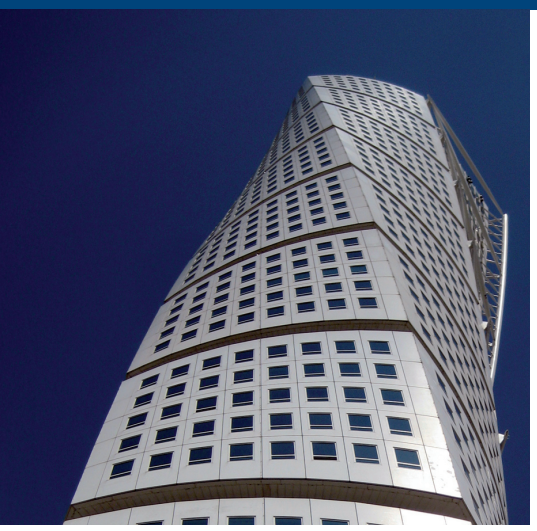


Federated Identity Management, het perspectief van de IT-auditor

Drs. W.A. Guensberg CISA
is sinds 1 januari 2007 in dienst bij KPMG IT Advisory. Zijn werkzaamheden spitsen zich voornamelijk toe op IT-auditing en Identity and Access Management (IAM). In maart 2009 rondde hij zijn IT-auditopleiding af aan de Vrije Universiteit met een scriptie over de IT-auditaandachtspunten van Federated Identity Management, en in september 2009 behaalde hij zijn CISA-titel.

guensberg.willem@kpmg.nl

P.E. van der Hulst
is manager bij KPMG IT Advisory te Amstelveen. In zijn dagelijkse werkzaamheden voert hij (certificerings)audits uit op het gebied van informatiebeveiliging en begeleidt hij organisaties als projectmanager en adviseur bij het implementeren van Identity & Access Management-concepten.

vanderhulst.emanuel@kpmg.nl

Drs. Willem Guensberg CISA en Emanuël van der Hulst

Identity & Access Management (IAM) is een vakgebied dat steeds professioneler wordt benaderd in de meeste moderne organisaties. Terwijl de volwassenheid van IAM-strategieën toeneemt, heeft zich een nieuwe grens afgetekend: Federated Identity Management of FIM. FIM definieert de verzameling overeenkomsten, standaarden en technologieën die het mogelijk maken identiteitsgegevens uit te wisselen over autonome domeinen. Naarmate de voordelen van FIM duidelijk worden, neemt de interesse toe in de vraag hoe FIM geïmplementeerd zou moeten worden en wat hierbij de belangrijkste aandachtspunten zijn. Door de belangrijkste aandachtspunten of 'kenmerken' van een FIM-implementatie in ogenschouw te nemen kunnen organisaties hun FIM op een betrouwbare wijze inrichten zodat IT-auditors dat op een effectieve wijze kunnen beoordelen.

Inleiding

In een wereld die steeds internationaler wordt, hebben steeds meer organisaties te maken met het immer toenemende tempo waarmee informatie met partners wordt uitgewisseld. Het effectief en efficiënt kunnen samenwerken met leveranciers en klanten, en tegelijkertijd 'in control' zijn over de informatiestromen, is één van de critical success factors geworden voor hedendaagse organisaties. Ook het beveiligen van toegang tot informatie is een belangrijk aandachtspunt voor moderne organisaties. Vanuit dit aandachtspunt zijn strategieën ontwikkeld voor het beheer van identiteiten en logische toegangsbeveiliging (Engels: Identity & Access Management, IAM) die van oorsprong gebaseerd zijn op een lokaal en afgeschermd beveiligingsdomein. Door het landschap van informatiebronnen te 'verdelen' in lokale domeinen, werd het mogelijk een nauwkeurig gedefinieerde groep gebruikers toegang te verlenen tot een nauwkeurig gedefinieerde groep bronnen. Echter, de toegang tot deze groep bronnen moet in de wereld van nu worden uitgebreid naar externe werknemers of vestigingen, autonome delen van de organisatie, externe partners en veel meer buitenstaanders. Zonder adequate beheersingsmaatregelen is te verwachten dat de risico's voor veiligheid toenemen. De concepten, technische oplossingen en standaarden zijn inmiddels dermate ontwikkeld dat veilige en gecontroleerde uitwisseling van informatie tussen autonome entiteiten mogelijk is. Onder de noemer *Federated Identity Management* stelt dit organisaties in staat de toegang van

partners tot hun bronnen te beheersen en om de bronnen van die partners te gebruiken.

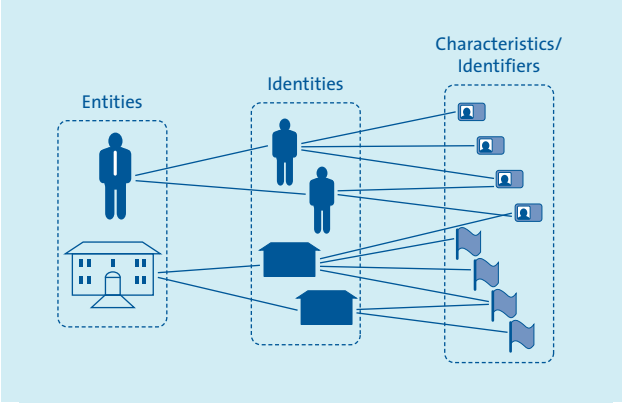
Terwijl FIM sinds de introductie begin 2000 ([Norlo2]) steeds meer wordt toegepast, zien IT-auditors en organisaties zich genoodzaakt een antwoord te vinden op de uitdagingen die dit nieuwe concept met zich meebrengt. Zowel de gebruikers als de organisaties kunnen significante voordelen behalen, gegeven dat de overeenkomstige risico's adequaat worden beheerst. Dit artikel biedt een high-level handvat door inzicht in de belangrijkste kenmerken van een FIM-implementatie te geven. Deze kenmerken kunnen organisaties helpen bij het implementeren van een betrouwbare FIM-omgeving en IT-auditors bij het uitvoeren van een adequate audit op deze FIM-omgeving. Hierbij benadert dit artikel FIM vanuit het perspectief van de dienstverleners.

Wat is Federated Identity Management?

Beheer van identiteiten

Een identiteit is een 'representatie van een entiteit in een specifiek applicatiedomein' ([Jøsa05]). In een typische werkelijke situatie vertegenwoordigen entiteiten gewoonlijk *juridische* entiteiten (bijvoorbeeld natuurlijke personen of organisaties). Voorbeeld van een identiteit zouden de geregistreerde persoonlijke gegevens van een werknemer kunnen zijn, mogelijk aangevuld met enkele fysieke karakteristieken van die persoon, alle binnen het applicatiedomein van de werkgever. Een identiteit kan ook een systeem representeren. Identiteiten zijn opgemaakt uit een verzameling karakteristieken, identificators genaamd (zoals de accountID, naam en geboortedatum van een persoon). Binnen het beheer van identiteiten (Engels: Identity Management) nemen dienstverleners ofwel serviceproviders een belangrijke positie in. Een serviceprovider is 'een entiteit die diensten verleent aan andere entiteiten. Voorbeelden van dit soort diensten zijn onder andere internettoegang, aanbieders van mobiele telefonie en hostingbedrijven voor webapplicaties.' ([Wiki09])

Zoals Jøsang en Pope ([Jøsa05]) beschrijven is het toegestaan een entiteit te koppelen aan nul of meer identiteiten binnen een gegeven domein. Het is bijvoorbeeld mogelijk dat een natuurlijk persoon zowel geregistreerd is als een werknemer van een productiebedrijf, als dat deze persoon klant is van datzelfde bedrijf. Hoewel het noodzakelijk is dat er een unieke identificator bestaat die gebruikt kan worden om de entiteit te herkennen (gedeelde identiteiten mogen niet bestaan als auditability vereist is), is het natuurlijk wel toegestaan dat een entiteit meerdere identiteiten heeft verspreid over meerdere domeinen. FIM biedt de mogelijkheid diensten te verlenen aan een enkele entiteit die meerdere identiteiten kent. Figuur 1 illustreert hoe een



Figuur 1. **De relatie tussen entiteiten (entities), identiteiten (identities) en identificators (identifiers).**

entiteit gekoppeld kan zijn aan meerdere identiteiten en hoe iedere identiteit op haar beurt opgemaakt kan zijn uit meerdere unieke of niet-unieke identificators.

Identity & Access Management

Identity and Access Management (IAM) definieert de processen en technologie voor het creëren, beheren van de levenscyclus (Engels: life cycle management), propageren (Engels: provisioning) en monitoren van digitale identiteitsgegevens teneinde conform het beleid van de organisatie toegang te verlenen tot informatie. Hermans ([Herm05]) definieert IAM als: 'Het beleid, de processen en de onderliggende technologie voor het effectief en efficiënt beheren en beheersen van wie toegang heeft tot wat binnen een organisatie'. Met andere woorden, IAM definieert wie je bent, beheerst wat je kunt doen en wat niet, en faciliteert het monitoren van compliance en audits op basis van deze informatie; alle binnen de context van het lokale beveiligingsdomein (dus de diensten die in scope zijn verklaard). Merk op dat IAM niet noodzakelijk beperkt is tot informatiesystemen. Integendeel: bijna alle IAM-oplossingen kunnen even gemakkelijk toegang beheersen tot logische als tot fysieke diensten.

Op dit moment zijn er twee overheersende IAM-modellen ([Jøsa05]):

1. *Het model van de geïsoleerde gebruikersidentiteit* (momenteel het meestgebruikte IAM-model) vereist dat iedere dienst een identificator en inlogcombinatie (gebruikersnaam en wachtwoord) hanteert voor de gebruikers van die dienst. De serviceprovider beheerst de naamgevingen binnen een lokaal beveiligingsdomein en wijst identificators toe aan gebruikers. Gebruikers zijn aan een unieke identificator gekoppeld (bijvoorbeeld het accountnummer) voor iedere logische of fysieke dienst waarvan zij gebruikmaken. Aparte inlogcombinaties worden gehanteerd voor de unieke identificators. Het voordeel van dit model is dat het een relatief eenvoudige benadering biedt tot

IAM omdat het beheer van identiteiten per serviceprovider in de meeste gevallen overzichtelijk is. Het nadeel echter is dat gebruikers zelf moeten bijhouden van welke verschillende diensten zij gebruikmaken en wat de identificators en inlogcombinaties zijn die daarbij horen.

2. *Het model van de gecentraliseerde gebruikersidentiteit* maakt gebruik van één aanbieder van identificators en de bijbehorende inlogcombinaties. Deze dienst kan vervolgens gebruikt worden door alle andere dienstverleners in het domein; ofwel als een extra aanbieder van identificators en/of inlogcombinaties, ofwel exclusief door de serviceprovider. Een uitbreiding van het model van de gecentraliseerde gebruikersidentiteit wordt bereikt door een gebruiker die door een vertrouwde serviceprovider is gecontroleerd ook voor andere serviceproviders als geauthenticeerd te beschouwen. Dit wordt gewoonlijk een Single Sign-On (SSO)-oplossing genoemd, omdat de gebruiker zich slechts eenmalig hoeft te authenticeren (één enkele inlogactie is vereist) om alle diensten te gebruiken.

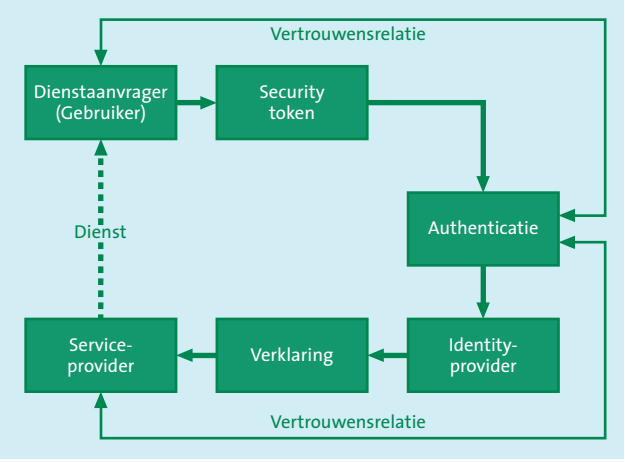
Om het gecentraliseerde model te kunnen gebruiken, is het nodig de informatie over identiteiten onderling te delen in een federatie. FIM, een optionele component in een IAM-raamwerk, maakt dat mogelijk. Federated Identity Management bestaat uit *de verzameling overeenkomsten, standaarden en technologieën die het mogelijk maken identiteitsgegevens uit te wisselen over autonome domeinen en op een veilige en beheerste wijze*. De volgende onderdelen van een FIM vallen op:

- *Overeenkomsten, standaarden en technologieën*. Alhoewel de technische voorzieningen belangrijk zijn, is FIM met nadruk afhankelijk van samenwerking op basis van vertrouwensrelaties.
- *Identiteitsgegevens*. De uitwisseling van identiteiten en inlogcombinaties staat samenwerking met partners toe, terwijl de partners 'in control' kunnen blijven ten aanzien van de autorisaties en de toegang van gebruikers tot informatie.
- *Over autonome domeinen*. Deze domeinen kunnen zich buiten de grenzen van de organisatie bevinden (externe partijen), maar zij kunnen zich ook bevinden binnen de grenzen van de organisatie (bijvoorbeeld in de keten van dienstverlening binnen de organisatie zelf). Implementatie van FIM binnen de organisatie zelf is een recente ontwikkeling die in het bijzonder van belang is binnen overheidsomgevingen (dit wordt in dit artikel verder niet uitgediept).

Federated Identity Management

In een FIM-raamwerk maken overeenkomsten tussen verschillende serviceproviders het mogelijk dat identiteiten die niet door de serviceprovider maar door afzonderlijke identiteitsverleners ofwel identityproviders worden beheerd, worden herkend over alle domeinen die onderdeel zijn van het FIM-raamwerk. Zulke overeenkomsten omvatten het beleid en de standaarden die gebruikt dienen te worden. Een identityprovider is de dienst of organisatie die verantwoordelijk is voor het vaststellen (authenticeren) van de identiteit van een gebruiker ten behoeve van zowel de lokale diensten als de diensten van externe partijen. Een serviceprovider verleent een dienst aan gebruikers en maakt daarbij gebruik van een identityprovider die, namens de serviceprovider, de authenticatie en het verzamelen van gebruikersattributen verzorgt. Hoewel autorisatie niet bij de identityprovider plaatsvindt maar bij de serviceprovider, levert de identityprovider in veel gevallen de voor autorisatie vereiste informatie die door de serviceprovider wordt gebruikt bij het wel of niet verlenen van toegang tot bepaalde informatie.

Figuur 2 toont een conceptueel overzicht van het FIM-concept. De figuur illustreert ook hoe de vertrouwensrelaties zijn opgebouwd tussen de gebruiker en de identityprovider, respectievelijk de identityprovider en de serviceprovider. FIM maakt het mogelijk dat beide vertrouwensrelaties worden getransporteerd naar een vertrouwensrelatie tussen de dienstverlener en de gebruiker. Nadat de gebruiker een bewijs van authenticiteit heeft overgelegd aan de identityprovider, bepaalt de identityprovider dat de gebruiker inderdaad geauthenticeerd is. Vervolgens wordt door de identityprovider een verklaring (Engels: assertion) afgegeven aan de serviceprovider die de informatie uit die verklaring kan gebruiken om de gebruiker verder te autoriseren. De dienst kan vervolgens verleend worden conform afspraak.



Figuur 2. **Conceptueel overzicht van het FIM-concept en de vertrouwensrelaties tussen gebruiker, identityprovider en serviceprovider.**

Aandachtsgebieden binnen een FIM-omgeving

Organisaties zetten FIM-oplossingen vandaag de dag steeds vaker in voor het op een beheerste wijze uitwisselen van informatie over autonome domeinen. Zo ook wordt steeds meer praktijkervaring opgedaan met de voor- en nadelen van FIM-

oplossingen. Op basis van deze ervaring kan een aantal 'good practices' worden onderkend. Zoals reeds aangegeven omvat een FIM-omgeving de organisatorische, procesmatige en technologische aspecten. In deze paragraaf zijn de 'good practices' per aspect inzichtelijk gemaakt.

Organisatorische kwaliteiten

Een FIM-omgeving heeft idealiter de volgende organisatorische kwaliteiten ([Compo9] [Praao4] [Autho9]):

- De eerste stap richting FIM is de *definitie van de FIM-businesscase*. Alleen als er een businesscase is gedefinieerd, zullen de belanghebbenden de mogelijke voor- en nadelen kunnen inschatten en kunnen bepalen wat de kosten zijn die zij bereid zijn te nemen om die voordelen te behalen en de risico's adequaat te beheersen. De betrokken organisaties moeten tot de conclusie komen dat het loont om samen te werken, waarna zij de obstakels één voor één in overleg moeten adresseren. Aansprakelijkheid moet duidelijk gedefinieerd zijn in overeenkomsten tussen de federatiepartners, inclusief aansprakelijkheidslimieten als gevolg van veiligheidsincidenten, fouten, etc.
- *Er moet een solide vertrouwensbasis bestaan* die wordt ondersteund door ondubbelzinnige toewijzing van rollen en verantwoordelijkheden (bijvoorbeeld in een RACI-matrix). De partijen in de federatie moeten audits toestaan van hun respectievelijke FIM-domeinen op basis van vooraf afgesproken beheersingsmaatregelen en uniforme auditprocedures. Net zoals dat bij outsourcing gebeurt, kunnen SAS 70-rapporten of Third-Party Mededelingen (TPM's) worden gebruikt om de vertrouwensrelatie te waarborgen. Eigenaarschap van processen en objecten moet duidelijk gedefinieerd zijn en door de federatiepartners worden onderschreven.
- Het is belangrijk dat er *een beveiligingsraamwerk* bestaat om de high-level beveiligingsvereisten te definiëren waar gebruikers en beheerders aan moeten voldoen. Een FIM-beveiligingsbeleid is idealiter onderdeel van het generieke (informatie) beveiligingsbeleid van de organisatie. Het beleidsdocument moet op basis van de ontwikkelingen in IT worden bijgehouden en van toepassing zijn op de federatie en de federatiepartners. Het stimuleert het verbeteren van de bekendheid met het beleid zelf (awareness) en beschrijft de vereisten voor het voldoen aan de wet- en regelgeving die van toepassing zijn binnen de federatie. Beveiligingsproblemen in de federatie kunnen de risico's van fraude, (identiteits)diefstal en interpretatiefouten doen toenemen als partijen foutieve informatie aan elkaar doorgeven en op die informatie vertrouwen.
- Problemen in het partnerschap kunnen alleen voorkomen worden als de organisaties investeren in het ondubbelzinnig vastleggen van rollen en verantwoordelijkheden in *gemeenschappelijk geaccordeerde en geaccepteerde overeenkomsten*. Dergelijke overeenkomsten bevatten afspraken die bepalen wie wat mag of moet doen, wie waarvoor betaalt en wie waarvan profiteert. Overeenkomsten moeten op zijn minst adresseren wat het bereik is van het vertrouwde domein (de overkoepelende doelstellingen, belanghebbenden, procesvereisten per partner), wat de expliciete overeenkomsten zijn voor auditing en op welke wijze de afspraken gewijzigd kunnen worden (meta-overeenkomsten).
- De FIM-omgeving moet voldoen aan de relevante *in- en externe privacywet- en regelgeving*. Idealiter ligt de controle over het gebruik van eigen gegevens bij de gebruiker zelf.
- *Toewijding van het management moet waarborgen dat de beveiliging van FIM adequaat wordt geadresseerd* in het FIM-businessplan en dat overeenstemming wordt bereikt over de toewijzingen van taken en verantwoordelijkheden in FIM-beveiliging. Dit geldt voor de organisatorische, procesmatige en technologische beheersingsmaatregelen en de wijze waarop FIM-beveiligingsinitiatieven worden ondersteund.

Procesmatige kwaliteiten

Een FIM-omgeving heeft idealiter de volgende procesmatige kwaliteiten ([Praao4]):

- Gebruikers moeten *uniek identificeerbaar* zijn binnen de federatie om auditability van gebruikersactiviteit te kunnen waarborgen. De levenscyclus van de gebruiker moet conform afgesproken tijdigheid in de identity repository worden gereflecteerd, inclusief het deactiveren of verwijderen van identificators als een gebruiker definitief of tijdelijk uit dienst gaat.
- Adequate maatregelen moeten waarborgen dat *de sterkte van authenticatie* binnen de federatie geïmplementeerd is conform de afspraken die daarover bestaan; alle partners hanteren een equivalent wachtwoordbeleid dat ten minste het volgende omvat: wachtwoordcomplexiteit en update regels, lockout na herhaaldelijk foutief inloggen en beveiligde opslag van wachtwoorden. Gemeenschappelijke overeenkomsten moeten bestaan zodat ondubbelzinnige classificatie van authenticatievereisten en -maatregelen wordt bereikt, inclusief de diensten die mogen worden verleend op basis van een bepaald authenticatieniveau van de gebruiker. Auditing van de authenticatiemiddelen moet zodanig frequent plaatsvinden dat technologische ontwikkelingen worden gereflecteerd in de sterkte van de gebruikte middelen. Audits moeten ten minste gericht zijn op het productieproces, de aanvraagprocedure, het uitgifteproces en het beheer van de authenticatiemiddelen die de partners gebruiken.

FIM maakt een vertrouwensrelatie tussen de dienstverlener en de gebruiker mogelijk

- De functionaris die verantwoordelijk is voor het aanmaken, wijzigen en intrekken van autorisaties moet alle autorisaties documenteren die direct of indirect (bijvoorbeeld via rollen) aan gebruikers zijn toegewezen in een autorisatiematrix of vergelijkbare administratie. Procedures moeten bestaan om de administratieve processen rondom het aanmaken, wijzigen en verwijderen van autorisaties te beheersen inclusief vereiste accordering. *De autorisatiematrix (SOLL) moet periodiek worden vergeleken met de werkelijke autorisaties (IST)* in een representatieve steekproef van de beschikbare diensten. Het resultaat daarvan dient periodiek door het hogere management te worden geaccordeerd.
- Op basis van een risicoanalyse moeten *gevoelige wijzigingen in de identificatie- en authenticatiegegevens worden gemonitord en opgeslagen* (bijvoorbeeld het aanmaken, uitlezen, wijzigen of verwijderen van gebruikers met bijzondere rechten). De monitoringinstellingen moeten periodiek gecontroleerd worden door het management van de informatiebeveiligingsafdeling. Monitoringrapportages moeten op een beveiligde locatie worden opgeslagen welke het onmogelijk maakt voor ongeautoriseerde gebruikers om deze rapportages aan te passen. Verantwoordelijkheden moeten zijn toegewezen voor het controleren van monitoringalarmsignalen en -rapportages, en voor het nemen van adequate actie in geval aan de daarvoor gedefinieerde condities wordt voldaan (als bijvoorbeeld sprake is van een daadwerkelijke inbraak).
- In federaties hebben de partners relatief veel controle over de verleende toegang tot de objecten van de auditee. Wegens de belangrijke functie van monitoring en audit bij het bereiken en handhaven van de wederzijdse vertrouwensrelatie, die voor een goed functionerende federatie vereist is, moeten er periodiek *onafhankelijke audits* plaatsvinden. Deze audits moeten worden uitgevoerd conform de daarover door middel van de FIM-overeenkomst gemaakte afspraken. Auditing biedt de mogelijkheid voor federatiepartners om de kwaliteit te controleren van de toegangsprocessen van hun gelijken. Dit is essentieel voor het bereiken van het vertrouwen dat de partners hun medewerking verlenen aan dergelijke audits. De IT-auditor dient bij het beoordelen van de federatie rekening te houden met de (on)volwassenheid van de federatiepartners en eventuele compenserende maatregelen.
- *Adequate functiescheiding (Engels: Segregation of Duties, SoD) moet bestaan* om te voorkomen dat gebruikers waarde aan de organisatie kunnen onttrekken zonder dat dit wordt opgemerkt. Op basis van een risicoanalyse moet worden voorkomen dat bijzondere rechten als gevolg van onbedoelde combinaties in de verdeling van rechten een beveiligingsrisico opleveren. De functionaris die verantwoordelijk is voor het aanmaken, wijzigen en intrekken van autorisaties mag niet in staat zijn aanpassingen te doen zonder dat het management daarvan voor- of achteraf op de hoogte wordt gesteld.

Technologische kwaliteiten

Een FIM-omgeving heeft idealiter de volgende technologische kwaliteiten ([Kuip08] [Blak08] [Davi07] [Ping09]):

- Een federatie zou moeten bestaan uit partijen die zo *los mogelijk verbonden* zijn (Engels: loosely coupled): actueel decentraal beheer van identiteiten verdient de voorkeur boven gedeelde verouderde identity repositories. Het gebruik van gemeenschappelijk afgesproken technologie is cruciaal voor het bereiken van FIM, maar de uitwisselbaarheid van de door de IAM-tooling geboden functionaliteit is dat evenzeer.
- Omdat standaardisatie van technologie essentieel is voor federaties, moet de auditee continu de *laatst beschikbare technologische standaarden* blijven overwegen, zoals SAML 2.0 (identiteitsattributen), XACML (interpretatie van uitgewisselde (SAML-) gegevens), SPML (uitwisseling van gebruiker, object en service-provisioninginformatie) en SOAP (transport van op XML gebaseerde berichten). Hoewel het voorbereid zijn op meerdere standaarden de interoperabiliteit van een organisatie zal vergroten, zullen de kosten en complexiteit waarschijnlijk ook toenemen.
- Er moet een *technische federatieovereenkomst* gehanteerd worden, waarin ten minste het volgende is gedefinieerd: gebruik, opslag en definitie van identiteitsattributen, de gebruikte risiconiveaus, sterkte van authenticatie en toegestane identityproviders per dienst, het verwerken van autorisaties door de serviceprovider (bijvoorbeeld individuele versus functionele accounts), vereisten aan de veiligheid van opgeslagen, verwerkte of verzonden gegevens, de te gebruiken standaarden en de vereisten aan certificering van alle partners (bijvoorbeeld het gebruik van PKI of een vergelijkbaar mechanisme voor veilige communicatie).

Onafhankelijke audits bieden de federatiepartners de mogelijkheid om de kwaliteit te controleren van de toegangsprocessen van hun gelijken

- Er moet een *gemeenschappelijk change-managementbeleid inzake FIM* worden gebruikt door alle partners in de federatie, waarin ten minste het volgende wordt geadresseerd: de documentatie, autorisatie en uitvoering van (nood)wijzigingen, het proces van testen en aftekenen inclusief testdocumentatie en het scheiden van ontwikkel-, test-, acceptatie- en productieomgevingen inclusief eventuele uitzonderingsprocedures voor directe wijzigingen in de productieomgeving.

• Er moet *een definitie zijn van voor de federatie gekozen topologie*. Mogelijke federatietopologieën zijn: point-to-point (ofwel: 'één-op-één'), mesh (ofwel: 'verbonden'), star (ofwel: 'as en spaak') en gecentraliseerd. Hoewel partnerships in een federatie gewoonlijk niet op een hiërarchische wijze zijn opgebouwd, is een verzameling van federaties (een *con*federatie) dat vaak wel.

FIM is gebaseerd op gedeeld vertrouwen, niet noodzakelijkerwijs op gedeelde technologieën

• Er moet *een definitie zijn van de voor de federatie gekozen implementatie*. Mogelijke implementatieopties zijn: proprietary (het ontwikkelen van een eigen oplossing), open source, een op standaarden gebaseerde federatieserver of uitbreiding van een bestaande IAM-suite.

FIM is gebaseerd op gedeeld vertrouwen, niet noodzakelijkerwijs op gedeelde technologieën. De FIM-technologieën hebben een *ondersteunende* functie ten opzichte van de vertrouwensrelatie in de federatie.

Conclusies en slotnotitie

Dit artikel laat zien dat het concept van FIM een waardevolle oplossing kan bieden voor een scala aan uitdagingen voor moderne organisaties die op een beheerste wijze informatie willen delen met externe partners buiten hun beveiligingsdomein. De volgende conclusies kunnen worden getrokken uit het in dit artikel gepresenteerde onderzoek.

De stand van zaken

Wat betekent FIM voor moderne organisaties? Wordt het gebruikt? Hoe?

Het concept van FIM heeft op dit moment een behoorlijk definitief stadium bereikt en het samensmelten van standaarden heeft met SAML 2.0 plaatsgevonden. De businesscase voor federatie wordt in toenemende mate gebaseerd op gebruikersgemak, efficiency en effectiviteit, doordat de externe processen van organisaties duidelijk ondersteund worden door deelname aan een federatie.

Voorbeelden van FIM-implementaties zijn momenteel gemakkelijker te vinden in de onderwijs- en overheidsomgevingen dan in de commerciële bedrijfsmatige omgeving. Volwassenheid zou een voorwaarde kunnen worden als de organisaties betrokken zijn in fusies en overnames; niet alleen de volwassenheid van FIM zal in dat geval een rol spelen, ook de algemene IAM-volwassenheid van de andere partijen.

De meeste auditkantoren bemerken een langzame toename van FIM-gerelateerde opdrachten in het internationale speelveld. Het nadeel van de eerste oplossingen voor logische identificatie was vaak dat de hele 'portemonnee' moest worden gepresenteerd, waardoor de serviceprovider irrelevante attributen moest verwerken en de gebruiker zich onnodig gedwongen zag persoonlijke informatie kenbaar te maken. FIM biedt hier in potentie oplossingen voor. Het IAM-onderzoek dat in 2008 door KPMG is uitgevoerd, vermeldt ([KPMG08]): 'In de meeste organisaties van de respondenten zijn IAM-projecten gericht op het beheer en beheersen van toegang door werknemers en externen tot interne systemen en informatie. Federated Identity Management, de grensoverschrijdende verbinding van IAM-omgevingen, wordt in de meerderheid van de organisaties van respondenten nog niet in brede zin gebruikt.'

In tegenstelling tot de meeste bedrijven is de overheid een organisatie die bestaat uit een groot aantal redelijk autonome suborganisaties. De IT-omgevingen van de overheid bevatten tegelijkertijd een groot aantal legacy systemen en state-of-the-arttechnologie zoals webportals op het intranet en, in toenemende mate, ook op het internet. De overheid ziet in dat er een behoefte zal bestaan aan samenwerking via FIM als de decentrale IAM-initiatieven volwassen zijn geworden.

Auditaandachtspunten

Wat zijn de belangrijkste aandachtspunten voor de IT-auditor en auditee in FIM-gerelateerde audits?

De belangrijkste aandachtspunten voor de IT-auditor en auditee betrokken bij FIM-audits zijn afgeleid van de eerder beschreven good practices rondom FIM. De aandachtspunten kunnen gegroepeerd worden in clusters die betrekking hebben op de organisatie, processen en technologie van een organisatie.

De belangrijkste FIM-auditaandachtspunten voor een beoordeling van de *organisatie* hebben te maken met de vertrouwensrelatie en het gegeven dat deze door een heldere businesscase moet worden ondersteund, met de wederzijds aangenomen en gehandhaafde beveiligingsraamwerken en met de toewijzing van verantwoordelijkheden en betrokkenheid van het management. FIM-overeenkomsten moeten bestaan en compliance met de relevante in- en externe wet- en regelgevingen moet worden bewaakt (bijvoorbeeld door de eindgebruiker de controle te laten voeren over eigen gegevens). Commitment van het management zorgt ervoor dat de beveiliging van FIM voldoende wordt geadresseerd.

De belangrijkste FIM-auditaandachtspunten voor een beoordeling van de *processen* hebben te maken met de unieke identificatie van gebruikers en de eenduidige implementatie van de authenticatie- en autorisatieprocessen. Auditen van de authenticatiemiddelen en IST/SOLL-vergelijkingen moeten op voldoende regelmatige basis plaatsvinden en worden opgevolgd. Wijzigingen in de identificatie en authenticatiegegevens moeten worden gemonitord en adequate functiescheiding moet van kracht zijn.

De belangrijkste FIM-auditaandachtspunten voor een beoordeling van de *technologie* hebben te maken met het los verbinden van federatiepartners (loose coupling) en het gebruik van passende technologische standaarden. Een technische federatieovereenkomst moet bestaan, evenals een change-managementbeleid inzake FIM en een definitie van de federatietopologie en de gekozen aanpak voor implementatie.

FIM-gerelateerde audits moeten, zo nodig periodiek, plaatsvinden op basis van een vooraf gedefinieerde frequentie. Auditinspanningen moeten altijd worden ontplooid op basis van een risicoanalyse om de juiste inzet van middelen te bepalen.

De belangrijkste kwaliteiten van een FIM-raamwerk

Dit artikel biedt een praktisch high-level handvat voor zowel de organisaties die hun FIM-raamwerken geaudit weten als de IT-auditors die een dergelijke audit uitvoeren.

Een goed FIM-ontwerp en een goede FIM-implementatie kunnen door de auditee worden bereikt door de hier volgende kwaliteiten te waarborgen. Overeenkomstig hiermee zou een IT-auditor de volgende belangrijkste aandachtspunten in een FIM-audit moeten betrekken om tot een gedegen audit te komen.

- Een FIM-omgeving heeft idealiter de volgende *organisatorische kwaliteiten:*
  - De FIM-businesscase is helder gedefinieerd voorafgaand aan implementatie.
  - Er bestaat een solide vertrouwensrelatie tussen de federatiepartners.
  - Er is een beveiligingsraamwerk van kracht om de high-level vereisten aan beveiliging te beheersen.
  - De federatiepartners hebben op ondubbelzinnige wijze de vereiste rollen en verantwoordelijkheden vastgelegd in wederzijds geaccordeerde en aangenomen overeenkomsten.
  - De auditee voldoet aan de relevante in- en externe (privacy) wet- en regelgeving. Idealiter heeft de gebruiker zelf de controle over de informatie die over hem of haar wordt gebruikt.
  - Betrokkenheid van het management waarborgt een adequate aanpak voor FIM-beveiliging.
- Een FIM-omgeving heeft idealiter de volgende *procesmatige kwaliteiten:*
  - Gebruikers zijn overal in de federatie altijd uniek identificeerbaar.
  - Sterkte van authenticatie is op eenduidige wijze geïmplementeerd in de federatie.
  - De autorisatiematrix (SOLL) wordt periodiek vergeleken met de werkelijke autorisaties (IST).
  - Wijzigingen in gevoelige identificatie- en authenticatiegegevens worden gemonitord en opgeslagen.
  - Er vinden periodieke onafhankelijke audits plaats.
  - Er bestaat adequate functiescheiding.
- Een FIM-omgeving heeft idealiter de volgende *technologische kwaliteiten:*
  - De federatie bestaat uit partijen die zo los mogelijk verbonden zijn (loose coupling).
  - De laatst beschikbare technologische standaarden worden gebruikt.
  - Een technische federatieovereenkomst wordt gehanteerd.
  - Er is een gemeenschappelijk change-managementbeleid inzake FIM aangenomen door de federatiepartners.
  - De federatietopologie is gedefinieerd.
  - De gekozen federatie-implementatie is gedefinieerd.

Idealiter heeft de gebruiker zelf de controle over de informatie die over hem of haar wordt gebruikt

Merk op dat zowel het adresseren van de belangrijkste kwaliteiten door de auditee als de beoordeling daarvan door de IT-auditor zou moeten plaatsvinden op basis van een voorafgaande risicoanalyse en een afweging van de voor- en nadelen van de kwaliteiten.

Slotnotitie

Hoewel FIM slechts gericht is op een beperkt onderdeel van de complete uitdaging, namelijk de uitwisseling van identiteitsgegevens tussen autonome domeinen, zijn de mogelijkheden op zijn minst veelbelovend te noemen. Echter, voordat organisaties FIM gaan implementeren zouden zij de in dit artikel genoemde belangrijkste kwaliteiten in ogenschouw moeten nemen. Hierbij kunnen de hier gepresenteerde high-level handvatten worden uitgewerkt naar de specifieke situatie van de auditee; concepten zoals 'voldoende frequent' worden dan vertaald naar een concrete meetbare indicator.

Literatuur

[Auth09] http://www.authenticationworld.com/Authentication-Federation/CreatingAFederatedAuthenticationTrust.pdf (laatst bezocht september 2009).

[Blak08] Bob Blakley, Dan Blum en Gerry Gebel, *Federated Identity – Reference Architecture Technical Position*, Burton Group, 2008.

[Comp09] http://www.computerworld.com.au/index.php/id;162794021;fp;2;fpid;2 (laatst bezocht september 2009).

[Davi07] Claire Davies en Matt Shreeve, *Federated access management: international aspects*, Curtis+Cartwright Consulting Limited, 7 juni 2007.

[Herm05] Ing. J.A.M. Hermans RE en drs. J. ter Hart, *Identity & Access Management: operational excellence of 'in control'?*, Compact 2005/3.

[Jøsa05] A. Jøsang en S. Pope, *User-Centric Identity Management*, Proceedings of AusCERT mei 2005, Brisbane, Australia.

[KPMG08] KPMG, *2008 European Identity & Access Management Survey*, KPMG, 2008.

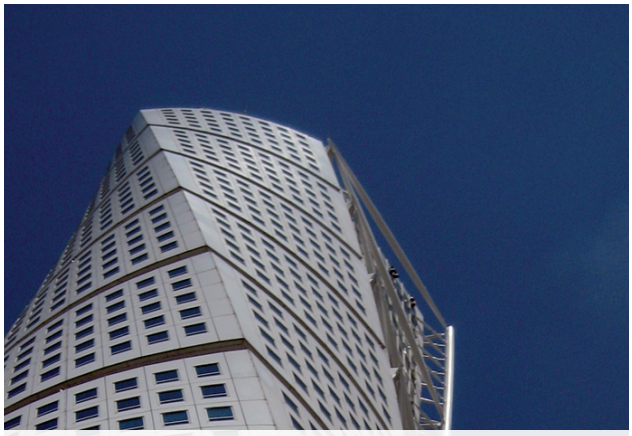
[Kuip08] Jaap Kuipers, *eID Convergence challenges* (slide 8), SURFnet/ECP.NL, 2008.

[Norl02] Eric Norlin en Andre Durand, *Federated Identity Management*, Whitepaper, PingID Network, 2002.

[Ping09] http://www.pingidentity.com/information-library/Federated-Identity-Management-Tutorial.cfm (laatst bezocht september 2009).

[Praa04] Jan van Praat en Hans Suerink, *Inleiding EDP-auditing*, Ten Hagen & Stam uitgevers, 2004.

[Wiki09] http://en.wikipedia.org/wiki/Service_provider (laatst bezocht september 2009).



Onlinebronnen

Ten slotte wordt hier een aantal websites opgesomd die aanknopingspunten vormen voor vervolgonderzoek en praktische toepassing van de theoretische concepten uit dit artikel:

http://openid.net/what/ – Deze website presenteert het OpenID-concept dat besproken wordt in dit artikel en dat een lezer een eerste aanraking biedt met de mogelijke voordelen van deze techniek.

http://www.inames.net/ – Deze website presenteert het i-name-concept van identificators die voor mensen gemakkelijk te onthouden zijn. Ze zijn ontworpen om het probleem van permanente adressering op te lossen; hoe kan een onlineadres worden gecreëerd dat niet onderhouden hoeft te worden en dat nooit verandert ongeacht hoe vaak de contactgegevens van de eigenaar veranderen.

http://identity20.com/media/OSCON2005/ – Dick Hardt's OSCON 2005 Keynote getiteld *Identity 2.0*: dit is een inspirerende en dynamische introductie van Identity 2.0 en laat zien hoe het concept van digitale identiteiten zich aan het ontwikkelen is.

http://www.identityblog.com/?p=352 – Kim Cameron's whitepaper getiteld *The Laws of Identity*: een verzameling 'wetten' die zouden moeten gelden voor de personen die werken met identiteiten. Door deze wetten te respecteren, zo beargumenteert Cameron, is het mogelijk een verenigd systeem te creëren dat universeel geaccepteerd wordt en duurzaam is.