

iDIN Acceptant Implementatie Gids

Document versie 1.05 (geldig vanaf 01-01-2017)



VERTROUWELIJK

September 2016

Copyright © Currence Services BV

All rights reserved.

Voorwaarden

De voorwaarden voor het beschikbaar stellen van de iDIN Acceptant Implementatie Gids zijn:

- 1 Currence Services BV (verder ook wel aangeduid als 'Currence') stelt deze Acceptant Implementatie Gids beschikbaar aan licentiehouders die deze vervolgens distribueren aan (potentiële) Acceptanten en Digital Identity Service Providers (DISPs) zodat zij als (potentiële) afnemers iDIN kunnen implementeren.
- 2 Currence behoudt zich het recht voor het beschikbaar stellen van deze Acceptant Implementatie Gids te weigeren aan (potentiële) Acceptanten en DISPs op grond van haar moverende redenen, in overleg met de licentiehouders waarmee de Acceptant/DISPs een contract heeft.
- 3 Deze Acceptant Implementatie Gids wordt nadrukkelijk uitsluitend met bovenstaand doel ter beschikking gesteld en enig ander gebruik van dit document is niet toegestaan. Aan het document of de in de bijgaande toelichting gegeven informatie kunnen geen rechten worden ontleend. Currence is op geen enkele wijze aansprakelijk voor de gevolgen van latere wijzigingen van de iDIN Standaard of de iDIN Acceptant Implementatie Gids. Indien licentiehouders of andere geïnteresseerden beslissingen nemen en/of investeringen doen op basis van de informatie die zij via deze iDIN Acceptant Implementatie Gids hebben verkregen, dan accepteert Currence hiervoor geen enkele aansprakelijkheid.
- 4 Deze Acceptant Implementatie Gids is een vertaling van de Engelstalige iDIN Merchant Implementation Guidelines. Deze vertaling is met grote zorgvuldigheid samengesteld. Indien er toch afwijkingen zijn tussen de Nederlandse vertaling en het Engelstalige origineel, dan is de Engelstalige versie leidend.
- 5 Deze Acceptant Implementatie Gids is gebaseerd op de informatie in de iDIN Standaard documentatie. In het geval dat er afwijkingen zijn tussen de iDIN Acceptant Implementatie Gids en de iDIN Standaard documentatie dan is de tekst in de Standaard documentatie leidend.

Vragen over dit document, of verzoeken om meer informatie, kunnen worden gericht aan de licentiehouders of uw DISP.

Inhoudsopgave

Voorwaarden	2
Inhoudsopgave	3
Tabellen	8
Figuren	10
1 Inleiding	11
1.1 Doelgroep	11
1.2 Document opzet	11
1.3 Andere referenties	12
1.4 Conventies met betrekking tot notaties	12
1.5 Definities van online bankieren	12
1.6 Revisies	13
1.7 Wijzigingen in vergelijking met eerdere versies	13
1.7.1 Veranderingen ten opzichte van versie 1.00	13
1.7.2 Veranderingen ten opzichte van versie 1.04	13
1.7.3 Veranderingen ten opzichte van versie 1.041	14
2 Overzicht	16
2.1 Het vier-partijen model	16
2.1.1 De relaties tussen deze rollen	17
2.1.2 Relaties bij gebruik van een DISP	17
2.2 iDIN services	17
2.3 iDIN proces	18
2.4 iDIN-transactie	18
2.4.1 Gedelegeerde authenticatie	18
2.4.2 Leveren van Gebruikersattributen	19
2.5 Acceptant registratie	20
2.6 Dispuutmanagement	20

3	iDIN protocollen.....	21
3.1	Technische basisprincipes	21
3.2	iDx protocollen	21
3.2.1	Directory Protocol	22
3.2.2	Transaction Protocol	22
3.2.3	Status Protocol	23
3.2.4	Error Protocol	23
3.3	SAML V2.0	23
4	iDIN bericht formaat	24
4.1	Algemeen	24
4.2	Karakter set	24
4.3	HTTP	24
4.4	XML header	24
4.5	XML namespaces	25
4.6	XML Schema's	25
5	iDIN data catalogus	27
5.1	iDx attributen	27
5.2	iDx data elementen	27
5.3	iDIN data elementen	30
5.3.1	iDIN Requested- en DeliveredServiceID	32
5.3.2	Adres	33
5.4	Gebruikersattributen	33
5.5	Gegarandeerde minimale set van aangevraagde attributen	37
6	iDIN Directory Protocol.....	38
6.1	General	38
6.2	Directory Request (DirectoryReq)	38
6.3	Directory Response (DirectoryRes)	39
6.4	Presentatie van de Issuer selectielijst	39

7	iDIN Transaction Protocol	41
7.1	General	41
7.2	Transaction Request (AcquirerTrxReq)	41
7.3	Transaction Response (AcquirerTrxRes)	43
7.4	Errors (fouten) bij het uitvoeren van het Transactie Protocol	43
7.5	Redirect naar de online bankiersomgeving (issuerAuthenticationURL)	44
7.5.1	Specifieke eisen aan iDIN mobiel: Redirect naar de Issuer (geen in-app browser)	44
7.6	Redirect naar de Acceptant omgeving (merchantReturnURL)	45
7.6.1	Eisen voor iDIN mobiel: redirect naar de omgeving van de Acceptant	45
7.7	Fouten tijdens het uitvoeren van de redirect naar de Issuer, het goedkeuren van de iDIN authenticatie en/of de redirect naar de omgeving van de Acceptant	46
7.8	Vier scenario's voor het afronden van het mobiele iDIN proces	46
7.8.1	Gebruiker wordt doorgestuurd van de (mobiele) webpagina van de Acceptant naar de (mobiele) webpagina van de Issuer	46
7.8.2	Gebruiker wordt doorgestuurd van de (mobiele) webpagina van de Acceptant naar de Issuer's mobiel bankieren applicatie	47
7.8.3	Gebruiker wordt doorgestuurd van de mobiele applicatie van de Acceptant naar de Issuer's (mobiele) webpagina	48
7.8.4	Gebruiker wordt doorgestuurd van de applicatie van de Acceptant naar de Issuer's mobiel bankieren applicatie	49
7.9	Verwerkingssnelheid en time-out van transactieberichten	50
8	iDIN Status Protocol	51
8.1	Algemeen	51
8.2	Status Request (AcquirerStatusReq)	51
8.3	Status Response (AcquirerStatusRes)	52
8.4	Foutsituaties tijdens het uitvoeren van het Statusprotocol	54
8.5	Restricties met betrekking tot AcquirerStatusReq	54
8.6	Verwerkingssnelheid en time-out van statusberichten	54
9	Foutafhandeling (Error Handling)	55
9.1	Algemeen	55
9.2	Error Response (AcquirerErrorRes)	55
9.3	Onbeschikbaarheid	56

10	Beveiliging en certificaten	57
10.1	Algemene principes van certificaten	57
10.2	Signeren van iDIN berichten	57
10.2.1	Signeren van de SAML 2.0 Assertion	59
10.3	SAML EncryptedID en EncryptedAttribute	59
10.4	Authenticatie van iDIN berichten	61
10.5	Maken van een sleutelpaar	61
10.5.1	Een certificaat aanschaffen bij een Certificate Authority	62
10.6	Signature data elementen	62
11	Presentatie van iDIN	64
11.1	Algemeen	64
11.2	Transactiestroom	64
11.3	Redirect naar de Issuer	64
11.4	Frames	64
11.5	Nieuw venster	65
11.5.1	Specifieke eisen aan iDIN mobiel: Nieuw venster of app	65
11.6	Issuer lijst	65
11.7	Banners en logo's	65
11.8	Eisen en aanbeveling iDIN teksten Acceptantschermen	65
11.8.1	Tonen van de laatste inlog (verplicht)	65
11.8.2	Uitleg iDIN aan de Gebruiker	65
11.8.3	Aanbevelingen teksten Acceptantschermen per RequestedServiceID	66
11.9	Issuer front-end	67
11.9.1	Teksten op de Issuerschermen per RequestedServiceID	68
12	Appendix A: Foutcodes (Error codes)	71
12.1	iDx error codes	71
12.2	SAML Error codes	72
12.3	SAML Error cases	73
12.4	Issuer kan niet alle attributen leveren volgens minimale set	74
12.5	Bericht aan de Gebruiker	74

13	Appendix B: Voorbeeld berichten	76
13.1	DirectoryReq (A)	76
13.2	DirectoryRes (A')	76
13.3	AcquirerTrxReq (B)	78
13.4	AcquirerTrxRes (B')	79
13.5	AcquirerStatusReq (F)	80
13.6	AcquirerStatusRes (F') Unencrypted	81
13.7	AcquirerStatusRes (F') Encrypted	84
13.8	AcquirerErrorRes (B'(X))	88
14	Appendix C: iDx Merchant-Acquirer Schema	90

Tabellen

Tabel 1: Referenties	12
Tabel 2: Revisie tabel	13
Tabel 3: Bericht naamgeving en beschrijving	22
Tabel 4: HTTP header	24
Tabel 5: XML header	25
Tabel 6: iDx namespaces	25
Tabel 7: XML schema's	26
Tabel 8: iDx attributen	27
Tabel 9: iDx data elementen	30
Tabel 10: Specifieke iDIN data elementen	31
Tabel 11: Overzicht van binaire waarden van Requested- en DeliveredServiceID.....	33
Tabel 12: Gebruikersattributen	36
Tabel 13: Minimale set attributen per attribuutgroep	37
Tabel 14: Elementen/attributen van het DirectoryReq	39
Tabel 15: Elementen/attributen van het DirectoryRes.....	39
Tabel 16: Elementen/attributen van het AcquirerTrxReq	42
Tabel 17: Elementen/attributen in de container van het AcquirerTrxReq.....	43
Tabel 18: Elementen/attributen van het AcquirerTrxRes	43
Tabel 19: Verschillende scenario's voor de mobiele iDIN processen	46
Tabel 20: Scenario: Redirect van (mobiele) webpagina van de Acceptant naar de Issuer's (mobiele) webpagina	47
Tabel 21: Scenario: Redirect van de (mobiele) webpagina van de Acceptant naar de Issuer's mobiele bankier applicatie	48
Tabel 22: Scenario: Redirect van de mobiele applicatie van de Acceptant naar de Issuer's (mobiele) webpagina	49
Tabel 23: Scenario: Redirect van de mobiele applicatie van de Acceptant naar de Issuer's mobiele bankier applicatie	49
Tabel 24: Verwerkingssnelheid eisen (voor het 95ste percentiel).....	50
Tabel 25: Elementen/attributen van het AcquirerStatusReq	51
Tabel 26: Elementen/attributen van het AcquirerStatusRes	52
Tabel 27: Elementen/attributen in de container van het AcquirerStatusRes	53

Tabel 28: Verwerkingssnelheid eisen (voor het 95ste percentiel)	54
Tabel 29: Elementen/attributen van het AcquirerErrorRes	55
Tabel 30: Elementen/attributen in de container van het AcquirerErrorRes	56
Tabel 31: Elementen/attributen van het Signature element	63
Tabel 32: Veranderingen in de Signature elementen bij ondertekenen van SAML 2.0 Assertion	63
Tabel 33: Aanbeveling teksten Acceptantschermen per use case	67
Tabel 34: Termen in Issuerschermen per use case	69
Tabel 34: Error code categorieën	71
Tabel 35: Error codes	72
Tabel 36: errorDetail	72
Tabel 37: Eerste SAML statuscodes	72
Tabel 38: Tweede SAML statuscodes	73
Tabel 39: Bericht aan de Gebruiker	75

Figuren

Figuur 1: Het vier-partijen model	16
Figuur 2: Transaction, Status en Error protocol	22
Figuur 3: Requested- en DeliveredServiceID lay-out.....	32
Figuur 4: Voorbeeld van een (open) dropdown list box welke de Issuer selectielijst laat zien	40
Figuur 5: Voorbeeld van goedkeuring van een iDIN-transactie.....	70

1 Inleiding

1.1 Doelgroep

Dit document geeft een gedetailleerde beschrijving van iDIN van de Nederlandse banken. Het document is bedoeld voor degenen die gedetailleerde informatie behoeven ten aanzien van deze oplossing.

Dit document is bedoeld voor Acceptanten die aan willen sluiten op het iDIN platform van hun bank. Het behandelt het berichtenverkeer tussen Acceptanten en hun bank. Voor Acceptanten is het berichtenverkeer tussen Acquirer en Issuer niet van belang. Dit deel van de iDIN Standaard wordt daarom in dit document niet behandeld, tenzij de berichten van belang zijn voor de implementatie van de Acceptant worden deze beschreven.

Dit document is niet bank-specifiek; dit wil zeggen dat alleen generieke iDIN zaken in dit document worden behandeld. Informatie over non-standaard aansluitvormen bij specifieke Acquirers en de hulp- (middelen) die een Acquirer verstrekt om aan te sluiten op iDIN zijn geen onderdeel van dit document. Voor informatie over deze onderwerpen verwijzen wij u naar de door uw Acquirer verstrekte (aanvullende) documentatie.

Om Acceptanten verder te ondersteunen, zijn er Software Libraries ontwikkeld in .NET, PHP en Java. Neem contact op met uw Acquirer voor meer informatie betreffende deze Software Libraries.

1.2 Document opzet

Dit document heeft de volgende structuur:

- Hoofdstuk 1: Inleiding
- Hoofdstuk 2: Introductie van iDIN en de betrokken partijen;
- Hoofdstuk 3: Introductie in de verschillende berichten binnen iDIN en de algemene structuur van de uitgewisselde berichten;
- Hoofdstuk 4: Algemene berichtgevingsstandaard;
- Hoofdstuk 5: Data catalogus; Alle parameters die relevant zijn voor de Acceptant in de iDIN omgeving;
- Hoofdstuk 6: Directory protocol: Ontvangen van de lijst van Issuers die iDIN aanbieden;
- Hoofdstuk 7: Transaction protocol: Aanvragen van Gebruikersattributen, identificatie of leeftijdsverificatie;
- Hoofdstuk 8: Status protocol: Ontvangen van de Gebruikersattributen;
- Hoofdstuk 9: Error handling;
- Hoofdstuk 10: Beveiliging en certificaten;
- Hoofdstuk 11: Presentatie van iDIN op de website van de Acceptant;

1.3 Andere referenties

Titel	Versie	Uitgegeven door:
AES, FIPS 197/ SO/IEC 18033-3	-	FIPS/ISO
Base16, Base32, and Base64 Data Encodings http://www.ietf.org/rfc/rfc3548.txt	Juli 2003	Network Working Group
Base64 Content-Transfer-Encoding http://tools.ietf.org/html/rfc2045#section-6.8	November 1996	Network Working Group
GUIDELINES ON ALGORITHMS USAGE AND KEY MANAGEMENT (EPC342-08)	Version 1.1 goedgekeurd op 23 Februari 2009	EPC
ISO 9362, 8901 Standard	2014	ISO
Multilingual European Subset 2 (MES-2) Unicode.org http://www.utf8-chartable.de/unicode-utf8-table.pl	15 April 2000	CEN
NEN 1888_2002, NEN 5825_2002	2002	NEN
Open SSL Library http://www.openssl.org	Maart 2015	OpenSSL
Security Assertion Markup Language (SAML) Core	2.0	OASIS
TLS Protocol version 1.0 http://www.ietf.org/rfc/rfc2246.txt	1.0, Januari 1999	IETF
TLS Protocol version 1.1 http://www.ietf.org/rfc/rfc4346.txt	1.1, April 2006	IETF
TLS Protocol version 1.2 http://www.ietf.org/rfc/rfc5246.txt	1.2, Augustus 2008	IETF
XML Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008 http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/	Second edition, 10 Juni 2008	World Wide Web Consortium (W3C)
XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002 http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#sec-EncryptedData	10 December 2002	World Wide Web Consortium (W3C)

Tabel 1: Referenties

1.4 Conventies met betrekking tot notaties

Berichten en redirects worden geschreven als *dit*, en data elementen worden geschreven als *dit*.

1.5 Definities van online bankieren

In dit document worden de termen 'internet bankieren' en 'online bankieren' gebruikt. Voor banken van de Gebruiker die iDIN mobiel implementeren, zouden deze termen geïnterpreteerd moeten worden als 'internet bankieren' en/of 'mobiel bankieren'. Waar internet of online gerelateerde terminologie gebruikt wordt, moet dit altijd gelezen worden als ook betrekking hebbende op het mobiele kanaal. In geval het mobiele gebruik van iDIN tot aanvullende vereisten (requirements) leidt, zullen deze specifiek benoemd worden in onderhavige Implementatie Gids.

1.6 Revisies

Versie	Beschrijving	Release datum
1.00	Initiële versie	1 September 2015
1.04	<ol style="list-style-type: none"> 1. Toevoeging foutafhandeling als de Issuer niet kan voldoen aan de minimale set van Consumentenattributen 2. Toevoeging apart kunnen aanvragen/terugsturen van het geslacht van de Consument 3. Toelichting op het formaat van DateTimeStamp <p>Let op: Er zijn geen andere versies gepubliceerd tussen v1.00 en v1.04. Dit is gedaan om de versie-nummering gelijk te trekken met andere documentatie.</p>	23 Oktober 2015
1.041	<ol style="list-style-type: none"> 1. Toevoeging aanbeveling teksten Acceptantschermen 2. Aanscherping standaard Consumentberichten 3. Enkele kleine verduidelijkingen toegevoegd 	22 januari 2016
1.05	<ol style="list-style-type: none"> 1. Herindeling van de Requested- and DeliveredServiceID bits 2. Toevoeging telefoon- en email aan de set van opvraagbare attributen 3. Verbetering en update van de Issuer front-end teksten 4. Verwijdering Appendix B die alle mogelijke waardes bevatte van het RequestedServiceID 5. Wijziging, van de door de Acceptant gebruikte TLS versie, naar minimaal 1.2 6. Kleine correcties en verduidelijkingen 	30 september 2016

Tabel 2: Revisie tabel

1.7 Wijzigingen in vergelijking met eerdere versies

1.7.1 Veranderingen ten opzichte van versie 1.00

1. Toevoeging foutafhandeling als de Issuer niet kan voldoen aan de minimale set van Consumentenattributen: Twee elementen zijn toegevoegd in het AcquirerStatusRes (DeliveredServiceID en een tweede SAML status code). Deze geven informatie aan de Acceptant als de Issuer niet alle attributen kan leveren conform de gedefinieerde minimale set (zie Sectie 5.5). De foutafhandeling staat beschreven in Sectie 12.4;
2. Toevoeging apart kunnen aanvragen/terugsturen van het geslacht van de Consument: De Acceptant kan nu het geslacht van de Consument apart aanvragen met het RequestedServiceID, waar dit attribuut voorheen onderdeel was van de attribuutgroep naam.;
3. Toelichting op het formaat van DateTimeStamp (in alle varianten, zoals de createDateTimestamp): Acceptanten mogen nul tot drie decimalen achter de seconde gebruiken in de DateTimeStamp van de berichten die ze naar de Routing Service sturen. De berichten die de Acceptant vanuit de Routing Service ontvangt bevatten wel altijd drie decimalen achter de seconde. Zie Tabel 9.

1.7.2 Veranderingen ten opzichte van versie 1.04

1. Toevoeging aanbeveling teksten Acceptantschermen: Dit is beschreven in hoofdstuk 11.8;
2. Aanscherping standaard Consumentberichten: Dit wordt beschreven in hoofdstuk 12.5.
3. Enkele kleine verduidelijkingen toegevoegd:

- a. In het formaat van `DateTimestamp` in Tabel 9 is toelichting toegevoegd dat `YYYY` staat voor het kalenderjaar, en dat 24-uurs notatie gebruikt moet worden;
- b. In de beschrijving van het formaat van `TransactionID` in Tabel 9 is toegevoegd dat de eerste vier cijfers zijn opgemaakt uit het `AcquirerID`;
- c. In de beschrijving van het tonen van de laatste inlog door de Acceptant in Sectie 11.8.1 is toegevoegd dat de datum en tijd getoond moeten worden (i.p.v. het tijdstip). Daarnaast is de reden voor deze eis toegevoegd, namelijk dat de Consument dan zelf kan controleren of dit tijdstip overeenkomst met zijn/haar laatste bezoek)
- d. In Appendix B in **Error! Reference source not found.** is de kolom 'use case' toegevoegd die aangeeft welk `ServiceID` hoort bij welke use case;
- e. Toevoeging aanbeveling op het gebruik van TLS in hoofdstuk 10.1: Acceptanten worden geadviseerd om TLS versie 1.1 of hoger te gebruiken. Het gebruik van TLS versie 1.0 wordt afgeraden, omdat deze versie is verouderd.

1.7.3 Veranderingen ten opzichte van versie 1.041

- 1. De bit-structuur van het `RequestedServiceID` en `DeliveredServiceID` zijn heringedeeld (zie sectie 5.3.1) om het telefoon- en emailattribuut toe te voegen. De herindeling heeft geen impact op de integere waarden van het `ServicesID` en is daardoor backwards compatible;
- 2. Het telefoon- en emailattribuut zijn toegevoegd in Tabel 12;
- 3. Update van de Issuer front-end teksten die aan de Gebruiker worden getoond afhankelijk van de attributen die zijn aangevraagd door de Acceptant (zie Sectie 11.9.1)
- 4. Appendix B is verwijderd. Deze Appendix bevatte alle mogelijke integere waarden van het `RequestedServiceID`. Door de toevoeging van het telefoon- en emailattribuut zou deze tabel te groot zijn geworden. De Excel '160529A_ServiceID_Calculator' die samen met deze implementatie Gids wordt verstrekt biedt de mogelijkheid om gemakkelijk het `ServiceID` te berekenen;
- 5. In de toekomst zullen verouderde TLS versies niet langer worden ondersteund door de Routing Service. Daarom moet de Acceptant minimaal TLS versie 1.2 gebruiken (zie Sectie 10.1);
- 6. Kleine correcties en verduidelijkingen:
 - a. In Sectie 10.2.1 is toegevoegd dat het `X509SubjectName` element mag worden ingegrepen door de Validation Service in het Signature element binnen de Assertion;
 - b. In Sectie 10.3 is toegevoegd dat xsi type definities mogen worden gebruikt binnen het `AttributeValue` element door de Validation Service;
 - c. Toevoeging van het `Issuer.x509` data element in Tabel 10. De beschrijving van dit element ontbrak;
 - d. Verwijdering van errorcode SE2000 en wijziging van errorcode SE2100 naar SE2700 (Invalid electronic signature). SE2000 en SE2100 worden niet gebruikt in iDIN;

- e. Update van de versleuteling voorbeelden en versleutelde voorbeeld berichten met de volledige namespace declaraties. De namespace declaraties stonden niet in de voorbeelden;
- f. Enkele namespace prefixen en de afsluitende tag van het eerste StatusCode element zijn toegevoegd in het voorbeeld in Sectie 12.2. Enkele namespace prefixen en de afsluitende tag ontbraken;
- g. Het tonen van de laatste login aan de Gebruiker in Sectie 11.8.1 is veranderd van verplicht naar sterk aangeraden;
- h. Update van de `Merchant.LegalIDs` in de voorbeeld berichten met geldige controle getallen.

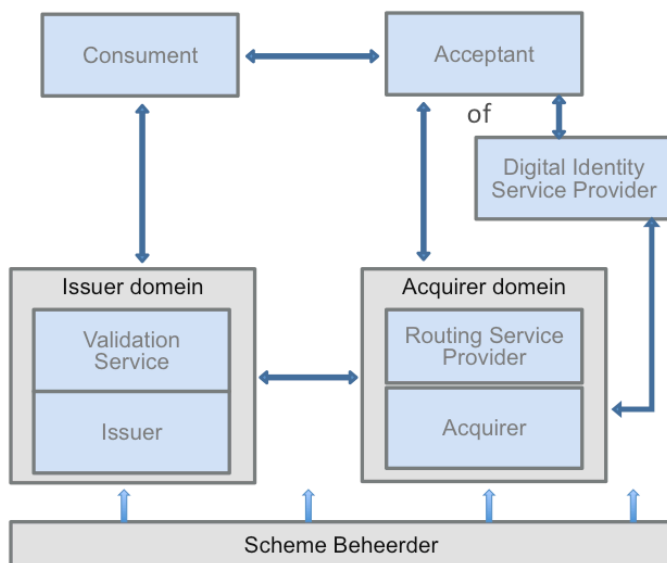
2 Overzicht

Dit hoofdstuk geeft een beschrijving van de algemene elementen in iDIN.

2.1 Het vier-partijen model

Het iDIN systeem is gebaseerd op het vier partijen model. Figuur 1 laat de rollen in dit model zien, vergezeld door hun wederzijdse primaire relaties in de context van iDIN. De rollen zijn die van de Gebruiker, Acceptant, Acquirer (bank van de Acceptant), Issuer (bank van de Gebruiker), Routing Service, Validation Service en Digital Identity Service Providers (DISP):

- **Acceptant:** De Acceptant is het bedrijf dat de Gebruiker wil identificeren, authentifieren en/of Gebruikersattributen wilt vergaren. Dit kan de daadwerkelijk Acceptant zijn, of een DISP die in naam van de uiteindelijke Acceptant de iDIN-transactie uitvoert;
- **Gebruiker:** De Gebruiker is een natuurlijk persoon wiens attributen worden beheerd door zijn/haar bank, de Issuer;
- **Acquirer:** De Acquirer is de bank bij welke de Acceptant zijn contract heeft voor het iDIN product;
- **Issuer:** De Issuer is de bank van de Gebruiker;
- **Routing Service:** Dit is een technische rol (routing van berichten) die wordt vervuld door de Acquirer, of door een derde partij die namens de Acquirer handelt. Waar in dit document de term 'Routing Service' wordt gebruikt, dient dit geïnterpreteerd te worden als 'Routing Service van de Acquirer';
- **Validation Service:** Dit is een technische rol die vervuld wordt door de Issuer of door een derde partij namens de Issuer. Waar in dit document de term 'Validation Service' wordt gebruikt, dient dit geïnterpreteerd te worden als 'Validation Service van de Issuer';
- **DISP:** Een derde partij die iDIN namens de Acceptant uitvoert als die goedkeuring heeft van zowel de Acceptant en de Acquirer.



Figuur 1: Het vier-partijen model

2.1.1 De relaties tussen deze rollen

Zowel contractuele als technische relaties bestaan tussen de genoemde rollen. Deze relaties zullen hieronder in meer detail worden toegelicht:

- Acceptant - Acquirer: De Acceptant heeft een contract met de Acquirer;
- Gebruiker - Issuer: De Gebruiker heeft een contract met de Issuer. De identiteit gerelateerd aan dit contract wordt gebruikt voor identificatie, authenticatie en voor het leveren van Gebruikersattributen;
- Gebruiker - Acceptant: De Gebruiker mag iDIN gebruiken om toegang te krijgen tot een service van de Acceptant;
- Acquirer - Issuer: Gebonden met een licentie binnen het iDIN scheme.

Technische relaties:

- Acceptant - Routing Service: De Acceptant heeft een technische relatie met de Routing Service. De Routing Service biedt de Acceptant de mogelijkheid om verzoeken voor iDIN naar de Validation Service te sturen. In relatie tot dit doel wisselen zij berichten uit;
- Routing Service – Validation Service: De Routing Service en Validation Service hebben een relatie voor het gebruik van iDIN. Ze wisselen in deze context berichten uit;
- Gebruiker – Validation Service: De Validation Service biedt de Gebruiker de mogelijkheid tot het afgeven van authenticatie en/of attributen aan Acceptanten, door het goedkeuren van iDIN verzoeken. De Gebruiker kan een verzoek goedkeuren in de omgeving van zijn/haar Issuer.

2.1.2 Relaties bij gebruik van een DISP

In het model waar een Acceptant de iDIN activiteiten heeft uitbesteed aan een DISP¹ de contract relatie tussen de Acceptant – Acquirer is vervangen door de volgende relaties:

- Acceptant - DISP: De Acceptant heeft een contract met een DISP;
- DISP - Acquirer: De DISP heeft een contract met de Acquirer.

De technische relatie tussen de Acceptant – Routing Service wordt vervangen door de volgende relaties:

- Acceptant - DISP: De Acceptant heeft een technische relatie met de DISP. De DISP levert aan de Acceptant de mogelijkheid om iDIN verzoeken te sturen naar de Routing Service en Validatie Service. In deze context wisselen zij berichten uit;
- DISP - Routing Service: De DISP heeft een technische relatie met de Routing Service. De Routing Service stuurt berichten door van de DISP naar de Validation Service. Ze wisselen in deze context berichten uit.

2.2 iDIN services

Deze paragraaf introduceert de services die iDIN biedt aan Gebruikers en Acceptanten.

¹ Voor due diligence redenen kan de DISP extra audits krijgen.

iDIN faciliteert de volgende services:

- Authenticatie van de Gebruikers bij de Acceptant gebaseerd op betrouwbare gegevens uitgegeven door de Issuer;
- Verstrekken van Gebruikersattributen uit de administratie van de Issuer inclusief leeftijdsverificatie.

Notie: In dit document wordt het proces van authenticatie en/of het leveren van Gebruikersattributen gerefereerd als een iDIN-transactie/verzoek.

Bovenstaande services kunnen onder andere door de Acceptant worden gebruikt voor de volgende doeleinden:

- Het aanmaken van nieuwe accounts voor Gebruikers, gebaseerd op gedelegeerde authenticatie en attributen verstrekt door de Issuer;
- Inloggen van bestaande Gebruikers die een account hebben aangemaakt met iDIN, of een bestaande account hebben gekoppeld met iDIN;
- Leeftijdsverificatie.

De volgende services worden vooralsnog **niet geleverd** met behulp van iDIN:

- Uitgebreidere leeftijdsverificatie (voorlopig alleen de controle of iemand 18 jaar of ouder is);
- Digitaal signeren van documenten;
- Verstrekking van attributen vanuit niet-banken;
- Implementatie van de DISP (Digital Identity Service Provider) rol. Deze is wel voorzien maar wordt nog niet ondersteund.

2.3 iDIN proces

Op de website van de Acceptant start de Gebruiker een iDIN-transactie door allereerst iDIN te selecteren voor inloggen en/of levering van attributen, en vervolgens zijn/haar Issuer uit de selectielijst te kiezen. De Gebruiker wordt vervolgens doorgestuurd naar de vertrouwde omgeving van zijn/haar Issuer waar het identificatie en authenticatie proces plaatsvindt. Na een succesvolle identificatie en authenticatie kan de Gebruiker de aanvraag van de Acceptant goed- of afkeuren. De Gebruiker wordt vervolgens teruggeleid naar de website van de Acceptant die de aangevraagde authenticatie en/of attributen ontvangt.

2.4 iDIN-transactie

Met een iDIN-transactie kan gedelegeerde authenticatie (inloggen), levering van Gebruikersattributen (inclusief leeftijdsverificatie), of een combinatie van beide worden aangevraagd.

2.4.1 Gedelegeerde authenticatie

Bij de start van een iDIN-transactie kan de Acceptant een unieke, Acceptant specifieke aanduiding van de Gebruiker aanvragen, een Bank Identificatie Nummer (BIN). Dit nummer blijft hetzelfde over meerdere aanvragen mits de Gebruiker bij dezelfde bank inlogt. Dit maakt het voor de Acceptant mogelijk om de aangevraagde BIN te koppelen aan een Gebruiker waarvan de BIN al bekend is in het systeem van de Acceptant. Ook kan de Acceptant een

nieuwe account aanmaken (of bestaande account zonder BIN koppelen) om een Gebruiker te koppelen aan een BIN. Bij het goedkeuren van deze aanvraag stemt de Gebruiker in met het inloggen op de website van de Acceptant.

2.4.2 Leveren van Gebruikersattributen

Naast de aanvraag van een BIN kan de Acceptant ook Gebruikersattributen aanvragen. De Gebruiker moet ook voor deze aanvraag altijd expliciete toestemming geven in het domein van zijn/haar bank. Niet alle attributen² kunnen individueel worden aangevraagd, de naam- en adresgegevens. Het geslacht en de geboortedatum (of leeftijdsverificatie) kunnen wel individueel worden aangevraagd. Zie Sectie 5.3.1 en 5.4 voor meer detail. Toestemming vanuit de Gebruiker moet altijd voor alle aangevraagde attributen worden gegeven. De Gebruiker kan dus niet in het domein van zijn/haar Issuer aangeven welke attributen hij/zij wel/niet wil verstrekken. Het is echter voor de Acceptant wel mogelijk, voor het starten van een iDIN-transactie, aan de Gebruiker te vragen welke attributen hij/zij wil verstrekken.

Let op: Doordat de Gebruiker van adres kan wisselen zonder dit aan zijn/haar Issuer door te geven wordt het sterk aangeraden altijd het adres bij de Gebruiker te verifiëren. Ook, in geval van een levering, hoeft het woonadres niet altijd het afleveradres te zijn.

Gebruikersattributen kunnen eenmalig worden aangevraagd zonder dat de sessie aan een specifieke Gebruiker wordt gekoppeld of aan een bestaand Gebruikersaccount. In dit geval ontvangt de Acceptant in plaats van een BIN een tijdelijk ID, gegenereerd door de Issuer enkel voor deze sessie. Als de Acceptant attributen aanvraagt in combinatie met gedelegeerde authenticatie (zie Sectie 2.4.1) ontvangt deze ook een BIN. De Acceptant kan met behulp van de door de Issuer verstrekte attributen en BIN makkelijk een nieuw account aanmaken voor gebruikers.

Let op dat de Gebruiker er altijd op gewezen moet worden dat hij/zij iDIN gaat gebruiken voor het aanmaken van een nieuw Gebruikersaccount. Dit ter voorkoming dat de gebruiker een nieuw account aanmaakt terwijl hij/zij al een bestaand account heeft. In dit geval kan het voor de Acceptant beter zijn het bestaand account te koppelen. Bij het koppelen van een bestaand account aan iDIN is het niet aan te raden om de ontvangen attributen te matchen met de totale database van de Acceptant, omdat gebruikers dezelfde attributen kunnen hebben (bijvoorbeeld naam). Door eerst de Gebruiker te laten inloggen op zijn/haar bestaand account, of een extra unieke identificatie te gebruiken die niet geleverd is door de Issuer bij de koppeling (e.g. gebruikersaccount of emailadres), kan dit worden voorkomen.

² Doordat de BIN op een andere plek in het SAML bericht zit (namelijk als het onderwerp), wordt het in deze context niet beschouwd als een attribuut.

2.5 Acceptant registratie

Als de Acceptant zich registreert voor iDIN verkrijgt deze van zijn Acquirer een `Merchant.MerchantID` en een `Merchant.LegalID` dat geassocieerd is met een `Merchant.Name`. Indien het nodig is krijgt de Acceptant ook een `Merchant.SubID` voor registratie van één of meer `Merchant.TradeName`. Dit komt voor als de Acceptant iDIN services gebruikt onder een andere handelsnaam, of als een DISP deze handelingen uitvoert namens de Acceptant. In het geval van de tussenkomst van een DISP is het gebruik van het `Merchant.SubID` verplicht. Alleen de `Merchant.MerchantID` en `Merchant.SubID` zijn voor de Acceptant relevant bij het uitvoeren van het iDIN protocol, omdat alleen deze twee waarden nodig voor een succesvolle iDIN-transactie. De andere identificatie elementen worden toegevoegd door de Acquirer en worden alleen in het Acquirer – Issuer domein gebruikt.

2.6 Dispuutmanagement

In het geval van een dispuut moet de Issuer de identiteit van de Gebruiker kunnen leveren. Hiervoor dienen de volgende stappen te worden uitgevoerd:

- De Acceptant moet het originele Security Assertion Markup Language (SAML) iDIN bericht dat de identiteit van de Gebruiker bevat aan zijn Acquirer kunnen leveren. Om te garanderen dat de Issuer de versleutelde berichten kan lezen moet de Acceptant de versleutelde Advanced Encryption Standard (AES) sleutels ontsleutelen met zijn private sleutel. De AES sleutels moeten met het originele bericht worden geleverd.
- De Acquirer moet deze informatie doorsturen naar de Issuer, met contact informatie van de Acceptant;
- De Issuer moet het certificaat van het bericht verifiëren door middel van de elektronische handtekening;
- Door de AES sleutels van de Acceptant te gebruiken kan makkelijk worden geverifieerd of deze ook bij het bericht horen;
- Als het bericht authentiek is moet de Issuer de details van het bericht direct leveren aan de Acceptant en/of de Gebruiker. Het leveren van deze details kan alleen worden gedaan als de Gebruiker zijn/haar goedkeuring heeft gegeven;
- Het geven van deze details wordt gedaan via telefoon:
 - De Acquirer moet het telefoonnummer van de Acceptant aan de Issuer geven;
 - De Issuer moet de Acceptant op dit nummer bellen om misbruik te voorkomen.

3 iDIN protocollen

Dit hoofdstuk geeft een algemene beschrijving van de iDx protocollen welke als standaard worden gebruikt voor iDIN.

3.1 Technische basisprincipes

- Alle iDIN processen worden geïnitieerd door de Gebruiker op de website van de Acceptant;
- iDIN gebruikt iDx als berichtenstandaard. Binnen deze standaard wordt het generieke container element gebruikt om SAML 2.0 berichten te inbedden, hierin zit informatie die nodig is voor een iDIN-transactie;
- Gebruikers worden aanhoudend geïdentificeerd met behulp van het Bank Identificatie Nummer (BIN), zie Sectie 5.3.1. Dit nummer wordt gegenereerd door de Issuer en is uniek voor elke combinatie Acceptant – Gebruiker bij die betreffende Issuer;
- Een Gebruiker heeft één identiteit per Issuer, onafhankelijk van het aantal accounts;
- De informatie van de Gebruiker wordt in de berichtgeving versleuteld zodat de Routing Service deze informatie niet kan bekijken.

3.2 iDx protocollen

Er zijn vier protocollen die deel uitmaken van iDIN:

- Het Directory Protocol: dit protocol wordt gebruikt om de meest recente lijst van Issuers (bank van de Gebruiker) op te vragen bij de Routing Service.
- Het Transaction Protocol: dit protocol omvat het volledige iDIN proces van initiatie tot voltooiing.
- Het Status Protocol: dit protocol wordt gebruikt om de status van een iDIN-transactie op te vragen bij de Validation Service (via de Routing Service).
- Het Error Protocol: treedt alleen op als response, en wordt gebruikt in het geval dat er iets fout gaat (error).

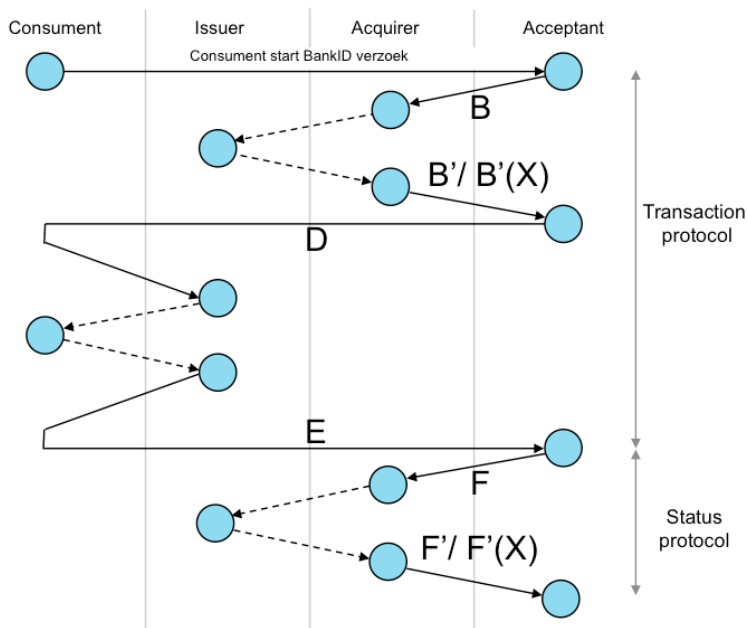
Een specifieke naam en bijbehorende letter is toegewezen aan elk bericht ter identificatie, zoals gespecificeerd in onderstaande tabel:

Bericht	Bericht omschrijving
A	DirectoryReq (Directory Request)
A'	DirectoryRes (Directory Response)
B	AcquirerTrxReq (Transaction Request)
B'	AcquirerTrxRes (Transaction Response)
F	AcquirerStatusReq (Status Request)
F'	AcquirerStatusRes (Status Response)
A' (X) B' (X) F' (X)	AcquirerErrorRes (Error Response)
Redirects:	
D	Acceptant stuurt de Gebruiker door naar de Issuer

E	Issuer stuurt de Gebruiker terug naar de Acceptant
---	--

Tabel 3: Bericht naamgeving en beschrijving

De volgorde van de protocollen is weergegeven in Figuur 2. De gestippelde lijnen geven berichtgeving aan tussen de Acquirer en Issuer en de Issuer en de Gebruiker. Deze berichtgeving vindt plaats buiten het domein van de Acceptant, maar is weergegeven voor redenen van compleetheid. Om als Acceptant authenticatie en/of Gebruikersattributen te verkrijgen moet zowel het Transaction en Status Protocol worden uitgevoerd. Het Directory Protocol is niet weergegeven, omdat het een simpel request/response bericht is tussen de Acceptant en de Acquirer. Een error bericht kan bij elk request ontstaan en heeft de toevoeging (X) achter de response.

**Figuur 2: Transaction, Status en Error protocol**

3.2.1 Directory Protocol

Door middel van het Directory Protocol stuurt de Acceptant een DirectoryReq naar de Routing Service. Het DirectoryReq is een verzoek, in XML formaat, van de Acceptant aan de Routing Service om de lijst met aangesloten Issuers op te leveren. De Routing Service levert deze lijst door middel van het DirectoryRes. De banken die de Acceptant in het DirectoryRes ontvangt toont hij aan de Gebruiker. De Gebruiker kiest uit de aangeleverde lijst zijn/haar bank waar hij bankiert aan het begin van het iDIN proces. Het Directoryprotocol wordt in meer detail beschreven in Hoofdstuk 6.

3.2.2 Transaction Protocol

Door middel van het Transaction Protocol stuurt de Acceptant een AcquirerTrxReq naar de Routing Service, waarin o.a. het ID van de door de Gebruiker gekozen Issuer staat, de benodigde iDIN informatie (welke authenticatie en/of Gebruikersattributen wordt aangevraagd) en andere transactiedetails worden doorgegeven. Dit bericht bevat ook de `merchantReturnURL` die wordt gebruikt om de Gebruiker terug te sturen naar de Acceptant

na het afronden van de iDIN-transactie in het bankdomein (redirect). Nadat de Routing Service het bericht van de Acceptant ontvangen heeft, voegt hij de door de Acceptant geregistreerde details toe en stuurt dit door naar de Validation Service die door de Gebruiker is geselecteerd. De Validation Service antwoordt met een bericht dat onder andere de `issuerAuthenticationURL` bevat. De Routing Service geeft deze `issuerAuthenticationURL` samen met een uniek `Transaction.TransactionID` via de `AcquirerTrxRes` terug aan de Acceptant. Dit is een antwoord op het `AcquirerTrxReq`. De Acceptant dient de Gebruiker nu te redirecten naar de `issuerAuthenticationURL`, een pagina van het internetbankiersysteem van de Issuer. De Gebruiker komt in zijn/haar internetbankieromgeving terecht waar hij de aanvraag van de Acceptant kan autoriseren. De Gebruiker keurt de iDIN aanvraag goed en ontvangt een bevestiging van zijn/haar bank. Daarna redirect de Issuer de Gebruiker terug naar de website van de Acceptant via de `merchantReturnURL`. Het Transaction Protocol en de twee redirects worden uitgebreider behandeld in Hoofdstuk 7.

3.2.2.1 Specifieke eisen voor iDIN mobiel

Het transactie proces op een mobiel apparaat is nagenoeg identiek aan het reguliere Transaction Protocol. Het enige verschil is dat er een redirect plaatsvindt naar een 'landing page' (gebruik makend van `issuerAuthenticationURL`) waar de Gebruiker, gebruik makend van zijn mobiele apparaat, kan kiezen om naar de mobiele webpagina of mobiele app van zijn/haar Issuer te worden gestuurd.

3.2.3 **Status Protocol**

Als het Transactie Protocol succesvol is afgerond kan de Acceptant het Status Protocol initiëren door een `AcquirerStatusReq` te versturen naar de Routing Service. De Routing Service vraagt de status van de iDIN-transactie op bij de betreffende Issuer en retourneert deze status aan de Acceptant. Als de gehele iDIN-transactie foutloos is verlopen, ontvangt de Acceptant de informatie van de Gebruiker in de `AcquirerStatusRes`. In Hoofdstuk 8 is meer informatie te vinden over het Statusprotocol.

3.2.4 **Error Protocol**

Als er een fout (error) plaatsvindt in één van de bovenstaande protocollen, ontvangt de Acceptant in plaats van een normaal response een `AcquirerErrorRes`. Dit kan het geval zijn indien een request een error bevat (`DirectoryReq`, `AcquirerTrxReq`, `AcquirerStatusReq`), of als een fout is opgetreden aan de kant van de Acquirer of Issuer. Deze berichten worden in detail beschreven in Hoofdstuk 9.

3.3 **SAML V2.0**

iDIN gebruikt de iDx standaard voor de berichtgeving. Echter, het generieke container element in het iDx protocol wordt gebruikt om SAML 2.0 te inbedden waarin iDIN specifieke informatie staat. Deze container wordt **alleen gebruikt** in het `AcquirerTrxReq`, `AcquirerStatusRes` en soms in het `AcquirerErrorRes` (afhankelijk van de type fout die optreedt). Voor alle andere berichten wordt de container weggelaten.

4 iDIN bericht formaat

4.1 Algemeen

Dit hoofdstuk bevat een algemene beschrijving van de bericht structuur voor het Directory, Transaction, Status en Error Protocol. De opeenvolgende secties beschrijven de specifieke velden binnen de XML berichten. Een lijst met data elementen en het formaat van deze elementen kan worden gevonden in de data catalogus in Hoofdstuk 5.

De volgende conventies worden gebruikt om aan te geven of een element in een bericht **verplicht** is:

- Ja Het element moet precies één keer aanwezig zijn;
- Ja (1..∞) Het element mag één of meerdere malen aanwezig zijn (onbeperkt);
- Nee Het element mag weggelaten worden of mag maximaal één keer aanwezig zijn;
- Nee (0..∞) Het element mag weggelaten worden of mag één of meerdere malen aanwezig zijn (onbeperkt).

4.2 Karakter set

- In alle iDIN berichten moet de Unicode karakterset worden gebruikt. Alleen de MES-2 (Multilingual European Character Set) wordt ondersteund.
- De codering moet worden gebruikt zoals aangegeven in de HTTP en XML headers: UTF-8 (Unicode Transformation Format).
- Het gebruik van karakters die geen onderdeel zijn van de Unicode karakterset zal niet leiden tot een weigering van een verzoek, maar het karakter kan gewijzigd worden naar een spatie, vraagteken of asterisk.
- Het Byte Order Mark (BOM) mag niet worden gebruikt. De UTF-8 representatie van de BOM is de byte sequentie 0xEF,0xBB,0xBF.

4.3 HTTP

- Alle berichten moeten voldoen aan de HTTP 1.1 standaard, gedefinieerd in RFC 2616 van W3C. Voor meer informatie zie: <http://www.w3.org/Protocols/rfc2616/rfc2616.html>;
- Elk XML request bericht moet worden verzonden binnen het body element van een HTTP POST bericht;
- Elk XML response wordt teruggestuurd binnen het body element van een HTTP 200 OK bericht.

De volgende HTTP header moet worden gebruikt voor alle berichten:

Data element	Verplicht	Uitleg
content-type	Ja	Definieert hoe de content wordt geïnterpreteerd. Moet zijn: text/xml; charset="utf-8"

Tabel 4: HTTP header

4.4 XML header

De volgende XML headers moet worden gebruikt voor alle berichten:

Data element	Verplicht	Uitleg
version	Ja	Moet zijn: "1.0"
encoding	Ja	Moet zijn: "UTF-8"

Tabel 5: XML header

4.5 XML namespaces

iDIN gebruikt de iDx standaard voor de berichtgeving. Echter, het generieke container element in het iDx protocol wordt gebruikt om SAML 2.0 berichten te inbedden waarin iDIN specifieke informatie staat. Er zijn namespace declaraties voor de iDx berichten en enkele namespace declaraties voor het SAML 2.0 bericht.

De namespaces voor alle berichten zijn als volgt:

Namespaces	Namespace declaratie in voorbeeld berichten
Namespace voor de iDIN iDx berichten tussen de Acceptant en Acquirer. Moet zijn: "http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"	xmlns
Namespace voor de XML digitale handtekening syntax. Moet zijn: "http://www.w3.org/2000/09/xmldsig#"	xmlns:ds
Namespace voor schema gerelateerde mark-up. Moet zijn: "http://www.w3.org/2001/XMLSchema-instance"	xmlns:xsi
Namespace voor de SAML 2.0 Assertion welke in de iDx container zit. Moet zijn: "urn:oasis:names:tc:SAML:2.0:assertion"	xmlns:saml
Namespace voor het SAML 2.0 Protocol welke in de iDx container zit. Moet zijn: "urn:oasis:names:tc:SAML:2.0:protocol"	xmlns:samlp
Namespace voor de XML encryptie syntax. Deze namespace is gedeclareerd in het container element in het iDx bericht, en wordt alleen gebruikt in het AcquirerStatusRes bericht voor de versleutelde XML elementen, zie 10.3. Moet zijn: "http://www.w3.org/2001/04/xmenc"	xmlns:xenc

Tabel 6: iDx namespaces

De namespace declaraties kan op elke manier worden uitgevoerd die is toegestaan binnen de XML standaard met de paar uitzonderingen zoals wordt vermeld in Sectie 10.3.

4.6 XML Schema's

Alle berichten moeten worden gevalideerd langs de iDIN, SAML 2.0 en W3C schema's. De schema namen en locaties zijn weergegeven in de onderstaande tabel:

XML schema	Uitleg
idx.merchant-acquirer.1.0.xsd	Schema voor de iDIN iDx berichten tussen de Acceptant en de Acquirer. Zie Appendix D
xmldsig-core-schema.xsd	Schema voor XML signaturen. Beschikbaar op: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd#
saml-schema-assertion-2.0.xsd	Schema voor de SAML 2.0 assertion. Beschikbaar op: http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd

XML schema	Uitleg
	protocol-2.0.xsd
saml-schema-protocol-2.0.xsd	Schema voor het SAML 2.0 protocol. Beschikbaar op: http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd
xenc-schema.xsd	Schema voor de XML encryptie syntax. Beschikbaar op: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd

Tabel 7: XML schema's

5 iDIN data catalogus

Dit hoofdstuk beschrijft de data elementen en ID's die binnen iDIN worden gebruikt. Als eerste wordt in Sectie 5.1 twee attributen beschreven die alle XML berichten moeten hebben in de root. Alle iDx data elementen zijn beschreven in Sectie 5.2. Vervolgens, in Sectie 5.3 worden de iDIN specifieke data elementen beschreven die specifiek voor iDIN worden gebruikt. Sectie 5.4 geeft alle Gebruikersattributen weer.

5.1 iDx attributen

De volgende twee attributen moeten in de root van elke bericht worden gezet zodat de Acquirer weet welk product (iDIN) en versie wordt gebruikt:

Attribuut	Beschrijving	Bericht	Format regels
version	Geeft aan welke versie van iDIN wordt gebruikt	ALLE	Moet zijn: "1.0.0"
productID	Geeft aan welke service wordt gebruikt	ALLE	Moet zijn: "NL:BVN:BankID:1.0"

Tabel 8: iDx attributen

5.2 iDx data elementen

iDIN gebruikt de aanduidingen binnen iDx zoals beschreven in Tabel 9. Als het element door de Acceptant moet worden gegenereerd in elk van de requests (DirectoryReq, AcquirerTrxReq, AcquirerStatusReq), dan wordt dat weergegeven in dikgedrukte letters in de beschrijving.

Naam	Beschrijving	Berichten	Format regel
Acquirer.AcquirerID	Uniek viercijferig nummer van de Acquirer binnen de iDx producten suite.	A', B', F', F'(X)	Viercijferig nummer
Country.countryNames	Bevat de countryNames (namen van landen) in de officiële taal van het land. Deze wordt gebruikt in de presentatie van de Acceptant naar de Gebruiker op de website, zie Sectie 6.4. Bij meerdere officiële talen worden deze met een '/' onderscheiden (e.g. 'België/Belgique')	A'	Max 128 alfanumeriek ³

³ Alfanumeriek wil zeggen dat de toegestane karakters de letters van het alfabet (kleine- en hoofdletters) en alle cijfers (0-9) zijn.

Naam	Beschrijving	Berichten	Format regel
<code>createDateTimeStamp</code>	De tijd dat een bepaald request/response bericht is gemaakt of informatie wanneer een laatste update is gedaan. Kan ook voorkomen als <code>directoryDateTimeStamp</code> , <code>statusDateTimeStamp</code> en <code>transactionCreateDateTimeStamp</code> maar volgt telkens dezelfde format regels. Dit is in meer detail besproken in Hoofdstuk 6-9. Gegenereerd door de Acceptant in request berichten	ALLE	ISO 8601 UTC time format (geen zomertijd) in format YYYY-MM-DDThh:mm:ss.sssZ e.g. 2015-10-01T20:53:12.123Z <ul style="list-style-type: none"> De drie decimalen achter de seconde zijn niet vereist en mogen worden weggelaten door de Acceptant. Berichten vanuit de RS zijn altijd voorzien van drie decimalen YYYY refereert naar het kalenderjaar hh moet 24-uurs notatie zijn, 12-uur notatie mag niet worden gebruikt
<code>Error.consumerMessage</code>	Een Acquirer kan dit veld gebruiken om een gestandaardiseerd bericht te geven dat de Acceptant aan de Gebruiker kan laten zien als er een fout optreedt	A'(X), B'(X), F'(X)	Zie Appendix A: Foutcodes (Error codes)
<code>Error.errorCode</code>	Uniek identificatie nummer voor een fout (error) binnen de iDx standaard	A'(X), B'(X), F'(X)	Zie Appendix A: Foutcodes (Error codes)
<code>Error.errorMessage</code>	Beschrijvende tekst bij <code>Error.errorCode</code>	A'(X), B'(X), F'(X)	Max 128 alfanumeriek Zie Appendix A: Foutcodes (Error codes)
<code>Error.errorDetail</code>	Detail van de error. De bericht genererende partij is vrij de inhoud te bepalen	A'(X), B'(X), F'(X)	Max 256 alfanumeriek
<code>Error.suggestedAction</code>	Suggestie met de bedoeling om het probleem op te lossen. De bericht genererende partij is vrij de inhoud te bepalen	A'(X), B'(X), F'(X)	Max 512 alfanumeriek
<code>issuerAuthenticationURL</code>	Bevat de Issuer authenticatie URL waar de Gebruiker heen wordt gestuurd	B'	Max 512 karakters
<code>Issuer.IssuerID</code>	Unieke aanduiding voor de Issuer	A', B	ISO 9362
<code>Issuer.Name</code>	Gegeven samen bij elke <code>Issuer.IssuerID</code> gebruikt voor de presentatie bij de Acceptant naar de Gebruiker, zie Sectie 6.3	A'	Max 35 alfanumeriek
<code>language</code>	Dit veld maakt het mogelijk de Issuer website of mobiele applicatie weer te geven in de taal van de Gebruiker. In geval van een error kan dit veld worden gebruikt om de <code>Error.consumerMessage</code> in de taal van de Gebruiker weer te geven, zie Hoofdstuk 9 Als een niet bestaande of niet ondersteunde taal wordt gegeven moet de standaard taal van de Issuer worden gebruikt e.g. 'en' voor English, 'nl' voor Nederlands. Gegenereerd door de Acceptant	B	ISO 639-1

Naam	Beschrijving	Berichten	Format regel
<code>Merchant.MerchantID</code>	Dit is het contractnummer voor iDIN. De Acceptant krijgt dit nummer nadat deze zich heeft geregistreerd voor iDIN	A,B,F	10 cijfers Gemaakt van <code>Acquirer.AcquirerID</code> (eerste vier posities) en een uniek nummer van precies zes posities
<code>Merchant.subID</code>	De <code>subID</code> die de Acceptant uniek identificeert met naam en adres. De Acceptant krijgt dit nummer na registratie van iDIN. Een Acceptant kan permissie van de Acquirer vragen om één of meer <code>subIDs</code> te gebruiken. De Acceptant moet deze waarde als 0 invullen of het element compleet weglaten tenzij anders aangegeven door de Acquirer	A,B,F	Max 6 cijfers Nummer van 0 tot en met 999999 waar elke waarde een andere geregistreerde iDIN gebruiker is. De standaard waarde is '0'
<code>merchantReturnURL</code>	URL waar de Gebruiker naartoe moet worden gestuurd na authenticatie of autorisatie van een iDIN-transactie bij de Issuer. Deze hoeft niet per se te beginnen met <code>http://</code> of <code>https://</code> , maar kan ook een app handler zijn e.g. <code>companyname-nl-service://</code> . Zolang het protocol deel maar wordt inbegrepen. De bron achter de URL moet verwijzen naar de website of app van de Acceptant, of een onderdeel daarvan. Gegenereerd door de Acceptant	B	Max 512 karakters
<code>Merchant.X509</code>	Certificaat van de Acceptant. Gebruikt voor herkenning van de Merchant en versleuteling in het domein van de Issuer	B	Base64 encoding
<code>Transaction.entranceCode</code>	Een 'authenticatie identifier' gegenereerd door de Acceptant om de sessie tussen de Acceptant en Acquirer te continueren, zelfs als de bestaande verbinding is verbroken (e.g. cookie verlopen). Dit maakt het de Acceptant mogelijk de Gebruiker te herkennen bij een voltooide iDIN-transactie. Zie Sectie 7.5.1 voor meer informatie. Gegenereerd door de Acceptant	B	Max 40 alfanumeriek Een minimum variatie van 1 miljoen is vereist
<code>Transaction.TransactionID</code>	Uniek 16-cijverig nummer binnen een iDx product. Dit nummer wordt aan een iDIN-transactie toegevoegd door de Acquirer en wordt door de Acceptant ontvangen in een <code>AcquirerTrxRes</code> . Dit wordt gebruikt om een <code>AcquirerStatusReq</code> te koppelen aan een bepaald response	B', F, F' F'(X)	16 cijfers De eerste vier cijfers van het <code>TransactionID</code> zijn gelijk aan het <code>AcquirerID</code>

Naam	Beschrijving	Berichten	Format regel
Transaction.status	Status van de iDIN-transactie: gerelateerd aan of een iDIN-transactie is geauthentiseerd door de Gebruiker	F'	<p>Heeft altijd een van de volgende waarden:</p> <p>Open: Laatste status nog niet bekend. Dit is de initiële status voor alle partijen en iDIN-transacties.</p> <p>Success: De Gebruiker heeft de iDIN-transactie goedgekeurd en de Issuer heeft dit ook herkend.</p> <p>Cancelled: De iDIN-transactie is niet goedgekeurd maar afgebroken door de Gebruiker.</p> <p>Expired: De iDIN-transactie is niet goedgekeurd binnen de vervaltijd <code>BankID.expirationPeriod</code> die door de Acceptant is bepaald of de standaard waarde van <code>BankID.expirationPeriod</code>.</p> <p>Failure: De iDIN-transactie is om onbekende redenen afgekeurd</p>

Tabel 9: iDx data elementen

5.3 iDIN data elementen

iDIN gebruikt specifieke data elementen buiten de iDX standaard zoals beschreven in onderstaande tabel. Als het element door de Acceptant moet worden gegenereerd in één van de requests (DirectoryReq, AcquirerTrxReq of AcquirerStatusReq), dan wordt dat weergegeven in dikgedrukte letters in de beschrijving.

Naam	Beschrijving	Berichten	Format regel
BankID. MerchantReference	Unieke iDIN-transactie referentie gegenereerd door de Acceptant (e.g. voor administratieve doeleinden) Gegenereerd door de Acceptant	B, F', F'(X)	Max 35 text en moet beginnen met een letter (kleine- of hoofdletter)
BankID. expirationPeriod	Tijd waarbinnen de totale iDIN-transactie moet worden voltooid voordat de status is verlopen. Minimaal 60 seconden en maximaal 300 seconden (dit is de standaard waarde mocht dit veld niet zijn ingevuld). Gegenereerd door de Acceptant	B	ISO 8601 e.g. PT300S or PT5M

Naam	Beschrijving	Berichten	Format regel
BankID.LOA	iDIN kan twee 'Level of Assurance' (beveiligingsniveaus) voor authenticatie bieden. De exacte vereiste zal in een separaat document worden gedefinieerd in een later stadium. Voor een request: de minimum vereiste level of assurance Voor een response: de level of assurance waarmee de iDIN-transactie is voltooid. Gegenereerd door de Acceptant	B, F'	Moet zijn: "nl:bvn:bankid:1.0:loa2" of "nl:bvn:bankid:1.0:loa3"
BankID. RequestedServiceID	Het nummer dat gebruikt wordt om een bepaalde set van services van iDIN aan te vragen, zie Sectie 5.3.1 voor meer informatie. Gegenereerd door de Acceptant	B	Integer zoals gespecificeerd in Sectie 5.3.1.
BankID. DeliveredServiceID	Volgt dezelfde structuur als het RequestedServiceID, maar wordt door de Issuer in het teruggestuurde bericht gezet om aan te geven welke aangevraagde attributen daadwerkelijk zijn geleverd volgens de minimale set (zie Sectie 5.5 en Sectie 12.4). Als de Issuer het DeliveredServiceID niet kan achterhalen wordt de waarde '0' gebruikt	F'	Integer zoals gespecificeerd in Sectie 5.3.1.
consumer.bin	BIN is een afkorting voor Bank Identificatie Nummer. Het is een unieke aanduiding voor de Gebruiker en is per Gebruiker-Acceptant-Acquirer combinatie uniek	F'	Max 256 karakters. BIN bevat twee delen: 1) Prefix: Twee-letter land code van de bank (ISO 3166-1) gevolgd door vier-letter (alfabetisch) bank aanduiding (ISO 9362 standaard) 2) Bank specifiek nummer
consumer.transientid	Kan worden aangevraagd in plaats van Consumer.BIN. Geeft aan dat de waarde een transient nummer is en moet als zodanig worden behandeld bij de Acceptant.	F'	Beginnt met de prefix 'TRANS' en is maximaal 256 karakters
Issuer.x509	Gebruikt in de SAML Response binnen het Signature element (zie Sectie 10.6), zodat de Acceptant de handtekening op de Assertion kan verifiëren.	F'	Base64 encoding
Merchant.LegalID	Het Merchant.LegalID is het creditorID van de Acceptant. Dit nummer is gebaseerd op het KvK. Het wordt door de Issuer gebruikt en wordt in de AcquirerStatusRes teruggestuurd om SAML compliance redenen. De Acceptant hoeft dit nummer niet te gebruiken voor het voltooien van een iDIN-transactie.	F'	-

Tabel 10: Specifieke iDIN data elementen

5.3.1 iDIN Requested- en DeliveredServiceID

De iDIN services kunnen worden aangevraagd door de Acceptant. Elke transactie request kan alleen een bepaalde set van ID's of attributen leveren van de Gebruiker, gebaseerd op de waarde van het RequestedServiceID. De teruggestuurde Gebruikersinformatie kan verschillen per Issuer, daarom zijn sommige van de attributen die deel uitmaken van een groep optioneel. De Issuer geeft in het teruggestuurde bericht in het element DeliveredServiceID aan welke attributen volgens de minimale set zijn geleverd (zie Sectie 5.5). In de meeste gevallen zal het DeliveredServiceID overeenkomen met het RequestedServiceID. Echter, het kan voorkomen dat de Issuer niet alles wat gevraagd is kan leveren. In dit geval is het RequestedServiceID niet hetzelfde als het DeliveredServiceID. De afhandeling van deze situatie wordt in meer detail besproken in Sectie 12.4.

Met behulp van het Excel '160529A_ServiceID_Calculator' dat bij deze Implementatie Gids wordt verstrekt kan het ServiceID gemakkelijk worden berekend.

Het Requested- en DeliveredServiceID zijn beide integers (een positief heel getal van 0 – 65536) vertaald van een binair formaat (16 bits). Binnen iDIN zijn maar enkele van de mogelijke waarden van het Requested- en DeliveredServiceID gekoppeld aan een valide aanvraag voor Gebruikersattributen. Figuur 3 geeft de binaire structuur aan van beide ServiceIDs. Het binaire nummer is opgesplitst in verschillende groepen. Deze groepen representeren een bepaalde categorie van attributen die de Acceptant mag aanvragen. Let op dat dit een bit patroon is en geen nummer waardoor de eerste bit links zit in plaats van rechts.

Binary ServiceID =

Category	R	1	R	2	R	3	R	4	R	5	R	6	R	7	R
Binary value	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Figuur 3: Requested- en DeliveredServiceID lay-out

Tabel 11 geeft een overzicht welke bits overeenkomen met welke attributen of ID's. De Gebruikersattributen worden behandeld in Sectie 5.4. Als de Acceptant één of meerdere attributen wilt aanvragen kan deze in de onderstaande tabel kijken voor de correcte binaire waarden. Vervolgens moet de vertaling worden gedaan naar een integere waarde.

Bit number	Categorie	Beschrijving	Waarde
1	Gereserveerd (R)	Gereserveerd voor backwards compatibility	0 (Moet de waarde nul hebben)
3,5,7,11,13, 16	Gereserveerd (R)	Niet toegewezen: gereserveerd voor toekomstige attributen	0 (Moet de waarde nul hebben)
2	Categorie 1: GebruikersID	Geeft aan welk Gebruikers ID wordt aangevraagd / is geleverd	0 Consumer.TransientID 1 Consumer.BIN
4	Categorie 2: Naam	Geeft aan welke naam attributen wordt aangevraagd / is geleverd. Zie Sectie 5.4 voor alle attributen	0 Geen naam attributen 1 Alle naam attributen
6	Categorie 3: Adres	Geeft aan welke adres attributen wordt aangevraagd / is geleverd. Zie Sectie 5.4 voor alle attributen	0 Geen adres attributen 1 Alle adres attributen
8..10	Categorie 4: Leeftijd gerelateerd	Geeft aan welke leeftijdsverificatie wordt aangevraagd / is geleverd. Zie Sectie 5.4 voor alle attributen	000 Geen leeftijdsattribuut 001 18orOlder 010 Gereserveerd 011 Gereserveerd 100 Gereserveerd 101 Gereserveerd 110 Gereserveerd 111 Geboortedatum
12	Categorie 5: Geslacht	Geeft aan of het geslacht wordt aangevraagd / is geleverd. Zie Sectie 5.4 voor alle attributen	0 Geen geslachtattribuut 1 Geslachtattribuut
14	Categorie 6: Telefoon	Geeft aan of het telefoonnummer wordt aangevraagd / is geleverd. Zie Sectie 5.4 voor alle attributen	0 Geen telefoonattribuut 1 Telefoonattribuut
15	Categorie 7: Email	Geeft aan of het emailadres wordt aangevraagd / is geleverd. Zie Sectie 5.4 voor alle attributen	0 Geen emailattribuut 1 Emailattribuut

Tabel 11: Overzicht van binaire waarden van Requested- en DeliveredServiceID

Het RequestedServiceID zit in het SAML request bericht om aan te geven welke attributen de Acceptant aanvraagt. Bijvoorbeeld, als de Acceptant alleen authenticatie wilt doen en de Gebruiker wil inloggen, dan moeten alle binaire waarden nul blijven behalve bit twee, waardoor de waarde van het RequestedServiceID 16384 wordt.

5.4 Gebruikersattributen

De Gebruikersattributen zitten in het SAML 2.0 bericht als resultaat van de aangevraagde service met het BankID.ServiceID. De consumer.bin en consumer.transientid **zijn niet** gedefinieerd als attributen en zitten daarom in een andere plaats binnen het SAML 2.0 bericht. Waar mogelijk worden de attributen ge-format aan de hand van de NEN-ISO 8601 standaard. iDIN kan de volgende Gebruikersattributen leveren:

Nr.	Gebruikersattribuut	Groep ⁴	Beschrijving	Format regel
1.	<code>consumer.deprecatedbin</code>	-	Hetzelfde als BIN maar wordt gebruikt voor continuïteit van het BIN. Dit element kan gebruikt worden als bijvoorbeeld twee Acceptanten fuseren of als, om één of andere reden, de BIN is gereset	Zie <code>consumer.bin</code>
2.	<code>consumer.gender</code>	Kan individueel worden aangevraagd	Geslacht van de Gebruiker	0 (= niet bekend) 1 (= man) 2 (= vrouw) 9 (= niet gespecificeerd)
3.	<code>consumer.legallastname</code>	Naam	Rechtsgeldige achternaam van de Gebruiker zonder prefix. (zie: NEN 1888_2002, p5, "significant deel van de achternaam")	Max200Text (zie: NEN 1888_2002, p10)
4.	<code>consumer.preferredlastname</code>	Naam	Achternaam die de voorkeur van de Gebruiker heeft (analoog tot <code>legallastname</code>)	Max200Text
5.	<code>consumer.partnerlastname</code>	Naam	Achternaam van de geregistreerde partner van de Gebruiker (analoog tot <code>legallastname</code>)	Max200Text
6.	<code>consumer.legallastnameprefix</code>	Naam	Prefix van de rechtsgeldige achternaam (<code>legallastname</code>) van de Gebruiker	Max10Text (zie: NEN 1888_2002, p11)
7.	<code>consumer.preferredlastnameprefix</code>	Naam	Prefix van de achternaam van de Gebruiker die de voorkeur heeft van de Gebruiker (analoog tot <code>legallastnameprefix</code>)	Max10Text
8.	<code>consumer.partnerlastnameprefix</code>	Naam	Prefix van de geregistreerde partner achternaam van de Gebruiker (analoog tot <code>legallastnameprefix</code>)	Max10Text
9.	<code>consumer.initials</code>	Naam	Initialen van de Gebruiker, zoals gedefinieerd bij NEN 1888_2002, p6: "voorletters-n". Alleen de eerste letter van alle voornamen worden teruggestuurd, in hoofdletters en zonder spaties	Max24Text (zie: NEN 1888_2002, p11)
10.	<code>consumer.dateofbirth</code>	Kan individueel worden aangevraagd	Geboortedatum van de Gebruiker	Basis format (CCYYMMDD) zie NEN-ISO 8601 Als de geboorte dag of maand onbekend is zal '00' worden teruggestuurd e.g. 19870400

⁴ Dit zijn de groepen zoals gedefinieerd in Tabel 11. Sommige attributen behoren niet tot een groep en kunnen apart worden aangevraagd en geleverd m.b.v. het ServiceID

Nr.	Gebruikersattribuut	Groep ⁴	Beschrijving	Format regel
11.	consumer. 18orolder	Kan individueel worden aangevraagd	Geeft aan of de Gebruiker ouder is dan 18 jaar	Boolean (true/false) Leeftijdsverificatie als de geboorte dag of maand onbekend is zal worden gebaseerd op basis van de laatste dag van de maand en de laatste maand van het jaar respectievelijk
12.	consumer.street	Adres	Straatnaam van de Gebruiker (van: NEN 5825_2002, p4, "straatnaam") Alleen gebruikt voor Nederlandse adressen	Max43Text (zie: NEN 5825_2002, 5.3.2)
13.	consumer. houseno	Adres	Huisnummer van de Gebruiker (van: NEN 5825_2002, p4, "huisnummer") Alleen gebruikt voor Nederlandse adressen	Max5Numerical (zie: NEN 5825_2002, 5.3.4)
14.	consumer. housenosuf	Adres	Huisnummer toevoeging (van: NEN 5825_2002, p4, "huisnummertoevoeging") Alleen gebruikt voor Nederlandse adressen	Max6Text (from: NEN 5825_2002, 5.3.5)
15.	consumer. addressextra	Adres	Additionele informatie van het adres (van: NEN 5825_2002, p4, "locatieomschrijving") Alleen gebruikt voor Nederlandse adressen	Max70Text (zie: NEN 5825_2002, 5.3.1)
16.	consumer. postalcode	Adres	Postcode van de Gebruiker (van: NEN 5825_2002, p4, "postcode") Alleen gebruikt voor Nederlandse adressen	Cijfer deel: n4 Alfabetisch deel: a2 Bijvoorbeeld: 0000AA (zie: NEN 5825_2002, 5.3.11-12)
17.	consumer.city	Adres	Stad van het adres van de Gebruiker Alleen gebruikt voor Nederlandse adressen	Max24Text
18.	consumer. intaddressline1	Adres	Alleen gebruikt voor niet- Nederlandse adressen. De diversiteit van internationale adressen wordt opgevangen door drie vrije tekst attributen.	Max70Text
19.	consumer. intaddressline2	Adres	Alleen gebruikt voor niet- Nederlandse adressen	Max70Text
20.	consumer. intaddressline3	Adres	Alleen gebruikt voor niet- Nederlandse adressen	Max70Text
21.	consumer.country	Adres	Landcode van het adres van de Gebruiker	2 code ISO 3166-1 (NL = Nederland)

Nr.	Gebruikersattribuut	Groep ⁴	Beschrijving	Format regel
22.	consumer. telephone	Telefoon	Telefoonnummer (mobiel of vast) van de Gebruiker	<p>Issuers streven ernaar alle telefoonnummers volgens de soft format eis terug te sturen</p> <p>Soft format eis</p> <p>Max 20 in lengte, beginnend met een plus gevolgd door alleen getallen. De volgende volgorde wordt gebruikt:</p> <ul style="list-style-type: none"> • '+' • Landcode • Nationaalnummer zonder <u>voorloop nul</u> <p>Voorbeeld: +31612345678 (Mobiel) +31203051900 (Vast)</p> <p>Het telefoonnummer wordt altijd volgens de harde format eis teruggestuurd:</p> <p>Harde format eis</p> <p>Max 20 in lengte, met de volgende toegestane karakters:</p> <ul style="list-style-type: none"> • getallen '0-9' • spatie ' ' • haakjes '()' • plus '+' • minus '-'
23.	consumer.email	Email	Emailadres van de Gebruiker	<p>Max255Text</p> <p>Moet het volgende bevatten:</p> <ul style="list-style-type: none"> • Eén @-symbool • Ten minste een karakter voor het @-symbool • Een punt ergens achter het @-symbool • Ten minste één karakter na de @, en voor de punt • Ten minste één karakter na de @, en na de punt <p>Voorbeeld: X@Y.Z</p>

Tabel 12: Gebruikersattributen

Notities:

- Gebruikersattributen zitten binnen het SAML Attribute element in het SAML 2.0 bericht. Het @Name geeft aan welk Gebruikersattribuut binnen het element Attribute zit. Het @Name heeft altijd de prefix "nl:bvn:bankid:1.0:attribute:" gevolgd door de naam van het Gebruikersattribuut in kleine letters e.g. "nl:bvn:bankid:1.0:attribute:consumer.city";
- Als één van de attributen langer is dan gespecificeerd in de NEN norm dan wordt deze ingekort en het laatste karakter wordt vervangen door een "-" symbool (zie NEN 1888_2002, p14);
- Sommige Gebruikersattributen zijn niet beschikbaar bij alle Issuers e.g. partnerlastname. In dat geval worden deze waarden door de Issuer weggelaten;

Voorbeeld van een SAML Attribute:

```
<Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.dateofbirth">
  <AttributeValue>19850101</AttributeValue>
</Attribute>
```

5.5 Gegarandeerde minimale set van aangevraagde attributen

Het kan voorkomen dat de Issuer niet alle attributen in de aangevraagde attribuutgroepen kan leveren (die de Acceptant heeft aangegeven te willen ontvangen met het `RequestedServiceID`). Om deze reden is er een minimale set attributen per attribuutgroep gedefinieerd die de Issuer moet leveren. Alle individueel aangevraagde attributen (e.g. ID's, leeftijd en geslacht) moet de Issuer leveren op aanvraag. Kan de Issuer hier niet aan voldoen dan krijgt de Acceptant alle attributen vanuit de aanvraag die de Issuer wel heeft. Echter wordt aangegeven in het teruggestuurde bericht m.b.v. het `DeliveredServiceID` en een status code dat niet alle aangevraagde attribuutgroepen voldoen aan de minimale set. Dit wordt in meer detail besproken in Sectie 12.4.

Groep	Minimale set of attributen
Naam	Eén van de drie onderstaande opties:
1	<code>consumer.legallastname</code>
2	<code>consumer.preferredlastname</code>
3	<code>consumer.partnerlastname</code>
Adres	Eén van de vijf onderstaande opties:
1	<code>consumer.postalcode</code> AND <code>consumer.houseno</code>
2	<code>consumer.streetname</code> AND <code>consumer.houseno</code> AND <code>consumer.city</code>
3	<code>consumer.postalcode</code> AND <code>consumer.addressextra</code> (voor adressen die geen huisnummer hebben e.g. a 'woonboot')
4	<code>consumer.streetname</code> AND <code>consumer.addressextra</code> AND <code>consumer.city</code> (voor adressen die geen huisnummer hebben e.g. a 'woonboot')
5	<code>consumer.intaddressline1</code> AND <code>consumer.country</code> (voor internationale adressen)

Tabel 13: Minimale set attributen per attribuutgroep

6 iDIN Directory Protocol

6.1 General

Het Directoryprotocol heeft als doel de Acceptant de actuele lijst met aangesloten Issuers te laten ophalen bij zijn Routing Service, zodat deze lijst getoond kan worden aan de Gebruiker. Het Directory Protocol zorgt ervoor dat wijzigingen in de Issuer lijst automatisch in de keuzelijsten van de Acceptanten worden doorgevoerd.

Het is **niet toegestaan het Directory Protocol voor elke iDIN-transactie met een Gebruiker uit te voeren**. Aangezien de lijst met Issuers slechts sporadisch wijzigt is het voldoende eenmaal per dag de lijst op te halen en op basis van de `directoryDateTimestamp` te bepalen of de lijst gewijzigd is. Deze datum specificeert wanneer de Acquirer als laatste de Issuer lijst heeft geüpdatet. De lijst dient, indien deze anders is dan de huidige lijst, opgeslagen te worden en voor alle volgende iDIN-transacties gebruikt te worden. Routing Services informeren normaliter alle Acceptanten (bijv. via e-mail) over wijzigingen in de Issuer lijst. Het Directory Protocol moet minstens eenmaal per week uitgevoerd worden.

Het Directory Protocol bestaat (zoals ook het Transactie Protocol en Status Protocol) uit een HTTP POST request van de Acceptant naar de Routing Service waarop hij een HTTP response ontvangt. Het DirectoryReq wordt verstuurd naar de URL, die door de Routing Service voor dit doel aan de Acceptant is verstrekt. Dit kan een andere URL zijn dan voor het AcquirerTrxReq en AcquirerStatusReq geldt, maar de Routing Service kan hier ook dezelfde URL voor gebruiken.

De Routing Service controleert de authenticiteit van het bericht van de Acceptant door de meegestuurde handtekening te controleren. De Routing Service moet hiervoor beschikken over het gebruikte certificaat van de Acceptant met daarin de publieke sleutel. De manier waarop de Acceptant het publieke deel van het certificaat met de Routing Service deelt verschilt per bank.

In Hoofdstuk 10 staat meer informatie over het controleren van authenticiteit en beveiliging. Appendix B toont een voorbeeld bericht van een DirectoryReq en een DirectoryRes.

6.2 Directory Request (DirectoryReq)

Het DirectoryReq bevat een XML bericht dat naar de Routing Service wordt verstuurd door middel van een HTTP POST. Alle elementen en attributen van het DirectoryReq zijn weergegeven in Tabel 14. De elementen en attributen zijn in het Engels, het element Merchant (Acceptant in Nederlands) bevat informatie van de Acceptant.

Element/attribuut	Verplicht	Inhoud
DirectoryReq	Ja	Root van het bericht
@version	Ja	Moet zijn: "1.0.0"
@productID	Ja	Moet zijn: "NL:BVN:BankID:1.0"
+ createDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop dit bericht is gegenereerd
+ Merchant	Ja	Bevat Merchant sub-elementen
++ MerchantID	Ja	Bevat <code>Merchant.MerchantID</code> dat gegeven is aan de Acceptant door de Acquirer

Element/attribuut	Verplicht	Inhoud
++ subID	Ja	Bevat <code>Merchant.subID</code> dat gegeven is aan de Acceptant door de Acquirer
+ Signature	Ja	Bevat alle Signature sub-elementen (digitale handtekening). Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6

Tabel 14: Elementen/attributen van het DirectoryReq

6.3 Directory Response (DirectoryRes)

De Acceptant ontvangt een DirectoryRes als een response van het DirectoryReq (als er geen fout optreedt). Dit XML bericht bevat paarsgewijs `Issuer.Name` met bijbehorende `Issuer.IssuerID`. Issuers zijn gegroepeerd per land. De Issuers uit het land van herkomst van de Gebruiker mag aan de top in de lijst van de Issuers worden gepresenteerd, de rest is alfabetisch gesorteerd, eerst bij land, dan bij naam. Alle elementen en attributen van het DirectoryReq zijn weergegeven in Tabel 15.

Element/attribuut	Verplicht	Inhoud
DirectoryRes	Ja	Root van het bericht
@version	Ja	Moet zijn: "1.0.0"
@productID	Ja	Moet zijn: "NL:BVN:BankID:1.0"
+ createDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop dit response bericht is gegenereerd
+ Acquirer	Ja	Bevat Acquirer sub-elementen
++ AcquirerID	Ja	Bevat <code>Acquirer.AcquirerID</code>
+ Directory	Ja	Bevat alle Directory sub-elementen
++ directoryDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop de lijst met Issuers als laatste is geüpdatet door de Acquirer
++ Country	Ja (1..∞)	Bevat alle Country sub-elementen
+++ countryNames	Ja (1..∞)	Bevat alle <code>Country.countryNames</code>
+++ Issuer	Ja (1..∞)	Bevat paarsgewijs <code>issuerID</code> en <code>issuerName</code> sub-elementen
++++ issuerID	Ja	Bevat <code>Issuer.IssuerID</code>
++++ issuerName	Ja	Bevat <code>Issuer.Name</code>
+ Signature	Ja	Bevat alle Signature sub-elementen (digitale handtekening). Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6

Tabel 15: Elementen/attributen van het DirectoryRes

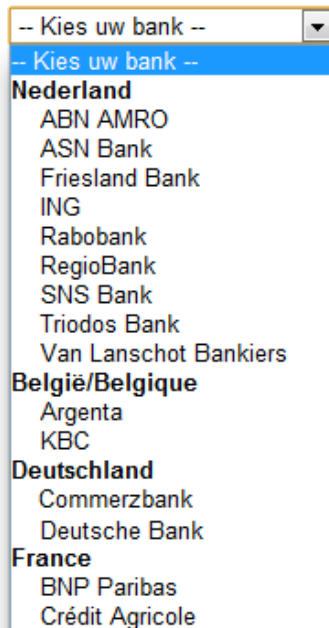
6.4 Presentatie van de Issuer selectielijst

Om ervoor te zorgen dat een iDIN-transactie voor de Gebruiker altijd op dezelfde wijze verloopt, dienen alle Acceptant de volgende presentatie aan te houden:

Alle Issuers uit de DirectoryRes moeten worden getoond in een "dropdown listbox". Het eerste element van deze lijst is "Kies uw bank..."; dit is ook het element dat voorgeselecteerd is. Vervolgens wordt de landsnaam van het voorkeursland van de Acceptant getoond (ofwel het land waar de Acceptant is gevestigd ofwel het land waar de Gebruiker (vermoedelijk) vandaan komt). De namen van alle Issuers uit het voorkeursland worden vervolgens getoond in afzonderlijke elementen, in dezelfde (alfabetische) volgorde als gehanteerd in de DirectoryRes. Daarna worden de namen van andere landen en de

bijbehorende Issuers getoond, ook weer in dezelfde (alfabetische) volgorde als in de DirectoryRes. De Acceptant moet een foutmelding genereren indien de Gebruiker een van de elementen “Kies uw bank...” of een landsnaam kiest.

Het is aan te bevelen het HTML “value” veld van de items in de listbox in te stellen op de Issuer bankID (BIC) van de betreffende Issuer, omdat deze nodig is in vervolgberichten. Een voorbeeld van een Issuer selectielijst is te vinden in onderstaande figuur:



Figuur 4: Voorbeeld van een (open) dropdown list box welke de Issuer selectielijst laat zien

Het is de Acceptant niet toegestaan om zelf Issuers (tijdelijk) uit de Issuer selectielijst te verwijderen c.q. uit te grijzen.

Indien de Acceptant middels het iDIN Notification System (Centraal Meldpunt voor iDIN banken om onbeschikbaarheid te melden) of via vanuit de Acquirer ontvangen foutmeldingen heeft vastgesteld dat een bepaalde Validation Service niet beschikbaar is, kan de Acceptant een melding tonen aan de Gebruiker op zijn website dat de betreffende Issuer op dat moment niet beschikbaar is. Een dergelijke melding tonen is dus toegestaan; het uitgrijzen of tijdelijk verwijderen van de Issuer uit de Issuer selectielijst is dat niet.

7 iDIN Transaction Protocol

7.1 General

Het Transactie Protocol initieert het berichtenverkeer van het daadwerkelijke iDIN proces. Nadat de Gebruiker voor iDIN als identificatiemethode heeft gekozen en zijn Issuer heeft geselecteerd, stuurt de Acceptant een Transaction Request naar zijn Routing Service. Binnen de standaard wordt dit bericht aangeduid als het AcquirerTrxReq. De Routing Service beantwoordt het AcquirerTrxReq met een AcquirerTrxRes. Deze bevat onder andere de `issuerAuthenticationURL` waarheen de browser van de Gebruiker moet worden geredirect om de Gebruiker de iDIN-transactie te laten autoriseren.

Het Transaction Protocol bestaat uit een HTTP POST request van de Acceptant naar de Routing Service waarop hij een HTTP response ontvangt. Het AcquirerTrxReq wordt verstuurd naar de URL, die door de Routing Service voor dit doel aan de Acceptant is verstrekt. Dit kan een andere URL zijn die wordt gebruikt voor het DirectoryReq en AcquirerStatusReq, maar de Routing Service kan hier ook dezelfde URL voor gebruiken.

De Routing Service controleert de authenticiteit van het bericht van de Acceptant door de meegestuurde handtekening te controleren. De Routing Service moet hiervoor beschikken over het gebruikte certificaat van de Acceptant met daarin de publieke sleutel. De manier waarop de Acceptant het publieke deel van het certificaat met de Routing Service deelt verschilt per bank.

In Hoofdstuk 10 staat meer informatie over het controleren van authenticiteit en de beveiliging. Appendix B toont een voorbeeld bericht van een AcquirerTrxReq en een AcquirerTrxRes.

7.2 Transaction Request (AcquirerTrxReq)

Het XML bericht dat door de Acceptant naar de Routing Service wordt verstuurd bevat de elementen en attributen zoals weergegeven in Tabel 16. iDIN product specifieke informatie (SAML 2.0 bericht) zit binnen het generieke container element in het AcquirerTrxReq en in de vorm van een SAML 2.0 AuthnRequest, zie Tabel 17.

Element/attribuut	Verplicht	Inhoud
AcquirerTrxReq	Ja	Root van het bericht
@version	Ja	Moet zijn: "1.0.0"
@productID	Ja	Moet zijn: "NL:BVN:BankID:1.0"
createDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop dit bericht is gegenereerd
+ Issuer	Ja	Bevat Issuer sub-elementen
++ IssuerID	Ja	Bevat <code>Issuer.IssuerID</code>
+ Merchant	Ja	Bevat alle Merchant sub-elementen
++ merchantID	Ja	Bevat <code>Merchant.MerchantID</code>
++ subID	Ja	Bevat <code>Merchant.subID</code>
++ merchantReturnURL	Ja	Bevat <code>Merchant.returnURL</code>
+ Transaction	Ja	Bevat alle Transaction sub-elementen
++ expirationPeriod	No	Bevat <code>expirationPeriod</code>
++ language	Ja	Bevat <code>language</code> van de Gebruiker

Element/attribuut	Verplicht	Inhoud
++ entranceCode	Ja	Bevat entranceCode
++ container	Ja	Bevat het SAML 2.0 AuthnRequest bericht, zie Tabel 17
+ Signature	Ja	Bevat alle Signature sub-elementen (digitale handtekening). Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6

Tabel 16: Elementen/attributen van het AcquirerTrxReq

Zoals eerder vermeld zit het SAML 2.0 AuthnRequest bericht, dat product specifieke (iDIN) informatie bevat, binnen het generieke container element. Het AuthnRequest bericht is een gestandaardiseerd bericht, en bevat elementen die niet worden gebruikt binnen iDIN, dit is aangegeven in de tabel. Alle elementen en attributen in de container van het AcquirerTrxReq zijn weergegeven in Tabel 17.

Element/attribuut (in het container element)	Verplicht	Inhoud
AuthnRequest	Ja	Root van het bericht (gezien vanuit het container element)
@ID	Ja	Bevat BankID.MerchantReference
@Version	Ja	Moet zijn: "2.0"
@IssueInstant	Ja	Bevat DateTime (tijd) waarop dit bericht is gegenereerd
@Destination		Zal niet aanwezig zijn
@Consent	Nee	Mag aanwezig zijn. Wordt genegeerd. Welk toestemming ook wordt gevraagd door de Acceptant, de Issuer is altijd verantwoordelijk voor het verkrijgen van toestemming van de Gebruiker
@ForceAuthn	Nee	Mag aanwezig zijn. Moet zijn: "true" (als aanwezig). Expliciete authenticatie wordt geforceerd voor elke iDIN service
@IsPassive	Nee	Mag aanwezig zijn. Moet zijn: "false" (als aanwezig). Omdat expliciete authenticatie wordt geforceerd kan de Issuer niet passief zijn
@ProtocolBinding	Ja	Moet zijn: "nl:bvn:bankid:1.0:protocol:iDx"
@AssertionConsumer-ServiceIndex		Zal niet aanwezig zijn
@AssertionConsumer-ServiceURL	Ja	Bevat Merchant.MerchantReturnURL
@AttributeConsuming-ServiceIndex	Ja	Bevat BankID.RequestedServiceID
@ProviderName		Zal niet aanwezig zijn
+ Issuer	Ja	Bevat Merchant.MerchantID
+ @NameQualifier		Zal niet aanwezig zijn
+ @SPNameQualifier		Zal niet aanwezig zijn
+ @Format		Zal niet aanwezig zijn
+ @SPPProviderID		Zal niet aanwezig zijn
+ Signature		Zal niet aanwezig zijn. De digitale handtekening zal worden geplaatst op iDx niveau (Signature element in Tabel 16)
+ Subject		Zal niet aanwezig zijn
+ NameIDPolicy		Zal niet aanwezig zijn
+ Conditions	Nee	Mag aanwezig zijn
+ RequestedAuthnContext	Ja	Bevat RequestedAuthnContext sub-elementen
++ @Comparison	Ja	Moet zijn: "minimum"

Element/attribuut (in het container element)	Verplicht	Inhoud
++ AuthnContextClassRef	Ja	Bevat BankID.LOA
++ AuthnContextDeclRef		Zal niet aanwezig zijn
+ Scoping	Nee	Mag aanwezig zijn

Tabel 17: Elementen/attributen in de container van het AcquirerTrxReq

7.3 Transaction Response (AcquirerTrxRes)

Als alles goed gaat reageert de Routing Service op het AcquirerTrxReq met een AcquirerTrxRes. Tabel 18 geeft alle elementen en attributen weer van het AcquirerTrxRes bericht. Het AcquirerTrxRes heeft geen container element, er is dus geen SAML 2.0 bericht in dit response (die is anders indien er sprake is van een Error Response, zie Hoofdstuk 9).

Element/attribuut	Verplicht	Inhoud
AcquirerTrxRes	Ja	Root van het bericht
@version	Ja	Moet zijn: "1.0.0"
@productID	Ja	Moet zijn: "NL:BVN:BankID:1.0"
+ createDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop dit bericht is gegenereerd
+ Acquirer	Ja	Bevat Acquirer sub-elementen
++ AcquirerID	Ja	Bevat <code>Acquirer.AcquirerID</code>
+ Issuer	Ja	Bevat Issuer sub-elementen
++ IssuerAuthenticationURL	Ja	Bevat <code>issuerAuthenticationURL</code>
+ Transaction	Ja	Bevat Transaction sub-elementen
++ transactionID	Ja	Bevat <code>Transaction.TransactionID</code>
++ transactionCreateDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop de transactie als eerste is geregistreerd bij de Routing Service. Dit kan door de Routing Service, Validation Service en Acceptant worden gebruikt voor reporting
+ Signature	Ja	Bevat alle Signature sub-elementen (digitale handtekening). Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6

Tabel 18: Elementen/attributen van het AcquirerTrxRes

7.4 Errors (fouten) bij het uitvoeren van het Transactie Protocol

Bij de uitvoering van het Transactie Protocol kunnen een aantal foutsituaties optreden. Deze kunnen te maken hebben met onbeschikbaarheid binnen uw omgeving (Acceptant), of de omgeving van de Routing Service/Validation Service.

De volgende situaties kunnen zich voordoen:

1. Het initiëren van de iDIN-transactie lukt niet.
2. U ontvangt binnen de ingestelde time-out periode een foutbericht (bericht B'(X)) van uw Routing Service.
3. U ontvangt geen bericht binnen de ingestelde time-out periode.

In alle bovenstaande gevallen, kan het Transactie Protocol niet succesvol worden uitgevoerd. Dit betekent dat het niet mogelijk is om een iDIN authenticatie en/of aanvraag Gebruikersattributen uit te voeren. Foutafhandeling wordt in meer detail besproken in Hoofdstuk 9.

7.5 Redirect naar de online bankiersomgeving (`issuerAuthenticationURL`)

Na het ontvangen van de `AcquirerTrxRes` dient de Acceptant de Gebruiker door te sturen (redirect) naar de `issuerAuthenticationURL` van de gekozen bank, zoals die in de `AcquirerTrxRes` is ontvangen. Als de pagina is opgebouwd met behulp van HTML-frames dan zullen deze door de Issuer verwijderd worden ("frame-busting"). Na terugkomst op de website van de Acceptant (middels de `merchantReturnURL`) zal de Acceptant ervoor moeten zorgen dat de frames weer opgebouwd worden voor het tonen van de iDIN bevestiging.

7.5.1 Specifieke eisen aan iDIN mobiel: Redirect naar de Issuer (geen in-app browser)

De Acceptant is verantwoordelijk voor het redirecten van de Gebruiker, vanaf de (mobiele) webpagina of applicatie van de Acceptant, naar de Issuer, die de Gebruiker heeft geselecteerd. Als het bij het doorsturen niet mogelijk is de Gebruiker in dezelfde webpagina te houden moet dit worden gecommuniceerd aan de Gebruiker (bijvoorbeeld: "*U zal nu worden doorgestuurd naar de applicatie of (mobiele) website van uw bank*").

In het geval dat een iDIN-transactie wordt geïnitieerd vanuit de mobiele applicatie van de Acceptant is het niet toegestaan de Issuer schermen te tonen in de applicatie omgeving van de Acceptant middels 'in-app-browsing' (web-view). Alle stappen van de transactiefLOW, tot aan de redirect terug naar de Acceptant, moeten doorlopen worden in een omgeving die door de Gebruiker vertrouwd wordt. Dit kan de voorkeurs webbrowsers zijn, die door de Gebruiker gekozen is, of de mobiele applicatie van de Issuer. De `issuerAuthenticationURL` moet daarom altijd voor uitvoering aan het mobiele OS worden aangeboden. Gedurende de opgestarte transactiefLOW mag het voor de Gebruiker niet mogelijk zijn een andere iDIN-transactie te initiëren in de applicatie van de Acceptant.

Relevante details over deze redirect van de Acceptant naar het mobiele kanaal van de Issuer:

- De Issuer bepaalt welke Gebruikers worden omgeleid naar welk kanaal. Sommige Issuers kunnen bijvoorbeeld gebruikers van een tablet op dezelfde manier behandelen als gebruikers van een smartphone, terwijl andere Issuers tablet gebruikers zullen behandelen als reguliere PC gebruikers;
- De Acceptant mag niet interfereren met de redirect. De `issuerAuthenticationURL` moet ook gebruikt worden voor mobiele iDIN-transacties;
- Als de Issuer iDIN mobiel heeft geïntegreerd in haar mobiel bankieren applicatie zal de Gebruiker, op de 'landing page' van de Issuer, de mogelijkheid geboden worden de mobiel bankieren applicatie te openen of verder te gaan via de (mobiele) webpagina. Op de 'landing page' kan de Gebruiker ook de mogelijkheid geboden worden de nieuwste versie van de mobiel bankieren applicatie te downloaden voor het geval deze nog niet geïnstalleerd is op het mobiele apparaat van de Gebruiker.

7.6 Redirect naar de Acceptant omgeving (merchantReturnURL)

Nadat de Gebruiker de interactie met de Issuer heeft doorlopen, biedt de Issuer hem een 'Doorgaan' knop aan die hem moet terugleiden naar de website van de Acceptant, middels de merchantReturnURL die de Acceptant heeft opgegeven in de AcquirerTrxReq.

Achter deze URL worden twee parameters als GET parameters meegegeven: de entranceCode (zie Sectie 7.2), met als GET parameter naam 'ec' en de Transaction.TransactionID (zie Sectie 7.3), met als GET parameter naam 'trxid'. Het is ook mogelijk voor de Acceptant om andere extra parameters toe te voegen. Als de Acceptant bijvoorbeeld als merchantReturnURL opgeeft:

```
http://www.webwinkel.nl/betaalafhandeling?productsoort=elektronica
```

kan de uiteindelijke URL er bijvoorbeeld uitzien als:

```
http://www.webwinkel.nl/betaalafhandeling?productsoort=elektronica&trxid=0010123456789012&ec=4hd7TD9wRn76w6gGwGFDgdL7jEtb
```

Het veld entranceCode dient een unieke waarde te bevatten, om "sniffing" van de berichtuitwisseling tegen te gaan. Kwaadwillenden kunnen door het gebruik van steeds dezelfde entranceCode de gegevens uit de merchantReturnURL onderscheppen, en hier misbruik van maken. Vandaar dat het gebruik van unieke waarden voor de entranceCode van groot belang is.

Let op dat een Gebruiker niet altijd gebruik zal maken van de knop die door de Issuer wordt aangeboden om terug te keren naar de omgeving van de Acceptant. Let ook op dat in uitzonderlijke gevallen de Issuer mogelijk niet in staat is de Transaction.TransactionID te vinden in zijn systemen of er andere storingen optreden, die het onmogelijk maken om de Gebruiker terug te leiden naar de Acceptant. In alle andere gevallen wordt de Gebruiker terug geleid met de complete URL, inclusief parameters zoals hierboven beschreven ongeacht de eindstatus van de iDIN-transactie ('success', 'cancelled', 'expired'). De Acceptant moet vervolgens het Status Protocol gebruiken (zie het volgende hoofdstuk) om de status van de iDIN-transactie vast te stellen.

7.6.1 Eisen voor iDIN mobiel: redirect naar de omgeving van de Acceptant

Nadat de Gebruiker geauthentiseerd is door de Issuer in ofwel de mobiele ofwel het reguliere kanaal, en de iDIN authenticatie/leeftijdsverificatie/verkrijgen van attributen door de Gebruiker is goedgekeurd, zal hij/zij worden terug geleid naar de Acceptant door middel van de merchantReturnURL. De merchantReturnURL begint normaalgesproken met 'https' en dit zorgt ervoor dat de Gebruiker terug wordt geleid naar een webpagina van de browser op het mobiele apparaat. Als de Gebruiker het iDIN proces geïnitieerd heeft vanaf de mobiele applicatie van de Acceptant kan de merchantReturnURL beginnen met de app-handler van de Acceptant, die de Gebruiker doorstuurt naar de applicatie van de Acceptant. Een app-handler is een mechanisme dat ervoor zorgt dat vanuit de ene applicatie (van de Issuer) een andere applicatie gestart wordt en er een bepaalde actie uitgevoerd wordt. Een Acceptant app-handler kan bijvoorbeeld starten met 'nl.companyname.idin://' en hiermee wordt de Acceptant applicatie geopend.

Let op: de merchantReturnURL moet altijd verwijzen naar een webpagina of applicatie van de Acceptant zelf (of een derde partij die handelt namens de Acceptant).

7.7 Fouten tijdens het uitvoeren van de redirect naar de Issuer, het goedkeuren van de iDIN authenticatie en/of de redirect naar de omgeving van de Acceptant

Bij het uitvoeren van de redirect naar de internetbankiersomgeving (Issuer), het uitvoeren van de iDIN-transactie bij de Issuer en/of de redirect terug naar uw (Acceptant-) omgeving kunnen de volgende foutsituaties zich voordoen:

- De bankpagina is onbereikbaar, waardoor de Gebruiker de iDIN-transactie niet kan goedkeuren, maar ook niet op de juiste manier kan worden teruggeleid naar uw bevestigingspagina;
- De bankpagina is wel bereikbaar maar de Gebruiker kan (na het goedkeuren van de iDIN-transactie, of het annuleren van het proces) niet op de juiste manier worden teruggeleid naar uw bevestigingspagina.

In beide situaties kan de Gebruiker (als gevolg van een storing) dus niet op de normale manier terugkeren naar uw bevestigingspagina. De Gebruiker kan in dat geval bijvoorbeeld via de 'back' knop van zijn browser of door de URL in te tikken terugkomen op uw website. Vanwege de korte geldigheid van de Assertion (30 seconden), is het voor de Merchant aan te raden om een nieuw iDIN-transactie verzoek naar de Acquirer te sturen. De restricties op het aanvragen van de status zijn zo dat de Acceptant **alleen** een status verzoek mag doen op het moment dat de Gebruiker succesvol is teruggekeerd naar de website van de Acceptant via de meegestuurde `merchantReturnURL`, zie Sectie 8.5.

7.8 Vier scenario's voor het afronden van het mobiele iDIN proces

Om een overzicht te geven van alle mogelijke processtappen en belangrijke opmerkingen met betrekking tot mobiele iDIN processen, zijn er vier verschillende scenario's gespecificeerd. Er zijn vier verschillende scenario's omdat de Issuer, de Acceptant of beiden gebruik kunnen maken van een (mobiele) webpagina of een mobiele applicatie.

Omdat deze scenario's (kunnen) verschillen van de reguliere (niet-mobiele) iDIN processen, zullen zij worden toegelicht in de volgende secties.

Sectie	Acceptant	Issuer
Sectie 7.8.1	(Mobiele) webpagina	(Mobiele) webpagina
Sectie 7.8.2	(Mobiele) webpagina	Mobiel bankieren applicatie
Sectie 7.8.3	Mobiele applicatie	(Mobiele) webpagina
Sectie 7.8.4	Mobiele applicatie	Mobiel bankieren applicatie

Tabel 19: Verschillende scenario's voor de mobiele iDIN processen

7.8.1 Gebruiker wordt doorgestuurd van de (mobiele) webpagina van de Acceptant naar de (mobiele) webpagina van de Issuer

Dit is een iDIN mobiel scenario, dat vrijwel identiek is aan het reguliere iDIN proces. Daarom zijn er ook geen specifieke opmerkingen voor het gebruik in een mobiele setting. Dit scenario is wel opgenomen in dit document voor redenen van compleetheid. De Gebruiker start het iDIN proces op de (mobiele) webpagina van de Acceptant en doorloopt de volgende stappen:

Stap	Beschrijving	Opmerkingen
1	De Gebruiker selecteert iDIN als methode voor authenticatie, afgeven van Gebruikersattributen of leeftijdsverificatie	
2	De Gebruiker selecteert zijn/haar Issuer	
3	De Gebruiker wordt doorgestuurd naar de Issuer van zijn/haar keuze	
4	De Issuer presenteert de 'landing page' aan de Gebruiker met daarin de optie de iDIN-transactie af te ronden in de Issuer's mobiel bankieren applicatie of in de (mobiele) webpagina van de Issuer	
5	De Gebruiker selecteert de (mobiele) webpagina	
6	De Gebruiker wordt doorgestuurd naar de (mobiele) webpagina van de Issuer waar hij/zij kan inloggen en het iDIN verzoek kan goedkeuren. Nadat de iDIN-transactie is afgerond wordt het resultaat van de iDIN-transactie getoond aan de Gebruiker door de Issuer	
7	De Gebruiker wordt teruggeleid door de Issuer naar de webpagina van de Acceptant. Hiervoor wordt gebruik gemaakt van de merchantReturnURL die meegegeven is door de Acceptant	De merchantReturnURL begint normaal gesproken met https:// en bevat twee parameters (entranceCode en Transaction.TransactionID) die gebruikt kunnen worden voor de correcte identificatie van de Gebruiker als deze teruggeleid is naar de Acceptant
8	De Acceptant laat het resultaat van de iDIN-transactie (authenticatie / afgeven van Gebruikersattributen) zien aan de Gebruiker.	

Tabel 20: Scenario: Redirect van (mobiele) webpagina van de Acceptant naar de Issuer's (mobiele) webpagina

7.8.2 Gebruiker wordt doorgestuurd van de (mobiele) webpagina van de Acceptant naar de Issuer's mobiel bankieren applicatie

De Gebruiker start de iDIN-transactie op de (mobiele) webpagina van de Acceptant en doorloopt de volgende stappen:

Stap	Beschrijving	Opmerking
1	De Gebruiker selecteert iDIN als methode voor authenticatie, afgeven van Gebruikersattributen of leeftijdsverificatie	
2	De Gebruiker selecteert zijn/haar Issuer	
3	De Gebruiker wordt doorgestuurd naar de Issuer van zijn/haar keuze	
4	De Issuer presenteert de 'landing page' aan de Gebruiker met daarin de optie de iDIN-transactie af te ronden in de Issuer's mobiel bankieren applicatie of in de (mobiele) webpagina van de Issuer	
5	De Gebruiker selecteert de mobiel bankieren applicatie	
6	De Gebruiker wordt doorgestuurd naar de mobiel bankieren applicatie van de Issuer waar hij/zij kan inloggen en het iDIN verzoek kan goedkeuren. Nadat de iDIN-transactie is afgerond wordt het resultaat	

Stap	Beschrijving	Opmerking
	van de iDIN-transactie getoond aan de Gebruiker door de Issuer	
7	De Gebruiker wordt teruggeleid door de Issuer naar de webpagina van de Acceptant. Hiervoor wordt gebruik gemaakt van de <code>merchantReturnURL</code> die meegegeven is door de Acceptant	<p>Aangezien de iDIN-transactie plaatsvindt in de mobiel bankieren applicatie van de Issuer, buiten de webbrowser setting, kan het zijn dat de browser sessie verloren gaat. Dit betekent dat de Acceptant niet in staat is de Gebruiker te herkennen aan de hand van de browser sessie.</p> <p>Daarnaast wordt de <code>merchantReturnURL</code>, bij het terugleiden van de Gebruiker van de Issuer mobiel bankieren applicatie naar de Acceptant, afgehandeld door het Operating System (OS) van het mobiele apparaat. Het OS kiest de als standaard ingestelde webbrowser voor de afhandeling van deze URL. Als de iDIN-transactie was gestart in een andere, niet standaard ingestelde webbrowser, gaat deze originele browser sessie verloren.</p> <p>De <code>merchantReturnURL</code> begint normaal gesproken met <code>https://</code> en bevat twee parameters (<code>entranceCode</code> en <code>Transaction.TransactionID</code>) die gebruikt kunnen worden voor de correcte identificatie van de Gebruiker als deze terug geleid is naar de Acceptant</p>
8	De Acceptant laat het resultaat van de iDIN-transactie (authenticatie / afgeven van Gebruikersattributen) zien aan de Gebruiker.	

Tabel 21: Scenario: Redirect van de (mobiele) webpagina van de Acceptant naar de Issuer's mobiele bankier applicatie

7.8.3 Gebruiker wordt doorgestuurd van de mobiele applicatie van de Acceptant naar de Issuer's (mobiele) webpagina

De Gebruiker start de iDIN-transactie in de applicatie van de Acceptant en doorloopt de volgende stappen:

Stap	Beschrijving	Opmerking
1	De Gebruiker selecteert iDIN als methode voor authenticatie, afgeven van Gebruikersattributen of leeftijdsverificatie	
2	De Gebruiker selecteert zijn/haar Issuer	
3	De Gebruiker wordt doorgestuurd naar de Issuer van zijn/haar keuze	Het is verplicht voor de Acceptant om het Operating System (OS) van het mobiele apparaat de <code>issuerAuthenticationURL</code> te laten afhandelen. Zie Sectie 7.5.1 voor meer informatie
4	De Issuer presenteert de 'landing page' aan de Gebruiker met daarin de optie de iDIN-transactie af te ronden in de Issuer's mobiel bankieren applicatie of in de (mobiele) webpagina van de Issuer	
5	De Gebruiker selecteert de (mobiele) webpagina van de Issuer.	
6	De Gebruiker wordt doorgestuurd naar de (mobiele) webpagina van de Issuer waar hij/zij kan inloggen en het iDIN verzoek kan goedkeuren. Nadat de iDIN-transactie is afgerond wordt het resultaat van de iDIN-transactie getoond aan de Gebruiker door	

	de Issuer	
7	De Gebruiker wordt teruggeleid door de Issuer naar de mobiele applicatie van de Acceptant. Hiervoor wordt gebruik gemaakt van de <code>merchantReturnURL</code> die meegegeven is door de Acceptant	De <code>merchantReturnURL</code> bevat een app handler en twee parameters (<code>entranceCode</code> en <code>Transaction.TransactionID</code>) die gebruikt kunnen worden voor de correcte identificatie van de Gebruiker als deze teruggeleid is naar de Acceptant, zie Sectie 7.6
8	De Acceptant laat het resultaat van de iDIN-transactie (authenticatie / afgeven van Gebruikersattributen) zien aan de Gebruiker.	

Tabel 22: Scenario: Redirect van de mobiele applicatie van de Acceptant naar de Issuer's (mobiele) webpagina

7.8.4 Gebruiker wordt doorgestuurd van de applicatie van de Acceptant naar de Issuer's mobiel bankieren applicatie

De Gebruiker start de iDIN-transactie in de applicatie van de Acceptant en doorloopt de volgende stappen:

Stap	Beschrijving	Opmerking
1	De Gebruiker selecteert iDIN als methode voor authenticatie, afgeven van Gebruikersattributen of leeftijdsverificatie	
2	De Gebruiker selecteert zijn/haar Issuer	
3	De Gebruiker wordt doorgestuurd naar de Issuer van zijn/haar keuze	Het is verplicht voor de Acceptant om het Operating System (OS) van het mobiele apparaat de <code>issuerAuthenticationURL</code> te laten afhandelen. Zie Sectie 7.5.1 voor meer informatie
4	De Issuer presenteert de 'landing page' aan de Gebruiker met daarin de optie de iDIN-transactie af te ronden in de Issuer's mobiel bankieren applicatie of in de (mobiele) webpagina van de Issuer	
5	De Gebruiker selecteert de mobiel bankieren applicatie	
6	De Gebruiker wordt doorgestuurd naar de mobiel bankieren applicatie van de Issuer waar hij/zij kan inloggen en het iDIN verzoek kan goedkeuren. Nadat de iDIN-transactie is afgerond wordt het resultaat van de iDIN-transactie getoond aan de Gebruiker door de Issuer	
7	De Gebruiker wordt teruggeleid door de Issuer naar de mobiele applicatie van de Acceptant. Hiervoor wordt gebruik gemaakt van de <code>merchantReturnURL</code> die is meegegeven door de Acceptant	De <code>merchantReturnURL</code> bevat een applicatie handler en twee parameters (<code>entranceCode</code> en <code>Transaction.TransactionID</code>) die gebruikt kunnen worden voor de correcte identificatie van de Gebruiker als deze is teruggeleid naar de Acceptant, zie Sectie 7.6
8	De Acceptant laat het resultaat van de iDIN-transactie (authenticatie / afgeven van Gebruikersattributen) zien aan de Gebruiker.	

Tabel 23: Scenario: Redirect van de mobiele applicatie van de Acceptant naar de Issuer's mobiele bankier applicatie

7.9 Verwerkingssnelheid en time-out van transactieberichten

De verwerkingssnelheid van de systemen van de Issuer en de Routing Service heeft een directe invloed op de gebruikerservaring van de Gebruiker. Daarom schrijft iDIN een streeftijd en een time-out periode voor de transactie responseberichten voor. De voor een Acceptant relevante streeftijd en time-out periode hebben betrekking op de communicatie met zijn iDIN Routing Service:

Communicatie	Streeftijd (in seconden)	Time-out (in seconden)
AcquirerTrxReq → AcquirerTrxRes	2.0	7.6

Tabel 24: Verwerkingssnelheid eisen (voor het 95ste percentiel⁵)

De streeftijd is de tijd (in seconden) waarbinnen normaal gesproken een AcquirerTrxRes bericht door de Acceptant ontvangen zou moeten zijn na verzending van een AcquirerTrxReq. De time-out is de tijdsduur waarna de Acceptant geen response meer mag verwachten (waarschijnlijk is er een fout opgetreden) en passende actie moet ondernemen (bijvoorbeeld het tonen van een toepasselijke foutmelding aan de Gebruiker).

⁵ 95th percentiel is een statistische term om aan te geven dat 95% van de geteste transacties binnen deze tijd moet zijn afgehandeld

8 iDIN Status Protocol

8.1 Algemeen

Om na te gaan of een transactie is geslaagd, start de Acceptant het Status Protocol door het versturen van een Status Request naar de Routing Service. In de iDIN Standaard wordt dit bericht aangeduid als het AcquirerStatusReq.

Om onnodige belasting van systemen te voorkomen, mogen statusverzoeken niet ongelimiteerd worden gedaan; zie Sectie 8.5 voor meer details over wat is toegestaan. Het statusprotocol mag alleen gestart worden bij terugkeer van de Gebruiker op de website van de Acceptant (na de redirect door de Issuer).

Het Status Protocol bestaat uit een HTTP POST request van de Acceptant naar de Routing Service waarop hij een HTTP response ontvangt. Het AcquirerStatusReq wordt verstuurd naar de URL, die door de Routing Service voor dit doel aan de Acceptant is verstrekt. Dit kan een andere URL zijn dan die wordt gebruikt voor het DirectoryReq en AcquirerTrxReq, maar de Routing Service kan hier ook dezelfde URL voor gebruiken.

De Routing Service controleert de authenticiteit van het bericht van de Acceptant door de meegestuurde handtekening te controleren. De Routing Service moet hiervoor beschikken over het gebruikte certificaat van de Acceptant met daarin de publieke sleutel. De manier waarop de Acceptant het publieke deel van het certificaat met de Routing Service deelt verschilt per bank.

In Hoofdstuk 10 staat meer informatie over het controleren van authenticiteit en beveiliging. Appendix B toont een voorbeeld bericht van een AcquirerStatusReq en een AcquirerStatusRes.

8.2 Status Request (AcquirerStatusReq)

Tabel 25 bevat alle elementen en attributen in het AcquirerStatusReq XML bericht. Het AcquirerStatusReq heeft geen container met daarin een SAML 2.0 bericht.

Element/attribuut	Verplicht	Inhoud
AcquirerStatusReq	Ja	Root van het bericht
@version	Ja	Moet zijn: "1.0.0"
@productID	Ja	Moet zijn: "NL:BVN:BankID:1.0"
+ createDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop dit bericht is gegenereerd
+ Merchant	Ja	Bevat Merchant sub-elementen
++ merchantID	Ja	Bevat <code>Merchant.MerchantID</code>
++ subID	Ja	Bevat <code>Merchant.subID</code>
+ Transaction	Ja	Bevat Transaction sub-elementen
++ transactionID	Ja	Bevat <code>Transaction.TransactionID</code>
+ Signature	Ja	Bevat alle Signature sub-elementen (digitale handtekening). Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6

Tabel 25: Elementen/attributen van het AcquirerStatusReq

8.3 Status Response (AcquirerStatusRes)

De Routing Service reageert met een AcquirerStatusRes als alles goed verloopt. Dit bericht heeft een SAML 2.0 Response binnen het generieke container element dat is gecreëerd door de Issuer en is doorgestuurd via de Routing Service als de transactie is goedgekeurd door de Gebruiker. Het AcquirerStatusRes bevat de elementen en attributen zoals weergegeven in Tabel 26. Dit bericht communiceert de status van de transactie (gerelateerd aan `Transaction.TransactionID` dat was meegestuurd in het AcquirerStatusReq) aan de Acceptant. Alleen als de status 'Success' is, is er een container element in het AcquirerStatusRes. De elementen en attributen in deze container, als deze aanwezig is, zijn weergegeven in Tabel 27.

Element/attribuut	Verplicht	Inhoud
AcquirerStatusRes	Ja	Root van het bericht
@version	Ja	Moet zijn: "1.0.0"
@productID	Ja	Moet zijn: "NL:BVN:BankID:1.0"
+ createDateTimeStamp	Ja	Bevat <code>DateTime</code> (tijd) waarop de Status Response is gegenereerd
+ Acquirer	Ja	Bevat Acquirer sub-elementen
++ acquirerID	Ja	Bevat <code>Acquirer.AcquirerID</code>
+ Transaction	Ja	Bevat Transaction sub-elementen
++ transactionID	Ja	Bevat <code>Transaction.TransactionID</code>
++ status	Ja	Bevat <code>Transaction.status</code>
++ statusDateTimeStamp	Nee	Alleen aanwezig als: <code>Transaction.status</code> = "Success", "Cancelled", "Expired" of "Failure" (Niet aanwezig als <code>Transaction.status</code> = "Open" of "Pending"). Bevat <code>DateTime</code> (tijd) waarop de Issuer de <code>Transaction.status</code> heeft bepaald voor deze transactie
++ container	Nee	Alleen aanwezig als: <code>Transaction.status</code> = "Success" Bevat het SAML 2.0 Response bericht, zie Tabel 27
+ Signature	Ja	Bevat alle Signature sub-elementen (digitale handtekening). Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6

Tabel 26: Elementen/attributen van het AcquirerStatusRes

Zoals vermeld zit het SAML 2.0 Response bericht in de generieke container als de status van de transactie 'Success' is. Ook het SAML 2.0 Response bericht is een gestandaardiseerd bericht wat elementen en attributen bevat die niet in de iDIN omgeving worden gebruikt. Het is aan de Validation Service en Routing Service om deze waardes weg te laten, daarom zijn deze niet weergegeven in Tabel 27.

Element/attribuut	Verplicht	Inhoud
Response	Ja	Root van dit bericht (wat in de container zit van de AcquirerStatusRes)
@ID	Ja	Bevat <code>Transaction.TransactionID</code> met een prefix van 'RES-'
@InResponseTo	Ja	Bevat <code>Merchant.MerchantReference</code>
@version	Ja	Moet zijn: "2.0"
@IssueInstant	Ja	Bevat <code>DateTime</code> (tijd) waarop dit SAML 2.0 Response bericht is gegenereerd
+ Issuer	Ja	Bevat <code>Acquirer.AcquirerID</code> Let op: Issuer in deze context is gereserveerde SAML terminologie en is

Element/attribuut	Verplicht	Inhoud
		niet gerelateerd aan de iDIN Issuer
+ Status	Ja	Bevat de status sub-elementen
++ StatusCode	Ja	Bevat de eerste status code
+++ @Value	Ja	Moet zijn: "urn:oasis:names:tc:SAML:2.0:status:Success"
+++ StatusCode	Ja	Bevat de tweede status code
++++ @Value	Ja	Heeft één van onderstaande waardes: "urn:nl:bvn:bankid:1.0:status:Success" of, als niet alle attributen zijn geleverd volgens de minimale set: "urn:nl:bvn:bankid:1.0:status:IncompleteAttributeSet" Het gebruik van deze status code wordt in meer detail besproken in Sectie 12.4
+ Assertion	Ja	Bevat Assertion sub-elementen
+ @Version	Ja	Moet zijn: "2.0"
+ @ID	Ja	Bevat een unieke ID gecreëerd door de Validation Service
+ @IssueInstant	Ja	Bevat <code>DateTime</code> (tijd) waarop dit Assertion element is gegenereerd
++ Issuer	Ja	Bevat <code>Issuer.IssuerID</code>
++ Signature	Ja	Bevat de Signature sub-elementen voor de SAML handtekening gecreëerd door de Validation Service. Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6. Sectie 10.2.1 gaat specifiek over de digitale handtekening die hier moet staan
++ Subject	Ja	Bevat Subject sub-elementen
+++ EncryptedID	Ja	Bevat de versleutelde element <code>NameID</code> waarbinnen <code>consumer.bin</code> of <code>consumer.transientid</code> zit. Zie Sectie 10.3
++ Conditions	Ja	Bevat Conditions sub-elementen
++ @NotBefore	Ja	Bevat <code>DateTime</code> (tijd) waarop het <code>AcquirerTrxReq</code> is gegenereerd
++ @NotOnOrAfter	Ja	Bevat <code>DateTime</code> (tijd) 30 seconden na de <code>Assertion@IssueInstant</code>
+++ AudienceRestriction	Ja	Bevat AudienceRestriction sub-elementen
++++ Audience	Ja	Bevat het <code>Merchant.LegalID</code>
++++ OneTimeUse	Ja	Is aanwezig maar wordt leeg gelaten
++ AuthnStatement	Ja	Bevat AuthnStatement sub-elementen
++ @AuthnInstant	Ja	Bevat <code>DateTime</code> (tijd) waarop de authenticatie plaats heeft gevonden
+++ AuthnContext	Ja	Bevat AuthnContext sub-elementen
++++ AuthnContextClassRef	Ja	Bevat <code>BankID.LOA</code>
++++ Authentication-Authority	Ja	Bevat <code>Issuer.IssuerID</code>
++ AttributeStatement	Ja	Bevat AttributeStatement sub-elementen
+++ Attribute	Ja	Een unencrypted Attribute
++++@Name	Ja	Moet zijn: "urn:nl:bvn:bankid:1.0:bankid.deliveredserviceid"
++++AttributeValue	Ja	Bevat <code>BankID.DeliveredServiceID</code>
+++ EncryptedAttribute	Nee (0..∞)	Bevat de versleutelde Gebruikersattributen. Eén voor elk van de Gebruikersattributen. Zie Sectie 10.3 voor meer informatie

Tabel 27: Elementen/attributen in de container van het `AcquirerStatusRes`

8.4 Foutsituaties tijdens het uitvoeren van het Statusprotocol

Bij het navragen van de iDIN status door middel van het Status Protocol kunnen foutsituaties optreden waardoor de status van de iDIN-transactie op dat moment niet door u kan worden opgehaald. De eindstatus van de iDIN-transactie kan op dat moment dus niet aan de Gebruiker worden getoond. Aanbevolen berichten die aan de Gebruiker getoond kunnen worden, worden later in dit document gespecificeerd.

8.5 Restricties met betrekking tot AcquirerStatusReq

Een Acceptant mag alleen een AcquirerStatusReq initiëren als:

- De Gebruiker is doorgestuurd naar de Acceptant (E) als onderdeel van het Transaction Protocol.

De SAML Assertion welke uitgegeven is door de Issuer is geldig voor een periode van 30 seconden. Van het moment dat de Gebruiker succesvol is doorgestuurd naar de website van de Acceptant, totdat de Assertion verloopt, kan de Acceptant een status request doen. Meerdere status verzoeken zijn alleen toegestaan als er niet is gereageerd binnen de afgesproken time-out periode. De Acceptant mag, nadat deze een status response heeft ontvangen met een verlopen Assertion, geen status verzoeken doen voor deze specifieke iDIN-transactie, zie Hoofdstuk 9 voor meer informatie.

Acceptanten die het Status Request vaker uitvoeren dan de bovenstaande beschreven limitatie, zullen worden beschouwd als een uitvoerder van ongewenste acties, omdat als ze dit doen er onnodige belasting aan de kant van de Routing Service en Validation Service ontstaat.

8.6 Verwerkingssnelheid en time-out van statusberichten

De verwerkingssnelheid van de systemen van de Issuer en de Routing service heeft een directe invloed op de gebruikerservaring van de Gebruiker. Daarom schrijft iDIN een streeftijd en een time-out periode voor de status responseberichten voor. De voor een Acceptant relevante streeftijd en time-out periode hebben betrekking op de communicatie met zijn iDIN Routing Service:

Communicatie	Streeftijd (in seconden)	Time-out (in seconden)
AcquirerStatusReq → AcquirerStatusRes	2.0	7.6

Tabel 28: Verwerkingssnelheid eisen (voor het 95ste percentiel⁶)

De streeftijd is de tijd (in seconden) waarbinnen normaal gesproken een AcquirerStatusRes bericht ontvangen zou moeten zijn door de Acceptant na verzending van een AcquirerStatusReq. De time-out is de tijdsduur waarna de Acceptant geen response meer mag verwachten (waarschijnlijk is er een fout opgetreden) en passende actie moet ondernemen (bijvoorbeeld het tonen van een toepasselijke foutmelding aan de Gebruiker).

⁶ 95th percentiel is een statistische term om aan te geven dat 95% van de geteste transacties binnen deze tijd moet zijn afgehandeld.

9 Foutafhandeling (Error Handling)

9.1 Algemeen

Als er iets fout gaat bij de verwerking van een DirectoryReq, AcquirerTrxReq of AcquirerStatusReq, bijvoorbeeld omdat het request een foutieve waarde bevat, wordt er geen normale response teruggegeven. In plaats daarvan komt er een AcquirerErrorRes bericht terug. Dit bericht heeft dezelfde hoofdstructuur als aangegeven in Tabel 29. De container is alleen in sommige gevallen aanwezig als er een fout optreedt na het versturen van een AcquirerStatusReq.

Appendix B geeft een voorbeeld bericht van een AcquirerErrorRes.

9.2 Error Response (AcquirerErrorRes)

In plaats van een regulier response (DirectoryRes, AcquirerTrxRes or AcquirerStatusRes) kan de Routing Service een AcquirerErrorRes sturen als er een fout is opgetreden in de ontvangst of verwerking van het request, of als er foutieve waarden in het bericht zijn die niet zijn toegestaan of overeenkomen zijn met de iDx/iDIN standaard. Alle elementen en attributen in het AcquirerErrorRes zijn weergegeven in Tabel 29, en de elementen en attributen in de container zijn weergegeven in Tabel 30.

Element/attribuut	Verplicht	Inhoud
AcquirerErrorRes	Ja	Root van het bericht
@version	Ja	Moet zijn: "1.0.0"
@productID	Ja	Moet zijn: "NL:BVN:BankID:1.0"
+ createDateTimeStamp	Ja	Bevat DateTime (tijd) waarop dit Error Response bericht is gegenereerd
+ Error	Ja	Bevat Error sub-elementen
++ errorCode	Ja	Bevat Error.errorCode zie Appendix A
++ errorMessage	Ja	Bevat Error.errorMessage zie Appendix A
++ errorDetail	Nee	Bevat Error.errorDetail
++ suggestedAction	Nee	Bevat Error.suggestedAction
++ consumerMessage	Nee	Bevat Error.consumerMessage zie Appendix A
++ container	Nee	Alleen aanwezig in sommige gevallen na het sturen van een AcquirerStatusReq: Bevat het SAML 2.0 Response bericht, zie Tabel 30
+ Signature	Ja	Bevat alle Signature sub-elementen (digitale handtekening). Hoofdstuk 10 bevat een gedetailleerde beschrijving van de digitale handtekening. Alle sub-elementen zijn weergegeven in Sectie 10.6

Tabel 29: Elementen/attributen van het AcquirerErrorRes

Element/attribuut	Verplicht	Inhoud
Response	Nee	Root van het bericht binnen de container en is alleen aanwezig in sommige gevallen in het AcquirerErrorRes
@ID	Ja	Bevat Transaction.TransactionID met prefix 'RES-'
@InResponseTo	Ja	Bevat BankID.MerchantReference
@Version	Ja	Moet zijn: "2.0"
@IssueInstant	Ja	Bevat DateTime (tijd) waarop dit Response bericht is gegenereerd
+ Issuer	Ja	Bevat Acquirer.AcquirerID

Element/attribuut	Verplicht	Inhoud
+ Status	Ja	Bevat Status sub-elementen
++ StatusCode	Ja	Bevat StatusCode sub-elementen.
++ @Value	Ja	Bevat de waarde van de eerste SAML status code welke gelijk is aan: "urn:oasis:names:tc:SAML:2.0:status:Requester" wat betekent dat er niet kan worden voldaan aan het verzoek
++ StatusCode	Ja	Bevat StatusCode sub-elementen
+++ @Value	Ja	Bevat een valide SAML status code één niveau dieper. Zie Appendix A voor het gebruik van de status codes
++ StatusMessage	Ja	Bevat een hint welk veld de fout heeft veroorzaakt

Tabel 30: Elementen/attributen in de container van het AcquirerErrorRes

9.3 Onbeschikbaarheid

Het kan zijn dat één van de Issuers tijdelijk niet beschikbaar is. Aanvragen voor die Issuer zullen dan een AcquirerErrorRes opleveren (Sectie 9.2). Nadat een Routing Service heeft vastgesteld dat er sprake is van een onbeschikbaarheid zal hij dit doorgeven aan de betreffende Issuer. Een Acceptant heeft dus nooit rechtstreeks contact met een Issuer.

Het kan voorkomen dat de Routing Service zelf tijdelijk niet beschikbaar is. In dit geval kunnen er geen iDIN aanvragen worden verwerkt (tenzij de Acceptant meer dan één Routing Service heeft) en levert ieder bericht een AcquirerErrorRes op of een time-out.

Ook kan het voorkomen dat uw return-webpagina niet goed functioneert.

In alle drie bovenstaande gevallen adviseren wij u een nette foutmelding te tonen aan de Gebruiker.

10 Beveiliging en certificaten

10.1 Algemene principes van certificaten

Bij asymmetrische encryptie wordt gebruik gemaakt van twee sleutels: een publieke en een private sleutel. De publieke sleutel is gekoppeld aan een certificaat en mag aan iedereen bekend worden gemaakt, de private sleutel moet door de eigenaar strikt geheim worden gehouden. Door bijzondere wiskundige eigenschappen van het private deel en het publieke deel van een certificaat, kan een stuk tekst dat versleuteld (encrypted) is met de publieke sleutel ontsleuteld worden met de private sleutel en vice versa. De RSA sleutels moeten 2048 bits lang zijn. Het is niet mogelijk een tekst te ontsleutelen (decrypted) met dezelfde publieke sleutel als waarmee deze versleuteld is.

Deze bijzondere eigenschappen maken twee toepassingen van certificaten mogelijk:

1. Versleutelen van een bericht. Door een bericht te versleutelen met de publieke sleutel van de ontvanger is de informatie alleen te lezen door de ontvanger (die de private sleutel, die nodig is om te ontsleutelen, als enige kent).
2. Signeren (digitaal ondertekenen) van een bericht. Door (de hash van) een bericht te versleutelen met de private sleutel van de verzender kan de ontvanger (door een succesvolle ontsleuteling met de publieke sleutel van de verzender) vaststellen dat het bericht daadwerkelijk van de verzender komt (authenticiteit) en dat de inhoud van het bericht niet door derden is aangepast (integriteit).

De binnen iDIN gebruikte enkelzijdige Transport Layer Security (TLS) verbinding tussen Acceptant en Routing Service is gebaseerd op de eerste toepassing. Deze TLS verbinding gebruikt 128 bits encryptie waarbij de Routing Service een servercertificaat gebruikt. Acceptanten dienen TLS versie 1.2 of hoger te gebruiken. Oudere versies van TLS zullen in de nabije toekomst niet meer worden ondersteund.

iDIN legt geen eisen op aan de communicatie tussen Acceptant en de Gebruiker. Deze kan al dan niet via TLS verlopen. Acceptanten worden echter aangeraden om altijd TLS te gebruiken voor de authenticatiepagina's van hun website. Binnen iDIN wordt ook gebruik gemaakt van de tweede toepassing, het elektronisch tekenen van een bericht om de authenticiteit, integriteit en onweerlegbaarheid te waarborgen van alle berichten. Doordat bijvoorbeeld de AcquirerStatusRes getekend wordt door de Routing Service kan de Acceptant de iDIN-transactiebevestiging op echtheid controleren.

10.2 Signeren van iDIN berichten

Alle berichten die tussen de Acceptant en Routing service worden verzonden (DirectoryReq, AcquirerTrxReq en AcquirerStatusReq) moeten worden gesigneerd door de Acceptant. Berichten worden gesigneerd volgens de standaard "XML Signature Syntax and Processing (2nd Edition) W3C Recommendation" van 10 Juni 2008⁷, met de volgende instellingen en restricties:

⁷ <http://www.w3.org/TR/xmldsig-core/>

- Het volledige XML bericht⁸ moet worden gesigneerd;
- Om de digest voor het volledige bericht te kunnen genereren moet het exclusive canonicalisatie algoritme⁹ worden toegepast;
- Om de waarde van de digitale handtekening te kunnen genereren moet het exclusive canonicalisatie algoritme¹⁰ worden toegepast;
- De syntax voor een "enveloped signature"¹¹ moet gebruikt worden. Voor dit doel moet de handtekening zelf uit het XML bericht worden verwijderd volgens het standaard transformatieproces;
- Voor hashing moet het SHA256¹² algoritme worden gebruikt.
- Voor digitale handtekening doeleinden moet het RSAWithSHA256¹³ algoritme gebruikt worden. RSA sleutels moeten 2.048 bits lang zijn.
- De publieke sleutel moet gerefereerd worden aan de hand van een fingerprint van een X.509 certificaat. De fingerprint wordt berekend op basis van de volgende formule HEX(SHA-1(DER certificaat))¹⁴.

Let op: Volgens de standaard Base64 specificaties mogen line breaks worden toegevoegd na iedere 76 karakters door gebruik te maken van CR/LF¹⁵.

In het algemeen hoeft een Acceptant geen diepgaande kennis van RSA te hebben, omdat er voor de meeste (web)programmeertalen libraries bestaan die XML Digital Signature functies implementeren. Het wordt sterk aanbevolen hiervan gebruik te maken.

Standaard functionaliteit voor het aanmaken en verifiëren van RSAWithSHA256 elektronische handtekeningen is voor de veelgebruikte softwareplatformen in elk geval beschikbaar vanaf de volgende versies en hoger:

- PHP 5.5
- Microsoft .NET versie 3.5 sp1
- Java 1.6 u18.

Deze functionaliteit is mogelijkwerwijs ook beschikbaar in eerdere versies van genoemde platformen en voor andere platformen (Python, Ruby en anderen).

Voor iDIN zijn Software Libraries ontwikkeld in .NET, PHP en Java. Neem contact op met uw Acquirer voor meer informatie betreffende deze Software Libraries.

Voor het aanmaken van een publieke en private sleutel zie Sectie 10.5.

⁸ XML Signature referentie tot het gesigneerde info URI wordt leeg gelaten. Zie voorbeeld bericht in APPENDIX B

⁹ <http://www.w3.org/2001/10/xml-exc-c14n>

¹⁰ <http://www.w3.org/2001/10/xml-exc-c14n>

¹¹ <http://www.w3.org/TR/xmldsig-core/#sec-EnvelopedSignature>

¹² <http://www.w3.org/2001/04/xmldsig-core#sha256>

¹³ <http://www.w3.org/TR/2002/REC-xmldsig-core-20021210/#sec-SHA256>

¹⁴ Zie voorbeeldberichten in APPENDIX B

¹⁵ <http://tools.ietf.org/html/rfc2045#section-6.8>

10.2.1 Signeren van de SAML 2.0 Assertion

Naast de reguliere digitale ondertekening van het totale XML bericht, tekent de Validation Service de SAML 2.0 Assertion apart. Deze Assertion wordt doorgestuurd naar de Acceptant via de Routing Service in het AcquirerStatusRes (alleen als de `Transaction.status` 'Success' is). Deze digitale handtekening van de SAML 2.0 Assertion heeft dezelfde instellingen en restricties zoals genoemd in de vorige sectie behalve voor het volgende:

- In plaats van een fingerprint te gebruiken om te refereren naar het certificaat van de Issuer wordt het **hele certificaat toegevoegd**. Het `KeyName` element wordt vervangen door een `X509Data` element waarin een `X509Certificate` element zit wat het volledige certificaat van de Validation Service bevat, zie Tabel 32. Het `X509SubjectName` element mag worden toegevoegd in het `X509Data` element. Andere elementen van `KeyInfo` zullen niet worden gebruikt. Dit is gedaan zodat de Acceptant, die geen relatie heeft met de Validation Service, toch toegang heeft tot het certificaat van de Validation Service om de digitale handtekening te valideren en de attributen te ontsleutelen;
- Het attribuut `Reference@URI` van de Signature verwijst naar `@ID` van de Assertion;
- Acceptanten zullen alleen SAML 2.0 berichten vertrouwen en verwerken die zijn gesignd met een geldig certificaat van de Validation Service uitgegeven onder de vertrouwde iDIN Issuers.

10.3 SAML EncryptedID en EncryptedAttribute

Voor privacy redenen worden de Gebruikersattributen versleuteld, zodat de Routing Service geen toegang heeft tot leesbare data. Let op dat het voor de Acceptant is toegestaan een ander certificaat te gebruiken voor het signeren van de berichten, als wordt gebruikt voor het ontsleutelen van de attributen. Voor de versleuteling van het EncryptedID en EncryptedAttribute element binnen de SAML 2.0 Assertion gelden de volgende eisen:

- Versleuteling van de Gebruikersattributen wordt gedaan met 256 bit AES sleutels;
 - Deze versleuteling wordt uitgevoerd met het <http://www.w3.org/2001/04/xmlenc#aes256-cbc> algoritme;
 - Standaard XML padding wordt toegepast¹⁶
- De Validation Service genereert een nieuwe AES sleutel voor elk van de EncryptedAttributes en EncryptedID elementen;
 - De AES sleutels worden versleuteld met de publieke sleutel van de Acceptant;
 - Versleuteling van de AES sleutels wordt uitgevoerd met een RSA algoritme in combinatie met OAEP: <http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p>;
- De versleutelde EncryptedAttributes en EncryptedID elementen bevatten alle relevante namespace declaraties;
- `xsi:type` definities mogen worden toegevoegd door de Issuer in het `AttributeValue` element e.g. `<saml:AttributeValue xsi:type="xs:int">`.

¹⁶ <http://www.w3.org/TR/xmlenc-core/#sec-Alg-Block>

Het NameID element bevat of de Consumer.BIN of de Consumer.TransientID en is in zijn totaliteit versleuteld (voor de bijbehorende namespaces zie Tabel 6). Een voorbeeld van de versleuteling van een NameID waarin een Consumer.BIN zit is hieronder weergegeven:

```
<saml:NameID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">%Consumer.BIN%</saml:NameID>
```

Versleuteling van dit NameID element resulteert in de onderstaande XML code. De %-tekens geven aan welke waarde binnen de elementen moet staan. Het EncryptedKey element, dat de versleutelde AES sleutel bevat, zit ingebed binnen het EncryptedData element.

```
<saml:EncryptedID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <xenc:EncryptedKey Recipient=%Merchant.LegalID%>
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        </xenc:EncryptionMethod>
        <xenc:CipherData>
          <xenc:CipherValue>%AESKey_Encrypted_With_Public_Key_Merchant%</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedKey>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>%NameID_Encrypted_With_AESKey%</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</saml:EncryptedID>
```

Op dezelfde manier kunnen de Gebruikersattributen worden versleuteld. Het hier onderstaande voorbeeld laat zien hoe de consumer.dateofbirth is versleuteld. Afhankelijk van de vraag van de Acceptant zijn er nul, één of meerdere EncryptedAttribute elementen aanwezig in de SAML 2.0 Assertion.

```
<saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  Name="urn:n1:bvn:bankid:1.0:consumer.dateofbirth">
  <saml:AttributeValue>19850101</saml:AttributeValue>
</saml:Attribute>
```

Het Attribute wat consumer.dateofbirth bevat is in zijn totaliteit versleuteld tot de volgende XML code:

```
<saml:EncryptedAttribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <xenc:EncryptedKey Recipient=%Merchant.LegalID%>
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        </xenc:EncryptionMethod>

```

```

    <xenc:CipherData>
      <xenc:CipherValue>%AESKey_Encrypted_With_Public_Key_Merchant%</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedKey>
</ds:KeyInfo>
<xenc:CipherData>
  <xenc:CipherValue>%Attribute_Encrypted_With_AES_Key%</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
</saml:EncryptedAttribute>

```

10.4 Authenticatie van iDIN berichten

Om zeker te zijn van de status van een iDIN-transactie, **moet** de Acceptant de elektronische handtekening van de Routing Service in de response berichten controleren. Ook moet deze de handtekening op de Assertion van de Issuer controleren in het AcquirerStatusRes.

Om de handtekening in het SignatureValue element te controleren, wordt aangeraden gebruik te maken van de standaard XML Digital Signature libraries die hiervoor beschikbaar zijn in de meeste (web)programmeertalen.

10.5 Maken van een sleutelpaar

Als u gebruik wilt maken van een zogenaamd “self signed certificate” leest u in deze sectie hoe u dit certificaat kunt maken. U kunt ook een certificaat inkopen bij een daarin gespecialiseerde partij (Certificate Authority), zie daarover de volgende sectie.

Doorloop de volgende stappen om een publieke en geheime sleutel aan te maken:

1. Download de ‘OpenSSL Library’ van www.openssl.org. Meer informatie over de te gebruiken ‘certificate generating utility’ vindt u hier: www.openssl.org/docs/apps/req.html. Het is ook mogelijk om met behulp van andere software een sleutelpaar te creëren, raadpleeg in dat geval de handleiding van de gebruikte software.
2. Genereer een ‘RSA private key’ met het volgende commando (gebruik een zelfgekozen wachtwoord voor het veld [privateKeyPass]):

```
openssl genrsa -aes128 -out priv.pem -passout pass:[privateKeyPass] 2048
```

3. Genereer een certificaat op basis van de ‘RSA private key’ (gebruik hetzelfde wachtwoord voor het veld [privateKeyPass]):

```
openssl req -x509 -sha256 -new -key priv.pem -passin pass:[privateKeyPass]
-days 1825 -out cert.cer
```

4. Deze openssl instructie genereert een certificaat in X.509 formaat, met een geldigheid van 5 jaar (1825 dagen), de maximumduur voor iDIN certificaten voor ondertekenen.
5. Het bestand priv.pem bevat de private key, het bestand cert.cer bevat het certificaat met de publieke sleutel. Het bestand priv.pem moet de Acceptant dus zelf houden en wordt gebruikt in de RSA versleuteling. Het cert.cer bestand moet beschikbaar worden gesteld

aan de Routing Service. Hoe dit beschikbaar moet worden gesteld, verschilt per Routing Service.

10.5.1 Een certificaat aanschaffen bij een Certificate Authority

Als een certificaat gekocht wordt van een Certificate Authority (CA), in plaats van een self-signed certificaat te gebruiken, is het volgende van belang: Het certificaat dat de CA gebruikt (en de rest van de *certificate chain*) moet ten minste even veilig zijn als het certificaat van de Acceptant.

CA-certificaten die worden gebruikt om elektronische handtekeningencertificaten te ondertekenen moeten dus ten minste SHA-256 als hashing algoritme gebruiken en RSA sleutels van ten minste 2.048 bits. Certificaten voor ondertekening mogen bovendien maximaal 5 jaar geldig zijn.

10.6 Signature data elementen

Alle berichten, inclusief de Error berichten, zijn ondertekend met een digitale handtekening. De digitale handtekening garandeert de authenticiteit van de zender, integriteit en onweerlegbaarheid van het bericht. De digitale handtekening zit binnen het XML Signature element dat is gedefinieerd volgens de standaard XML-Signature Syntax and Processing W3C Recommendation 12 februari 2002, zie Tabel 7 voor de schema locatie. Alle elementen en attributen relevant voor de digitale handtekening in alle iDx en SAML 2.0 berichten zijn hieronder beschreven, **andere elementen moeten niet worden gebruikt.**

Element/attributen	Verplicht	Inhoud
Signature	Ja	Root
+ SignedInfo	Ja	Bevat SignedInfo sub-elementen
++ CanonicalizationMethod	Ja	Moet één attribuut hebben
++ @algorithm	Ja	De XML inhoud die wordt gesigneerd moet worden gecanonicaliseerd. Dit zorgt ervoor dat inhoudelijk gelijke berichten ook exact hetzelfde worden weergegeven in XML Moet zijn: "http://www.w3.org/2001/10/xml-exc-c14n#"
++ SignatureMethod	Ja	Moet één attribuut hebben
++ @algorithm		Voor alle ondertekeningen moet RSA met SHA256 algoritme worden gebruikt Moet zijn: "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
++ Reference	Ja	Bevat Reference sub-elementen
++ Reference@URI	Ja	Attribuut van Reference dat leeg gelaten moet worden. Dit geeft aan dat het totale XML bericht moet worden gesigneerd. Moet zijn: ""
+++ Transforms	Ja	Bevat Transforms sub-elementen. Dit element bevat een lijst met Transform elementen, waarvan elk een stap specificeert voordat het document door wordt gestuurd naar het digest algoritme. Alle berichten gebruiken een 'enveloped signature' d.w.z. dat de digitale handtekening binnen het ondertekende staat. Een transform is nodig om de digitale handtekening te verwijderen uit de getekende data.
++++ Transform		Moet één attribuut hebben
++++ Transform@algorithm		Moet zijn: "http://www.w3.org/2000/09/xmldsig#enveloped-signature"
++++ Transform		Moet één attribuut hebben

Element/attributen	Verplicht	Inhoud
++++ Transform@algorithm		Moet zijn: "http://www.w3.org/2001/10/xml-exc-c14n#"
+++ DigestMethod		Moet één attribuut hebben
+++ @algorithm		Dit attribuut specificeert welk hashing algoritme is gebruikt (SHA256) Moet zijn: "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
+++ DigestValue	Ja	De base64 waarde van de hash van het totale document
+ SignatureValue	Ja	De waarde van de digitale handtekening
+ KeyInfo	Ja	Bevat KeyInfo sub-elementen
++ KeyName	Ja	Bevat de fingerprint van het X.509 certificaat die nodig is om de digitale handtekening te valideren. De fingerprint moet gemaakt worden van het X.509 certificaat van de Acceptant, Acquirer of Issuer. Deze wordt berekend volgens de volgende formule: HEX(SHA-1(DER certificate))

Tabel 31: Elementen/attributen van het Signature element

Het ondertekenen van het SAML 2.0 Assertion wordt anders gedaan. In plaats van te refereren naar het X.509 certificaat d.m.v. een fingerprint wordt het hele certificaat van de Issuer toegevoegd. Bovendien moet het attribuut @URI van Reference verwijzen naar de @ID van de Assertion in plaats van de waarde "" bevatten. Dit leidt tot de vervanging van de inhoud van het KeyInfo element zoals weergegeven in onderstaande tabel, de rest van de elementen en attributen zijn hetzelfde als in Tabel 31:

Element/attributen	Verplicht	Inhoud
Signature	Ja	Root
+ SignedInfo/ Reference@URI	Ja	Attribuut van Reference dat moet verwijzen naar de @ID van de Assertion. Moet zijn: Waarde Assertion@ID bevatten (let op dat een verwijzing in XML altijd moet beginnen met '#')
+ KeyInfo	Ja	Bevat KeyInfo sub-elementen
++ X509Data	Ja	Bevat X509Data sub-elementen
+++ X509Certificate	Ja	Bevat het Issuer.x509 element (hele certificaat van de Validation Service).

Tabel 32: Veranderingen in de Signature elementen bij ondertekenen van SAML 2.0 Assertion

11 Presentatie van iDIN

11.1 Algemeen

Ten aanzien van de presentatie van iDIN op de site van de Acceptant geldt een aantal eisen. Het voornaamste doel van deze eisen is het creëren van een uniforme gebruikerservaring, ongeacht op welke website deze iDIN gebruikt. De verschillende eisen worden in de volgende secties genoemd en toegelicht.

De Acceptant draagt primaire verantwoordelijkheid voor het initiëren van het iDIN proces en voor communicatie naar de Gebruiker over de status van het iDIN proces. Acceptanten die iDIN beschikbaar stellen voor hun Gebruikers moeten iDIN in hun bestaande lijst opnemen van authenticatie methoden (als de Acceptant andere methoden aanbiedt). Zodat iDIN op dezelfde wijze wordt gepresenteerd in de lijst als de concurrerende methoden.

Een iDIN-transactie (e.g beginnen van een authenticatie en/of aanvraag Gebruikersattributen) moet altijd ondubbelzinnig door de Gebruiker worden herkend. Dit betekent dat de Acceptant iDIN als dusdanig moet presenteren aan de Gebruiker, dat de selectie en start van een iDIN proces als zodanig herkenbaar is. De Acceptant moet ook duidelijk onderscheid maken tussen de verschillende iDIN processen (authenticatie, leeftijdsverificatie of aanvraag van Gebruikersattributen).

11.2 Transactiestroom

Wanneer de Gebruiker een iDIN-transactie start, krijgt de Gebruiker onmiddellijk een Issuer selectielijst gepresenteerd zonder dat er tussenschermen worden getoond door de Acceptant (bv. Gebruiker login en/of registratieschermen). Nadat de relevante Issuer is geselecteerd door de Gebruiker, wordt hij/zij meteen doorgestuurd naar de Issuer bankomgeving van de geselecteerde bank (op basis van de `issuerAuthenticationURL` die de Acceptant ontvangt in de `AcquirerTrxRes`).

11.3 Redirect naar de Issuer

Een Acceptant dient de redirect naar de Issuer binnen het browservenster te laten plaatsvinden waar de Gebruiker de Issuer heeft geselecteerd, waarna de volledige pagina van de Acceptant vervangen wordt door de volledige pagina van de gekozen Issuer. Het is dus niet toegestaan de redirect naar de Issuer in een nieuw browservenster te laten plaatsvinden. Het is wel toegestaan een nieuw venster, met zichtbare adresbalk, te openen vóór de Gebruiker zijn bank selecteert.

11.4 Frames

Frames in de site van de Acceptant worden toegestaan. Het scherm van de Issuer zal deze frames wegdrukken met een framebusting techniek zodat de Gebruiker beter kan controleren dat het iDIN proces werkelijk bij zijn/haar Issuer plaats vindt. Na de redirect moet de Acceptant het eigen scherm weer volledig opbouwen, voor het tonen van de bevestiging van het inloggen en/of aanvraag Gebruikersattributen aan de Gebruiker.

11.5 Nieuw venster

Het afhandelen van een iDIN-transactie in een nieuw browservenster is toegestaan, als de Acceptant dit venster laat verschijnen bij (of voorafgaand aan) de authenticatiekeuze door de Gebruiker. Het openen van een nieuw venster mag alleen op initiatief van de Gebruiker gebeuren (geen pop-up). De gehele transactiestroom dient in dit venster plaats te vinden tot en met de bevestiging van het iDIN proces door de Acceptant. Dit nieuw geopende venster dient ook voorzien te zijn van een zichtbare adresbalk, zodat dit adres gebruikt kan worden om te controleren of er bij de Issuer een iDIN proces plaatsvindt door verificatie van het adres (URL) en het SSL-certificaat. Gedurende het proces moet het voor de Gebruiker niet mogelijk zijn via het oorspronkelijke browservenster van de Acceptant nogmaals een iDIN proces voor hetzelfde doel te starten.

11.5.1 Specifieke eisen aan iDIN mobiel: Nieuw venster of app

Het mobiele iDIN proces kan een Gebruiker omleiden naar een andere mobiele webpagina of applicatie als onderdeel van de iDIN-transactie. De Acceptant moet ernaar streven om de Gebruiker zoveel mogelijk binnen één browserpagina te houden maar de Acceptant mag geen gebruik maken van een in-app browser (web view) in zijn applicatie (zie Hoofdstuk 7 voor meer details). In die gevallen waar het switchen naar een andere applicatie of venster noodzakelijk is (zoals de redirect naar de Issuer) moet de Gebruiker hierover worden geïnformeerd om verwarring te voorkomen. (Bijvoorbeeld: *“U zal nu worden doorgestuurd naar de applicatie of (mobiele) website van uw bank”*).

11.6 Issuer lijst

De Issuer lijst moet worden gepresenteerd zoals beschreven in Sectie 6.4.

11.7 Banners en logo's

Deze informatie zal beschikbaar worden gemaakt op idin.nl.

11.8 Eisen en aanbeveling iDIN teksten Acceptantschermen

Dit hoofdstuk beschrijft eisen en aanbevelingen van teksten in de Acceptantschermen die aan de Gebruiker worden getoond.

11.8.1 Tonen van de laatste inlog

Als de Gebruiker iDIN gebruikt en heeft ingelogd bij de Acceptant, dan wordt het sterk aangeraden om aan de Gebruiker de datum en tijd tonen van de laatste login (in het algemeen, niet specifiek iDIN), bv. 'De laatste keer dat U bent ingelogd was op 1 Oktober 2015, om 15:41'. De exacte tekst mag door de Acceptant worden bepaald. Dit is zodat de Gebruiker zelf kan controleren of dit tijdstip overeenkomt met zijn/haar laatste bezoek.

11.8.2 Uitleg iDIN aan de Gebruiker

Acceptanten kunnen onderstaande teksten gebruiken om iDIN uit te leggen aan hun klanten.

Uitleg iDIN aan de Gebruiker

- **Korte versie:** Makkelijk en veilig online identificeren met uw bank.
- **Uitgebreide versie (voorkeur):** Met iDIN kunt u zich online identificeren bij een bedrijf of instelling. Gemakkelijk, vertrouwd en veilig met de inlogmethode van uw bank.

Uitleg voordelen iDIN aan de Gebruiker

1. Makkelijk en veilig online identificeren.
2. Met de vertrouwde inlogmethode van uw bank.
3. Eén manier van inloggen bij bedrijven en instellingen.
4. Geen aparte gebruikersnamen en wachtwoorden meer onthouden.
5. Zelf invullen van persoonlijke gegevens is niet meer nodig.

11.8.3 Aanbevelingen teksten Acceptantschermen per RequestedServiceID

iDIN biedt verschillende services, die zijn onderverdeeld in de volgende vier use cases.

De vier use cases zijn als volgt:

1. **Gegevens verstrekken/versturen:** De Gebruiker kiest ervoor gegevens te verstrekken met iDIN, met of zonder het aanmaken van een account. De Acceptant vraagt deze gegevens op met of zonder BIN. Hieronder valt b.v. ook het verstrekken van de geboortedatum of NAW gegevens met/zonder BIN;
2. **Inloggen:** De Gebruiker logt in met iDIN. Er worden geen gegevens verstrekt, alleen een BIN;
3. **Leeftijd bevestigen:** Bevestiging leeftijd 18+ (hierbij wordt het attribuut `18orOlder` aangevraagd met of zonder BIN). Dit kan worden gebruikt voor zowel verificatie van leeftijd boven of onder 18 jaar;
4. **Bankbevestiging:** Gebruiker bevestigt dat hij klant is van een bepaalde bank. Er wordt alleen een `TransientID` geleverd.

Elke combinatie die gemaakt kan worden met het `RequestedServiceID` hoort bij één van de vier bovenstaande use cases. Appendix A, waar alle waarden van het `RequestedServiceID` zijn weergegeven, toont ook de bijbehorende use case.

Tabel 33 geeft per use case een aanbeveling van de teksten voor de website van de Acceptant. Het verwijzingsscherm van de Acceptant is het scherm waar de Gebruiker kiest voor het gebruik van iDIN. De return-webpagina is de webpagina van de Acceptant waar de Gebruiker terugkeert nadat deze de transactie heeft goedgekeurd in zijn internetbankieromgeving.

Use case	Aanbeveling Acceptant verwijzingsscherm	Aanbeveling Acceptant return-webpagina
1 Gegevens verstrekken	<ul style="list-style-type: none"> • Maak uw account aan met iDIN • Gegevens verstrekken/versturen met iDIN 	<ul style="list-style-type: none"> • Uw gegevens zijn succesvol ontvangen • Wij hebben de volgende gegevens ontvangen: [overzicht gegevens]
2 Inloggen	<ul style="list-style-type: none"> • Inloggen met iDIN 	<ul style="list-style-type: none"> • U bent ingelogd met iDIN • Tonen laatste inlog (verplicht)

Use case	Aanbeveling Acceptant verwijzingsscherm	Aanbeveling Acceptant return-webpagina
3 Leeftijd bevestigen	<ul style="list-style-type: none"> Leeftijd bevestigen met iDIN 	<ul style="list-style-type: none"> Bedankt voor het bevestigen van uw leeftijd Direct toegang tot de site
4 Bankbevestiging	<ul style="list-style-type: none"> Bevestig dat u klant bent bij uw bank met iDIN 	<ul style="list-style-type: none"> U heeft bevestigd dat u klant bent bij <code>Issuer.Name</code>

Tabel 33: Aanbeveling teksten Acceptantschermen per use case

11.9 Issuer front-end

Het volgende proces en eisen zijn buiten de scope van de implementatie van de Acceptant, maar zijn toch toegevoegd om een beeld te scheppen van de ervaring van de Gebruiker bij het gebruik van iDIN in het domein van zijn/haar bank.

De Issuer draagt primaire verantwoordelijkheid voor het iDIN proces en voor de communicatie naar de Gebruiker in de omgeving van de Issuer. De pagina volgorde en lay-out (vanaf de redirect van de Acceptant naar de Issuer tot de redirect terug naar de Acceptant) worden bepaald door de Validation Service. Aan de volgende eisen moet worden voldaan:

- Na het selecteren van zijn/haar Issuer op de website van de Acceptant wordt de Gebruiker doorgestuurd naar de Validation Service website. In het actieve browser venster wordt de complete pagina van de Acceptant vervangen door de webpagina van de Validation Service. Als alternatief kan de Validation Service er voor kiezen om automatisch de Gebruiker door te sturen naar de mobiele website of mobiele applicatie van de Issuer. De criteria met betrekking tot wanneer deze automatische redirect plaatsvindt wordt overgelaten aan de Validation Service;
 - Optioneel kan de Validation Service de Gebruiker laten kiezen indien de Validation Service meerdere kanalen beschikbaar heeft voor de Gebruiker (e.g. door de Gebruiker te laten kiezen tussen de mobiele webpagina of app). Als deze optie aan de Gebruiker wordt geboden vindt er een tweede redirect plaats naar de authenticatie website of applicatie;
- Ten allen tijde moet het voor de Gebruiker duidelijk zijn dat deze een iDIN-transactie begint. Daarom moet de Validation Service het iDIN logo op elke webpagina/mobiele applicatie laten zien binnen het iDIN proces;
- De Validation Service laat geen informatie zien die niet gerelateerd en irrelevant is voor de iDIN-transactie, en wat de Gebruiker kan afleiden om de iDIN-transactie te voltooien. Informatie die als relevant wordt gezien is:
 - Een help functie die beschikbaar wordt gesteld door de Validation Service waar de Gebruiker extra informatie kan krijgen met betrekking tot de iDIN service(s);
 - Als de Issuer een mobiele applicatie heeft dan mag deze worden aangeboden aan de Gebruiker als download en activatie in het iDIN proces. Let op: downloaden en installeren van deze applicatie kan er voor zorgen dat de expiratieperiode van de transactie verloopt.

- De Validation Service faciliteert alle services van iDIN. De Validation Service moet helder aangegeven aan de Gebruiker voor welke iDIN service de Gebruiker toestemming gaat geven;
- De Validation Service garandeert dat de integriteit en lay-out van de Validation Service webpagina/mobiele applicatie niet verandert als deze de inhoud toont van tekst velden (e.g. door een op malafide Acceptant die kwaadaardige/frauduleuze inhoud verstuurt in de transactie informatie);
- Alle iDIN-transactie gerelateerde informatie (i.e. transactieinformatie, Gebruikersinformatie en Acceptant informatie), moet worden gepresenteerd aan de Gebruiker voor goedkeuring;
- De Gebruiker kan tijdens het iDIN proces of toestemming geven voor het afgeven van alle Gebruikersattributen, of het verzoek in zijn totaliteit weigeren;
- De Gebruiker is niet toegestaan informatie in de transactie te wijzigen tijdens het iDIN proces;
- De Validation Service moet duidelijk aan de Gebruiker aangeven hoe deze toestemming kan geven voor de iDIN-transactie;
- De Gebruiker moet al zijn/haar attributen met de bijhorende waarden kunnen zien om een geïnformeerde keuze te maken voor het goedkeuren van de iDIN-transactie. Om deze informatie te verkrijgen moet de Gebruiker eerst inloggen bij de Validation Service. Zodoende kan de Validation Service de Gebruiker authenticiseren en de bijhorende informatie aan de Gebruiker tonen;
- De Validation Service geeft duidelijk aan hoe de Gebruiker de transactie kan afbreken;
- Als optie kan de Validation Service een bericht tonen aan de Gebruiker als deze de transactie probeert af te breken door de browser te sluiten, of als deze terug of voorwaarts navigeert door de pijltoetsen in de browser te gebruiken. Dit bericht mag worden getoond omdat dit ongewenst gedrag is binnen de iDIN-transactie. In het bericht kan de Gebruiker worden aangeraden de transactie op een normale manier af te breken of te voltooien;
- De Validation Service is vrij om altijd instructies aan de Gebruiker te tonen die beschrijven hoe de Gebruiker zijn/haar attributen kan wijzigen;
- Als de Validation Service niet aan de minimale set van attributen kan voldoen dan mag deze aan de Gebruiker aangegeven welke attributen missen, en welke stappen moeten worden gedaan om deze informatie aan te vullen. De Validation Service is hierin vrij in keuze en implementatie;
- Na goedkeuring van de iDIN-transactie moet de Gebruiker de optie hebben om onmiddellijk terug te keren naar de website van de Acceptant waar de iDIN-transactie was geïnitieerd. Dit kan worden bereikt door een 'Continue/Akkoord' knop. Het klikken op deze knop redirect de Gebruiker naar de URL van de Acceptant die is meegestuurd naar de Validation Service in de transactie aanvraag.

11.9.1 Teksten op de Issuerschermen per RequestedServiceID

iDIN biedt verschillende services die de Acceptant kan aanvragen met behulp van het RequestedServiceID. Elke service is gekoppeld aan één van drie use cases. Afhankelijk van de aangevraagde service zal de Issuer een andere tekst aan de Gebruiker tonen. Tabel 34 toont deze teksten per use case, met de volgende opmerkingen:

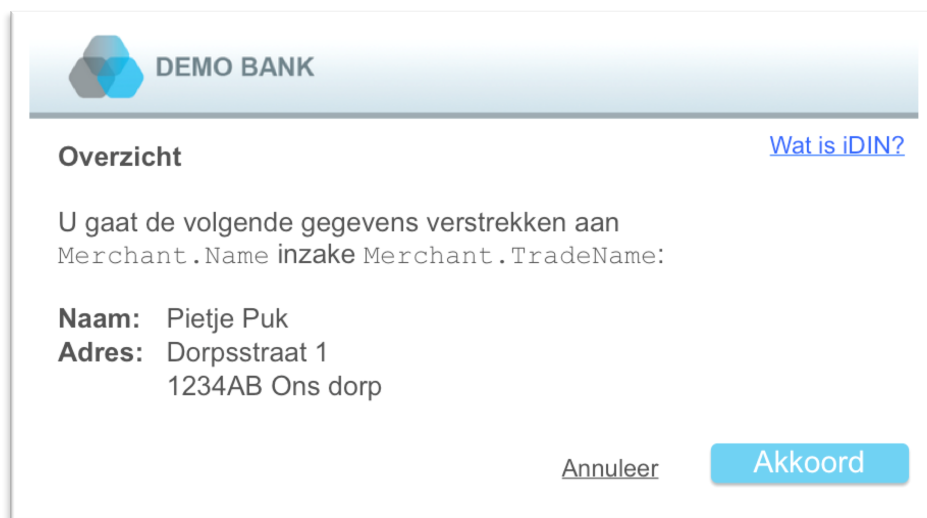
- Teksten en termen die altijd door de Issuer worden gebruikt zijn **dikgedrukt**. Ter illustratie wordt een voorbeeld gegeven, de exacte formulering van de zinnen kan verschillen per bank;

- 'Voor/Inzake `Merchant.TradeName`' wordt alleen getoond indien deze aanwezig is;
- De verplichte Issuer termen en teksten worden getoond voor en/of na inloggen door de Gebruiker in het Issuerderein;
- De Validation Service toont de attributen van de Gebruiker (bij use case 1 en 3) die zijn aangevraagd door de Acceptant. De Gebruiker kan vervolgens toestemming geven voor het versturen van zijn/haar gegevens aan de Acceptant. **Let op:** `consumer.transientid`, `consumer.bin` en `consumer.deprecatedbin` worden niet aan de Gebruiker getoond, alle andere Gebruikersattributen worden wel getoond.

Use case	Issuer termen die altijd worden getoond	Voorbeeld
1 Gegevens verstrekken	<ul style="list-style-type: none"> • Gegevens verstrekken/versturen • Merchant.Name (voor/inzake Merchant.TradeName) 	U gaat de volgende gegevens verstrekken aan Merchant.Name (inzake Merchant.TradeName) : [overzicht gegevens] bijvoorbeeld: Naam: Pietje Puk Adres: Dorpstraat 1 1234AB Ons dorp
2 Inloggen	<ul style="list-style-type: none"> • Inloggen • Merchant.Name (voor/inzake Merchant.TradeName) 	U gaat inloggen bij Merchant.Name (inzake Merchant.TradeName)
3 Leeftijd bevestigen	<ul style="list-style-type: none"> • Leeftijd bevestigen • Merchant.Name (voor/inzake Merchant.TradeName) 	U bevestigt uw leeftijd aan Merchant.Name (inzake Merchant.TradeName) [overzicht gegevens] bijvoorbeeld: 18 jaar of ouder: JA

Tabel 34: Termen in Issuerschermen per use case

De onderstaande screenshot geeft een voorbeeld hoe het goedkeuringsscherm op de website of mobiele applicatie van de Issuer kan worden weergegeven bij het verzoek om gegevens te verstrekken met iDIN.



The screenshot shows a web interface for a 'DEMO BANK'. At the top left is a logo consisting of three overlapping hexagons in shades of blue and grey. To the right of the logo, the text 'DEMO BANK' is displayed in a bold, sans-serif font. Below the header, the word 'Overzicht' (Overview) is shown in bold. To the right of 'Overzicht' is a blue hyperlink that reads 'Wat is iDIN?'. The main content area contains the text 'U gaat de volgende gegevens verstrekken aan' (You will provide the following data to) followed by 'Merchant.Name inzake Merchant.TradeName:'. Below this, the transaction details are listed: 'Naam: Pietje Puk' and 'Adres: Dorpsstraat 1, 1234AB Ons dorp'. At the bottom right of the form, there are two buttons: a text link 'Annuleer' (Cancel) and a blue button with white text 'Akkoord' (Agree).

Figuur 5: Voorbeeld van goedkeuring van een iDIN-transactie

12 Appendix A: Foutcodes (Error codes)

Als er iets mis gaat op iDx niveau, dan stuurt de Acquirer een AcquirerErrorRes met een bijbehorende errorCode naar de Acceptant. Als er iets misgaat op SAML niveau dan is deze iDx errorCode gelijk aan AP3000 en zit er een container in het error bericht. Deze container bevat een SAML Response zoals besproken in Sectie 9.2.

12.1 iDx error codes

De `Error.errorCode` is samengesteld uit:

- Een categorie (twee letters)
- Een getal (vier cijfers)

Er wordt onderscheid gemaakt tussen de volgende categorieën:

Categorie	Toelichting
IX	Ongeldige XML en alle gelieerde problematiek. Zoals verkeerde encoding, ongeldige versie, anderszins onleesbaar.
SO	Systeemonderhoud. De fouten die gecommuniceerd worden ten behoeve van systeemonderhoud of -storing. Omvat ook de situatie waarin nieuwe Requests niet meer geaccepteerd worden, maar Requests die al zijn ontvangen nog wel worden afgehandeld (tot een bepaald tijdstip).
SE	Security en authenticatie fouten. Verkeerde authenticatie methoden en verlopen certificaten.
BR	Veldfouten. Extra informatie over foutieve velden.
AP	Applicatie fouten. Fouten met betrekking tot ID's, rekeningnummers, tijdzones, iDIN-transacties, valuta.

Tabel 35: Error code categorieën

De volgende iDx error codes bestaan:

errorCode	errorMessage	errorDetail	Komt voor in bericht
IX1100	Received XML not valid	Zie 1)	A'(X), B'(X), F'(X)
IX1200	Encoding type not UTF-8	Zie 1)	A'(X), B'(X), F'(X)
IX1300	XML version number invalid	Zie 1)	A'(X), B'(X), F'(X)
IX1600	Mandatory value missing	Zie 1)	A'(X), B'(X), F'(X)
SO1000	Failure in system	Zie 2)	A'(X), B'(X), F'(X)
SO1100	Issuer unavailable	Zie 3)	B'(X)
SO1200	System busy. Try again later	Zie 2)	A'(X), B'(X), F'(X)
SO1400	Unavailable due to maintenance	Zie 2)	A'(X), B'(X), F'(X)
SE2700	Invalid electronic signature	Zie 1)	A'(X), B'(X), F'(X)
BR1200	Version number invalid	Zie 1)	A'(X), B'(X), F'(X)
BR1205	ProductID invalid	Zie 1)	A'(X), B'(X), F'(X)
BR1210	Value contains non-permitted character	Zie 1)	A'(X), B'(X), F'(X)

errorCode	errorMessage	errorDetail	Komt voor in bericht
BR1220	Value too long	Zie 1)	A'(X), B'(X), F'(X)
BR1230	Value too short	Zie 1)	A'(X), B'(X), F'(X)
BR1270	Invalid date/time	Zie 1)	A'(X), B'(X), F'(X)
BR1280	Invalid URL	Zie 1)	B'(X)
AP1100	MerchantID unknown	Zie 1)	A'(X), B'(X), F'(X)
AP1200	IssuerID unknown	Zie 1)	B'(X)
AP1300	SubID unknown	Zie 1)	A'(X), B'(X)
AP1500	MerchantID not active	Zie 1)	A'(X), B'(X), F'(X)
AP2600	Transaction does not exist	Zie 1)	F'(X)
AP2920	Expiration period is not valid	Zie 1)	B'(X)
AP3000	iDIN product specific code	Zie 1)	A'(X), B'(X), F'(X)

Tabel 36: Error codes

Het veld `errorDetail` in de bovenstaande tabel bevat één van de waardes weergegeven in onderstaande tabel. De schuingedrukte woorden, worden vervangen door daadwerkelijk waardes.

Indicatie	errorDetail
1)	Field generating error: location-reference in XML message
2)	System generating error: <i>Issuer/Acquirer</i>
3)	System generating error: <i>Name of Issuer</i>

Tabel 37: errorDetail

12.2 SAML Error codes

Om aan te geven aan de Acceptant wat er precies fout is gegaan wordt er gebruik gemaakt van het SAML status element, zoals hieronder aangegeven:

```
<samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <samlp:StatusCode Name=%Eerste status code%>
    <samlp:StatusCode Name=%Tweede status code% />
  </samlp:StatusCode>
  <samlp:StatusMessage>Text determined by Routing or Validation Service</samlp:StatusMessage>
</samlp:Status>
```

SAML definieert twee statuscodes. De eerste status code kan de volgende waardes hebben:

StatusCode@Value	Beschrijving
urn:oasis:names:tc:SAML:2.0:status:Success	Het verzoek is gelukt. <u>Dit wordt niet gebruikt in geval van een error Response</u>
urn:oasis:names:tc:SAML:2.0:status:Requester	Het verzoek kan niet worden volbracht vanwege een fout aan de kant van de Acceptant

Tabel 38: Eerste SAML statuscodes

De tweede status code is aanwezig voor alle gevallen beschreven in Sectie 9.2. Er zijn enkele standaard SAML codes op dit niveau, en enkele die alleen binnen iDIN worden gebruikt. De mogelijke waarden voor de tweede status code is weergegeven in onderstaande tabel:

StatusCode@Value	Beschrijving
urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	De aanvraag kan niet worden uitgevoerd omdat het aangevraagde BankID.ServiceID of BankID.LOA niet wordt ondersteund. Deze waarde wordt alleen gebruikt in combinatie met de eerste status code: urn:oasis:names:tc:SAML:2.0:status:Requester
urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue	De aanvraag kan niet worden uitgevoerd omdat er invalide of onverwachte inhoud in een SAML element zit, of dat er elementen ontbreken. Deze status code wordt gebruikt als de inhoud of een attribuut van een SAML element niet in lijn is met de iDIN specificaties, anders dan het BankID.ServiceID of BankID.LOA. E.g. verkeerde formatting, verkeerd gebruik van elementen etc. Deze waarde wordt alleen gebruikt in combinatie met de eerste status code: urn:oasis:names:tc:SAML:2.0:status:Requester
urn:nl:bvn:bankid:1.0:status:MismatchWithIdx <i>Deze status code wordt alleen gebruikt binnen iDIN</i>	De aanvraag kan niet worden uitgevoerd omdat één of meerdere velden in het SAML AuthnRequest niet overeenkomen met de waarden in het iDx bericht zoals gespecificeerd in iDIN e.g. MerchantID in het SAML AuthnRequest komt niet overeen met het MerchantID in het iDx bericht. Deze waarde wordt alleen gebruikt in combinatie met de eerste status code: urn:oasis:names:tc:SAML:2.0:status:Requester
urn:oasis:names:tc:SAML:2.0:status:RequestDenied	Het verzoek is geweigerd omdat de Assertion is verlopen. Zie volgende sectie voor meer informatie. Deze waarde wordt alleen gebruikt in combinatie met de eerste status code: urn:oasis:names:tc:SAML:2.0:status:Requester
urn:nl:bvn:bankid:1.0:status:Success <i>Deze status code wordt alleen gebruikt binnen iDIN</i>	Aanwezig als waarde van de tweede status code als de Validation Service alle attributen heeft geleverd conform de minimale set (zie Sectie 5.5 en Sectie 12.4)
urn:nl:bvn:bankid:1.0:status:IncompleteAttributeSet <i>Deze status code wordt alleen gebruikt binnen iDIN</i>	De aanvraag is succesvol beantwoord, echter niet alle aangevraagde attributen zijn geleverd volgens de minimale set (zie Sectie 5.5). Het element <code>DeliveredServiceID</code> geeft aan welke attributen wel aan de minimale set voldoen (als de Validation Service de minimale set niet kan bepalen wordt de waarde '0' gebruikt). In beide gevallen is het <code>DeliveredServiceID</code> ongelijk aan het <code>RequestedServiceID</code>

Tabel 39: Tweede SAML statuscodes

12.3 SAML Error cases

Er zijn twee gevallen waar de eerste SAML status code niet “urn:oasis:names:tc:SAML:2.0:Success” maar “urn:oasis:names:tc:SAML:2.0:Requester” is.

1. Er zit een fout in de container in het AcquirerTrxReq (B): In dit geval wordt een iDx AcquirerErrorRes (B'(X)) teruggestuurd met een SAML Response in de container. De iDx errorCode en errorMessage zijn respectievelijk AP3000 en “Product specific error”. De tweede SAML status code is afhankelijk van de type fout.
2. De Acceptant heeft een status verzoek ingediend maar de Assertion is verlopen. Het kan voorkomen dat de Gebruiker de iDIN-transactie heeft goedgekeurd, echter is de Acceptant er niet in geslaagd de status binnen 30 seconden op te vragen. De 30 seconden starten vanaf het moment dat de Gebruiker terug wordt gestuurd naar de website van de Acceptant. In dit geval

wordt een `AcquirerStatusRes` teruggestuurd naar de Acceptant. De `iDx` status staat op "Success", echter de SAML Response bevat geen attributen maar heeft de opbouw zoals weergegeven in Tabel 30: Elementen/attributen in de container van het `AcquirerErrorRes`. Hier is de tweede SAML status code gelijk aan "urn:oasis:names:tc:SAML:2.0:status:RequestDenied".

12.4 Issuer kan niet alle attributen leveren volgens minimale set

Er kan zich de mogelijkheid voordoen dat de Issuer niet alle attributen volgende de minimale set kan leveren. In dit geval wordt het volgende gedaan:

- Een normaal SAML Response bericht wordt teruggestuurd zoals wordt besproken in Sectie 8.3;
- De Issuer levert alle attributen die wel beschikbaar zijn gebaseerd op `RequestedServiceID`;
- De eerste SAML status code staat gewoon op "urn:oasis:names:tc:SAML:2.0:Success";
- De tweede SAML status code staat op "urn:nl:bvn:bankid:1.0:status:IncompleteAttributeSet";
- Het `DeliveredServiceID` geeft aan welke attributen wel volgens de minimale set zijn geleverd. Als de Issuer dit niet kan bepalen wordt de waarde '0' gebruikt.

Voorbeeld:

- De Acceptant vraagt de geboortedatum en de attribuutgroep adres met `RequestedServiceID 1472`;
- De Issuer kan de attribuutgroep adres niet volgens de minimale set leveren (de Issuer heeft de postcode, stad en straatnaam maar heeft geen huisnummer). Hierdoor kan hij geen match maken vanuit de minimale set zoals beschreven in Sectie 5.5;
- De Issuer berekent het `DeliveredServiceID` dat overeenkomst met de aangevraagde attributen die wel volgens de minimale set kunnen worden geleverd. In dit geval is dit 448, omdat alleen de geboortedatum volledig kan worden geleverd.
- De Issuer levert de geboortedatum en alle attributen uit de (incomplete) groep adres.

12.5 Bericht aan de Gebruiker

Het element `Error.consumerMessage` bevat één van vier gestandaardiseerde teksten die door de Routing Service naar de Acceptant wordt gestuurd, zie Tabel 40. De Acceptant moet de tekst in het element `Error.consumerMessage` aan de Gebruiker tonen.

Situatie	Bericht om te laten zien aan de Gebruiker (Engels)	Bericht om te laten zien aan de Gebruiker (Nederlands)
Fout opgetreden bij zenden of ontvangen van berichten <i>A, A', B, B'</i>	It is currently not possible to use iDIN. Please try again later.	Het is op dit moment niet mogelijk om iDIN te gebruiken. Probeer het later nog een keer.
Fout opgetreden bij verzenden of ontvangen van bericht <i>F, F'</i>	It is currently not possible to use iDIN. Please try again later.	Het is op dit moment niet mogelijk om iDIN te gebruiken. Probeer het later nog een keer.
Fout opgetreden door onbeschikbaarheid van Validation Service (SO1000, SO1100, SO1200, SO1400 of geen response ontvangen van Validation Response door Routing Service na verzenden van bericht C)	The selected bank is currently unavailable. Please try again later.	De geselecteerde bank is op dit moment niet beschikbaar. Probeer het later nog een keer.

Situatie	Bericht om te laten zien aan de Gebruiker (Engels)	Bericht om te laten zien aan de Gebruiker (Nederlands)
Fout opgetreden door onbeschikbaarheid van Issuer (zie boven) EN additionele informatie beschikbaar uit het Notificatiesysteem	The selected bank is currently unavailable due to maintenance until projected time of [DateTime received from the Notification System]. Please try again later.	De geselecteerde bank is op dit moment niet beschikbaar i.v.m. onderhoud tot naar verwachting [DateTime ontvangen van Notification System]. Probeer het later nog een keer.

Tabel 40: Bericht aan de Gebruiker

13 Appendix B: Voorbeeld berichten

Let op:

- De digitale handtekeningen in de voorbeeld berichten zijn niet te valideren;
- De voorbeelden zijn niet noodzakelijk aan elkaar gerelateerd.

13.1 DirectoryReq (A)

```
<?xml version="1.0" encoding="UTF-8"?>
<DirectoryReq version="1.0.0" productID="NL:BVN:BankID:1.0" xmlns="
http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <createDateTimeStamp>2001-12-17T09:30:47.123Z</createDateTimeStamp>
  <Merchant>
    <merchantID>1234123456</merchantID>
    <subID>1</subID>
  </Merchant>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
        <DigestValue>VW+VjenRyZVFCNfBTeoxDflQ4yfR8KYFvwPvinVPqBs</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>
      IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOr8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE/GPHZShuMw+8WHq4
      fCmInOwKURgwjDOz8UYaIMqG0Ojiz8dFYGn+dH2lL0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
    </SignatureValue>
    <KeyInfo>
      <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
    </KeyInfo>
  </Signature>
</DirectoryReq>
```

13.2 DirectoryRes (A')

```
<?xml version="1.0" encoding="UTF-8"?>
<DirectoryRes version="1.0.0" productID=" NL:BVN:BankID:1.0" xmlns="
http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```

<createDateTimestamp>2001-12-17T09:30:47.123Z</createDateTimestamp>
<Acquirer>
  <acquirerID>1234</acquirerID>
</Acquirer>
<Directory>
  <directoryDateTimestamp>2004-11-10T10:15:12.123Z</directoryDateTimestamp>
  <Country>
    <countryNames>Nederland</countryNames>
    <Issuer>
      <issuerID>BANKNL2U</issuerID>
      <issuerName>Bank 1</issuerName>
    </Issuer>
    <Issuer>
      <issuerID>BANANL2U</issuerID>
      <issuerName>Bank 2</issuerName>
    </Issuer>
    <Issuer>
      <issuerID>BANBNL2UXXX</issuerID>
      <issuerName>Bank 3</issuerName>
    </Issuer>
    <Issuer>
      <issuerID>BANCNL2U</issuerID>
      <issuerName>Bank 4</issuerName>
    </Issuer>
  </Country>
  <Country>
    <countryNames>België/Belgique</countryNames>
    <Issuer>
      <issuerID>BANKBE2U</issuerID>
      <issuerName>Banque 1</issuerName>
    </Issuer>
  </Country>
</Directory>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <Reference URI="">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
      <DigestValue>VW+VjenRyZVFCnfBTeoxDflQ4yfr8KYFvwPVinVPqBs=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
    IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOr8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE/GPHZShuMw+8WHq4
    fCMInOwKURgwjD0z8UYaIMqG0Ojiz8dFYGn+dH21L0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
  </SignatureValue>
</Signature>

```

```

</SignatureValue>
<KeyInfo>
  <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
</KeyInfo>
</Signature>
</DirectoryRes>

```

13.3 AcquirerTrxReq (B)

```

<?xml version="1.0" encoding="UTF-8"?>
<AcquirerTrxReq version="1.0.0"
  productID="NL:BVN:BankID:1.0"
  xmlns="http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <createDateTimestamp>2015-01-01T09:30:00.123Z</createDateTimestamp>
  <Issuer>
    <issuerID>BANKNL2U</issuerID>
  </Issuer>
  <Merchant>
    <merchantID>1234123456</merchantID>
    <subID>1</subID>
    <merchantReturnURL>https://merchantwebsite.nl/returnPage.php?param1=true&param2=3</merchan
tReturnURL>
  </Merchant>
  <Transaction>
    <expirationPeriod>PT5M</expirationPeriod>
    <language>nl</language>
    <entranceCode>1234567890</entranceCode>
    <container>
      <samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        AttributeConsumingServiceIndex="21952"
        ID="REF1234567890"
        IssueInstant="2015-01-01T09:30:00Z"
        Version="2.0"
        ProtocolBinding="nl:bnv:bankid:1.0:protocol:iDx"
        AssertionConsumerServiceURL="https://merchantwebsite.nl/returnPage.php?param1=true&param2=
3">
        <saml:Issuer>1234123456</saml:Issuer>
        <samlp:RequestedAuthnContext Comparison="minimum">
          <saml:AuthnContextClassRef>nl:bnv:bankid:1.0:loa2</saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
      </samlp:AuthnRequest>
    </container>
  </Transaction>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

```

```

    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <Reference URI="">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>VW+VjenRyZVFCnfBTcoxDflQ4yfR8KYFvwPvinVPqBs=</DigestValue>
    </Reference>
  </SignedInfo>

  <SignatureValue>IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOr8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE
  /GPHZShuMw+8WHq4fCMInOwKURgwjDOz8UYaIMqG00jiz8dFYGn+dH2lL0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
</SignatureValue>

  <KeyInfo>
    <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
  </KeyInfo>
</Signature>
</AcquirerTrxReq>

```

13.4 AcquirerTrxRes (B')

```

<?xml version="1.0" encoding="UTF-8"?>
<AcquirerTrxRes version="1.0.0" productID="NL:BVN:BankID:1.0" xmlns="
http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <createDateTimeStamp>2001-12-17T09:30:47.123Z</createDateTimeStamp>
  <Acquirer>
    <acquirerID>1234</acquirerID>
  </Acquirer>
  <Issuer>
    <issuerAuthenticationURL>https://issuer.nl?param=true&paramRandom=1234567890123456789012
34567890</issuerAuthenticationURL>
  </Issuer>
  <Transaction>
    <transactionID>1234123456789012</transactionID>
    <transactionCreateDateTimeStamp>2001-12-17T09:30:47.123Z</transactionCreateDateTimeStamp>
  </Transaction>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

```

```

        <DigestValue>VW+VjenRyZVFCNfBTeoxDflQ4yfr8KYFvwPVinVPqBs=</DigestValue>
    </Reference>
</SignedInfo>
<SignatureValue>
IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOR8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE/GPHZShuMw+8WHq4
fCMInOwKURgwjDOz8UYaIMqG00jiz8dFYGn+dH21L0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
</SignatureValue>
<KeyInfo>
    <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
</KeyInfo>
</Signature>
</AcquirerTrxRes>

```

13.5 AcquirerStatusReq (F)

```

<?xml version="1.0" encoding="UTF-8"?>
<AcquirerStatusReq version="1.0.0" productID="NL:BVN:BankID:1.0" xmlns="
http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
    <createDateTimeStamp>2001-12-17T09:30:47.123Z</createDateTimeStamp>
    <Merchant>
        <merchantID>1234123456</merchantID>
        <subID>1</subID>
    </Merchant>
    <Transaction>
        <transactionID>1234123456789012</transactionID>
    </Transaction>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <Reference URI="">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
                <DigestValue>VW+VjenRyZVFCNfBTeoxDflQ4yfr8KYFvwPVinVPqBs=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>
IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOR8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE/GPHZShuMw+8WHq4
fCMInOwKURgwjDOz8UYaIMqG00jiz8dFYGn+dH21L0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
        </SignatureValue>
        <KeyInfo>
            <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
        </KeyInfo>
    </Signature>

```



```
</AcquirerStatusReq>
```

13.6 AcquirerStatusRes (F') Unencrypted

Let op: Dit bericht zal nooit on-versleuteld aan de Acceptant worden verstuurd en dient alleen als voorbeeld.

```
<?xml version="1.0" encoding="UTF-8"?>
<AcquirerStatusRes version="1.0.0" productID="NL:BVN:BankID:1.0"
    xmlns="http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <createDateTimestamp>2015-01-01T09:30:47.123Z</createDateTimestamp>
  <Acquirer>
    <acquirerID>1234</acquirerID>
  </Acquirer>
  <Transaction>
    <transactionID>1234123456789012</transactionID>
    <status>Success</status>
    <statusDateTimestamp>2015-01-01T09:30:47.123Z</statusDateTimestamp>
    <container>
      <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="RES-
1234123456789012"
        InResponseTo="REF1234567890" Version="2.0" IssueInstant="2015-01-
01T09:30:47.123Z">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1234</saml:Issuer>
        <samlp:Status>
          <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">
            <samlp:StatusCode Value="urn:nl:bnv:bankid:1.0:status:Success"/>
          </samlp:StatusCode>
        </samlp:Status>
        <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
          ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc" IssueInstant="2015-01-
01T09:30:47.123Z">
          <saml:Issuer>BANKNL2U</saml:Issuer>
          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
              <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
              <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
              <ds:Reference URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
                <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>AA+VjenRyZVFCNfBTexDflQ4yfR8KYFvwPvinVPqBs</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>
```

```
<ds:SignatureValue>AAAAAwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOr8dcI+aJTbQ+YtryP9C1cK62Obs5aynHBE/GPHZShuMw+8WHq4fCMInOwkURgwjDOz8UYaIMqG00jiz8dFYgn+dH2lL0QVss4jmIIAD8MCijb27oqi j6PclXw9Y9veI=</ds:SignatureValue>  
    <ds:KeyInfo>  
        <ds:X509Data>  
  
<ds:X509Certificate>MIICyCCAygOgAWIBAgICAnUwDQYJKoZIhvcNAQEEBQAwwgakxCzAJBgNVBAYTA lVTMRIWEAYDVQQIEwlEXA nxb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAOTF1Vu eAXZlcNpdHkgb2YgV2lyZ29uc2luMSswKQYDVQL E y J Ea X Z p c 2 l v b i B v Z i B JbmZvcmlhdGlviBUZWNObm9sb2d5MSUWI w Y D V Q Q DE x x I R V B L S S B T Z X J 2 Z X Ig Q O EgLS0gMj Aw M j A 3 M D F B M B 4 X D TA y MDcy N j A 3 M j c l M V o X D TA 2 M D k w N DA 3 M j c l M V ow g Y s x C z AJ B g NV B AY T Al VT M RE W Dw Y DV QQ IE wh Na WN oa W dh bj ES MB AGAlUEBxMJQW5 u IEFyYm9yMQ4wDAYDVQKEwVVQOFJRDEcMBoga1UEAxMTc2hpYjEuaW50ZXJuZXRyYmVk dTE n MCUGCSgsGSib3DQEJARYYcm9vdEBzaGliMS5pb nRl cm5ldDIuZWR1MiGFMAOG CS q GS Ib 3 D QE BA QUAA4GNADCBIQBKgQDZSAb2sxvhAXnXVIvtx8vuRay+x50z7GJjIHRYQgiV6IqaGG04eTcyVMhoeke0b45QGvbIaoAPSZBl13R6+KYie7x4XAWIRCP+c2MZVeXeTgv3YZ+USLg2Ylon+jh4HXwkPFmZBctyiUr6DXf8rvoP9W7027rhRJEp mqOI f GTWQIDAQABox0wgZAMBgNVHRMBAf8EAJAAMAsGA1UdDwQEawIFo DAN BGkqhkiG9w0BAQQFAAOBGQBfdqEW+OI3jqBQHIBzhujN/Pizdn7s/z4D5d3pptWDJff2nqqgi7lFV6MDkhmTvTqbTbjmNk3No7v/dnP6Hr7wHxvCCRWubnmIfz6QZA v 2FU78pLXI8I3bsbmRAUg4UP9hH6ABVq4KKMKmnxlqxLhpRlYLGPdiowMNTrEG8cCx3w/w==</ds:X509Certificate>  
    </ds:X509Data>  
    </ds:KeyInfo>  
</ds:Signature>  
  
<saml:Subject>  
    <saml:NameID  
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">NLBANKsd45232432663dd34ja8sj sah439h28834HS h23h192h3</saml:NameID>  
    </saml:Subject>  
  
    <saml:Conditions NotBefore="2015-01-01T09:30:47.123Z" NotOnOrAfter="2015-01-01T09:31:17.123Z">  
        <saml:AudienceRestriction>  
            <saml:Audience>NL69ZZZ123456780000</saml:Audience>  
        </saml:AudienceRestriction>  
        <saml:OneTimeUse/></saml:OneTimeUse>  
    </saml:Conditions>  
  
    <saml:AuthnStatement AuthnInstant="2015-01-01T09:30:47.123Z">  
        <saml:AuthnContext>  
            <saml:AuthnContextClassRef>n l :bv n :bankid:1.0:l oa3</saml:AuthnContextClassRef>  
            <saml:AuthenticatingAuthority>BANKNL2U</saml:AuthenticatingAuthority>  
        </saml:AuthnContext>  
    </saml:AuthnStatement>  
  
    <saml:AttributeStatement>  
        <saml:Attribute Name="urn:n l :bv n :bankid:1.0: bankid.deliveredserviceid">  
            <saml:AttributeValue>21952</saml:AttributeValue>  
        </saml:Attribute>  
        </saml:Attribute>  
  
        <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  
Name="urn:n l :bv n :bankid:1.0: consumer.gender">  
            <saml:AttributeValue>1</saml:AttributeValue>
```

```
</saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.legallastname">
    <saml:AttributeValue>Vries</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.preferredlastname">
    <saml:AttributeValue>Vries-Jansen</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.partnerlastname">
    <saml:AttributeValue>Jansen</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.legallastnameprefix">
    <saml:AttributeValue>de</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.preferredlastnameprefix">
    <saml:AttributeValue>de</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.initials">
    <saml:AttributeValue>JV</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.dateofbirth">
    <saml:AttributeValue>19850101</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.street">
    <saml:AttributeValue>Gustav Mahlerplein</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.houseno">
    <saml:AttributeValue>33</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.housenosuf">
    <saml:AttributeValue>bis</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.addressextra">
    <saml:AttributeValue>woonboot t.o. de Albert Heijn</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bvn:bankid:1.0:consumer.postalcode">
    <saml:AttributeValue>1082MS</saml:AttributeValue>
  </saml:Attribute>
```

```

        <saml:Attribute Name="urn:nl:bn:bankid:1.0:consumer.city">
          <saml:AttributeValue>Amsterdam</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="urn:nl:bn:bankid:1.0:consumer.country">
          <saml:AttributeValue>NL</saml:AttributeValue>
        </saml:Attribute>
      </saml:AttributeStatement>
    </saml:Assertion>
  </samlp:Response>
</container>
</Transaction>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <Reference URI="">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig#sha256" />
      <DigestValue>VW+VjenRyZVFCNfBTcoxDflQ4yfr8KYFvwPvinVPqBs=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOr8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE
/GPHZShuMw+8WHq4fCMInOwKURgwjDOz8UYaIMqG00jiz8dFYGn+dh21L0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
</SignatureValue>
  <KeyInfo>
    <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
  </KeyInfo>
</Signature>
</AcquirerStatusRes>

```

13.7 AcquirerStatusRes (F') Encrypted

Dit bericht bevat twee versleutelde attributen.

```

<?xml version="1.0" encoding="UTF-8"?>
<AcquirerStatusRes version="1.0.0" productID="NL:BVN:BankID:1.0"
  xmlns="http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <createDateTimestamp>2015-01-01T09:30:47.123Z</createDateTimestamp>
  <Acquirer>
    <acquirerID>1234</acquirerID>
  </Acquirer>
  <Transaction>
    <transactionID>1234123456789012</transactionID>
    <status>Success</status>
  </Transaction>
</AcquirerStatusRes>

```

```
<statusDateTimestamp>2015-01-01T09:30:47.123Z</statusDateTimestamp>
<container>
  <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="RES-
1234123456789012"
    InResponseTo="REF1234567890" Version="2.0" IssueInstant="2015-01-
01T09:30:47.123Z">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1234</saml:Issuer>
    <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">
        <samlp:StatusCode Value="urn:nl:bnv:bankid:1.0:status:Success"/>
      </samlp:StatusCode>
    </samlp:Status>
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
      ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc" IssueInstant="2015-01-
01T09:30:47.123Z">
      <saml:Issuer>BANKNL2U</saml:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
          <ds:Reference URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmllenc#sha256" />
            <ds:DigestValue>AA+VjenRyZVFCNfBTeoxDf1Q4yfR8KYFvWPVinVPqBs=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>VGhpcyBpcyBhIHRlc3QgbWVzc2FnZSE=</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
<ds:X509Certificate>MIICyJCCAjOgAwIBAgICANUwDQYJKoZIhvcNAQEEBQAwgaxCzAJBgNVBAYTA1VT
MRIwEAYDVQQIEw1XaXNjb25zaW4xEDA0BGNVBAcTB01hZGlzb24xIDAeBgNVBAoT
F1VuaXZ1cnNpdHkqb2YgV21zY29uc2luMSswKQYDVQQLEyJEaXZpc21vbiBvZiBj
bmZvcmlhdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgc0Eg
LS0gMjAwMjA3MDFBMB4XDTAyMDcyNjA3Mjc1MV0XDTA2MDkwNDA3Mjc1MVoWogYsX
CzAJBgNVBAYTA1VTMREwDwYDVQQIEWhNaWNoaWdhbjESBAGAlUEBxMJQW5uIEFy
Ym9yMQ4wDAYDVQQKEwVvVQ0FJRDECMBoGA1UEAxMTc2hpYjEuaW50ZXJzXzQyLmVh
dTenMCUGCSqGSIB3DQEJARYYcm9vdEBzaGlms5pbnRlcm5ldDIuZWZR1MIGFMA0G
CSqGSIB3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvhAXnXVIVTx8vuRay+x50z7GJj
IHRyQgIv6IqaGG04eTcyVMhoeKE0b45QgvBIaOAPSZB113R6+KYiE7x4XAWIRcP+
c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE
pmqOI fGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq
hkiG9w0BAQQFAAOBqQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n
qqi7lFV6MDkhmTvtTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfz6QZAv2FU78pLX

```

```
8I3bsbmRAUg4UP9hH6ABVq4KQKMknxulxQxLhpR1ylGPdiowMNTREg8cCx3w/w==</ds:X509Certificate>
    </ds:X509Data>
    </ds:KeyInfo>
</ds:Signature>
<saml:Subject>
  <saml:EncryptedID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
      Type="http://www.w3.org/2001/04/xmlenc#Element">
      <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <xenc:EncryptedKey Recipient="NL69ZZZ123456780000">
          <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          </xenc:EncryptionMethod>
          <xenc:CipherData>
<xenc:CipherValue>jenRyZVFCnfBTExDflQ4yfR8KYFwPVinVPqBsVW+V=</xenc:CipherValue>
            </xenc:CipherData>
          </xenc:EncryptedKey>
        </ds:KeyInfo>
        <xenc:CipherData>
<xenc:CipherValue>VW+VjenRyZVFCnfBTExDflQ4yfR8KYFwPVinVPqBs=</xenc:CipherValue>
          </xenc:CipherData>
        </xenc:EncryptedData>
      </saml:EncryptedID>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-01-01T09:30:47.123Z" NotOnOrAfter="2015-01-
01T09:31:17.123Z">
      <saml:AudienceRestriction>
        <saml:Audience>NL69ZZZ123456780000</saml:Audience>
      </saml:AudienceRestriction>
      <saml:OneTimeUse></saml:OneTimeUse>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-01-01T09:30:47.123Z">
      <saml:AuthnContext>
        <saml:AuthnContextClassRef>nl:bvn:bankid:1.0:loa2</saml:AuthnContextClassRef>
        <saml:AuthenticatingAuthority>BANKNL2U</saml:AuthenticatingAuthority>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="urn:nl:bvn:bankid:1.0:bankid.deliveredserviceid">
        <saml:AttributeValue>21952</saml:AttributeValue>
      </saml:Attribute>
      <saml:EncryptedAttribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
          Type="http://www.w3.org/2001/04/xmlenc#Element">
          <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
```

```

        <ds:KeyInfo >
            <xenc:EncryptedKey Recipient="NL69ZZZ123456780000">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p">
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                </xenc:EncryptionMethod>
                <xenc:CipherData>
<xenc:CipherValue>jenRyZVFCnfBTeoxDflQ4yfR8KYFwVPinVPqBsVW+V=</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedKey>
        </ds:KeyInfo>
        <xenc:CipherData>
<xenc:CipherValue>BTeoxDflQ4yfR8KYFwVPinVPqBsVW+VjenRyZVFCnf=</xenc:CipherValue>
        </xenc:CipherData>
    </xenc:EncryptedData>
</saml:EncryptedAttribute>
<saml:EncryptedAttribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        Type="http://www.w3.org/2001/04/xmlenc#Element">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <xenc:EncryptedKey Recipient="NL69ZZZ123456780000">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p">
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                </xenc:EncryptionMethod>
                <xenc:CipherData>
<xenc:CipherValue>jenRyZVFCnfBTeoxDflQ4yfR8KYFwVPinVPqBsVW+V=</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedKey>
        </ds:KeyInfo>
        <xenc:CipherData>
<xenc:CipherValue>nVPqBsVW+VjenRyZVFCnfBTeoxDflQ4yfR8KYFwVPi=</xenc:CipherValue>
        </xenc:CipherData>
    </xenc:EncryptedData>
</saml:EncryptedAttribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
</container>
</Transaction>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <Reference URI="">
            <Transforms>
                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

```

```

    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <DigestValue>VW+VjenRyZVFCNfBTeoxDflQ4yfr8KYFvwPvinVPqBs=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOr8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE
/GPHZShuMw+8WHq4fCMInOwKURgwjDOz8UYaIMqG00jiz8dFYGn+dh21L0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
</SignatureValue>
  <KeyInfo>
    <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
  </KeyInfo>
</Signature>
</AcquirerStatusRes>

```

13.8 AcquirerErrorRes (B'(X))

```

<?xml version="1.0" encoding="UTF-8"?>
<AcquirerErrorRes version="1.0.0" productID="NL:BVN:BankID:1.0"
xmlns="http://www.betalvereniging.nl/idx/messages/Merchant-Acquirer/1.0.0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <createDateTimeStamp>2015-01-01T09:30:47.123.123Z</createDateTimeStamp>
  <Error>
    <errorCode>AP3000</errorCode>
    <errorMessage>Product specific error</errorMessage>
    <container>
      <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="RES-
1234123456789012" InResponseTo="REF1234567890" Version="2.0" IssueInstant="2015-01-
01T09:30:47.123Z">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">1234</saml:Issuer>
        <samlp:Status>
          <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Requester">
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported"/>
          </samlp:StatusCode>
          <samlp:StatusMessage>Requested BankID.ServiceID not
supported</samlp:StatusMessage>
        </samlp:Status>
      </samlp:Response>
    </container>
  </Error>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

```



```
</Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <DigestValue>VW+VjenRyZVFCNfBTcoxDflQ4yfR8KYFvwPvinVPqBs=</DigestValue>
  </Reference>
</SignedInfo>
<SignatureValue>
IELLwKSGFMk64US23YrpZ8//hJ8DeJEtYht5knlxJvBOr8dcI+aJTBq+YtyzP9ClcK62Obs5aynHBE/GPHZShuMw+8WHq4
fCMInOwKURgwjDOz8UYaIMqG00jiz8dFYGn+dH2lL0QVss4jmIIAD8MCijb27oqij6PclXw9Y9veI=
</SignatureValue>
<KeyInfo>
  <KeyName>7D665C81ABBE1A7D0E525BFC171F04D276F07BF2</KeyName>
</KeyInfo>
</Signature>
</AcquirerErrorRes>
```

14 Appendix C: iDx Merchant-Acquirer Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- iDx Messages version 1.0.0: interface Merchant/Acquirer -->
<!-- Copyright © Betaalvereniging -->
<xs:schema xmlns="http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  targetNamespace="http://www.betalvereniging.nl/iDx/messages/Merchant-Acquirer/1.0.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0.0">
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="xmldsig-core-
  schema.xsd"/>
  <xs:annotation>
    <xs:documentation>elements defined</xs:documentation>
  </xs:annotation>
  <xs:element name="DirectoryReq">
    <xs:annotation>
      <xs:documentation>Directory Request (A)</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="createDateTimeStamp" type="dateTime"/>
        <xs:element name="Merchant">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="merchantID" type="Merchant.merchantID"/>
              <xs:element name="subID" type="Merchant.subID"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element ref="ds:Signature"/>
      </xs:sequence>
      <xs:attributeGroup ref="MessageAttributes"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="DirectoryRes">
    <xs:annotation>
      <xs:documentation>Directory Response (A')</xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="createDateTimeStamp" type="dateTime"/>
        <xs:element name="Acquirer">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="acquirerID" type="Acquirer.acquirerID"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="Directory">
```

```

        <xs:complexType>
          <xs:sequence>
            <xs:element name="directoryDateTimeStamp" type="dateTime"/>
            <xs:element name="Country" maxOccurs="unbounded">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="countryNames" type="Country.countryNames"/>
                  <xs:element name="Issuer" maxOccurs="unbounded">
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element name="issuerID" type="Issuer.issuerID"/>
                        <xs:element name="issuerName" type="Issuer.issuerName"/>
                      </xs:sequence>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attributeGroup ref="MessageAttributes"/>
  </xs:complexType>
</xs:element>
<xs:element name="AcquirerTrxReq">
  <xs:annotation>
    <xs:documentation>Acquirer Transaction Request (B)</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="createDateTimeStamp" type="dateTime"/>
      <xs:element name="Issuer">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="issuerID" type="Issuer.issuerID"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="Merchant">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="merchantID" type="Merchant.merchantID"/>
            <xs:element name="subID" type="Merchant.subID"/>
            <xs:element name="merchantReturnURL" type="url"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

    <xs:element name="Transaction">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="expirationPeriod" type="Transaction.expirationPeriod"
minOccurs="0"/>
          <xs:element name="language" type="Transaction.language"/>
          <xs:element name="entranceCode" type="Transaction.entranceCode"/>
          <xs:element name="container" type="Transaction.container"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element ref="ds:Signature"/>
  </xs:sequence>
  <xs:attributeGroup ref="MessageAttributes"/>
</xs:complexType>
</xs:element>
<xs:element name="AcquirerTrxRes">
  <xs:annotation>
    <xs:documentation>Acquirer Transaction Response (B')</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="createDateTimeStamp" type="dateTime"/>
      <xs:element name="Acquirer">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="acquirerID" type="Acquirer.acquirerID"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="Issuer">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="issuerAuthenticationURL"
type="Issuer.issuerAuthenticationURL"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="Transaction">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="transactionID" type="Transaction.transactionID"/>
            <xs:element name="transactionCreateDateTimeStamp" type="dateTime"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attributeGroup ref="MessageAttributes"/>
  </xs:complexType>
</xs:element>

```

```
</xs:complexType>
</xs:element>
<xs:element name="AcquirerStatusReq">
  <xs:annotation>
    <xs:documentation>Acquirer Status Request (F)</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="createDateTimeStamp" type="dateTime"/>
      <xs:element name="Merchant">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="merchantID" type="Merchant.merchantID"/>
            <xs:element name="subID" type="Merchant.subID"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="Transaction">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="transactionID" type="Transaction.transactionID"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attributeGroup ref="MessageAttributes"/>
  </xs:complexType>
</xs:element>
<xs:element name="AcquirerStatusRes">
  <xs:annotation>
    <xs:documentation>Acquirer Status Response (F')</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="createDateTimeStamp" type="dateTime"/>
      <xs:element name="Acquirer">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="acquirerID" type="Acquirer.acquirerID"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="Transaction">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="transactionID" type="Transaction.transactionID"/>
            <xs:element name="status" type="Transaction.status"/>
            <xs:element name="statusDateTimeStamp" type="dateTime" minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

```

        <xs:element name="container" type="Transaction.container" minOccurs="0"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element ref="ds:Signature"/>
</xs:sequence>
<xs:attributeGroup ref="MessageAttributes"/>
</xs:complexType>
</xs:element>
<xs:element name="AcquirerErrorRes">
  <xs:annotation>
    <xs:documentation>Acquirer Error Response (X')</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="createDateTimeStamp" type="dateTime"/>
      <xs:element name="Error">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="errorCode" type="Error.errorCode"/>
            <xs:element name="errorMessage" type="Error.errorMessage"/>
            <xs:element name="errorDetail" type="Error.errorDetail" minOccurs="0"/>
            <xs:element name="suggestedAction" type="Error.suggestedAction"
minOccurs="0"/>
            <xs:element name="consumerMessage" type="Error.consumerMessage"
minOccurs="0"/>
            <xs:element name="container" type="Transaction.container" minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attributeGroup ref="MessageAttributes"/>
  </xs:complexType>
</xs:element>
<xs:annotation>
  <xs:documentation>simpleTypes defined</xs:documentation>
</xs:annotation>
<xs:simpleType name="Acquirer.acquirerID">
  <xs:restriction base="xs:token">
    <xs:length value="4" fixed="true"/>
    <xs:pattern value="[0-9] +"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Country.countryNames">
  <xs:restriction base="xs:token">
    <xs:minLength value="1"/>
    <xs:maxLength value="128"/>
  </xs:restriction>

```

```
</xs:simpleType>
<xs:simpleType name="Error.consumerMessage">
  <xs:restriction base="xs:string">
    <xs:maxLength value="512" fixed="true"/>
    <xs:minLength value="1" fixed="true"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Error.errorCode">
  <xs:restriction base="xs:token">
    <xs:length value="6" fixed="true"/>
    <xs:pattern value="[A-Z]{2}[0-9]{4}" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Error.errorDetail">
  <xs:restriction base="xs:string">
    <xs:maxLength value="256" fixed="true"/>
    <xs:minLength value="1" fixed="true"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Error.errorMessage">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
    <xs:maxLength value="128"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Error.suggestedAction">
  <xs:restriction base="xs:string">
    <xs:maxLength value="512" fixed="true"/>
    <xs:minLength value="1" fixed="true"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Issuer.issuerAuthenticationURL">
  <xs:restriction base="url"/>
</xs:simpleType>
<xs:simpleType name="Issuer.issuerID">
  <xs:restriction base="BIC"/>
</xs:simpleType>
<xs:simpleType name="Issuer.issuerName">
  <xs:restriction base="xs:token">
    <xs:maxLength value="35" fixed="true"/>
    <xs:minLength value="1" fixed="true"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Merchant.merchantID">
  <xs:restriction base="xs:token">
    <xs:length value="10" fixed="true"/>
    <xs:pattern value="[0-9]+" />
  </xs:restriction>
</xs:simpleType>
```

```

<xs:simpleType name="Merchant.merchantReturnURL">
  <xs:restriction base="url"/>
</xs:simpleType>
<xs:simpleType name="Merchant.subID">
  <xs:restriction base="xs:nonNegativeInteger">
    <xs:maxInclusive value="999999" fixed="true"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Transaction.entranceCode">
  <xs:restriction base="xs:token">
    <xs:minLength value="1" fixed="true"/>
    <xs:maxLength value="40" fixed="true"/>
    <xs:pattern value="[a-zA-Z0-9]+"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Transaction.expirationPeriod">
  <xs:restriction base="xs:duration">
    <xs:minInclusive value="PT1M" fixed="true"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Transaction.language">
  <xs:restriction base="language"/>
</xs:simpleType>
<xs:simpleType name="Transaction.status">
  <xs:restriction base="xs:token">
    <xs:pattern value="Open|Success|Failure|Expired|Cancelled|Pending"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Transaction.transactionID">
  <xs:restriction base="xs:token">
    <xs:length value="16" fixed="true"/>
    <xs:pattern value="[0-9]+"/>
  </xs:restriction>
</xs:simpleType>
<xs:annotation>
  <xs:documentation>basic simpleTypes defined</xs:documentation>
</xs:annotation>
<xs:simpleType name="BIC">
  <xs:restriction base="xs:token">
    <xs:pattern value="[A-Z]{6,6}[A-Z2-9][A-NP-Z0-9]([A-Z0-9]{3,3}){0,1}" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="dateTime">
  <xs:restriction base="xs:dateTime">
    <xs:pattern value=".+Z"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="language">
  <xs:restriction base="xs:token">

```



```
<xs:length value="2" fixed="true"/>
<xs:pattern value="[a-z]+"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="productID">
  <xs:restriction base="xs:string"/>
</xs:simpleType>
<xs:simpleType name="url">
  <xs:restriction base="xs:anyURI">
    <xs:maxLength value="512"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="version">
  <xs:restriction base="xs:string">
    <xs:pattern value="1\.0\.0"/>
  </xs:restriction>
</xs:simpleType>
<xs:annotation>
  <xs:documentation>complexTypes defined</xs:documentation>
</xs:annotation>
<xs:complexType name="Transaction.container">
  <xs:sequence>
    <xs:any namespace="##any" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:annotation>
  <xs:documentation>attributeGroups defined</xs:documentation>
</xs:annotation>
<xs:attributeGroup name="MessageAttributes">
  <xs:annotation>
    <xs:documentation>attributes of each message</xs:documentation>
  </xs:annotation>
  <xs:attribute name="version" type="version" use="required"/>
  <xs:attribute name="productID" type="productID" use="required"/>
</xs:attributeGroup>
</xs:schema>
```