



Documentation technique

CRYPTO SMART

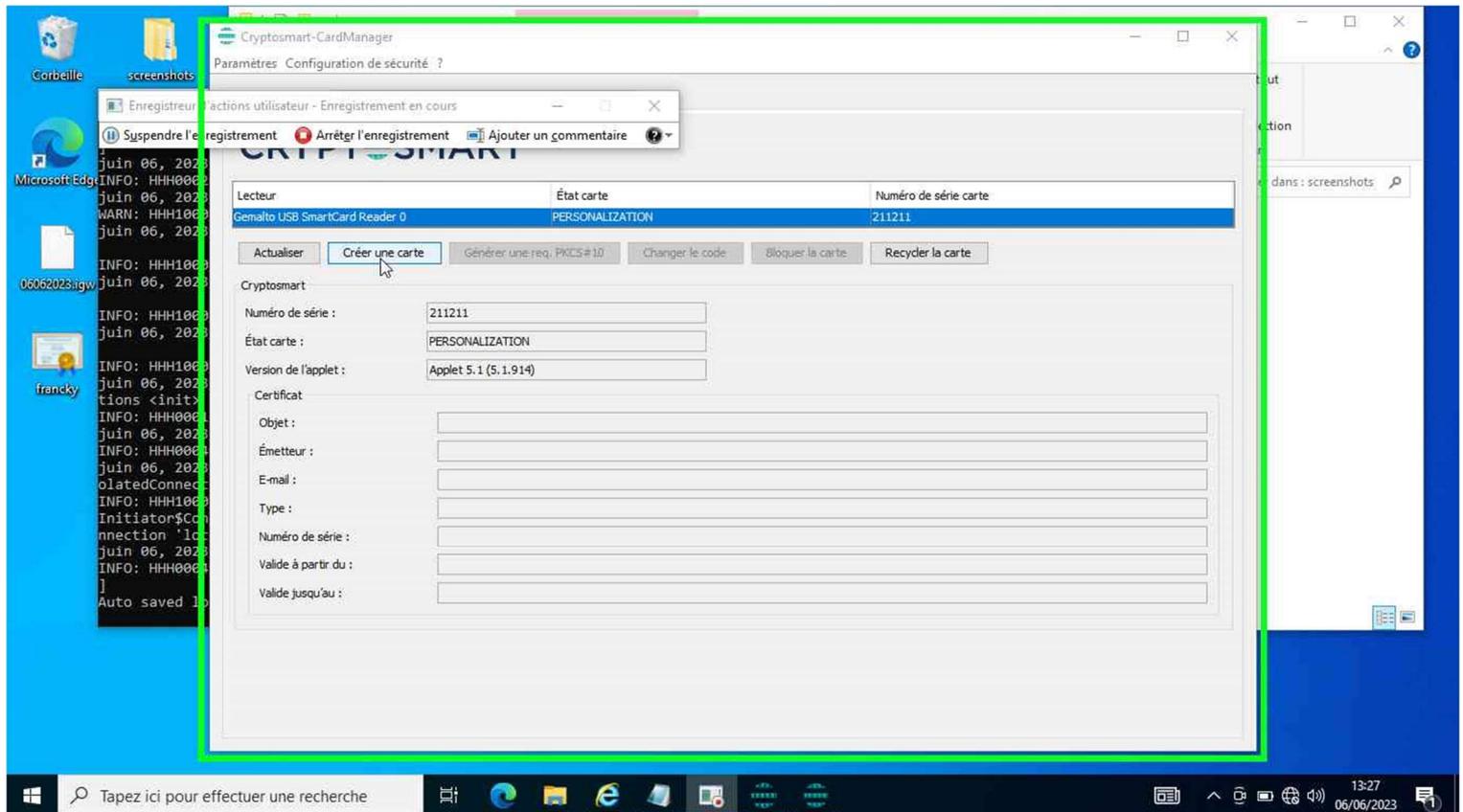
BY ERCOM

Sommaire

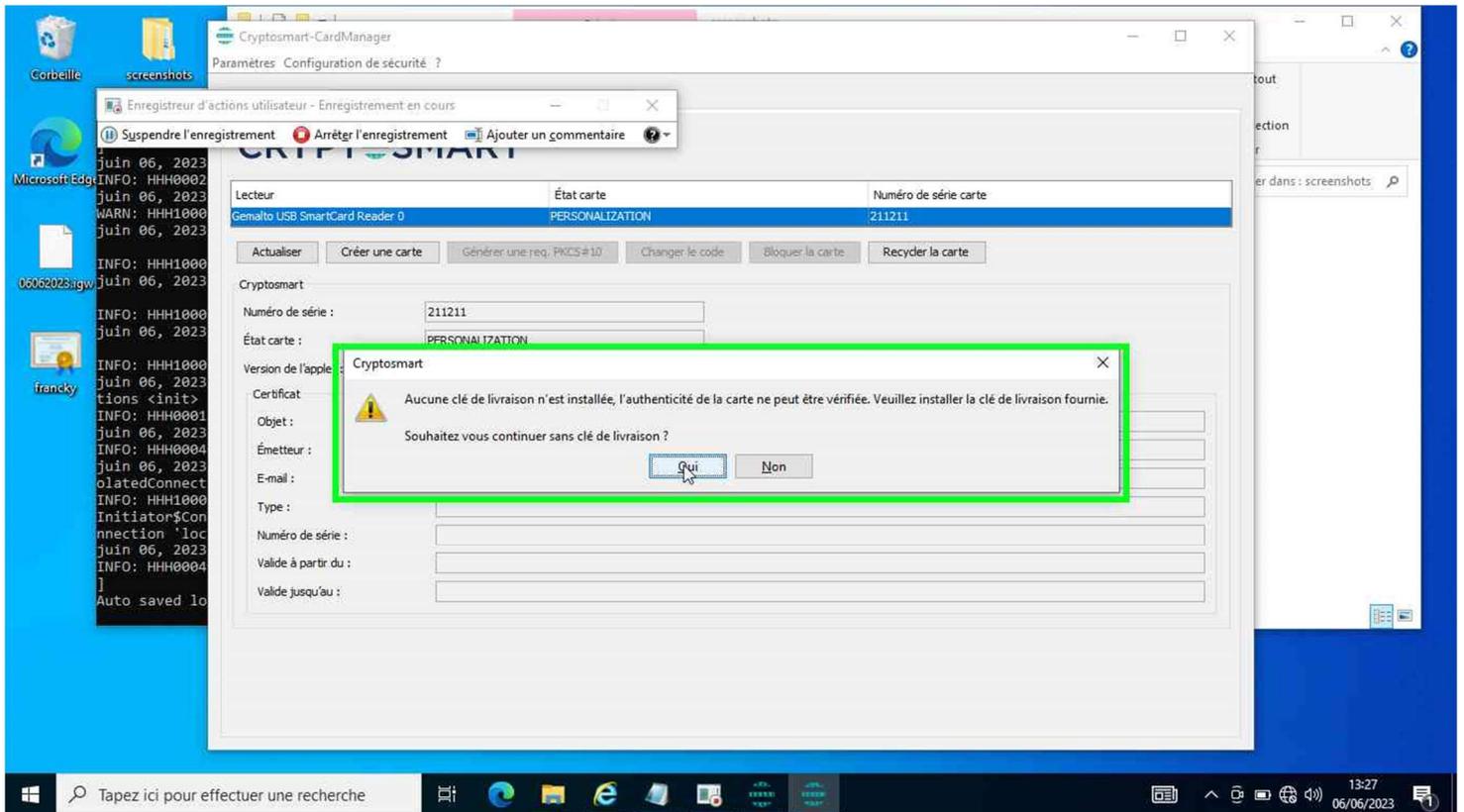
<u>1.Création d'une carte serveur avec Cryptosmart-CardManager</u>	3
<u>2.Création d'une carte client avec Cryptosmart-CardManager</u>	7
<u>3.Exportation d'un certificat</u>	10
<u>4.Infos utiles (A lire !)</u>	12

1.Création d'une carte serveur avec Cryptosmart-CardManager

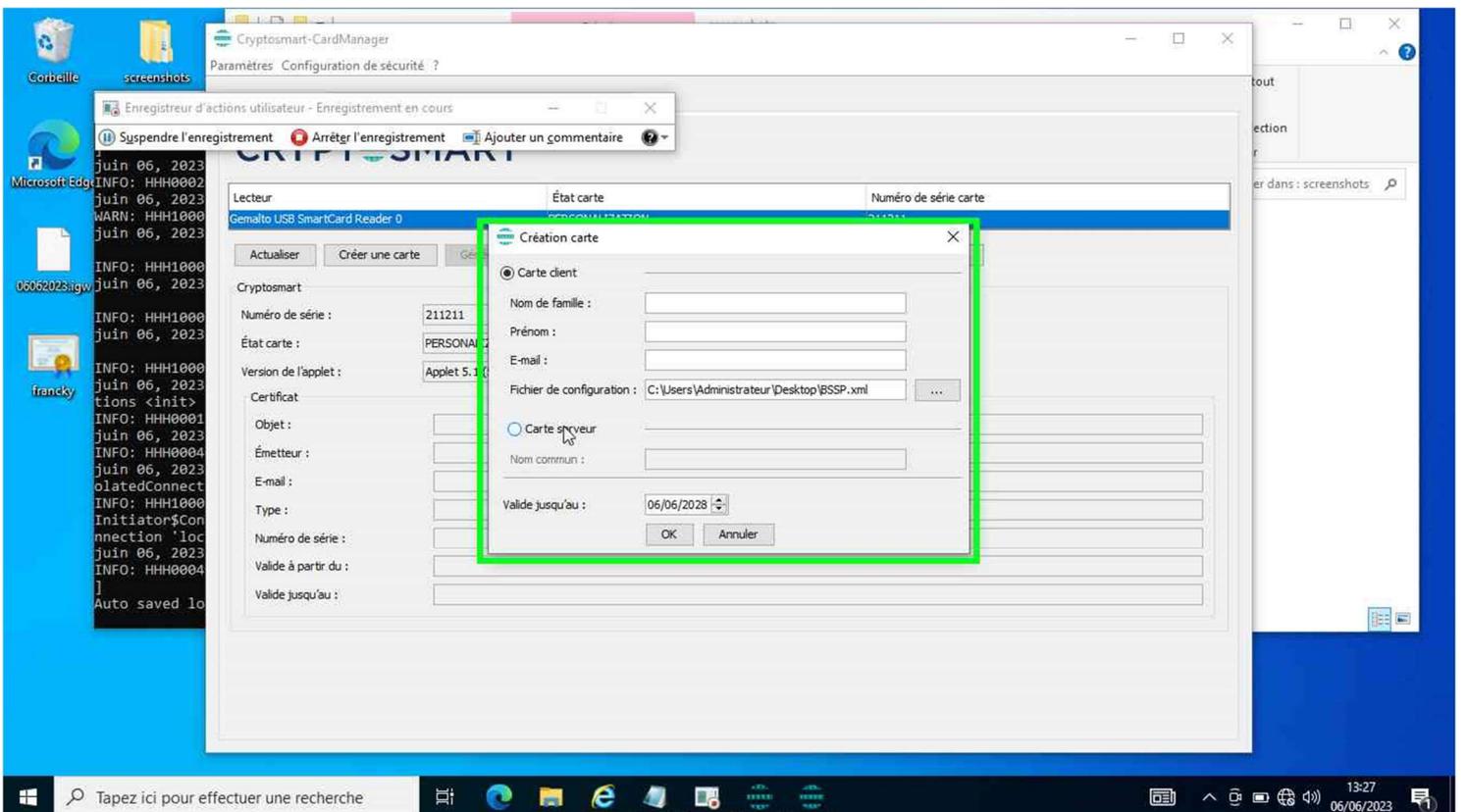
- Exécuter Cryptosmart-CardManager en tant qu'Administrateur
- Insérer la carte dans le port USB
- Cliquer sur le bouton « Actualiser » pour afficher la carte dans l'appli



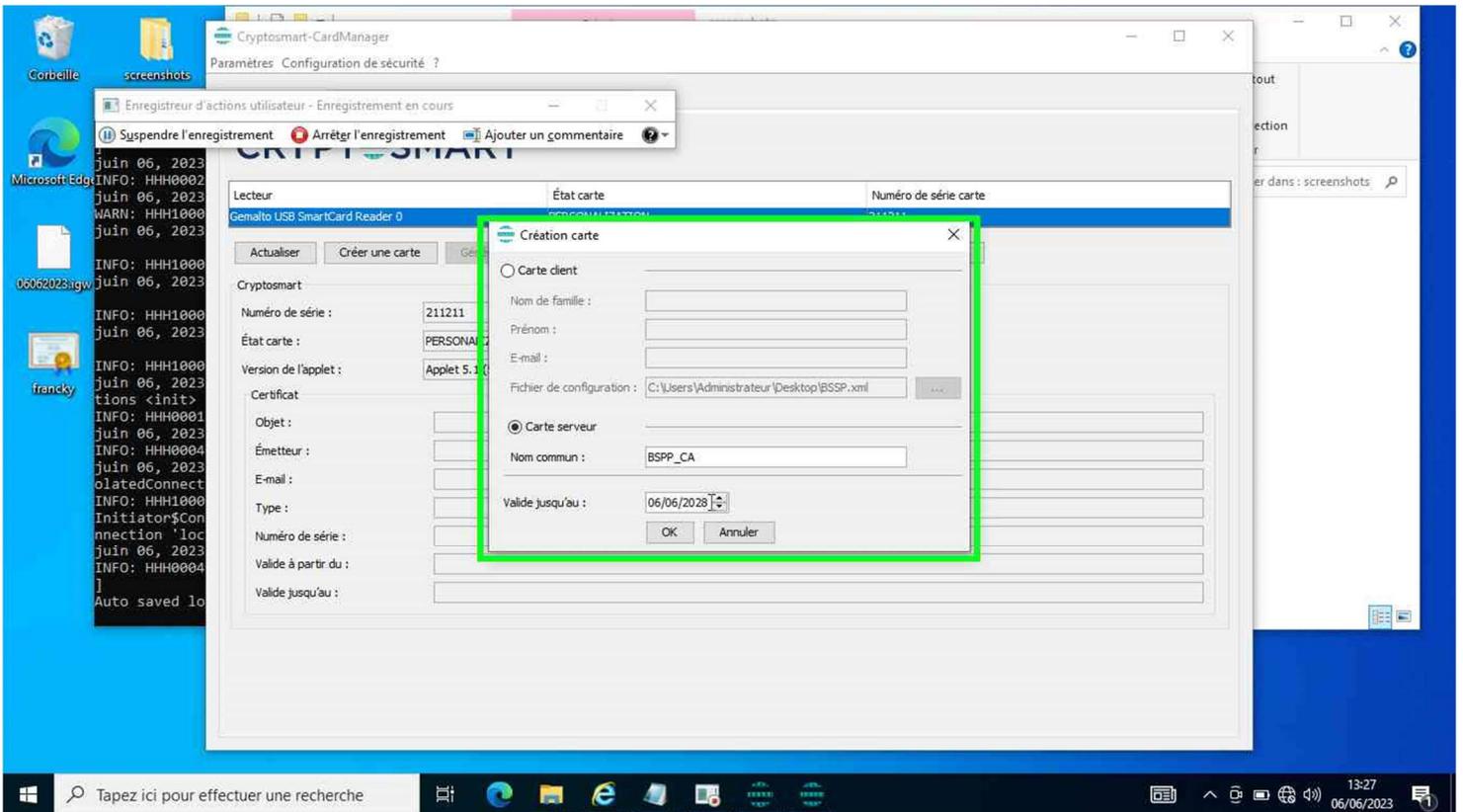
1-Cliquer sur « Créer une carte »



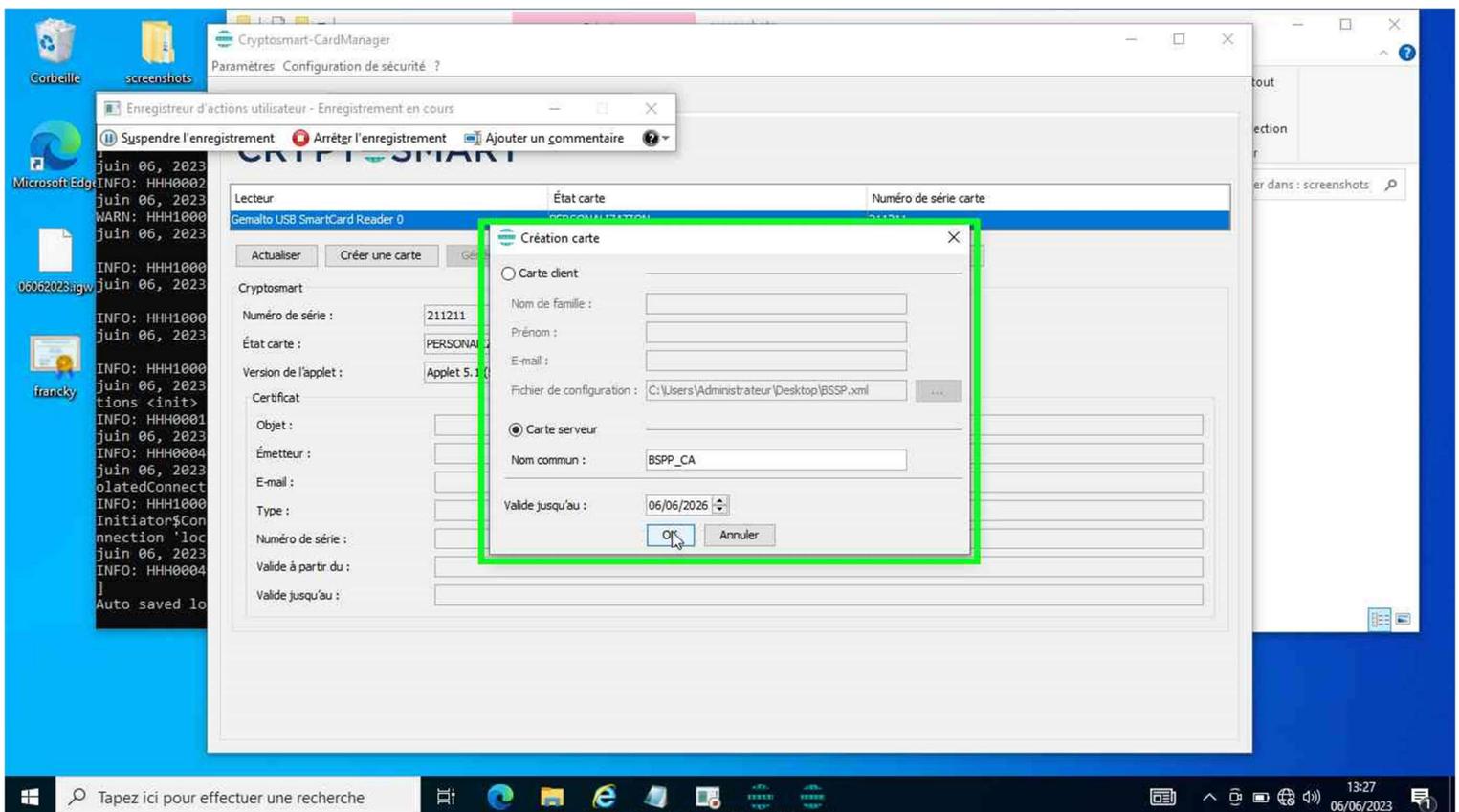
2-Appuyer sur « oui »



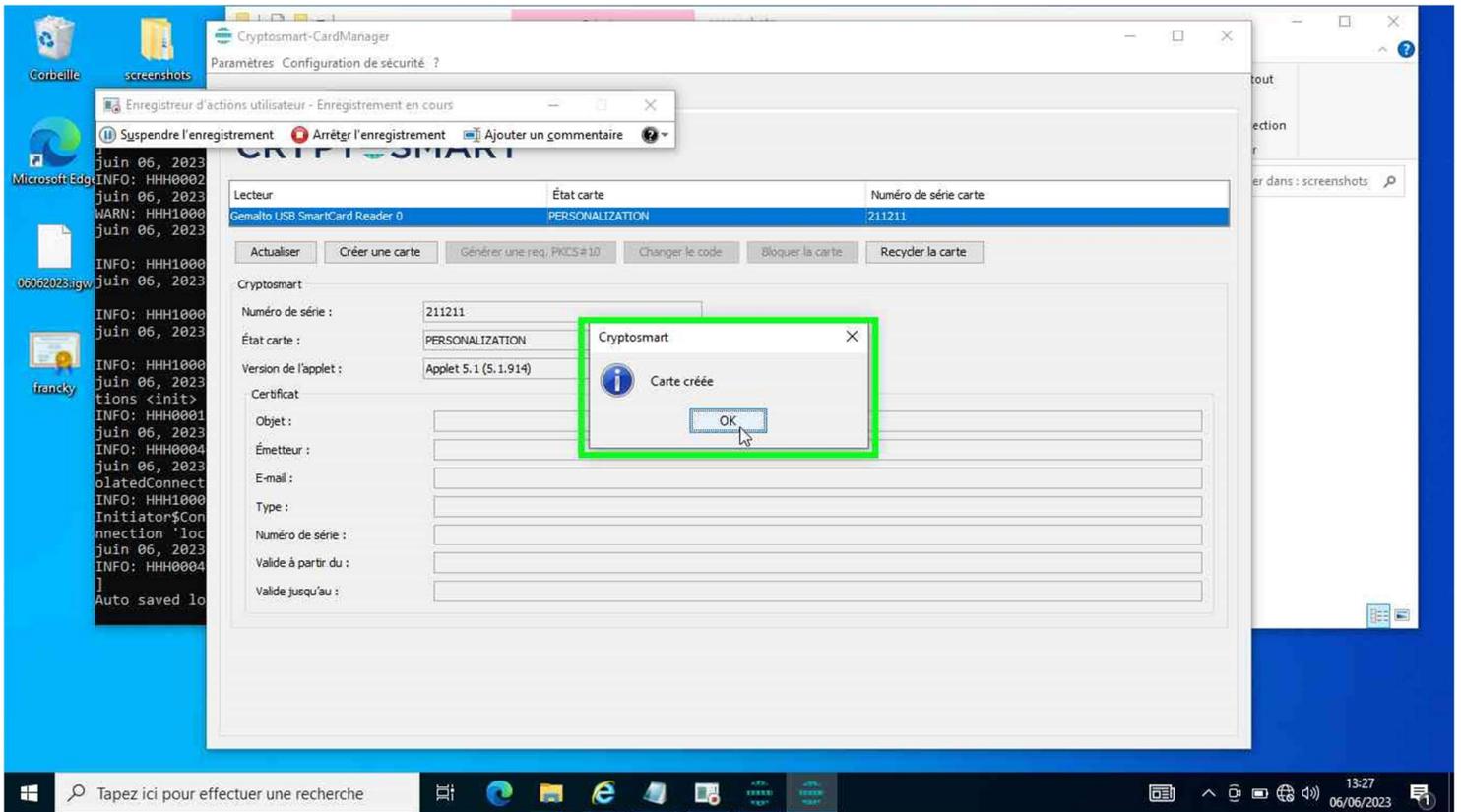
3-Sélectionner « carte serveur »



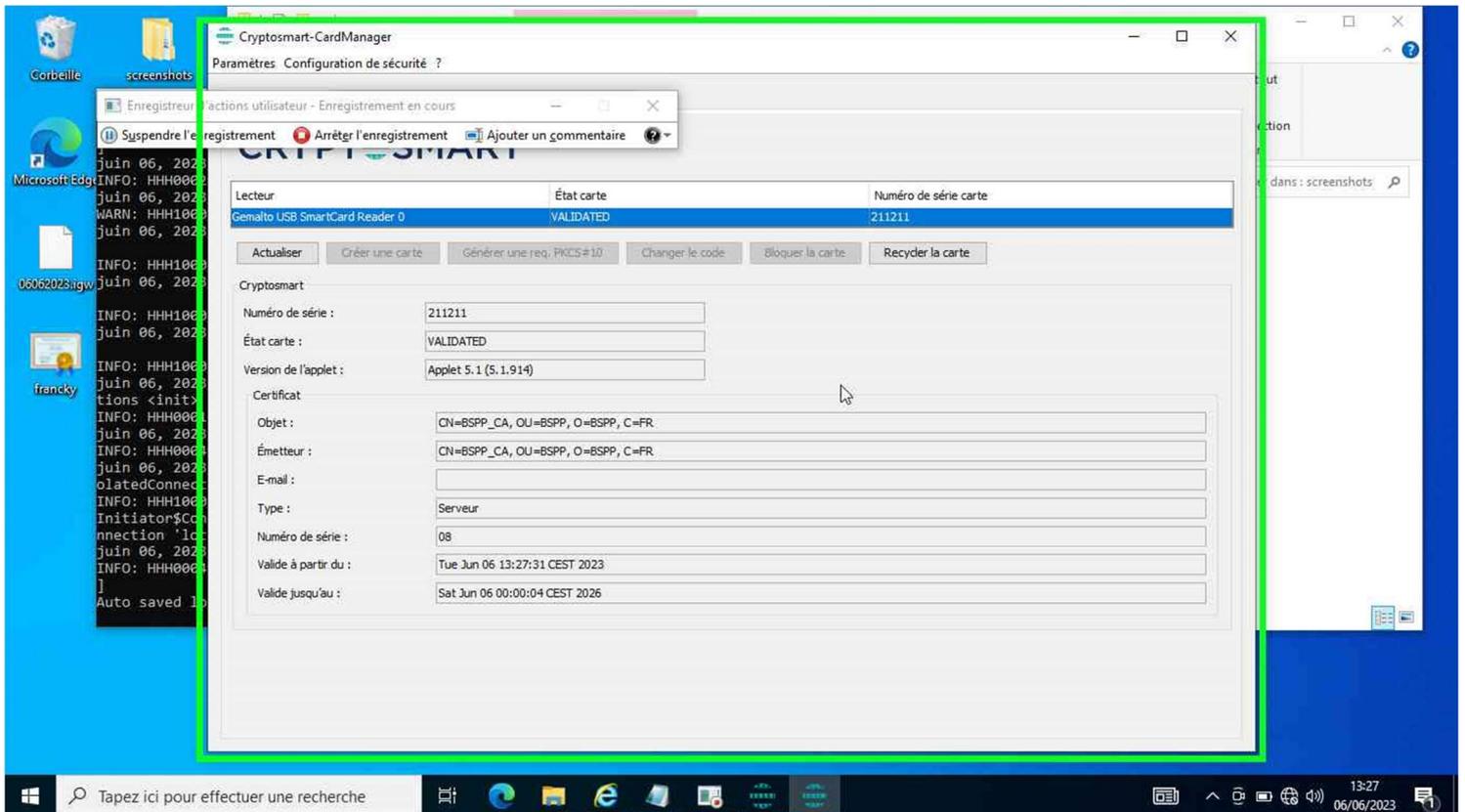
4- Dans « Nom commun », entrez : BSPP_CA



5-La carte a une durée de validité de 3 ans. Choisissez l'année actuelle +3 (2026 si on est en 2023)



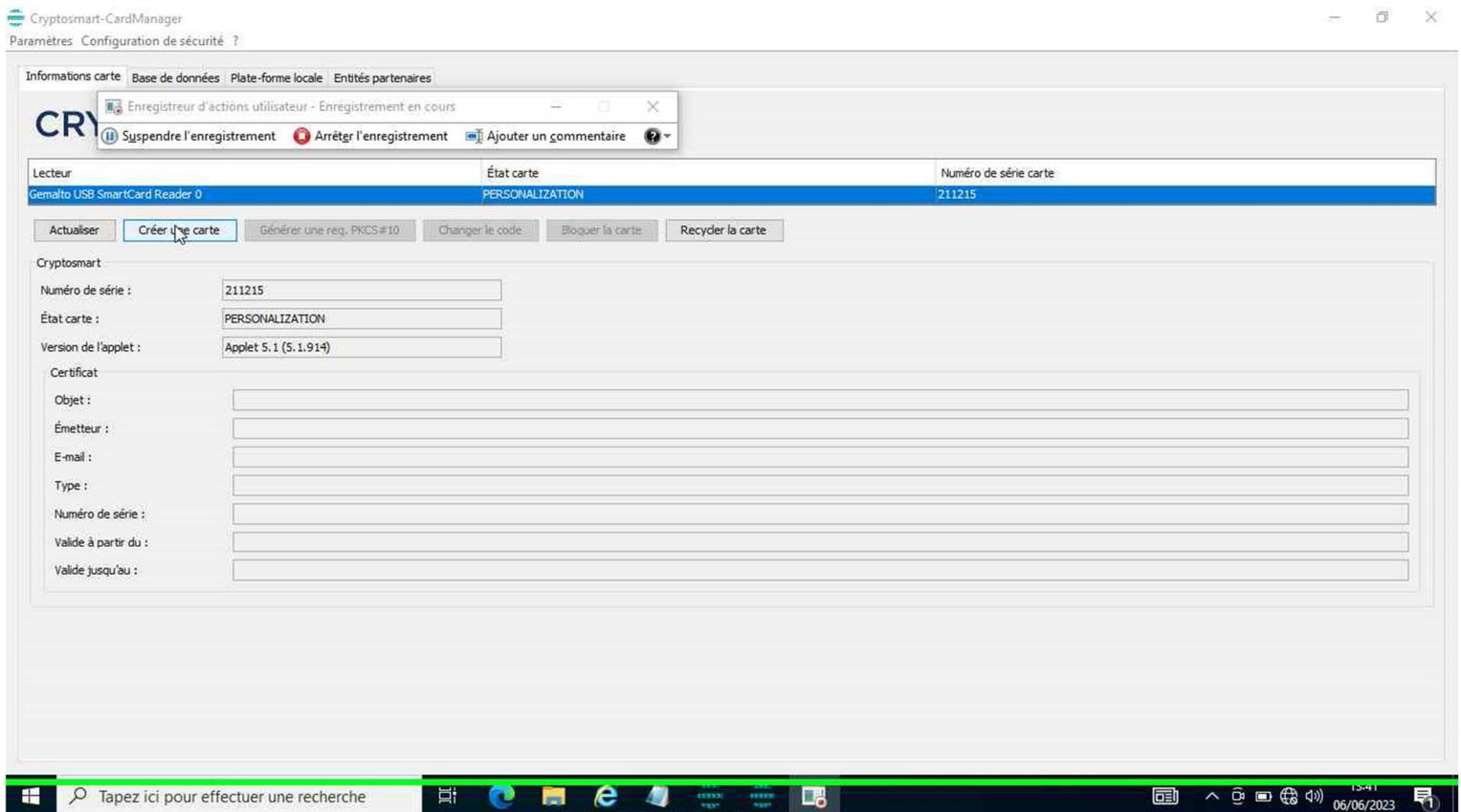
6-La carte est créée



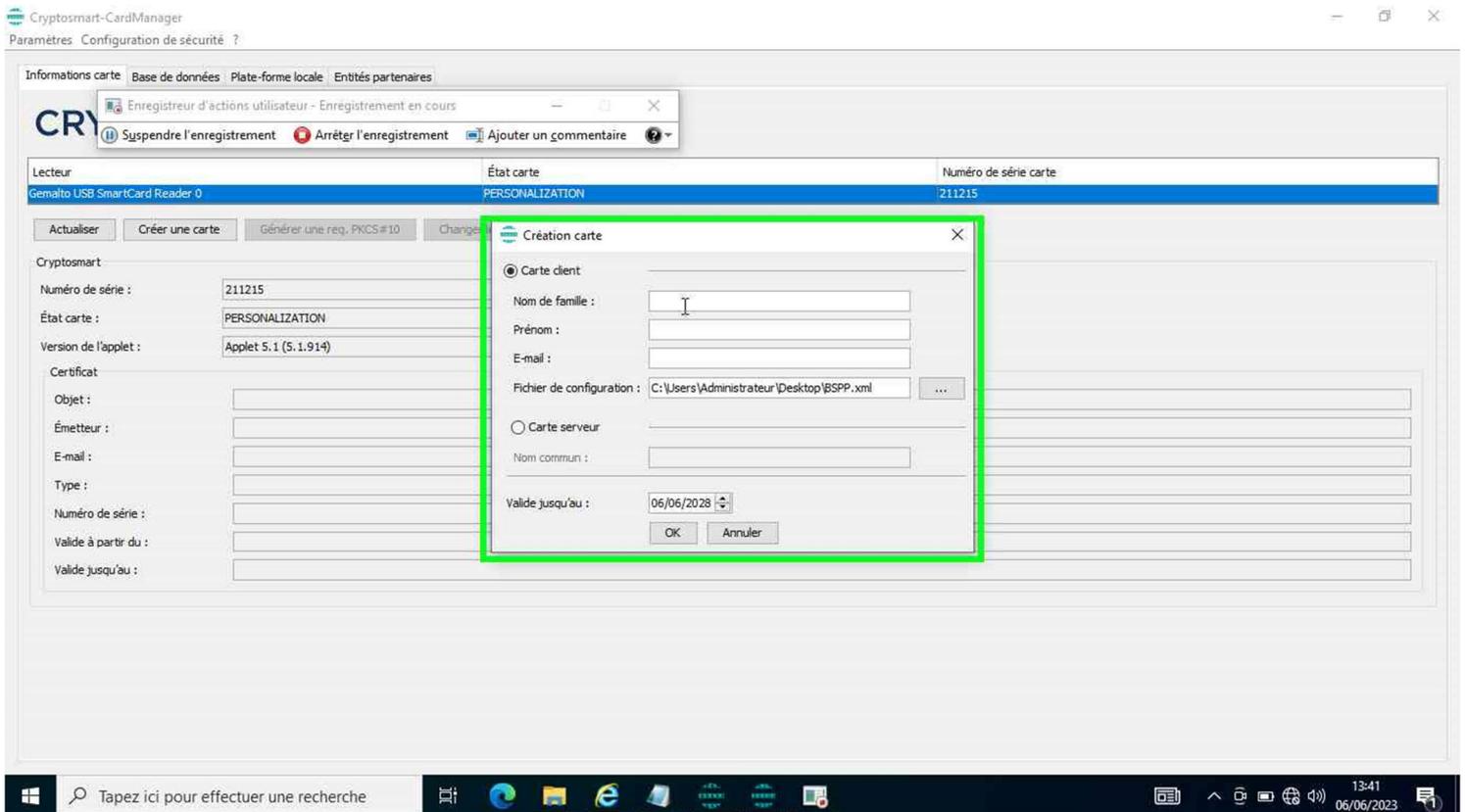
Enjoy !

2. Création d'une carte client avec Cryptosmart-CardManager

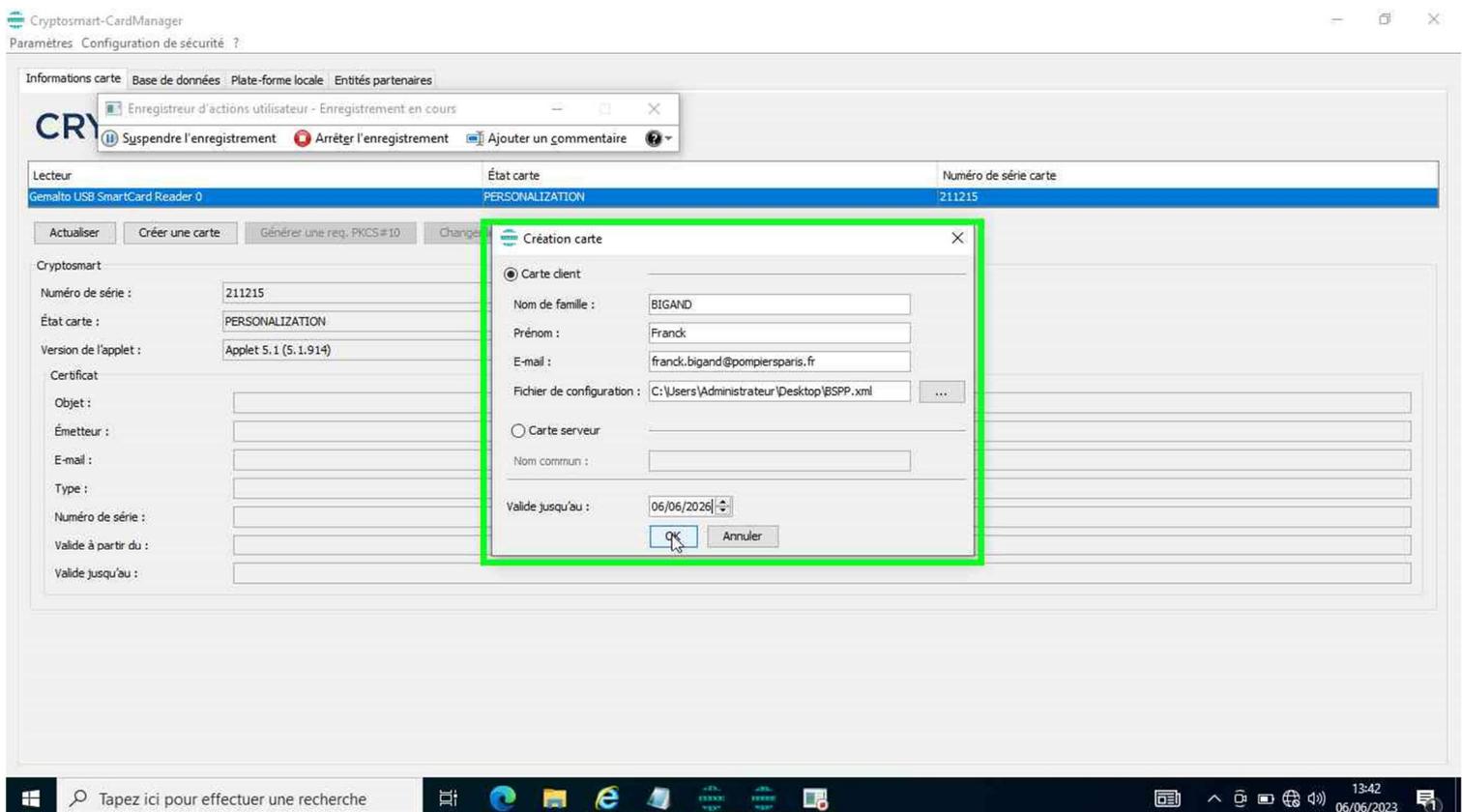
- Exécuter Cryptosmart-CardManager en tant qu'Administrateur
- Insérer la carte dans le port USB
- Cliquer sur le bouton « Actualiser » pour afficher la carte dans l'appli



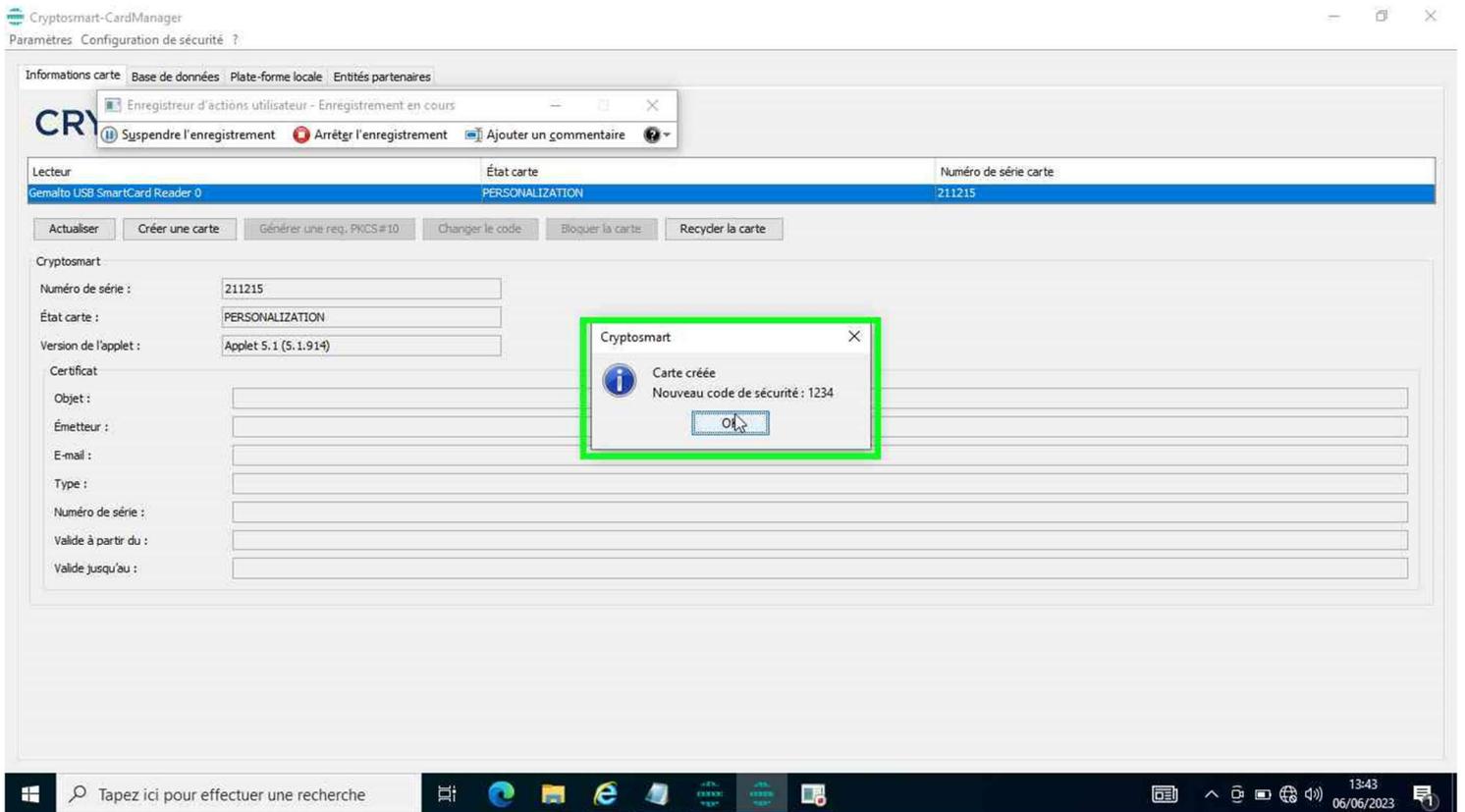
1-Créer une carte



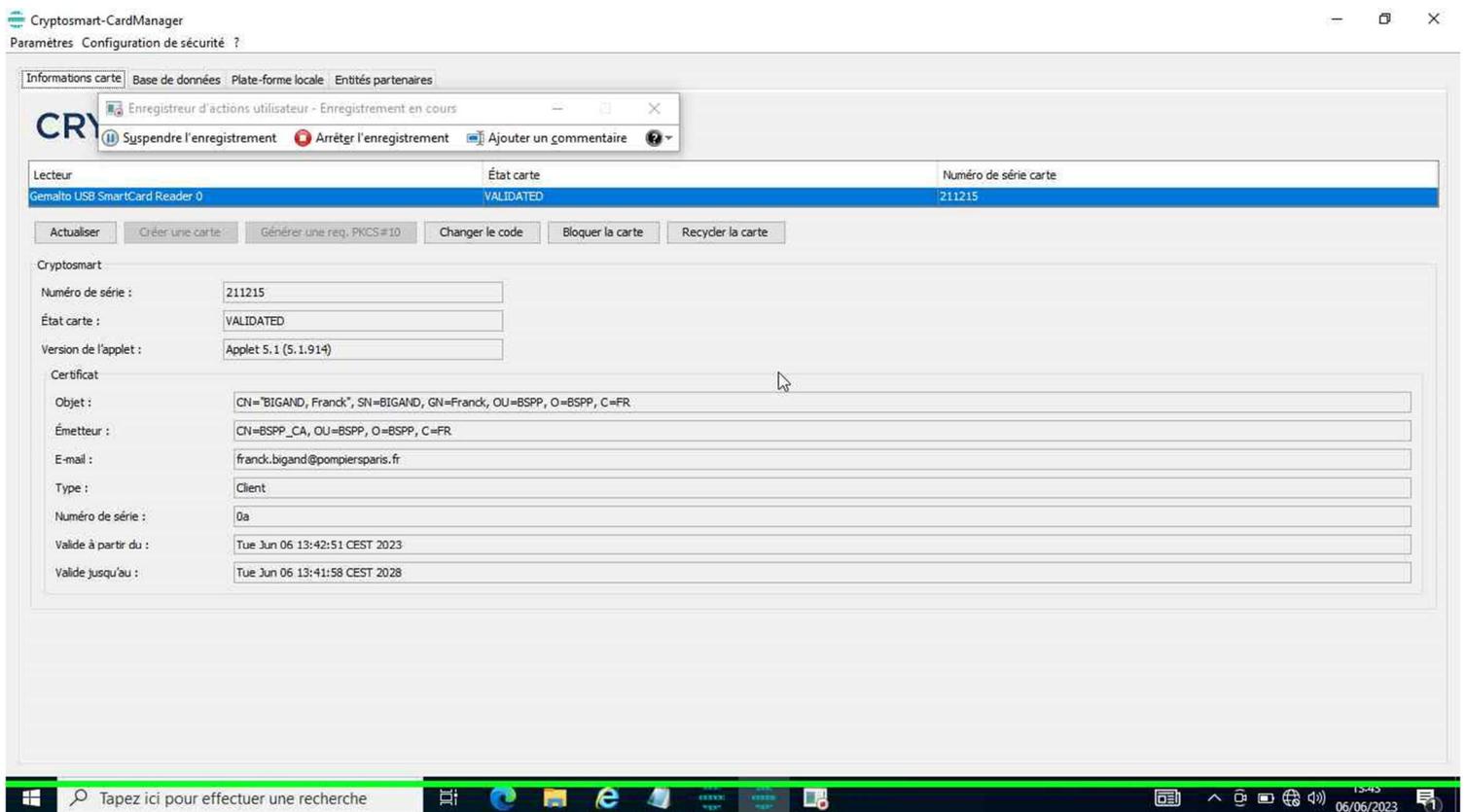
2-Sélectionner « Carte client » et entrer toutes les infos en donnant votre boîte mail BSPP.



3-La carte a une durée de validité de 3 ans. Choisissez l'année actuelle +3 (2026 si on est en 2023)



4-La carte est créée. Un code de sécurité est fourni. Ce code sera demandé lors de la connexion au VPN.



5-Enjoy ta carte frero

3. Exportation d'un certificat

Après chaque création de carte client, un certificat est créé.

Ce dernier doit être exporté et gardé dans un gestionnaire, il sera associé au code PUK qui servira en cas de perte du code de sécurité.

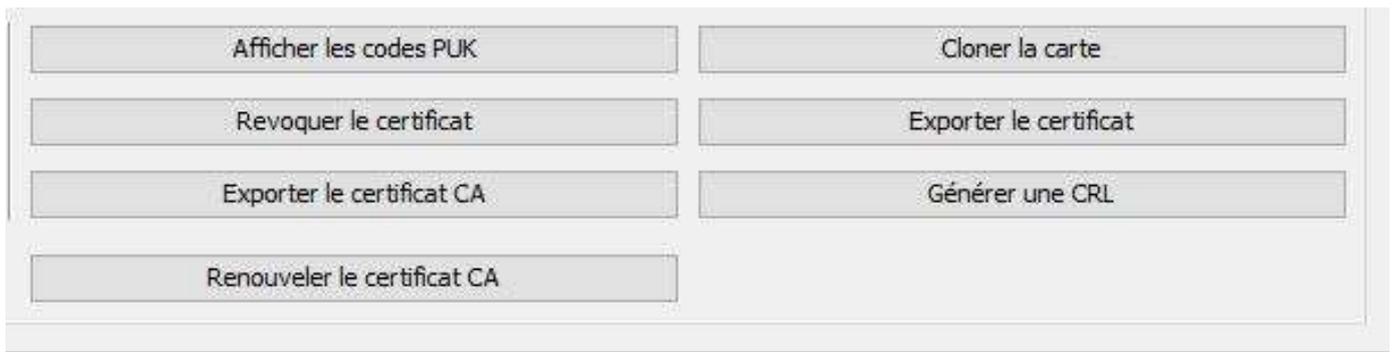
The screenshot shows the 'Cryptosmart-CardManager' application window. The 'Base de données' tab is active, displaying a table with the following data:

Num. de série carte	Type de carte	Nom commun	E-mail	Num. de série cert.	Version de l'applet	Commentaires	Date de création	Date de modification
211 211	Carte serveur	BSPP_CA		08	Applet 5.1		mardi 6 juin 2023 1...	mardi 6 juin 2023 13:2...
211 215	Carte client	BIGAND, Franck	frank.bigand@...	0a	Applet 5.1		mardi 6 juin 2023 1...	mardi 6 juin 2023 13:4...
333 694	Carte serveur	BSPP_CA		03	Applet 5.1		mardi 6 juin 2023 1...	mardi 6 juin 2023 10:0...
333 695	Carte serveur	BSPP_CA		05	Applet 5.1		mardi 6 juin 2023 1...	mardi 6 juin 2023 10:0...
333 697	Carte serveur	BSPP_CA		06	Applet 5.1		mardi 6 juin 2023 1...	mardi 6 juin 2023 10:1...
333 703	Carte serveur	BSPP_CA		04	Applet 5.1		mardi 6 juin 2023 1...	mardi 6 juin 2023 10:0...

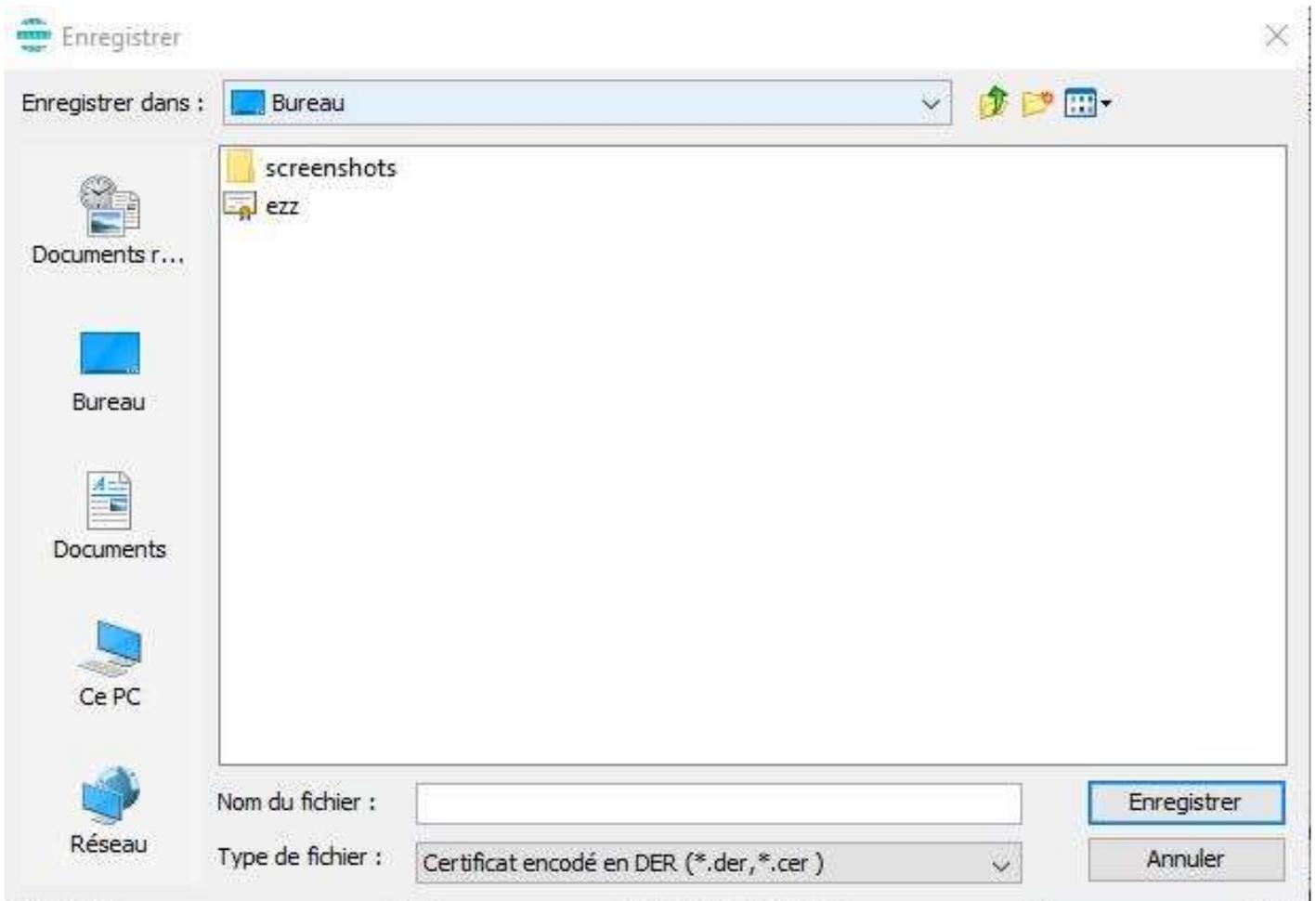
Below the table, there are several management options:

- Certificats révoqués
- Cartes recyclées
- Afficher les cartes archivées
- Archiver
- Rechercher...
- Afficher les codes PUK
- Revoquer le certificat
- Exporter le certificat CA
- Renouveler le certificat CA
- Cloner la carte
- Exporter le certificat
- Générer une CRL

1. Se rendre dans l'onglet « Base de données »



2-En bas à droite, sélectionner « Exporter le certificat »



3-L'enregistrer dans l'endroit voulu

4.Infos utiles (A lire !)

Pré requis pour PC client:

- Installation de CryptoSmart 5.2.112
- Installation de TAP Windows 9.4.2

Pré requis pour PC PKI:

- Interface RZO / Wifi désactivé
- Chiffrement Bitlocker du PC
- Utilisation d'un coffre-fort pour le stockage
- Utilisation d'un autre coffre-fort pour stockage des sauvegardes de BDD

Installation du logiciel PKI Cryptosmart-Card Manager :

- Chemin par default
- Exécuter en tant qu'administrateur

Création d'une clef serveur :

- Aller dans l'onglet information carte
- Brancher une clefs
- Cliquer sur actualiser
- Cliquer sur créer une carte
- Cliquer sur oui
- Renseigner Carte Serveur
- Renseigner nom commun : BSPP_CA
- Modifier la date d'expiration à Année + 3
- En cas d'erreur possibilité de recycler la carte
- A chaque fin de session de création de clefs, effectuer une sauvegarde de la BDD en suivant la procédure du dossier d'exploitation

Création d'une clef client :

- Aller dans l'onglet information carte
- Brancher une clef
- Cliquer sur actualiser
- Créer une carte
- Sélectionner « carte client »
- Renseigner les informations de l'utilisateur
- Bien renseigner l'email de l'utilisateur à la création de la clef sinon ne fonctionnera pas
- Cliquer sur parcourir sur le fichier de configuration, spécifier le fichier BSSP présent sur le bureau de l'utilisateur SMI-ADMIN
- Code de sécurité par défaut : 1234 (changement de code / bloquer la carte possible via le bouton dans l'onglet informations carte)
- Conseil (exportation des codes PUK de l'onglet BDD dans une clef USB pour dépannage ultérieur d'un client)
- A chaque fin de session de création de clefs, effectuer une sauvegarde de la BDD en suivant la procédure du dossier d'exploitation

Perte de code pin :

- Onglet BDD
- Afficher les codes PUK

Perte de Clefs USB :

CRL : Contrôle Revocation List

⇒ Permet de révoquer un certificat (en cas de clefs perdue)

CAT :

- Révoquer la clef sur le logiciel cryptosmart – cardmanager
- Exporter le fichier CRL sur une clef USB
- L'apporter à RZO sécurité pour Uploading sur le serveur et prise en compte de la revocation

Informations pratiques :

- Temps de validité des clefs clients et serveur : 3 ans (à renouveler avant cette date pour chaque client)
- Temps de validité du CA root: 15 ans
- Les clefs serveurs et les cartes clients sont les même (modèle)
- Il existe une documentation d'exploitation.

Export de l'IGW : Permet de d'indiquer à la passerelle la configuration de l'IGS et de la Root_CA.

- A exporter en cas de changement de Root_CA et de reconfiguration de la passerelle.
- Voir fichier joint
- Voir documentation ci-jointe.

Sauvegarde de le BDD :

- Copier le dossier Families situé c:/programfiles(x86)/ercom/cryptosmart-cardmanager/families
- Voir le DEX pour de plus amples informations.

Sauvegarde des logs :

- Copier administration

Fichier de configuration 'BSPP.txt' :

- Ne change pas sauf si modification de l'IP publique de la Gateway.