|  |
| --- |
| Projet IGO |
| Sécurité |
| Description des fonctionnalités |

|  |
| --- |
| MORIN Frédéric  21 Juillet 2014 |

# Introduction

## Objectif

Ce document présente les différents objectifs à atteindre au niveau de la sécurité et du contrôle d’accès dans IGO. Ces fonctionnalités sont découpées en différents éléments indépendants ce qui permettra un développement itératif en différentes phases afin de s’assurer que le développement progresse de façon à supporter les différentes organisations participant au développement de IGO.

IGO se compose de deux applications distinctes, la première étant le Navigateur, la deuxième étant l’outil de pilotage. Le contrôle d’accès au niveau du Navigateur et de ses services sera priorisé étant donné que cet outil s’adresse aux utilisateurs finaux alors que le pilotage s’adresse principalement aux administrateurs de système ainsi qu’aux pilotes.

## Mise en contexte

La configuration du navigateur et de son contenu s’effectue à travers le module d’intégration du Navigateur. Sa configuration est réalisée par des développeurs ainsi que par des administrateurs de système à travers un fichier XML de configuration. Ce fichier XML permet de spécifier les panneaux, les outils ainsi que les couches qui seront disponibles pour l’application. Le pilotage de son côté permet de spécifier des permissions au niveau des couches et des services.

# Authentification

L’authentification est l’aspect de la sécurité permettant de valider l’identité d’un utilisateur. L’implémentation de l’aspect authentification dans IGO devra demeurer flexible afin de permettre aux différentes organisations qui utiliseront IGO de la réaliser avec leur infrastructure existante.

Tout d’abord, il y a principalement deux options concernant l’authentification.

### Authentification en amont

Dans le cas de l’authentification en amont, l’authentification est effectuée par un système externe à l’application et les informations sur l’utilisateur sont ajoutées dans l’entête du message. Dans ce cas, l’application n’interrogera pas l’utilisateur afin de connaître son identifiant et mot de passe, et ne vérifiera pas l’exactitude de ces informations.

### Authentification dans l’application

Dans le cas de l’authentification dans l’application, l’application vérifie la correspondance entre l’identifiant et le mot de passe de l’utilisateur dans une base de données avant de donner accès à l’utilisateur à l’application.

**Requis : Permettre à l’administrateur du système de configurer le mécanisme d’authentification de IGO à travers le fichier de configuration config.php (amont = true ou amont=false)**

**Requis : Permettre à l’administrateur du système de configurer l’élément responsable de l’authentification dans l’application à travers le fichier de configuration config.php**

**Requis : Permettre au développeur d’implémenter une interface permettant de réaliser l’élément responsable de l’authentification dans l’application IGO.**

**Requis : Réaliser un exemple d’élément responsable de l’authentification dans l’application IGO.**

# Rôles

Afin de personnaliser le navigateur et l’interface de pilotage de IGO, le système doit permettre de déterminer le rôle de l’utilisateur. Certains utilisateurs seront associés à un seul rôle alors que d’autres seront associés à plusieurs rôles. Il devra leur être possible de déterminer le rôle actif afin de personnaliser le navigateur ainsi que le pilotage. Il devra aussi leur être possible de changer de rôle sans avoir à se déconnecter du système.

**Requis : Permettre aux utilisateurs qui sont associés à plus d’un rôle de déterminer le rôle actif au moment de l’accès au Navigateur.**

**Requis : Permettre aux utilisateurs qui sont associés à plus d’un rôle de changer leur rôle actif sans avoir à se déconnecter du système.**

**Requis : L’élément responsable de l’authentification sera aussi responsable de spécifier les rôles accessibles pour l’utilisateur en cours.**

L’architecture cible contient la table « igo\_role » qui permet la création de rôles IGO. L’identifiant de chacun des rôles devra être compatible.

# Autorisation

L’aspect autorisation permet de déterminer si l’utilisateur est autorisé à interroger une page ou un service. Ceci afin de demeurer le plus flexible possible pour répondre aux besoins des différentes organisations qui utiliseront IGO. Il doit être possible de spécifier que certaines pages sont accessibles au public et que d’autres pages ne sont accessibles que pour certains groupes d’utilisateurs.

**Requis : Permettre à l’administrateur de spécifier quelles pages sont accessibles de façon anonyme. (Dans fichier XML de configuration ou dans base de données?)**

**Requis : Permettre à l’administrateur de spécifier quels groupes ont accès à quelles pages.**

L’architecture cible contient les tables « igo\_services » et « igo\_service\_profil ». Ces tables permettent aux administrateurs ainsi qu’aux pilotes de déterminer quel quels profils ont accès aux différents services.

# Contrôle d’accès

Le contrôle d’accès est l’aspect de la sécurité qui valide qu’un utilisateur puisse accéder, modifier, créer ou effacer des éléments d’informations.

Le contrôle d’accès au niveau de IGO se situe au niveau des couches disponibles dans le système. Chacune des couches pourra être :

* Lue -> Visualisé avec un Service WMS
* Analysée -> Analysée avec le service d’analyse spatiale
* Ecriture -> Modifiée par le service d’édition en ligne
* Exporté -> Exportée et téléchargé par l’utilisateur

L’architecture cible contient la table igo\_permission qui permet d’associer les permissions de lecture, analyse, écriture et exportation à une couche, ou un groupe de couche et un profil.

**Requis : Permettre à l’administrateur de donner des droits de lecture à un profil pour une couche ou un groupe de couche.**

**Requis : Permettre à l’administrateur de donner des droits d’analyse à un profil pour une couche ou un groupe de couche.**

**Requis : Permettre à l’administrateur de donner des droits d’écriture à un profil pour une couche ou un groupe de couche.**

**Requis : Permettre à l’administrateur de donner des droits d’exportation à un profil pour une couche ou un groupe de couche.**

### Visualisation des couches

Lors de l’accès aux couches, un module de sécurité « proxy » doit sécuriser l’accès aux couches d’informations.

**Requis : Les couches qui ne peuvent être lue par le profil courant de l’utilisateur doivent être sécurisés afin de l’assurer qu’un utilisateur malveillant ne puisse y avoir accès.**

### Personnalisation des couches du Navigateur

Les couches disponibles dans le navigateur devront être personnalisées selon le profil courant de l’utilisateur. Les couches qui ne peuvent être visualisées par l’utilisateur selon son profil courant ne devront pas être ajoutées à l’interface utilisateur.

**Requis : Les couches qui ne peuvent être lues par le profil courant de l’utilisateur ne doivent pas être ajoutées dans le Navigateur.**

### Analyse spatiale

Un contrôle d’accès doit être effectué au niveau des fonctionnalités d’analyse spatiale. L’architecture cible prévoit déjà la réalisation de cet aspect de la sécurité, cependant l’analyse spatiale est en cours de développement. L’aspect sécurité sera donc réalisé dans une phase subséquente.

Note : L’analyse spatiale devra pouvoir se baser sur les méta données de la base de données. Migrer les méta données existantes dans le nouveau schéma d’analyse spatiale.

Discussion : Discuter avec François afin de savoir quelle est sa vision concernant les méta données d’analyse spatiale. Classifications, Classe d’entités, Attributs.

# Authentification interministérielle

Dans un monde idéal, certaines couches et certains services pourraient être hébergés par un ministère et utilisés par plusieurs ministères. Dans le cas où on voulait sécuriser l’accès à ces couches par profils, un mécanisme d’authentification interministérielle à identification unique (Single Sign-On) devrait être implémenté.

# Priorités

Le développement des fonctionnalités de sécurité de IGO sera exécuté en différentes phases selon les priorités.

### Phase 1

Les fonctionnalités suivantes devront être implémentées dans une première phase :

1. Authentification
   1. Permettre à l’administrateur de configurer le mécanisme d’authentification dans IGO.
      1. Permettre de se fier à l’authentification en amont.
   2. Permettre à l’utilisateur d’entrer son identifiant et son mot de passe.
   3. Permettre au développeur d’implémenter un composant personnalisé pour valider l’authentification de l’utilisateur.
   4. Implémenter un composant permettant de valider l’authentification de l’utilisateur dans le LDAP du Ministère de la Sécurité publique.
2. Rôle
   1. Permettre à l’utilisateur de déterminer son rôle actif.
3. Autorisation
   1. Permettre à l’administrateur de rendre des pages de navigateur accessibles sans authentification.
   2. Permettre à l’administrateur de configurer quels profils a accès aux différentes configurations de Navigateur.
   3. Sécuriser l’accès aux ressources (URL) avec un « Front controller Phalcon »
4. Contrôle d’accès
   1. Permettre à l’administrateur de spécifier quels profils ont les droits de lecture sur quelles couches.
   2. Ne pas ajouter les couches qui ne possèdent pas les droits de lecture pour le profil courant dans le navigateur.
   3. Sécurisé l’accès aux couches selon les permissions de lecture afin qu’un utilisateur malveillant ne puisse y avoir accès.

### Phase 2

### Un mécanisme devra être mis en place afin de synchroniser les permissions et l’accès aux services entre l’environnement de pré production et l’environnement de production.

### Phase 3

Analyse spatiale

Exportation

Édition en ligne

### Phase 4

Authentification interministérielle

# Plan de version

