Interne eindgebruikers Federale Overheid loggen vlotter in met ShaD

Veilige toegang is de basis van zowat elke ICT-toepassing binnen de overheid. Tegelijk is het erg omslachtig om voor elk stukje e-government een aparte gebruikerslijst te maken en te beheren. G-Cloud Shared Directory (ShaD) zorgt daarom voor één oplossing voor authenticatie. "G-Cloud ShaD verzoent een centrale authenticatie-infrastructuur met decentraal gebruikersbeheer", vertelt Luc Coppens, ICT Directeur bij de Federale Pensioendienst.

Het lijkt een triviaal ICT-probleem: eindgebruikers online identificeren, gebruikers toevoegen en hun toegangsrechten beheren. Het komt bij iedere toepassing kijken. Toch is het niet de bedoeling dat voor elke toepassing, voor elke instelling, aparte toegangslijsten blijven bestaan. Zoiets is immers een struikelblok voor gezamenlijke diensten. Het is ook een nodeloze kostenfactor en een permanent veiligheidsrisico.

"Voor de website van de Pensioenmotor of het samenwerkingsplatform BeConnected, werken overheidsmedewerkers uit meerdere instellingen samen. Het is gekkenwerk om met zoveel organisaties het toegangsbeheer 'ad hoc' op te zetten. Wanneer we dezelfde applicatie wilden delen met twee of drie verschillende instellingen, had je dus twee of drie verschillende technische oplossingen. Er moest een betere, generieke oplossing komen. Daar hebben we zelf mee onze schouders onder gezet", aldus Luc Coppens, ICT Directeur bij de Federale Pensioendienst (FPD).

"Na een rondvraag bij andere instellingen, federaal en in de sociale zekerheid, werd vastgesteld dat we het best konden voortbouwen op de bestaande gebruikerslijsten (directories) bij elke instelling. Dat hebben we dus gedaan", aldus Luc Coppens. Het resultaat is Shared Directory (ShaD), een generieke G-Clouddienst voor authenticatie en op termijn autorisatie.

Gebruikersbeheer blijft decentraal

"De eerste stap naar de 'Cloud', ook naar Public Cloud, is altijd de identiteit", stelt Bart Billiet, solutions architect bij de Federale Pensioendienst. De eigen directory van de instelling moet daarbij de unieke bron van de waarheid zijn. De G-Cloud

Luc Coppens, ICT Directeur, Federale Pensioendienst: "De eerste stap is de eenvoudige identificatie, met gebruikersnaam en wachtwoord, gebaseerd op de gegevens in de eigen gebruikerslijst van de instelling."

ShaD-dienst ligt als een koepel boven de gebruikerslijsten per instelling. "Instellingen behouden zelf het gebruikersbeheer. Als je daar een nieuwe 'user' maakt, dan wordt die bekend voor de G-Cloudapplicaties, en wordt die ook onmiddellijk gedeactiveerd wanneer iemand de instelling verlaat. De bedoeling is dat elke instelling dit beheer voor zich kan houden, dat dit niet centraal komt."

"Het federatie-model, waarmee we zijn gestart, is het mooiste model. De toepassingen zijn slechts 'losjes gekoppeld' met de ShaD-dienst en dus makkelijk integreerbaar, in het bijzonder voor webtoepassingen", vervolgt Bart Billiet. "Steeds meer toepassingen ondersteunen zogenaamde 'claims'. Het is een techniek waarbij de toepassing niet langer zelf de identiteitscontrole doet. De gebruiker legitimeert zich bij de directory van de instelling. De ShaD federatie-service registreert welke identiteit de eindgebruiker 'claimt', en stuurt de informatie door naar de toepassing. Waar nodig helpen we ook andere instellingen om hun toepassingen hiermee conform te maken."

In meerdere smaken en varianten

"De eerste stap is de eenvoudige identificatie, met gebruikersnaam en wachtwoord, gebaseerd op de gegevens in de eigen gebruikerslijst van de instelling", vervolgt Luc Coppens. "De claims-techniek is sterk aangewezen voor webtoepassingen van de jongere generatie. Daarnaast ondersteunen we twee andere oplossingen, voor specifieke technologie: er is een ShaD-dienst voor Office 365 en verwante diensten. Een andere ShaD-dienst ondersteunt G-Cloud

Lees verder >

Bart Billiet, solutions architect, Federale Pensioendienst: "Voor de eindgebruiker moet de identificatie nog altijd even transparant gebeuren."

UCC-as-a-Service, met Skype for Business en Exchange als belangrijkste toepassingen. De ShaD-architectuur is de enige die deze toepassingen ondersteunt en werd overlegd met vakspecialisten in Europa en de Verenigde Staten."

"Voor de eindgebruiker moet de identificatie nog altijd even transparant gebeuren. Je mag niet voor elke applicatie een verschillend wachtwoord hebben", benadrukt Bart Billiet. "De bekendste toepassing vandaag is waarschijnlijk de Loonmotor, waarmee meer dan 12.000 medewerkers in een tiental openbare instellingen van sociale zekerheid hun loonfiches elektronisch kunnen consulteren," bevestigt Luc Coppens, "of het kennisportaal BeConnected, de vertaaltool BabelFed, of technische G-Clouddiensten zoals VM-as-a-Service, Backup-as-a-Service en GITLab. De meest verregaande integratie is er voor UCCaaS en de toegang tot het federale kennisplatform BeConnected."

"Voor oudere toepassingen is er een oplossing in aanbouw. Daar moeten we ons per geval de vraag stellen of het rendabel is om de koppeling te maken. Het kan dat ShaD niet altijd de beste oplossing is, in het bijzonder voor systeembeheer of zeer specifieke toepassingen. Onze focus zal blijven liggen bij de gewone, interne eindgebruiker."

Toekomstgericht dankzij open standaarden

Terwijl de ShaD-diensten gebouwd zijn op commerciële technologie, kunnen ze met allerhande toepassingen koppelen. "De federatie-dienst is volledig op open standaarden gebouwd, meer bepaald SAML v2. De toepassingen die we vandaag gekoppeld hebben, zijn vaak open source-toepassingen. Technische specialisten uit deze wereld hebben mee aangedrongen op het gebruik van ShaD. Dan zie je dat het kan – de Windows- en Linuxwereld die in vrede samenleven", besluit Luc Coppens.

Over G-Cloud Shared Directory (ShaD)

ShaD (Shared Directory) is de centrale authenticatie -oplossing voor de G-Clouddiensten, die toelaat dat interne gebruikers van verschillende overheidsinstellingen hun identiteit kunnen aantonen bij het inloggen, en waarbij elke overheidsinstelling de eigenaar blijft van zijn eigen lokale directory.
ShaD is gebouwd met volgende doelstellingen:

- Eenvoudig identificeren van de interne gebruikers van verschillende instellingen.
- Mogelijk maken om gemeenschappelijke applicaties te centraliseren met identificatie gebaseerd op de directory van elke instelling.
- Het beheer van gebruikersaccounts blijft binnen elke instelling.
- Minimaliseren van de impact op de bestaande Active Directory (AD) van de instellingen.

Gebaseerd op het type applicatie zijn vandaag verschillende authenticatiemodellen ondersteund:

- ShaD Federation Services: Zorgt voor Single-Sign-On in claims-aware applicaties.
- ShaD UCCaaS: Biedt Single-Sign-On voor Skype For Business & Exchange UCCaaS services. Architectuur in samenwerking met Microsoft en Dimension Data, implementatie door Dimension Data.
- ShaD Online: Zorgt voor connectiviteit met Azure AD en gebruikersidentificatie binnen Office 365. Maakt hybride functionaliteiten in UCCaaS voor Skype mogelijk, waarbij services transparant tussen UCCaaS en Office 365 kunnen worden gebruikt.

Binnen ShaD en G-Cloud wordt verder gewerkt aan bijkomende functionaliteit (bijv. ShaD Domain Services, een authenticatie-oplossing voor oudere toepassingen) en aan de verdere uitbouw van een visie en nodige componenten om gebruikers op een veilige en gecontroleerde manier toegang te geven tot diensten.

Meer informatie:

Contacteer ons via
shad@gcloud.belgium.be