

**CASIMIRO-EBU**

**Elcano**

**Terminal**

# **Rapport de Stage**

## **PFMP N°4**

Du 15/01/2024 au 09/02/2024

**Baccalauréat Professionnel Réseaux Informatique Et  
systèmes communicants**



**Lycée Professionnel Gustave Ferrié**

**7 Rue des Écluses Saint - Martin, 75010 Paris**

**Tel: 01 42 02 19 55**

## **Sommaire**

Remerciements.....	3
Introduction.....	4
Présentation de l'entreprise.....	5
→Organisation.....	6
→Organigramme.....	7
→Organigramme de L'EMEA.....	8
Compte rendu d'activités.....	9
Etude de cas.....	10
Conclusion.....	24

# **Remerciements**

Je voudrais tout d'abord exprimer ma gratitude envers Camille Durin, référente du programme P-TECH, ainsi que tous les intervenants du programme, qui partagent leurs connaissances et expériences professionnelles avec nous à travers différentes activités.

Notamment Khaoula Masbough, Analyste de Configuration d'Offres chez Deezer et mentor, qui joue un rôle clé dans mon développement tant personnel que professionnel. De même, je suis reconnaissant envers Rachel Cartier, Responsable de la Musique pour la France chez Deezer, qui, en tant qu'ancienne mentor, a également contribué à mon épanouissement et à ma maturité professionnelle.

Par ailleurs, Maryline Blejean, correspondante pour la Diversité, l'Inclusion et l'Engagement (ressources humaines) et Agent de liaison pour le programme P-TECH chez BNP Paribas, a été essentielle dans la réalisation de mon premier stage au sein de BNP Paribas. Elle a constamment été une source de soutien, répondant à toutes mes interrogations, en particulier celles liées à l'élaboration de ce rapport de stage.

Je vais maintenant remercier Monsieur Belluchi, mon professeur principal qui m'a encadré et enseigné depuis mon année de première, tant sur le plan professionnel que technique.

Je tiens également à exprimer ma gratitude envers Lahouari Saidat, Head of Security Operations chez BNP Paribas, pour m'avoir offert l'opportunité de faire ce stage en cybersécurité au sein de l'entreprise. Sachant mon intérêt pour ce domaine, il a pris ma demande à cœur et m'a permis de rejoindre l'une de ses équipes.

Enfin, étant donné la sensibilité du domaine de la cybersécurité, je tiens également à remercier ma chef d'équipe, Sarra Azzoug, ainsi que tous mes collègues de l'équipe SecurID, qui m'ont accordé leur confiance, m'ont encadré et m'ont accepté au sein de leur équipe.

# **Introduction**

Actuellement en classe de Terminale RISC (Réseaux Informatiques et Systèmes Communicants), au lycée professionnel Gustave Ferrié, dans le 10<sup>e</sup> arrondissement de Paris, je prépare un baccalauréat SN (Système Numérique) pour lequel je dois effectuer 16 semaines de formation professionnelle en entreprise.

La PFMP, qui est une période de formation en milieu professionnel, constitue un élément indispensable pour obtenir mon baccalauréat. Elle offre également une expérience pratique en entreprise pour approfondir les connaissances acquises en classe, en mettant en pratique la théorie étudiée.

Cette période nous confronte à des situations réelles en entreprise, nous permet de nous familiariser avec l'environnement de travail et de nous mettre en situation professionnelle.

Pour ce faire, j'ai donc choisi d'effectuer ma quatrième et dernière période de stage d'une durée de 4 semaines au sein de BNP Paribas – Campus Valmy à Montreuil-sous-Bois.

# Présentation de l'entreprise

**Nom** : BNP PARIBAS SA ITG GROUPE

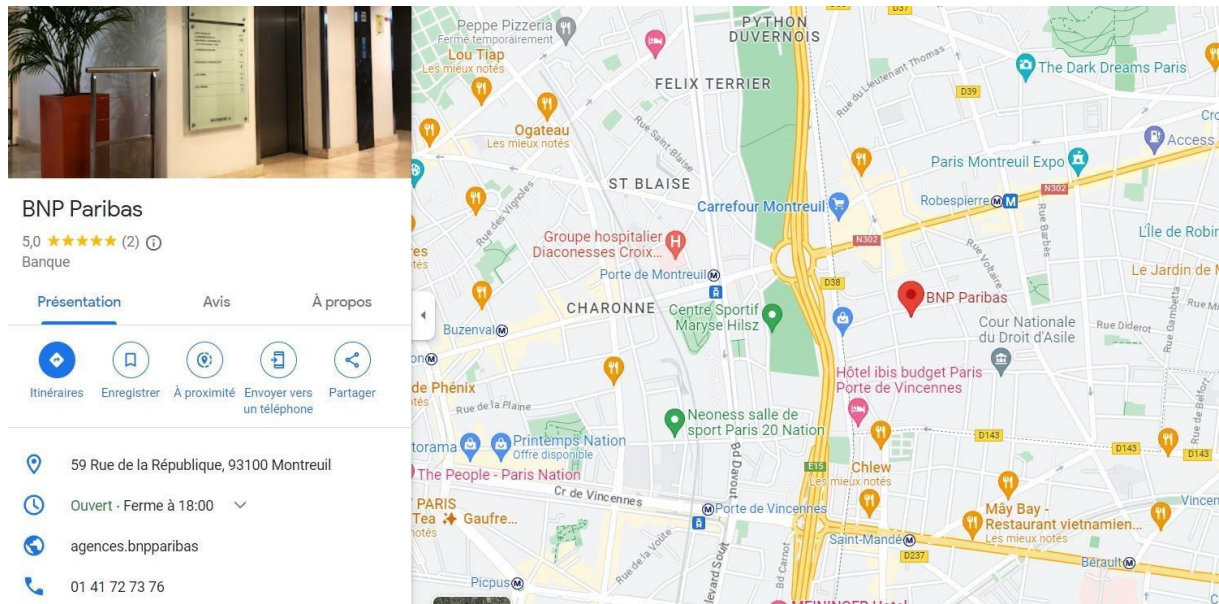
**Numéro de Siret** : 66204244900014

**Adresse** : 59 rue de la République 93100 Montreuil

**Numéro de téléphone** :

**Domaine d'activités** : Activité principalement bancaire

## Situation géographique



# **Organisation de l'entreprise**

**Nombre de salariés** : 193 000 Collaborateurs

**Chiffre d'affaires** : 50,4 milliards EUR (2022)

## **Filiale** :

BNP Paribas possède de multiples filiales et succursales dans le monde entier. De plus, les nombreuses filiales opèrent sous des noms différents dans différents pays.

Voici tout de même quelques filiales de BNP-Paribas en France :

- BNP Paribas Cardif : une filiale spécialisée dans l'assurance vie, l'assurance emprunteur et l'assurance dommage.
- BNP Paribas Lease Group : une filiale spécialisée dans la location financière de biens d'équipement.
- BNP Paribas Real Estate : une filiale spécialisée dans l'immobilier commercial, résidentiel et d'entreprise.

**Type de client** : Particulier | Professionnel

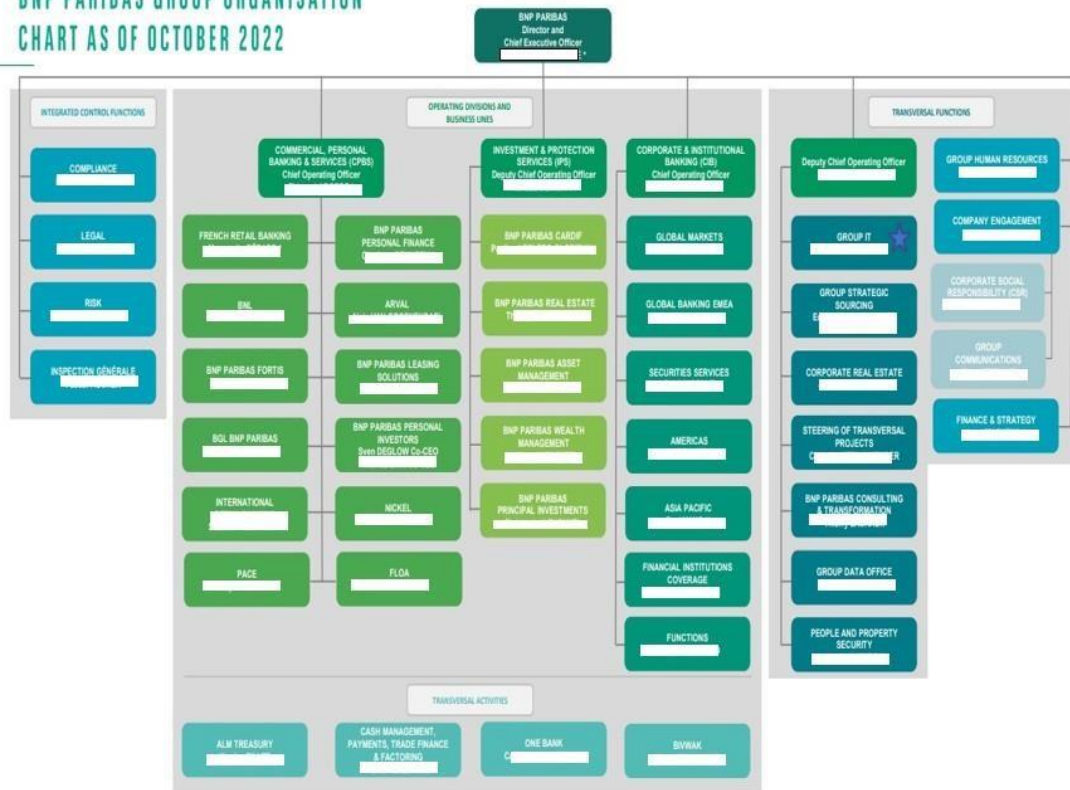
## **Partenaires** :

Les partenariats de BNP Paribas dans le secteur bancaire varient en fonction des réglementations locales et des conditions du marché dans chaque pays.

**Concurrents** : Crédit Agricole, HSBC, Barclays, Deutsche Bank, Société générale.

# Organigramme de l'entreprise

## BNP PARIBAS GROUP ORGANISATION CHART AS OF OCTOBER 2022



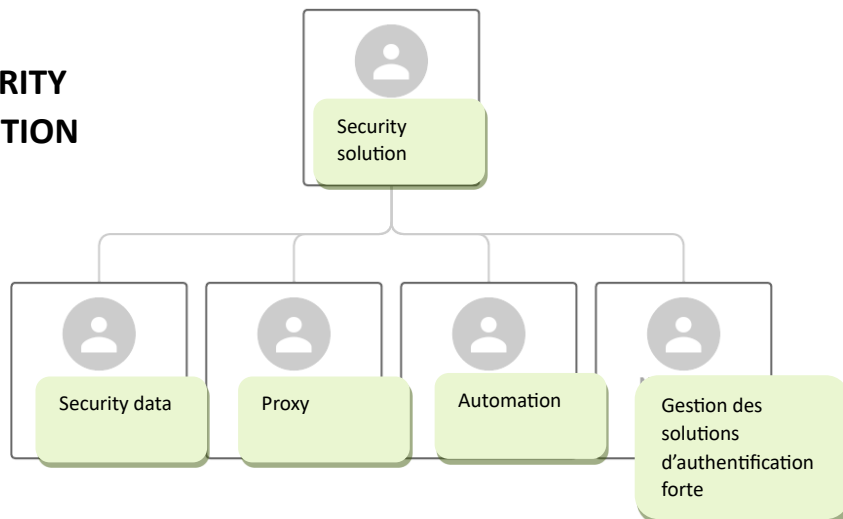
BNP PARIBAS

The bank for a changing world

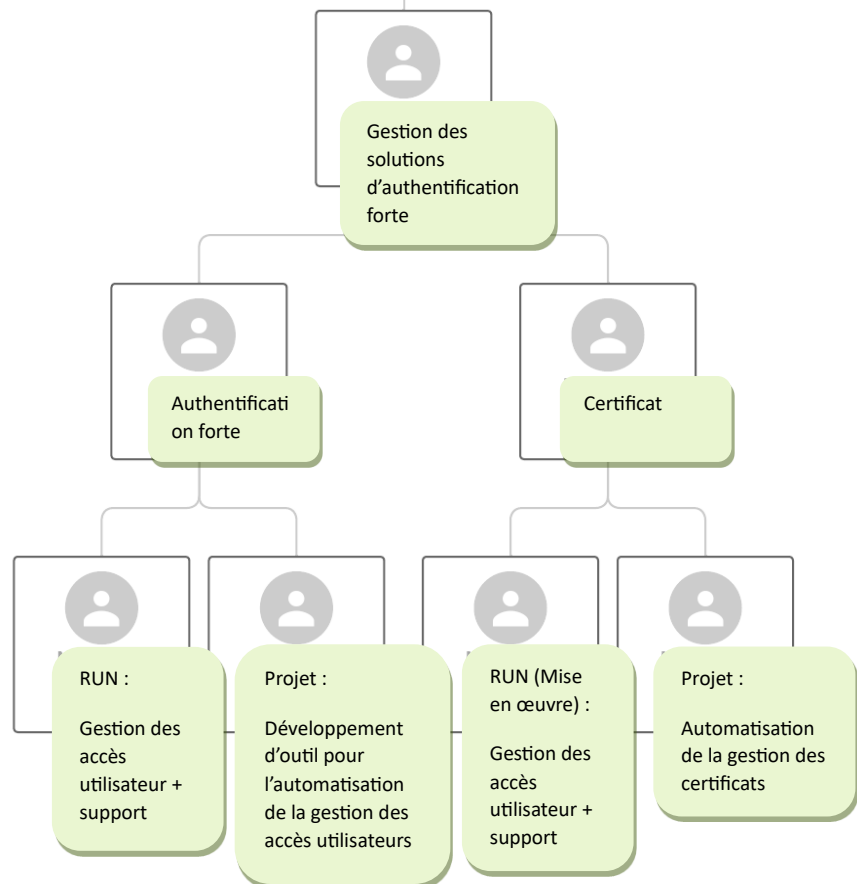
\* members of the Executive Committee of BNP Paribas.  
\*\* Paul YANG oversees all of the Group's activities in the APAC region.

# Organigramme de L'EMEA (Equipe ASAU)

## SECURITY SOLUTION

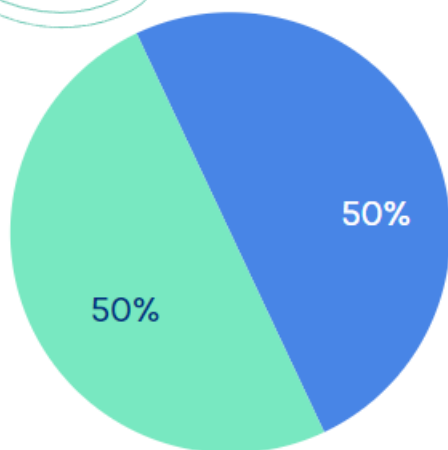


## EQUIPE ASAU





# Compte rendu d'activité



● **RUN**

Gestion des accès utilisateurs + support.

● **PROJETS**

Développement d'outils pour l'automatisation de la gestion des accès utilisateurs.

● **RUN**

Gestion des accès utilisateurs + support.

● **PROJETS**

Automatisation de la gestion des certificats.



# **Etude de cas**

## **Introduction :**

Le choix de se concentrer sur la gestion des certificats SSL chez BNP PARIBAS pour cette étude de cas est motivé par le rôle crucial de ces derniers dans la sécurisation des communications sur internet, particulièrement pour les institutions financières. Les certificats SSL sont essentiels pour chiffrer les données échangées entre les serveurs et les clients, prévenant ainsi l'accès non autorisé.

Les défis uniques auxquels font face les secteurs financiers, tels que BNP PARIBAS, comprennent la nécessité d'une gestion rigoureuse pour éviter les brèches de sécurité et maintenir la confiance. Cette étude vise à mettre en lumière ces défis et les stratégies employées pour y répondre, offrant un aperçu de l'importance des certificats SSL dans le contexte plus large de la sécurité financière et de la confiance numérique.

## **Problématique :**

Je reçois une demande de certificat SSL (web) Secure Sockets Layer, permettant d'identifier, d'authentifier et de sécuriser les échanges des sites web.

## **Solutions :**

- **Hardware** : Mon poste de travail
- **Système** : Windows 10
- **Logiciels d'infrastructure** : Certis (API de gestion de demandes), Entrust (outils de gestion et fournisseur des certificats externes), PKI (outils de gestion et fournisseur de certificats internes)
- **Les connaissances scientifiques** :

## Le certificat SSL :

Un certificat électronique (aussi appelé certificat numérique ou certificat de clé publique) peut être vu comme **une carte d'identité numérique**. Il est utilisé principalement pour **identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges**. Il est signé par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique (virtuelle). Pour un site web il s'agit d'un certificat SSL.

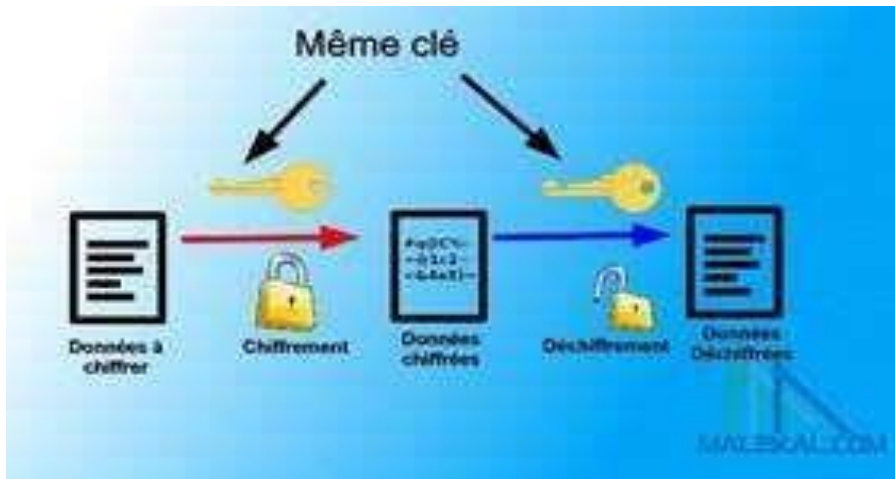
Un certificat électronique est un petit fichier qui contient des informations similaires. Les certificats contiennent les informations suivantes :

- Le nom de l'autorité de certification qui a créé le certificat
- Le nom et le prénom de la personne
- La localisation
- Son adresse électronique
- Sa clé publique
- Les dates de validité du certificat
- La signature électronique de ce certificat

**Le principe de fonctionnement des certificats électroniques est basé sur le chiffrement d'informations et sur la confiance.** Pour cela, il existe deux méthodes de chiffrement : **symétrique et asymétrique**.

### Chiffrement symétrique

Dans les algorithmes symétriques, aussi appelés algorithmes à clé secrète, **la clé de chiffrement est la même que la clé de déchiffrement**. De ce fait, pour que le texte chiffré ne soit lisible que par le destinataire, la valeur de cette clé doit être un secret partagé entre l'émetteur et le destinataire uniquement. Ceci explique le qualificatif de « clé secrète »

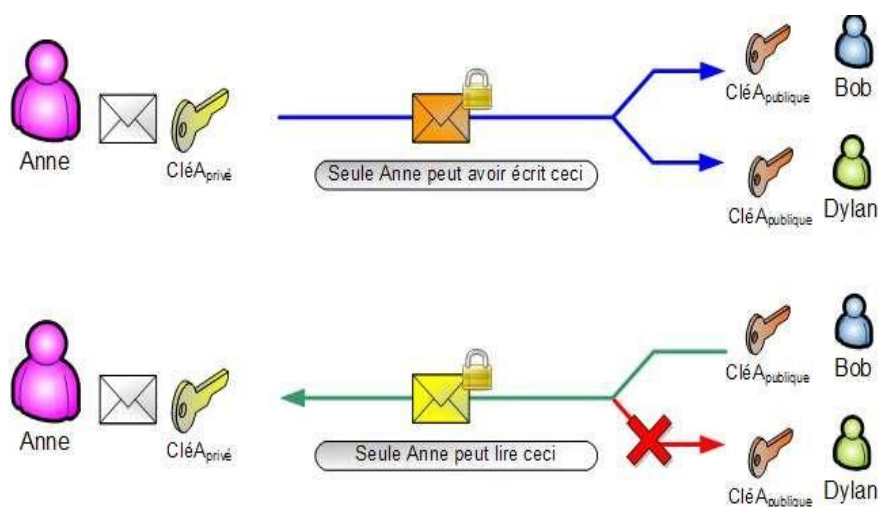


## Chiffrement asymétrique

La propriété des algorithmes asymétriques est qu'un message chiffré par **une clé privée qui sera lisible par tous ceux qui possèdent la clé publique** correspondante. À l'inverse, un message chiffré par une **clé publique n'est lisible que par le propriétaire de la clé privée correspondante**.

Ainsi avec sa clé privée, Anne :

- Signe ses messages
- Lit (déchiffre) les messages qui lui sont adressés



Un certificat électronique est un ensemble de données contenant :

- Au moins une clé publique
- Des informations d'identification, par exemple : nom, localisation, adresse électronique
- Au moins une signature (construite à partir de la clé privée). De fait quand il n'y en a qu'une, l'entité signataire est la seule autorité permettant de prêter confiance (ou non) à l'exactitude des informations du certificat.

### Utilité d'un certificat :

Les certificats électroniques sont utilisés dans différentes applications informatiques dans le cadre de la sécurité des systèmes d'information pour garantir :

- La non-répudiation et l'intégrité des données avec la **signature numérique**
- La confidentialité des données grâce **au chiffrement des données**
- **L'authentification ou l'authentification forte** d'un individu ou d'une identité numérique.

### La signature numérique

C'est un mécanisme permettant de **garantir la non-répudiation d'un document électronique et d'en authentifier l'auteur**, par analogie avec la signature manuscrite d'un document papier. Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères. Elle ne doit pas être confondue avec la signature électronique manuscrite.

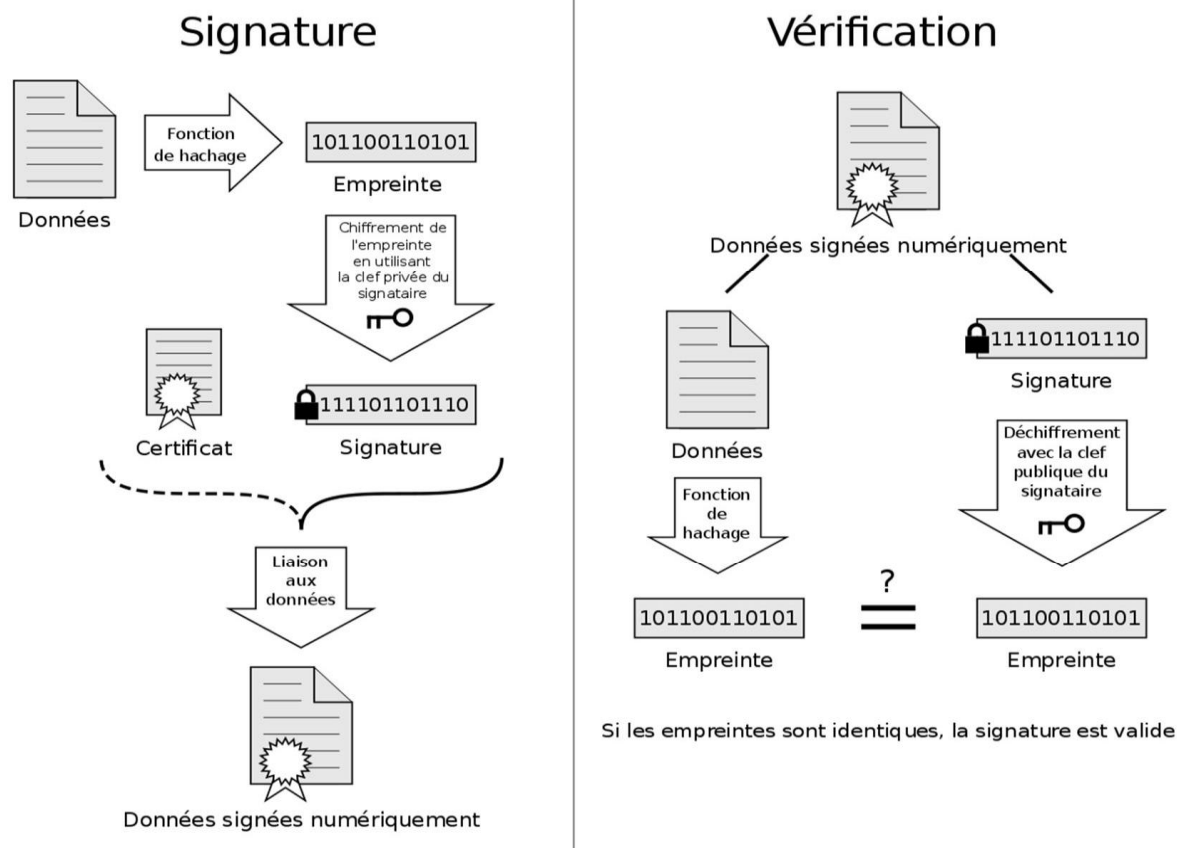


Figure : Diagramme montrant comment des données sont signées, puis vérifiées

### Autorité de Certification :

Une Autorité de Certification **C'est** un tiers de confiance (des organismes enregistrés et certifiés auprès d'autorités publiques et/ou de gouvernance de l'Internet) permettant d'authentifier l'identité des correspondants. **Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fournis.** Ces organismes diffusent leurs propres clés publiques, Ces clés sont appelées clés publiques racines ou certificats racines et sont utilisées pour identifier les clés publiques d'autres organismes.

Les services des autorités de certification sont principalement utilisés dans le cadre de la sécurisation des communications numériques via protocole Transport Layer Security (TLS) utilisé par exemple pour sécuriser les

communications web (HTTPS) ou email (SMTP, POP3, IMAP... sur TLS), ainsi que pour la sécurisation des documents numériques (par exemple au moyen de signatures électroniques avancées telles que PADES pour des documents PDF, ou via le protocole S/MIME pour les emails).

Plus généralement toute application qui utilise le réseau (transfert de fichiers, accès interactif, accès à des bases de données, calcul distribué) et tous les objets (postes nomades, équipements de réseau) **peuvent avoir un couple de clés et un certificat pour mettre en œuvre ces fonctions de sécurité.**

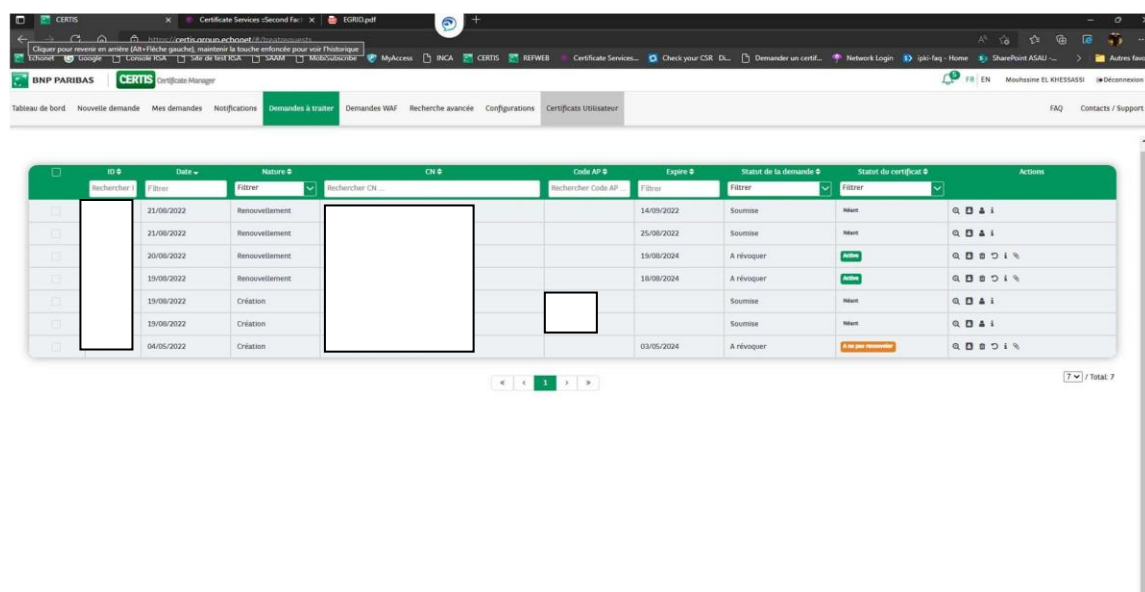
- **Les connaissances linguistiques :**

Afin de répondre au besoin qui est international, maîtriser l'anglais est indispensable afin de communiquer avec l'ensemble des collaborateurs.

## Etapes de travail

### 1. Réception la demande sur l'API Certis :

( Les demandes sont traitées par ordres d'arrivées.)



The screenshot displays the 'Certis Certificate Manager' web application. The interface includes a top navigation bar with various links and a main menu with options like 'Tableau de bord', 'Nouvelle demande', 'Mes demandes', 'Notifications', 'Demandes à traiter', 'Demandes WAF', 'Recherche avancée', 'Configurations', and 'Certificats Utilisateur'. The 'Demandes à traiter' section is active, showing a table of certificate requests.

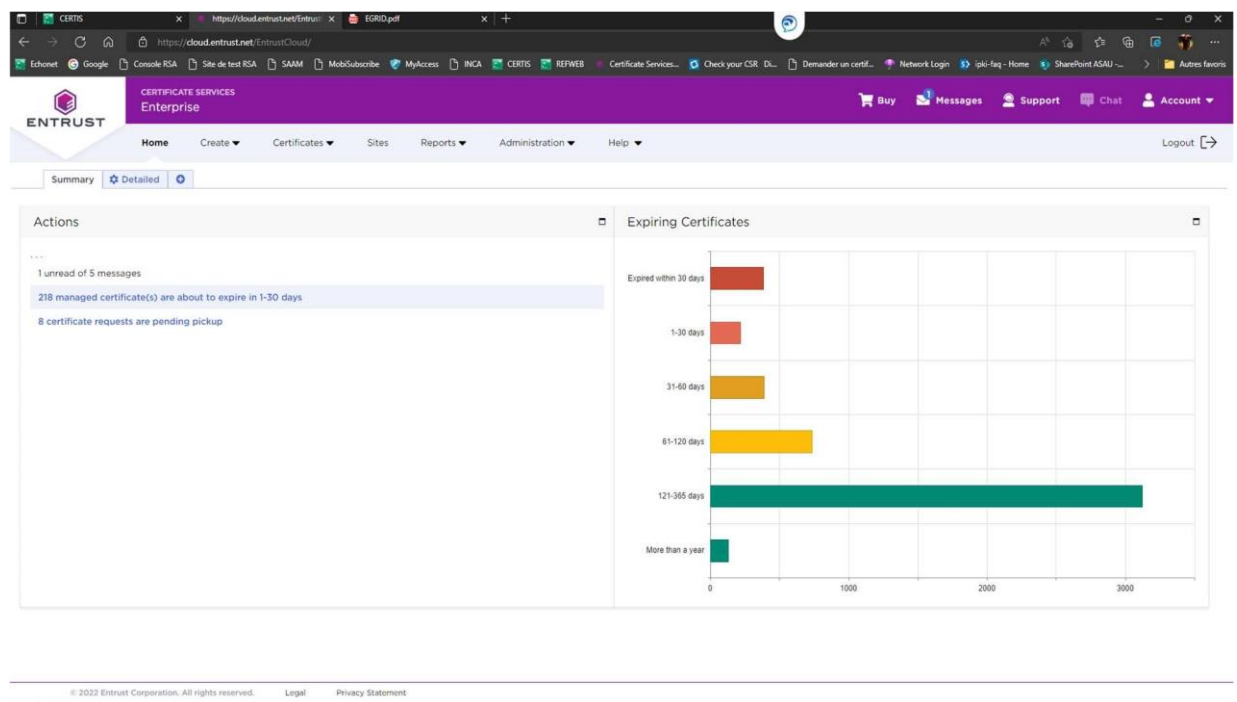
ID	Date	Nature	CN	Code AP	Expire	Statut de la demande	Statut du certificat	Actions
21/06/2022	Renouvellement				14/06/2022	Soumise	Valid	[Icons]
21/06/2022	Renouvellement				25/06/2022	Soumise	Valid	[Icons]
20/06/2022	Renouvellement				19/06/2024	A révoquer	Revoque	[Icons]
19/06/2022	Renouvellement				18/06/2024	A révoquer	Revoque	[Icons]
19/06/2022	Création					Soumise	Valid	[Icons]
19/06/2022	Création					Soumise	Valid	[Icons]
04/05/2022	Création				03/05/2024	A révoquer	6 m 20 s restantes	[Icons]

Vue d'ensemble de Certis

## 2. Détermination du type de certificat a générer :

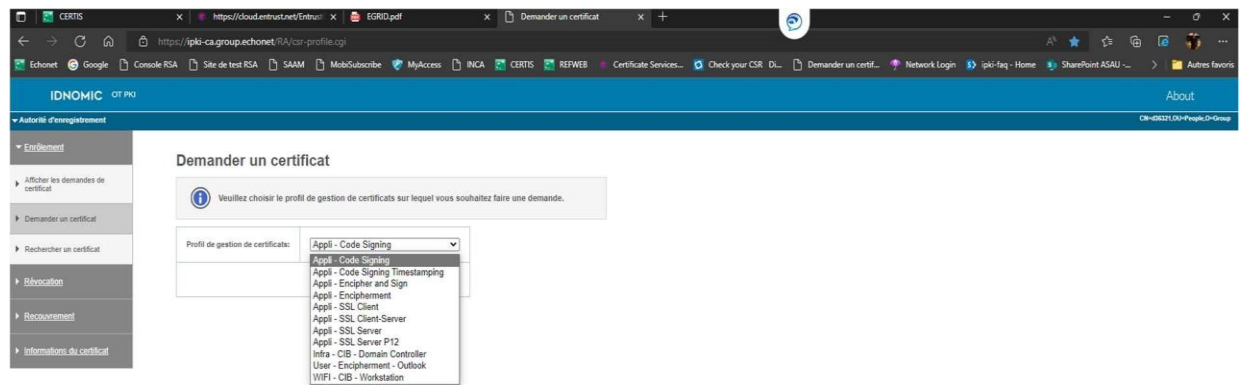
Il y a deux type demandes de certificats que je traite : interne et externe.

- Les demandes de certificats **internes concernant la délivrance de certificats intranet « accessible en interne de la BNPP uniquement »**, j'utilise PKI l'autorité de certification interne pour délivrer des certificats intranet appartenant à la BNP PARIBAS avec une durée de validité de 2 ans.
- Les demandes de certificats **externes concernant la délivrance de certificats internet « accessible à l'extérieur de la banque »**, j'utilise ENTHRUST une autorité de certification externe pour délivrer des certificats internet qui sont facturés aux entités avec une durée de validité de 1 an.



Vue d'ensemble d'Entrust





---

## Vue d'ensemble de PKI

Je fournis plusieurs types de chiffrement de certificats à savoir :

- **SSL Server :**

Les certificats SSL Server sont des **certificats d'authentification serveur permettant à des serveurs ou des applications d'être identifiés de façon sûre auprès d'utilisateurs ou d'applications tierces via le protocole SSL** (HTTPS, LDAPS...). Ils sont utilisés en particulier pour la mise en œuvre du HTTPS sur des plateformes web telles que IIS, IHS, Apache...

2 variantes supplémentaires :

« **SAN** » : Les certificats SSL Server/Internet « SAN », aussi connus sous le nom de certificats SSL pour Communication Unifiées, **permettent de sécuriser plusieurs serveurs ou plusieurs domaines avec un seul certificat. Les certificats SSL avec SAN sont adaptés pour être installés sur plusieurs serveurs et pour sécuriser entre autres des technologies telles que Microsoft Exchange et Microsoft Office Communications Server.**

« **EV** » : Les certificats SSL Server Internet « EV » activent l'indicateur de sécurité le plus visible : la barre verte d'adresse (haute sécurité) dans les navigateurs, **assurant ainsi aux utilisateurs une visibilité accrue sur la fiabilité du site et que l'identité du serveur a été authentifiée selon les normes les plus élevées de l'industrie.**

- **SSL Client Serveur :**

Les certificats SSL Client-Serveur sont des certificats d'authentification client-serveur **permettant à des serveurs ou des applications internes de s'identifier mutuellement en tant que client ou serveur.**

- **SSL Client :**

Les certificats SSL Client **sont des certificats d'authentification client permettant à des serveurs ou des applications internes de s'identifier de façon sûre auprès d'applications tierces via le protocole SSL (HTTPS, LDAPS...). Ils sont indispensables pour permettre d'établir une session sécurisée bi-authentifiée entre un serveur et un équipement qui s'authentifie comme client (authentification SSL mutuelle).**

- **SSL Serveur P12 :**

Les certificats SSL Server P12 sont des certificats SSL Server délivrés sous la forme **d'un conteneur P12 contenant le certificat et la clé privée associée. Ils peuvent être utilisés dans le cas où l'émetteur n'est pas en mesure de générer une bi-clé et une CSR sur le serveur cible.**

- **WildCard :**

Les certificats Wildcard, également appelés certificats génériques, **permettent d'identifier un domaine et tous ses sous-domaines. L'avantage principal est de pouvoir sécuriser un nombre illimité de sous-domaines, peu importe le nombre total des sous-domaines.** La plupart des certificats Wildcard permettent de sécuriser l'ensemble des sous-domaines sur un nombre illimité de serveurs.

- **Encipher and Sign :**

**Les certificats Encipher and Sign permettent de signer et ou chiffrer des fichiers afin de sécuriser une transaction entre 2 serveurs ou applications et de s'assurer l'identité de l'émetteur.** Ils peuvent être notamment utilisés pour la sécurisation des flux CFT avec PGP.

- **Code Signing :**

Les certificats Code Signing **sont des certificats de signature de code qui peuvent être utilisés sur toutes les plateformes pour signer des applications et des programmes.** Les codes signés **incluent le nom de l'auteur et sont protégés contre les injections de malware et tout autre type de corruption.** Les messages d'alerte sur l'origine inconnue qui apparaissent lorsqu'un code n'est pas signé sont alors remplacés par des notifications qui affichent les informations relatives à l'auteur. Ceci réduit considérablement le nombre d'abandons de téléchargements et d'installation de programmes.

**La signature de code apporte un niveau de confiance supplémentaire au processus d'installation.**

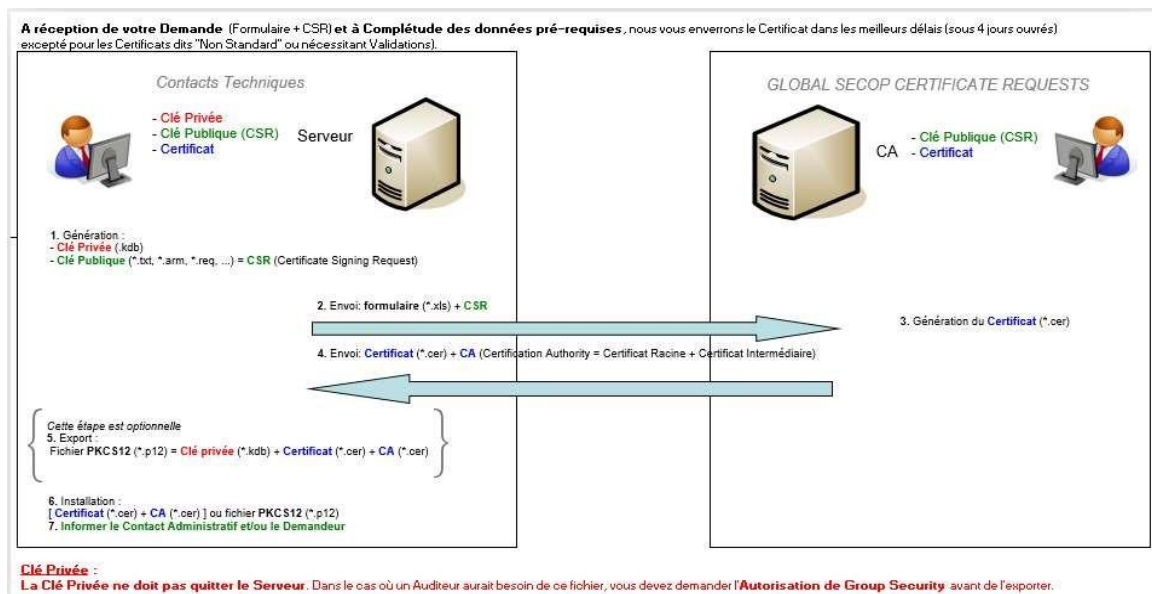


Figure : processus de création de certificat

### 3. La CSR fourni dans la demande et soumettre la génération du certificat.

(Sur Entrust si il s'agit d'une demande externe / PKI si il s'agit d'une demande interne (URL interne = sur l'intranet ; externe = sur internet)

#### **Demande de signature de certificat CSR :**

Dans une infrastructure PKI (en anglais Public Key Infrastructure soit infrastructure à clés publiques), une demande de signature de certificat (en anglais CSR pour Certificate Signing Request) est un message envoyé à partir d'un demandeur à une autorité de certification afin de demander un certificat d'identité numérique. Le format le plus commun pour les CSR est la spécification PKCS#10.

#### **Procédure :**

Avant de créer un CSR, le requérant crée une paire de clés (une publique et une privée) en gardant la clé privée secrète. Le CSR contient des informations d'identification du demandeur et la clé publique choisie par le demandeur. La clé privée correspondante n'est pas incluse dans le CSR, mais **est utilisée pour signer numériquement la demande**. Le CSR peut être accompagné d'autres informations d'identification ou des preuves d'identité requises.

Je traite 3 types de demandes certificats : création, renouvellement et révocation de sorte interne ou externe.

Exemple de traitement d'une demande de certificats externe (renouvellement)

La demande s'affiche comme ceci sur Certis :

Retour à la liste

Demande de certificat n° 348934

Modifier les contacts
Ajouter
Complément d'information
Change Status

Informations projet

Identifiant de l'application :  
Nom de votre application : test@refact.com.es  
Entité : BPS - BNP PARIBAS PERSONAL FINANCE  
Pays : France  
Créé par :

Contacts

Boîte mail générique

#	Rôle	Boîte mail
1	RSSI	

Contacts administratifs

#	Rôle	UID	Prénom	Nom	Boîte mail
1	RSSI				

Contacts techniques

#	Rôle	UID	Prénom	Nom	Boîte mail
1	Mise en œuvre				

Détail de la demande

Date: 21/06/2022  
Nouveau certificat ou renouvellement?: Renouvellement  
Usage: Externe  
Environnement: Production

Contacts techniques

#	Rôle	UID	Prénom	Nom	Boîte mail
1	Mise en œuvre				

Détail de la demande

Date: 21/06/2022  
Nouveau certificat ou renouvellement?: Renouvellement  
Usage: Externe  
Environnement: Production  
Type du certificat: Client-Serveur SSL/TLS Externe  
Usage de l'authentification PKI?: Non  
Nom du certificat ou Common name: ✓ Le nom du certificat existe dans RefWeb.  
SANs (Subject Alternative Name):  
Statut de la demande: Soumise

Commentaires: Manual reason: Request is rejected by Entrust because invalid certificate request. Cannot find domain used for the certificate. Dernière modification : 2022-06-21 18:12:45, par CERTIS API

Détail du certificat

Expire: 14/09/2022  
Entrust id: 3118251  
Plateforme: FS  
Nom du serveur:  
Organisation: BNP PARIBAS PERSONAL FINANCE SA  
Validation étendue: Standard  
CSR:

Télécharger la CSR

Fichiers

Type	Fichier
CSR	test@refact.com.es.csr

Je vérifie les informations suivantes, l'usage du certificat, le Common Name, la date d'expiration, CSR fourni et le type de demande (révocation, renouvellement, création) après je m'affecte la demande et je choisis de la rejeter ou l'accepter, dans notre cas la demande sera validée.

Je rejette la demande si le Common Name n'est pas actif dans le référencement des sites web BNP PARIBAS (REFWEB) ou la CSR n'est pas valide.

**BNP PARIBAS CERTIS** Certificate Manager FR EN Mouhame EL KHESASSI Déconnexion

Tableau de bord Nouvelle demande Mes demandes Notifications **Demandes à traiter** Demandes WAF Recherche avancée Configurations Certificats Utilisateur FAQ Contacts / Support

[Retour à la liste](#)

Demande de certificat n° 348934 Modifier les contacts Complément d'information Joindre un fichier Change Status

**Informations projet**

Identifiant de l'application :  
 Nom de votre application :  
 Entrée : **IFS - BNP PARIBAS PERSONAL FINANCE**  
 Pays : **France**  
 Créé par :  
 Prise en compte par :

**Contacts**

**Boite mail générique**

#	Rôle	Boite mail
1	RSSI	

**Contacts administratifs**

#	Rôle	UID	Prénom	Nom	Boite mail
1	RSSI				

**Contacts techniques**

#	Rôle	UID	Prénom	Nom	Boite mail
1	Mise en œuvre				

**Détail de la demande**

Date: 21/09/2022  
 Nouveau certificat ou renouvellement?: **Renouvellement**  
 Usage: **Externe**  
 Environnement: **Production**  
 Type du certificat: **Client-Serveur SSL/TLS Externe**  
 Usage de l'authentification PKI?: **Non**  
 Nom du certificat ou Common name: **test@francetelem.es**  
 SANs (Subject Alternative Name): **✓ Le nom du certificat existe dans RefWeb.**  
 Statut de la demande: **Terminée**

Commentaires: Manual reason: Request is rejected by Entrust because invalid certificate request. Cannot find domain/used for the certificate. Dernière modification: 2022-09-21 16:12:45, par CERTIS API

**Détail du certificat**

Expire: **14/09/2023**  
 Entrust id:  
 Plateforme: **IFS**  
 Nom du serveur:  
 Organisation: **BNP PARIBAS PERSONAL FINANCE SA**  
 Validation étendue: **Standard**  
 CSR: [Télécharger la CSR](#)

**Fichiers**

Type	Fichier
Certificate	
CSR	

Je vérifie bien la date d'expiration et qu'un nouveau fichier (CSR) est bien présent, un email est automatiquement envoyé aux demandeurs afin qu'il puisse récupérer son certificat sur Certis.

Pour les demandes de révocation c'est-à-dire tuer un certificat qui ne sera plus utilisable, je clique sur le bouton révoque sur Certis, l'API vérifie le bon numéro de série de certificat qui se trouve sur Certis est bien le même que sur PKI ou Entrust ainsi il procède à la révocation.

CERTIS Certificate Services (second fac... EGRID.pdf

https://certis.group.echonet/#/requests/348896

Echoet Google Console RSA Site de test RSA SAAM MobSubscrib MyAccess INCA CERTIS SELFWEB Certificate Services... Check your CSR DL... Demander un certif... Network Login ipk-faq - Home SharePoint ASAU ... Autres favoris

BNP PARIBAS CERTIS Certificate Manager

FR EN Mouhssine EL KHESSASSI Déconnexion

Tableau de bord Nouvelle demande Mes demandes Notifications Demandes à traiter Demandes WAF Recherche avancée Configurations Certificats Utilisateur FAQ Contacts / Support

Retour à la liste

Demande de certificat n° 348896

Modifier les contacts Accepter Révocation Rejeter Révocation Complément d'information Joindre un fichier Change Status

Informations projet

Identifiant de l'application :  
Nom de votre application :  
Entité : FG - ITG - IPS  
Pays : France  
Créé par :

Contacts

Boîte mail générique

#	Rôle	Boîte mail
1		

Contacts administratifs

#	Rôle	UID	Prénom	Nom	Boîte mail
1	Demandeur				

Contacts techniques

#	Rôle	UID	Prénom	Nom	Boîte mail
1	Mise en œuvre				

Le certificat sera automatiquement révoqué.

Les demandes de certificats sont bien automatisées avec Certis, mais en cas de panne je dois générer les certificats manuellement.

# **Conclusion**

Pour conclure, ce stage a été pour moi une expérience très positive. J'ai pu acquérir une meilleure compréhension du fonctionnement de l'entreprise, ainsi que des notions essentielles en matière de gestion et d'organisation.

Une des leçons que j'ai particulièrement retenues concerne l'importance de l'automatisation, en particulier dans l'utilisation d'outils tels qu'Excel et VBA. Lorsqu'on est confronté à un volume important de tâches à exécuter, l'automatisation se révèle être une solution incontournable. Bien qu'il faille investir un certain temps pour mettre en place un système d'automatisation, les bénéfices en termes d'efficacité sont considérables, avec un gain de productivité significatif.

Ce stage m'a également offert l'opportunité de travailler dans le domaine de la cybersécurité, qui est un domaine dans lequel je souhaite me spécialiser. J'ai eu la chance d'effectuer ce stage au sein d'un groupe renommé, où les infrastructures de sécurité sont très développées. J'ai donc pu découvrir différentes technologies en constante évolution, telles que Radius, qui offre une solution de sécurité.

De plus, j'ai intégré une équipe agréable où j'ai pu comprendre une fois de plus l'importance du travail d'équipe et de la répartition des tâches. J'ai également appris l'équilibre entre le plaisir, le rire et le travail. Mes collègues m'ont fait comprendre que lorsque nous avons un objectif à atteindre, il est essentiel que tout le monde soit mobilisé et prêt à contribuer. Une personne seule, peu importe ses compétences, sera confrontée à des difficultés face à une charge de travail importante.

Cette expérience m'a permis de gagner en maturité, d'élargir mes connaissances et de les renforcer, non seulement dans le domaine de l'IT, mais aussi dans d'autres domaines. J'ai été confronté à des situations réelles et concrètes où j'ai pu passer à l'action et ainsi obtenir des résultats concrets. Cette approche pratique m'a apporté une efficacité que je n'aurais probablement jamais pu acquérir uniquement par l'étude théorique.



Je tiens donc à exprimer ma gratitude envers tous mes collègues pour la confiance qu'ils m'ont accordée, leur accompagnement, leur expertise et leur sens de la pédagogie. J'ai ressenti un réel sentiment d'acceptation au sein de l'équipe.

En tant que personne constamment avide d'apprendre, j'ai réellement bénéficié d'une expérience enrichissante non seulement grâce à mes collègues, mais aussi en découvrant d'autres services et secteurs. Je tiens donc à remercier tous les alternants et toutes les personnes extérieures à mon équipe qui ont partagé avec moi leur parcours et leur métier.

J'espère sincèrement avoir l'opportunité de revenir vivre cette expérience enrichissante dans un avenir proche.

Enfin, je suis reconnaissant envers tous ceux qui ont contribué à rendre cette expérience de stage enrichissante et valorisante.