Réseau de transport d'électricité

Date d'approbation : 03/12/2010
Date d'applicabilité : 03/12/2010
Date de fin de validité :

| | | | | |
|---|---|---|---|---|
| NT | - | PSI-CEESI-DPSC-GSF | 10 | 00999 |

Indice : 3

# Echanges de données entre RTE et un Partenaire au moyen du protocole HTTPS

13 Pages 1 annexe

Documents annulés :
Documents de référence :
Référence fonctionnelle :
Résumé :

Accessibilité :

| | |
|---|---|
| Libre | |
| RTE | X |
| Restreinte | |
| Confidentielle | |

Métier et processus porteurs directement impliqués :

| | |
|---|---|
| Métier, fonction | SI |
| Macroprocessus RTE | |
| Processus local | |

Domaine GED :

| | |
|---|---|
| Public | X |
| Privé | |

Programmes & SI (PSI)
***TOUR MARCHAND***
***41 RUE BERTHELOT - 92411 COURBEVOIE CEDEX***
***TEL : 01.78.66.50.00 - FAX : 01.78.66.50.64***

Echanges de données entre RTE et un Partenaire
au moyen du protocole HTTPS

| Rédacteur(s) | | Vérificateur(s) | | Approbateur(s) | |
|---|---|---|---|---|---|
| Nom | Visa | Nom | Visa | Nom | Date/Visa |
| Y.Djerroud<br>G-d.Nguyen | | G-d.Nguyen | | P.Bourdon | |
| Lieu de conservation (ou...) : | | | | | |

| DIFFUSION | |
|---|---|
| Pour action | Pour information |
| | P. Bourdon (DAUSI)<br>G. Bonnary (DAUSI)<br>F. Lenoir (DPSC / GSF)<br>J. Viseux (DPSC / GSF) |

## HISTORIQUE

| Indice | Date | Projet ou Pour approbation | Rédacteur(s) | Modifications |
|---|---|---|---|---|
| 0.1 | 25/11/10 | Projet | Y.Djerroud / G.Nguyen | Création du document |
| 1 | 26/11/10 | Approuvé | S.Pham | Prise en compte des remarques |
| 2 | 03/12/10 | Approuvé | S.Pham | Prise en compte des remarques de P.Bourdon |
| 3 | 05/01/12 | Approuvé | Y.DJERROUD | Ajout d'un exemple de requête HTTP POST MULTIPART en cURL |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# SOMMAIRE

# 1. Objet du document

Ce document est destiné à un Partenaire avec lequel RTE va réaliser des échanges électroniques au moyen du protocole https (*Hypertext Transfer Protocol Secure*).

Le document indique les paramétrages et configurations pour ces échanges, qu'ils soient dans le sens de RTE vers le Partenaire, ou dans le sens du Partenaire vers RTE.

Les échanges décrits ne présupposent ni n'imposent aucun outil. Le protocole https est un standard (voir IETF RFC 2818).

# 2. Configuration réseau requise

Le Partenaire doit disposer d'un point d'accès au réseau Internet sur une liaison haut débit.

Les échanges nécessitent l'établissement d'une connexion entre un équipement du Front-Office de RTE (l'infrastructure de RTE pour les accès externes de données) et un équipement du Partenaire.

RTE ne peut pas garantir l'acheminement de la connexion et des données sur le réseau du partenaire ou sur le réseau Internet. On notera que la technique utilisée pour les échanges, permet, parce qu'elle se base sur l'établissement d'une connexion entre les deux SI, de détecter immédiatement l'impossibilité d'un échange quelle qu'en soit la cause. L'émetteur peut ainsi à ce moment décider de toute mesure qu'il juge nécessaire.

Remarque : Une haute disponibilité est mise en œuvre dans le SI de RTE qui s'applique à l'accès au réseau Internet et à l'équipement réalisant les échanges.

# 3. Réception par RTE d'un fichier transmis par le Partenaire

RTE dispose d'un module pour recevoir un fichier envoyé par un Partenaire au moyen du protocole https. Le fonctionnement de ce module est le suivant :

- L'établissement de la connexion https nécessite que le Partenaire s'authentifie à l'aide d'un certificat délivré par RTE (voir § 6 pour l'obtention d'un tel certificat).
- Le fichier est joint à une requête http « POST multipart ». Le terme « fichier » signifie ici un document électronique dont la matérialisation en un fichier à l'émission ou la réception n'est pas une nécessité. Le principe et un exemple de requête http POST multipart sont donnés en § 5.
- Si le fichier est bien réceptionné par le module, celui-ci retourne un ART (Accusé de Réception Technique) formé d'une réponse http dont le corps est vide et dont

le code retour est 200[1]. Le contenu du fichier joint n'est ni vérifié ni validé au moment de la réponse.

Le module répond avec un code différent de 200 pour indiquer que le fichier n'a pu été reçu par RTE. Diverses causes sont possibles :

- Mauvaise formation de la requête http reçue,
- Authentification incorrecte (certificat non reconnu ou invalide),
- Partenaire non autorisé (habilitation),
- URL incorrecte,
- Erreur interne, indisponibilité du service.

RTE indique au Partenaire lors de la mise en œuvre d'un échange l'URL précis qui lui permettra d'envoyer des fichiers.

# 4. Envoi par RTE d'un fichier vers le Partenaire

RTE dispose d'un module pour envoyer un fichier vers un Partenaire au moyen du protocole https. Le fonctionnement de ce module est le suivant :

1) L'établissement d'une connexion https est demandée par le module RTE vers l'URL indiquée par le Partenaire.
2) Un équipement frontal du Partenaire doit pouvoir établir la connexion https en sollicitant l'authentification du demandeur de la connexion (c.-à-d. le module RTE) avec l'une des deux techniques suivantes (*à définir lors de la mise en œuvre de l'échange*) :
   a. Authentification par utilisation d'un certificat logiciel X509 délivré par le Partenaire à RTE.
   b. « Basic Authentication », c'est-à-dire un couple login/mot de passe délivré par le Partenaire à RTE.
3) Le module RTE authentifie le certificat serveur présenté par l'équipement frontal du Partenaire. Pour cela il doit identifier et faire confiance à l'autorité de certification du Partenaire. La chaîne complète de certification doit donc être fournie à RTE pour la mise en œuvre.
4) Le module RTE transmet le fichier via une requête http « POST multipart » et attend un ART (Accusé de Réception Technique), c'est-à-dire un code retour 200 pour signifier que le fichier a bien été reçu, ou un code différent sinon. L'équipement frontal du Partenaire doit pouvoir réceptionner le fichier et transmettre cet ART. Le principe et un exemple de requête http « POST multipart » sont donnés en § 5.

[1] La signification usuelle du code retour 200 en http est « Requête traitée avec succès ».

# 5. Requête « http POST Multipart »

## 5.1 Définition

L'utilisation de la requête « POST multipart » permet à un logiciel client d'envoyer un fichier en http vers un serveur web.

Elle s'appuie sur le transfert dans le corps de la requête http (comprenant plusieurs parties), des champs éventuels d'un formulaire suivi du fichier.

Ce mode d'échanges de fichier est défini dans les documents RFC 2616 et RFC 1867 de l'IETF, et il est utilisé communément lors de l'upload de fichier à l'aide de formulaires HTML (voir un exemple en § 5.3).

## 5.2 Exemple de requête

Dans l'exemple qui suit, le fichier envoyé se nomme « **test001.txt** ». Il contient la chaîne de caractères : « test 123456789 »

**Établissement de la connexion**
https://domain.com/myserver/upload/appli/

**Requête http POST multipart**
*POST /myserver/upload/appli HTTP/1.1*
*Host: - Domain.com*
*Accept: text/html,application*
*Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3*
*Content-Type: multipart/form-data; boundary=**----------265001916915724***
*Content-Length: 213*
***----------265001916915724***
*Content-Disposition: form-data; name="monFichier"; filename="**test001.txt**"*
*Content-Type: text/plain*

***test 123456789***
***----------265001916915724**--*

**Réponse ok du serveur**
*HTTP/1.1 200 OK*

Remarque :

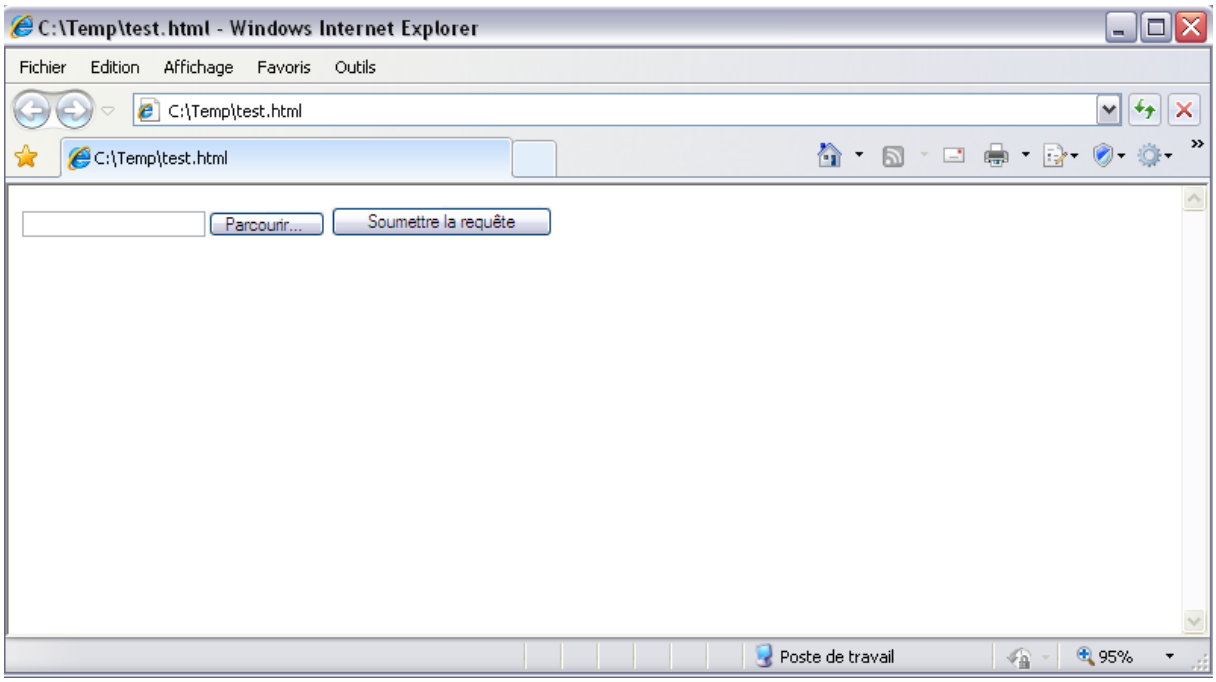
- RTE n'impose aucune contrainte sur les entêtes de la requête http.
- Le nom du paramètre définissant la partie (de la requête http POST multipart) contenant le fichier est libre. Dans l'exemple précédemment donné, le nom choisi est « monFichier ».

## 5.3 Formulaire de test

On peut facilement générer une telle requête http et tester le fonctionnement d'un serveur en utilisant un formulaire HTML simple dont le code est le suivant :

```
<html>
   <body>
      <form name="monFormulaire" method="post" action="
https://domain.com/myserver/appli " enctype="multipart/form-data">
         <input name="monFichier" type="file"/>
         <input type="submit"/>
      </form>
   </body>
</html>
```

Son exécution avec un navigateur (ici Internet Explorer) engendre un écran équivalent au suivant :




Le choix d'un fichier (*Parcourir*) suivi de son envoi (*Soumettre la requête*) entraine l'exécution de toutes les étapes décrites en § 4, dès lors qu'un serveur répond à l'url https://domain.com/myserver/upload/appli/. La vérification de l'authentification du domaine distant et la demande d'authentification de l'utilisateur sont ici prises en charge par le navigateur lui-même.

Le fichier est ensuite transmis au serveur à l'aide d'une requête http « POST multipart ». Le code 200 de retour avec un corps vide entraînera l'apparition d'une page blanche.

### 5.4 Exemple en cURL

Voir en annexe.

## 6. Certificats nécessaires pour l'authentification mutuelle lors d'un envoi du Partenaire à RTE

### 6.1 Caractéristiques nécessaires du logiciel client utilisé par le Partenaire

Le Partenaire doit accéder au SI de RTE avec un logiciel client qui permet l'établissement d'une connexion chiffrée (protocole HTTPS) avec un serveur, et qui permet une authentification mutuelle entre le client et le serveur. Pour cela, ce logiciel doit remplir les conditions suivantes :

- Activer et gérer le protocole SSLv3 ou TLS.
- Pouvoir s'authentifier auprès du serveur RTE avec un certificat logiciel délivré par RTE.

La demande et le retrait d'un tel certificat logiciel X509, délivré par l'Autorité de Certification RTE, sont décrits dans la suite.

### 6.2 Authentification du Partenaire par RTE à l'aide d'un certificat client émis par RTE

Demande à RTE d'un certificat logiciel client

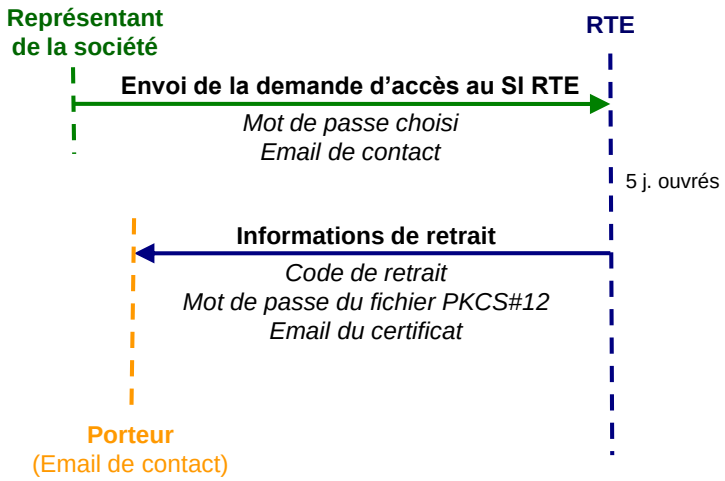
Le Partenaire fait une demande d'accès aux services SI de RTE auprès du chef de projet RTE qui lui fournira un formulaire permettant le retrait d'un certificat logiciel dit « client » qui doit être installé avec le logiciel ou le poste de travail en charge de l'établissement de la connexion chiffrée avec le SI de RTE.

Retrait du certificat logiciel client émis par RTE

Suite à la réception du formulaire, RTE procède à l'enregistrement et la validation de la demande de certificat. Un e-mail de notification intitulé « Accès aux services SI de RTE » est envoyé à l'adresse « E-mail de contact » renseignée dans le formulaire de demande d'accès aux services SI de RTE. Cette adresse est celle de la personne physique, nommé « Porteur du certificat » qui sera responsable de la conservation et de l'utilisation du certificat.

Le Partenaire réalise le retrait avec le « mot de passe choisi » indiqué à RTE dans le formulaire de demande d'accès aux services SI de RTE, et avec les informations complémentaires indiquées dans l'e-mail de notification.

Pour réaliser le retrait le Porteur du certificat se connecte, depuis un poste informatique ayant un accès Internet et un navigateur installé[2], sur le site Web de retrait de certificats logiciels dont l'url est indiquée dans l'e-mail de notification. Il télécharge le certificat sous la forme d'une bi-clé (certificat privée et public) sous forme d'un fichier PKCS#12, c'est-à-dire dont l'extension est « .p12 ».




Pour plus de détails sur le retrait, l'installation et l'utilisation du certificat logiciel, un manuel utilisateur est disponible à l'adresse suivante :

http://clients.rte-france.com/lang/fr/visiteurs/accueil/portail.jsp

Remarques :

- Le temps de demande, de délivrance et d'intégration du certificat chez le Partenaire est estimé à environ trois semaines à compter de la date de demande dans le cadre de la production.

- Le certificat client logiciel est valide 3 ans et la taille de sa clé est de 2048 bits. Quarante jours avant l'expiration du certificat, un courriel est envoyé à l'e-mail de contact pour informer le Porteur du certificat de l'expiration prochaine de son certificat. Il est donc nécessaire et important d'informer RTE en cas de changement du Porteur du certificat et de l'email de contact pour éviter une interruption technique des échanges qui se produira en cas de dépassement de l'échéance.

- Le certificat logiciel client X509, délivré par l'autorité de certification RTE, doit être présenté par le logiciel client qui établit la connexion https avec le SI de RTE. Il permet d'authentifier le Partenaire auprès de RTE. Lors de cette phase, le module RTE de réception vérifie que le certificat est émis par l'autorité de certification RTE, vérifie qu'il est valide et qu'il n'a pas été révoqué.

[2] Pour se connecter à l'interface de retrait, RTE recommande au client d'utiliser les versions de navigateurs supportées par le RTE (cf. Annexe SI Générale § 8.)

## 6.3 Authentification du serveur RTE par le Partenaire

Le certificat présenté par le serveur de RTE lors qu'il reçoit une demande d'établissement d'une connexion https est un certificat délivré par Verisign valide 3 ans à partir de sa date d'émission.

Acceptation du certificat présenté par le serveur RTE

Le logiciel client du Partenaire doit être configuré pour accepter le certificat présenté par le serveur RTE. Les solutions possibles sont les suivantes :

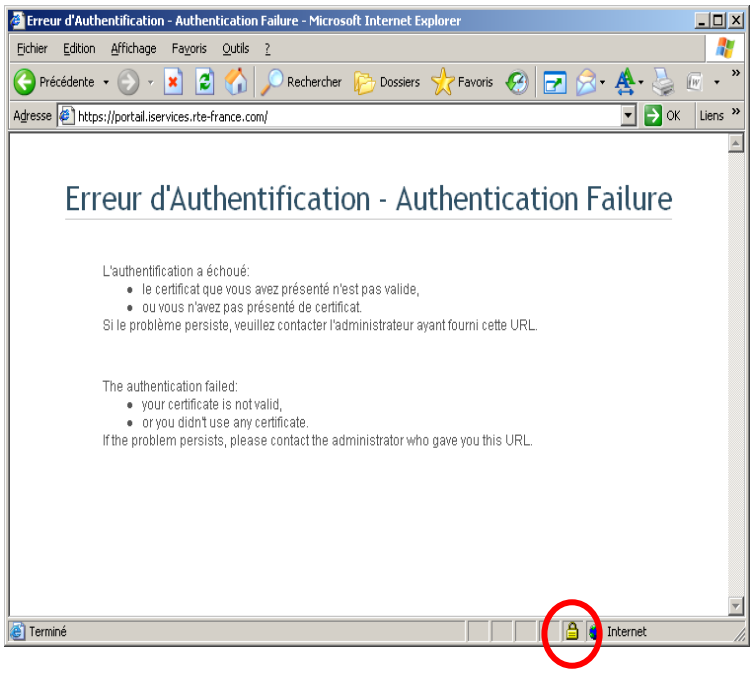
| | Solution | Avantage | Principe |
|---|---|---|---|
| **A** | Aucune | Simple. | Le partenaire n'authentifie pas le serveur RTE. Ce fonctionnement présente un risque de sécurité (phishing). |
| **B** | Vérification et confiance en le « certificat serveur RTE » | Le partenaire authentifie le serveur de RTE. | Configuration : Le Partenaire configure son logiciel avec le « certificat serveur » de RTE.<br>Fonctionnement : Le logiciel du Partenaire reconnaît que le certificat présenté par le serveur auquel il se connecte est bien celui dont il dispose par configuration.<br>Inconvénient : Lors du renouvellement du certificat du serveur RTE, le partenaire doit configurer son logiciel avec le nouveau certificat. Pour éviter une interruption de service, cette opération doit être réalisée le jour même du changement de certificat par RTE.<br>A noter : RTE anticipe toujours de quelques semaines le changement du certificat. Le Partenaire doit donc se rapprocher de RTE pour connaître la date de mise en place du nouveau certificat. |
| **C** | Vérification du certificat serveur de RTE et confiance en l'un des certificats de la chaine. | Le partenaire authentifie le serveur de RTE.<br>Pas de geste lors du renouvellement du certificat du serveur RTE (si la chaine de certification ne change pas). | Configuration : Le Partenaire configure son logiciel avec un des certificats de la chaine de certification du serveur de RTE.<br>Fonctionnement : Le Partenaire vérifie la chaine de certification présentée par le serveur RTE, c'est-à-dire que la liste ordonnée est correctement signée et que l'un des certificats de cette chaine est celui configuré. Le logiciel Partenaire vérifie que le 1er certificat de la liste a été délivré pour l'URL appelée.<br>A noter : Les certificats intermédiaires ou racine ont également des dates limites, mais leurs durées de validité sont beaucoup plus longues. |

RTE recommande la solution « C » *(c'est la vérification réalisée par les navigateurs internet).*

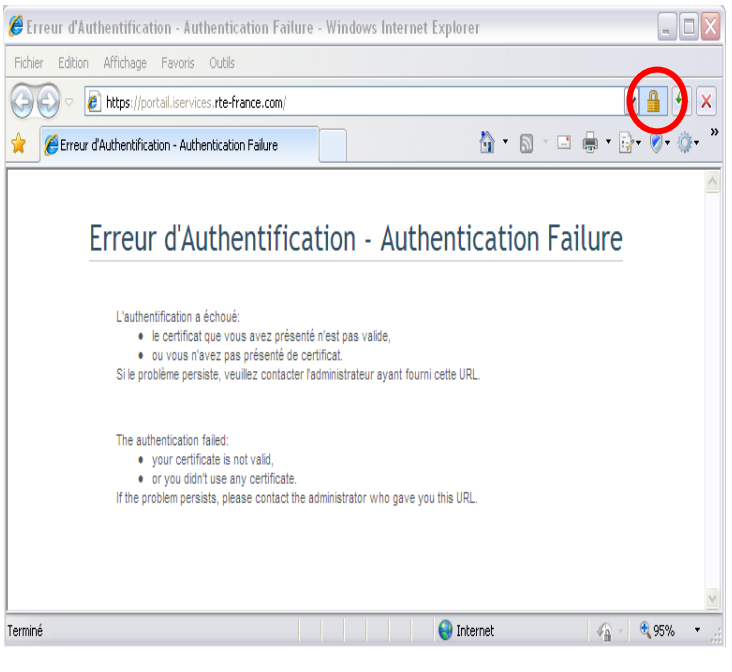
Obtention de la chaine de certification du serveur RTE

La chaine de certification, c'est-à-dire l'ensemble des certificats depuis le certificat RTE jusqu'au certificat racine Verisign, peut être récupérée par le Partenaire comme suit :

- Se connecter à l'adresse https://portail.iservices.rte-france.com. Une authentification est demandée : faire **Annuler**. Avec Internet Explorer, un clic sur le cadenas en bas à droite de l'écran ou en face de l'adresse permet alors de consulter, d'installer dans le navigateur puis d'exporter les différents certificats de la chaîne de certification utilisée par RTE.




**Obtention de la chanine de certification avec Internet Explorer 6**




**Obtention de la chanine de certification avec Internet Explorer 8**

# 7. Certificats nécessaires pour l'authentification mutuelle lors d'un envoi de RTE au Partenaire

Dans le cas où le module d'émission de RTE doit s'authentifier auprès du SI du Partenaire avec un certificat logiciel que lui-même délivre, il indiquera à RTE la procédure de demande et de retrait ainsi que les délais de mise à disposition.

# 8. Gestion des erreurs, Moyens de diagnostic et Traçabilité des échanges

Lors de la mise en œuvre des échanges et en cas d'incident, chaque partie doit disposer des moyens permettant le diagnostic rapide et l'analyse d'un incident.

Notamment l'absence de code retour ou un code retour erroné suite à l'envoi d'un fichier est un événement qui doit être traité, remonté et visualisable par une supervision applicative, pour identifier rapidement un incident (ex : problème de télécommunication sur Internet) et décider des mesures nécessaires qui s'ensuivent.

S'il existe dans son SI des équipements intermédiaires entre les modules d'émission et de réception (ex : pare-feu, proxy, reverse-proxy), le Partenaire doit s'assurer d'une traçabilité des échanges, permettant d'analyser et vérifier les requêtes sortantes de son SI, et les requêtes reçues à l'entrée de son SI.

RTE est capable d'analyser toute réception de données du Partenaire, ou toute requête émise par le SI de RTE sur une période de 7 jours en cas d'incident majeur.

# 9. Annexe : exemple cURL

L'exemple qui suit est donné à titre indicatif. Les scripts, progiciels, ou développements ad hoc réalisés pour échanger des données doivent être mis en œuvre par les personnes compétentes. RTE n'apporte pas de support pour la mise en œuvre de cet exemple.

cURL (Client URL Request Library) est une interface en ligne de commande qui permet l'accès à des ressources localisées par des URL — voir http://curl.haxx.se.

La ligne de code de commande cURL ci-après réalise l'envoi d'un fichier vers un serveur cible désigné par une URL.

*curl.exe --cacert IntCA.cer --cert userCert.pem --form upload=@test001.txt https://domain.com/myserver/upload/appli/Appli1*

- « IntCA.cer » est le fichier qui contient le certificat racine de l'Autorité de Certification qui a émis le certificat du serveur cible. Il permet d'authentifier le serveur cible.
- « test001.txt » est le fichier à transmettre.
- « https://domain.com/myserver/upload/appli/Appli1 » est l'URL du serveur cible.
- « userCert.pem » est le fichier qui contient le certificat-client (la clé privée) qui permet à l'émetteur de s'authentifier auprès du serveur cible.
- Remarques :
  - ✓ Dans cet exemple le programme cURL et les fichiers référencés sont tous placés dans le répertoire courant d'où est lancée la commande.
  - ✓ Le logiciel « openssl » (http://www.openssl.org) permet de transformer des fichiers contenant des certificats en des fichiers au format « .cer » ou « .pem ».

**FIN DU DOCUMENT**