

# NIEUWE AUTHENTICATIEMETHODE MAAKT EINDE AAN COMPLEXITEIT INLOGGEN MET JE HELE IDENTITEIT

**Hoe groter onze afhankelijkheid van online applicaties, hoe lastiger het is om het authenticatieproces in goede banen te leiden. Zou het niet mooi zijn als we de gebruiker konden bevrijden van al die gebruikersnamen en wachtwoorden zonder concessies te doen aan het beveiligingsniveau? Dat kan als we overstappen van het traditionele accountbeheersysteem naar een systeem gebaseerd op claims. Een kennismaking in vier vragen.**

## **W**at is claims-based authenticatie?

Hoewel de term 'claims-based authenticatie' misschien niet meteen een belletje doet rinkelen, is het geen nieuw principe. Bij niet-digitale identiteiten wordt deze manier van authenticeren en verifiëren al jaren toegepast. Maar als het gaat om het authenticeren van digitale identiteiten is deze techniek nog betrekkelijk jong. Desondanks maakt iedereen in Nederland er (onbewust) gebruik van. Een authenticatiesysteem gebaseerd op claims werkt met een vertrouwde partij die identiteitsbewijzen uitgeeft. Met zo'n identiteitsbewijs kan een gebruiker toegang verkrijgen tot bepaalde bronnen. Daarbij wordt gecontroleerd of het aangeboden identiteitsbewijs daadwerkelijk is uitgegeven door een partij die vertrouwd wordt. Dat maakt het hele authenticatieproces stukken eenvoudiger dan voorheen.

De meestgebruikte vorm van authenticatie op basis van claims is de niet-digitale vorm.

Neem bijvoorbeeld een paspoort of identiteitskaart. Bijna niemand beseft dat het hier om claims-based authenticatie gaat. De houder van een paspoort of identiteitskaart overlegt het document bij de douane van een vreemd land. Op basis van de gegevens op het paspoort beoordeelt men of de houder

## **Een authenticatiesysteem gebaseerd op claims werkt met een vertrouwde partij die identiteitsbewijzen uitgeeft**

het land in mag. In dit voorbeeld is de houder van het paspoort het subject en de Nederlandse overheid de vertrouwde partij: die laatste heeft de identiteit geverifieerd waarop de dienstdoende douanier vertrouwt. Claims zijn dus bepaalde beweringen over het subject (in dit geval naam, nationaliteit, geboortedatum, lengte, et cetera) die als 'waar' worden beschouwd omdat men de uitgevende partij vertrouwt.

Ook in de digitale wereld zijn dergelijke au-

thenticatiemethoden inmiddels gemeengoed. In Nederland gebruiken we bijvoorbeeld DigiD en Live ID. Hier zijn respectievelijk de Nederlandse overheid en Microsoft de vertrouwde partij. Derden kunnen gemakkelijk gebruikmaken van deze geverifieerde identiteiten. In het geval van DigiD zijn dat voor-

namelijk andere overheidsinstellingen. Zij kunnen via de geverifieerde vertrouwde partij diverse diensten ontsluiten.

## **Wanneer passen we het toe?**

Momenteel werken veel organisaties met een breed geaccepteerde authenticatieprovider als Microsoft Active Directory, dat voor het authenticeren van gebruikers afhankelijk is van het Kerberos-protocol. Maar wat als we gaan werken met meerdere applicaties die

## MICROSOFT GENEVA

Zelf ervaren hoe eenvoudig claims-based authenticatie is? Maak dan gebruik van de bèta die momenteel actief is voor Windows Live ID. Ga naar <http://tinyurl.com/nkq96n> en meld u aan. Na aanmelding kunt u eenvoudig inloggen op alle websites die gebruikmaken van Windows Live ID. Kijk voor meer informatie over Microsoft Geneva op <http://www.microsoft.com/forefront/geneva/en/us/>.

ook nog eens worden afgenomen bij verschillende online aanbieders? Dan zal er behoefte komen aan andere beveiligingsarchitectuur. Met de groeiende populariteit van cloudcomputing ontdekken steeds meer bedrijven dat de huidige manier van authenticeren niet langer volstaat.

Er zijn tal van gebruiksscenario's denkbaar. De claims-based methode zal echter vooral tot haar recht komen bij het aanbieden van webapplicaties. Wie een applicatie maakt waarbij gebruikers geverifieerd moeten worden, dient rekening te houden met verschillende aspecten. Zo stellen applicaties die gebruikt worden door verschillende gebruikersgroepen mogelijk strengere eisen aan de toegangscontrole. Ook de geplande locatie van de webapplicatie heeft een sterke invloed op de authenticatiemethode. Wordt de webapplicatie bijvoorbeeld geplaatst binnen het bedrijfsnetwerk, bij een hostingpartij of misschien in de cloud? Vroeger zou in de meeste gevallen gekozen worden voor een gebruikersdatabase binnen de applicatie, maar bij claims-based authenticatie is dat niet langer nodig. Onlinediensten van bedrijven als Microsoft, Google en Amazon kunnen namelijk naad-

## In de meeste gevallen is de beschikbare gebruikersinformatie veel rijker dan een gebruikersnaam en wachtwoord alleen

loos geïntegreerd worden met de bestaande IT-infrastructuur. Voor de gebruiker levert dat een prettige SSO-ervaring op. Het werken met allerhande webapplicaties, aangeboden vanuit de cloud, zal stukken eenvoudiger worden.

### Wat hebben we nodig?

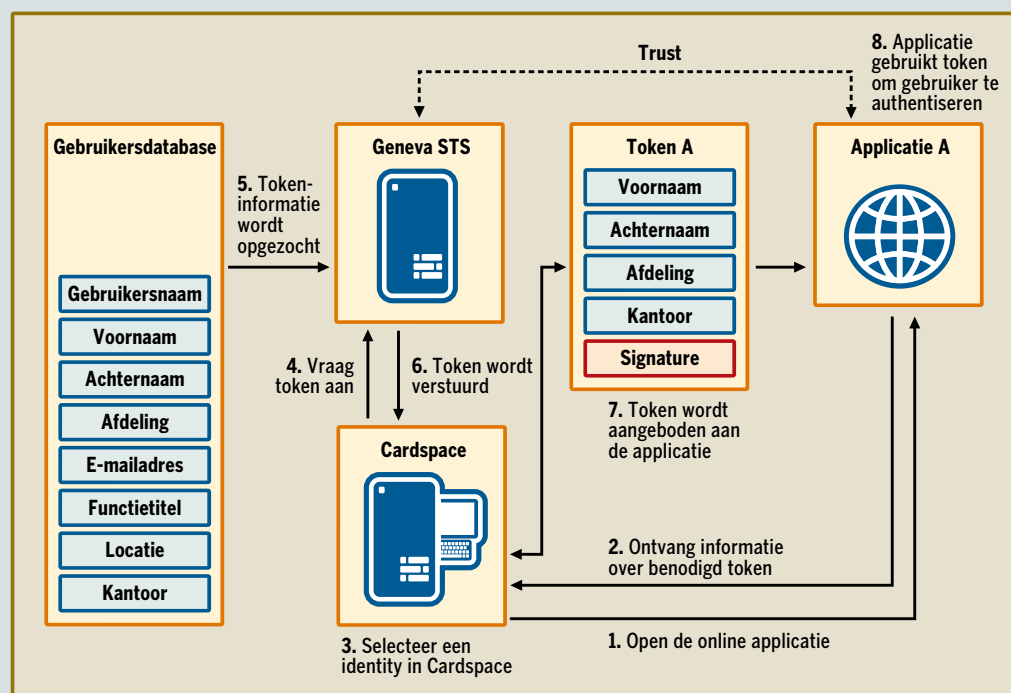
Voor deze vorm van authenticatie hebben we een paar componenten nodig. Te beginnen met de belangrijkste: een opslagplaats voor alle digitale identiteiten en hun attributen. Meestal wordt hiervoor Active Directory gebruikt. Uit deze vergaarbak van identiteiten kan de Security Token Service (STS) tokens samenstellen. Deze service is de tweede component. De tokens die worden uitgegeven, bestaan uit verschillende claims (attributen) van de opgeslagen digitale identiteiten. Daarmee kan de gebruiker inloggen bij de gewenste webapplicatie. Vervolgens controleert de webapplicatie of het token op de juiste manier versleuteld is. De webapplicatie kan deze controle uitvoeren omdat er van tevoren een vertrouwensrelatie is opgesteld met de STS.

Doordat het principe van claims-based authenticatie berust op open standaarden is het niet moeilijk om producten van verschillende leveranciers te combineren. De gebruik-

te componenten hoeven dus niet allemaal van dezelfde makelij te zijn. Zo kan een STS van leverancier A eenvoudig aangevuld worden met componenten van leverancier B.

Bij Microsoft bestaat claims-based authenticatie uit drie onderdelen: een gebruikersdeel, een serverdeel en een framework voor applicaties. De authenticatiearchitectuur van het bedrijf, die voorlopig de codenaam Geneva draagt, verkeert nog in de bètafase. Het gebruikersdeel, Windows Cardspace, is een standaardfunctie van Windows Vista en Windows 7. Hiermee worden de digitale identiteiten beheerd. Ook mensen die met Windows XP SP3 werken, kunnen Windows Cardspace gebruiken. Voorwaarde is wel dat zij beschikken over .NET Framework 3.0 en Internet Explorer 7.0 (of een latere editie). De verkregen claims worden opgeslagen in Windows Cardspace en vervolgens aan de gebruiker getoond als deze wil inloggen bij een bepaalde webapplicatie.

Voor het maken van een webinterface die overweg kan met deze authenticatiemethode, hebben we een applicatieframework nodig. Microsoft zet in op Windows Identity Foundation, dat de WS\*-instructies levert voor het authenticeren van gebruikers op basis van claims. Wat betreft het serverdeel heeft Microsoft de Active Directory Federation Services



Afbeelding 1. Bij claims-based authenticatie wordt de volledige digitale identiteit van de gebruiker benut

uitgebreid met de mogelijkheid tot het verstreken van claims. Deze STS vormt in feite het belangrijkste onderdeel van de architectuur: dit is de partij die instaat voor de claims die worden uitgegeven. De locatie van de STS bepaalt dus wie de vertrouwde partij is. Als de STS zich binnen het bedrijfsnetwerk bevindt, is het bedrijf de vertrouwde partij. Maar als we gebruikmaken van Windows Live ID is Microsoft de vertrouwde partij.

### Hoe werkt het precies?

Om een beeld te krijgen van de technische verschillen tussen het traditionele authenticatieproces en een claims-based authenticatieproces, kijken we eerst even hoe het traditionele authenticatieproces in zijn werk gaat. In de meeste situaties zal de gebruiker bij binnenkomst op kantoor zijn computer aanzetten en inloggen op het netwerk. Deze inlogpoging wordt uitgevoerd door het bestaande beveiligingsmechanisme, bijvoorbeeld het Kerberos-protocol bij gebruik van Active Directory. Bij deze vorm van inloggen vraagt de medewerker een zogenaamd securitytoken aan. Dit token wordt verkregen als de ingevoerde combinatie van de gebruikersnaam en wachtwoord correct blijkt. De combinatie van gebruikersnaam en wachtwoord is opgeslagen in de Active Directory-database.

Bij de meeste applicaties die we op dit moment gebruiken, wordt alleen naar de gebruikersnaam en het wachtwoord gevraagd. Dat terwijl in de meeste gevallen de informatie

over de gebruiker, opgeslagen in zijn digitale identiteit, veel rijker is dan een gebruikersnaam en wachtwoord alleen. Van de gebruiker is vaak ook geregistreerd wie zijn manager is, op welke afdeling hij werkt, hoe zijn e-mailadres en telefoonnummer luiden en van welke groepen hij deel uit maakt. Het is juist dergelijke informatie die prima gebruikt kan worden in een claims-based scenario.

In afbeelding 1 opent de gebruiker een browser en vervolgens de webapplicatie die hij wil gaan gebruiken (step 1). De inlogpagina bevat intelligentie uit Windows Identity Foundation. Dat maakt dat de inlogpagina tokens zal accepteren. De applicatie laat weten welke claims een token moet bevatten om toegang te krijgen en bij welke STS een token verkregen kan worden (step 2). In Windows Cardspace, waar de identiteiten worden be-

## Op basis van de gegevens uit één database kan de STS precies het token samenstellen dat een webapplicatie nodig heeft

heerd, selecteert de gebruiker nu de identiteit die gebruikt moet worden bij het inloggen (step 3). Als de gebruiker zijn keuze heeft gemaakt, wordt er een token aangevraagd bij de STS (step 4). De aanvrager moet zichzelf authenticeren op de STS om zijn identiteit te bewijzen. De gebruiker is al aangemeld op de pc en beschikt dus over een Kerberos-ticket dat overlegd kan worden aan de STS. Hiermee is

de identiteit van de gebruiker gewaarborgd en kan de STS een token gaan samenstellen (step 5). Het aangemaakte token wordt aangeboden aan de aanvrager (step 6), die het token vervolgens doorstuurt naar de webapplicatie (step 7). De webapplicatie opent het versleutelde token en controleert of de vereiste claims aanwezig zijn. Als de gegevens correct zijn, zal de gebruiker toegang krijgen tot de webapplicatie (step 8). Bij het opzetten van vertrouwensrelatie tussen de webapplicatie en de STS worden er met behulp van de tool FedUtil metadata uitgewisseld tussen de STS en de webapplicatie. Tokens zijn alleen geldig als ze zijn uitgegeven door deze specifieke STS.

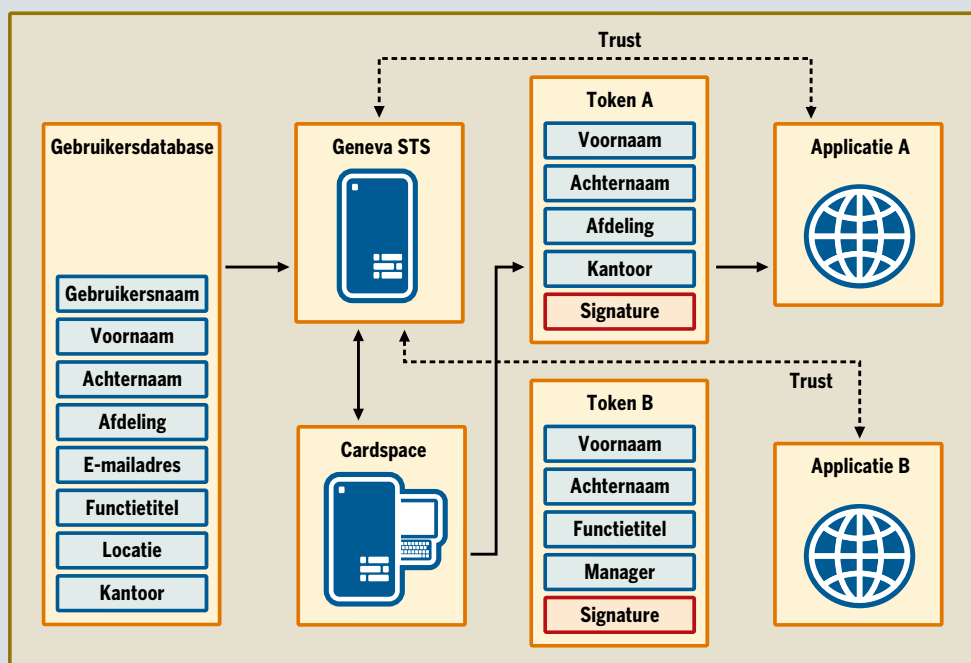
In enterpriseomgevingen gebruikt men vaak meerdere online applicaties. Dat betekent dat er ook meerdere vertrouwensrelaties

worden geconfigureerd tussen de verschillende applicaties en de STS. Als er meerdere vertrouwensrelaties zijn, kan de STS voor iedere webapplicatie passende tokens creëren. Deze identiteiten worden weergegeven in Windows Cardspace. De gebruiker hoeft alleen maar de juiste identiteit te selecteren en het bijbehorende token wordt aangevraagd bij de STS en vervolgens aangeboden aan de webapplicatie.

Kortom, op basis van de gegevens uit één gebruikersdatabase kan de STS precies het token samenstellen dat een webapplicatie nodig heeft (zie afbeelding 2).

### Conclusie

Claims-based authenticatie maakt een einde aan de complexiteit rond het inloggen. Dat geldt niet alleen voor ontwikkelaars maar ook voor gebruikers. Webapplicaties kunnen nu eenvoudig ontsloten worden zonder dat de gebruikers allerlei verschillende inloggegevens moeten onthouden. Meer dan hun eigen digitale identiteit hebben ze niet nodig. Bovendien maakt het niet uit op welke locatie de webapplicatie wordt aangeboden – als er maar een vertrouwensrelatie bestaat tussen de STS en de webapplicatie in kwestie. ◀



**Afbeelding 2.** Als er meerdere vertrouwensrelaties zijn, kan de STS voor iedere webapplicatie passende tokens creëren