AAA opnieuw gedefinieerd.

Inleiding

Iedereen heeft wel ‘s van de term triple A of AAA gehoord. Het stamt nog uit de tijd van het inbellen op bulletinboards en staat voor Authenticatie, Autorisatie en Accounting; als je inbelt moet je wachtwoord kloppen (authenticatie), je moet toegelaten worden tot resources (autorisatie) en de start- en eindtijd wordt gelogd zodat er een rekening verstuurd kan worden (accounting). Dit is de gangbare betekenis van AAA en wordt ook zo toegepast in identity management procesessen [zie kader]. Maar identity management, het beheer en gebruik van electronische identiteiten om gecontroleerd toegang tot resources te krijgen, omvat inmiddels veel meer dan inbellen op een bulletin board. De definitie van AAA vereist een update om op de huidige visie van identity management aan te sluiten.

In het Identity management procesmodel [zie kader] zijn de vier IdM hoofdprocessen: Administreren, Opvoeren, Toegang Controleren en Monitoren. Nu blijkt dat in elk proces de triple A functies worden uitgevoerd, maar wel in op een verschillende wijze. Kortom de exacte definitie van triple A wordt bepaald door het IdM proces dat de functie uitvoert!

Het Identity Management proces model en AAA

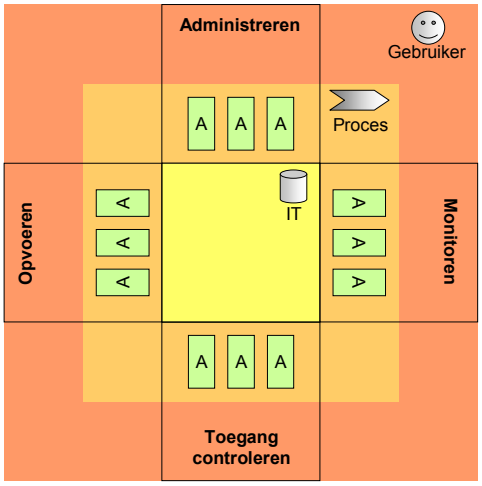
De definitie van de drie AAA functies wordt gerelateerd aan de vier hoofdprocessen uit het Identity Management procesmodel. Deze processen komen in het kort op het volgende neer.

Bij het Administeren gaat het om het registreren van een toekomstige gebruiker met zijn contractuele rechten. Tijdens het Opvoeren worden de geregistereerde contractuele rechten vertaald naar systeem rechten en gedistribueerd naar de verschillende repositories.

De Toegangs controle neemt een besluit, wel of geen toegang verlenen, aan de hand van de vastgelegde rechten. Bij het monitoren gaat het om controle van de drie andere processen.

De vier AAA functies zijn een verfijning van het Identity Management proces model dat er dan als volgt komt uit te zien:

Hierna wordt per AAA functie de verschillende betekenis toegelicht; de betekenis die afhankelijk is van het specifieke hoofdproces. Bij deze processen gaan we uit van hun primaire doel dat een gebruiker toegang moet krijgen tot de gewenste resources[1].



Monitoren heeft een dubbele bril op: enerzijds wordt gekeken of het administreren en opvoeren rechtmatig verloopt, en anderzijds wordt gekeken of de resources alleen door rechtmatige gebruikers zijn benaderd.

Authenticeren

De controle van een identiteit vindt plaats in het authenticatieproces aan de hand van een authenticatiemiddel of de zogenaamde credentials; aan de balie bijvoorbeeld met een paspoort of identititeitskaart en op een website met een wachtwoord. In het laatste geval zijn gebruikers op een eerder moment al met een e-id en wachtwoord als credential opgevoerd.

Het toekennen van een mogelijk e-id vindt hier plaats in het administratie proces maar kan ook in het opvoerproces plaatsvinden.

Bij het opvoeren wordt niet zozeer gecontroleerd, maar op een veilige manier een e-id met bijbehorende credentials gegeneerd.

[1] Administratief personeel of systeembeheerders moeten zelf ook inloggen om een nieuwe gebruikers op te voeren. Dit personeel is heeft dan al in een eerder stadium al toegang gekregen hebben tot het IdM systeem, middels een Administratie, Opvoer, Toegangscontrole en Monitor proces.

Authenticeren[2]	
Administreren	Controleer of het identititeitsbewijs van de nieuwe gebruiker OK is en administreer de gebruiker met zijn kemmerken en het gewenste e-id.
Opvoeren	Check de uniciteit van het e-id voor alle repositories. Ken de credentials toe aan het e-id en schrijf het e-id met de credentials in alle repositories; stuur het e-id met credentials aan de nieuwe gebruiker.
Toegang controleren	Stel vast of het getoonde e-id bekend is, en controleer of de getoonde credentials correct zijn voor dit e-id.
Monitoren	Comtroleer of de gebruikte credentials van de IdM medewerkers en alle andere gebruikers geldig zijn.

De authenticatie functie in het monitorproces lijkt op het eerste gezicht wat kunstmatig, maar controle of ingetrokken certificaten of verlopen tokens niet hebben geleid tot onjuiste handelingen is nodig.

Autoriseren
Autoriseren gaat over het toekennen en gebruiken van rechten. In de administratie worden de contractuele rechten vastgelegd en vervolgens worden bij het opvoeren worden deze (automatisch) vertaald naar de technische instellingen. Bijvoorbeeld een moderne internetgebruiker met een triple-play contract moet het technische opgevoerde recht hebben om zijn mailbox te benaderen, te kunnen internetten en te kunnen bellen.

Autoriseren	
Administreren	Ken de werkgrelateerde of contractuele rechten toe aan de nieuwe gebruiker.
Opvoeren	Schrijf bijpassende (technisch vertaalde) rechten in de repositories.
Toegang controleren	Verleen toegang tot resources indien de e-id de juiste rechten heeft gekregen credentials OK zijn en voor toegang tot afgeschermde diensten.
Monitoren	Controleer of IdM medewerkers of andere gebruikers de juiste rechten hadden voor hun handelingen. Controleer tevens of er voldoende functie-scheiding is.

Vaak zal in de administratie gebruik worden gemaakt van rollen om de administratieve last te beperken. De vertaling van deze rollen naar de techniek zoals systeemrechten vindt in het opvoerproces plaats en worddt zo mogelijk geautomiseerd uitgevoerd.

Accounting
Onder accounting verstaan we het vastleggen van relevante gebeurtenissen. Dat geldt uiteraard ook voor het monitor proces. Omdat we zijn uitgegaan van het primaire proces, het toegang verlenen aan een gebruiker, spitsen we hier de definitie van accounting voor het monitorproces op toe; de focus wordt dan de contole of de accounting volledig en afdoende is.

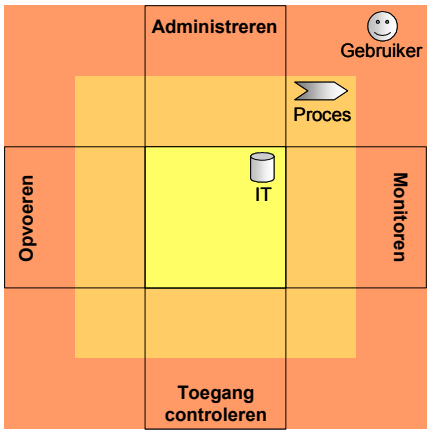
Accounting	
Administreren	Vastleggen van Administratie gebeur-tenissen in een logfile.
Opvoeren	Vastleggen van Opvoer gebeur-tenissen in een logfile.
Toegang controleren	Vastleggen van Toegangscontrole gebeur-tenissen in een logfile.
Monitoren	Controleer of alle relevante gebeurtenissen zijn vastgelegd, zijn accounting files compleet.

Conclusie
De term AAA of triple A is niet afdoende voor een goed begrip van identity management. De AAA functies hebben elk afzonderlijk een specifieke betekenis die afhankelijk is van het identity management proces waarin ze worden vervuld.

Wim Geurts is consultant bij Largos. Largos is het adviesbureau voor informatie-beveiliging en risicobeheersing sinds 2001.
Contact: wim.geurts@largos.nl of www.largos.nl

[2] Authenticeren is nog te splitsen in identificeren (kenbaar maken van je indentiteit) en vervolgens authenticeren (controleren van deze identieit). En subtiel verschil dat nu niet nodig is om verder uit te diepen voor het begrip van AAA in relatie tot IDM.

Het identity management procesmodel
Identity management wordt gedefinieerd als het toekennen, beheren en gebruiken van electronische identiteiten, om veilig en gecontroleerd toegang te geven tot specifieke resources. Deze definitie toont al een natuurlijke opdeling in de vier identity management hoofdprocessen: Administreren, Opvoeren, Toegang controleren en Monitoren.



- *Administreren:* Het toekennen (of intrekken) van een electronische identiteit en toegangsrechten aan geïdentificeerde gebruikers.
- *Opvoeren:* Na administratie van de electronische identiteit moet deze met de beoogde rechten opgevoerd (of afgevoerd) worden in de technische identiteiten databases.
- *Toegang controleren:* De toegangscontrole of access control waakt over de resources. Alleen na geslaagde authenticatie én autorisatie wordt een gebruiker toegang verleend.
- *Monitoren:* Onterecht opgevoerde of achtergebleven identiteiten en rechten, of het frauduleus gebruik van identiteiten moeten worden opgespoord en gerapporteerd

Van buiten naar binnen zijn in het model de gebruikers, de processen en de IT met identiteiten databases, als aparte lagen geschetst in alle vier de hoofdprocessen. Het model toont belangrijke interacties tussen de hoofdprocessen onderling én de interacties tussen de mens-, proces- en IT-lagen. Onvoldoende begrip en afstemming van deze interacties is een bron voor inconsistenties, niet verwijderde usercodes of incorrecte rapportages.

Hoewel de gebruikte terminologie kan afwijken, hanteren leveranciers en standaards een indeling van identity management systemen die past in het geschetste model.

In een eerder artikel 'Identity Management: De CD-rom voorbij' wordt dieper ingegaan op het identity management model en de veiligheidsrisico's van een louter technische benadering van identity managament.

Largos
Postbus 63
2501 CB Den Haag

Telefoon: 070 – 383 6467
Telefax: 070 – 383 6492
KvK Haaglanden 27245111