

(Remplir cette partie à l'aide de la notice)

Concours / Examen : ISIC PAL Recrutement :  
Epreuve : Cas pratique Spécialité : Sujet 1 Session : 2023

CONSIGNES

- Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.
- Ne pas signer la composition et ne pas y apporter de signe distinctif pouvant indiquer sa provenance.
- Numéroté chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.
- Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.
- N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.

## Note de lancement du projet d'identité unique (INU)

### Plan

- 1 - Contexte
- 2 - Objectifs et Enjeux
- 3 - Mise en oeuvre du projet
- 4 - Macro Planning
- 5 - Risques
- 6 - Avantages / Contraintes
- 7 - Impact sur les directions métiers

### 1- Contexte

L'accélération de la mobilité et de l'usage des services numériques dans le ministère depuis la crise du Covid-19, le recours massif au télétravail, la recrudescence des risques cyber depuis fin 2021 et la multitude d'identités numériques à gérer pour délivrer ses services aux utilisateurs (agents, externes, ayants droits et citoyens) pousse le ministère à rationaliser l'ensemble et converger vers une identité numérique unique (INU).

## 2- Objectifs et Enjeux

Les objectifs du projet INU sont :

- rationaliser les identités des agents en évitant qu'elles soient définies à plusieurs endroits avec des méthodes d'authentification et des mots de passe différents pour les services du ministère mais aussi dans un second temps pour les services de l'Etat, auxquels ils accèdent.

- renforcer la sécurité <sup>avec</sup> de l'authentification à multiples facteurs pour tous les agents.

- s'inscrire dans le processus de modernisation de l'Etat en se raccordant à France Connect Agent en tant que fournisseur d'identité pour ~~simplifier~~ simplifier l'usage des services de l'Etat à nos agents.

## 3- Mise en oeuvre du projet

Cette partie propose de présenter d'un point de vue macro les éléments du projet permettant de mieux apprécier le parti sur les avantages et contraintes de la partie 6.

### 3.1 Solution

On propose de mettre en oeuvre une fédération d'identité (ou fournisseur d'identité) s'appuyant sur les protocoles Open ID Connect s'appuyant sur des briques Open Source (type Keycloak) totalement compatible avec les services de France Connect Agent.

Cette solution permet de faire de l'authentification à multiples facteurs (mot de passe, SMS, empreinte digitale, email, carte à puce, ...). On propose que l'authentification soit à 2 facteurs pour les agents utilisateurs (mot de passe + carte à puce ou mot de passe + sms) et à 3 facteurs pour les utilisateurs "sensibles" de type administrateurs (mot de passe + carte à puce + empreinte digitale).

L'identité numérique de l'agent contiendra les attributs suivants : nom, prénom, identifiant login, carte agent, matricule, ~~adresse~~. Par exemple, seul les trois premiers attributs sont fournis par défaut dans le jeton d'authentification attestant son identité (voir FS: Document 3).

La fédération d'identité peut être vue comme un simplificateur du SI du ministère. Néanmoins, la centralisation de son identification et de l'authentification en un seul point, est risqué, il faut absolument éviter qu'un incident sur ce point bloque toutes les authentifications du ministère. Il faut mettre en oeuvre des mécanismes de haute disponibilité sur ce système.

Le dernier point est la revue de la méthode d'authentification de toutes les applications des directions métiers nécessitant de l'authentification. Ce chantier à traiter au cas par cas peut être assez lourd en adaptation du développement suivant l'âge de l'application (pour utiliser le protocole OpenID Connect) et ses interactions avec les annuaires fournissant les droits des utilisateurs. Suivant le volume d'adaptation, la recette des métiers et le déploiement des applications pourront être adaptés de l'application auront des impacts sur les directions métiers.

## 3.2 Architecture cloud

Depuis juin 2021, la doctrine de l'Etat "Cloud au centre" impose que les nouveaux projets des ministères soient pensés et déployés sur cloud parmi les clouds internes, les clouds EcNum, Cloud et les clouds commerciaux.

Le projet de déploiements de fédération d'identité se prête bien à une exploitation dans un cloud interne géré par l'Etat. Aujourd'hui, il existe deux clouds internes celui de la DGFIP "Nubo" et celui du ministère de l'Intérieur "Pi".

On propose, après choix du cloud "Nubo" ou "Pi", de partir sur le déploiement sur deux sites au sein du même cloud, un site principal qui traite l'ensemble des requêtes et site secondaire capable de basculer en primaire en quelques secondes en mode PCA (Plan de continuité d'activité). Cette architecture pourrait évoluer plus tard en l'ajout d'un nouveau site sur le 2<sup>e</sup> cloud.

## 3.3 Méthode de projet

Quand on travaille sur des clouds, il convient de travailler en méthodologie DevOps (constitution d'équipe pluridisciplinaire contenant des personnes de ~~métiers~~ métiers, du développement et de l'exploitation travaillant en agilité).

On propose que les phases de réalisations et finalisation soit traitées en méthode agile.

## 3.4 Conduite du changement

Comme ce projet va toucher tous les utilisateurs (ajouts) du ministère, il convient de mettre en place une conduite du changement au plus tôt.

(Remplir cette partie à l'aide de la notice)

Concours / Examen : ISIC PAL Recrutement : .....

Epreuve : Cas pratique Spécialité : Sujet 1 Session : 2023

**CONSIGNES**

- Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.
- Ne pas signer la composition et ne pas y apporter de signe distinctif pouvant indiquer sa provenance.
- Numéroté chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.
- Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.
- N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.

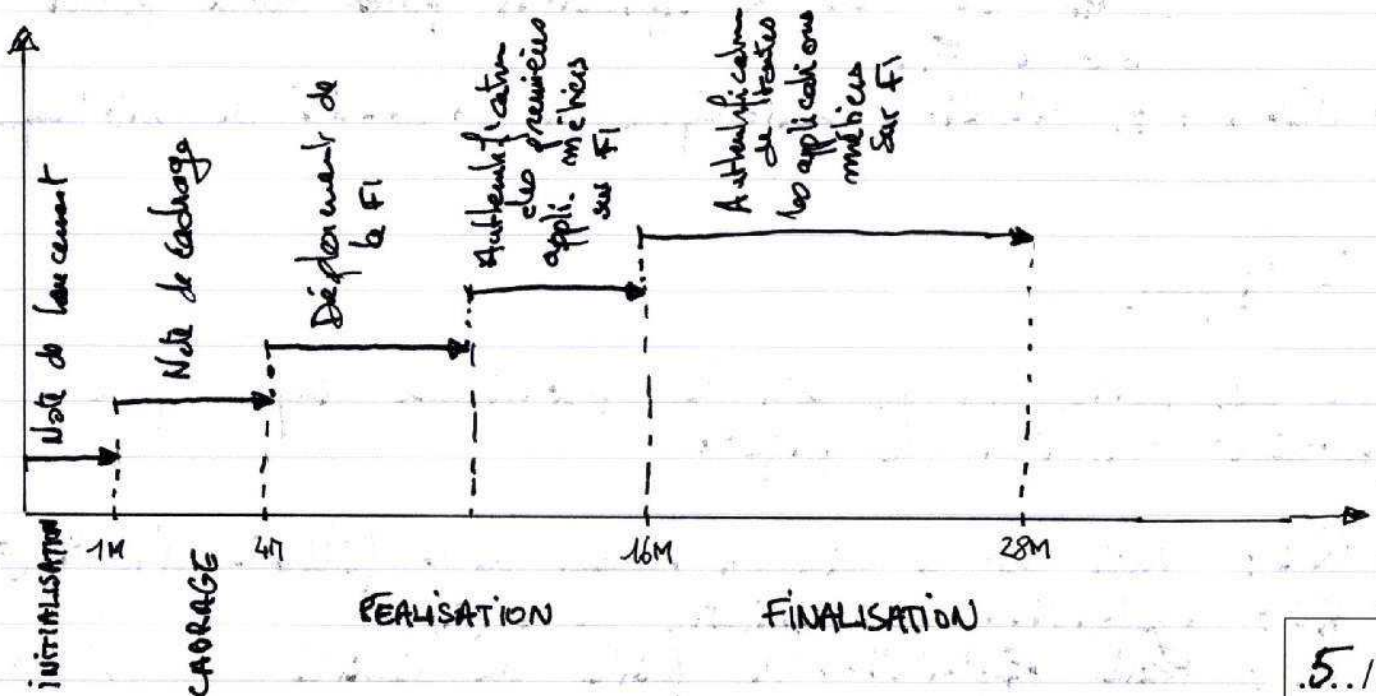
Cette conduite de changement pourra se matérialiser par la mise en place d'un comité des utilisateurs possédant au moins un utilisateur de chaque direction métier.

Le comité pourra aider à la conception des processus de création des identités que l'on a pas encore évoqués.

Comme il va s'appliquer à chaque agent à l'ouverture de la fédération d'identité, il faudra qu'il soit le plus efficient possible pour les gestionnaires de ce processus et par les directions métiers.

4 - Macro Planning

Le planning est composé de 4 phases qui se déroulent de manière séquentielle :



### Phase 1 : Initialisation

- Durée : 1 mois
- Livrable : Note de lancement
- Jalons : validation par le comité d'investissement

### Phase 2 : Cadrage

- Durée : 3 mois
- Livrable : Cahier des charges
- Jalons : validation par le comité de direction

### Phase 3 : Réalisation

- Durée : 12 mois
- Livrable : - la fédération d'identité (FI)  
- VABF de d'au moins 3 applications par direction métier <sup>passé sur FI</sup>
- Jalons :  $\emptyset$ , validation périodique par un comité de pilotage

### Phase 4 : Finalisation

- Durée : 12 mois
- Livrable : - Documentation de la FI (Exploitation)  
- VABF de toutes les applications ~~passé~~ devant passer sur la FI.
- Jalons :  $\emptyset$ , validation périodique par un comité de pilotage

## 5 - Risques

Dans cette partie, on va tester les principaux risques que pourraient rencontrer le projet.

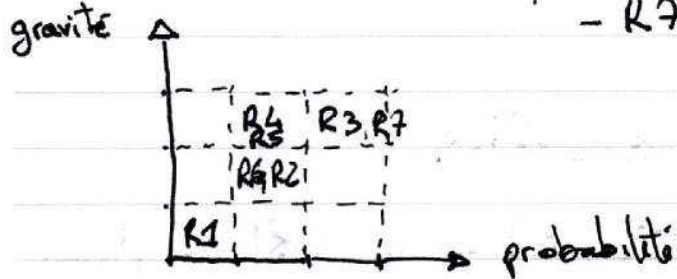
- R1 : Retard sur la mise en oeuvre de la fédération d'identité (FI)
- R2 : Dysfonctionnement applicatif de la (FI)
- R3 : ~~Problème~~ Exploitation de failles de sécurité

- R4 Processus de création de nouvelle identité numérique unique (INU) trop lourd

- R5 Mauvaise tenue à la charge

- R6 Retard de l'adaptation technique des applicatifs

- R7 Refus des poids du projet à supporter par les directions métiers



Le positionnement des risques sur une échelle de gravité, probabilité nous montre la sensibilité au risque de ce projet, il faudra donc mettre en place un comité de suivi et de maîtrise des risques.

## 6- Avantages / Contraintes

### 6.1 Avantages

- A l'état de l'art concernant, l'identité numérique et l'authentification
- Possibilité de se raccorder par la suite à France Connect Agent pour accéder aux nouveaux services de la DNUM (comme Asmose).
- Centralisation et meilleure maîtrise du processus de création de compte et d'identité.
- En investissant sur cette solution, il est possible d'obtenir pour certains actes, un très haut niveau de sécurité.
- Les journaux de log des authentifications se trouvent qu'à un seul endroit

### 6.2 Contraintes

- La centralisation de l'authentification en fait un point critique pour le ministère et impose de bien gérer la disponibilité et la sécurité du dispositif sous peine de voir dégrader .7.1.8..

l'état de service complet de son SI.

- La création du processus de création d'identité numérique unique est sensible d'un point de vue légal et se joue dans le temps.
- Le coût et l'accompagnement utilisateurs et technique sera important pour les directions métiers.

## 7. Impacts ~~et~~ sur les directions métiers

Le paradoxe est que ce projet très technique dans sa phase de réalisation a un impact fort sur les utilisateurs (agents) et donc sur les directions métiers.

Pour chaque direction métier, il va falloir recenser quelles sont les applications qui ont besoin d'authentification par les agents et qui doivent passer sur la fédération d'identité (FI).

L'adaptation technique à supporter sera très différente d'une application à l'autre suivant l'âge et la technologie de l'application, ses adhérences aux annuaires et ses besoins d'échanges avec l'application de manière sécurisée.

Ces adaptations viendront "ponctionner" les budgets informatiques de maintenance des directions métiers. Elles demanderont aussi des moyens de recette utilisateurs car bien souvent les applications lourdes à adapter n'ont pas de test unitaires et la recette avant mise en production doit se faire de façon manuelle.

Pour ce projet, il convient de bien adapter la communication et la conduite du changement avec les directions métiers.