Attribution des smartphones

Introduction

Cette mission avait pour objectif de préparer et déployer des smartphones professionnels pour plusieurs utilisateurs dans le cadre d'un renouvellement de matériel. Elle comprenait la création des comptes, la gestion des certificats de sécurité, l'intégration des équipements dans l'outil EasyVista ainsi que la configuration des applications nécessaires. L'ensemble de ces actions vise à fournir aux utilisateurs un environnement mobile sécurisé et opérationnel.

I. Création des comptes Gmail

Dans un premier temps, des comptes Google ont été créés pour chaque utilisateur afin de configurer le smartphone Android et permettre *l'accès au* ***Play Store*** pour l'installation des applications nécessaires. Cette étape consistait à renseigner les informations des utilisateurs et à définir des identifiants sécurisés. Des mots de passe robustes ont été générés à l'aide du gestionnaire de mots de passe ***KeePass*** afin de garantir la sécurité des comptes.

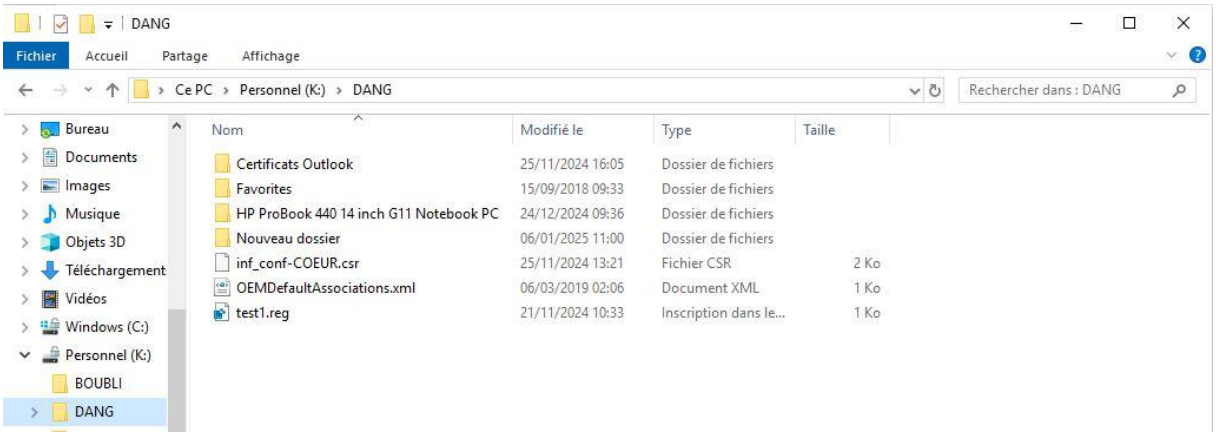
La validation des comptes a été réalisée par une *authentification par SMS*, permettant de sécuriser l'accès dès la création.
Ces comptes ont ensuite été utilisés pour configurer le client de messagerie et les différents services associés sur les smartphones.

II. Création des certificats

La création des certificats permet de ***sécuriser les échanges*** *entre les smartphones et le serveur de messagerie.*

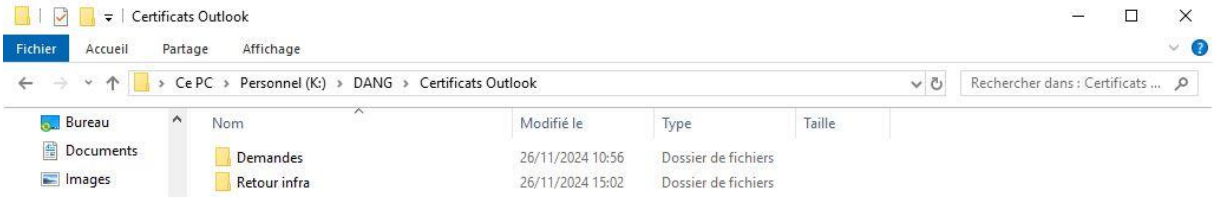
1. Préparation de l'environnement :
   Cette étape consiste à organiser les fichiers liés aux certificats en créant des dossiers dédiés aux demandes et aux certificats signés.
   Cela permet de structurer le travail et d'éviter les erreurs lors du traitement des certificats.

   A. Création de la structure de dossiers : Sur le lecteur (K:), créer un dossier nommé « Certificats Outlook ».
   Le dossier s'appelle « Certificats Outlook » car les certificats sont utilisés pour sécuriser la messagerie ***Exchange, historiquement associée à Outlook****.*
   Même si l'application utilisée est différente (comme Nine), le service de messagerie reste le même.



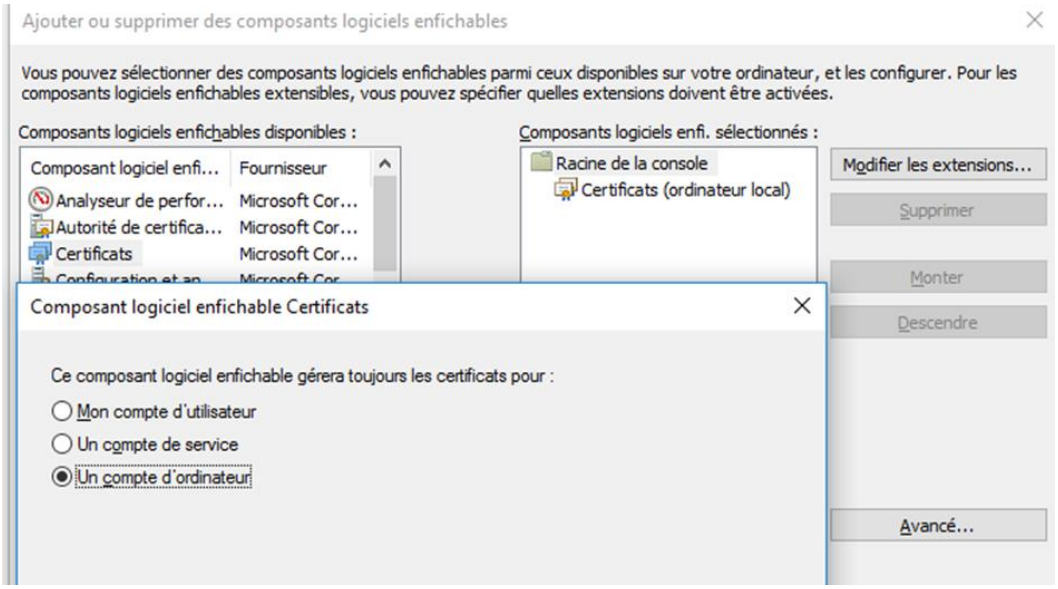
À l'intérieur de ce dossier, créer deux sous-dossiers : « Demandes » pour stocker les demandes de

certificats et « Retour infra » pour les certificats signés.



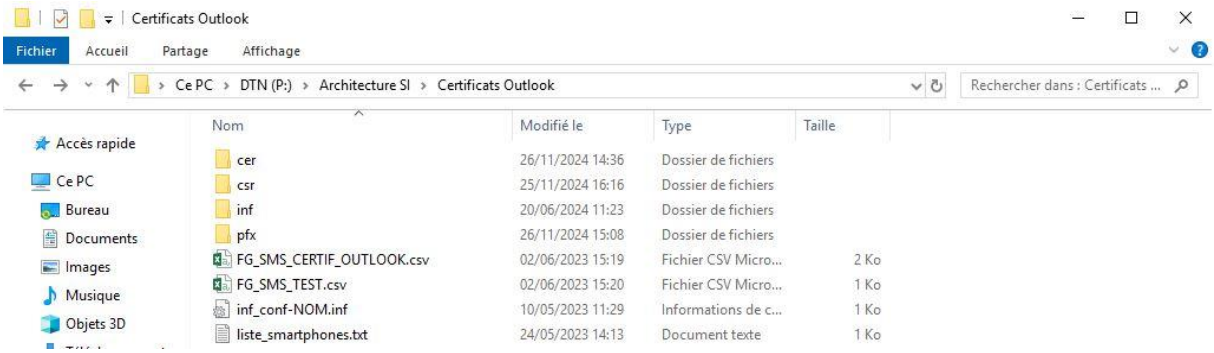
2. Génération de la demande de certificat :

A. Ouverture de la console MMC : Lancer l'outil MMC (Microsoft Management Console) et ajouter le composant « Certificats » pour un compte d'ordinateur.

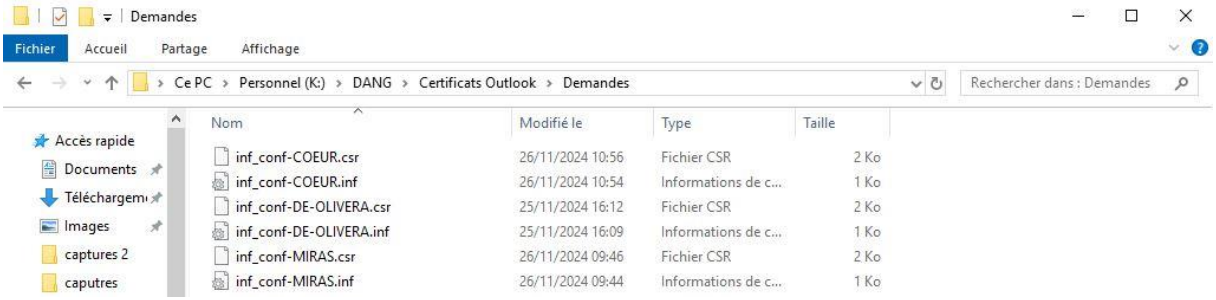


Cette étape consiste à ouvrir l'outil MMC afin d'accéder au magasin de certificats de Windows. Cela permet ensuite ***d'importer et d'exporter les certificats*** *nécessaires à la configuration du smartphone.*

B. Création du fichier de configuration : Copier le fichier « inf_conf.inf » depuis le répertoire source P:\Architecture SI\Certificats Outlook.



Puis le coller dans le répertoire « Demandes » et le renommer avec le nom de l'utilisateur (par exemple, « inf_conf-COEUR.inf »).



*Cette étape consiste à copier un fichier **.inf** existant, qui est un **modèle contenant les paramètres nécessaires à la création d'un certificat**.*
Le fichier est ensuite renommé et placé dans le dossier "Demandes" afin de préparer sa personnalisation pour l'utilisateur.

C. Personnalisation du fichier de configuration : Modifier les paramètres surlignés dans le fichier de configuration pour y insérer les initiales et le nom de l'utilisateur en majuscules. Enregistrez les modifications.

*Cette étape consiste à personnaliser le fichier .inf en modifiant les informations de l'utilisateur, notamment son nom dans le champ « Subject » et « FriendlyName ». Cette modification est nécessaire **afin que le certificat soit associé à un utilisateur précis et puisse être reconnu correctement lors de l'authentification**.*

[Version] indique le début du fichier de configuration.
Signature="$Windows NT$" indique que le fichier est destiné à être lu par Windows.

[NewRequest] annonce la partie qui contient les paramètres de la nouvelle demande de certificat.

Subject correspond à l'identité du certificat. C'est ici qu'on met le nom de l'utilisateur, par exemple COEUR, pour que le certificat soit associé à la bonne personne.

KeySpec indique l'usage principal de la clé, par exemple authentification ou chiffrement.

KeyLength=2048 indique la taille de la clé. Plus la taille est élevée, plus la sécurité est forte.

Exportable=TRUE permet d'exporter la clé privée avec le certificat. C'est indispensable pour créer ensuite le fichier .pfx.

MachineKeySet=TRUE signifie que la clé est stockée au niveau de la machine, et non uniquement dans le profil d'un utilisateur Windows.

ProviderName indique le fournisseur cryptographique utilisé par Windows pour générer la clé.

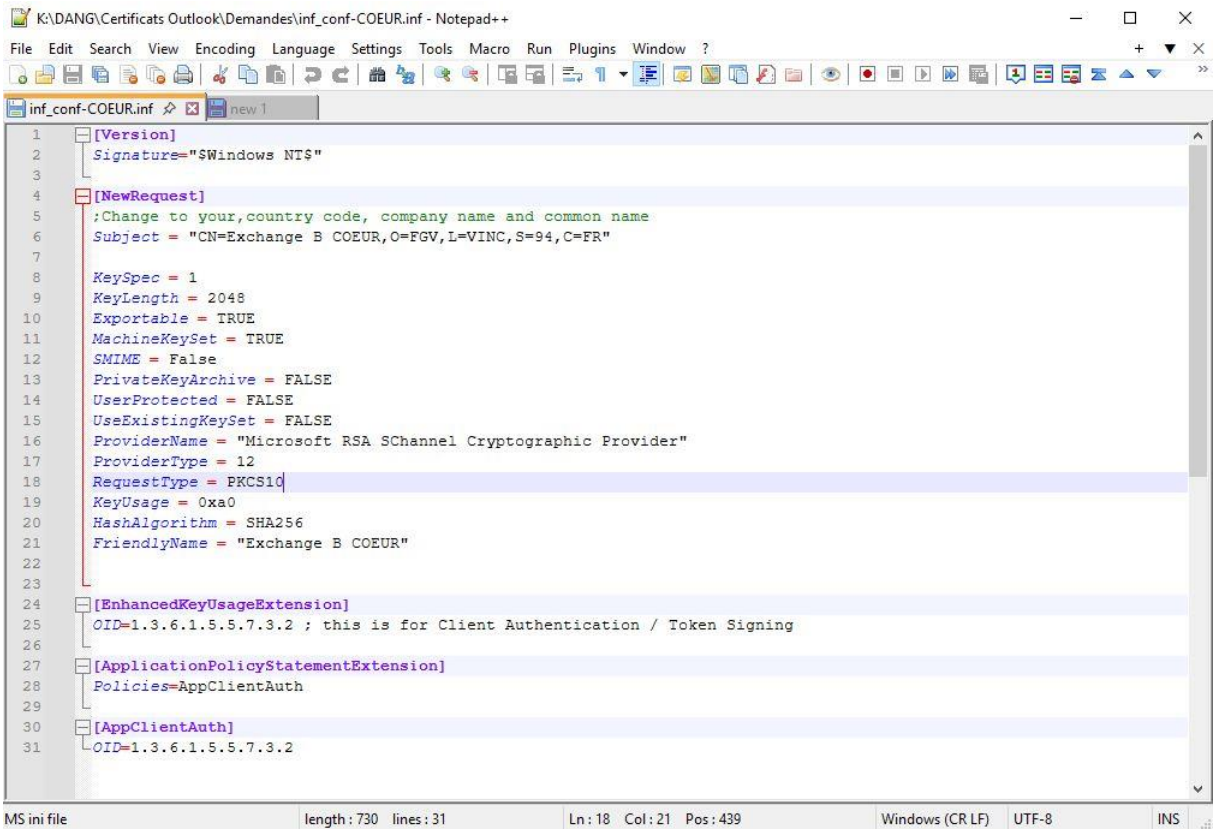
RequestType=PKCS10 indique que la demande générée sera au format CSR, donc une demande de certificat à faire signer.

KeyUsage définit ce que le certificat a le droit de faire, par exemple servir à l'authentification ou au chiffrement.

HashAlgorithm=SHA256 indique l'algorithme utilisé pour sécuriser la demande. SHA256 est un standard courant et sécurisé.

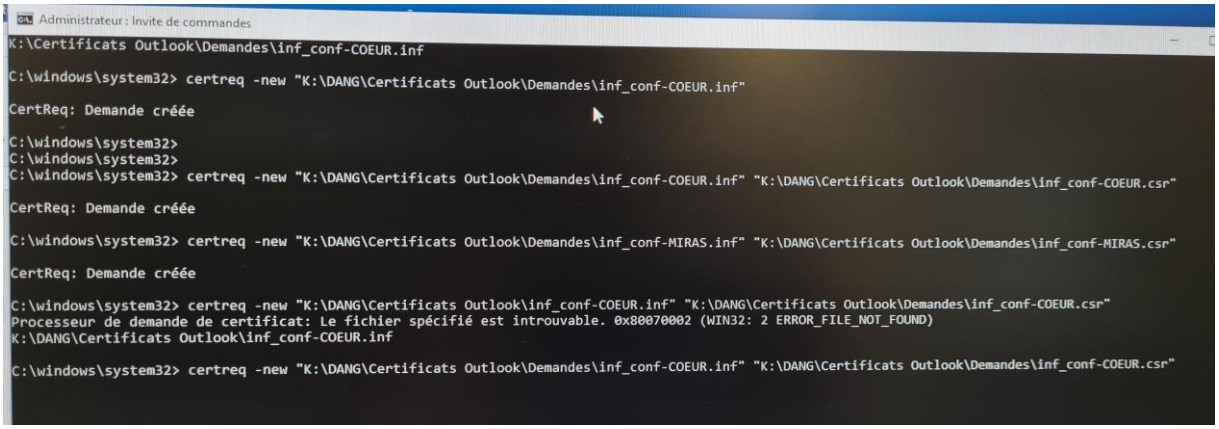
[EnhancedKeyUsageExtension] précise l'usage avancé du certificat.

OID=Client Authentication signifie que le certificat sert à authentifier un client, ici le smartphone qui se connecte au serveur Exchange.

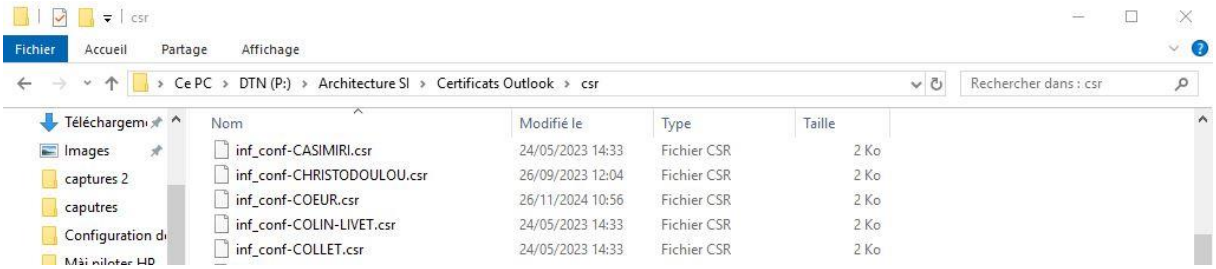


D. Génération de la demande de certificat : Exécuter la commande suivante dans une console d'administration avec les droits élevés : certreq -new « K:\Certificats Outlook\Demandes\inf_conf-COEUR.inf » « K:\Certificats Outlook\Demandes\inf_conf-COEUR.csr »

*Cette étape consiste à utiliser la **commande certreq afin de générer une demande de certificat au format CSR** à partir du fichier de configuration .inf.*
*Lors de cette opération, le système crée automatiquement une **clé privée**, qui reste stockée sur le poste, et génère un fichier **.csr contenant les informations du certificat** ainsi que la **clé publique**. Ce fichier CSR (Certificate Signing Request) constitue une demande formelle destinée à l'infrastructure, qui pourra ensuite le signer pour produire le certificat final.*



E. Envoi de la demande : Copier le fichier CSR dans le répertoire dédié aux demandes d'infrastructure P:\Architecture SI\Certificats Outlook\csr



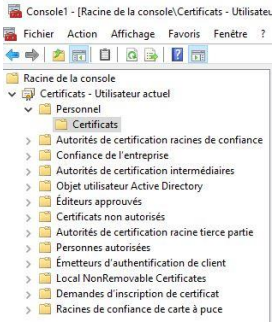
Cette étape consiste à récupérer le fichier CSR généré localement dans le dossier « Demandes » puis à le copier dans le dossier partagé de l'infrastructure. Cela permet au service d'infrastructure de traiter la demande et de générer le certificat signé.

3. Signature du certificat par l'infrastructure

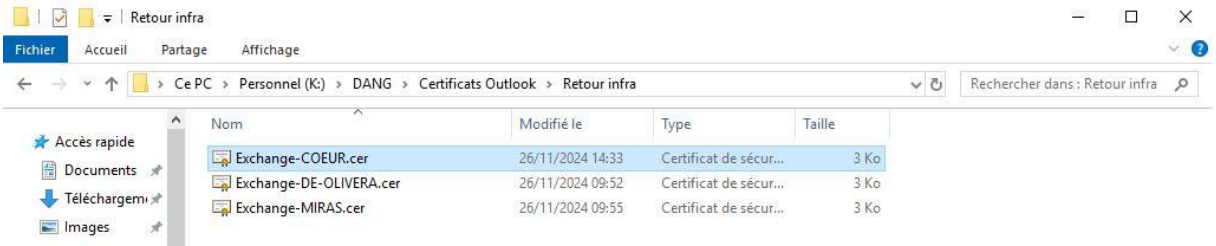
Cette étape consiste à **faire signer la demande de certificat par l'infrastructure**. Le fichier CSR est transformé en certificat au format **.cer, qui est le certificat signé contenant la clé publique**, puis placé dans le dossier « Retour infra ».

4. Installation du certificat

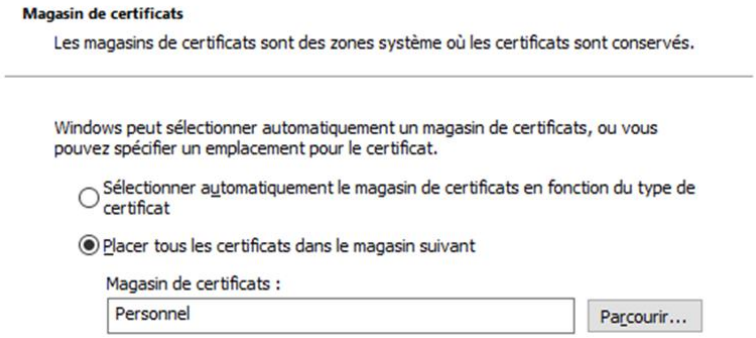
A. Importer le certificat CER dans le magasin de certificats personnel de l'utilisateur : Lancer l'outil MMC (Microsoft Management Console). Ajouter le composant « Certificats » pour un compte d'ordinateur. Dans le volet d'actions, faire un clic droit sur « Certificats », puis sélectionner « Toutes les tâches » > « Importer ».



Suivre les instructions de l'assistant pour sélectionner le fichier du certificat à importer (par exemple, « Exchange-CŒUR.cer »).



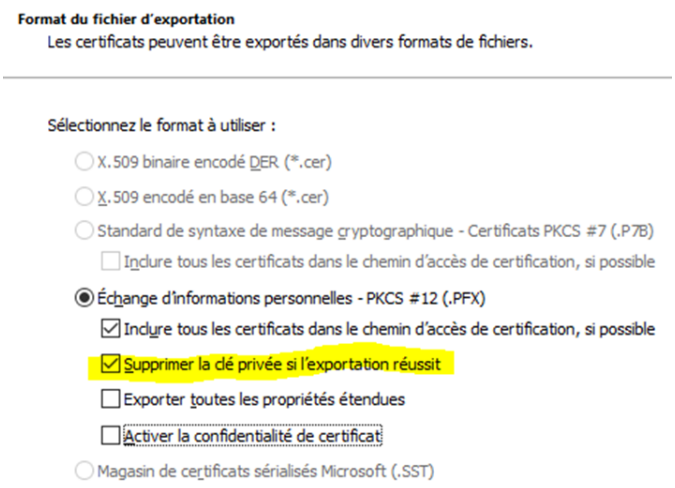
Indiquer que le certificat doit être placé dans le magasin « Personnel »



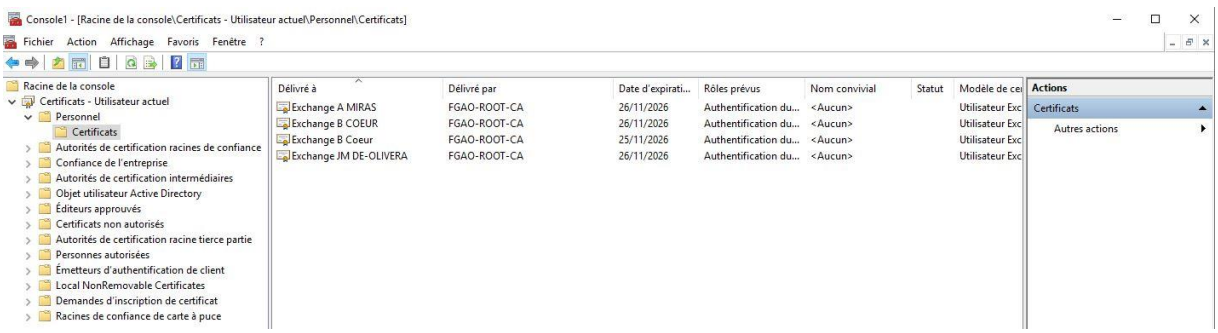
*Cette étape consiste à importer le certificat au format .cer dans le magasin de certificats de Windows, plus précisément dans le magasin « Personnel », **afin de l'associer à la clé privée** générée précédemment. Cela **permet aux applications de le retrouver pour l'authentification** et de pouvoir ensuite l'exporter pour une utilisation sur le smartphone.*

B. Exportation du certificat avec clé privée :

Dans la console MMC, sélectionner le certificat à exporter. Lancement de l'assistant d'exportation : Dans le volet d'actions, cliquer droit sur le certificat (par exemple : Exchange B Cœur), puis

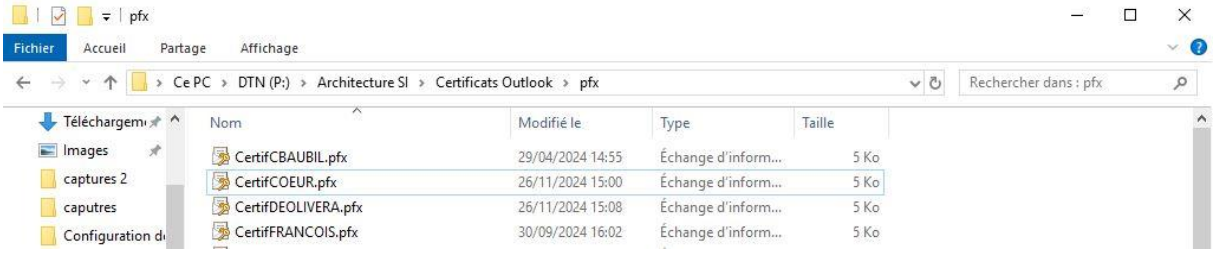


sélectionner « Toutes les tâches » > « Exporter ».



Suivez l'assistant d'exportation du certificat :
Cocher l'option pour exporter la clé privée avec le certificat.

Puis, il faut définir un mot de passe fort pour protéger la clé privée. Il est d'ailleurs recommandé d'utiliser un mot de passe généré par un gestionnaire de mots de passe comme KeePass.
Ensuite, nous devons choisir le format PFX pour exporter le certificat et sa clé privée dans un seul fichier et enfin, spécifier le chemin et le nom du fichier à exporter.



Cette étape consiste à exporter le certificat avec sa clé privée depuis le magasin de certificats de Windows afin de créer un fichier au format .pfx. Ce format permet de ***regrouper le certificat et la clé privée dans un seul fichier****, nécessaire pour une utilisation sur un autre appareil. Un mot de passe fort est défini afin de protéger la clé privée, et le fichier est ensuite enregistré dans un emplacement sécurisé.*

III. Attribution d'un smartphone à un utilisateur via l'inventaire EasyVista

L'objectif de cette étape est d'associer de manière unique un smartphone à un utilisateur au sein du parc informatique de l'entreprise, afin d'assurer la traçabilité des équipements.
Cette opération nécessite l'utilisation d'un smartphone à attribuer, d'un scanner de codes-barres permettant d'identifier l'équipement, ainsi que de l'outil EasyVista, utilisé pour la gestion de l'inventaire informatique.

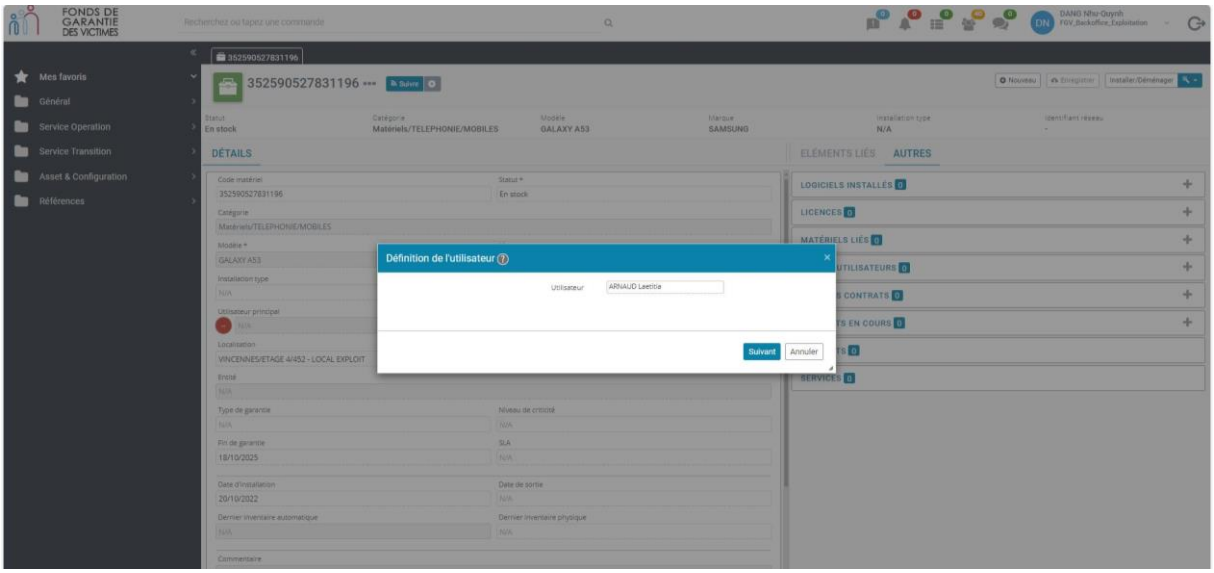
1. Préparation

Le scanner de codes-barres est utilisé pour identifier le smartphone à attribuer.
Une fois scanné, l'équipement est automatiquement recherché dans l'interface EasyVista afin d'accéder à sa fiche détaillée.

2. Attribution à l'utilisateur

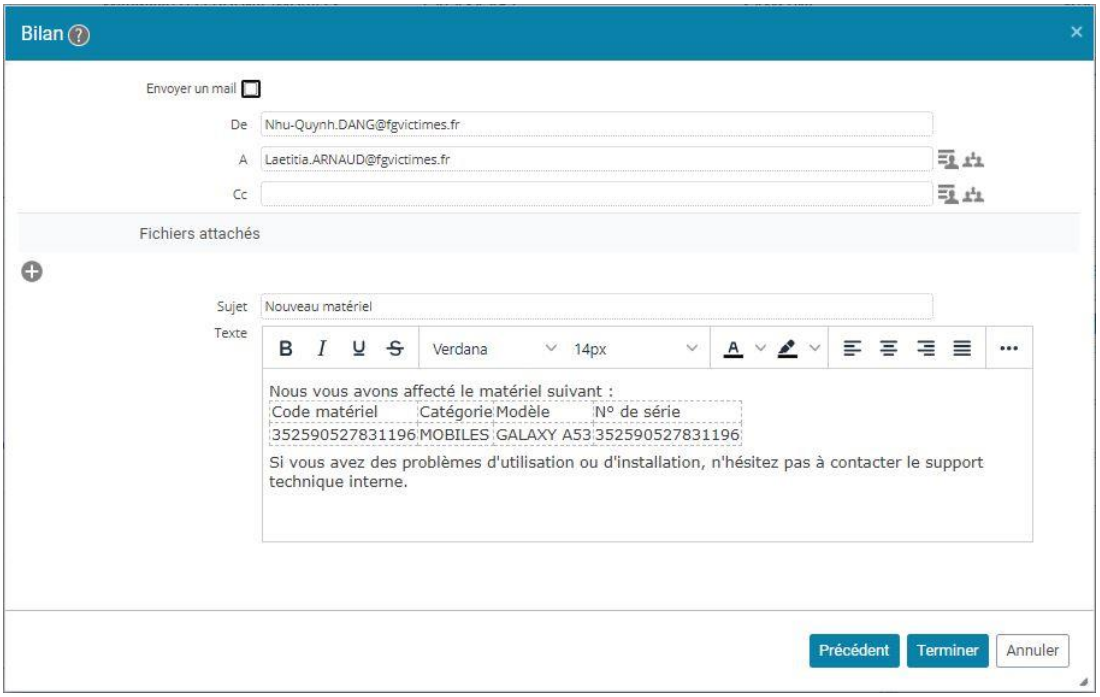
Cette étape consiste à configurer le smartphone afin de le rendre opérationnel pour l'utilisateur, notamment en installant les applications nécessaires et en appliquant les paramètres de sécurité.

Sur la fiche détaillée du smartphone, le bouton « Installer/Déménager », permet de lancer la procédure d'attribution.
La fenêtre « Définition de l'utilisateur » s'affichera demandant de sélectionner l'utilisateur à qui attribuer le smartphone.



Après avoir indiqué le nom du nouvel utilisateur et faire suivant pour arriver sur « localisation et entité », ici nous indiquerons le nouveau statut du smartphone en mettant « En service ».

Le Bilan de la procédure enverra un message pour le nouvel utilisateur, confirmant que le smartphone lui a été attribué et qu'en cas de problème, elle peut contacter le service de support.



Cette configuration permet de garantir un usage sécurisé et fonctionnel du smartphone dans l'environnement professionnel.

IV. Nine

La configuration du client de messagerie Nine a été réalisée afin de permettre aux utilisateurs d'accéder à leur messagerie professionnelle depuis leur smartphone de manière sécurisée.

Pré-requis :

- ✓ Avoir reçu le certificat Outlook et le mot de passe du certificat par mail « Certif*NOM*.pfx », dans sa boite mail GMAIL.

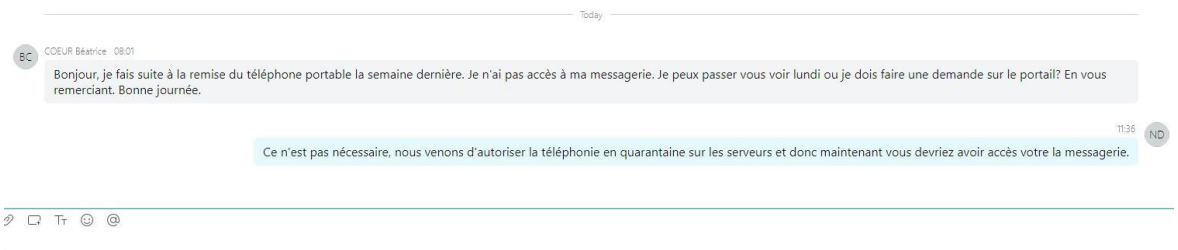
Sur le Smartphone :

Etape 1 : Installation du certificat

- Le certificat de sécurité est installé à partir du fichier transmis par messagerie électronique dans la boîte Gmail de l'utilisateur.
- Le fichier joint au format PFX est ouvert, puis le mot de passe associé est renseigné afin de permettre son importation sur le smartphone.
- Lors de l'installation, le type de certificat est sélectionné, puis celui-ci est enregistré dans le système.
- Le certificat est ensuite renommé « Certificat Outlook » afin de faciliter son identification.
- Une fois ces opérations réalisées, le certificat est correctement installé sur l'appareil.

Etape 2 : Installation du client de messagerie mobile

- Le client de messagerie **Nine – Email & Calendar** est installé depuis le PlayStore afin de permettre l'accès à la messagerie professionnelle sur le smartphone.
- Une fois l'application lancée, la configuration du compte est réalisée manuellement en renseignant l'adresse de messagerie professionnelle de l'utilisateur ainsi que ses identifiants Windows.
- Le type de compte Exchange est sélectionné, puis les paramètres du serveur sont configurés, notamment le domaine, le nom d'utilisateur et l'adresse du serveur de messagerie.
- Le certificat précédemment installé est ensuite associé au compte afin de sécuriser l'authentification auprès du serveur.
- Les autorisations nécessaires, telles que l'accès aux contacts et à l'agenda, sont accordées afin de garantir le bon fonctionnement de l'application. Un mot de passe est également défini pour sécuriser l'accès à l'application, et le chiffrement des données est activé.
- Une fois la configuration terminée, le smartphone peut se connecter aux serveurs Exchange du Fonds de Garantie. Toutefois, l'appareil est initialement placé en zone de quarantaine et doit être validé par un administrateur avant que la synchronisation des données ne soit effective.



Etape 3 : Configuration du mobile

- Après l'installation des applications, le smartphone est configuré afin de garantir un usage sécurisé et conforme aux exigences de l'entreprise.
- Cette configuration comprend la modification du code PIN de la carte SIM ainsi que la mise en place d'un mode de déverrouillage sécurisé (code, schéma ou biométrie).
- Ces paramètres permettent de protéger l'accès à l'appareil et aux données professionnelles en cas de perte ou de vol.

Etape 4 : Configuration du client de messagerie mobile :

- Le client de messagerie est ensuite paramétré afin d'adapter son fonctionnement aux besoins de l'utilisateur et aux exigences de sécurité de l'entreprise.
- La période de synchronisation des e-mails est configurée afin de définir la durée de conservation des messages sur le smartphone, permettant ainsi de limiter le volume de données stockées.
- Les paramètres de sécurité sont également ajustés, notamment la fréquence de demande du mot de passe, qui peut être modifiée (par exemple de 5 minutes à plusieurs heures) afin de trouver un équilibre entre sécurité et confort d'utilisation.
- Enfin, une licence Nine est attribuée à l'utilisateur via les paramètres de l'application, en activant une licence en volume, ce qui permet de débloquer l'ensemble des fonctionnalités professionnelles du client de messagerie.

Conclusion

Cette activité a permis de mettre à disposition des smartphones sécurisés et fonctionnels pour les utilisateurs, en assurant notamment une authentification fiable grâce aux certificats. Elle m'a permis de mieux comprendre les enjeux liés à la sécurité des équipements mobiles ainsi que les processus de déploiement en environnement professionnel. J'ai ainsi développé des compétences en gestion de certificats, en configuration de terminaux et en organisation du déploiement.