

e-Identity Pflichtenheft

Version: 2.1.0



Datum: 24.02.2020

Autoren:

Mag. Alexander Schilling

Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH

Mag. Joachim Geisler

Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH

Markus Brejla, MSc.

ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H.

Thomas Pircher

ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H.

Matthias Kautz

ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H.

INHALTSVERZEICHNIS

E-IDENTITY PFLICHTENHEFT	1
INHALTSVERZEICHNIS	2
1. DOKUMENTATIONSHISTORIE	8
2. VORWORT	9
3. EINLEITUNG	10
3.1. AUFBAU UND INHALT DES DOKUMENTS	10
3.2. E-IDENTITY SERVICE	10
3.3. BEGRIFFE	11
3.4. REFERENZEN IM DOKUMENT	11
3.5. REFERENZEN AUF WEITERE DOKUMENTE	11
4. LOGO E-IDENTITY SERVICE.....	12
5. ORGANISATORISCHE VORAUSSETZUNGEN	13
5.1. E-SERVICE SCHEME OPERATOR	13
5.2. E-SERVICE HÄNDLERVEREINBARUNG.....	13
5.3. TEILNAHMEVORAUSSETZUNGEN.....	13
6. IDENTITÄTSDATEN	14
7. ABLAUF DES E-IDENTITY SERVICES	15
7.1. ABLAUFBESCHREIBUNG – ÜBERSICHT	15
7.2. ABLAUFBESCHREIBUNG IM DETAIL	16
7.3. DIE EINZELNEN SCHRITTE.....	17
7.3.1. <i>Schritt 1: Entscheidung zur Nutzung des e-Identity Service</i>	17
7.3.2. <i>Schritt 2: Übermittlung e-Identity Service Initiierung</i>	17
7.3.3. <i>Schritt 3: Rückmeldung auf e-Identity Service Initiierung</i>	17
7.3.3.1. a) ohne Fehler	17
7.3.3.2. b) bei Auftreten eines Fehlers.....	17
7.3.4. <i>Schritt 4: Redirect des Kunden auf die Bankenauswahl</i>	18
7.3.5. <i>Schritt 5: Redirect des Kunden auf das Online-Banking</i>	18
7.3.6. <i>Schritt 6: e-Identity Service Confirmation</i>	18
7.3.7. <i>Schritt 7: Rückmeldung zur e-Identity Service Confirmation</i>	19
7.3.8. <i>Schritt 8: Redirect des Kunden zum Händler</i>	19
7.3.9. <i>Schritt 9: Fortsetzung Workflow beim Händler</i>	19
7.3.10. <i>Schritt 10: e-Identity Service Statusabfrage (optional)</i>	19
7.3.11. <i>Schritt 11: Rückmeldung zur e-Identity Service Statusabfrage</i>	20
7.3.12. <i>Schritt 12: e-Identity Tokenabfrage</i>	20
8. EID4MOBILE	21
8.1. TECHNISCHE ANFORDERUNGEN QR-CODE.....	21
ABBILDUNG 5: BEISPIEL QR-CODE	22
8.2. EID4MOBILE BROWSER2APP VIA QR-CODE.....	22
ABBILDUNG 6: ABLAUFBESCHREIBUNG BROWSER2APP	22
8.3. EID4MOBILE POS2APP VIA QR-CODE	24

ABBILDUNG 7: ABLAUFBESCHREIBUNG POS2APP	24
8.4. EID4MOBILE APP2APP	25
ABBILDUNG 8: ABLAUFBESCHREIBUNG APP2APP	25
9. EID TOKEN	27
10. TECHNISCHE ANFORDERUNGEN	28
10.1. XML SPEZIFIKATION	28
10.2. E-IDENTITY SERVICE XML DEFINITIONEN	28
10.3. ZEICHENSATZ E-IDENTITY SERVICE XML SCHEMA.....	28
10.3.1. eingeschränkter Zeichensatz	28
10.3.2. erweiterter Zeichensatz	28
10.4. PROTOKOLL NACHRICHTENAUSTAUSCH.....	28
10.5. TIME OUT	29
10.6. ZEITSYNCHRONITÄT	29
10.7. URL ANGABEN	29
10.7.1. URL/XML Encoding	29
10.7.1.1. Beispiel.....	29
10.8. SICHERHEIT	29
10.9. PFLICHTFELDER.....	29
10.10. WINDOW-MANAGEMENT.....	29
20. EINLEITUNG – BANKENSEITE	31
20.1. AUFBAU DES DOKUMENTS.....	31
21. ABLAUF DES E-IDENTITY SERVICES AUF BANKENSEITE	32
21.1. ABLAUFBESCHREIBUNG - ÜBERSICHT.....	32
21.2. ABLAUFBESCHREIBUNG IM DETAIL	33
21.3. DIE EINZELNEN SCHRITTE.....	34
21.3.1. Schritt 4: Bankenauswahl	34
21.3.2. Schritt A: e-Identity Service Initiierung.....	34
21.3.3. Schritt B: Rückmeldung auf e-Identity Service Initiierung	34
21.3.4. Schritt 5: Redirect des Kunden auf das Online-Banking.....	34
21.3.5. Anzeige Identitätsdaten	34
21.3.6. Autorisierung durch Kunden	34
21.3.7. Schritt C: e-Identity Service Confirmation	35
21.3.8. Schritt D: Rückmeldung zur e-Identity Service Confirmation.....	35
21.3.9. Schritt 8: Redirect des Kunden zum Händler.....	35
21.4. ABFRAGE DETAILDATEN FÜR EID4MOBILE	35
21.4.1. IdentityDetailsRequest.....	35
21.4.2. IdentityDetailsResponse.....	35
A. ANHANG – XML-NACHRICHTEN	36
A.1. ALLGEMEIN	36
A.1.1. Schema-Aufbau	36
A.1.2. eIdentity:MsgHeader.....	36
A.1.2.1. eIdentity:MsgId.....	36
A.1.2.2. eIdentity:CreDtTime	36

A.2. DIE NACHRICHTEN IM EINZELNEN.....	37
A.2.1. <i>eIdentity:IdentityServiceInitiationRequest</i>	37
A.2.1.1. eIdentity:CustomerBIC.....	37
A.2.1.2. eIdentity:MerchantData.....	37
A.2.1.2.1. eIdentity:ReturnUrl	37
A.2.1.2.2. eIdentity:ConfirmationUrl.....	37
A.2.1.2.3. eIdentity:MerchantName	38
A.2.1.3. eIdentity:IdentityRequest	38
A.2.1.3.1. eIdentity:IdentityDataRequest.....	38
A.2.1.3.2. eIdentity:Query.....	38
A.2.1.3.3. eIdentity:Data	39
A.2.1.4. eIdentity:TransactionId	39
A.2.1.5. eIdentity:QRCodeUrl	39
A.2.1.6. eIdentity:AuthenticationDetails	39
A.2.1.6.1. eIdentity:UserId.....	39
A.2.1.6.2. eIdentity:SHA256Fingerprint.....	40
A.2.1.6.2.1. Beispiel	40
A.2.1.6.3. dsig:Signature	40
A.2.2. <i>eIdentity:IdentityServiceInitiationResponse</i>	41
A.2.2.1. eIdentity:StatusReference	41
A.2.2.2. eIdentity:BankData.....	41
A.2.2.2.1. eIdentity:RedirectUrl.....	41
A.2.2.3. eIdentity:TransactionId	42
A.2.2.4. eIdentity:QRCodeUrl	42
A.2.2.5. eIdentity:ResponseStatus	42
A.2.2.5.1. eIdentity:ResponseStatus@from	42
A.2.2.5.2. eIdentity:ResponseCode.....	42
A.2.2.5.3. eIdentity:ResponseMessage	42
A.2.3. <i>eIdentity:IdentityServiceConfirmation</i>	43
A.2.3.1. eIdentity:IdentityResponse	43
A.2.3.1.1. eIdentity:IdToken	43
A.2.3.1.2. eIdentity:IdentityDataResult.....	43
A.2.3.2. eIdentity:ResponseStatus	44
A.2.3.2.1. eIdentity:ResponseStatus@from	44
A.2.3.2.2. eIdentity:ResponseCode.....	44
A.2.3.2.3. eIdentity:ResponseMessage	44
A.2.3.3. eIdentity:BankId	44
A.2.3.4. dsig:Signature.....	44
A.2.4. <i>eIdentity:IdentityServiceConfirmationResponse</i>	44
A.2.4.1. eIdentity:ResponseStatus	44

A.2.4.1.1. eIdentity:ResponseStatus@from	44
A.2.4.1.2. eIdentity:ResponseCode	45
A.2.4.1.3. eIdentity:ResponseMessage	45
A.2.5. <i>eIdentity:IdentityStatusRequest</i>	45
A.2.5.1. eIdentity:StatusReference	45
A.2.5.2. eIdentity:AuthenticationDetails	45
A.2.5.2.1. eIdentity:UserId.....	45
A.2.5.2.2. eIdentity:SHA256Fingerprint.....	45
A.2.5.2.3. dsig:Signature	46
A.2.6. <i>eIdentity:IdentityStatusResponse</i>	46
A.2.6.1. eIdentity:IdentityResponse	46
A.2.6.2. eIdentity:ResponseStatus	46
A.2.6.2.1. eIdentity:ResponseStatus@from	46
A.2.6.2.2. eIdentity:ResponseCode.....	46
A.2.6.2.3. eIdentity:ResponseMessage	46
A.2.6.3. dsig:Signature.....	46
A.2.7. <i>eIdentity:IdentityDataTokenRequest</i>	47
A.2.7.1. eIdentity:IdToken	47
A.2.7.2. eIdentity:AuthenticationDetails	47
A.2.7.2.1. eIdentity:UserId.....	47
A.2.7.2.2. eIdentity:SHA256Fingerprint.....	47
A.2.8. <i>eIdentity:IdentityDataTokenResponse</i>	48
A.2.8.1. eIdentity:IdentityResponse	48
A.2.8.2. eIdentity:ResponseStatus	48
A.2.8.2.1. eIdentity:ResponseStatus@from	48
A.2.8.2.2. eIdentity:ResponseCode.....	48
A.2.8.2.3. eIdentity:ResponseMessage	48
A.2.8.3. dsig:Signature.....	48
B. ANHANG – RESPONSECODES	49
B.1. 000 – KEIN FEHLER	49
B.2. 001 – XML UNGÜLTIG.....	49
B.3. 002 – FEHLER BEI FELDPRÜFUNG	49
B.4. 004 – AUTORISIERUNG FEHLERHAFT	49
B.5. 008 – UNSPEZIFISCHER FEHLER.....	49
B.6. 009 – INTERNER FEHLER	49
B.7. 014 – CONNECTION TIMEOUT.....	49
B.8. 016 – DUPLICATE CONFIRMATION.....	49
B.9. 030 – ABBRUCH DURCH KUNDEN	49
B.10. 100 – ERFOLGREICHE IDENTIFIKATION	49
B.11. 105 – UNVOLLSTÄNDIGE IDENTIFIKATION	49

B.12. 110 – FEHLGESCHLAGENE IDENTIFIKATION	50
B.13. 120 – UNGÜLTIGE STATUSREFERENZ	50
B.14. 121 – TRANSAKTION NICHT ABGESCHLOSSEN	50
B.15. 122 – UNGÜLTIGER TOKEN	50
B.16. 123 – TOKEN ABGELAUFEN	50
L. ANHANG – XML-NACHRICHTEN ZWISCHEN BANK UND E-SERVICE SCHEME OPERATOR.....	51
L.1. DIE NACHRICHTEN IM EINZELNEN	51
L.1.1. <i>eIdentity:IdentityServiceInitiationRequest</i>	51
L.1.2. <i>eIdentity:IdentityServiceInitiationResponse</i>	51
L.1.2.1. <i>eIdentity:StatusReference</i>	51
L.1.2.2. <i>eIdentity\RedirectUrl</i>	51
L.1.3. <i>eIdentity:IdentityServiceConfirmation</i>	51
L.1.3.1. <i>eIdentity:ResponseStatus@from</i>	51
L.1.3.2. <i>eIdentity:ResponseMessage</i>	51
L.2. BEISPIELE.....	51
L.2.1. <i>eIdentity:IdentityServiceInitiationRequest</i>	52
L.2.1.1. ohne Signatur.....	52
L.2.1.2. mit Signatur	52
L.2.1.3. Mit Signatur: SO -> Bank.....	53
L.2.1.4. <i>IdentityServiceInitiationResponse</i> : ohne Fehler.....	55
mit Fehler	55
L.2.1.5.	55
L.2.2. <i>eIdentity:IdentityServiceConfirmation</i>	55
L.2.2.1. ohne Fehler: Bank -> SO	55
L.2.2.2. mit Fehler: SO -> Händler.....	56
L.2.2.3. Mit Token: SO -> Händler	58
L.2.3. <i>eIdentity:IdentityServiceConfirmationResponse</i>	59
L.2.3.1. ohne Fehler: Händler -> SO	59
L.2.3.2. mit Fehler: SO -> Bank	59
L.2.4. <i>eIdentity:IdentityServiceStatusRequest</i>	59
L.2.5. <i>eIdentity:IdentityServiceStatusResponse</i>	60
L.2.5.1. ohne Fehler	60
L.2.5.2. mit Fehler	61
L.2.6. <i>eIdentity:IdentityDetailsRequest</i>	62
L.2.7. <i>eIdentity:IdentityDetailsResponse</i> – ohne Fehler.....	63
L.2.8. <i>eIdentity:IdentityDetailsResponse</i> – mit Fehler	64
L.2.9. <i>eIdentity:IdentityDataTokenRequest</i>	65
L.2.10. <i>eIdentity:IdentityDataTokenResponse</i>	65
M. ANHANG – ANZEIGEMASKE IM ONLINE-BANKING	67
M.1. BEISPIEL	67
N. ANHANG – STAGING	68
N.1. PRODUKTION	68

N.2. TEST.....	68
N.3. ABNAHME	68
TABELLENVERZEICHNIS	69
ABBILDUNGSVERZEICHNIS.....	70

1. DOKUMENTATIONSHISTORIE

Version 1.0 Februar 2015

Mag. Alexander Schilling / Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH

Mag. Joachim Geisler / Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH

Markus Brejla, MSc. / ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H.

Thomas Pircher / ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H.

e-Identity Projektteam

Erstveröffentlichung

Version 1.0.1 März 2015

- Ersetzung des Blocks "AuthenticationDetails" durch das Feld "Signature" in der IdentityServiceConfirmation- sowie IdentityServiceResponse-Nachricht
- Ergänzung des Feldes "BankId" in der IdentityServiceConfirmation-Nachricht

Version 1.0.2 März 2015

- eIdentity:UserId für SHA256-Fingerprint-Berechnung ergänzt
- eIdentity:StatusReference aus eIdentity:IdentityServiceConfirmation entfernt
- Diverse inhaltliche Ergänzungen

Version 1.0.3 Mai 2015

- eID-Logo ergänzt
- Diverse inhaltliche Ergänzungen

Version 1.0.4 Juni 2015

- XML-Beispiel-Nachrichten korrigiert

Version 1.1.0 Dezember 2017

- eID Version 1.1

Version 1.1.1 Juni 2018

- Ergänzung akademischer Grad

Version 2.0 Oktober 2018

Mag. Alexander Schilling / Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH

Martin Pass / Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH

Matthias Kautz / ARZ Allgemeines Rechenzentrum Gesellschaft m.b.H.

e-Identity Projektteam

Version 2.0.1 Mai 2019

- Korrektur SHA-256 Fingerprint Berechnung

Version 2.0.2 August 2019

- 21.3.7 Erklärende Ergänzung zur Banknachricht bei unvollständiger Datenlieferung

Version 2.0.3 September 2019

- 21.3.2 Ergänzungen zu UserId und MerchantName bei Bankkommunikation

Version 2.1.0 Februar 2020

- eID Token

2. VORWORT

Das vorliegende Dokument behandelt den technischen Aufbau des e-Identity Service.

Das e-Identity Service stellt die Verifikation personenbezogener Daten über das Online-Banking der teilnehmenden Banken zur Verfügung.

Das e-Identity Service basiert auf einem offenen XML-Standard, alle Dokumentationen und technischen Spezifikationen sind unter **<https://eservice.stuzza.at>** zu finden.

3. EINLEITUNG

3.1. Aufbau und Inhalt des Dokuments

Das Dokument besteht aus mehreren Teilen.

- Kapitel 1-5 geben einen Überblick über das e-Identity Service.
- Das Kapitel „7. Ablauf des e-Identity Services“ selbst zeigt den Ablauf des Prozesses und beschreibt die einzelnen Schritte.
- „ definiert technische Rahmenbedingungen.
- Kapitel „6. Identitätsdaten“ listet alle personenbezogenen Daten auf, welche über das Service verifiziert werden können.
- In „A. Anhang – XML-Nachrichten“ sind die XML-Nachrichten dann einzeln auf XML-Ebene beschrieben.
- Details zu möglichen Fehlern liefert „B. Anhang – ResponseCodes“.

Das Dokument beschreibt als technische Dokumentation den Soll-Zustand. Auf Formulierungen wie „kann, soll, darf, muss“ wird verzichtet. Jede Abweichung von der Beschreibung ist ein Verstoß gegen das Pflichtenheft.

3.2. e-Identity Service

Das e-Identity Service ermöglicht die Anforderung und Verifikation personenbezogener Daten einer natürlichen Person über das Online-Banking-Portal der Kundenbank. Die anforderbaren bzw. verifizierbaren Daten umfassen Vorname, Nachname, Geburtsdatum, Adresse (Adresszeile, PLZ, Ort und Land), akademischer Grad sowie IBAN. Der Standard ist bewusst offen gestaltet, sodass zukünftig weitere Felder mit aufgenommen werden können ohne das Protokoll zu ändern.

Der Ablauf sieht vor, dass der Händler die von ihm benötigten persönlichen Daten bei der Kundenbank anfragt. Alternativ kann auch über eine Abfragemöglichkeit die Verifikation von Daten angefordert werden (zB Alter > 17, Nachname = ‚Mustermann‘)

Das hier beschriebene e-Identity Service wurde von der bankenübergreifenden Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr (STUZZA) gemeinsam mit den österreichischen Banken erarbeitet.

Das e-Identity Service basiert auf einem offenen, normierten XML Standard (Schnittstelle)!

Das e-Identity Service setzt auf dem jeweiligen Online-Banking System der Kundenbank auf und ermöglicht allen Bankkunden eine einfache Abwicklung bezüglich einer e-Identity Anfrage eines Händlers, beispielsweise bei Einkäufen über das Internet.

Der Vorteil liegt in der Vertrautheit, die der Kunde bereits gegenüber dem Online-Banking System gewonnen hat bzw. an den hohen Sicherheitsstandards der Online-Banking Systeme.

Der Kunde muss sich immer direkt in seinem Online-Banking identifizieren und den e-Identity Service Prozess in diesem autorisieren und damit freigeben. Der Kunde hat die Kontrolle darüber, welche Daten an den Händler übermittelt werden.

Dieser Online Service kann in Webshops von Unternehmen und der öffentlichen Verwaltung eingebunden werden und wird von den am e-Identity Service teilnehmenden (österreichischen) Banken unterstützt.

3.3. Begriffe

Im vorliegenden Pflichtenheft werden die folgenden Begriffe verwendet.

- Händler: jeder Webshop-Betreiber z.B. Unternehmen, Verein, Spendenorganisation, E-Government Anbieter / registriert und speichert personenbezogene Daten seiner Kunden
- Kunde: jede natürliche Person, die via Internet bei einem Händler registriert ist und über ein Konto verfügungsberechtigt ist.
- e-Identity Service Bank: Bank bzw. Kreditinstitut, die/das entweder als Händler- oder als Kundenbank Dienste im Wege des e-Identity Service anbietet
- Händlerbank: Bank bzw. Kreditinstitut, die/das mit einem bestimmten Händler eine e-Service Händlervereinbarung mit inkludiertem e-Identity Service geschlossen hat
- Kundenbank: Bank bzw. Kreditinstitut, die/das ihren Kontoinhabern bzw. Verfügungsberechtigten auf der Basis der e-Identity Service Schnittstelle die e-Identity Abwicklung mit einem Händler ermöglicht
- e-Service Scheme Operator: der im e-Identity Service Ablauf eingeschaltete Intermediär für das technische Routing von e-Identity Service Nachrichten (wird im Pflichtenheft auch als SO abgekürzt geführt)
- e-Identity Service Nachrichten: XML Nachricht gemäß des jeweils gültigen und frei verfügbaren technischen Pflichtenheftes
- BIC: Business Identifier Code (ISO 9362), online Abfrage unter <http://www.swift.com>, BIC Directory Online
- Online-Banking: Umfassender Begriff für elektronische Banking Anwendungen, z.B. Internet Banking
- SO Vertrag: Vereinbarung für die Nutzung der e-Services über den SO.
- XMLDSig: W3C Standard (<http://www.w3c.org>), beschreibt Regeln für digitale Signatur in XML Syntax

3.4. Referenzen im Dokument

Referenzen innerhalb des Dokuments erfolgen immer unter Angabe von Absatznummer und Absatztext.

In der technischen Beschreibung werden XML-Elemente über XPath-Angaben referenziert.

3.5. Referenzen auf weitere Dokumente

Dokument	Version und Datum
e-Identity Service-Beschreibung	https://eservice.stuzza.at
e-Identity Schema-Definitionen	https://eservice.stuzza.at
e-Identity Signaturprofil	https://eservice.stuzza.at
e-Service technisches Beiblatt	immer aktuell auf https://eservice.stuzza.at

Tabelle 1: Referenzen auf weitere Dokumente

4. LOGO E-IDENTITY SERVICE

Das e-Identity Service bildet ein bankenübergreifende Produkt für die Verifikation personenbezogener Daten im Internet. Das Service wird unter einer gemeinsamen Wort-Bild-Marke vertrieben.



Abbildung 1: Logo

Unter **<https://eservice.stuzza.at>** steht für die Integration des e-Identity Service ein entsprechendes Logo zum Download zur Verfügung.

5. ORGANISATORISCHE VORAUSSETZUNGEN

5.1. e-Service Scheme Operator

Das technische Routing aller e-Identity Service Nachrichten erfolgt ausschließlich über den zentralen e-Service Scheme Operator (SO).

Der SO ist für den Händler über den zentralen Routing Server <https://routing.e-identity.at> erreichbar.

Falls eine Händlerbank einen speziellen Namen für den Routing Server anbietet, informiert diese den Händler im Zuge des Abschlusses der Händlervereinbarung darüber.

5.2. e-Service Händlervereinbarung

Voraussetzung für das Anbieten des e-Identity Service beim Händler ist der Abschluss einer e-Service Händlervereinbarung über die Abwicklung von e-Identity Verifikationen mit einer für dieses Service zugelassenen Bank nach dem Standard des hier beschriebenen e-Identity Service.

5.3. Teilnahmevoraussetzungen

Unterzeichnung einer e-Service Vereinbarung zur Nutzung des e-Identity Service über den Scheme Operator. Weitere Details dazu in „e-Identity Service-Beschreibung“ (3.5. Referenzen auf weitere Dokumente).

6. IDENTITÄTSDATEN

Der e-Identity Service bietet die Möglichkeit persönliche Daten vom Online-Banking-System des Kunden abzufragen oder die Gültigkeit von eingegebenen Daten zu verifizieren. Folgende Identitätsdaten werden derzeit unterstützt:

- Vorname
- Nachname
- Akademischer Grad
- Geburtsdatum
- Adresse
 - Straße
 - PLZ
 - Ort
 - Land
- IBAN
- Alter

Die Kundenbank liefert, abgesehen von Fehlerfällen, immer die angeforderten Daten. Sollte eine Verifikation vom Händler verlangt werden, wird diese im SchemeOperator durchgeführt. Mittels einer einfachen Abfragelogik kann der Händler für einzelne Datenfelder Abfragen erstellen. Beispielsweise können folgende Abfragen erstellt werden:

- Alter > 17
- Vorname = Max

Bei der Prüfung auf Gleichheit werden Toleranzen bezüglich Groß-/Kleinschreibung und Sonderzeichen (zB ß,é,-) eingebaut.

7. ABLAUF DES E-IDENTITY SERVICES

7.1. Ablaufbeschreibung – Übersicht

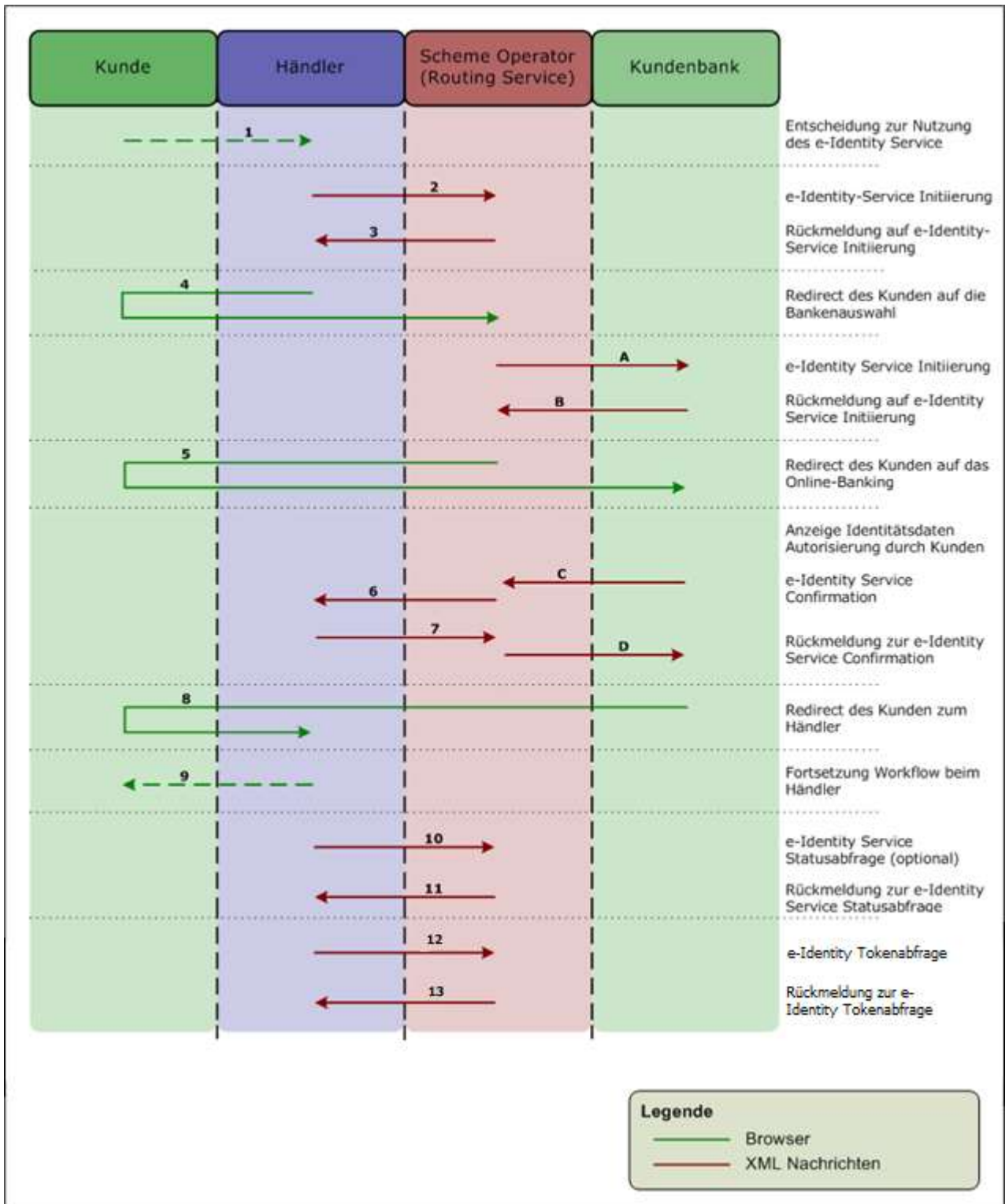
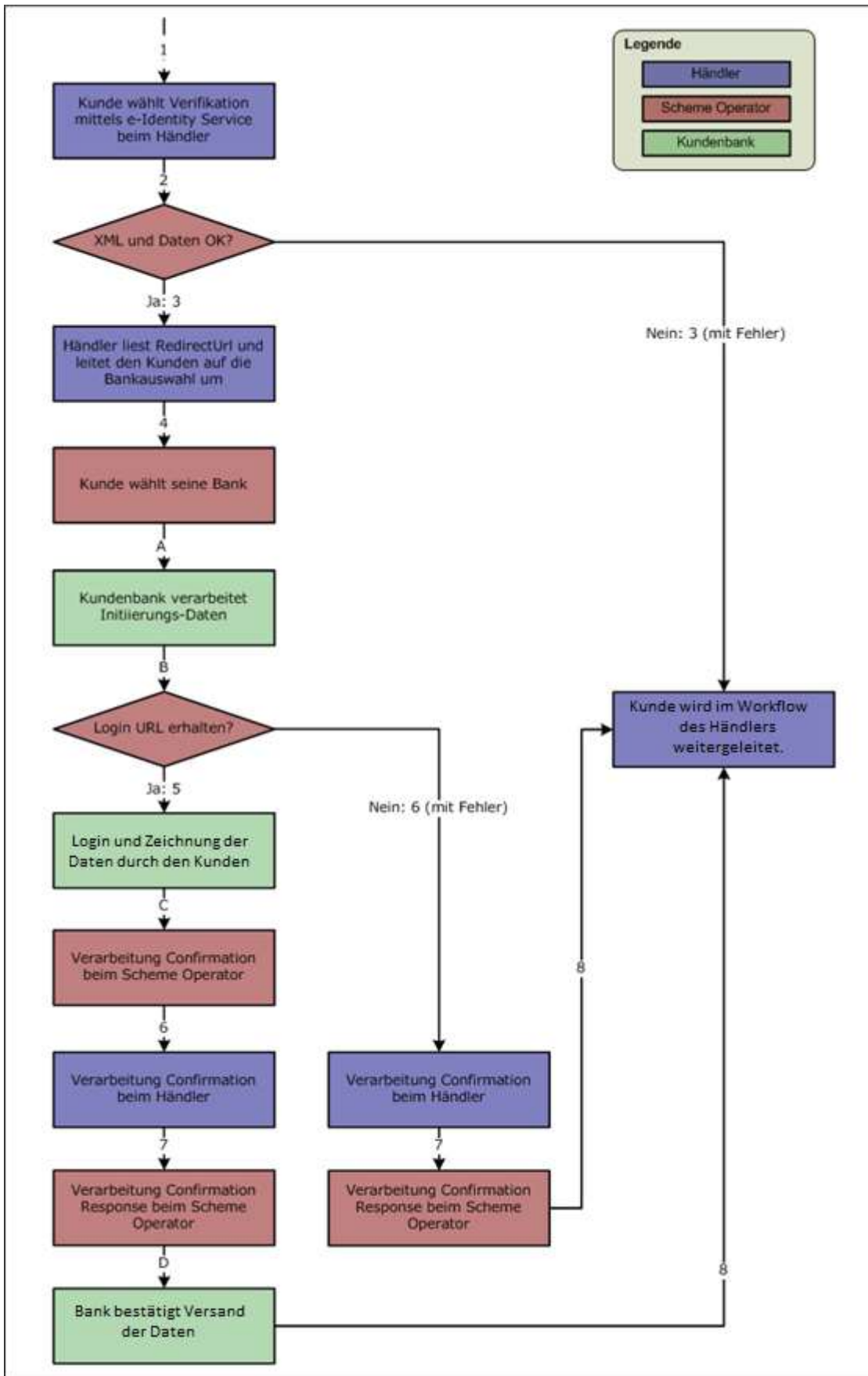


Abbildung 2: Ablaufbeschreibung – Übersicht

Die Ablaufbeschreibung stellt den Workflow eines erfolgreichen e-Identity Service Prozesses im Kontext aller beteiligten Parteien dar.

7.2. Ablaufbeschreibung im Detail



Abbildung

3: Ablaufbeschreibung im Detail

Die Detailablaufbeschreibung versteht sich als Zustandsdiagramm und zeigt alle möglichen Wege, die ein e-Identity Service-Prozess nehmen kann.

7.3. Die einzelnen Schritte

Der einzelne e-Identity Service Prozess läuft in mehreren Schritten ab, die im Folgenden fachlich beschrieben sind. Die zugehörigen XML-Nachrichten sowie deren Felder beschreibt „A. Anhang – XML-Nachrichten“.

7.3.1. Schritt 1: Entscheidung zur Nutzung des e-Identity Service

Der Kunde wählt im Webshop die Option „e-Identity Verifikation“ und nutzt die entsprechende Prüfung durch das e-Identity Service.

7.3.2. Schritt 2: Übermittlung e-Identity Service Initiierung

Der Händler übermittelt die „A.2.1 eIdentity:IdentityServiceInitiationRequest“ Nachricht an den SO. Diese beinhaltet alle durch die Kundenbank zu liefernden Daten bzw. Abfragen. Außerdem hat der Händler die Möglichkeit bereits bei der Zahlungsinitiierung die BIC der Käuferbank als Anhang der Initiierungsurl oder als Teil der XML Nachricht zu übermitteln. Wenn die gewählte Bank das e-Identity Service unterstützt erfolgt direkt der Redirect zur Kundenbank im Schritt 5. Ansonsten wird der Kunde, wie in den folgenden Schritten beschrieben, über die Bankauswahlseite geroutet. Weiters kann der Händler entscheiden, ob in der Confirmation Nachricht die eigentlichen Daten, oder nur ein eIdentity Token vom SchemeOperator geliefert wird. Bei Verwendung eines eIdentity Tokens können die Echtdaten vom Händler zu einem späteren Zeitpunkt abgefragt werden.

7.3.3. Schritt 3: Rückmeldung auf e-Identity Service Initiierung

Nach einer syntaktischen Prüfung der einlangenden Initiierungsnachricht erstellt der SO eine „A.2.2 eIdentity:IdentityServiceInitiationResponse“ Nachricht, die immer eine Status-Referenz für genau diesen einen Prozess enthält. Zusätzlich wird dem Händler noch die TransactionId und eine QRCodeUrl mitgeliefert. Diese Daten werden für die alternativen mobilen Workflows benötigt. Diese Workflows werden detailliert im Kapitel 8. eid4mobile beschrieben)

7.3.3.1. a) ohne Fehler

Sind die Daten in der e-Identity Service Initiation Request Nachricht (7.3.2. Schritt 2: Übermittlung e-Identity Service Initiierung) korrekt, speichert der SO diese zwischen und sendet dem Händler in der Antwortnachricht eine URL für den Redirect auf die beim SO implementierte Bankenauswahl (7.3.4. Schritt 4: Redirect des Kunden auf die Bankenauswahl).

7.3.3.2. b) bei Auftreten eines Fehlers

Sind die Daten der Initiierungsnachricht Nachricht (7.3.2. Schritt 2: Übermittlung e-Identity Service Initiierung) nicht verarbeitbar (leerer IdentityData-Block, Autorisierungsfehler, Fehler im XML, ...) werden außer der Status-Referenz keine Daten übermittelt. Der Ablauf setzt direkt mit der Statusabfrage (7.3.10. Schritt 10: e-Identity Service) fort.

7.3.4. Schritt 4: Redirect des Kunden auf die Bankenauswahl

Der Kunde wird von der der Seite des Händlers mittels Redirect auf die Bankenauswahl beim SO geleitet. Dieser Schritt entfällt bei den Mobile Varianten POS2App (8.3.) und App2App (8.4) Die URL dazu kommt aus den Daten aus „7.3.3. Schritt 3: Rückmeldung auf e-Identity Service Initiierung“.



ELEKTRONISCHES IDENTIFIKATIONSVERFAHREN

Bitte wählen Sie Ihre Bank aus.

Bankname/BIC/BLZ:

Vorgang abbrechen

Weiter zum Online-Banking

Abbildung 4: Bankenauswahl

Neben der Wahl einer Bank kann der Kunde den Prozess an der Stelle auch abbrechen. Der Ablauf setzt mit „7.3.8. Schritt 8: Redirect des Kunden zum Händler“ fort.

7.3.5. Schritt 5: Redirect des Kunden auf das Online-Banking

Nach der Wahl seiner Bank gelangt der Kunde zum Login des Online-Bankings seiner Bank, wo er sich wie gewohnt gegenüber der Anwendung authentifiziert.

Analog „7.3.4. Schritt 4: Redirect des Kunden auf die Bankenauswahl“ besteht die Möglichkeit für den Kunden schon vor dem Login den Prozess abzubrechen. Der Ablauf setzt mit „7.3.8. Schritt 8: Redirect des Kunden zum Händler“ fort.

7.3.6. Schritt 6: e-Identity Service Confirmation

Nach dem Login im Online-Banking wird dem Kunde die e-Identity-Maske angezeigt, welche alle vom Händler geforderten Daten listet. Der Kunde sieht die Daten, welche bei der Bank hinterlegt sind und an den Händler gesendet werden. Sollte die Bank den gewünschten Feldtyp nicht unterstützen erhält der Händler für dieses Feld den Status „UNKNOWN“ und den ResponseCode 105 (Unvollständige Identifikation) bzw. 110 (Fehlgeschlagene Identifikation) wenn gar kein Feld geliefert wird. Der Kunde zeichnet die e-Identity Datenlieferung mittels der mit seiner Bank vereinbarten Autorisierungsmethode.

Die Bank erstellt eine entsprechende „A.2.3 eIdentity:IdentityServiceConfirmation“ Nachricht mit Response-Code (ein Überblick zu den Response-Codes findet sich unter „B Anhang – ResponseCodes“) und schickt diese dem SO retour.

Hierbei ist zu beachten, dass der SO die eingehende Confirmation-Nachricht u.a. auch auf folgendes hin prüft:

- Ist bei einem Response-Code „100“ (Erfolgreiche Datenlieferung) jedes angeforderte Feld befüllt.
- Ist bei einem Response-Code „105“ (Unvollständige Identifikation) zumindest ein angefordertes Feld nicht vorhanden.

Schlägt eine dieser Prüfungen fehl, verschickt der SO eine Confirmation-Response-Nachricht an die Käuferbank mit Response-Code „002“ (Fehler bei Feldprüfung). Der Händler wird in diesem Fall nicht informiert.

Vor der Autorisierung besteht für den Kunden jederzeit die Möglichkeit den Prozess abzubrechen, wodurch eine Nachricht mit entsprechendem Response Code (siehe „B Anhang – ResponseCodes“) generiert wird.

Die von der Kundenbank an den SO gerichtete Confirmation-Nachricht wird von diesem an den Händler weitergereicht. Wenn vom Händler Verifikationsergebnisse angefragt wurden, werden die Daten am SO mit den vom Händler gelieferten überprüft und das Ergebnis wird an den Händler geliefert. Der Händler kann pro Feld entscheiden ob ein Verifikationsergebnis oder eine Datenlieferung gewünscht wird. Wurde vom Händler im Initiierungsrequest die Erstellung eines eIdentity Tokens verlangt, sendet der SchemeOperator anstelle des Prüfergebnisses bzw. der Echtdaten den generierten Token.

7.3.7. Schritt 7: Rückmeldung zur e-Identity Service Confirmation

Der Händler quittiert den Empfang der Confirmation-Nachricht durch den Versand einer „A.2.4 eIdentity:IdentityServiceConfirmationResponse“ Nachricht an den SO, welcher diese wiederum an die Kundenbank weiterleitet.

Sollte der Händler eine nicht XML-Schema-konforme Nachricht erhalten bzw. die vom SO gesetzte Signatur nicht validieren können, antwortet er in seiner Confirmation-Response-Nachricht mit Response-Code „001“ (XML-Fehler) bzw. „004“ (Autorisierung fehlerhaft), in allen anderen Fällen (sofern die Verarbeitung der eingehenden Confirmation-Nachricht möglich war) aber mit Response-Code „000“.

7.3.8. Schritt 8: Redirect des Kunden zum Händler

Als letzter Schritt im regulären Workflow erfolgt ein Redirect des Kunden auf den Webaufttritt des Händlers. Die dafür verwendete URL wird aus den weitergeleiteten Initiierungsdaten aus „7.3.2. Schritt 2: Übermittlung e-Identity Service Initiierung“ extrahiert.

7.3.9. Schritt 9: Fortsetzung Workflow beim Händler

Auf Basis der Confirmation kann der Händler den Workflow in seiner Anwendung fortsetzen.

7.3.10. Schritt 10: e-Identity Service Statusabfrage (optional)

Der Händler hat zusätzlich die Möglichkeit, unter Zuhilfenahme der Status-Referenz aus „7.3.3. Schritt 3: Rückmeldung auf e-Identity Service Initiierung“, eine „A.2.5 eIdentity:IdentityStatusRequest“ Nachricht an den SO abzusetzen. Eine Abfrage ist bis zu der in „e-Service technisches Beiblatt“ (3.5. Referenzen auf weitere Dokumente) spezifizierten Dauer möglich.

Die Statusabfrage gibt dem Händler die Möglichkeit bei unvorhergesehenen Workflow-Abbrüchen (beispielsweise ist die Übermittlung der Confirmation an den Händler fehlgeschlagen) den Ausgang der e-Identity Verifikation im Nachhinein abzufragen.

7.3.11. Schritt 11: Rückmeldung zur e-Identity Service Statusabfrage

Inhalt der „A.2.6 eIdentity:IdentityStatusResponse“ Nachricht sind grundsätzlich jene Daten, welche auch in der Confirmation-Nachricht aus „7.3.6 Schritt 6: e-Identity Service Confirmation“ enthalten sind. Bei Verwendung einer eIdentity Tokens wird auch bei der Statusabfrage nur der generierte Token zurückgeliefert. Zur Anforderung der Echtdaten muss der Token Request verwendet werden.

Erfolgt die Status-Abfrage noch vor Ausstellung der Confirmation durch die Kundenbank, wird die Status-Response mit einem entsprechendem ResponseCode gesetzt.

Aufschluss über die Ursache, weshalb der Prozess gegebenenfalls nicht erfolgreich beendet wurde, geben die definierten ResponseCodes („B. Anhang – ResponseCodes“).

7.3.12. Schritt 12: e-Identity Tokenabfrage

Sollte der Händler die tatsächlichen Identitätsdaten seiner ursprünglichen Anfrage benötigen, hat er die Möglichkeit, mit dem zur Verfügung gestellten Token, die Identitätsdaten abzufragen. Geliefert werden die gleichen Daten, welche auch in der Confirmation Nachricht ohne Tokenabfrage bereitgestellt werden.

8. EID4MOBILE

Zur besseren Unterstützung der Mobile Apps der Banken wurde aufsetzend auf den herkömmlichen eid Ablauf der eid4mobile Workflow entwickelt. Ziel ist es die Identifikation für den Kunden bei Verwendung von mobile Apps möglichst einfach und effizient zu gestalten. Zentraler Bestandteil für die Mobile Funktionalität sind die Felder TransactionID und QRCodeUrl, welche in der eIdentity:IdentityServiceInitiationResponse dem Händler übermittelt werden. Die TransactionID dient dem Händler nur als zusätzliche Referenz. Bankenseitig wird die TransactionID zum Abholen der Initiierungsdaten vom Händler verwendet. Die QRCodeUrl kann vom Händler für die Anzeige eines QR Codes zur Initiierung verwendet werden.

eps4mobile kann in folgenden Szenarien eingesetzt werden:

1. Browser2App via QR-Code

Nach dem Redirect zur Login Seite der Bank kann der Käufer neben dem bekannten Login in das Online-Banking auch via QR-Code die eIdentifikation starten. Der QR-Code kann vom Käufer in die mobile Banking App am mobilen Gerät importiert werden (durch Scanning Funktion der Banking App). Danach erfolgt die eIdentifikation in der mobile Banking App und nicht im Online-Banking.

2. POS2App via QR-Code

Die eIdentifikation erfolgt nicht im Online-Banking, sondern mittels QR-Code in einer mobilen Banking App.

Der Händler erzeugt eine Initiierung, die an den SO übermittelt wird. Dieser übermittelt dem Händler Informationen, mit denen der Händler einen QR-Code erstellen kann, der dem Käufer an einem POS oder lokalen PC angezeigt werden kann. Der QR-Code kann vom Käufer in die mobilen Banking App am mobilen Gerät importiert werden (durch Scanning Funktion der mobilen Banking App), die eps Zahlung erfolgt in einer mobilen Banking App.

3. App2App

Die gesamte Identifikation erfolgt auf einem mobilen Gerät. Die Identifikation wird aus einer App des Händlers initiiert. Der Händler erzeugt einen IdentityServiceInitiationRequest, der an den SO übermittelt wird. Dieser übermittelt dem Händler Informationen in Form einer URL mit dem spezifischen Schema „eidentity“ (z.B. eidentity://eps.or.at/?transactionid=123HOXA123). Der Käufer wird auf seinem mobilen Gerät von der Händler App unter Verwendung des URL Schemas zur Banking App (App2App) weitergeleitet, um die Identifikation durchführen zu können. Falls der Käufer über mehrere Bankverbindungen und somit Banking Apps verfügt, so muss er diese gegebenenfalls gem. seinem Betriebssystem manuell auf seinem Gerät auswählen. In allen angeführten Szenarien werden niemals bankspezifische Zugangsdaten des Käufers von einer dritten Stelle abgefragt oder zwischengespeichert, der Käufer muss sich immer direkt gegenüber der Bank Applikation autorisieren und die Identifikation durch bekannte Autorisierungsverfahren freigeben.

8.1. Technische Anforderungen QR-Code

Anhand der vom SO erzeugten QRCodeUrl Information kann der Händler bzw. die Bank (auf der Login Seite des Online-Banking) einen QR-Code für die weitere Bearbeitung in der mobilen Banking App des Käufers generieren.

Im QR-Code ist z.B. folgender Link enthalten:
eidentity://eps.or.at/?transactionid=123HOXA123

Dieser beinhaltet die TransactionID als Parameter (transactionid=123HOXA123).

Der QR-Code Aufbau (Größe, Farbe, etc.) obliegt dem Händler bzw. der Bank. Wir empfehlen die Darstellung in schwarz, ohne Rand und ohne Logo (siehe Abbildung 5: Beispiel QR-Code).



Abbildung 5: Beispiel QR-Code

8.2. eid4mobile Browser2App via QR-Code

In den folgenden Schritten wird der Ablauf eid4mobile Browser2App via QR-Code beschrieben. Es werden nur die Schritte beschrieben, welche abweichend vom bereits zuvor beschriebenen eid Workflow sind.

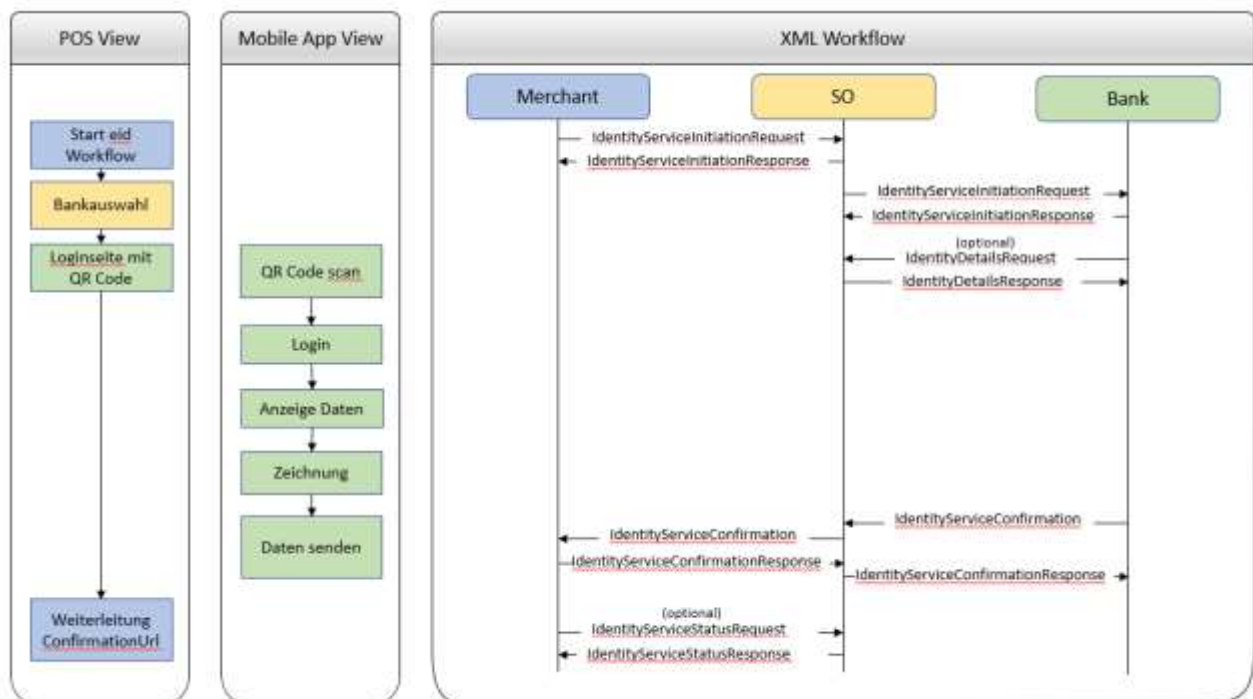


Abbildung 6: Ablaufbeschreibung Browser2App

SO - eid Initiierungsauftrag an Käuferbank

Die vom SO erzeugten Datenelemente "epsp:TransactionID" und "epsp:QRCodeUrl" werden vom SO an die Käuferbank übermittelt.

Anhand der vom SO erzeugten epsp:QRCodeUrl Information kann die Käuferbank einen QR-Code für das Käufer Login in eine mobile Banking App generieren.

Scanning QR-Code von Banking Login-Seite

Auf der Login Seite der Käuferbank kann der Käufer zwischen dem bekannten Login zum Online-Banking (z.B. ID und PIN), oder mittels QR-Code die Weitergabe des Logins an ein mobiles Gerät wählen.

Im Szenario „Browser2App“ scannt der Käufer den QR-Code mit der mobilen Banking App.

Bank – Init Request an SO

Optional kann die Käuferbank die eps4mobile Transaktionsdaten über einen eIdentity:IdentityDetailsRequest, der an den SO gesendet werden muss, vom SO anfordern.

SO – Antwort auf Init Request an Bank

Der SO beantwortet den eIdentity:IdentityDetailsRequest wiederum mit einer eIdentity:IdentityDetailsResponse Nachricht.

Käufer – Anzeige Daten

Die Käuferbank muss sicherstellen können, dass die angorderten Daten nach dem erfolgreichen QR-Code Scan in der mobilen Banking App dem Käufer angezeigt werden. Mittels der in der Käuferbank üblichen Autorisierungsmethoden wird die Datenlieferung freigegeben.

Statusinformation an Käufer

Am mobilen Gerät (z.B. Handy) wird dem Käufer in der Banking App der Status der Identifikation angezeigt (OK/NOK).

8.3. eid4mobile POS2App via QR-Code

In den folgenden Schritten wird der Ablauf eid4mobile POS2App via QR-Code beschrieben.

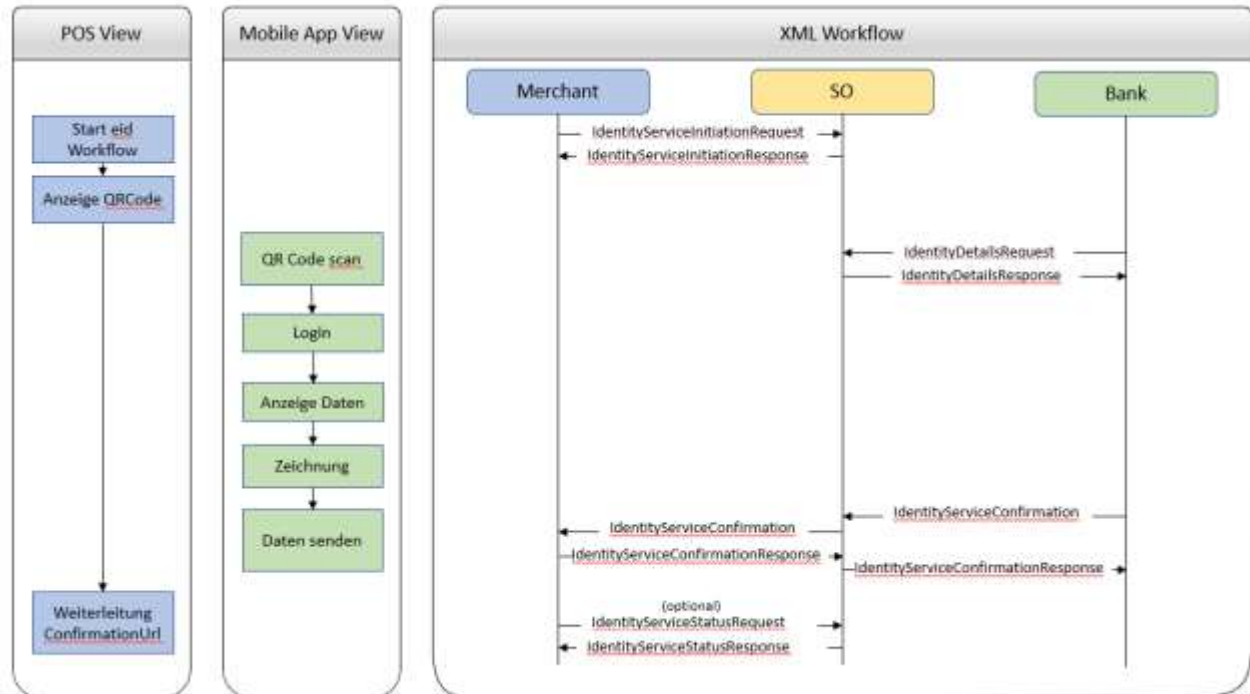


Abbildung 7: Ablaufbeschreibung POS2App

Händler - Anzeige QR-Code

Der Händler zeigt dem Käufer den QR-Code an.

Käufer - Scanning QR-Code

Im Szenario „POS2App“ scannt der Käufer den QR-Code mit der mobilen Banking App.

Die Bank muss die TransactionID aus dem Parameter „transactionid“ (z.B: transactionid=123HOXA123) parsen und den Wert als TransactionID in den Folgeschritten mitgeben (z.B. 123HOXA123).

Bank – Init Request an SO

Die Käuferbank muss die eps4mobile Transaktionsdaten über einen eIdentity:IdentityDetailsRequest, der an den SO gesendet werden muss, vom SO anfordern.

SO – Antwort auf Init Request an Bank

Der SO beantwortet den eIdentity:IdentityDetailsRequest wiederum mit einer eIdentity:IdentityDetailsResponse Nachricht.

8.4. eid4mobile App2App

In den folgenden Schritten wird der Ablauf eid4mobile App2App beschrieben.

Der gesamte Prozess (Kauf beim Händler, Bezahlvorgang in Banking App) erfolgt am selben Gerät des Käufers.

Etwaige spezielle Authentifizierungsvorgaben gegenüber der Bank werden hier nicht dargestellt!

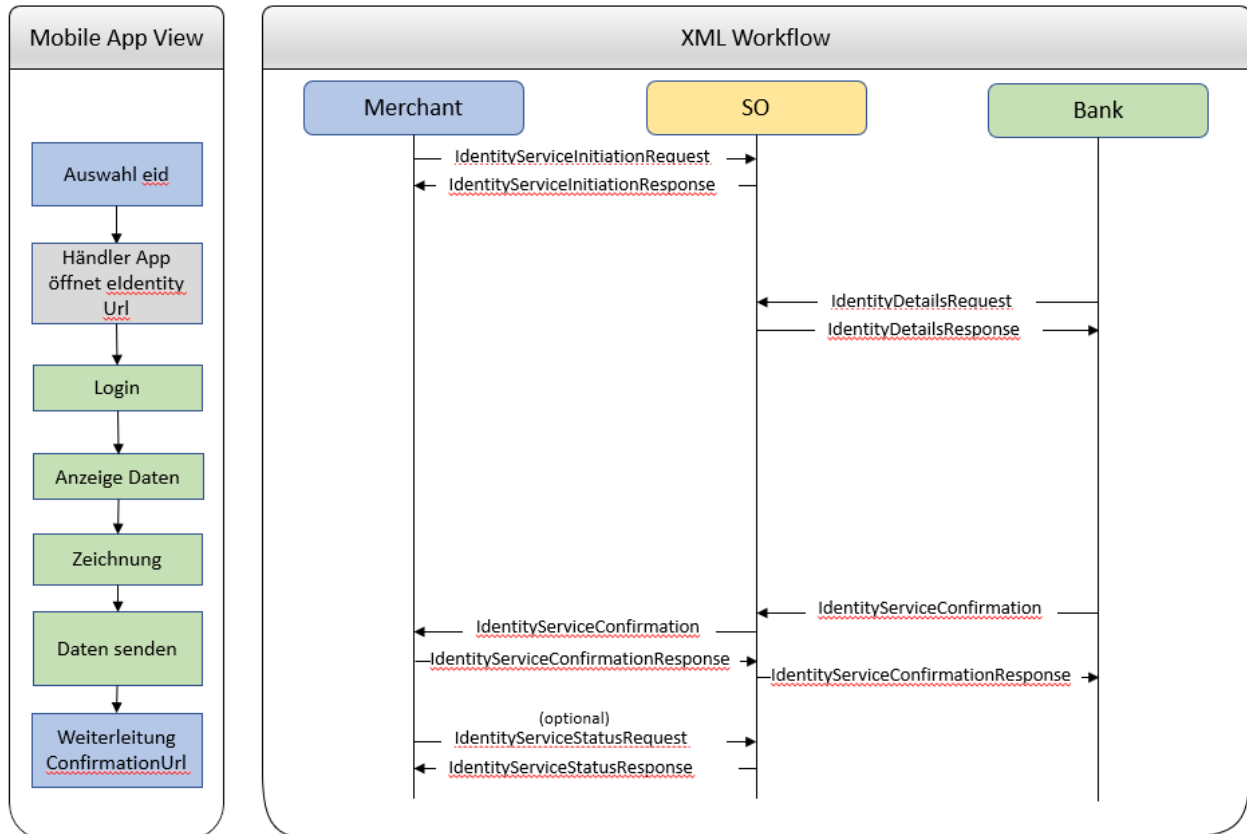


Abbildung 8: Ablaufbeschreibung App2App

Käufer - Auswahl eIdentity

Der Käufer wählt in der HändlerApp den Identifizierungsprozess über eIdentity aus.

Händler - eid Initiierung an SO

Der Händler erstellt den eIdentity:IdentityServiceInitiationRequest und übermittelt diesen an die URL des SO.

In der Initiierungsnachricht ist in diesem Szenario keine Käuferbic enthalten.

Weiterleitung App2App

Der im Element QRCodeUrl übermittelte Link wird aufgerufen, woraufhin der Käufer auf seinem mobilen Gerät von der Händler App zur Banking App (App2App) weitergeleitet wird, um die Identifizierung durchführen zu können.

Das Wechseln der App wird vom mobilen Betriebssystem bewerkstelligt und funktioniert nur, wenn auf dem mobilen Gerät eine App für das benutzerdefinierte URI-Schema „eidentity“ registriert ist.

Falls der Käufer über mehrere Bankverbindungen und somit Banking Apps verfügt, die auf „eidentity“ registriert sind, so ist das Ergebnis Betriebssystem abhängig.

9. EID TOKEN

Mit der Version 2.1 wurde für den Händler eine Möglichkeit eröffnet anstelle der Identitätsdaten vom Kunden, ein Identitätstoken vom SchemeOperator anzufordern. Für dieses Token kann der Händler auch ein Gültigkeitsdatum angeben. Maximal kann aber ein Token nur für 3 Jahre ab Initiierungszeitpunkt angefordert werden. Unter Angabe des Tokens kann der Händler über den autorisierten IdentityDataTokenRequest bei Bedarf die Echtdaten des Kunden anfordern. Die Echtdaten können auch mehrmals vom Händler angefordert werden.

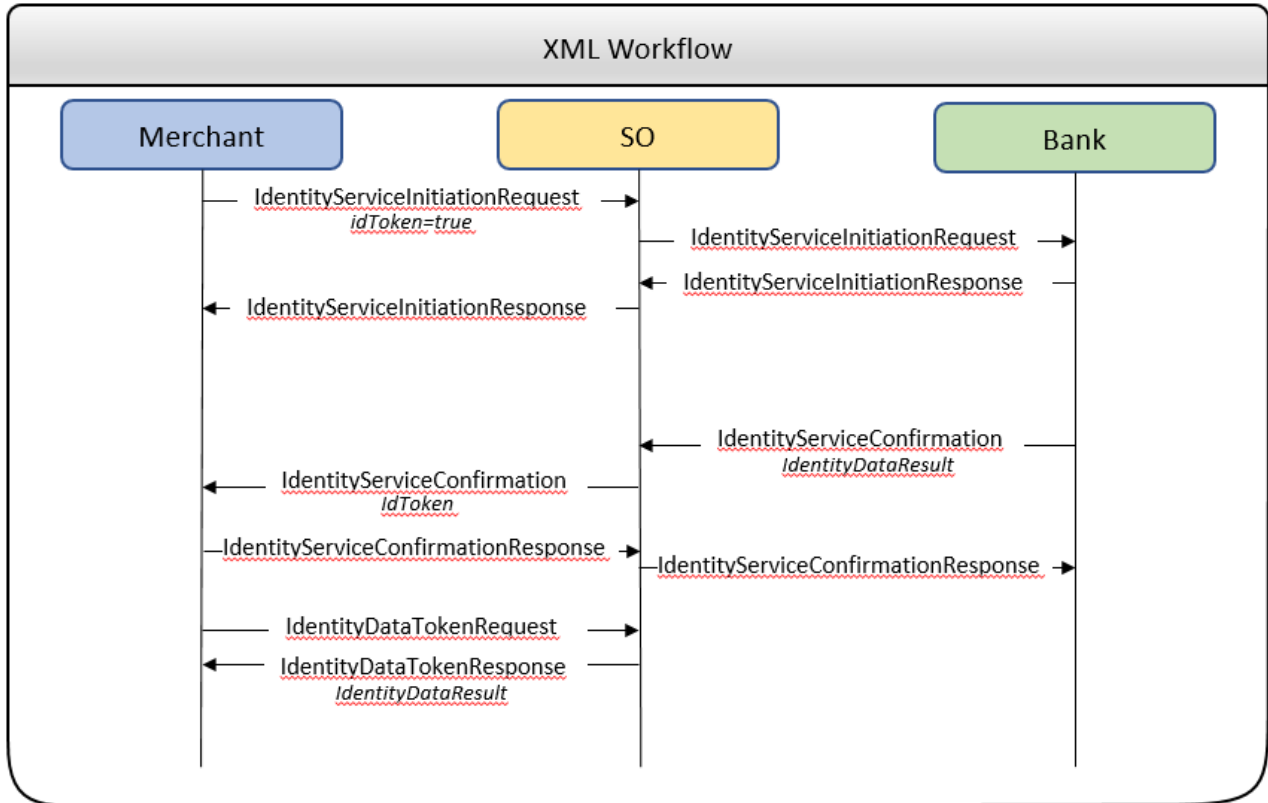


Abbildung 9: Workflow eID Token

10. TECHNISCHE ANFORDERUNGEN

10.1. XML Spezifikation

Die XML Struktur der e-Identity Service XML Schemata entsprechen dem W3C Standard. Es wird ausschließlich UTF-8 Encoding unterstützt. Der Content Type der Nachrichten lautet „text/xml“.

10.2. e-Identity Service XML Definitionen

Alle e-Identity Service relevanten Nachrichten sind in einem Schema definiert. Die jeweils gültigen e-Identity Service XML Schemata sind unter <https://eservice.stuzza.at> verfügbar und vom Händler zu unterstützen. Sämtliche Felder haben eine Längenbeschränkung. Die Gesamtgröße des XML inkl. Kommentaren darf maximal 120% der Maximalgröße des XML ohne Kommentare unter Ausnutzung aller Feldlängen aller (auch optionalen) Felder betragen.

10.3. Zeichensatz e-Identity Service XML Schema

Um eine Weiterverarbeitung der Nachrichten in den Bankensystemen garantieren zu können, werden wohl definierte Zeichensätze verwendet.

10.3.1. eingeschränkter Zeichensatz

Sofern beim jeweiligen Datenelement (A. Anhang – XML-Nachrichten) nicht ausdrücklich anders angegeben gilt folgender eingeschränkter Zeichensatz.

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
/ - ? : () . , ' +
Space

10.3.2. erweiterter Zeichensatz

Bspw. für Namen/Adressen stehen weiterhin die gewohnten AT Zeichen (erweiterter Zeichensatz) zur Verfügung.

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
- € \$ § % ! = # ~ ; + / ? : () . , ' & > < " | * { } [] @ \ _ ° ^
Ä Ö Ü ä ö ü ß
Space

10.4. Protokoll Nachrichtenaustausch

Der Transfer erfolgt ausschließlich mit HTTPS. Details sind in „e-Service technisches Beiblatt“ (3.5. Referenzen auf weitere Dokumente) spezifiziert.

10.5. Time Out

Die technischen TimeOut-Vorgaben (Connection/Socket Timeout) sind in „e-Service technisches Beiblatt“ (3.5. Referenzen auf weitere Dokumente) zusammengefasst.

10.6. Zeitsynchronität

Beginnend beim Händler, über den Scheme Operator bis hin zur Online-Banking Applikation sollen alle beteiligten Systeme zeitlich synchronisiert sein. Details in „e-Service technisches Beiblatt“ (3.5. Referenzen auf weitere Dokumente).

10.7. URL Angaben

Alle für den e-Identity Service Workflow relevanten URL-Angaben erfolgen absolut, z.B. <https://www.example.com:8080/banking/login.html>. Die Länge ist generell auf 512 Zeichen beschränkt.

10.7.1. URL/XML Encoding

(Query-)Parameter an einer URL sind gemäß Spezifikation urlcodiert. Die URL selbst ist dann innerhalb eines XML entsprechend xmlcodiert.

10.7.1.1. Beispiel

URL: <http://www.example.com/shop/transactionOk>

Parameter 1: param1=value 1

Parameter 2: param2=temp&xxx

Parameter 3: param3=Händler

⇒ URL:

<http://www.example.com/shop/transactionOk?param1=value+1¶m2=temp%26xxx¶m3=H%E4ndler>

⇒ XML-encoded URL-encoded URL:

<http://www.example.com/shop/transactionOk?param1=value+1&param2=temp%26xxx&param3=H%E4ndler>

10.8. Sicherheit

Die Kommunikation vom Händler zum SO und in weiterer Folge zwischen SO und Bankrechner erfolgt ausschließlich über HTTPS. Es wird empfohlen, dass auch die Kommunikation zwischen Käufer und Händler im Zuge des Zahlungsvorganges mittels HTTPS verschlüsselt sein sollte.

Weitere technische Vorgaben zu den erlaubten Verschlüsselungsprotokollen sind als technisches Beiblatt veröffentlicht (siehe „3.5. Referenzen auf weitere Dokumente“).

10.9. Pflichtfelder

Alle in der Schnittstellenbeschreibung angeführten Pflichtfelder (lt. Schemadefinition) müssen in der XML-Nachricht vorhanden und mit Inhalt befüllt sein.

10.10. Window-Management

Der empfohlene Ablauf erfolgt komplett in einem Browserfenster.

Der Händler stellt in seinem Webauftritt sicher, dass das Browserfenster keinen Namen hat.

Die Banking-Anwendung (bzw. die Bankenauswahl beim SO als vorgeschalteter Teil) lässt sich nicht in Frames einbinden. Der Redirect hat bei Verwendung von Frames somit auf Top-Level-Ebene zu erfolgen.

Darüber hinaus prüft das Online-Banking, dass keine Cross-Domain Zugriffe über Referenzen auf dieses Fenster (bspw. durch Erstellen des Fensters als Popup) möglich sind.

Der abschließende Redirect des Kunden zum Händler erfolgt wiederum im selben Fenster, sofern der allgemeine Workflow im Online-Banking dies zulässt.

20. EINLEITUNG – BANKENSEITE

20.1. Aufbau des Dokuments

Das Gesamtdokument ist so konzipiert, dass zu jeder Zeit durch einfaches Löschen der bank-spezifischen Kapitel das Pflichtenheft für den Händler erstellt werden kann.

Letztere enthalten Informationen, die für den Händler nicht relevant sind. Umgekehrt finden sich darüber hinausgehende Informationen ausschließlich in den bankspezifischen Kapiteln (Beschreibungen ab „20. Einleitung – Bankenseite“ und Anhänge ab „L. Anhang – XML-Nachrichten zwischen Bank und e-Service Scheme Operator“). Diese sind nicht als eigenständige Dokumentation für die Bankseite zu verstehen sondern als Ergänzung zum übrigen Pflichtenheft.

Die Nummerierung der bankspezifischen Kapitel lässt Raum für mögliche zukünftige Erweiterungen (ohne, dass sich die bestehenden Kapitelnummern ändern müssen).

21. ABLAUF DES E-IDENTITY SERVICES AUF BANKENSEITE

21.1. Ablaufbeschreibung - Übersicht

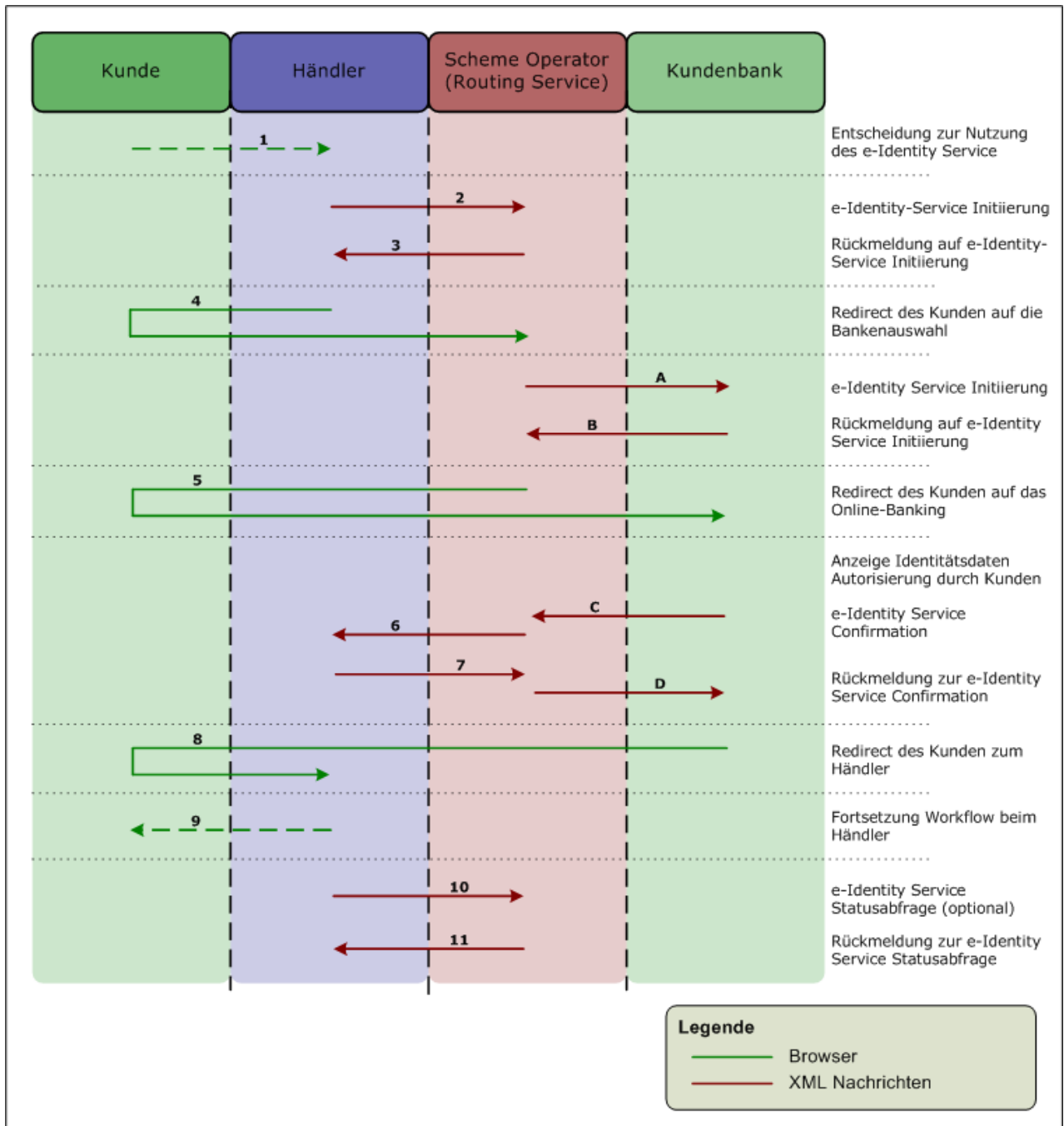


Abbildung 10: Ablaufbeschreibung – Übersicht

Die Ablaufbeschreibung stellt den Workflow eines erfolgreichen e-Identity Service Prozesses im Kontext aller beteiligten Parteien dar.

21.2. Ablaufbeschreibung im Detail

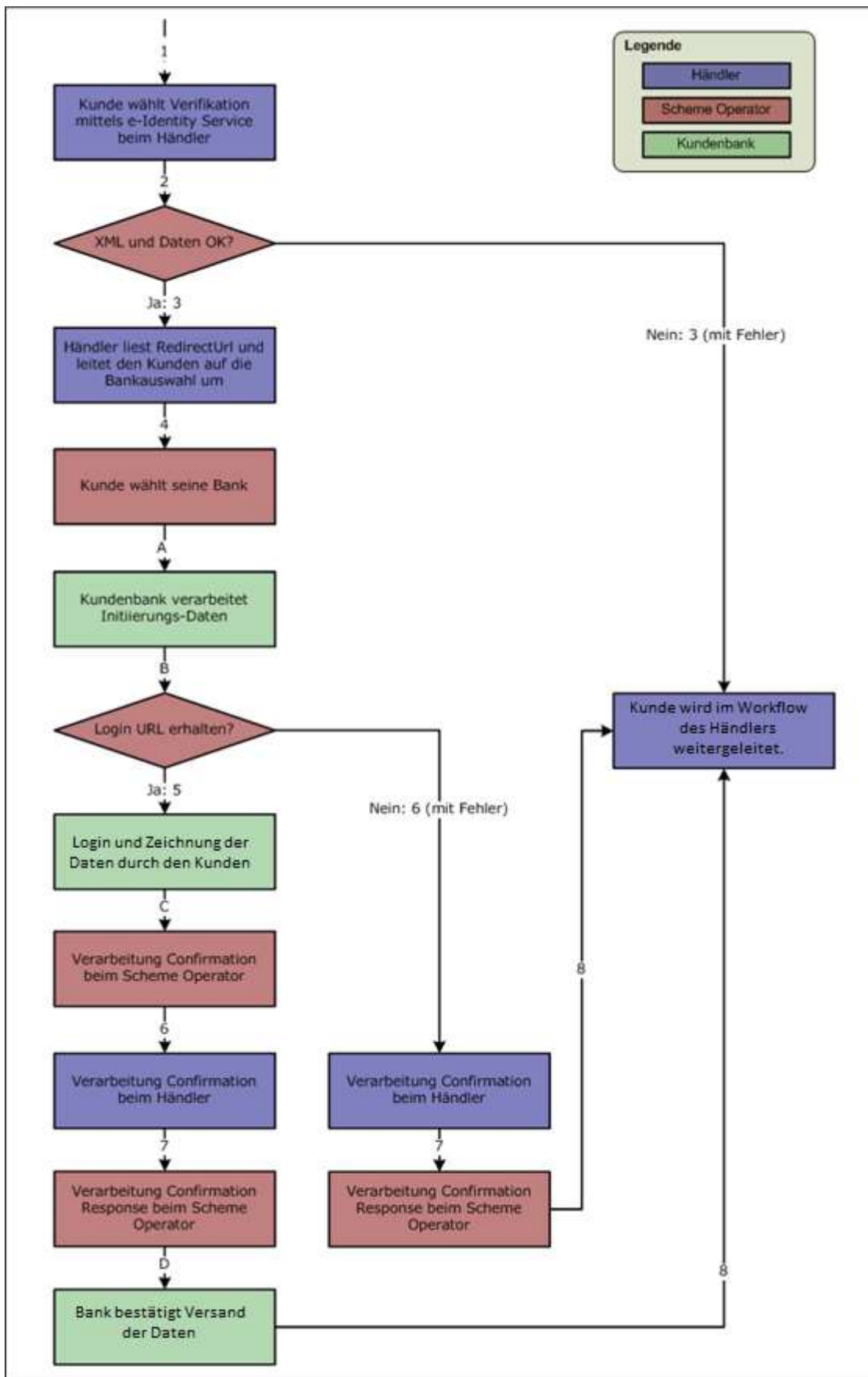


Abbildung 11: Ablaufbeschreibung im Detail

Die Detailablaufbeschreibung versteht sich als Zustandsdiagramm und zeigt alle möglichen Wege, die ein e-Identity Service-Prozess nehmen kann.

21.3. Die einzelnen Schritte

Die folgende Beschreibung ersetzt nicht sondern ergänzt die Sicht des Händlers: Die bereits im Kapitel „7.3. Die einzelnen Schritte“ ausgeführten Schritte haben auch aus Bankensicht Gültigkeit.

21.3.1. Schritt 4: Bankenauswahl

Bei Abbruch in der Bankenauswahl werden die e-Identity-Daten gar nicht erst an die Kundenbank übermittelt.

Der Status gegenüber dem Händler wird direkt vom SO gesetzt.

21.3.2. Schritt A: e-Identity Service Initiierung

Die e-Identity Service Initiierung des Händlers wird am SO geprüft. Bei Anfrage von Verifikationsergebnissen wandelt der SO diese zunächst in Datenabfragen an die Kundenbank um. An die Kundenbank werden somit immer nur Datenabfragen gesendet. Der SO ersetzt zusätzlich die UserId durch seine eigene (siehe auch „L.2.1 eIdentity:IdentityServiceInitiationRequest“) und authentifiziert sich mittels digitaler Signatur. Wahlweise kann die Bank allerdings auch veranlassen, dass die UserId vom SO nicht geändert wird und die Original HändlerId an die Bank weitergeleitet wird. Weiters wird vom SO, falls vom Händler nicht angegeben, immer der MerchantName aus der Händlerdatenbank befüllt.

21.3.3. Schritt B: Rückmeldung auf e-Identity Service Initiierung

Die Kundenbank liefert bei erfolgter Übernahme der Daten die URL zum Login des Online-Bankings.

21.3.4. Schritt 5: Redirect des Kunden auf das Online-Banking

Siehe „7.3.5. Schritt 5: Redirect des Kunden auf das Online-Banking“.

21.3.5. Anzeige Identitätsdaten

Im Onlinebanking der Kundenbank werden alle angeforderten Daten aus dem Kundenstamm aufgelistet bzw. wie beim Feld IBAN eine Auswahl für den Kunden angeboten. Änderungen an den Daten können vom Kunden keine vorgenommen werden. In speziellen Fällen (zB IBAN) kann der Kunde aber eine Auswahl treffen.

Wird ein Datenfeld von der Bank nicht unterstützt wird die entsprechende Datenstruktur in der Confirmation Nachricht nicht gesendet. Der ResponseCode muss in diesem Fall mit 105 (Unvollständige Identifikation) belegt werden.

21.3.6. Autorisierung durch Kunden

Der Kunde autorisiert die Übermittlung der e-Identity Daten mittels der von der Kundenbank angebotenen und üblichen Autorisierungsmethoden. Hinweis: bei einmalig verwendbaren Autorisierungstokens ist dieses sofort als verbraucht markiert, auch wenn die Abwicklung in weiterer Folge nicht abgeschlossen werden kann.

21.3.7. Schritt C: e-Identity Service Confirmation

Die Kundenbank sendet die generierte Confirmation an die Confirmation-URL des SO, welche in der Initiierung übermittelt wurde.

Die Kundenbank übermittelt in jedem möglichen Fall auch ohne erfolgreichen Abschluss des Prozesses eine Statusnachricht an den SO. Dies betrifft vor allem folgende Fälle:

- Abbruch durch Kunde vor dem Login
- Abbruch durch Kunde in der Online-Banking-Session
- Timeout der Online-Banking-Session

21.3.8. Schritt D: Rückmeldung zur e-Identity Service Confirmation

Der SO speichert die von der Kundenbank angelieferte Confirmation und leitet diese an den Händler weiter.

Der Händler wiederum bestätigt den Erhalt mit einer entsprechenden Confirmation Response an den SO, welcher die Nachricht an die Kundenbank retour liefert.

Zusätzlich ermöglicht der SO, durch Datenhaltung der übermittelten Confirmation, dem Händler die Abfrage der Daten zu einem späteren Zeitpunkt direkt vom SO. (siehe auch „7.3.10 Schritt 10: e-Identity Service Statusabfrage (optional)“).

21.3.9. Schritt 8: Redirect des Kunden zum Händler

Der Redirect des Kunden zum Händler erfolgt möglichst im selben Fenster unter der Verwendung der vom Händler in der Initiierung angegebenen Return-URL

21.4. Abfrage Detaildaten für eid4mobile

21.4.1. IdentityDetailsRequest

Mittels IdentityDetailsRequest kann die Bank die Daten der ursprünglich initiierten Identifizierung beim SO abfragen. Diese Nachricht muss von der Bank signiert werden und enthält die TransactionId, welche bei der Bank entweder über die Initiierungsnachricht oder als Parameter der QRCodeUrl bekannt ist.

21.4.2. IdentityDetailsResponse

Der SO übermittelt in der Antwort auf den IdentityDetailsResponse die Daten der ursprünglichen Identifizierung. Die Nachricht wird vom SO ebenfalls signiert. Sollte die Transaktion nicht gefunden oder schon abgeschlossen sein, wird anstelle der Initiierungsdaten ein ResponseStatus mit entsprechendem Fehlercode gesendet.

A. ANHANG – XML-NACHRICHTEN

A.1. Allgemein

22. ES GELTEN DIE XML-SPEZIFISCHEN VORGABEN UNTER „9. EID TOKEN

Mit der Version 2.1 wurde für den Händler eine Möglichkeit eröffnet anstelle der Identitätsdaten vom Kunden, ein Identitätstoken vom SchemeOperator anzufordern. Für dieses Token kann der Händler auch ein Gültigkeitsdatum angeben. Maximal kann aber ein Token nur für 3 Jahre ab Initiierungszeitpunkt angefordert werden. Unter Angabe des Tokens kann der Händler über den autorisierten IdentityDataTokenRequest bei Bedarf die Echtdata des Kunden anfordern. Die Echtdata können auch mehrmals vom Händler angefordert werden.

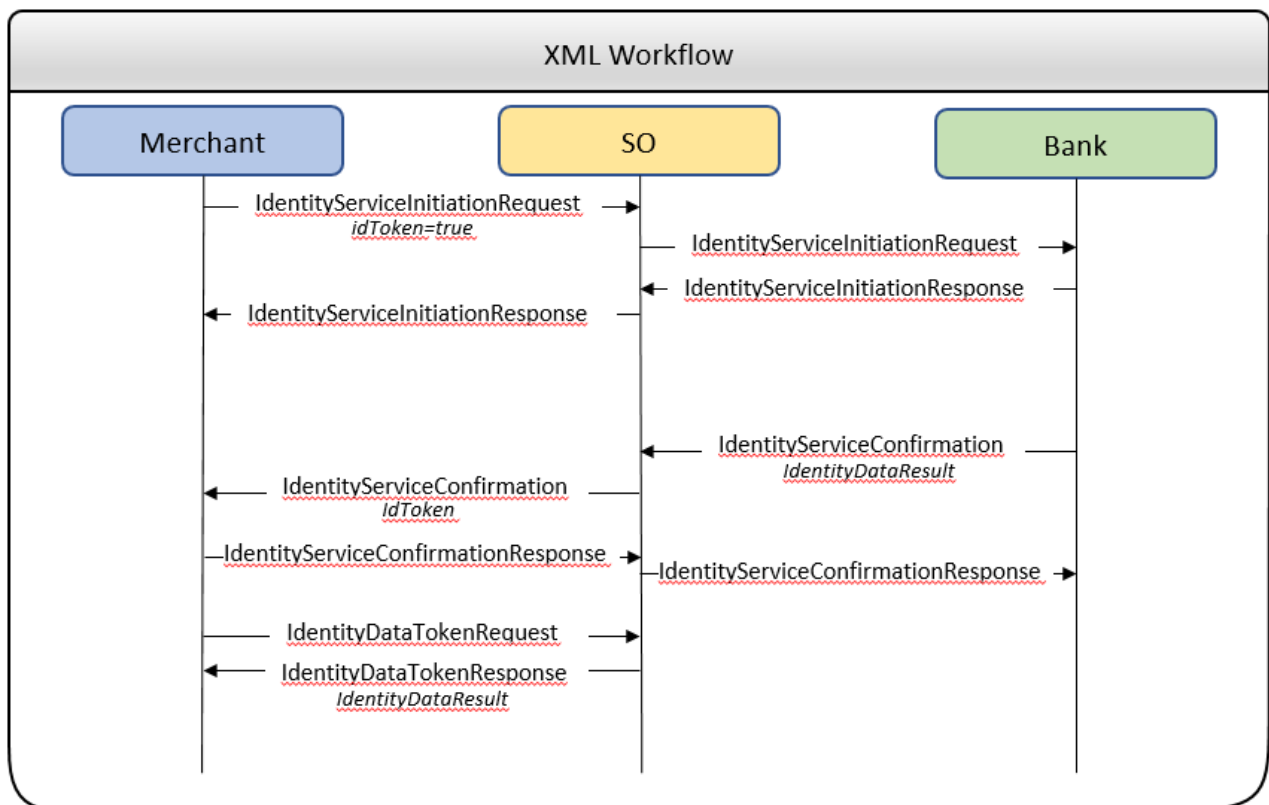


Abbildung 9: Workflow eID Token

Technische Anforderungen“

Die Art der Verwendung (mandatory, conditional, optional) ist bei jedem Element angegeben, wobei Elemente innerhalb eines optionalen Elternelements mandatory gekennzeichnet sind, wenn bei Vorhandensein des Elternelements das Element selbst dann verpflichtend ist.

Damit ist eine spezielle Verwendung von Datenelementen (z.B. verpflichtende Angabe eines im Iso XML Schema optionalen Datenelemente) jeweils entsprechend dokumentiert.

A.1.1. Schema-Aufbau

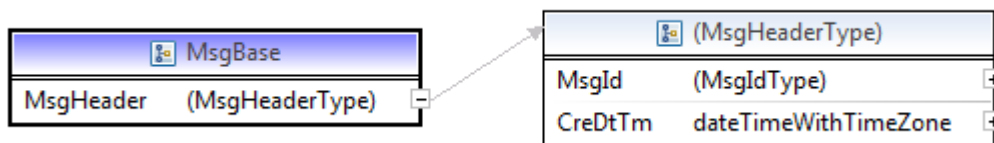
Das e-Identity Service Schema setzt sich inhaltlich aus mehreren XML-Datencontainern zusammen, die jeweils mit einem eigenen Namespace gekennzeichnet sind und im Dokument wie folgt mit Prefixes referenziert werden.

Schema	beschreibt	Prefix
eIdentityService.xxx..xsd	die verwendeten XML-Nachrichten, importiert die weiteren Schemadefinitionen	eIdentity
W3C-XMLDSig.xsd	signaturbezogene Daten	dsig

Tabelle 2: Schema und Prefixes

A.1.2. eIdentity:MsgHeader

Verwendung: mandatory



Alle Nachrichten haben als gemeinsame Basis einen Message-Header.

A.1.2.1. eIdentity:MsgId

Verwendung: mandatory

Eine je Prozess und Händler eindeutige Id, die in jeder Nachricht mitgesendet wird.

Sie wird in „A.2.1 eIdentity:IdentityServiceInitiationRequest“ vom Händler vergeben und ist dann für jede Nachricht des Prozesses dieselbe.

A.1.2.2. eIdentity:CreDtTime

Verwendung: mandatory

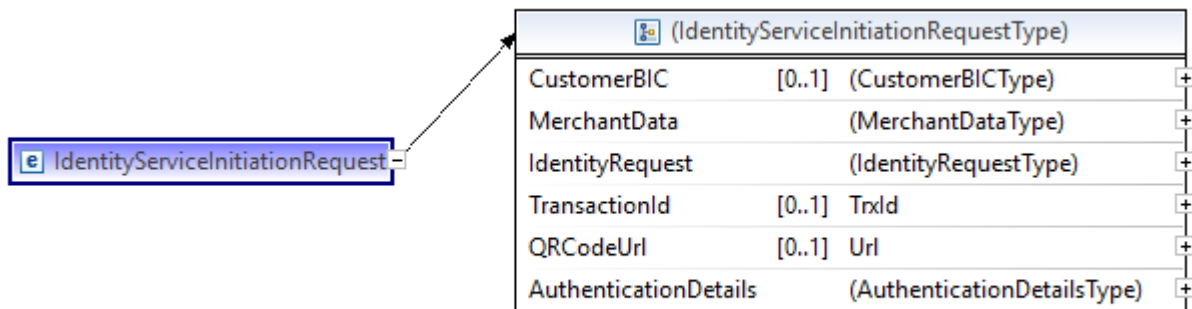
Der Erstellungszeitpunkt des Prozesses.

Er wird in „A.2.1 eIdentity:IdentityServiceInitiationRequest“ vom Händler gesetzt und ist dann für jede Nachricht des Prozesses derselbe.

Der SO prüft bei der Initiierung („A.2.1 eIdentity:IdentityServiceInitiationRequest“), dass die angegebene Zeit - unter Berücksichtigung der geforderten Zeitsynchronität - mit dem Anlieferungszeitpunkt des XML beim SO übereinstimmt.

A.2. Die Nachrichten im Einzelnen

A.2.1. eIdentity:IdentityServiceInitiationRequest



A.2.1.1. eIdentity:CustomerBIC

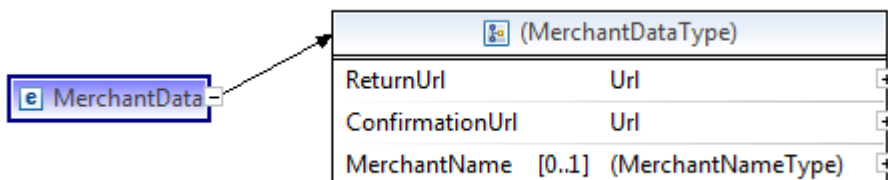
Verwendung: optional

KäuferBIC, wenn der Händler eine eigene Bankauswahl anbietet und der Kunde dann direkt auf die Banking Login Seite geroutet wird. Es wird auf eine syntaktisch korrekte BIC geprüft ([A-Z]{6}[A-Z2-9][A-NP-Z0-9]([A-Z0-9]{3}){0,1})

A.2.1.2. eIdentity:MerchantData

Verwendung: mandatory

Daten, die der Händler vergibt bzw. welche vom SO ergänzt oder geändert werden.



A.2.1.2.1. eIdentity:ReturnUrl

Verwendung: mandatory

Jene URL, auf die der Workflow beim Händler nach Beendigung des Prozesses fortgesetzt werden sollte – unabhängig vom Ergebnis im Online-Banking.

A.2.1.2.2. eIdentity:ConfirmationUrl

Verwendung: mandatory

Jene URL, auf welche die Confirmation-Nachricht gesendet wird.

A.2.1.2.3. eIdentity:MerchantName

Verwendung: optional

Jene Händlerbezeichnung, welche zwecks Weitergabe an die Käuferbank vom SO anhand der UserID gesetzt wird.

A.2.1.3. eIdentity:IdentityRequest

Verwendung: *mandatory*

Anforderung der gewünschten Daten. Optional kann für jedes Datenfeld eine Verifikation mittels dem optionalen Query Parameter angefordert werden. Mit dem Attribut idToken kann anstelle der Echtdaten ein Token angefordert werden. Optional kann der Händler im Attribut validTo ein Gültigkeitsdatum für den Token festlegen. Maximal werden jedoch nur 3 Jahre in die Zukunft akzeptiert.



A.2.1.3.1. eIdentity:IdentityDataRequest

Verwendung: *mandatory*

Parameter: *typ (mandatory)*

Für jedes Datenfeld, welches verifiziert oder angefordert wird, muss ein IdentityDataRequest Element angegeben werden. Die Art des Datenfeldes wird im Parameter ‚typ‘ angegeben. Folgende Datentypen werden derzeit unterstützt:

- FIRST_NAME – Vorname
- LAST_NAME – Nachname
- TITLE – Akademischer Grad
- DATE_OF_BIRTH – Geburtsdatum, Format yyyy-MM-dd
- AGE – Alter in Jahren
- STREET – Wohnadresse Straße
- TOWN – Wohnadresse Ort
- ZIPCODE – Wohnadresse Postleitzahl
- COUNTRY – Wohnadresse Nation
- IBAN – Verfügungsberechtigte Kontoverbindung

A.2.1.3.2. eIdentity:Query

Verwendung: *optional*

Mittels Query initiiert der Händler eine Verifikation.

Parameter: *op (mandatory) Operator*

Im Parameter op (Operator) können folgende Verifikationen mit dem zu liefernden ‚Data‘ Feld vorgenommen werden.

- eq – ‚ist gleich‘ Inhalt vom Feld ‚Data‘ wird auf Gleichheit innerhalb der Toleranz (Groß- Kleinschreibung, Accents, ß etc.) überprüft.
- neq – ‚ist ungleich‘ Inhalt vom Feld ‚Data‘ wird auf Ungleichheit geprüft (strikt Zeichenvergleich)
- lt – ‚kleiner‘ nur bei numerischen Feldern erlaubt (derzeit nur AGE)

gt – ‚größer‘ nur bei numerischen Feldern erlaubt (derzeit nur AGE)

Parameter: *sendData (optional) default="false"* – Anlieferung Originaldaten

Der Parameter *sendData* (erlaubte Werte true|false) gibt an ob die Originaldaten an den Händler übermittelt werden sollen.

A.2.1.3.3. eIdentity:Data

Verwendung: *conditional*

Das zu verifizierende Datum.

A.2.1.4. eIdentity:TransactionId

Verwendung: *conditional*

Die *TransactionId* wird vom SO für die Nachricht an die Bank befüllt. Vom Händler darf dieses Feld nicht verwendet werden bzw. wird vom SO ignoriert. Die *TransactionId* gibt die Referenz auf die gesendeten Daten an, damit diese von der Bank mit einem späteren ‚*IdentityDetailsRequest*‘ abgeholt werden kann.

A.2.1.5. eIdentity:QRCodeUrl

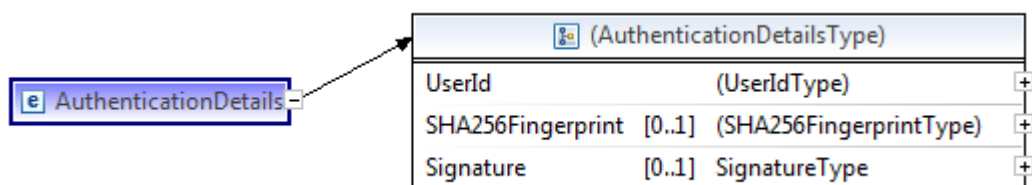
Verwendung: *conditional*

Die *QRCodeUrl* wird analog zur *TransactionId* vom SO für die Nachricht an die Bank befüllt. Die Bank hat die Möglichkeit dem Kunden parallel zum Login diese Url als QrCode anzuzeigen, Um die Transaktion über eine App zu initiieren.

A.2.1.6. eIdentity:AuthenticationDetails

Verwendung: *mandatory*

Es werden 2 Arten der Authentifizierung unterstützt: Fingerprint und digitale Signatur.



A.2.1.6.1. eIdentity:UserId

Verwendung: *mandatory*

Die User-ID ist Teil der Zugangsdaten für das Routing-Service beim SO, die der Händler nach Abschluss der e-Identity Service Händlervereinbarung zugestellt bekommt.

A.2.1.6.2. eIdentity:SHA256Fingerprint

Verwendung: *conditional*

Das Element enthält für die Authentifizierung mittels Fingerprint die Hex-Darstellung des aus relevanten Daten des XML generierten SHA256-Hashes.

Dazu wird der (textliche) Inhalt folgender Datenelemente zu einer Zeichenkette in genau der angegebenen Reihenfolge aneinandergesetzt:

- eIdentity:MsgId
- eIdentity:CreDtTm
- eIdentity:CustomerBIC
- eIdentity:ReturnUrl
- eIdentity:ConfirmationUrl
- eIdentity:idToken
- eIdentity:validTo

Pro angefordertem Datenfeld werden folgende Daten verwendet:

- eIdentity:IdentityDataRequest:typ
- eIdentity:Data
- eIdentity:UserId

Sollte dabei ein Feld nicht belegt sein, wird dieses auch nicht zur Erstellung der Zeichenkette herangezogen.

Dieser Zeichenkette wird die PIN aus den dem Händler übermittelten Zugangsdaten vorgelegt.

Über die UTF-8-Byte-Array-Repräsentation der Zeichenkette wird der Hash gerechnet.

Die Übermittlung eines falschen Fingerprints drei Mal hintereinander führt zur Sperre des Händlers im System.

A.2.1.6.2.1. Beispiel

Als Grundlage für die Berechnung dient das XML-Beispiel aus Kapitel L.2.1.1.

Somit ergibt sich mit dem PIN „fluxkompensator!85“ als Input für die Hashberechnung die Zeichenkette

```
fluxkompensator!85ARZTAT22XXX_120674XXXXXXX_1234567892018-06-28T12:00:00ZARZTAT22XXXhttps://shop.example.net/eIdentity-landinghttps://routing.example.net/eIdentity-confirmationtrue2022-10-01FIRST_NAMELAST_NAMEAGE17ATARZTAT22XXX_120674
```

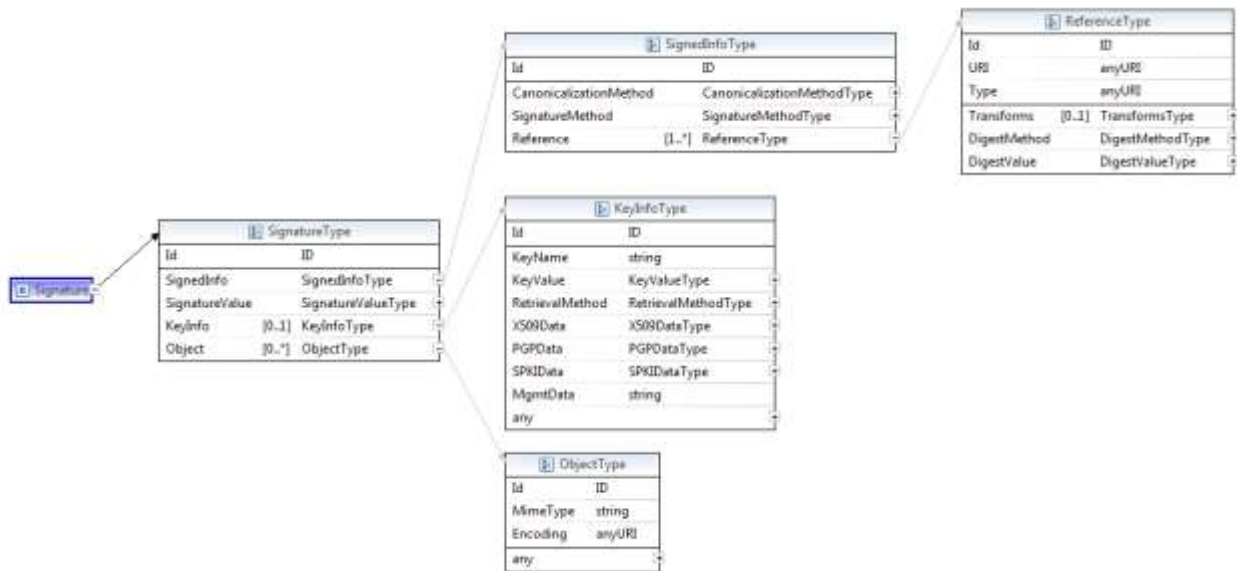
und daraus resultierend der Hashwert

```
3EE73A785D642FB0628096DE86A0643C9DBD3AEBA2D247C5E1916AC4232652DC
```

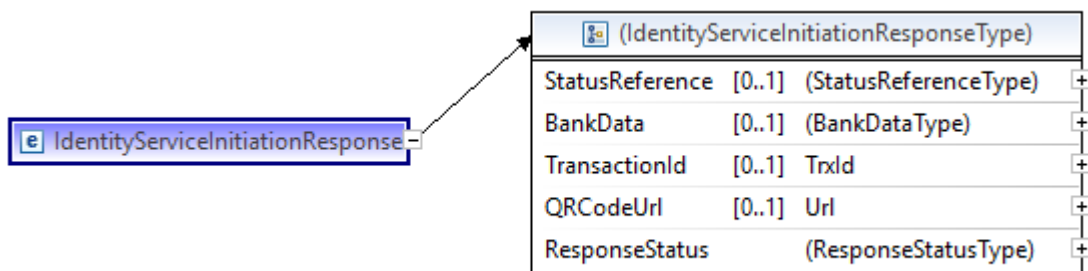
A.2.1.6.3. dsig:Signature

Verwendung: conditional

Als Alternative zu „A.2.1.6.2 eIdentity:SHA256Fingerprint“ kann auch eine digitale Signatur nach XMLDsig entsprechend (siehe „3.5 Referenzen auf weitere Dokumente“) verwendet werden.



A.2.2. eIdentity:IdentityServiceInitiationResponse



A.2.2.1. eIdentity:StatusReference

Verwendung: *optional*

Jene vom SO vergebene Referenz, auf deren Basis in weiterer Folge der Status des Prozesses („A.2.5 eIdentity:IdentityStatusRequest“) durch den Händler abgefragt werden kann.

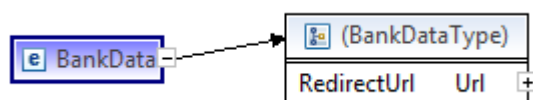
A.2.2.2. eIdentity:BankData

Verwendung: *conditional*

Daten, welche für den weiteren Ablauf im Online-Banking zur Verfügung gestellt werden.

Dieses Element muss bei einem ResponseCode 0 verpflichtend gesetzt werden.

War die Initiierung „A.2.1 eIdentity:IdentityServiceInitiationRequest“ fehlerhaft, wodurch der Prozess bei der Bank nicht fortgesetzt werden kann, wird das Element in XML nicht geliefert.



A.2.2.2.1. eIdentity:RedirectUrl

Verwendung: *mandatory*

Jene URL, welche für die Weiterleitung des Kunden auf die Bankauswahlseite herangezogen wird.

A.2.2.3. eIdentity:TransactionId

Verwendung: conditional

Die TransactionId wird vom SO in der Nachricht an den Händler befüllt. Diese Id wird für die Referenzierung der Detaildaten im Request verwendet und dient dem Händler nur als Zusatzinformation zur QrCodeUrl

A.2.2.4. eIdentity:QRCodeUrl

Verwendung: conditional

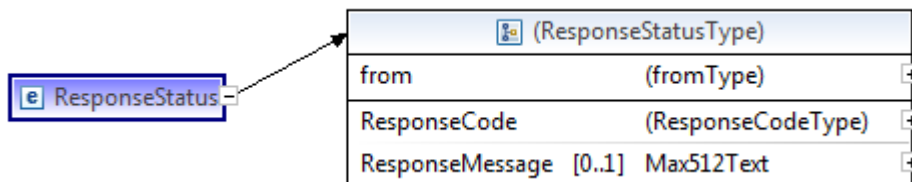
Die QRCodeUrl kann vom Händler verwendet werden, um dem Kunden die Url mittels QRCodes anzuzeigen. Diese Variante wird für die Initiierung über eine Banking App verwendet.

A.2.2.5. eIdentity:ResponseStatus

Verwendung: mandatory

Status und/oder Fehlerursache zum Prozess.

Der Empfänger einer Nachricht quittiert immer den Erhalt bzw. die Verarbeitung einer eingehenden Nachricht.



A.2.2.5.1. eIdentity:ResponseStatus@from

Verwendung: optional

Das Attribut kennzeichnet den Ursprung der Statusnachricht.

Ist die „A.2.1 eIdentity:IdentityServiceInitiationRequest“ schon fehlerhaft, sodass keine Daten an die Kundenbank übermittelt werden konnten, endet der Prozess bereits am und durch den SO.

A.2.2.5.2. eIdentity:ResponseCode

Verwendung: mandatory

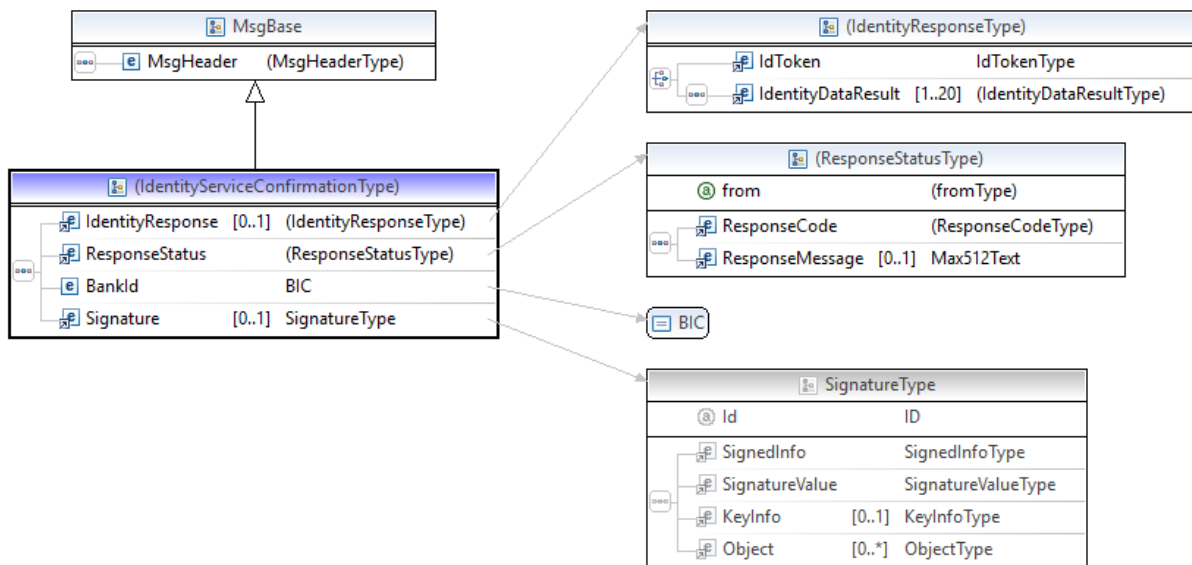
Ein Prozess kann verschiedene Zustände annehmen, welche unter „B Anhang – ResponseCodes“ beschrieben sind.

A.2.2.5.3. eIdentity:ResponseMessage

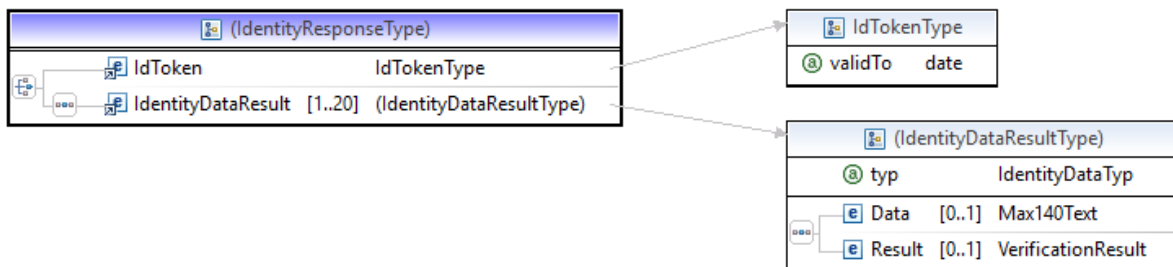
Verwendung: optional

Unstrukturierter Text, der „A.2.2.5.2 eIdentity:ResponseCode“ näher beschreibt. Das Feld wird dabei zur Übermittlung von Fehlertexten verwendet.

A.2.3. eIdentity:IdentityServiceConfirmation



A.2.3.1. eIdentity:IdentityResponse



Verwendung: conditional

Wurde in der IdentityServiceInitiationRequest ein Token angefordert, wird vom SchemeOperator ein IdToken geliefert. Andernfalls werden die geforderten Daten im IdentityDataResult zurückgeliefert.

A.2.3.1.1. eIdentity:IdToken

Verwendung: conditional

Base64 codierter Token. Im Attribut validTo wird das Gültigkeitsdatum des Tokens mitgeliefert.

A.2.3.1.2. eIdentity:IdentityDataResult

Verwendung: conditional

Pro angefordertem Datenfeld vom Händler wird ein Element vom Typ IdentityDataResult geliefert. In dieser Objektstruktur werden entweder die geforderten Daten, oder wenn in der Anfrage mittels Query eine Verifikation gefordert wurde, das Verifikationsergebnis. Wenn der Händler bei der Anfrage im Objekt Query das Attribut ‚sendData‘ mit „true“ belegt hat, wird zusätzlich zum Verifikationsergebnis auch die Originaldaten der Kundenbank im Feld Result gesendet.

A.2.3.2. eIdentity:ResponseStatus

Verwendung: mandatory

Siehe „A.2.2.5 eIdentity:ResponseStatus“.

A.2.3.2.1. eIdentity:ResponseStatus@from

Verwendung: mandatory

Siehe „A.2.2.5.1 eIdentity:ResponseStatus@from“.

A.2.3.2.2. eIdentity:ResponseCode

Verwendung: mandatory

Siehe „A.2.2.5.2 eIdentity:ResponseCode“.

A.2.3.2.3. eIdentity:ResponseMessage

Verwendung: optional

Siehe „A.2.2.5.3 eIdentity:ResponseMessage“.

A.2.3.3. eIdentity:BankId

Verwendung: mandatory

Die BIC jener Bank, welche die Confirmation bestätigt.

Diese Information wird zur Verrechnung anfallender SO-Gebühren verwendet.

A.2.3.4. dsig:Signature

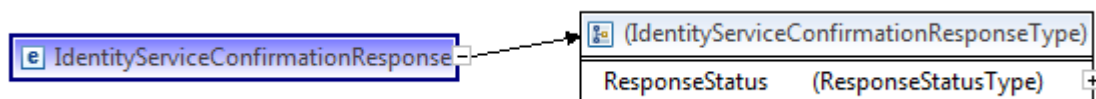
Verwendung: mandatory

Siehe „A.2.1.6.3 dsig:Signature“.

Hinweis: sowohl Kundenbank (an SO) als auch SO (an Händler) verwenden ihre jeweilige digitale Signatur und nicht einen SHA256-Fingerprint („A.2.1.6.2 eIdentity:SHA256Fingerprint“) zur Authentifizierung.

A.2.4. eIdentity:IdentityServiceConfirmationResponse

Der Händler quittiert den erfolgreichen Erhalt einer Confirmation mit ResponseCode 0. Für Abweichungen siehe „B Anhang – ResponseCodes“.



A.2.4.1. eIdentity:ResponseStatus

Verwendung: mandatory

Siehe „A.2.2.5 eIdentity:ResponseStatus“.

A.2.4.1.1. eIdentity:ResponseStatus@from

Verwendung: mandatory

Siehe „A.2.2.5.1 eIdentity:ResponseStatus@from“.

A.2.4.1.2. eIdentity:ResponseCode

Verwendung: *mandatory*

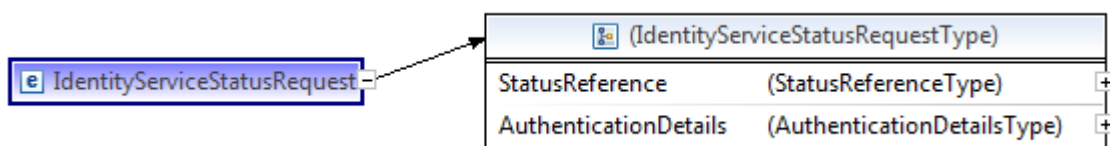
Siehe „A.2.2.5.2 eIdentity:ResponseCode“.

A.2.4.1.3. eIdentity:ResponseMessage

Verwendung: *optional*

Siehe „A.2.2.5.3 eIdentity:ResponseMessage“.

A.2.5. eIdentity:IdentityStatusRequest



A.2.5.1. eIdentity:StatusReference

Verwendung: *mandatory*

Siehe „A.2.2.1 eIdentity:StatusReference“.

A.2.5.2. eIdentity:AuthenticationDetails

Verwendung: *mandatory*

Siehe „A.2.1.6 eIdentity:AuthenticationDetails“.

A.2.5.2.1. eIdentity:UserId

Verwendung: *mandatory*

Siehe „A.2.1.6.1 eIdentity:UserId“.

A.2.5.2.2. eIdentity:SHA256Fingerprint

Verwendung: *conditional*

Siehe „A.2.1.6.2 eIdentity:SHA256Fingerprint“.

Zur Berechnung des Fingerprint wird der (textliche) Inhalt folgender Datenelemente zu einer Zeichenkette in genau der angegebenen Reihenfolge aneinandergesetzt:

- eIdentity:MsgId
- eIdentity:CreDtTm
- eIdentity:StatusReference
- eIdentity:UserId

Dieser Zeichenkette wird die PIN aus den dem Händler übermittelten Zugangsdaten vorangestellt.

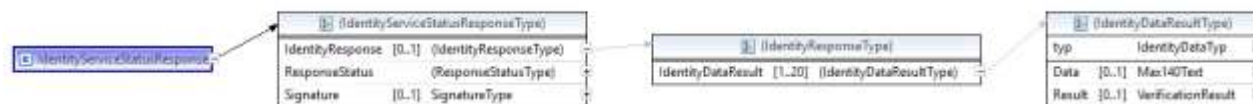
Über die UTF-8-Byte-Array-Repräsentation der Zeichenkette wird der Hash gerechnet.

A.2.5.2.3. dsig:Signature

Verwendung: *conditional*

Siehe „A.2.1.6.3 dsig:Signature“.

A.2.6. eIdentity:IdentityStatusResponse



A.2.6.1. eIdentity:IdentityResponse

Verwendung: *conditional*

Siehe „A.2.3.1 eIdentity:IdentityResponse“.

A.2.6.2. eIdentity:ResponseStatus

Verwendung: *mandatory*

Siehe „A.2.2.5 eIdentity:ResponseStatus“.

A.2.6.2.1. eIdentity:ResponseStatus@from

Verwendung: *mandatory*

Siehe „A.2.2.5.1 eIdentity:ResponseStatus@from“.

Sofern eine Identity-Confirmation-Nachricht der Bank vorliegt, steht im Attribut „BANK“, in allen anderen Fällen (z.B. ungültige Status-Referenz, Abbruch bei Initiierung, etc.) „SO“.

A.2.6.2.2. eIdentity:ResponseCode

Verwendung: *mandatory*

Siehe „A.2.2.5.2 eIdentity:ResponseCode“.

A.2.6.2.3. eIdentity:ResponseMessage

Verwendung: *optional*

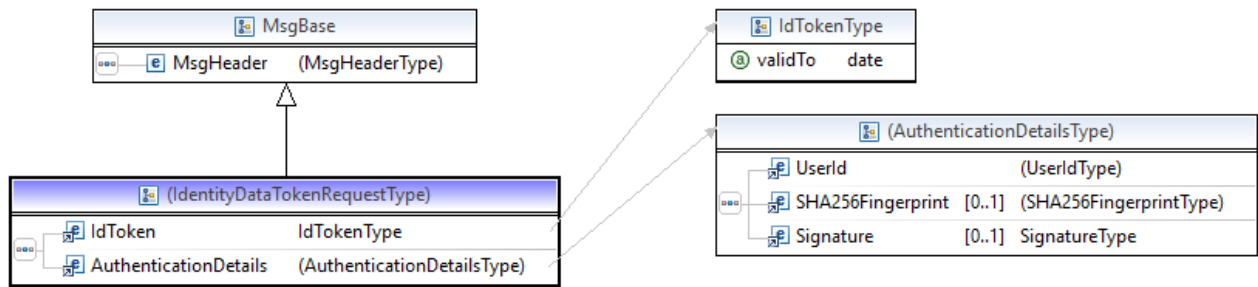
Siehe „A.2.2.5.3 eIdentity:ResponseMessage“.

A.2.6.3. dsig:Signature

Verwendung: *mandatory*

Siehe „A.2.1.6.3 dsig:Signature“.

A.2.7. eIdentity:IdentityDataTokenRequest



A.2.7.1. eIdentity:IdToken

Verwendung: mandatory

Bei der Anforderung der Identitätsdaten muss dieselbe Struktur wie in der Confirmation Nachricht mitgegeben werden.

Verwendung: mandatory

A.2.7.2. eIdentity:AuthenticationDetails

Siehe „A.2.1.6 eIdentity:AuthenticationDetails“.

A.2.7.2.1. eIdentity:UserId

Verwendung: mandatory

Siehe „A.2.1.6.1 eIdentity:UserId“.

A.2.7.2.2. eIdentity:SHA256Fingerprint

Verwendung: conditional

Siehe „A.2.1.6.2 eIdentity:SHA256Fingerprint“.

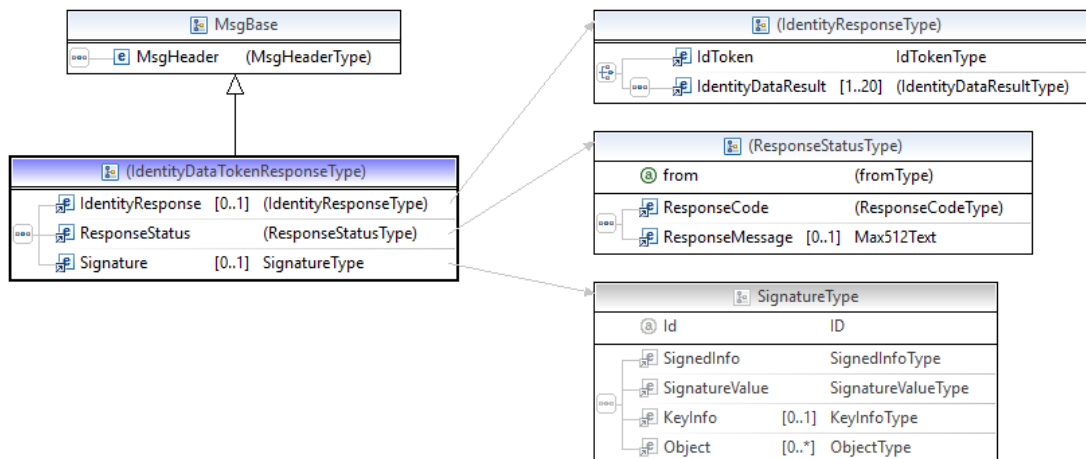
Zur Berechnung des Fingerprint wird der (textliche) Inhalt folgender Datenelemente zu einer Zeichenkette in genau der angegebenen Reihenfolge aneinandergesetzt:

- eIdentity:MsgId
- eIdentity:CreDtTm
- eIdentity:validTo
- eIdentity:IdToken
- eIdentity:UserId

Dieser Zeichenkette wird die PIN aus den dem Händler übermittelten Zugangsdaten vorangestellt.

Über die UTF-8-Byte-Array-Repräsentation der Zeichenkette wird der Hash gerechnet.

A.2.8. eIdentity:IdentityDataTokenResponse



A.2.8.1. eIdentity:IdentityResponse

Verwendung: conditional

Hier wird dieselbe Datenstruktur wie in der Confirmation Nachricht geliefert (A.2.3.1A.2.3.1.2). Allerdings wird immer das IdentityDataResult zurückgeliefert.

A.2.8.2. eIdentity:ResponseStatus

Verwendung: mandatory

Siehe „A.2.2.5 eIdentity:ResponseStatus“.

A.2.8.2.1. eIdentity:ResponseStatus@from

Verwendung: mandatory

Siehe „A.2.2.5.1 eIdentity:ResponseStatus@from“.

Sofern eine Identity-Confirmation-Nachricht der Bank vorliegt, steht im Attribut „BANK“, in allen anderen Fällen (z.B. ungültige Status-Referenz, Abbruch bei Initiierung, etc.) „SO“.

A.2.8.2.2. eIdentity:ResponseCode

Verwendung: mandatory

Siehe „A.2.2.5.2 eIdentity:ResponseCode“.

A.2.8.2.3. eIdentity:ResponseMessage

Verwendung: optional

Siehe „A.2.2.5.3 eIdentity:ResponseMessage“.

A.2.8.3. dsig:Signature

Verwendung: mandatory

Siehe „A.2.1.6.3 dsig:Signature“.

B. ANHANG – RESPONSECODES

B.1. 000 – Kein Fehler

Kein Fehler aufgetreten, Nachricht erfolgreich verarbeitet, Workflow wird fortgesetzt.

B.2. 001 – XML ungültig

Das XML ist ungültig bzw. die XML-Schemavalidierung ist fehlgeschlagen.

B.3. 002 – Fehler bei Feldprüfung

Trotz syntaktischer Korrektheit der Nachricht weisen darüber hinausgehende (logische) Prüfungen auf inhaltliche Fehler hin.

B.4. 004 – Autorisierung fehlerhaft

Die Prüfung der Autorisierung (Fingerprint, Signatur) gegen die hinterlegten Daten ist fehlgeschlagen.

B.5. 008 – Unspezifischer Fehler

Ein Fehler außerhalb des Einflussbereichs des SO ist aufgetreten.

B.6. 009 – Interner Fehler

Ein (technischer) Fehler ist aufgetreten.

B.7. 014 – Connection Timeout

Die Kundenbank ist nicht erreichbar.

B.8. 016 – Duplicate Confirmation

Zum in der Confirmation referenzierten eIdentity-Prozess wurde bereits früher eine Confirmation zugestellt und erfolgreich am SO verarbeitet.

B.9. 030 – Abbruch durch Kunden

Der Kunde hat den Prozess abgebrochen (z.B. auf Bankauswahlseite oder im Online-Banking).

B.10. 100 – Erfolgreiche Identifikation

Die Kundenbank hat alle vom Händler geforderten Daten zur Verfügung gestellt.

B.11. 105 – Unvollständige Identifikation

Die Kundenbank konnte nicht alle vom Händler übermittelten Kundendaten anliefern.

Mindestens ein einzelnes Verifikations-Ergebnisse (aus „A.2.3.1 eIdentity:IdentityResponse“) liefert den Wert „UNKNOWN“.

B.12. 110 – Fehlgeschlagene Identifikation

Mindestens ein Datenfeld, welches vom Händler geliefert wurde konnte geliefert bzw. durch den SO gültig verifiziert werden.

B.13. 120 – Ungültige Statusreferenz

Entweder die übergebene Statusreferenz konnte keiner beim SO gespeicherten Transaktion zugeordnet werden oder die angefragte Transaktion liegt bereits zu lange in der Vergangenheit (für die entsprechenden zeitlichen Fristen siehe technisches Beiblatt).

B.14. 121 – Transaktion nicht abgeschlossen

Die eIdentity-Transaktion wurde fehlerfrei initiiert, allerdings liegt noch keine Datenlieferung der Bank bzw. Verifikationsergebnis vom SO vor.

B.15. 122 – Ungültiger Token

Fehlercode kann in der IdentityDataTokenResponse auftreten, wenn der gelieferte Token nicht gefunden wurde.

B.16. 123 – Token abgelaufen

Fehlercode kann in der IdentityDataTokenResponse auftreten, wenn das Gültigkeitsdatum des Tokens bereits abgelaufen ist.

L. ANHANG – XML-NACHRICHTEN ZWISCHEN BANK UND E-SERVICE SCHEME OPERATOR

L.1. Die Nachrichten im Einzelnen

L.1.1. eIdentity:IdentityServiceInitiationRequest

Siehe „A.2.1 eIdentity:IdentityServiceInitiationRequest“.

Gegenüber der Kundenbank ersetzt der SO „A.2.1.2.2 eIdentity:ConfirmationUrl“ mit einer SO-eigenen URL. Unter dieser URL erwartet der SO auch die Confirmation der Kundenbank.

Der SO autorisiert sich immer mit digitaler Signatur und der UserId „eIdentitySchemeOperator“.

Idealerweise prüft die Bank die Autorisierung mit einem optionalen Fallback-Zertifikat, sodass es bei einem Zertifikatsupdate beim SO zu keiner Unterbrechung des Services zur Bank hin kommt.

L.1.2. eIdentity:IdentityServiceInitiationResponse

Siehe „A.2.2 eIdentity:IdentityServiceInitiationResponse“.

L.1.2.1. eIdentity:StatusReference

Siehe „A.2.2.1 eIdentity:StatusReference“.

Die Status-Referenz wird niemals von der Kundenbank sondern vom SO gesetzt.

L.1.2.2. eIdentity:RedirectUrl

Siehe „A.2.2.2.1 eIdentity:RedirectUrl“.

Die URL für die Weiterleitung des Kunden auf das Login des Online-Bankings.

L.1.3. eIdentity:IdentityServiceConfirmation

Siehe „A.2.3 eIdentity:IdentityServiceConfirmation“.

L.1.3.1. eIdentity:ResponseStatus@from

Das Attribut ist von der Kundenbank fix mit „BANK“ belegt.

L.1.3.2. eIdentity:ResponseMessage

Optionale Ausführungen zum Status werden in englischer Sprache ausgeführt.

L.2. Beispiele

Hinweis: die in den Beispielen angeführten Daten sind reine Fantasiewerte, welche zwar Schema-konform angeführt sind, dennoch wurde beispielsweise die digitale Signatur nicht bei jeder Nachricht neu berechnet.

L.2.1. eIdentity:IdentityServiceInitiationRequest

L.2.1.1. ohne Signatur

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityServiceInitiationRequest
  xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020
eIdentityService_v2.1.xsd" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:CustomerBIC>ARZTAT22XXX</eIdentity:CustomerBIC>
  <eIdentity:MerchantData>
    <eIdentity:ReturnUrl>https://shop.example.net/eIdentity-
landing</eIdentity:ReturnUrl>
    <eIdentity:ConfirmationUrl>https://routing.example.net/eIdentity-
confirmation</eIdentity:ConfirmationUrl>
  </eIdentity:MerchantData>
  <eIdentity:IdentityRequest idToken="true" validTo="2022-10-01">
    <eIdentity:IdentityDataRequest typ="FIRST_NAME"/>
    <eIdentity:IdentityDataRequest typ="LAST_NAME"/>
    <eIdentity:IdentityDataRequest typ="AGE">
      <eIdentity:Query op="gt" sendData="false">
        <eIdentity:Data>17</eIdentity:Data>
      </eIdentity:Query>
    </eIdentity:IdentityDataRequest>
  </eIdentity:IdentityRequest>
  <eIdentity:AuthenticationDetails>
    <eIdentity:UserId>ARZTAT22XXX_120674</eIdentity:UserId>
  <SHA256Fingerprint>
3EE73A785D642FB0628096DE86A0643C9DBD3AEB2D247C5E1916AC4232652DC</SHA256Fingerprint>
  </eIdentity:AuthenticationDetails>
</eIdentity:IdentityServiceInitiationRequest>
```

L.2.1.2. mit Signatur

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityServiceInitiationRequest
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020
eIdentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:CustomerBIC>ARZTAT22XXX</eIdentity:CustomerBIC>
  <eIdentity:MerchantData>
    <eIdentity:ReturnUrl>https://shop.example.net/eIdentity-
landing</eIdentity:ReturnUrl>
    <eIdentity:ConfirmationUrl>https://routing.example.net/eIdentity-
confirmation</eIdentity:ConfirmationUrl>
  </eIdentity:MerchantData>
  <eIdentity:IdentityRequest>
    <eIdentity:IdentityDataRequest typ="FIRST_NAME"/>
    <eIdentity:IdentityDataRequest typ="LAST_NAME"/>
    <eIdentity:IdentityDataRequest typ="AGE">
      <eIdentity:Query op="gt" sendData="false">
        <eIdentity:Data>17</eIdentity:Data>
      </eIdentity:Query>
    </eIdentity:IdentityDataRequest>
  </eIdentity:IdentityRequest>
  <eIdentity:AuthenticationDetails>
```

```

    <eIdentity:UserId>ARZTAT22XXX_120674</eIdentity:UserId>
    <dsig:Signature Id="hotVault"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><dsig:SignedInfo><dsig:CanonicalizationM
ethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><dsig:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /><dsig:Reference Id="reference-
data-0" URI=""><dsig:Transforms><dsig:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" /></dsig:Transforms><dsig:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" /><dsig:DigestValue>QQdGuyY0BUYxbkJvJw
ldly+YiUM=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>fp8
DuK4t5ijVLRXiME7axUutwSdWiBHgzx41r6QRvxFpCQ3ZqqdwoPHwMQuBKuIO
NQUDFUM67NxB3CotDovgaVoXuaU+ZXJ+ge5ImZ+ZgAXbypav55Vc5tbOMFDbbrpD
1JaUvUXN+WrVpEVNOJpyvE7Xi6dW0+UuR/3H2JXbdCnNRvkXL70wBlrRw+H18xmq
Havq95KVVBUnBvFLU54qt10OhGni5gDA9qb5RCUGF9cuE5Ti17UDciQdMgTF5iOZ
guV08rqM/LMD2aqeoRLW6RM1NPzqMB9hJ60OXIcy1IeoZRGor90/Apk4CT8IjplH
hiqyIImBwPSN+912Cnr8Zw==</dsig:SignatureValue><dsig:KeyInfo><dsig:X509Data><dsig:X509Cer
tificate>MIIGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIGTMOswCQYDVQQGEWJB
VDFIMEYGA1UECgw/QS1UcnVzdCBHZXMuIGYyIFNpY2hlcmhlaXRzc3lzdGVtZSBp
bSB1bGVrdHlUaERhdGVudmVya2VociBhbWJIMRwwGgYDVQQLDBNlLXNpZ24tY29y
cG9yYXR1LTA1MRwwGgYDVQQDDBNhLXNpZ24tY29ycG9yYXR1LTA1MB4XDTE1MTEEx
MDA3MDUyOVVzZDQyMTE1MTE1MTE1MTE1MTE1MTE1MTE1MTE1MTE1MTE1MTE1MTE1MTE1
DDFBUlogQWxsZ2VtZWluZXZmUmVjaGVuemVudHJlbnSBH2XNlbnGxZ2hhZnZnQgbs5i
LkqumR0wGwYDVQLDBRjbnR1cm5ldCBDbndlbmR1bmdlbjEVMBMGA1UEAwwMQVJa
LVNpZ25hdHVMRUwEYDQVQFEwW2ODAZMTk5NzI3NTcwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCnm2DNSUqChfwDjBrLRHeI IpvsaG/yQTUXVwjs5mlt
9xuTevWIjul/qtFa+NdPGLmfl6SvT1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/1N
Q/5dzhLzuF+PQmd9dcKN5q/AR9Jxuk9rqrBZ6uKAKDCgxm07L++OnLLqjrEOsm5
2ohDo6O+RNqFi68ASQ/vdKqizLPc/xpqPDZKGR6P1c8yJnGjvSHaBDMnkojaBb3K
47mkQW5SGoDXGL1tFGtbCTLqJqlbxxXwjQD7p13GyJagusoP13JE882iKNgHPUYB
JFIwZxa/duKOYgbsS2CGxbwI5g5Ub0pS3tHZp3sSVpjAgMBAAGjggFbMIIBVzB4
BggrBgEFBQcBAQRsMgowPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZXJ2cy9hLXNpZ24tY29ycG9yYXR1LTA1LmNydDAnBggrBgEFBQcwAYYbaHR0
cDovL29jc3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDFuM6AxcC+GLWh0dHA6
Ly9jc29uYS10cnVzdC5hdC9jcmVvYS1zaWduLWNvcnBvcnF0ZS0wNTATBgNVHSME
DDAKGhKe9V2TRchVTAJBGNVHRMEAjaAMBEGA1UdDgQKBAhe5k8IGBy85zaOBGNV
HQ8BAf8EBAMCBaAwWYDVR0gBFewTzBNBgcqKAARAQcBMEIwQAYIKwYBBQUHAQEW
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUT
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRuTSMIT225v8mMvnXDxtkzpz9aRpZwZ
/Ym5foInVdktuAt6jz076c10iQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Av1f1e08Bt3DE7EOgujjdEmDIg0Vx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpugmtYIRKgbje1tZSP3S2P2jMwE3MxL6jC6M6+FcnBTtdlt
iXJ6fxxCtUxFQvzv67obuJfDLJE9MfdNwYqR90y+9C8n1frkx7kknTPK6lpu4j5b
O117F2QFVd5IdtLIGYtx+oOfzJoo6V4MerzyP9KfEbmSHNG4NEZE1rP8P04Dk0i
hVUn140q9w/H4uIppvJp3hpW/GSouYlIGGnZ8qnUWNat7+qP1cKYOHmcXS1FmMxx
FPtKycT8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGVklBObY57YXhfjnHNS
WURfGIA5okvG7WkfvNpc6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbYsoqWhAkCT
3wE7gGsWtumQI8zwlywviedrfTHTBxQCWJA3+Wt3AyhJVPbM+OR5dYQEHRM61sLH
Wks3t9iKvBN7+TNNeVWwylP1fQT2dpyGQ9eMAGuSvZIrroFVMEAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signature>
</eIdentity:AuthenticationDetails></eIdentity:IdentityServiceInitiationRequest>

```

L.2.1.3. Mit Signatur: SO -> Bank

```

<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><eIdentity:IdentityServiceInitiationRequest
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:CustomerBIC>ARZTAT22XXX</eIdentity:CustomerBIC>

```

```
<eIdentity:MerchantData>
  <eIdentity:ReturnUrl>https://shop.example.net/eIdentity-
landing</eIdentity:ReturnUrl>
  <eIdentity:ConfirmationUrl>https://routing.example.net/eIdentity-
confirmation</eIdentity:ConfirmationUrl>
</eIdentity:MerchantData>
<eIdentity:IdentityRequest>
  <eIdentity:IdentityDataRequest typ="FIRST_NAME"/>
  <eIdentity:IdentityDataRequest typ="LAST_NAME"/>
  <eIdentity:IdentityDataRequest typ="DATE_OF_BIRTH"/>
</eIdentity:IdentityRequest>
<eIdentity:TransactionId>123HOXA123</eIdentity:TransactionId>
<eIdenti-
ty:QRCodeUrl>eidentity://eps.or.at/?transactionid=123HOXA123</eIdentity:QRCodeUrl>
  <eIdentity:AuthenticationDetails>
    <eIdentity:UserId>ARZTAT22XXX_120674</eIdentity:UserId>
    <dsig:Signature Id="hotVault"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><dsig:SignedInfo><dsig:CanonicalizationM
ethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><dsig:SignatureMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><dsig:Reference Id="reference-data-
0" URI=""><dsig:Transforms><dsig:Transform Algo-
rithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></dsig:Transforms><dsig:DigestMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#sha1"/><dsig:DigestValue>uW0/wro2rTDj1/b14FnIV9
ZKFAg=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>Vi6eUEG
ZXHVuZyI8voWtmnpGfMkj7Yl+LWf6Lg8Re5bej/ovMfdr1PBUqGxux8ZX
yH6Fq8dXD3qot87Pv5PdNHL3pCXI/XVji+Xs+m3SP5sxMq0Zmj/AN1b5ezRroFaG
lCjDJ9s4s2ipA6II/UmQv/ususSoDlsqHJNI4RwmmEFvGPNFrXwAj/PTV7Qpjs6o
5ESj5PspATLT00oKv/jtgGIW+CnHBPLYL46DwruLta0VG9H9DLH/ExQn7jyoF3sC
9jj/YWth/2phXaWkArO++fcAT7B6nGN3e9vfeCT90aBaBE3ijTnMveq45jbW3jDD
z2q/yrjTyFeJUSPTAr9dUQ==</dsig:SignatureValue><dsig:KeyInfo><dsig:X509Data><dsig:X509Cer
tificate>MIIGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIGTMQswCQYDVQQGEwJB
VDFIMEYGA1UECgw/QS1UcnVzdCBHZXMuIGYyIFNpY2hlcmhlaXRzc3lzdGVtZSBp
bSB1bGVrdHIuIERhdGVudmVya2VociBhbWJIMRwwGgYDVQQLDBNlLXNpZ24tY29y
cG9yYXR1LTA1MRwwGgYDVQQDDDBNlLXNpZ24tY29ycG9yYXR1LTA1MB4XDTE1MTEEx
MDA3MDUyOVowXDTIwMTEExMDA2MDUyOVowZDYyYzA5BjBqNVBAYTAKFUMTowOAYDVQQK
DDFBUlogQWxsZ2VtZWluZXZMcGUmVjAGVuemVudHJ1bSBHZXNlbnGxzY2hhZnQgbS5i
LkguMR0wGwYDVQQLDBRjbnRlcm5ldCBDbndlbmR1bmdlbjEVMBMGA1UEAwM0VjJa
LVNpZ25hdHVyMRUwEwYDVQQFEw2ODAzMTk5NzI3NTcwggEiMA0GCSqGSIb3DQEBA
AQUAA4IBDwAwggEKAoIBAQCnm2DNSUqChfwDjBrLRHeiIpvsaG/yQTUXVwjs5m1t
9xuTezWIjul/qtFa+NdPGLmfL6SvT1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/1N
Q/5dzhLzuF+PQmd9dcKN5q/AR9Jxuk9rpxBZ6uKAKDCgxm07L++OnLLqjrEOsm5
2ohDo60+RNqFi68ASQ/vdKqizLPc/xpqPDZKGR6PIc8yJnGjvSHaBdmnkojaBb3K
47mkQW5SgoDXGL1tFGtbCTLqJqlbxxXwjqD7p13GyJagusoP13JE882iKNgHPUYB
JFIwZxa/dduKOYgbs2CGxbwI5g5Ub0pS3tHzp3sSvpjAgMBAAGjggFbMIIBVzB4
BggrBgEFBQcBAQRsMGowPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZXJ0cy9hLXNpZ24tY29ycG9yYXR1LTA1LmNydDAnBggrBgEFBQcwAYYbaHR0
cDovL29jc3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDUwM6AxcC+GLWh0dHA6
Ly9jc3AuYS10cnVzdC5hdC9jcmwvYS1zaWduLWNvcnBvcnF0ZS0wNTATBgNVHSME
DDAKGhAke9V2TRchVTAJBqNVHRMEAjaAMBEGA1UdDgQKBAhE5k8IGBy85zaOBGnV
HQ8BAf8EBAMCBAaWAWAYDVR0gBFewTzBNBgcqKAARAQCBEIwQAYIKwYBBQUHAGew
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUt
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRuTSMIT225v8mMvnXDxtkz9aRpZwZ
/Ym5foInVdktuAt6jz076c1OiQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Avlf1eo8Bt3DE7EOgujjdEmDIg0Vx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpugmtYIRKqBjelTzSP3S2P2jMwE3MxL6jC6M6+FcnBTTdlT
iXJ6fxxCtUxFQvzv67obuJfLJE9MfdNwYqR90y+9C8n1frkx7kknTPK61pu4j5b
0117F2QqFD5IdtLIGYtX+oOfZJoo6V4MeRzyP9KFeBmsHNG4NEZE1rP8P04Dk0i
hVUn14Oq9w/H4uIpvYJ3hpW/GSOUY1IGGnZ8qnUWnat7+qPlcKYOHmcXS1FmMxx
FPtKycztZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGvklBOBY57YXhfjnHNS
WURfGIA5okvG7WkfvNpc6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbYsoqWhAkCT
3wE7gGsWtumQI8zwlYwviedrftHTBxQCWJA3+Wt3AyhJVPbM+OR5dYQEHRM61sLH
Wks3t9iKvBN7+TNNwVWylP1fQT2dpyGQ9eMAGuSvZIrrroFVmeAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signature>
  </eIdentity:AuthenticationDetails>
</eIdentity:IdentityServiceInitiationRequest>
```


L.2.1.4. IdentityServiceInitiationResponse: ohne Fehler

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityServiceInitiationResponse
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020
eIdentityService_v2.1.xsd" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:BankData>
    <eIdentity\RedirectUrl>https://banking.example.net/eIdentity-banking/login-
prepare?id=898F6512061974DE657A7</eIdentity\RedirectUrl>
  </eIdentity:BankData>
  <eIdentity:TransactionId>123HOXA123</eIdentity:TransactionId>
  <eIdentity:QRCodeUrl>eidentity://eps.or.at/?
transactionid=123HOXA123</eIdentity:QRCodeUrl>
  <eIdentity:ResponseStatus from="SO">
    <eIdentity:ResponseCode>000</eIdentity:ResponseCode>
  </eIdentity:ResponseStatus>
</eIdentity:IdentityServiceInitiationResponse>
```

L.2.1.5. mit Fehler

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityServiceInitiationResponse
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:BankData>
    <eIdentity\RedirectUrl>https://banking.example.net/eIdentity-banking/login-
prepare?id=898F6512061974DE657A7</eIdentity\RedirectUrl>
  </eIdentity:BankData>
  <eIdentity:ResponseStatus from="BANK">
    <eIdentity:ResponseCode>008</eIdentity:ResponseCode>
    <eIdentity:ResponseMessage>Fehler bei der Initiierung - Backend nicht verfü-
bar</eIdentity:ResponseMessage>
  </eIdentity:ResponseStatus>
</eIdentity:IdentityServiceInitiationResponse>
```

L.2.2. eIdentity:IdentityServiceConfirmation

L.2.2.1. ohne Fehler: Bank -> SO

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><eIdentity:IdentityServiceConfirmation
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020
eIdentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:IdentityResponse>
    <eIdentity:IdentityDataResult typ="FIRST_NAME">
      <eIdentity:Data>Max</eIdentity:Data>
    </eIdentity:IdentityDataResult>
  </eIdentity:IdentityResponse>
</eIdentity:IdentityServiceConfirmation>
```



```

    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="LAST_NAME">
      <eIdentity:Data>Mustermann</eIdentity:Data>
    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="DATE_OF_BIRTH">
      <eIdentity:Data>1980-06-01</eIdentity:Data>
    </eIdentity:IdentityDataResult>
  </eIdentity:IdentityResponse>
  <eIdentity:ResponseStatus from="BANK">
    <eIdentity:ResponseCode>100</eIdentity:ResponseCode>
  </eIdentity:ResponseStatus>
  <eIdentity:BankId>VBOEATWWAPO</eIdentity:BankId><dsig:Signature Id="hotVault"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><dsig:SignedInfo><dsig:CanonicalizationM
ethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><dsig:SignatureMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><dsig:Reference Id="reference-data-
0" URI=""><dsig:Transforms><dsig:Transform Algo-
rithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></dsig:Transforms><dsig:DigestMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#sha1"/><dsig:DigestValue>QTa4Urldfi+uVaORy4zh/t
aLbMo=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>Gb9bXU7
ps8U/Lx+PUAHmVs8WyhZjhlP2vob0WdpZQ3IYYOT8GqWr/XRzPt4wBugT
WZxWp5cZsXhQEZ+c6IRNli+YncRdulEj1Czjib+bLiLZHqoXhHqQ6krMWvT+dduk
bdAGXTFUapj/LkXWniEJPCyRr/7sZbXv2iRaUbc5sBsmNdEwsJG4q+KUS9UsfO4B
YAOG/Wisdpfd1CDexccvG/GTAgnAF+unypidKapSKlgHTVBVJ7fd4hUigaVUoQ1
o9GsPZoevFzZ6N62Yu+nd6yW8ysYrh/Fx77E7mvPo8UMXr00DtNg3FndmlpylYzl
TBk+NZ6/nugvt3+jvsKDXg==</dsig:SignatureValue><dsig:KeyInfo><dsig:X509Data><dsig:X509Cer-
tificate>MIIGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIGTMQswcQYDVQQGEwJb
VDFIMEYGA1UECgwvQS1UcnVzdCBhZXMuIGYyIFNpY2hlcmhlaXRzc3lzdGVtZSBp
bSB1bGVrdHluIERhdGVudmVya2VociBhbWJIMRwwGgYDVQQGLDBNbnhLXNpZ24tY29y
cG9yYXR1LTA1MRwwGgYDVQQDDDBNbnhLXNpZ24tY29ycG9yYXR1LTA1MB4XDTE1MTEe
MDA3MDUyOVoXDTE1MTEeMDA3MDUyOVowZyYzCzAJBgNVBAYTAkFUMTowAAYDVQQQK
DDEFBuIogWxsZ2VtZWluZXMQmUvVjaGVuemVudHJlbSBHZNlbnGxzY2hhZnQgbsS5i
LkguMR0wGwYDVQQGLDBRbnR1cm5ldCBBbnRlbnR1bmdlbjEVMGMGA1UEAwwMQVJa
LVNpZ25hdHViMRUwEyYDVQQFEww2ODAzMTk5NzI3NTcwggEiMA0GCSqGSIb3DQEBA
QUAA4IBBwAwggEKAoIBAQCnm2DNsUqChfWdjBrLRHeiIpvsaG/yQTUXVwjs5mlt
9xuTezWIju/qFta+NdPGLmfL6SvT1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/1N
Q/5dzhLzuF+PQmd9dcKN5q/AR9JxuK9rxqBz6uKAKDCGxm07L++OnLlqjrEOsm5
2ohDo60+RNQFi68ASQ/vdKqizLpC/xpqPDZKgr6P1c8yJnGjvSHaBdmnkojaBb3K
47mkQW5SgoDXGL1tFGtbCTLqJqlbxxXwjQD7p13GyJagusoP13JE882iKNGHPUYB
JFIWzxa/duKOYgbsS2CGxbwI5g5Ub0pS3tHZp3sVpJAgMBAAGjggFbMIIBVzB4
BggrBgEFBQcBAQRSMGowPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZXJ0cy9hLXNpZ24tY29ycG9yYXR1LTA1LmNyYDAnBggrBgEFBQcWAWYbaHR0
cDovL29jc3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDUwM6Axc+GLWh0dHA6
Ly9jcmwuYS10cnVzdC5hdC9jcmwuYS1zaWduLWNvcnBvcmF0ZS0wNTAtBGNVHSM
E DDAKGAhKe9V2TRchVTAJBGNVHRMEAjaAMBEGA1UdDgQKBAhE5k8IGBy85zaOBGNV
HQ8BAf8EBAMCBaAWAwYDVVR0gBFEwTzBNBgqcKAARAQcBMEIwQAYIKwYBBQUHAgEW
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUt
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRUtSmIT225v8mMvnxDXtkz9aRpZwZ
/Ym5foInVdktuAt6jz076c10iQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Avl1fo8Bt3DE7EOgUjjdEmDIg0Vx60vf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpugmtYIRKgBje1tZSP3S2P2jMwE3MxL6jC6M6+FcnBTTdlt
iXJ6fxxCtUxFQwvz67obuJFDLJE9MfdNwYqR90y+9C8n1frkx7kknTpK6lpu4j5b
O117F2QFVFD5IdtLIGYtx+oOfZJoo6V4MerZyP9KfEBSmHNG4NEZE1rP8P04Dk0i
hVUn140q9w/H4uIpvYJP3hpW/GSouY1IGGnZ8qnUWnat7+qP1cKYOHmcXS1FmMxx
FPtKyctZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGvklBObY57YXhfjnHNS
WURfGIA5okvG7WkfvNpc6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbysoqWhAkCT
3wE7gGSwtumQI8zwlywviedrfTHTBxQCWJA3+Wt3AyhJVPBm+OR5dYQEHRM61sLH
Wks3t9ikvBN7+TNNEwVwylP1fQ2TdpYGQ9eMAGUsvZiRrwoFVmeAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signature>
</eIdentity:IdentityServiceConfirmation>

```

L.2.2.2. mit Fehler: SO -> Händler

```

<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><eIdentity:IdentityServiceConfirmation
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

```

```

xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020
eIdentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:IdentityResponse>
    <eIdentity:IdentityDataResult typ="FIRST_NAME">
      <eIdentity:Data>Max</eIdentity:Data>
    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="LAST_NAME">
      <eIdentity:Data>Mustermann</eIdentity:Data>
    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="AGE">
      <eIdentity:Result>NOK</eIdentity:Result>
    </eIdentity:IdentityDataResult>
  </eIdentity:IdentityResponse>
  <eIdentity:ResponseStatus from="SO">
    <eIdentity:ResponseCode>100</eIdentity:ResponseCode>
  </eIdentity:ResponseStatus>
  <eIdentity:BankId>VBOEATWWAPO</eIdentity:BankId><dsig:Signature Id="hotVault"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><dsig:SignedInfo><dsig:CanonicalizationM
ethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><dsig:SignatureMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"><dsig:Reference Id="reference-data-
0" URI=""><dsig:Transforms><dsig:Transform Algo-
rithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></dsig:Transforms><dsig:DigestMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#sha1"><dsig:DigestValue>k8k3+Twt9LTrWojCwaGsSF
hrGgM=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>g0qs7WZ
+oJNP/Mzt8qY23db5R95LmXQhsvCU2+DWZ2IIi9nszPiJF56ybXDOtH1
zPH3qNICSDYd84U0bCvoWeMmHK95ugQyQoVM3AaZoicqDRr339j7CNxDi7yhK86y9
4JtXYS14YVso0mpC3UXQ5ShN7mMGe0JNq1vYwaNVb5gLGyr3DtvZlhAkwdwxCE5w
soHRrtPq4ezqang34fqqzj4ecwOoFzYijoh13+q8F1FKcNqj6qFpSpkkl9EmcTn
Eqaeks3pejeTE9a/Vl0fenHq1DcEVuDVdtGoSip3j9TYdwESBcDokx4r2vi3a2DS
t9feh96SWyNZs/xn6J+YA==</dsig:SignatureValue><dsig:KeyInfo><dsig:X509Data><dsig:X509Cer
tificate>MIIGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIGTMOswCQYDVQQGEwJB
VDFIMEYGA1UECgw/QS1UcnVzdCBHZXMuIGYyIFNpY2hlcmhlaXRzc3lzdGVtZSBp
bSB1bGVrdHlUeRhdGVudmVya2VociBHbWJIMRwwGgYDVOQLDBNhLXNpZ24tY29y
cG9yYXR1LTA1MRwwGgYDVOQDDBNhLXNpZ24tY29yYXR1LTA1MB4XDTE1MTEEx
MDA3MDUyOVoXDTIwMTEwMDA2MDUyOVoYDzYxZCZAJBgNVBAYTAKFUMTowOAYDVQQK
DDFBU0gWxsZ2VtZWluZXMgUmVjaGVuemVudHJ1bSBHZXN1bGxzY2hhZnZnZnZnZn
LkGuMR0wGwYDVOQLDBRjbnR1cm5ldCBDbndlbmR1bmd1bjEVMBMGA1UEAwMQVJa
LVNpZ25hdHVyMRUwEwYDVOQFEww2ODAzMTk5NzI3NTcwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCNm2DNsUqChfwdjBrLRHeiIpvsaG/yQTUXVwjs5m1t
9xuTezWIjul/qtFa+NdPGLmfL6SvT1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/1N
Q/5dzhLzuF+PQmd9dcKN5q/AR9JxuK9rqxBZ6uKAKDCgxmX07L++OnLLqjrEOsm5
2ohDo60+RNqFi68ASQ/vdKgiZLpc/xpQPDZKGR6PIc8yJnGjvSHaBdmkojaBb3K
47mkQW5SGoDXGL1tFGtbCTLqJqlbxxXwJQD7p13GyJagusoP13JE882iKNgHPUYB
JFIwZxa/duKOYgbsS2CGxbwI5g5Ub0pS3tHZp3sVpjAgMBAAGjggFbMIIBVzB4
BggrBgEFBQcBAQRSMGowPwYIKwYBBQUHMAKG2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZlZlcy9hLXNpZ24tY29yYXR1LTA1LmNydDAnBggrBgEFBQcwAYYYbaHR0
cDovL29jZ3AuYS10cnVzdC5hdC9yY3NwMD4GA1UdHwQ3MDUwM6AxcC+GLWh0dHA6
Ly9jcmwvYS10cnVzdC5hdC9jcmwvYS1zaWduLWNvcnBvcnF0ZS0wNTATBgNVHSME
DDAKGahKe9V2TRchVTAJBgNVHRMEAjAAMBEGA1UdDgQKBAhE5k8IGBy85zaOBGNV
HQ8BAf8EBAMCBAAwAYDVR0gBFewTzBNBgcqKAARAQcBMEIwQAYIKwYBBQUHAQEW
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUt
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRUtSmIT225v8mMvnXDxtkz9aRpZwZ
/Ym5foInVdktuAt6jz076c1OIQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Avl1e08Bt3DE7EOgujJdEmDIg0Vx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXsk8FqJS+6pLiKRpugmtYIRKgBje1tZSP3S2P2jMwE3MxL6jC6M6+FcNBTTdlt
iXJ6fxxCtUxFQvwz67obuJfDLJE9MfdNwYqR90y+9C8n1frkx7kknTPK61pu4j5b
O117F2QFVfD5IdtLIGYtx+oOfzJoo6V4MeRzyP9KfEBSmHNG4NEZE1rP8P04Dk0i
hVUnl40q9w/H4uIppvYJP3hpW/GSouYlIGGnZ8qnUWNat7+qP1cKYOHmcXS1FmMxx
FPtKyctZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGVk1BOBv57YXhfjnhNS
WURfGIA5okvG7WkfvNpc6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbYsoqWhAkCT
3wE7gGSwTumQI8zwlyWviedrfTHTBxQCWJA3+Wt3AyhJVPbM+OR5dYQEHRM61sLH
Wks3t9iKvBN7+TNnwVWylP1fQT2dpyGQ9eMAGuSvZ1rrwoFVMEAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signature>
</eIdentity:IdentityServiceConfirmation>

```



```

/Ym5foInVdktuAt6jz076c1OiQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Avl1f1eo8Bt3DE7EOgujjdEmDIg0Vx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpugmtYIRKgBjelTZSP3S2P2jMwE3MxL6jC6M6+fCnBTtdlt
iXJ6fxxCtUxFQwvz67obuJFdLJE9MfdNwYqR90y+9C8n1frkx7kntPK61pu4j5b
O117F2QFvFD5IdtLIGYtx+oOfzJoo6V4MeRzyP9KFeBmsHNG4NEZE1rP8P04Dk0i
hVUnl40q9w/H4uIpvYJP3hpW/GSouYlIGGnZ8qnUWNat7+qPlcKYOHmcXS1FmMxx
FPtKyctZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGVklBObY57YXhfjnHNS
WURfGIA5okvG7WkfVnPC6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbYsoqWhAkCT
3wE7gGSwTumQI8zwlYwviedrfTHTBxQCWJA3+Wt3AyhJVPbM+OR5dYQEHRM61sLH
Wks3t9iKvBN7+TNNeWVWy1P1fQT2dpyGQ9eMAGuSvZlrrwoFVmEAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate>
</dsig:X509Data>
</dsig:KeyInfo>
</dsig:Signature>
</eIdentity:IdentityServiceConfirmation>

```

L.2.3. eIdentity:IdentityServiceConfirmationResponse

L.2.3.1. ohne Fehler: Händler -> SO

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityServiceConfirmationResponse
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:ResponseStatus>
    <eIdentity:ResponseCode>000</eIdentity:ResponseCode>
  </eIdentity:ResponseStatus>
</eIdentity:IdentityServiceConfirmationResponse>

```

L.2.3.2. mit Fehler: SO -> Bank

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityServiceConfirmationResponse
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:ResponseStatus from="SO">
    <eIdentity:ResponseCode>001</eIdentity:ResponseCode>
    <eIdentity:ResponseMessage>eIdentity:MsgId end Tag miss-
ing</eIdentity:ResponseMessage>
  </eIdentity:ResponseStatus>
</eIdentity:IdentityServiceConfirmationResponse>

```

L.2.4. eIdentity:IdentityServiceStatusRequest

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityServiceStatusRequest
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:StatusReference>eisI1QW7IMV3</eIdentity:StatusReference>

```



```

    <eIdentity:AuthenticationDetails>
      <eIdentity:UserId>ARZTAT22XXX_120674</eIdentity:UserId>
      <eIdenti-
ty:SHA256Fingerprint>F17C342F6A4165A6B43548BDC7AC1346AC7677E0FAA9B19138A7220725279EAA</e
Identity:SHA256Fingerprint>
    </eIdentity:AuthenticationDetails>
  </eIdentity:IdentityServiceStatusRequest>

```

L.2.5. eIdentity:IdentityServiceStatusResponse

L.2.5.1. ohne Fehler

```

<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><eIdentity:IdentityServiceStatusResponse
xmlns:dsig="http://www.w3.org/2000/09/xmlldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020
eIdentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:IdentityResponse>
    <eIdentity:IdentityDataResult typ="FIRST_NAME">
      <eIdentity:Data>Max</eIdentity:Data>
    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="DATE_OF_BIRTH">
      <eIdentity:Data>1980-05-03</eIdentity:Data>
    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="AGE">
      <eIdentity:Result>OK</eIdentity:Result>
    </eIdentity:IdentityDataResult>
  </eIdentity:IdentityResponse>
  <eIdentity:ResponseStatus from="SO">
    <eIdentity:ResponseCode>100</eIdentity:ResponseCode>
  </eIdentity:ResponseStatus><dsig:Signature Id="hotVault"
xmlns:dsig="http://www.w3.org/2000/09/xmlldsig#"><dsig:SignedInfo><dsig:CanonicalizationM
ethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><dsig:SignatureMethod Algo-
rithm="http://www.w3.org/2000/09/xmlldsig#rsa-sha1"><dsig:Reference Id="reference-data-
0" URI=""><dsig:Transforms><dsig:Transform Algo-
rithm="http://www.w3.org/2000/09/xmlldsig#enveloped-
signature"/></dsig:Transforms><dsig:DigestMethod Algo-
rithm="http://www.w3.org/2000/09/xmlldsig#sha1"><dsig:DigestValue>mgCAUCC8K1ABk0FV3hjTmf
FbWL4=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>IpKBFLo
FaRMs4tL05Q/xpFjlbliOXFvk5jWNJX6MSgeZzYr2d0nYeO+47VEXBC8+
fVCppJyqEpUvWqEbNUpeftXdtgPYcXtyaSTFYqvbExoYjz4sgTbGBCzDgJLNPQq7
5qa+IOwSfus3Wbuny2y3iVCh1KFvVZ5RsKdjQevRQfaDrUF7lah/R6rDVe+3Dy6
ztyYc6SKYc/zINHeN5xSbvs0hScvV5LTl1/zLeiYaYX/EDHrPkbqmSASZJZ81K2
A8KhFHFpaMOxBqPyMBQgIGUrD9DTHHUTbzjEhMTK7XIVZ911i91C25RgU6DpWpcM
QCjoduhWIbY-
SpCbIGYgnNg==</dsig:SignatureValue><dsig:KeyInfo><dsig:X509Data><dsig:X509Certificate>MI
IGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIGTMQswCQYDVQQGEwJB
VDFIMEYGA1UECgw/QS1UcnVzdCBHZXMuIGYyIFNpY2hlcmhlaXRzc3lzdGVTZSBp
bSB1bGVrdHluIERhdGVudmVya2VociBHBWJIMRwwGgYDVQQLDBNlLXNpZ24tY29y
cG9yYXRlLTA1MRwwGgYDVQQDDBNhLXNpZ24tY29yY29yYXRlLTA1MB4XDTE1MTEEx
MDA3MDUyOVowXDTIwMTEeMDA2MDUyOVowZGYyYzA5BjBnVBAyTAKFUMTowOAYDVQQK
DDFBUlogQWxsZ2VtZWluZXMgUmVjaGVuemVudHJlbSBHZXNlbnGxzY2hhZnQgbS5i
LkguMR0wGwYDVQQLDBRlbnR1cm5ldCBDbndlbmR1bmdlbjEVMBMGA1UEAwMQVJa
LVNpZ25hdHVyMRUeYwYDVQQFEw2ODAZMTk5NzI3NTcwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCnm2DNSUqChfwDjBrLRHeiIpvsaG/yQTUXVwjs5mlt
9xuTezWIjul/qtFa+NdPGLmfL6SvT1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/1N
Q/5dzhLzuF+PQmd9dcKN5q/AR9Jxuk9rpxBZ6uKAKDCgxm07L++OnLLqjrEOsm5
2ohDo60+RNqFi68ASQ/vdKgizLpC/xpqPDZKgR6PIc8yJnGjvSHaBdmnkojaBb3K
47mkQW5SGoDXGL1tFGtbCTLqJqlbxxXwjqD7p13GyJagusoP13JE882iKNGHPUYB
JFIwZxa/dduKOYgbsS2CGxbwI5g5Uub0pS3tHZp3sSVpjAgMBAAGjggFbMIIBVzB4

```

```
BggrBgEFBQcBAQRsMGowPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZXJ0cy9hLXNpZ24tY29ycG9yYXR1LTA1LmNydDAnBggrBgEFBQcAwYYbaHR0
cDovL29jZ3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDUwM6AxcC+GLWh0dHA6
Ly9jcmwuYS10cnVzdC5hdC9jcmwvYS1zaWduLWNvcnBvcnF0ZS0wNTATBgNVHSME
DDAKgAhKe9V2TRchVTAJBGNVHRMEAjAAMBEGA1UdDgQKBAhE5k8IGBy85zAObGnV
HQ8BAf8EBAMCBaAwWAYDVr0gBFewTzBNBgcqKAARAQcBMEIwQAYIKwYBBQUHAgEW
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUt
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRuTSMIT225v8mMvnXDxtkzp9aRpZwZ
/Ym5foInVdktuAt6jz076c10iQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhuI4Avlf1eo8Bt3DE7EOgujjdEmDIg0Vx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpugmtYIRKGBjelTzSP3S2P2jMwE3MxL6jC6M6+FcNBTtdlt
iXJ6fxxCtUx9FQvz7obuJfdLJE9MfdNwYqR90y+9C8n1frkx7kknTP61pu4j5b
O117F2QFVFD5IdtLIGYtx+oOfZJoo6V4MeRzyp9KfE8msHNG4NEZELrP8P04Dk0i
hVUnl4Oq9w/H4uIppvYJP3hpW/GSouYlIGGnZ8qnUWNat7+qP1cKYOHmcXS1FmMxx
FPtKycztZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGvklBObY57YXhfjnHNS
WURfGIA5okvG7WkfVnPC6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbYsoqWhAkCT
3wE7gGsWtumQI8zwlYwviedrftHTBxQCWJA3+Wt3AyhJVPbm+OR5dYQEHM61sLH
Wks3t9iKvBN7+TNNwVWYlP1fQT2dpyGQ9eMAGuSvZIRRwFVMEAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signature>
</eIdentity:IdentityServiceStatusResponse>
```

L.2.5.2. mit Fehler

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><eIdentity:IdentityServiceStatusResponse
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020
eIdentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXXX_123456789</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-28T12:00:00Z</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:ResponseStatus from="SO">
    <eIdentity:ResponseCode>120</eIdentity:ResponseCode>
    <eIdentity:ResponseMessage>Ungültige Statusreferenz</eIdentity:ResponseMessage>
  </eIdentity:ResponseStatus><dsig:Signature Id="hotVault"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><dsig:SignedInfo><dsig:CanonicalizationM
ethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><dsig:SignatureMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><dsig:Reference Id="reference-data-
0" URI=""><dsig:Transforms><dsig:Transform Algo-
rithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></dsig:Transforms><dsig:DigestMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#sha1"/><dsig:DigestValue>cWF75tcNB6PMUEmSHYrXer
D0DRA=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>C/CIRXu
TIsG5/nSolzeLc+jIYk30/AddA3iiJE/0G9Nkvs9mZH/IA5qvphuOPj
vX8dnmocUB2DaHaCu1lZQocxh01LsYoXxGndKDJFwadN8B4z7QR6XB1L5J9t/Fn
4RhrqgGbmJaSyYabarzXgyZ6h8Sa3gfYtEzd94uJh3ox1n5XjFgs+V/RfTr8mJmU
qnOGOfb/Edlzi/C7wKwg681JpDIa2TaSGIa/sM+gfkGzRd2Lfl0jRaptXZwfAJa
WR3wtmRQXlWFM2I6R4bXP1fnsCBhocW9jz/eilYC97+mBGcvsp/IaqaN0t16keMI
Kv4gxIsQklgc7lBQV8i6ug==</dsig:SignatureValue><dsig:KeyInfo><dsig:X509Data><dsig:X509Cer
tificate>MIIGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIGTMQswCQYDVQOGEwJB
VDFIMEYGA1UECgw/QS1UcnVzdCBHZXMuIGYyIFNpY2hlcmlhlaXRzc3lzdGVtZSBp
bSB1bGVrdHlUeRhdGVudmVya2VociBHbWJIMRwwGgYDVQQLDBNhLXNpZ24tY29y
cG9yYXR1LTA1MRwwGgYDVQQDDDBNhLXNpZ24tY29ycG9yYXR1LTA1MB4XDTE1MTEEx
MDA3MDUyOVowXDTIwMTEwMTE5MDUyOVowZyZyXCAzA1BGNvbnBAYTAkFUMTowOAYDVQQK
DDFBUlogQWxsZ2VtZWluZXMgUmVjaGVuemVudHJ1bSBHZXN1bGxzY2hhZnZnQW9jZS5i
LkguMR0wGwYDVQQLDBRjbnR1cm5ldCBDbndlbmR1bmdlbjEVMBMGA1UEAwMQVJa
LVNpZ25hdHVyMRUwEwYDVQQFEwW2ODAZMTk5NzI3NTcwGgEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCnm2DNSUqChfwDjBrLRHeiIppsaG/yQTUXVwjs5mlt
9xuTezWIjul/qtFa+NdPGLmfL6SvT1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/1N
Q/5dzhLzuF+PQmd9dcKN5q/AR9Jxuk9rqrqBZ6uKAKDCgmx07L++OnLLqjrEOsm5
2ohDo60+RNqFi68ASQ/vdKgilZLpC/xpqPDZKGR6PIc8yJnGjvSHaBdmnkojaBb3K
47mkQW5SgoDXGL1tFGtbCTLqJqlbxxXwJQD7p13GyJagusoP13JE882iKNGHPUYB
JFIwZxa/dduKOYgbsS2CGxbwI5g5Ub0pS3tHZp3sSvpjAgMBAAGjggFbMIIBVzB4
BggrBgEFBQcBAQRsMGowPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYS10cnVzdC5h
```

```
dC9jZxJ0cy9hLXNpZ24tY29ycG9yYXR1LTA1LmNyDDAnBggrBgEfbQcwAyybaHR0
cDovL29jc3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDUwM6AxC+GLWh0dHA6
Ly9jcmlwYS10cnVzdC5hdC9jcmVvYS1zaWduLWNvcnBvcmlwZS0wNTAtBgNVHSME
DDAKGhAKe9V2TRchvTAJBgNVHRMEAjAAMBEGA1UdDgQKBAhE5k8IGBy85zAOBgNV
HQ8BAf8EBAMCBaAwAYDVR0gBFewTzBNBgcqKAARAQCBMEIwQAYIKwYBBQUHAQEW
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUt
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRUtSmIT225v8mMvnXDxtkzp9aRpZwZ
/Ym5foInVdktuAt6jz076c1OIQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Avlfl1e08Bt3DE7E0gujjdEmDIgOVx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpuGMTYIRKgbjeItzSP3S2P2jMwE3MxL6jC6M6+FcnBTtDlT
iXJ6fxXctUxFeQvzw67obuJfDlJE9MfdNwYqR90y+9C8n1frkx7kntpK61pu4j5b
O117F2QFVfD5IdtLVIGYtx+oOfZJoo6V4MeRzyp9KfEBmsHNG4NEZE1rP8P04Dk0i
hVUnl4Oq9w/H4uIIPvYJP3hpW/GSouY1IGGnz8qnUWNat7+qP1cKYOHmcXs1FmMxx
FPtKycZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGvklBoBy57YXhfjNHNs
WURfGIA5okvG7WkfVnPC6s81V3g/kt8mf2RnxWRHQ3kK+Msbc5VWkbYsoqWhAkCT
3wE7gGsWtumQI8zwlYwviedrftHTBxQCWJA3+Wt3AyhJVPbM+OR5dYQEHRM61sLH
Wks3t9iKvBN7+TNNwVWYlPlfQT2dpyGQ9eMAGuSvZIrrwoFVMEaQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signature>
</eIdentity:IdentityServiceStatusResponse>
```

L.2.6. eIdentity:IdentityDetailsRequest

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><eIdentity:IdentityDetailsRequest
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>1234567</eIdentity:MsgId>
    <eIdentity:CreDtTm>2018-06-06T23:30:13.919+02:00</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:TransactionId>123HOXA123</eIdentity:TransactionId>
  <eIdentity:BankId>BKAUATWW</eIdentity:BankId><dsig:Signature Id="hotVault"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><dsig:SignedInfo><dsig:CanonicalizationM
ethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></dsig:SignatureMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><dsig:Reference Id="reference-data-
0" URI=""><dsig:Transforms><dsig:Transform Algo-
rithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></dsig:Transforms><dsig:DigestMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#sha1"/><dsig:DigestValue>dSxz1KNmngv+OwljcaOW9N
vFuBI=</dsig:DigestValue></dsig:Reference></dsig:SignedInfo><dsig:SignatureValue>BYLqNJ6
yXPukG8QUsHpmJ+HFR0oFwo3rnFEsbFBS5lmfRuihvjtqdw9XG8ItIN
DNZmBrhgk6v7/JYulxpBcShbW0NVhwjfn3QrQj3cVEpaKajcDQhcEYB0S1X7pd9
vUgnOUow7bFdo0vOOMg6gISbe1uCnqtTnV+5JRpWyV8kk3SDPlrnGPUQvda+7yVX
r7gHzulh8s5Hp1Q5HWHtDnR/t7bggjpJ+pi2STHda/m/PV6jbcFcpCnkvHdgMPtM
WbSDPevVdbGPcJlncXV0gpbKTJcmxsXBJhQGR2CelTs1eNvBKFzb7tI8pc5Jyo
ZSW0V9yUck/NB5CXanc7ow==</dsig:SignatureValue><dsig:KeyInfo><dsig:X509Data><dsig:X509Cer-
tificate>MIGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIgMTQswCQYDVQQGEWJB
VDFIMEYGA1UECgw/QS1UcnVzdCBHZAuIGYUuIFNpY2hlcmhlaXRzc3lzdGvtZSBp
bsBlbGVrdHIuIERhdGVudmVya2VociBHhWJIMRwwGgYDVQQGLDBNhhLXNpZ24tY29y
cG9yYXR1LTA1MRwwGgYDVQQDDDBNhhLXNpZ24tY29yYyYXR1LTA1MB4XDTE1MTEe
MDA3MDUyOVoXDTIwMTEeMDA2MDUyOVowgZyXcZAJBgNVBAYTAKFUMTowOAYDVQQK
DDFBUlogQWxsZ2VtZWlucXZMcGUmVjagVuemVudHJ1bSBHZXNlbnGxzY2hhZnZnQgB5Si
LkquMR0wGwYDVQQLEDBRjbnR1cm5ldCBbnbdlbmR1bmdlbjEVMBMGAlUEAwMQVjJa
LVNpZ25hdHVVyMRUwEYDVRQFEew2ODAzMTk5NzI3NTcwggEiMA0GCSqGSIb3DQEBC
AQUAA4IBDwAwggEKAoIBAQCNm2DNSUqChfwdjBrLRHeiIpsaG/yQTUXVwjs5mlt
9xuTezWIjul/qtFa+NdPGLmfl6Svt1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/lN
Q/5dzhLzuF+PQmd9dcKN5q/AR9Jxuk9rQXbz6uKAKDCgxmx07L++OnLlqjrEOsm5
2ohDo6O+RNqfi68ASQ/vdkgizLPc/xpqPDZKGR6PIc8yJnGjvSHaBDMnkojaBb3K
47mkQW5SGoDXGL1tFGtbCTLqJqlbxrxWjQD7p13GyJagusopl3JE882iKNgHPUYB
JFIwZga/duKOYgbsS2CGxbwI5g5Ub0pS3tHzp3sSvpjAgMBAAGjggFbMIIBVzB4
BggrBgEFBQCBAQRsMGowPwYIKwYBBQUHMAKM2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZxJ0cy9hLXNpZ24tY29yYyYXR1LTA1LmNyDDAnBggrBgEfbQcwAyybaHR0
cDovL29jc3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDUwM6AxC+GLWh0dHA6
Ly9jcmlwYS10cnVzdC5hdC9jcmVvYS1zaWduLWNvcnBvcmlwZS0wNTAtBgNVHSME
```



```

47mkQW5SGoDXGL1tFGtbCTLqJqlbXrXwjQD7p13GyJagusoP13JE882iKNgHPUYB
JFIwZxa/duuKOYgbsS2CGxbwI5g5Ub0pS3tHZp3sSvPjAgMBAAGjggFbMIIBVzB4
BggrBgEFBQcBAQRsMGowPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZlZlcy9hLXNpZ24tY29yG9yYXR1LTA1LmNyDDAnBggrBgEFBQcwAYYbaHR0
cDovL29jZ3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDUwM6Axc+GLWh0dHA6
Ly9jcmwuYS10cnVzdC5hdC9jcmwvYS1zaWduLWNvcnBvcnF0ZS0wNTATBgNVHSME
DDAKGhKe9V2TRchVTAJBgNVHRMEAjAAMBEGA1UdDgQKBAhE5k8IGBy85zAOBgNV
HQ8BAf8EBAMCBaAwWAYDVR0gBFewTzBNBgcqKAARAQcBMEIwQAYIKwYBBQUHAQEW
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUt
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRuTSMIT225v8mMvnXDxtkzp9aRpZwZ
/Ym5foInVdktuAt6jz076c1OiQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Av1fleo8Bt3DE7E0gujjdEmDIg0Vx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpugmtYIRKGBje1tZSP3S2P2jMwE3MxL6jC6M6+FcnBTtdlt
iXJ6fxxCtUxFQvzw67obuJfLJE9MfdNwYqR90y+9C8n1frkx7kntpk61pu4j5b
O117F2QVfD5IdtLIGYtx+oOfzJoo6V4MeRzyP9KFeBmsHNG4NEZE1rP8P04Dk0i
hVUnl4Oq9w/H4uIpvYJP3hpW/GSouYlIGGnZ8qnUWNat7+qP1cKYOHmcXS1FmMxx
FPtKyctZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGvklBObY57YXhfjnhNS
WURfGIA5okvG7WkfVnPC6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbYsoqWhAkCT
3wE7gGsWtumQI8zwlYwviedrfTHTBxQCWJA3+Wt3AyhJVPbM+OR5dYQEHrM61sLH
Wks3t9iKvBN7+TNNwVWylP1fQT2dpyGQ9eMAGuSvZIrroFVMEAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo></dsig:Signature>
</eIdentity:IdentityDetailsResponse>

```

L.2.9. eIdentity:IdentityDataTokenRequest

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityDataTokenRequest
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>MSGID6546464646</eIdentity:MsgId>
    <eIdentity:CreDtTm>_TIME_</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:IdToken validTo="2099-01-01+01:00">_TOKEN_</eIdentity:IdToken>
  <eIdentity:AuthenticationDetails>
    <eIdentity:UserId>STSPAT2GXXX_123503</eIdentity:UserId>
    <eIdentity:SHA256Fingerprint>_SHA256_</eIdentity:SHA256Fingerprint>
  </eIdentity:AuthenticationDetails>
</eIdentity:IdentityDataTokenRequest>

```

L.2.10. eIdentity:IdentityDataTokenResponse

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eIdentity:IdentityDataTokenResponse xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2020"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2020 eI-
dentityService_v2.1.xsd">
  <eIdentity:MsgHeader>
    <eIdentity:MsgId>MSGID6546464646</eIdentity:MsgId>
    <eIdentity:CreDtTm>2020-02-24T17:43:42</eIdentity:CreDtTm>
  </eIdentity:MsgHeader>
  <eIdentity:IdentityResponse>
    <eIdentity:IdentityDataResult typ="FIRST_NAME">
      <eIdentity:Result>OK</eIdentity:Result>
    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="AGE">
      <eIdentity:Result>NOK</eIdentity:Result>
    </eIdentity:IdentityDataResult>
    <eIdentity:IdentityDataResult typ="LAST_NAME">

```

```
<eIdentity:Data>Musterlogin</eIdentity:Data>
</eIdentity:IdentityDataResult>
</eIdentity:IdentityResponse>
<eIdentity:ResponseStatus>
  <eIdentity:ResponseCode>100</eIdentity:ResponseCode>
</eIdentity:ResponseStatus>
<dsig:Signature Id="hotVault" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo>
    <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
    <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
    <dsig:Reference Id="reference-data-0" URI="">
      <dsig:Transforms>
        <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
      </dsig:Transforms>
      <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmllenc#sha256" />
    <dsig:DigestValue>5eNhNh9dnR0lxVb97Yf7vjeiNZPJVYjXqrIwTIUxtCQ=</dsig:DigestValue>
    </dsig:Reference>
  </dsig:SignedInfo>
  <dsig:SignatureValue>MTJkE0627dmc+X6Mu2rIq2K/PD780/0Mb5F5UTjcxJBvJizyYp5CJER23Crj9es0
qIrnJuCh9JbRue0dwASKUFV/CztLX3/mcC230fLzJ2WELsoya6BBok9ss2sPlDPi
lWWw6XDvm+dP4BBIEtflLlk6ZuRNSSIYw5ptfprOekiN6UoU4SGurW91r+U9w19X
N15oxdvl/t6YnS7KJRsp2KoQ8etcMsNAKMkZB4RWezihI1BQsuIPIzuG+FmoDtpn
6UbGpa60X7hz2/MVPW9M6IYYwzTdlLvowc2NiPIzItBCYRIax9Lkx+L+plyr8EUq
k8Fb7SBWN+MCWAHQp9jp9Q==</dsig:SignatureValue>
  <dsig:KeyInfo>
    <dsig:X509Data>
      <dsig:X509Certificate>
        MIIGBTCCA+2gAwIBAgIDGkVxMA0GCSqGSIb3DQEBCwUAMIGTMQswCQYDVQQGEwJB
VDFIMEYGA1UECgw/QS1UcnVzdCBHZXMuIGYyIFNpY2hlcmhlaXRzc3lzdGVtZSBp
bSB1bGVVrdhIuIERhdGVudmVya2VociBhbWJIMRwwGgYDVQQLDBNlLXNpZ24tY29y
cG9yYXR1LTA1MRwwGgYDVQDDBNhLXNpZ24tY29ycG9yYXR1LTA1MB4XDTE1MTEeX
MDA3MDUyOV0xODTIwMTEeXMDA2MDUyOV0wZyZyCzAJBgNVBAYTAkFUMTowOAYDVQQK
DDFBUlogQWxsZ2VtZW1uZXMGUmVjaGVuemVudHJ1bSBHZNlBzY2hhZnZnQgB5i
LkguMR0wGwYDVQQLDBRlbnR1cm5ldCBBbndlbnR1bmdlbjEVMBMGA1UEAwwMQVJa
LVNpZ25hdHVyMRUwEwYDVQQFEww2ODAzMTk5NzI3NTcwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCnm2DNSUqChfwDjBrLRHeiIpsaG/yQTUXVwjs5mlt
9xuTezWIju1/qtFa+NdPGLmfL6SvT1cRAGmEUS2zynvod7vep4G6YNY1BCq6M/1N
Q/5dzhLzuF+PQmd9dcKN5q/AR9JxuK9rqbZ6uKAKDCgxm07L++OnLLqjrEOsm5
2ohDo60+RNqFi68ASQ/vdKqizLPc/xpqPDZKGR6PIc8yJnGjvSHaBDMnkojaBb3K
47mkQW5SGoDXGL1tFGtbCTLqJqlbxrXwJQD7p13GyJagusoPl3JE882iKNGHPUYB
JFIwZxa/dduKOYgbsS2CGxbwI5g5Ub0pS3tHZp3sSvpjAgMBAAGjggFbMIIBVzB4
BggrBgEFBQcBAQRsMGowPwYIKwYBBQUHMAKGM2h0dHA6Ly93d3cuYS10cnVzdC5h
dC9jZjZlcy9hLXNpZ24tY29ycG9yYXR1LTA1LmNydDAnBggrBgEFBQcwAYYbaHR0
cDovL29jZ3AuYS10cnVzdC5hdC9vY3NwMD4GA1UdHwQ3MDUwM6AxcC+GLWh0dHA6
Ly9jcmwuYS10cnVzdC5hdC9jcmwvYS1zaWduLWNvcnBvcnF0ZS0wNTATBgNVHSME
DDAKGhKe9V2TRchVTAJBgNVHRMEAjAAMBEGA1UdDgQKBAhE5k8IGBy85zaOBGnV
HQ8BAf8EBAMCBaAwAYDVR0gBFewTzBNBgcqKAARAQcBMEIwQAYIKwYBBQUHAGew
NGh0dHA6Ly93d3cuYS10cnVzdC5hdC9kb2NzL2NwL2Etc2lnbi1jb3Jwb3JhdGUt
bGlnaHQwDQYJKoZIhvcNAQELBQADggIBAMRuTSMIT225v8mMvnXDxtkz9aRpZwZ
/Ym5foInVdktuAt6jz076c10iQPv/uAN4Fje6dhKYqWtHybLr9oo7k8scljBcLk5
TQBSKhUI4Av1f1eo8Bt3DE7EOgujjdEmDIg0Vx6oVf6QdE2oqE4EwV8vET9KJIq2
gaXak8FqJS+6pIiKRpugmtYIRKgbje1tZSP3S2P2jMwE3MxL6jC6M6+FcNBTtdlt
iXJ6fxxCtUxFQvzv67obuJfDLJE9MfdNwYqR90y+9C8n1frkx7kknTPK61pu4j5b
O117F2QVfD5IdtLIGYtx+oOfzJoo6V4MeRzyP9KFeBmsHNG4NEZE1rP8P04Dk0i
hVUnl4Oq9w/H4uIpvYJP3hpW/GSouYlIGGnZ8qnUWNat7+qP1cKYOHmcXS1FmMxx
FPtKyctZ8aSetpVqV5nWIX4JNquHdpPFZ695vm75inq0tGVkl1BOBY57YXhfjnHNS
WURfGIA5okvG7WkfVnPC6s81V3g/kt8mf2RnxWRHQ3kK+MsbC5VWkbYsoqWhAkCT
3wE7gGsWtumQI8zwlYwviedrfTHTBxQCWJA3+Wt3AyhJVPbM+OR5dYQEHM61sLH
Wks3t9iKvBN7+TNNeWVWyLP1fQT2dpyGQ9eMAGuSvZlrrwoFVMEAQ2BrJCP3VtFy
IKFesw/oHJbX</dsig:X509Certificate>
    </dsig:X509Data>
  </dsig:KeyInfo>
</dsig:Signature>
</eIdentity:IdentityDataTokenResponse>
```

M. ANHANG – ANZEIGEMASKE IM ONLINE-BANKING

M.1. Beispiel

E-IDENTITY SERVICE

26.10.2014, 12:01 Uhr

Max Mustermann, Verfügter: 1

Angeforderte Daten:

Vorname:	Max	<input checked="" type="checkbox"/>
Nachname:	Mustermann	<input checked="" type="checkbox"/>
Geburtsdatum:	12.11.1956	<input checked="" type="checkbox"/>
IBAN:	<input type="text" value="AT485730054011026801"/>	

Mit der Zeichnung ermächtige ich mein Kreditinstitut dem Händler "Mustershop D.O.C. Brown" die ausgewählten Daten zuzustellen.

Die Identifikation ist **fehlgeschlagen**, da die vom Händler verschickten Kundendaten nicht vollständig mit den bei der Bank hinterlegten Daten übereinstimmen.

Abbildung 12: Beispiel-Anzeigemaske im Online-Banking

N. ANHANG – STAGING

Der e-Service Scheme Operator wird in drei Umgebungen betrieben. Es handelt sich dabei jeweils um getrennte Datenbestände.

N.1. Produktion

Diese ist die einzig SLA-relevante Stage. In dieser Umgebung werden Echtdatei geroutet und die abgewickelten Prozesse entsprechend Vertrag verrechnet.

N.2. Test

Es handelt sich um eine komplett getrennte Installation zur Produktion aber mit dem selben Codestand der Produktion. Die Umgebung dient hauptsächlich dazu, Händlern eine nicht-produktive Umgebung für die Integration zur Verfügung zu stellen.

N.3. Abnahme

Die Abnahmeumgebung erfüllt zweierlei Zwecke:

- Abnahme einer neuen Version des e-Service Operators
- Umgebung zu bankinternen Tests einer neuen Version auf Banking-Seite

TABELLENVERZEICHNIS

<i>Tabelle 1: Referenzen auf weitere Dokumente</i>	<i>11</i>
<i>Tabelle 2: Schema und Prefixes</i>	<i>36</i>

ABBILDUNGSVERZEICHNIS

<i>Abbildung 1: Logo</i>	12
<i>Abbildung 2: Ablaufbeschreibung – Übersicht</i>	15
<i>Abbildung 3: Ablaufbeschreibung im Detail</i>	16
<i>Abbildung 4: Bankenauswahl</i>	18
<i>Abbildung 5: Beispiel QR-Code</i>	22
<i>Abbildung 6: Ablaufbeschreibung Browser2App</i>	22
<i>Abbildung 7: Ablaufbeschreibung POS2App</i>	24
<i>Abbildung 8: Ablaufbeschreibung App2App</i>	25
<i>Abbildung 9: Workflow eID Token</i>	27
<i>Abbildung 10: Ablaufbeschreibung – Übersicht</i>	32
<i>Abbildung 11: Ablaufbeschreibung im Detail</i>	33