[redacted]

TELMA

Mode Opératoire

Assistance à la connexion ETENDER

(accès externe)

VERSION Janvier 2025

Suivi du document

Version	Date	Statut	Auteur	Commentaires
Décembre 2024	12/12/2024	Draft		Création du document

BANQUE DE FRANCE
EUROSYSTÈME

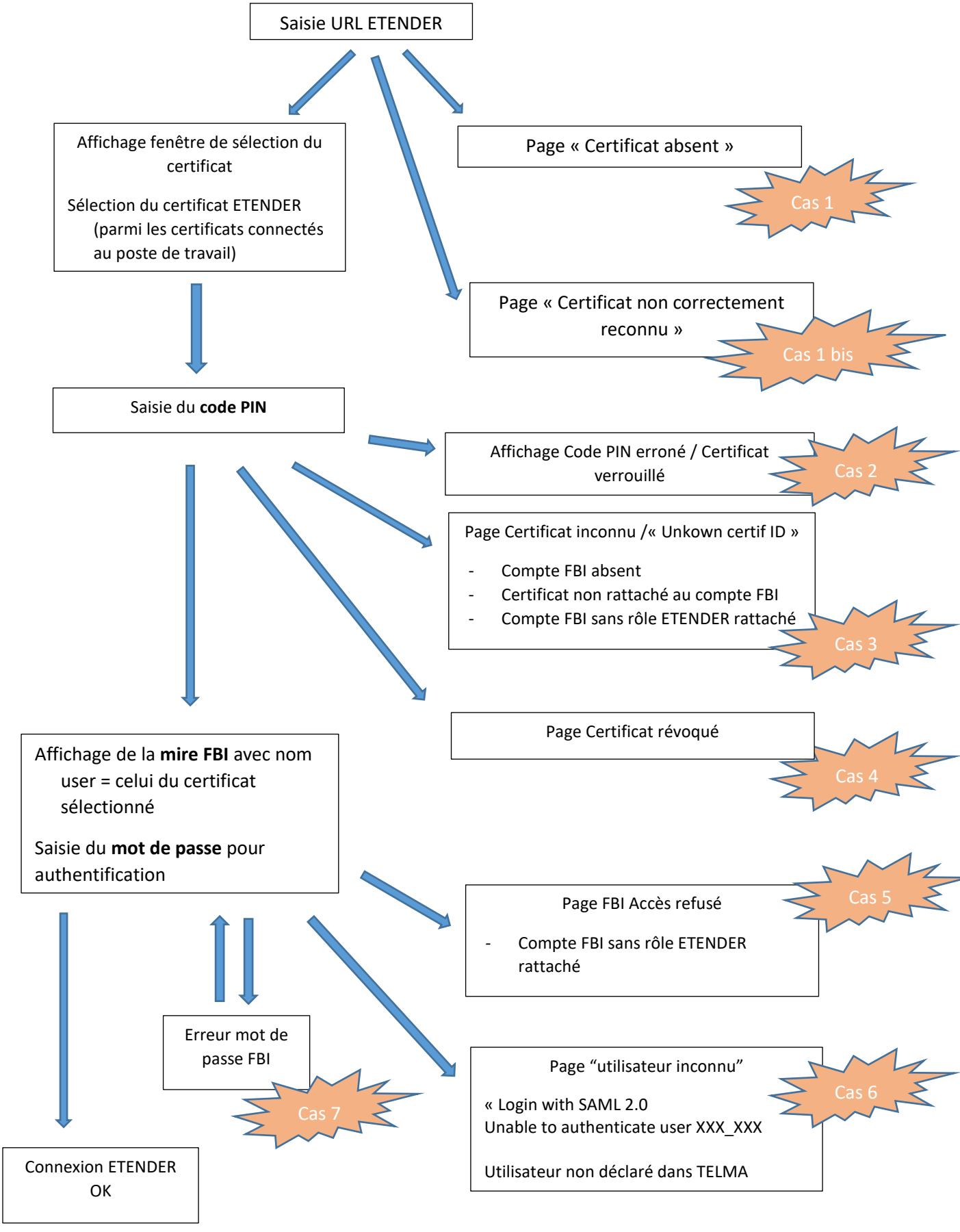
Table des matières

1. Assistance aux phases de connexion des utilisateurs des contreparties

Ce mode opératoire est un guide destiné aux utilisateurs des contreparties de politique monétaire dans l'analyse des erreurs rencontrées lors de la phase de connexion à ETENDER.

Différents message d'erreur ont été référencés dans les paragraphes suivants.

1.1. Description du process de connexion Etender

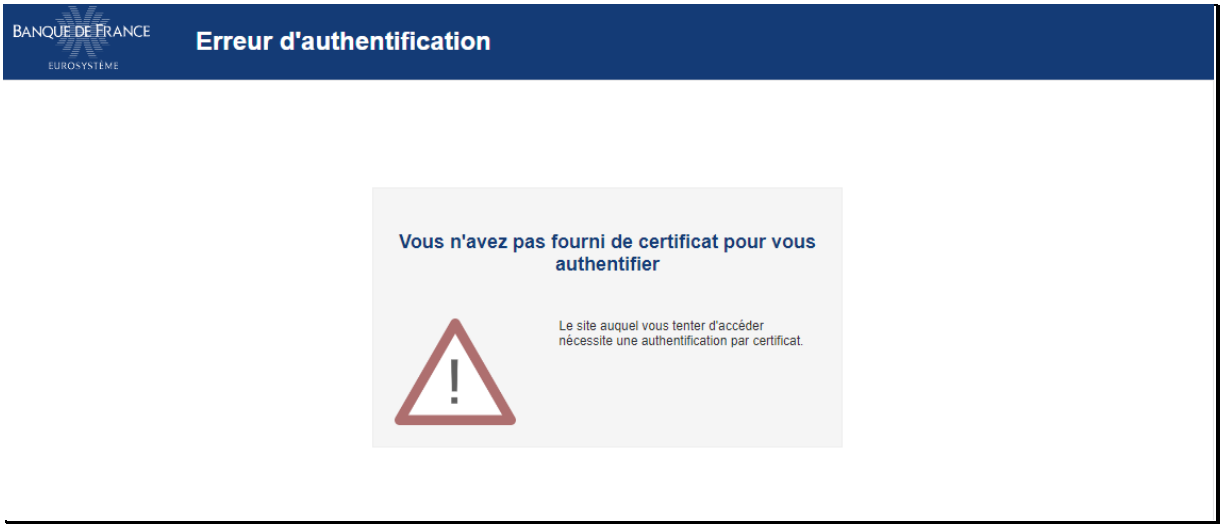


1.2. Cas 1 – Certificat absent

Actions réalisées :

- Exécution de l'URL de connexion ETENDER

Cas : Affichage de l'erreur « Vous n'avez pas fourni de certificat pour vous authentifier. »



⇨ **Diagnostic** : Aucun certificat n'est connecté

⇨ **Actions à réaliser par l'utilisateur** :

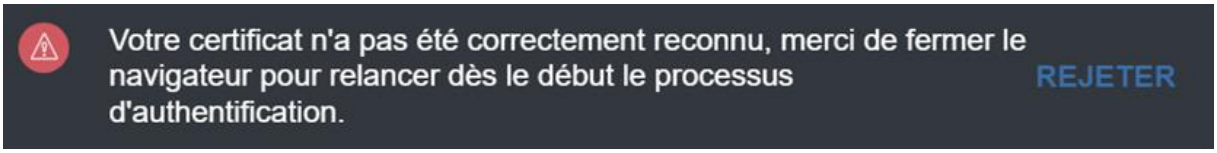
- Fermer son navigateur internet
- Connecter son certificat authentification forte (ETENDER)
- Attendre quelques minutes
- Relancer son navigateur internet
- Vider les caches
- Lancer de nouveau l'URL ETENDER

1.3. Cas 1 bis – Certificat non correctement reconnu

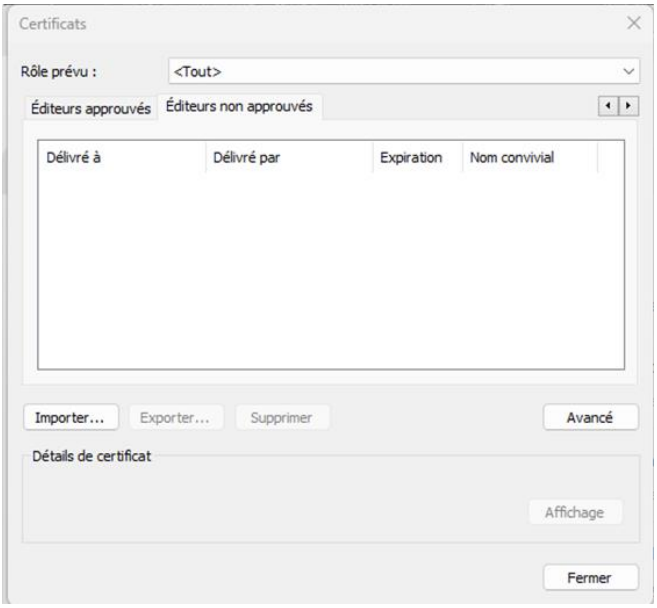
Actions réalisées :

- Exécution de l'URL de connexion ETENDER
- Sélection du certificat
- Le code PIN n'est pas été demandé

⇨ Apparition du message :



- Vérification dans l'onglet « Autorité de certification racine » du certificat que l'AC racine Banque de France est bien présente et que les données détails peuvent être lues



⇨ **Diagnostic** : Un certificat est détecté mais un problème ou un blocage logiciel empêche l'exploitation des informations qu'il contient

⇨ **Actions à réaliser par l'utilisateur** :

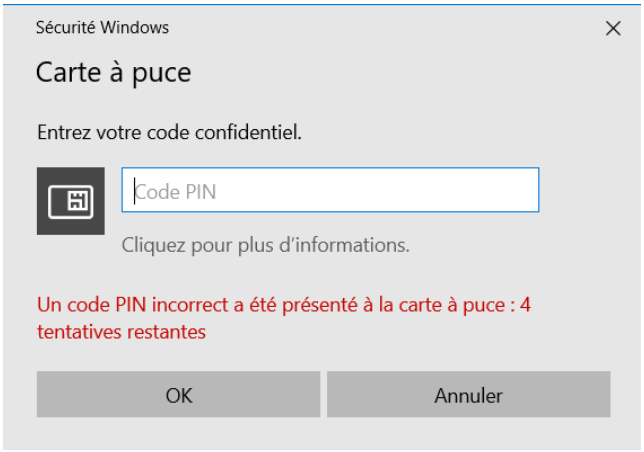
- Fermer son navigateur internet
- Connecter son certificat authentification forte (ETENDER)
- Attendre quelques minutes
- Relancer son navigateur internet
- Vider les caches
- Lancer de nouveau l'URL ETENDER
- Si le problème se répète l'utilisateur doit alerter le support informatique de son entité en lui décrivant le problème

1.4. Cas 2 - Code PIN erroné

Actions réalisées :

- Exécution de l'URL de connexion ETENDER
- Sélection du certificat
- Saisie du code PIN / Code PIN : **KO**

Cas : Affichage de l'erreur « Un code PIN incorrect a été présenté à la carte à puce : X tentatives restantes » apparaît :



⇨ **Diagnostic** : L'utilisateur n'est plus en possession du bon code PIN du certificat. Après 5 tentatives infructueuses, le certificat est 0000alors verrouillé.

⇨ **Actions à réaliser :**

- Remonter l'incident à ARC
- (ARC) Récupérer l'identifiant de l'utilisateur, l'email rattaché au certificat et un moyen de le contacter
- (ARC) Contacter R4F puis leur fournir ces éléments : le service R4F contactera le client et effectuera une réinitialisation du Code PIN du certificat ou le déverrouillage du certificat avec lui.

1.5. Cas 3 – Échec de l'authentification Unknow CertID

Actions réalisées :

- Exécution de l'URL de connexion ETENDER
- Sélection du certificat
- Saisie du code PIN
- Code PIN **OK**

Cas : Affichage de l'erreur « Echec de l'authentification. UnknownCertID »

⇨ **Diagnostic** :

- Certificat non rattaché sur le compte FBI de l'utilisateur externe (si certificat hors offre BDF)

⇨ **Actions à réaliser :**

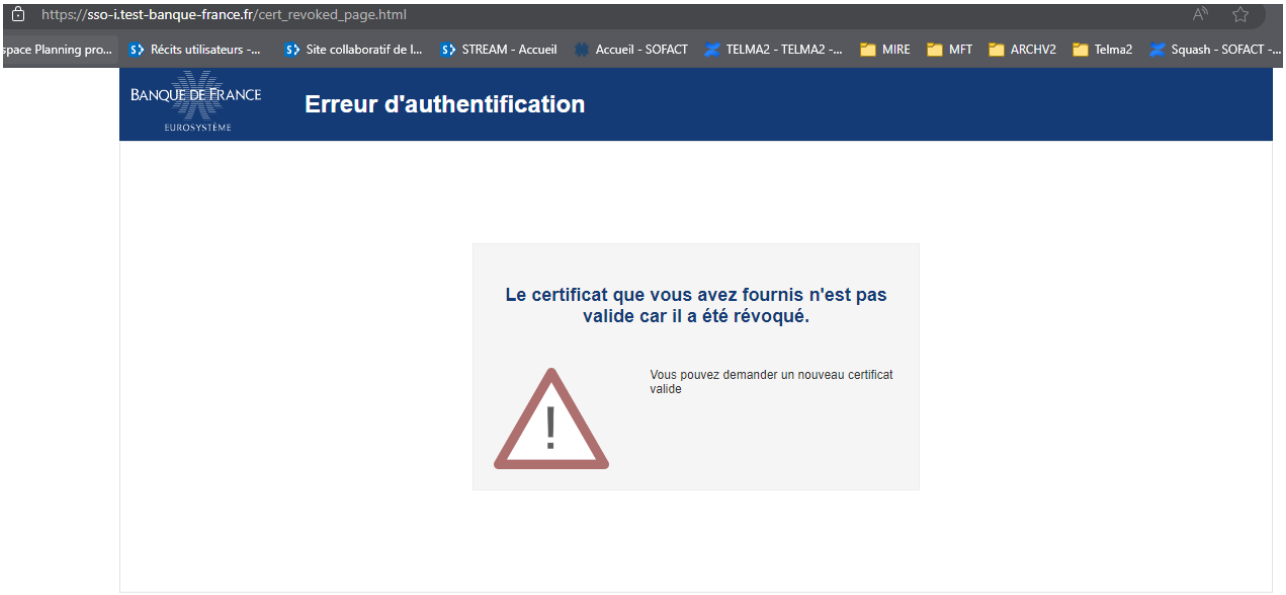
- (ARC) Modifier le paramétrage dans FBI
- L'utilisateur devra ensuite
  - Fermer son navigateur internet
  - Relancer son navigateur internet
  - Vider les caches
  - Lancer de nouveau l'URL ETENDER

1.6. Cas 4 - Certificat révoqué

Actions réalisées :

- Exécution de l'URL de connexion ETENDER
- Sélection du certificat
- Saisie du code PIN
- Code PIN **OK**

Cas : Affichage de l'erreur « Le certificat que vous avez fourni n'est pas valide car il a été révoqué. »



CAS : Tentative de connexion à ETENDER à l'aide d'un certificat révoqué.

⇨ **Diagnostic** : La date de validité du certificat a expiré.

⇨ **Actions à réaliser** :

- Le certificat doit être renouvelé. L'utilisateur doit demander une nouvelle création de certificat.

1.7. Cas 5 – FBI – Accès refusé

Actions réalisées :

- Exécution de l'URL de connexion ETENDER
- Sélection du certificat
- Saisie du code PIN
- Code PIN : **OK**
- Saisie du mot de passe d'authentification
- Mot de passe d'authentification : **OK**

Cas : Affichage de l'erreur « Accès refusé – Vous n'êtes pas autorisé à accéder à cette application. Veuillez contacter votre support ou "You are not authorized to acces this application. »

You are not authorized to access this application

⇨ **Diagnostic :** L'utilisateur possède bien un compte FBI avec le certificat référence.

Cependant, le rôle ETENDER n'est pas référencé sur le compte de cet utilisateur externe.

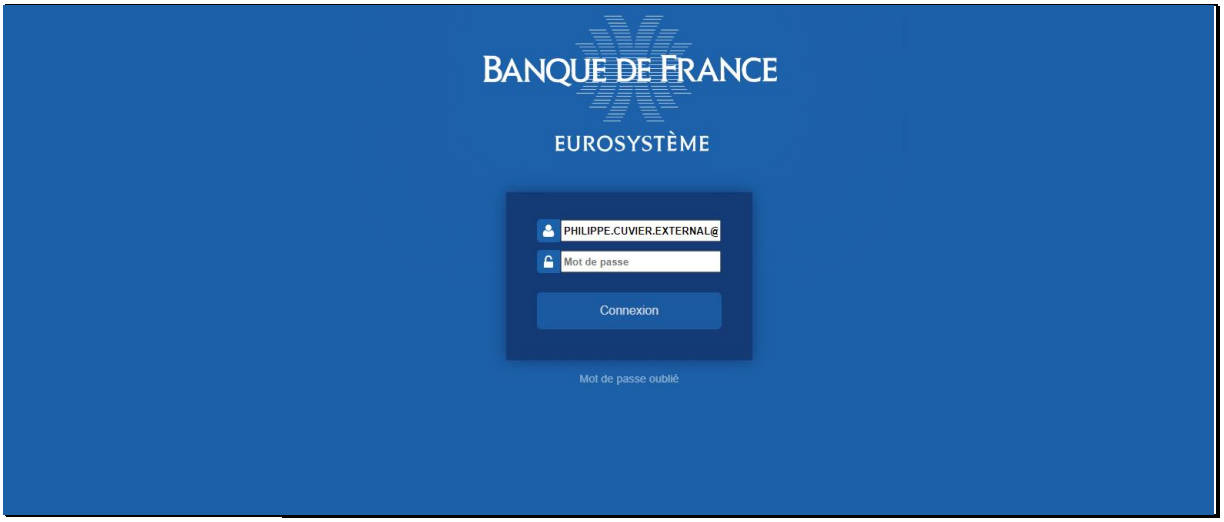
⇨ **Actions à réaliser par ARC, après transmission de l'information par l'utilisateur.**

1.8. Cas 6 – Unable to authenticate user X

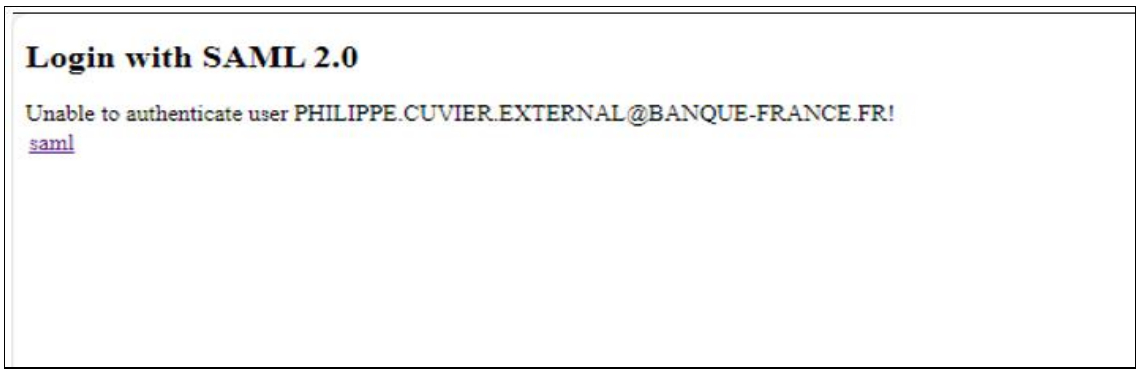
Actions réalisées :

- Exécution de l'URL de connexion ETENDER
- Sélection du certificat
- Saisie du code PIN
- Code PIN : **OK**
- Saisie du mot de passe d'authentification
- Mot de passe d'authentification : **OK**

Cas : Affiche de l'erreur « Login with SAML2.05 » après l'authentification FBI



saisie du mot de passe



⇨ **Diagnostic :** L'utilisateur est absent de la liste des utilisateurs (Counterparty user) dans TENDER

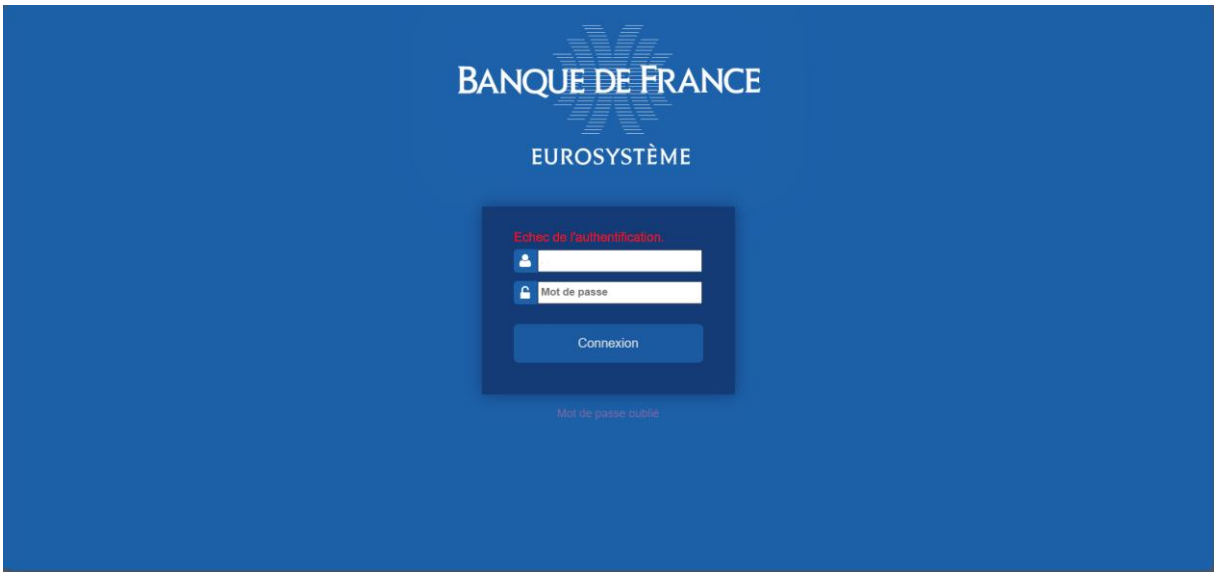
⇨ **Actions à réaliser par ARC : Modifier le paramétrage dans TELMA.**

1.9. Cas 7 - Mot de passe Erroné

Actions réalisées :

- Exécution de l'URL de connexion ETENDER
- Sélection du certificat
- Saisie du code PIN
- Code PIN : **OK**
- Mot de passe du compte FBI **KO**

Cas : Affichage de l'erreur « Echec de l'authentification » sur FBI »



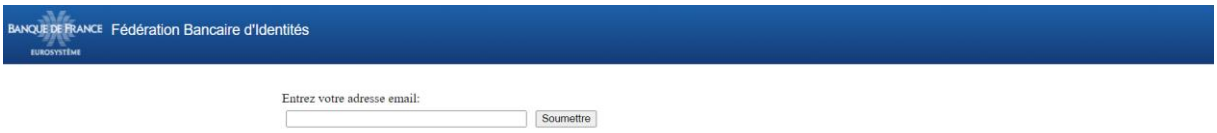
⇨ **Diagnostic** : L'utilisateur est alors dans l'un des cas suivants :

- Il n'est pas en possession du bon mot de passe,
- Il a oublié quel est le bon mot de passe,
- Il a saisi 5 fois un mauvais mot de passe.
- Le compte de l'utilisateur est verrouillé.

⇨ **Actions à réaliser par l'utilisateur** :

- Vérifier si le clavier est en mode QWERTY ou AZERTY et si le mode majuscules est activé.
- Demander la réinitialisation de son mot de passe via le bouton « Mot de passe oublié »

À l'activation du bouton « Mot de passe oublié », il faut d'abord renseigner l'adresse mail servant à l'authentification. À l'activation du bouton « Soumettre », un courriel contenant un lien permettant la réinitialisation du mot de passe du compte est alors envoyé vers l'adresse mail renseignée.



Une fois le lien activé, un formulaire permettant la configuration d'un nouveau apparait. Cette étape franchie, il est alors possible d'utiliser le nouveau mot de passe pour se connecter.