



05.03.2025

Guide rapide

Délivrance de certificats sur carte à puce (CMC)

Statut : publié

V2.0



L'application « LRA », également appelée CMC (Certificate Management Console), est disponible exclusivement sur le client BAB sous « Swiss Government PKI - Officer Tools ». Cette application permet notamment d'établir et de révoquer les classes de certificats A, B, C Standard et C Customised.

Ce Quickguide fait partie de la documentation CMC et se réfère concrètement à l'émission. Vous pouvez également utiliser ce guide pour l'émission multiple de certificats de classe B. Vous trouverez d'autres quickguides sur l'application CMC sur notre [page d'accueil PKI](#).

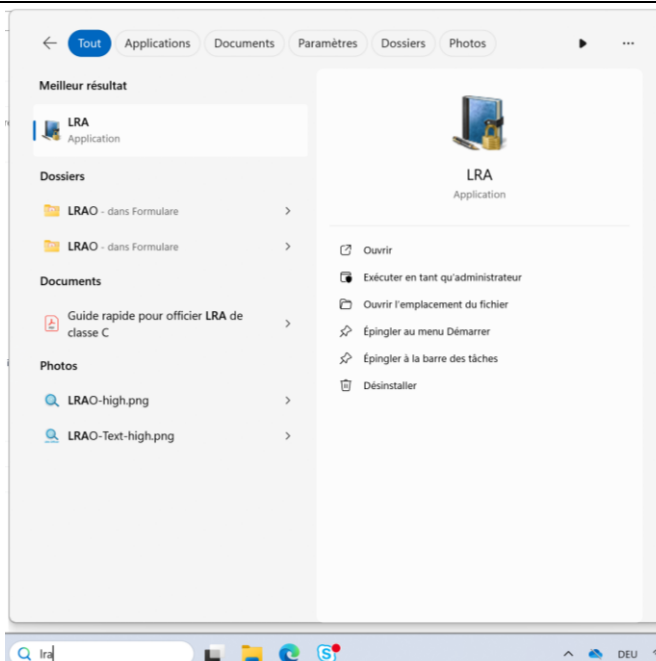
Table des matières

Guide rapide	1
Délivrance de certificats sur carte à puce (CMC)	1
1. Connexion avec un profil existant	3
2. Délivrer des certificats	4
3. Imprimer la confirmation	9
4. Débloquer la carte à puce	11

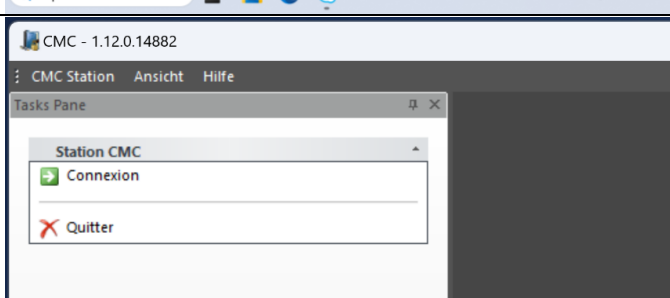
1. Connexion avec un profil existant

Un profil CMC entièrement configuré est nécessaire pour cette étape. Les instructions relatives à la création d'un tel profil figurent dans un [document séparé](#).

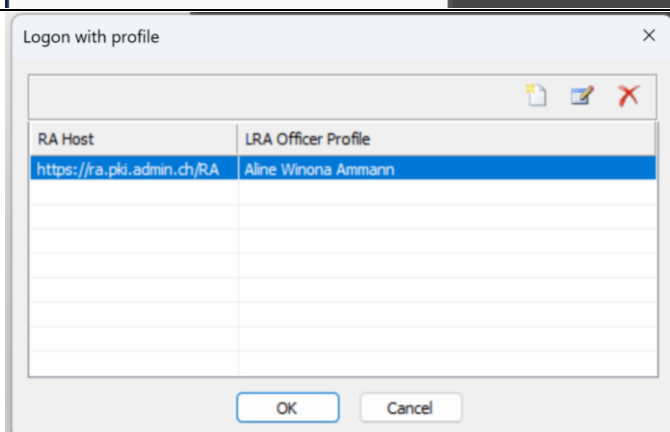
Démarrez l'application LRA.



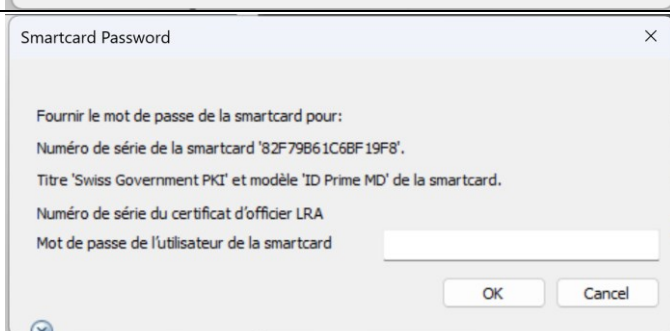
Après le lancement de l'application, cliquez sur « Connexion ».



Cliquez sur votre profil d'officier LRA dans la liste et confirmez votre choix en cliquant sur « OK ».



Saisissez votre code PIN de carte dans le champ de texte prévu à cet effet et appuyez ensuite à nouveau sur « OK ».

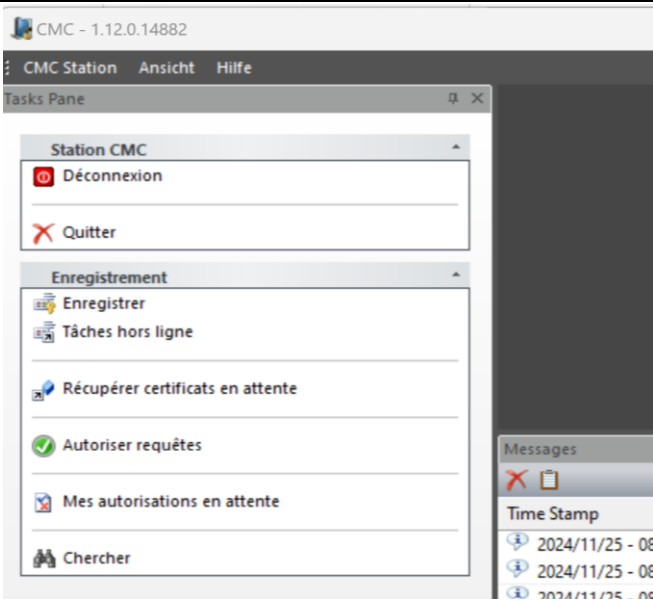


2. Délivrer des certificats

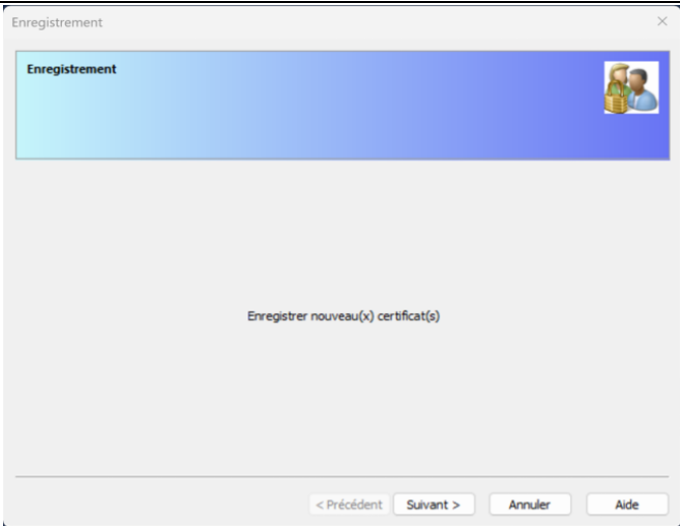
Pour cette étape, vous avez besoin d'une carte à puce prestaged supplémentaire.

Une fois que vous êtes connecté, le ruban du menu s'élargit pour inclure la vignette « Enregistrement ». Le chargement complet de la barre de menu peut prendre un certain temps.

Cliquez sur l'option « Enregistrer » dans la vignette.

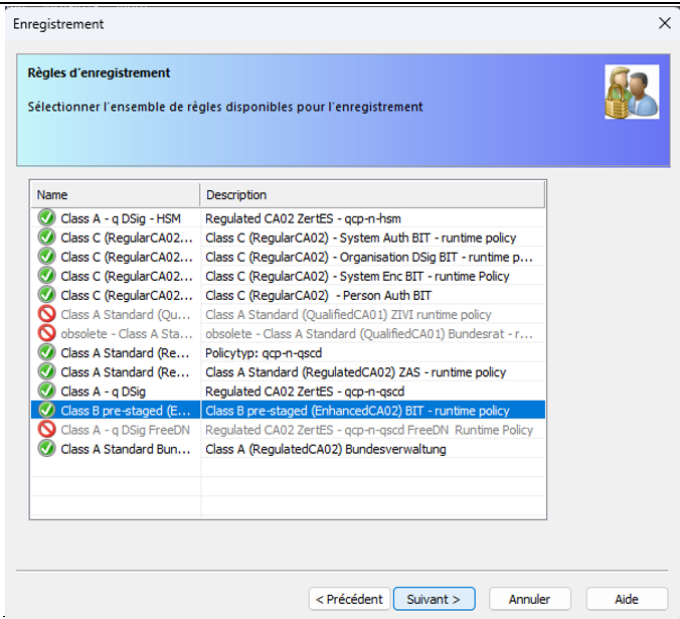


Cliquez sur « Suivant ».



Sélectionnez la politique correspondante dans la liste et appuyez ensuite sur « Suivant ».

Attention : les procédures présentées dans ce document peuvent ne pas correspondre à la classe de certificat que vous avez choisie. Veuillez respecter les **directives d'enregistrement** en vigueur.



Choisissez l'option « Envoyer cet enregistrement au RA quand il est terminé » pour envoyer la demande au RA dès qu'elle est terminée et pour que le certificat soit délivré.

La deuxième option permet de créer des demandes hors ligne et de les envoyer plus tard au RA.

Cliquez ensuite sur « Suivant ».

Si la politique que vous avez choisie exige une demande de certificat (CSR), vous pouvez télécharger un tel fichier à l'aide de l'icône Browse (📁).

Cliquez ensuite sur « Suivant ».

Recherchez la personne qui fait la demande.

Vous pouvez soit rechercher le nom de la personne dans le champ « Common Name », soit effectuer la requête à partir de l'e-mail.

Une fois la saisie terminée, cliquez sur l'icône de recherche (🔍).

Choisissez votre utilisateur en sélectionnant l'entrée dans la liste et en cliquant ensuite sur « Suivant ».

Lors de la sélection, vérifiez l'e-mail afin d'éviter toute confusion.

Enregistrement

Rechercher utilisateur
Recherche de la source de données

Common Name: Enke Felix*

Email:

Account ID / External ID:

Insurance Number:

Common Name	Email
Enke Felix R8P8CV	felix.enke@bit.admin.ch
Enke Felix TEST TR8P8CV	felix.test.enke@bit.admin.ch

< Précédent Suivant > Cancel Aide

Identifiez la personne qui fait la demande à l'aide du document de voyage présenté et sélectionnez le résultat correspondant dans les options.

Si vous avez réussi à identifier la personne, vous pouvez poursuivre le processus en cliquant sur « Suivant ».

Enregistrement

Vérification de l'utilisateur
Recherche de la source de données

USER DATA

Nom: Enke

Prénom: Felix

Nom (selon doc ID):

Prénom (selon doc ID):

Check result:

☐ Identifié avec Given Name / Surname selon le document d'identité.

☐ Nom (selon doc ID) / Prénom (selon doc ID) incorrect.

☒ Identifié avec Enke / Felix.

☐ Emission avec condition pour les Enke / Felix.

☐ Nom / Prénom invalide.

Missing Attributes:

adminGivenNameLong

adminSurnameLong

Duplicate Attributes:

< Précédent Suivant > Cancel Aide

Contrôlez les données pour le certificat à émettre.

Cliquez ensuite sur « Suivant ».

Enregistrement

Nom unique du sujet (SDN)
Définir le nom d'utilisateur final utilisé pour l'émission du ou des certificats

SDN Attribute	SDN Value
Common Name	Enke Felix TEST TR8P8CV
Organizational Unit	Weisse Seiten
Organization Name	Admin
Country Name	CH

< Précédent Suivant > Cancel Aide

Contrôlez encore une fois l'adresse e-mail (rfc822) et confirmez en cliquant sur « Suivant ».

Enregistrement

Nom alternatif du sujet
Définir les valeurs SAN par certificat.

☐ L'extension est critique

Attribute	Value
rfc822	felix.test.enke@bit.admin.ch

DSig Auth Enc

< Précédent Suivant > Cancel Aide

Si vous avez déjà scanné le document de voyage du demandeur, vous pouvez sélectionner le fichier en cliquant sur l'icône « Browse » (📁).

Sinon, vous pouvez numériser le document de voyage du client en cliquant sur l'icône de numérisation (📄).

Cliquez ensuite sur « Suivant ».

Attention : il est interdit d'archiver des documents de voyage sur le client BAB. Veillez à supprimer tout fichier local après l'émission (y compris dans les dossiers de courrier !).

Enregistrement

Documents d'enregistrement
Sélectionner les documents d'enregistrement de l'utilisateur final

Document(s) d'enregistrement

File	Size
SCAB70E.pdf	243 KB

< Précédent Suivant > Cancel Aide

Au plus tard à ce moment-là vous devez insérer la carte à puce d'utilisateur insérer le lecteur de carte.

Sélectionnez d'abord le pilote « SafeNet smartcard » pour la carte dans le champ déroulant.

Marquez ensuite la carte dans le tableau et cliquez sur « Suivant ».

Sélection de la smartcard

Smartcard
Sélectionner une smartcard pour la génération de la clé ou de la requête

Select Smartcard SafeNet smartcard

Model	Serial	Label
ID Prime MD	EF67CBB2A448275C	Swiss Government PKI

< Précédent Suivant > Cancel Aide

Il faut maintenant lire les clés doivent être lues. Pour cela, il faut d'abord cliquer sur le symbole de la paire de clés.

Cette étape permet en outre d'attribuer le L'étiquette du token est alors placée sur le nom commun de la personne qui fait la demande.

Les barres bleues vous permettent de voir l'avancement du processus.

Attendez que toute la colonne de droite soit remplie et cliquez ensuite sur « Suivant ».

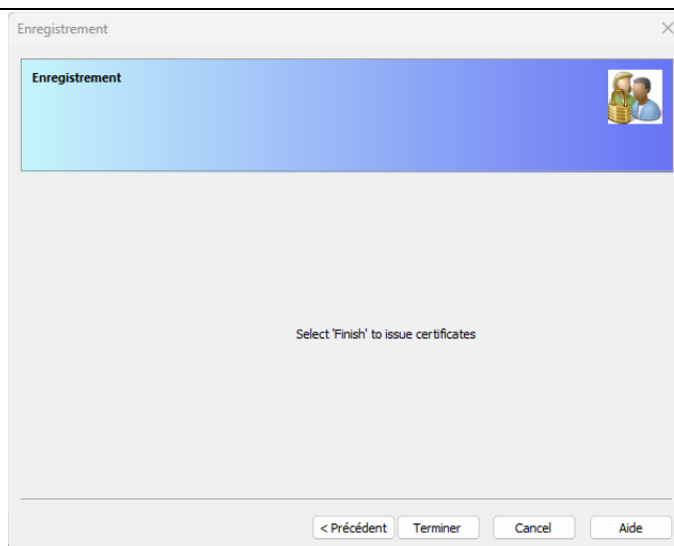
Vous pouvez saisir ici des remarques supplémentaires sur l'établissement ou les certificats délivrés, qui seront reprises dans le journal de bord de l'application LRA.

Confirmez en cliquant sur « Suivant ».

Cliquez sur « Terminer ».

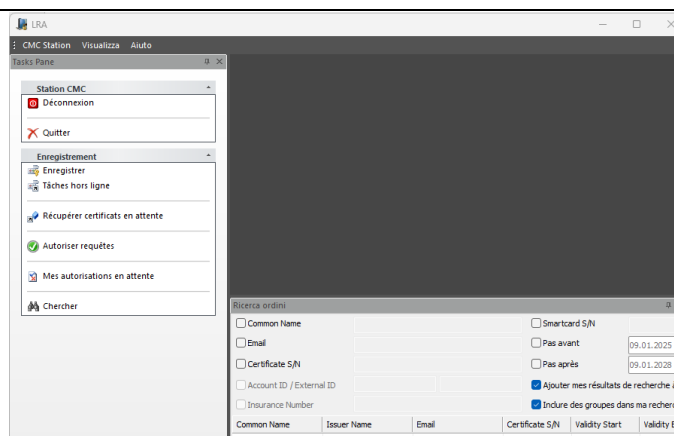
Attention : les certificats ne sont pas encore présents sur la carte à puce de l'utilisateur.

La requête est maintenant envoyée à la RA si vous avez choisi cette option au début.



3. Imprimer la confirmation

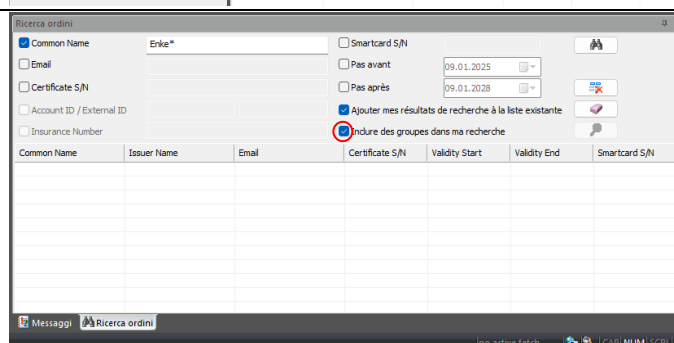
Dans le menu band, cliquez sur l'option « Chercher ».



Assurez-vous que l'option « Inclure des groupes dans ma recherche » est activée dans le masque de recherche.

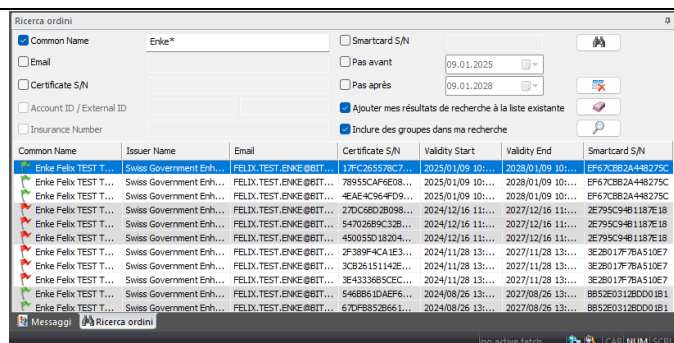
Recherchez maintenant le certificat émis précédemment à l'aide des options de recherche. Vous pouvez abrégier le terme avec un astérisque supplémentaire.

Cliquez sur l'icône de recherche pour lancer la requête (🔍).

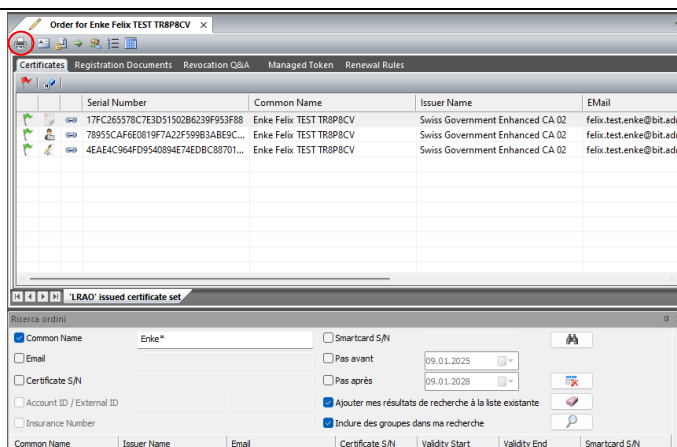


Tous les certificats qui répondent aux critères de recherche apparaissent dans le tableau.

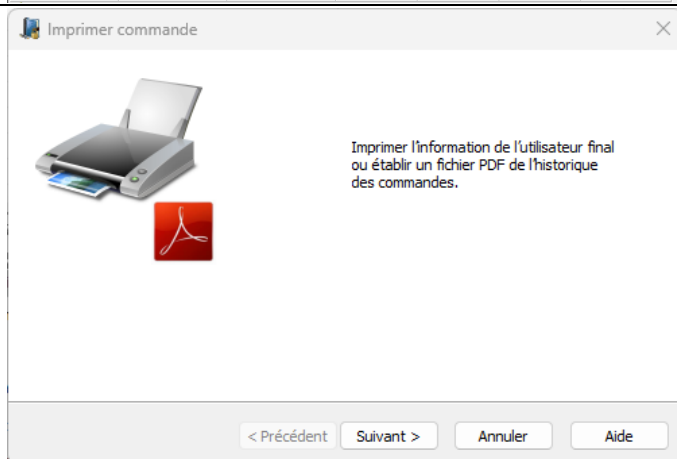
Double-cliquez sur l'entrée souhaitée.



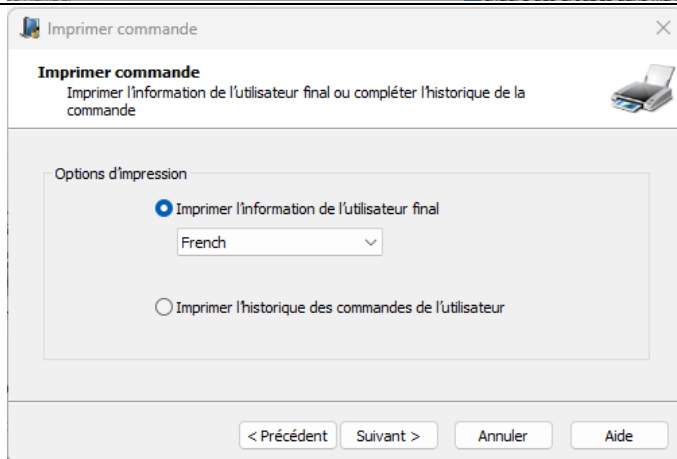
Une nouvelle fenêtre apparaît pour l'entrée sélectionnée. Dans l'onglet « Certificates », cliquez sur le symbole de l'imprimante.



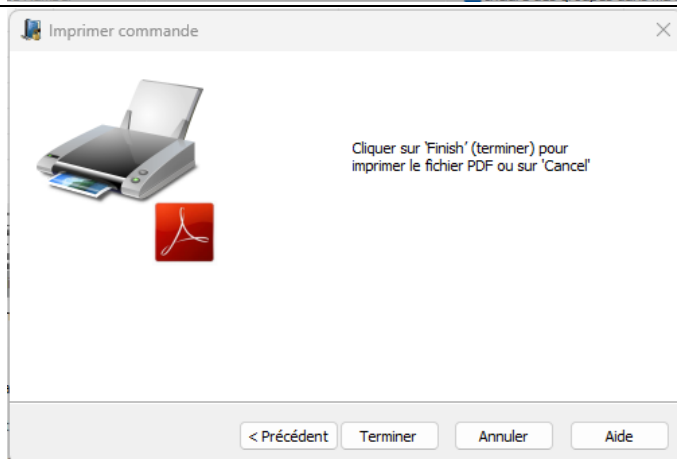
Cliquez sur « Suivant ».



Choisissez la langue souhaitée et cliquez ensuite sur « Suivant ».



Cliquez sur « Terminer ».



La confirmation peut maintenant être imprimée. Adaptez les paramètres si nécessaire et confirmez ensuite en cliquant sur « OK ».

Impression

Imprimante

Nom : SECPRINT Propriétés...

Statut : Prêt

Type : HP Universal Printing PCL 6 (v7.0.1)

Emplacement : _SecurePrint

Commentaire : SecurePrint (new) & PullPrint (old)

Zone d'impression

☒ Tout

☐ Pages de : à :

☐ Sélection

Copies

Nombre de copies : 2

☒ Copies assemblées

Aide OK Annuler

Le « PIN Unseal » de la carte est imprimé dans le document.

Attention : tant que le code PIN n'a pas été utilisé, il peut être réimprimé à l'aide de l'application LRA. Une fois utilisé, le code PIN disparaît de l'impression.

Les lignes directrices et le contrat d'utilisation ne sont pas encore intégrés dans le système. Veuillez les télécharger à partir de <https://www.bit.admin.ch/fr/sq-pki-swiss-government-pki-fr>.

Par votre signature, vous confirmez :

- la réception de la smartcard
- l'exactitude des données sauvegardées sur la carte (notamment le nom, le prénom et l'adresse électronique)
- avoir reçu une copie du document „Droits et obligations des porteurs de certificats de la Swiss Government PKI” et remplir vos devoirs

Lieu, date

CN Enke Felix TEST TR8P8CV

Email felix.test.enke@bit.admin.ch

Signature

Lorsque vous aurez besoin d'utiliser votre carte, vous devrez la débloquent à l'aide du code d'activation, conformément aux instructions ci-jointes. Ensuite, vous pourrez utiliser votre certificat avec le NIP que vous êtes seul à connaître.

Le code d'activation pour votre smartcard personnelle est :

68B5-819B-EBF9-5D5F

4. Débloquer la carte à puce

Une fois que l'utilisateur a reçu la carte à puce personnelle et la confirmation avec le code PIN Unseal, la carte à puce peut être descellée. Les certificats émis précédemment sont ainsi téléchargés sur la carte à puce et protégés par un code PIN choisi par l'utilisateur lui-même. La carte est ensuite entièrement fonctionnelle.

Vous trouverez une description plus détaillée du processus de descellement sur la [page d'accueil PKI](#).