Enterprise PKI

Guide de prise en main rapide

Version 2.0

GlobalSign®

« EPKI » en un coup d'œil

Enterprise PKI (EPKI) est l'une des options disponibles depuis le portail de gestion de certificats GlobalSign (GCC).

**Optionel :* si votre compte a été configuré pour l'authentification client à deux facteurs (option de sécurité supplémentaire), il vous faudra d'abord installer un certificat d'authentification client, afin de pouvoir accéder à la section MES CERTIFICATS de votre compte.

Tutoriel de prise en main rapide du portail EPKI

Ce guide est un tutoriel simple de prise en main de votre compte EPKI. Pour des informations complètes et détaillées, veuillez vous référer au guide de l'administrateur EPKI et/ou cliquer sur les liens dans ce document pour accéder aux différents articles d'assistance technique.

Pour commencer

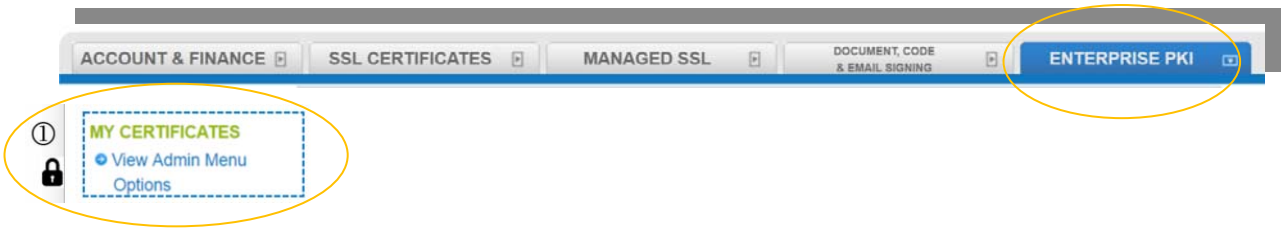
1. Veuillez vous connecter à votre compte GCC sur www.globalsign.fr/connexion
2. Entrez votre **identifiant d'utilisateur** (ex : PAR12345_username) et **mot de passe**
3. Cliquez sur l'onglet « ENTERPRISE PKI »

*Optionnel : si votre compte EPKI est configuré pour l'authentification client à deux facteurs (option de sécurité supplémentaire), il vous faudra installer un certificat d'authentification client, afin de pouvoir accéder à la section de gestion du cycle de vie de vos certificats. Les administrateurs du compte EPKI peuvent contacter l'équipe d'assistance GlobalSign pour activer (ou désactiver) l'option d'authentification client à deux facteurs.

Remarque : le certificat d'authentification client ne peut être utilisé que pour vous authentifier à votre compte GCC. Le nom commun du certificat correspond à votre identifiant d'utilisateur (ex : PAR10101_UserName).

Configuration du certificat d'authentification client EPKI (optionnel)

- Remarque : veuillez passer à la section suivante si votre compte n'est pas configuré pour l'authentification client.



1. Cliquez sur « **View Admin Menu Options »** dans le menu de gauche.

2. Entrez un mot de passe temporaire de téléchargement pour pouvoir télécharger votre certificat.

3. Vous allez recevoir un e-mail pour télécharger votre certificat. Veuillez installer le certificat (comme indiqué ci-dessous). Vous pouvez également lire ou télécharger les instructions via ce lien.

4. Cliquez sur le lien indiqué dans l'e-mail et entrez votre mot de passe temporaire de téléchargement. Vous devrez alors choisir un mot de passe **définitif** pour votre certificat.

5. Téléchargez ensuite le fichier .pfx qui contient les clés publique et privée. Cliquez deux fois sur le fichier pour lancer l'assistant d'importation du certificat et commencer à installer votre certificat dans votre magasin de certificats Windows. La plupart des paramètres par défaut peuvent être gardés.

6. Lorsque vient le moment d'entrer votre mot de passe, pensez à entrer le mot de passe **définitif** que vous avez créé lorsque vous avez téléchargé votre certificat. Nous vous recommandons de cocher l'option : « marquer la clé privée comme étant exportable ». Une fois ce processus terminé, le certificat d'administrateur EPKI est installé dans le magasin de certificats Windows et il peut être utilisé dans Internet Explorer, Edge et Chrome.

7. Une fois l'installation terminée, cliquez à nouveau sur **« View Admin Menu Options ».** Vous devrez alors vous authentifier à l'aide de votre certificat d'administrateur EPKI (le certificat qui doit être utilisé est celui qui a été émis pour le nom correspondant à votre **identifiant d'utilisateur**).

8. Vous serez peut-être déconnecté de votre compte, dans quel cas, veuillez réentrer vos identifiants de connexion. Vous serez alors automatiquement authentifié au portail et vous pourrez accéder aux options de gestion de vos certificats.

Emission de certificats

- **Remarque** : la vérification du profil doit être complétée avant de pouvoir émettre des certificats (2 à 3 jours ouvrés)

Options d'émission de certificats:

Intitulé du menu	Explication
MES CERTIFICATS Commander des certificats	**Emission à l'unité** Permet d'émettre des certificats individuels pour chaque utilisateur. L'e-mail de téléchargement du certificat est envoyé directement à l'utilisateur (plus d'informations ci-dessous).
Commander des certificats (EN NOMBRE)	**Emission de certificats en lot** Permet d'émettre des certificats en lot à partir d'un fichier CSV. Les e-mails de téléchargement de chaque certificat seront envoyés individuellement aux utilisateurs correspondants. Solution idéale pour émettre plus de 25 certificats.
Demande multiple d'enregistrements et de téléchargements au format PKCS#12	**Approvisionnement en lot** Permet de faire des demandes de certificats et de les télécharger en lot pour le compte des utilisateurs. Les certificats sont délivrés à l'administrateur (ou chargé de compte) dans un fichier ZIP contenant les PKCS12. Solution idéale pour émettre plus de 25 certificats.

MON PORTAIL DE COMMANDES Configuration du portail	**Lien de commande directe pour les utilisateurs** Les utilisateurs peuvent commander leur certificat depuis une URL de commande unique à chaque profil. Les utilisateurs choisissent eux-mêmes leur mot de passe de téléchargement. Remarque : l'administrateur ou le chargé de compte devront approuver les demandes de certificats en attente avant qu'ils ne soient émis (depuis la section « **Approuver les certificats en attente »**).

Comment émettre des certificats à l'unité :

1. Cliquez sur **« Commander des certificats »** dans la section « MES CERTIFICATS » du menu principal.

2. Choisissez le pack de licences et le profil appropriés. Cliquez sur « Suivant ».

3. Sur la page « Informations d'identification du certificat », entrez les informations relatives à l'utilisateur :
    a. **Nom commun :** correspond au prénom et au nom de famille (le nom complet sera affiché sur le certificat).
    b. **Adresse e-mail :** l'adresse e-mail de l'utilisateur (à laquelle sera envoyé le certificat)

4. Entrez un **mot de passe de téléchargement** : l'utilisateur aura besoin de ce mot de passe pour télécharger son certificat.

5. Cliquez sur « Suivant », confirmez les informations données et cliquez sur « Terminer » pour confirmer la demande.

6. L'utilisateur du certificat va recevoir un e-mail l'invitant à le télécharger dans quelques instants. Vous trouverez des guides d'installation pour les utilisateurs aux liens ci-dessous :
    a. GUIDE D'INSTALLATION PERSONALSIGN
    b. GUIDE D'INSTALLATION AATL (avec clé USB cryptographique)

Gestion des certificats

Intitulé du menu	Explication
MES CERTIFICATS Rechercher les commandes de certificats	**Rechercher des certificats émis** Cliquez sur le bouton **« Demande »** à côté du numéro de commande du certificat. **Options de gestion du certificat**

	• **Réémettre** : une nouvelle paire de clés est créée pour le certificat. La date d'expiration reste celle indiquée sur le certificat d'origine. • **Annuler** : l'option d'annulation n'est disponible que pendant sept jours après l'émission du certificat d'origine. Vous pouvez annuler une commande et recréditer le pack de licences utilisé lors de la commande. • **Révoquer** : à utiliser si la clé privée a été compromise. Les certificats révoqués sont ajoutés à la liste de révocation des certificats dans les 24 heures qui suivent, ce qui rend le certificat invalide pour la majorité des cas d'utilisation.
Rechercher dans l'historique des commandes en nombre de certificats au format PKCS#12	Cliquez sur ce bouton pour voir et télécharger le fichier ZIP qui contient les fichiers PKCS12 (si vous avez commandé vos certificats à l'aide de la méthode de demande et de téléchargement en nombre). Le fichier ZIP n'est conservé que pendant trente jours après que la commande ait été placée.

Autres fonctions EPKI

③	**MES LICENCES** • Rechercher les commandes de licences	Achetez des **packs de licences de certificats** et accédez à l'inventaire de vos packs existants. **Remarque :** seul l'administrateur du compte EPKI peut commander des licences à l'aide de l'option **« Commander des licences ».**
④	**MES PROFILS** • Configuration du profil • Rechercher les profils • Liste des domaines d'e-mail	Un **profil** est un « modèle pré-vérifié » de l'organisation et contient les informations relatives à l'identité de l'organisation. Les demandes de certificat sont émises depuis un profil choisi. Une fois la vérification du profil complétée, vous pouvez immédiatement émettre des certificats contenant les informations du profil. Options disponibles : modifier la configuration du profil, ajouter des profils, rechercher des profils existants et rechercher des listes de domaines d'e-mail pré-vérifiés.
⑥	**E-MAILS** • Gérer les modèles d'e-mails • Afficher tous les e-mails envoyés • Afficher les e-mails aux utilisateurs du portail	Utilisez l'option « Gérer les modèles d'e-mail » pour personnaliser les modèles d'e-mail utilisés par le système. Vous pouvez, par exemple, modifier l'e-mail de téléchargement du certificat « Enrollment (Invite) » pour ajouter les instructions de téléchargement et d'installation du certificat. • GUIDE D'INSTALLATION PERSONALSIGN • GUIDE D'INSTALLATION AATL (avec clé USB cryptographique) Vous pouvez également lire et renvoyer les e-mails envoyés aux utilisateurs depuis le système.
⑦	**AUTRES FONCTIONS** • Action Log • Configurer LDIF	Créez un rapport au format LDIF (Lightweight Directory Access Protocol) que vous pourrez télécharger dans un annuaire LDAP.
⑧	**RESSOURCES** • Guide d'authentification de l'admin EPKI • Guide de l'administrateur EPKI	Accédez au guide de l'administrateur EPKI et au guide de l'administrateur et de l'authentification EPKI (spécifique au certificat d'authentification client EPKI).

Ajouter des utilisateurs GCC

1. Cliquez MON ESPACE CLIENT, puis sur l'icône « Utilisateurs » et, enfin, sur **« New Registration ».**

2. Entrez les informations requises et cliquez sur « Confirm » pour confirmer la demande.

Types d'utilisateur GCC :

- **Administrateur du compte :** il ne peut y avoir qu'un seul administrateur par compte. Il en a le contrôle intégral , il peut **acheter des packs de licences**, modifier les informations du compte ou d'un profil et créer d'autres types d'utilisateur. L'administrateur peut aussi voir toutes les commandes placées par les autres utilisateurs et peut notamment réémettre, annuler et révoquer des certificats.

- **Chargé de compte :** les droits du chargé de compte sont semblables à ceux de l'administrateur mais il **ne peut pas acheter de pack de licences.** Le chargé de compte peut ajouter des utilisateurs de type « personnel responsable ».
  ***Remarque :** l'**administrateur** et le(s) **chargé(s) de compte** peuvent installer des certificats d'administrateur EPKI qui permettent d'accorder des privilèges de gestion de certificats.

- **Personnel responsable :** les droits administratifs des utilisateurs à ce niveau (commande de certificats, approbation, révocation, ajout d'acompte) sont définis par l'administrateur du compte ou le chargé de compte. Contrairement aux autres types d'utilisateurs, le personnel responsable ne peut pas créer d'utilisateurs supplémentaires.

Coordonnées GlobalSign

GlobalSign Americas Tel : 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	**GlobalSign EU** Tel : +32 16 891900 www.globalsign.eu sales@globalsign.com	**GlobalSign UK** Tel : +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel : +33 9 75 18 32 00 www.globalsign.fr ventes@globalsign.com	**GlobalSign DE** Tel: +49 800 723 79 80 www.globalsign.de verkauf@globalsign.com	**GlobalSign NL** Tel : +31 85 888 2424 www.globalsign.nl verkoop@globalsign.com