

Certification X509 avec SR Infosystèmes

Version 0.02
Édition du 10 février 2006

Copyright © 2006, SR Infosystèmes.

Ce document peut être copié, en partie ou entièrement, sous n'importe quelle forme et par n'importe quel moyen pourvu que les altérations soient clairement repérées et que la notice de copyright soit incluse sans modification dans toutes les copies.

Contact :

SR Infosystèmes
La Morinière
17550 Dolus d'Oléron
France

Tél : +33 (0) 6.70.70.54.57
Fax : +33 (0) 5.46.85.24.08

contact@sriviere.info
<http://sriviere.info>

Table des matières

1	Introduction	1
1.1	Généralités	1
1.2	X509 en quelques lignes	1
1.3	Installation	1
1.3.1	Téléchargement de X509-SRI	1
1.3.2	Installation	1
2	Utilisation	2
2.1	Demande du certificat X509	2
2.2	Création du certificat X509	2
3	Importation X509 dans Mozilla/Thunderbird	4
3.1	Importation du certificat de l'Autorité	4
3.1.1	Importation	4
3.1.2	Contrôle de l'authenticité du certificat	4
3.1.3	Importation du certificat de Stéphane Rivière	4
3.1.4	Contrôle de l'authenticité du certificat	4
3.2	Importation de votre certificat	4
3.3	Sélection de votre certificat	5
4	Importation X509 dans Outlook/Outlook express	6
4.1	Importation du certificat de l'Autorité	6
4.1.1	Importation	6
4.1.2	Contrôle de l'authenticité du certificat	6
4.1.3	Importation du certificat de Stéphane Rivière	6
4.1.4	Contrôle de l'authenticité du certificat	6
4.2	Importation de votre certificat	6
4.3	Sélection de votre certificat	6
5	Désinstallation	8
Annexe A	Références	9
Annexe B	Versions	10

1 Introduction

1.1 Généralités

X509-SRI est une application de création de certificats X509 compatibles avec les logiciels de courrier tels que Thunderbird, Mozilla, Outlook et Outlook express.

L'utilisation d'un certificat X509 permet d'établir une communication sûre avec SR Infosystèmes.

1.2 X509 en quelques lignes

X509-SRI permet de demander un certificat à l'autorité de certification SR Infosystèmes.

SR Infosystèmes signe la demande de certificat reçue, puis la renvoie au demandeur.

À partir de cette demande validée, X509-SRI peut créer un certificat X509 propre au demandeur. Ce certificat X509 personnel, et validé par l'autorité de certification, est alors importé dans le logiciel de courrier utilisé.

C'est donc une opération en deux temps (demande puis création), qui permet, à travers un canal non sûr (internet par exemple) de créer un moyen de communication raisonnablement sécurisé (niveau commercial).

Les principaux paramètres de sécurité sont, pour le système à clé privée, un DES3 (168 bits) et pour la clé publique un RSA (2048 bits).

X509 est une technologie d'authentification et de chiffrement à clé publique normalisée par l'UIT, comparable à PGP, mais parfaitement standardisée et déjà intégrée dans les logiciels de courriers usuels.

X509 est une technologie mûre, dont la première version remonte à 1988. X509 est actuellement en version 3.

1.3 Installation

1.3.1 Téléchargement de X509-SRI

X509-SRI est disponible sur le site : <http://sriviere.info>

Par mesure de protection, le programme d'installation est auto-chiffré par un algorithme RC4 avec une clé de 128 bits.

1.3.2 Installation

Lancer l'installation par la commande : *Setup Certification X509-SRI 1.0.exe*

- À l'écran d'accueil, cliquez sur **Suivant** ;
- Saisissez le mot de passe demandé¹ et cliquez sur **Suivant** ;
- Validez le répertoire d'installation par défaut *C:\Program iles\Certification X509-SRI* ou changez de répertoire, puis cliquez sur **Suivant** ;
- Cochez la case "icônes supplémentaires" si vous souhaitez avoir les icônes de demande et de création de certificat sur le bureau, puis cliquez sur **Suivant** ;
- Cliquer sur **Installer**, puis sur **Terminer**.

¹ Contacter SR Infosystèmes pour l'obtention du mot de passe.

2 Utilisation

2.1 Demande du certificat X509

Dans l'exemple ci-dessous, le nom d'utilisateur est *Jean Dupont* et l'email est jean@dupond.com

Lancer la demande de certificat X509, soit :

- Par Démarrer / Programmes / Certification X509-SRI / Demande du certificat X509 ;
- Ou en cliquant sur l'icône Demande du certificat X509, si l'option d'affichage des icônes a été sélectionnée pendant lors de l'installation.

Dans la console, comme indiqué sur l'écran :

- Saisissez vos initiales en minuscules sur deux caractères maximum ("jd" dans ce cas) et appuyer sur ;
- Entrez votre prénom et votre nom, séparés par un espace, en minuscules et sans accents ("jean dupont" dans ce cas) et appuyer sur .
- Renseignez votre email ("jean@dupond.com" dans ce cas) et appuyer sur .

Un certificat X509 est lié à l'adresse email utilisé ! Prenez garde de bien saisir l'email qui sera ensuite utilisé dans votre logiciel de courrier pour communiquer avec SR Infosystèmes.

Deux fichiers ont été créés dans le répertoire d'installation (par défaut *C:\Program Files\Certification X509-SRI*) :

- Le fichier *usr-jd.key*, clé privée appartenant à Jean Dupont. Attention, le fichier est en clair et il devrait être placé dans un endroit sûr.
- Le fichier *usr-jd.csr*, fichier chiffré contenant le formulaire de demande de certification pour Jean Dupond.

Envoyez ce fichier de demande '*usr-jd.csr*' à x509@sriviere.info email de l'autorité de certification X509 SR Infosystèmes.

2.2 Création du certificat X509

Dans l'exemple ci-dessous, le nom d'utilisateur est *Jean Dupont* et l'email est jean@dupond.com.

Quand la demande est signée par l'autorité de certification X509 SR Infosystèmes, elle est renvoyée par x509@sriviere.info à jean@dupond.com.

Le message contient le fichier '*usr-jd.crt*' en pièce jointe, qui doit être placé dans le répertoire d'installation (par défaut *C:\Program Files\Certification X509-SRI*).

Lancer la création du certificat X509, soit :

- Par Démarrer / Programmes / Certification X509-SRI / Création du certificat X509 ;
- Ou en cliquant sur l'icône Création du certificat X509, si l'option d'affichage des icônes a été sélectionnée pendant lors de l'installation.

Dans la console, comme indiqué sur l'écran :

- Saisissez vos initiales en minuscules sur deux caractères maximum ("jd" dans ce cas) et appuyer sur ;
- Entrez votre prénom, sans espace, en minuscules et sans accents ("jean" dans ce cas) et appuyer sur .

- Entrez votre nom, sans espace, en minuscules et sans accents (“dupont” dans ce cas) et appuyer sur Entrée.
- Au message “Enter export password :”, saisissez un mot de passe pour votre certificat et appuyer sur Entrée.
- Au message “Verifying password - Enter export password :”, saisissez à nouveau, pour contrôle, le mot de passe de votre certificat et appuyer sur Entrée.

Félicitation ! Votre certificat X509 pour SR Infosystèmes vient d’être créé.

Il se présente sous la forme d’un fichier chiffré ‘usr-jd.p12’, situé dans le répertoire d’installation (par défaut *C:\Program Files\Certification X509-SRI*).

Il ne vous reste plus qu’à insérer ce certificat dans votre logiciel de courrier favori.

3 Importation X509 dans Mozilla/Thunderbird

Si vous n'avez jamais créé de "mot de passe principal" dans ce logiciel, allez dans "Préférences / Confidentialité et sécurité / mot de passe principal", afin de protéger la gestion de vos certificats, puis cliquer sur "Créer un mot de passe".

Après cette opération, allez dans "Préférences / Confidentialité et sécurité / Certificats / Gestion des certificats".

3.1 Importation du certificat de l'Autorité

3.1.1 Importation

Aller dans l'onglet "Autorités".

Importer le certificat 'ca-sri.crt', situé dans le répertoire d'installation (par défaut *C:\Program Files\Certification X509-SRI*).

Confirmer cette autorité de certification pour Web, Courrier et Développeurs.

3.1.2 Contrôle de l'authenticité du certificat

À titre d'ultime précaution, il peut être intéressant de vérifier que le certificat de l'autorité SR Infosystèmes est bien authentique.

Cliquer sur "Voir".

Le certificat peut être contrôlé en comparant l'empreinte numérique SHA1 affichée à la séquence hexadécimale suivante : *E1 19 29 60 A4 70 D0 D5 88 82 0A 0C F5 40 A8 4A D9 5A 07 22*

3.1.3 Importation du certificat de Stéphane Rivière

Aller dans l'onglet "Autres personnes"

Importer le certificat 'usr-sr.crt', situé dans le répertoire d'installation (par défaut *C:\Program Files\Certification X509-SRI*).

3.1.4 Contrôle de l'authenticité du certificat

À titre d'ultime précaution, il peut être intéressant de vérifier que le certificat de Stéphane Rivière est bien authentique.

Cliquer sur Voir.

Le certificat peut être contrôlé en comparant l'empreinte numérique SHA1 affichée à la séquence hexadécimale suivante *78 99 DE 7D 09 CA 61 08 23 CA 74 DC E1 6C 36 24 A0 E2 73 BB*.

3.2 Importation de votre certificat

Dans l'exemple ci-dessous, le nom d'utilisateur est *Jean Dupont* et l'email est jean@dupond.com.

Aller dans l'onglet "Vos certificats"

Importer le certificat 'usr-jd.p12', situé dans le répertoire d'installation (par défaut *C:\Program Files\Certification X509-SRI*).

Saisir le mot de passe principal (le mot de passe du logiciel).

Saisir le mot de passe de la clé (le mot de passe du certificat).

3.3 Sélection de votre certificat

Allez dans “Edition / Paramètre / <Votre compte>¹ / Sécurité”.

Sélectionner votre certificat nouvellement importé pour la signature et le chiffrement.

Vous pouvez cocher la case “Signer les messages numériquement”, mais il est déconseillé de sélectionner “Toujours chiffrer les messages” si la majorité des messages que vous envoyez n’est pas chiffrée.

Félicitations ! Votre système de communication sécurisé X509 avec SR Infosystèmes est prêt à l’emploi. Utilisez toujours l’email contact@sriviere.info

¹ Assurez vous de sélectionner le compte ayant la même adresse e-mail que votre certificat

4 Importation X509 dans Outlook/Outlook express

Allez dans “Outils / Options / Sécurité”.

Cliquez sur “Certificats”.

4.1 Importation du certificat de l’Autorité

4.1.1 Importation

Aller dans l’onglet “Autorités principales de confiance”.

Importer le certificat ‘`ca-sri.crt`’, situé dans le répertoire d’installation (par défaut `C:\Program Files\Certification X509-SRI`).

4.1.2 Contrôle de l’authenticité du certificat

À titre d’ultime précaution, il peut être intéressant de vérifier que le certificat de l’autorité SR Infosystèmes est bien authentique.

Cliquer sur “Affichage / Détail / Empreinte numérique”.

Le certificat peut être contrôlé en comparant l’empreinte numérique SHA1 affichée à la séquence hexadécimale suivante : `E1 19 29 60 A4 70 D0 D5 88 82 0A 0C F5 40 A8 4A D9 5A 07 22`.

4.1.3 Importation du certificat de Stéphane Rivière

Aller dans l’onglet “Autres personnes”

Importer le certificat ‘`usr-sr.crt`’, situé dans le répertoire d’installation (par défaut `C:\Program Files\Certification X509-SRI`).

4.1.4 Contrôle de l’authenticité du certificat

À titre d’ultime précaution, il peut être intéressant de vérifier que le certificat de Stéphane Rivière est bien authentique.

Cliquer sur “Affichage / Détail / Empreinte numérique”.

Le certificat peut être contrôlé en comparant l’empreinte numérique SHA1 affichée à la séquence hexadécimale suivante `78 99 DE 7D 09 CA 61 08 23 CA 74 DC E1 6C 36 24 A0 E2 73 BB`.

4.2 Importation de votre certificat

Dans l’exemple ci-dessous, le nom d’utilisateur est *Jean Dupont* et l’email est jean@dupond.com.

Aller dans l’onglet “Personnel”

Importer le certificat ‘`usr-jd.p12`’, situé dans le répertoire d’installation (par défaut `C:\Program Files\Certification X509-SRI`).

Saisir le mot de passe de la clé (le mot de passe du certificat).

4.3 Sélection de votre certificat

Allez dans “Outil / Comptes / Courrier / <votre compte>¹ / Propriétés / Sécurité”.

Sélectionner votre certificat nouvellement importé pour la signature et le chiffrement.

Assurez vous d’avoir sélectionné l’algorithme de chiffrement “3DES”.

¹ Assurez vous de sélectionner le compte ayant la même adresse e-mail que votre certificat

Vous pouvez cocher la case “Signer les messages numériquement”, mais il est déconseillé de sélectionner “Toujours chiffrer les messages” si la majorité des messages que vous envoyez n’est pas chiffrée.

Félicitations ! Votre système de communication sécurisé X509 avec SR Infosystèmes est prêt à l’emploi. Utilisez toujours l’email contact@sriviere.info

5 Désinstallation

Le programme peut être désinstallé par :

Le menu Démarrer : Démarrer / Programmes / Certification X509-SRI / Désinstaller Certification X509-SRI

L'application d'ajout et de suppression de programmes du panneau de configuration.

Dans tous les cas, vos éléments privés et publics créés sont conservés dans le répertoire d'installation (par défaut *C:\Program Files\Certification X509-SRI*).

Annexe A Références

Fichiers remarquables

Le répertoire d'installation (par défaut *C:\Program Files\Certification X509-SRI*) contient des fichiers remarquables :

- ca-sri.crt : certificat public autorité de certification SR Infosystèmes ;
- usr-sr.crt : certificat public du correspondant Stéphane Rivière ;
- sri.rnd : aléa spécifique SR Infosystèmes.

Extensions courantes

Les fichiers X509 sont facilement identifiables par leur extension :

- .csr : Demande de certificat ;
- .crt : Certificat public ;
- .key : Clé privée du certificat, à conserver en lieu sûr ;
- .p12 : Certificat personnel contenant l'intégralité des éléments privés et publics, à conserver en lieu sûr ;

Annexe B Versions

Versions

0.01	09/02/06	Version initiale
0.02	10/03/06	Version de distribution initiale