



IGC-BDF-V3

Guide Utilisateur

**Retrait du code d'activation (code PIN) d'un
certificat matériel émis par l'IGC-BDF-V3**

Table des matières

Suivi du document.....	3
1. Objet du document	3
2. Prérequis Techniques	3
3. Accès à l'interface Utilisateur de l'IGC Banque de France	3
3.1. Compte utilisateur.....	3
3.2. Authentification sur l'interface Utilisateur de l'IGC Banque de France	4
4. Retrait du code PIN associé au certificat Matériel	5
5. Changement du code PIN de votre support matériel	8
6. Vérification et accusé de réception du certificat	10

Suivi du document

Version	Date	Acteur(s)	Objet de la modification
1.0	01/10/2020	RSI	Version initiale

1. Objet du document

Ce document présente un guide utilisateur lié au retrait du code d'activation (code PIN) d'un certificat matériel émis par l'IGC de la Banque de France.

Le retrait du code PIN se fait à l'aide de l'interface utilisateur de l'IGC de la Banque de France.

2. Prérequis Techniques

1. L'installation de la chaîne de confiance (certificats des Autorités de certification) de la Banque de France est un prérequis à toute utilisation des certificats Banque de France.
La chaîne de confiance est disponible au format [ZIP](#) ou [P7B](#).
NB : Veuillez prendre contact avec votre service informatique afin de vérifier l'installation de la chaîne de confiance sur votre système.
2. L'utilisation d'une carte à puce (ou token USB) fourni par la Banque de France nécessite l'installation d'un driver disponible en utilisant le lien correspondant suivant : Windows ([32 bits](#), [64 bits](#)).
3. L'utilisation d'un lecteur de carte à puce fourni par la Banque de France nécessite l'installation d'un driver qui peut être téléchargé en utilisant le lien correspondant ci-dessous :
 - Windows 8 et 8.1 ([32 bits](#), [64 bits](#))
 - Windows 10 ([32 bits et 64 bits](#))

3. Accès à l'interface Utilisateur de l'IGC Banque de France

3.1. Compte utilisateur

Après vérification et validation de la demande de certificat transmise par courrier à l'Autorité d'Enregistrement de l'IGC de la Banque de France, un compte utilisateur sera créé afin d'accéder à votre espace sur l'interface utilisateur de l'IGC Banque de France.

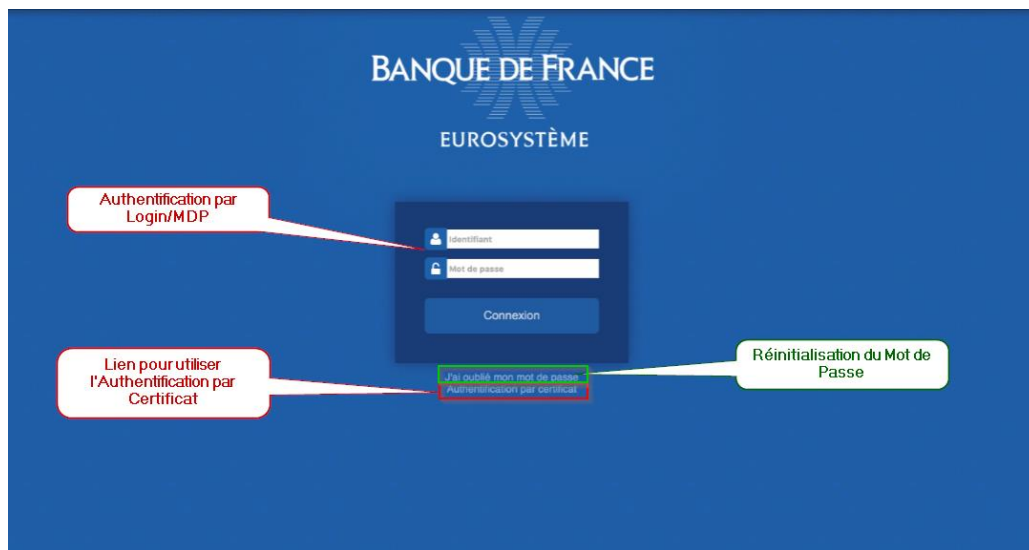
Une fois le compte créé, l'utilisateur recevra par courriel ses identifiants de connexion à l'interface utilisateur de l'IGC Banque de France. Le mot de passe transmis devra être modifié après la première connexion.

NB : Dans le cas où l'utilisateur possède déjà un compte utilisateur sur le système de gestion des identités et des accès de la Banque de France, il devra se connecter avec ses identifiants de connexion.

3.2. Authentification sur l'interface Utilisateur de l'IGC Banque de France

L'accès à l'interface utilisateur de l'IGC Banque de France nécessite une authentification possible selon deux méthodes :

- **Authentification par login/mdp** : l'utilisateur s'authentifie avec les identifiants (login et mot de passe) pour accéder à l'interface utilisateur.
- **Authentification par certificat** : Si l'utilisateur possède déjà un certificat d'authentification émis par la Banque de France, il peut s'authentifier avec ce certificat pour accéder à l'interface utilisateur de l'IGC.



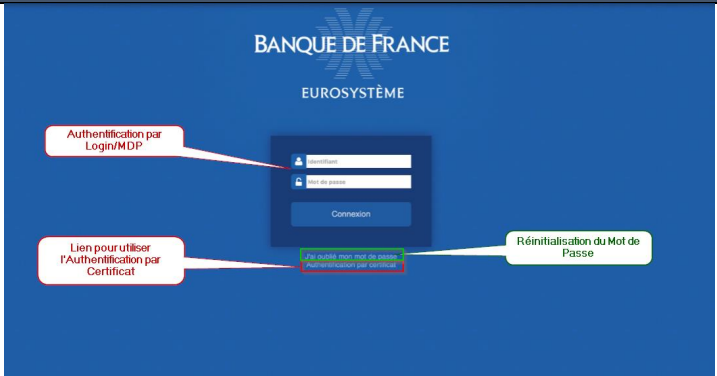
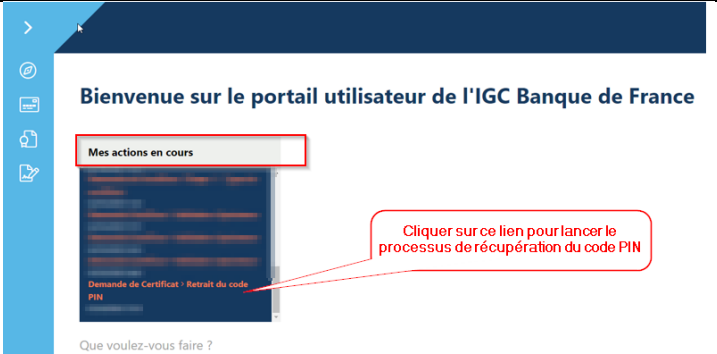
4. Retrait du code PIN associé au certificat Matériel


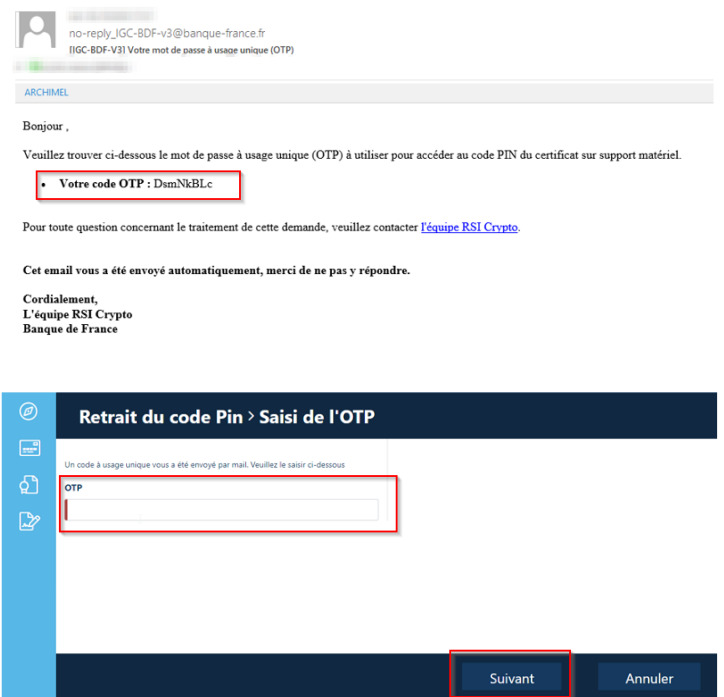
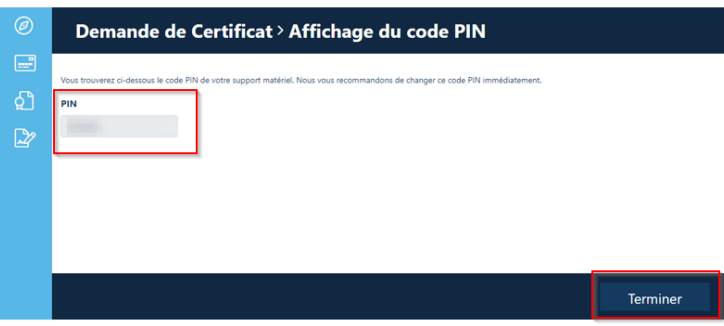
Une fois la demande de certificat traitée par l'Autorité d'Enregistrement de l'IGC Banque de France, l'utilisateur recevra un courriel l'informant de l'envoi par courrier de son support matériel et de la mise à disposition du code d'activation (code PIN) sur l'interface utilisateur de l'IGC Banque de France.

Le retrait du code PIN sur l'interface utilisateur doit être réalisée uniquement après la réception du support matériel reçu par courrier.

L'utilisateur dispose d'un délai de 21 jours pour accuser réception du certificat. Passé ce délai, s'il n'a pas accusé réception de son certificat, l'Autorité d'Enregistrement peut prendre des mesures allant jusqu'à la révocation du certificat.

La procédure pour accuser réception depuis l'interface utilisateur de l'IGC Banque de France est décrite dans le chapitre 6.

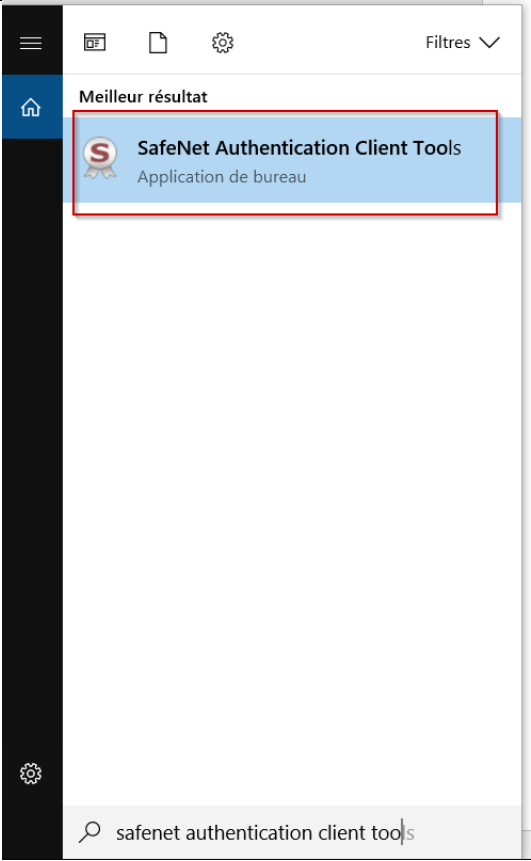
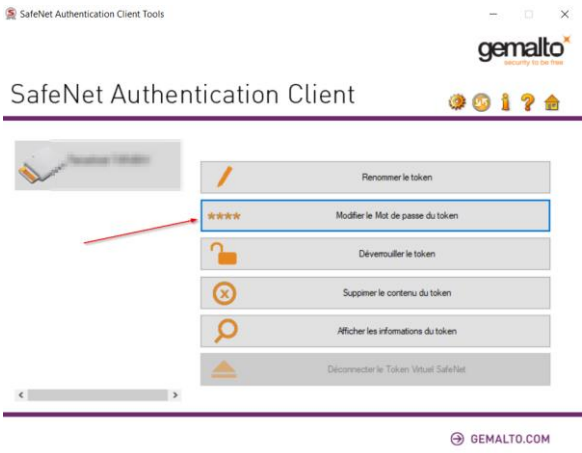
ID	Description	Exemple
1	<p>Réception d'une notification email informant de l'envoi du support matériel par courrier et de la mise à disposition du code PIN sur l'interface utilisateur.</p> <p>Le lien présent dans la notification permettra d'accéder directement à l'interface utilisateur.</p> <p>Une fois le support matériel reçu, accéder à l'interface utilisateur (cf 3.2)</p>	
2	<p>Une fois connecté, aller dans le menu « Mes actions en cours » et cliquer sur le lien Demande de Certificat > Retrait du Code PIN pour commencer le processus de retrait du Code PIN.</p>	
3	<p>Sur la page suivante, vous pouvez visualiser les informations liées au support matériel concerné :</p> <ul style="list-style-type: none"> - Identifiant de la demande de certificat associée - Numéro de support matériel - Profils de certificats associés au support matériels 	

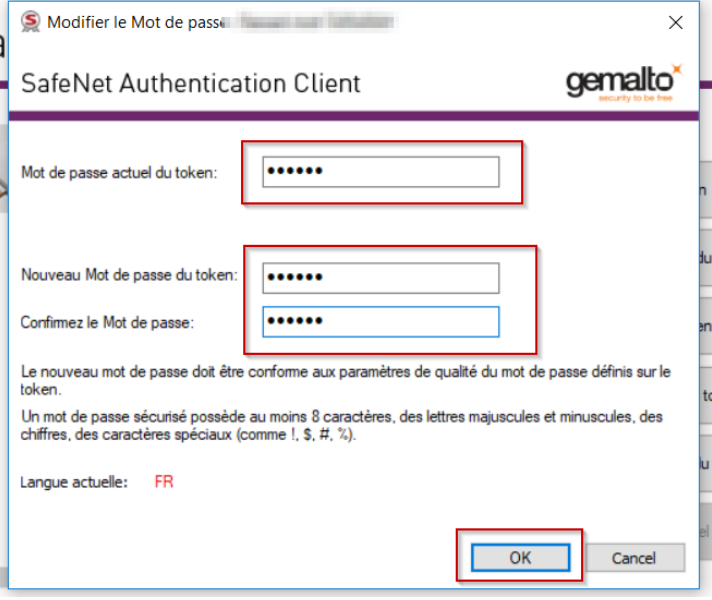
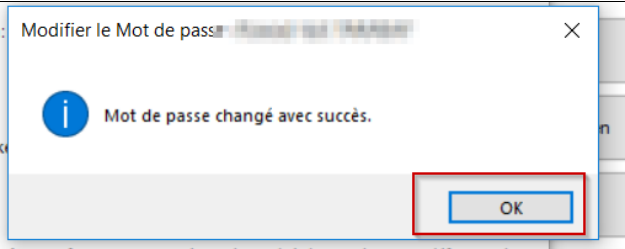
	<p>En cliquant sur « Suivant » vous aller recevoir par email un mot de passe à usage unique. Ce mot de passe sera demandé à l'étape suivante pour pouvoir visualiser le code PIN du support matériel.</p>	
4	<p>Sur la page suivante, saisir le mot de passe à usage unique qui a été transmis par email et cliquer sur « Suivant »</p>	
5	<p>Le code PIN du support matériel est affiché.</p> <p>Attention : Ce code PIN est accessible en accès unique sur l'interface utilisateur. Une fois que vous quittez cette page, ce code PIN ne sera plus accessible.</p> <p>NB : Nous vous recommandons de modifier le code PIN du support matériel dès sa réception, en suivant la procédure décrite au chapitre 5.</p> <p>Cliquer sur « Suivant » pour terminer.</p>	
6	<p>Une fois la récupération du code PIN est terminée, vous devez accuser réception du certificat, et accepter son contenu. Une action associée apparait donc dans le menu « Mes actions en cours » vous</p>	

<p>permettant d'effectuer cet accusé de réception.</p> <p>Suivre la procédure décrite au chapitre 6 pour effectuer cet accusé de réception.</p>	
---	--

5. Changement du code PIN de votre support matériel

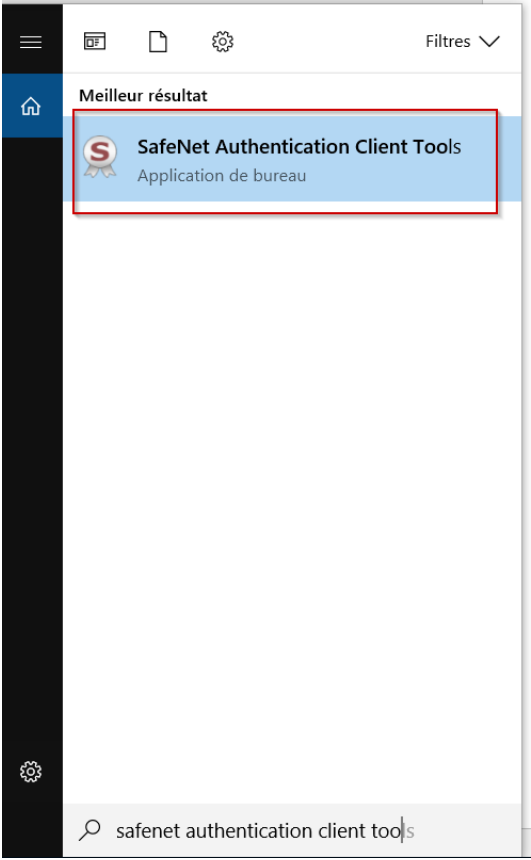
Une fois le code PIN du support est récupéré depuis l'interface utilisateur de l'IGC Banque de France, il est recommandé de changer ce code PIN immédiatement.

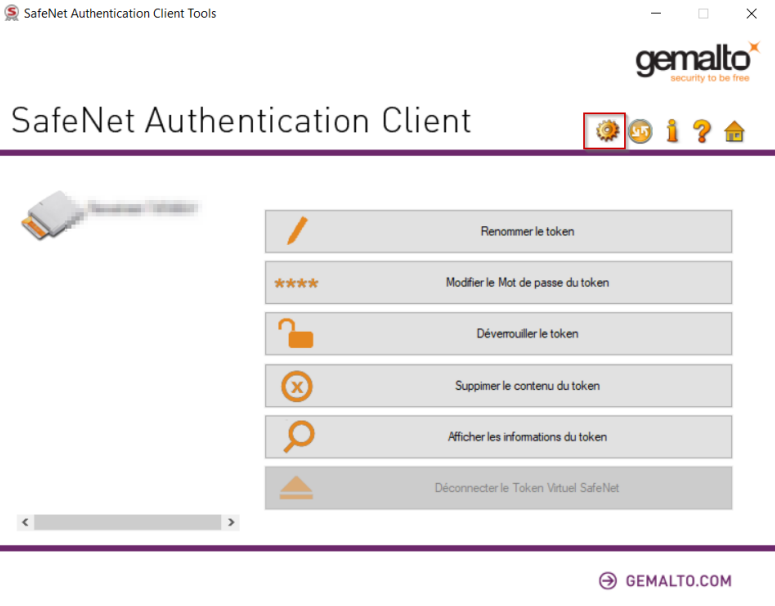
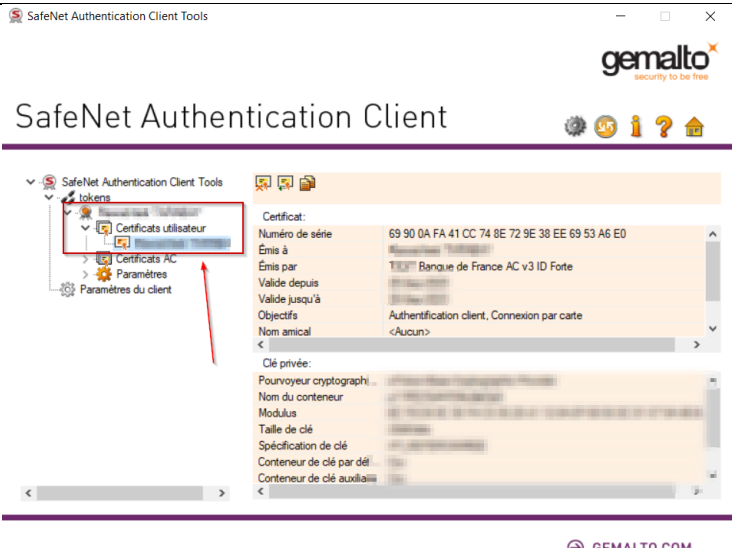
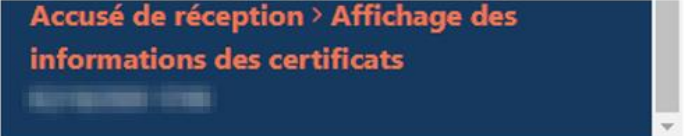
ID	Description	Exemple
1	Connecter le support matériel (brancher le token USB ou insérer la carte à puce dans le lecteur de carte).	
2	Ouvrir le programme « Safenet Authentication Client Tool » en cliquant sur « Recherche » et recherchant ce programme sur votre ordinateur.	 <p>The screenshot shows a Windows search interface. At the top, there are icons for home, files, and settings, along with a 'Filtres' dropdown. Below the search bar, the results are displayed under the heading 'Meilleur résultat'. A single result is shown: 'SafeNet Authentication Client Tools' with a blue ribbon icon and the text 'Application de bureau'. A red rectangular box highlights this result. At the bottom of the search bar, the text 'safenet authentication client tools' is visible.</p>
3	Cliquer sur « Modifier le Mot de passe du Token » pour changer le code PIN du support.	 <p>The screenshot shows the 'SafeNet Authentication Client' application window. The title bar reads 'SafeNet Authentication Client Tools' and the Gemalto logo is in the top right corner. The main interface has a purple header with the text 'SafeNet Authentication Client' and several icons. Below the header, there is a list of options for token management. A red arrow points to the 'Modifier le Mot de passe du token' option, which is highlighted with a blue border. Other options include 'Renommer le token', 'Déverrouiller le token', 'Supprimer le contenu du token', 'Afficher les informations du token', and 'Déconnecter le Token Virtuel SafeNet'. The Gemalto logo and 'GEMALTO.COM' are visible at the bottom right.</p>

4	<p>Saisir le mot de passe actuel (code PIN récupéré au chapitre 4), ainsi que le nouveau mot de passe (2 fois pour confirmation).</p> <p>Cliquer ensuite sur « OK »</p>	 <p>The screenshot shows a window titled 'Modifier le Mot de passe' with the Gemalto logo. It contains three password input fields, each with a red box around it. Below the fields is a message: 'Le nouveau mot de passe doit être conforme aux paramètres de qualité du mot de passe définis sur le token. Un mot de passe sécurisé possède au moins 8 caractères, des lettres majuscules et minuscules, des chiffres, des caractères spéciaux (comme !, \$, #, %).' At the bottom right, the 'OK' button is highlighted with a red box.</p>
5	<p>Un message confirme le changement du code PIN.</p> <p>Cliquer sur « OK » pour terminer.</p>	 <p>The screenshot shows a smaller dialog box with a blue information icon and the text 'Mot de passe changé avec succès.' The 'OK' button is highlighted with a red box.</p>

6. Vérification et accusé de réception du certificat

Une fois le retrait du code PIN terminé, vous pouvez suivre les étapes ci-dessous pour vérifier le contenu du certificat, et accuser la réception de ce certificat depuis votre interface utilisateur de l'IGC Banque de France.


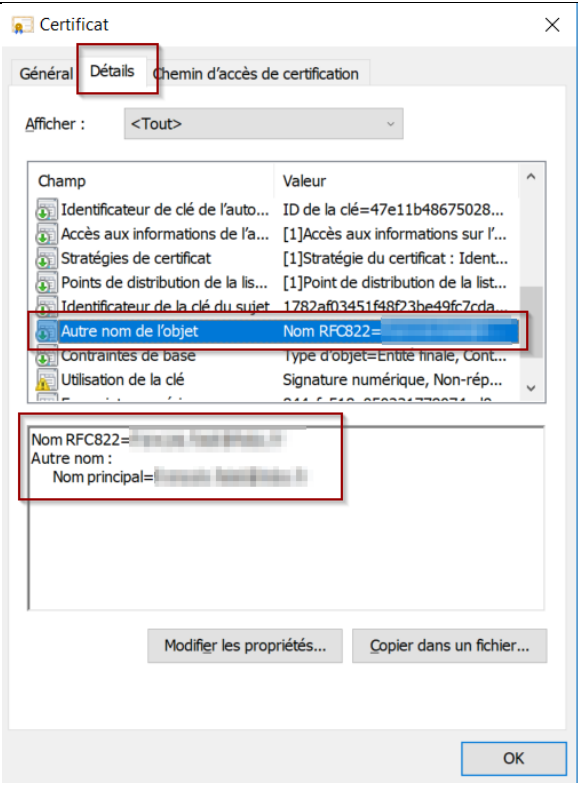
ID	Description	Exemple
1	Connecter votre support matériel (brancher le token USB ou insérer la carte à puce dans le lecteur de carte).	
2	Ouvrir le programme « Safenet Authentication Client Tool » en cliquant sur « Recherche » et recherchant ce programme sur votre ordinateur.	 A screenshot of a Windows search interface. The search bar at the bottom contains the text 'safenet authentication client tools'. The search results are displayed in a list. The top result is highlighted with a blue background and a red border. It is titled 'Meilleur résultat' and shows a search result for 'SafeNet Authentication Client Tools', which is identified as a 'Application de bureau' (Desktop Application). The result includes a small icon of a document with a red 'S' and a ribbon.

3	<p>Cliquer sur l'icône « Vue Avancée » pour visualiser le contenu du support matériel.</p>	 <p>The screenshot shows the 'SafeNet Authentication Client Tools' window. At the top right, there is a 'gemalto' logo and a navigation bar with several icons. A red box highlights the 'Advanced View' icon (a gear with a magnifying glass). Below the navigation bar, there is a list of actions: 'Renommer le token', 'Modifier le Mot de passe du token', 'Déverrouiller le token', 'Supprimer le contenu du token', 'Afficher les informations du token', and 'Déconnecter le Token Virtuel SafeNet'.</p>
4	<p>Dans le menu à gauche, aller dans « Certificats Utilisateur » et sélectionner le certificat pour visualiser ses informations.</p>	 <p>The screenshot shows the 'SafeNet Authentication Client Tools' window with the 'Certificates' menu expanded on the left. The 'User Certificates' option is selected and highlighted with a red box. The main area displays the details of a selected certificate, including the serial number, issuer, validity period, and other technical specifications.</p>
5	<p>Aller sur l'interface Utilisateur de l'IGC, et, dans le menu « Mes actions en cours », sélectionner Accusé de réception > Affichage des informations des certificats</p>	 <p>The screenshot shows a notification banner with the text 'Accusé de réception > Affichage des informations des certificats' in orange and white text on a dark blue background.</p>
5	<p>Sur la page suivante, l'ensemble des informations du certificat vont être affichés. Vérifier ces informations en les comparant avec le certificat présent sur le support matériel.</p> <p>Si les informations affichées sont correctes, vous pouvez accuser la réception et accepter le certificat en cliquant sur le bouton « Accepter ».</p> <p>Dans le cas contraire, vous pouvez révoquer le certificat en cliquant sur « Révoquer »</p>	

Ci-dessous un exemple vous permettant de comparer les informations du certificat avec les informations affichées à l'écran.

- **CN (Nom Commun)** : Dans « Safenet Authentication Client », vérifier la valeur correspondante à « **Émis à** »

- **Valide jusqu'au** : Dans « Safenet Authentication Client », vérifier la valeur correspondante à « **Valide jusqu'à** »

<ul style="list-style-type: none"> • Numéro de série : Dans « Safenet Authentication Client », vérifier la valeur correspondante à « Numéro de série » 	 <p>The screenshot shows the 'SafeNet Authentication Client Tools' window. On the left, a tree view shows 'tokens' > 'Certificats utilisateur' > 'Certificats AC'. The main area displays details for a certificate. The 'Numéro de série' field is highlighted with a red box and contains the hexadecimal value: 69 90 0A FA 41 CC 74 8E 72 9E 38 EE 69 53 A6 E0. Other fields include 'Émis par' (Banque de France AC v3 ID Forte), 'Validé depuis', 'Validé jusqu'à', 'Objectifs' (Authentication client, Connexion par carte), and 'Nom amical' (<Aucun>).</p>																		
<ul style="list-style-type: none"> • UPN (Nom Principal), et Adresse de messagerie : Dans Safenet Authentication Client, double cliquer sur le certificat. Aller ensuite dans l'Onglet « Détails » et vérifier le contenu du champ « Autre Nom de l'Objet » 	 <p>The screenshot shows the 'Certificat' dialog box with the 'Détails' tab selected. A table lists certificate properties:</p> <table border="1"> <thead> <tr> <th>Champ</th> <th>Valeur</th> </tr> </thead> <tbody> <tr> <td>Identificateur de clé de l'auto...</td> <td>ID de la clé=47e11b48675028...</td> </tr> <tr> <td>Accès aux informations de l'a...</td> <td>[1]Accès aux informations sur l'...</td> </tr> <tr> <td>Stratégies de certificat</td> <td>[1]Stratégie du certificat : Ident...</td> </tr> <tr> <td>Points de distribution de la lis...</td> <td>[1]Point de distribution de la list...</td> </tr> <tr> <td>Identificateur de la clé du sujet</td> <td>1782af03451f48f23be49f7cda</td> </tr> <tr> <td>Autre nom de l'objet</td> <td>Nom RFC822=</td> </tr> <tr> <td>Contraintes de base</td> <td>Type d'objet=Entête finale, Cont...</td> </tr> <tr> <td>Utilisation de la clé</td> <td>Signature numérique, Non-rép...</td> </tr> </tbody> </table> <p>Below the table, the 'Autre nom de l'objet' field is expanded, showing:</p> <pre>Nom RFC822= Autre nom : Nom principal=</pre> <p>The 'Autre nom de l'objet' and 'Nom principal=' fields are highlighted with red boxes.</p>	Champ	Valeur	Identificateur de clé de l'auto...	ID de la clé=47e11b48675028...	Accès aux informations de l'a...	[1]Accès aux informations sur l'...	Stratégies de certificat	[1]Stratégie du certificat : Ident...	Points de distribution de la lis...	[1]Point de distribution de la list...	Identificateur de la clé du sujet	1782af03451f48f23be49f7cda	Autre nom de l'objet	Nom RFC822=	Contraintes de base	Type d'objet=Entête finale, Cont...	Utilisation de la clé	Signature numérique, Non-rép...
Champ	Valeur																		
Identificateur de clé de l'auto...	ID de la clé=47e11b48675028...																		
Accès aux informations de l'a...	[1]Accès aux informations sur l'...																		
Stratégies de certificat	[1]Stratégie du certificat : Ident...																		
Points de distribution de la lis...	[1]Point de distribution de la list...																		
Identificateur de la clé du sujet	1782af03451f48f23be49f7cda																		
Autre nom de l'objet	Nom RFC822=																		
Contraintes de base	Type d'objet=Entête finale, Cont...																		
Utilisation de la clé	Signature numérique, Non-rép...																		