Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

EXAMEN PROFESSIONNEL DE VERIFICATION D'APTITUDE AUX FONCTIONS D'ANALYSTE-DEVELOPPEUR

1ERE SESSION 2019

❖❖❖

EPREUVE ECRITE D'ADMISSIBILITE

DU MERCREDI 16 JANVIER 2019

ETUDE D'UN CAS D'AUTOMATISATION PERMETTANT D'APPRECIER LA CONNAISSANCE DES TECHNIQUES D'ANALYSE, L'APTITUDE A LA SYNTHESE, A LA REDACTION D'UN DOSSIER TECHNIQUE ET SUPPOSANT EVENTUELLEMENT DES CONNAISSANCES EN MATIERE DE PROGRAMMATION

(Durée : 6 heures)

Remarques importantes :

- l'usage de règles à calcul, de tables de logarithmes et de tout document est strictement interdit.
- l'usage de la calculatrice non programmable est autorisé.
- les copies doivent être rigoureusement anonymes et ne comporter aucun signe distinctif ni signature, même fictive, sous peine de nullité.
- le candidat s'assurera, à l'aide de la pagination, qu'il détient un sujet complet (le sujet comporte 9 pages et 1 page de garde).

TOUTE NOTE INFERIEURE A 10 SUR 20 EST ELIMINATOIRE

Table des matières

1. Sujet à traiter

Le sujet concerne la mise en place du Fichier des Personnes Recherchées (FPR) au profit des services régaliens de l'État :

- L'**environnement** de ce fichier sera présenté comme suit **(1.1.)** :
  - description du FPR ***(1.1.1.)*** ;
  - problématiques d'identification et d'authentification avec FranceConnect Agent[1] ***(1.1.2.)*** ;
  - présentation succincte d'un système tiers, le N-SIS II (système d'information Schengen II) ***(1.1.3.)***.

- Une **référence réglementaire** interministérielle sur la protection du secret de la défense nationale sera ensuite fournie pour prendre en compte les risques relatifs à la sécurité des systèmes d'information (SSI) **(1.2.)**.

1.1 Environnement

1.1.1 Description du FPR

Chiffres clés : le fichier FPR contient environ 620 000 fiches actives.

Qu'est-ce que ce fichier informatique ?

En recensant toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique, le FPR sert à faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives

À quoi sert ce fichier ?

En recensant toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique, le FPR sert à faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives.

Qui est responsable de ce fichier ?

Le ministère de l'intérieur.

Que contient ce fichier ?

Les informations enregistrées sont :

- l'identité de la personne recherchée ;
- son signalement et éventuellement sa photographie ;
- le motif de la recherche ;
- la conduite à tenir en cas de découverte des personnes recherchées.

[1] FranceConnect est un dispositif permettant de garantir l'identité d'un utilisateur en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée. Ce dispositif est un bien commun mis à la disposition de toutes les autorités administratives. Il est mis en œuvre par la DINSIC, un service du premier ministre. Certains acteurs du secteur privé peuvent aussi en bénéficier s'ils contribuent à l'action publique (banques et assurances par exemple).

Le FPR est divisé en vingt et un sous-fichiers regroupant les personnes concernées en fonction du fondement juridique de la recherche.

Exemple de catégories :

- *« E » (police générale des étrangers),*
- *« IT » (interdiction du territoire),*
- *« R » (opposition à résidence en France),*
- *« TE » (opposition à l'entrée en France),*
- *« AL » (aliénés),*
- *« M » (mineurs fugueurs),*
- *« V » (évadés),*
- *« S» (Sûreté de l'État),*
- *« PJ » (recherches de police judiciaire),*
- *« T » (débiteurs envers le Trésor)...*

Quels sont les critères d'inscription dans ce fichier ?

L'inscription au FPR intervient pour des motifs :

- **judiciaires** (exécution de mandats, de condamnation, d'un contrôle judiciaire, enquête de police judiciaire, etc.) ;
- **administratifs** (application de réglementations spécifiques de police administrative : étrangers — *ex. mesure d'expulsion, opposition à l'entrée sur le territoire* — législation fiscale, protection des personnes — *ex. recherches de personnes disparues à la demande d'un membre de leur famille, etc.*) ;
- **d'ordre public** (prévention de menaces contre la sécurité publique ou la sûreté de l'État) ;

Sans donner lieu à inscription, le FPR est également consulté lors de l'instruction des demandes de carte nationale d'identité, de passeport, de titre de séjour ou encore de visa.

Qui peut procéder à une inscription ?

Les services dûment habilités de la direction générale de la police nationale ou la direction générale de la gendarmerie nationale, ainsi que, dans le cadre de leurs attributions, les préfectures.

La mise à jour des informations est réalisée à l'initiative du service ayant demandé l'inscription. La radiation des personnes inscrites doit en particulier être effectuée sans délai en cas de découverte ou d'extinction du motif de la recherche.

Combien de temps sont conservées les informations ?

- Les durées de conservation dépendent du motif d'enregistrement.
- Les radiations sont opérées sans délai en cas de découverte de la personne ou d'extinction du motif de l'inscription.

Qui peut consulter ce fichier ?

Peuvent seuls être destinataires de la totalité ou d'une partie de ces informations dans le cadre de leurs compétences :

- les autorités judiciaires ;
- les services de police, de gendarmerie et des douanes ;
- les autorités administratives pour les seules recherches relevant de leurs attributions ;

- les services de police d'Etats liés à la France par une convention ou un accord international leur autorisant l'accès à tout ou partie des informations enregistrées dans le fichier des personnes recherchées. […]

1.1.2 Problématiques d'identification et d'authentification avec FranceConnect Agent

FRANCECONNECT SE DECLINE EGALEMENT POUR LES AGENTS DE LA FONCTION PUBLIQUE

Le Ministère de l'Intérieur et la DINSIC conduisent une expérimentation autour d'un FranceConnect Agent (FCA). Par rapport à FranceConnect Particulier, le futur dispositif introduit une nouvelle dimension : la notion de rôle et d'habilitation des agents.

La problématique de la gestion des identifiants et des mots de passe pour accéder aux services publics en ligne n'est pas la panacée de l'internaute particulier. Elle concerne également les agents des services publics. En l'occurrence tous ceux qui doivent s'authentifier dans le cadre de leur mission auprès de multiples applications dont la gestion ne relève pas de leur administration d'appartenance. Or la gestion de ces différentes identités numériques complexifie grandement le parcours numérique des agents.

C'est dans ce contexte que la DINSIC et le Ministère de l'Intérieur étudient en ce moment la faisabilité d'une déclinaison de l'actuel FranceConnect en un FranceConnect Agent. Son but : garantir aux agents un mode d'accès unique (basé sur l'identifiant et le mot de passe utilisé au sein de leur administration) à l'ensemble des applications et services opérés à l'extérieur de leur administration d'appartenance.

DES OPENSLAB ET UNE EXPERIMENTATION

Après une phase d'étude ponctuée par 5 openlab, qui ont mis en évidence les principaux irritants et ont permis d'envisager une architecture cible, les deux partenaires conduiront en fin d'année un POC autour de FranceConnect Agent. Passage en revue des différents composants du dispositif. […]

PRINCIPAL ENJEU : LA GESTION DES HABILITATIONS

Si les deux FranceConnect visent à identifier et à authentifier des personnes physiques, FranceConnect Agent comporte une dimension supplémentaire : la notion d'habilitation, grâce à laquelle un agent est autorisé ou non à accéder aux services. Cette composante est sûrement le volet le plus délicat de FranceConnect Agent. Elle en conditionne d'ailleurs son architecture.

Une gestion propre à chaque administration

En premier lieu, la gestion des droits et des habilitations est propre à chaque organisation publique. Elle implique différents volets, notamment des règles d'ordre politique (qui accède à quoi, qui autorise qui et dans quel cadre,...), sémantique (notions de rôles, profils, métiers, fonctions,...) ou technique (annuaires centralisés ou multiples...). Au final, la gestion des droits n'a jamais fait l'objet d'une normalisation entre organismes publics.

Autre difficulté : **la notion même de rôle est parfois protéiforme**. A l'image d'un agent au service de l'Etat qui serait également maire élu de sa commune, une personne peut cumuler plusieurs rôles. Sans compter enfin que ces rôles évoluent dans le temps (mutation ou délégation temporaire d'une nouvelle fonction de l'agent) entraînant une source de vulnérabilité des systèmes. En cause : la non désactivation ou suppression systématique des comptes des agents lorsque ceux-ci ne disposent plus d'accréditations.

UNE GESTION DES HABILITATIONS AU PLUS PRES DE L'AGENT

Dans ce contexte, FranceConnect Agent introduit un nouveau type d'acteur : le fournisseur d'habilitation (FH). Ce dernier est situé au plus près de l'agent, c'est à dire au sein de son administration (ou opérateur de mutualisation dans les territoires). Généralement, il est couplé au FI (fournisseur d'identité), une fonction là aussi assurée par l'administration de l'agent. D'ailleurs, même si ces fonctions (FH et FI) sont distinctes, celles-ci partagent souvent la même infrastructure technique. Cette proximité avec l'agent garantit au couple FI / FH d'être perpétuellement à jour des mouvements et changement d'affectation des agents.

Mais quel est le rôle exact de ce couple FI/FH ?

Il communique les caractéristiques de l'agent au fournisseur de service (FS) qui lui permettront, sur la base de sa propre politique d'accès, de vérifier que cet agent est bien autorisé à solliciter son service. Cet échange entre FH et FS sera réalisé par le biais de FCA qui agit ici comme un tiers de confiance.

Autre caractéristique primordiale sans laquelle le FS ne saurait interpréter les données reçues : tous les FH partie-prenante dans FranceConnect Agent se seront au préalable alignés sur une norme technique d'échange rendant interopérables les caractéristiques de l'agent entre FI/FH et FS. Cette norme, ou grammaire commune, sera élaborée au cours du projet FCA qui suivra le POC.

DEVELOPPER UN CERCLE DE CONFIANCE ENTRE FOURNISSEURS D'HABILITATION ET DE SERVICES

On l'aura compris, **FranceConnect Agent ne se substitue pas au système de gestion des droits des fournisseurs de services** qui restent maîtres de leur politique d'accès. En revanche, il garantit un cercle de confiance entre les agents, leur administration et les services externes sur lesquels ils cherchent à se connecter.

Il permet surtout à ces mêmes administrations de simplifier la gestion des comptes d'agents externes à leur organisation. Coté utilisateur, la promesse est bien la même que celle de FranceConnect Particulier : faciliter drastiquement la connexion aux services externes en s'affranchissant du foisonnement d'identifiants et de mots de passe à retenir.

1.1.3 Système d'information Schengen II (SIS II)

Le SIS II a pour objet de permettre aux Etats membres de l'espace Schengen de mettre en place une politique commune de contrôle des entrées dans l'espace Schengen et, ainsi, de faciliter la libre circulation de leurs ressortissants tout en préservant l'ordre et la sécurité publics.

70 millions de signalements en 2015 dans la base de signalements C-SIS II

En juillet 2016, les signalements relatifs à des personnes s'élevaient au nombre de 810 640 dans le SIS II dont 115 621 ont été inscrits par des services français.

La finalité principale de la base de données est d'assurer un niveau de sécurité élevé au sein des États Schengen en l'absence de contrôles aux frontières intérieures, en permettant aux autorités nationales compétentes, comme les forces de police et les gardes-frontières, de saisir et de consulter des signalements concernant des personnes ou des objets. [...]

Qui est le responsable du fichier ?

Le ministère de l'intérieur, direction générale de la police nationale.
[...]

Informations contenues dans ce fichier

Le système d'information Schengen de deuxième génération («SIS II») est une grande base de données qui contient des informations sur des personnes recherchées ou disparues, des personnes sous surveillance policière et des personnes non ressortissantes d'un État membre de l'espace Schengen auxquelles l'entrée sur le territoire Schengen est interdite, ainsi que des informations sur des véhicules et objets volés ou disparus, comme des documents d'identité, des certificats d'immatriculation de véhicules et des plaques d'immatriculation de véhicules.
[...]

Qui peut procéder à une inscription ?

Chaque Etat membre désigne une instance (« l'office N.SIS II ») qui assume la responsabilité centrale du N.SIS II. Les données du SIS II sont introduites, mises à jour, supprimées et consultées par le biais des systèmes N.SIS II de chaque Etat membre. Chaque Etat membre transmet ses signalements par l'intermédiaire de son office N.SIS II.

Les signalements effectués par l'Etat français dans le N.SIS II découlent des signalements introduits dans le FPR, le fichier des objets volés et signalés (FOVeS), le fichier des titres électroniques sécurisés (TES) et DOCVERIF.
[...]

1.2 Référence réglementaire

Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale

[…]

TITRE V - MESURES DE SECURITE RELATIVES AUX SYSTEMES D'INFORMATION

[…]

Chapitre 2 : La protection des systèmes d'information

Art. 88 : Principes généraux de protection des systèmes d'information

L'objectif général de la protection d'un système d'information est de garantir l'intégrité, l'authenticité, la confidentialité et la disponibilité des informations traitées par ce système. La protection d'un système d'information s'appuie sur des principes portant sur l'organisation et sur les moyens techniques, auxquels s'ajoutent des principes de défense en profondeur. Ces principes doivent être respectés strictement dès lors que le système est susceptible de traiter des informations classifiées.

1) Principes relatifs à l'organisation

Ces principes comprennent :

- **la prise en compte de la sécurité** : la sécurité du système d'information doit être prise en compte dans toutes les phases de la vie du système, sous le contrôle de l'autorité d'homologation, notamment lors des études de conception et de spécification du système, tout au long de son exploitation et lors de son retrait du service ;
- **la politique de sécurité du système d'information** : une politique de sécurité définissant les principes et les exigences, techniques et organisationnels, de sécurité du système doit être établie et approuvée par l'autorité d'homologation. Cette politique s'appuie sur une gestion des risques prenant en compte les menaces pesant sur le système et sur les informations, et les vulnérabilités identifiées sur le système ;

- **l'homologation du système** : tout système doit être homologué par une autorité désignée conformément à l'article 90 avant sa mise en service opérationnel ;
- **l'organisation de la chaîne des responsabilités** : il convient d'identifier clairement les personnes qui ont des responsabilités dans la sécurité du système d'information, de les habiliter au niveau requis et de veiller à les informer des menaces pesant sur le système et sur les informations ;
- **le contrôle de la sécurité du système en phase d'exploitation** : la mise en œuvre des mesures de sécurité et le respect des conditions dont est assortie l'homologation sont contrôlés tout au long de l'exploitation du système d'information notamment en conduisant régulièrement des audits de sécurité ;
- **la gestion des incidents de sécurité** : des procédures de détection et de traitement des incidents de sécurité susceptibles d'affecter la sécurité du système d'information doivent être mises en place. Il est rendu compte à l'autorité d'homologation des incidents rencontrés et des moyens mis en œuvre pour leur traitement. L'ANSSI est tenue informée des incidents et de leurs caractéristiques techniques affectant les systèmes d'information traitant d'informations classifiées.

2) Principes relatifs aux moyens techniques

Ces principes comprennent :

- **la protection technique du système** : le système d'information doit être conçu de manière à protéger l'information qu'il traite et à garantir son intégrité, sa disponibilité et la confidentialité des informations sensibles relatives à sa conception et à son paramétrage de sécurité ;
- **la gestion des composants sensibles du système** : une gestion des ACSSI et des autres composants sensibles du système d'information doit être mise en place, permettant d'en assurer la traçabilité tout au long de leur cycle de vie, conformément à l'article 91 ;
- **la protection physique du système** : les mesures de protection physique d'un système d'information doivent être appliquées ;
- **la gestion et le contrôle des accès au système** : le système d'information doit être conçu et géré de manière à ne permettre son accès qu'aux seules personnes ayant le niveau d'habilitation requis et le besoin d'en connaître ;
- **l'agrément des dispositifs de sécurité** : des dispositifs de sécurité agréés par l'ANSSI conformément à l'article 89 du présent chapitre doivent être utilisés.

3) Principes de défense en profondeur

La protection d'un système d'information nécessite d'exploiter tout un ensemble de techniques de sécurité, afin de réduire les risques lorsqu'un composant particulier de sécurité est compromis ou défaillant. Cette défense en profondeur se décline en cinq axes majeurs :

- **prévenir** : éviter la présence ou l'apparition de failles de sécurité ;
- **bloquer** : empêcher les attaques de parvenir jusqu'aux composants de sécurité du système ;
- **contenir** : limiter les conséquences de la compromission d'un composant de sécurité du système ;
- **détecter** : pouvoir identifier, en vue d'y réagir, les incidents et les compromissions survenant sur le système d'information ;
- **réparer** : disposer de moyens pour remettre le système en fonctionnement et en conditions de sécurité à la suite d'un incident ou d'une compromission.

[…]

2. Définitions et précisions

2.1 POC

Une preuve de concept (de l'anglais : *proof of concept*, POC) ou démonstration de faisabilité, est une réalisation expérimentale concrète et préliminaire, courte ou incomplète, illustrant une certaine méthode ou idée afin d'en démontrer la faisabilité.

Située très en amont dans le processus de développement d'un produit ou d'un process nouveau, la preuve de concept est habituellement considérée comme une étape importante sur la voie d'un prototype pleinement fonctionnel.

2.2 Photo des individus

Les objets binaires ne sont pas stockés en base de données. En effet, ceci est une mauvaise pratique.

Un stockage objets (stockage cloud) sera utilisé au sein de l'architecture. Ainsi, on trouvera au minimum en base l'URL desdites photos.

2.3 Stockage objets

Du point de vue de l'utilisateur, c'est un webservice utilisable afin d'y stocker et publier des fichiers statiques. Ce mécanisme est utilisé notamment par des produits publics tels que *Google Photos* ou *Microsoft OneDrive*.

Au niveau de l'architecture, c'est un ensemble de serveurs web regroupés derrière un répartiteur de charge.

3. Travail à faire

3.1 Étude du rôle de l'application

Avec les documents fournis, vous expliquerez de manière concise les enjeux et les contraintes fonctionnelles et techniques de l'application. Les acteurs, les applications externes et des cas d'utilisation seront également abordés.

3.2 Modélisation statique de l'application

Vous réaliserez la modélisation des données de l'application.

3.3 Étude de fonctionnalités

Vous modéliserez l'activité d'insertion d'une fiche. Ensuite, vous représenterez les écrans nécessaires à l'insertion d'une fiche dans le fichier.

3.4 Architecture de la solution

Après avoir présenté les risques SSI selon les quatre piliers de la sécurité des systèmes d'informations (DICT), à savoir : Disponibilité, Intégrité, Confidentialité et Traçabilité, vous décrierez la stratégie employée afin de construire l'architecture de votre application.

Ensuite vous produirez un schéma qui décrit l'implémentation logique de l'application.

Enfin, les centres d'hébergement disponibles proposent une offre cloud unifiée et pilotée par la DINSIC, vous expliquerez l'intérêt d'utiliser des ressources interministérielles multiples.

3.5 Analyse de données

Vous fournirez sous forme d'un pseudo-code ou d'une requête SQL :

- le nombre de fiches contenues dans le logiciel ;
- le top 5 des types de fiches inscrites.