MINISTÈRE
DE L'ÉDUCATION
NATIONALE

Liberté
Égalité
Fraternité

EDE ISI 2

SESSION 2025

CAPET ET CAFEP
Concours externe

Section
ÉCONOMIE ET GESTION

Option
Informatique et systèmes d'information

Épreuve écrite disciplinaire appliquée

L'épreuve porte sur l'enseignement de sciences de gestion.
Elle a pour but d'évaluer l'aptitude du candidat à concevoir et à organiser une séquence pédagogique sur la thématique proposée en exploitant de façon critique et argumentée un dossier documentaire fourni.
Le sujet de l'épreuve est spécifique à l'option choisie.

Durée : 5 heures

Sont autorisés les matériels suivants :

- **Le lexique SQL**, sans commentaire ni exemple d'utilisation des instructions.
- **La règle à dessiner les symboles** informatiques.

L'usage de tout autre ouvrage de référence, de tout dictionnaire et de tout matériel électronique (y compris la calculatrice) est rigoureusement interdit.

Il appartient au candidat de vérifier qu'il a reçu un sujet complet et correspondant à l'épreuve à laquelle il se présente.

Si vous repérez ce qui vous semble être une erreur d'énoncé, vous devez le signaler très lisiblement sur votre copie, en proposer la correction et poursuivre l'épreuve en conséquence. De même, si cela vous conduit à formuler une ou plusieurs hypothèses, vous devez la (ou les) mentionner explicitement.

NB : Conformément au principe d'anonymat, votre copie ne doit comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé consiste notamment en la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de la signer ou de l'identifier.
Le fait de rendre une copie blanche est éliminatoire.

A

Tournez la page S.V.P.

INFORMATION AUX CANDIDATS

Vous trouverez ci-après les codes nécessaires vous permettant de compléter les rubriques figurant en en-tête de votre copie. Ces codes doivent être reportés sur chacune des copies que vous remettrez.

CAPET EXTERNE - ÉCONOMIE ET GESTION

Option : Informatique et systèmes d'information

► Concours externe du CAPET de l'enseignement public

Concours	Section/option	Epreuve	Matière
EDE	8031E	102	9312

► Concours externe du CAPET de l'enseignement privé

Concours	Section/option	Epreuve	Matière
EDF	8031E	102	9312

IMPRIMERIE NATIONALE – 25 0229 – D'après documents fournis

CAPET Économie et gestion – Option Informatique et systèmes d'infromation
Épreuve écrite disciplinaire appliquée
Session 2025

Structure du sujet

Le sujet porte sur une exploitation pédagogique en section de techniciens supérieurs (STS) Services informatiques aux organisations (SIO). La candidate ou le candidat traitera l'un des deux sujets suivants, en indiquant clairement son choix sur sa copie.

Sujet A – Exploitation pédagogique option « Solutions d'infrastructure, systèmes et réseaux » - SISR

Sujet B – Exploitation pédagogique option « Solutions logicielles et applications métier » - SLAM

La documentation est structurée de la façon suivante

Dossier documentaire commun

Document 1	Acquis des étudiantes et étudiants en première année de STS SIO
Document 2	Extraits du référentiel du BTS Services informatiques aux organisations
Document 3	Contexte organisationnel du ministère de l'Europe et des Affaires étrangères

Dossier documentaire spécifique au sujet A

Document A.1	Dossier d'infrastructure du système d'information de France-Visas
Document A.2	Politique de gestion des mots de passe de France-Visas
Document A.3	Recommandations de l'ANSSI relatives aux mots de passe, à l'administration à distance et nomadisme
Document A.4	Schéma de l'infrastructure du portail *web* de France-Visas
Document A.5	Protection des données sensibles accessibles par les services web
Document A.6	Extrait de la table de filtrage des pare-feux

Dossier documentaire spécifique au sujet B

Document B.1	L'application *web* de « Demande en ligne DDE »
Document B.2	France-Visas : communiqué conjoint des ministères de l'Europe et des Affaires étrangères et de l'Intérieur (3 septembre 2021)
Document B.3	Schéma conceptuel des données portant sur la demande de visa
Document B.4	Extrait du schéma logique de données (schéma relationnel) portant sur la demande de visa
Document B.5	Maquette de l'interface de saisie des demandes de visas
Document B.6	Diagramme de classes de conception
Document B.7	Code PHP des classes
Document B.8	Résultat d'exécution : les pays de l'espace Schengen

Contexte France-Visas
Gestion des demandes de visa

Vous enseignez en section de techniciens supérieurs Services informatiques aux organisations (STS SIO). L'équipe pédagogique a choisi un contexte organisationnel qui sera utilisé dans l'enseignement des blocs professionnels. Ce contexte permet de mettre les étudiantes et étudiants en situation de participer, au sein de la structure France-Visas, aux missions d'évolution, de maintenance et de sécurisation de l'infrastructure système et réseau et des solutions applicatives.

Outre des éléments décrivant l'environnement de la classe, le dossier documentaire présente des ressources qui devront être mobilisées et éventuellement retravaillées avant d'être exploitées dans le cadre d'une séquence pédagogique.

À partir de vos connaissances et des ressources documentaires fournies, vous concevez une séquence pédagogique située au début de deuxième année :

- soit pour l'option « Solutions d'infrastructure, systèmes et réseaux » SISR (sujet A) ;
- soit pour l'option « Solutions logicielles et applications métier » SLAM (sujet B).

Votre travail sera décomposé en deux étapes :

– la première doit permettre de préparer certaines ressources et d'identifier des notions de la séquence pédagogique destinées aux étudiantes et étudiants ;

– la seconde doit permettre de formuler une proposition de séquence pédagogique.

Sujet A – Exploitation pédagogique
Option « Solutions d'infrastructure, systèmes et réseaux » - SISR

<u>Dossiers documentaires à exploiter</u> : dossier commun et dossier spécifique au sujet A

En STS Services informatiques aux organisations, vous assurez plus particulièrement l'enseignement du bloc de compétences **3–Cybersécurité des services informatiques** pour les étudiantes et étudiants de l'option A « Solutions d'infrastructure, systèmes et réseaux » (SISR).

Dans le cadre de cet enseignement, vous décidez d'exploiter le contexte France-Visas pour travailler les compétences suivantes :

- **B3.3 Sécurisation des équipements et des usages des utilisateurs**
  - Gérer les accès et les privilèges appropriés
  - Vérifier l'efficacité de la protection
- **B3.5A Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service**
  - Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique
  - Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure
  - Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité

Votre séquence portera sur la mise en place d'une solution de sécurisation des services *web* et des données sensibles dans le contexte du projet de dématérialisation des démarches proposées par France-Visas.

Étape 1 – Préparation de ressources et identification de notions pour la séquence pédagogique

Travail à faire

1 - Exploitation des documents A1, A.2 et A.3.

a) Critiquer la politique de mots de passe actuelle de l'organisation concernant en particulier les administrateurs.

b) Proposer une évolution permettant de sécuriser l'accès à distance aux serveurs *web* par les administrateurs.

2 - Exploitation des documents A.1, A.4, A.5 et A.6.

a) Expliquer en quoi l'architecture actuelle est insuffisante pour garantir un niveau de sécurité suffisant au regard des recommandations de l'ANSSI.

c) Proposer une évolution de l'infrastructure pour être en accord avec les recommandations de l'ANSSI.

d) Rédiger les règles de filtrage nécessaires pour que les services *web* aient accès aux serveurs de bases de données.

3 - Identification de notions mobilisables dans la séquence.

a) Définir les notions d'authentification forte et d'authentification multi-facteurs en les distinguant.

b) Définir la notion de zone démilitarisée (DMZ) et de défense en profondeur.

Étape 2 – Proposition de séquence pédagogique

Travail à faire

Proposer la séquence pédagogique sur la mise en place d'une solution de sécurisation des services *web* dans le contexte du projet de dématérialisation des démarches proposées par France-Visas, en précisant les points suivants :

- les objectifs d'apprentissage ;
- le déroulement : prérequis mobilisés, découpage en différentes phases, équipements ou technologies mobilisés ;
- les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
    - les consignes fournies ou les éléments d'évaluation à traiter par les étudiantes et les étudiants ;
    - la ou les ressources choisie(s) dans les dossiers joints en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjonction d'indications, etc.) ;
    - les attendus de chaque travail demandé aux étudiantes et aux étudiants.

Attention : la démarche proposée dans l'étape 1 ne doit pas constituer le plan de la séquence. Cependant, des éléments travaillés dans l'étape 1 doivent être mobilisés dans le cadre de la séquence.

Sujet B – Exploitation pédagogique
Option « Solutions logicielles et applications métier » - SLAM

<u>Dossiers documentaires à exploiter</u> : dossier commun et dossier spécifique au sujet B

En STS Services informatiques aux organisations, vous assurez plus particulièrement l'enseignement du bloc de compétences **2–Conception et développement d'applications** pour les étudiantes et étudiants de l'option B « Solutions logicielles et applications métier » (SLAM).

Dans le cadre de cet enseignement, vous décidez d'exploiter le contexte France-Visas pour travailler les compétences suivantes :

- **B2.1B – Concevoir et développer une solution applicative**
  - Modéliser une solution applicative
  - Identifier, développer, utiliser ou adapter des composants logiciels
  - Utiliser des composants d'accès aux données
- **B2.3B – Gérer les données**
  - Exploiter des données à l'aide d'un langage de requêtes

Votre séquence portera, dans le cadre de l'évolution de l'application de demande de visa, sur la représentation des données, la persistance des données et le développement de composants logiciels en langage orienté objet en tenant compte des exigences de qualité et de sécurité.

Étape 1 – Préparation de ressources et identification de notions pour la séquence pédagogique

Travail à faire

1 - Exploitation des documents B.1, B.2, B.3, B.4 et B.5.

a) Modéliser l'évolution portant sur la circulation du demandeur au sein de l'espace Schengen.

b) Commenter la solution proposée dans le cadre du passage du schéma conceptuel des données au schéma logique relationnel en s'appuyant sur des alternatives possibles. Proposer un mécanisme technique à mettre en œuvre par le système de gestion de bases de données relationnelles (SGBDR) pour permettre de garantir la cohérence des données.

1 - Exploitation des documents B.6, B.7 et B.8.

a) Présenter le patron de conception DAO (*data access object* ou objet d'accès aux données) et l'intérêt de son emploi.

b) Implémenter la méthode *isSchengen()* de la classe Pays et la méthode *listerPaysSchengen()* de la classe PaysControleur. La solution proposée ne devra pas modifier la classe PaysDAO.

2 - Identification de notions mobilisables dans la séquence

a) Expliquer l'intérêt de recourir à l'usage de patrons de conception.

b) Présenter le concept d'héritage et les bonnes pratiques de programmation : qualité du code, intégrité des données, etc.

c) Exposer les règles de passage d'un schéma conceptuel de données à un schéma logique relationnel.

Étape 2 – Proposition de séquence pédagogique

Travail à faire

Proposer une séquence pédagogique, dans le cadre de l'évolution de l'application de demande de visa, sur la représentation des données, la persistance des données et le développement de composants logiciels en langage orienté objet, en tenant compte des exigences de qualité et de sécurité et en précisant les points suivants :

- les objectifs d'apprentissage ;
- le déroulement : prérequis mobilisés, découpage en différentes phases, équipements ou technologies mobilisés ;
- les travaux demandés aux étudiantes et étudiants en indiquant, pour chacune des phases,
    - les consignes fournies ou les éléments d'évaluation à traiter par les étudiantes et les étudiants ;
    - la ou les ressources choisie(s) dans les dossiers joints en explicitant les raisons de votre choix. Pour les documents retenus, vous préciserez la transposition didactique nécessaire pour satisfaire les objectifs fixés (extraction d'une partie du document, suppression de certains termes ou informations, adjonction d'indications, etc.) ;
    - les attendus de chaque travail demandé aux étudiantes et aux étudiants.

Attention : la démarche proposée dans l'étape 1 ne doit pas constituer le plan de la séquence. Cependant, des éléments travaillés dans l'étape 1 doivent être mobilisés dans le cadre de la séquence.

Dossier documentaire commun

Document 1 - Acquis des étudiantes et étudiants en première année de STS SIO

Ce document rassemble les acquis des étudiantes et étudiants lors de leur première année en section de techniciens supérieurs SIO, en matière de savoirs. Ces acquis sont mobilisables dans les scénarios pédagogiques des sujets A et B.

Les compétences travaillées dans les blocs 1 et 3 ont permis d'aborder les notions suivantes :

- Modèle OSI et protocole TCP/IP, adressage IPv4.
- Notions de routage, de segmentation, de réseaux sans fil et service d'annuaire (LDAP/Domaine active directory).
- Principaux protocoles et services associés : services *web*, services d'architecture (protocoles DNS/DHCP, NTP), services de communication (fichiers, messagerie, annuaire LDAP).
- Programmation procédurale, bases de la programmation orientée objet et de la programmation *web*, langage de script.
- Notions sur le fonctionnement d'une base de données relationnelle et du langage SQL.
- Bases sur la protection des données personnelles et de l'identité numérique de l'organisation.
- Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.
- Principes et techniques sur la protection, la gestion des droits d'accès et l'archivage des données, le chiffrement, l'authentification et la preuve.
- Typologie des risques et de leurs impacts, initiation à l'analyse de risques.
- Bases sur la résolution des incidents : processus ITIL (recueil de bonnes pratiques informatiques), cycle de vie d'un incident.

Les étudiantes et étudiants ont une pratique courante des technologies suivantes :

- Bases de l'administration système sous *Windows* et *Linux* : commandes de base, consultation de fichiers, filtres, installation de paquets, etc.
- Bases de l'administration réseau : mise à disposition d'un accès à un réseau.
- Installation, administration et sécurisation du poste de travail.
- Utilisation de l'outil de simulation *Cisco Packet Tracer* et d'équipements physiques : commutateurs, routeurs, points d'accès sans-fil (sécurisation par WPA2 PSK), etc.
- Pratique d'un outil de gestion de projet (tâches, planification, ressources etc.).
- Pratique d'un outil de gestion des incidents.
- Techniques de mise à disposition de site *Web* (local, nuage –*cloud*- privé, nuage public).
- Étude et modification de site *web* (langages HTML, CSS, *Javascript*).
- Étude et modification de site PHP MySQL (langage de script serveur et accès aux données).
- Étude et modification de site *web* (système de gestion de contenus tel que *WordPress*).
- Interprétation et modification des formats de données structurées (JSON, XML).
- Génération et exploitation de scripts de création de base de données.
- Manipulation des données à l'aide du langage SQL.

Spécifiquement pour l'option SISR :

Les compétences travaillées dans le bloc 2 ont permis d'approfondir les principes et la mise en œuvre des architectures réseau et système : séparation des flux (réseaux virtuels – *VLAN*, propagation de réseaux virtuels - 802.1q, zone démilitarisée – *DMZ*, autres périmètres de sécurité, etc.), adressage IP, routage (avec routage dynamique), translation d'adresses réseau (*NAT*), accès distant, langage de script, déploiement de postes de travail et d'applications, administration d'un serveur *Windows* et/ou *Linux*.

Spécifiquement pour l'option SLAM :

Les compétences travaillées dans le bloc 2 ont permis d'approfondir les principes et la mise en œuvre de la programmation (notamment orientée objet) et des bases de données : modélisation et maquettage d'une solution applicative, architectures applicatives n-tiers, adaptation d'une base de données en réponse à de nouveaux besoins, accès aux données à travers des requêtes du langage de la base de données depuis une application, gestion de versions de code source.

Document 2 - Extraits du référentiel du BTS Services informatiques aux organisations

Bloc de compétences n° 3 - Cybersécurité des services informatiques - Option A « Solutions d'infrastructure, systèmes et réseaux »

Compétences	Indicateurs de performances	Savoirs associés
B3.3 - Sécuriser les équipements et les usages des utilisateurs • Gérer les accès et les privilèges appropriés • Vérifier l'efficacité de la protection	Les accès et privilèges respectent les règles organisationnelles : - les utilisateurs sont authentifiés ; - les habilitations sont configurées ; - l'accès aux données est contrôlé ; - les privilèges sont restreints. L'efficacité de la protection mise en œuvre est évaluée.	Authentification, privilèges et habilitations des utilisateurs : principes et techniques. Sécurité des applications Web : risques, menaces et protocoles. Sûreté des infrastructures réseaux : bonnes pratiques, normes et standards. Cybersécurité : bonnes pratiques, normes et standards.
B3.5A - Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service • Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique • Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure • Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité	Les bonnes pratiques de sécurité sont prises en compte. Les éléments de sécurité de l'architecture sont conformes et documentés. Les exigences de sécurité sont prises en compte dans le projet de mise en en œuvre d'une solution d'infrastructure.	Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services.

Bloc de compétences n° 2 - Solutions logicielles et applications métier - Option B « Solutions logicielles et applications métier »

Compétences	Indicateurs de performance	Savoirs associés
B2.1B - Concevoir et développer une solution applicative • Analyser un besoin exprimé et son contexte juridique • Modéliser une solution applicative • Identifier, développer, utiliser ou adapter des composants logiciels • Utiliser des composants d'accès aux données • Réaliser les tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés • Intégrer en continu les versions d'une solution applicative	Le choix des composants logiciels à utiliser et/ou à développer est pertinent. Les composants logiciels sont validés par les procédures de tests unitaires et fonctionnels. Les données persistantes liées à la solution applicative sont exploitées à travers un langage de requête lié à la base de données qui peut être le langage de requête proposé par les échanges applicatifs des technologies Web, un langage de requête présent dans l'outil de correspondance objet-relationnel ou toute autre solution de persistance. L'application développée est opérationnelle conformément au cahier des charges et stable dans l'environnement de production. Les tests d'intégration sont réalisés. Un outil collaboratif de gestion des itérations de développement et de versions est utilisé. Une documentation des versions vient appuyer l'intégration continue.	Méthodes, normes et standards associés au processus de conception et de développement d'une solution applicative. Architectures applicatives : concepts de base et typologies. Techniques et outils d'analyse et de rétroconception. Concepts de la programmation objet : classe, objet, abstraction, interface, héritage, polymorphisme, annotations, patrons de conception, interface de programmation d'applications. Persistance et couche d'accès aux données. Fonctionnalités d'un outil de gestion de projets. Concepts et techniques de développement agile.
B2.3B - Gérer les données • Exploiter des données à l'aide d'un langage de requêtes • Concevoir ou adapter une base de données • Administrer et déployer une base de données	L'exploitation des données permet de construire l'information attendue. Les accès aux données sont contrôlés conformément aux habilitations définies par le cahier des charges. Les données sont modélisées conformément au besoin de la solution applicative.	

Document 3 - Contexte organisationnel du ministère de l'Europe et des Affaires étrangères

Le ministère de l'Europe et des Affaires étrangères (MEAE) intervient dans un très large champ d'activités à l'international. Il agit en étroite relation avec les autres ministères et dispose pour ce faire d'un réseau diplomatique, consulaire et culturel très étendu. Le territoire européen de la France fait partie de l'espace Schengen, réunion de 27 États situés sur le continent européen, pour constituer un espace commun de libre circulation des personnes.

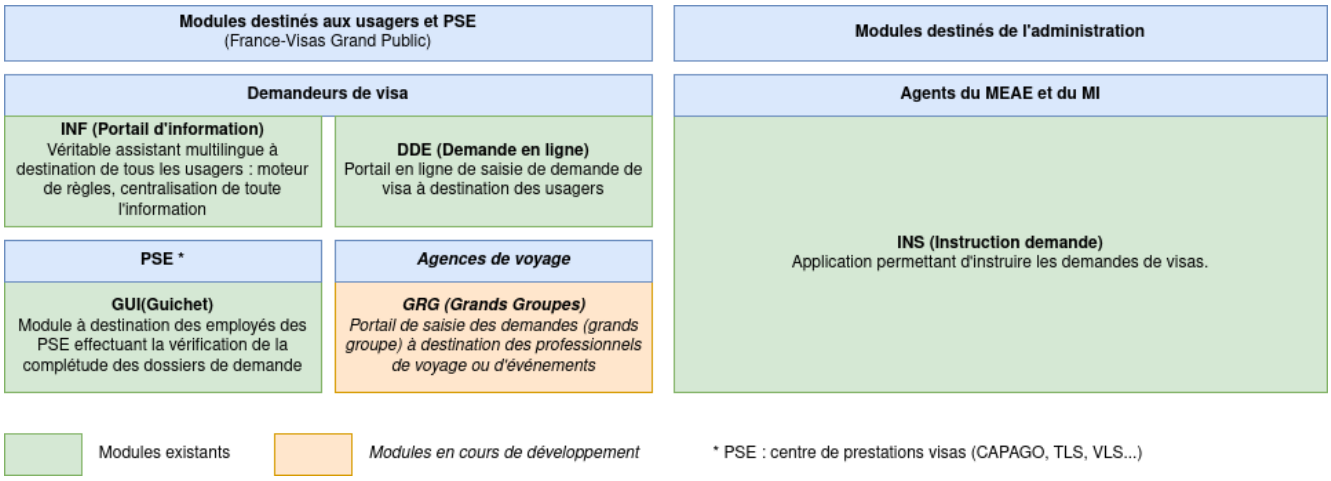
La direction du numérique (DNum) du MEAE compte 400 personnes, implantées à Paris, à Nantes et à l'étranger. Les personnes travaillant en France relèvent de cinq unités, tandis qu'à l'étranger, les agents sont implantés sur 22 centres régionaux d'assistance des systèmes d'information et de communication (CRASIC), répartis partout dans le monde.

L'unité PSI - Projets des systèmes d'information – de la DNum élabore les projets et effectue les tâches d'étude, de réalisation et de validation des projets applicatifs (démarches en lignes, applications et portails métiers, etc.) en coordination avec les maîtrises d'ouvrage, en prenant en compte les besoins de sécurité exprimés.

L'unité IDA - infrastructure, déploiements et acquisitions – de la DNum acquiert et diffuse l'ensemble des matériels, logiciels et services requis par les systèmes d'information. Elle conçoit et déploie le réseau de communication privé du ministère sur près de 400 sites dans le monde. Elle fournit aux utilisateurs un environnement de travail bureautique et de communication complet. Elle gère la sécurité des systèmes d'information et les documents associés (échanges confidentiels protégés).

Le programme France-Visas

Lancé en 2017, le programme France-Visas conjointement piloté par le ministère de l'Intérieur et des Outre-Mer (MI) et le MEAE a permis de développer divers modules applicatifs portant sur la demande de visa et son instruction.



Source : DNum

Le processus de demande de visa

L'application *web* de « Demande en ligne DDE » permet de déposer en ligne une demande de visa pour toute personne n'ayant pas une nationalité d'un pays appartenant à l'espace Schengen. Une fois la demande saisie sur l'application, les demandeurs doivent se rendre dans une autorité compétente (services diplomatiques, consulaires ou opérateur privé habilité) pour déposer l'ensemble des pièces justificatives.

En 2021, le MEAE s'est engagé dans un plan de transformation numérique. Dans ce cadre, une expérimentation a permis de proposer aux étudiants étrangers hors espace Schengen de transmettre une copie numérique de leurs pièces justificatives au moment de la saisie en ligne de leur demande de visa, conduisant ainsi à une démarche 100 % dématérialisée. Le MEAE envisage de déployer ce dispositif à l'échelle mondiale sur l'ensemble des demandes de visa pour la France et ses territoires d'outre-mer.

Une telle modernisation vise à faciliter les procédures de demande de visa vers la France pour entrer dans l'espace Schengen, avec une possible augmentation des recettes budgétaires liées à la délivrance des visas.

Dossier documentaire spécifique au sujet A

Document A.1 - Dossier d'infrastructure du système d'information de France-Visas

Document A.1.1 - Schéma général de l'infrastructure réseau

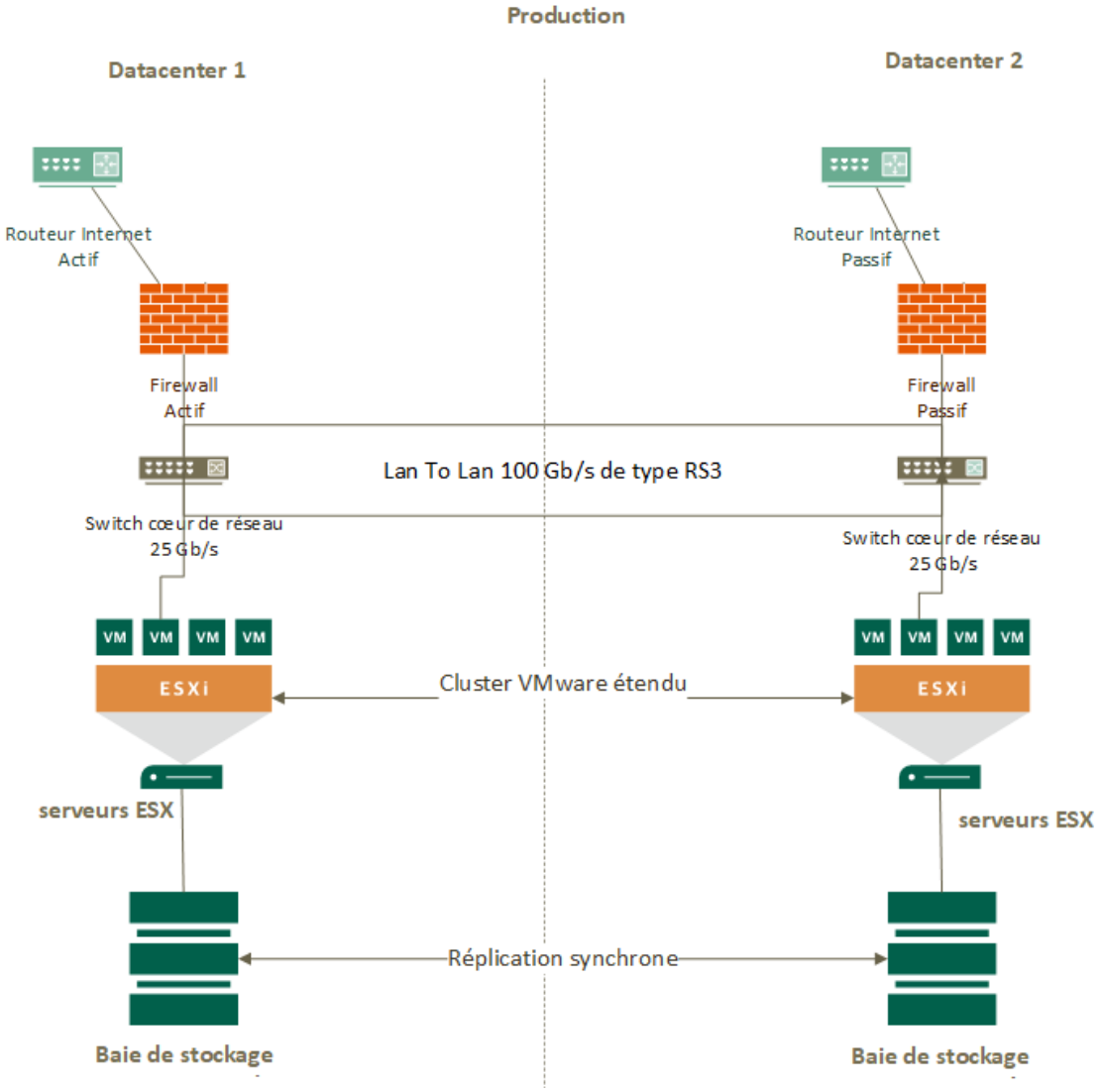


Schéma d'interconnexion des sites de France-Visas

Les centres de données entièrement redondants possèdent deux lignes dédiées entre eux de 100Gb passant par des chemins géographiques différents pour éviter la coupure des liaisons. Le centre de données *datacenter 1* est le plus actif, son routeur internet est en mode actif et celui du second est en mode passif. Le fonctionnement est identique pour les pare-feux physiques aux routeurs internet, en mode actif sur le centre de données *datacenter 1* et en mode passif sur le deuxième. Les pare-feux exécutent du filtrage applicatif (IPS).

Tous les équipements sont administrables via le réseau virtuel « VLAN DSI ».

Extrait du plan d'adressage du site principal de Nantes (datacenter 1)

Adresse du réseau des utilisateurs du site principal de Nantes	**10.10**.0.0/16
Adresse VLAN Serveur du site principal de Nantes	**10.50.**1.0/18
Adresse VLAN DSI du site principal de Nantes	**10.100**.0.0/16
Adresse réseau de la zone démilitarisée (DMZ) FrontOffice	**172.16.**0.0/16
Adresse réseau de la zone démilitarisée (DMZ) BackOffice	**172.17.**0.0/16

Liste des serveurs du site principal de Nantes (extrait)

Nom des serveurs	Fonction	Adresse IP	Port
esx1	Serveur hyperviseur VMWare	10.50.1.1	
esx2	Serveur hyperviseur VMWare	10.50.1.2	
esx3	Serveur hyperviseur VMWare	10.50.1.3	
dc1	Serveur d'authentification (CD Active Directory)	10.50.1.10	
mx1	Serveur de messagerie principal	10.50.1.11	25,110,143, …
cas1	Serveur de gestion des certificats	10.50.1.13	
antivir1	Serveur antivirus	10.50.1.41	
back1	Serveur backoffice	10.50.1.21	
back2	Serveur backoffice	10.50.1.22	
log	Serveur de centralisation des journaux	10.50.1.100	
HAProxy	Serveur proxy FrontOffice	172.16.0.10	
web	Serveur web BackOffice	172.17.0.10	443
PostgreSQL	Serveur de bases de données	172.17.0.20	5432

Document A.1.2 - Éléments complémentaires sur l'infrastructure du système informatique

- **Infrastructure dupliquée**

Dans le cadre d'un plan de continuité de l'activité (PCA), l'infrastructure réseau a été dupliquée avec 2 salles serveurs (datacenter) et 2 cœurs de réseau répartis sur 2 sites géographiques différents : un sur le site nantais du ministère de l'Intérieur et un dans le bâtiment Direction du numérique (DNum). Les journaux des serveurs, commutateurs, routeurs et pare-feux sont centralisés sur une machine de centralisation.

- **Services exposés**

Tous les services exposés sur internet (comme le portail *web* de France-Visas) sont regroupés dans une zone démilitarisée (DMZ). Adresse réseau de la zone démilitarisée : 172.16.0.0/16.

- **Pare-feu (*firewall*) et anti-virus**

Les contrôles de flux (ainsi que l'analyse anti-spam) sont assurés par plusieurs pare-feux (*firewalls*) et serveurs mandataires (*proxies*). L'analyse anti-virus repose sur une solution professionnelle.

- **Serveurs**

6 serveurs physiques dotés de l'hyperviseur ESX (3 dans chaque centre de données), configurés en grappe (*cluster*) avec une fonctionnalité de basculement en cas d'incident sur un des serveurs physiques, virtualisent plus de 60 serveurs (serveurs de fichiers, serveurs LDAP *Active Directory*, serveurs DNS, serveurs de

supervision, serveurs de gestion du service informatique, serveurs de bases de données, serveurs de messagerie, etc.).

- **Disponibilité des données**

Les données sont stockées dans 2 baies de stockage SAN (200 To x 2) configurées selon un système RAID de niveau 50. Chaque baie est reliée en fibre optique aux serveurs de virtualisation *via* un commutateur *Fibre Channel*. Les données sont répliquées (par un lien de synchronisation fibre) entre les 2 centres de données (*datacenters*).

- **Disponibilité dans le réseau local (LAN)**

Le protocole RSTP (*Rapid Spanning Tree Protocol*) est activé sur tous les commutateurs afin d'avoir une topologie redondante sans boucle.

- **Locaux sécurisés**

Les salles serveurs sont équipées de portes avec accès par badge et biométrie, d'un système de vidéosurveillance, d'un dispositif alarme-incendie, d'une double climatisation et d'un courant fort ondulé.

- **Sauvegardes**

Les sauvegardes sont chiffrées et gérées par 2 équipements de la solution *VeeamBackup* (sauvegardes complètes et incrémentielles). Les jeux de sauvegardes sont stockés sur 2 sites géographiques différents, sur des supports déconnectés du réseau et nécessitent une habilitation pour accéder au contenu. Des exercices de restauration sont réalisés régulièrement pour éprouver les procédures et vérifier les sauvegardes.

Document A.2 - Politique de gestion des mots de passe de France-Visas

Document A.2.1 - Extrait des mots de passe des administrateurs

Nom	Prénom	Identifiant	Mot de passe
Thomas	Leo	leo.thomas	Samoht_007
Saindou	Ambdoul	ambdoul.saindou	Drwitui_125tgre
Respringer	Elizio	elizio.respringer	Azerty_12345
Rebbah	Rayan	rayan.rebbah	Juhyt_2354gt

Document A.2.2 - Script Powershell de vérification de la date de dernier changement de mot de passe

```
# Importer le module Active Directory

Import-Module ActiveDirectory
# Définir la limite d'âge du mot de passe en jours
$PasswordAgeLimit = 0
# Obtenir la date du jour
$CurrentDate = Get-Date
# Récupérer la liste des utilisateurs de l'Active Directory
$Users = Get-ADUser -Filter * -Properties PasswordLastSet
# Parcourir chaque utilisateur et vérifier l'âge de leur mot de passe
foreach ($User in $Users) {
       # Calculer l'âge du mot de passe en jours
       $PasswordAge = ($CurrentDate - $User.PasswordLastSet).Days
       # Vérifier si l'âge du mot de passe est supérieur à la limite
       if ($PasswordAge -gt $PasswordAgeLimit) {
       # Afficher le nom d'utilisateur et l'âge du mot de passe
       Write-Output "Username: $($User.SamAccountName)"
       Write-Output "Password age: $PasswordAge days"
       }
}
```

Document A.2.3 - Résultat du script Powershell de vérification de la date de dernier changement de mot de passe

```
Username: leo.thomas
Password age: 546 days
Username: ambdoul.saindou
Password age: 2040 days
Username: elizio.respringer
Password age: 1036 days
Username: rayan.rebbah
Password age: 30 days
```

Document A.3 - Recommandations de l'ANSSI relatives aux mots de passe, à l'administration à distance et nomadisme

Document A.3.1 - Recommandations de l'ANSSI relatives aux mots de passe (extraits)

Source : « Guide de recommandations relatives à l'authentification multifacteur et aux mots de passe »

Longueur et complexité des mots de passe

La longueur est une composante importante de la sécurité d'une authentification par mot de passe. Il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe pour en augmenter l'entropie. Définir une longueur minimale permet d'avoir un certain contrôle sur le niveau de sécurité apporté par les mots de passe lors de leur création par les utilisateurs.

R21 : Il est recommandé de définir une longueur minimale pour les mots de passe lors de leur création en fonction du niveau de sécurité visé par le système d'information.

Les recommandations de longueurs minimales en fonction du niveau de sensibilité sont résumées dans le tableau ci-dessous :

Niveau de sensibilité	Longueur minimale en nombre de caractères	Taille de clé équivalente en bits
Faible à moyen	Entre 9 et 11	≈ 65
Moyen à fort	Entre 12 et 14	≈ 85
Fort à très fort	Au moins 15	≥ 100

R23 : Au moment de la création ou du renouvellement d'un mot de passe par un utilisateur, il est recommandé de mettre en œuvre des règles de complexité tout en proposant un jeu de caractères le plus large possible.

Délai d'expiration des mots de passe

Le choix d'imposer ou non un délai d'expiration fixe est un sujet qui a évolué ces dernières années. Fixer un délai d'expiration sur des moyens d'authentification est une bonne mesure en général mais s'avère souvent contre-productif dans le cas des mots de passe. […]

Pour des comptes peu sensibles, imposer un délai d'expiration trop court (3 à 6 mois par exemple) peut se révéler contre-productif étant donné les comportements des utilisateurs observés lorsqu'ils sont soumis à ce type de contrainte. En revanche, pour les comptes très sensibles comme les comptes à privilèges, conserver un délai d'expiration des mots de passe reste une bonne mesure à mettre en œuvre.

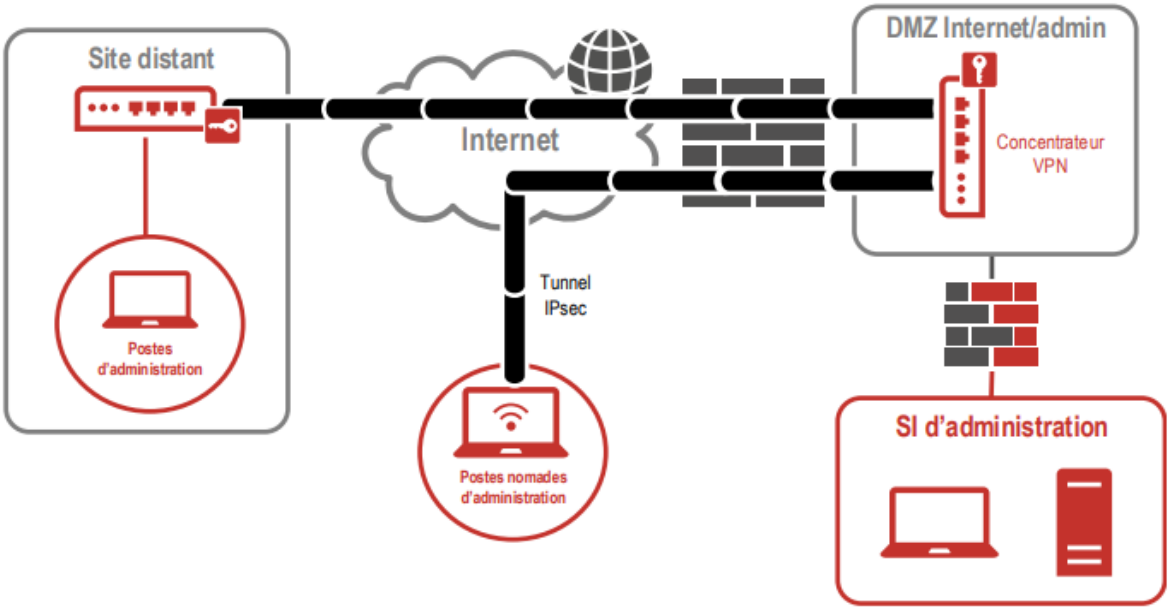
R24 : Ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles.

Si la politique de mots de passe exige des mots de passe robustes et que les systèmes permettent son implémentation, alors il est recommandé de ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles comme les comptes utilisateur.

R25 : Imposer un délai d'expiration sur les mots de passe des comptes à privilèges.
Il est recommandé d'imposer un délai d'expiration sur les mots de passe des comptes très sensibles comme les comptes administrateurs. Ce délai d'expiration peut par exemple être fixé à une durée comprise entre 1 et 3 ans. En cas d'incidents de sécurité (comme une suspicion de compromission de la base de données contenant des mots de passe), une expiration immédiate des mots de passe des comptes concernés doit être imposée.

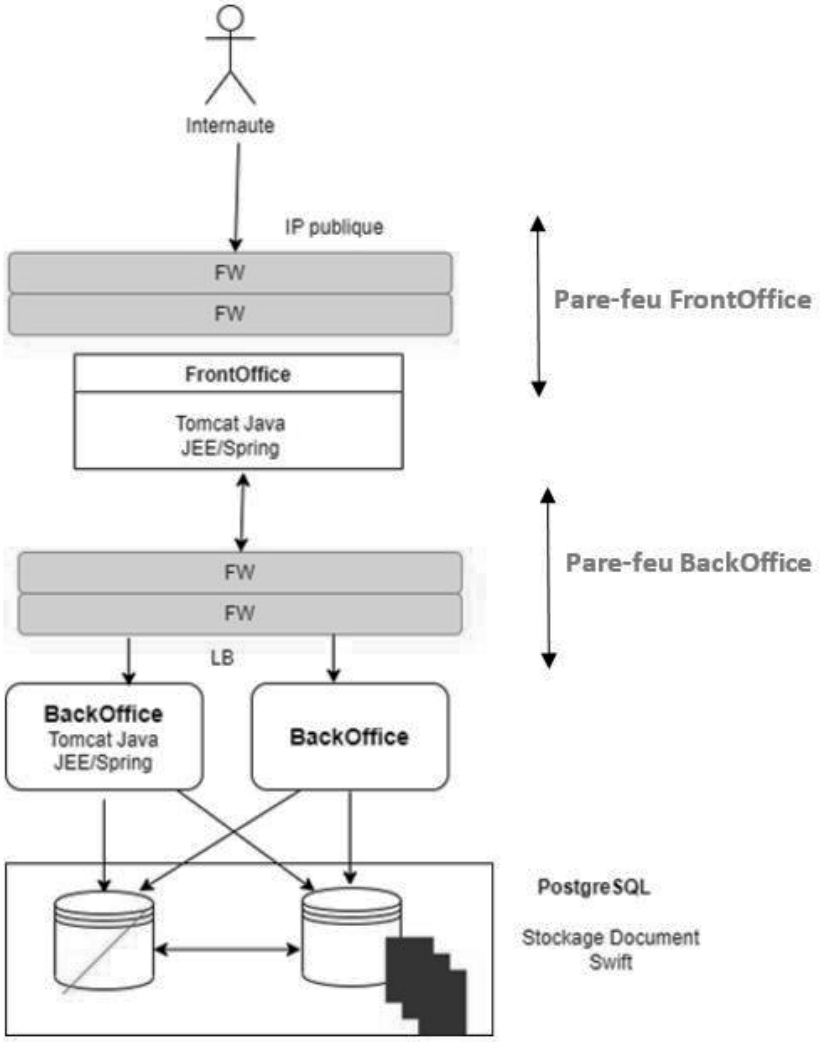
Document A.3.2 - Recommandations de l'ANSSI relatives à l'administration à distance et nomadisme

Source : « Guide de recommandations relatives à l'administration sécurisée des systèmes d'information ». On convient dans ce guide de parler de nomadisme pour l'utilisation d'un poste d'administration dans un lieu extra-professionnel (lieu public, domicile, etc.) et d'administration à distance de manière plus générale pour tout accès au système d'information en dehors du réseau local de l'entité. Ainsi l'administration à distance couvre non seulement le nomadisme mais également l'utilisation d'un poste d'administration depuis des locaux distants d'un centre de données.



Administration à distance et nomadisme

Document A.4 - Schéma de l'infrastructure du portail *web* de France-Visas



Document A.5 - Protection des données sensibles accessibles par les services *web*

Document A.5.1 - Expression des besoins

Le portail *web* de France-Visas, à partir duquel les internautes étrangers peuvent accomplir des démarches en ligne, est actuellement hébergé sur un serveur *web* situé en zone démilitarisée (DMZ). Les internautes peuvent aujourd'hui y télécharger le document CERFA de demande de visa, qu'ils devront compléter et déposer dans un consulat avec les pièces justificatives.

Dans un souci d'accroître la dématérialisation des démarches de demande de visa, France-Visas a développé une première version de l'application destinée aux étudiants étrangers.

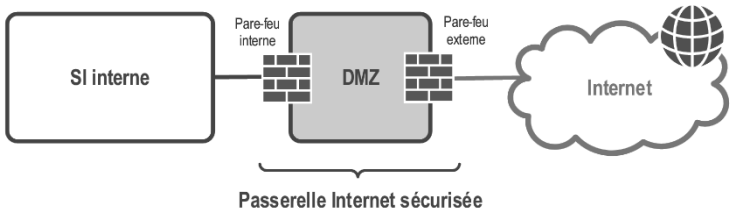
Suite à cette expérimentation, France-Visas souhaite améliorer la disponibilité de son site *web* afin de l'étendre à une plus grande échelle. En effet, l'indisponibilité du site web constituerait un incident majeur pour France-Visas.

La DNum réfléchit à une solution permettant de protéger l'accès aux données sensibles depuis le serveur *web*. Le service mandataire HAProxy est placé dans la zone démilitarisée (DMZ) nommée « FrontOffice », les serveurs *web* sont placés dans une autre zone démilitarisée nommée « BackOffice ».

Une configuration simple d'un serveur voit généralement la connexion TLS d'un client déchiffré par le serveur recevant la demande.

Document A.5.2 - Recommandations minimales de l'ANSSI

- l'interconnexion entre internet et la zone démilitarisée (*DMZ*) doit être protégée de façon périmétrique par un pare-feu dédié nommé pare-feu externe ;
- l'interconnexion entre le réseau interne et la zone démilitarisée doit être protégée de façon périmétrique par un pare-feu spécifique nommé pare-feu interne.



Une passerelle internet sécurisée est constituée d'une ou plusieurs zones démilitarisées protégées par des pare-feux périmétriques et servant, en leur sein et autant que possible, à la rupture protocolaire[1] et à l'analyse du trafic échangé entre un réseau public et le SI interne de l'entité.

La zone démilitarisée (*DMZ*) est ici considérée comme une zone neutre et perdable. En effet, sa sensibilité n'est pas nulle (des données du système d'information de l'entité peuvent y être exposées ou au moins y transiter) mais une attaque en intégrité ou en confidentialité sur ses composants ne doit pas remettre en cause de manière irréversible et durable le bon fonctionnement du SI de l'entité. À titre d'exemple, la compromission d'un relais de messagerie au sein d'une zone démilitarisée pourrait amener à décider sa destruction et sa reconstruction sans que les boîtes aux lettres électroniques hébergées et protégées de manière *ad hoc* dans le SI interne de l'entité ne soient elles-mêmes détruites. Ainsi, une zone démilitarisée intermédiaire permettant de séparer les services des données est fortement recommandée.

Il est donc nécessaire de distinguer quatre principaux types de zones réseaux :

- la zone de services relais pour la rupture protocolaire et l'analyse des flux, située entre le pare-feu interne et le pare-feu externe, appelée *DMZ externe ;*
- la zone de services exposés pour l'hébergement éventuel de serveurs métier appelée *DMZ intermédiaire* ;
- la zone hébergeant les données accessibles par les services exposés appelée *DMZ interne* ;
- la zone de services internes pour les ressources mises à disposition du réseau local.

[1] Une rupture protocolaire consiste à casser en entrée et reconstruire en sortie la communication entre deux ressources (généralement un client et un serveur) au niveau d'une des couches du modèle OSI (*open system interconnections*). Les protocoles en entrée et en sortie peuvent être distincts suivant les contraintes techniques de l'environnement et les objectifs de sécurité.

Document A.6 - Extrait des tables de filtrage des pare-feux

Extrait FW-FRONTOFFICE

N° règle	Action	Protocole	Source	Port source	Destination	Port destination
…	…	…	…	…	…	…
10	Passer	TCP	*IP Publique* FW-Front	any	172.16.0.10	https (443)
default	Bloquer	any	any	any	any	any

Remarque : il s'agit de filtrage en mode « stateful », les règles de retour sont donc implicites.

Une redirection de port est réalisée de l'interface publique du pare-feu vers le serveur *web* en *https*.

Extrait FW-BACKOFFICE

N° règle	Action	Protocole	Source	Port source	Destination	Port destination
…	…	…	…	…	…	…
9	Passer	TCP	VLAN-DSI (10.100.0.0/16)	any	VLAN-SERVEUR (10.10.0.0/16)	ssh (22)
10	Passer	TCP	Reseau_utilisateurs (10.10.0.0/16)	any	Reseau_DMZ_BackOffice (172.17.0.0/16)	https (443)
11	Passer	TCP	Reseau_DMZ_FrontOffice (172.16.0.0/16)	any	Reseau_DMZ_BackOffice (172.17.0.0/16)	https (443)
default	Bloquer	any	any	any	any	any

Dossier documentaire spécifique au sujet B

Document B.1 - L'application *web* de « Demande en ligne DDE »

Le règlement européen n°810/2009 établit le « code communautaire des visas » définissant les procédures et conditions de délivrance de visas pour les séjours dans l'espace Schengen.

L'espace Schengen comprend les États membres de l'Union Européenne (Allemagne, Autriche, Belgique, Portugal, etc.) et des États non-membres de l'Union Européenne (Islande, Liechtenstein, etc.).

Lorsqu'un pays membre de l'espace Schengen accorde un visa d'entrée sur son territoire, cette autorisation donne aussi droit à l'entrée dans tous les autres États signataires de l'accord de Schengen du 14 juin 1985.

L'application *web* DDE doit évoluer afin de permettre au demandeur :

- d'indiquer la destination principale du séjour (France métropolitaine ou territoires des DOM-TOM). L'État membre de l'Union européenne dont le territoire constitue la destination unique ou principale du voyage a la responsabilité d'examiner la demande de visa.
- de préciser les États (ou territoires) membres qui seront visités au cours du séjour et notamment le pays de première entrée à qui pourrait revenir la responsabilité d'étude de la demande de visa (s'il est impossible de déterminer la destination principale).

Au sein de l'unité PSI de la Dnum, une équipe projet prend en charge cette demande d'évolution. Une phase d'analyse a permis de produire un ensemble de documents fournis dans le dossier documentaire.

Document B.2 - France-Visas : communiqué conjoint des ministères de l'Europe et des Affaires étrangères et de l'Intérieur (3 septembre 2021)

Le 10 août 2021, un module de la plate-forme France-Visas a été l'objet d'une attaque informatique qui a pu être rapidement neutralisée. Des données personnelles enregistrées lors de la saisie d'une demande de visa (adresses de courriel et données d'identité[2]) ont néanmoins pu être dérobées. Ces données pourraient donner lieu à des utilisations détournées mais limitées dans leur effet, notamment parce que les renseignements ne comprennent pas de données financières ou sensibles au sens du règlement général sur la protection des données (RGPD). Elles ne permettent pas non plus d'engager des démarches administratives au nom de la personne dont les données ont été divulguées, que ce soit sur le portail France-Visas ou sur tout autre site institutionnel français. Des messages individuels d'information aux personnes concernées ont été envoyés avec des recommandations de vigilance et des précautions à prendre.

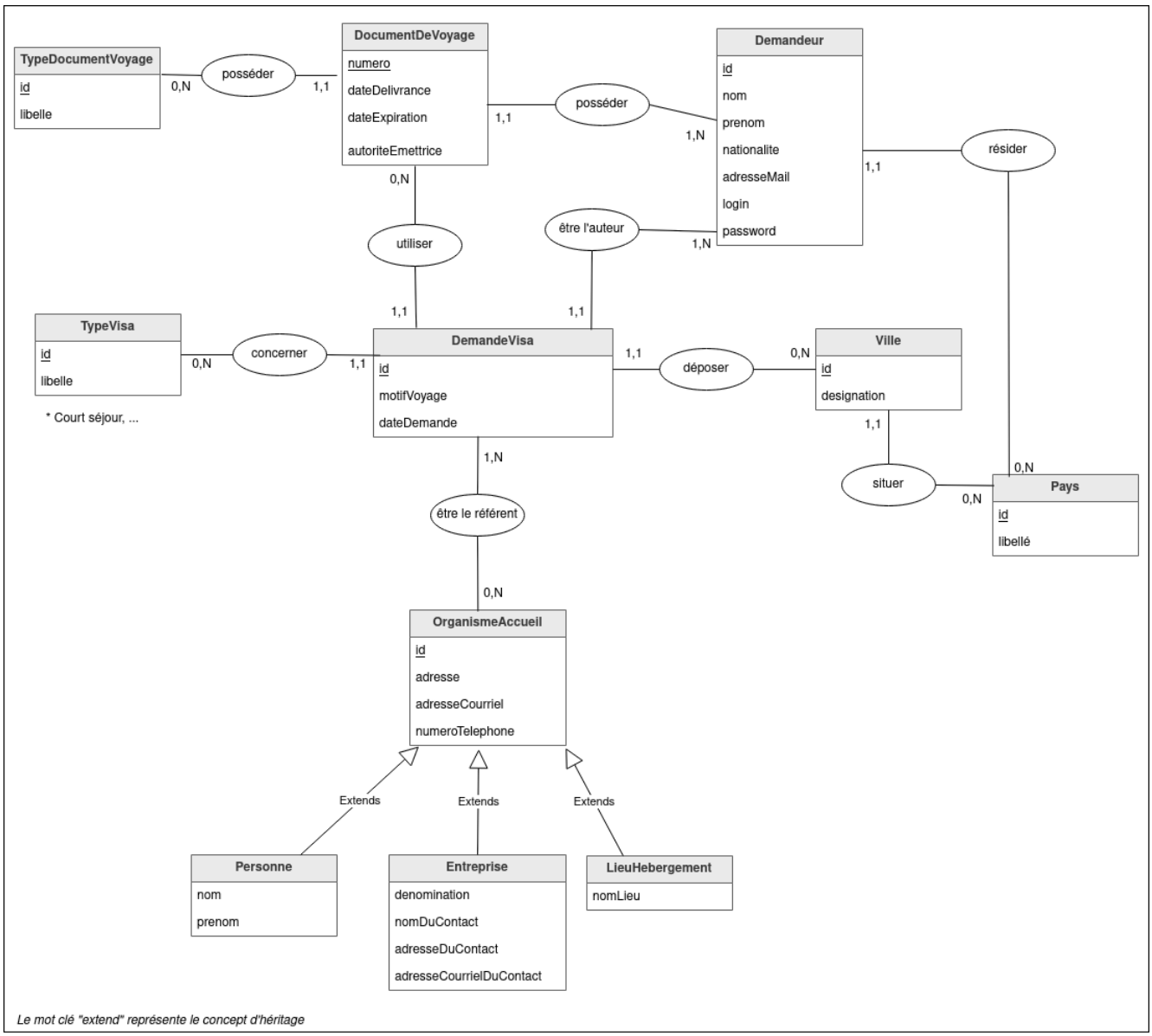
Le ministère de l'Intérieur et le ministère de l'Europe et des Affaires étrangères ont immédiatement pris les mesures nécessaires pour sécuriser la plate-forme et éviter que des événements de ce type ne se reproduisent. La Commission nationale de l'informatique et les libertés (CNIL) a été saisie des faits constatés. Le gouvernement a par ailleurs porté plainte et une enquête judiciaire est en cours.

Ces mesures permettent de garantir que l'utilisation de France-Visas par les ressortissants de pays étrangers souhaitant se rendre en France s'effectue bien dans les conditions de sécurité requises.

Le ministère de l'Intérieur et le ministère de l'Europe et des Affaires étrangères se tiennent à la disposition des usagers pour répondre aux questions que cet incident de sécurité peut susciter. Ces questions peuvent être adressées à l'adresse suivante : webmestre.france-visas@diplomatie.gouv.fr.

[2] Liste non nécessairement cumulative : nom, prénom, numéro de passeport ou carte d'identité, date de naissance, nationalité.

Document B.3 - Schéma conceptuel des données portant sur la demande de visa



Document B.4 - Extrait du schéma logique de données (schéma relationnel)

OrganismeAccueil(id, adresse, adresseCourriel, numeroTelephone)

Clé primaire : id

Personne(idOrga, nom, prenom)

Clé primaire : idOrga

Clé étrangère : idOrga en référence à id de OrganismeAcccueil

Entreprise(idOrga, denomination, nomDuContact, adresseDuContact, adresseCourrielDuContact)

Clé primaire : idOrga

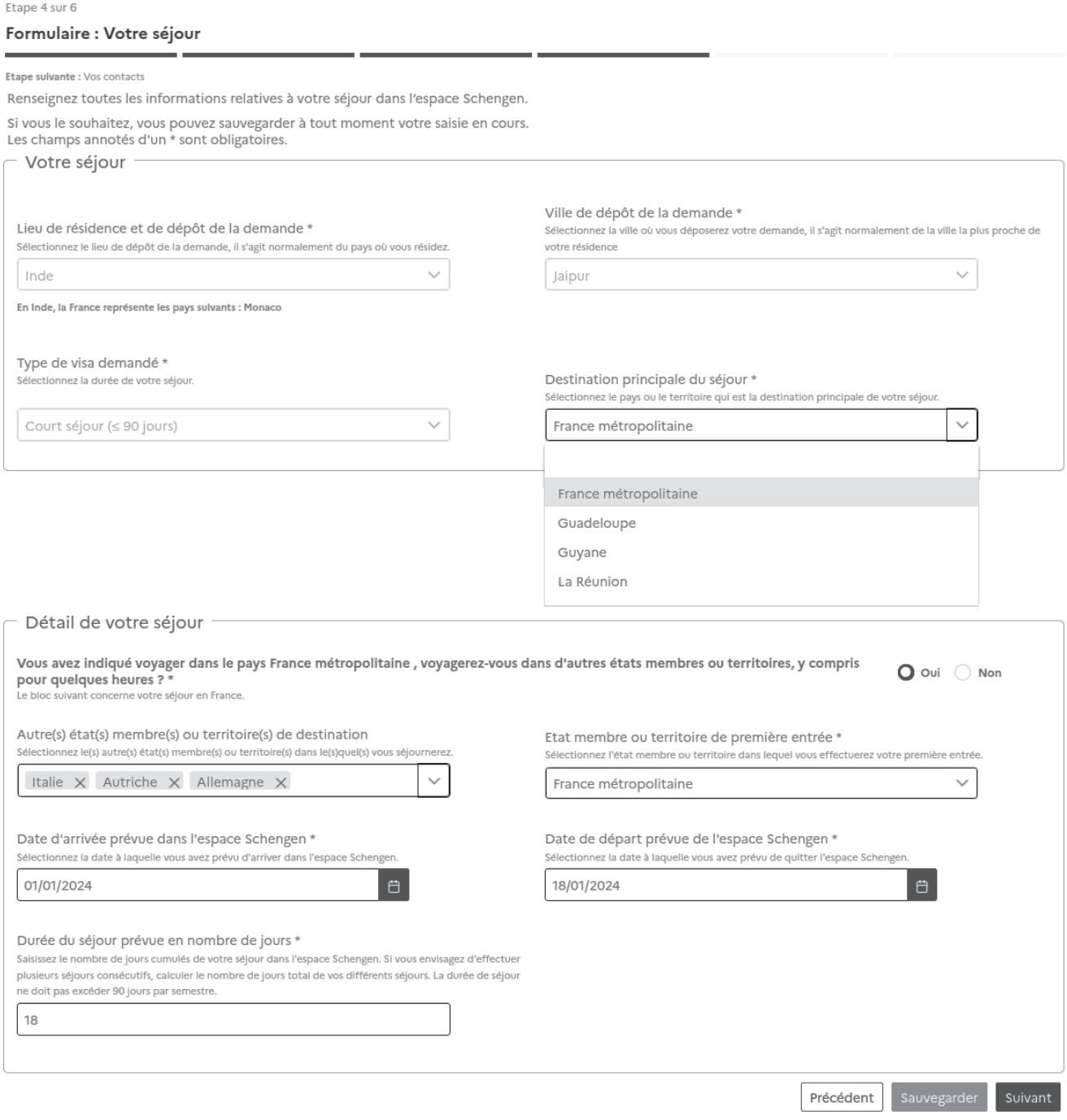
Clé étrangère : idOrga en référence à id de OrganismeAcccueil

LieuHerbergement(idOrga, nomLieu)

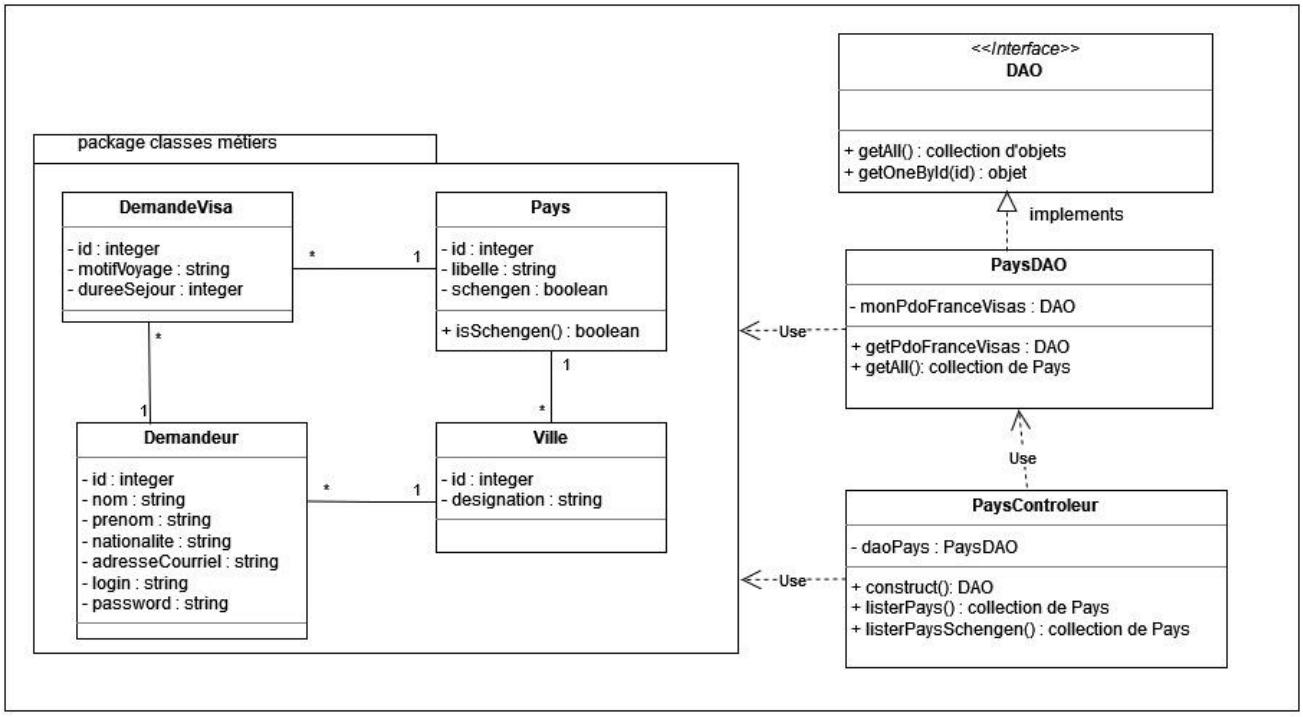
Clé primaire : idOrga

Clé étrangère : idOrga en référence à id de OrganismeAcccueil

Document B.5 - Maquette de l'interface de saisie des demandes de visas



Document B.6 - Diagramme de classes de conception



Document B.7 - Code PHP des classes

Remarque : en *PHP*, une méthode utilise **obligatoirement $this->** pour travailler avec un attribut ou une méthode de la classe dans laquelle elle est implémentée. Exemples :

```
$this->id ;       // accède à l'attribut $id de la classe
$this->getId() ;  // appelle la méthode getId() de la classe
```

fichier Pays.php

```php
<?php
class Pays
{
    private int $id;
    private string $libelle;
    private bool $schengen;
    public function __construct(int $id, string $libelle, bool $schengen)
    {
        $this->id = $id;
        $this->libelle = $libelle;
        $this->schengen = (bool)$schengen;
    }
//CODE A COMPLETER
}
?>
```

fichier PaysDAO.php

```php
<?php
require_once "Pays.php";

class PaysDAO implements DAO
{
    private static $serveur = 'mysql:host=172.17.0.20’;
    private static $bdd = 'dbname=franceVisas';
    private static $user = 'testeur';
    private static $mdp = 'azerty';
    private static $monPdo;
    private static $monPdoFranceVisas = null;
    /*
     * Constructeur privé,
     * crée une unique instance de PDO qui sera sollicitée
     * pour toutes les méthodes de la classe
     */
    private function __construct()
    {
        PaysDAO::$monPdo = new PDO(PaysDAO::$serveur . ';' . PaysDAO::$bdd, PaysDAO::$user,
PaysDAO::$mdp);
        PaysDAO::$monPdo->query("SET CHARACTER SET utf8");
    }
    /*
     * Fonction publique statique qui crée l'unique instance de la classe
     * @return l'unique objet de la classe PdoFranceVisas
     */
    public static function getPdoFranceVisas()
    {
        if(PaysDAO::$monPdoFranceVisas == null) {
            PaysDAO::$monPdoFranceVisas = new PaysDAO();
        }
        return PaysDAO::$monPdoFranceVisas;
    }

    public function getAll() : array
    {
        $txtReq = "select id, libelle, schengen from pays";
        $req = PaysDAO::$monPdo->prepare($txtReq);
        $req->execute();
         // Construction d'une collection d'objets Pays (array PHP)
        $lesPays = array();
         // Lit la première ligne du résultat de la requête
         // $uneLigne est une référence à un objet dont les
         // propriétés correspondent aux noms des colonnes de la requête
         // ou false s’il n’y a plus de ligne à lire dans le jeu de résultats
        $uneLigne = $req->fetch(PDO::FETCH_OBJ);
        while($uneLigne != false) {
               // Création d'un objet Pays
            $unPays = new Pays($uneLigne->id, $uneLigne->libelle,$uneLigne->schengen);
             // Ajout de l'objet à la collection des pays
            $lesPays[] = $unPays;
             // Lit la ligne suivante sous forme d'objet
            $uneLigne = $req->fetch(PDO::FETCH_OBJ);
        }
        $req->closeCursor();    // Libère les ressources du jeu de données
        return $lesPays;    // Fournit la collection
    }
}
?>
```

fichier PaysControleur.php

```php
<?php
require_once 'PaysDAO.php';
class PaysControleur
{
    private  $dao;  // Instance de la classe DAO
    public function __construct()
    {
        // Connexion du serveur web à la base de données
        $this->dao = PaysDAO::getPdoFranceVisas();
    }
    // Liste de tous les pays
    public function listerPays() : array
    {
        $lesPays = $this->dao->getAll();
        return $lesPays;
    }
//CODE A COMPLETER
}
?>
```

Document B.8 - Résultat d'exécution : les pays de l'espace Schengen

La table Pays contient un jeu d'essai constitué des 6 pays suivants : Allemagne, Bulgarie, Chypre, France, Italie, Luxembourg.
Chypre et la Bulgarie ne sont pas membres de l'espace Schengen.

L'exécution du code ...

```
$paysControleur=new PaysControleur();
var_dump($paysControleur→listerPaysSchengen());
```

produit le résultat ...

```
array(4) {
 [0]=>  object(Pays)#8 (3) {
   ["id":"Pays":private]=>    int(1)
   ["libelle":"Pays":private]=>    string(9) "Allemagne"
   ["schengen":"Pays":private]=>    bool(true)
  }
 [1]=>  object(Pays)#5 (3) {
   ["id":"Pays":private]=>    int(4)
   ["libelle":"Pays":private]=>    string(6) "France"
   ["schengen":"Pays":private]=>    bool(true)
  }
 [2]=>  object(Pays)#6 (3) {
   ["id":"Pays":private]=>    int(5)
   ["libelle":"Pays":private]=>    string(6) "Italie"
   ["schengen":"Pays":private]=>    bool(true)
  }
 [3]=>  object(Pays)#4 (3) {
   ["id":"Pays":private]=>    int(6)
   ["libelle":"Pays":private]=>    string(10) "Luxembourg"
   ["schengen":"Pays":private]=>    bool(true)
  }
}
```