SCRIPTIE

DE TOEPASSINGSMOGELIJKHEDEN VAN HET CONCEPT VAN ANONIEME ATTRIBUTEN

VERSIE 1.0

Student: Arjan de Jong
Studentnummer: 08064733
Opleiding: Information Security Management

Bedrijf: Centric Nederland BV
Plaats: Gouda
Datum: 07-06-2013

CENTRIC

" Personal data is best protected if not revealed at all "

- IBM Research

Titel	De toepassingsmogelijkheden Van anonieme attributen
Centric Nederland B.V.	
Naam auteur:	Arjan de Jong
Studentnummer:	08064733
Opleiding:	Information Security Management
Onderwijsinstelling:	De Haagse Hogeschool
Begeleiders:	Marjolein Faassen Henk van de Ven
Opdrachtgever:	Centric Nederland B.V.
Begeleider:	Gé Iking
Plaats	Gouda
Datum	07-06-2013

Versiehistorie

Versienummer	Versiedatum	Controle door	Wijzigingen
0.6	18-05-2013	Arjan de Jong	Concept
1.0	07-06-2013	Arjan de Jong	Definitief

Distributielijst

Versienummer	Datum	Naam	Organisatie
0.6	18-05-2013	Marjolein Faassen Henk van de Ven	De Haagse Hogeschool
1.0	07-06-2013	Marjolein Faassen Henk van de Ven	De Haagse Hogeschool

Referaat

Om de toegangscontrole tot onder meer applicaties en informatiesystemen te kunnen beheren wordt er binnen vele organisaties gebruik gemaakt van Identity & Access Management. Zoals de naam van dit proces al doet vermoeden speelt de identiteit van de gebruikers hierin een belangrijke rol.

Door onderzoek uit te voeren naar de toepassingsmogelijkheden van anonieme attributen is er een adviesrapportage tot stand gekomen waarin Centric Nederland B.V. wordt geadviseerd over de mogelijkheden die anonieme attributen voor de eigen organisatie een haar klanten te bieden heeft in situaties waarbij het niet mogelijk is om gebruik te maken van identificerende gegevens van de gebruikers.

- Identity & Access Management
- Centric Nederland B.V.
- Anonieme attributen
- Toegangscontrole
- Informatiebeveiliging
- Privacy
- Anonimiteit

Voorwoord

Voor u ligt het afstudeerverslag van Arjan de Jong. Dit document is geschreven ter afronding van mijn opleiding Information Security Management aan De Haagse Hogeschool te Zoetermeer en de daarbij behorende afstudeerperiode.

Gedurende de periode van 11 februari 2013 tot en met 7 juni 2013 heb ik binnen Centric Nederland B.V. onderzoek gedaan naar de toepassingsmogelijkheden van anonieme attributen ter behoeve van de toegangscontrole voor Centric en haar klanten.

Dit afstudeerverslag heeft als doel om de examinatoren inzicht te geven in de wijze waarop ik deze afstudeeropdracht heb uitgevoerd en tevens om te onderbouwen waarom ik het onderzoek op deze wijze heb uitgevoerd.

Een onderzoek wordt nooit tot een succesvol einde gebracht zonder de hulp van anderen. Ik wil daarom ook de volgende mensen bedanken die mij hebben geholpen gedurende mijn afstudeerperiode;

Mijn afstudeercoaches vanuit De Haagse Hogeschool te Zoetermeer, **Marjolein Faassen** en **Henk van de Ven** voor hun goede adviezen betreffende de afstudeeropdracht zelf en de hulp bij het schrijven van deze scriptie.

Mijn afstudeerbegeleider vanuit Centric Nederland B.V. **Gé Iking** voor de coaching gedurende het afstuderen.

Mijn **familie** en **vrienden** die een luisterend oor waren en mij gedurende het afstuderen hebben gesteund.

Gouda, 07 juni 2013
Arjan de Jong

Inhoudsopgave

1 Inleiding 9
2 Achtergrond 10
2.1 Over Centric 10
2.2 De afstudeeropdracht 12
2.1.1 Doelstelling en resultaten 12
2.1.2 Centrale- en deelvragen 12
2.1.3 Fasering 12
2.1.4 Betrokkenen 13
3 Aanpak bepalen 14
3.1 De doelstelling 14
3.2 De gehanteerde werkwijze en methoden 14
3.2.1 Scope vaststellen 14
3.2.2 Afstudeerplan 14
3.2.3 Probleemanalyse 15
3.2.4 Begripsafbakening 16
3.2.5 Project Initiation Document 17
3.2.6 Verschillen tussen het afstudeerplan en PID 17
3.2.7 Verschillen tussen het afstudeerplan en PID 18
4 Vooronderzoek – Fase 2 19
4.1 De doelstelling 19
4.2 De gehanteerde werkwijze en methoden 19
4.2.1 Deskresearch 19
4.2.2 Bijeenkomsten 22
4.2.3 Interviews 23
4.3 De resultaten 24
4.3.1 Definitie Identity & Access Management 24
4.3.2 Concept van anonieme attributen 24
4.3.3 Achterom kijken 24
5 De requirements analyse – Fase 3 26
5.1 De doelstelling 26
5.2 De gehanteerde werkwijze en methoden 26
5.2.1 MoSCoW-methode 26
5.3 De resultaten 26
5.3.1 Achterom kijken 27
6 Het productonderzoek 28
6.1 De doelstelling 28
6.2 De gehanteerde werkwijze en methoden 28
6.2.1 Deskresearch 28
6.3 De resultaten 30
6.3.1 Achterliggende techniek en cryptografie 30
6.3.2 Mogelijkheden en functionaliteiten 30
6.3.3 Achterom kijken 32
7 Het scenario onderzoek 33
7.1 De doelstelling 33
7.2 De gehanteerde werkwijze en methoden 33
7.2.1 Deskresearch 33
7.2.2 Brainstorm sessies 35
7.2.3 Uitwerken scenario's 35
7.3 De resultaten 35
7.3.1 Breed toepasbaar 35

7.3.2 Autorisatieprocessen. 36
7.3.3 Achterom kijken 38
8 Afsluiting project en advies 39
8.1 De doelstelling 39
8.2 De gehanteerde werkwijze en methoden 39
8.2.1 Indeling adviesrapport bepalen 39
8.2.2 Het adviesrapport schrijven 40
8.2.3 Controle 40
8.2.4 Uitloop 40
8.2.5 Rondvraag binnen Centric 40
8.3 De resultaten 42
8.3.1 Het advies 42
8.3.2 Achterom kijken 45
9 Evaluatie 46
9.1 Procesevaluatie 46
9.2 Productevaluatie 49
9.3 Competenties 50
10 Literatuurlijst 54
11 Lijst met tabellen en figuren 57
Bijlage A: Afstudeerplan 58
Bijlage B: Project Initiation Document 63
Bijlage C: Achtergrond: Identity & Access Management 75
Bijlage D: Achtergrond: Europese privacywetgeving 77
Bijlage E: Het productonderzoek 79

1 Inleiding

Dit document is geschreven naar aanleiding van mijn afstuderen bij Centric op de afdeling Techniek en Kwaliteit gedurende de periode van 11 februari 2013 tot en met 7 juni 2013. Het document heeft tot doel om de lezer een zo volledig mogelijk beeld te geven van het doorlopen proces bij het kunnen uitvoeren van deze afstudeeropdracht binnen Centric.

Het afstudeerverslag is in drie onderdelen opgebouwd. Het eerste gedeelte (hoofdstuk 2) beschrijft de achtergrond van de afstudeeropdracht. In dit eerste hoofdstuk wordt er aandacht wordt besteed aan de organisatie Centric, het tot stand komen van de afstudeeropdracht, de fasen waarin het onderzoek is onderverdeeld en tot slot de personen die betrokken zijn geweest bij deze afstudeeropdracht. In het tweede gedeelte van dit document (hoofdstuk 3 tot en met hoofdstuk 7) wordt er per doorlopen fase weergegeven wat het beoogde doel van iedere fase is geweest en op welke wijze deze fase is uitgevoerd en tot slot wordt er per fase het resultaat weergegeven. Tot slot wordt er in het laatste gedeelte (hoofdstuk 8 tot en met hoofdstuk 9) teruggekeken op de doorlopen stappen gedurende het afstuderen door middel van een productevaluatie, procesevaluatie en een beschrijving van de behandelde competenties.

Als bijlage zijn aan dit afstudeerverslag alle documenten bijgevoegd welke aan Centric en/of De Haagse Hogeschool zijn opgeleverd gedurende het afstuderen. Het uiteindelijke adviesrapport is als externe bijlage bijgevoegd.

2 Achtergrond

Dit hoofdstuk beschrijft de achtergrond van de afstudeeropdracht, als eerste zal de organisatie worden beschreven waarbinnen deze afstudeeropdracht is uitgevoerd en vervolgens wordt de afstudeeropdracht zelf beschreven.

2.1 Over Centric

Centric[1] is een gespecialiseerde IT-organisatie en biedt met zo'n 5.300 medewerkers standaard- en maatwerksoftware, infrastructuren en professionals voor het inrichten, optimaliseren, beheren en ondersteunen van bedrijfsprocessen en informatiestromen. Centric verzorgt deze diensten en oplossingen op basis van advies, trainingen, licenties, personele ondersteuning, projecten en volledige outsourcing. Daarbij werkt Centric samen met gerenommeerde partners.

Centric is een onderdeel van de groep Centric B.V., waar ruim 15.500 medewerkers werkzaam zijn. Naast Centric maken onder meer advies- en ingenieursbureau Oranjewoud en het bedrijf Strukton onderdeel uit van deze groep.

Geschiedenis

Centric is in 1992 opgericht door Gerard Sanderink. Dankzij autonome groei en een strategisch acquisitiebeleid is Centric in korte tijd uitgegroeid tot een van de meest vooraanstaande aanbieders van Informatie Technologie in de Benelux. Centric heeft inmiddels vestigingen in de Benelux, Duitsland, Noorwegen, Roemenië, Zweden en Zwitserland. Sinds 2005 is Centric – dankzij de overname van het bedrijf Finance – ook actief op het gebied van financiële dienstverlening. In onderstaand figuur (Figuur 2) wordt een overzicht weergegeven van de Nederlandse vestigingen.

Figuur 2.1 Vestigingen Centric Nederland

[1] Centric | http://www.centric.eu/

Branches

Centric is actief in diverse branches waaronder onder meer;

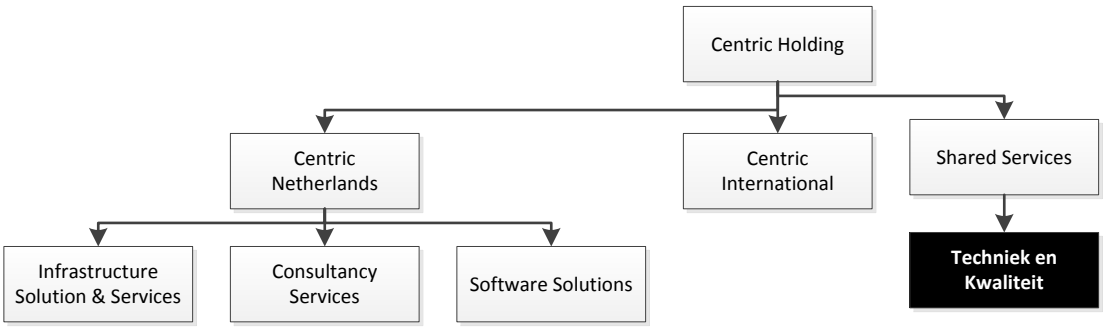
- Lokale overheden
- Waterschappen
- Onderwijs
- Bouw
- Woningcorporaties
- Groothandel
- Retail
- Logistiek
- Zorg
- Financiële dienstverlening
- Uitgeverijen

Organigram

In onderstaande afbeelding is de organisatiestructuur van Centric, en dan met name de afdeling waarbinnen ik gedurende mijn afstuderen werkzaam ben geweest weergegeven (Figuur **2.2**). Deze afdeling Techniek & Kwaliteit heeft de volgende hoofdtaken;

- Het mede bepalen en richting geven aan het huidige en toekomstige gebruik van technieken voor softwareontwikkeling en onderhoud, en ook de hierbij behorende ondersteuning en dienstverlening.
- Het mede bepalen en richting geven aan het beleid, uitvoering en handhaving van kwaliteitszorg.

De afdeling Techniek & Kwaliteit is een onderdeel van de tak Shared Services binnen Centric, wat zelf weer een onderdeel is van Centric Holding. In de tak Shared Services zitten een aantal Centric brede afdelingen waaronder dus Techniek & Kwaliteit maar bijvoorbeeld ook Legal Affairs en Human Resources. De holding bestaat naast Shared Services uit de takken Centric International en Centric Netherlands. Hierbij is Centric International het gedeelte waar de verschillende buitenlandse vestigingen onder vallen. Het gedeelte Centric Netherlands bestaat uit de takken Infrastructure Solutions & Services, Consultancy Services en Software Solutions.



Figuur 2.2 Organisatiestructuur Centric

2.2 De afstudeeropdracht

In deze paragraaf beschrijf ik de totstandkoming van de afstudeeropdracht en worden de centrale- en deelvragen weergegeven.

2.1.1 Doelstelling en resultaten

De doelstelling van deze afstudeeropdracht was enerzijds het uitvoeren van een onderzoek naar de toepassingsmogelijkheden van anonieme attributen ter behoeve van de toegangscontrole om Centric zodoende hierover te kunnen adviseren over gebruik binnen Centric en haar klanten. Daarnaast heeft deze afstudeeropdracht als doel gehad om mijn opleiding Information Security Management aan De Haagse Hogeschool te Zoetermeer te kunnen afronden.

De producten die gedurende deze afstudeeropdracht opgeleverd zouden worden waren als volgt;

- Adviesrapportage (Centric)
- Afstudeerverslag (dit document) (De Haagse Hogeschool)

2.1.2 Centrale- en deelvragen

De centrale vraag van het afstudeeronderzoek is na overleg met mijn afstudeerbegeleider als volgt geformuleerd;

- Onderzoek voor Centric en haar klanten de toepassingsmogelijkheden van Identity & Access Management (IAM) op basis van attributen i.p.v. identiteiten.

Om deze centrale vraag te kunnen beantwoorden zijn er de onderstaande deelvragen opgesteld;

- Wat wordt er bedoeld met anonieme attributen?
- Waar worden anonieme attributen voor gebruikt?
- In welke situaties kan er gebruik worden gemaakt van anonieme attributen?
- Waarom zou dit nuttig kunnen zijn voor Centric?

2.1.3 Fasering

Het afstudeeronderzoek is opgesplitst in een zestal fasen te weten;

Fase	Omschrijving
Fase 1:	Plan van aanpak
Fase 2:	Vooronderzoek
Fase 3:	Vaststellen requirements
Fase 4:	Productonderzoek
Fase 5:	Scenario onderzoek
Fase 6:	Afsluiting project en advies

Tabel 2.1 Fasering van het afstudeeronderzoek

2.1.4 Betrokkenen

Het onderstaande overzicht (Figuur 2.3) geeft inzicht in de personen die bij deze afstudeeropdracht betrokken zijn geweest;

Afstudeerder	Examinator en Begeleider	Examinator en Toezichthouder
Arjan de Jong student Information Security Management	Marjolein Faassen De Haagse Hogeschool	Henk van de Ven De Haagse Hogeschool

Opdrachtgever	Afstudeerbegeleider
Gé Iking Centric Nederland B.V.	Gé Iking Centric Nederland B.V.

Figuur 2.3 Betrokkenen bij deze afstudeeropdracht

3 Aanpak bepalen

Dit hoofdstuk beschrijft de wijze waarop de planning van het afstudeeronderzoek tot stand is gekomen.

3.1 De doelstelling

Deze eerste fase heeft tot doel gehad om de aanpak van het afstudeeronderzoek te bepalen. Hiervoor zijn een tweetal documenten opgeleverd, het afstudeerplan en het Project Initiation Document.

3.2 De gehanteerde werkwijze en methoden

3.2.1 Scope vaststellen

De scope van deze afstudeeropdracht betreft het onderzoeken van de toepassingsmogelijkheden van het concept van het gebruik van anonieme attributen ter behoeve van de autorisatie van gebruikers. Het onderzoek richt zich niet tot de vraag van welk van de bestaande oplossingen geschikt zou kunnen zijn voor Centric en ook de technische achtergrond waaronder de cryptografie waarop het concept is gebaseerd wordt niet in het onderzoek meegenomen. Het onderzoek beantwoord enkel de vraag of het gebruik van anonieme attributen nuttig kan zijn voor Centric en haar klanten. Om deze scope te kunnen vaststellen hebben er al voorafgaande aan het afstuderen een tweetal gesprekken plaatsgevonden met de opdrachtgever.

3.2.2 Afstudeerplan

Voorafgaande aan de afstudeerstage is er een afstudeerplan opgeleverd aan De Haagse Hogeschool en de afstudeerbegeleider vanuit Centric. Naar aanleiding van de verkregen feedback vanuit De Haagse Hogeschool en Centric heb ik me gedurende de eerste week bezig gehouden met het actualiseren van dit afstudeerplan. Hierbij zijn de probleemstelling en doelstelling van de afstudeeropdracht scherper geformuleerd en zijn de uit te voeren werkzaamheden en de op te leveren tussenproducten aangevuld.

De fasering van het onderzoek is gebaseerd op Nel Verhoeven (Wat is onderzoek). Daarbij komen niet alle fasen overeen met Nel Verhoeven, ik heb hier namelijk deels mijn eigen invulling aan gegeven om zodoende beter aan te kunnen sluiten op het uit te voeren onderzoek. De onderstaande tabel geeft een overzicht weer van de fasering van het onderzoek zoals was opgesteld in het afstudeerplan;

Fase	Omschrijving
Fase 1:	Opstellen van een plan van aanpak aan de hand van de Prince2 methodiek.
Fase 2:	Uitvoeren van literatuuronderzoek naar de wijze waarop huidige IAM systemen eruitzien en werken, welke systemen er naast de reeds bekende (IDEMX van IBM en UPROVE van Microsoft) er zijn welke voldoen aan het criteria "de gebruiker toegang verlenen op basis van attributen in plaats van op basis van zijn identiteit".
Fase 3:	Het vaststellen van requirements waaraan de IAM systemen aan dienen te voldoen.
Fase 4:	Uitvoeren van productonderzoek naar IDEMIX van IBM en UPROVE van Microsoft om vast te stellen of deze systemen voldoen aan de requirements. Indien er uit het vooronderzoek is gebleken dat er ook andere systemen beschikbaar zijn zal de overweging worden gemaakt om deze wel of niet in het onderzoek mee te nemen.
Fase 5:	Aan de hand van de theorie of een praktijktest (in een proefopstelling) vaststellen welke

	systeem het meest geschikt is voor gebruik door Centric.
Fase 6:	Het opstellen van een adviesrapport voor Centric met daarin de wijze waarop het onderzoek is uitgevoerd, welke resultaten het onderzoek heeft opgeleverd en een overzicht van de voors en tegens ten opzichte van het gebruik door Centric.

Tabel 3.1 De fasering van het onderzoek volgens het afstudeerplan

In overleg met mijn afstudeerbegeleider zijn de op te leveren (tussen)producten bepaald, in de onderstaande tabel worden per fase de op te leveren (tussen)producten weergegeven zoals was beschreven in het afstudeerplan;

Fase	(Tussen)producten
Fase 1:	• Afstudeerplan • Project Initiation Document
Fase 2:	-
Fase 3:	• Rapportage van het productonderzoek (inclusief de requirements waaraan de systemen dienen te voldoen).
Fase 4:	
Fase 5:	• Rapportage van bevindingen aan de hand van de theorie of praktijktest naar de werking en functionaliteiten van Idemix en U-Prove.
Fase 6:	• Adviesrapportage richting Centric.

Tabel 3.2 De op te leveren (tussen)producten volgens het afstudeerplan

Het afstudeerplan is tot stand gekomen aan de hand van overleg met mijn afstudeerbegeleider en de verkregen feedback vanuit De Haagse Hogeschool.

Na oplevering van het afstudeerplan aan De Haagse Hogeschool volgde er nogmaals feedback op het plan. De te demonstreren competenties bevatte in eerste instantie enkel de algemene competenties en moest dan ook worden aangevuld met vakspecifieke competenties. Daarbij was het ook noodzakelijk om in het afstudeerplan op te nemen op welke wijze er gedurende het afstuderen invulling zou worden geven aan deze competenties.

Het afstudeerplan is aan dit document toegevoegd in bijlage A.

3.2.3 Probleemanalyse

Naar aanleiding van de feedback vanuit De Haagse Hogeschool op de probleemstelling in het afstudeerplan heb ik besloten om een probleemanalyse uit te voeren aan de hand van de 6W-formule[2] van Nel Verhoeven. Hierbij zijn onderstaande vragen beantwoord. Het resultaat hiervan is in zowel het afstudeerplan als het Project Initiation Document terug te vinden.

- Wat is het probleem?
- Wie heeft het probleem?
- Wanneer is het probleem ontstaan?
- Waarom is het een probleem?
- Waar doet het probleem zich voor?
- Wat is de aanleiding van het probleem?

De uiteindelijke probleemstelling bestaat uit een centrale vraag en een viertal deelvragen.

[2] Wat is onderzoek | Nel Verhoeven | pagina 80

- Onderzoek voor Centric en haar klanten de toepassingsmogelijkheden van Identity & Access Management op basis van anonieme attributen in plaats van identiteiten.

De deelvragen:

- Wat wordt er bedoeld met anonieme attributen?
- Waar worden anonieme attributen voor gebruikt?
- In welke situaties kan er gebruik worden gemaakt van anonieme attributen?
- Waarom zou dit nuttig kunnen zijn voor Centric?

Om tot deze probleemstelling en centrale- en deelvragen te komen hebben er diverse gesprekken plaatsgevonden met de opdrachtgever.

3.2.4 Begripsafbakening

In de centrale vraag van het onderzoek worden twee begrippen genoemd, Identity & Access Management en Anonieme attributen. Om een helder beeld te krijgen van wat er met deze begrippen wordt bedoeld heb ik gezocht naar definities betreffende deze onderwerpen. Hieronder wordt weergegeven hoe deze begrippen in mijn afstudeeropdracht wordt bedoeld.

Identity & Access Management:

Er zijn vele definities voor het begrip Identity & Access Management, de definitie die Rob van de Staaij in zijn boek Identiteitsmanagement beschrijft past naar mijn idee het beste bij mijn afstudeeronderzoek;

" Identiteitsmanagement is het op efficiënte, veilige en transparante wijze overzien, beheren en beschermen van identiteits- en toegangsgegevens van personen en entiteiten. "

De reden dat ik deze definitie zal aanhouden in mijn onderzoek is de toevoeging welke Rob van de Staaij aan deze definitie heeft meegegeven;

" Het is eigenlijk niet goed mogelijk om een dergelijk complex en veelomvattend begrip in een paar woorden samen te vatten "

Met het begrip Identity & Access Management wordt in mijn afstudeeronderzoek dan ook het gehele proces van beheren en beschermen van identiteits- en toegangsgegevens van personen en entiteiten bedoeld.

Anonieme attributen:

Het begrip anonieme attributen wordt in de literatuur door onder meer professor Bart Jacobs[3] en Patrik Bichsel en Jan Camenisch[4] omschreven als alle (persoonlijke) eigenschappen en kenmerken[5] van een persoon of groep personen welke anoniem gebruikt kunnen worden in een autorisatieproces.

[3] B. Jacobs | Attributen in plaats van Identiteiten | http://www.cs.ru.nl/B.Jacobs/PAPERS/IT-auditor-1-2013-irma.pdf

[4] P. Bichsel en J. Camenisch | Mixing Identities with Ease | http://www.zurich.ibm.com/pdf/security/idemix/BC2010-Mixing_Identities_with_Ease.pdf

[5] Als de naam, leeftijd en woonplaats van een persoon, maar ook de functie binnen een organisatie waarin iemand werkzaam is worden erkend als een persoonlijke eigenschap.

3.2.5 Project Initiation Document

Gedurende de tweede week van het afstuderen is er een plan van aanpak opgesteld, hiervoor heb ik gebruik gemaakt van de structuur van een Project Initiation Document (PID) volgens de Prince 2 methodiek. Ik heb bewust voor deze methodiek gekozen, omdat deze in voorgaande projecten tijdens mijn studie met succes is toegepast.

In de onderstaande tabel wordt de fasering van het onderzoek weergegeven;

Fase	Omschrijving
Fase 1:	Aanpak bepalen
Fase 2:	Vooronderzoek
Fase 3:	Vaststellen requirements
Fase 4:	Productonderzoek
Fase 5:	Scenario onderzoek
Fase 6:	Afsluiting project en advies

Tabel 3.3 De fasering van het onderzoek volgens het PID

De Fasering van het afstudeeronderzoek is gebaseerd op de door Nel Verhoeven beschreven fasen in onderzoek[6], Omdat deze fasen niet één op één overgenomen konden worden in mijn onderzoek heb ik deze aangepast en heb ik de fase requirements analyse eraan toegevoegd.

In de onderstaande tabel worden de op te leveren (tussen)producten weergegeven;

Fase	(Tussen)producten
Fase 1:	• Afstudeerplan • Probleemanalyse • Project Initiation Document
Fase 2:	• Achtergrond Identity & Access Management • Achtergrond Privacy wetgeving • Achtergrond Anonieme attributen
Fase 3:	
Fase 4:	• Productonderzoek
Fase 5:	• Scenario onderzoek
Fase 6:	• Advies- en onderzoeksrapport

Tabel 3.4 De op te leveren (tussen)producten volgens het PID

Deze (tussen)producten zijn in overleg met mijn afstudeerbegeleider tot stand gekomen. Om de voortgang van het project te kunnen managen hebben we tevens de afspraak gemaakt om gedurende het gehele afstudeertraject iedere maandag morgen een uur in te roosteren om de stand van het onderzoek door te kunnen nemen.

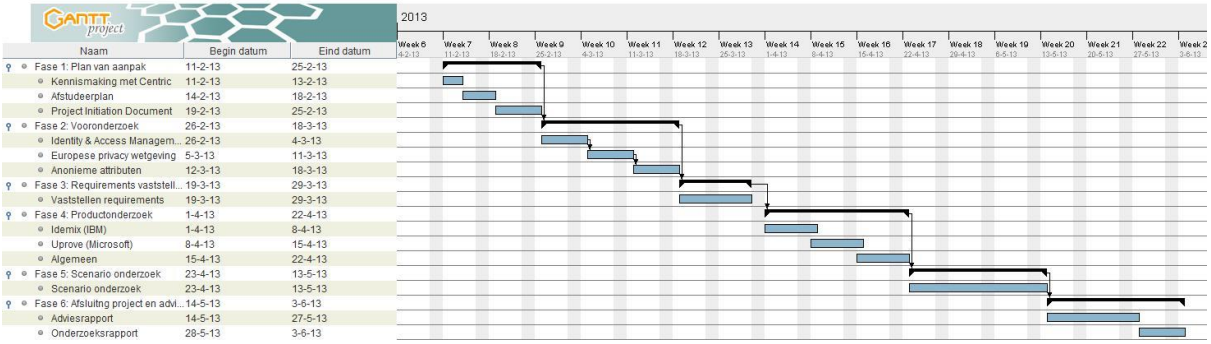
3.2.6 Verschillen tussen het afstudeerplan en PID

Het PID dat gedurende de tweede week van de afstudeerperiode is opgesteld bevatte wat inhoudelijke verschillen ten opzichte van het eerder opgeleverde afstudeerplan. Dit komt doordat er tijdens het opstellen van het PID meer inzicht was in de uit te voeren afstudeeropdracht dan op het moment van het opstellen van het afstudeerplan.

[6] Wat is onderzoek | Nel Verhoeven | Pagina 41

3.2.7 Verschillen tussen het afstudeerplan en PID

De opsplitsing van de fasen waaruit het onderzoek zal gaan bestaan is uitgewerkt in een Gannt Chart, welke is weergegeven in onderstaand figuur (Figuur 3.1).



Naam	Begin datum	Eind datum
Fase 1: Plan van aanpak	11-2-13	25-2-13
Kennismaking met Centric	11-2-13	13-2-13
Afstudeerplan	14-2-13	18-2-13
Project Initiation Document	19-2-13	25-2-13
Fase 2: Vooronderzoek	26-2-13	18-3-13
Identity & Access Managem...	26-2-13	4-3-13
Europese privacy wetgeving	5-3-13	11-3-13
Anonieme attributen	12-3-13	18-3-13
Fase 3: Requirements vaststell...	19-3-13	29-3-13
Vaststellen requirements	19-3-13	29-3-13
Fase 4: Productonderzoek	1-4-13	22-4-13
Idemix (IBM)	1-4-13	8-4-13
Uprove (Microsoft)	8-4-13	15-4-13
Algemeen	15-4-13	22-4-13
Fase 5: Scenario onderzoek	23-4-13	13-5-13
Scenario onderzoek	23-4-13	13-5-13
Fase 6: Afsluitng project en advi...	14-5-13	3-6-13
Adviesrapport	14-5-13	27-5-13
Onderzoeksrapport	28-5-13	3-6-13

Figuur 3.1 Gannt Chart

4 Vooronderzoek – Fase 2

Dit hoofdstuk beschrijft de beoogde doelstelling, de gehanteerde werkwijze en methoden en de uiteindelijke resultaten van het vooronderzoek (fase 2).

4.1 De doelstelling

Het doel van deze fase is het opdoen van achtergrond kennis van de onderwerpen Identity & Access Management, de nieuwe Europese privacywetgeving en het concept van anonieme attributen om zodoende de rest van het afstudeeronderzoek te kunnen uitvoeren. Na afloop van deze fase zullen ook de geselde deelvragen 1. Wat wordt er bedoeld met anonieme attributen? En 2. Waar worden anonieme attributen gebruikt? beantwoord kunnen worden.

4.2 De gehanteerde werkwijze en methoden

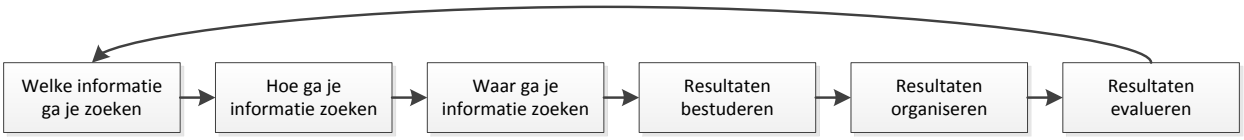
Deze paragraaf beschrijft de gehanteerde werkwijze en methoden gedurende het vooronderzoek.

4.2.1 Deskresearch

Om algemene kennis te kunnen opdoen van de onderwerpen Identity & Access Management, de nieuwe Europese privacywetgeving en het concept van anonieme attributen is er een literatuuronderzoek uitgevoerd. Hierbij is gebruik gemaakt van de Big 6™ methode om vast te stellen hoe het literatuuronderzoek uitgevoerd zal worden en naar welke informatie er gezocht zal gaan worden om de in de doelstelling van dit hoofdstuk beschreven vragen te kunnen beantwoorden. Daarnaast is er gebruik gemaakt van de Sneeuwbal methode om zodoende meer literatuur te kunnen vinden.

Big 6™

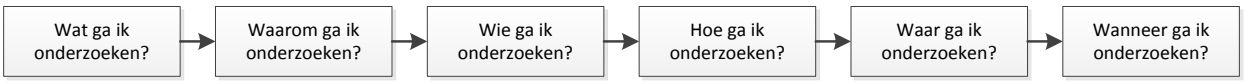
Om de juiste informatie te kunnen vinden den de hoeveelheid aan informatie niet uit de hand te laten lopen heb ik ervoor gekozen om de Big 6™ methode van onder meer Berkowitz[7] (Figuur 4.1**Fout! Verwijzingsbron niet gevonden.**) toe te passen. Deze methode helpt ervoor te zorgen dat het literatuuronderzoek niet te groot wordt en dat er op een gerichte manier naar de juiste informatie wordt gezocht. Hiervoor had ik ook gebruik kunnen maken van de onderzoekscyclus van Nel Verhoeven[8] (Figuur 4.2), maar omdat ik de vragen van de Big 6™ beter bij het onderzoek vind passen en deze ook ingaan op het verwerken van de resultaten heb ik niet voor de onderzoekscyclus van Nel Verhoeven gekozen.



Figuur 4.1 De Big 6™ (Eisenberg & Berkowitz, 1992; Canning, 2002)

[7] Wat is onderzoek | Nel Verhoeven | pagina 62

[8] Wat is onderzoek | Nel Verhoeven | pagina 39



Figuur 4.2 De onderzoekscyclus Nel Verhoeven (vooruit kijken)

Informatie verzamelen;

Voorafgaande aan het vooronderzoek heb ik de eerste drie vragen uit de Big 6™ methode beantwoord.

1). Welke informatie ga je zoeken?

Het vooronderzoek zal zich richten tot het verkrijgen van informatie over Identity & Access Management, de nieuwe Europese privacywetgeving en het concept van anonieme attributen, om zodoende de benodigde kennis op te kunnen doen voor de rest van het afstudeeronderzoek.

2). Hoe ga je informatie zoeken?

De benodigde literatuur zal voornamelijk worden verzameld met behulp van zoekmachines Google en Google Scholar. De hiervoor te gebruiken zoektermen worden in onderstaande tabel (Tabel 4.1) per onderwerp weergegeven.

Onderwerp	Zoektermen
Identity & Access Management	" Identity & Access Management " " Identity Management " " Access Management " Identity & Access Management IAM
De nieuwe Europese privacywetgeving	" Europese privacywetgeving " " General Data Protection Regulation " GDPR
Het concept van anonieme attributen	" Anonieme attributen " " Anonymous Credentials " " IBM Idemix " " Microsoft U-Prove " " Idemix U-Prove " Idemix U-Prove

Tabel 4.1 Zoektermen per onderwerp

Om zoveel mogelijk literatuur te kunnen verzamelen zal ik ook mijn afstudeerbegeleider benaderen met de vraag welke relevante bronnen en literatuur hij heeft betreffende deze onderwerpen.

3). Waar ga je informatie zoeken?

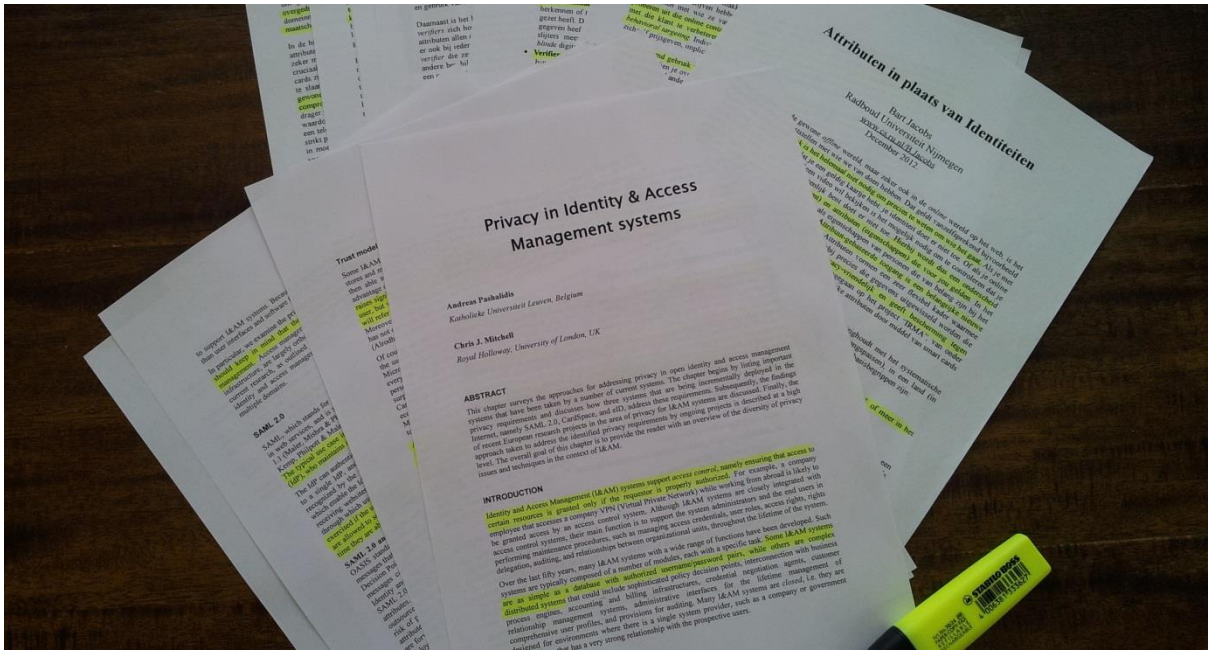
Er zal gezocht worden naar wetenschappelijke artikelen en onderzoeksverslagen betreffende de bovengenoemde onderwerpen in zowel de Nederlandse als Engelse taal.

Informatie analyseren;

Aansluitend op het verzamelen van de literatuur heb ik de laatste drie stappen uit de Big 6™ methode uitgevoerd.

4). Resultaten bestuderen

De verkregen informatie heb ik geïnventariseerd op de aanwezigheid van de eerder genoemde zoektermen in (Tabel 4.1) de relevante stukken uit deze documenten heb ik daarbij gemarkeerd om zo in een later stadium eenvoudig weer deze informatie te kunnen raadplegen (Figuur 4.3).



Figuur 4.3 Resultaten bestuderen

5). Resultaten organiseren

De relevante bronnen zijn opgenomen in een Excel sheet om deze in een later stadium van het onderzoek eenvoudig te kunnen raadplegen.

6). Resultaten evalueren

Met behulp van de verkregen informatie heb ik naar mijn idee voldoende kennis opgedaan over de onderwerpen Identity & Access Management en de nieuwe Europese Privacywetgeving. Over het concept van anonieme attributen had ik naar mijn mening nog onvoldoende literatuur verzameld om verder te kunnen gaan met het onderzoek en dus te starten met de volgende fase. Hoewel het gebruikelijk is om in zo'n situatie opnieuw te starten bij punt 1 heb ik ervoor gekozen om doormiddel van de sneeuwbal methode aanvullende literatuur te verzamelen.

Sneeuwbal

Naast het gebruik maken van de Big 6™ methode heb ik dus ook de sneeuwbal methode toegepast. Dit is een handige manier van literatuur zoeken, met als enige nadeel dat er vaak enkel (ver)ouder(d)e literatuur wordt gevonden. Hiervoor heb ik uitsluitend gebruik gemaakt van de literatuur welke ik relevant acht voor het onderzoek. De verwijzingen uit deze bronnen heb ik doorgelopen om zo nieuwe bronnen te kunnen verzamelen die op mijn onderzoek van toepassing zijn.

Deze methode heb ik voornamelijk gebruikt om meer literatuur te kunnen vinden betreffende het concept van anonieme attributen. Uiteindelijk heb ik hierdoor voldoende informatie en kennis kunnen opdoen om te starten met de volgende fase van het onderzoek.

4.2.2 Bijeenkomsten

Om meer informatie te kunnen verzamelen betreffende het afstudeeronderwerp – het concept van anonieme attributen – heb ik ervoor gekozen om een tweetal bijeenkomsten bij te wonen. De reden dat ik hiervoor gekozen heb is dat er vaak diverse experts aanwezig zijn bij dergelijke bijeenkomsten en de onderwerpen mogelijkerwijs aan zouden kunnen sluiten op mijn afstudeeronderzoek.

Bijeenkomst Platform voor Informatiebeveiliging

Het Platform voor Informatiebeveiliging (PvIB)[9] organiseerde een bijeenkomst ~~in Gouda~~ voor haar leden met als thema: Nieuwe ontwikkelingen rond Identity Management.

Hoewel uit het literatuuronderzoek is gebleken dat het concept van anonieme attributen al meer dan tien jaar oud is, is het mij ook duidelijk geworden dat er pas sinds de laatste drie jaar intensief onderzoek wordt uitgevoerd naar het concept van anonieme attributen. Voorafgaande aan de bijeenkomst had ik dan ook de verwachting dat dit thema zou kunnen aansluiten op mijn afstudeeronderzoek.

De onderwerpen welke gedurende de avond aan bod zijn gekomen bleken echter niet of onvoldoende aan te sluiten op mijn onderzoek. Het enige dat enigszins aansloot op mijn onderzoek was de probleemstelling in één van de presentaties was het niet hoeven of kunnen gebruiken van identiteiten en/of identificerende gegevens ter behoeve van de autorisatie van een gebruiker of groep gebruiker(s). Als oplossing voor dit probleem werd het gebruik van Social Sign In genoemd (inloggen via sociale media als Facebook en Google+). Hoewel mijn onderzoek zich op een andere oplossing richt voor dit probleem was het wel nuttig om vast te kunnen stellen dat dit probleem niet alleen Centric speelt.

Aan het einde van de avond volgde er nog een vragen ronde waarbij één van de aanwezigen een vraag stelde aan de vier gastsprekers van de avond over het gebruik van anonieme attributen. Deze vraag "Is het gebruik kon echter niet door hen beantwoord worden

Na afloop van deze avond was er voor het aanwezige publiek de mogelijkheid om vragen te stellen aan de gastsprekers. Vanuit het publiek volgde de vraag of het gebruik van anonieme attributen ook gezien kan worden als een nieuwe ontwikkeling op het gebied van Identity Management. Geen van de gastsprekers kond daar een antwoord op geven omdat zij niet of onvoldoende bekend waren met het onderwerp, en ook vanuit het publiek volgde er geen reactie op deze vraag.

[9] Platform voor InformatieBeveiliging | http://www.pvib.nl

Deze bijeenkomst heeft helaas niet kunnen voldoen aan de verwachtingen die ik ervan had.

Bijeenkomst Platform Identity Management Nederland

Het Platform Identity Management Nederland (PIMN)[10] en het Platform voor de informatiesamenleving (ECP)[11] organiseerde een bijeenkomst in Delft voor haar leden met als thema: Online leeftijdsverificatie in Nederland. Leeftijdsverificatie is in de literatuur een veelgenoemde voorbeelden van situaties waarbij er gebruik gemaakt kan worden van anonieme attributen.

Ook van deze bijeenkomst had ik vooraf dan ook de verwachting dat het zou kunnen aansluiten op mijn afstudeeronderzoek. In twee van de vier presentaties werd het gebruik van anonieme attributen aangehaald als een mogelijke oplossing voor de online leeftijdsverificatie. Er werden echter meerdere oplossingen benoemd, waardoor er niet inhoudelijk in deze oplossing werd ingegaan. Wel werd er meer duidelijk over het Nederlandse IRMA project dat onderzoek doet naar het gebruik van anonieme attributen. Zij zijn er in geslaagd om leeftijdsverificatie mogelijk te maken zonder dat er identificerende gegevens kenbaar worden gemaakt aan de dienstverlener. Deze dienstverlener (bijvoorbeeld een slijter) krijgt enkel te zien of een gebruiker (klant) ouder is dan de minimum leeftijd.

4.2.3 Interviews

Om inzicht te kunnen krijgen in de wijze waarop Identity & Access Management wordt toegepast binnen Centric hebben er vier interviews plaatsgevonden met experts binnen Centric die zich bezig houden met Identity & Access Management. Hiervoor is gekozen voor een ongestructureerd interview zoals beschreven in het boek wat is onderzoek van Nel Verhoeven[12], waarbij de gesprekspartner eerst heeft toegelicht op welke wijze betrokken te zijn bij Identity & Access Management waarna er vervolgens ruimte was voor inhoudelijke vragen rondom dit proces.

Er is enkel gesproken met medewerkers vanuit de eigen organisatie, omdat deze interviews tot doel hadden om inzicht te krijgen in de wijze waarop Centric het Identity & Access Management proces toepast.

In onderstaande tabel (Tabel 4.2) is een overzicht weergegeven van de deelnemers aan deze interviews en de behandelde onderwerpen.

Deelnemer onderzoek	Onderwerp interview	Afdeling
Thomas van der Bijl	Identity & Access Management	Housing & Healthcare
Dennis Boerboom	Identity & Access Management	Governance & Infra Services
Koen Laan	Identity & Access Management	-
Rene Bliekendaal	Identity & Access Management	SMC – Gouda

Tabel 4.2 deelnemers interviews

Deze interviews hebben naar mijn idee goed duidelijk gemaakt op welke wijze Identity & Access Management op dit moment binnen Centric wordt toegepast. Het interview met Thomas van der Bijl was voor mijn onderzoek het meest relevant, dit gaf mij namelijk ook ideeën voor fase 5 (het scenario onderzoek). Binnen de afdeling Housing & Healthcare worden er verschillende applicaties

[10] Platform Identity Management Nederland | http://www.pimn.nl

[11] Platform voor de Informatiesamenleving | http://www.ecp.nl

[12] Wat is onderzoek | Nel Verhoeven | pagina 150

ontwikkeld waarbij het concept van anonieme attributen in de toekomst toegepast zou kunnen gaan worden.

4.3 De resultaten

De belangrijkste resultaten van het vooronderzoek worden in deze paragraaf beschreven. Afsluitend aan deze fase zijn een tweetal deelproducten opgeleverd aan mijn afstudeerbegeleider. Het eerste document betreft de achtergrond van Identity & Access Management en het tweede document betreft de achtergrond van de nieuwe Europese privacywetgeving. De resultaten betreffende het concept van anonieme attributen zijn in deze fase nog niet verwerkt en zullen worden meegenomen naar fase 4 (het productonderzoek).

4.3.1 Definitie Identity & Access Management

Gedurende het literatuuronderzoek ben ik meerdere definities tegen gekomen van het begrip Identity & Access Management. De definitie[13] die Rob van de Staaij in zijn boek Identiteitsmanagement beschrijft past naar mijn idee het beste bij mijn afstudeeronderzoek;

" Identiteitsmanagement is het op efficiënte, veilige en transparante wijze overzien, beheren en beschermen van identiteits- en toegangsgegevens van personen en entiteiten. "

De reden dat ik deze definitie zal aanhouden in mijn onderzoek is de toevoeging welke Rob van de Staaij aan deze definitie heeft meegegeven;

" Het is eigenlijk niet goed mogelijk om een dergelijk complex en veelomvattend begrip in een paar woorden samen te vatten "

Met het begrip Identity & Access Management wordt in mijn afstudeeronderzoek dan ook het gehele proces van beheren en beschermen van identiteits- en toegangsgegevens van personen en entiteiten bedoeld.

4.3.2 Concept van anonieme attributen

Uit het vooronderzoek is gebleken dat er sinds 2001 een tweetal oplossingen bestaan welke het gebruik van anonieme attributen mogelijk kunnen maken. Dit zijn Microsoft U-Prove en IBM Idemix. Beiden zijn ze nog nauwelijks in de praktijk toegepast. Enkel Microsoft heeft haar oplossing in een tweetal applicaties op hun oplossing gebaseerd, Microsoft Passport en Windows CardSpace. Beide applicaties worden inmiddels niet langer door Microsoft doorontwikkeld om zodoende naar eigen zeggen ruimte te kunnen maken voor de doorontwikkeling van Microsoft U-Prove[14]. Daarnaast is uit het literatuuronderzoek gebleken dat er een aantal onderzoeksprojecten lopen naar het gebruik van anonieme attributen, waaronder het Nederlandse IRMA project van onder meer de Radboud Universiteit Nijmegen en het Europese ABC4Trust welke op dit moment verder zijn met hun onderzoeken dan de overige onderzoeksprojecten.

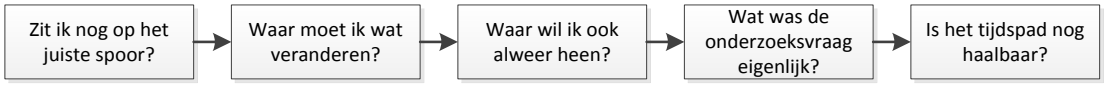
4.3.3 Achterom kijken

Aan het einde van deze fase heb ik aan de hand van de onderzoekscyclus van Nel Verhoeven (Figuur 4.4) terug gekeken op het uitgevoerde onderzoek en de resultaten. Door met mijn

[13] Identiteitsmanagement | Rob van der Staaij | pagina

[14] RIP, Windows CardSpace. Hello, U-Prove | http://www.zdnet.com/blog/microsoft/rip-windows-cardspace-hello-u-prove/8717

afstudeerbegeleider in gesprek te gaan hierover heb ik kunnen vaststellen dat ik op de goede weg zit en inmiddels voldoende kennis heb opgedaan om verder te kunnen gaan met de volgende fase van het onderzoek, de requirements analyse.



Figuur 4.4 De onderzoekscyclus Nel Verhoeven (achterom kijken)

5 De requirements analyse – Fase 3

Dit hoofdstuk beschrijft de beoogde doelstelling, de gehanteerde werkwijze en methoden en de uiteindelijke resultaten van fase 3, de requirements analyse.

5.1 De doelstelling

Om de wensen en eisen van de opdrachtgever aan het uiteindelijke adviesrapport in kaart te brengen is er in fase 3 een requirements analyse uitgevoerd. Deze fase is bewust na het vooronderzoek gepland, omdat er dan al voldoende informatie zou zijn

5.2 De gehanteerde werkwijze en methoden

Om de eisen aan het uiteindelijke adviesrapport vast te kunnen stellen is er doormiddel van de MoSCoW-methode een overzicht gemaakt van deze eisen. Hiervoor is gekozen omdat er met behulp van deze methode een duidelijk beeld ontstaat aan welke eisen er minimaal voldaan dient te worden, welke eisen optioneel zijn en welke eisen er in dit project niet aan bod zullen komen.

5.2.1 MoSCoW-methode

Doormiddel van de MoSCoW-methode[15] is er in kaart gebracht welke eisen er worden gesteld aan het eindresultaat (het uiteindelijke adviesrapport).

MoSCoW-methode	Beschrijving
Must haves	Deze eisen moeten in het eindresultaat terugkomen, zonder deze eis is het product niet bruikbaar.
Should haves	Deze eisen zijn zeer gewenst, maar zonder is het product wel bruikbaar.
Could haves	Deze eisen zullen alleen aan bod komen als er tijd genoeg is.
Won't haves	Deze eisen zullen in dit project niet aan bod komen, maar kan in de toekomst, bij een vervolgproject interessant zijn.

Tabel 5.1 De MoSCoW-methode

Om deze eisen in kaart te kunnen brengen hebben er gesprekken plaatsgevonden met mijn afstudeerbegeleider.

5.3 De resultaten

Hieronder worden de eisen weergegeven die we aan het adviesrapport hebben gesteld;

[15] MoSCoW-methode | http://nl.wikipedia.org/wiki/MoSCoW-methode

Must haves:

- Het adviesrapport moet ten minste duidelijk maken in welke situaties het concept van anonieme attributen wel en niet te gebruiken is.
- Het adviesrapport moet ten minste duidelijk maken op welke wijze het toegepast kan worden in Persoon – Service en Service – Service autorisatieprocessen.
- Het adviesrapport moet ten minste duidelijk maken waarom er gebruik gemaakt zou moeten worden van het concept van anonieme attributen.
- Theoretische situatiebeschrijving waarbij het concept van anonieme attributen toegepast kan worden

Should haves:

- De (hulp)middelen welke gebruikt kunnen worden in het autorisatieproces.
- De bij een autorisatieproces betrokken partijen.
- Situatiebeschrijvingen waarbij het concept van anonieme attributen toegepast kan worden die van toepassing zijn op Centric.

Could haves:

- De resultaten van de onderzoeksprojecten (IRMA en ABC4Trust).

Wont haves:

- Het adviesrapport zal niet ingaan op de technische achtergrond van de mogelijke oplossingen.
- Het adviesrapport zal niet ingaan op de cryptografische achtergrond van de mogelijke oplossingen.
- Het adviesrapport zal niet ingaan op de vraag welk van de beschikbare oplossingen het meest geschikt is voor Centric en haar klanten.

5.3.1 Achterom kijken

Voorafgaande aan deze fase had ik het idee dat er gedurende deze fase de eisen en wensen aan de beschikbare tooling zouden worden vastgesteld. Aangezien het onderzoek zich echter minimaal tot de beschikbare tooling richt bleek dit een onjuiste verwachting. Hierop heb ik deze fase gebruikt om de eisen en wensen aan het uiteindelijke adviesrapport vast te kunnen stellen. Uit de gesprekken met mijn afstudeerbegeleider is gebleken dat ik nog steeds op de goede weg ben, maar dat ik me niet teveel moet richten op de tooling en meer op het concept zelf.

6 Het productonderzoek

Dit hoofdstuk beschrijft de beoogde doelstelling, de gehanteerde werkwijze en methoden en de uiteindelijke resultaten van het uitgevoerde productonderzoek in fase 4.

6.1 De doelstelling

Uit het vooronderzoek is gebleken dat er sinds 2001 een tweetal oplossingen bestaan welke gebaseerd zijn op het concept van anonieme attributen. Dit zijn Microsoft U-Prove[16] en IBM Idemix[17]. Om Centric aan het einde van deze afstudeeropdracht te kunnen adviseren over de toepassingsmogelijkheden van het concept van anonieme attributen heb ik ervoor gekozen om de mogelijkheden en functionaliteiten van beide oplossingen in kaart te brengen. Uit de requirements analyse van de voorgaande fase is gebleken dat het uiteindelijke advies minimaal antwoord moet geven op een viertal vragen. Het doel van deze fase is dan ook het verzamelen en analyseren van informatie betreffende de mogelijkheden en functionaliteiten van beide oplossingen en deze te beschrijven in een rapportage (het productonderzoek, Bijlage E) om een antwoord te kunnen geven op deze vragen. Doormiddel van het productonderzoek zal uiteindelijk een antwoord gegeven kunnen worden op deelvraag 4 van het onderzoek: Waarom zou dit nuttig kunnen zijn voor Centric en haar klanten en hoe kan Centric dit gebruiken?

6.2 De gehanteerde werkwijze en methoden

Deze paragraaf beschrijft de gehanteerde werkwijze en methoden gedurende het productonderzoek.

6.2.1 Deskresearch

Om een antwoord te kunnen geven op de vraag: wat zijn de mogelijkheden en de functionaliteiten van IBM Idemix en Microsoft U-Prove heb ik een literatuuronderzoek uitgevoerd. De gebruikte methoden uit het vooronderzoek zijn goed bevallen en zijn daarom dan ook in deze fase opnieuw gehanteerd.

Big 6™

Ook deze in deze fase is er gebruik gemaakt van de Big 6™ methode. Ik heb hiervoor gekozen omdat het me in de voorgaande fasen voldoende houvast heeft gegeven voor de uitvoer van de literatuurstudies.

<u>Informatie verzamelen;</u>

Voorafgaande aan het vooronderzoek heb ik de eerste drie vragen uit de Big 6™ methode beantwoord.

1). Welke informatie ga je zoeken?

Het literatuuronderzoek zal zich richten tot het verkrijgen van informatie over de mogelijkheden en functionaliteiten van IBM Idemix, Microsoft U-Prove en het concept van anonieme attributen, om vervolgens een antwoord te kunnen geven op deelvraag 4 van het onderzoek.

2). Hoe ga je informatie zoeken?

[16] IBM Idemix http://www.zurich.ibm.com/security/idemix/

[17] Microsoft U-Prove http://research.microsoft.com/en-us/projects/u-prove/

De benodigde literatuur zal voornamelijk worden verzameld met behulp van zoekmachines Google en Google Scholar. De hiervoor te gebruiken zoektermen worden in onderstaande tabel (Tabel 4.1) per onderwerp weergegeven. Deze zoektermen worden ook met elkaar gecombineerd om zodoende meer literatuur te kunnen verzamelen. Omdat de mogelijkheden en functionaliteiten van beide oplossingen na verloop van tijd kunnen veranderen zal er ook gebruik gemaakt worden van de filters in de genoemde zoekmachines om ook gericht te kunnen zoeken naar recentelijke literatuur. Hiervoor zullen de filters "Afgelopen jaar" en "Afgelopen maand" worden gebruikt.

Daarnaast wordt er gebruik gemaakt van de in voorgaande fasen verzamelde literatuur.

Onderwerp	Zoektermen
Het concept van anonieme attributen	" Anonymous credentials " Anonymous credentials " " Anonieme attributen " Anonieme attributen
IBM Idemix	" IBM Idemix " IBM Idemix
Microsoft U-Prove	" Microsoft U-Prove " Microsoft U-Prove

Tabel 6.1 Zoektermen per onderwerp

3). Waar ga je informatie zoeken?

Er zal gezocht worden naar wetenschappelijke artikelen en onderzoeksverslagen betreffende de bovengenoemde onderwerpen in zowel de Nederlandse als Engelse taal. Hiervoor zullen naast de publicaties van IBM en Microsoft ook de publicaties van de onderzoeksprojecten als het Nederlandse IRMA project, het Europese ABC4Trust en de bij deze projecten aangesloten universiteiten (Katholieke Universiteit Leuven en de Radboud Universiteit Nijmegen) worden geraadpleegd.

<u>Informatie analyseren;</u>

Aansluitend op het verzamelen van de benodigde literatuur heb ik de laatste drie stappen uit de Big 6^{TM} methode uitgevoerd.

4). Resultaten bestuderen

De verkregen informatie heb ik geïnventariseerd op de aanwezigheid van de eerder genoemde zoektermen in (Tabel 4.1) de relevante stukken uit deze documenten heb ik daarbij gemarkeerd om zo in een later stadium eenvoudig weer deze informatie te kunnen raadplegen

5). Resultaten organiseren

De relevante bronnen zijn opgenomen in een Excel sheet om deze in een later stadium van het onderzoek eenvoudig te kunnen raadplegen.

6). Resultaten evalueren

Met behulp van de verkregen informatie uit het uitgevoerde literatuuronderzoek heb ik een overzicht kunnen maken van de mogelijkheden en functionaliteiten van beide oplossingen en deze beschreven in het document: productonderzoek.

Sneeuwbal

Hoewel het uitgevoerde literatuuronderzoek door middel van de Big 6™ methode voldoende informatie heeft opgeleverd om de gestelde vragen te kunnen beantwoorden heb ik wederom ook de sneeuwbal methode toegepast. De verwijzingen in de literatuur welke van toepassing waren op mijn onderzoek heb ik daarbij geraadpleegd. Dit leverde een aantal nieuwe bronnen op waaronder een blog post over de voor- en nadelen van Idemix[18] en U-Prove[19] voor NSTIC[20]. Deze documenten leken nuttige informatie te beschikken en daardoor bruikbaar te zijn in mijn onderzoek. Nadere analyse van deze informatie wees echter uit dat deze informatie niet geheel overeen kwam met de informatie uit de officiële publicaties van Microsoft en IBM. Hierop heb ik dan ook besloten om deze informatie niet te gebruiken in mijn onderzoek.

6.3 De resultaten

De belangrijkste resultaten van deze fase worden hieronder weergegeven. Deze en ook de andere resultaten van het onderzoek naar de mogelijkheden en functionaliteiten van beide oplossingen zijn in het productonderzoek opgenomen en opgeleverd aan mijn afstudeerbegeleider.

6.3.1 Achterliggende techniek en cryptografie

Gedurende het productonderzoek werd het duidelijk dat er veel technische kennis nodig is voor de implementatie van Idemix en / of U-Prove. Omdat het afstudeeronderzoek zich enkel richt tot het beantwoorden van de vraag op welke wijze het concept van anonieme attributen toepasbaar is op Centric en haar klanten is er in overleg met mijn afstudeerbegeleider besloten om in het onderzoek niet verder in te gaan op de benodigde techniek en cryptografie.

6.3.2 Mogelijkheden en functionaliteiten

Het literatuuronderzoek heeft de mogelijkheden en functionaliteiten van beide oplossingen en het concept van anonieme attributen in het algemeen inzichtelijk gemaakt. Hieronder wordt een gedeelte hiervan weergegeven, een volledig overzicht van de mogelijkheden en functionaliteiten is terug te vinden in het productonderzoek (Bijlage F).

Mogelijkheden

<u>Autorisatieproces;</u>

[18] Voor- en nadelen van Idemix | http://pomcor.com/2011/10/10/pros-and-cons-of-idemix-for-nstic/

[19] Voor- en nadelen van U-Prove | http://pomcor.com/2011/10/04/pros-and-cons-of-u-prove-for-nstic/

[20] National Strategy for Trusted Identities in Cyberspace | http://www.nist.gov/nstic

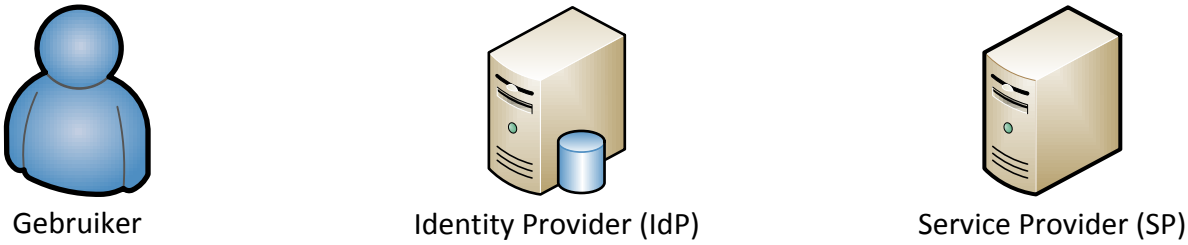
Uit het literatuuronderzoek is gebleken dat het concept van anonieme attributen toe te passen is in zowel Persoon – Service als Service – Service autorisatieprocessen. In deze fase van het onderzoek is hier niet verder op ingezoomd, dit staat gepland voor fase 5 (het scenario onderzoek).

Autorisatie (hulp)middelen;

Het literatuuronderzoek heeft duidelijk gemaakt middels welke (hulp)middelen het autorisatieproces bij het gebruiken van anonieme attributen uitgevoerd kan worden. Naast het gebruik van een desktop, mobile device (laptop, tablet en smartphones[21]) is het ook mogelijk om gebruik te maken van een desktop of mobile device in combinatie met een smartcard[22]. Deze hulpmiddelen zullen eveneens gebruikt worden in de volgende fase van het onderzoek om de mogelijke scenario's te kunnen uitwerken.

Betrokkenen;

Om minimaal gebruik te kunnen maken van anonieme attributen zijn er drie partijen nodig (Figuur 6.1). Dit zijn de gebruikers, welke door middel van het gebruik van anonieme attributen geautoriseerd kunnen worden door een dienstverlener. Deze dienstverlener wordt in de literatuur omschreven als Service Provider (SP), dit is de partij welke de policyvoorwaarden (welke attributen er getoond moeten worden) bepaald waaraan gebruikers moeten voldoen om gebruik te kunnen maken van de geleverde dienst. Tot slot is er een Identity Provider (IdP) nodig welke de benodigde attributen geanonimiseerd kan afgeven aan de gebruikers.



Figuur 6.1 Betrokkenen

Gebruiker

De gebruiker wordt in het autorisatieproces gezien als de persoon welke bepaalde attributen bezit, zoals bijvoorbeeld de organisatie waarvoor deze persoon werkzaam is en ook de functie binnen deze organisatie. Deze persoonlijke attributen kunnen door de gebruiker in een autorisatieproces worden gebruikt om te kunnen aantonen te voldoen aan de gestelde policyvoorwaarden[23] om zodoende toegang te kunnen krijgen tot de betreffende dienst(en).

Identity Provider

De gebruikers kunnen de eigen persoonlijke attributen ophalen bij één of meerdere zogenoemde Identity Provider(s) (IdP). Een mogelijk voorbeeld van een IdP kan de organisatie zijn waarbij iemand werkzaam is (welke de persoonlijke attributen kan verschaffen op basis van het HRM systeem). De gebruiker bepaald zelf welke van de attributen hij/zij wilt ophalen bij een IdP. De uitgegeven attributen worden door deze IdP ondertekend met een certificaat, om zodoende kenbaar te kunnen

[21] I Reveal My Attributes | 3. How do I obtain and use attributes | https://www.irmacard.org/irma/#03

[22] Efficient Selective Disclosure on Smart Cards Using Idemix | http://www.cs.ru.nl/~pim/publications/2013_idman.html

[23] De voorwaarde waaraan een gebruiker dient te voldoen om gebruik te kunnen maken van de aangeboden dienst(en).

maken dat de attributen afkomstig zijn van deze IdP. Deze attributen worden door de IdP geanonimiseerd uitgegeven, in de vorm die de gebruiker wilt hebben.

Service Provider

Als laatste is er de Service Provider (SP), dit is de dienstverlener waarbij een gebruiker een dienst wilt kunnen afnemen (bijvoorbeeld de toegang tot een applicatie). Deze SP maakt de policyvoorwaarden kenbaar aan de gebruiker en deze maakt aantoonbaar hieraan te voldoen door middel van de persoonlijke attributen. Pas vanaf het moment dat er aan deze policyvoorwaarden is voldaan krijgt de gebruiker toegang tot deze dienst.

6.3.3 Achterom kijken

Terugkijkend op de wijze waarop deze fase is uitgevoerd en het resultaat hiervan was ik zelf zeer tevreden, door middel van het uitgevoerde onderzoek heb ik een duidelijk en helder beeld weten te vormen van het gebruik van anonieme attributen en de mogelijkheden en functionaliteiten van de beschikbare oplossingen. Mijn begeleider was het hier mee eens, maar merkte wel terecht op dat ik me niet te veel moet richten op de tooling, maar op de toepassingsmogelijkheden zelf.

7 Het scenario onderzoek

Dit hoofdstuk beschrijft de beoogde doelstelling, de gehanteerde werkwijze en methoden en de uiteindelijke resultaten van fase 5 het scenario onderzoek.

7.1 De doelstelling

Het doel van het scenario onderzoek was het verkrijgen van inzicht in de toepassingsmogelijkheden van het concept van anonieme attributen ter behoeve van de autorisatie van gebruikers in huidige dienstverleningen, waar nu voornamelijk nog gebruik gemaakt wordt van identiteiten en / of identificerende gegevens van deze gebruikers. Dit onderzoek is dan ook uitgevoerd om een beeld te kunnen vormen van de wijze waarop dit concept nuttig zou kunnen zijn of worden voor Centric en haar klanten, en zal een antwoord geven op deelvraag 3. In welke situatie kan er gebruik worden gemaakt van anonieme attributen? Uit het literatuuronderzoek dat gedurende het productonderzoek is uitgevoerd is gebleken dat het gebruik van anonieme attributen zowel in Persoon – Service autorisatieprocessen als Service – Service autorisatieprocessen gebruik kunnen worden. Tijdens de requirements analyse uitgevoerd in fase 3 is vastgesteld dat het adviesrapport minimaal antwoord dient te geven op de vraag hoe dit concept te gebruiken is in bovengenoemde autorisatieprocessen en in welke situaties het gebruik van anonieme attributen wel of niet toegepast zou kunnen worden. Deze punten zijn dan ook het uitgangspunt geweest van het scenario onderzoek. Daarnaast is in de uitwerking hiervan ook inzichtelijk gemaakt hoe de mogelijke autorisatiemiddelen (desktop, mobile device en smartcard hierin te gebruiken zijn).

7.2 De gehanteerde werkwijze en methoden

Deze paragraaf beschrijft de gehanteerde werkwijze en methoden gedurende het scenario onderzoek.

7.2.1 Deskresearch

De begrippen "Persoon – Service" en "Service – Service" autorisatie zijn gedurende de requirements analyse en het productonderzoek al eerder aan bod gekomen. Om mijn beeld van deze begrippen te kunnen bevestigen heb ik ervoor gekozen om een literatuurstudie uit te voeren.

Big 6™

De eerder al succesvol gebruikte Big 6™ methode heb ik ook in deze fase van het onderzoek weer toegepast om de literatuurstudie uit te voeren.

Informatie verzamelen;

Voorafgaande aan het scenario onderzoek heb ik de eerste drie vragen uit de Big 6™ methode beantwoord.

1). Welke informatie ga je zoeken?

Om het beeld van Persoon - Service en Service – Service autorisatie te kunnen bevestigen zal er worden gezocht naar literatuur betreffende deze onderwerpen. De informatie moet antwoord geven op de vragen 1. Wat wordt er bedoeld met Persoon – Service autorisatie en 2. Wat wordt er bedoeld met Service – Service autorisatie.

2). Hoe ga je informatie zoeken?

De benodigde informatie zal voornamelijk worden verzameld met behulp van zoekmachines Google en Google Scholar. De hiervoor te gebruiken zoektermen worden in onderstaande tabel (Tabel 4.1) per onderwerp weergegeven. Omdat er in de huidige Identity & Access Management oplossing ook gebruik gemaakt wordt van authenticatie is ervoor gekozen om niet alleen naar autorisatie, maar ook authenticatie te zoeken.

Onderwerp	Zoektermen
Persoon – Service autorisatie	" User to Service " Authentication " User to Service " Authorization " Persoon tot Service " Authenticatie " Persoon tot Service " Autorisatie
Service – Service autorisatie	" Service to Service " Authentication " Service to Service " Authorization " Service tot Service " Authenticatie " Service tot Service " Autorisatie

Tabel 7.1 Zoektermen per onderwerp

3). Waar ga je informatie zoeken?

Er zal gezocht worden naar literatuur betreffende de bovengenoemde onderwerpen in zowel de Nederlandse als Engelse taal.

<u>Informatie analyseren;</u>

Aansluitend op het verzamelen van de literatuur heb ik de laatste drie stappen uit de Big 6™ methode uitgevoerd.

4). Resultaten bestuderen

De verkregen informatie heb ik geïnventariseerd op de aanwezigheid van de eerder genoemde zoektermen in (Tabel 7.1). Hieruit bleek al snel dat mijn denkwijze betreffende deze autorisatieprocessen juist was. Bij het Persoon – Service autorisatieproces wordt vastgesteld waartoe een gebruiker bevoegd is, en bij het Service – Service autorisatieproces wordt vastgesteld waartoe de service (of de persoon die deze service aanstuurt) bevoegd is.

5). Resultaten organiseren

De relevante bronnen zijn opgenomen in een Excel sheet om deze in een later stadium van het onderzoek eenvoudig te kunnen raadplegen.

6). Resultaten evalueren

Het beeld dat ik vooraf had betreffende beide autorisatieprocessen bleek juist te zijn. Deze kennis is in de loop van deze fase gebruikt om vast te stelen in welke situaties het concept van anonieme

attributen toepasbaar is, in de uitwerking hiervan in het adviesrapport is onderscheid gemaakt tussen Persoon – Service autorisatie en Service – Service autorisatie.

7.2.2 Brainstorm sessies

Gedurende deze fase hebben er vele brainstorm sessies plaatsgevonden met mijn afstudeerbegeleider. Samen hebben we meerdere bestaande situaties aangehaald waarbij er autorisatie plaats vind aan de hand van de identiteit(en) en/of identificerende gegevens van een gebruiker of groep gebruikers. Deze brainstorm sessies hadden tot doel om zodoende te kunnen discussiëren over de mogelijkheid of dit ook opgevangen zou kunnen worden door gebruik te maken van anonieme attributen. In onderstaande tabel (Tabel 7.2) worden een aantal behandelde scenario's weergegeven.

Situaties
Anoniem gebruik kunnen maken van de diensten van een bibliotheek
Anoniem gebruik kunnen maken van webwinkels als Bol.com
Anoniem gebruik kunnen maken van klantenkaarten of spaarkaarten
Anoniem gebruik kunnen maken van applicaties van Centric

Tabel 7.2 Behandelde scenario's

Zoals ook eerder al is gebleken in de voorgaande fasen is het concept van anonieme attributen in theorie zeer breed toepasbaar. Echter hangt het sterk af van het beoogde doel waarom er in de huidige autorisatieprocessen gebruik gemaakt wordt van identiteiten en / of identificerende gegevens. Zo kan het gebruik van identificerende gegevens namelijk kostbare informatie opleveren, waaronder het aankoopgedrag van klanten om hen vervolgens gerichte advertenties te kunnen tonen.

7.2.3 Uitwerken scenario's

De verkregen inzichten over het gebruik van het concept van anonieme attributen, de situaties waarin deze toegepast kunnen worden en de autorisatiemiddelen (desktop, mobile device en smartcard) welke hiervoor gebruik kunnen worden zijn door middel van Visio tekeningen uitgewerkt met daarbij een stapsgewijze beschrijving van de wijze waarop het autorisatieproces wordt uitgevoerd. Deze uitwerkingen zijn opgenomen in het adviesrapport en het productonderzoek (om deze te kunnen aanvullen).

7.3 De resultaten

Hieronder staan een de belangrijke resultaten uit het Scenario Onderzoek weergegeven. Deze zijn tevens in de vorm van een tussentijdse rapportage opgeleverd aan mijn afstudeerbegeleider.

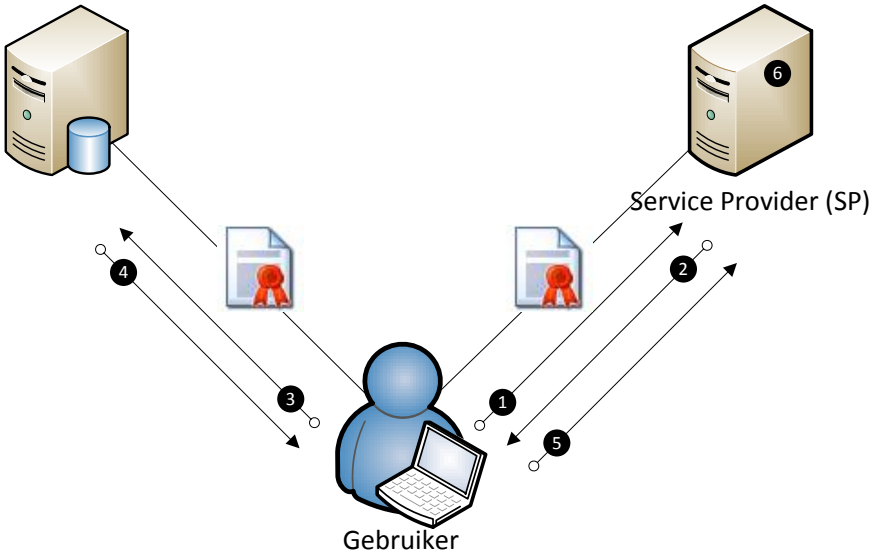
7.3.1 Breed toepasbaar

Uit het uitgevoerde onderzoek gedurende deze fase en de voorgaande fase (het productonderzoek) is gebleken dat het concept van anonieme attributen in theorie zeer breed toepasbaar moet zijn. In iedere denkbare situatie waarbij een dienstverlenende partij wilt kunnen vaststellen waartoe iemand bevoegd is zou er gebruik gemaakt kunnen worden van anonieme attributen (mits het gebruik van identiteiten en/of identificerende gegevens niet verplicht is vanuit wet- en regelgeving of deze voor de doorbelasting benodigd zijn).

7.3.2 Autorisatieprocessen.

De mogelijke situaties waarbij er gebruik gemaakt kan worden van het concept van anonieme attributen zijn aan de hand van Visio tekeningen duidelijk uitgewerkt en doormiddel van de doorlopen stappen beschreven. Hieronder worden de van elk autorisatieproces (Persoon – Service en Service – Services) één mogelijkheid weergegeven. De overige uitwerkingen zijn in het productonderzoek (Bijlage F) en het adviesrapport (hoofdstuk 3) terug te vinden.

Persoon – Service autorisatie
In onderstaande tekening (Figuur 7.1) wordt het Persoon – Service autorisatieproces weergegeven. Het uitgangspunt in deze situatie was dat de benodigde applicatie zonder tussenkomst van een andere service te benaderen is.



Figuur 7.1 Persoon – Service

Stap 1: De gebruiker opent de applicatie.

Stap 2: De SP stelt de gebruiker op de hoogte van de policyvoorwaarden waaraan voldaan dient te worden om gebruik te kunnen maken van deze applicatie.

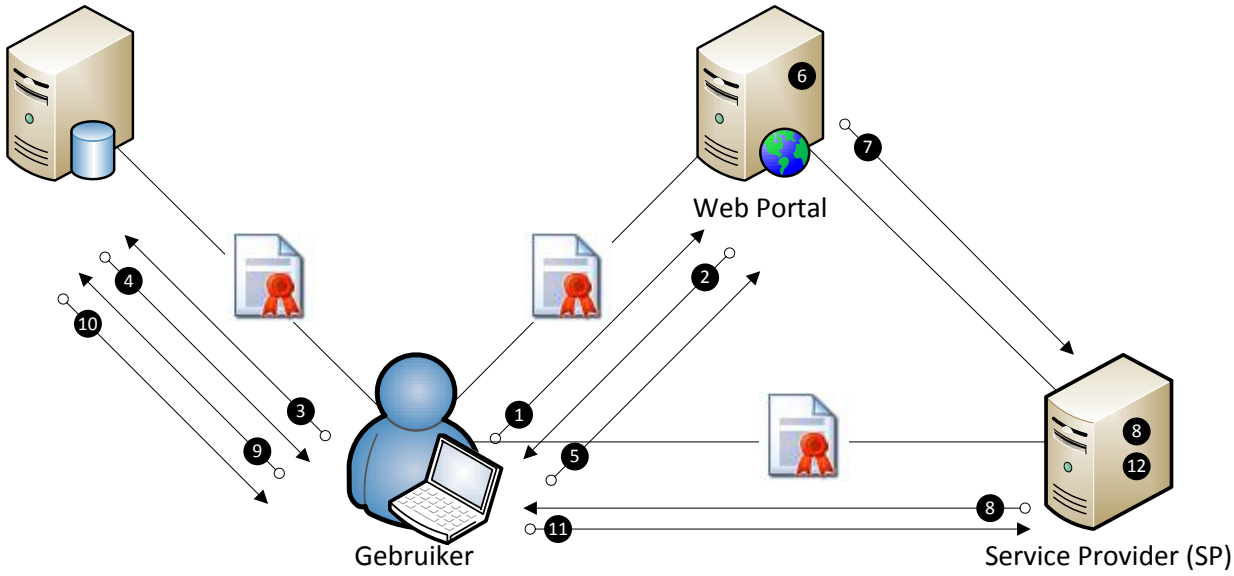
Stap 3: De gebruiker vraagt de voor het autorisatieproces benodigde attributen aan bij een IdP, in deze situatie de eigen organisatie.

Stap 4: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen. De attributen worden in een geanonimiseerde vorm ontvangen.

Stap 5: De gebruiker toont de attributen aan de SP. De exacte inhoud van de getoonde attributen wordt hierbij niet inzichtelijk gemaakt, enkel het kunnen aantonen te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 6: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de betreffende applicatie.

Persoon – Service autorisatie
In onderstaande tekening (Figuur 7.2) wordt het Persoon – Service autorisatieproces weergegeven. Het uitgangspunt in deze situatie was dat de benodigde applicatie enkel benaderd kon worden via een web portal.



Figuur 7.2 Service – Service

Stap 1: De gebruiker opent de web portal.

Stap 2: De SP stelt de gebruiker op de hoogte van de policyvoorwaarden waaraan voldaan dient te worden om gebruik te kunnen maken van deze web portal.

Stap 3: De gebruiker vraagt de voor het autorisatieproces benodigde attributen aan bij een IdP, in deze situatie de eigen organisatie.

Stap 4: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen.

Stap 5: De gebruiker toont de attributen aan de SP. De exacte inhoud van de getoonde attributen wordt hierbij niet inzichtelijk gemaakt, enkel het kunnen aantonen te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 6: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de web portal.

Stap 7: De gebruiker opent de applicatie.

Stap 8: De SP verleent de gebruiker toegang tot de betreffende applicatie indien er hierop dezelfde policyvoorwaarden van kracht zijn als voor de toegang tot de web portal. Indien er aanvullende

attributen nodig zijn om te kunnen voldoen aan de policyvoorwaarden behorende bij deze applicatie wordt de gebruiker hiervan op de hoogte gesteld.

Stap 9: De gebruiker vraagt de voor het autorisatieproces benodigde attributen aan bij een IdP, in deze situatie de eigen organisatie.

Stap 10: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen.

Stap 11: De gebruiker toont de attributen aan de SP. De exacte inhoud van de getoonde attributen wordt hierbij niet inzichtelijk gemaakt, enkel het kunnen aantonen te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 12: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de betreffende applicatie.

7.3.3 Achterom kijken

Uit de gevoerde gesprekken met mijn afstudeerbegeleider is gebleken dat de uitwerking van het scenario onderzoek voldoende duidelijk maakt op welke wijze het concept van anonieme attributen toegepast kan worden binnen de twee verschillende autorisatieprocessen. Deze beschrijvingen moeten in het uiteindelijke adviesrapport echter meer gekoppeld worden aan het gebruik van dit concept binnen Centric, zodat het een duidelijker beeld kan schetsen over de toepassingsmogelijkheden van anonieme attributen.

Achteraf is gebleken dat de door mij gebruikte theoretische scenarioschetsen, waarmee ik een duidelijk beeld dacht te geven over de toepassingsmogelijkheden binnen Centric onvoldoende aansloten op de wens van mijn begeleider. Dit gebeurde in de laatste week, waarop besloten is om een week langer door te gaan met het schrijven van het adviesrapport en alsnog een rondvraag te houden binnen Centric om vast te stellen binnen welke situaties het concept van anonieme attributen binnen Centric toegepast zou kunnen worden. Deze stap had ik achteraf beter al tijdens deze fase kunnen uitvoeren, maar dit leek toen niet nodig.

8 Afsluiting project en advies

In deze afsluitende fase van het afstudeeronderzoek "De toepassingsmogelijkheden van het concept van anonieme attributen" wordt Centric geadviseerd over de toepassingsmogelijkheden van het concept van anonieme attributen en welke vervolgstappen er uitgevoerd zouden moeten worden wanneer Centric besluit om hiermee verder te gaan. Deze paragraaf beschrijft de doelstelling, gehanteerde aanpak en het resultaat van deze fase.

8.1 De doelstelling

Deze laatste afsluitende fase van de afstudeeropdracht heeft tot doel om de afstudeeropdracht af te ronden door het beantwoorden van de hoofvraag van het onderzoek en Centric te voorzien van een beargumenteerd advies over de toepassingsmogelijkheden van het concept van anonieme attributen.

8.2 De gehanteerde werkwijze en methoden

8.2.1 Indeling adviesrapport bepalen

De eerste handeling van deze fase bestond uit het bepalen van de uiteindelijke indeling van het adviesrapport. Hiervoor hebben gesprekken plaats gevonden met mijn afstudeerbegeleider. De eerder al opgeleverde tussendocumenten vormen de basis van het adviesrapport, maar zullen niet 1 op 1 in het adviesrapport terugkomen. Deze documenten zullen wel als bijlage aan het uiteindelijke rapport worden toegevoegd.

Hoewel ik van te voren van plan was om zowel een advies- als onderzoeksrapport op te leveren is er in overleg met mijn afstudeerbegeleider besloten om enkel een adviesrapport op te leveren, met in de inleiding een paragraaf over de wijze waarop het onderzoek is uitgevoerd. Deze paragraaf is echter later toch weer uit het adviesrapport geschrapt, omdat dit voor de lezer van het adviesrapport niet relevant zou zijn.

In onderstaande tabel (Tabel 8.1) wordt de indeling van het adviesrapport weergegeven zoals deze na overleg met mijn begeleider is opgesteld;

Inhoudsopgave;
Voorwoord
Managementsamenvatting
1. Inleiding
2. Het concept van anonieme attributen
3. Scenario's
4. Conclusie en advies
5. Literatuurlijst
Bijlage A: Lijst met tabellen en figuren
Bijlage B: Identity & Access Management
Bijlage C: Europese privacy wetgeving
Bijlage D: Productonderzoek

Tabel 8.1 Hoofdstuk indeling adviesrapport

8.2.2 Het adviesrapport schrijven

Nadat was vastgesteld op welke wijze er invulling zou worden gegeven aan het adviesrapport ben ik begonnen met het schrijven van het rapport. De eerder opgeleverde tussenproducten hebben de basis gevormd voor dit adviesrapport.

In onderstaande tabel (Tabel 8.2) wordt weergegeven welke documenten er in welk hoofdstuk van het adviesrapport zijn gebruikt;

Hoofdstukken	Gebruikte producten
Management samenvatting	Alle hoofdstukken uit het adviesrapport
Inleiding	Project Initiation Document (fase 1) Probleemstelling (fase 1)
Het concept van anonieme attributen	Productonderzoek (fase 4)
Scenario's	Productonderzoek (fase 4) Scenario onderzoek (fase 5)
Conclusie en advies	Alle hoofdstukken uit het adviesrapport
Bijlage B: Identity & Access Management	Identity & Access Management (fase 2)
Bijlage C: Europese privacywetgeving	Europese privacywetgeving (fase 2)
Bijlage D: Productonderzoek	Productonderzoek (fase 4)

Tabel 8.2 Gebruikte producten

8.2.3 Controle

Om de voortgang van het adviesrapport te kunnen bewaken zijn mijn begeleider en ik gebruik gaan maken van het programma Microsoft OneNote, waarmee eenvoudig documenten met elkaar te delen zijn. Aan het einde van iedere werkdag gedurende deze laatste fase werden door mij de laatste versies van het document en/of de hoofdstukken hiermee beschikbaar gesteld aan mijn begeleider. Deze voorzag de documenten vervolgens van opmerkingen, zodat ik daar de volgende dag weer mee aan de slag kon.

Deze manier van werken heb ik als zeer prettig en nuttig ervaren, mede ook vanwege de mogelijkheid om met behulp van dit programma korte notities voor elkaar achter te laten.

8.2.4 Uitloop

In de laatste week waarin deze scriptie opgeleverd moest worden was het adviesrapport nog niet geheel naar wens van mijn afstudeerbegeleider. Met name de vraag hoe dit concept binnen Centric (en haar klanten) van nut kan zijn bleek nog onvoldoende aanwezig te zijn, hierop heb ik besloten om ook de week na oplevering van deze scriptie verder te gaan met het adviesrapport om alsnog aan de wens van mijn begeleider te kunnen voldoen. In deze week zullen de resultaten van de rondvraag (paragraaf 8.2.5) worden gebruikt om de uitgangspunten in de situatieschetsen aan te passen naar specifieke situaties binnen Centric. Daardoor zullen ook de conclusie en advies inhoudelijk nog worden aangepast om aan te kunnen sluiten op deze situatieschetsen.

8.2.5 Rondvraag binnen Centric

De scenario beschrijvingen waarmee in het adviesrapport de werking van het concept van anonieme attributen wordt beschreven was gebaseerd op theoretische uitgangspunten. In de laatste week van het afstudeertraject is er besloten om deze meer te richten op de praktijk binnen Centric, om zodoende te kunnen voldoen aan de wens van mijn afstudeerbegeleider.

Omdat ik zelf niet bekend ben met de verschillende applicaties binnen Centric heb ik een email opgesteld welke binnen Centric is rondgestuurd, met als doel inzichtelijk te maken in welke situaties er gebruik gemaakt kan worden van het concept van anonieme attributen.

Geachte collega,

Sinds februari dit jaar ben ik binnen Centric bezig met mijn afstudeeropdracht om de toepassingsmogelijkheden van het concept van anonieme attributen te onderzoeken.

Om duidelijk te maken wat er met dit concept bedoeld wordt citeer ik hieronder professor Bart Jacobs van de Radboud Universiteit Nijmegen;

" In veel situaties, in de gewone *offline* wereld, maar zeker ook in de *online* wereld op het web, is het belangrijk om te kunnen vaststellen met wie we van doen hebben. Dat geld vanzelfsprekend bijvoorbeeld bij een bank. Maar vaak ook is het helemaal niet nodig om precies te weten om wie het gaat. Als je met de bus gaat is het voldoende dat je een geldig kaartje hebt: je identiteit doet er niet toe. Of als je online een bepaalde game wilt kopen of een video wilt bekijken is het mogelijk nodig om te controleren dat je boven de 16 bent, maar wie je eigenlijk bent doet er niet toe. "

- Bart Jacobs | Attributen in plaats van Identiteiten | http://www.cs.ru.nl/B.Jacobs/PAPERS/IT-auditor-1-2013-irma.pdf

Om dit mogelijk te kunnen maken wordt er gewerkt met anonieme attributen, de dienstverlenende partij controleert daarbij enkel of een persoon in het bezit is van de benodigde attributen.

Hoewel het vanwege brandveiligheid noodzakelijk is om te weten wie er in een gebouw aanwezig is wil ik u doormiddel van onderstaande situatiebeschrijving een beeld schetsen van de wijze waarop het gebruik van anonieme attributen toegepast kan worden;

Huidige situatie
Binnen Centric wordt er gebruik gemaakt van toegangspassen waarmee medewerkers toegang hebben tot het bedrijfspand en de verschillende afdelingen. Hierbij wordt gebruik gemaakt van identificerende gegevens, de toegangspassen bevatten namelijk een nummer welke wordt gecontroleerd in een database waarin de toegangsrechten zijn vastgesteld.

Gebruik van anonieme attributen
Door gebruik te maken van anonieme attributen kan deze toegangscontrole plaats vinden zonder gebruik te maken van onze identificerende gegevens. Door te beschikken over het attribuut "Medewerker Centric" kan toegang verleend worden tot het bedrijfspand. En voor de specifieke toegang tot een bepaalde afdeling kan er gebruik gemaakt worden van het attribuut "Afdeling x".

Wie er toegang heeft gehad is vaak namelijk niet zo interessant om te weten, maar wel dat enkel bevoegden (personen met de juiste attributen) toegang kunnen krijgen. En omdat er geen gebruik gemaakt hoeft te worden van de identificerende gegevens hoeven deze ook niet beheerd te worden. Daarnaast is het gebruik van anonieme attributen privacy-vriendelijk en geeft het bescherming

tegen identiteitsfraude (doordat onze gegevens niet langer in allerlei databases wordt gebruikt).

Omdat mijn afstudeeronderzoek zich richt tot de toepassingsmogelijkheden van dit concept voor Centric (en haar klanten) ben ik dan ook benieuwd of er situaties bij u bekend zijn waarbij het voor de betreffende applicatie (voor eigen medewerkers of klanten van Centric) niet noodzakelijk is om exact te weten wie er toegang heeft, maar wel vastgesteld kan worden dat enkel personen met de juiste attributen toegang kan krijgen.

Bij voorbaat dank!

Met vriendelijke groet,
Arjan de Jong

8.3 De resultaten

8.3.1 Het advies

Hoewel het adviesrapport nog niet geheel af was ten tijde van de oplevering van deze scriptie, had ik mijn uiteindelijke advies aan de organisatie al grotendeels op papier staan. Enkel de specifieke situaties waarin gebruik gemaakt zou kunnen worden van het concept van anonieme attributen ontbrak hier nog in.

Conclusie en advies

In dit laatste hoofdstuk wil ik afsluiten met een conclusie en advies over de toepassingsmogelijkheden van het concept van anonieme attributen voor Centric en haar klanten ter behoeve van de autorisatie van een gebruiker of groep gebruikers. Zonder daarvoor gebruik te maken van identiteit(en) en identificerende gegevens. Dit hoofdstuk is opgedeeld in twee delen, de eerste paragraaf beschrijft de conclusie naar aanleiding van de voorgaande hoofdstukken en de tweede paragraaf beschrijft mijn advies en aanbevelingen aan Centric.

Conclusie

In deze paragraaf wordt de conclusie beschreven, hiervoor worden de gestelde deelvragen zoals deze in de inleiding van dit document zijn gesteld in het kort beantwoord om zodoende tot slot de hoofvraag van het onderzoek " Onderzoek voor Centric en haar klanten de toepassingsmogelijkheden van Identity & Access Management op basis van anonieme attributen in plaats van identiteiten en identificerende gegevens " te kunnen beantwoorden.

In de huidige Identity & Access Management oplossingen binnen Centric wordt er gebruik gemaakt van de identiteiten en identificerende gegevens van gebruikers om hen gebruik te kunnen laten maken van de aangeboden diensten. Ook in situaties waarbij het voor de betreffende dienstverlening of vanwege wet- en regelgeving niet nodig is om de identiteit van deze gebruikers te kennen. In deze situaties zou ervoor gekozen kunnen worden om gebruik te gaan maken van het concept van anonieme attributen. Dit is een privacy-vriendelijke oplossing waarmee gebruikers anoniem gebruik kunnen maken van aangeboden diensten, welke daardoor tevens ook bescherming biedt tegen identiteitsfraude.

Anonieme attributen zijn alle (persoonlijke) eigenschappen en kenmerken van een persoon of groep personen welke anoniem gebruikt kunnen worden in een autorisatieproces. Gebruikers worden hierbij geautoriseerd op basis van het wel of niet kunnen aantonen te voldoen aan de door de dienstverlener vastgestelde policyvoorwaarden. De exacte inhoud van deze attributen wordt hierbij niet inzichtelijk gemaakt. Het kunnen aantonen over de benodigde attributen te beschikken is voldoende.

Uit het onderzoek is gebleken dat het concept van anonieme attributen in theorie in iedere denkbare situatie is toe te passen waarbij een dienstverlener wilt kunnen vaststellen waartoe iemand bevoegd is, daarbij dient opgemerkt te worden dat het gebruik van anonieme attributen niet mogelijk is in situaties waarbij er expliciet gebruik gemaakt dient te worden van identiteiten vanwege wet- en regelgeving (bijvoorbeeld financiële systemen of de toegang tot bedrijfspanden) maar ook de doorbelasting van het gebruik. Uit aanvullend onderzoek binnen Centric is gebleken dat het concept van anonieme attributen onder meer is toe te passen in { deze diensten volgen nog uit de rondvraag binnen Centric }

Het gebruiken van anonieme attributen is voor Centric en haar klanten toe te passen in situaties waarbij het niet nodig is om de identiteit van de gebruiker(s) te kennen. Door middel van anonieme attributen hoeft Centric ook geen identiteit(en) en/of identificerende gegevens vast te leggen en beheren om vast te kunnen stellen of een gebruiker wel of geen toegang behoort te hebben tot een bepaalde applicatie. Om gebruik te kunnen maken van anonieme attributen moet er tenminste één Identity Provider (IdP) zijn welke de persoonlijke attributen kan uitgeven aan gebruikers en een SP (dienstverlener) waarbij er gebruik gemaakt kan worden van deze attributen ter behoeve van de autorisatie (hiervoor dienen de applicaties aangepast te zijn op het gebruik van anonieme attributen).

Advies en aanbeveling

In deze laatste paragraaf beschrijf ik mijn advies aan Centric betreffende de toepassingsmogelijkheden van het gebruik van anonieme attributen voor Centric en haar klanten. Hierbij geef ik ter afsluiting ook enkele aanbevelingen voor verder en gedetailleerder onderzoek naar het gebruik van anonieme attributen ter behoeve van de autorisatie van een gebruiker of groep gebruikers zonder gebruik te (hoeven) maken van de identiteit(en) en identificerende gegevens.

Hoewel het concept van het gebruik van anonieme attributen ter behoeve van de autorisatie van gebruikers inmiddels al meer dan tien jaar bestaat is het nog nauwelijks in de praktijk toegepast, de voornaamste redenen hiervoor lijken de complexiteit van de beschikbare oplossingen en het ontbreken van de vraag naar deze oplossing vanuit het bedrijfsleven en gebruikers te zijn.

Inmiddels worden er door verschillende onderzoeksprojecten (IRMA en ABC4Trust) onderzoeken uitgevoerd naar het gebruik en toepasbaarheid van anonieme attributen. Recentelijk hebben de ontwikkelaars van het IRMA project het mogelijk gemaakt om op basis van anonieme attributen studenten gebruik te kunnen laten maken van een printer (hierbij is het niet nodig om exact te weten wie er print, maar is het belangrijk om vast te kunnen stellen dat alleen studenten van deze printer gebruik kunnen maken) door aan te tonen te bezitten over het attribuut "Student".

Mede vanwege de huidige en aanstaande privacywetgeving (de General Data Protection Regulation) en de vele berichtgevingen in de media betreffende het schaden van de privacy van gebruikers van vele uiteenlopende diensten, ben ik sterk van mening dat het gebruik van identiteiten en identificerende gegevens van gebruikers tot een absoluut minimum beperkt zou moeten worden en er in situatie waarbij het voor de dienstverlening niet nodig is om de identiteit van de gebruiker(s) te

kennen er zelfs helemaal geen identiteiten en identificerende gegevens gebruikt zouden moeten worden. Ik ben dan ook een voorstander van het concept van anonieme attributen ter behoeve van de autorisatie van gebruikers. Daarnaast verwacht ik dat er in de nabije toekomst zeker meer vraag zal komen naar deze oplossing en het ook in de praktijk toegepast zal gaan worden.

Voor Centric lijkt het me echter op dit moment nog iets te vroeg om gebruik te gaan maken van deze oplossing. Er zijn nog geen grootschalige praktijktesten uitgevoerd naar het gebruik van anonieme attributen op applicatieniveau, en daarbij zal eerst vastgesteld moeten worden of er vanuit de eigen organisatie of vanuit klanten (welke gebruik maken van de door Centric aangeboden diensten) vraag is naar deze oplossing. Wanneer er (meer) vraag ontstaat naar een dergelijke oplossing, er meer is getest met dit principe in de praktijk zal de organisatie wel al een antwoord klaar moeten hebben op de vraag of het concept van anonieme attributen de oplossing is waarmee zij aan de vraag willen gaan voldoen.

Om gebruik te kunnen maken van anonieme attributen zal er tenminste één (vertrouwde) IdP moeten zijn welke de persoonlijke attributen kan uitgeven aan de gebruikers. Gemeenten, banken, verzekeraars en andere landelijke instanties zouden uitermate geschikt zijn om de rol als IdP op zich te nemen. Zij bezitten immers al over de identificerende gegevens voor hun eigen dienstverlening(en) en worden over het algemeen gezien als vertrouwde partijen.

Tot slot zou ik de organisatie wel willen aanbevelen om nader onderzoek uit te voeren naar het concept van anonieme attributen. Dit onderzoeksrapport heeft duidelijk gemaakt dat dit concept een interessante oplossing is voor Centric en haar klanten, maar gaat niet in op de wijze waarop applicaties nu worden ontwikkeld en in de toekomst ontwikkeld zouden moeten worden om het gebruik van anonieme attributen mogelijk te kunnen maken. Hieronder volgen mijn aanbevelingen voorzien van een korte toelichting.

1. **Nader onderzoek naar mogelijke situaties binnen Centric welke in de toekomst gebruik zouden kunnen maken van anonieme attributen.** Zoals beschreven in dit document kan het gebruik van anonieme attributen niet in iedere situatie worden toegepast. Centric zou dan ook moeten onderzoeken welke van haar diensten hier wel en niet voor geschikt zijn.

2. **Nader onderzoek om vast te kunnen stellen of er vanuit de eigen organisatie of de klanten van Centric behoefte is om gebruik te kunnen maken van deze oplossing.** De vraag naar het gebruik van anonieme attributen is er nog nauwelijks, organisaties gebruiken nog steeds identiteiten en identificerende gegevens om gebruikers te kunnen autoriseren. Voordat er wordt gestart met de ontwikkeling en het in gebruik nemen van het concept van anonieme attributen zou er vastgesteld moeten worden of gebruikers en klanten de behoefte hebben aan deze oplossing.

3. **De ontwikkelingen rondom het gebruik van anonieme attributen voorlopig op de achtergrond te blijven volgen.** Het gebruik van anonieme attributen wordt inmiddels in Nederland onderzocht door het IRMA project. Het is de organisatie aan te raden om deze ontwikkelingen (en die van de andere lopende projecten) op de voet te blijven volgen.

4. **Om de tafel te gaan zitten met de ontwikkelaars van het Nederlandse IRMA project en eventueel aan te sluiten bij de ontwikkeling van het gebruik van anonieme attributen.** Indien de organisatie ervan overtuigt is geraakt dat het gebruik van anonieme attributen in de toekomst een interessante oplossing kan worden voor Centric is het raadzaam om eens met de ontwikkelaars van

het Nederlandse IRMA project in gesprek te gaan en eventueel

5. **Nader onderzoek naar de technische achtergrond van dit concept.** De techniek achter het concept van anonieme attributen is cruciaal voor de werking, en is mede vanwege de gebruikte cryptografie erg complex. Het is aan te raden om te onderzoeken of Centric de benodigde experts in huis heeft om met deze oplossing te kunnen werken, en eventueel vast te stellen hoe het personeel opgeleid kan worden om hiermee aan de slag te kunnen.

6. **Centric als Service Provider en Identity Provider.** Centric zal als dienstverlener in ieder geval de rol als SP op zich moeten nemen om het gebruik van anonieme attributen voor de eigen dienstverlening(en) mogelijk te kunnen maken. Daarnaast kan Centric ervoor kiezen om ook de rol als IdP op zich te nemen om zodoende de uitgifte van attributen aan de eigen medewerkers mogelijk te kunnen maken.

8.3.2 Achterom kijken

Hoewel het adviesrapport dus nog niet volledig af was op het moment dat deze scriptie werd opgeleverd kijk ik toch wel met een positief gevoel terug op de wijze waarop ik deze fase heb uitgevoerd. Alle voorgaande fasen en handelingen hebben er uiteindelijk toe geleid dat ik invulling heb kunnen geven aan het adviesrapport. Wel vind ik het persoonlijk erg jammer dat het adviesrapport niet direct heeft voldaan aan de wensen van mijn afstudeerbegeleider en dus ook niet op tijd opgeleverd kon worden. Over de wijze waarop ik alsnog aan deze wens ga voldoen ben ik ook positief. De email voor de rondvraag is inmiddels verstuurt en de resultaten hiervan zullen naar verwachting een duidelijk beeld geven van de wijze waarop het concept van anonieme attributen binnen Centric (en haar klanten) toe te passen is, waarna het adviesrapport afgerond kan worden.

9 Evaluatie

In dit hoofdstuk volgt de evaluatie op mijn afstudeerstage bij Centric. Deze evaluatie bestaat drie delen, het eerste gedeelte beschrijft de procesevaluatie. Vervolgens komt de productevaluatie aan bod en gevolgd door de beroepstaken welke gedurende het afstudeertraject aan bod zijn gekomen. Tot slot volgt er aan het einde van dit hoofdstuk een algemene evaluatie over het geheel.

9.1 Procesevaluatie

In deze paragraaf worden de doorlopen processen per fase geëvalueerd. Hierbij wordt niet alleen stil gestaan bij de punten welke goed zijn verlopen, maar waar nodig worden ook de punten benoemd welke in het vervolg verbeterd zouden kunnen worden.

Aanpak bepalen – Fase 1

De eerste fase van het afstudeertraject bestond uit het bepalen van de aanpak van het project. Voorafgaande aan de afstudeerperiode is een afstudeerplan opgesteld voor De Haagse Hogeschool om het uit te voeren afstudeeronderzoek te kunnen laten goedkeuren. Dit document is in samenwerking met mijn afstudeerbegeleider opgesteld. Op de eerste werkdag ben in na een korte introductie met en op de afdeling Techniek en Kwaliteit – de afdeling waarbinnen ik gedurende het afstuderen werkzaam ben geweest – gestart met het opstellen van een projectplanning volgens de Prince2 methodiek. Het eerder opgeleverde afstudeerplan vormde de basis voor het Project Initiation Document (PID).

Hoewel er in deze eerste fase nog geen volledig inzicht was in de complexiteit van het onderzoek en de benodigde tijd om de verschillende fasen van het onderzoek uit te kunnen voeren was het de verwachting dat de planning gedurende het onderzoek nog inhoudelijk zou moeten worden aangepast. Dit is na afsluiting van fase 3 de requirements analyse dan ook gebeurd (scope van het onderzoek).

Omdat ik gedurende de opleiding al meerdere malen succesvol gebruik gemaakt heb van een PID voor de projectplanning heb ik besloten om deze methode ook te gebruiken voor mijn afstudeeronderzoek. Mijn afstudeerbegeleider was echter van mening dat een Plan van Aanpak (PvA) beter zou passen bij het onderzoek. De eerste conceptversie van mijn projectplanning was inmiddels al opgeleverd aan mijn afstudeerbegeleider en hierop hebben we besloten om het om te zetten naar een PvA. Tijdens de uitwerking hiervan leek het mij echter toch verstandiger om verder te gaan met het PID, hier kon ik naar mijn idee de projectplanning beter in uitwerken.

Het eerder al opgeleverde afstudeerplan is na afronding van het PID inhoudelijk aangepast, enerzijds om de feedback vanuit De Haagse Hogeschool te verwerken (beschrijving van de wijze waarop er aan de competenties voldaan zal gaan worden) en anderzijds om de probleemstelling uit het PID hierin over te nemen.

Nu ik aan het einde van mijn afstudeertraject terug kijk op deze fase ben ik redelijk tevreden over het behaalde resultaat. De indeling in fasen van het afstudeeronderzoek heeft eraan bijgedragen dat het onderzoek op een gestructureerde wijze en in een logische volgorde is uitgevoerd. Wel zou ik een volgende keer vooraf met de opdrachtgever in gesprek gaan over de wijze en methode waarop er invulling gegeven zal worden aan de projectplanning, om dit zodoende in een vroeg stadium op elkaar af te stemmen.

Vooronderzoek – Fase 2

Fase 2 van het afstudeeronderzoek stond in het teken van het vooronderzoek. Om aan het einde van het project een goed onderbouwd advies te kunnen geven aan Centric over de toepassingsmogelijkheden van het concept van anonieme attributen is er als eerste gestart met een literatuuronderzoek naar de onderwerpen: Identity & Access Management (IAM), de aanstaande Europese Privacywetgeving en het concept van anonieme attributen zelf. Dit had tot doel om de algemene kennis betreffende deze onderwerpen eigen te maken.

Het verzamelen en analyseren van de benodigde literatuur betreffende de onderwerpen IAM en de aanstaande Europese privacywetgeving verliep mede door de gebruikte onderzoeksmethoden zonder al te veel moeite. Over beide onderwerpen is veel literatuur te vinden en ook de gesprekken met de medewerkers van Centric en mijn afstudeerbegeleider leverde voldoende informatie op om een duidelijk beeld te kunnen vormen over deze onderwerpen. Het verzamelen en analyseren van de benodigde literatuur betreffende het concept van anonieme attributen verliep daarentegen wat moeizamer. Voorafgaande aan het afstudeeronderzoek was ik nog niet eerder met dit onderwerp in aanraking gekomen en ik had dan ook moeite om de juiste zoektermen te vinden. Mede door de gehanteerde sneeuwbal methode heb ik aan de hand van de literatuurlijsten van de gevonden bronnen meerdere relevante bronnen kunnen vinden. Daarnaast bracht het doornemen van deze literatuur mij tot nieuwe zoektermen welke gebruikt zijn om het literatuuronderzoek uit te kunnen breiden.

Gedurende de analyse van de verzamelde literatuur werd mij al vrij snel duidelijk dat deze onderling enkele tegenstrijdigheden beschreven. Dit verschil zat hem voornamelijk tussen de officiële publicaties van de ontwikkelaars van de ontwikkelaars welke zich bezig houden met de ontwikkeling van tooling gebaseerd op het concept van anonieme attributen (IBM en Microsoft), de verschillende onderzoeksprojecten die lopen naar het gebruik van anonieme attributen (IRMA en ABC4Trust) en de onofficiële publicaties als weblogs en andere internetpagina's. Dit heeft mij ertoe doen besluiten om voornamelijk gebruik te maken van de officiële publicaties en enkel gebruik te maken van de onofficiële publicaties als deze informatie in meerdere publicaties werd bevestigd.

Over de wijze waarop deze fase is uitgevoerd en de behaalde resultaten ben ik zelf erg tevreden. De verzamelde informatie was ruim voldoende om te kunnen starten met de volgende fase van het onderzoek (de requirements analyse). En mede doordat ik de verzamelde literatuur steeds zorgvuldig heb bijgehouden in een Excel Sheet was het gedurende deze fase, maar ook in alle volgende fasen redelijk eenvoudig om deze informatie wanneer nodig erbij te kunnen pakken en gebruiken.

Requirements analyse – Fase 3

Als derde stond de requirements analyse op de planning, voorafgaande aan het onderzoek had ik het idee dat er in deze fase zou worden vastgesteld aan welke wensen en eisen de tooling welke het gebruik van anonieme attributen mogelijk maken dienden te voldoen om gebruikt te kunnen worden voor Centric. Dit was echter niet het geval, het afstudeeronderzoek zou zich namelijk niet richten tot het beantwoorden van de vraag welke tooling het meest geschikt zou zijn voor Centric, maar tot het beantwoorden van de vraag wat de toepassingsmogelijkheden van het concept van anonieme attributen zouden kunnen zijn voor Centric. Deze fase is dan ook gebruik om de wensen en eisen aan het uiteindelijke adviesrapport vast te stellen in samenwerking met mijn afstudeerbegeleider.

Na afloop van deze fase ben ik echter toch tevreden over het behaalde resultaat, dit heeft er namelijk toe geleid dat ik een duidelijk beeld had van de werkzaamheden welke in de hierop volgende fasen uitgevoerd zouden moeten gaan worden. Naar aanleiding van deze fase is de scope van het onderzoek aangepast en is er tevens een aanpassing gedaan op de deelvragen van het onderzoek (welke in eerste instantie meer gericht waren op de tooling dan het concept op zich).

Productonderzoek – Fase 4

Fase 4 stond in het teken van het productonderzoek, welke was gericht op het onderzoeken van de mogelijkheden en functionaliteiten van IBM Idemix en Microsoft U-Prove en het concept van anonieme attributen. De kennis welke dit onderzoek zou opleveren moest de basis vormen voor de volgende fase (het scenario onderzoek).

Om de mogelijkheden en functionaliteiten van de beschikbare tooling in kaart te kunnen brengen heb ik als eerste gebruik gemaakt van de officiële publicaties van de ontwikkelaars en later de publicaties van de verschillende onderzoeksprojecten. De mogelijkheden van het concept van anonieme attributen zijn voornamelijk duidelijk geworden uit de publicaties van deze onderzoeksprojecten.

Ter afronding van deze fase heb ik de verzamelde informatie verwerkt in het document: productonderzoek, welke aan het einde van deze fase werd opgeleverd aan mijn afstudeerbegeleider. Uit de feedback van mijn afstudeerbegeleider bleek echter dat ik me teveel heb gericht op de tooling en te weinig op de mogelijkheden van het concept. Om de toepassingsmogelijkheden van het concept van anonieme attributen duidelijk te maken is er besloten om dit gedurende het scenario onderzoek nog verder te onderzoeken en het in deze fase alsnog te beschrijven.

Terugkijkend op de wijze waarop ik deze fase heb uitgevoerd ben ik gematigd tevreden. Uit het gesprek met mijn afstudeerbegeleider vanuit Centric en mijn afstudeerbegeleider vanuit De Haagse Hogeschool werd duidelijk dat ik teveel zelf probeer uit te zoeken en daardoor te weinig gebruik maakte van de beschikbare kennis van anderen (waaronder mijn afstudeerbegeleider). In deze opmerkingen kon ik me helemaal vinden, omdat ik van sommige punten naar mijn eigen mening nog onvoldoende kennis had wilde ik deze verder onderzoeken, zonder daarbij gebruik te maken van de kennis van anderen. De reden dat ik dit eerst zelf wilde uitzoeken was voornamelijk dat ik naar mijn idee niet de juiste vragen wist te formuleren en te stellen om tot de benodigde informatie te kunnen komen. Als feedback kreeg ik van beiden te horen dat ik me sterker moest opstellen en minder onzeker moest worden over mijn eigen kennis en kunnen. Dit heb ik dan ook in het verdere verloop van het afstudeertraject meegenomen.

Scenario onderzoek – Fase 5

Om de toepassingsmogelijkheden van het gebruik van anonieme attributen te onderzoeken is er in fase 5 een scenario onderzoek uitgevoerd. Hierbij is onderscheid gemaakt tussen twee scenario's waarvan in de requirements analyse is vastgesteld dat deze minimaal in het adviesrapport opgenomen dienen te worden, het Persoon – Service en Service – Service autorisatieproces.

De resultaten van dit onderzoek zijn verwerkt in een Visio tekening voorzien van de te doorlopen stappen om autorisatie mogelijk te kunnen maken. Hierbij heb ik een situatieschets beschreven om de voorbeelden te kunnen verduidelijken. Voor deze situatieschets heb ik gekozen voor een theoretisch model. Uit gesprekken met mijn afstudeerbegeleider is gebleken dat deze voorbeelden een duidelijk weergeven op welke wijze het autorisatieproces kan plaatsvinden, wel dienen de

theoretische situatieschetsen in het uiteindelijke adviesrapport te worden vervangen door situatieschetsen welke specifiek van toepassing zijn op Centric zodat deze voor de doelgroep herkenbaar zijn.

Over deze fase ben ik uiteindelijk het meest tevreden, voorafgaande wist ik niet zo goed hoe ik de verzamelde informatie zou kunnen verwerken in voorbeelden. Door gebruik te maken van Visio tekeningen en de autorisatieprocessen stapsgewijs te beschrijven heb ik niet alleen inzichtelijk kunnen maken op welke wijze autorisatie kan plaatsvinden, maar ook inzichtelijk kunnen maken welke stappen er doorlopen moeten worden.

Afsluiting project en advies – Fase 6

De laatste fase van het afstudeeronderzoek was de afsluiting van het project en de oplevering van het advies. Helaas heb ik in de laatste week van mijn afstudeerperiode moeten concluderen dat het adviesrapport zoals het er nu ligt nog niet aansluit op de wens van mijn afstudeerbegeleider. Dit zit voornamelijk in de theoretische situatieschetsen waarmee wordt aangegeven in welke situaties er gebruik gemaakt zou kunnen worden van het concept van anonieme attributen.

Dit ondanks de vele communicatie die ik met mijn begeleider heb gehad. Als eerste hebben we gezamenlijk de structuur en opbouw van het adviesrapport opgesteld en ben ik vervolgens bezig gegaan met het geven van invulling aan dit document. Hiervoor dienden de eerder opgeleverde tussendocumenten als basis. Doormiddel van Microsoft OneNote heb ik dagelijks de laatste versie van mijn adviesrapport ter beschikking gesteld aan mijn begeleider zodat deze de volgende morgen kon worden doorgenomen.

Hoewel ik tevreden ben over de wijze waarop de werkzaamheden in deze fase zijn uitgevoerd, baal ik er wel van dat het adviesrapport uiteindelijk toch niet aan de verwachtingen wist te voldoen. De theoretische situatieschetsen voldoen niet aan de verwachtingen en zouden aangepast moeten worden naar praktijkvoorbeelden. Dit had dan ook in de requirements analyse als Must have benoemd moeten worden. Hierop heb ik besloten om alsnog een rondvraag te houden binnen Centric om zo tot betere praktijkvoorbeelden te komen waarna ik deze alsnog in het adviesrapport zal verwerken.

9.2 Productevaluatie

In deze paragraaf worden de producten geëvalueerd welke zijn opgeleverd aan Centric gedurende het afstudeertraject.

Project Initiation Document (Bijlage B)

Het Project Initiation Document beschrijft de probleemstelling en doelstelling van mijn afstudeeropdracht en de wijze waarop het project aangepakt zal worden. Voor het opstellen van deze planning heb ik bewust gekozen voor de Prince 2 methodiek, omdat ik gedurende mijn opleiding daar al meerdere malen succesvol gebruik van heb gemaakt. De eerste feedback die ik op dit document kreeg was dat deze methode wellicht niet de juiste zou zijn, en ik de planning beter zou kunnen omzetten in een PvA. Ik heb overwogen om mijn planning in een PvA op te nemen, maar eigenlijk ben ik achteraf tevreden over de wijze waarop ik mijn planning heb opgesteld in het PID.

Achtergrond: Identity & Access Management (Bijlage C) & Europese privacywetgeving (Bijlage D)

Deze documenten zijn het resultaat van het uitgevoerde vooronderzoek. Het eerste document (Achtergrond: Identity & Access Management) geeft een korte toelichting op het begrip Identity & Access Management en beschrijft de onderliggende deelprocessen en de redenen waarom organisaties gebruik maken van dit proces. Het tweede document (Achtergrond: Europese privacywetgeving) geeft een overzicht weer van de belangrijkste punten uit de nieuwe Europese privacywetgeving. Beide documenten zijn opgesteld voor mijn eigen beeldvorming en het opstellen van beide documenten heeft een positieve bijdrage geleverd aan mijn kennis betreffende deze onderwerpen.

Het productonderzoek (Bijlage E)

In fase 4 (productonderzoek) en fase 5 (scenario onderzoek) is er invulling gegeven aan het productonderzoek. In dit document worden de mogelijkheden en functionaliteiten beschreven van de op dit moment beschikbare tooling waarmee gebruik gemaakt kan worden van het concept van anonieme attributen. Dit document is gebaseerd op de beschikbare publicaties waarin deze functionaliteiten en mogelijkheden worden beschreven en geeft naar mijn mening dan ook een volledig beeld van de beschikbare oplossingen. Ik ben dan ook zeer tevreden over de wijze waarop dit document tot stand is gekomen en het resultaat.

Adviesrapport (Externe bijlage)

Het adviesrapport maakt duidelijk waarom er gebruik gemaakt zou moeten worden van het concept van anonieme attributen en geeft een inzicht in de wijze waarop dit concept in de praktijk toegepast kan worden door middel van twee theoretische situatieschetsen. Naar mijn mening voldoet het adviesrapport daarmee aan de gemaakte afspraken met mijn afstudeerbegeleider. Echter bleek in de laatste week van de afstudeerperiode dat het rapport nog niet geheel naar zijn wens was. Hierop heb ik dan ook besloten om in de week na oplevering van mijn afstudeerdossier aan De Haagse Hogeschool alsnog de benodigde wijzigingen in het adviesrapport op te nemen om zodoende te kunnen voldoen aan de verwachtingen van mijn begeleider. Over het adviesrapport in de huidige vorm ben ik dan ook nog niet geheel tevreden, maar met de geplande aanpassingen in het vooruitzicht ben ik van mening dat het adviesrapport alsnog gaat voldoen aan de verwachtingen van mijn afstudeerbegeleider.

9.3 Competenties

Deze paragraaf beschrijf de wijze waarop de in het afstudeerplan benoemde competenties aan bod zijn gekomen. Hierbij wordt onderscheid gemaakt tussen de algemene competenties en vakspecifieke competenties.

Algemene competenties;

Hieronder worden de algemene competenties weergegeven welke in dit afstudeertraject aan bod zouden gaan komen, voorzien van een beschrijving van de wijze waarop aan deze competenties voldaan zou worden tijdens het afstuderen.

1.) Het uitvoeren van een probleemoriëntatie. Zoals een krachtenveldanalyse, cultuurscan etc. Leidend tot probleem- en opdrachtformulering (scope, fiattering). In gesprekken welke gevoerd zullen gaan worden met mijn stagebegeleider binnen Centric zal de probleem- en opdrachtformulering worden vastgesteld. Vooraf is afgesproken dat het onderzoek zich alleen zal richten op de Access Management oplossingen Idemix (IBM) en U-Prove (Microsoft) tenzij uit het vooronderzoek alsnog blijkt dat er nog een andere belangrijke oplossing op de markt is welke niet in het onderzoek mag ontbreken.

2.) Het kiezen van een passende aanpak. Voldoen aan randvoorwaarden voor integriteit en vertrouwelijkheid. Kiezen van referentiekader bij het uitvoeren van onderzoek en/of IB-werkzaamheden. In de eerste fase van deze afstudeeropdracht zal er worden gestart met het opstellen van een plan van aanpak. Dit plan zal ingaan op de probleem- en doelstelling van het onderzoek en de wijze waarop het onderzoek uitgevoerd zal gaan worden. Na goedkeuring van de stagebegeleider binnen Centric zal er worden overgegaan op de uitvoer van het onderzoek.

3.) Het lezen, begrijpen en gebruiken van onderzoek Waaronder lezen van literatuur/publicaties. De eerder genoemde Access Management oplossingen Idemix (IBM) en U-Prove (Microsoft) en het Attribute Based Access Control (ABAC) principe bestaan al enkele jaren en zijn al in enkele onderzoeken gebruikt. In de tweede fase van de afstudeeropdracht "zelfstudie" zal ik doormiddel van literatuuronderzoek deze bronnen gebruiken om kennis op te doen over het Access Management principe en de wijze waarop boven genoemde oplossingen op dit moment gebruikt worden en wat de mogelijkheden van beiden kunnen zijn voor gebruik binnen Centric.

4.) Het uitvoeren van onderzoek. In de derde fase van het onderzoek zal er in overleg met mijn stagebegeleider een use case worden opgesteld. Er wordt gekeken naar een bestaande situatie intern binnen Centric of extern bij één of meerdere klanten van Centric waarbij het huidige Access Management proces als uitgangspunt wordt genomen om de mogelijkheden van één van de Access Management oplossingen te toetsen. Er zal worden onderzocht of Idemix of U-Prove het bestaande Access Management proces kan vervangen en wat de toegevoegde waarde kan zijn voor de organisatie.

5.) Het vormgeven van een adviesproces en het tot uitvoer brengen daarvan. De bevindingen van het onderzoek zullen aan Centric worden gerapporteerd in een adviesrapport.

6.) Creëren van draagvlak voor implementatie van IB-beleid, richtlijnen en procedures. Een belangrijk onderdeel van het adviesrapport is het creëren van draagvlak voor implementatie van één van de eerder genoemde Access Management oplossingen en het beschrijven van de mogelijkheden en toegevoegde waarde hiervan.

Competentie	Voldaan?	Wijze waarop aan deze competentie is voldaan
1.	Ja	Ik heb aan deze competentie voldaan door in gedurende de eerste week van de afstudeerperiode een probleemanalyse uit te voeren door middel van de 6W methode uit het boek van Nel Verhoeven. De communicatie met mijn afstudeerbegeleider hebben de basis gevormd van deze probleemanalyse.
2.	Ja	In de eerste fase van het afstudeeronderzoek waarin de projectplanning centraal stond heb ik de aanpak van het onderzoek bepaald en afgestemd met mijn afstudeerbegeleider vanuit Centric. Het onderzoek is daarbij in een zestal fasen opgesplitst. Per fase is het doel vastgesteld en welke resultaten en/of tussenproducten er aan het einde van iedere fase opgeleverd dienen te worden.

3.	Ja	Het gebruiken van literatuur/publicaties heeft een belangrijke rol gespeeld in mijn onderzoek. Het concept van anonieme attributen is nog nauwelijks in de praktijk toegepast, maar er zijn inmiddels al een hoop geschreven over dit concept. Voor mijn literatuurstudie(s) heb ik voornamelijk gebruik gemaakt van Engelstalige literatuur, dit vanwege het feit dat er nog maar weinig is gepubliceerd in het Nederlands. Het begrijpen van deze teksten verliep (mede vanwege de benodigde achtergrondkennis) in het begin wat moeizaam, maar naarmate het onderzoek vorderde en ik een beter beeld kreeg van het onderwerp werden de teksten uit deze literatuur en publicaties mij ook duidelijker.
4.	Ja	Ik heb aan deze competentie voldaan door in bijna iedere fase van het onderzoek een literatuuronderzoek en in fase 5 een scenario onderzoek uit te voeren. Daarnaast zijn er gedurende het vooronderzoek een aantal interviews afgenomen met medewerkers binnen Centric.
5.	Ja	In de laatste fase van het onderzoek (afsluiting project en advies) heb ik een adviesrapportage opgesteld om Centric te kunnen adviseren over de toepassingsmogelijkheden van het concept van anonieme attributen. De wensen en eisen van mijn afstudeerbegeleider ten aanzien van dit document zijn halverwege de afstudeeropdracht vastgesteld en alle voorgaande fasen hebben bijgedragen aan het uiteindelijke advies. Ten tijde van de oplevering van deze scriptie was het adviesrapport echter nog niet geheel naar wens en wordt er nog één week aan dit document gewerkt om dit te realiseren.
6.	Ja	Het adviesrapport maakt duidelijk waarom en in welke situaties Centric gebruik zou kunnen maken van het concept van anonieme attributen en geeft daarbij tevens aan wat de voor- en nadelen hiervan zullen zijn

Tabel 9.1 Algemene competenties

Vakspecifieke competenties;

Hieronder worden de vakspecifieke competenties weergegeven welke in dit afstudeertraject aan bod zouden gaan komen, voorzien van een beschrijving van de wijze waarop aan deze competenties voldaan zou worden tijdens het afstuderen.

11.) Het vertalen van recht, regelgeving en eigen (IB-) beleid naar richtlijnen en procedures, op technisch, organisatorisch en/of menselijk vlak. Een van de redenen waarom het onderzoek naar Attribute Based Access Control uitgevoerd gaat worden is de nieuwe Europese privacy wetgeving welke eraan zit te komen. In het onderzoek zal worden gekeken naar de impact van deze wetgeving op de huidige IAM situatie en zal worden ingegaan op hoe Attribute Based Access Control ten goede komt aan het privacyaspecten.

13.) Het ontwerpen van IB-oplossingen, op technisch, organisatorisch en menselijk vlak.
Gedurende het onderzoek zullen beide Access Management oplossingen worden getest op werking en mogelijkheden.

15.) Het overdragen van kennis m.b.t. IB aan stakeholders. Middels een adviesrapportage richting Centric zal worden ingegaan op de bevindingen uit het onderzoek en zal er worden stil gestaan bij de wijze waarop het onderzoek is uitgevoerd en de wijze waarop Centric Attribute Based Access Control zowel intern als extern kan inzetten.

16.) Het maken en/of uitvoeren van een plan voor implementatie van IB- richtlijnen, -procedures en –oplossingen. In het adviesrapport zal worden stil gestaan bij de wijze waarop Centric Attribute Based Acces Control zowel intern als extern kan inzetten.

Competentie	Voldaan?	Wijze waarop aan deze competentie is voldaan
11.	Ja	Ik heb aan deze competentie voldaan door onderzoek te doen naar de aanstaande Europese privacywetgeving en de belangrijkste gevolgen daarvan in kaart gebracht.
13.	Ja	Gedurende het onderzoek is niets ontworpen, wel zijn de mogelijkheden en functionaliteiten van beide oplossingen zorgvuldig in kaart gebracht. Deze zijn in het scenario onderzoek gebruikt om te kunnen beoordelen of het gebruik van anonieme attributen nuttig kan zijn voor Centric en haar klanten.
15.	Ja	Hieraan is voldaan door middel van het adviesrapport waarin ik met name in het hoofdstuk conclusie en advies mijn advies en aanbevelingen beschrijf. Daarnaast zijn alle door mij opgestelde documenten als bijlage aan het adviesrapport toegevoegd.
16.	Ja	Aan deze competentie is voldaan door twee theoretische scenarioschetsen op te nemen in het adviesrapport. Hoewel deze nog aangepast zullen worden naar praktijk voorbeelden binnen Centric wordt hiermee inzichtelijk gemaakt op welke wijze het gebruik van anonieme attributen is toe te passen.

Tabel 9.2 Vakspecifieke competenties

10 Literatuurlijst

Boeken
De boeken welke gedurende het afstudeeronderzoek zijn geraadpleegd worden hieronder weergegeven.

Camenisch, J. Leenes, R. & Sommer, D (2011). *Digital Privacy: PRIME – Privacy and Identity Management for Europe.* Springer

Staaij, R. van der (2008). *Identiteitsmanagement, Beheersen van Identiteiten.* Uitgeverij Tutein Nolthenius.

Verhoeven, N. (2010). *Wat is onderzoek? Praktijkboek methoden en technieken voor het hoger onderwijs.* Boom Lemma Uitgevers.

Publicaties en rapporten
De publicaties en rapporten welke gedurende het afstudeeronderzoek zijn geraadpleegd worden hieronder weergegeven.

Alpár, G. & Jacobs, B. (2013). *Credential Design in Attribute-Based Identity Management*.

Alpár, G. & Jacobs, B. (2013). *Towards Practical Attribute-Based Identity Management.*

Bichsel, P. Camenisch, J. Groß, T. & Shoup, V. *Anonymous Credentials on Standard Java Card.*

Bichsel, P. & Camenisch, J. *Mixing Identities with Ease*. IBM Research, Switzerland.

Brands, S. Demuynck, L. & Decker, B de. (2006). *A practical system for globally revoking the unlinkable pseudonyms of unknow users.*

Bronw, J. Stradling, P. & Wittenberg C.H. (2011). *U-Prove CTP R2 Whitepaper*. Microsoft Corporation.

Camenisch, J. & Herreweghen, E. *Design and Implementation of the Idemix Anonymous Credential System.*

Camenisch, J. Kohlweiss, M. & Soriente, C. *Solving Revocation with Efficient Update of Anonymous Credentials.* Microsoft Research.

Camenisch, J. & Lysyanskaya, A. (2001). *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation.* IBM Research.

Danes, L. (2007). *Een pseudoniem-systeem, wat is het en wat gaat Luuk ermee doen?*

Danes, L. (2007). *Master thesis: Smart card integration in the pseudonym system Idemix.* Groningen: University of Groningen.

Gelfand, A. (2008). *Startup Plans to Solve Online Identity Theft, But Does Anyone Care?*

IBM Research Zürich Security Team. (2012). *Technical report: Specification of the Identity Mixer cryptographic library, version 2.3.4.* IBM Research, Zürich.

Jacobs, B (2013). Attributen in plaats van Identiteiten. *De IT-Auditor*, 22 (1), 29-35.

Mostowski, W. & Vullers, P (2012). *Efficient U-Prove Implementation for Anonymous Credentials on Smart Cards.*

Neven, G. (2008). *A Quick Introduction to Anonymous Credentials.* IBM Zürich Research Laboratory

Paquin, C. (2011) *Technical report: U-Prove Cryptographic Specification v1.1.* Microsoft Corporation.

Pashalidis, A. & Mitchell, C.J. (2011) *Privacy in Identity & Access Management Systems.*

Rijswijk-Deij, R van. (2013). *IRMA: Privacy en authenticatie gaan prima samen!*

Rogaar, P. (2011). *Attributes and tokens in U-Prove: Interval proofs and use cases.*

Rogaar, P (2011). Privacybescherming met U-Prove bij de elektronische Nederlandse Identiteitskaart. *Informatiebeveiliging*, 11 (6), 4-7.

Smaling, N.& Boersma, J. (2013). *Thesis: Online leeftijdsverificatie in Nederland.* Innopay.

Vullers, P. & Alpár, G. (2013). *Efficient Selective Disclosure on Smart Cards using Idemix*.

Elektronische bronnen

De Elektronische bronnen welke gedurende het afstudeeronderzoek zijn geraadpleegd worden hieronder weergegeven.

Are Privacy-Enhancing Technologies Really Needed for NSTIC? (2011, 13 oktober). Opgevraagd maart 2013, van http://pomcor.com/2011/10/13/are-privacy-enhancing-technologies-really-needed-for-nstic/

Attribute-Based Credentials for Trust. Opgevraagd maart 2013, van https://abc4trust.eu/

Consortium werkt aan internetpaspoort (2011, 28 januari). Opgevraagd april 2013, van http://www.nu.nl/internet/2434024/consortium-werkt-internetpaspoort.html

Deployment and Usability of Cryptographic Credentials. (2011, 16 oktober). Opgevraagd maart 2013, van http://pomcor.com/2011/10/16/deployment-and-usability-of-cryptographic-credentials/

General Data Protection Regulation. Opgevraagd februari 2013, van http://en.wikipedia.org/wiki/General_Data_Protection_Regulation

IBM Idemix. Opgevraagd februari 2013, van http://www.zurich.ibm.com/security/idemix/

IRMA: I Reveal My Attributes. Opgevraagd maart 2013, van https://www.irmacard.org/

Microsoft U-Prove. Opgevraagd februari 2013, http://research.microsoft.com/en-us/projects/u-prove/

Pros and Cons of Idemix for NSTIC. (2011, 10 oktober). Opgevraagd maart 2013, van http://pomcor.com/2011/10/10/pros-and-cons-of-idemix-for-nstic/

Pros and Cons of U-Prove for NSTIC. (2011, 4 oktober). Opgevraagd maart 2013, van http://pomcor.com/2011/10/04/pros-and-cons-of-u-prove-for-nstic/

Technologies and Features: U-Prove. Opgevraagd februari 2013, van http://www.microsoft.com/privacy/technologies/uprove.aspx

Wet Bescherming Persoonsgegevens. Opgevraagd februari 2013, van http://nl.wikipedia.org/wiki/Wet_bescherming_persoonsgegevens

11 Lijst met tabellen en figuren

Tabellen;

Tabel 2.1 Fasering van het afstudeeronderzoek 12
Tabel 3.1 De fasering van het onderzoek volgens het afstudeerplan 15
Tabel 3.2 De op te leveren (tussen)producten volgens het afstudeerplan 15
Tabel 3.3 De fasering van het onderzoek volgens het PID 17
Tabel 3.4 De op te leveren (tussen)producten volgens het PID 17
Tabel 4.1 Zoektermen per onderwerp 20
Tabel 4.2 deelnemers interviews 23
Tabel 5.1 De MoSCoW-methode 26
Tabel 6.1 Zoektermen per onderwerp 29
Tabel 7.1 Zoektermen per onderwerp 34
Tabel 7.2 Behandelde scenario's 35
Tabel 8.1 Hoofdstuk indeling adviesrapport 39
Tabel 8.2 Gebruikte producten 40
Tabel 9.1 Algemene competenties 52
Tabel 9.2 Vakspecifieke competenties 53

Figuren;

Figuur 2.1 Vestigingen Centric Nederland 10
Figuur 2.2 Organisatiestructuur Centric 11
Figuur 2.3 Betrokkenen bij deze afstudeeropdracht 13
Figuur 3.1 Gannt Chart 18
Figuur 4.1 De Big 6™ (Eisenberg & Berkowitz, 1992; Canning, 2002) 19
Figuur 4.2 De onderzoekscyclus Nel Verhoeven (vooruit kijken) 20
Figuur 4.3 Resultaten bestuderen 21
Figuur 4.4 De onderzoekscyclus Nel Verhoeven (achterom kijken) 25
Figuur 6.1 Betrokkenen 31
Figuur 7.1 Persoon – Service 36
Figuur 7.2 Service – Service 37

Bijlage A: Afstudeerplan

Afstudeerplan

Informatie afstudeerder en gastbedrijf

Afstudeerblok: 2013-1.1 (start uiterlijk 11 februari 2013)
Startdatum uitvoering afstudeeropdracht: 11 februari 2013
Inleverdatum afstudeerdossier volgens jaarrooster: 7 juni 2013

Studentnummer: 08064733
Achternaam: dhr. de Jong
Voorletters: J.J.G.
Roepnaam: Arjan
Adres: Gebroken Meeldijk 119
Postcode: 2991CG
Woonplaats: Barendrecht
Telefoonnummer: 0643691265
Mobiel nummer: 0643691265
Privé emailadres: Arjan1@gmail.com

Opleiding: Information Security Management
Locatie: Zoetermeer
Variant: voltijd

Naam studieloopbaanbegeleider: Dhr. Leo van Koppen
Naam begeleidend examinator: Mw. Marjolein Faassen
Naam tweede examinator: Dhr. Henk van de Ven

Naam bedrijf: Centric
Afdeling bedrijf: Techniek en Kwaliteit
Bezoekadres bedrijf: Antwerpseweg 8
Postcode bezoekadres: 2803 PB
Postbusnummer: 338
Postcode postbusnummer: 2800 AH
Plaats: Gouda
Telefoon bedrijf: +31 182 345000
Telefax bedrijf: +31 182 345001
Internetsite bedrijf: www.centric.eu

Achternaam opdrachtgever: Dhr. Iking
Voorletters opdrachtgever: G.W.M.
Titulatuur opdrachtgever:
Functie opdrachtgever: Senior consultant business development
Doorkiesnummer opdrachtgever: n.v.t
Email opdrachtgever: ge.iking@centric.eu

Achternaam bedrijfsmentor: Dhr. Iking
Voorletters bedrijfsmentor: G.W.M.
Titulatuur bedrijfsmentor:
Functie bedrijfsmentor: Senior consultant business development
Doorkiesnummer bedrijfsmentor: n.v.t
Email bedrijfsmentor: ge.iking@centric.eu

Doorkiesnummer afstudeerder: n.v.t.
Functie afstudeerder (deeltijd/duaal): n.v.t.

Titel afstudeeropdracht:
Onderzoek voor Centric en haar klanten de toepassingsmogelijkheden van IAM op basis attributen i.p.v. identiteiten.

Opdrachtomschrijving

1. Bedrijf

Met ruim 5.300 medewerkers biedt Centric maatwerk- en standaardsoftware, infrastructuur, branche specifieke oplossingen en een uitgebreid portfolio van gerelateerde diensten en werken daarbij samen met diverse gerenommeerde partners

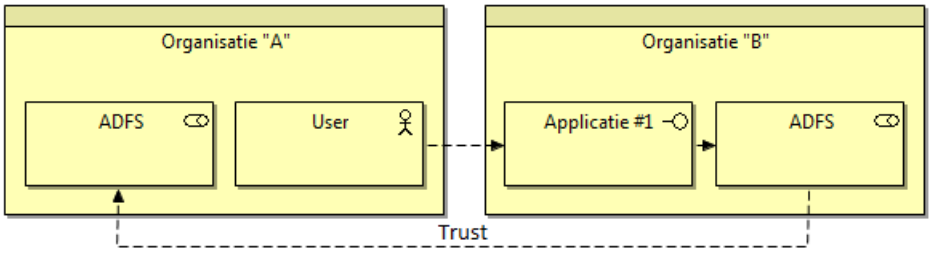
De afdeling Techniek en Kwaliteit Gouda houdt zich bezig met het adviseren en controleren van de units over keuze en gebruik van zowel interne en externe standaarden voor de ontwikkeling van toepassingen. Deze toepassingen worden gebruikt door een groot aantal klanten.

2. Probleemstelling

Centric heeft de behoefte om de mogelijkheden van Identity & Access Management (IAM) op basis van Attributen (geplaatst op een Smart Card) in plaats van identiteiten te laten onderzoeken. In de huidige IAM situatie binnen Centric wordt het Access Management (AM) proces veelal ingebakken in de applicaties en wordt het Identity Management (IDM) proces uitgevoerd middels een op zich zelf staande Identity store.

Figuur A.0.1.

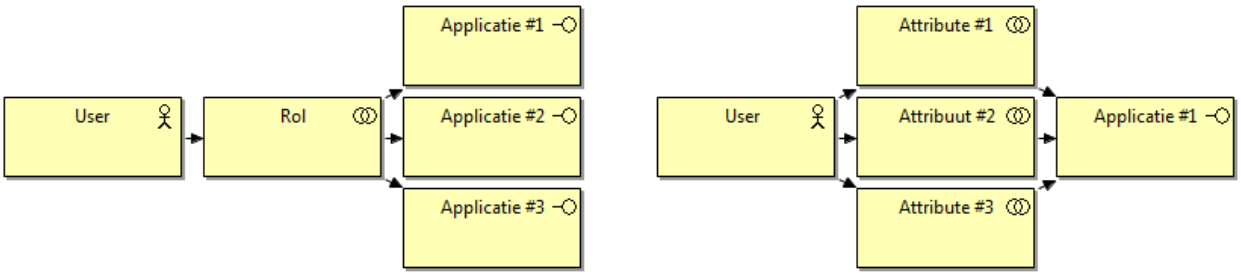
Door samenwerking tussen organisaties kan de behoefte ontstaan tot het delen van informatie, waardoor bovengenoemde methode van IAM niet meer toereikend is. Gebruikers van organisatie "A" zijn immers niet bekend in het IAM systeem van organisatie "B". Dit vraagt een grotere beheerinspanning van beide organisaties. Hoe weet de organisatie "A" bijvoorbeeld of een gebruiker "X" nog bij organisatie "B" in dienst is? Het gebruik van Federated Identity Management (FIM), Waarbij door middel van Active Directory Federated Services (ADFS) de Active Directory omgevingen van beide organisaties aan elkaar worden gekoppeld, lost dit probleem grotendeels op. Hierbij vertrouwen beide organisaties erop dat de ander een goed en betrouwbaar IAM systeem gebruikt.



Figuur A.0.2.

Een nadeel dat echter aan ieder IAM systeem kleeft is dat het omgaan met de daarin opgeslagen gegevens over de gebruikers dient te voldoen aan wetgeving wat betreft de privacybescherming. Een mogelijkheid om dit probleem op te kunnen lossen is de gebruiker niet op basis van zijn identiteit, maar op basis van zijn attributen toegang te verlenen, Attribute Based Access Control (ABAC).

In de huidige situatie wordt er veelal gebruik gemaakt van Role Based Access Control (RBAC), waarbij identiteiten in het IAM systeem worden gekoppeld aan bepaalde rollen binnen de organisatie. De rol(len) waaraan de gebruiker is gekoppeld zijn bepalend voor de toegangsrechten tot de informatiesystemen. In de ABAC situatie worden de toegangsrechten juist bepaald door de attributen welke de gebruiker bezit.



Figuur A.0.3. Role Based Access Control, Attribute Based Access Control

3. Doelstelling van de afstudeeropdracht

Het doel van deze afstudeeropdracht is enerzijds het kunnen schrijven van een scriptie over de mogelijkheden van ABAC door middel van het gebruik van Idemix (IBM) en U-Prove (Microsoft) AM oplossingen voor zowel intern als extern gebruik bij klanten van Centric. In de scriptie zal tevens worden ingegaan op het doorlopen proces, de reden van het onderzoek, de wijze waarop het onderzoek is uitgevoerd en de resultaten van het onderzoek. Anderzijds heeft deze afstudeeropdracht het doel om een adviesrapportage op te leveren aan Centric waaruit duidelijk moet worden welke mogelijkheden ABAC Centric te bieden heeft voor zowel intern als extern gebruik en welke gevolgen dit met zich mee brengt.

4. Resultaat

Het resultaat moet uitmonden in een beargumenteerd advies aan Centric over de inzet van AM op basis van attributen voor zowel intern als extern bij klanten van Centric.

5. Uit te voeren werkzaamheden, inclusief een globale fasering, mijlpalen en bijbehorende activiteiten

1.) Opstellen van een plan van aanpak aan de hand van de Prince2 methodiek.
2.) Uitvoeren van literatuuronderzoek naar de wijze waarop huidige IAM systemen eruitzien en werken, welke systemen er naast de reeds bekende (IDEMX van IBM en UPROVE van Microsoft) er zijn welke voldoen aan het criteria "de gebruiker toegang verlenen op basis van attributen in plaats van op basis van zijn identiteit".
3.) Het vaststellen van requirements waaraan de IAM systemen aan dienen te voldoen.

4.) Uitvoeren van productonderzoek naar IDEMIX van IBM en UPROVE van Microsoft om vast te stellen of deze systemen voldoen aan de requirements. Indien er uit het vooronderzoek is gebleken dat er ook andere systemen beschikbaar zijn zal de overweging worden gemaakt om deze wel of niet in het onderzoek mee te nemen.
5.) Aan de hand van de theorie of een praktijktest (in een proefopstelling) vaststellen welke systeem het meest geschikt is voor gebruik door Centric.
6.) Het opstellen van een adviesrapport voor Centric met daarin de wijze waarop het onderzoek is uitgevoerd, welke resultaten het onderzoek heeft opgeleverd en een overzicht van de voors en tegens ten opzichte van het gebruik door Centric.

6. Op te leveren (tussen)producten

1.) Plan van aanpak.
2.) Rapportage van het productonderzoek (inclusief de requirements waaraan de systemen dienen te voldoen).
3.) Rapportage van bevindingen aan de hand van de theorie of praktijktest naar de werking en functionaliteiten van Idemix en U-Prove.
4.) Adviesrapportage richting Centric.

7. Te demonstreren competenties en wijze waarop

Gedurende het onderzoek zal worden voldaan aan onderstaande competenties;

1.) Het uitvoeren van een probleemoriëntatie. Zoals een krachtenveldanalyse, cultuurscan etc. Leidend tot probleem- en opdrachtformulering (scope, fiattering). In gesprekken welke gevoerd zullen gaan worden met mijn stagebegeleider binnen Centric zal de probleem- en opdrachtformulering worden vastgesteld. Vooraf is afgesproken dat het onderzoek zich alleen zal richten op de Access Management oplossingen Idemix (IBM) en U-Prove (Microsoft) tenzij uit het vooronderzoek alsnog blijkt dat er nog een andere belangrijke oplossing op de markt is welke niet in het onderzoek mag ontbreken.

2.) Het kiezen van een passende aanpak. Voldoen aan randvoorwaarden voor integriteit en vertrouwelijkheid. Kiezen van referentiekader bij het uitvoeren van onderzoek en/of IB-werkzaamheden. In de eerste fase van deze afstudeeropdracht zal er worden gestart met het opstellen van een plan van aanpak. Dit plan zal ingaan op de probleem- en doelstelling van het onderzoek en de wijze waarop het onderzoek uitgevoerd zal gaan worden. Na goedkeuring van de stagebegeleider binnen Centric zal er worden overgegaan op de uitvoer van het onderzoek.

3.) Het lezen, begrijpen en gebruiken van onderzoek Waaronder lezen van literatuur/publicaties. De eerder genoemde Access Management oplossingen Idemix (IBM) en U-Prove (Microsoft) en het Attribute Based Access Control (ABAC) principe bestaan al enkele jaren en zijn al in enkele onderzoeken gebruikt. In de tweede fase van de afstudeeropdracht "zelfstudie" zal ik doormiddel van literatuuronderzoek deze bronnen gebruiken om kennis op te doen over het Access Management principe en de wijze waarop boven genoemde oplossingen op dit moment gebruikt worden en wat de mogelijkheden van beiden kunnen zijn voor gebruik binnen Centric.

4.) Het uitvoeren van onderzoek. In de derde fase van het onderzoek zal er in overleg met mijn stagebegeleider een use case worden opgesteld. Er wordt gekeken naar een bestaande situatie intern binnen Centric of extern bij één of meerdere klanten van Centric waarbij het huidige Access Management proces als uitgangspunt wordt genomen om de mogelijkheden van één van de Access Management oplossingen te toetsen. Er zal worden onderzocht of Idemix of U-Prove het bestaande Access Management proces kan vervangen en wat de toegevoegde waarde kan zijn voor de organisatie.

5.) Het vormgeven van een adviesproces en het tot uitvoer brengen daarvan. De bevindingen van het onderzoek zullen aan Centric worden gerapporteerd in een adviesrapport.

6.) **Creëren van draagvlak voor implementatie van IB-beleid, richtlijnen en procedures.** Een belangrijk onderdeel van het adviesrapport is het creëren van draagvlak voor implementatie van één van de eerder genoemde Access Management oplossingen en het beschrijven van de mogelijkheden en toegevoegde waarde hiervan.

11.) **Het vertalen van recht, regelgeving en eigen (IB-) beleid naar richtlijnen en procedures, op technisch, organisatorisch en/of menselijk vlak.** Een van de redenen waarom het onderzoek naar Attribute Based Access Control uitgevoerd gaat worden is de nieuwe Europese privacy wetgeving welke eraan zit te komen. In het onderzoek zal worden gekeken naar de impact van deze wetgeving op de huidige IAM situatie en zal worden ingegaan op hoe Attribute Based Access Control ten goede komt aan het privacyaspect.

13.) Het ontwerpen van IB-oplossingen, op technisch, organisatorisch en menselijk vlak. Gedurende het onderzoek zullen beide Access Management oplossingen worden getest op werking en mogelijkheden.

15.) Het overdragen van kennis m.b.t. IB aan stakeholders. Middels een adviesrapportage richting Centric zal worden ingegaan op de bevindingen uit het onderzoek en zal er worden stil gestaan bij de wijze waarop het onderzoek is uitgevoerd en de wijze waarop Centric Attribute Based Access Control zowel intern als extern kan inzetten.

16.) Het maken en/of uitvoeren van een plan voor implementatie van IB- richtlijnen, -procedures en –oplossingen. In het adviesrapport zal worden stil gestaan bij de wijze waarop Centric Attribute Based Acces Control zowel intern als extern kan inzetten.

Volgens: Beroepstaken opleiding ISMv3.0.pdf

Bijlage B: Project Initiation Document

Document historie

Versie	Status	Controle door	Datum
0.1	Concept	Arjan de Jong	25-02-2013
1.0	Final	Arjan de Jong	-

Distributie historie

Naam	Versie	Organisatie	Datum
Gé Iking	0.1	Centric	25-02-2013
Gé Iking	1.0	Centric	-

Inhoudsopgave

1. Inleiding en achtergrond project 65
2. Projectdefinitie 66
2.1 Doelstelling 66
2.2 Aanpak en fasering 66
2.3 Resultaten 66
2.4 Omvang 68
2.5 Scope 68
2.5 Randvoorwaarden en beperkingen 68
2.6 Relaties met andere projecten 68
3. Initiële Business Case 69
3.1 Redenen 69
4. Organisatiestructuur 71
4.1. Opdrachtgever 71
4.2. Opdrachtnemer 71
4.3. Examinatoren 71
4.4. Communicatieplan 71
5 Initiële projectplanning 73
5.1 Randvoorwaarden 73
5.2 Projectplanning 73
6. Beheersingsmechanismen 74
6.1 Toleranties 74
6.2 Beheersen 74
6.2 Voortgangsrapportage 74
7. Projectrisico's 74

1. Inleiding en achtergrond project

Dit onderzoeksvoorstel is geschreven met betrekking tot de afstudeerstage, "*Onderzoek voor Centric en haar klanten de toepassingsmogelijkheden van Identity & Access Management (IAM) op basis van anonieme attributen i.p.v. identiteiten.*" in opdracht van Centric. Het onderzoeksvoorstel wordt gezien als een plan van aanpak tijdens de stageperiode.

In dit document wordt de aanleiding, probleemstelling, doelstelling en de onderzoeksvragen weergegeven. Daarnaast worden de te gebruiken onderzoeksmethoden, bronnen en materialen besproken en zal de projectorganisatie in kaart worden gebracht. Tot slot wordt er in het voorlaatste hoofdstuk de planning weergegeven voor de gehele stageperiode en in het laatste hoofdstuk komen de beheeraspecten aan bod. De afstudeeropdracht wordt uitgevoerd door Arjan de Jong (08064733), student Information Security Management aan De Haagse Hogeschool te Zoetermeer.

De stage zal lopen van 18-02-2013 tot en met 12-07-2013 en de stage zal bestaan uit vier werkdagen per week.

Centric
Met ruim 5.300 medewerkers biedt Centric maatwerk- en standaardsoftware, infrastructuur, branche specifieke oplossingen en een uitgebreid portfolio van gerelateerde diensten.

De afdeling Techniek en Kwaliteit te Gouda houdt zich bezig met het adviseren en controleren van de units over keuze en gebruik van zowel interne en externe standaarden voor de ontwikkeling van toepassingen. Deze toepassingen worden gebruik door een groot aantal klanten.

De stafafdeling Techniek en Kwaliteit heeft de volgende hoofdtakken:

- Het mede bepalen van en richting geven aan het huidige en toekomstige gebruik van technieken voor software ontwikkeling en onderhoud, ook de hierbij behorende ondersteuning en dienstverlening.
- Het mede bepalen en richting geven aan het beleid, uitvoering en handhaving van kwaliteitszorg.

2. Projectdefinitie

Dit hoofdstuk beschrijft gedetailleerd de opdracht, de opdrachtgevers en de opdrachtnemer, de probleemstelling, het beoogde resultaat, de scoop van de opdracht, de randvoorwaarden en de mogelijke risico's.

2.1 Doelstelling

Het doel van het onderzoek is het opdoen van voldoende kennis over Identity & Access Management (IAM) en Access Management (AM) op basis van attributen, Attribute-Based Access Control (ABAC) voor zowel intern als extern gebruik bij klanten van Centric om te kunnen rapporteren over de voor en nadelen van het gebruik van ABAC door Centric.

De onderzoeksvragen zijn als volgt geformuleerd;

Centrale vraag;

- Onderzoek voor Centric en haar klanten de toepassingsmogelijkheden van Identity & Access Management (IAM) op basis van attributen i.p.v. identiteiten.

Deelvragen;

- Wat wordt er bedoeld met anonieme attributen?
- Waar worden anonieme attributen voor gebruikt?
- In welke situaties kan er gebruik worden gemaakt van anonieme attributen?
- Waarom zou dit nuttig kunnen zijn voor Centric?

2.2 Aanpak en fasering

Het project zal worden aangepakt volgens de Prince2 methodiek en bestaat uit de volgende fasen:

Fase	Omschrijving
Fase 1	Plan van aanpak
Fase 2	Vooronderzoek
Fase 3	Vaststellen requirements
Fase 4	Productonderzoek
Fase 5	Scenario onderzoek
Fase 6	Afsluiting project en advies

2.3 Resultaten

Het project moet uitmonden in een beargumenteerd advies aan Centric over de inzet van AM op basis van attributen voor zwel intern als extern bij klanten van Centric. Gedurende het gehele project zullen er in fases een aantal producten worden opgeleverd, hieronder volgt een verdeling van de verschillende (deel)producten toebedeeld aan hun fase:

Fase 1: Plan van aanpak

In deze eerste fase staat het opstellen van het plan van aanpak aan de hand van de Prince2 methodiek centraal. Hiervoor wordt een periode van twee weken uitgetrokken waarin ook tijd is gemaakt voor zelfstudie (zie fase 2) om meer inzicht te krijgen in de materie welke in het onderzoek aan bod komt.

Product	Omschrijving	Op te leveren aan
Project Initiation Document	Planning voor het gehele project	Opdrachtgever

Fase 2: Vooronderzoek (zelfstudie)
Het uitvoeren van literatuuronderzoek naar de wijze waarop huidige IAM systemen worden toegepast en werken. Welke ABAC systemen er naast de reeds bekende, Idemix (IBM) en U-Prove (Microsoft) er zijn die voldoen aan het criteria "de gebruiker toegang verlenen op basis van attributen i.p.v. op basis van zijn identiteit".

Product	Omschrijving	Op te leveren aan
-	-	-

Fase 3: Vaststellen requirements
De requirements waaraan een ABAC systeem aan dient te voldoen worden in fase drie vastgesteld, hiervoor zullen gesprekken plaatsvinden met medewerkers binnen Centric.

Product	Omschrijving	Op te leveren aan
Requirements	Hoe zien de gebruikelijke IAM situaties eruit, en waar willen we naar toe met ABAC.	Opdrachtgever

Fase 4: Productonderzoek
In deze vierde fase staat het uitvoeren van een productonderzoek naar Idemix (IBM) en U-Prove (Microsoft) centraal om vast te kunnen stellen of deze systemen voldoen aan de in fase drie vastgestelde requirements. Indien er uit het vooronderzoek is gebleken dat er ook andere systemen beschikbaar zijn zal de overweging worden gemaakt om deze wel of niet in het verdere onderzoek mee te nemen.

Product	Omschrijving	Op te leveren aan
Product onderzoek	Beschrijving van de systemen welke er op dit moment zijn, de functies welke deze systemen te bieden hebben en een vergelijking tussen deze systemen onderling.	Opdrachtgever

Fase 5: Scenario onderzoek
Aan de hand van een scenario onderzoek zal er in fase vijf worden vastgesteld in welke situaties het gebruik van anonieme attributen van toegevoegde waarde kan zijn voor Centric en haar Klanten.

Product	Omschrijving	Op te leveren aan
Onderzoeksrapport	Beschrijving van de bevindingen aan de hand van het scenario onderzoek.	Opdrachtgever

Fase 6: Afsluiting project en advies
Als afsluiting van het project zal er een advies- en onderzoeksrapport worden opgeleverd aan Centric met daarin de verantwoording voor de wijze waarop het onderzoek is uitgevoerd en een geargumenteerd advies over de toepassingsmogelijkheden van anonieme attributen voor Centric en haar klanten.

Product	Omschrijving	Op te leveren aan
Adviesrapport & Onderzoeksrapport	Het complete advies- en onderzoeksrapport waarin ook alle voorgaande documenten worden opgenomen.	Opdrachtgever & De Haagse Hogeschool

2.4 Omvang

Deze afstudeeropdracht zal worden uitgevoerd in de periode van 11 februari 2013 tot en met 7 juni 2013. Gedurende deze periode zal er 4 dagen in de week worden gewerkt aan het onderzoek zelf en zal er 1 dag per week aandacht worden besteed aan het afstudeerverslag behorende bij dit onderzoek.

2.5 Scope

De scope van het afstudeeronderzoek betreft het onderzoeken van de toepassingsmogelijkheden van anonieme attributen voor Centric en haar klanten. Dit onderzoek zal leiden tot een adviesrapportage gericht aan Centric over de mogelijkheden van anonieme attributen en in welke situaties dit gebruik van toegevoegde waarde kan zijn.

2.5 Randvoorwaarden en beperkingen

Om het project succesvol te kunnen afronden zijn er de volgende randvoorwaarden en beperkingen opgesteld;

- Centric stelt de afstudeerder in de gelegenheid om de faciliteiten aan te wenden, welke nodig zijn voor het op de juiste wijze af te kunnen ronden van de afstudeeropdracht. Dit betekend dat de afstudeerder binnen toegang heeft tot een werkplek en een laptop met werkende Internetverbinding gedurende de 32 uur durende werkweek (Ma - Do).
- Er dient ruimte te zijn voor een wekelijks overleg met de afstudeerbegeleider.
- Begeleiding vanuit De Haagse Hogeschool

2.6 Relaties met andere projecten

Er zijn geen directe relaties met andere projecten bekend.

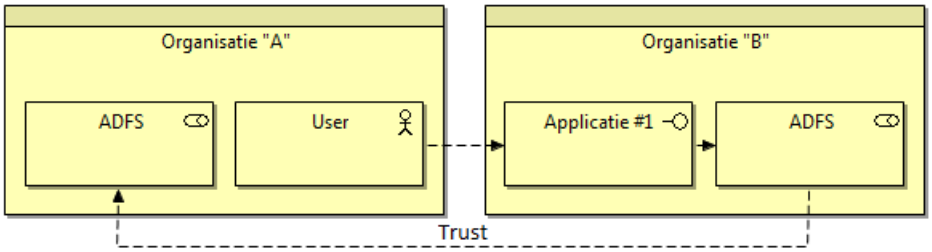
3. Initiële Business Case

3.1 Redenen

Centric heeft de behoefte om de mogelijkheden van Identity & Access Management (IAM) op basis van Attributen (geplaatst op een Smart Card) in plaats van identiteiten te laten onderzoeken. In de huidige IAM situatie binnen Centric weergegeven in *Figuur 0.1*, wordt het Access Management (AM) proces veelal ingebakken in de applicaties en wordt de authenticiteit gecheckt tegen een Identity Store.

Figuur 0.1. Access Management proces

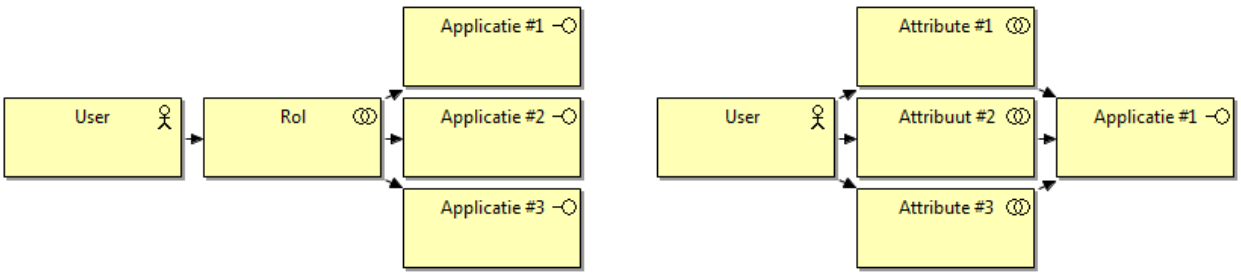
Door samenwerking tussen organisaties kan de behoefte ontstaat tot het delen van informatie, waardoor bovengenoemde IAM methode niet meer toereikend is. De gebruikers van organisatie "A" zijn niet bekend in het Identity systeem van organisatie "B". Dit vraagt voornamelijk bij de samenwerking tussen grotere organisaties, waarbij een grote hoeveelheid gebruikers over en weer gebruik maken van applicaties van de andere organisatie, een grotere beheerinspanning van beide organisaties. Hoe weet organisatie "A" bijvoorbeeld of gebruiker "X" nog in dienst is bij organisatie "B"? Het gebruik van bijvoorbeeld Active Directory Federated Services (ADFS) zoals weergegeven in *Figuur 0.2* waarbij de Active Directory omgevingen van beide organisaties aan elkaar worden gekoppeld, lost dit probleem grotendeels op. Hierbij vertrouwen beide organisaties erop dat de ander een goed en betrouwbaar IAM systeem gebruikt.



Figuur 0.2. Active Directory Federated Services (ADFS)

Een nadeel dat echter aan ieder IAM systeem kleeft is dat het omgaan met de daarin opgeslagen gegevens over de gebruikers dient te voldoen aan wetgeving wat betreft de privacybescherming. Een mogelijkheid om dit probleem op te kunnen lossen is de gebruiker niet op basis van zijn identiteit, maar op basis van zijn attributen toegang te verlenen, Attribute Based Access Control (ABAC).

In de huidige situatie wordt er veelal gebruik gemaakt van Role Based Access Control (RBAC), waarbij identiteiten in het IAM systeem worden gekoppeld aan bepaalde rol(len) binnen de organisatie. Deze rol(len) waaraan de gebruiker is gekoppeld zijn bepalend voor de toegangsrechten tot de informatiesystemen. In de ABAC situatie worden de toegangsrechten juist bepaald door de attributen welke de gebruiker bezit. In *Figuur 0.3* worden beide bovengenoemde methoden weergegeven.



Figuur 0.3., Role Based Access Control en Attribute Based Access Control

4. Organisatiestructuur

4.1. Opdrachtgever

Naam bedrijf	Centric Antwerpseweg 8 2803 PB Gouda P.O. Box 338 2800 AH Gouda 0182 - 648000 0182 - 648001
Contactpersoon / Bedrijfsbegeleider	Dhr. Gé Iking Business development consultant ge.iking@centric.eu 06 – 53940343

4.2. Opdrachtnemer

Naam	Dhr. J.J.G. de Jong (Arjan) Student Information Security Management De Haagse Hogeschool arjan1@gmail.com 06 – 43691265
Studentnummer	08064733

4.3. Examinatoren

Naam bedrijf	De Haagse Hogeschool Bredewater 24 2715 CA Zoetermeer 079 – 3208787
Contactpersonen	Dhr. Henk van de Ven Docent H.A.J.vandeVen@hhs.nl Mw. Marjolein Faassen Docent M.M.Faassen@hhs.nl

4.4. Communicatieplan

Na afronding van iedere fase zal er door de uitvoerder een rapportage worden verstrekt aan de opdrachtgever. Tussentijds zal er een conceptversie worden opgeleverd zodat onduidelijkheden in de rapportage nog voor definitieve oplevering kunnen worden aangepast. Iedere maandag ochtend wordt er een kort overleg ingeroosterd om de voortgang van het onderzoek te kunnen bespreken.

In het geval dat de deadline van een opdracht niet gehaald dreigt te worden zal dit middels een exception report aan de opdrachtgever worden gemeld.

Naam (functie)	Telefoon nummer	E-mail adres
Arjan de Jong (uitvoerder)	0643691265	arjan1@gmail.com
Gé Iking (Stage begeleider)	-	ge.iking@centric.eu
Marjolein Faassen (Begeleidend examinator)	-	m.m.faassen@hhs.nl
Henk van de Ven (Examinator)	-	h.a.j.vandeven@hhs.nl

5 Initiële projectplanning

5.1 Randvoorwaarden

Om de onderstaande projectplanning te kunnen realiseren dient er aan de randvoorwaarden te worden voldaan die in hoofdstuk 2.5 staan beschreven.

5.2 Projectplanning

In de onderstaande tabel zijn alle data en weeknummers opgenomen alsmede een korte omschrijving van hetgeen van start tot afsluiting van iedere fase wordt uitgevoerd.

Datum	Weeknummer	Project week	Omschrijving
18/02 - 23/02	8	1	Start Fase 1: Planning
25/02 - 01/03	9	2	
04/03 - 08/03	10	3	Start Fase 2: Zelfstudie
11/03 - 15/03	11	4	
18/03 - 22/03	12	5	
25/03 - 31/03	13	6	Start Fase 3: Requirements vaststellen
01/04 - 05/04	14	7	
08/04 - 12/04	15	8	Start Fase 4: Product onderzoek
15/04 - 19/04	16	9	
22/04 - 26/04	17	10	
29/04 - 03/05	18	11	Start Fase 5: Scenario onderzoek
06/05 - 10/05	19	12	
13/05 - 17/05	20	13	
20/05 - 24/05	21	14	Start Fase 6: Afsluiting project en advies
27/05 - 31/05	22	15	
03/06 - 07/06	23	16	**Opleveren projectdossier**

6. Beheersingsmechanismen

Voor het project wordt er een plan van aanpak / Project Initiation Document (PID) en (deel)producten opgeleverd. Om deze (deel)producten op te leveren worden er verschillende taken uitgevoerd. Om dit project succesvol af te ronden heb ik vastgelegd hoe ik dit project ga beheersen, bewaken en rapporteren.

6.1 Toleranties

Tijdens de uitvoering van het project controleert de uitvoerder regelmatig de voortgang. Indien de afwijking van de plannen naar verwachting groter is dan de afgesproken tolerantie, wordt daarover apart gerapporteerd aan de coach en opdrachtgever. De tolerantie op projectniveau is als volgt gedefinieerd:

- Doorlooptijd + / - 10%

6.2 Beheersen

Het beheersen van het project wordt gedaan door het PID als richtlijn te gebruiken. Door één document als richtlijn te nemen weten de opdrachtgever en de uitvoerder waar zij aan toe zijn.

Daarnaast worden gebruik gemaakt van de volgende Prince2 processen:

Initiating a Project (IP)

- De PID is samen gesteld om een beeld te krijgen van het project.

Planning (PL)

- Er wordt een gedetailleerde planning gemaakt en bijgehouden. Hierbij wordt de prince2-techniek product based planning toegepast.

Naast de methodes komen de volgende Prince2 Componenten aanbod:

- Plans
- Management of risk

Daarnaast passen we de volgende Prince2 technieken toe:

- Product-based planning
- Quality plan

6.2 Voortgangsrapportage

Tussentijds zullen de documenten/rapportages naar de opdrachtgever toe gestuurd worden om feedback te krijgen op het gemaakte werk. We hebben afgesproken dat het tijdig per mail word toegestuurd.
De feedback zal vervolgens verwerkt worden, zodat er een definitieve versie gemaakt kan worden.
Er kan gebruik gemaakt van drie soorten voortgangsrapportages:

- Highlight Report (reguliere voortgangsrapportage kwalitatief en kwantitatief)
- Exception Report (rapportage indien de tolerantiegrenzen van het project of de fase in tijd dreigt te worden overschreden)
- End Stage Report (terugblik op de afgelopen fase (evaluatie) en vooruitblik op de eerstkomende fase (faseplanning)).

7. Projectrisico's

Het risico bestaat dat er door een toenemende werkdruk of door ziekte de beoogde doelstellingen niet binnen de gestelde tijd behaald kunnen worden. De kans is dan ook aanwezig dat de einddatum bijgesteld dient te worden.

Bijlage C: Achtergrond: Identity & Access Management

Het onderzoek richt zich op de vraagstelling wat de toepassingsmogelijkheden zijn van Identity & Access Management (IAM) op basis van anonieme attributen in plaats van identiteiten. In deze bijlage worden toegelicht wat we verstaan onder het begrip IAM.

C.1 Deelprocessen

Het gehele IAM proces kent een aantal verschillende deelprocessen, hieronder worden de drie basis processen genoemd die bij iedere denkbare vorm van toegangscontrole plaats vinden, te weten: identificatie, authenticatie en tot slot autorisatie.

C.1.1 Identificatie

Identificatie is de eerste stap in het proces en is bedoeld om de identiteit van een persoon vast te stellen, deze identiteit is in de huidige situatie leidend voor de toegangsrechten op applicaties en informatiesystemen. De identiteiten van alle gebruikers van een applicatie en of informatiesysteem worden vastgelegd in een Identity Store.

C.1.2 Authenticatie

De tweede stap is Authenticatie, aan de hand van iets dat je weet (gebruikersnaam), iets dat je bezit (wachtwoord) en iets dat je bent (persoonlijke eigenschap) wordt er nagegaan of iemand daadwerkelijk die persoon is die hij of zij zegt te zijn.

C.1.3 Autorisatie

Autorisatie is de laatste stap en bepaald welke rechten iemand heeft op de betreffende applicatie of informatiesysteem.

C.2 Waarom toegangscontrole?

Het gehele IAM proces maakt het mogelijk om de toegangscontrole tot informatiesystemen en applicaties binnen een organisatie te kunnen managen. Het inrichten van een IAM systeem is complex en organisaties zitten hier dan vaak ook niet op te wachten. De redenen waarom er toch wordt gekozen om dit proces te implementeren komen voort vanuit zowel externe verplichtingen (wetgeving) als ook de interne behoefte (regelgeving).

C.2.1 Externe verplichting(en)

Mede door de toenemende en strenger wordende wet- en regelgeving op het gebied van veiligheid en privacybescherming worden organisaties geconfronteerd met een aantal verplichtingen waaraan zij dienen te voldoen. Organisaties welke genoteerd zijn aan de Amerikaanse beurs zijn onder meer bij de wet verplicht om te voldoen aan de Sarbanes-Oxley (2002)[24]. Financiële instellingen dienen op hun beurt te voldoen aan de Basel Capital Accord (Basel II, 2006)[25] en indien deze financiële instelling is gevestigd in Nederland dient er ook te worden voldaan aan de Code-Tabaksblad (2004)[26]. Daarnaast zijn alle Nederlandse organisaties welke persoonsgegevens verwerken verplicht om te

[24] Sarbanes-Oxley (2002) | http://nl.wikipedia.org/wiki/Sox

[25] Basel II (2006) | http://nl.wikipedia.org/wiki/Basel_II

[26] Code-Tabaksblad (2004) | http://nl.wikipedia.org/wiki/Code-Tabaksblat

voldoen aan de Wet Bescherming Persoonsgegevens (WBP, 2001)[27]. Op Europees niveau wordt er sinds enkele jaren gewerkt aan een nieuwe Europese privacy wetgeving, de General Data Protection Regulation (GDPR)[28] welke van toepassing zal zijn op alle lidstaten van de Europese Unie.

C.2.2 Interne regelgeving(en)

Naast de verplichting om te moeten voldoen aan de geldende wet- en regelgeving kan de invoering van het Identity & Access Management proces ook het gevolg zijn van de interne regelgeving van de organisatie zelf. Hierbij kunnen redenen als het klaarmaken van de organisatie voor een aanstaande fusie, overname of samenwerkingsverband met een andere organisatie een rol spelen, waardoor de implementatie van dit proces gewenst is. Daarnaast is ook het willen voldoen aan (inter)nationale standaarden zoals onder meer de ISO 27001 (Information Security Management System, 2005)[29] behoort tot de mogelijke redenen voor de implementatie van dit proces. Een juiste implementatie van Identity & Access Management brengt tevens vele voordelen met zich mee voor organisaties, haar medewerkers, klanten en partners op de vlakken van beveiliging, efficiëntie, kostenbesparing en gebruikersgemak.

[27] Wet Bescherming Persoonsgegevens (2001) | http://nl.wikipedia.org/wiki/Wet_bescherming_persoonsgegevens

[28] General Data Protection Regulation | http://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[29] ISO 27001 (2005) | http://nl.wikipedia.org/wiki/ISO_27001

Bijlage D: Achtergrond: Europese privacywetgeving

Binnen de Europese Unie geld sinds 1995 de Data Protection Directive richtlijn ter bescherming van persoonlijke gegevens. Deze richtlijn heeft er binnen de Europese Unie toe geleid dat iedere lidstaat haar eigen wetgeving heeft opgesteld op het gebied van bescherming van persoonsgegevens. Sinds 2011 is de Europese Unie dan ook begonnen met het opstellen van een nieuwe privacy wetgeving voor al haar lidstaten, de General Data Protection Regulation (GDPR). Met deze wetgeving hoopt Europa één lijn te kunnen trekken voor het beschermen van persoonsgegevens waaraan alle lidstaten dienen te voldoen.

De nieuwe wetgeving is op het moment nog volop in ontwikkeling, maar uit de laatste versie van de wet blijkt duidelijk welke richting de Europese Unie op wilt. De burger krijgt bij de invoering van deze wetgeving meer invloed op de gegevens welke over hen worden bijgehouden en verwerkt door organisaties en dienen zij voldoende te worden geïnformeerd door deze organisaties over de wijze waarop en waarom persoonlijke gegevens worden verwerkt.

Enkele punten welke in de Data Protection brochure[30] behorende bij de nieuwe wetgeving worden genoemd zijn als volgt;

Who can you trust?

- If you don't know how your information is being used it's hard to know who to trust it with. In future you'll be better informed and your data will be better protected. So you'll feel more confident when you're sharing your data with friends or when you go shopping online.

Putting you back in control

- Under the new laws, you'll have more control over what happens to your data. And you'll know where to go and who to talk to if you're not happy.

Giving your permission and understanding why

- In future you will know better how your data is being used and when your permission is required, you'll be asked to give it explicitly. If you're not happy you'll be able to change your mind. Everything will be explained clearly so you understand the decisions that you're making.

One set of rules

- They'll give the same protection to your personal data everywhere in the EU. Your data will also be protected outside the EU. So you'll have a high level of protection regardless of where your personal data is stored or handled. Good news for you, your businesses and for the economy.

Designed to protect your privacy

- They'll also make the settings of all sites privacy-friendly. So when using a social network you'll know that your data is protected unless you decide to change the privacy settings yourself.

What if you just want to be forgotten?

- It's not always easy to permanently delete your personal information after you've shared it. With the new rules it'll be much easier to take your data back. And to easily remove it completely and give it to another service provider, if that's what you decide.

Protecting your data worldwide

- Because your data is often collected, processed or stored outside the EU, your data will continue to be protected worldwide, for cloud computing or web-based email, for example.

Setting the standard

[30] http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf

- The new EU laws set high standards and have been written to stand the rest of time. They're safe, simple and effective and we hope that they'll become a model for the rest of the world to follow.

What happens if your data gets lost or stolen?

- At the moment, if your data is lost or stolen, it may take some time for you to find out. In future if this happens, and the consequences are expected to be serious, then both you and your country's Data Protection Authority will have to be told as soon as possible.

And Finally

- The new EU laws will put you in control of the information about yourself that you share online. They'll give you the right to know who's using your data and why and to know if the security of your data is at risk. And, of course, they'll give you the right to be forgotten.

Deze nieuwe wetgeving zal voor een groot aantal Europese organisaties betekenen dat er intern een aantal maatregelen doorgevoerd dienen te worden om aan deze wetgeving te kunnen voldoen. Zo dienen zij namelijk in de toekomst hun klanten op de juiste wijze te informeren over de wijze waarop zij gebruik maken van de verkregen persoonsgegevens, deze verwerken en beschermen. Daarnaast moeten organisaties hun klanten in staat stellen om persoonlijke informatie te laten aanpassen of zelfs permanent te laten verwijderen.

Bijlage E: Het productonderzoek

In deze bijlage worden de mogelijkheden en functionaliteiten van de twee oplossingen (IBM Idemix en Microsoft U-Prove) benoemd en beschreven. Deze zullen voornamelijk worden beschreven aan de hand van theoretische voorbeelden, zodat het duidelijk wordt op welke wijze deze oplossingen van nut kunnen zijn voor Centric en haar klanten. De achterliggende techniek en cryptografie vallen buiten de scope en zullen hierin ook niet worden opgenomen

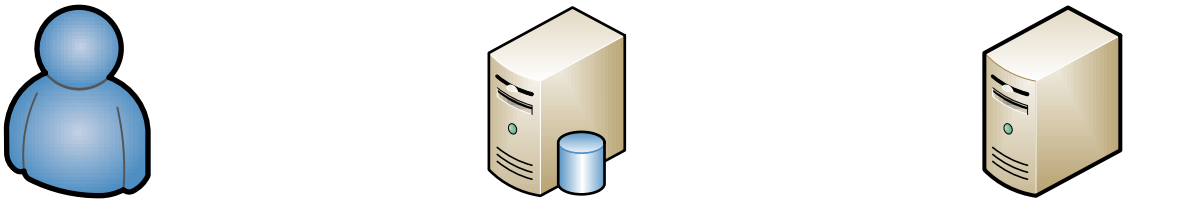
E.1 Achtergrond

IBM Idemix en Microsoft U-Prove zijn beide zogenoemde anonieme credential systemen gebaseerd op het concept van anonieme attributen.

Het systeem van Idemix is gebaseerd op de door Jan Camenisch en Anna Lysyanskaya (2001) ontwikkelde protocollen voor anonieme credentials[31]. Deze protocollen werden later door IBM Research Zurich geïmplementeerd in Idemix. De broncode is inmiddels beschikbaar gesteld onder de IBM Open Innovation Initiative[32]. Hierdoor is het systeem kosteloos door iedereen te gebruiken voor evaluatiedoeleinden en het ontwikkelen van eigen projecten. Deze broncode is enkel beschikbaar gesteld in Java.

Het anonieme credential systeem U-Prove is gebaseerd op de door Stephan Brands (2000) beschreven protocollen in zijn boek: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy[33]. Deze protocollen zijn door Credentica geïmplementeerd in U-Prove, waarna deze technologie in 2007 werd overgenomen door Microsoft. De broncode van deze oplossing is beschikbaar gesteld onder de Open Specification Promise[34] en is zowel beschikbaar in Java als C#.

E.1.1 Betrokkenen



Figuur E.0.1

Gebruiker

De gebruiker wordt in het autorisatieproces gezien als de persoon welke bepaalde attributen bezit, zoals bijvoorbeeld de organisatie waarvoor deze persoon werkzaam is en ook de functie binnen deze organisatie. Deze persoonlijke attributen kunnen door de gebruiker in een autorisatieproces worden gebruikt om te kunnen aantonen te voldoen aan de gestelde policyvoorwaarden[35] om zodoende toegang te kunnen krijgen tot de betreffende dienst(en).

[31] Camenisch, J and Herrewegen, E.V. | Design and implementation of the Idemix anonymous credential system. (2002)
[32] IBM's Open Innovation Initiative http://www.zurich.ibm.com/news/10/innovation.html
[33] Stephan Brands, Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy (2000)
[34] Open Specification Promise http://www.microsoft.com/openspecifications/en/us/programs/osp/security/default.aspx
[35] De voorwaarde waaraan een gebruiker dient te voldoen om gebruik te kunnen maken van de aangeboden dienst(en).

Identity Provider

De gebruikers kunnen de eigen persoonlijke attributen ophalen bij één of meerdere zogenoemde Identity Provider(s) (IdP). Een mogelijk voorbeeld van een IdP kan de organisatie zijn waarbij iemand werkzaam is (welke de persoonlijke attributen kan verschaffen op basis van het HRM systeem). De gebruiker bepaald zelf welke van de attributen hij/zij wilt ophalen bij een IdP. De uitgegeven attributen worden door deze IdP ondertekend met een certificaat, om zodoende kenbaar te kunnen maken dat de attributen afkomstig zijn van deze IdP. Deze attributen worden door de IdP geanonimiseerd uitgegeven, in de vorm die de gebruiker wilt hebben.

Service Provider

Als laatste is er de Service Provider (SP), dit is de dienstverlener waarbij een gebruiker een dienst wilt kunnen afnemen (bijvoorbeeld de toegang tot een applicatie). Deze SP maakt de policyvoorwaarden kenbaar aan de gebruiker en deze maakt aantoonbaar hieraan te voldoen door middel van de persoonlijke attributen. Pas vanaf het moment dat er aan deze policyvoorwaarden is voldaan krijgt de gebruiker toegang tot deze dienst.

E.1.2 Credentials

In beide genoemde systemen worden de persoonlijke attributen ondergebracht in een zogenoemde **Credential** (Idemix) of **Token**[36] (U-Prove). De structuur van deze is zonder naar de achterliggende technieken te kijken grotendeels gelijk aan elkaar.

Idemix credential;
- Een set attributen.
- Certificaat van de (IdP) welke de attributen heeft afgegeven.
- Privé sleutel.

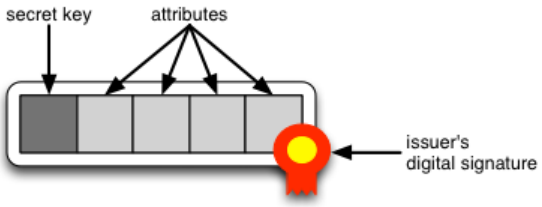
U-Prove token;
- Een set attributen.
- Certificaat van de (IdP) welke de attributen heeft afgegeven.
- Publieke sleutel.

Naast het verschil dat er in een Idemix credential de privé sleutel en in een U-Prove token de publieke sleutel wordt opgeslagen is er nog een verschil tussen beiden. In U-Prove is er namelijk voor het kunnen tonen van een attribuut uit een token voor iedere benodigde token een unieke privé sleutel nodig. In Idemix is één enkele privé sleutel voldoende om alle credentials te kunnen gebruiken. Het behoort echter ook in Idemix tot de mogelijkheden om ervoor te kiezen om meerdere privé sleutels[37] te gebruiken voor de verschillende credentials.

Gebruikers kunnen over meerdere credentials / tokens beschikken, afkomstig van verschillende IdP's. Daarnaast is het ook mogelijk dat een bepaald attribuut door meerdere (IdP)s wordt afgegeven, waardoor een gebruiker in een autorisatieproces kan kiezen met welke Prudential of token hij of zij wilt aantonen te voldoen aan de gestelde policyvoorwaarde(n).

[36] U-Prove Technology Overview V1.1 | http://research.microsoft.com/pubs/166980/U-Prove%20Technology%20Overview%20V1.1%20Revision%202.pdf

[37] Pim Vullers and Gergely Alpar | Efficient Selective Disclosure on Smart Card using Idemix | http://www.cs.ru.nl/~pim/publications/2013_idman.pdf



Figuur E.0.2 Idemix credential

E.1.3 Lopende projecten

In de afgelopen jaren zijn de Idemix en U-Prove bronsystemen in een aantal onderzoeksprojecten gebruikt, hieronder een kort overzicht van alle bekende onderzoeken en het bronsysteem welke in het project wordt gebruikt.

- I Reveal My Attributes, **IRMA**[38] (Idemix en U-Prove)
- 2010 – 2013: **ABC4TRUST**[39] (Idemix en U-Prove)
- 2010 – 2012: **di.me**[40] (Idemix)
- 2010: **FI-Ware**[41] (Idemix)
- 2008 – 2011: **PrimeLife**[42] (Idemix)
- 2004 – 2008: **PRIME**[43] (Idemix)

E.2 Autorisatie

Dit hoofdstuk beschrijft de wijze waarop autorisatie binnen Idemix en U-Prove kan plaatsvinden. Als eerste worden in paragraaf 1.2.1 de verschillende (hulp)middelen en paragraaf 1.2.2 de authenticatiemethoden benoemd. In paragraaf 1.2.3 wordt vervolgens het gehele autorisatieproces beschreven. Er zijn zonder naar de achterliggende techniek te kijken geen noemenswaardige verschillen tussen Idemix en U-Prove, waardoor deze in de uitwerking van dit hoofdstuk niet afzonderlijk van elkaar worden beschreven.

E.2.1 (hulp)middelen

Om gebruik te kunnen maken van Idemix en of U-Prove kunnen er een aantal verschillende autorisatiemiddelen worden gebruikt. Hoewel deze middelen onderling enigszins van elkaar verschillen blijft het uiteindelijke resultaat gelijk. De gebruiker kan door middel van zijn of haar persoonlijke attributen in een autorisatieproces aantonen te voldoen aan de gestelde policyvoorwaarden van de SP.

Het gebruik van een desktop of mobile device (laptop, smartphone en tablet) is één van de mogelijke (hulp)middelen. Naast het gebruik van een mobile device behoort het ook tot de mogelijkheden om een smartcard (al dan niet in combinatie met een desktop of mobile device) te gebruiken.

E.2.2 Autorisatiemethoden

[38] I Reveal My Attributes | IRMA | https://www.irmacard.org/
[39] ABC4TRUST - http://www.abc4trust.eu/
[40] di.mi - http://www.dime-project.eu/
[41] FI-Ware - http://fi-ware.morfeo-project.org/
[42] PrimeLife - http://www.primelife.eu/
[43] PRIME - https://www.prime-project.eu/

In deze paragraaf worden de verschillende mogelijkheden van autorisatie door middel van het gebruik van het concept van anonieme attributen benoemd.

Het gebruik van het concept van anonieme attributen kan zowel worden toegepast in Persoon – Service als Service – Service autorisatieprocessen. Deze situatie kan zich zowel online als offline voordoen, maar omdat het onderzoeksproject zich enkel richt op de digitale situaties zal er alleen worden ingegaan op de online processen.

Aan de hand van de in de voorgaande twee paragrafen benoemde (hulp)middelen en methoden wordt er in deze paragraaf het gehele autorisatieproces beschreven.

Persoon – Service autorisatieproces

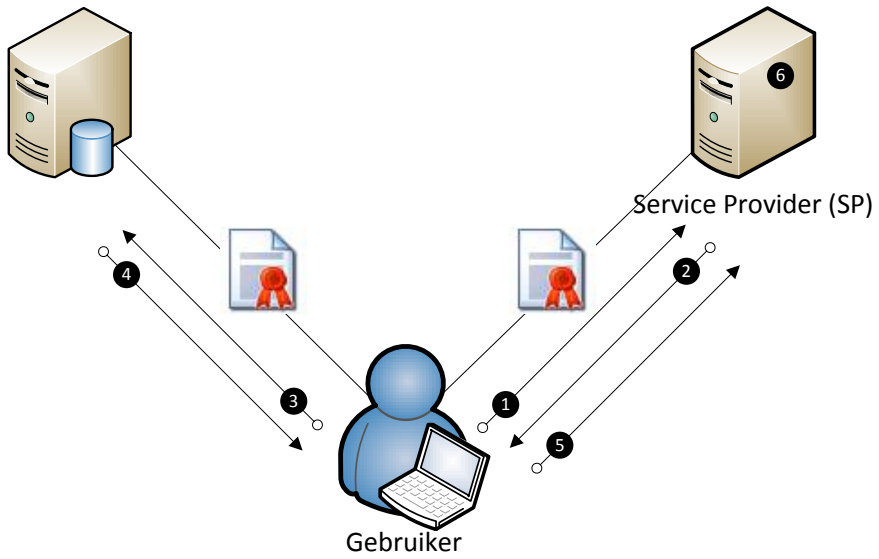
Het Persoon – Service autorisatieproces kan op een tweetal verschillende manieren worden ingericht, waarbij de benodigde attributen gedurende het autorisatieproces worden opgehaald bij één of meerdere IdP's of de benodigde attributen al voorafgaande aan het autorisatieproces zijn opgehaald bij één of meerdere IdP's. Om de te doorlopen processen te kunnen verduidelijken wordt er gebruik gemaakt van een theoretisch voorbeeld.

Uitgangssituatie;

De medewerkers van de afdeling inkoop van organisatie x maken voor hun dagelijkse werkzaamheden gebruik van applicatie y. De ontwikkelaars hebben bij de ontwikkeling van deze applicatie de policyvoorwaarden opgesteld waaraan gebruikers dienen te voldoen om toegang te kunnen krijgen tot deze applicatie. Gebruikers die de gevraagde attributen "Medewerker organisatie x" en "Afdeling inkoop" kunnen tonen wordt toegang verleent tot deze applicatie.

Het ophalen en tonen van attributen

In onderstaande voorbeeld (Figuur 0.3) wordt de mogelijkheid weergegeven waarbij een gebruiker de benodigde attributen gedurende het autorisatieproces ophaalt bij één IdP.



Figuur 0.3 Het ophalen en tonen van attributen

Stap 1: De gebruiker opent de applicatie.

Stap 2: De SP stelt de gebruiker op de hoogte van de policyvoorwaarden waaraan voldaan dient te worden om gebruik te kunnen maken van deze applicatie.

Stap 3: De gebruiker vraagt de voor het autorisatieproces benodigde attributen aan bij een IdP, in deze situatie de eigen organisatie.

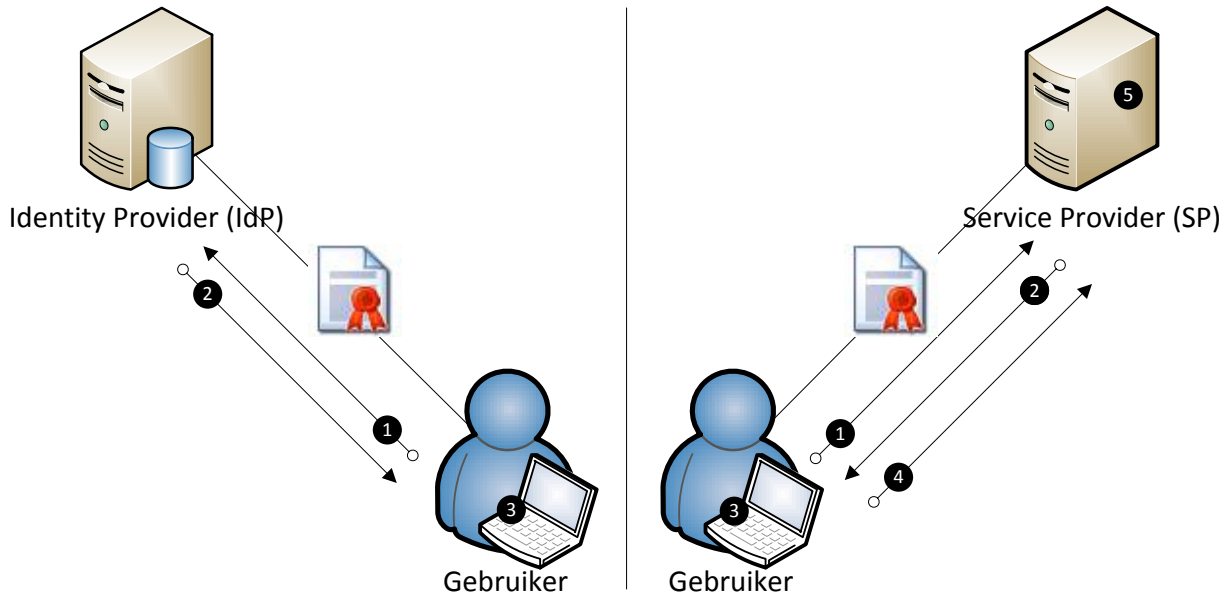
Stap 4: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen. De attributen worden in een geanonimiseerde vorm ontvangen.

Stap 5: De gebruiker toont de attributen aan de SP, omdat deze in een geanonimiseerde vorm zijn opgehaald bij de IdP worden er geen identificerende gegevens getoond. Enkel het kunnen aantonen te beschikken over de benodigde attributen en daarmee te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 6: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de betreffende applicatie.

Het ophalen en tonen van attributen als twee losse processen

Het behoort eveneens tot de mogelijkheden om voorafgaande aan het autorisatieproces de persoonlijke attributen bij een IdP (of meerdere IdP's) op te halen, om deze vervolgens op een later moment te kunnen gebruiken in een autorisatieproces. In onderstaande voorbeeld (Figuur 0.4) worden deze mogelijkheid weergegeven en vervolgens stapsgewijs toegelicht.



Figuur 0.4 Het ophalen en tonen van attributen als twee losse processen

Het ophalen van attributen bij een IdP (links).

Stap 1: De gebruiker vraagt zijn of haar persoonlijke attributen (of een selectie daarvan) aan bij een IdP.

Stap 2: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen. De attributen worden in een geanonimiseerde vorm ontvangen.

Stap 3: De opgehaalde attributen worden in een credential store opgeslagen.

Het tonen van attributen aan een SP (rechts).

Stap 1: De gebruiker opent de applicatie.

Stap 2: De SP stelt de gebruiker op de hoogte van de policyvoorwaarden waaraan voldaan dient te worden om gebruik te kunnen maken van deze applicatie.

Stap 3: De credential store, waarin de eerder opgehaalde attributen in opgeslagen staan wordt door de gebruiker geopend (door middel van zijn privé sleutel).

Stap 4: De gebruiker toont de attributen aan de SP, omdat deze in een geanonimiseerde vorm zijn opgehaald bij de IdP worden er geen identificerende gegevens getoond. Enkel het kunnen aantonen te beschikken over de benodigde attributen en daarmee te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 5: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de betreffende applicatie.

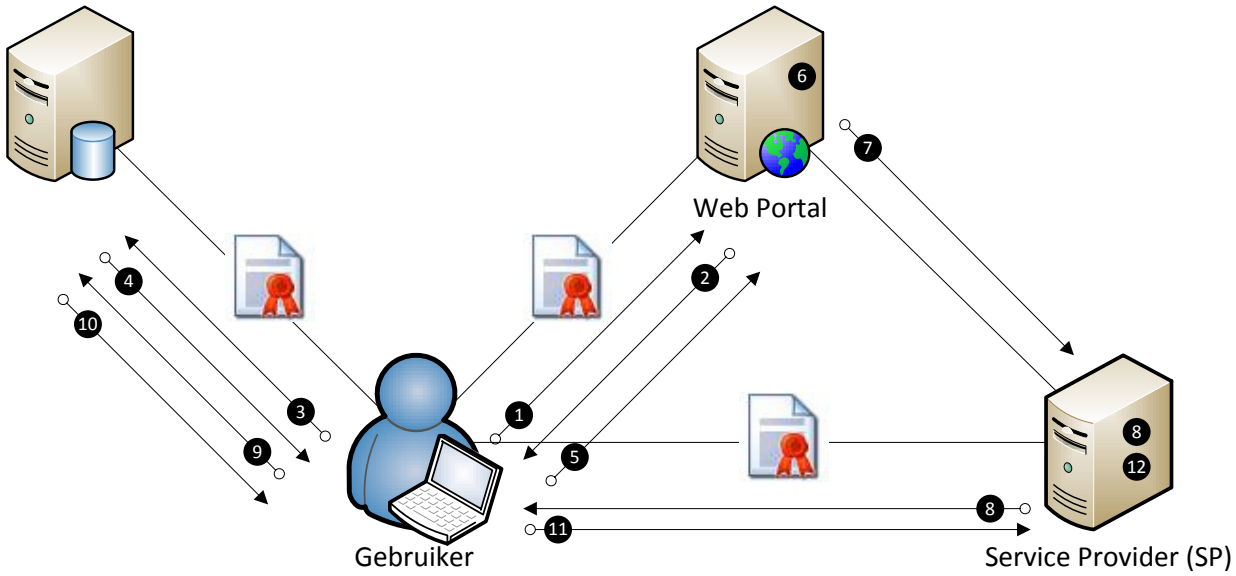
Persoon – Service autorisatie

Naast het Persoon – Service autorisatieproces kan er ook Service – Service autorisatie plaatsvinden, hierbij valt te denken aan de toegang tot applicaties die te benaderen zijn via een web portal. Ook hierbij zijn de twee eerdergenoemde manieren mogelijk, waarbij de benodigde attributen gedurende het autorisatieproces worden opgehaald bij één of meerdere IdP's of de benodigde attributen al voorafgaande aan het autorisatieproces zijn opgehaald bij één of meerdere IdP's. Om de te doorlopen processen te kunnen verduidelijken wordt er eveneens gebruik gemaakt van een theoretisch voorbeeld.

<u>Uitgangssituatie;</u>
De medewerkers van de afdeling sales van organisatie x maken voor hun dagelijkse werkzaamheden gebruik van applicatie y en applicatie z. Deze applicaties zijn te benaderen via een web portal. De ontwikkelaars hebben bij de ontwikkeling van deze applicaties de policyvoorwaarden opgesteld waaraan gebruikers dienen te voldoen om toegang te kunnen krijgen tot deze applicatie. Gebruikers die de gevraagde attributen "Medewerker organisatie x" en "Afdeling sales" kunnen tonen wordt toegang verleent tot de web portal, voor applicatie y gelden dezelfde policyvoorwaarden en voor applicatie z is enkel toegankelijk voor de managers van deze afdeling en daarbij geld dan ook als aanvullende policyvoorwaarde het kunnen aantonen van het attribuut "Manager afdeling sales".

Het ophalen en tonen van attributen

In onderstaande voorbeeld (Figuur 7.2) wordt de mogelijkheid weergegeven waarbij een gebruiker de benodigde attributen gedurende het autorisatieproces ophaalt bij een IdP.



Figuur 0.5 Het ophalen en tonen van attributen

Stap 1: De gebruiker opent de web portal.

Stap 2: De SP stelt de gebruiker op de hoogte van de policyvoorwaarden waaraan voldaan dient te worden om gebruik te kunnen maken van deze web portal.

Stap 3: De gebruiker vraagt de voor het autorisatieproces benodigde attributen aan bij een IdP, in deze situatie de eigen organisatie.

Stap 4: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen.

Stap 5: De gebruiker toont de attributen aan de SP, omdat deze in een geanonimiseerde vorm zijn opgehaald bij de IdP worden er geen identificerende gegevens getoond. Enkel het kunnen aantonen te beschikken over de benodigde attributen en daarmee te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 6: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de web portal.

Stap 7: De gebruiker opent de applicatie.

Stap 8: De SP verleent de gebruiker toegang tot de betreffende applicatie indien er hierop dezelfde policyvoorwaarden van kracht zijn als voor de toegang tot de web portal. Indien er aanvullende attributen nodig zijn om te kunnen voldoen aan de policyvoorwaarden behorende bij deze applicatie wordt de gebruiker hiervan op de hoogte gesteld.

Stap 9: De gebruiker vraagt de voor het autorisatieproces benodigde attributen aan bij een IdP, in deze situatie de eigen organisatie.

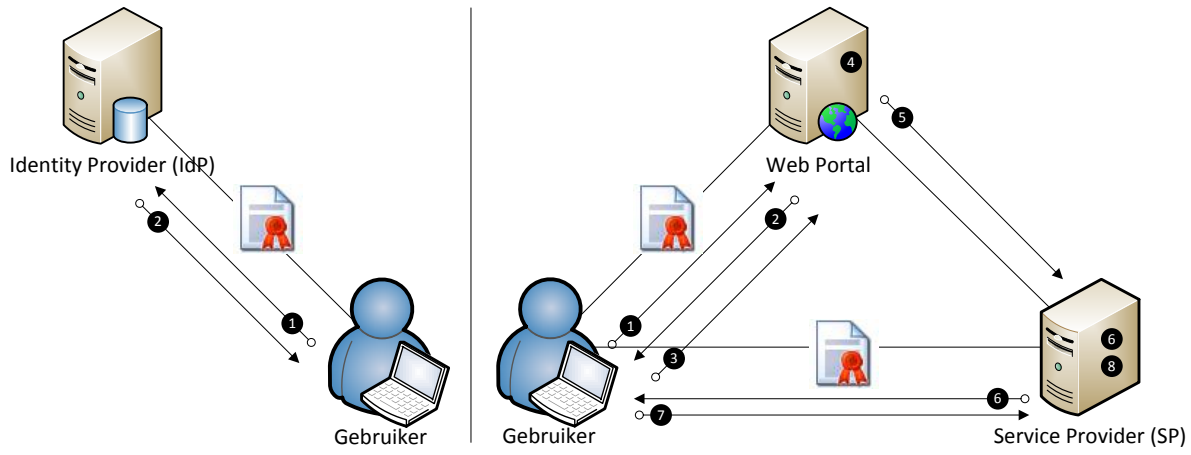
Stap 10: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen.

Stap 11: De gebruiker toont de attributen aan de SP, omdat deze in een geanonimiseerde vorm zijn opgehaald bij de IdP worden er geen identificerende gegevens getoond. Enkel het kunnen aantonen te beschikken over de benodigde attributen en daarmee te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 12: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de betreffende applicatie.

Het ophalen en tonen van attributen als twee losse processen

Het behoort eveneens tot de mogelijkheden om voorafgaande aan het autorisatieproces de persoonlijke attributen bij een IdP (of meerdere IdP's) op te halen, om deze vervolgens op een later moment te kunnen gebruiken in een autorisatieproces. In onderstaande voorbeeld (Figuur 0.6) worden deze mogelijkheid weergegeven en vervolgens stapsgewijs toegelicht.



Figuur 0.6 Het ophalen en tonen van attributen als twee losse processen

Het ophalen van attributen bij een IdP (links).

Stap 1: De gebruiker vraagt zijn of haar persoonlijke attributen (of een selectie daarvan) aan bij een IdP.

Stap 2: De IdP controleert of de gebruiker is wie hij of zij zegt te zijn en verstrekt vervolgens de aangevraagde attributen. Deze attributen worden daarbij voorzien van een certificaat waarmee wordt aangegeven van welke IdP de attributen afkomstig zijn. Het HRM systeem is een mogelijke bron voor de uitgifte van deze attributen. De attributen worden in een geanonimiseerde vorm ontvangen.

Stap 3: De opgehaalde attributen worden in een credential store opgeslagen.

Het tonen van attributen aan een SP (rechts).

Stap 1: De gebruiker opent de web portal.

Stap 2: De SP stelt de gebruiker op de hoogte van de policyvoorwaarden waaraan voldaan dient te worden om gebruik te kunnen maken van deze web portal.

Stap 3: De gebruiker toont de attributen aan de SP, omdat deze in een geanonimiseerde vorm zijn opgehaald bij de IdP worden er geen identificerende gegevens getoond. Enkel het kunnen aantonen te beschikken over de benodigde attributen en daarmee te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 4: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de web portal.

Stap 5: De gebruiker opent de applicatie.

Stap 6: De SP verleent de gebruiker toegang tot de betreffende applicatie indien er hierop dezelfde policyvoorwaarden van kracht zijn als voor de toegang tot de web portal. Indien er aanvullende attributen nodig zijn om te kunnen voldoen aan de policyvoorwaarden behorende bij deze applicatie wordt de gebruiker hiervan op de hoogte gesteld.

Stap 7: De gebruiker toont de attributen aan de SP, omdat deze in een geanonimiseerde vorm zijn opgehaald bij de IdP worden er geen identificerende gegevens getoond. Enkel het kunnen aantonen te beschikken over de benodigde attributen en daarmee te voldoen aan de gestelde policyvoorwaarden is voldoende.

Stap 8: De SP controleert tot slot aan de hand van de certificaten of de getoonde attributen afkomstig zijn van een vertrouwde IdP en verleent de gebruiker daarna toegang tot de betreffende applicatie.

E.3 Functionaliteiten

Zowel Idemix als U-Prove beschikken over een aantal functionaliteiten waarmee de privacy en anonimiteit van de eindgebruiker kan worden gewaarborgd. In deze paragraaf worden deze functionaliteiten beschreven. De achterliggende techniek wordt waar nodig benoemd, maar wordt niet in detail beschreven.

E.3.1 Unlinkability

In de huidige Identity & Access Management (IAM) toepassingen is het mogelijk om gegevens over een identiteit aan elkaar te linken. Hierbij valt te denken aan de verschillende informatiesystemen en applicaties waarop een persoon in heeft gelogd, het tijdstip waarop is ingelogd. In het kader van privacy en anonimiteit is het niet langer wenselijk dat deze gegevens aan elkaar te linken zijn.

Met Idemix (IBM) is het niet mogelijk om het gebruik van de verkregen attributen met elkaar te linken. De (IdP) komt niet te weten waar en wanneer de verkregen attributen zijn gebruikt. Zelfs niet in situaties waarbij de (IdP) ook de rol heeft van Verifier (bijvoorbeeld een gemeentehuis). Hiermee kunnen we voorkomen dat dienstverleners de getoonde attributen kunnen gebruiken om een profiel op te stellen van individuele klanten.

Bij U-Prove (Microsoft) is het in principe ook mogelijk om het linken van getoonde attributen te kunnen voorkomen, echter is dit in de praktijk erg omslachtig om toe te passen. Ieder verkregen attribuut is uniek, maar het gebruik van attribuut zorgt ervoor dat het gebruik te linken is aan eerder of toekomstig gebruik. In theorie is het zelfs mogelijk om het gebruik van een attribuut bij twee verschillende services met elkaar te linken. Hiervoor dienen beide services wel de logbestanden naast elkaar te leggen om deze link te kunnen maken. Om te kunnen voorkomen dat het gebruik van een attribuut te linken is kan de gebruiker ervoor kiezen om bij de (IdP) het gebruikte attribuut te laten vervangen door een nieuw uniek attribuut.

E.3.2 Untreceability

Door middel van de Selective Disclosure functionaliteit welke beide systemen ondersteunen wordt de inhoud van de attributen niet getoond aan de (SP). Er wordt enkel aangetoond dat de Prover in het bezit is van het gevraagde attribuut en voldoet aan de door de (SP) gestelde policy. De gebruiker kan hierdoor in beide systemen zijn persoonlijke attributen gebruiken in een authenticatieproces, en toch volledig anoniem blijven waardoor zijn of haar privacy volledig wordt gewaarborgd.

E.3.3 Revocability

Attributen als de achternaam, voornaam, geboortedatum en geboorteplaats van een persoon veranderen zelden tot niet. Vele andere attributen zoals student, functie en medewerker organisatie x zullen na verloop van tijd hoogst waarschijnlijk veranderen.

In een situatie waarbij de fysieke toegang tot het bedrijfspand afhankelijk is van het wel of niet kunnen tonen van het attribuut "medewerker organisatie x" is het uitsluitend mogelijk om binnen te komen nadat een medewerker heeft aangetoond in het bezit te zijn van het gevraagde attribuut. De organisatie heeft hierin zowel de rol van (IdP) als Verifier. De medewerkers worden door de organisatie voorzien van de benodigde attributen op de persoonlijke smartcard en in ieder authenticatie proces binnen de organisatie wordt gecontroleerd of de eigenaar van de smartcard in het bezit is van de benodigde attributen. Het attribuut "medewerker organisatie x" zou na verloop van tijd niet langer meer van toepassing kunnen zijn op de eigenaar van de smartcard, bijvoorbeeld na het beëindigen van het dienstverband. Hierdoor is het niet langer wenselijk dat de betreffende persoon toegang heeft tot het bedrijfspand en of de informatiesystemen en applicaties van de organisatie. De afgegeven attributen dienen dan ook te worden ingetrokken.

Het intrekken van attributen is in U-Prove mogelijk, echter is hiervoor wel direct contact tussen de smartcard en een terminal noodzakelijk. De organisatie dient een zogenaamde zwarte lijst bij te houden waarin wordt bijgehouden welke attributen van welke smartcard / persoon dienen te worden ingetrokken. Deze lijst dient vervolgens te worden gekoppeld aan één of meerdere terminals, iedere keer dat een medewerker zijn smartcard gebruikt bij de betreffende terminal wordt er in de zwarte lijst gecontroleerd of er eventueel attributen dienen te worden ingetrokken. Het intrekken van attributen kan op basis van verschillende methoden, het token ID, het serie nummer bijgevoegd in een token informatie veld, het serie nummer in een geheim attribuut of het innemen van de gehele smartcard. Deze laatste mogelijkheid is alleen een optie als het om een bedrijfspas gaat en niet wanneer het een persoonlijke smartcard betreft welke de gebruiker ook in andere situaties gebruikt.

Daarnaast heeft dit proces van het intrekken van attributen een vertraging tot gevolg, welke iedere keer optreed wanneer er een smartcard wordt getoond aan de terminal. Deze vertraging kan worden geminimaliseerd door te kiezen voor het spreiden of juist centraliseren van dit proces. Bij het spreiden wordt er bij iedere terminal op de eigen zwarte lijst gecontroleerd of er attributen

ingetrokken dienen te worden, hierdoor is er een geringe vertraging per terminal welke echter wel bij ieder gebruik plaats vind. En daarnaast dient de organisatie niet één, maar meerdere zwarte lijsten bij te houden. Door de controle plaats te laten vinden op een centrale plaats, bijvoorbeeld de terminal bij de entree van het bedrijfspand waarbij de toegang tot het pand wordt bepaald, hoeft er slechts één enkele zwarte lijst te worden bijgehouden. De vertraging wordt daardoor op deze locatie wel groter, maar er hoeft vervolgens nergens meer een tweede controle plaats te vinden.

Het intrekken van attributen is bij Idemix niet mogelijk, omdat deze smartcards zo ingericht kunnen worden dat ze alleen aantoonbaar maken in het bezit te zijn van het gevraagde attribuut zonder het daadwerkelijke attribuut te tonen. Het systeem biedt wel de mogelijkheid om een verloopdatum te koppelen aan een attribuut, voor het attribuut "medewerker organisatie x" kan de verloopdatum bijvoorbeeld gelijk zijn aan het einde van het contract van de betreffende medewerker (in het geval van een vast dienstverband kan er worden gekozen voor een x aantal maanden). Zodra deze periode is verstreken is het niet langer mogelijk om het betreffende attribuut te gebruiken en dient er in het geval van een contractverlenging het attribuut opnieuw op de smartcard te worden geladen door de (IdP).

In beide systemen is het tevens een mogelijkheid om de toegangscontrole niet enkel te laten plaatsvinden op basis van het attribuut "medewerker organisatie x", maar een combinatie van dit attribuut met een attribuut "einddatum dienstverband". De terminal controleert of de medewerker in het bezit is van het attribuut "medewerker organisatie x" en of het attribuut "einddatum dienstverband" niet verstreken is. Zodra deze datum is verstreken is de eigenaar van de smartcard nog wel in het bezit van beide attributen, maar is de toegang tot het bedrijfspand alsnog niet mogelijk. Ook in dit geval kan er bij het verlengen van het dienstverband het attribuut "einddatum dienstverband" door de (IdP) worden vervangen voor een nieuw attribuut.

E.3.4 Full Disclosure

Met het systeem van Microsoft is het mogelijk om in een authenticatieproces de exacte inhoud van de attributen weer te geven. Door gebruik te maken van deze optie veranderd er in principe weinig tot niets ten opzichte van de wijze waarop authenticatie op dit moment plaats vind in de persoon – service situaties. De (SP) krijgt inzicht in de persoonlijke attributen, iets wat we juist willen voorkomen doormiddel van de implementatie van Idemix en of U-Prove.

E.3.5 Selective Disclosure

In beide systemen is het mogelijk[44] om enkel aan te kunnen tonen in het bezit te zijn van de gevraagde attributen, de gebruiker toont de (SP) enkel de gevraagde (strikt noodzakelijke) attributen. De (SP) krijgt hierbij enkel de gevraagde attributen te zien en verder niets. Daarnaast is het ook mogelijk om in zowel Idemix[38] als U-Prove aan te kunnen tonen te voldoen aan een bepaalde policy als 16+ of 18+ ter behoeve van bijvoorbeeld de leeftijdsverificatie bij de aankoop van leeftijdsgebonden producten, zonder dat de exacte geboortedatum kenbaar gemaakt hoeft te worden. Enkel het gegeven dat een gebruiker voldoet aan de gestelde policy is voldoende. De gebruiker wordt zowel bij Idemix als U-Prove (bijvoorbeeld na het plaatsen van de smartcard in de cardreader of terminal) geïnformeerd over de policy waaraan voldaan dient te worden. Indien de gebruiker in het bezit is van meerdere Credentials waarin het gevraagde attribuut staat, kan de gebruiker (mits de (SP) de (IdP) welke de Credential / Token heeft afgegeven als vertrouwde partij erkend) zelf beslissen welke Credential / Token hij of zij wenst te gebruiken om aan te tonen aan de gestelde policy te voldoen. Indien de akkoord wordt gegaan met de gestelde policy en men wilt kunnen aantonen hieraan te voldoen dient de persoonlijke pincode behorende bij de Credential / Token te worden ingevoerd op de terminal of cardreader.

[44] Internet2.edu | https://spaces.internet2.edu/download/attachments/33099874/anonymous-credentials-v3.pdf?version=1&modificationDate=1361419049989