EGIZ

www.egiz.gv.at
E-Mail: post@egiz.gv.at
Telefon: ++43 (316) 873 5514
Fax: ++43 (316) 873 5520
Inffeldgasse 16a / 8010 Graz / Austria

Webservice Schnittstelle für das Signaturprüfservice

Konzept und Dokumentation

Graz, am 12. Mai 2021

DI. Alexander Marsalek – alexander.marsalek@iaik.tugraz.at
DI. Dominik Ziegler – dominik.ziegler@iaik.tugraz.at
DI. Thomas Lenz – thomas.lenz@egiz.gv.at

Zusammenfassung:

Ziel dieser Arbeit war, das bestehende Signaturprüfservice um eine Webservice-Schnittstelle zu erweitern. Durch diese Schnittstelle soll das Signaturprüfservice seine Funktionalität anderen Applikationen über eine standardisierte Schnittstelle zur Verfügung stellen. Als Standard für dieses Webservice wurde SOAP in der Version 1.2 verwendet, wobei aus Kompatibilitätsgründen auch SOAP in der Version 1.1 angeboten wird. Das XML Schema für diese Schnittstelle ist an MOA-SPSS angelehnt, wobei eine exakte Umsetzung der MOA-SPSS Spezifikationen aus Anforderungsgründen nicht angestrebt wurde.

Die Webservice-Schnittstelle nimmt beliebige signierte Dokumente an, ermittelt das Format und prüft die Signaturen. Anschließend wird der Prüfbericht in der gewünschten Sprache erstellt, signiert und an die Anwendung retourniert. Zusätzlich zum XML-Bericht kann ein PDF-Prüfbericht angefordert werden.

Inhaltsverzeichnis:

Revision History

Version	Datum	Autor(en)	
1.0	24.04.2012	Thomas Lenz	erstellt.
1.1	20.12.2012	Thomas Lenz	XML Schema überarbeitet
1.2	15.04.2013	Alexander Marsalek	Erweiterung der Prüfschnittstelle
1.3	27.05.2015	Alexander Marsalek	Erweiterung der Prüfschnittstelle (Detached-Signaturen, RequestSignerCertificate)
1.4	11.04.2017	Alexander Marsalek Dominik Ziegler	Erweiterung der Prüfschnittstelle
1.5	12.05.2021	Alexander Marsalek	Erweiterung der Prüfschnittstelle

1 Einleitung

Das Signaturprüfservice zur automatischen Überprüfung von digitalen Signaturen ist in der aktuellen Form seit einigen Jahren unter www.signaturpruefung.gv.at in Betrieb. Hierbei kann über ein Web-Frontend das zu prüfende Dokument manuell ausgewählt und an das Prüfservice übertragen werden. Dieses Dokument wird automatisiert geprüft und nach Abschluss der Prüfung wird dem/der Anwender/in ein signierter Prüfbericht übermittelt.
Es zeigte sich jedoch, dass die Schnittstelle über das Web-Frontend für automatisierte Anfragen an das Prüfservice nicht optimal ist. Ziel dieses Projekt war es, das Signaturprüfservice um eine Webservice-Schnittstelle zu erweitern, um auch automatisierte Anfragen in einer geregelten und standardisierten Form verarbeiten zu können.
Dieses Dokument stellt eine Erweiterung zur Dokumentation des Signaturprüfservice [DOKPR] dar und beschreibt somit ausschließlich die Neuerungen und Änderungen, die sich durch die Integration der Webservice-Schnittstelle ergeben.
In den nachfolgenden Kapiteln werden die Schnittstellenspezifikation und die Integration der Webservice-Schnittstelle in das Signaturprüfservice beschrieben.

2 Schnittstellenspezifikation

Für die Webservice-Schnittstelle wird das SOAP Protokoll mit HTTP Binding verwendet. Die Schnittstelle basiert auf der SOAP Version 1.2 [SOAP12]. Aus Kompatibilitätsgründen wurde die Schnittstelle jedoch auch für SOAP Version 1.1 [SOAP] konfiguriert. Die WSDL Spezifikation beruht auf der WSDL Version 1.1 [WSDL]. Die Bindung des SOAP Protokolls an HTTP hat sich als günstig erwiesen, da diese Schnittstelle bereits vom Web Frontend verwendet wird und somit eine einfache Integration in bestehende Systeme möglich ist.
Das SOAP Protokoll beschreibt jedoch nur den Transport von Nutzdaten über das Netzwerk. Die Nutzdaten müssen bei SOAP in einer eigenen XML Struktur gekapselt werden. Da es sich in diesem Fall um ein Signaturprüfservice handelt, ist es naheliegend, als Basis für dieses XML Nutzdaten Schema, einen Standard für digitale Signaturprüfung zu verwenden. Hierbei bieten sich die beiden Standards MOA-SPSS [MOA] und OASIS-DSS [OASIS] an. Diese beiden Standards spezifizieren Webservice-Schnittstellen für die Überprüfung von digitalen Signaturen nach dem XMLDSig Standard [XMLDSig] und dem CMS Standard [RFC 3369].

2.1 Anforderungen

Um die aktuell durch das Signaturprüfservice angebotene Funktionalität auch über die Webservice-Schnittstelle anbieten zu können, müssen folgende Informationen über diese Schnittstelle ausgetauscht werden:

Anfrage:

- Das zu prüfende Dokument.
- Referenzen
- FileID
- Trust Profile
- Auswahl der Sprache der Prüfantwort (Deutsch oder Englisch).
- Auswahl des Formats der Prüfantwort (nur XML Bericht oder XML & PDF Bericht).
- Auswahl ob Zertifikate des Unterzeichners benötigt wird.

Antwort:

- FileID
- Dokumententyp
- Hashwert des geprüften Dokuments.
- Prüfbericht für alle Signaturen.

  - Unterzeichner
  - Prüfwerte (Signatur, Zertifikat, Manifest)
  - Signierte Daten
  - Anmerkungen zur Signatur.
- Prüfbericht in der gewünschten Sprache, im XML Format, optional auch im PDF-Format.
- Der Prüfbericht soll vom Prüfdienst signiert werden.

Durch den Betreiber können die möglichen bzw. standardmäßigen Antwort- und Sprach-Varianten über die Konfiguration eingestellt werden. Dies vor allem auch, da die XML- und PDF-Prüfberichte unterschiedliche Belastungen des Prüfservices im Massenbetrieb haben.

Konfiguration:

- Berichte im PDF-Format ermöglichen
- Default-Sprache der Antwort, sofern nicht im Request angegeben (Deutsch)
- Unterstützte Sprachen definieren/einschränken

Die geforderte Funktionalität an die Webservice-Schnittstelle wird jedoch von keinem der beiden Standards (MOA-SPSS, OASIS-DSS) vollständig abgebildet. Im Besonderen konnte der Dokumententyp und der Prüfbericht für jede Signatur am Prüfdokument in dieser Form, durch keinen der beiden Standards vollständig abgebildet werden. Da der gesamte Prüfbericht durch den Prüfdienst auch signiert werden soll und keiner der beiden Standards alle Anforderungen erfüllt, wurde für die Spezifikation der Schnittstelle eine MOA-SPSS nahe Implementierung gewählt, da dadurch ein Bezug zur im österreichischen E-Government bereits existierenden Infrastruktur gegeben ist.

2.2 Anfrage

Abbildung 1 zeigt die XML Struktur der Anfrage an das Signaturprüfservice.

```
<xsd:element name="VerifyDocumentRequest">
  <xsd:complexType>
  <xsd:sequence>
    <xsd:element minOccurs="0" name="Version" type="xsd:int"/>
    <xsd:element name="Document" type="xsd:base64Binary"/>
    <xsd:element maxOccurs="unbounded" minOccurs="0" name="ExternalDocuments"
type="xsd:base64Binary"/>
    <xsd:element minOccurs="0" name="FileID" type="xsd:token"/>
    <xsd:element minOccurs="0" name="TrustProfileID" type="xsd:token"/>
    <xsd:element minOccurs="0" name="RequestPDFReport" type="xsd:boolean"/>
    <xsd:element minOccurs="0" name="Language" type="xsd:string"/>
    <xsd:element minOccurs="0" name="RequestSignerCertifcate"
type="xsd:boolean"/>
    <xsd:element minOccurs="0" name="RequestVerificationTime"
type="xsd:boolean"/>
```

Abbildung 1: Anfrage an das Signaturprüfservice

Die Anfrage kann aus bis zu acht Elementen bestehen, dem zu prüfenden Dokument und den sieben optionalen Elementen *‚Version‘, ‚ExternalDocuments‘, ‚FileID‘, ‚TrustProfileID‘, ‚RequestPDFReport‘*, *‚Language‘* *‚RequestSignerCertificate‘* und *‚RequestVerificationTime‘*. Pro Anfrage kann ein Dokument und beliebige viele

Referenzen an das Prüfservice übermittelt werden. Die Referenzen (*‚ExternalDocuments‘*) werden nur für „Detached“-Signaturen benötigt. Bei einer „Detached“-Signatur handelt es sich um eine Signatur in einer separaten Datei. Alle Dokumente müssen BASE64 codiert übermittelt werden. Die Identifikation des Dokumententyps wird serverseitig vorgenommen und somit ist die Anfrage für jeden Dokumententyp identisch. Das optionale Element *‚Version‘* wurde für zukünftige Erweiterungen hinzugefügt und erlaubt die Version des Anfrage zu definieren. Aktuell werden Anfragen der Version ‚1‘ oder ‚2‘ und Anfragen ohne dem Element *‚Version‘* unterstützt. Das optionale Element *‚FileID‘* kann zur Identifikation des Dokuments bei der Anfrage angegeben werden und wird identisch in die Antwort eingefügt. Falls ein PDF-Prüfbericht angefordert wird, wird *‚FileID‘* als Dateiname der zu prüfenden Datei im PDF-Prüfbericht verwendet. Die Anforderung eines speziellen TrustProfiles (siehe MOA-SPSS Spezifikation [MOA]) für die Signaturprüfung ist auch für die Webservice-Schnittstelle vorgesehen. Dieses Element wird jedoch in der aktuellen Version nicht unterstützt, da eine generelle Verwendung bei allen Dokumententypen aktuell nicht möglich ist. Für eine generelle Unterstützung müsste PDF-AS so erweitert werden, dass bei der Signaturprüfung mit PDF-AS ebenfalls ein TrustProfil angegeben werden kann. Diese Funktionalität ist jedoch nicht gegeben. Zusätzlich ergibt sich durch die Verwendung von TrustProfilen die Schwierigkeit, dem/der Anwender/in Informationen über die aktuell verfügbaren TrustProfile und deren Inhalte zugänglich zu machen, da dieser Parameter andernfalls nicht sinnvoll verwendet werden kann. Eine solche Funktion wird von MOA-SP/SS jedoch nicht zur Verfügung gestellt. Wenn das optionale Element *‚RequestPDFReport‘ auf ‚true‘* gesetzt ist, wird zur Antwort des Webservices ein PDF-Prüfbericht hinzugefügt. Das optionale Element *‚Language‘* erlaubt die Wahl der Sprache der Antwort, gültige Werte sind *‚de‘* für Deutsch und *‚en‘* für Englisch. Über das optionale Element *‚RequestSignerCertificate‘* kann das Zertifikat des Unterzeichners angefordert werden und das optionale Element *‚RequestVerificationTime‘* kann der Zeitpunkt angefordert werden, zu dem die Unterschrift geprüft wurde.

2.3 Prüfantwort

Abbildung 2 zeigt die XML Struktur der Antwort vom Signaturprüfservice.

```
<xsd:element name="VerifyDocumentResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="0" name="Version" type="xsd:int"/>
      <xsd:element name="VerificationReport"
type="tns:VerificationReportType"/>
      <xsd:element minOccurs="0" name="PDFDocument"
type="xsd:base64Binary"/>
      <xsd:element ref="dsig:Signature"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Abbildung 2: Antwort vom Signaturprüfservice

Die Struktur beinhaltet bis zu vier Elemente. Das optionale Element *‚Version‘* ist wie bei der Anfrage für zukünftige Erweiterungen vorgesehen. Aktuell wird es zur Antwort hinzugefügt wenn die Anfrage ein *‚Version‘* Element enthält. Das optionale Element *‚PDFDocument‘* wird zur Antwort hinzugefügt, falls bei der Anfrage das Element *‚RequestPDFReport‘* gesetzt ist. Das Element enthält den Base64-kodierten signierten PDF Prüfbericht. Die Prüfantwort enthält noch den XML- Prüfbericht als

‚*VerificationReport*' und eine Signatur ‚*Signature*', welche die Unterschrift für den gesamten Prüfbericht darstellt. Diese Signatur ist als „enveloped-signature" laut XMLDSig Standard in die ‚*VerifyDocumentResponse*' eingebunden und deren Aufbau kann dem XMLDSig Standard [XMLDSig] entnommen werden. Die XML Struktur des ‚*VerificationReport*' Elements ist in Abbildung 3 dargestellt.

```
<xsd:complexType name="VerificationReportType">
  <xsd:sequence>
    <xsd:element name="FileInfo" type="tns:FileInfoType/>
    <xsd:element name="SignatureInfo" type="tns:SignatureInfoType"/>
  </xsd:sequence>
</xsd:complexType>
```

Abbildung 3: XML Struktur - VerificationReport

Der ‚*VerificationReport*' besteht aus zwei Elementen. Das erste Element ‚*FileInfo*' beinhaltet Informationen zum gesamten Dokument. Das zweite Element ‚*SignatureInfo*' beinhaltet die Ergebnisse der Prüfung einer Signatur. Dieses Element kann auch mehrfach auftreten, sollten im Prüfdokument mehrere Signaturen erkannt werden. Der Aufbau des Elements *‚FileInfo'* ist in Abbildung 4 dargestellt und besteht aus drei Elemente, welche Informationen zum gesamten Dokument beinhalten.

- **FileID:** Dieses optionale Element beinhaltet die Kennung, welche in der Anfrage für das zu prüfende Dokument angegeben wurde. Sollte in der Anfrage keine Kennung angegeben worden sein ist dieses Element nicht vorhanden.
- **FileType:** Dieses Element beinhaltet den Dokumententyp der durch das Signaturprüfservice ermittelt wurde.
- **File-Hash:** Dieses Element beinhaltet den SHA1-Hash in BASE64 encodierter Form über das gesamte Dokument, welches zur Signaturprüfung an das Prüfservice übertragen wurde.

```
<xsd:complexType name="FileInfoType">
  <xsd:sequence>
    <xsd:element name="FileID" type="xsd:token"/>
    <xsd:element name="FileType" type="xsd:string/>
    <xsd:element name="File-Hash" type="xsd:base64Binary"/>
  </xsd:sequence>
</xsd:complexType>
```

Abbildung 4: XML Struktur - FileInfo

Abbildung 5 zeigt die XML Struktur des *‚SignatureInfo'* Elements aus Abbildung 3.
Zu jeder Signatur am Prüfdokument gibt es im Prüfbericht ein *‚SignatureInfo'* Element, welches folgende Informationen beinhaltet.

```
<xsd:complexType name="SignatureInfoType">
  <xsd:sequence>
    <xsd:element maxOccurs="unbounded" minOccurs="0" name="InputData"
type="tns:ContentExLocRefBaseType"/>
    <xsd:element name="SignerName" type="xsd:string"/>
    <xsd:element minOccurs="0" name="SignatureCheck"
type="tns:CheckResultType"/>
    <xsd:element name="CertificateCheck" type="tns:CheckResultType"/>
    <xsd:element minOccurs="0" name="ManifestCheck"
type="tns:ManifestCheckType"/>
    <xsd:element minOccurs="0" name="Annotations"
type="tns:AnnotationsType"/>
    <xsd:element minOccurs="0" name="SignerCertificate"
type="xsd:base64Binary"/>
    <xsd:element minOccurs="0" name="VerificationTime" type="xsd:string"/>
    <xsd:element minOccurs="0" name="SignatureType" type="xsd:string"/>
    <xsd:element maxOccurs="unbounded" minOccurs="0" name="SignedFile"
type="xsd:string"/>
    <xsd:element minOccurs="0" name="IssuerCountryCode" type="xsd:string"/>
    <xsd:element minOccurs="0" name="ByteRangeCovered" type="xsd:string"/>
    <xsd:element minOccurs="0" name="SignatureAlgorithm" type="xsd:string"/>
    <xsd:element minOccurs="0" name="signatureCoversFullPDF"
type="xsd:boolean"/>
    <xsd:element minOccurs="0" name="TSLInformation"
type="tns:TSLInformationType"/>
  </xsd:sequence>
</xsd:complexType>
```

Abbildung 5: XML Struktur - SignatureInfo

- **InputData:** Das Element *‘InputData’* ist optional und beinhaltet die der Signatur zugrundeliegenden Daten in BASE64 encodierter Form. Dieses Element ist je nachdem welcher Dokumententyp ermittelt wurde, vorhanden. (siehe Dokumentation Signaturprüfservice [DOKPR] Kapitel 2.2). Zusätzlich wird der Dokumententyp angegeben, um eine korrekte Darstellung der encodierten Daten zu ermöglichen. Die XML Struktur dieses Elements ist in Abbildung 6 dargestellt.
- **SignerName:** Dieses Element muss vorhanden sein und beinhaltet den Namen des Signators der jeweiligen Signatur.
- **SignatureCheck:** Das Element *‚SignatureCheck‘* beinhaltet das Prüfergebnis zur Signatur als Ergebniscode *‚Code‘* und als textuelle Kurzbeschreibung *‚Info‘*. Diese Ergebniscodes sind identisch zu den in der Spezifikation von MOA-SP [MOA] angegebenen Ergebniscodes und können dieser Spezifikation entnommen werden. Zusätzlich wird auch eine textuelle Beschreibung des Ergebnisses mitangegeben. Die XML Struktur dieses Elements ist in Abbildung 6 dargestellt.
- **CertificateCheck:** Das Element *‚CertificateCheck‘* beinhaltet das Prüfergebnis zum Zertifikat als Ergebniscode und als textuelle Kurzbeschreibung. Die Spezifikationen zu den Prüfcodes sind identisch zu den in der Spezifikation von MOA-SP [MOA] angegebenen Ergebniscodes und können dieser Spezifikation entnommen werden. Zusätzlich wird eine textuelle Beschreibung des Ergebnisses angefügt. Die XML Struktur dieses Elements ist in Abbildung 6 dargestellt.
- **ManifestCheck:** Das Element *‚ManifestCheck‘* beinhaltet zwei Subelemente. Eine allgemeine Information zum Manifest mit Checkcode und textueller Kurzinfo und ein zweites optionales Element mit den Ergebnissen der MOA-SP XMLDsig Manifest Prüfung. Diese Ergebniscodes sind identisch zu den in der Spezifikation von MOA-SP [MOA] angegebenen Ergebniscodes und können dieser

Spezifikation entnommen werden. Zusätzlich wird eine textuelle Beschreibung des Ergebnisses angefügt. Die XML Struktur dieses Elements ist in Abbildung 6 dargestellt.

- **Annotation:** Das Element *‚Annotations‘* beinhaltet Anmerkungen zur jeweiligen Signatur. Diese Anmerkungen können mehrfach vorhanden sein und werden sowohl als Ergebniscode, als auch als textuelle Kurzinformation angefügt. Die XML Struktur dieses Elements ist in Abbildung 6 dargestellt. Die Ergebniscodes für Anmerkungen sind in Tabelle 1 dargestellt.
- **SignerCertificate:** Dieses Element enthält das BASE-64 kodierte Zertifikat des Unterzeichners.
- **VerificationTime:** Dieses Element enthält den Zeitpunkt der Signaturprüfung.
- **SignatureType**: Dieses Element gibt den Signaturtyp an.
- **IssuerCountryCode:** Dieses Element enthält den Ländercode des Zertifikatsaustellers.
- **ByteRangeCovered:** Dieses Element gibt bei PDF-Signaturen den von der Signatur abgedeckten ByteRange ab.
- **SignatureAlgorithm:** Dieses Element enthält den verwendeten Signaturalgorithmus.
- **signatureCoversFullPDF:** Dieses Element gibt an ob die Signatur das gesamte PDF abdeckt.
- **TSLInformation:** Dieses Element ist nur vorhanden wenn Informationen zu dem Zertifikat auf der TSL gefunden wurden. Die Subelemente enthalten detaillierter Informationen, wie das Herausgeberland, den ServiceTypeStatus und den ServiceTypeIdentifer.

```
<xsd:complexType name="ContentExLocRefBaseType">
  <xsd:sequence minOccurs="0">
    <xsd:element name="Base64Content" type="xsd:base64Binary"/>
  <xsd:element name="FileType" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="AnnotationsType">
  <xsd:sequence>
    <xsd:element maxOccurs="unbounded" minOccurs="0" name="Annotation"
type="tns:CheckResultType"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ManifestCheckType">
  <xsd:sequence minOccurs="0">
    <xsd:element minOccurs="0" name="Manifest" type="tns:CheckResultType"/>
    <xsd:element minOccurs="0" name="XMLDsigManifest"
type="tns:CheckResultType"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CheckResultType">
  <xsd:sequence>
    <xsd:element name="Code" type="xsd:integer"/>
    <xsd:element minOccurs="0" name="Info" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="TSLInformationType">
  <xsd:sequence>
    <xsd:element name="TSLIssuerCountryCode" type="xsd:string"/>
    <xsd:element name="ServiceTypeStatus" type="xsd:string"/>
    <xsd:element name="ServiceTypeIdentifier" type="xsd:string"/>
    <xsd:element maxOccurs="unbounded" minOccurs="0" name="Qualifier"
type="xsd:string"/>
    <xsd:element maxOccurs="unbounded" minOccurs="0"
name="AdditionalServiceInformation" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
```

Abbildung 6: XML Struktur - Verschiedene Infotypen

Tabelle 1: Annotation Ergebniscodes

Code	Beschreibung
8800	Das Dokument ist für die Bundesverwaltung geeignet.
8801	Das Dokument ist NICHT für die Bundesverwaltung geeignet.
8802	Der Zertifizierungsdiensteanbieter wurde bereits bei einer früheren Prüfung als ungeeignet für die Verwendung für die Rechnungslegung begutachtet.

8803	Der Zertifizierungsdiensteanbieter ist nicht explizit als für die Rechnungslegung geeignet gekennzeichnet. Aus diesem Grund kann nicht ausgeschlossen werden, dass die Zertifizierungsstatements die Verwendung für die Rechnungslegung ausschließen.
8804	Alle Signaturen erfüllen die durch das BMF zu prüfenden Kriterien der Signatur.
8805	Zumindest eine der Signaturen erfüllt NICHT die durch das BMF zu prüfenden Kriterien der Signatur.
8806	Die Signatur erfüllt die durch das BMF zu prüfenden Kriterien der Signatur.
8807	Die Signatur erfüllt NICHT die durch das BMF zu prüfenden Kriterien der Signatur.
8808	Das Zertifikat erfüllt die technischen Voraussetzungen für eine Amtssignatur.
8809	Das Zertifikat dieser Signatur erfüllt NICHT die technischen Voraussetzungen für eine Amtssignatur, da der Aussteller nicht in der Liste der bekannten Aussteller für Amtssignaturen geführt wird.
8810	Das Zertifikat dieser Signatur erfüllt NICHT die technischen Voraussetzungen für eine Amtssignatur, da der Aussteller nicht in der Liste der bekannten Aussteller für Amtssignaturen geführt wird und der Vertrauensstatus nicht festgestellt werden konnte.
8811	Das Zertifikat dieser Signatur erfüllt NICHT die technischen Voraussetzungen für eine Amtssignatur, da der Vertrauensstatus nicht festgestellt werden konnte.
8812	Das Dokument wurde nach Aufbringung dieser Signatur ergänzt. Die Daten, die dieser Signatur zu Grunde liegen, sollten gesondert betrachtet werden.
8813	Diese Signatur umfasst nicht das vollständige Dokument. Die Daten, die dieser Signatur tatsächlich Grunde liegen, sollten gesondert betrachtet werden.
8814	Gewöhnliches Zertifikat.
8815	Qualifiziertes Zertifikat.
8816	Sichere Signaturerstellungseinheit
8817	Qualifiziertes Zertifikat (Quelle: TSL)
8818	Qualifiziertes Zertifikat (Quelle: Zertifikat)
8819	Diese Signatur bzw. dieses Siegel enthält zwei Erstellungszeitpunkte, einen der Dokumentenvorbereitung und einen des Signaturgeräts. Diese weichen voneinander um über übliche Verarbeitungszeiten hinausgehend ab, der tatsächliche Erstellungszeitpunkt sollte gesondert ermittelt werden.

2.4 Verarbeitungsfehler

Sollte während der Verarbeitung der Anfrage ein Fehler auftreten, wird dieser über eine geeignete Fehlermeldung an den/die Benutzer/in übermittelt. Die Antwort im Fehlerfall weist die in Abbildung 7 dargestellte XML Struktur auf. Diese XML Struktur besteht aus einem Fehlercode und einer textuellen Fehlerbeschreibung. In Tabelle 2 sind die Fehlercodes mit den dazugehörigen Fehlerbeschreibungen dargestellt.

```
<xsd:element name="ErrorResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ErrorCode" type="xsd:integer"/>
      <xsd:element name="Info" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Abbildung 7: XML Struktur - Error Response

Tabelle 2: Fehlercodes und Beschreibungen

Code	Beschreibung
1900	Die angeforderte Methode ist am Webservice nicht verfügbar.
1901	Die Anfrage beinhaltet kein Dokument.
1902	Fehler in der BASE64 Encodierung des Dokuments.
1903	TrustProfile werden aktuell nicht unterstützt. Entfernen Sie das Element ‚TrustProfileID' aus der Anfrage.
1904	Die angeforderte Sprache wird nicht unterstützt
1905	PDF-Prüfberichte werden nicht unterstützt. Schicken Sie die Anfrage noch einmal mit RequestPDFReport=false
1906	Die angeforderte Version wird nicht unterstützt. Schicken Sie die Anfrage noch einmal mit version=1
2100	Es konnten keine prüfbaren Signaturen gefunden werden.
2101	Überprüfen Sie, ob die Signatur mit der Liste der unterstützten Profile korrespondiert. Die Liste ist unter http://www.buergerkarte.at/signature-verification/service.do?action=showSupportedPDFASProfiles.
2102	Es ist möglich, dass vorhandene PDF-AS Signaturen durch die Software eines Drittherstellers entfernt wurden. Bitte aktualisieren Sie die Software, die Sie ggf. zum Signieren verwendet haben. Sollten Sie das gegenständliche Dokument selbst via E-Mail erhalten haben, speichern Sie es bitte direkt aus dem Mailprogramm heraus auf Ihrer Festplatte ab, ohne es dabei zu öffnen und wiederholen Sie die Prüfung.
2103	Dieser Dateityp wird nicht unterstützt.
2200	Das Dokument konnte nicht verarbeitet werden, da es geschützt (ggf. verschlüsselt) ist.

2201	Das PDF Dokument wurde nach Anbringen der letzten Signatur verändert. Möglicherweise enthält es aber auch mehrere Signaturen von denen nicht alle über die vorgegebenen Signaturprofile erkannt wurden.
2202	Die Signaturprüfung wurde so konfiguriert, dass ausschließlich binäre Signaturen geprüft werden. Das Dokument enthält jedoch nicht-binäre Signaturen.
2203	Dieser PDF-Signaturtyp wird noch nicht unterstützt.
2204	Das vorliegende Dokument kann nicht verarbeitet werden. Möglicherweise enthält es komprimierte Teile.
2205	Das vorliegende Dokument wurde mit einer Version von "a.sign VPDFSign" signiert, die nicht unterstützt wird. Bitte verwenden Sie das A-Trust Online-Verifications-Service https://www.a-trust.at/pdfverify.
2206	Es trat ein Fehler beim Prüfen der Signatur des vorliegenden Dokuments auf. Möglicherweise handelt es sich um eine Signatur eines Drittherstellers, die nicht unterstützt wird und/oder die Signatur ist nicht spezifikationskonform.
2207	Die Signatur des vorliegenden Dokuments konnte nicht geprüft werden, da diese nicht unterstützt wird. Möglicherweise handelt es sich um eine Signatur eines Drittherstellers. In diesem Fall verwenden Sie bitte die Software des Drittherstellers für die Prüfung.
2208	Die Prüfung dieser Version der Strafregisterbescheinigung wird derzeit nicht unterstützt. Bitte verwenden Sie den Prüfdienst, der im Signaturblock Ihres Dokuments genannt wird.
2209	Für diesen Dateityp werden keine separaten Signaturen unterstützt
3900	Während der Signierung des Prüfberichts ist ein Fehler aufgetreten.
4900	Das Dokument ist zu groß um verarbeitet werden zu können.
4999	Es ist ein nicht näher spezifizierter interner Fehler aufgetreten.

2.5 Funktionsbeschreibung

Die ersten drei Schritte der Dokumentprüfung sind äquivalent zu den in Kapitel 2 der Dokumentation des Prüfservices [DOKPR] beschriebenen Abläufen. Zusätzlich zu diesen Schritten sind in diesem Fall weitere Schritte erforderlich.

1. Anfrage mit signiertem Dokument.
2. Formaterkennung.
3. Signaturprüfung.
4. XML Prüfbericht Generierung.
5. Signierten PDF Prüfbericht generieren (optional).
6. Signierung des XML Prüfberichts
7. Antworten mit signiertem Prüfbericht

Im Schritt 4 wird der Prüfbericht im XML Format, laut Spezifikation aus Kapitel 2.3, erstellt. Im Schritt 5, der optional ist wird zusätzlich ein signierter PDF Prüfbericht erstellt. Im Schritt 6 wird der Prüfbericht zusätzlich durch das Prüfservice signiert. Hierfür wird eine Instanz von MOA-SS für die Generierung einer serverseitigen Signatur verwendet. Anschließend wird der signierte Prüfbericht an den/die Anwender/in retourniert. Sollte

während der Verarbeitung ein Fehler aufgetreten sein wird anstatt des Prüfberichts eine Fehlerbeschreibung retourniert.

3 Integration in der Signaturprüfservice

Die Webservice Schnittstelle ist über die http Adresse des Signaturprüftools erreichbar. Das nachfolgende Beispiel zeigt eine mögliche Variante dieser Adresse.

http://localhost:8080/signature-verification/services/VerificationService

Abbildung 8 zeigt beispielhaft eine SOAP Anfrage an das Signaturprüfservice. Die im Kapitel 2 dieser Dokumentation spezifizierten Teile der Anfrage sind orange eingefärbt. Der restliche Teil der Anfrage entspricht dem SOAP Standard in der Version 1.1.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:q0="http://reference.e-government.gv.at/namespace/verificationservice/20120922#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <q0:VerifyDocumentRequest>
   <q0:Version>1</q0:Version>
   <q0:Document>JVBE……</q0:Document>
   <q0:FileID>test.pdf</q0:FileID>
   <q0:RequestPDFReport>true</q0:RequestPDFReport>
   <q0:Language>de</q0:Language>
  </q0:VerifyDocumentRequest>
 </soapenv:Body>
</soapenv:Envelope>
```

Abbildung 8: Beispiel SOAP Request

3.1 Konfiguration

Die Konfiguration ist in weiten Bereichen identisch zur ursprünglichen Konfiguration des Signaturprüfservices (siehe Signaturprüfservice-Dokumentation [DOKPR]). Durch die Signierung des Prüfberichts sind jedoch zusätzliche Konfigurations-parameter nötig, die in der Kategorie *‚SS‘* zusammengefasst wurden. Die Konfigurationsmöglichkeiten des Prüfberichtes (Sprache, Format) wurden in der Kategorie ‚*report*‘ zusammengefasst. *Abbildung 9* zeigt den geänderten Konfigurationsteil wobei die neuen Parameter gelb hinterlegt sind.

SS:

- **Key.identifier:** Entspricht dem in der MOA Konfiguration festgelegten KeyIdentifier und steht stellvertretend für den privaten Schlüssel mit dem das Prüfprotokoll unterzeichnet wird.
- **Connection.url:** Kennzeichnet die URL mit der die Serversignierfunktion von MOA genutzt werden kann.

Report:

- **default.language:** ermöglicht dem Betreiber zu definieren in welcher Sprache geantwortet wird, wenn der ‚*VerifyDocumentRequest*' kein ‚*Language*' Element enthält.
- **supported.language:** Ermöglicht es, die unterstützten Sprachen zu definieren bzw. einzuschränken.
- **pdfreport.enabled:** Ermöglicht es dem Betreiber zu definieren, ob die Erstellung eines PDF-Prüfberichtes unterstützt wird.

```
<category name="moa">
  <category name="sp">
    <service.uri>SignatureVerification</service.uri>
    <connection.url>
      http://localhost:8080/moa-spss/services/SignatureVerification
    </connection.url>
    <trustprofile.id>signature-verification-trustprofile-id</trustprofile.id>
  </category>
  <category name="ss">
    <key.idendifier>signature-verification-keygroup-id</key.idendifier>
    <connection.url>
      http://localhost:8080/moa-spss/services/SignatureCreation
    </connection.url>
  </category>
</category>
<category name="report">
        <default.language>de</default.language>
        <supported.language>de,en</supported.language>
        <pdfreport.enabled>true</pdfreport.enabled>
</category>
```

Abbildung 9: Konfiguration Webservice

4 Referenzen

[DOKPR] A. Marsalek, T. Knall: Signaturprüfservice Projektdokumentation, Version 1.8, 19.05.2015.

[MOA] MOA SP-SS Spezifikation, Module für Online Anwendungen – SP und SS; Version 2.0.x; 4.11.2014; https://joinup.ec.europa.eu/site/moa-idspss/moa-spss-2.0.0/doc/handbook/index.html

[OASIS] N. Pope, J. C. Cruellas, S. Drees: Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0. OASIS Standard, April 2007. Abgerufen aus dem World Wide Web am 20. 02. 2012 unter http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf

[RFC 3369] RFC 3369: Cryptographic Message Syntax (CMS), http://www.ietf.org/rfc/rfc3369.txt

[SOAP] Simple Object Access Protocol (SOAP) 1.1; W3C Note 08 May 2000; http://www.w3.org/TR/2000/NOTE-SOAP-20000508

[SOAP12] SOAP Version 1.2 Part 1: Messaging Framework (Second Edition); W3C Recommendation 27 April 2007; http://www.w3.org/TR/2007/REC-soap12-part1-20070427/

[WSDL] Web Services Description Language (WSDL) 1.1; W3C Note 15 March 2001; http://www.w3.org/TR/2001/NOTE-wsdl-20010315

[XMLDSig] XML-Signature Syntax and Processing. W3C Recommendation, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/