvinceName"/>
    <xs:enumeration value="bosMsg:CountryName"/>
    <xs:enumeration value="bosMsg:Initials"/>
    <xs:enumeration value="bosMsg:GenerationQualifier"/>
    <xs:enumeration value="bosMsg:EmailAddress"/>
    <xs:enumeration value="bosMsg:DomainComponent"/>
    <xs:enumeration value="bosMsg:PostalAddress"/>
    <xs:enumeration value="bosMsg:Pseudonym"/>
    <xs:enumeration value="bosMsg:DateOfBirth"/>
    <xs:enumeration value="bosMsg:PlaceOfBirth"/>
    <xs:enumeration value="bosMsg:Gender"/>
    <xs:enumeration value="bosMsg:CountryOfCitizenship"/>
    <xs:enumeration value="bosMsg:CountryOfResidence"/>
    <xs:enumeration value="bosMsg:NameAtBirth"/>
    <xs:enumeration value="bosMsg:CommonName"/>
    <xs:enumeration value="bosMsg:DistinguishedNameQualifier"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.3 simpleType CertificateRevocationReasonType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	element **CertificateRevocationReason**
facets	enumeration bosMsg:Unspecified enumeration bosMsg:KeyCompromised enumeration bosMsg:CaCompromised enumeration bosMsg:AffiliationChanged enumeration bosMsg:Superseded enumeration bosMsg:CessationOfOperation enumeration bosMsg:CertificateHold enumeration bosMsg:RemoveFromCRL enumeration bosMsg:None enumeration bosMsg:PrivilegeWithdrawn enumeration bosMsg:AACompromise
source	<xs:simpleType name="CertificateRevocationReasonType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:Unspecified"/> <xs:enumeration value="bosMsg:KeyCompromised"/> <xs:enumeration value="bosMsg:CaCompromised"/> <xs:enumeration value="bosMsg:AffiliationChanged"/> <xs:enumeration value="bosMsg:Superseded"/> <xs:enumeration value="bosMsg:CessationOfOperation"/> <xs:enumeration value="bosMsg:CertificateHold"/> <xs:enumeration value="bosMsg:RemoveFromCRL"/> <xs:enumeration value="bosMsg:None"/> <xs:enumeration value="bosMsg:PrivilegeWithdrawn"/> <xs:enumeration value="bosMsg:AACompromise"/> </xs:restriction> </xs:simpleType>

10.3.4 simpleType certQualityType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	element **CertQuality**
facets	enumeration bosMsg:advanced enumeration bosMsg:qualified enumeration bosMsg:accredited enumeration bosMsg:pki1verwaltung
source	<xs:simpleType name="certQualityType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:advanced"/>

```
    <xs:enumeration value="bosMsg:qualified"/>
    <xs:enumeration value="bosMsg:accredited"/>
    <xs:enumeration value="bosMsg:pki1verwaltung"/>
  </xs:restriction>
</xs:simpleType>
```

10.3.5 simpleType ExtendedKeyUsageContentType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	element **ExtendedKeyUsageContent**
facets	enumeration bosMsg:ServerAuthentication enumeration bosMsg:ClientAuthentication enumeration bosMsg:CodeSigning enumeration bosMsg:EmailProtection enumeration bosMsg:TimeStamping enumeration bosMsg:OCSPSigning
source	<xs:simpleType name="ExtendedKeyUsageContentType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:ServerAuthentication"/> <xs:enumeration value="bosMsg:ClientAuthentication"/> <xs:enumeration value="bosMsg:CodeSigning"/> <xs:enumeration value="bosMsg:EmailProtection"/> <xs:enumeration value="bosMsg:TimeStamping"/> <xs:enumeration value="bosMsg:OCSPSigning"/> </xs:restriction> </xs:simpleType>

10.3.6 simpleType KeyUsageContentType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	element **KeyUsageContent**
facets	enumeration bosMsg:DigitalSignature enumeration bosMsg:NonRepudation enumeration bosMsg:KeyEncipherment enumeration bosMsg:DataEncipherment enumeration bosMsg:KeyAgreement enumeration bosMsg:KeyCertSign enumeration bosMsg:CRLSign enumeration bosMsg:EncipherOnly enumeration bosMsg:DecipherOnly
source	<xs:simpleType name="KeyUsageContentType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:DigitalSignature"/> <xs:enumeration value="bosMsg:NonRepudation"/> <xs:enumeration value="bosMsg:KeyEncipherment"/> <xs:enumeration value="bosMsg:DataEncipherment"/> <xs:enumeration value="bosMsg:KeyAgreement"/> <xs:enumeration value="bosMsg:KeyCertSign"/> <xs:enumeration value="bosMsg:CRLSign"/> <xs:enumeration value="bosMsg:EncipherOnly"/> <xs:enumeration value="bosMsg:DecipherOnly"/> </xs:restriction> </xs:simpleType>

10.3.7 simpleType ReasonFlagsType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	element **ReasonFlags**

facets	enumeration bosMsg:Unused enumeration bosMsg:KeyCompromised enumeration bosMsg:CaCompromised enumeration bosMsg:AffiliationChanged enumeration bosMsg:Superseded enumeration bosMsg:CessationOfOperation enumeration bosMsg:CertificateHold
source	<xs:simpleType name="ReasonFlagsType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:Unused"/> <xs:enumeration value="bosMsg:KeyCompromised"/> <xs:enumeration value="bosMsg:CaCompromised"/> <xs:enumeration value="bosMsg:AffiliationChanged"/> <xs:enumeration value="bosMsg:Superseded"/> <xs:enumeration value="bosMsg:CessationOfOperation"/> <xs:enumeration value="bosMsg:CertificateHold"/> </xs:restriction> </xs:simpleType>

10.3.8 simpleType reasonType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	attribute **ErrorExtensionType/@Reason**
facets	enumeration bosMsg:MissingParentCertificate enumeration bosMsg:AttributeCertificateDontMatch enumeration bosMsg:OpaqueClientDataToLong enumeration bosMsg:TrustCenterNotReachable enumeration bosMsg:WrongCertificateFormat enumeration bosMsg:UnknownCA enumeration bosMsg:WrongTimeInstant enumeration bosMsg:SignatureKeyToShort
source	<xs:simpleType name="reasonType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:MissingParentCertificate"/> <xs:enumeration value="bosMsg:AttributeCertificateDontMatch"/> <xs:enumeration value="bosMsg:OpaqueClientDataToLong"/> <xs:enumeration value="bosMsg:TrustCenterNotReachable"/> <xs:enumeration value="bosMsg:WrongCertificateFormat"/> <xs:enumeration value="bosMsg:UnknownCA"/> <xs:enumeration value="bosMsg:WrongTimeInstant"/> <xs:enumeration value="bosMsg:SignatureKeyToShort"/> </xs:restriction> </xs:simpleType>

10.3.9 simpleType ValidateSchemeType

namespace	http://www.bos-bremen.de/2003/11/bosMsgExt#
type	restriction of **xs:QName**
used by	element **ValidateScheme**
facets	enumeration bosMsg:LOCAL enumeration bosMsg:OCSP enumeration bosMsg:CRL enumeration bosMsg:CRL_LDAP enumeration bosMsg:LDAP
source	<xs:simpleType name="ValidateSchemeType"> <xs:restriction base="xs:QName"> <xs:enumeration value="bosMsg:LOCAL"/> <xs:enumeration value="bosMsg:OCSP"/> <xs:enumeration value="bosMsg:CRL"/> <xs:enumeration value="bosMsg:CRL_LDAP"/> <xs:enumeration value="bosMsg:LDAP"/> </xs:restriction>

	</xs:simpleType>

11 Verzeichnisse

11.1 Referenzdokumente

Folgende Dokumente enthalten weitere Informationen zum OCSP/CRL-Relay:

Dokument	Inhalt
XKMS2 [27]	Beschreibt das vom OCSP/CRL-Relay verwendete XKMS-Protokoll
XKMS2-Bindings (Part2)[28]	Beschreibt den Transport von XKMS-Anfragen über das SOAP-Protokoll
SOAP1.2 [29]	Spezifikation des SOAP1.2-Protokolls
XML Signature[30]	Spezifikation des verwendeten XML-Signatur Formats
XML Encryption[31]	Spezifikation des XML-Encryption Formats
JMS1.1 [32]	Spezifikation des Java Messaging Service
ISO 8601 [33]	ISO-Standard zu Datums- und Zeitformaten
Releasebeschreibung des OCSP/CRL-Relays	Beschreibung der Funktionalitäten OCSP/CRL-Relays
SCHNITTKERN	VPS-Schnittstellenbeschreibung-Kernsystem
Feinzept für das OCSP/CRL-Relay	Beschreibung der Softwarearchitektur des OCSP/CRL-Relays
Fachkonzept der Virtuellen Poststelle	Fachkonzept in der finalen Version 2.3.1 vom 28. April 2003
Kernsystem der Virtuellen Poststelle: Schnittstellenbeschreibung	Spezifikation der externen Schnittstellen des VPS-Kernsystems
DV-Grobkonzept der Virtuellen Poststelle	DV-Grobkonzept in Version 3.6.1 vom 15. Dezember 2003
ISIS-MTT[34]	Spezifikation der der Public-Private Key Infrastruktur
ISIS-MTT SigG-Profil[35]	Profilierung des ISIS-MTT Standards nach SigG, um die Anforderungen des SigG zu erfüllen.

Tabelle 13: Referenzdokumente

[27] http://www.w3.org/TR/2003/WD-xkms2-20030418/

[28] http://www.w3.org/TR/2003/WD-xkms2-bindings-20030418

[29] http://www.w3.org/TR/2003/REC-soap12-part1-20030624/

[30] http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[31] http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[32] http://java.sun.com/products/jms/

[33] http://www.w3.org/TR/NOTE-datetime

[34] http://www.t7-isis.de/ISIS-MTT/isis-mtt.html

[35] http://www.t7-isis.de/ISIS-MTT/isis-mtt.html

11.2 Abbildungen

11.3 Tabellen

11.4 Listings