Overleg 22 okt ‘14 in S2M Amersfoort-Noord met Wouter

Aanleiding

Het is wenselijk om bij gebruik van CMIS de (eind)gebruiker correct mee te kunnen geven naar het DMS (ook als de eindgebruiker werkt met een applicatie die via StUF met het Zaaksysteem communiceert).

Single sign on (SSO) via SAML v2 zou de meest wenselijke oplossing zijn (SAML v2 is momenteel de generieke overheidsstandaard voor SSO: https://lijsten.forumstandaardisatie.nl/open-standaard/saml). Deze is echter niet breed genoeg binnen gemeenten geïmplementeerd om als randvoorwaarde voor deze oplossing gebruikt te kunnen worden. Wanneer dit in de toekomst wel het geval is, kan deze functionaliteit met toepassing van SAML uitgebreid worden.

Voorstel

- Uitbreiden hoofdstuk 3 (authenticatie/autorisatie beschrijving)
- Opnemen aanvullende eisen bij de generieke eisen aan de genoemde componenten
- Onderdeel maken van basisfunctionaliteit in eerstvolgende nieuwe versie van de standaard Zaak- en Documentservices (versie 1.1).

Schets van globale werking

Gegevens die in het StUF-bericht aanwezig zijn, worden gebruikt om via een CMIS-extension de gebruiker (en eventueel zijn organisatie) bij het DMS bekend te maken.

De CMIS-extension kent de volgende structuur:

```
<extension> <!-- Dit is de CMIS-extension node -->
      <zender xmlns=”StUF”>
            <organisatie>Organisatienaam</organisatie>
            <applicatie>Applicatienaam</applicatie>
            <administratie>Administratienaam</administratie>
            <gebruiker>Gebruikersnaam</gebruiker>
      </zender>
</extension>
```

Eisen aan de betrokken componenten

- Eisen aan de StUF document-/zaakserviceconsumer voor alle berichten die (uiteindelijk leiden tot een interactie met het DMS):
    - Het element `<StUF:zender />` MOET opgenomen zijn als geldige CMIS-extension (zodat ze geïnterpreteerd kunnen worden door het DMS). Toelichting: nadere specificatie van de vulling van `<StUF:zender />` is niet nodig: bij ontbrekende `<StUF:gebruiker>` is in elk geval `<StUF:applicatie>` gevuld (verplicht veld). Dit is voldoende voor interpretatie door het DMS.
- Eisen aan de CMIS documentserviceconsumer:

    - Het CMIS-element `<cmis:extension>` MOET in elke aanroep een element: `<zender xmlns="StUF" />` bevatten met de naam van de gebruiker die de actie uitvoert conform de volgende logica:
        - Als er geen eindgebruiker is (bij systeemacties) MOET uit het element: `<zender xmlns="StUF" />` de identiteit van de aanroepende applicatie afgeleid kunnen worden.
        - Als de CMIS aanroep volgt uit een aanroep van een StUF Zaak-/Documentserviceconsumer MOET het element: `<zender xmlns="StUF" />` gevuld zijn met de inhoud van het element `<StUF:zender />` uit het aanroepende bericht van de StUF Zaak-/Documentserviceconsumer.
        - Als de aanroepende applicatie zelf de applicatie is die zich via usernameToken authenticeert, MOET het element <StUF:applicatie> binnen het element `<zender xmlns="StUF" />` gelijk zijn aan de 'username' binnen het usernameToken.
          Toelichting: Zo blijft de applicatienaam zowel in de WS-Security als in de StuF-context gelijk.
    - Toelichting:
        - Het veld als 'extension' opnemen is de enige mogelijkheid om bij een CMIS-functieaanroep extra informatie mee te geven waarop het CMIS-ondersteunende DMS actie kan ondernemen.
        - De extension-naam 'zender' is gekozen omdat dit dezelfde naam is als in het StUF-bericht.
- Eisen aan het DMS:
    - Het DMS MOET indien het CMIS-extension-element `<zender xmlns="StUF" />` in de aanroep aanwezig is, uitsluitend dit element gebruiken om de gebruiker te identificeren
    - Het DMS MOET indien het CMIS-extension-element `<zender xmlns="StUF" />` in de aanroep aanwezig is, uitsluitend de 'zender'-identificatie gebruiken om te bepalen met welke rechten en met welke gebruikersimpersonatie de betreffende aanroep (operatie) uitgevoerd wordt.
    - Toelichting:
        - Op deze wijze wordt geborgd dat het autorisatiesysteem van het DMS correct wordt toegepast voor de verzender van de aanroep en dat de juiste gebruiker in de betreffende CMIS-elementen gevuld wordt. Het DMS toont deze dan op alle plaatsen waar het DMS een gebruikersverwijzing heeft (zoals 'last edited by', 'checked out by', etc.). Deze gebruiker kan dus een eindgebruiker zijn of een applicatie.
        - het DMS kan op deze manier zowel met als zonder de extension-data werken. Zo blijven CMIS-clients die geen gebruik maken van de Zaak- en Documentservices (zoals scan applicaties) ook toegang houden tot het DMS.