Gestion du code PIN RSA SecurID

Ordinateur portable

Cette fiche s'adresse aux personnes qui disposent d'un accès au réseau interne RTE.

Elle présente les différentes manipulations qu'un utilisateur muni d'un token SecurID physique ou d'un soft-token (appelé également token logiciel) peut être amené à effectuer pour créer son CODE PIN depuis l'interne.

Préambule

Les accès externes au SI de RTE ainsi que certains accès d'administration des composants du SI sont protégés par la solution d'authentification forte double facteur RSA SecurID qui vient généralement en complément du couple identifiant (NNI ou Windows) & mot de passe.

L'authentification forte double facteur est basée sur un **CODE PIN** composé de 4 chiffres et un dispositif RSA SecurID nommé **TOKEN**.

Deux types de TOKENs RSA SecurID sont disponibles chez RTE :
- les TOKENs physiques,
- les TOKENs logiciels.

INFOS

Le **TOKEN physique** fournit un code à 6 chiffres, appelé **TOKENCODE**, toutes les 60 secondes. Les barres à gauche du tokencode indiquent le temps restant avant le changement de code, chaque barre valant 10 secondes.

TOKEN physique

Il s'agit d'un générateur matériel de codes conçu pour se brancher au trousseau de clés de l'utilisateur.

Le code d'authentification qui est utilisé se nomme **PASSCODE** et est le résultat de la combinaison du CODE PIN suivi immédiatement (sans espace) du TOKENCODE.

Exemple : Si votre CODE PIN est **1847** et que le TOKENCODE affiché est *159759*, votre PASSCODE sera alors **1847***159759*.

INFOS

Le **TOKEN logiciel** fournit un code à 8 chiffres, appelé **PASSCODE**, toutes les 60 secondes. Le temps restant est indiqué sous le PASSCODE.

TOKEN logiciel

Il s'agit d'un logiciel installé sur l'iPhone qui permet la génération de **TOKENCODE** ou **PASSCODE**, c'est-à-dire d'un jeton à usage unique. L'objectif du TOKEN logiciel est d'éviter aux utilisateurs de transporter un dispositif matériel dédié d'authentification.
Pour obtenir ce PASSCODE, vous devez au préalable avoir renseigné votre code **CODE PIN** et ensuite valider :

Exemple : si votre **CODE PIN** est **1847**, lancez le token logiciel, renseignez 1847 dans le champ « Enter PIN » et valider. L'application affiche 93054800 ; votre PASSCODE sera alors 93054800.

INFOS

Les codes triviaux (0000, 1234…) sont interdits.

NB: Si vous n'avez pas de CODE PIN, il faut simplement cliquer sur la flêche bleue (voir encadré rouge ci-dessous), sans remplir la case blanche, pour générer un PASSCODE.

ASTUCE

Vous pouvez également renseigner directement « **RSA** » dans la barre d'adresses de votre navigateur et vous serez redirigé vers la bonne URL.

Création du CODE PIN

INFOS

Il est nécessaire de mémoriser le CODE PIN. Ce dernier n'étant connu que de vous seul, il ne pourra pas vous être communiqué en cas d'oubli.

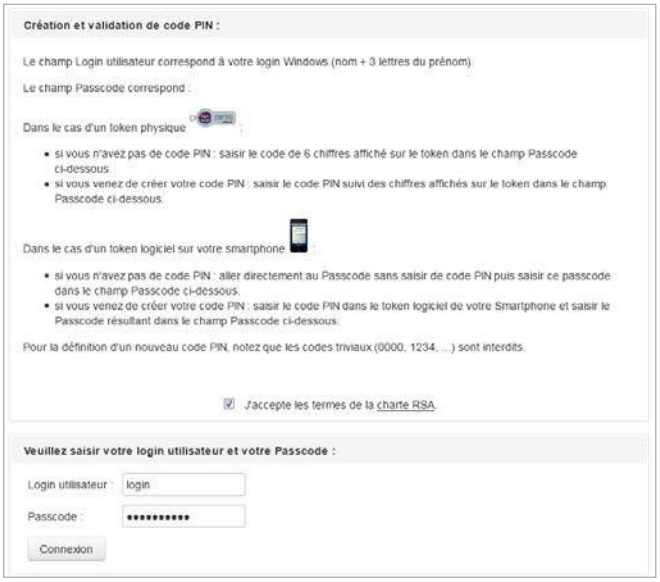
Dès lors que vous êtes en possession de votre token (SecurID ou soft-token), vous avez la possibilité de créer un CODE PIN.
Pour cela, rendez-vous sur le portail utilisateur de création des codes PIN accessible via l'URL suivante : **Connexion P3S**

Voici les actions à mener :

1 - Dans l'interface ci-contre, renseigner votre login utilisateur dans le champ « Login utilisateur ». Il s'agit du même login que votre **login WINDOWS** (nom + 3 premières lettres du prénom en général).
Appuyer ensuite sur le bouton « OK ».

Renseigner également dans le champ « Passcode », le code généré par votre token (les chiffres indiqués par votre token) : **il est nécessaire de vérifier que vous avez le temps pour le faire, c'est-à-dire que vous disposez d'au moins 20s avant la génération d'un nouveau code.**

Une fois les chiffres renseignés, cliquer sur « Log In ».



Remarque : Afin de définir votre code PIN, il est nécessaire d'accepter la charte, en cochant la case « J'accepte les termes de la charte RSA ».

ATTENTION

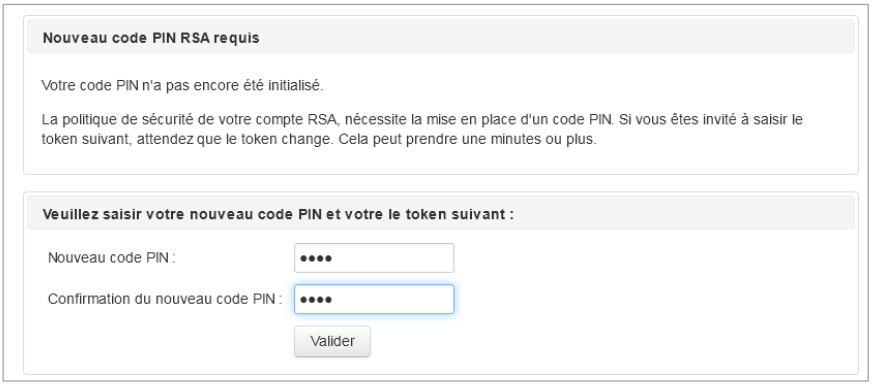
Tout comme un code de carte bleue, il vous faudra préserver le secret du code PIN : ne l'écrire nulle part, ne le communiquer à personne notamment par téléphone.
Si toutefois vous deviez noter temporairement ce code, il vous faudra bien veiller à ne pas le stocker avec le token SecurID physique et à supprimer la note dès que le code sera mémorisé.

INFOS

Il est nécessaire de mémoriser le CODE PIN. Ce dernier n'étant connu que de vous seul, il ne pourra pas vous être communiqué en cas d'oubli.

2 - L'application affiche la page ci-contre permettant de choisir son code PIN. Renseigner le code PIN que vous souhaitez dans le champ « Nouveau PIN ». Retaper ce même code PIN dans le champ « Confirmation du nouveau code PIN ».

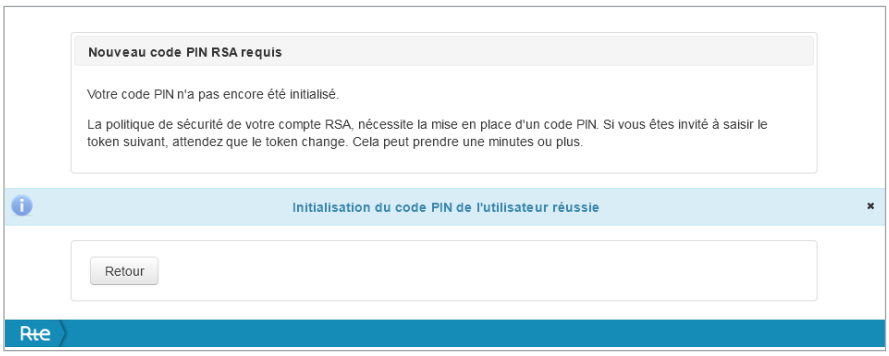
Une fois les deux champs renseignés, cliquez sur « OK ».



ATTENTION

Tout comme un code de carte bleue, il vous faudra préserver le secret du code PIN : ne l'écrire nulle part, ne le communiquer à personne notamment par téléphone.
Si toutefois vous deviez noter temporairement ce code, il vous faudra bien veiller à ne pas le stocker avec le token SecurID physique et à supprimer la note dès que le code sera mémorisé.

3 - Si l'authentification a réussi, vous êtes redirigé vers la page ci-dessous. Dans le cas contraire, merci de renouveler les opérations décrites ci-dessus.



Perte / oubli du CODE PIN

Lors de la perte ou l'oubli de votre CODE PIN, il est nécessaire dans un premier temps d'ouvrir un incident auprès de l'accueil pour demander une réinitialisation du CODE PIN, c'est-à-dire un reset qui va supprimer votre code PIN.

Une fois le code PIN réinitialisé, vous pouvez en créer un nouveau en exécutant la procédure de création du code PIN décrite au § Création du code PIN.

Renouvellement du TOKEN physique ou logiciel

Lors du renouvellement de votre token physique ou token logiciel, **il est nécessaire de changer votre code PIN.**