

FUNCTIONEEL CONCEPT

AUTORISATIE

DATUM: 7 JUNI 2023

VERSIE: 0.2

PROJECT: VERNIEUWING DMS

Versiegeschiedenis

VERSIE	DATUM	AUTEUR(S)	AFSTEMMING MET
0.1	31 mei 2023	Bert de Lange	Fransien Sijtsma, Kurt Cordesius
0.2	7 juni 2023	Bert de Lange	Review van Fransien Sijtsma, Kurt Cordesius
0.3			

Inhoudsopgave

1. Functioneel Concept: Autorisatie	5
1.1 Context	5
2. Authenticatie	5
3. Autorisatie	5
3.1 Autorisatie : Access control lists	5
2.2 Opzet autorisatie en vertrouwelijkheid in het metadata model: vertrouwelijkheid op diverse niveau's	6
2.2.1 A) (sub)dossier niveau	6
2.2.2 B) Document niveau	6
2.2.3 Beheerfunctie: vertrouwelijkheid op dossier niveau:	7

1. Functioneel Concept: Autorisatie

1.1 Context

Wat is je rol binnen de SVB? Welke gebruiker mag wat raadplegen en wijzigen in het vernieuwde CSP?

Dat moet duidelijk zijn in het vernieuwde CSP. Tevens wordt hier beschreven welke uitgangspunten er gehanteerd/gekozen zijn in het metamodel met betrekking tot autorisatie en hiermee samenhangend de vertrouwelijkheid van documenten.

Daarnaast moeten ook de diverse gevolgen van deze keuzes duidelijk worden beschreven, zodat er een samenhangend beeld ontstaat en geen misverstanden die leiden tot een verkeerde toegang tot documenten en/of datalek.

In de SVB worden de SVB medewerkers geautoriseerd volgens een rollenmodel. Indien een medewerker moet worden geautoriseerd, wordt één of meerdere rollen toegevoegd en worden op basis hiervan de toegangsrechten toegekend. In het huidige DMS logt een medewerker aan en krijgt volledig toegang tot alle documenten, in het nieuwe CSP platform dient de mogelijkheid te bestaan dat een medewerker in een rol/functiegroep slechts beperkte toegang heeft tot objecten (bijv. dossiers of documenten).

1.2 Authenticatie

Authenticatie en Autorisatie werken samen. Authenticatie is het proces waarbij er bepaald wordt of een bepaalde gebruiker toegang heeft tot het CSP systeem, hierbij wordt tevens bepaald of een gebruiker is wie hij beweert te zijn. Het is op dit moment nog niet duidelijk hoe dit geïmplementeerd gaat worden. Echter, in ieder geval wordt ervan uit gegaan dat:

- Een gebruiker logt in middels een UserID/wachtwoord combinatie of middels een LTPA token
- Er komt een sessie tot stand waarmee een verbinding met het CSP gemaakt kan worden. Een deel van de in-sessie opgeslagen informatie is de UserID van de ingelogde gebruiker
- Aan de hand van de UserID wordt er bepaald wat de Autorisatie structuur wordt voor de ingelogde sessie

2. Autorisatie

Terwijl de authenticatie een antwoord geeft op de vraag “wie krijgt toegang tot het CSP”, geeft Autorisatie een antwoord op de vraag “wat mag de gebruiker doen bij het CSP”.

De implementatie van het autorisatie model is het mechanisme dat bepaalt wat voor rechten (privileges) een gebruiker heeft op een bepaalde item (dataobject) of ItemType.

Kortom: Authenticatie regelt de **toegang tot** het CSP systeem, Autorisatie regelt de **acties binnen** het CSP systeem.

2.1 Autorisatie : Access control lists

In het Content Management Systeem worden toegangslijsten (ACL's) bijgehouden welke aangeven wie, wat mag doen met een Item. Dit betreft dan zowel de mogelijkheden (creatie, lezen, verwijderen) betreffende een dossier, een document of een versie. Voorbeeld: hierbij geeft een lijst aan dat bijvoorbeeld de rol 'beoordelaar' een dossier mag aanmaken en een document mag maken in dat

betreffende dossier. Echter het wijzigen of verwijderen van een document is voorbehouden aan een andere rol.

De ACL lijst wordt of bij de opslag (bijv. dossier of document), bij het creëren, of volgens een default lijst aangemaakt.

Per repository (AA, PGB, overig) wordt per object-type een matrix opgesteld, aangezien voor iedere repository andere functie-rollen kunnen bestaan.

2.2 Opzet autorisatie en vertrouwelijkheid in het metadata model: vertrouwelijkheid op diverse niveau's

In het metadatamodel is op twee plaatsen de vertrouwelijkheid gedefinieerd

2.2.1A) (sub)dossier niveau

Dit gegeven bepaalt niet de vertrouwelijkheid binnen het betreffende dossier maar geeft weer welke vertrouwelijkheid categorie een nieuwe document(versie) krijgt wanneer deze opgeslagen wordt in het CSP. In het dossier eventueel al aanwezige documenten behouden hun reeds toegekende vertrouwelijkheid-status. Indien noodzakelijk moet die status vanuit een bedrijfsapplicatie aangepast worden.

- Creatie (sub)dossier

Een subdossier heeft een eigen vertrouwelijk-categorie, eventueel is deze afgeleid van het niveau van het bovenliggende parent dossier niveau.

2.2.2B) Document niveau

Vervolgens wordt deze vertrouwelijkheid categorie gebruikt bij het creatie en plaatsen van documenten in het (sub)dossier. Deze categorie wordt dus meegenomen in de metadata van de documentversie. Deze categorie bepaalt vervolgens dan ook de ACL (access control list) van het document.

Deze vertrouwelijkheid categorie op het document bepaalt dus in feite of het document zichtbaar/raadpleegbaar is voor een bepaalde rol.

Opmerkelijke situaties:

- Dit houdt dus ook de volgende 'opmerkelijke' situatie in: op het dossier niveau geldt op een bepaald moment de vertrouwelijkheid categorie 'openbaar', terwijl er document(versies) in het dossier zijn met diverse vertrouwelijkheid categorieën. (bijv. 1 versie 'geheim', 1 versie 'openbaar' en wellicht nog een versie 'intern')

Voorbeeld:

Dossier A is 'geheim'. Document wordt in dit dossier geplaatst. Het document erft hierbij de vertrouwelijkheid van het dossier.

De vertrouwelijkheid van het document wordt aangepast en bevat dus ook 'geheim': Dat wil zeggen; de toegang wordt beperkt tot degenen die 'geheime' documenten mogen inzien.

Vervolgens wordt de vertrouwelijkheid van het dossier 'openbaar': Echter de toegang van de reeds bestaande documenten (met overerfde vertrouwelijkheid 'geheim') blijft bestaan: de beperkte toegang blijft dus bestaan tot de 'geheime' documenten.

- Het kan dus zijn dat dossier wel raadpleegbaar zijn (via bijv. via zoekopdrachten) terwijl men het document niet kan raadplegen.

2.2.3 Beheerfunctie: vertrouwelijkheid op dossier niveau:

Het wijzigen van de vertrouwelijkheids(periode) op dossier niveau kan slechts gebeuren via een specifieke onderhoudsfunctie die slechts door specifieke bevoegde medewerkers opgeroepen kan worden. Deze rubriek kan dus niet via de 'wijzigen metadata dossier' functie niveau gewijzigd worden.

(Deze mogelijkheden zijn nog niet verder gebouwd/ontworpen en moeten nog verder bepaald/besproken worden met informatiebeheer/systemen.)

De mogelijkheden voor wijziging voor deze medewerkers geldt:

- Slechts de laatste periode van de VertrouwelijkheidsPeriode kan gewijzigd worden:
- Datum-van kan niet samenvallen of eerder vallen dan de datum-vanaf van het voorafgaande voorkomen van VertrouwelijkheidPeriode.
- Niveau kan zowel verhoogd als verlaagd worden