# Security Service, Authentication for GISC, DCPC and NC, OpenWIS Philosophy

## Security and Management of data access policies

### Presentation plan

* Security Service Requirements
	+ Generalities - Functions Overview
	+ Domains and Circles of Trust
* OpenWIS Design
* Architecture
* Authentication Process
* Authorisation Process
* Manage session token
* Blacklisting
* User Management Services
* Circles of trust scenarii in a virtual organisation
* Overview
	+ Setup
	+ Pro and Cons
* ANNEX
	+ LDAP Schema
	+ Login Glossary

# Security Service Requirements

## Generalities - Functions Overview

The Security Service of the GISC (WMO Functions A2 & A4) has to provide:

**Authentication**: Identifying who the user is.

**Authorisation**: Identifying what the user is allowed to do.

In this document, we analyse the authentication process and the authorisation process to access the different portals. Matching with the WMO rules, we propose

* Chapter 2: a design based on OpenWIS
* Chapter 3: a strategy of circles of trust for the WIS

## Domains and Circles of Trust

An architecture has to be proposed for the identity management within the GISC domain and across domains (Virtual Organization), as well for local and remote Authentication / Authorization scenarios.

**Domain:**

The domain gathers all the WIS functions belonging to the same organisation

The domain has an IdP (Identity Provider) with a LDAP database

Example 1: Météo France with 1 NC, 8 DCPCs and 1 GISC

Example 2: Spain with one NC and a few DCPCs

**Circle of trust (IDP Federation):**

Security and identity management involve the concept of trust relationships among interacting parties according to the agreed levels of trust.

A known authenticated user is allowed Single Sign-On, and may freely navigate from one Centre to trusted Centre at a remote Site.

Users at a GISC may discover data located at a remote trusted Centre (an Internal DCPC). In order to retrieve the data or product, the authorized user is transferred to the Internal DCPC Centre with Single Sign-On. Authorization is checked again at this Centre, where the user needs to be acknowledged with his own User Role.

This scenario is not valid for a product where the user is transferred to the External DCPC and needs to authenticate as a user known to the DCPC.

A glossary is available in Annex A

#

# OpenWIS Design

##

## Architecture

Each GISC domain typically contains one GISC, one NC and one or several DCPC, all connected to one Security Service (with one IdP and a LDAP database).

The domain corresponds to an organisation or a company, for example Meteo France deployment.

Each Circle of Trust contains one Identity Provider Discovery Service (IdP Discovery) which is used for Authentication, Single Sign-On and Federation.

A circle of trust can be setup between organisations, each organisation owning its IdP and local user LDAP database.

Potential example of COT: Meteo France deployment with Spain NC (local IdP), Portugal NC etc …

Figure 1 : Circle of Trust Schema

In this example,

* Domain 1 is composed of a GISC, a NC and two DCPCs, and a Security Service
* Domain 2 is composed of a GISC, a NC and two DCPCs, and a Security Service
* The Circle of Trust contains Domain 2, Domain 1 without DCPC2 and an IdP Discovery.

The architecture of the Security Service is shown below:

Figure 2 : Security Service Architecture

OpenDS is an open source directory service (LDAP), developed in the OpenDS project.

OpenAM is an open source access management and federation server developed by ForgeRock.

OpenAM proposes a seamless integration with OpenDS.

Open AM is used for:

* User Authentication
* Single Sign-On
* Federation
* Managing user session : login / logout / check if the session is valid

The User Management Component is used to manage users and groups. It uses LDAP Protocol for communicating with OpenDS.

## Authentication Process

The following figure illustrates the authentication process implemented in OpenWIS.

Figure 3 : Authentication Process

1. The user clicks on Login button.
2. OpenWIS Init servlet redirects to IdP Discovery if *\_saml\_idp* cookie exists.
3. IdP Discovery redirects to portal and return the preferred IdP if the cookie exists.
4. Three possibilities can occurred :
	1. User is already connected on the Centre, the authorisation phase can begin.
	2. User has never chosen his preferred IdP. Choose your domain page is displayed
		1. User validates his choice.
		2. OpenWISDomainSelected class redirects to IdP login previously selected.
	3. User has already chosen his preferred IdP and he isn’t connected on the Centre. The user is redirected to his preferred IdP for login.
5. Authentication is successful
6. IdP Discovery creates *\_saml\_idp* cookie.
7. The Authorisation can begin.

The system only logs the user login and no other personal information.

## Authorisation Process

When the user is authenticated, the user must be authorised to access the portal.

The authorisation is function of the user profile, “Need user account” value and user groups.

A user belongs to one or several groups of Centre or/and GLOBAL groups.

After checking that user is authorised, a user session is created:

When a user is authorised, he can access to a particular metadata, data or service.

## Manage session token

When the authentication process is successful, a session token is created by the IdP. This token allows to know if the session is valid.

A REST API is available on the IdP to check the token validity as well as retrieving information such as user attributes from this token. This REST API will be used in particular when retrieving remote subscriptions of a user.

## Blacklisting

The blacklisting process allows to prevent a user from performing an excessive amount of requests (volume) and then to protect the system from abusive use.

The process of blacklisting is local to a Centre (related to the Data Service). The blacklisting thresholds and the blacklisted state are then locally defined on each center, along with the current volume of data and number of files disseminated per day for each user.

For each user and each of these two parameters (volume of data and number of files disseminated per day for each user), 2 thresholds are defined:

* Warning: exceeded, send an email to warn the user his quota has been exceeded,
* Blacklisting: exceeded, the user is automatically blacklisted; an email is sent to the user and the administrator. The user is blacklisted until an administrator sets him as not blacklisted.

## User Management Services

Figure 4 : User Management Deployment

The User Management Component is used to manage users and groups:

* create / update / remove user
* create / delete Centre
* add group to Centre
* add user to a Centre group
* remove user from a Centre group
* blacklist / un-blacklist user
* get user information
* create / add / update / get / remove email or ftp for dissemination parameters (favourites)
* test if user is blacklisted
* get / modify user profile
* get / modify list of deployments on which the user can be backed up
* modify user’s class of services

The User Management Component uses LDAP Protocol for communicating with OpenDS.

All of User Management services are exposed to others components via EJB (exposed as Web Services).

The solutions proposed in the following text (adapted to the vGISC management) could be used for the WIS management.

We have to take into account that:

* A domain needs a local circle of trust
* Internet Area and RMDCN area need each one a circle of trust

The solution proposed runs for two Met Services with their own IdP, for example Meteo France (GISC,DCPCs,NC) and MetOffice (GISC,DCPCs,NC) or Meteo France and Spain Meteorological Center (NC).

**Example MF-MetOffice**: In the following text, the Meteo-France MetOffice circles of trust solutions illustrate the topic.

## Two levels of circle of trust

### Description

The solution that we decided to implement in the framework of the vGISC is based on two levels of COT.

Level 1:

On each side, we keep our relative circles of trust (inside the domains)

In Toulouse premises, a Circle of Trust (COT) will keep on managing the RMDCN platforms ( IDPMeteoFrance, user portal RMDCN, GISC admin portal and RMDCN DCPC Odyssey user portal), a COT Internet will gather Internet platforms( IDPMeteoFranceInternet, GISC Internet portal and DCPC Odyssey admin and user portals).

Level 2:

The idea is to create a circle of trust gathering UK and French identity and services providers.

A global Internet COT is built for SSO on Internet area.

A global RMDCN COT is built for SSO on RMDCN area.

The figure below illustrates the two levels of COT.

MetOffice

Meteo France

COT Internet

2 IdP

COT RMDCN

2 IdP

COT MetOffice Internet

COT MetOffice RMDCN

COT MF Internet

COT MF RMDCN


###

### Setup

This solution sticks to the possibility to create 2 COT for one identity and service provider. The last tests done in the Météo France premises confirm the solution.

The IdP Discovery can be located on one location only.

vGISC preferred solution:

* + - * UKMO manages the RMDCN IdP Discovery
			* Meteo France manages the Internet IdP Discovery

### Pro and Cons

Pro

* This solution is very interesting because each partner keeps its own configuration. We have just to add two new circles of trust that overlap the MF-UK area.
* The solution provides an IdpDiscovery backup
* The IdP Discovery backup can be done warmly (the two IdP Discovery running at the same time) or coldly

Cons :

* The configuration may be tricky and needs to take into account security setup at each site

# ANNEX

### LDAP Schema

Figure 5 : LDAP Schema

 “People” is a group which contains all users.

A user is defined by:

* + - Name
		- Username
		- Surname
		- Password
		- Contact email
		- Email list: list of email addresses (favourites) for dissemination
		- Address (address, zip, state, city, country)
		- Need user account
		- Black listed (true if the user if blacklisted, false otherwise)
		- Black list threshold : maximum volume of disseminated data per day
		- Profile (Admin or Operator or Registered User)
		- Class of service: Gold, Silver or Bronze.
		- Backup: list of deployments on which the user can be backed up.

GLOBAL contains groups which are known to all Centres of the Circle of Trust.

A user belongs to one or several groups of Centre or/and GLOBAL groups.

The common understanding of User Roles (GLOBAL group) corresponds to concerted decisions and actions between administrators of the different involved Centres.

### Login Glossary

#### Single Sign-On

Single Sign-On (abbreviated SSO) is a user authentication process that allows a user to enter one name and password in order to access multiple applications on this own domain.

With this property, a user logs in once and gains access to all portals, on this own domain, without being prompted to log in again at each of them.

#### Circle of Trust

A Circle of Trust (abbreviated CoT) contains one or several domains and an identity provider discovery (IdP Discovery), enabling federation between them.

#### Federation

Federation is the process that allows a user to access to all portals of the CoT if he is authorised to do it. SSO Federation is a SSO protocol for a Circle of Trust.

#### Discovery Service

The discovery service is a simple web application, deployed on a server in the Circle of Trust, and available at a secure URL (using https). It reads and writes the cookie \_saml\_idp which is created the first time the user is logged into the Circle of Trust and redirects the browser back to a defined URL corresponding to the preferred user Identity Provider.

#### Fedlet / Service Provider

The Fedlet is a streamlined Service Provider implementation of SAMLv2 single sign-on (SSO) protocols.

The Fedlet is designed to be used by Service Providers when the primary goals are to achieve single sign-on with an Identity Provider while also retrieving some user attributes from the Identity Provider.

**A Fedlet instance is included on each portal.**

In a typical OpenWIS deployment of a Partner site, several Fedlet instances are installed.

In case of federation across multiple sites, each Fedlet talks to several Identity Providers.

#### Identity Provider

An Identity Provider (abbreviated “IdP”) is a service hosted by an organisation which publishes electronic information for users that have a firm relationship with the organisation.

An “Identity Federation” is a structured co-operation between different Identity Providers. In a federation, IdPs will multilaterally exchange electronic identity information, such as names and other personal data.

OpenAM is one example of an Identity Federation.

OpenAM used SAML (Security Assertion Mark-up Language) protocol to define SSO Federation.

#### User Attributes

The user attributes become part of the SAML Response from the Identity Provider. After the user has successfully authenticated to the Identity Provider, the Identity Provider sends the SAML Response to the Fedlet.

The user attributes coming from the IdP are

* + - Name
		- Username
		- Surname
		- Contact email
		- Address (address, zip, state, city, country)
		- Need user account : (true if the user must have a local account for connect on a Centre, false otherwise)
		- Profile
		- Class of service: Gold, Silver or Bronze.
		- Backup: list of deployments on which the user can be backed up.
		- List of groups

Private information of users must reside inside the system (not distributed)

* + - Password
		- Email list: list of email addresses (favourites) for dissemination parameters. Each email is composed of an email address, an header line, an email attachment mode (To, CC, BCC), a subject, an email attachment mode (As Attachment or Embedded in Body), a file name and dissemination tool (RMDCN or Public)
		- FTP list: list of FTP destinations (favourites) for dissemination parameters. Each FTP is composed of an host, a path, a user, a password, a port, a mode (passive or not), a check file size and dissemination tool (RMDCN or Public)

#### Self Registration

The Self-Registration process is managed at portal level only.

#### Authentication

The Fedlet supports multiple Identity Providers. Additionally, the Fedlet supports the use of a separate Identity Provider Discovery Service to allow the user to select a preferred Identity Provider to authenticate against. When configured this way, the Identity Provider Discovery Service will remember the user's preferred Identity Provider, and communicate this to the Fedlet. The Fedlet will then be able to determine which Identity Provider to have the user authenticate to.