GvIB Expert Brief – Maart 2007

ISSN 1872-4876, Jaargang 3 – Nr. 1

Maart 2007

Single Sign-On voor Organisaties

Ernst Lopes Cardozo

Egbert Dijkgraaf

Lex Dunn

Rob Greuter

Edwin Haaring

Ernst Mellink

Eddie Michiels

Peter Rietveld

Rob van der Staaij

Gerard Zwiers

Single Sign-On (SSO) voor Organisaties, ook wel Enterprise Single Sign-On (ESSO) genoemd, wordt vaak voorgesteld als een concreet systeem met specifieke eigenschappen zoals centrale registratie en administratie van identiteiten en hun attributen. Er zijn echter zeer verschillende constructies die weinig meer gemeen hebben dan dat gebruikers meestal niet opnieuw hoeven in te loggen als ze van applicatie wisselen. Hier beschouwen we SSO daarom als een eigenschap van sterk verschillende architecturen. Dat heeft consequenties voor de argumenten die een rol spelen in de businesscase. We beperken ons tot de "enterprise", waarbij de gebruikers een formele relatie met de organisatie hebben, bijvoorbeeld als medewerker, student of patiënt. In een dergelijke omgeving is het wenselijk én acceptabel dat gebruikers één unieke (digitale) identiteit gebruiken voor alle applicaties. Welk type SSO is voor uw organisatie geschikt, welke argumenten komen er in uw businesscase en wat komt er bij de invoering allemaal kijken?

http://www.gvib.nl/

✉ expertbrief@gvib.nl

http://www.ibpedia.nl/

2

INLEIDING

Het begon allemaal eenvoudig. De eerste computer stond bij de boekhouder en vrijwel niemand wist hoe je hem moest gebruiken. De beveiliging was beperkt tot fysieke beveiliging. Een decennium later stond er een mainframe met terminals en een groot aantal applicaties. Daarop moest de gebruiker inloggen, zich identificeren met zijn naam of personeelsnummer (inlogcode) en authenticeren met een wachtwoord. Zo lang de sessie duurde kon de gebruiker van applicatie wisselen zonder opnieuw in te loggen. Het mainframe kende één bestand met gebruikers en hun wachtwoorden. Al snel werden daar gegevens aan toegevoegd: welke applicaties zijn toegankelijk voor deze gebruiker? Alles geregeld.

Daarna kwamen de minicomputers, de PCs en de netwerken. Gebruikers moesten eerst op hun PC of het netwerk inloggen en als ze dan verbinding maakten met een applicatie op minicomputer of mainframe, moesten ze opnieuw inloggen, meestal met telkens een andere inlogcode en een ander wachtwoord . Er waren en zijn organisaties waar de gebruikers tientallen inlogcodes met bijbehorende wachtwoorden hebben. Elk systeem stelt eigen eisen aan de inlogcodes en wachtwoorden. Sommige wachtwoorden moeten elke twee maanden worden veranderd, andere elke drie maanden. Geen wonder dat deze gebruikers een lijst onder handbereik houden met hun inlogcodes en wachtwoorden. Bijzonder lastig wordt het voor ambulante werkers, zoals in ziekenhuizen en aan balies van gemeenten, die voortdurend van plaats en dus van terminal wisselen en waarvoor de wet- en regelgeving individuele identificatie vereisen. En dus zijn deze organisaties op zoek naar een systeem waarin er maar één keer, of in ieder geval veel minder vaak moet worden ingelogd.

Die verschillende inlogcodes en wachtwoorden leveren een aantal grote problemen op:

- Tijdrovend, irriterend en demotiverend voor gebruikers;
- Belastend voor de helpdesk: vergeten wachtwoorden kunnen een substantieel deel uitmaken van het werk van de helpdesk;
- Onveilig: gebruikers zijn niet in staat grote aantallen wachtwoorden te onthouden en schrijven ze dus op, met alle mogelijke gevolgen van dien;
- Onveilig: sterke wachtwoorden en snel wisselende wachtwoorden zijn moeilijk te onthouden. Gebruikers en organisatie bieden weerstand aan pogingen om de kwaliteit van de wachtwoorden te verbeteren. Geavanceerde middelen als eenmalige wachtwoorden en smartcards worden nog minder geaccepteerd wanneer ze tientallen malen per dag moeten worden gebruikt en zijn moeilijk te implementeren zonder centralisatie van identificatie en authenticatie.

Daarnaast zijn er nadelen die niet direct samenhangen met het herhaald inloggen, maar wel het gevolg zijn van het achterliggende probleem, de ongecoördineerde identiteitstabellen:

- Het onderhouden van de afzonderlijke identiteitstabellen in alle systemen kost veel extra mankracht;
- Het is moeilijk een nieuwe gebruiker tijdig in alle systemen in te voeren of een vertrokken gebruiker tijdig overal te blokkeren;
- Het is moeilijk functiescheiding toe te passen, doordat er geen overzicht is over rechten die een persoon in de verschillende systemen heeft;
- Het controleren (auditen) van de afzonderlijke identiteitstabellen is tijdrovend en daardoor kostbaar. Bovendien levert het geen inzicht in de combinatie van rechten van personen;
- Als systemen gebruik moeten maken van elkaars gegevens, is het niet mogelijk de inlogcode van de gebruiker van het eerste systeem door te geven aan het geraadpleegde systeem om zo te verzekeren dat de toegangsrechten van de eindgebruiker worden gerespecteerd. Dit leidt gemakkelijk tot compromitteren van vertrouwelijke informatie en maakt dat het transactieverslag van het tweede systeem niet kan aangeven wie de eindgebruiker was;
- Bovenstaande punten krijgen extra gewicht binnen een organisatie die gebonden is aan wettelijke voorschriften als VIR (Voorschrift Informatiebeveiliging Rijksoverheid), Basel II (financiële sector), NEN 7510 (Nederlandse norm voor zorgverleners), SOX (Ondernemingen die aan een van de Amerikaanse beurzen zijn genoteerd), etc;
- Zonder enkelvoudige gebruikersidentiteit is het moeilijk gebruikersspecifieke instellingen (bv. taal) voor alle applicaties te laten gelden;
- Het signaleren van afwijkend gedrag is moeilijk wanneer dat over veel systemen moet gebeuren en er geen punt is waar alle inlogpogingen kunnen worden gevolgd.

Al deze problemen zijn evenzoveel argumenten voor SSO. Toch heeft de oude situatie naast deze ernstige nadelen ook enkele voordelen:

- Risicospreiding:
  - als een gebruikersnaam en wachtwoord, of een hele identiteitstabel worden gecompromitteerd, blijft de schade beperkt tot het betreffende systeem.
- Flexibiliteit:
  - nieuwe systemen (bv. uit een fusie of overname) kunnen direct worden ingezet, zonder dat identificatie, authenticatie en autorisatie moeten worden geïntegreerd met de bestaande omgeving;
  - differentiatie van beveiligingsniveau voor verschillende applicaties is eenvoudig te realiseren.
- Beschikbaarheid:
  - de systemen en applicaties zijn niet afhankelijk van centrale faciliteiten.

Daarnaast zijn er nog generieke overwegingen die tegen SSO kunnen worden aangevoerd:

- SSO producten en hun invoering kosten geld, tijd en aandacht;
- Eén authenticatiesysteem kan betekenen dat de organisatie afhankelijk is van één leverancier;
- Een SSO project raakt de automatisering en de processen van de hele organisatie.

Hoewel de nadelen doorgaans niet opwegen tegen de voordelen, zijn het wel aandachtspunten voor elk SSO project.

4

DEFINITIES EN SCOPE

Helaas is de terminologie rond het thema SSO nog niet gestandaardiseerd. Je kunt in dit verband de volgende termen tegen komen:

Single Sign-On (SSO)	De eigenschap van een systeem of infrastructuur waarbij de gebruikers nooit meer dan één keer per sessie hoeven in te loggen.
Reduced Sign-On (RSO)	De eigenschap van een systeem of infrastructuur waarbij het aantal inlogmomenten sterk verminderd is. De reden voor hernieuwd inloggen kan technisch zijn (incompatibiliteit tussen systemen) of logisch (scheiding van identiteitstabellen om reden van beveiliging).
Enterprise Single Sign-On (ESSO) of Reduced Enterprise Sign-On (RESO)	Het element “Enterprise” kan er op duiden dat het systeem ook of vooral geschikt is voor omgevingen met ‘legacy’ applicaties (minicomputers, mainframes, terminalsessies). “Enterprise” kan er ook op duiden dat het vooral bedoeld is voor gesloten omgevingen, in tegenstelling tot bv. op Internet georiënteerde systemen.
Web Single Sign-On (WebSSO)	Identificatie en authenticatie voor systemen die gebruik maken van webbrowsers en het http- of https-protocol, zowel in een intranet als op het openbare Internet.

Scope

Deze Expert Brief richt zich op Single Sign-on binnen organisaties, waarbij er dus enige mate van controle is over beleid, applicaties en de technische infrastructuur. “Enige mate van”, want in grote organisaties werken er zo veel krachten dat het vaak illusoir is te denken dat de hele organisaties zich aan één set regels kan houden. Zo worden multinationale organisaties geconfronteerd met tegenstrijdige wet- en regelgeving. Fusies en overnames brengen afwijkende systemen en applicaties samen, zodat een homogene infrastructuur moeilijk is te realiseren en handhaven. Het is dan ook niet ongebruikelijk om zowel Windows clients en servers als webbased, terminalbased ERP en Unix applicaties binnen één enterprise te vinden, samen met diverse directories van bv. Microsoft, Oracle en Novell.

SSO kan moeilijk los gezien worden van de noodzaak voor sterke identificatie en authenticatie. Onze scope sluit echter de problematiek van identificatie en authenticatie van het grote publiek uit, met zijn specifieke aspecten als schaal, privacy en het gebrek aan standaardisatie en controle over de werkstations.

FEATURE

Welke smaak men ook kiest, belangrijk is dat SSO geen “systeem” is, maar een *eigenschap van een systeem*; dit ondanks het feit dat er onder de noemer SSO (en aanverwante termen) heel wat producten worden aangeboden. Bij nadere beschouwing blijken er diverse, onderling sterk verschillende configuraties te zijn die de eigenschap SSO in meer of mindere mate vertonen. De aangeboden producten hebben dan ook heel verschillende architecturen. Sommige schermen de gebruikers af van de diversiteit van de achterliggende applicaties, zodat de gebruiker ervaart dat hij veel minder vaak moet inloggen, zonder dat er achter schermen veel is veranderd - de applicaties werken elk nog met hun eigen identiteiten, wachtwoorden en autorisaties. Maar er zijn ook producten die centraal Identity en Access Management (IAM) implementeren, met SSO als één van de resultaten. In het hoofdstuk ARCHITECTUREN gaan we verder in op de verschillende architecturen die de eigenschap

SSO hebben, maar eerst maken we een uitstapje naar een (vooralsnog utopische) IAM architectuur.

BV Utopia

Utopia is een grote, geografisch verspreide organisatie, bijvoorbeeld een cluster gefuseerde ziekenhuizen. Wet- en regelgeving dwingen deze organisatie om de toegang tot patiëntgegevens strikt te regelen, maar er zijn daarnaast nog talloze andere digitale verzamelingen waarvoor steeds andere toegangsregels gelden, van volledig openbaar tot alleen toegankelijk onder specifieke omstandigheden.

De organisatie beschikt over verschillende identiteitstabellen (directories), databases gevuld met digitale identiteiten van medewerkers, patiënten, stagiaires, etc.. Om de Identity Management-processen slagvaardig te houden, zijn deze per vestiging en soms per afdeling ingericht. De systemen en applicaties waarvoor toegangsbeheer nodig is, zijn allemaal zo ingericht dat ze identiteiten en hun attributen van elk van de directories van de organisatie kunnen accepteren. Op basis van de attributen, waaronder de rollen die aan een identiteit zijn toebedeeld, kunnen de applicaties gedifferentieerd toegang geven tot informatie en functies. Daarmee zijn ze ook in staat alle transacties te loggen met de identiteit van de gebruiker. Dat geldt ook voor de applicaties die niet rechtstreeks worden benaderd maar diensten aan andere applicaties leveren: de identiteit van de eindgebruiker wordt bij elk verzoek doorgegeven en bepaald mede welke informatie en functies beschikbaar zijn.

Voor het zo ver is, moet de gebruiker zich echter identificeren en authenticeren. Zijn identificatie, bestaande uit gebruikersnaam plus directory (bv. piet.derksen@neurologie) geeft het authenticatiesysteem toegang tot de authenticatie-attributen (bv. wachtwoord) in het record van Piet Derksen. Daarmee worden de door de gebruiker ingevoerde authenticatie-gegevens gevalideerd. Bij succes wordt er een “visum” afgegeven, een sessiecertificaat waarmee de (terminal van) de gebruiker zich automatisch bij alle applicaties kan identificeren en authenticeren.

Het sessiecertificaat bevat naast de identiteit van de gebruiker ook zijn “rollen”, die door de applicaties worden gebruikt om te bepalen tot welke informatie en functies hij toegang heeft. Bovendien vertelt het sessiecertificaat op welk kwaliteitsniveau de gebruiker zich heeft geauthenticeerd (eenvoudig wachtwoord of smartcard?), wat de applicaties in staat stelt om te bepalen welke informatie en functies er onder die omstandigheden toegankelijk mogen worden gemaakt. De gebruiker hoeft meestal maar één maal in te loggen, tenzij hij op een applicatie stuit die een hogere kwaliteit authenticatie vereist. In dat geval zal hem om een extra authenticatie worden gevraagd. Zo zal een arts misschien met een eenvoudig wachtwoord toegang tot zijn agenda krijgen, maar een authenticatie op basis van twee elementen (bijvoorbeeld smartcard plus pincode) moeten gebruiken om de medicatie van een patiënt te veranderen.

Identity Management

SSO is dus een eigenschap van een Identity Management (IDM of IdM) systeem of systemen. Binnen één enkele organisatie is het wenselijk dat elke persoon één identiteit heeft, gebaseerd op zijn relatie met de organisatie, zodat al zijn activiteiten in zowel de fysieke als de digitale wereld tot hem zijn terug te voeren. Dat is een belangrijk verschil met de wereld van het

openbare Internet, waar één persoon heel verschillende relaties heeft met de diverse partijen (bank, dokter, gemeente, belastingen, verzekeringen, winkel, etc.). Op Internet wil niemand dat die partijen door het combineren van gegevens een volledig profiel van iemand kunnen maken; binnen de relatie met onze werkgever is dat geen probleem, al kunnen er uitzonderingen zijn, bv. voor de ondernemingsraad.

Binnen een organisatie houdt Identity Management in: het creëren van identiteiten en hun attributen, het onderhouden van deze gegevens, het gebruik van identiteiten en de controle op en verslaglegging van deze processen. Identiteiten worden gebruikt om conform het beleid en achteraf traceerbaar toegang te geven tot fysieke of digitale objecten. Identiteiten worden dus ook gebruikt om vast te leggen wie wanneer wat en waarmee heeft gedaan. Voor digitale objecten kan dat zowel voor het inzien als het muteren van het object gelden. Het verslag wordt soms alleen in een los transactieverslag geschreven, maar steeds vaker als historie in het object zelf opgeslagen.

Om niet bij elke applicatie een volledige lijst van alle identiteiten en hun autorisaties te moeten onderhouden, worden in de identiteit “rollen” opgenomen en aan de applicaties gecommuniceerd. Die kennen aan de (hopelijk beperkte verzameling) rollen autorisaties toe. Deze constructie wordt Role Based Access Control (RBAC) genoemd.

Aangezien traceerbaarheid en toegangsbeheer de twee doelen van de activiteit Identity Managent zijn, wordt vaak de term Identity and Acces Management gebruikt (IAM). Daartoe worden ook gerekend de processen waarmee de autorisatietabellen van de applicaties worden beheerd. Ook daarvoor geldt: aanmaken, muteren, controleren en verslagleggen. Zie ook de Handreiking Identiteitenbeheer, te vinden op de www.gvib.nl.

Federatie

Federated Identity Management wordt doorgaans beschreven als de mogelijkheid dat een gebruiker met één naam en wachtwoord met applicaties van verschillende organisaties kan werken. Vanuit de organisatie gezien is dit ook te beschrijven als: applicaties die gebruikers toelaten die in verschillende directories zijn geregistreerd. Soms zijn de directories eigendom van ongerelateerde organisaties, bijvoorbeeld partners in een logistieke keten, soms zijn het dochters binnen één holding of onderdelen van dezelfde onderneming. Niet zelden is die situatie ontstaan door een fusie.

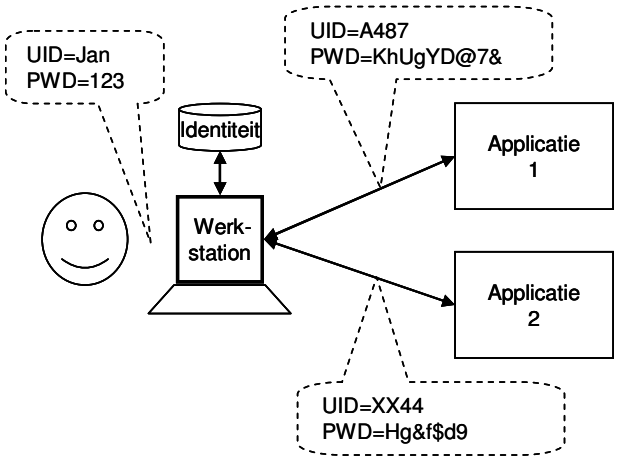
Centrale gedachte is dat elke gebruiker in één directory is geregistreerd, dus ook maar één identiteit heeft. De gebruiker authenticeert zich bij zijn eigen directory. De applicaties moeten de verschillende directories vertrouwen. Voor RBAC moeten afspraken over te hanteren rollen worden gemaakt, variërend van een rol ‘A-gast’ die binnen B-applicaties bepaalde rechten krijgen, tot nagenoeg volledige synchronisatie van alle rollen in een gefuseerde organisatie. Het fuseren van de directories zelf kan op praktische bezwaren stuiten, zoals de kosten van nieuwe tokens, de impact op de organisatie of verschil in wettelijke mogelijkheden in verschillende landen.

ARCHITECTUREN

De producten, applicaties en systemen die in meer of mindere mate Single Sign-on realiseren, kunnen op grond van hun architectuur in vijf hoofdgroepen worden verdeeld. In dit hoofdstuk beschrijven we elk van die architecturen en hun belangrijkste eigenschappen. Ze zijn zo verschillend dat de SSO eigenschap de enige overkomst is.

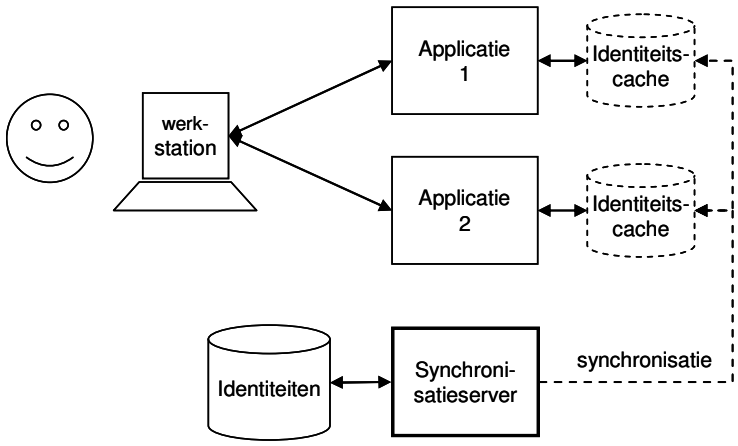
Vijf maal architectuur

1. **Client-proxy software** op het werkstation met een lokaal opgeslagen identiteitentabel. De gebruiker authenticeert zich tegen de gegevens uit een lokale tabel, waarna de client-proxy software hem inlogt op de diverse applicaties, op basis van de identiteiten en wachtwoorden uit de lokale tabel. In sommige implementaties kan de client-proxy software automatische een nieuw wachtwoord genereren als een applicatie daarom vraagt.

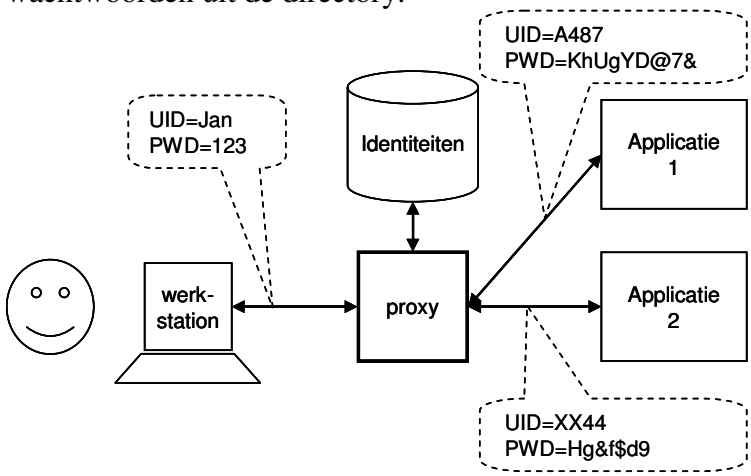


   De identiteiten van de gebruiker zijn alleen beschikbaar op zijn werkstation, tenzij ze worden opgeslagen op een extern geheugen, bijvoorbeeld een smartcard. Autorisatie moet geheel in de applicatie(server)s gebeuren.

2. **Synchronisatie** van identiteiten en wachtwoorden over meerdere applicaties en systemen. De synchronisatie kan vanaf een centraal punt worden gestuurd of gedistribueerd zijn over alle deelnemende systemen.
   In de eenvoudigste opzet worden alleen wachtwoordwijzigingen gesynchroniseerd; bij het wisselen van applicatie probeert een stukje cliëntsoftware 'achter het scherm' met de naam en het wachtwoord van de huidige gebruiker in te loggen bij de nieuwe applicatie. Dit kan effectief SSO opleveren.
   Als wijzigingen de hele identiteit betreft (naam, wachtwoord en bv. rollen) en deze real-time worden gesynchroniseerd, is er sprake van IAM met een enkele identiteit per gebruiker. De lokale directories per applicatie kunnen dan als een cache van de centrale directory worden gezien.

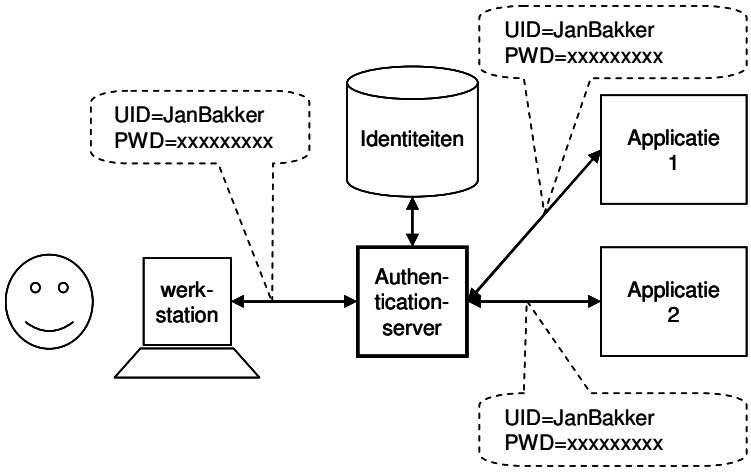


3. **In-line proxy**: de gebruiker logt in op de proxy. De proxy heeft (toegang tot) een directory en logt in op de applicaties met de applicatiespecifieke identiteiten en wachtwoorden uit de directory.

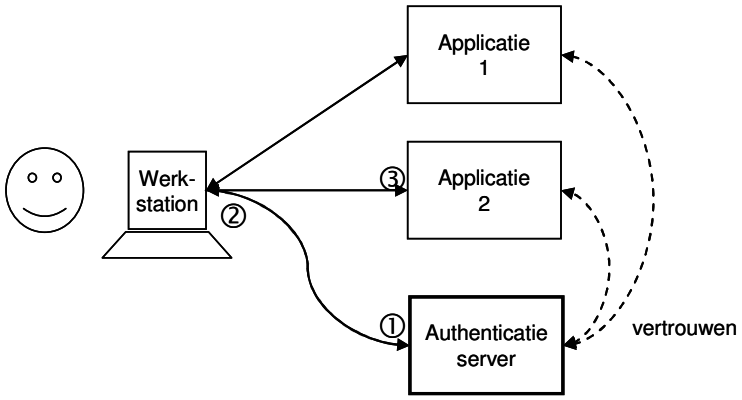


   Soms kan de proxy worden gebruikt voor centraal identiteitsbeheer, waarbij de proxy in staat is op de applicatiesystemen nieuwe identiteiten te creëren en oude te verwijderen. Voorwaarde is een vertrouwensrelatie tussen proxy en applicaties.
   Het is mogelijk twee of meer in-line proxy's toe te passen, bv. een voor medewerkers en een voor klanten, elk met een eigen set identiteiten.

4. **In-line Authenticatieserver.** Als de in-line proxy, maar nu met de mogelijkheid om nieuwe accounts op de applicaties aan te maken en oude op te heffen.



5. **Trusted Authenticatieservice**: Een centrale authenticatieserver heeft (toegang tot) alle identiteiten en hun authenticatie- en autorisatieattributen. ①De gebruiker identificeert en authenticeert zich eerst bij de authenticatieserver. ②Deze verstrekt het werkstation een "ticket", te vergelijken met een visum, een cryptografisch gesigneerd bewijs van een vertrouwde instantie die de authenticatie heeft geverifieerd. ③Het ticket wordt door de applicatie op echtheid gecontroleerd. Het ticket bevat de identiteit van de gebruiker en zijn autorisatieattributen, zoals zijn rollen voor Role Based Access Control (RBAC).



Voor deze architectuur is enige software op de client nodig. Dat kan een specifieke client zijn, of een generiek mechanisme in een Internet browser.

Eigenschappen

Vanuit het perspectief van SSO voor organisaties beoordelen we de bovenstaande architecturen op de volgende zes aspecten:

1. Hebben gebruikers één inlogcode voor alle systemen, d.w.z. gelden de identiteiten voor alle systemen?
2. Faciliteert het systeem sterke vormen van authenticatie, zoals eenmalige wachtwoorden, smartcards en biometrie?
3. Is Role Based Access Control (RBAC) mogelijk?
4. Is federatie van Identity en Access Management mogelijk?

	Client-proxy software	Synchronisatie over applicaties	In-line Proxy	In-line Authentica-tieserver	Trusted authentication service
Identiteit voor alle applicaties gelijk	Nee	Soms*	Nee	Ja	Ja
Sterke authenticatie is mogelijk	Ja	Soms **	Ja	Ja	Ja
Role Based Access Control is mogelijk	Nee	Nee	Ja	Ja	Ja
Centraal IAM mogelijk?	Nee	Ja	Nee	Ja	Ja
Transparantie (aantoonbare uniciteit van identiteiten)?	Nee	Ja	Nee	Ja	Ja
Federatie van Identity en Access Management is mogelijk	Nee	Nee	Ja	Ja	Ja

* *De identiteiten zijn alleen gelijk indien en zolang de synchronisatie perfect werkt, niet alleen voor wachtwoorden maar voor álle attributen van de identiteit.*
** *Dit stelt eisen aan de systemen en applicaties, die in de praktijk zelden zijn te realiseren.*

Uit bovenstaande matrix blijkt dat alleen de In-line Authentication server en de Trusted Authentication service alle eigenschappen hebben die (nu of in de toekomst) noodzakelijk zijn om goede informatiebeveiliging te realiseren. Het verschil tussen beide zit vooral in de eisen die zij aan de applicaties stellen. De In-line Authentication server praat tegen de normale gebruikers en beheerinterface van de applicatie, de Trusted Authentication server vereist dat de applicaties (of het platform waarop zij draaien) een protocol als Kerberos spreken.

De eerste drie architecturen (Client-proxy software, Synchronisatie van wachtwoorden en In-line Proxy) bieden vooral gebruiksgemak, maken gebruik van sterke authenticatie mogelijk, maar missen essentiële elementen voor IAM en dus informatiebeveiliging in een moderne applicatiearchitectuur. De belangrijkste beperking van de In-line Proxy is dat er bij gekoppelde systemen, zoals in de Service Oriented Architecture, geen echt unieke identiteiten zijn.

Hoe makkelijk of moeilijk de implementatie van elk van de architecturen is hangt sterk af van de omgeving: het soort gebruikers, het aantal clients, het aantal verschillende type servers en applicaties, de geografische spreiding en de organisatorische omgeving.

Uit oogpunt van beveiliging is de Client-proxy het zwakste: clients ontberen per definitie fysieke beveiliging en zijn daardoor eigenlijk niet te vertrouwen. De overige architecturen kunnen met bekende methoden goed worden beveiligd. Een cruciale stap is daarbij goed te regelen wie geautoriseerd is om Identiteiten te creëren en modificeren.

Beschikbaarheid en betrouwbaarheid

Elke vorm van centralisatie verhoogt de impact van een incident. Dat moet worden gecompenseerd. Als alle systemen met één identiteit toegankelijk zijn, vergroot dat de impact van een identiteitsdiefstal. Het antwoord daarop is de kans op diefstal te verkleinen door een betere beveiliging van de identiteitsgegevens en sterkere authenticatie, twee maatregelen die gelukkig aanzienlijk eenvoudiger worden juist door de beperking van het aantal identiteiten en authenticaties.

Eén database met identiteitsgegevens maakt de organisatie kwetsbaar voor uitval, corruptie of compromittering van deze gegevens. Ook hier is het antwoord maatregelen tot verhoging van de beschikbaarheid en beveiliging, die weer worden vereenvoudigd doordat er maar één identiteitsdatabase moet worden beschermd.

Eén database met identiteitsgegevens maakt het mogelijk inlogpogingen centraal te monitoren en zo (pogingen tot) misbruik snel te signaleren. Gebruikers kunnen leren hun ene wachtwoord zorgvuldig te gebruiken, of gebruik te maken van authenticatie op basis van twee factoren.

Uiteraard dienen autorisaties altijd ‘op maat’ te worden toegekend (‘least privilege’ principe). In een omgeving die RBAC ondersteunt is dat aanzienlijk makkelijker in te richten, te onderhouden en te evalueren.

Als de (netwerk)infrastructuur onvoldoende garanties biedt voor de beschikbaarheid en/of performance van de toegang, kan een gerepliceerde opstelling soulaas bieden: in elke (hoofd)vestiging staat dan een replica van de identiteitsdatabase. Automatische en onmiddellijke synchronisatie van elke wijziging is wel noodzakelijk.

Invoering van SSO kan ook leiden tot onderlinge afhankelijkheden van alle applicaties en systemen: een update of vervanging van één systeem kan gevolgen hebben voor een of meer andere systemen.

ELEMENTEN VAN DE BUSINESSCASE

Uit bovenstaande zal duidelijk zijn dat er *twee hoofdmotieven* zijn om tot implementatie van een Single Sign-On systeem over te gaan: verlaging van kosten en verbetering van informatiebeveiliging door versterken van Identity en Access Management. Vaak is de noodzaak om te voldoen aan nieuwe regelgeving de aanleiding voor een SSO project. Hoewel deze motieven niet strijdig zijn, kunnen ze tot verschillende keuzes en dus verschillende businesscases leiden.

Het financiële motief

De volgende aspecten zijn vooral voor het motief kostenverlaging van belang:

- Efficiëntie van de gebruikers;
- Minder werkdruk voor de helpdesk.

Deze elementen gelden voor alle vormen van SSO, al zal de opbrengst van organisatie tot organisatie verschillen. Verbetering van efficiëntie leidt immers niet automatisch tot een beter bedrijfsresultaat.

De volgende aspecten kunnen wel tot kostenverlaging leiden, maar gelden alleen voor bepaalde implementaties van SSO:

- Minder administratieve lasten (bij centralisatie van IAM);
- Voorkomen van excessieve kosten voor wettelijke verplichte audits;
- Slagvaardigheid door snel kunnen invoeren en aanpassen van identiteiten en autorisaties;
- Minder implementatiekosten voor nieuwe maatwerkprogrammatuur (bij centralisatie van identificatie, authenticatie en RBAC); daar staat tegenover dat bestaande programmatuur soms moet worden aangepast.

Gebruik van sterke authenticatie kán efficiëntie als primaire doelstelling hebben. Wanneer medewerkers vaak van terminal wisselen (zorgverleners in een ziekenhuis, baliepersoneel) biedt vrijwel automatisch inloggen een wezenlijke productiviteit- en kwaliteitverbetering. Dat kan reageren op de nabijheid van een pasje (token), waarbij de applicatie de gebruiker van terminal naar terminal volgt (fast user switching).

Het motief informatiebeveiliging

Als het hoofdmotief verbetering van de informatiebeveiliging is, zijn de baten voor elke implementatievorm van SSO:

- Bredere acceptatie van sterke authenticatie door vermindering van het aantal inlogmomenten;
- Daardoor uitbannen van telefonische ‘password reset’ verzoeken aan de helpdesk, een aangrijppunt voor “social engineering” aanvallen.

Afhankelijk van de architectuur van de gekozen implementatievorm kunnen de baten aanzienlijk toenemen:

- Unieke identiteit per gebruiker maakt consistent toegangscontrole mogelijk in een software omgeving waarin applicaties elkaar raadplegen. Enkele voorbeelden:
  - het wettelijk verplichte gebruik van basisregistraties voor gemeenten;
  - geografische informatiesystemen die *uit naam van* de gebruiker databases bevragen;
  - documentaire informatiesystemen die vanuit kantoorapplicaties worden aangestuurd.
- Bij invoering van centrale IAM zijn regels beter te handhaven;
- Identiteiten, authenticatie en rollen zijn beter te auditen;
- Rijkere functionaliteit voor authenticatie en autorisatie, bv. de mogelijkheid tot differentiëren van authenticatiekwaliteit en autorisatieniveau, afhankelijk van applicatie, tijdstip, locatie van de gebruiker en de aard van zijn werkstation.

Alternatieven voor SSO

Afhankelijk van de gekozen doelstelling en oplossing kan invoering van SSO een kostbaar en langdurig project zijn. De businesscase zal niet altijd positief zijn. Zijn er alternatieve

maatregelen die ten minste een deel van de voordelen van SSO realiseren tegen lagere initiële en operationele kosten?

- Vermindering van het aantal verschillende platformen; in een homogene omgeving zit SSO vaak al ingebouwd;
- Het “web-enabelen” van applicaties, vaak ondernomen om werken op afstand mogelijk te maken en software distributie te vereenvoudigen, kan tot reductie van het aantal inlogstappen leiden, of ten minste een omgeving creëren waarin SSO gemakkelijker is te realiseren;
- Invoeren van één inlogcode per gebruiker, geldig op alle systemen en applicaties;
- Verhoging bewustwording van het belang van informatiebeveiliging voor de medewerkers. Dit verbetert niet alleen het gebruik van wachtwoorden, maar ook “clean desk” beleid en andere vormen van zorgvuldigheid;
- Creëren van de mogelijkheid dat gebruikers zelf het wachtwoord van een applicatie kunnen resetten, waardoor de belasting van de helpdesk wordt verminderd. Als de gebruikers daarvoor inloggen op het netwerk en het antwoord op een ‘geheime vraag’ weten, kan dat voldoende zekerheid geven om een nieuw wachtwoord te genereren en bv. als SMS naar het nummer van hun geregistreerde GSM toestel te sturen. Als dat niet mogelijk is, kan een gedeeltelijke automatisering met workflowtechniek enig soulaas bieden;
- Consolidatie van applicaties kan een alternatief zijn (terug van 1100 applicaties naar slechts 50).

Bovenstaande maatregelen zijn doorgaans niet eenvoudig of goedkoop uit te voeren, maar kunnen onder bijzondere omstandigheden een gedeeltelijk alternatief zijn. De meeste van deze maatregelen maken dat het op termijn eenvoudiger en goedkoper wordt om SSO alsnog in te voeren. Alleen het automatiseren van wachtwoord-resets wordt waarschijnlijk overbodig wanneer later een systeem met SSO wordt ingevoerd.

SELECTIE ARCHITECTUUR EN TECHNOLOGIE

Hoe komen we nu in een concrete situatie tot de keuze voor een architectuur en techniek? Stap één is het bepalen van het hoofdmotief: willen we SSO vooral om efficiëntie te vergroten of is verbetering van de informatiebeveiliging het primaire doel?

Als het uitsluitend om efficiëntie gaat, komen alle architecturen in aanmerking. De aard en diversiteit van de aanwezige systemen en de bestaande IAM processen bepalen dan welke architectuur het meest doelmatig is. Het ligt misschien voor de hand daarbij vooral naar de technische inpassing van de verschillende oplossingen te kijken, maar de kosten en inspanning om de noodzakelijke organisatorische wijziging door te voeren zouden wel eens veel groter kunnen zijn. Zo kan een In-line Authenticatieserver een aantrekkelijke oplossing lijken, totdat men zich realiseert dat dit ook inhoudt dat alle IAM processen moeten worden gecentraliseerd. Kortom: bij de evaluatie moet de organisatorische impact goed worden meegewogen.

Als het primaire doel verbetering van de informatiebeveiliging is, komen nu alleen de In-line Authenticatieserver en de Trusted Authenticatieserver in aanmerking, eventueel in combinatie met software op de clients om legacy applicaties te integreren. Naarmate de organisatie meer gebruik van Service Oriented Architecture (SOA) en Software As A Service (SAAS) maakt, wordt het zowel makkelijker als noodzakelijker om onafhankelijke authenticatieserver(s) in te zetten. Het uitgangspunt van SOA is dat applicaties als generieke

diensten voor de hele organisatie werken en er dus geen “afdelingsapplicaties” meer zijn. Als dat principe is aanvaard, zou centralisatie van IAM geen discussie meer mogen opleveren. Merk op dat autorisatie (ten opzichte van rollen) nog wél een afdelingsverantwoordelijkheid kan zijn. Zo zal in een gemeente de afdeling Burgerzaken verantwoordelijk blijven voor de GBA-gegevens, die als basisregistratie door alle afdelingen moeten worden gebruikt (wettelijk voorgeschreven!) om gegevens van burgers op te zoeken. De afdelingen bepalen welke rollen hun medewerkers worden toegekend (vastgelegd in de authenticatieserver), burgerzaken legt in de GBA-applicatie vast voor welke rollen de GBA toegankelijk is en in welke mate.

REALISATIE

Voor de invoering van SSO gelden de standaard principes en technieken van project management, bijvoorbeeld volgens de Prince2 methode. Elk Prince2 project start met de businesscase. Die moet zijn gebaseerd op een goede analyse, inclusief risico’s, impact en een realistische planning van alle aspecten van het project. Daar onder vallen naast de technische implementatie van hard- en software zeker ook de organisatorische aanpassingen (IAM processen), training van beheerders en gebruikers - SSO raakt per definitie álle gebruikers!

Processen

Ook bij SSO bestaat het gevaar dat het te veel als een technisch project wordt gezien en dat de procedurele en relationele veranderingen te weinig aandacht krijgen. Vooral als de gekozen architectuur centralisatie van identiteitsbeheer inhoudt, kunnen de organisatorische consequenties groot zijn en veel mensen en afdelingen raken. Er zal veel aandacht moeten worden gegeven aan de herinrichting van de processen voor identiteitsbeheer. Wie mag een nieuwe identiteit invoeren en welke controles moeten er daarvoor zijn uitgevoerd? Wie bepalen welke rollen aan een identiteit worden toegekend? Ook bij een centraal identiteitsbestand kan het nodig zijn dat het identiteitsbeheer decentraal wordt uitgevoerd om voldoende slagvaardig te zijn. Nieuwe en tijdelijke medewerkers, gasten, cursisten, etc. moeten snel kunnen worden ingevoerd en van basisrollen worden voorzien, zodat ze aan het werk kunnen. Het kan nodig zijn vaste medewerkers een gedelegeerde bevoegdheid te geven voor aanmaken van zulke ad-hoc of voorlopige identiteiten, gebonden aan beperkingen van looptijd, aantallen en rollen van de gecreëerde identiteiten.

In grotere organisaties ontbrandt hierbij vaak de discussie over het eigendom en de correctheid van de bestaande identiteitsgegevens. Om de dagelijkse voortgang niet te verstoren acht elke afdeling haar eigen gegevens heilig, ook al leert de praktijk dat zulke registers vaak sterk vervuild zijn. Het opschonen kan zeer arbeidsintensief zijn, waarbij de vraag gesteld wordt: wie gaat dat doen en wie zal dat betalen? Om dit proces beheersbaar te houden kan het nuttig zijn met een kopgroep van enkele afdelingen en applicaties te starten en vervolgens andere groepen uit te nodigen c.q. aan te wijzen zich daarbij aan te sluiten. Cruciaal is dat alle identiteiten in de nieuwe, gecentraliseerde database conform de (wellicht ook nieuwe) regels worden ingevoerd. Dat kan inhouden dat de gebruikers zich met hun identiteitsbewijs moeten melden voordat hen een nieuwe digitale identiteit wordt toegekend.

Project

Afhankelijk van welke doelstelling het zwaarste weegt - alleen kostenbesparing of ook versterking van informatiebeveiliging - wordt voor een architectuur en de opzet van de businesscase gekozen. De hierboven aangehaalde aspecten rond de herinrichting van de processen spelen daarbij een belangrijke rol, zowel aan de kosten- als de batenkant.

Als de businesscase helder is en de doelstellingen daarmee zijn gevalideerd, is de eerste stap het ontwerpen, toetsen en zo ver mogelijk invoeren van de procesveranderingen rond IAM. Pas daarna is het tijd voor de productkeuze. Let daarbij goed op of de voorgestelde producten werkelijk de eigenschappen hebben waarop de businesscase is gebaseerd! Maak ook de afweging of álle applicaties het waard zijn om mee te worden genomen. Applicaties die nog maar een beperkte levensduur hebben of door een gering aantal mensen worden gebruikt, kunnen wellicht beter buiten het project blijven. Als men 95% van de voordelen bereikt tegen 70% van de kosten…

Voor het overige is invoering van SSO een project als elk ander en geldt de goede raad die elders daarvoor wordt gegeven: plannen, structureren, mijlpalen definiëren, successen vieren, verwachtingen managen, communicatie, communicatie en communicatie. SSO raakt de hele organisatie en iedereen zal er een mening over hebben. Het GvIB heeft een Expert Brief in voorbereiding over het managen van IB aspecten in Prince2 projecten, te zijner tijd te vinden op www.gvib.nl.

Tenslotte: zorg dat de behaalde voordelen ook zichtbaar worden gemaakt.

BEHEER VAN SSO

Na invoering van SSO moeten we het resultaat borgen en zorgen dat de organisatie er ook ten volle de vruchten van plukt. De eerste zorg is dat er in de loop der tijd toch weer identiteits-eilanden kunnen ontstaan. Toen, bij de opkomst van het Internet, alle organisaties plotseling het Internet op moesten, ontstonden er projecten die vaak volledig onafhankelijk van de bestaande ICT organisatie werden ontwikkeld en daar op geen enkele manier op aansloten: beheer, beveiliging, backup, alles werd lokaal opgezet (of vergeten), met alle gevolgen van dien. Ook voor SSO dreigt dat een decentraal project dat snel even iets moet realiseren, buiten de nieuw verworven structuur om gaat. De exclusieve rol van het centrale IAM moet formeel worden vastgelegd, maar meestal zijn ook handhaving en sancties nodig. In organisaties die IT Service Management processen hanteren, vormt het Change Management proces een goed aanknopingspunt voor handhaving.

Het hogere afbreukrisico vereist een zorgvuldige, periodieke evaluatie: het uitvoeren van een Intern Controle Programma (ICP) en het formuleren van een set normen om kwaliteit van systemen en processen op peil houden. Externe auditors, hetzij vanuit de financiële controle, hetzij vanuit de wet- en regelgevers, zijn hier doorgaans enthousiast over en zullen hun controlerende taak sneller en goedkoper uitvoeren. Dit argument is vooral geldig als SSO wordt geïmplementeerd op basis van een gecentraliseerd identiteitsbeheer.

AANDACHTSPUNTEN

De werkelijkheid is altijd complexer en weerbarstiger dan de theorie en de productbrochure. Hier noemen we een aantal potentiële valkuilen.

Tijdigheid bronsystemen

Bij de invoering van centraal identiteitsbeheer is de verwachting vaak dat deze gevoed kan worden vanuit bestaande registraties, bijvoorbeeld het personeelssysteem. Dat blijkt in de praktijk bitter tegen te vallen. Lang niet alle 'gebruikers' worden in het personeelssysteem opgenomen. Personeelszaken heeft als doelstelling alle mutaties voor het eind van de maand verwerkt te hebben, zodat de salarissen correct kunnen worden berekend. Die planning strookt niet met de noodzaak om nieuwe gebruikers en wijzigingen in rollen per direct (binnen enkele uren of sneller) in te voeren. Personeelszaken is zelf vaak afhankelijk van de aanlevering van gegevens en autorisaties vanuit de organisatie, een proces dat doorgaans niet eenvoudig kan worden versneld. Anderzijds, de wettelijke verplichting om van elke medewerker vanaf de eerste dag een kopie identiteitsbewijs te kunnen overleggen vraagt om aanpassing van deze processen. Wordt deze verplichting straks ingevuld door het IAM proces of worden de bestaande processen van Personeelszaken versneld?

Kwaliteit bronsystemen

Een andere potentiële teleurstelling is de kwaliteit van bestaande registraties, of het nu directories van systemen en applicaties zijn, of bestanden van personeelzaken of andere bronnen. Als verschillende bronnen worden samengevoegd, bv. omdat de ene wel de namen en afdelingen bevat, maar niet de e-mailadressen of kamernummers, ontstaan steevast problemen door verschillen in schrijfwijze, afkortingen en vervuiling van de bestanden. Houdt rekening met een flinke inspanning om het nieuwe systeem initieel te vullen en ga na hoe discrepanties in de bronsystemen kunnen worden gecorrigeerd.

Behoeften verschillen

Het lijkt alsof elke gebruiker dankbaar zal zijn voor SSO, maar de werkomstandigheden en gewoontes van mensen kunnen sterk verschillen. Wat voor de een de perfecte oplossing is, kan een ander juist voor nieuwe problemen stellen. Kunnen de nieuwe authenticatiemiddelen worden gesteriliseerd? Mogen de nieuwe tokens in een explosiegevaarlijk laboratorium worden gebruikt? Werkt de nieuwe inlogprocedure ook voor systeembeheerders die een netwerkstoring moeten verhelpen? Een proefopstelling, op een centrale plaats, die door zo veel mogelijk gebruikers wordt bezocht, helpt om die problemen in een vroeg stadium zichtbaar te maken.

Lock-in

Als overkoepelend mechanisme levert een systeem dat SSO implementeert per definitie het gevaar voor afhankelijkheid van het product en de leverancier. Neem dus maatregelen voor het geval de leverancier van het toneel verdwijnt. Het in escrow plaatsen van de broncode is een maatregel, maar waarschijnlijk wilt u bij wegvallen van de leverancier over kunnen stappen naar een ander, ondersteund product.

Standaarden

Ook als de leverancier nog springlevend is, kunt u door ontwikkelingen in uw organisatie (fusie) of ICT infrastructuur geconfronteerd worden met beperkingen van het gekozen

product. Goed gedocumenteerde interfaces die aan publieke standaarden voldoen kunnen dan de weg openen naar combinaties of migraties. Tegelijkertijd biedt de vermelding van zulke standaarden “op de doos” nog lang geen garantie voor probleemloze samenwerking met ander producten die dezelfde standaarden aanhalen. Het hele gebied van IAM is (2007) sterk in ontwikkeling, onder meer aangejaagd door de toenemende problemen met identiteits-diefstal op Internet. Dit heeft recent geleid tot een overeenkomst tussen de ontwikkelaars van OpenID en Microsoft’s CardSpace. De industrie lijkt tot de overtuiging te zijn gekomen dat er nu werkelijk één standaard moet komen. Die zal op termijn ook invloed krijgen in het Enterprise domein. Laat de opstelling tegenover en participatie aan standaardisatie een rol spelen in uw productevaluatie.

CONCLUSIES

Single Sign-on binnen organisaties, het niet vaker dan strikt noodzakelijk moeten inloggen, is een aantrekkelijke eigenschap voor een ICT-infrastructuur die efficiëntie verbetert en invoering van sterke authenticatie vereenvoudigt. SSO kan worden gerealiseerd door de invoering van volwaardige Identity en Access Management (IAM) systemen, die een grote bijdrage leveren aan de informatiebeveiliging en cruciaal zijn voor organisaties die aan specifieke wet- en regelgeving moeten voldoen (bijvoorbeeld gemeenten, zorginstellingen en financiële dienstverleners), maar er zijn ook oplossingen die nauwelijks meer bieden dan het reduceren van het aantal inlogmomenten.

SSO maakt sterke authenticatie niet alleen mogelijk, maar ook noodzakelijk. Invoering van SSO is dus hét moment om voor sterke authenticatie te kiezen.

Afhankelijk van het doel en de gekozen middelen zal de businesscase voor SSO alleen op kostenbesparing steunen of ook of zelfs vooral op verbetering van de beveiliging als baten aanwijzen.

Invoering van SSO heeft organisatorische consequenties die belangrijker zijn naarmate er meer IAM wordt ingevoerd.

Op de site www.ibpedia.nl kunt u meewerken aan verdere verrijking en kennisdeling over SSO en andere onderwerpen met betrekking tot informatiebeveiliging. Iedereen is van harte uitgenodigd om hieraan deel te nemen.

De expertgroep is erg benieuwd naar de toegevoegde waarde van deze expertbrief voor u en ontvangt graag commentaar. U kunt uw reacties sturen naar expertbrief@gvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

18 BEGRIPPENLIJST

Begrippenlijst	
Directory	Database met Identiteiten van mensen en objecten. In dit document concentreren we ons op de identiteiten van mensen.
Identiteit	Een record in een directory. Elk record bevat een unieke naam of nummer, gegevens ten behoeve van Authenticatie, gegevens ten behoeve van toegangsbeheer en overige gegevens (bv. afdeling, kamernummer, etc.)
Identificatie	Het proces waarmee een gebruiker door het opgegeven van een naam of nummer een relatie met een Identiteit legt (“ik ben P53871”).
Authenticatie	Het proces waarmee een gebruiker door het opgeven van een of meer authenticatie-gegevens (bv. een wachtwoord), bewijst dat hij gerechtigd is de opgegeven Identiteit te gebruiken.
Inloggen	De combinatie van Identificatie en Authenticatie.
Autorisatie	De processen waarmee een gebruiker toegang krijgt tot applicaties, functies of gegevens. Vaak wordt aan Identiteiten Rollen toegekend, en verlenen de applicatiebeheerders toegang aan bepaalde Rollen. (Jan heeft de rol Boekhouder, het financiële pakket is toegankelijk voor Boekhouders, dus Jan heeft toegang tot het financiële pakket).
Logging	Het vastleggen van gebeurtenissen en activiteiten, in dit verband: van activiteiten van gebruikers inclusief de gebruikte Identiteit, tijdstip, etc.
SSO	Single Sign-On, de eigenschap van systemen waarbij de gebruikers één maal inloggen om al hun applicaties te kunnen gebruiken.
ESSO	Enterprise Single Sign-On. SSO geschikt voor een grootzakelijke omgeving.
RESO	Reduced Enterprise Sign-On, een minder strikte vorm van SSO, waarbij gebruikers niet vaker dan strikt noodzakelijk moeten inloggen om al hun applicaties te kunnen gebruiken.

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/

Deze pagina ziet er op het moment van schrijven als volgt uit:

creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

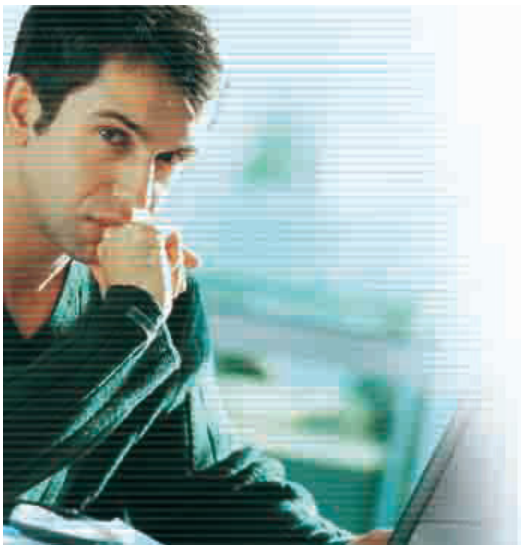
Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

20

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm