Analyse doorgeven van identificatie in Zaak-DMS services

Roel de Bruin, Centric PSS, 12-03-2014

Inleiding

In dit document zijn de resultaten beschreven van een analyse waarin is onderzocht op welke wijze in de Zaak-DMS services moet worden omgegaan met identificatie van de ingelogde gebruiker.

Probleembeschrijving

Uiteraard het van belang dat te weten wie welke functionaliteit aanspreekt in de betrokken applicaties. In de eerste plaats als basis voor de autorisatie waarmee we regelen dat iemand alleen kan beschikken over functionaliteit en data waarover hij mag beschikken en als basis voor het vastleggen van een audit trail waarin staat wie wanneer wat gedaan heeft.

Meer specifiek is het in de Zaak-DMS services van belang de identificatie van de ingelogde gebruiker van een Zaak-DMS service consumer door te geven aan het DMS om de beschreven functionaliteit van in- en uitchecken van documenten in het DMS te kunnen realiseren. Immers, alleen de gebruiker die een document uitcheckt kan deze weer inchecken.

Uitgangspunten

In versie 1.0 van de Zaak-Document service specificaties staat hierover in hoofdstuk 3 het volgende:

> ***Authenticatie***
> *De authenticatie dient door het ontvangende systeem, de serviceprovider, plaats te vinden. Het ontvangende systeem dient de identiteit van het zendende systeem vast te stellen.*
>
> *Voor CMIS interfaces is in de CMIS 1.0 specificatie vastgesteld dat Authenticatie op basis van het WS-Security Username Token Profile 1.1 dient plaats te vinden.*

In de eerste alinea wordt gesproken over de vaststelling van het identiteit van het zendende systeem. Dit betekent in ieder geval dat de Zaak-DMS services de identiteit van de applicatie moeten vaststellen die als consumer in de koppeling optreedt. Aangezien in de koppeling van de Zaak-DMS services met het DMS de laatste als service provider optreedt zou je dit uitgangspunt hier ook kunnen toepassen, ware het niet dat in de tweede alinea staat dat voor de CMIS interface authenticatie op basis van het WS-Security Username Token Profile 1.1 moet worden toegepast. Deze standaard is echter niet bedoeld voor identificatie van applicaties maar van gebruikers.

Samengevat kan uit deze alinea dus worden geconcludeerd dat in beide koppelingen de service provider de identiteit van de consumer dient vast te stellen.

Vervolgens staat er in de specificaties (eveneens hoofdstuk 3):

> ***Autorisatie***
>
> *Op basis van het StUF:Stuurgegeven </applicatie> van het zendende systeem dient het ontvangende systeem te bepalen of de gevraagde service / functie/ koppeling door het*

zendende systeem mag worden gebruikt. Additioneel kan door het zendende en ontvangende systeem het stuurgegeven </gebruiker> gebruikt worden. Het is aan te raden om als waarde voor </gebruiker> een binnen de gemeente unieke identificatie van de actieve gebruiker te gebruiken.

Ten eerste staat hier dat de autorisatie van de zendende applicatie (consumer) op basis van het StUF:Stuurgegeven <applicatie> moet worden bepaald. Dit betekent dus dat we de consumer identificeren op basis van dit stuurgegeven. Omdat de provider tevens verantwoordelijk is voor de authenticatie zijn aanvullende maatregelen nodig om vast te stellen dat de consumer inderdaad de applicatie is die hier is opgenomen.

Tevens staat hier dat het is toegestaan de identificatie van de gebruiker op te nemen in het stuurgegeven <gebruiker>. Dit is dus geen verplichting.

Analyse

Uitgaande van de in de specificaties opgenomen uitgangspunten dienen we twee aspecten van de identificatie te onderzoeken:

1. Identificatie van de zendende applicatie
2. Identificatie van de betrokken (ingelogde) gebruiker

Beide worden hieronder nader beschouwd.

Identificatie van de zendende applicatie

De wijze van identificatie van de zendende applicatie is in het geval van de koppeling tussen service consumers en de Zaak-Document services expliciet in de specificaties beschreven. We dienen hiervoor het stuurgegeven <applicatie> in de StUF-berichten te gebruiken. Om zeker te stellen dat de consumer de juiste identiteit aanlevert moeten aanvullende maatregelen worden genomen. De aanbevolen methode is SSL in combinatie met een client-side certificaat. Het gebruik van SSL wordt sowieso verplicht gesteld in de vereiste StUF protocolbindingen versie 3.02.

In de koppeling tussen de Zaak-Document services en het DMS zijn de CMIS 1.0 specificaties van toepassing. Daarin is wel opgenomen dat authenticatie op basis van het WS-Security Username Token Profile 1.1 dient plaats te vinden, maar die standaard gaat over identificatie c.q. authenticatie van gebruikers. Er is niets gespecificeerd over de identificatie van aangesloten applicaties. Aangezien in de specificaties is opgenomen dat service provider hiervoor verantwoordelijk is, hoeven we hiervoor dus geen specifieke maatregelen te treffen in de zaak-document services. Het lijkt me wel realistisch in ieder geval rekening te houden met de mogelijke eis van het DMS van communicatie op basis van SSL in combinatie met een client-side certificaat.

Omdat in de CMIS specificaties niets is opgenomen over identificatie van applicaties hoeven de Zaak-Document services deze identificatie niet door te geven. Volgens de Zaak-Document service specificaties moet de identificatie wel gebruikt gaan worden voor autorisatie van applicaties.

Identificatie van de betrokken (ingelogde) gebruiker

Volgens de Zaak-Document service specificaties mag de ingelogde gebruiker worden opgenomen in het stuurgegeven <gebruiker>. Dit is dus niet verplicht.

Volgens de CMIS specificaties moet het WS-Security Username Token Profile 1.1 worden gebruikt voor authenticatie van de gebruiker. Dit betekent dat, wanneer de gebruiker niet is opgenomen in de stuurgegevens, de Zaak-Document services richting het DMS een standaard, voorgedefinieerde gebruiker moet hanteren.

In het WS-Security Username Token Profile 1.1 is specificatie van de gebruikersnaam verplicht. Het wachtwoord is optioneel. Maar aangezien de CMIS specificatie spreekt over authenticatie is het weglaten van het wachtwoord geen optie. In dat geval kan immers niet worden vastgesteld dat de gebruiker is wie hij zegt dat hij is.

Gezien bovenstaande moet worden geconcludeerd dat de eisen ten aanzien van authenticatie in de Zaak-Document service specificaties onvolledig en tegenstrijdig zijn.

Als in CMIS de authenticatie moet worden uitgevoerd op basis van het WS-Security Username Token Profile 1.1 met de verplichting een wachtwoord op te nemen, dan kan dat praktisch alleen worden gerealiseerd als dezelfde eis wordt gesteld aan de koppeling tussen de Zaak-Document services en hun consumers. Het enige alternatief is het lokaal vastleggen van wachtwoorden van geautoriseerde gebruikers of het creëren van de mogelijkheid deze op te vragen. Beide alternatieven zijn ons inziens in verband met beveiliging ongewenst.

Het WS-Security Username Token Profile 1.1 kent twee varianten in de specificatie van het wachtwoord: PasswordText en PasswordDigest. In de laatste variant wordt het wachtwoord opgenomen in Base64 encoded formaat van een SHA-1 hash van het wachtwoord, al dan niet in combinatie met aanvullende gegevens voor extra beveiliging. Deze variant kan alleen worden gebruikt als de wachtwoorden van geautoriseerde gebruikers aan beide zijden bekend zijn. Ook deze variant is ons inziens ongewenst in verband met de noodzaak van lokale opslag van wachtwoorden in het DMS.

Al met al kan uit bovenstaande worden afgeleid dat authenticatie van de gebruiker op basis van het WS-Security Username Token Profile 1.1 alleen kan werken als dit ook verplicht wordt gesteld in de communicatie met de Zaak-DMS services en als het gebruik van de PasswordText variant verplicht wordt gesteld, uiteraard in combinatie met transport encryptie zoals die reeds wordt vereist in StUF protocolbindingen versie 3.02.

Het heeft geen zin bovenstaande te implementeren zonder dat de standaard hierop is aangepast c.q. uitgebreid. Het is daarom van belang hierover in contact te treden met KING. In de implementatie van de huidige standaard kunnen we eigenlijk alleen maar uitgaan van het opnemen van een standaard gebruiker in de communicatie met het DMS. Dat betekent in de praktijk dat de gegevens van de ingelogde gebruikers in de Zaak-Document service consumers verloren gaan in de koppeling naar het DMS. Om die reden zal onder meer de checkout/checkin functionaliteit in deze implementatie niet optimaal functioneren.

Conclusies en aanbevelingen

Aanbevolen wordt de volgende aanpassingen aan de standaard met KING te bespreken:

1. Uitbreiden van de Zaak-Document service specificaties met de eis dat het WS-Security Username Token Profile 1.1 ook wordt toegepast in de communicatie van consumers met de Zaak-Document services.

2. Verplicht stellen van de PasswordText variant in het gebruik van het WS-Security Username Token Profile 1.1.

3. Authenticatie van Zaak-Document service consumers door gebruik van client certificaten expliciet als eis opnemen (in plaats van de vage aanduiding "…eisen die gelden voor de normale eindgebruikerfuncties…").