Memo

Aan
Sander Loos, Bob van der Staak, Robin Ganpat, Jan-Maarten Verbree, Reinout van Rees, Geri Wolters, Flip Dirksen, Erik de Rooij
Cc: Rianne Giesen, Jeroen Gerrits

Datum	**Kenmerk**	**Aantal pagina's**
25 oktober 2017	11200534-DSC-0022-v0.9	3
Van	**Doorkiesnummer**	**E-mail**
Stef Hummel	+31(0)6 1019 8112	stef.hummel@deltares.nl

Onderwerp
Aangepaste versiee “High-level design authentication and authorisation”

This memo is an adapted version of the document “High-level design authentication and authorization” as produced by HydroLogic (Sander Loos) during the project “Realisatie Digitale Delta, 2016”.
The changes were made according to the various meetings on authentication/authorisation in the project “Realisatie Digitale Delta, 2017”.

Introduction

The Digital Delta will be a distributed network in which various data sources exchange information using a standard Web service. The mechanics and technical specifications for the Digital Delta Web API are described in:
https://github.com/DigitaleDeltaOrg/dd-api-spec:

- DigitalDelta.raml: specification in RAML (RESTful API Modelling Language)
- DigitalDelta.html: documentation generated from that specification

This memo presents high-level approach and requirements (functional and technical) for authentication and authorisation of users and their access to data in the Digital Delta. The objective is to present the architecture along which water data and information platforms can work together in the Digital Delta.

Goal

Goal is to permit users to work across different platforms (for example Lizard, HydroNET, RWS DDL) within the Digital Delta without having to re-login at each platform or application that uses Digital Delta standards.

Definitions

- DD-API: the Digital Delta Web API
- (User) Authentication: confirming that a user who uses the Digital Delta network is actually the user he/she claims to be, by confirming given identification credentials with registered identification credentials in an Authentication Provider service.

- Authorisation: confirming that a user has access to certain (meta)data that is made available in the Digital Delta network.
- Authentication Provider (AP): OAuth2 service where users register and receive an account (for example: Digital Delta, Lizard, HydroNET, …).
- DD Data Node (DN): a node (in fact a url) that exposes data and related metadata according to the DD AP.
- DD Data Node with harvested metadata (DNM): a node that has harvested metadata from Data Nodes.
  Note: a node can be a DN and a DNM and at the same time, when it harvests metadata and provides its own data and related metadata.

Architecture and authentication control flow

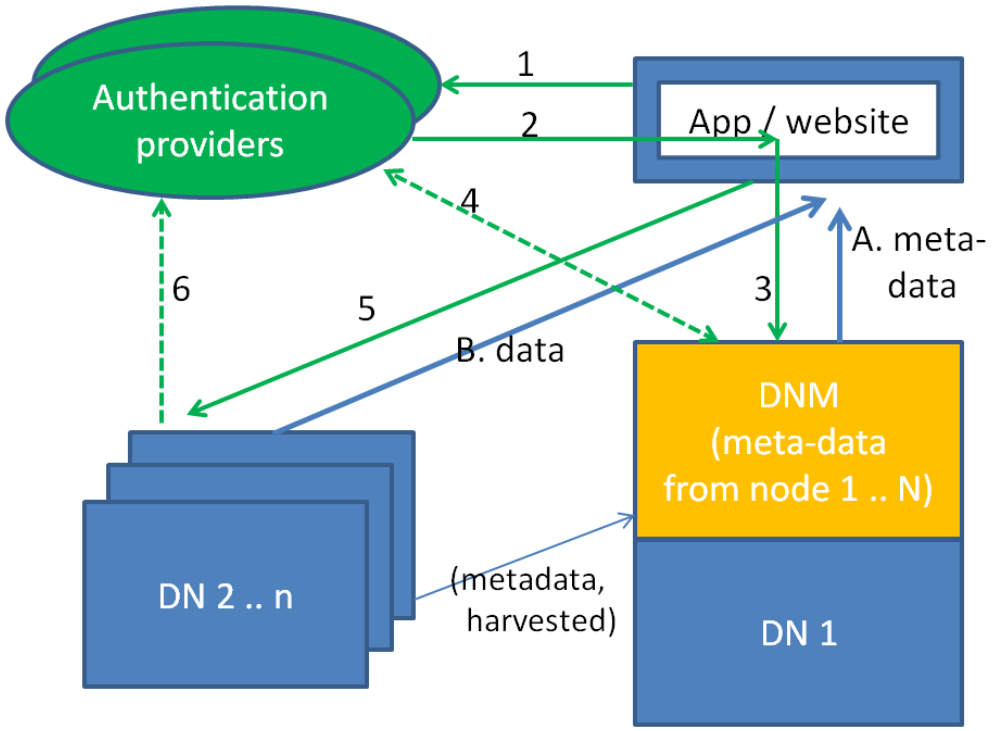
The Digital Delta will consist of a distributed network of DN, DNM and AP implementations in which there is no predefined hierarchy: there is no central point in the network where necessarily all (meta)data or users are registered.

The roles are:

- AP's are the leading (and only) places for user registration and authentication.
  Anyone may set up an OAuth2 AP service for users. It is however up to DN(M)'s administrator to actually make use (acknowledge and connect) an AP service or not. If a DN(M) decides not to connect to an AP service, the users of that AP will not be granted access to the non-public (non-open) DN(M) data and metadata.
  APs may implement groups optionally.
- DN(M)'s are the leading (and only) places where authorisation is configured. This means users are linked to access rights on (meta)data.
  DN(M) administrators can implement authorisation at user level or group level.
  They can make use of the AP services to pre-configure users (optionally: AP groups) and their access to (meta)information.
  Note: if a DN(M) has only public (open) data there is no need for authorisation.

The figure on the next page shows how the authentication process works. The figure contains:

- Two AP's
  One AP is for example HydroNET, the other Lizard.
- A number of DN's
- One DNM (a Data Node that has its own data and meta-data, and has harvested metadata from some other DN's)
- An application or website (e.g. a viewer)



The steps during the authentication process:

- *Step 1 and 2*
  In the viewer, the user chooses to login using his/her HydroNET or Lizard account (or in the future, maybe his DD-account). The viewer accesses the chosen AP and receives a token.
- *Step 3 and 4*
  This token is provided in the call for metadata to the DNM. The DNM checks with the AP if indeed this person is who he/she claims to be.
  If identified correctly, the user receives the requested metadata (step A).
  The DN may cache the authorisation information for the session.
- *Step 5 and 6*
  If the user selects data that is provided by the same node, *step 4* is repeated when the call for the data perform.
  If the user selects data that is provided by another node (say DN 3), in the call for the data to DN 3 the same token is provided (i.e. the token received from *step 2*).
  DN 3 checks the user's authenticity at the AP.
  If identified correctly, the user receives the requested data (step B).

User groups

An administrator of a DN manages several internal access groups, defines the access right for such a group, and includes users in one more groups.
In a first step, the 'external users' (i.e. the ones know in the AP of the other system) could be put in one internal group.
The question is whether we want to know groups on a central level or not. This will be discussed in a later stage.