



## Technische Dokumentation (TDoc)

### Einheitliche Elster - Datenschnittstelle XML

Bezeichnung	Verfahren: <b>ELSTER</b> Produkt: <b>Einheitliche Elster-Datenschnittstelle XML</b> Auftragnehmer: Bay LfSt - Dienststelle München -	
Verfahrensmanager	Roland Krebs	
Produktmanager	RB	
Dokumentverantwortlicher	RB	
Version	4.2.14	
Erstellt am	Donnerstag, 10. Oktober 2013	
Zuletzt geändert	2023-06-05	
Bearbeitungszustand	<input checked="" type="checkbox"/>	in Bearbeitung Vorgelegt fertig gestellt



## Änderungsnachweis

Änderung		Geänderte Kapitel	Beschreibung der Änderung	Autor	Zustand
Datum	Version				
2015-06-01	4.2.5		Anpassung an Version 11	RB	
2016-08-26	4.2.6		Feldwertbeschreibungen in Schema überführt.	RB	
2017-03-13	4.2.8		Kleine Korrekturen	RB	
2018-07-13	4.2.9		Neue URL eingetragen Einschränkung auf ISO-8859-15 und Ankündigung von UTF-8	RB	
2019-08-04	4.2.10		Wechsel auf UTF-8 Aufnehmen der Zeichensatzbeschränkung	RB	
2020-07-30	4.2.12		Entfernen veralteter Hinweise auf iso-8859-15 und kleinere Korrekturen Verschlüsselungsarten PKCS#7v1.5 und PKCS#7v1.5enveloped auf deprecated gesetzt.	RB	
2020-08-28	4.2.13		Beschreibung von Verfahren / Datenart in Kapitel 3.4 angepasst.	RB	
2023-06-05	4.2.14		Beschreibung Testmerker angepasst	TA	

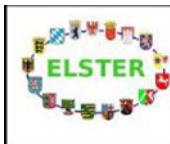


## Inhaltsverzeichnis

Änderungsnachweis .....	2
Inhaltsverzeichnis.....	3
Abbildungsverzeichnis .....	5
Referenzliste .....	5
1    Einleitung .....	5
1.1    Übersicht Datenaufbau .....	6
1.2    Übersicht Ablauf .....	6
1.2.1    Das Online-Verfahren .....	7
1.2.2    Das Offline-Verfahren .....	8
2    Standards und Technik .....	8
2.1 XML-Encoding.....	8
2.2 Zeichenumfang .....	8
2.3 Namespace .....	9
2.4    Authentifizierung.....	9
2.4.1    DatenTeil-Authentifizierung (Signaturdaten werden im TransferHeader abgelegt).....	10
2.5 Kompression .....	11
2.6 Verschlüsselung.....	11
2.7 Kommunikation .....	12
2.7.1    Protokoll: https .....	12
3    Datenstrukturen - Header .....	13
3.1    Spezifikation .....	13
3.2    TransferHeader (THeader).....	13
3.2.1    Allgemeines .....	13
3.2.2 Aktuelle Version des THeaders.....	13
3.2.3 Elemente im Transferheader.....	13
3.2.4 Aufbau der XML-Struktur des TransferHeaders .....	13
3.2.4.1 Datenlieferung an die Clearingstelle .....	13
3.2.4.2 Datenrücklieferung von der Clearingstelle an den Hersteller.....	14
3.3    NutzdatenHeader (NHeader) .....	16
3.3.1    Allgemeines .....	16
3.3.2 Elemente im Nutzdatenheader.....	16
3.3.3 Aufbau der XML-Struktur des NutzdatenHeaders .....	16
3.3.3.1 Datenlieferung an die Clearingstelle .....	16
3.3.3.2 Datenrücklieferung von der Clearingstelle an den Hersteller (nur bei Online-Verfahren) .....	16
3.4    Unterstützte Feldinhalte und Dienste .....	17
3.4.1    Gültige Feldinhalte im TransferHeader.....	17
3.4.1.1 Auflistung der möglichen Kombinationen der Elementinhalte von „Verfahren“, „DatenArt“ und „Vorgang“ .....	18



3.4.2	Gültige Feldinhalte im NutzdatenHeader:.....	18
3.5	Sammellieferungen (nur teilweise unterstützt!) .....	19
4	Nutzdaten .....	20
5	Beispiele .....	20
5.1	Daten mit geplanter Authentifizierung VOR der Verschlüsselung.....	20
5.2	Daten mit Authentifizierung NACH der Verschlüsselung .....	22
5.3	RSA-OAEP-verschlüsselte Daten .....	23
6	Abkürzungsverzeichnis .....	26



## Abbildungsverzeichnis

Abb. 1: ElsterXML-Daten ..... 6

## Referenzliste

elster11_bisNH_extern.xsd	/Schemas
headerbasis000003.xsd	
headerbasis_datenarten.xsd	
headerbasis_datentypen.xsd	
headerbasis_verfahren.xsd	
headerelemente.xsd	/Schemas/header
ndh000011.xsd	
ndh000010_intern.xsd	
th000011_extern.xsd	
th000011_intern.xsd	

## 1 Einleitung

In diesem Dokument wird die einheitliche XML-Datenschnittstelle für alle ELSTER-Verfahren beschrieben. Sie stellt die universelle Schnittstelle für alle Verfahren dar. Diese Schnittstelle beinhaltet den allgemeinen Aufbau des ElsterXMLs, sowie die Kommunikation mit der ELSTER-Clearingstelle, die die Daten entgegennimmt.

Die Elster Datensatzkoordination ist ausschließlich für die Freischaltung des Datenweges zuständig.

Spezielle Informationen zu den einzelnen Fachverfahren (z.B. ElsterLohn) die unterstützt werden, finden Sie im Downloadbereich von ELSTER ([www.elster.de](http://www.elster.de) – Entwickler – Mitglieder – Download – Schnittstellenbeschreibungen)

**Hinweise** sind in einem grünen Kasten hervorgehoben.

Wichtige Änderungen zum vorhergehenden Dokument sind gelb markiert.

Bestimmte Elementinhalte des ElsterXML müssen komprimiert, verschlüsselt und je nach Fachverfahren ggf. authentifiziert werden (siehe Tz. 3). Die versandfertigen Daten werden dann an die Clearingstelle übermittelt.

Zur Unterstützung der Realisierung wird eine Clientkomponente ERiC (=Elster Rich Client) auf den Downloadseiten zur Verfügung gestellt. Mit Hilfe dieser Komponente kann das ElsterXML komprimiert, verschlüsselt, authentifiziert und mittels https versendet werden ([www.elster.de](http://www.elster.de) – Entwickler – Mitglieder – Download – ERiC)

Die Schnittstelle kann aber auch für einzelne Datenlieferungen vollkommen selbstständig entwickelt werden, ohne Verwendung der, von der Finanzverwaltung zur Verfügung gestellten Komponente (offene Schnittstelle). Eine Auflistung hierzu befindet sich in dem Dokument „Verzeichnis\_der\_Datenarten“

Unterstützung erhalten Sie in unserem Entwicklerforum [www.elster.de](http://www.elster.de) – Mitglieder – ElsterEntwickler – Forum, in dem Ihnen ein eigener Bereich zur Verfügung steht. Hier finden Sie z.B. Artikel zum Thema „HerstellerIDs und Testlauf“ oder „Viele Wege führen zu ELSTER“.



Um auf dem Laufenden zu bleiben können Sie einen ELSTER-Newsletter im Downloadbereich abonnieren. Dort finden Sie einen entsprechenden Link zum Bestellformular.

In diesem Dokument werden die einzelnen Felder der ElsterXML- Datenstruktur erläutert, sowie ggf. Formate festgelegt und mögliche Inhalte vorgegeben. Des Weiteren wird die Struktur des ElsterXMLs dargestellt.

## 1.1 Übersicht Datenaufbau

Es wird ein zum Teil verschlüsselter XML-Datensatz an die Server der Steuerverwaltung übermittelt. Dieser besteht aus TransferHeader (THeader), NutzdatenHeader (NHeader) sowie einer anwendungsspezifischen Datenstruktur (Nutzdaten, NDS) (Abb. 1).

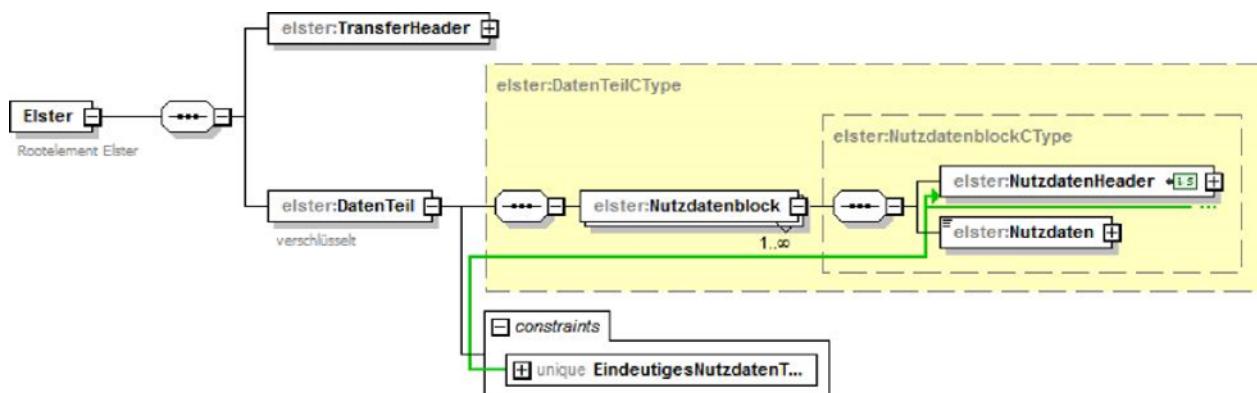


Abb. 1: ElsterXML-Daten

Der TransferHeader ist der XML-Datenteil, der weitestgehend unverschlüsselt bleibt. Er wird dem verschlüsselten Teil des XML-Datensatzes vorangestellt. Der TransferHeader enthält wichtige Informationen für die Verarbeitung der Daten in der Clearingstelle und für die Verteilung in die Bundesländer, außerdem kann er Rückgabemeldungen und Fehlermeldungen aufnehmen.

Innerhalb des verschlüsselten Teils des XML-Datensatzes befinden sich sowohl der NutzdatenHeader, der alle Informationen für die Verarbeitung des Datensatzes, sowie Rückgabemeldungen und Fehlermeldungen aufnehmen kann, als auch der eigentliche datentypabhängige Datensatz (Nutzdaten).

Es können grundsätzlich ein oder - bei Sammellieferungen - mehrere Nutzdatenblöcke vorkommen.

Das XML kann bzw. muss bei bestimmten Datenlieferungen authentifiziert werden. Die Authentifizierung erfolgt über den verschlüsselten, komprimierten, base64-Kodierten DatenTeil und wird im TransferHeader abgelegt (Vorgang: „send-Auth“). DieAuthentifizierung ist im getrennten Dokument „Einheitliche\_Datenschnittstelle\_XML\_Authentifizierung“ beschrieben.

Ob Authentifizierung unterstützt oder verlangt wird, steht im Dokument „Verzeichnis\_der\_Datenarten“.

## 1.2 Übersicht Ablauf

Die Daten werden von einem beliebigen Programm erzeugt, komprimiert, verschlüsselt, base64-kodiert, und ggf. authentifiziert. Danach werden die Daten an einen Server der Steuerverwaltung (Clearingstelle) versendet. Dieser entschlüsselt und verarbeitet je nach Datenart die Datenlieferung online (siehe Tz. 1.2.1) oder offline (siehe Tz. 1.2.2). Der Anwender erhält sofort eine Rückantwort ob die Daten erfolgreich übermittelt wurden. Der Rückweg ist analog.



Die Schnittstelle ist die XML-Struktur.

### 1.2.1 Das Online-Verfahren

Es werden ElsterXML-Daten an die Clearingstelle übermittelt, die Annahme der Daten wird online bestätigt oder Fehler angezeigt.

Im Erfolgsfall (keine Fehler sind aufgetreten) erhält der Client ein komplettes ElsterXML (incl. TransferHeader, NutzdatenHeader und Nutzdaten). Dieses ElsterXML beinhaltet die Daten der Lieferung, ergänzt um einige weitere Elemente. Der Anwender kann bei einem Online-Verfahren sicher sein, dass seine Daten entgegengenommen und verarbeitet wurden, wenn sowohl im TransferHeader, als auch im NutzdatenHeader unter <Rueckgabe> <Code> eine „0“ eingetragen ist.

Im Fehlerfall (Daten konnten nicht verarbeitet werden):

Es können Fehlermeldungen im TransferHeader oder im NutzdatenHeader auftreten.

- Es sind Fehler bei der Übermittlung oder grundsätzliche Strukturfehler aufgetreten 4 Fehlermeldung wird im TransferHeader zurückgeliefert. Das Element DatenTeil wird leer zurückgeliefert, d.h. es existiert kein NutzdatenHeader/Nutzdaten.
- Es sind Fehler, die die Nutzdaten betreffen, festgestellt worden 4 Rückgabewert im TransferHeader ist „0“, da die Übermittlung grundsätzlich erfolgreich war. Qualifizierter Rückgabewert (ungleich „0“) im NutzdatenHeader wird zurückgeliefert. Das Element Nutzdaten wird leer zurückgeliefert.

Beispiel RC - TransferHeader und NutzdatenHeader:

```
<RC>
<Rueckgabe>
  <Code>...</Code>
  <Text>...</Text>
</Rueckgabe>
<Stack>
  <Code>...</Code>
  <Text>...</Text>
</Stack>
</RC>
```

Beispiel:

Eine Anfrage, bei der gleich ein Ergebnis oder Fehler zurückkommt

Steueranmeldungen werden gesendet, Erfolg oder Fehler kommen sofort zurück (UStVA, LStA).

#### Hinweis:

##### Bei Verwendung der Clientkomponente ERiC:

Bei Verwendung von ERiC kommt bei der Abgabe von bestimmten Datenlieferungen in der Serverantwort kein Inhalt im Element DatenTeil auch bei Online-Verfahren.

Hier kann der Anwender bei einem Online-Verfahren sicher sein, dass seine Daten entgegengenommen und verarbeitet wurden, wenn im TransferHeader unter <Rueckgabe> <Code> eine „0“ eingetragen ist und der Inhalt des Elements „DatenTeil“ leer ist.



### 1.2.2 Das Offline-Verfahren

Beim Offline-Verfahren werden die Daten entgegengenommen und in einer Datenbank abgelegt, es wird zu einem späteren Zeitpunkt (offline) geprüft, ob die Daten verarbeitet werden können. Das Ergebnis kann dann zu einem späteren Zeitpunkt angefordert werden. D.h. beim Offline-Verfahren muss sich der Anwender zum Abholen des Verarbeitungsergebnisses (Protokollanforderung) erneut an den Server (mittels Online-Verfahren) wenden.

Beim Offline-Verfahren ist ggf. die Mitgabe eines <TransportSchluessel> (vgl. Tz. 3.2 TransferHeader) nötig, um das Verarbeitungsergebnis zu einem späteren Zeitpunkt abholen und entschlüsseln zu können.

Beim Offline-Verfahren erhält der Client von der Clearingstelle ein sofortiges Antwort-XML, bestehend aus TransferHeader und leerem DatenTeil. Im TransferHeader ist entweder der Rückgabewert „0“ vermerkt, wenn die Daten grundsätzlich angenommen werden konnten und ein Wert ungleich „0“, falls bereits die Übermittlung gescheitert ist. Aufgrund dieses Ergebnisses kann aber KEIN Rückschluss auf die Verarbeitbarkeit der Datenlieferung gezogen werden. Dies ist erst nach Abholung des Protokolls mittels einer eigenen Protokollanforderung möglich.

#### **Beispiel:**

Eine Anfrage wird geschickt, das Ergebnis muss zu einem späteren Zeitpunkt abgeholt werden.

Lohnsteuerbescheinigungen werden geliefert. Das Ergebnis, ob die Daten erfolgreich verarbeitet werden konnten, kann erst zu einem späteren Zeitpunkt abgefragt werden (LStB und Protokollanforderung->Protokoll).

Sammellieferungen (s. Tz. 3.5) sind im Offline-Verfahren möglich.

## 2 Standards und Technik

### 2.1 XML-Encoding

Die Daten werden mit <?xml version="1.0" encoding="utf-8"?> erwartet. Bitte beachten Sie die Dokumentation der entsprechenden Fachverfahren.

### 2.2 Zeichenumfang

Der Zeichenumfang in Headern und Nutzdaten war bisher auch auf eine Teilmenge von ISO-8859-15 beschränkt. (VdMZulZeich) Auch mit der Umstellung auf utf-8 ändert sich dieser Umfang nicht.



Nur Zeichen die dem folgenden Ausdruck entsprechen sind in den XMLs zulässig:

```
<xs:pattern  
value="[\u000a;\u000d;\u0020;\u0021;\u0022;\u0023;\u0024;\u0025;\u0026;  
\u0027;\u0028;\u0029;\u002a;\u002b;\u002c;\u002d;\u002e;\u002f;\u0030;  
\u0031;\u0032;\u0033;\u0034;\u0035;\u0036;\u0037;\u0038;\u0039;\u003a;  
\u003b;\u003c;\u003d;\u003e;\u003f;\u0040;\u0041;\u0042;\u0043;\u0044;  
\u0045;\u0046;\u0047;\u0048;\u0049;\u004a;\u004b;\u004c;\u004d;\u004e;  
\u004f;\u0050;\u0051;\u0052;\u0053;\u0054;\u0055;\u0056;\u0057;\u0058;  
\u0059;\u005a;\u2022[\u005c;\u005d;\u005e;\u005f;\u0060;\u0061;\u0062;\u0063;  
\u0064;\u0065;\u0066;\u0067;\u0068;\u0069;\u006a;\u006b;\u006c;\u006d;  
\u006e;\u006f;\u0070;\u0071;\u0072;\u0073;\u0074;\u0075;\u0076;\u0077;  
\u0078;\u0079;\u007a;\u007b;\u007c;\u007d;\u007e;\u00a1;\u00a2;\u00a3;\u00a5;\u00a7;\u00aa;\u00ab;\u00ac;\u00ae;\u00af;\u00b0;\u00b1;\u00b2;\u00b3;\u00b5;\u00b9;\u00ba;\u00bb;\u00bf;\u00c0;\u00c1;\u00c2;\u00c3;\u00c4;\u00c5;\u00c6;\u00c7;\u00c8;\u00c9;\u00ca;\u00cb;\u00cc;\u00cd;\u00ce;\u00cf;\u00d0;\u00d1;\u00d2;\u00d3;\u00d4;\u00d5;\u00d6;\u00d7;\u00d8;\u00d9;\u00da;\u00db;\u00dc;\u00dd;\u00de;\u00df;\u00e0;\u00e1;\u00e2;\u00e3;\u00e4;\u00e5;\u00e6;\u00e7;\u00e8;\u00e9;\u00ea;\u00eb;\u00ec;\u00ed;\u00ee;\u00ef;\u00f0;\u00f1;\u00f2;\u00f3;\u00f4;\u00f5;\u00f6;\u00f7;\u00f8;\u00f9;\u00fa;\u00fb;\u00fc;\u00fd;\u00fe;\u00ff;\u0152;\u0153;\u0160;\u0161;\u0178;\u017d;\u017e;\u20ac;]*"/>
```

## 2.3 Namespace

Die ElsterXML-Datei unterliegt folgendem Default Namespace:

□ <http://www.elster.de/elsterxml/schema/v11>

Der Namespace ist bei dem ersten Element im ElsterXML einmalig zu setzen:

<Elster xmlns="<http://www.elster.de/elsterxml/schema/v11>">

....

</Elster>

**Im Element „Elster“ und in den Bereichen TransferHeader, Nutzdatenheader und im Element Nutzdaten dürfen keine weiteren Namespaces gesetzt und verwendet werden. (siehe Abb.1)**

Einzelne Fachverfahren verwenden innerhalb des Elements „**Nutzdaten**“ eigene Namespaces. Hierzu bitte die Dokumentationen bzw. Schnittstellenbeschreibungen der einzelnen Fachverfahren beachten. Die Deklaration des Namespaces erfolgt hier erst innerhalb des Elements Nutzdaten.

## 2.4 Authentifizierung

### Hinweis:

Genauere Informationen zur Authentifizierung befinden sich in den Dokumenten „Einheitliche\_Datenschnittstelle\_XML\_Authentifizierung\_\*.pdf und Spezifikation\_ELSTER-Token\_\*.pdf, welche sich auch in diesem Downloadpaket befinden.

Im Folgenden werden ausschließlich die für den XML Aufbau entscheidenden Aspekte aufgezeigt:



## 2.4.1 DatenTeil-Authentifizierung (Signaturdaten werden im TransferHeader abgelegt)

Die Authentifizierung erfolgt über das Element „DatenTeil“ und dessen komprimierten, verschlüsselten, base64-kodierten Inhalt. Die Signatur und die zugehörigen Informationen werden im TransferHeader im Element <SigUser> erwartet.

Als Vorgang muss im TransferHeader angegeben werden: <Vorgang>send-Auth</Vorgang> bzw. bei einzelnen Fachverfahren <Vorgang>send-Auth-Part</Vorgang>.

Kurzer Überblick zur Authentifizierung mit Vorgang „send-Auth“

- a) Komprimierung, Verschlüsselung, und Base64-Kodierung des Inhalts des Elements <DatenTeil>.
- b) Signaturerstellung über das Element <DatenTeil> und dessen Inhalt. Die Signatur wird im TransferHeader abgelegt im Element <SigUser> im Unterelement <Sig>.
- c) Das <SigUser>- Element im TransferHeader muss komprimiert, verschlüsselt<sup>1</sup> und Base64-kodiert werden, da es datenschutzrechtliche Inhalte enthält. Bei der Rückantwort vom Server wird das Element <SigUser> nicht mehr übermittelt.

Aufbau des ElsterXML bei Vorgang „send-Auth“ bzw. welche Elemente haben verschlüsselten, komprimierten und base64-kodierten Inhalt:

```
<Elster xmlns="http://www.elster.de/elsterxml/schema/v11">
```

```
  <TransferHeader version="xx">
```

```
    ....
```

```
    <SigUser>
```

Komprimierter, verschlüsselter1, Base64-kodierter Inhalt (Verschlüsselt ist der Inhalt von „SigUser“, ohne das Element „SigUser“ selbst.)

```
    </ SigUser>
```

```
    ...
```

```
    <DatenLieferant>
```

Komprimierter, verschlüsselter2, Base64-kodierter Inhalt (Verschlüsselt ist der Inhalt von „DatenLieferant“, ohne das Element „DatenLieferant“ selbst.)

```
    </ DatenLieferant >
```

```
    <TransportSchluessel>
```

Komprimierter, verschlüsselter1, Base64-kodierter Inhalt (Verschlüsselt ist der Inhalt von „TransportSchluessel“, ohne das Element „TransportSchluessel“ selbst.)

```
    </ TransportSchluessel>
```

```
  </TransferHeader>
```

```
  <DatenTeil>
```

---

<sup>1</sup> Hybride Verschlüsselung mit RSA-OAEP als asymmetrisches Verfahren und DES-EDE3-CBC (Triple-DES im CBC-Modus nach ANSI X9.52) als symmetrisches Verfahren

<sup>2</sup> GZIPInputStream und GZIPOutputStream



Komprimierter, verschlüsselter, Base64-kodierter Inhalt (Verschlüsselt1 ist der Inhalt von „DatenTeil“, ohne das Element „DatenTeil“ selbst.)

```
</DatenTeil>  
</Elster>
```

## 2.5 Kompression

Kompression erfolgt ausschließlich mit GZIP. Die Kompression muss bei jedem Element, das verschlüsselt ist, vor der Verschlüsselung<sup>1</sup> erfolgen.

Hierzu können die Java-GZip-Klassen unter „java.util.zip“ verwendet werden.

Eine Dokumentation zu GZIP finden Sie unter:

<http://www.rfc-editor.org/rfc/rfc1952.pdf>

## 2.6 Verschlüsselung

Verschlüsselungsverfahren RSA-OAEP nach PKCS#1, kodiert in dem Format „CMS“<sup>1</sup> (Nachfolger von PKCS#7)

Kodierung der verschlüsselten Daten mit Cryptographic Message Syntax (CMS) mit folgenden Inhaltstypen und kryptographischen Algorithmen:

- Für online Request (Anfrage) - enveloped data –
  - zufälliger, symmetrischer SessionKey (DES-EDE3-CBC) wird erzeugt.
  - mit diesem Schlüssel werden die Daten mit Triple-DES (DES-EDE3-CBC) nach ANSI X9.52 verschlüsselt ("Encrypted Content").
  - der SessionKey wird mit dem öffentlichen asymmetrischen 2048 Bit langen EmpfängerSchlüssel (Clearingstelle) mit RSAES-OAEP nach PKCS#1 ab Version 2.0 verschlüsselt ("Recipient Info"). Die Berechnung des Paddings bei RSA-OAEP erfolgt mit SHA-256 als HashAlgorithm, MGF1 mit SHA-256 als MaskGenFunc sowie einem leeren String als pSourceFunc (vgl. [RFC 4055](#)).
  - Es sind auch mehrere Empfänger möglich.
  - Die CMS-Syntax muss konform zu [RFC 2560](#) sein.
- Für online Response (Antwort), wenn im Tag „Datei -> Verschlüsselung“ des Requests der Wert „CMSEncryptedData“ steht:
  - es erfolgt nur eine symmetrische Triple-DES-Verschlüsselung nach ANSI X9.52 (DES-EDE3-CBC) mit dem beim Request erzeugten SessionKey.
- Für online Response (Antwort), wenn im Tag „Datei -> Verschlüsselung“ des Requests der Wert „CMSEnvelopedData“ steht und im XML-Tag <Transportschlüssel> des Requests ein öffentlicher Schlüssel (X.509-Zertifikat) zur Rückverschlüsselung mitgegeben wird:
  - Drei zufällige, symmetrische DES-SessionKeys mit jeweils 56 Bit Länge werden erzeugt.<sup>2</sup>
  - Mit diesen drei DES-Schlüsseln werden die Daten mit Triple-DES (DES-EDE3-CBC) nach ANSI X9.52 verschlüsselt ("Encrypted Content").
  - Die drei SessionKeys werden konkateniert und mit dem beim Request im XML-Tag <Transportschlüssel> übermittelten öffentlichen Schlüssel (asymmetrischer 2048 Bit langer Schlüssel) mit RSAES-OAEP nach PKCS#1 ab Version 2.0 verschlüsselt ("Recipient Info"). Die Berechnung des Paddings bei RSA-OAEP erfolgt mit SHA-256 als HashAlgorithm, MGF1 mit SHA-256 als MaskGenFunc sowie einem leeren String als pSourceFunc (vgl. [RFC 4055](#)).

<sup>1</sup> S. [RFC 5652](#)

<sup>2</sup> DES-Schlüssel sind eigentlich 64 Bit lang, aber die letzten 8 sind Parity-Bits.



- Die CMS-Syntax ist konform zu [RFC 2560](#) sein.

Weitere Informationen zu CMS finden Sie unter:

<https://tools.ietf.org/html/rfc5652>

Um den verschlüsselten DatenTeil in das XML-Dokument einzufügen, darf dieser nicht im binären Format vorliegen. Deshalb müssen die CMS-Daten vor dem Einfügen Base64-kodiert werden. Die Base64-Kodierung ist in [RFC 4648](#) beschrieben.

**Hinweis:**

Eine Dokumentation zu Base64 finden Sie unter:

<https://tools.ietf.org/html/rfc4648>

## 2.7 Kommunikation

### 2.7.1 Protokoll: https

Verfahren: POST

Es wird der unter Tz. 3 beschriebene ElsterXML-Datensatz erwartet.

URL:

[https://datenannahme1.elster.de:443/ERIC\\_IAS/ERiClet](https://datenannahme1.elster.de:443/ERIC_IAS/ERiClet)

[https://datenannahme2.elster.de:443/ERIC\\_IAS/ERiClet](https://datenannahme2.elster.de:443/ERIC_IAS/ERiClet)

[https://datenannahme3.elster.de:443/ERIC\\_IAS/ERiClet](https://datenannahme3.elster.de:443/ERIC_IAS/ERiClet)

[https://datenannahme4.elster.de:443/ERIC\\_IAS/ERiClet](https://datenannahme4.elster.de:443/ERIC_IAS/ERiClet)

Die Verteilung und Zuordnung auf die einzelnen 4 URLs muss vom Sender sichergestellt werden.

**Hinweis:**

Wird die Anzahl der Clearingstellen selbst programmiert, so soll bei den drei Verfahren die Verfahrensbezeichnung an die jeweilige URL angehängt werden:

- ElsterAnmeldung (UStVA, LStA)
- ElsterLohn (LStB, Protokollanforderung)

Für die einzelnen Verfahren können so gesonderte Eingangsserver verwendet werden. Es kann aber nach wie vor auch über die URLs ohne Verfahrensbezeichnung gesendet werden, jedoch ist es aus Gründen der Performance ratsam die URLs um die Fachverfahren zu ergänzen.

Beispiel für URLs mit Verfahrensbezeichnung:

Die 4 URL sollen um das Verfahren der Datenlieferung erweitert werden, d.h. am Beispiel der URL

[https://datenannahme1.elster.de:443/ERIC\\_IAS/ERiClet](https://datenannahme1.elster.de:443/ERIC_IAS/ERiClet):

ElsterAnmeldungen (UStVA, LStA) –

[https://datenannahme1.elster.de:443/ERIC\\_IAS/ERiClet/ElsterAnmeldung](https://datenannahme1.elster.de:443/ERIC_IAS/ERiClet/ElsterAnmeldung)

ElsterLohn(LStB, Protokollanforderung)  
[https://datenannahme1.elster.de:443/ERIC\\_IAS/ERiClet/ElsterLohn](https://datenannahme1.elster.de:443/ERIC_IAS/ERiClet/ElsterLohn)



## 3 Datenstrukturen - Header

### 3.1 Spezifikation

Nachfolgend werden die Felder für den TransferHeader und den NutzdatenHeader, sowie die einzelnen Datenstrukturen erläutert.

Der „TransferHeader“ (THeader) ist der oberste Header in der Datenstruktur. Er enthält Felder für die Kommunikation zwischen Server und Client, sowie allgemeine Verarbeitungsfelder.

Auf der gleichen Ebene wie der „TransferHeader“ befindet sich der „DatenTeil“, dieser enthält einen (bei Sammelfilen mehrere) Element/e „NutzdatenBlock“, dieses beinhaltet wiederum ein Element „NutzdatenHeader“, sowie ein Element „Nutzdaten“.

Der NutzdatenHeader (NHeader) ist unterhalb des TransferHeaders angesiedelt und enthält primär datenteilspezifische Inhalte, Fehlermeldungen und –codes. Auf der gleichen Ebene wie der NutzdatenHeader befindet sich dann die XML-Datenstruktur des jeweiligen anwendungsspezifischen Nutzdatensatzes („Nutzdaten“).

Innerhalb einer Lieferung kann es nur einen „TransferHeader“ geben.

Bei Sammellieferungen kann es mehrere NutzdatenBlöcke geben. Ein „NutzdatenBlock“ kann nur einen „NutzdatenHeader“ und in der Regel ein Element „Nutzdaten“ enthalten. Sind in einer Lieferung mehrere NutzdatenBlöcke enthalten, so sind in dieser Lieferung nur NutzdatenHeader mit der gleichen Versionsnummer zulässig.

Als ElsterXML- Datensatz (ElsterXML) wird ein kompletter XML- Datensatz mit TransferHeader und DatenTeil bezeichnet.

### 3.2 TransferHeader (THeader)

#### 3.2.1 Allgemeines

Der THeader wird dem Datenteil (Nutzdatenblöcke, aus NHeader und Nutzdatensatz bestehend) vorangestellt.

Der THeader enthält Informationen für den Transport.

#### 3.2.2 Aktuelle Version des THeaders

Version 11

#### 3.2.3 Elemente im Transferheader

Die Elementbeschreibungen sind im Schema zu finden.

#### 3.2.4 Aufbau der XML-Struktur des TransferHeaders

Alles ohne Bemerkung = Pflicht

##### 3.2.4.1 Datenlieferung an die Clearingstelle

Beispiel für TransferHeader:

```
<TransferHeader version="11">  
  <Verfahren>ElsterAnmeldung</Verfahren>  
  <DatenArt>UStVA</DatenArt>  
  <Vorgang>send-Auth</Vorgang>  
  <Testmerker>700000004</Testmerker> optional
```



<SigUser>sdfgsdgsgs</SigUser> optional (Beim Vorgang "send-Auth" muss das Element „SigUser“ vorhanden sein:

<!-- Der SigUser-Teil ist mit demselben Schlüssel, wie die Nutzdaten verschlüsselt, er wird online entschlüsselt, falls dies nicht funktioniert, wird dem Anwender online ein Fehler zurückgegeben. Vor der Verschlüsselung sieht das SigUser Element folgendermaßen aus:

```
<SigUser> optional (wenn signiert wird, dann muss es geliefert werden) <Sig>

    <dsig:Signature Id="Sign1"
mlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        XXXXXX
    </dsig:Signature>
</Sig>
</SigUser>-->

<HerstellerID>74931</HerstellerID>

<DatenLieferant> XYZ-Lieferant </DatenLieferant>

<!-- Der DatenLieferant-Teil ist mit demselben Schlüssel, wie die Nutzdaten verschlüsselt, er wird online entschlüsselt, falls dies nicht funktioniert, wird dem Anwender online ein Fehler zurückgegeben.-->

<Datei> <!-- ist Pflicht -->
    <Verschluesselung>CMSEnvelopedData</Verschluesselung>
    <Kompression>GZIP</Kompression>

    <TransportSchluessel>gfhjdfghjsdgdsgfjaskdgfjsdgfjsegfjsadfhjasvfgf</TransportSchluessel> optional
</Datei>

    <VersionClient>2001121212</VersionClient> optional, d.h. Element entweder gefüllt oder nicht vorhanden

    <Zusatz> optional
        <Info/> optional kann mehrfach geliefert werden
    </Zusatz>
</TransferHeader>
```

### 3.2.4.2 Datenrücklieferung von der Clearingstelle an den Hersteller

Beispiel für TransferHeader:

```
<TransferHeader version="11">
    <Verfahren>ElsterAnmeldung</Verfahren>
    <DatenArt>UStVA</DatenArt>
    <Vorgang>send-Auth</Vorgang>
    <TransferTicket>et123456789012345678901234567890</TransferTicket>
    <Testmerker>700000004</Testmerker> optional
```



```
<!-- Das <SigUser> Element - falls es bei Datenlieferung vorhanden war- wird  
NICHT zurückgeliefert -->  
<HerstellerID>74931</HerstellerID>  
<DatenLieferant>XYZ-Lieferant </DatenLieferant>  
<EingangsDatum>20120515121212</EingangsDatum>  
<Datei>  
  <Verschluesselung>CMSEnvelopedData</Verschluesselung>  
  <Kompression>GZIP</Kompression>  
<TransportSchluessel>gfhjdfghjsdgsfjadsgfjaskdgfjsdgifjsegfjsadfhjasvfgf</Transp  
ortSchluessel>  
</Datei>  
<RC>  
  <Rueckgabe>  
    <Code>...</Code>  
<Text>...</Text>  
  </Rueckgabe>  
<Stack>  
  <Code>...</Code>  
  <Text>...</Text>  
</Stack>  
</RC>  
<VersionClient>2001121212</VersionClient>  
<Zusatz> optional  
  <Info/> optional, kann mehrfach vorhanden sein  
  <ElsterInfo>Text</ElsterInfo> optional, kann mehrfach vorhanden sein  
</Zusatz>  
</TransferHeader>
```



### 3.3 NutzdatenHeader (NHeader)

#### 3.3.1 Allgemeines

Der NHeader enthält Verarbeitungsanweisungen, sowie andere Informationen für das verarbeitende Programm. Er wird zusammen mit den Nutzdaten verschlüsselt.

#### 3.3.2 Elemente im Nutzdatenheader

Die Elementbeschreibungen sind im Schema zu finden.

#### 3.3.3 Aufbau der XML-Struktur des NutzdatenHeaders

Alles ohne Bemerkung = Pflicht

##### 3.3.3.1 Datenlieferung an die Clearingstelle

```
<NutzdatenHeader version="11">  
<NutzdatenTicket>1</NutzdatenTicket> Pflicht, bei Einzelfalllieferungen ggf. mit  
1 zu füllen  
<Empfaenger id="F">9123</Empfaenger>  
<Hersteller> optional  
    <ProduktName>Elsterformular</ProduktName>  
    <ProduktVersion>ElsterFormular x.y</ProduktVersion>  
</Hersteller>  
<DatenLieferant>String, der Lieferanteninfo enthält</DatenLieferant> optional  
<Zusatz> optional  
    <Info/> optional, kann mehrfach vorhanden sein  
</Zusatz>  
</NutzdatenHeader>
```

##### 3.3.3.2 Datenrücklieferung von der Clearingstelle an den Hersteller (nur bei Online-Verfahren)

```
<NutzdatenHeader version="11">  
<NutzdatenTicket>1</NutzdatenTicket>  
<Empfaenger id="F">9123</Empfaenger>  
<Hersteller>  
    <ProduktName>Elsterformular</ProduktName>  
    <ProduktVersion>ElsterFormular x.y</ProduktVersion>  
</Hersteller>  
<DatenLieferant>String, der Lieferanteninfo enthält</DatenLieferant>  
<RC>  
    <Rueckgabe>  
        <Code>...</Code>  
        <Text>...</Text>  
</Rueckgabe>
```



```
<Stack>
  <Code>...</Code>
  <Text>...</Text>
</Stack>
</RC>
<Zusatz> optional
  <Info/> optional, kann mehrfach vorhanden sein
  <ElsterInfo>Text</ElsterInfo> optional, kann mehrfach vorhanden sein
</Zusatz>
</NutzdatenHeader>
```

#### Hinweis:

Bei Offline-Verfahren wird ein **leeres** DatenTeil-Element zurückgeliefert. (Kein Element NutzdatenHeader und Nutzdaten)

- Hier reicht der Returncode „0“ des TransferHeaders um zu sehen, dass die Daten von der Finanzverwaltung angenommen wurden. Um zu sehen, ob die Daten verarbeitbar sind, muss dies über eine Protokollanforderung erfragt werden.

#### Hinweis:

##### bei Verwendung der Clientkomponente ERiC:

Bei Verwendung von ERiC kommt bei der Abgabe von bestimmten Datenlieferungen in der Serverantwort kein Inhalt im Element DatenTeil auch bei Online-Verfahren.

Hier kann der Anwender bei einem Online-Verfahren sicher sein, dass seine Daten entgegengenommen und verarbeitet wurden, wenn der Inhalt des Elements „DatenTeil“ leer ist und im TransferHeader unter `<Rueckgabe> <Code>` eine „0“ eingetragen ist.

### 3.4 Unterstützte Feldinhalte und Dienste

Zum Verständnis vorab:

Verfahren ist ein übergeordneter Begriff, der mehrere Datenarten bündelt. Dies kann auf fachlicher (ElsterErklärung), oder technischer (ElsterDatenabholung) Ebene geschehen.

Datenart ist die genauere Bestimmung, um was für Daten es sich handelt (USt, ESt, ...).

Die Kombination von Verfahren und Datenart ist für die Zuordnung zur nachfolgenden Verarbeitung wichtig.

#### 3.4.1 Gültige Feldinhalte im TransferHeader

Die Auflistung gültiger Feldinhalte und eine kurze Erklärung finden Sie im Headerbasisschema.



Testmerker:

Eine Auflistung gültiger Testmerker finden Sie im Headerbasisschema.

**Hinweis:**

Wenn bei einer Datenlieferung kein Testmerker gesetzt wird, handelt es sich um **echte/produktive Daten**. Daten mit Testmerker dürfen nicht produktiv verarbeitet werden, jedes Produkt muss sicherstellen, dass Daten mit Testmerker keine produktiven Daten verändern. Spätestens die letzte verarbeitende Stelle muss Daten mit Testmerker aussteuern.

HerstellerID
Siehe Schema

Verschlüsselung	
CMSEncryptedData	
CMSEnvelopedData	Ein X.509-Zertifikat als TransportSchlüssel (im TransferHeader) für die Antwort (öffentlicher Schlüssel) ist mit zu versenden.
PKCS#7v1.5	Deprecated
PKCS#7v1.5enveloped	Deprecated Ein X.509-Zertifikat als TransportSchlüssel (im TransferHeader) für die Antwort (öffentlicher Schlüssel) ist mit zu versenden.
NO_BASE64	Wird intern verwendet!
EnvelopedData;RSA-OAEP;AES-128;GZip;B64	Neuer Verschlüsselungstag. Noch nicht unterstützt.

Kompression	
GZIP	
NO_BASE64	Wird intern verwendet!

### 3.4.1.1 Auflistung der möglichen Kombinationen der Elementinhalte von „Verfahren“, „DatenArt“ und „Vorgang“

**Hinweis:**

Einen Überblick, bei welchen Datenlieferung welche Authentifizierung möglich ist, finden Sie in dem Dokument „Verzeichnis\_der\_Datenarten.xml“, welches sich auch in diesem Downloadpaket befindet.

### 3.4.2 Gültige Feldinhalte im NutzdatenHeader:

Die Auflistung gültiger Feldinhalte und eine kurze Erklärung finden Sie im Headerbasisschema.

**Hinweis:**

Die einzelnen Fachverfahren legen separat fest ob beim Empfänger Element entweder die Bundesfinanzamtsnummer und/oder das Länderkürzel angegeben werden darf.



Die Vorgaben finden Sie in den einzelnen Schnittstellenbeschreibungen der Fachverfahren!

### 3.5 Sammellieferungen (*nur teilweise unterstützt!*)

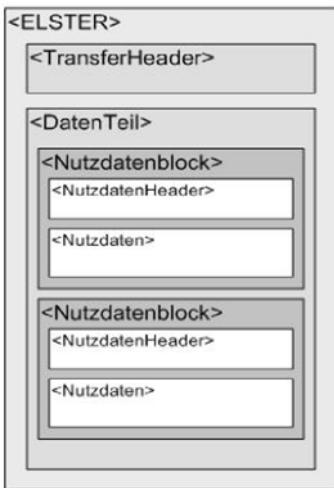


Abb. 2: ElsterXML-Daten

In einigen Fällen ist es möglich, dass mehrere Nutzdatenblöcke in einem Paket geliefert werden. Die Größe (Anzahl der Nutzdatenblöcke) der Sammeldatei liegt in der Eigenverantwortung der Datenlieferer. Bei einem Verbindungsabbruch oder einer fehlerhaften Lieferung wird keine Teilverarbeitung vorgenommen. Die Datenübermittlung ist vollständig neu aufzusetzen.

Pro Paket ist ein <TransferHeader> nötig, sowie ein dazugehöriger <DatenTeil>. Unter dem <DatenTeil> können sich dann x Nutzdatenblöcke befinden, die wiederum aus jeweils einem <NutzdatenHeader> und dem zugehörigen Element <Nutzdaten> bestehen.

Ein Ticket, das die komplette Lieferung betrifft wird im <TransferHeader> unter <TransferTicket>, eingestellt. Dieses Ticket wird serverseitig von der Clearingstelle erzeugt und an den Absender zu Nachforschungszwecken und für Nachfragen das Paket betreffend zurückgeliefert.

Für die einzelnen Nutzdaten-Unterpakete ist jeweils ein eigenes NutzdatenTicket in den zugehörigen <NutzdatenHeader> einzustellen, dieses wird vom Softwarehersteller erzeugt und gefüllt. Dieses eindeutige Ticket dient für Nachfragen einen einzelnen Nutzdatensatz betreffend.

Wird authentifiziert, wird beim Vorgang „send-Auth“ der komplette <DatenTeil> authentifiziert und die Signaturdaten werden im Element SigUser im <TransferHeader> abgelegt.



**Hinweis:**

Pro Sammellieferung ist es nur möglich mehrere Daten mit der **gleichen** DatenArt, Verfahren und Vorgang zu liefern.

Eine Sammellieferung kann aktuell bei den Verfahren ElsterAnmeldung, ElsterLohn, ElsterKMF, ElsterLohn2, ElsterNachricht/Einspruch und DatenAbholung erfolgen.

**Wichtig:**

Sammellieferungen bei ElsterAnmeldungen gehen nur in Verbindung mit der Clientkomponente ERiC!

Sammellieferungen mit ERiC bei ElsterAnmeldung müssen wie folgt aufgebaut sein:

In EINEM ElsterXML dürfen sich nur Daten für ein Ziel-Bundesland befinden.

Außerdem gibt es in einem Nutzdatenblock genau ein Element NutzdatenHeader und ein Element Nutzdaten.

Die xml-Datei darf maximal 50 MB groß sein, bei authentifizierten Daten 15 MB

## 4 Nutzdaten

Die einzelnen Fachverfahren (z.B. ElsterLohn) entsprechen zwar dem allgemeinen Aufbau dieser Datenschnittstelle. Sie unterscheiden sich aber jeweils unterhalb des Bereichs <Nutzdaten> im Aufbau. Die jeweiligen Informationen dazu sind unter

[www.elster.de](http://www.elster.de) – Mitglieder – ElsterEntwickler – Download

## 5 Beispiele

Zu den einzelnen Fachverfahren finden Sie Beispiele jeweils im entsprechenden ELSTER-Downloadbereich.

### 5.1 Daten mit geplanter Authentifizierung VOR der Verschlüsselung

Beispiel einer Umsatzsteuervoranmeldung:

```
<?xml version="1.0" encoding="utf-8"?>
<Elster xmlns="http://www.elster.de/elsterxml/schema/v11">
  <TransferHeader version="11">
    <Verfahren>ElsterAnmeldung</Verfahren>
    <DatenArt>UStVA</DatenArt>
    <Vorgang>send-Auth</Vorgang>
    <Testmerker>700000004</Testmerker>
    <HerstellerID>74931</HerstellerID>
    <DatenLieferant>Name</DatenLieferant>
    <Datei>
      <Verschluesselung>CMSEnvelopedData</Verschluesselung>
      <Kompression>GZIP</Kompression>
      <TransportSchluessel/>
    </Datei>
  </TransferHeader>
</Elster>
```



```
<VersionClient>Programm Version 3.5.0 - 16.11.20xx</VersionClient>
<Zusatz>
  <Info>test</Info>
</Zusatz>
</TransferHeader>
<DatenTeil>
  <Nutzdatenblock>
    <NutzdatenHeader version="11">
      <NutzdatenTicket>234234234</NutzdatenTicket>
      <Empfaenger id="F">9198</Empfaenger>
      <Hersteller>
        <ProduktName>Programm XY</ProduktName>
        <ProduktVersion>V 1.0</ProduktVersion>
      </Hersteller>
      <DatenLieferant>Datenlieferant; Teststr.3; 12345 Test; test@email.de
    </DatenLieferant>
    <Zusatz>
      <Info>....</Info>
    </Zusatz>
    </NutzdatenHeader>
    <Nutzdaten>
      <Anmeldungssteuern art="UStVA" version="201301">
        <DatenLieferant>
          <Name>Vorname Nachname</Name>
          <Strasse>Meiserstr. 6</Strasse>
          <PLZ>80335</PLZ>
          <Ort>München</Ort>
          <Telefon>089/0815 0815</Telefon>
          <Email>email@adresse.de</Email>
        </DatenLieferant>
        <Erstellungsdatum>20130209</Erstellungsdatum>
        <Steuerfall>
          <Umsatzsteuervoranmeldung>
            <Jahr>2013</Jahr>
            <Zeitraum>41</Zeitraum>
            <Steuernummer>9198058870707</Steuernummer>
        <Kz09>74931*NameSteuerberater*Berufsbezeichnung*089*12345678*Mandantenname</K
z09>
        <Kz83>-1.99</Kz83>
      </Anmeldungssteuern>
    </Nutzdaten>
  </Nutzdatenblock>
</DatenTeil>
```



```
</Umsatzsteuervoranmeldung>
</Steuerfall>
</Anmeldungssteuern>
</Nutzdaten>
</Nutzdatenblock>
</DatenTeil>
</Elster>
```

## 5.2 Daten mit Authentifizierung NACH der Verschlüsselung

Beispiel einer Umsatzsteuervoranmeldung:

```
<?xml version="1.0" encoding="utf-8"?>
<Elster xmlns="http://www.elster.de/elsterxml/schema/v11">
    <TransferHeader version="11">
        <Verfahren>ElsterAnmeldung</Verfahren>
        <DatenArt>UStVA</DatenArt>
        <Vorgang>send-Auth</Vorgang>
        <Testmerker>700000004</Testmerker>
        <SigUser>MIAGCSqGSIB3DQEHA6CAMIACAQAxggF6MIIIBdgIBADBeMFkxCzAJBgNVBAYTAKRFMQ8w
DQYDVQQKEwZFTFNURVIxDDAKBgNVBAsTA0VCQTEPMA0GA1UEAxMGQ29kaW5nMRowGAYDVQQFEExEyMDA
MDkzMDE0MzMyM3gwMAIBADANBgkqhkiG9w0BAQEFAASCAQArY21kwVHnuzIbFNubMu4376PVBY78ekBM
N7AGI8M40SWy1XhXUeIcC5VqkCRxloG3Tx20NTUBuOYNy2LSCdVqe8GeP2LFWr+gIhY4jHOVv5S4TyWU
1NXMyIbggnrjxf7/I/P9HnMPkVrogUF5E1YhbU2klezOIAwNPEUPE+vL29jidwCiAut/2FaYLwrdrVAs+
prKmD8ke3InEfG9gzhX/goYZQ9CRLFiBkbAgpaucwbg3eSSciNBDD/pgHSsK9nA/FeVzvYfU7rjRYiHj
oATWT/0eqHbzmf0GQM1046tbMxXPNqOM6gVamGQGF2y99aiDKjB/374Jj0PDa7QvJWikMIAGCSqGSIB3
DQEHATAUBggqhkjG9w0DBwQIVqlKB04M2USggARIyUjUj1IyyGmYTggSndGypi359egPF2TI2xVcob09
f8tLrnisglTsm1p1/Y5H5H/jeXnopbkp17MON1La/V7jhTRr8Di0CUXAAAAAAAAAAAAAA==</SigUser>
        <HerstellerID>74931</HerstellerID>
    <DatenLieferant>MIAGCSqGSIB3DQEHA6CAMIACAQAxggF6MIIIBdgIBADBeMFkxCzAJBgNVBAYTAKRF
MQ8wDQYDVQQKEwZFTFNURVIxDDAKBgNVBAsTA0VCQTEPMA0GA1UEAxMGQ29kaW5nMRowGAYDVQQFEExEy
MDA MDkzMDE0MzMyM3gwMAIBADANBgkqhkiG9w0BAQEFAASCAQArY21kwVHnuzIbFNubMu4376PVBY78
ekBMN7AGI8M40SWy1XhXUeIcC5VqkCRxloG3Tx20NTUBuOYNy2LSCdVqe8GeP2LFWr+gIhY4jHOVv5S4
TyWU1NXMyIbggnrjxf7/I/P9HnMPkVrogUF5E1YhbU2klezOIAwNPEUPE+vL29jidwCiAut/2FaYLwrdr
VAs+prKmD8ke3InEfG9gzhX/goYZQ9CRLFiBkbAgpaucwbg3eSSciNBDD/pgHSsK9nA/FeVzvYfU7rjR
YiHjoATWT/0eqHbzmf0GQM1046tbMxXPNqOM6gVamGQGF2y99aiDKjB/374Jj0PDa7QvJWikMIAGCSqG
SIb3DQEHATAUBggqhkjG9w0DBwQIVqlKB04M2USggARIyUjUj1IyyGmYTggSndGypi359egPF2TI2xVc
ob09f8tLrnisglTsm1p1/Y5H5H/jeXnopbkp17MON1La/V7jhTRr8Di0CUXAAAAAAAAAAAAAA==</DatenLieferant>
        <Datei>
            <Verschluesselung>CMSEnvelopedData</Verschluesselung>
            <Kompression>GZIP</Kompression>
    </TransferHeader>
</Elster>
```



```
<TransportSchluessel>MIAGCSqGSIB3DQEHA6CAMIACAQAxggF6MII BdgIBADBeMFkxCzAJBgNVBAYTAKRFMQ8wDQYDVQQKEwZFTFNURVIXDDAKBgNVBAsTA0VCQTEPMA0GA1UEAxMGQ29kaW5nMRowGAYDVQQFExEyMDAzMDkzMDE0MzMyM3gwMAIBADANBgqhkiG9w0BAQEFAASCAQAs1eU0DJGqcmcZ34BKzp0nxpBV2uTQnLIHNEgHfqOmypoMpj kUUAAg5HvMalwJ3LDqPfpY2a9IDMtavgHN64FVfg74m2c45wT5GUDBvxdi7D8du6J37yrLcaWKmM1HvkF8uRQLWJq7Ncui75wulI+6W2s0CP/2DojgQ2EGIqCCZ+PUqI1WEqJuP+u5RYTBCg5FS8tKVOWRcu/LvLNY9EYA5qFxOcLWmmzbzSkG6Nb14elt6IN1C9QD0kZaayfTakihzt23R5tFDwmdGrqISczu7fK5F+q/JbnCqHDtJntKr6BtbZh6kAsjec0LjxJaqLD68QRMLh1HgG+AotHqhDKMIA GCSqGSIB3DQEHAATAUBggqhkiG9w0DBwQIdm4SwMGcxy2ggAQY9LEMYrvN3LIJPE+Z44UkQOsdxSqtCJqeAAAAAAAAAAAAA==</TransportSchluessel>
</Datei>
<RC>
<Rueckgabe>
<Code>0</Code>
<Text/>
</Rueckgabe>
<Stack>
<Code>0</Code>
<Text/>
</Stack>
</RC>
<VersionClient>Programm Version 3.5.0 - 16.11.20xx</VersionClient>
</TransferHeader>
<DatenTeil>MIAGCSqGSIB3DQEHA6CAMIACAQAxggF6MII BdgIBADBeMFkxCzAJBgNVBAYTAKRF.... verschlüsselter Inhalt ....e01vAAAAAAAAAAAAA==</DatenTeil>
</Elster>
```

**Hinweis:**

**Verschlüsselt ist der Inhalt von „DatenTeil“, ohne das Element „DatenTeil“ selbst.**

Außerdem der Inhalt der Elemente „SigUser“ (bei Vorgang „send-Auth“), „DatenLieferant“ und „TransportSchluessel“ im TransferHeader verschlüsselt.

### 5.3 RSA-OAEP-verschlüsselte Daten

Beispiel einer Einkommensteuererklärung:

```
<?xml version="1.0" encoding="utf-8"?>
<Elster xmlns="http://www.elster.de/elsterxml/schema/v11">
  <TransferHeader version="11">
    <Verfahren>ElsterErklaerung</Verfahren>
    <DatenArt>EST</DatenArt>
    <Vorgang>send-Auth</Vorgang>
    <Testmerker>700000004</Testmerker>
```



```
<SigUser>MIIJJgYJKoZIhvcNAQcDoIJJFzCCRMCAQAxggGLMIIBhwIBADBeMFkxCzAJBgNVBAYTAKR
FMQ8wDQYDVQQKEwZFTFNURVIxDDAKBgNVBAAsTA0VCQTEPMA0GA1UEAxMGQ29kaW5nMRowGAYDVQQFExE
yMDA5MDcyOTE1NTQ0MXgwMAIBADAeBgkqhkiG9w0BAQcwEaIPMA0GCSqGSIB3DQEBCQQABIIBAAIcOYB
1HtmenqrN2tkR22pZFWIQZHxYhyJ5ojO/fPgWVDhkus5Csm0gV+JRh8RjP6AXs7n5zt/LMWtaE6+JgOD
gWG6dPiKaa6Dg/LR+kyCPZQaMrX3f6Q5/h6ZUW13/xcyA8BgwmLM0KInFrYjPtdE/hwt64I438UqyZL
5QmZrNfbz2XU9Yp/HrBy7L9RemPqbFAUOct3egjHVD4Q3bGj/RhwVfaf6/xBuq2KwIKMwBo1K3QCWufW
Wdpoj+bDHBZTj88Y/Y9D8zcrC84Z9Hn0FlAsnTeOr+8m6jkX0f6kKehqt9IBPGkRV/RqnZoPztsb8VNf
0pBCBm1+Y/Ch06rgwggd9BgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECAGcmjV5XHSAgIIHWMRP+jY/Wt2
72MXWRU2LwZwQHIG3YAd1vOQ+cdWOIiDKXXWqtPdHdtcHtlF3oEOQMS0AW6D/4mlow+v6lumVjxucZbu
hQA9tLS/VUq+VPSUCC9kEmGLFsnCBV6Bvj/Kf30KROqRXKlebaMuiUYthXChZ2veORz/BD9WUiIdnen
u0Xpo8i5N400Jr9z1SRno2m+z/tVS7MmfvN18aCg75gk/z7RyENbdKhk5vp2yHCStGWEuaGVPgISi5eA
cunnCDac9UwEBMgsFxtKmmi3gOv+5UwGnpWqoW4FPLCTLKVb3tAb7fUoIeVz2obCr38qwo1dFg6qfCY9
PcrzJGdgY910/xVpv0apBzM6cqSvM0F/VfuAq05UP2d/uvvVNtrEGeKCv+1v4jJVL9KVxiX1H1Eg/Ag9
+2G1LAG+4NZp5riXG67TPQz18yCvaixLGNYLseV5xyO/KPBbSanJyM8WEURg91lybu0iogk8659ihdMw
EP1RMyBZgQPdzC7KmURujvI0Bf+as7A4UL1E19Use5q+IZXj5FzAx+vhah30Lct1RNp+AkCarv94oa9YA
66aeRsy+sse1ksP711j+VHKDQr48TWmLstPb+/uAWe43KExEp/um0qcicA8wS11BLBOujY3q0mRe21B3
kombq1gg5ZXyyvo4qLbp449njC+KcV8cDK3YsbqH5H8ZoaHozKlpMv6y5Nd18YMMMD8g5KTskKkqTHQt
e0BMRhnj0gNSQzN6W8wqbrMkmNzcrTvyO36oGtz8RUSiXrmjw+1ELcm0F+OuDiZNSa1XcxKzjGyuI03e
U+3avjVd18/pPwsj7EywsFOJ0IzJpQJKHSynQenDbHRLhDPD7c8CqIHBXTkjunoUmV8o5fm4ap5Le5X6
4/GcBDMz/0X7CsyfM2jUCU1NXHGIvdFNl2w7tt1HOPOTbmvltdj5qrKkEx3UFpwLpTqscd10IU33LD18
WN3MX0quh63kkLdMpy/x4uEEFx26EhWJwlw9Bh32fMwY+VTk+fK/8OGY7KBsDKUUjkkgnCd+XeNKF5WI
D2FaGAzTQkWh7XHOCYpwSzNmBsc2tn5bzMNa0cvjGKUHH3HysWJ07er+Z17F71QW3SAu/OE08y7jA3Ae
ItAYzIWxETBOHMp5nqYdL6BmA6nV1Vga4qasAGd4tUKJwvDtyV5e4ZxxfzOrMtJ7U/+SIjmb6mPnWe8g
Ew6cWci4ambUn5YeYEApU8+U7DmJA Pavuj1n/SBVtqe02e8vyNHtt8k33td1vNapa2bDymfYBzLsoAT
hWoJxumiqI0QN9Fvws1N1Y3WcZLqLihOI9IbYr0WHT8KQgdLaH4JR1QmJ8tJ1wBN0vaZJV8j8bQXhWS6
PXCRthmW02U7qkEPrl1+U5MDaRALKcFuTiuXmXakiO29C+/4qQ8AKUK6W1Ek7RQTBXVHMXFuHTFDc7NL
i64hygAHRqFkwOUVZhckhMDJwFuDUpto07eMq4exdYeApPeVmvmAInTPUhsoVjqqUnTMqDE+oYxuw1BXz
vhq6txafDqMyeL7Y+g9sJ7r7z7r8FEXHctPrm1j73eCAGL5uyqZE6QCOh6Yo3ZLDbLLWQKxTUo0miGjY
YgoYekIDM3qSC/yw1X/3Emk0Wijs0VfflwYS3UvG7RmPFheKeRucsV7nS0yrPCD2s1hVbHVXEn8i7ANI
zExab/RTuTHX3p0YA4EBvjXEveoM96hmz2d+/JQZkv0hQkOwXp7GxatsESyC4qHDInY1QiGo+QDgJvR
WLKxUSP1Jn615smz/sB11AfAvJrk3M26batuU0Gg4f7/Vic6LH9nf2iZCg2875QbpDvbftGcyaqegSu
2aTxHnClq+ijzdi15X0nMX7BP1WZ+0d3X0c6qUwN2wpeT7hCQN7mDvQGQ0PIittzALNuzK+bd01QX5cX
Nfy1gVAKjHhkzwF1abjcwYUwxaEWj4Y2bn+sDX8A8Vurg2tqJ9DwG1ovRp22+rktG81GFArxXHtvjpwg
r4E0y0eY+76H8TDm6Q6fVpJbWOKNmKGxoSbaNpgmV8GFkrJC9gLH0YHMccGjcsUyuwtxUr68Zl+g/g0M
Dvkg3gw6GUgUrMg8jVNG0JA+VYrqZRMi9QH6FBPmyYFzoCw6jabcAlxkUXTMkwTzkxt/NvyrDuOpnU8J
Rxssn18jSP89UMI9T81MdMj1apBSgZVzs181Wa0yuxRs3kn7T+IkPipAbBYSGGRZWSi0dkfRh6Vp7u9C
prBDHon8ECWHESJPJHuvS4BWYxp7xBQTxgFekOzMZA2AOvv78NIxvPGYnfaM+Kld6J3vDITczAiyia8
fAY/ULznCbP5Ia2jdRsSOi2WQbh8RMPmy6HGD7u8dBu2vC9LpKOKqi/2CdB/wYmify+IqqYJAH/44fb
t4qoBzYDcDgSWGGRocXogD7pfOsRuQrD5s2Dn3nuVEJOxNi dDW0IkuoajDNgLzJDok0ffHznwh4LKKvY
ACEo2gqHnVnyTPlhN</SigUser>
```

```
<Empfaenger id="L">
  <Ziel>BY</Ziel>
</Empfaenger>
<HerstellerID>74931</HerstellerID>
```

```
<DatenLieferant>MIIICQwYJKoZIhvcNAQcDoIICNDCCAjACAQAxggGLMIIBhwIBADBeMFkxCzAJBgNV
BAYTAKRFMQ8wDQYDVQQKEwZFTFNURVIxDDAKBgNVBAAsTA0VCQTEPMA0GA1UEAxMGQ29kaW5nMRowGAYD
VQQFEExyMDA5MDcyOTE1NTQ0MXgwMAIBADAeBgkqhkiG9w0BAQcwEaIPMA0GCSqGSIB3DQEBCQQABIIB
AF1jdjhKm1/PSOJTF2RaKRwiAxH06yWzURZGjLkkJhcY1IPPRGQ+nPEmda8tIa2POY//e0QC/Dx25is
9w0TQw7jDNezAy7rsFJtCRfg2oAdHAL9PKC7RXnQJe2Q7U0Hv1ACJTM48MBFmVxu7W+kvpQNJUWFCjKF
tfz9GUoJ0iLbPyBaj13PBh1RA925OXf21b/x+HoS6GtE+Ni/jFJeWnVDI7YVCNc6JkcC6Jj2x3kj0FD9
KmdzPIxZ5qdAOzO9mMLd0XTkDWpn7i7+SvYibVOgi6vnG0z6fSSOA0mmUBBcaqgZKnLcS03ZQoYuk7p
1eHW4wrtFFnKE0IEW9AOEmAwgzsGCSqGSIB3DQEHAATAUBggqkhiG9w0DBwQI72KU/a3B5ZGAeO1+f1wV
Q2yun0eyzo5fg/0B9G55s2Tz1xQkfXg1KLKg5gOrNqZBDZkTD0ccwBItamSDinFlUI6Slh//kzuBi/6H
8v1aCe61MaX+LD6RseNTEOTvKYz1B8cf0QXHuZzFw1E3JcinPOgrov5VMVbR8MuRP9jpB4reTg==</Da
tenLieferant>
```



```
<Datei>
  <Verschluesselung>CMSEnvelopedData</Verschluesselung>
  <Kompression>GZIP</Kompression>

<TransportSchluessel>MIIGRgYJKoZIhvcNAQcDoIIGNzCCBjmCAQAxggGLMIIBhwIBADBeMFkxCzA
JBgNVBAYTAkRFMQ8wDQYDVQQKEwZFTFNURVIXDDAKBgNVBAstA0VCQTEPMA0GA1UEAxMGQ29kaW5nMRow
GAYDVQQFEyMDA5MDcyOTE1NTQ0MXgwMAIBADeBgkqhkiG9w0BAQcxEaIPMA0GCSqGSIb3DQEBCQQ
ABIIBACcSOI3aIzOjEQmm8O4OPLK/wboryCL+mQtOl5x6ihzKQiDftbGjyKluaV1y6pKEExgXxCr1ON1+
zsYwURRmYn/YHO2ds3jaeDhBOgnAijvUY16P0XYE1GHPMAmMLweuaMAN07bnFxQa1XLl8ulqkEP7anhZ
t1JVCkjKeXyQ4iNq1PhWxaXbe9Zx3OzjSNG7kNnKjy1HSjN3QmvxGvRy+ywrt2YRH8u5uQD4ZPhoyRwA
hgoSPQ5t8Qs/mU7p3hkG1UqWzNxCCULMxuVJCtEU4vxBTyqj/wd+TS9C1gEAX1GSOfKAFR4yMxnXN1C+
AerAjQ7SbcXgYRPij1yOUPTrLoGMwggSdBgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECMS35WEgs1hIgII
EeORXh4oNNLPWYPsFKGjMYuFFwpAInC9n0VOZDFNxVuWgISxDeGsMOI4GljocNFTqe19TGi/zOL6/l+Q
kSupu+iFvNgOya0St938H2jFANvdCU6eRz1AQTAZ2Y3yrSnovIppbR0Nt29Op/dZhXZ6tqr9SgXzvac/
RRXRF8naI EraQW7a91M7AcK8g8DeS0oW2/Hj+XaTezSNrdzEi9645S8s3Lew1uXnUR36notwFSeGWia
EV6fxKJ8MTVCrqLLXz8otqvqXvy+9Ff+ppU561+SprqxVHuwpC8flynobdHxoNF1vBKKnE9vLM1R/U4e
sbv/MoOikUHXORFRuCICl1dfv0aABBbL8NNsLeEVTv2236/yN2wJUWYtTWWvr7gg908eXHLQWveB85Id
2ecS5xGRScFXbyAwzGTk9Z4cBpNGttET0PkLZCxH8FEAzp46ac60HCjsCFpAtp36ZFW8+I8y1BiwKXYo
5PyOVQuSK5lx0p3os26ACA+PUMZ9Mog1SduhBXCq3aB68jb3djd/S0kgz0BFQSzhEWoWteeC0HdgJ1K
vD3L1VONfbVW6K8HQolt614jt97g8a+euxdCw56h2owjY+LJQUVTyfpUybUmelnG2o2yzCgXTGwU6jOQ
1j3aY1S5u+GVEtDjDFtPoHxrwDwvfnLwZCJSvi4P8Hndj3BIGTN49F1N1X18XAT/kqVXJ8RT4v3imLx2
JnxsLAruRGX8YHTEZtkhjUzXPodNs7L4v5JncMuyUPyGdzgr1JAOIN5x6iqKTFsMhHBU/+RM4tNzxu8/
vqou3vjZaYShMZJFjt/WvPoBMy1z4I4STUS10//bpDdWua3M3P2hBCN3ViwFtsuoAocEiTlZMwpmtVu0
weoS56JrZxZYRFs5Qc/jQUQnJz8Fo+qFA126+UfAErkhWfTMB4LssY6mwH/YlsJCC0OInAoSKMAZ8O20
Byy7YHSnHB4r/47I4Cmy4E73/kxBKHpr7xYnu9Ig+fI59azFBxEziWxrD9pelj9wu8NumY2fRIYfi0YDt
ZLI+NLdq28MnhSL0tzQc1pjhhpWCyngjmQGbo+5E2LW0cXkktTbXCwmLhvKL1U8XQchLc1KXIVvqXv+w
JJd5iaJ4qQeTWULat5/6kCkZnSCz4+uvKouLU8FDWKR332JadTidXVaTAEfPnFRID5voCgXmfDaiTt+x
fyGhxqJvB5kL13A2Z6waDlGERrOpRGfhQ/c1XP2mbthrF6U5mrl1Xk8KUeApToKpF3NcpCF8HaJxJzoZ
+ets1yOBt2EqCgjnhtLIRWLaCBkC+k9GPrPIfuRCz1lOp2Q0l10IEqrzJ8pB1j4z4D6rgyV1JdNU5Yp
EmrbnmPxeHUDFxByVZk8vPQ1binZSUv1l1KQK4YI/eYLT1IQUtxwO6o2qHV5qQRHw6kP0aABNk9eBpY3
CCv0QLed68/Lz3QrxquQpNvmb7xfXNeKu44xBJrqZQ12F2zOcUTDuWiYpw6idcGm7MTT9xBmj7fZrckg
Tc5yEgsk=</TransportSchluessel>
  </Datei>
</TransferHeader>

<DatenTeil>MIIEhgYJKoZIhvcNAQcDoIIEdzCCBHMAQAxggGLMIIBhwIBADBeMFkxCzAJBgNVBAYTA
kRFMQ8wDQYDVQQKEwZFTFNURVIXDDAKBgNVBAstA0VCQTEPMA0GA1UEAxMGQ29kaW5nMRowGAYDVQQF
xEyMDA5MDcyOTE1NTQ0MXgwMAIBADeBgkqhkiG9w0BAQcxEaIPMA0GCSqGSIb3DQEBCQQABIABN15
SJjJStRsNMLxKTy2cP/hnXAzqU9wVVFiXE1ePiCiJ1EP8oTEfJSooAig0jmOI88PDbHTy6iNmY+LPS62
QWulgJtg6x10QpAah7tJ825zT88M2H21ZAx2OyK+XTvQma6E4s5Z1w7ZwldQWEg7vIohnNL7UyvoE1SQ
e6aHuvuxCm4dvsBjMV5YU1IRM37+m4g1H7XRY3etPQkqgibt98QG8gcXzjoZzIsVSr+13xWRvjHA8GUO
ZWRHIB5vY4kiMCU1IsAXB0HJr+HJ7uAoXbK961L8QnVMPWYr8Sb6EkxMkAlka4HzA5UNCscfHAFkf
+RaNnbRjFi4cq6uBwgwgLdBgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECOAjeKwMwc3/gIICuOfODHgb
N9upnIp17avgK1NagK0OdgUU6cnW1ztEw6Js+mZp1Wt+vU72y+Xro/hv1B05s0vrnsNbzwAHelpbxoL
pR1xdZMXOISwZie2FnHuVaTIf1Fp2WMkQWmLttGkxtU7RRTv1ugseMB8ElgIBKGcrmzijjIntZEfwgS
o5ci9IK8SBJutTv56sZzTqvfp77d+OraHmvBgr4OKPnonetGxbU9GKav1FFN26pUyXPNkt4ZNPLtIVA
Bsb3SEotBTsJok0kYSmHVM88wAS0CuVVPK9D6BRQII/zENqUT4MJMd0bvlojG/haXCdPBV78qoQG2PTS
5DJuoVX4JbKOJooWoyMx9Am4wBSzwTfJcmwUhohJTZNpdLBpPxzwBkq8IFU7SfwYKnK/ZX8tmpipd0
yE17UKYYe3j07Onu72+H0zGBM2iDUAoqmBMaimDD5+1Ajs1grXULL90EkiAU/Qw8wxpxcx+8Pt1FpD27
5v828LNxuNkAyUbhcQ7zlpvPbhq69h6G1auKCULVyo00gf0+01gb500VGrUevP9YpzsHrdVrXAf
h2Mc
5eN8PO+WBoM30pKcWknGbzyTivi9Lo1rIyp1p8w3LuGZfaxxf1XuD+Fjw9QXDMrnzzF2hZKI3AEJUja
sqE2oqItjUL2iI5wuptcK10E3z3puijed+iam6S+WG1A9vf26CnVF9A1alyMiJpmmyjOpudMsHieDOF
Wx5Ts8Yd3yeASoTJRktqD6DgZ+UNSfOdLqyvk7cluqFtrj6LUMzqu87EPL697bjn5H1iBzEnojZFrZ2
pkj3bPd1D7uK+XFh6zEenSVX8tRmAv1e6tyTetFkwhdvK9ur5+G9VrZzeGAAe5kaR8BqtgzBOPtamdh2
Vc72aGFqml3aduwHF1gZ1NeDfK0md5qost4Wr6gow==</DatenTeil>
</Elster>
```



## 6 Abkürzungsverzeichnis

Abkürzung	Erklärung
RBM	Rentenbezugsmitteilung
UUID	Universally Unique Identifier
TH	TransferHeader: Spezieller Bereich innerhalb des XML-Datensatzes von ELSTER
NH	NutzdatenHeader: Spezieller Bereich innerhalb des XML-Datensatzes von ELSTER



## A RSAES-OAEP (standardisiert im PKCS#1 ab der Version 2.1)

Für die Verschlüsselung mit RSAES-OAEP müssen folgende Parameter verwendet werden:

- Hash-Algorithmus: SHA256  
Falls dieser nicht unterstützt wird, ist SHA-1 zulässig
- Mask Generation Function: MGF1 mit SHA-256  
Die Hash-Funktion der Mask Generation Function muss identisch mit der Hash-Funktion aus dem oberen Punkt sein. Eine Mischung zwischen SHA-1 und SHA-256 ist nicht zulässig.
- pSourceAlgorithm: id-pSpecified mit leerem String (entspricht dem Default-Wert)

Die Antworten der Clearingstelle mit RSAES-OAEP werden immer als Hash-Algorithmus SHA-256 verwenden. Testdaten befinden sich im Entwicklerbereich der ELSTER-Webseite.