Comment extraire le certificat public d'un certificat matériel ?

Préambule

L'application Egide nécessite l'utilisation d'un certificat matériel pour s'authentifier.

Un certificat matériel contient deux éléments complémentaires : une clé privée et un certificat public. Le certificat public est l'élément à fournir à l'application Egide.

Cette documentation détaille la procédure de récupération du certificat public depuis un certificat matériel et s'applique aux navigateurs Microsoft Internet Explorer 9 ou Mozilla Firefox (version 24 minimum).

Procédure

La procédure diffère selon le navigateur utilisé.

Microsoft Internet Explorer 9

- S'assurer de la présence du certificat matériel sur le système.
- Ouvrir Internet Explorer.
- Ouvrir le menu paramètres (sous la flèche rouge sur la figure 1).
- Cliquer sur Options Internet (encadré en rouge sur la figure 1).

Imprimer Fichier Zoom (100%) Sécurité	
Afficher les téléchargements Gérer les modules complémentaires Outils de développement F12 Atteindre les sites épinglés	
Options Internet	
A propos de Internet Explorer	

Figure 1 - Accéder aux Options Internet

• Cliquer sur l'onglet Contenu (encadré en rouge sur la figure 2).

Sécurité Confide	entialité Contenu Con	nexions Programm	es Avancé
e démarrage –			
Pour créer des	onglets de page de déma	arrage, entrez une a	dresse pa <mark>r lig</mark> ne.
http://portal.	.corp.sopra/		* *
	Page actuelle	Par défaut	Page vierge
que de navigation		2503	
Supprimer 11	historique de navigation (en quittant le naviga	Paramètres
rches		Supprinterm	J [raidined to]
Modifier les par	amètres de recherche pa	ar défaut.	Paramètres
s —		1 I. I.	[- 1;]
Modifier la pres	entation des pages Web	dans les onglets.	Paramétres
ence			
			2 · · · · · · · · · · · · · · · · · · ·
	e démarrage Pour créer des Pour créer des http://portal que de navigation Supprimer les fi enregistrés et l Supprimer l' rches Modifier les par s Modifier la prés	e démarrage Pour créer des onglets de page de déma http://portal.corp.sopra/ Page actuelle que de navigation Supprimer les fichiers temporaires, l'hist enregistrés et les données de formulaire Supprimer l'historique de navigation crches Modifier les paramètres de recherche pa	e démarrage Pour créer des onglets de page de démarrage, entrez une a http://poital.corp.sopra/ Page actuelle Par défaut que de navigation Page actuelle Supprimer les fichiers temporaires, l'historique, les cookies, l'enregistrés et les données de formulaires Web. Supprimer l'historique de navigation en quittant le naviga Supprimer l'historique de navigation en quittant le naviga Supprimer rches Modifier les paramètres de recherche par défaut. Modifier la présentation des pages Web dans les onglets.

Figure 2 - Options Internet

- Cliquer sur Certificats (encadré rouge sur la figure 3).
- Sélectionner le certificat correspondant à l'authentification à exporter, dans l'un des onglets (encadré vert sur la figure 3).
- Une fois le certificat sélectionné, cliquer sur Exporter (encadré bleu sur la figure 3).

Options Internet ? 🔀	Certificats
Général Sécurité Confidentialité Contenu Connexions Programmes Avancé	Rôle prévu : <a>
Gestionnaire d'accès Centrolidite l'égramètres I de contrôle d'accès vous permet de contrôler le type de contenu Internet qui peut être visualisé sur cet ordinateur. I de contrôle d'accès vous permet de contrôler le type de contenu Internet qui peut être visualisé sur cet ordinateur. I de contrôle d'accès vous permet de contrôler le type de contenu Internet qui peut être visualisé sur cet ordinateur. I de contrôle d'accès vous permet de contrôler le type de contenu Internet qui peut être visualisé sur cet ordinateur. I diser d'état SSL I diteurs Saisie semi-automatique I La saisie semi-automatique stocke les entrées précédentes sur des pages Web et suggère des correspondances.	Personnel Autorités de certification intermédiaires Autorités de certification intermédiaires Délivré à Délivré par Expiration Nom convivial
Flux et composants Web Slice Paramètres Les flux et les composants Web Slice offrent un contenu mis à jour à partir de sites Web, lisible dans Internet Explorer et dans d'autres programmes. Paramètres	Importer Exporter Supprimer Avancé Détails de certificat Authentification du client Affichage En savoir plus sur les certificats Fermer
OK Annuler Appliquer	

Figure 3 - Onglet Contenu et fenêtre des certificats

• L'assistant d'exportation s'ouvre. Cliquer sur suivant (figure 4).

Bienvenue !
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats depuis le magasin de certificats vers votre disque dur.
Un certificat, émis par une autorité de certification, est une confirmation de votre identité et contient des informations utilisées pour protéger vos données ou établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés. Cliquez sur Suiverst pour continuer.

Figure 4 - Assistant d'exportation (1)

• S'assurer que la case « Non, ne pas exporter la clé privée » est sélectionnée (encadré en rouge sur la figure 5) puis cliquer sur suivant.

Vous pouvez choisir d'exporter la c	dé privée avec le certificat.
Les dés privées sont protégées pa avec le certificat, vous devrez enti	n mot de passe. Pour pouvoir exporter la dé privée rer un mot de passe.
Voulez-vous exporter la clé privée	avec le certificat ?
Oui, exporter la dé privée	
Non, ne pas exporter la dé	privée
Remarque : la dé privée associée e	est marquée comme non exportable. Seul le
Remarque : la dé privée associée e certificat peut être exporté.	est marquée comme non exportable. Seul le
Remarque : la clé privée associée e certificat peut être exporté. 1formations sur <u>l'exportation des clés (</u>	est marquée comme non exportable. Seul le

Figure 5 - Assistant d'exportation (2)

• Sélectionner « X.509 encodé en base 64 (.cer) » (encadré en rouge sur la figure 6) puis cliquer sur suivant.

Forr	nat de fichier d'exportation Les certificats peuvent être exportés sous plusieurs formats de fichier.
Séle	ctionnez le format à utiliser :
10	🔿 X.509 binaire encodé DER (.cer)
Г	X.509 encodé en base 64 (.cer)
	Standard de syntaxe de message de chiffrement - Certificats PKCS #7 (.p7b)
	Inclure tous les certificats dans le chemin d'accès de certification si possible
	Échange d'informations personnelles - PKCS #12 (.pfx)
	🗌 Inclure tous les certificats days le chemin d'accès de certification si possible
	Supprimer la dé privée si l'exportation s'effectue correctement
	Exporter toutes les propriétés étendues
	Magasin de certificats sérialisés Microsoft (.sst)
Info	rmations sur les <u>formats de fichiers de certificats</u>
	(Defendent Output)

Figure 6 - Assistant d'exportation (3)

• Sélectionner un dossier où sauvegarder le fichier en cliquant sur parcourir (encadré en rouge sur la figure 7), entrer un nom de fichier puis cliquer sur suivant.

Fichier à exporter Spécifiez le nom du fichier à e	voorter		
opeanez le nom da nemer a e			
Nom du fichier :			
certificat_public		Parcourir	
			1

Figure 7 - Assistant d'exportation (4)

• Cliquer sur terminer (figure 8).

Vous avez terminé l'exécut certificat. Vous avez spécifié les para Nom du fichier Exporter les clés Indure tous les certificats Format de fichier	ion de l'Assistant Exportation o mètres suivants : : dans le chemin d'accès de ce
Vous avez spécifié les para Nom du fichier Exporter les dés Indure tous les certificats Format de fichier	mètres suivants : ; dans le chemin d'accès de ce
Nom du fichier Exporter les dés Indure tous les certificats Format de fichier	: dans le chemin d'accès de ce
Exporter les dés Indure tous les certificats Format de fichier	: dans le chemin d'accès de ce
Inclure tous les certificats Format de fichier	: dans le chemin d'accès de ce
Format de fichier	
۲. m	
۲. III III III III III III III III III I	
٠ •	1
×	K I

Figure 8 - Assistant d'exportation (5)

- Ouvrir l'explorateur de fichier.
- Renommer le fichier « certificat_public.cer » en « certificat_public.crt ».
- Sur la fenêtre de confirmation qui s'ouvre, cliquer sur « Oui » (encadré en rouge sur la figure

٩١	
~	•

Renomm	ner					
	Si vous modifiez l'extension d'un fichier, le fichier risque d'être inutilisab					

Figure 9 - Confirmation de renommage

Mozilla Firefox (version 24 minimum)

- S'assurer de la connexion du certificat matériel sur l'ordinateur.
- Ouvrir Mozilla Firefox.
- Ouvrir le menu principal (sous la flèche rouge sur les figures 10 et 11)
- Cliquer sur Options (encadré en rouge sur les figures 10 et 11)



Figure 10 – Accéder aux options sur Firefox 24



Figure 11 - Accéder aux options sur Firefox 29

- Cliquer sur l'onglet avancé (encadré jaune sur la figure 12).
- Cliquer sur l'onglet Certificats (encadré rouge sur la figure 12).
- Cliquer sur Afficher les certificats (encadré cyan sur la figure 12).
- Sélectionner le certificat privé correspondant à l'authentification dans l'un des onglets de la fenêtre Gestionnaire de Certificats (encadré vert sur la figure 12).
- Une fois le certificat sélectionné, cliquer sur Voir (encadré bleu sur la figure 12).

Options	Sestionnaire de certificats	~
Options Général Onglets Contenu Applications Vie privée Sécurité Sync Avancé Sénéral Données collectées, Réseau Mises à jour Cettificats Lorsqu'un serveur demande mon cettificat personnel : • gn sélectionner un automatiquement • me demander à chaque fois Affricher les cettificats Yalidation Dériphériques de sécurité	Gestionnaire de certificats Gestionnaire de certificats Vos certificat Vos certificats Vos certificat Vos ceri	
OK Annuler Ajde	OK Rechercher refox et vous souhaitez accéder à vos marque-pages, mots us, depuis n'importe quel appareil ? Créez un compte Sync.	

Figure 12 - Options et gestionnaire de certificats sous Firefox

- Cliquer sur l'onglet Détails (encadré en rouge sur la figure 13).
- Cliquer sur Exporter (encadré en bleu sur la figure 13).

Figure 13 - Détails d'un certificat sur Firefox

• Sélectionner un dossier où sauvegarder le fichier, entrer un nom de fichier, s'assurer d'avoir sélectionné le type Certificat X.509 (PEM) (*.crt ; *.pem) (encadré en rouge sur la figure 14) puis cliquer sur Enregistrer.

Enregistrer le certificat dans un fichier						
S → Bibliothèques > Documents >					echercher dans : Documents	0
Organiser 👻	Nouveau dossier					0
Nom	<u>^</u>	Modifié le	Туре	Taille		
Nom du fichier	; certificat_public.crt					+
Туре	: Certificat X.509 (PEM) (*.crt;*.pem)				
			45		nregistrer Appule	
Cacher les doss	lers				Annule	