A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 1b
The Mall E02
A-1030 Wien

https://www.a-trust.at
E-Mail: office@a-trust.at

Beschreibung

Identitätsschnittstelle und Identitätsrecord

Version: 3.3
Datum: 3. Juli 2019

Inhaltsverzeichnis

History

Datum	Rev	Autor	Änderungen
03.07.2019	3.3	Patrick Hagelkruys	Siegel Schnittstellen, Kapitel 3.1.7, 5
28.11.2017	3.2	Patrick Hagelkruys	textuelle Anpassungen
31.05.2017	3.1	Patrick Hagelkruys Ramin Sabet	Lange Zeile in Kapitel 3 Pseudocode für HashValue Generierung Kapitel 3.1.9 Klarstellung UTF-8 Encoding in Kapitel 3.1.9 Anpassung Regular Expression für CIN in Kapitel 8 IdMethod in Kapitel 3.1.4 Beispiele für XML Aufbau zu den jeweiligen Beschreibungen der XML-Tags Änderung von AcosExtCardNumber auf ExtCardNumber Änderung von ACOS Karte auf A-Trust Karte Beschreibung RegEx Engine in Kapitel 8 Aktualisieren des Literatur-Verzeichnis
29.05.2017	3.0	Patrick Hagelkruys	Anpassung von SHA1 auf SHA256 Anpassung auf RSA-OAEP Verschlüsselung Ausweisarten (IdType) Kapitel 8 - Regex Prüfungen Glossar entfernt
22.04.2016	2.2	Ramin Sabet	Ausweisarten (IdType) ServerToken-Beispiel
04.04.2016	2.1	Patrick Hagelkruys	Klarstellungen zur Verschlüsselung
11.03.2016	2.0	Patrick Hagelkruys	Tippfehler in Kapitel 5
05.02.2016	1.9	Patrick Hagelkruys	Zertifikat für Verschlüsselung
03.02.2016	1.8	Patrick Hagelkruys	Version 2 der Schnittstelle Verschlüsselung
20.10.2015	1.7	Patrick Hagelkruys	Mögliche Werte für ActivationProcess
24.07.2015	1.6	Patrick Hagelkruys	Fehler in XML Darstellung behoben
06.07.2015	1.5	Patrick Hagelkruys	Signaturvertrag entfernen
16.06.2015	1.4	Patrick Hagelkruys	neues A-Trust Design textuelle Erweiterungen und Anpassungen Aktualisierung der XML-Elemente
02.04.2012	1.3	Patrick Hagelkruys	Payment Data
30.03.2012	1.2	Patrick Hagelkruys	Binding AcosExtCardNumber

Fortsetzung auf der nächsten Seite

Datum	Rev	Autor	Änderungen
			Binding Bestellnummer
22.08.2011	1.1	Patrick Hagelkruys	XML Beispiele angepasst
02.08.2011	1.0	Patrick Hagelkruys	XML Beispiel Server Token
11.02.2010	0.1	Patrick Hagelkruys	Erste Version

Tabelle 1: Dokumentenhistorie

1. Übersicht

Die Identitätsschnittstelle ist die Implementierung des Konzeptes „E-Identitätsbestätigung für BK Aktivierung“ vom 29. Oktober 2009 von DI Herbert Leitold, Dr. Reinhard Posch und Dr. Thomas Rössler [HL09].

Auf Basis dieses Konzeptes hat A-Trust ein Web-Service implementiert welches elektronisch signierte und verschlüsselte Identitätsbestätigung (IdentRecords) entgegennimmt, diese prüft und eine Bürgerkarte auf Basis der bestätigten Identität ausstellt. Dieses Dokument beschreibt das Web-Service, das Schema für einen Identitätsrecord und die von A-Trust zur Verfügung gestellten Testumgebung.

2. Ablauf

Die Registrierungsstelle welche die Identität bestätigt muss eine Identitätsbestätigung (Identrecord) erstellen und diese signiert an ein Web-Service der A-Trust senden. Daraus ergibt sich folgender Ablauf:

1. Falls noch nicht vorhanden, abfragen der Handynummer des Kunden
2. Generieren einer Freischalte-PIN
   - Der Freischalte-PIN kann durch den Kunden vergeben werden z. B. als Widerrufspasswort
   - Wird der Freischalte-PIN per Brief an den Kunden versendet, wird empfohlen keine leicht verwechselbaren Ziffern und Buchstaben zu verwenden (z. B.: O=0; I=l)
3. Erstellen einer Identitätsbestätigung wie in Kapitel 3 beschrieben
4. Signatur der Identitätsbestätigung nach dem XMLDsig Standard [W3C08] mit einem RO-Zertifikat (RO=Registration Officer) der Firma A-Trust
5. Verschlüsselung der Identitätsbestätigung wie in Kapitel 4 beschrieben.
6. Übertragung der Identitätsbestätigung und des symmetrischen Schlüssels an das A-Trust Webservice, wie in Kapitel 5 beschrieben.
7. Falls der Freischalte-PIN nicht vom Kunden selbst gewählt wurde, muss dieser dem Kunden mitgeteilt werden (z. B. per Brief zugesandt).

3. Identitätsbestätigung

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
  <pd:CompactPhysicalPerson>
    <pd:CompactName>
      <pd:GivenName>Max Xaver</pd:GivenName>
      <pd:FamilyName>Mustermann</pd:FamilyName>
    </pd:CompactName>
    <pd:Sex>male</pd:Sex>
    <pd:DateOfBirth>1976-11-11</pd:DateOfBirth>
    <pd:PlaceOfBirth>Wien</pd:PlaceOfBirth>
  </pd:CompactPhysicalPerson>
  <idr:SignatoryData>
    <idr:HomeZIP>8042</idr:HomeZIP>
    <idr:PhoneNumber>+436505555555</idr:PhoneNumber>
    <idr:EMailAddress>test@test.com</idr:EMailAddress>
  </idr:SignatoryData>
  <idr:Identification>
    <idr:IdMethod>VideoId</idr:IdMethod>
    <idr:IdType>PERS</idr:IdType>
    <idr:IdNumber>12345678</idr:IdNumber>
    <idr:IdIssueDate>2011-08-01</idr:IdIssueDate>
    <idr:IdAuthority>Mag. Wien</idr:IdAuthority>
    <idr:IdNation>AT</idr:IdNation>
  </idr:Identification>
  <idr:Binding>
    <pd:Mobile>
      <pd:FormattedNumber>+436505555555</pd:FormattedNumber>
    </pd:Mobile>
  </idr:Binding>
  <idr:Hash>
    <idr:HashValue>8jew91qk...1982qw=</idr:HashValue>
  </idr:Hash>
  <dsig:Signature>...</dsig:Signature>
</idr:Confirmation>
```

3.1. Aufbau der Identitätsbestätigung

Der Identitätsrecord ist ein XML mit dem Wurzelelement Confirmation. Darunter können folgende Elemente definiert werden:

- CompactPhysicalPerson
- CompactPostalAddress
- SignatoryData
- Identification
- PaymentData
- ServerToken
- Custom
- Binding
- Hash
- IdentityLinkSaml
- ValidTo
- Signature

Zumindest die Elemente `CompactPhysicalPerson`, `Identification`, `Hash` und `Signature` müssen angegeben werden. Ebenso ist das Attribut `Version` mit dem Wert `3` anzugeben.

3.1.1. CompactPhysicalPerson

Das Element `CompactPhysicalPerson` beinhaltet die Personendaten.

- CompactName
- Sex (female, male)
- DateOfBirth (Format: YYYY-MM-DD)
- PlaceOfBirth

Der Name wird im Element `CompactName` zusammengefasst, eine genauere Beschreibung findet man im Kapitel 3.1.1.1.

Das Feld `Sex` kann die Werte `male` oder `female` beinhalten.

Das Feld `PlaceOfBirth` wird im Falle einer Aktivierung einer ACOS Karte als zusätzlicher Parameter bei der ZMR Abfrage verwendet.

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
  <pd:CompactPhysicalPerson>
    <pd:CompactName>
      <pd:GivenName>Max Xaver</pd:GivenName>
      <pd:FamilyName>Mustermann</pd:FamilyName>
    </pd:CompactName>
    <pd:Sex>male</pd:Sex>
    <pd:DateOfBirth>1976-11-11</pd:DateOfBirth>
    <pd:PlaceOfBirth>Wien</pd:PlaceOfBirth>
  </pd:CompactPhysicalPerson>
...
</idr:Confirmation>
```

Listing 1: Beispiel CompactPhysicalPerson

3.1.1.1. CompactName

- GivenName
- FamilyName
- Affix

Die Angabe von `GivenName` und `FamilyName` ist verpflichtend.

Das Feld `Affix` wird nur berücksichtigt, wenn das Attribut `position` den Wert `prefix` hat und das Attribut `type` entweder `academicGrade`, `aristocraticTitle` oder `qualification` ist.

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
  <pd:CompactPhysicalPerson>
    <pd:CompactName>
      <pd:GivenName>Max Xaver</pd:GivenName>
      <pd:FamilyName>Mustermann</pd:FamilyName>
    </pd:CompactName>
    <pd:Sex>male</pd:Sex>
    <pd:DateOfBirth>1976-11-11</pd:DateOfBirth>
    <pd:PlaceOfBirth>Wien</pd:PlaceOfBirth>
  </pd:CompactPhysicalPerson>
...
</idr:Confirmation>
```

Listing 2: Beispiel CompactPhysicalPerson

3.1.2. CompactPostalAddress

Dieses Element kann folgende Daten enthalten, welche auch weiterverarbeitet werden:

- CountryCode
- CountryName
- PostalCode
- Municipality
- DeliveryAddress/StreetName
- DeliveryAddress/BuildingNumber
- DeliveryAddress/Unit
- DeliveryAddress/DoorNumber

Umwandlung der PostalAddress in die für A-Trust benötigten Adresszeilen
Aus dem Wert „CompactPhysicalPerson/CompactName/GivenName“ wird die Adresszeile 1, aus dem Wert „CompactPhysicalPerson/CompactName/FamilyName“ wird die Adresszeile 2 befüllt.
Die Adresszeile 3 wird aus den Werten „DeliveryAddress/StreetName“ „DeliveryAddress/BuildingNumber“ „DeliveryAddress/Unit“ „DeliveryAddress/DoorNumber“ erstellt, jeweils mit einem Leerzeichen getrennt.
Der Wert „Municipality“ wird der Adresszeile 4 zugeordnet.
Der Wert „PostalCode“ wird als Postleitzahl verwendet, der Wert „CountryCode“ als

Länderkennzeichen (2-stellig) für das Land.
Für die Adresszeilen gelten folgende Längenbeschränkungen:

- Adresszeile 1 max. 32 Zeichen
- Adresszeile 2 max. 32 Zeichen
- Adresszeile 3 max. 32 Zeichen
- Adresszeile 4 max. 24 Zeichen
- Postleitzahl max. 6 Zeichen
- Länderkennzeichen max. 2 Zeichen

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
...
  <pd:CompactPostalAddress>
    <pd:CountryCode>AT</pd:CountryCode>
    <pd:PostalCode>1000</pd:PostalCode>
    <pd:Municipality>Wien</pd:Municipality>
    <pd:DeliveryAddress>
      <pd:StreetName>StreetName</pd:StreetName>
      <pd:BuildingNumber>32</pd:BuildingNumber>
      <pd:Unit>5256</pd:Unit>
    </pd:DeliveryAddress>
  </pd:CompactPostalAddress>
...
</idr:Confirmation>
```

Listing 3: Beispiel CompactPostalAddress

3.1.3. SignatoryData

Das Element `SignatoryData` ist ein optionales Feld und enthält zusätzliche Informationen zum Signator.

- PhoneNumber
- EMailAddress
- HomeZIP

Das Element `HomeZIP` wird als zusätzlicher optionaler Parameter bei der ZMR Abfrage während der Aktivierung einer e-card oder Handy-Signatur verwendet.

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
...
  <idr:SignatoryData>
    <idr:HomeZIP>8042</idr:HomeZIP>
    <idr:PhoneNumber>+436505555555</idr:PhoneNumber>
    <idr:EMailAddress>test@test.com</idr:EMailAddress>
  </idr:SignatoryData>
...
</idr:Confirmation>
```

Listing 4: Beispiel SignatoryData

3.1.4. Identification

In diesem Feld werden Identifikationsmerkmale angegeben, wenn ein Ausweis herangezogen wurde, sind die Ausweisdaten anzugeben.

Wenn die Identifizierung der Person auf eine Videoidentifizierung zurückzuführen ist, dann muss diese zwingend im Feld `IdMethod` angegeben werden.

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
...
  <idr:Identification>
    <idr:IdMethod>VideoId</idr:IdMethod>
  </idr:Identification>
...
</idr:Confirmation>
```

Listing 5: Beispiel IdMethod für Videoidentifizierung

Im Falle einer Identifikation des Signators mittels Ausweis (z. B. durch einen Registration Officer) müssen auch die weiteren Ausweisdaten angegeben werden.

- IdNation
- IdAuthority
- IdIssueDate

- IdNumber
- IdType

Folgend die häufigst genutzten Werte für den Typ des Ausweisdokumentes (*IdType*). Eine vollständige Liste ist dem XML-Schema der Schnittstelle zu entnehmen.

REIS Internationaler Reisepass

FUEH Österreichischer Führerschein

IDKA Österreichische Identitätskarte

PERD Deutscher Personalausweis

RA Rechtsanwaltsausweis

eDA eDA Dienstausweis Republik Österreich

eDAO eDA Land Oberösterreich

EDU EDU-Card

GEME Gemeindeausweis

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
...
  <idr:Identification>
    <idr:IdType>PERS</idr:IdType>
    <idr:IdNumber>12345678</idr:IdNumber>
    <idr:IdIssueDate>2011-08-01</idr:IdIssueDate>
    <idr:IdAuthority>Mag. Wien</idr:IdAuthority>
    <idr:IdNation>AT</idr:IdNation>
  </idr:Identification>
...
</idr:Confirmation>
```

Listing 6: Beispiel Ausweisdaten

3.1.5. PaymentData

Das Element `PaymentData` wird bei Bezahlprodukten (z.B.: ACOS-Karte) verwendet und beinhaltet die Kontodaten des Kunden.

- IBAN
- BIC

- AccountInformation

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
...
  <idr:PaymentData>
    <idr:IBAN>AT151420000124356789</idr:IBAN>
    <idr:BIC>EASYATW1</idr:BIC>
    <idr:AccountInformation>Max Mustermann
        Test</idr:AccountInformation>
  </idr:PaymentData>
...
</idr:Confirmation>
```

Listing 7: Beispiel CompactPostalAddress

3.1.6. ServerToken

Das Element `ServerToken` lässt eine Bindung und Rückmeldung an die, den Identitätsrecord einbringende, Applikation zu. Sowie eine Verknüpfung mit dem e-Tresor. Es können die folgende Elemente angegeben werden:

- Token
- ServerIdentification
- ResponseUrl

Das Element `Token` ist eine der einbringenden Applikation bekannter Wert, um den Benutzer nach der Aktivierung zu erkennen (z. B.: Vertragsnummer, Datenbank-ID,...). Ist das Element `ServerIdentification` angegeben, wird zu diesem Benutzer im Handy-Signatur Konto (früher e-Tresor) eine Verbindung zu der in `ServerIdentification` angegeben Applikation angelegt. Als Kopplung zwischen Handy-Signatur Konto und einbringender Applikation wird der in `Token` angegeben Wert verwendet. Ist das Element `ResponseUrl` angegeben, wird nach erfolgreicher Aktivierung eine Rückmeldung an diese URL gegeben, Parameter und Aufruf werden je nach URL und Applikation getrennt vereinbart.

Mögliche Parameter:

- Zertifikatsseriennummer
- Ausstellungsdatum des Zertifikates
- Ablaufdatum des Zertifikates

- Token

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Version='3'>
  ...
  <idr:ServerToken>
    <idr:Token>MIACAQMw...gDC==</idr:Token>
    <idr:ServerIdentification>
      testapp
    </idr:ServerIdentification>
    <idr:ResponseUrl>
      https://www.testapp.at/mobsig/response.aspx
    </idr:ResponseUrl>
  </idr:ServerToken>
  <idr:Binding>...</idr:Binding>
  <idr:Hash>...</idr:Hash>
  <dsig:Signature>...</dsig:Signature>
</idr:Confirmation>
```

3.1.7. Custom

Das Element `Custom` enthält nicht näher definierte Zusatzfelder. Derzeit sind folgende Werte für Custom Felder vergeben:

- tag
- ActivationProcess
  Mögliche Werte:
  - TestCa
  - WEBID
  - EuIdentity
  - Seal
- Customer
  - <Name des Kunden>

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
```

```
5  Version='3'>
6    ...
7    <idr:Custom>
8      <idr:Value Name='tag'>...</idr:Value>
9      <idr:Value Name='ActivationProcess'>...</idr:Value>
10   </idr:Custom>
11   <idr:Binding>...</idr:Binding>
12   <idr:Hash>...</idr:Hash>
13   <dsig:Signature>...</dsig:Signature>
14 </idr:Confirmation>
```

3.1.8. Binding

Das Element `Binding` lässt eine frühzeitige Bindung an einen Aktivierungsprozess zu. Es können folgende Elemente angegeben werden, es darf jeweils immer nur ein Element angegeben werden.

- Mobile
- CIN
- SVNR
- CINCSN
- ExtCardNumber
- Bestellnummer

Das Element `Mobile` erzwingt die Ausstellung einer Handy-Signatur, wobei in einem untergeordneten Element `FormattedNumber` die Mobiltelefonnummer der auszustellenden Handy-Signatur angegeben wird. Hierbei ist zu beachten, dass die Mobiltelefonnummer im Format Ländercode (+43) + Provider (664) + Telefonnummer ohne Leerzeichen angegeben wird. z. B.: `+436641234563`
Dies ist wichtig, da der Benutzer auf der Aktivierungsseite darauf hingewiesen wird, die Mobiltelefonnummer in diesem Format anzugeben.

Die Elemente `CIN` und `SVNR` erzwingen die Ausstellung einer eCard, wobei in `SVNR` die Sozialversicherungsnummer der auszustellenden eCard angegeben wird oder im Element `CIN` die Kennnummer der Karte der auszustellenden eCard.

Das Element `CINCSN` erzwingt die Ausstellung einer A-Trust Karte, wobei als Wert die Kartennummer und Kartenfolgenummer (16-stellig) angegeben wird.

Das Element `ExtCardNumber` erzwingt die Ausstellung einer A-Trust Karte, wobei als Wert die Chipseriennummer des Chips verwendet wird. z. B.:0101606100000 7f0

Sollte keiner der Karten/Geräte spezifischen Werte vorhanden sein kann das Element `Bestellnummer` verwendet werden. Eine Bindung an einen Aktivierungsprozess ist durch

das erste Zeichen der Bestellnummer gegeben.

'A' oder 'a' ACOS/CardOS Aktivierung

'E' oder 'e' e-card Aktivierung

'M' oder 'm' Handy-Signatur Aktivierung

Die Übergebenen Werte werden mittels Regular-Expresions überprüft, die entsprechenden Prüfungen finden Sie im Kapitel 8.

3.1.9. Hash

Das Element `Hash` enthält ein untergeordnetes Element `HashValue` welches den Base64 encodierten SHA256 Hashwert aus AktivierungsCode und FreischaltePIN enthält (diese werden aneinandergehängt).

$Hash = Base64(SHA256(UTF8\_Bytes(AktivierungsCode + FreischaltePIN)))$

Die Werte AktivierungsCode und FreischaltePIN müssen hierbei UTF-8 kodiert werden. Eine Implementierung in Psudocode ist in Listing 8 gezeigt.

```
var identifier = AktivierungsCode+FreischaltePIN;
var utf8bytes = UTF8.GetBytes(identifier);
var hash = SHA256(utf8bytes);
var HashValue = Base64.Encode(hash);
```

Listing 8: Pseudocode der HashValue Generierung

Der AktivierungsCode ist der Inhalt des Binding Elements. Im Fall Handy-Signatur die Mobiltelefonnumer, im Fall eCard die SVNR oder die CIN, im Fall ACOS die Kartennummer und Kartenfolgenummer (CINCSN).

Der FreischaltePIN ist:

- Ein vom identifizierenden System generierter Code, welcher nur der zu identifizierenden Person bekannt sein darf (z. B.: Aktivierungscode, welcher per RSa Brief zugesandt wird)
- Ein von der zu identifizierenden Person gewähltes und nur Ihr bekanntes Geheimnis (z. B.: Widerrufspasswort)

3.1.10. IdentityLinkSaml

Dieses Element enthält die Personenbindung des Registration Officers für eine verbesserte Zuordnung der RO-Rechte

3.1.11. ValidTo

Dieses Element einhält eine optionale Einschränkung der Gültigkeit des Identitätsrecords.

```
<idr:Confirmation
xmlns:idr="http://ref...nt.gv.at/namespace/idconfirmation#"
xmlns:pd="http://ref...nt.gv.at/namespace/persondata/20020228#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
   ...
  <idr:Binding>...</idr:Binding>
  <idr:Hash>...</idr:Hash>
  <idr:ValidTo>2015-06-16T13:43:20</idr:ValidTo>
  <dsig:Signature>...</dsig:Signature>
</idr:Confirmation>
```

3.1.12. Signature

Dieses Element enthält eine XMLDSIG Signatur über die identifizierten Daten.

3.2. Erforderliche und empfohlene Elemente

Die folgenden Elemente müssen zumindest angegeben werden:

- CompactPhysicalPerson/CompactName/GivenName
- CompactPhysicalPerson/CompactName/FamilyName
- CompactPhysicalPerson/DateOfBirth
- Binding
- Hash/HashValue
- Signature

Weiters wird zumindest empfohlen die folgenden Elemente anzugeben:

- CompactPhysicalPerson/Sex
- SignatoryData/HomeZIP

4. Verschlüsselung der Identitätsbestätigung

Die signierte Identitätsbestätigung muss vor dem Senden an das A-Trust Webservice verschlüsselt werden. Dazu wird die Identitätsbestätigung mit einem AES 256 Schlüssel (Algorithmus: Galois/Counter Mode (GCM) [Wik16a]) verschlüsselt und dieser AES Schlüssel weiter mit dem öffentlichen RSA-Schlüssel des A-Trust Service (siehe dazu [Wik16b]). Das Ergebnis der Verschlüsselung sind 2 Binärblöcke, die verschlüsselte Identitätsbestätigung und der verschlüsselte AES256 Schlüssel. Diese Daten werden durch aneinanderreihen verkettet, zuerst die verschlüsselter Identitätsbestätigung und anschließend der verschlüsseltem AES Schlüssel.

Ablauf:

1. Generieren eines neuen zufälligen AES256 Schlüssel. Für jeden Identrecord ist ein eigener Schlüssel zu verwenden.
2. Verschlüsseln der signierte Identitätsbestätigung mit AES256/GCM. (UTF-8 Repräsentation der Identitätsbestätigung)
   - Algorithmus: AES256/GCM
   - IV: Byte Array mit Länge 16 gefüllt mit 0x00
   - Der beim GCM Algorithmus entstandene MAC wird dem verschlüsselten Block angehängt (Standard verhalten)
3. Verschlüsseln des AES256 Schlüssel mit dem öffentlichen RSA Schlüssel (RSA-OAEP) der A-Trust
4. Aneinanderreihen von verschlüsselter Identitätsbestätigung und verschlüsseltem AES. Aufgrund der Schlüssellänge des RSA-Schlüssels können die Daten getrennt werden.

5. Web-Service für Identitätsrecords

5.1. Signaturprodukte

Zum Einbringen des verschlüsselten Identitätsbestätigung werden folgende Methoden zur Verfügung gestellt:

POST /v3/Identification: Als POST Inhalt werden die Binärdaten der verschlüsselten Identitätsbestätigung übergeben. Dieses Dokument wird entschlüsselt und gegen das IdConfirmation Schema geprüft. Anschließend wird die Signatur, der Signaturzeitpunkt und das Signaturzertifikat geprüft. Zum Abschluss wird der Hashwert extrahiert und der Record mit diesem Hashwert als Index in der Datenbank abgespeichert. Sollte bereits ein Eintrag mit diesem Hashwert vorhanden sein wird der bestehenden Eintrag überschrieben.

POST /v3/Identification/Base64: Bei dieser Funktion wird der Inhalt Base64 kodiert übergeben.

GET /v3/Certificate: Liefert das Zertifikat zum Verschlüsseln zurück. (Format: Binary)

GET /v3/Certificate/PEM: Liefert das Zertifikat zum Verschlüsseln im PEM Format zurück.

5.2. Siegelprodukte

Zum Einbringen des verschlüsselten Identitätsbestätigung werden folgende Methoden zur Verfügung gestellt. Die Beschreibung der Methoden ist äquivalent zum Kapitel 5.1

POST /v3/Seal/Identification

POST /v3/Seal/Identification/Base64

GET /v3/Seal/Certificate

GET /v3/Seal/Certificate/PEM

6. Parameter für die Aktivierungsseite

Die Aktivierungsseite kann durch GET Parameter vor ausgefüllt und angepasst werden. Die folgenden Parameter sind möglich:

aktivierungscode	Mit diesem Parameter wird das Feld `Aktivierungscode` auf der Webseite vor ausgefüllt
binding	siehe aktivierungscode
freischaltepin	Mit diesem Parameter wird das Feld `Freischalte-PIN` auf der Webseite vor ausgefüllt und das Formular abgesendet. Dadurch ergibt sich für den Kunden keine Interaktion auf dieser Seite, sondern er wird sofort zum Aktivierungsprozess weitergeleitet.
widerrufspasswort	siehe freischaltepin

Beispiel: `Aktivierung.aspx?aktivierungscode=123456789`

7. Testumgebung

Das von A-Trust zur Verfügung gestellt Testsystem kann unter https://hs-abnahme.a-trust.at/Aktivierung/v3/Identification getestet werden. Zu beachten ist, dass es sich hierbei um ein Testsystem handelt. Dieses kann zeitweise nicht verfügbar sein bzw. werden Neuentwicklungen und Änderungen zuerst hier installiert und getestet.

Die Identifikationsseite für den Registration Officer Prozess kann über https://hs-abnahme.a-trust.at/Aktivierung/RO aufgerufen werden.

Die Seite für das Abfragen der Identitätsbestätigung kann über https://hs-abnahme.a-trust.at/Aktivierung/ aufgerufen werden.

Für Testzwecke wurde derzeit auch ein Upload einer Identitätsbestätigung eingebaut https://hs-abnahme.a-trust.at/Aktivierung/Upload/. **Diese Webseite dient derzeit nur zu Testzwecken!**

8. Überprüfung der Eingabewerte

Die in Kapitel 3.1.8 übergebenen Werte für das XML Tag `Binding` werden mittels der nachfolgend Regular Expression überprüft.

Die verwendete Regular Expression Engine entspricht einer Nondeterministic Finite Automaton (NFA) Engine wie diese in Perl, Python, Emacs, und Tcl eingesetzt wird. (siehe auch [Mic17])

8.1. Mobiltelefonnummer für Handy-Signatur (Mobile)

```
^\+[1-9]{1}[0-9]{1,14}$
```

Listing 9: Regular Expression für Mobiltelefonnummer

8.2. CIN

```
^800400[0-9]{14}$
```

Listing 10: Regular Expression für CIN

8.3. SVNR

```
^[0-9]{10}$
```

Listing 11: Regular Expression für SVNR

8.4. CINCSN

```
^[0-9]{16}$
```

Listing 12: Regular Expression für CINCSN

8.5. ExtCardNumber

```
^[0-9A-Fa-f]{16,24}$
```

Listing 13: Regular Expression für ExtCardNumber

8.6. Bestellnummer

```
^[aAmMeE]{1}[0-9a-zA-Z]{3,25}$
```

Listing 14: Regular Expression für Bestellnummer

A. Schnittstelle V2

Im Unterschied zur Version 3 der Schnittstelle waren in der Version 2 folgende Änderungen:

- Im Kapitel 3 und den nachfolgenden Beispielen wurde in Version 3 im XML Tag `Confirmation` das Attribute `Version` hinzugefügt.
- Im Kapitel 3.1.9 wurde in Version 2 SHA1 als Hashalgorithmus eingesetzt.
- Im Kapitel 5 wurde in Version 2 der Schnittstelle `v2` in der URL verwendet
- Im Kapitel 7 wurde in Version 2 der Schnittstelle `v2` in der URL verwendet
- Im Kapitel 4 wurde in Version 2 noch RSA Verschlüsselung
- Die Regular-Expression Überprüfungen in Kapitel 8 wurden in Version 3 hinzugefügt.

B. Schnittstelle V1 - SOAP Service

Das SOAP Service ist dem im Konzept beschriebenen IDA-Service [HL09] gleichzusetzen. Als externe Schnittstelle wird nur das Einbringen des Identitätsrecords angeboten, dazu werden die folgenden 2 Methoden zur Verfügung gestellt:

AddIdentification(XmlRecord): Als einziger Parameter wird das signierte XML-Dokument übergeben. Dieses Dokument wird gegen das IdConfirmation Schema geprüft. Anschließend wird die Signatur, der Signaturzeitpunkt und das Signaturzertifikat geprüft. Zum Abschluss wird der Hashwert extrahiert und der Record mit diesem Hashwert als Index in der Datenbank abgespeichert. Sollte bereits ein Eintrag mit diesem Hashwert vorhanden sein wird der bestehenden Eintrag überschrieben.

AddIdentificationB64(B64Record): Bei dieser Funktion wird anstelle des XML Dokuments, das Dokument Base64 kodiert übergeben. Nach dem Base64 decodieren werden die gleiche Schritte wie bei der Funktion `AddIdentification` durchgeführt.

B.1. Testumgebung

Das von A-Trust zur Verfügung gestellt Testsystem kann unter https://hs-abnahme.a-trust.at/Aktivierung/IdentService.asmx getestet werden. Zu beachten ist, dass es sich hierbei um ein Testsystem handelt. Dieses kann zeitweise nicht verfügbar sein bzw. werden Neuentwicklungen und Änderungen zuerst hier installiert und getestet.

Die Identifikationsseite für den Registration Officer Prozess kann über https://hs-abnahme.a-trust.at/Aktivierung/RO aufgerufen werden.

Die Seite für das Abfragen der Identitätsbestätigung kann über https://hs-abnahme.a-trust.at/Aktivierung/ aufgerufen werden.

Für Testzwecke wurde derzeit auch ein Upload einer Identitätsbestätigung eingebaut https://hs-abnahme.a-trust.at/Aktivierung/Upload/. **Diese Webseite dient derzeit nur zu Testzwecken!**

Literatur

[HL09] Herbert Leitold, Reinhard Posch, Thomas Rössler: *E-Identitätsbestätigung für BK Aktivierung - Konzept*. EGIZ E-Government Innovationszentrum, Oktober 2009.

[Mic17] Microsoft: *Details of Regular Expression Behavior*, 2017. https://msdn.microsoft.com/en-us/library/e347654k(v=vs.110).aspx, besucht: 2017-05-31.

[W3C08] W3C: *XML Signature Syntax and Processing (Second Edition)*, 2008. https://www.w3.org/TR/xmldsig-core/, besucht: 2017-05-31.

[Wik16a] Wikipedia: *Galois/Counter Mode — Wikipedia, The Free Encyclopedia*, 2016. https://de.wikipedia.org/wiki/Galois/Counter_Mode, besucht: 2017-05-31.

[Wik16b] Wikipedia: *Hybride Verschlüsselung — Wikipedia, The Free Encyclopedia*, 2016. https://de.wikipedia.org/wiki/Hybride_Verschl%C3%BCsselung, besucht: 2017-05-31.