

Gestionnaire du Réseau de Transport d'Electricit

Access to RTE's IT system with digital certificates under Microsoft Windows XP

PKI User Manual

Version3, 4/11/2008

This document is the property of RTE. All communication, reproduction or publication, even partial, is prohibited without authorisation in writing from RTE.

www.rte-france.com



CONTENTS

1. Intro	duction	5
1.1	Document subject	5
1.2	Context	5
1.3	A warning concerning security procedures	5
1.4	The stakeholders	6
1.4.′	1 The customer	6
1.4.2	2 The Registration Authority (RA)	6
1.4.3	3 The Certification Authority (CA)	7
1.5	The certificate management process	7
1.5.1	I Issuance of a certificate	7
1.5.2	2 Renewal of a certificate	7
1.5.3	3 Revocation of a certificate	7
2. Insta	allation and configuration of the workstation	8
2.1	Network configuration	8
2.2	Software configuration	8
3. Inter	net Explorer 6	10
3.1	Configuration for SSL/TS protocols	10
3.2	Request for a digital certificate	11
3.2.1	Preliminary measures	11
3.2.2	2 Overall schematic	11
3.3	Installation of the RTE CA root certificate	12
3.3.1	1 Download and installation	12
3.3.2	2 Verification of the root certificate fingerprint	16
3.3.3	3 Contents of the RTE CA certificate	16
3.4	Downloading your certificate	17
3.4.1	1 Generation of the key pair	19
3.4.2	2 Installation of the certificate	20
3.4.3	3 Contents and verification of your digital certificate	20
3.5	Usage in your browser	22
3.5.1	Authentication and encryption	22
3.5.2	2 Example of accessing the "RTE Customer Services Portal"	22
4. Inter	net Explorer 7	24
4.1	Configuration for SSL/TS protocols	24
4.2	Request for a digital certificate	25



4	4.2.1	Preliminary measures	25
	4.2.2	Overall schematic	25
4.3	3 I	nstallation of the RTE CA root certificate	26
	4.3.1	Download and installation	26
4	4.3.2	Verification of the root certificate fingerprint	30
4	4.3.3	Contents of the RTE CA certificate	30
4.4	1 C	Downloading your certificate	31
4	4.4.1	Generation of the key pair	33
	4.4.2	Installation of the certificate	34
4	4.4.3	Contents and verification of your digital certificate	35
4.5	5 L	Jsage in your browser	37
4	4.5.1	Authentication and encryption	37
4	4.5.2	Example of accessing the "RTE Customer Services Portal"	37
5. I	Mozill	la Firefox	39
5.1	I (Configuration for SSL/TS protocols	
5.2	2 F	Request for a digital certificate	
!	5.2.1	Preliminary measures	
!	5.2.2	Overall schematic	40
5.3	3 I	nstallation of the RTE CA root certificate	40
!	5.3.1	Download and installation	40
!	5.3.2	Verification of the root certificate fingerprint	41
5.4	1 C	Downloading your certificate	43
!	5.4.1	Generation of the key pair	45
!	5.4.2	Installation of the certificate	45
!	5.4.3	Viewing and verification of your digital certificate	46
5.5	5 L	Jsage in your browser	48
!	5.5.1	Authentication and encryption	48
!	5.5.2	Example of accessing the "RTE Customer Services Portal"	48
6.	Certifi	icates and email software	50
6.1	I C	Dutlook 2000/XP/2003	50
(6.1.1	Configuration	50
(6.1.2	User Guide	54
6.2	2 (Outlook Express	58
(6.2.1	Configuration	58
(6.2.2	User Guide	61
6.3	3 N	Mozilla Thunderbird	63
(6.3.1	Configuration	63
(6.3.2	User Guide	64
6.4	1 L	_otus Notes	66



7.	SSL	. VPN	۷	67
7	.1	Fore	eword	67
7	.2	Initia	al configuration	67
	7.2.	1	Prerequisites	67
	7.2.	2	First connection	68
7	.3	Use	r Guide	72
	7.3.	1	Establishing a connection	72
	7.3.	2	Using SSL VPN to access hosted email folders	75
8.	Ren	ewal	of certificates	76
9.	Rev	ocati	on of certificates	77
9	.1	The	revocation scenario	77
9	.2	The	revocation request	77
10.	Inci	dent	handling and support	78
1	0.1	Erro	or codes returned by email	78
1	0.2	Sup	port	79
11.	Арр	endix	x A – Importing and exporting certificates	80
1	1.1	Ехр	orting a certificate under Mozilla Firefox	80
1	1.2	Ехр	orting a certificate under Internet Explorer (Windows)	83
1	1.3	Imp	orting a certificate into Mozilla Firefox	85
1	1.4	Imp	orting a certificate into Internet Explorer (Windows)	
1	1.5	Imp	orting a certificate into Mozilla Thunderbird	91
12.	Арр	endi	x B – (PKI) secured environment	95
1	2.1	Cor	cepts and objects generated by a PKI	
	12.1	1.1	What is a secured process?	95
	12.1	.2	The role of the key pair	96
	12.1	1.3	The certificates	
1	2.2	Doc	sumentation	
13.	Арр	endix	x C – Glossary	



1. Introduction

1.1 Document subject

This document is intended for the end user who wishes to access the RTE's IT system with digital certificates.

This current document allows certificate holders to:

- know how to install and use their digital certificates in the following environments:
 - Windows XP,
 - Browsers: Mozilla Firefox and Internet Explorer for secure access using the HTTPS protocol,
 - Email clients: Mozilla Thunderbird, Outlook 2000/XP/2003 and Outlook Express for secure communications in the S/MIME format,
 - Lotus Notes: please refer to the following reference document "PKI User Manual - digital certificates - Windows XP Notes";
- understand the context and the principles of a secured environment, as well as the general operation of a public key infrastructure (IGC, or PKI in English).

NOTE

Throughout this document, the pronoun "you" is used to reference the certificate holder. References to he/him/his/himself are for brevity and are also implied to refer to she/her/herself wherever they occur.

1.2 Context

In the context of the February 10th 2000 legislation (2000-108) and the implementing decree 2001-630 of July 16th 2001, the administrator of a public transport network has an obligation to protect the confidentiality of all information of economic, commercial, industrial, financial or technical natures whose communication might adversely impact the rules of free and fair competition and non-discrimination as defined by the law.

1.3 A warning concerning security procedures

Each holder of a digital certificate uses a cryptographic module to maintain their own securely-generated private key on the hard drive of their workstation. Therefore, every digital certificate holder must take the necessary precautions to prevent:

- the breach of their private key;
- the loss of their private key;



RTE

- the disclosure of their private key;
- the modification of their certificate;
- and any abusive use of their certificate.

Every certificate holder has, and recognises having, complete responsibility for the protection of their private key(s). The private keys and their associated certificates are stored on the hard disk, hence their being known as "digital" certificates; these private digital keys can be protected by a password only known by the certificate holder.

The Certification Authority (CA) of "RTE France" declines all responsibility relating to litigation arising or associated with inappropriate use of these private keys.

Please refer to:

• chapter 2 of the *Certification Policy of the RTE France CA*, which is found in the package that has been supplied to the company manager:

<PACKAGE>:\RTE Installation\fr\Politique de Certification RTE.pdf

the IT System access regulations.

<PACKAGE>:\Sécurité - Charte d'utilisation des certificats logiciels.pdf

1.4 The stakeholders

Certificate lifecycle management revolves around three entities:

- the customer (*i.e.* your company);
- The Registration Authority (RA);
- The Certification Authority (CA).

NOTE

To make things easier to understand, an analogy can be made with the allocation of official identity documents: a citizen requesting an identity document corresponds to the customer entity, the municipality acts as the registration authority, and the central Internal Affairs department as the certification authority.

1.4.1 The customer

The customer makes certificate requests on behalf of the certificate holders. The customer can similarly issue requests for revocation of its certificates.

1.4.2 The Registration Authority (RA)

The Registration Authority (the RTE customer relations officer for the Operator's team) receives a certificate request and verifies the identity of the certificate holders who will be using the certificates.



1.4.3 The Certification Authority (CA)

The (RTE) Certification Authority is responsible for and vouches for the certificates signed in its name and for the smooth operation of the PKI. It defines its own policies for the administration and usage of its certificates.

The RTE certification authority is defined as:

CN = RTE Autorite de Certification, O = RESEAU DE TRANSPORT D ELECTRICITE

1.5 The certificate management process

The principle processes implemented to manage the combined collection of digital certificates delivered to certificate holders are as follows:

- the issuance of a certificate (issuance of one or more certificates),
- the renewal of a certificate (replacing someone's certificate with a new one for a new validity period and for a new key pair,
- the revocation of a certificate.

The RTE's certification policy is available on the RTE corporate internet site.

1.5.1 Issuance of a certificate

Certificates are issued in compliance with the RTE Certification Policies upon the initiative of the representative of the company for contractual relationships with RTE.

The requests are issued by the customer through its RTE customer relations officer, who forwards them to the appropriate groups to register the certificate holder. Then the certificate holder himself registers on the site assigned for digital certificates. After that, the browser generates a key pair on the certificate holder's workstation and downloads the associated certificate.

1.5.2 Renewal of a certificate

Forty days before the expiry of a certificate, an electronic message is sent to the certificate holder to inform him of the renewal of his digital certificate.

If modifications need to be made relating to the certificate holder's details, then the certificate holder's representative contacts the RTE customer relations officer to tell him what those changes are.

Otherwise an email is sent to the certificate holder with the information necessary for the retrieval of his new certificate.

1.5.3 Revocation of a certificate

For scenarios involving a change of the certificate holder, loss or a compromised certificate, the customer directly contacts the RTE Hotline (see §10.2) to request the revocation of that certificate. The customer will be notified of the revocation of that certificate. The revocation request may originate from RTE itself in the event of fraud.



2. Installation and configuration of the workstation

All operations in this chapter are to be performed just once by computer staff with Administrative privileges over your workstation when you receive your RTE applications access kit.

In addition, note that **only a few chapters of this manual are of interest to the certificate holder:** those being the chapters relating to digital certificates.

2.1 Network configuration

Electronic messages (emails) passing between RTE and the certificate holder will be transported over the Internet (SMTP protocol, S/MIME format).

Access with web a browser employs – quite transparently to the certificate holder – an access authentication system for the RTE portal and encryption of data communicated over the Internet (HTTPS protocol).

IMPORTANT NOTE

The messaging and antivirus routers, firewalls and content analysers must be configured to not alter or refuse encrypted and signed messages in S/MIME format (application/x-pkcs7-mime, .p7s, .p7m), nor to block HTTP data traffic (port 443).

The network administrator can be consulted to perform these operations

2.2 Software configuration

The software configuration required for your workstation is as follows:

Operating systems:

• Windows XP,

Web browsers:

- Mozilla Firefox 1.5 or later,
- Internet Explorer 6.0 or later,

Email software:

- Mozilla Thunderbird 1.5 or later,
- Outlook 2000, XP and 2003,
- Outlook Express 6.0 or later,
- Lotus Notes 5 or later.

NOTE

Generally speaking, reading messages over a webmail type interface does not permit messages to be signed.

Microsoft software updates for 128-bit encryption



If you are not aware what these updates consist of, please contact your Windows system administrator so that he can perform the necessary tasks. Listed below are the web addresses for these updates as well as the path locations for them in the package supplied by RTE.

Outlook 2000:

Office 2000 Update: Service Pack 3 (optional)

<PACKAGE>\Windows Updates\Outlook 2000\Service Pack 3 (SP3)\

Office 2000 FR

<PACKAGE>\Windows Updates\Outlook 2000\frenchconfiguration.reg

IMPORTANT

In order to retrieve your software certificate, you will need administration rights on your workstation.

During the retrieval of your certificate under Internet Explorer, two ActiveX controls are downloaded to your workstation, one from the "ConfigChkr" class (which verifies the cryptographic configuration of the browser) and "Cenroll" for the download itself. The network administrator must make sure that these ActiveX controls will not be blocked by network security measures.

In addition, Internet Explorer must be configured to accept the download and execution of signed ActiveX controls: Open the menu item "Tools > Internet options...", the "Security" tab, and click on the "Personalise the level... " button:

 Connexion automatique uniquement dans la zone int Demander le nom d'utilisateur et le mot de passe Ouverture de session anonyme Contrôles ActiveX et plugins Contrôles ActiveX reconnus sûrs pour l'écriture de scripts Activer Demander Désactiver Contrôles d'initialisation et de script ActiveX non marqués Activer Demander Desactiver Exécuter les contrôles ActiveX et les plugins Activer Rétablir les paramètres personnalisés 	Exécuter les contrôles ActiveX et les plugins Activer Approuvé par l'administrateur Demander Désactiver Télécharger les contrôles ActiveX non signés Activer Demander Désactiver Télécharger les contrôles ActiveX signés Activer Télécharger les contrôles ActiveX signés Activer Demander Désactiver Télécharger les contrôles ActiveX signés Activer Demander Désactiver Félécharger les contrôles ActiveX signés Activer Félécharger les contrôles ActiveX signés Activer Perander Désactiver Télécharger les personnalisés
<u>R</u> établir : Moyen 💌 Réta <u>b</u> lir	Rétablir : Moyen 💌 Réta <u>b</u> lir



3. Internet Explorer 6

3.1 Configuration for SSL/TS protocols

In the browser, select the "Tools > Internet options..." menu item:



🚰 about:blank - Microsoft Internet Ex	plorer	
Fichier Edition Affichage Favoris	Outils ?	
🛛 🕞 Précédente 👻 📀 👻 💈	Courrier et News Synchroniser	ers 🥎 Favoris 🧭 🂙
Adresse about:blank	Afficher les liens apparentés Console Java (Sun)	🔽 🔁 ок
	Rétablir les paramètres Web	
	Options Internet	
	И	•
Permet de modifier les paramètres.		li.

Select the "Advanced" tab:

Options Internet		
Général Sécurité Confidentialité Contenu Connexions Programmes Avancé		
Para <u>m</u> ètres :		
Securité Activer l'Assistant Profil		
 Activer l'authentification intégrée de Windows (nécessite un redémai Avertir en cas de changement entre mode sécurisé et non sécurisé Avertir pour les sites dont les certificats sont non valides 		
Avenus sites formulaines sources sources and the disque Ne pas enregistrer les pages cryptées sur le disque SSL 2.0 SSL 3.0		
 TLS 1.0 Vérifie les signatures des programmes téléchargés Vérifier la révocation des certificats (redémarrage nécessaire) Vérifier la révocation des certificats de l'éditeur 		
Vider le dossier Temporary Internet Files lorsque le navigateur est fer		
<u>Paramètres par défaut</u>		
OK Annuler Appliquer		

In the section labelled "**Security**", makes sure that checkboxes for SSL 2.0, SSL 3.0 and TLS 1.0 have been checked, as shown above.





3.2 Request for a digital certificate

3.2.1 Preliminary measures

The following steps must have been completed in advance:

• The company representative has made an access request:

The company representative must have filled out and signed the "RTE IT System and Applications Access Request Forms"; and must have sent them to the RTE customer relations officer:

• We have registered your request:

Upon reception of those forms, we will have created your application access account(s).

3.2.2 Overall schematic

Once the certificate request has been registered and validated by our services (within 5 working days), a message will be sent to the company representative to acknowledge receipt of the forms and asking him to call us to fix a phone meeting with the certificate holder for the day of the certificate installation.

Then, a message will be sent to the certificate holder after this call, reminding him of the scheduled meeting and giving him the address of the download web site and the retrieval code which will allow him to download his certificate from his own workstation.



The certificate holder must then connect to the digital certificate administration web site from his workstation to fill out and validate the registration form online. At that moment, a key pair will be generated on his workstation and his certificate will be downloaded.



3.3 Installation of the RTE CA root certificate

3.3.1 Download and installation

The RTE root certificate must now be installed in your browser so that RTE is known as the trusted Certification Authority.

To do this, please navigate to the RTE customer site at the following address:

http://rte.certplus.com/default.htm

The following page will be displayed.

Portail des porteurs RTE - Microsoft Internet Explorer	
Eichier Edition Affichage Favoris Qutils 2	A
🕒 🔆 Précédente 🔹 🕥 🗴 📓 🐔 🔎 Rechercher 📂 Dossiers	🔆 Favoris 🚱 🖃 🗟 • 🏝 🥌 🐨 • 🔏 📋 🚺
Adresse 🖉 http://rte.certplus.com/default.htm	Э ок
RTE du Réseau de Transport d Electricité	
Certificats logiciels	Cartes et tokens USB
<u>Retrait de certificat</u>	Acquittement de support
Retrait par CSR	
Test de certificat	Test de support
Révocation de certificat	Révocation de support
Recherche	Recherche
Autorité de Certification Installer le certificat racine de RTE	_
ê	Internet

Click on the link "Installer le certificat racine de RTE / Install the RTE root certificate"

The RTE CA root certificate will then be installed in the Windows certificate store, as per the process described below.



Téléchar	gement de fichier 🛛 🗙
?	Certains fichiers peuvent endommager votre ordinateur. Si les informations sur le fichier ci-dessous semblent suspectes, n'ouvrez ou n'enregistrez pas ce fichier.
	Nom du fichier : getcertif.p7b
	Type du fichier : Certificats PKCS #7
	De : rte.certplus.com
	Voulez vous ouvrir la fichier ou l'enregister aur votre preimeteur 2
	Voulez-vous ouvrir le richier ou renregistrer sur votre ordinateur ?
	Ouvrir Enregistrer Annuler Informations
	☑ Ioujours demander avant d'ouvrir ce type de fichier

Click on the "Open" button.

🚟 Certificats			
Eichier <u>A</u> ction Aff <u>i</u> chage <u>?</u>			
← → € 🖬 🖻 🗟 🔮			
🗐 Certificats - Utilisateur actuel	Délivré à 🔺	Délivré par	Date d'expiration
⊡ C:\CERTIF~1\GETCER~1.P7B	RTE Autorite de Certification	RTE Autorite de	29/05/2012
I Le magasin C:\CERTIF~1\GETCER~1.P7E	Contient 1 certificat.		

Double-click on "**RTE Autorite de Certification (RTE Certification Authority)**".



Certi	ificat		<u>? ×</u>		
Gé	Général Détails Chemin d'accès de certification				
			_		
	Informations	sur le certificat			
	Ce certificat est conç	u pour les rôles suivants :	_		
	 Toutes les stratégies d' Toutes les stratégies d' 	émissions application			
	·····				
	Délivré à :	RTE Autorite de Certification			
	Délivré par :	RTE Autorite de Certification			
	Valide à partir de	u 29/05/2002 j usqu'au 29/05/2012			
	Installe	r le <u>certificat</u> <u>D</u> éclaration de l'émetteu	<i>r</i>		
			ок		

Click on the "Install the certificate" button.

Assistant Importation de certi	ificat	×
	Bienvenue ! Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation de certificats depuis votre disque vers un magasin de certificats. 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. Pour continuer, cliquez sur Suivant.	
	< Précédent Suivant > Annuler	



Assistant Importation de certificat	×
Magasin de certificats	
Les magasins de certificats sont des zones système où les	certificats sont stockés.
Windows peut sélectionner automatiquement un magasin o spécifier l'emplacement du certificat.	de certificats, ou vous pouvez
Sélectionner automatiquement le magasin de certifie	cats selon le type de certificat
C Placer tous les certificats dans le magasin suivant	
Magasin de certificats :	
	Parc <u>o</u> urir
< <u>P</u> récédent	Suivant > Annuler

Leave the selected default option as it is and click on "Next".

Assistant Importation de certificat	×
Fin de l'Assista certificat Vous avez terminé correct	nt Importation de
Certificat. Vous avez spécifié les par Magasin de certificats se Contenu	amètres suivants : ślectionné Déterminé automatiq. Certificat
< Précéde	nt Terminer Annuler

Click on "**Finish**", and the following window then displays the contents of the root certificate to be imported.

Magasin	de certificats principal 🔀				
⚠	Voulez-vous ajouter le certificat suivant au magasin principal ? Objet : RTE Autorite de Certification, RESEAU DE TRANSPORT D ELECTRICITE				
	Émetteur : auto-émis Limite de validité : de mercredi 29 mai 2002 à mardi 29 mai 2012 Numéro de série : 75230902 54AEC749 818427D3 8CCC21EB Empreinte numérique (sha1) : A29A4FA1 77142C87 FA302DB0 8F2C0237 37C7AE37 Empreinte numérique (md5) : 53426A2E A510AB2A 2109EE88 1367A031				
	<u>Oui</u> <u>N</u> on				





3.3.2 Verification of the root certificate fingerprint

To make sure that you have downloaded the genuine RTE AC root certificate, carefully check that the "SHA1" or "MD5" digital fingerprint displayed in the window shown is **identical** to that shown above.

 The root certificate digital fingerprints for RTE CA are listed here:

 SHA1
 A29A
 4FA1
 7714
 2C87
 FA30
 2DB0
 8F2C
 0237
 37C7
 AE37

 MD5
 53:42:6A:2E:A5:10:AB:2A:21:09:EE:88:13:67:A0:31

If the hash fingerprint is not identical, click on "No" and contact our support services.

If it is identical, click on "Yes" to finish the import.

Assistan	t Importation de certificat	×
(į)	L'importation s'est terminée correct	ement.
	ОК	

Click on "OK".

3.3.3 Contents of the RTE CA certificate

The root certificate that you have just downloaded is stored in the certificate store appropriate to the browser used. For example, it can be viewed in Internet Explorer with:

Menu "Tools > Internet options...", "Contents" tab, "Certificates..." button, "Trusted root authorities" tab:

Certificats	?× (ertificat		<u>? ×</u>
Rôle prévu : <pre><tout></tout></pre>	-	Général Détails Chemin d'accès d	le certification	
Autorités principales de confignee		Contrain a contra		1
Autres personnes Autorites internieulaires Autorites principales de connunce		Afficher : <tout></tout>	•	
Délivré à Délivré par Date d'exp N	lom con 🔺			_
PTT Post Root CA PTT Post Root CA 26/06/2019 K	ieyMail	Champ	Valeur	▲
RTE Autorite de Certification RTE Autorite de Certifi 29/05/2012 «	(Aucun>	E Version	V3	
Saunalahden Serveri CA Saunalahden Serveri CA 26/06/2019 S	iaunala	🖃 Numéro de série	75 23 09 02 54 ae c7 49 81 84	
Saunalahden Serveri CA Saunalahden Serveri CA 26/06/2019 S	iaunala	🖃 Algorithme de signature	sha1RSA	
Secure Server Certificatio Secure Server Certific 08/01/2010	eriSign	Émetteur	RTE Autorite de Certification,	
SecureNet CA Class A SecureNet CA Class A 16/10/2009 S	iecureN	🖃 Valide à partir du	mercredi 29 mai 2002 01:00:00	-
SecureNet CA Class B SecureNet CA Class B 16/10/2009 S	ecureN	E Valide jusqu'au	mardi 29 mai 2012 00:59:59	
SecureMet CA Root SecureMet CA Root 16/10/2010 S	ecureiv	Objet	RTE Autorite de Certification	
			PSA (1024 Bitc)	-1
			KOH (1024 bics)	
Importer Exporter Supprimer	Avancé	CN DTE Autorite de Cautification		- 1
		O = RESEAU DE TRANSPORT D EU	ECTRICITE	
Détails de certificat				
<tout></tout>				
	Affichage			
	Eermer			
			1	- 1
		Modifi <u>e</u> r les propriété	s <u>C</u> opier dans un fichier	
Click on the "Display!" butto	un and			
Click on the "Display"" butto	on, and			
then on the " Details " button				
				OK



3.4 Downloading your certificate

To create your key pair and your certificate, you must then connect, on the RTE meeting day specified, to the following web site:

http://rte.certplus.com/default.htm



Click on the "Retrait de certificat / Retrieve the certificate" button.

It is possible that the following dialogue box might be displayed:



If it does, reply with "**Yes**" to make sure you have the correct encryption mechanism (key size) installed.



Fill out the following form:

🚳 Enregistrement u	tilisateur Microsoft - Microsoft Internet Explorer		
Eichier Edition A	ffichage Fa <u>v</u> oris <u>O</u> utils <u>?</u>		
Précédente 👻	🕥 - 💌 🙋 🏠 🔎 Rechercher 🎼 Doss	siers 👷 Favoris 🚱 🖃 🖂 🛧 😓 📄	X 🗈 🔒
Adresse 🖉 https://rt	e.soft-id.certplus.com/client/userEnrollMS.htm		💌 ラ ок
Informations	pour le certificat numérique		
Remplissez tous sont incluses dan	les champs. N'utilisez que l'alphabet latin, sans ca s votre certificat et seront accessibles à tous.	aractères accentués. Les informations des champs précé	édés d'un "*"
	Nom Complet : * (obligatoire) Ex : DUPONT	Client RTE 2	
	Adresse Email : * (obligatoire) Ex: jean.dupont@societe.com	client.rte@services.rte-france.com	
	Authentifiant PKI: (obligatoire)	•••••	
	Code de retrait : (obligatoire)	ABC123	
	Soumettre	Annuler	-
🙋 Terminé		📄 📄 😫 Intern	et //

The fields marked with an asterisk must be completed **without diacritic marks** (i.e. accents, cedillas, ...) **or punctuation marks**; as they would also appear in the certificate that will be generated.

The **retrieval code** is the code supplied in the 2nd email that you received from us which allows you to authenticate yourself. To make things easier, you can do simple copy-paste commands to enter the data.

You must likewise enter your **Authentifiant Utilisateur PKI (PKI User Credentials)**, just as they were supplied in the RTE IT system access technical specifications; they will serve to authenticate you with the RTE Hotline any time that you contact them.

Lastly, click on "Submit" to send your request for the digital certificate.

A dialogue box will ask you to confirm your email address:

Microsoft	Internet Explorer
2	Confirmez votre adresse e-mail : client.rte@services.rte-france.com
	Si votre adresse e-mail est correcte, cliquez sur OK, sinon sur CANCEL et corrigez là dans le formulaire.
	Si votre adresse e-mail est incorrecte, vous ne pourrez pas utiliser votre Identification numérique
	OK Annuler

Click on the "**OK**" button, or "Cancel" to return to the form data entry screen.



Violation	de script potentielle	\times
<u>.</u>	Ce site Web nécessite in nouveau certificat de votre part. Vous ne devriez autoriser que les sites Web approuvés à demander u certificat de votre part. Voulez-vous demander un certificat maintenant ?	ΠL
	Qui <u>N</u> on	

Click on the "Yes" button.

3.4.1 Generation of the key pair

The dialogue box shown below will then be displayed, indicating that an RSA key pair has been created by Internet Explorer on your workstation:

Création d'une nouvelle clé d'échar	nge RSA 📃 🛃	Création d'une nouvelle	clé d'échange RSA
Une application crée Dié privée CryptoAPI Niveau de sécurité de Moyen	sctuellement un élément protégé.		Choisissez un niveau de sécurité approprié à cet élément.
			< Précédent Suivant > Annuler

Click on the **"Define the security** Select the **"High**" option, then click on **level**" button. **"Next**".

The key pair that will be generated is, by default, at a "**medium security**" level, which means that each later use of this key pair will cause the display of a simple acknowledgement message: the certificate holder is also warned of this usage but no password is requested.

For protected use of your key pair, which we recommend, you should rather choose "**high security**", which will mean that a password, that you will choose here, will be asked of you for every later use of your key pair. The screens below describe the procedure to set this security level.

Création d'une nouvelle	clé d'échange R5A	×	Création d'une	nouvelle clé d'échange R5A 🛛 🔀
<u>a</u> 0,	Créer un mot de passe pour protéger cet élément.			Une application crée actuellement un élément protégé.
	Créer un nouveau mot de passe pour cet élément.			Clé privée CryptaAPI
	Moi de passe pour . The privee cryptica.Pr		A Cal	
	Mot de passe :			Niveau de sécurité défini à Définir le <u>n</u> iveau de sécurité
	Confirmer :			OK Annuler <u>D</u> étails
		1		
		1		

Enter a password, then click on the Click on the "**OK**" button. "**Finish**" button.





Click on the "Yes" button.

3.4.2 Installation of the certificate

🗿 ID Download - Microsoft Internet Explorer	
Eichier Edition Affichage Favoris Outils 2	-
🛛 😋 Précédente 🔹 📀 🗸 😰 🏠 🔎 Rechercher 🌮 Dossiers 🤺 Favoris 🤣 🖃 😞 + 🌉 🕞 👗 💼	<mark>1</mark>
Adresse 🖗 https://rte.soft-id.certplus.com/cgi-bin/sophialite.exe	🔰 ОК
Félicitations !	
Votre certificat numerique a ete telecharge et installe.	
Informations sur votre Certificat numérique	
	* -
Organizational Unit= Soft ID	
Organizational Unit = ISO 6523 - 0000 0000	
Common Name = Client RTE 2 Email Address = client de Meenices de france com	
Numéro de Série = 2c5b4029165afe38928702cb25dd0a09	
Torminá 🗛 🗿 Tokorost	
	11.

Next, the certificate is automatically downloaded and installed in the Internet Explorer certificate store. The page opposite is displayed to indicate the end of this process.

IMPORTANT

Once downloaded, your certificate with its key pair and root certificate must be saved on a removable medium (e.g. a diskette) that you must store securely to prevent unauthorised access. Refer to the appendix for the certificate export procedure.

3.4.3 Contents and verification of your digital certificate

Regardless of the browser used, the contents of the downloaded certificate will obviously be the same, only the presentation of the information on the screen will vary. For downloads with Internet Explorer, open the certificate store with the following menu choices:

"Tools > Internet options...", "Contents" tab, "Certificates..." button:



Page: 21/102

Access to the IT system with digital certificates under Microsoft Windows XP PKI user manual

Certificat <i>s</i>			<u>? ×</u>
Rôle prév <u>u</u> :	<tout></tout>		•
Personnel Autres pe	rsonnes Autorités intermédiai	res Autorités princi	pales de confiance া 🕨
Délivré à	Délivré par	Date d'expiration	Nom convivial
🔛 Client RTE 2	RTE Autorite de Certification	01/11/2007	<aucun></aucun>
Importer	orter <u>S</u> upprimer		<u>A</u> vancé
Détails de certificat —			
<tout></tout>			Affichage
			<u>E</u> ermer

Select your certificate, then click on "Display".

Certificat	? × Certificat	<u>?</u> ×
Général Détails Chemin d'accès de certification	Général Détails Chemin d'accès de certification	1
Informations sur le certificat Ce certificat est conçu pour les rôles suivants : •Toutes les stratégies d'application	Chemin d'accès de certification	
Délivré à : Client RTE 2		1
Delivré par : RTE Autorite de Certification Valide à partir du 31/10/2005 jusqu'au 01/11/2007 P Vous avez une clé privée qui correspond à ce certificat. Déclaration de l'émetteur	Etat <u>d</u> u certificat : Ce certificat est valide.	

date.

It is valid for 2 years from the download This tab allows you to verify your certificate.



RTE



The "valid" status of your certificate, as well as the complete display of the certificate access path (2 levels), shows that your certificate has been correctly installed along with the root certificate, and therefore all the correct usage conditions for your certificate have been satisfied.

Certificat		?× C	ertificat		? ×
Général Détails Chemin d'accès d	le certification		Général Détails Chemin d'accès	de certification	
,					1
Afficher : <tout></tout>	•		Afficher : <a>Tout>	-	
Champ	Valeur		Champ	Valeur	
Version	V3		Version	V3	
Numero de serie	2c 5b 40 29 16 5a fe 38 92 87		Numero de serie	2c 5b 40 29 16 5a fe 38 92 87	
Algorithme de signature	sha1RSA		Algorithme de signature	sha1R5A	
Emetteur	RTE Autorite de Certification,		Emetteur	RTE Autorite de Certification,	
Valide à partir du	lundi 31 octobre 2005 01:00:00		Valide à partir du	lundi 31 octobre 2005 01:00:00	
Valide jusqu'au	jeudi 1 novembre 2007 00:59:59		Valide jusqu'au	jeudi 1 novembre 2007 00:59:59	
Objet	client.rte@services.rte-france		Objet	client.rte@services.rte-france	
Clé publique	RSA (1024 Bits)		Clé publique	RSA (1024 Bits)	
CN = RTE Autorite de Certification O = RESEAU DE TRANSPORT D EL	ECTRICITE		E = client.rte@services.rte-franc CN = Client RTE 2 OU = ISO 6523 - 0000 0000 OU = Soft ID O = TEST C = FR	e.com	
Modifier les propriété	s Copier dans un fichier		Modifi <u>e</u> r les propriét	<u>C</u> opier dans un fichier	
	C	ж			ж

3.5 Usage in your browser

3.5.1 Authentication and encryption

Steps to follow:

- Start Internet Explorer;
- Enter the URL for the RTE application or for the "RTE Customer Services Portal" (this URL starts with "https://");
- During authentication, the browser will ask you to choose the certificate before attempting to authenticate you, and then prompt for the certificate store security password;
- If several certificates are offered to you, you should choose the one that was supplied to you for the application which you are currently attempting to access (use the "Display the certificate" button to look at their contents);
- Now all the data that you send and receive will be encrypted.

3.5.2 Example of accessing the "RTE Customer Services Portal"

Whenever you access the welcome page with "https" as the prefix, you will have to select your certificate:



Authentifi	cation du	client		? ×
	ation Le site We Sélectionn	b que vous voulez v ez le certificat à utilis	isiter requiert une ider er pour vous connect	itification. er.
\rightarrow	Client RT	2		
	·	<u>P</u> lus d'infos	Afficher le cert	ificat
			<u>(0K)</u>	Annuler



The contents of the selected certificate, certificate. then click on "OK".

"Display the certificate..." If necessary, this window will ask you button allows you to look at the for the store password for your

The welcome page will then be displayed in a secure setting:





4. Internet Explorer 7

4.1 Configuration for SSL/TS protocols

In the browser, select the "**Tools > Internet options...**" menu options:



Select the "Advanced" tab:

ernet Upti	ions - Security A	At Risk			<u> </u>
eneral Se	curity Privacy	Content Con	nections F	programs	Advanced
Settinas —					
scongs					
	Empty Temporary	/ Internet Files	folder whe	n browse *	r is clc 🔺
	Enable Integrate	a windows Aut	nentication	Ŧ	
	Phishing Filter	CHITP Support			
	O Disable Phishi	ina Filter			
	O Turn off auto	matic website	checking		
	O Turn on autor	matic website o	hecking		
	Use SSL 2.0				
	Use SSL 3.0				
	Use TLS 1.0	o			
	Use TLS 1.0 Warn about certil Warn if changing	ficate address	mismatch*		
	Use TLS 1.0 Warn about certil Warn if changing Warn if POST sub	ficate address between secu mittal is redire	mismatch* re and not s tted to a zo	secure mo	bde
	Use TLS 1.0 Warn about certii Warn if changing Warn if POST sub	ficate address between secu pmittal is redire	mismatch* re and not s cted to a zo	secure mo one that d	
	Use TLS 1.0 Warn about certii Warn if changing Warn if POST sub	ficate address between secu omittal is redire	mismatch* re and not s cted to a zo	secure mo one that d	
	Use TLS 1.0 Warn about certii Warn if changing Warn if POST sub	ficate address between secu omittal is redire estart Internet	mismatch* re and not s cted to a zo Explorer	secure mo	ode Joesky
♥ ■ ♥ *Takes	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub	ficate address between secu omittal is redire estart Internet	mismatch* re and not s tted to a zo Explorer Restore a	secure mo one that d dvanced	ode Joes v
Takes	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub	ficate address between secu mittal is redire estart Internet	mismatch re and not s cted to a zo Explorer Restore a	secure mo one that d dvanced	
Takes	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub effect after you re net Explorer settii	ficate address between secu mittal is redire estart Internet	mismatch re and not s ted to a zo Explorer Restore a	secure mo one that d dvanced	settings
Takes	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub effect after you re net Explorer setti all temporary files, , and resets all the	ficate address between secu mittal is redire estart Internet ngs disables brow e changed setti	mismatch re and not s tted to a zo Explorer Restore a ser ngs.	secure mo one that d dvanced	settings
Takes of add-ons,	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub effect after you re met Explorer setti all temporary files, and resets all the id only use this if	ficate address between secu mittal is redire estart Internet g disables brow changed setti	mismatch* re and not s cted to a zo Explorer Restore a ser ngs. s in an unus	secure mo one that d dvanced Res sable stat	settings
Takes of add-ons, You shou	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub effect after you re rnet Explorer setting all temporary files, and resets all the uld only use this if	ficate address between secu mittal is redire estart Internet ngs disables brow changed setti your browser is	mismatch* re and not s cted to a zo Explorer Restore a ser ngs. s in an unus	dvanced Res	settings
set Inter Deletes a add-ons, You shou	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub effect after you re rnet Explorer settin all temporary files, , and resets all the uld only use this if	ficate address between secu omittal is redire estart Internet ngs disables brow changed setti your browser is	mismatch* re and not s cted to a zo Explorer Restore a ser ngs. s in an unus	dvanced	settings
set Inter Deletes a add-ons, You shou	Use TLS 1.0 Warn about certi Warn if changing Warn if POST sub effect after you re rnet Explorer setti all temporary files, , and resets all the uld only use this if	ficate address between secu omittal is redire estart Internet disables brow changed setti your browser is	mismatch* re and not s cted to a zo Explorer Restore a ser ngs. s in an unus	dvanced	settings settings

In the section labelled "**Security**", makes sure that checkboxes for SSL 2.0, SSL 3.0 and TLS 1.0 have been checked, as shown above.







4.2 Request for a digital certificate

4.2.1 Preliminary measures

The following steps must have been completed in advance:

• The company representative has made an access request:

The company representative must have filled out and signed the "RTE IT System and Applications Access Request Forms"; and must have sent them to the RTE customer relations officer:

• We have registered your request:

Upon reception of those forms, we will have created your application access account(s).

4.2.2 Overall schematic

Once the certificate request has been registered and validated by our services (within 5 working days), a message will be sent to the company representative to acknowledge receipt of the forms and asking him to call us to fix a phone meeting with the certificate holder for the day of the certificate installation.

Then, a message will be sent to the certificate holder after this call, reminding him of the scheduled meeting and giving him the address of the download web site and the retrieval code which will allow him to download his certificate from his own workstation.



The certificate holder must then connect to the digital certificate administration web site from his workstation to fill out and validate the registration form online. At that moment, a key pair will be generated on his workstation and his certificate will be downloaded.



4.3 Installation of the RTE CA root certificate

4.3.1 Download and installation

The RTE root certificate must now be installed in your browser so that RTE is known as the trusted Certification Authority.

To do this, please navigate to the RTE customer site at the following address:

http://rte.certplus.com/default.htm

The following page will be displayed.

Portail des porteurs RTE - Wanadoo	X
S → M http://rte.certplus.com/default.htm	Scoogle
😭 🍻 🔃 Portail des porteurs RTE	🛐 🔻 🗟 👻 🖶 Page 👻 🎯 Tools 👻
RTE du Réseau de Transport d Electricité	
Certificats logiciels	Cartes et tokens USB
Retrait de certificat	Acquittement de support
Retrait par CSR	
Test de certificat	Test de support
Révocation de certificat	Révocation de support
Recherche	Recherche
Autorité de Certification	
Installer le certificat rad	cine de RTE
	N Diternet 18:100% -

Click on the link "Installer le certificat racine de RTE / Install the RTE root certificate"

The RTE CA root certificate will then be installed in the Windows certificate store, as per the process described below.





File Dow	nload			×
Do yo	u want to open o	or save this fi	le?	
	Name: geto Type: PKC From: rte.	certif.p7b :S #7 Certificate certplus.com	s, 694 bytes	
🔽 Alw	ays ask before ope	Open	Save	Cancel
?	While files from th harm your compu save this file. <u>Wh</u>	he Internet can b liter. If you do no hat's the risk?	be useful, some f t trust the source	iles can potentially e, do not open or

Click on the "Open" button.

🚟 Certificats			
Eichier Action Affichage ?			
🗐 Certificats - Utilisateur actuel	Délivré à 🔺	Délivré par	Date d'expiration
⊡⊡ C:\CERTIF~1\GETCER~1.P7B	RTE Autorite de Certification	RTE Autorite de	29/05/2012
Le magasin C:\CERTIF~1\GETCER~1.P76	3 contient 1 certificat.		

Double-click on "**RTE Autorite de Certification (RTE Certification Authority)**".

NT-SI-CN2I-OEM-ST-08-00236 Version: 3

RTE

Access to the IT system with digital certificates under Microsoft Windows XP PKI user manual

Certificat		? ×
Général Détails Chemin d	accès de certification	
		— II
Informations	sur le certificat	
Ce certificat est conç	u pour les rôles suivants :	
•Toutes les stratégies d' •Toutes les stratégies d'	émissions application	
	approximite the second s	
Délivré à :	RTE Autorite de Certification	
Délivré par :	RTE Autorite de Certification	
Valide à partir de	u 29/05/2002 jusqu'au 29/05/2012	
		.
Installe	er le <u>certificat</u> <u>D</u> éclaration de l'émetteur	
	(ж

Click on the "Install the certificate" button.

Assistant Importation de certificat		×
Bie Cet. certi certi certi utilis conr la zo Pour	Assistant vous aide à copier des certificats, des listes de ficats de confiance et des listes de révocation de ficats depuis votre disque vers un magasin de ficats. ertificat, émis par une Autorité de certification, est une irmation de votre identité et contient des informations ées pour protéger vos données ou établir des jexions réseau sécurisées. Le magasin de certificats est ne système où les certificats sont conservés. continuer, cliquez sur Suivant.	
	< Précédent Suivant > Annuler	





Assistant Importation de certificat	×
Magasin de certificats	
Les magasins de certificats sont des zones système où les certificats sont stockés.	
Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat.	
Sélectionner automatiquement le magasin de certificats selon le type de certificat	
Placer tous les certificats dans le magasin suivant	
Magasin de certificats :	
Parcourir	
	_
< <u>P</u> récédent <u>Suivant</u> Annuler	

Leave the selected default option as it is and click on "Next".

Assistant Importation de cert	ificat	×
	Fin de l'Assistant Importation de certificat Vous avez terminé correctement l'Assistant Importation de certificat. Vous avez spécifié les paramètres suivants : Magasin de certificats sélectionné Déterminé automatiqu Contenu Certificat	
	< Précédent Terminer Annuler	

Click on "**Finish**", and the following window then displays the contents of the root certificate to be imported.

Magasin	de certificats principal 🛛 🔀
	Voulez-vous ajouter le certificat suivant au magasin principal ? Objet : RTE Autorite de Certification, RESEAU DE TRANSPORT D ELECTRICITE Émetteur : auto-émis Limite de validité : de mercredi 29 mai 2002 à mardi 29 mai 2012 Numéro de série : 75230902 54AEC749 818427D3 8CCC21EB Empreinte numérique (sha1) : A29A4FA1 77142C87 FA302DB0 8F2C0237 37C7AE37
	Empreinte numérique (md5) : 53426A2E A510AB2A 2109EE88 1367A031





4.3.2 Verification of the root certificate fingerprint

To make sure that you have downloaded the genuine RTE AC root certificate, carefully check that the "SHA1" or "MD5" digital fingerprint displayed in the window shown is **identical** to that shown above.

 The root certificate digital fingerprints for RTE CA are listed here:

 SHA1
 A29A
 4FA1
 7714
 2C87
 FA30
 2DB0
 8F2C
 0237
 37C7
 AE37

 MD5
 53:42:6A:2E:A5:10:AB:2A:21:09:EE:88:13:67:A0:31

If the hash fingerprint is not identical, click on "No" and contact our support services.

If it is identical, click on "Yes" to finish the import.

Assistant	Importation de certificat	×
(į)	L'importation s'est terminée correcte	ment.
	OK	

Click on "OK".

4.3.3 Contents of the RTE CA certificate

The root certificate that you have just downloaded is stored in the certificate store appropriate to the browser used. It can be viewed in Internet Explorer, for example:

Use the menu option "Tools > Internet options...", "Contents" tab, "Certificates..." button, "Trusted root authorities" tab:

Certificats	?X Certificat ?X
Rôle prévu : <pre></pre>	Cénéral Détails Chemin d'accès de certification
Autoritée principales de configures 1 é la	
Autres personnes Autorites intermediaires Autorites principales de connance Editeurs	Afficher : <tout></tout>
Délivré à Délivré par Date d'exp Nom con	
PTT Post Root CA PTT Post Root CA 26/06/2019 KeyMail	. Champ Valeur
RTE Autorite de Certification RTE Autorite de Certifi 29/05/2012 <aucun></aucun>	Version V3
Saunalahden Serveri CA Saunalahden Serveri CA 26/06/2019 Saunala	 • ENuméro de série 75 23 09 02 54 ae c7 49 81 84
Saunalahden Serveri CA Saunalahden Serveri CA 26/06/2019 Saunala	· El Algorithme de signature sha1RSA
Secure Server Certificatio Secure Server Certific 08/01/2010 VeriSign	Émetteur RTE Autorite de Certification,
SecureNet CA Class A SecureNet CA Class A 16/10/2009 SecureN	Valide à partir du mercredi 29 mai 2002 01:00:00
SecureNet CA Class B SecureNet CA Class B 16/10/2009 SecureN	Valide jusqu'au mardi 29 mai 2012 00:59:59
SecureNet CA SGC Root SecureNet CA SGC Root 16/10/2009 SecureN	Objet RTE Autorite de Certification
	Clé publique R5A (1024 Bits)
Importer Exporter Supprimer Avan	ncé CN = RTE Autorite de Certification
- Dátaile do covtificat	O = RESEAU DE TRANSPORT D ELECTRICITE
- Decais de Cercificat	
<tout></tout>	
	<u>19e</u>
Ferr	rmer
	Modifier les propriétés Copier dans un fichier
Click on the "Display"" button,	and
then on the "Details" button	
then on the "Details" button.	ОК



4.4 Downloading your certificate

To create your key pair and your certificate, you must then connect, on the RTE meeting day specified, to the web site:

http://rte.certplus.com/default.htm

🖉 Portail des porteurs RTE - Wanadoo		_ 8 ×
🕞 🕞 👻 http://rte.certplus.com/default.htm	💽 🏍 🗙 Google	₽ •
😪 🏟 🔟 Portail des porteurs RTE	🚹 • 🗟 - 🖶 • 🔂	Page 🔹 🎯 Tools 👻 🎇
RTE du Réseau de Transport d'Electricité		
Certificats logiciels	Cartes et tokens USB	1
Retrait de certificat	Acquittement de support	
Retrait par CSR		
Test de certificat	Test de support	
Révocation de certificat	Révocation de support	
Recherche	Recherche	
Autorité de Certification		
Installer le certificat racine de RTE		
	Therefore the second se	€ 100% · //

Click on the "Retrait de certificat / Retrieve the certificate" button.

It is possible that a warning message might be displayed at the top of the web page (tagged with the following icon 0).

If it does, then click on the message and select "Add-on disabled" > "Run ActiveX control":

2) Your current security settings put your computer at risk. Click here to change your se <u>curity settings</u>					
	Add-on Disabled 🔹 🕨	Run ActiveX Concor			
Informations pour le certificat numériqu	Security Settings at Risk 🕨	What's the Risk?			
	More information				
Bassallana ing ing akanan kutuku ang Uning kutuku i					



Fill out the following form:

🖉 Enregistrement utilisateur Microso	oft - Wanadoo		_ 8 ×
COO - M https://rte.soft-id.certp	olus.com/client/userEnrollMS.htm	🔽 🔒 😽 🗙 Google	P -
🙀 🕸 🔃 Enregistrement utilisateur M	Microsoft	🟠 💌 🔝 👻 🖶 Page 💌	🌀 Tools 👻 »
Informations Remplissez tous	s pour le certificat numérique les champs. Nutilisez que l'alphabet latin, sans d is votre certificat et seront accessibles à tous	caractères accentués. Les informations des champs précédés d'un "*"	
	Nom Complet : * (obligatoire) Ex : DUPONT	Client-RTE1 TEST	
	Adresse Email : * (obligatoire) Ex: jean.dupont@societe.com	rte1.test@services.rte-france.com	
	Authentifiant PKI: (obligatoire)		
	Code de retrait : (obligatoire)	2V4AU0	
	Soumettre	Annuler	
-			
			-
Done		🛛 👔 🚱 Internet	100% •

The fields marked with an asterisk must be completed **without diacritic marks** (i.e. accents, cedillas, ...) **or punctuation marks**; as they would also appear in the certificate that will be generated.

The **retrieval code** is the code supplied in the 2nd email that you received from us which allows you to authenticate yourself. To make things easier, you can do simple copy-paste commands to enter the data.

You must likewise enter your **Authentifiant Utilisateur PKI (PKI User Credentials)**, just as they were supplied in the RTE IT system access technical specifications; they will serve to authenticate you with the RTE Hotline any time that you contact them.

Lastly, click on "Submit" to send your request for the digital certificate.

A dialogue box will ask you to confirm your email address:

Windows	Internet Explorer
?	Confirmez votre adresse e-mail : test-rte-client1@services.rte-france.com
	Si votre adresse e-mail est correcte, cliquez sur OK, sinon sur CANCEL et corrigez là dans le formulaire.
	Si votre adresse e-mail est incorrecte, vous ne pourrez pas utiliser votre Identification numérique
	OK Cancel

Click on the "**OK**" button, or "Cancel" to return to the form data entry screen.



Violation	de script potentielle	\times
⚠	Ce site Web nécessite in nouveau certificat de votre part. Vous ne devriez autoriser que les sites Web approuvés à demander u certificat de votre part. Voulez-vous demander un certificat maintenant ?	IN

Click on the "Yes" button.

4.4.1 Generation of the key pair

The dialogue box shown below will then be displayed, indicating that an RSA key pair has been created by Internet Explorer on your workstation:

Création d'une nouvelle clé d'échar	nge RSA 📃 🛃	Création d'une nouvelle	clé d'échange RSA
Une application crée Dié privée CryptoAPI Niveau de sécurité de Moyen	sctuellement un élément protégé.		Choisissez un niveau de sécurité approprié à cet élément.
			< Précédent Suivant > Annuler

Click on the **"Define the security** Select the **"High**" option, then click on **level**" button. **"Next**".

The key pair that will be generated is, by default, at a "**medium security**" level, which means that each later use of this key pair will cause the display of a simple acknowledgement message: the certificate holder is also warned of this usage but no password is requested.

For protected use of your key pair, which we recommend, you should rather choose "**high security**", which will mean that a password, that you will choose here, will be asked of you for every later use of your key pair. The screens below describe the procedure to set this security level.

Création d'une nouvelle	clé d'échange RSA	×	Création d'une	nouvelle clé d'échange RSA	×
<u>a</u>	Créer un mot de passe pour protéger cet élément.			Une application crée actuellement un élément protégé.	
	Créer un nouveau mot de passe pour cet élément.			Clé privée CryptoAPI	
	Mot de passe pour : Clé privée CryptoAPI		Ca (
Ť,	Mot de passe :		S.E	Niveau de sécurité défini à Définir le <u>n</u> iveau de sécurité	
	Confirmer :		V	OK Annuler Détails	
	< Précédent Terminer Annuler				

Enter a password, then click on the Click on the "**OK**" button. "**Finish**" button.



 Violation de script potentielle
 Image: Ce site Web ajoute un ou plusieurs certificats à cet ordinateur. L'autorisation donnée à un site Web non approuvé de mettre à jour vos certificats pose un risque de sécurité. Le site Web pourrait installer des certificats que vous n'approuvez pas, ce qui permettrait à des programmes que vous n'approuvez pas de s'exécuter sur cet ordinateur et d'accéder à vos données.

 Voulez-vous que ce programme ajoute les certificats maintenant ? Cliquez sur Oui si vous faites confiance à ce site Web. Sinon, cliquez sur Non.

Click on the "Yes" button.

4.4.2 Installation of the certificate

🖉 ID Download - Wanadoo			_ 8 ×
COO - M https://rte.soft-id.certp	olus.com/cgi-bin/sophialite.exe	💌 🔒 🐓 🗙 Google	P -
😪 🕸 🔝 ID Download		🟠 + 🗟 - 🖶 Pag	e 🕶 🎯 Tools 👻 »
Félicitations			
Votre certificat nur	nérique a été téléchargé et installé.		
Informations	s sur votre Certificat numerique		
	Country = FR Organization = TEST Organizational Unit = Soft ID Organizational Unit = ISO 6523 - 0000 0000 Common Name = Client-RTE1 TEST Email Address = test-fr-client1@services.de-france.com		
	Numéro de Série = 7f9f03b2b43f89d21c9e8427091157db		
Done		🧊 🚱 Internet	100% - //

Next, the certificate is automatically downloaded and installed in the Internet Explorer certificate store. The page opposite is displayed to indicate the end of this process.

IMPORTANT

Once downloaded, your certificate with its key pair and root certificate must be saved on a removable medium (e.g. a diskette) that you must store securely to prevent unauthorised access. Refer to the appendix for the certificate export procedure.



4.4.3 Contents and verification of your digital certificate

Regardless of the browser used, the contents of the downloaded certificate will obviously be the same, only the presentation of the information on the screen will vary. For downloads with Internet Explorer, open the certificate store with the following menu choices:

"Tools > Internet options...", "Contents" tab, "Certificates..." button:

ificates				?
ended purpose: <al ersonal Other People </al 	l> Intermediate Certification A	uthorities Tru	sted Root Certifica	atior 🔳
Issued To	Issued By	Expiratio	Friendly Name	•
Client-RTE1 TEST	RTE Autorite de Certif	23/04/2009	<none></none>	
				-
				Ţ
Import Export.	Remove		Adv	vanced
ertificate intended purpo	ses			
All>				
			Vi	0141
				C 11
				-

Select your certificate, then click on "Display".



Certificate	<u>?</u> ×	Certificate	? ×
General Details Certification Path		General Details Certification Path	_
Certificate Information This certificate is intended for the following purpose(s): •All application policies	-	Certification path Certification - RESEAU DE TRANSPORT D ELECTR Client-RTE1 TEST	đ
Issued to: Client-RTE1 TEST Issued by: RTE Autorite de Certification	-	View Certificate	1
Valid from 24/04/2007 to 23/04/2009			-
\mathscr{P} You have a private key that corresponds to this certificate.		Certificate status: This certificate is OK.	-
Issuer Stateme	nt K		

It is valid for 2 years from the download This tab allows you to verify your date.

The "valid" status of your certificate, as well as the complete display of the certificate access path (2 levels), shows that your certificate has been correctly installed along with the root certificate, and therefore all the correct usage conditions for your certificate have been satisfied.

Certificate	?	Eertificate	? ×
General Details Certificatio	n Path]	General Details Certification F	Path
Show: <all></all>		Show: <all></all>	
Field Version Serial number Signature algorithm Issuer Valid from Valid to Subject Public key	Value V3 7f 9f 03 b2 b4 3f 89 d2 1c 9e sha1R5A RTE Autorite de Certification, mardi 24 avril 2007 17:55:54 jeudi 23 avril 2009 17:55:54 test-rte-client1@services.rte-f RSA (1024 Bits) Image: State State	Field Serial number Signature algorithm Sissuer Valid from Valid to Subject CRL Distribution Points	Value 7f 9f 03 b2 b4 3f 89 d2 1c 9e sha1RSA RTE Autorite de Certification, mardi 24 avril 2007 17:55:54 test-rte-rtient1@services.rte-f RSA (1024 Bits) [1]CRL Distribution Point: Distr
CN = RTE Autorite de Certifi O = RESEAU DE TRANSPORT		E = test-rte-client1@services.r CN = Client-RTE1 TEST OU = 150 6523 - 0000 0000 OU = 50f ID O = TEST C = FR	te-france.com
	Edit Properties Copy to File OK		Edit Properties Copy to File OK


4.5 Usage in your browser

4.5.1 Authentication and encryption

Steps to follow:

- Start Internet Explorer; •
- Enter the URL for the RTE application or for the "RTE Customer • Services Portal" (this URL starts with "https://");
- During authentication, the browser will ask you to choose the certificate • before attempting to authenticate you, and then prompt for the certificate store security password;
- If several certificates are offered to you, you should choose the one that • was supplied to you for the application which you are currently attempting to access (use the "Display the certificate" button to look at their contents);
- Now all the data that you send and receive will be encrypted. •

4.5.2 Example of accessing the "RTE Customer Services Portal"

Whenever you access the welcome page with "https" as the prefix, you will have to select your certificate:

×
tégé.
de passe
ils
ai

The contents of the selected certificate, certificate. then click on "OK".

"Display the certificate..." If necessary, this window will ask you button allows you to look at the for the store password for your



The welcome page will then be displayed in a secure setting:





5. Mozilla Firefox



5.1 Configuration for SSL/TS protocols

From the "**Tools** > **Options...**" menu, select the "Advanced" section, and then the "Security" tab.

In this window, select the 3 checkboxes "Use SLL [...]" and "Use TLS 1.0":

Options							×
7 3				4	203		
Général	Vie privée	Contenu	Onglets	Téléchargements	Avancé		
Général	Mises à jour	Sécurité					
denorar		I					1
Protoco	oles —						
Uti	liser SSL <u>2</u> .0 <			🔽 Utiliser SSL	<u>3</u> .0 🔶		
Uti	liser TLS <u>1</u> .0	<u> </u>					
_ Certific	ats ———						[
Lorsqu	un site Web n	écessite un c	ertificat :				
O En	sél <u>e</u> ctionner u	un automatiq	uement (Me demander à ch	ague fois		
							_
Affich	er les certifica	ts Listes	; de <u>r</u> évocat	ion <u>V</u> érification	Périphé	rique <u>s</u> de sécuri	ité
					·····		
				OK	Ar		Aide

5.2 Request for a digital certificate

5.2.1 Preliminary measures

The following steps must have been completed in advance:

• The company representative has made an access request:

The company representative must have filled out and signed the "RTE IT System and Applications Access Request Forms"; and must have sent them to the RTE customer relations officer:

• We have registered your request:

Upon reception of those forms, we will have created your application access account(s).



5.2.2 Overall schematic

Once the certificate request has been registered and validated by our services (within 5 working days), a message will be sent to the company representative to acknowledge receipt of the forms and asking him to call us to fix a phone meeting with the certificate holder for the day of the certificate installation.

Then, a message will be sent to the certificate holder after this call, reminding him of the scheduled meeting and giving him the address of the download web site and the retrieval code which will allow him to download his certificate from his own workstation.



The certificate holder must then connect to the digital certificate administration web site from his workstation to fill out and validate the registration form online. At that moment, a key pair will be generated on his workstation and his certificate will be downloaded.

5.3 Installation of the RTE CA root certificate

5.3.1 Download and installation

The RTE root certificate must now be installed in your browser so that RTE is known as the trusted Certification Authority.

To do this, please navigate to the RTE customer site at the following address:

http://rte.certplus.com/default.htm

🥹 Portail des porteurs RTE - Mozilla Firefox	
Eichier Edition Affichage Aller à Marque-pages Outils ?	
🔶 - 🍌 - 🥞 🙁 🟠 🔟 http://rte.certplus.com/default.htm	• О ок С.
RTE du Reseau de Transport d Electricité	
Certificats logiciels	Cartes et tokens USB
Retrait de certificat	Acquittement de support
Retrait par CSR	
<u>Test de certificat</u>	<u>Test de support</u>
Révocation de certificat	Révocation de support
Recherche	<u>Recherche</u>
Autorité de Certification	_
Terminé	

Click on the link "Installer le certificat racine de RTE / Install the RTE root certificate"

A dialogue box will be displayed, in which you must select the 3 checkboxes "Confirm this CA for identification [...]" to confirm confidence in the RTE CA:

Téléchargement du certificat	×
On vous a demandé de confirmer une nouvelle autorité de certification (AC).	
Voulez-vous faire confiance à « RTE Autorite de Certification » pour les actions suivantes ?	
Confirmer cette AC pour identifier des sites Web.	
Confirmer cette AC pour identifier les utilisateurs de courrier.	
Confirmer cette AC pour identifier les développeurs de logiciels.	
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
Voir Examiner le certificat d'AC	
OK Annuler	

5.3.2 Verification of the root certificate fingerprint

Click on "**View**" to verify that the certificate to which you are about to grant trusted status is indeed the RTE root certificate:



Page: 42/102

Access to the IT system with digital certificates under Microsoft Windows XP PKI user manual

To make sure that you have downloaded the genuine RTE AC root certificate, carefully check that the "SHA1" or "MD5" digital fingerprint displayed in the dialogue box shown is identical to that shown opposite.

	conce de certificación	_
Général Détails		
Impossible de vérifier ce	certificat car son émetteur n'est pas digne de confiance.	
Émis pour Nom commun (CN) Organisation (O) Unité d'organisation (OU) Numéro de série Émis par Nom commun (CN)	RTE Autorite de Certification RESEAU DE TRANSPORT D ELECTRICITE <ne certificat="" du="" fait="" partie="" pas=""> 75:23:09:02:54:AE:C7:49:81:84:27:D3:8C:CC:21:EB RTE Autorite de Certification</ne>	
Organisation (O) Unité d'organisation (OU)	RESEAU DE TRANSPORT D ELECTRICITE <ne certificat="" du="" fait="" partie="" pas=""></ne>	
Validité Émis le Expire le	29/05/2002 29/05/2012	
Empreintes numériques Empreinte numérique SHA1 Empreinte numérique MD5	A2:9A:4F:A1:77:14:2C:87:FA:30:2D:80:8F:2C:02:37:37:C7:AE:37 53:42:6A:2E:A5:10:AB:2A:21:09:EE:88:13:67:A0:31	
	Fermer	

 The root certificate digital fingerprints for RTE CA are listed here:

 SHA1
 A29A
 4FA1
 7714
 2C87
 FA30
 2DB0
 8F2C
 0237
 37C7
 AE37

 MD5
 53:42:6A:2E:A5:10:AB:2A:21:09:EE:88:13:67:A0:31

If it is not identical, click on "Close" to return to the previous window where you should click on "Cancel" and contact our support services.

If it is identical, continue the process to finish the import. The "Details" tab:

tails du certificat :"RTE Autorite de Certification"	X	Détails du certificat :"RTE Autorite de Certification"	2
Général Détails		Général Détails	
Hiérarchie des certificats		Hiérarchie des certificats	
RTE Autorite de Certification		RTE Autorite de Certification	
Champs du certificat		Champs du certificat	
RTE Autorite de Certification	<u>►</u>	Émetteur	
Certificat		- Validité	
Version		Pas avant	_
-Numéro de série		-Pas après	
Algorithme de signature des certificats		Sujet	
-Émetteur		Info clé publique du sujet	
- Validité		-Algorithme clé publique du sujet	
Pasavant		Clé publique du sujet	
Pas aprés	<u> </u>	Extensions	_
Valeur du champ		Valeur du champ	
CN = RTE Autorite de Certification O = RESEAU DE TRANSPORT D ELECTRICITE		CN = RTE Autorite de Certification O = RESEAU DE TRANSPORT D ELECTRICITE	
]			
		·	
	Fermer		Fermer

Click on "Close" to return to the initial screen (see above) where you can click on "OK": the RTE CA root certificate is now installed in Mozilla Firefox.



To view this certificate later in Mozilla Firefox, you must use the "**Tools** > **Options...**" menu, and select the "**Advanced**" section, and the "**Security**" tab.

Dptions						×
		§		4	Sold State	
Général	Vie privée	Contenu	Onglets	Téléchargements	Avancé	
Général 1	Mises à jour	Sécurité				1
C Protoco	oles ———					
🔽 Uti	liser SSL <u>2</u> .0			🔽 Utiliser SSL	3.0	
🔽 Uti	liser TLS 1.0					
)	
Certific	ats ———					
Lorsqu	un site Web r	écessite un c	ertificat :			
O En	sél <u>e</u> ctionner	un automatiq	uement (Me demander à ch	ague fois	
Affich	er les certifica	ats Listes	; de <u>r</u> évocat	ion <u>V</u> érification	Périphérique <u>s</u> de sécurité	
	1					
				OK	Annuler Aide	

In the previous window, you must click on the "Display the certificates" button.

🥹 Gestionnaire de certificats	
Vos certificats Autres personnes Sites Web Autorités Vous possédez des certificats enregistrés identifiant ces autorités de certificat	ion :
Nom du certificat Périphérique de sécurité	E
RESEAU DE TRANSPORT D ELECTRICITE	
·RTE Autorite de Certification Sécurité personnelle	
🖃 RSA Data Security, Inc.	
Secure Server OCSP Responder Builtin Object Token	_
Voir Modifier Importer Supprimer	
	ОК

In the "Authorities" tab, you can verify that the "RTE Autorite de Certification" root certificate has indeed been registered on your PC hard drive ("Personal security"), and view it by selecting it and clicking on "View".

5.4 Downloading your certificate

To create your key pair and certificate, you must connect to the following site:

http://rte.certplus.com/default.htm



😻 Portail des p	oorteurs RTE - Mozi	la Firefox						
<u>Fichier</u> <u>E</u> dition	<u>A</u> ffichage Aller à	<u>M</u> arque-pages	Ou <u>t</u> ils <u>?</u>					0
<	- 🛃 🛞 😚	http://rte.ce	rtplus.com/defa	ult.htm		🔹 🜔 oi	< <mark>G</mark> .	
RTE	Gestionnaire du Réseau de	Transport d'Electric	iné					
Certif	icats logicie	els			Cartes et	tokens USB		
Retra	it de certifi	cat	_		Acquittem	ient de supp	ort	
<u>Retrai</u>	it par CSR							
<u>Test c</u>	le certifica	t			<u>Test de su</u>	ipport		
<u>Révoc</u>	ation de ce	ertificat			<u>Révocatio</u>	n de suppor	t	
<u>Reche</u>	erche				<u>Recherch</u>	2		
Autor	ité de Certi	fication						
Insta	ler le certi	ficat racin	e de RT	E				
Terminé								

Click on the "Retrait de certificat / Retrieve the certificate" button to install your digital certificate.

🕲 Enregistrement u	utilisateur Netscape - Mozilla Firefox	
Eichier Edition Af	fichage Aller à Marque-pages Outils ?	
	Image: Second	nt/userEnrollNS.htm 🔂 🔽 💿 OK 🔀
Information	s pour le certificat numérique	
Remplissez tous sont incluses dan	les champs. N'utilisez que l'alphabet latin, sans cai is votre certificat et seront accessibles à tous.	actères accentués. Les informations des champs précédés d'un "*"
	Nom Complet : * (obligatoire) Ex : DUPONT	Client RTE 1
	Adresse Email : * (obligatoire) Ex : jean.dupont@societe.com	client.rte@services.rte-france.con
	Authentifiant PKI: (obligatoire)	
	Code de retrait : (obligatoire)	ABC123
Obligatoire :	Choisissez le niveau de chiffrement à	1024
Le niveau de crypt	tage indiqué ci-dessous est le maximum permis par	votre navigateur. Nous vous recommandons de choisir 1024.
	Niveau de cryptage	1024 (Grade moyen) 💌
	Soumettre	Annuler
Terminé		rte.soft-id.certplus.com 🔒

Copyright RTE. This document is the property of RTE. All communication, reproduction or publication, even partial, is prohibited without written authorisation from the Electricity Transport Network Operator (RTE)





The fields marked with an asterisk must be completed **without diacritic marks** (i.e. accents, cedillas, ...) **or punctuation marks**; as they would also appear in the certificate that will be generated.

The **retrieval code** is the code supplied in the 2nd email that you received from us which allows you to authenticate yourself. To make things easier, you can do simple copy-paste commands to enter the data.

You must likewise enter your **Authentifiant Utilisateur PKI (PKI User Credentials)**, just as they were supplied in the RTE IT system access technical specifications; they will serve to authenticate you with the RTE Hotline any time that you contact them.

On this form, a dropdown list directly asks you to select the key size. You must **absolutely** select a size of **1024 bits**.

Lastly, click on "Submit" to send your request for the digital certificate.

A dialogue box will ask you to confirm your email address:

https://i	te.soft-id.certplus.com	×
j	Confirmez votre adresse e-mail : client.rte@services.rte-france.com	
	Si votre adresse e-mail est correcte, cliquez sur OK, sinon sur CANCEL et corrigez là dans le formulaire.	
	Si votre adresse e-mail est incorrecte, vous ne pourrez pas utiliser votre Identification numérique	
	OK Annuler	

Click on "OK".

5.4.1 Generation of the key pair

Finally, the RSA key pair is generated by Mozilla Firefox, and the following message is displayed:



5.4.2 Installation of the certificate

Your certificate is finally downloaded and installed in the Mozilla Firefox certificate store. The following page will then be displayed to indicate the end of the process:

RTE

Access to the IT system with digital certificates under Microsoft Windows XP PKI user manual



IMPORTANT

Once downloaded, your certificate with its key pair and root certificate must be saved on a removable medium (e.g. a diskette) that you must store securely to prevent unauthorised access. Refer to the appendix for the certificate export procedure.

5.4.3 Viewing and verification of your digital certificate

Regardless of the browser used, the contents of the downloaded certificate will obviously be the same, only the presentation of the information on the screen will vary.

For Mozilla Firefox, you must click on the "Advanced" section, and then on the "Security" tab:



Options X Image: Second state of the private o
Image: Selection of the privée Général Vie privée Contenu Onglets Téléchargements Avancé
Général Vie privée Contenu Onglets Téléchargements Avancé
Général Mises à jour Sécurité
C Protocoles
✓ Utiliser SSL 2.0
✓ Utiliser TLS 1.0
Certificats
Lorsqu'un site Web nécessite un certificat :
C En sél <u>e</u> ctionner un automatiquement Me demander à chague fois
Afficher les certificats Listes de révocation Vérification Périphériques de sécurité
OK Appuler Aide

Click on the "Display the certificates" button.

😻 Gestionnaire de certificats	- D ×
Vos certificats Autres personnes Sites Web Autorités Vous possédez des certificats de ces organisations qui vous identifient :	
Nom du certificat Périphérique de Sujets Numéro de Expire	e 🖽
Client RTE 1 Sécurité personnelle Client,Signature,Chiffr 39:2D:6B:2A 29/10/2	007
Voir Exporter Tout exporter Importer Supprimer	
	ОК

The "Your certificates" tab.

The certificate is a digital certificate: once installed, it will be described as "Personal security". You can view it by selecting it and clicking on "View".





Détails du certificat :"Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID"	Détails du certificat :"Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID"
Général Détails Ce certificat a été vérifié pour les utilisations suivantes : Certificat clerk S3. Certificat de signature de courrier Certificat de réception de courrier	Général Détais Hiérarchie des certificats RTE Autorite de CertificationClient RTE 1
Émis pour Client RTE 1 Organisation (0) TEST Unité d'organisation (0) Soft ID Numéro de série 392/DE82A11628/90133:D3:DE:B6149:08:80:C0:21 Émis par Nom commun (CN) Nom commun (CN) RTE Autorité de Certification Organisation (0) RESEAU DE TRANSPORT D ELECTRICITE Unité d'organisation (0) RESEAU DE TRANSPORT D ELECTRICITE Unité d'organisation (0) Ven faits par partie du certificat.> Validité Ense le Expre le 29/10/2005 Expre le 29/910/2007 Empreintes numérique MD5 49/2F/C8/E1/2F/36/0C6/75/19/D1:60/86/CC149/E5:1C	Champs du certificat Champs du certificat Champs du certificat Certification Certific
Fermer	Fermer

The 1st tab displays the message "This certificate has been verified for the following uses". The 2nd tab displays the certification hierarchy with the RTE CA root certificate. This ensures that all the certificates have been correctly installed, and that all the correct usage conditions for your certificate have been satisfied.

5.5 Usage in your browser

5.5.1 Authentication and encryption

Steps to follow:

- Start Mozilla Firefox;
- Enter the URL for the RTE application or for the "RTE Customer Services Portal" (this URL starts with "https://");
- During authentication, the browser will ask you to choose the certificate before attempting to authenticate you, and then prompt for the certificate store security password;
- If several certificates are offered to you, you should choose the one that was supplied to you for the application which you are currently attempting to access (the contents of the selected certificate from the dropdown list are displayed beneath the list);
- Now all the data that you send and receive will be encrypted.

5.5.2 Example of accessing the "RTE Customer Services Portal"

Whenever you access the welcome page with "https" as the prefix, you will be requested to select your certificate:



Organisation : « RTE » Émis sous : « RSA Data Security, Inc. » Choisir un certificat à présenter comme identification : Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID [39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:B0:C0 Détails du certificat sélectionné : Émis pour : E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft ID,O=TEST,C=FR Numéro de série: 39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:B0:C0:21
Émis sous : « RSA Data Security, Inc. » Choisir un certificat à présenter comme identification : Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID [39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:B0:C0 Détails du certificat sélectionné : Émis pour : E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft ID,O=TEST,C=FR Numéro de série: 39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:B0:C0:21
Choisir un certificat à présenter comme identification : Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID [39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:B0:C0 Détails du certificat sélectionné : Émis pour : E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft ID,O=TEST,C=FR Numéro de sérvice: 39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:B0:C0:21
Client RTE 1'S RESEAU DE TRANSPORT D ELECTRICITE ID [39:2D:68:2A:16:28:90:33:D3:DE:86:49:08:80:C0 Détails du certificat sélectionné : Émis pour : E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft ID,O=TEST,C=FR Numéro de série: 39:2D:68:2A:16:28:90:33:D3:DE:86:49:08:80:C0:21
Détails du certificat sélectionné : Émis pour : E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft ID,O=TEST,C=FR Numéro de série: 39:2D:68:2A:16:28:90:33:D3:DE:86:49:08:80:C0:21
Émis pour : E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft ID,O=TEST,C=FR Numéro de série: 39:2D:68:2A:16:28:90:33:D3:DE:86:49:08:80:C0:21
Valide de 28/10/2005 02:00:00 pour 29/10/2007 00:59:59 Sujets: Client, Signature, Chiffrement Émis par : CN=RTE Autorite de Certification,O=RESEAU DE TRANSPORT D ELECTRICITE Stocké dans : Sécurité personnelle

Select your certificate from the dropdown list labelled "Choose a certificate to present as identification" and click on "OK". If necessary, this window will ask you for the password to the Mozilla Firefox certificate store.

Invite	×
j	Veuillez saisir le mot de passe principal de Sécurité personnelle.

	OK

The welcome page will then be displayed in a secure setting:





6. Certificates and email software

Depending on the email client that you use (Outlook 2000/XP/2003, Outlook Express, Mozilla Thunderbird), we suggest that you refer to the appropriate one of the following sections.

Steps to follow:

- install the "RTE Autorité de Certification" root certificate, so that the email software trusts your certificates and the applications' certificates (refer to the installation of the RTE root certificate in the associated web browser);
- configure your email account assigned for communications with RTE, so that the email software always encrypts and signs your messages (being sent from the RTE IT system);
- install the application certificate(s), so that messages that you send to those applications are encrypted.

Here are the associated web browsers that you should configure (if they have not already been done), in order that your email client is correctly configured and operational:

Email client	Associated web browser
Outlook 2000/XP/2003	Internet Explorer
Outlook Express	Internet Explorer
Mozilla Thunderbird	Mozilla Firefox (similar configuration)
Lotus Notes	Configuration is specific to Lotus Notes

6.1 Outlook 2000/XP/2003

6.1.1 Configuration



IMPORTANT

Before starting Outlook 2000 (French version), run the following command:

<PACKAGE>\Windows Updates\Outlook 2000\french-configuration.reg

Doing this will make Outlook 2000 conformant with the most recent cryptographic standards in use in France.





To be able to associate your certificate with your email account under Outlook, your certificate must be installed under Internet Explorer. This is automatically the case if you have downloaded it in Internet Explorer; but if you downloaded it with Mozilla Firefox, you must export it from that browser and import it into Internet Explorer, with the corresponding private key and the RTE CA root certificate. Refer to the section at the end of this document.

Start up Outlook and click on the "?", and then on "About Microsoft Outlook 2000".

If the Outlook installation is of the "Internet Email only" type, as shown below:

À propos de l	Microsoft Outlook	<u>? ×</u>
ß	Microsoft® Outlook® 2000 SR-(9.0.0.3821) Messagerie Internet uniquement Copyright © 1995-1999 Microsoft Corp. Tous droit	ts réservés.
	Inipole 2, 2010 Construction of the serves o	set vérificateur ent, Toulouse (France). Tous ipell™ spelling correction ducts N.V. All rights reserved. 998. Two-Level Compiler: © Spelling ©1996-1997. echten voorbehouden. se taal, © Nederlandse du Uitgevers. Arabic spelling n, Egypt.
	Administrateur cgey Product ID: 51097-335-8958336-02612	
Avertissemen d'auteur et pa distribution pa soit, est stricte dispositions se sanctions péna	: : Ce logiciel est protégé par la loi relative au droit r les conventions internationales. Toute reproduction ou tielle ou totale du logiciel, par quelque moyen que ce ment interdite. Toute personne ne respectant pas ces rendra coupable du délit de contrefaçon et des les prévues par la loi.	OK Infos système Support technique Informations de sécurité

Then open the "Tools -> Accounts" menu option:



Comptes Int	ternet			? ×
Tout C	ourrier Servi	ce d'annuaire		<u>Ajouter</u>
Compte		Туре	Connexion	Supprimer
)iapason] Publication	Courrier (par défaut) Courrier	Réseau local Réseau local	<u>P</u> ropriétés
				Par dé <u>f</u> aut
				Importer
				Exporter
				Définir l'ordre
				Fermer

In the "Email" tab, select your RTE communications account, then click on the "By default" button, and finally click on the "Close" button,

On the other hand, if the Outlook installation is of the "Company or workgroup" type" as below:

À propos de	Microsoft Outlook	? ×		
	Microsoft® Outlook® 2000 SR-(9.0.0.3821) Société ou groupe de travail Copyright © 1995-1999 Microsoft Corp. Tous dro Import/Export Converters © 1988-1999 DataViz, (203) 268-0300 Tous droite récervés Dictionnaire	its réservés. Inc. à www.dataviz.com ou		
	orthographique © 1994-98 SYNAPSE Développem droits réservés. Portions of International Correct? system © 1993 by Lernout & Hauspie Speech Pro Deutsche Rechtschreibprüfung: © Lingsoft, Inc. 1 Xerox Corporation 1994. Alle Rechte vorbehalten Polderland Language & Speech Technology. Alle r Gebaseerd op de officiële Woordenlijst Nederland Taalunie/Instituut voor Nederlandse Lexicologie/S checker developed by COLTEC Consultancy Group Licence d'utilisation accordée à :	set venificated ient, Toulouse (France). Tous 5pell™ spelling correction ducts N.V. All rights reserved. 1998. Two-Level Compiler: © . Spelling ©1996-1997. echten voorbehouden. se taal, © Nederlandse idu Uitgevers. Arabic spelling o, Egypt.		
	Planchephi GRT Product ID: 34503-OEM-0099665-66611			
Avertissemer d'auteur et pa distribution pa soit, est stricte dispositions se sanctions pén	it : Ce logiciel est protégé par la loi relative au droit ir les conventions internationales. Toute reproduction ou irtielle ou totale du logiciel, par quelque moyen que ce ement interdite. Toute personne ne respectant pas ces e rendra coupable du délit de contrefaçon et des ales prévues par la loi.	OK Infos système Support technique Informations de sécurité		

You do not need to do anything more in particular at the account level.



Concerning all types of Outlook installations.

Still from within Outlook, start the "Tools > Options..." menu:

	électronique	sécurisé — ter le content	u des messages e	t des pièces ioint	es pour les messa	des sortants
X	Ajoute	r la signature	numérique au me	essage sortant		
	Envoy	er un messag	e en <u>t</u> exte clair si	gné lors de l'envoi	i de messages sigi	nés
	Paramètre	s par dé <u>f</u> aut	:		7	Paramètres
Protéger	le contenu					
Protéger	le contenu Les zones contenus	de sécurité vi dans des mes	ous permettent d sages HTML. Séle	e personnaliser l'a ctionnez la zone c	ictivation ou non (le sécurité Intern	de scripts ou de et Explorer à
Protéger	Les zones contenus utiliser. Zon <u>e</u> :	de sécurité vo dans des mes:	ous permettent d sages HTML, Séle	e personnaliser l'a ctionnez la zone d	ictivation ou non (le sécurité Intern Paramètre	de scripts ou de et Explorer à es de la zo <u>n</u> e
Protéger	r le contenu Les zones contenus utiliser. Zon <u>e</u> :	de sécurité v dans des mes Internet	ous permettent d sages HTML, Séle	e personnaliser l'a ctionnez la zone o v	ictivation ou non (le sécurité Intern Paramètre Sécurité des	de scripts ou de et Explorer à es de la zo <u>n</u> e… s pièces jointes…
Protéger	le contenu Les zones contenus utiliser. Zon <u>e</u> :	de sécurité v. dans des mes Internet iques (certific	ous permettent d sages HTML. Séle ats) —————————————————————	e personnaliser l'a ctionnez la zone o v	ictivation ou non (le sécurité Intern Paramètre <u>S</u> écurité des	de scripts ou de et Explorer à es de la zo <u>n</u> e s pièces jointes
Protéger	le contenu Les zones contenus utiliser. Zon <u>e</u> : Zon <u>e</u> : Les identif prouver v	de sécurité vi dans des mes Internet iques (certific ications numé otre identité c	ous permettent d sages HTML. Séle ats) riques ou les cert lans les transactio	e personnaliser l'a ctionnez la zone d	ictivation ou non d le sécurité Intern Paramètre Sécurité des ocuments qui vous	de scripts ou de et Explorer à es de la zo <u>n</u> e s pièces jointes s permettent de

Select the "Security" tab, then click on the "Parameters..." button:

Changer les paramètres de sécurité	×
Préférences des paramètres de sécurité	
Nom des paramètres de sécurité : Mes paramètres S/MIME (client1.services@s	-
Eormat de message sécurisé :	
Paramètre de sécurité par défaut pour ce format de message sécurisé	-
Paramètre de sécurité par défaut pour tous les messages sécurisés	
Nouveau Supprimer Mot de passe.	
Certificats et algorithmes	
Certificat de signature : Utilisateur TEST1 Choisir	
Alexikhere back :	-
Certificat de chiffrement : Utilisateur TEST1 Choisir	_ ←
Algorithme de chiffrement : 30ES	
Envoyer ces certificats avec les messages signés	
OK Annuler	

Version: 3



Access to the IT system with digital certificates under Microsoft Windows XP PKI user manual

Click on the two "Select..." buttons in order to select your certificate for signing and encryption from the list of selectable certificates that is presented to you (you can also display any certificate in the list to view its contents and assure yourself that you have chosen the right one). Finally, verify that the data is the same as that above (S/MIME, boxes checked, certificates, algorithms); if the "Name of the security parameters" field is empty, enter a name like "RTE Certification". At last, click on "OK". The following window will then be displayed:

Options ?X				
Préférences Remise du courrier Format du courrier Orthographe Sécurité Autre				
Courrier électronique sécurisé				
🖸 💽 🚾 Encrypter le contenu des messages et des pièces jointes pour les messages sortants				
Ajouter la signature numérique au message sortant 🛛 🛶 🔤 🔤				
Envoyer un message en <u>t</u> exte clair signé lors de l'envoi de messages signés				
Paramètres par défaut : Mes paramètres S/MIME (client1.services@se 💌 Paramètres				
Proteger le contenu				
Les zones de sécurité vous permettent de personnaliser l'activation ou non de scripts ou de contenus dans des messages HTML. Sélectionnez la zone de sécurité Internet Explorer à utiliser.				
Zon <u>e</u> : 😰 Internet 💽 💽 Paramètres de la zo <u>n</u> e				
Sécurité des pièces jointes				
Identifications numériques (certificats)				
Les identifications numériques ou les certificats sont des documents qui vous permettent de prouver votre identité dans les transactions électroniques.				
Importer/Exporter				
OK Annuler Appliquer				

Check the "Encrypt the contents of messages and attached documents for outgoing messages" and "Add the digital signature to outgoing messages" boxes and click on "OK".

All your emails destined for RTE applications sent from the default account will now be encrypted and signed.

6.1.2 User Guide

6.1.2.1 When to use the certificate

By using your certificate, you can:

- authenticate yourself to RTE applications;
- sign and encrypt emails destined for RTE applications;
- decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several



ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you recover their certificates.

To do this, when you receive a signed message, use the "Add to contacts" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Outlook does.

IMPORTANT NOTE

The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

6.1.2.2 Application certificates

Upon receiving the first signed and encrypted message from an application, you should install the sending application's certificate. To do so, you must add the application's email address to your address book by clicking on "Add to contacts" with the right mouse button when positioned over the sender's name of the message received:

🔀 REJ - Message (Texte brut)		
Eichier Edition Affichage Insertion	Forma <u>t</u> <u>O</u> utils Action <u>s</u> <u>?</u>	
Sev Répondre Sev Répondre à tous	📢 Transférer 🛛 🚑 🗎 🤻	' 📴 🗙 🔺 • 🔹 • 🔏 😰 🗸
De : RTE - DIAPASON [diapason@serv À : CLIENT1 Cc :	iros eta fespos com ¹ Propriétés Ajouter aux contacts eta Rechercher un contact	Date : lun. 03/05/2004 16:55
Sécurité : Signé & crypté	Couper Copier	₽ 6
Madame, Monsieur,	Coller Effacer	
Votre mail a bien été rec lun. 03/05/04 à 16:54.	Sélectionner tout	aux lettres RTE le

The "General" tab:

Etwegstrer et fermer 🗗 🗃 🕯 🔻	Ø 30	
Général Détails Activités Centifici	ets Champs	
Rest Non cogplet] RTE - DGAPASON Tage 1 Scogle 1 Gaster sous 1 CLAPASON, RTE -	Donacie Streau Télécopie (bureau)	
Adresse	Adresse de messagerie 🔔	dessenderrices 👖
C Adresse gostale	Page 2001	2

The "Certificates" tab:

ERTE - DIAPASON - Contact	
Echier Edition Affichage Insertion Format Qubis Actions 2	
📓 treegstrer et fenner 🛃 🗃 📋 🔻 🔣 🖓 + 🔺 + 🕈 +	
Général Détais Activités Certificats Champs	
In de ces certificats sera utilisé pour envoyer du courrier crypté à ce contact, lous pouver obtenir un certificat en recevant de ce contact du courrier signé numériquement ou en important un fichier de certificats de ce contact.	
Gertificats (Identifications numériques) :	-
ILTE-DUARASON(bar default)	Broprietofs
	Differ partition
	befor participat
	thifter partiting t Igporter Egporter

"Ctrl+S" to save.



6.1.2.3 Message encryption and signing

To encrypt and sign a message with Outlook, first create a new message by clicking on "New" (or Ctrl+N),

🔀 Objet - Message (Texte brut)	
Eichier Edition Affichage Insertion Format Outils Actions ?	
] 🖃 Envoyer 🗸 🔚 🐰 👫 💼 🚦 💺 🔻 🔝 Options 😰 🏹	• *
À diapason@services.rte-france.com	
<u></u>	
Objet : Objet	
Contenu	<u>_</u>
	-

To verify the security parameters, click on the "**Options...**" button.

In Outlook 2000 with XP, verify that the "Encrypt the contents of messages and attached documents" and "Add the digital signature to outgoing messages" boxes have been checked by default.

Options des messages	<u>? ×</u>
Paramètres Sécurité	
Importance : Normale 🔽 😥 Krypter le contenu et le	es pièces jointes du message
Critère de diffusion : Normal	nerique au message sortant
Options d'envoi	
Envoyer les réponses à :	Sélectionner des noms
Enregistrer le message envoyé dans : Éléments envoyés	Parcourir
Ne pas envoyer avant :	
Expire après :	
Envoyer le message en utilisant : RTE Diapason	
Options de suivi	
Demander une confirmation de lecture pour ce message	
<u>Contacts</u>	
Catégories	
	Fermer



In Outlook 2003, click on the "Security parameters"" button, then verify that the "Encrypt the contents of messages and attached documents" and "Add the digital signature to outgoing messages" boxes have been checked by default.

Options des messages		×
Paramètres	Sécurité	
Importance : Normale	Modifier les paramètres de sécurité pour ce messa Paramètres de sécurité	ige.
Options de vote et de suivi		
Utiliser les boutons de vote : Demander un accusé de réception pour Demander une confirmation de lecture p	ce message pour ce message	×
Options de remise		
Envoyer les réponses à :		Sélectionner des noms
Enregistrer le message envoyé dans :	Éléments envoyés	Parcourir
🔲 Ne pas envoyer avant :	Néant 🗸 00:00	
🔲 Expire après :	Néant 🗸 00:00	
Format des pièces jointes :	Par défaut	
Codage :	Sélection automatique	
Contacts		
Catégories		
		Fermer

Propriétés de séc	urité	×
Crypter le cont Ajouter une sig Envoyer le Demander Paramètres de séc	renu et les pièces jointes du message gnature numérique au message e message en clair signé r un accusé S/MIME pour ce message urité	
Paramètre de sécurité :	<automatique> Modifier les paramètres</automatique>	
Étiquette de sécu Module de stratégie : Classification : Marque de confidentialité ;	urité Configurer	
	OK Annuler	_



6.2 Outlook Express

6.2.1 Configuration



To associate your certificate with your email account under Outlook Express, your certificate must be installed under Internet Explorer. This is automatically the case if you have downloaded it in Internet Explorer; but

if you downloaded it with Mozilla Firefox, you must export it from that browser and import it into Internet Explorer, with the corresponding private key and the RTE CA root certificate. Refer to the section at the end of this document.

Outlook Express automatically associates an account with the certificate carrying the same email address in order to sign messages.

To configure Outlook Express, start the "Tools > Accounts..." menu option and select the "Email" tab:

Comptes Internet				
Tout Courrier New	vs Service d'annuaire	L .	Ajouter	
Compte	Туре	Connexion	Supprimer	
RTE Diapason	Courrier (par défaut) Courrier	Disponible Disponible	Propriétés	
-			Par dé <u>f</u> aut	
			Importer	
			Exporter	
			Définir l'ordre	
			Eermer	
			renner	



Select your RTE communications account and click on "Properties":

😤 Propriétés de RTE Diapason	? X	
Général Serveurs Connexion Sécurité Avancé		
Certificat de signature		
Sélectionnez le certificat de signature ci-dessous. Il sert à déterminer l'identificateur numérique utilisé lors de la signature des messages en utilisant ce compte.		
Certificat : Utilisateur TEST1 Sélectionner		
Préférences de cryptage		
Sélectionnez le certificat et l'algorithme de cryptage. Ils sont inclus dans vos messages signés numériquement de façon à ce que d'autres personnes puissent vous envoyer des courriers cryptés selon ces paramètres.		
C <u>e</u> rtificat : Utilisateur TEST1 Sélectionner		
Algorithme : 3DES		
(ÖK Annuler App	liquer	

Then click on the "Security" tab, and use the two "Select..." buttons to select your certificate for signing and encryption. Then click on "OK".

Still from within Outlook Express, start the "Tools > Options..." menu:

General	Lecture	 Confirmations de lect 	ure Envois	Message	Signatures
Orth	nographe	Sécurité	Connexion	Mair	ntenance
Protection	antivirus ———				
	Sélectionnez la zone de sécurité Internet Explorer à utiliser :				
I	🗹 <u>M</u> 'avertir lorsq	ue d'autres applications ess	aient d'envoyer des mé	essages électroniq	ues de ma pa
I	Ne pas autoris virus.	er l'ouverture ou l'enregistre	ement des pièces jointe	es susceptibles de (contenir un
Courrier sé	écurisé ———				
On !	Les identificateurs	numériques (appelées aus	si certificats) sont des -	<u>E</u> n savoi	ir plus
	transactions électi	roniques.		<u>I</u> dentificateurs	numériques
l	Pour signer électroniquement des messages ou recevoir des messages cryptés, vous devez avoir un identificateur numérique.				
→ İ	Crypter le con	tenu et les pièces jointes de	e tous les messages so	tants	
→ I	🔽 Signer <u>n</u> umérie	quement tous les messages	sortants		
				Auan	cá

Select the "Security" tab, check the two checkboxes labelled "Encrypt the contents of messages and attached documents for outgoing messages"



and "**Digitally sign all outgoing messages**", and then click on the "Advanced" button:

Paramè	tres de sécurité avancés	? ×
Messag	ges cryptés	_
മ	Avertir lors du <u>c</u> ryptage de messages à un niveau inférieur à :	
	128 bits	
	▼ Toujours crypter <u>m</u> a copie lors de l'envoi de courrier crypté	
Messag	jes signés numériquement	
_	Inclure l'identificateur numérique lors de l'envoi de messages sign	iés
	Coder le message avant de le signer (signature opaque)	
F	Ajouter le certificat des expéditeurs au Carnet d'adresses	
Vérificati	ion de révocation	
	Vérifier les identificateurs numériques révoqués :	
<u></u>	◯ <u>U</u> niquement en ligne	
	💿 Jamais	
	OK Annuler	

Verify that the configuration is identical to that above; please specifically check the two boxes labelled "Include the digital identification when sending messages" and "Add the certificate of senders to the address book" have been checked; then click on "OK".

All your emails destined for RTE applications and sent from this account will now be encrypted and signed.



6.2.2 User Guide

6.2.2.1 When to use the certificate

By using your certificate, you can:

- authenticate yourself to RTE applications;
- sign and encrypt emails destined for RTE applications;
- decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you obtain a copy of their certificates.

To do this, when you receive a signed message, use the "Add to contacts" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Outlook 2000 does.

IMPORTANT NOTE

The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

6.2.2.2 Application certificates

Upon receiving the first signed and encrypted message from an application, you should install the sending application's certificate. To do so, you must add the application's email address to your address book by clicking on "Add to the address book" with the right mouse button when positioned over the sender's name of the message received:

🙈 REJ		
Fichier Edition Affichag	e Outils Message ?	.
Répondre Répondre	VS Imprimer X Imprimer Y Transférer Imprimer Supprimer Précédent Suivant	M Adresses
De: <u>RTE - DIAPASO</u> Date: lundi 3 mai 2004 À: CLIENT1 Objet: REJ Sécurité: Signé numérique	Ajouter au Carnet d'adresses Rechercher Bloquer l'expéditeur Copier	유 8
Madame, Monsieur, Votre mail a bien été re	Propriétés çu sur notre boîte aux lettres RTE le lun. 03/05/04 à 17:41.	×

The "Summary" tab:

The "Digital identifiers" tab:

Copyright RTE. This document is the property of RTE. All communication, reproduction or publication, even partial, is prohibited without written authorisation from the Electricity Transport Network Operator (RTE)



opriétés de RTE - DIAPAS	ion	<u>. 1</u> 13
Résumé Nom Domicile	Buresu Personnel Autre NetMeeting Identific nations sur ce contact	ateurs numériques
Nom :	RTE - DIAPASON	
Adresse de	dapason@services.ite-france.com	
Téléphone personnel :		
Radomessagerie :		
Téléphone mobile :		
Page Web (domicile) :		
Téléphone professionnel		
Télécopie professionnelle :		
Ttre :		
Service :		
Bureau :		
Nom de la société :		
Page Web (bureau) :		
		K Arnuler



Click on the "OK" button to validate.

6.2.2.3 Message encryption and signing

To encrypt and sign a message with Outlook Express, first create a new message by clicking on "New" (or Ctrl+N),

👔 Objet									
Fichier	Edition	Affichage	Insertion	Format	Outils	Message	?		- 2
		X			Orth	ographe		F7	»
Envoye	r	Couper	Copier	Coller	Dem	ander une co	nfirmation de le	cture	
Dev	-track d				Vérif	er les noms		Ctrl+K	
De.		services@ser	vices.rte-rra	nce.com	Sélec	tionner les d	estinataires		A
🔮 À :	diapaso	n@services.r	te-france.co	m	Carn	et d'adresses	s	Ctrl+Maj+B	- ₿←
🛐 Co :					- Cryp	or			-
Objet :	Objet				 Siane 	r numériaue	ment		
					Dem	ander un reçi	u de sécurité		
Arial IIII E G I E A SA A F F F E E E E E SA *									
Contenu	Contenu 🔽								
Contient des	Contient des commandes utiles lors de l'utilisation des courriers et des news.								

Verify that the two boxes "Encrypt" and "Sign digitally" have been checked,



6.3 Mozilla Thunderbird

6.3.1 Configuration



To be able to associate your certificate with your email account

under Mozilla Thunderbird, your certificate must be installed under Mozilla Thunderbird. To do this, you must export it from the browser that you installed it into, and import it into Mozilla Thunderbird, with the corresponding private key and the RTE CA root certificate. Refer to the section at the end of this document.

Start Mozilla Thunderbird, and open the "**Tools > Account parameters...**" menu, then select the "**Security**" item of the RTE communications accounts (e.g. "Client RTE 1"):

amètres des comptes		
Client RTE Paramètres serveur Copies et dossiers Rédaction et adressage Espace disque Accusés de réception Sécurité Dossiers locaux Espace disque Serveur sortant (SMTP)	Sécurité Pour envoyer et recevoir des messages signés ou chiffrés, il a certificat de signature numérique et un certificat de chiffreme. Signature Certificat personnel pour signer numériquement les message Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE Image: Signer les messages numériquement Chiffrement Certificat personnel pour chiffrer et déchiffrer les message Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE Utiliser le chiffrement pour chiffrer et déchiffrer les messages : Image: Damais Toujours chiffrer les messages Certificats Afficher les certificats Lériphériques de sécurité	est nécessaire de spécifier à la fois un int. jes envoyés : Sélectionner un certificat Effacer s envoyés : Sélectionner un certificat Effacer
Ajouter un compte		
Compte par dé <u>f</u> aut		

Click on "Select a certificate" to select (see above) your certificate for signing and encryption. Then check the two boxes labelled "Sign messages digitally" and "Always encrypt messages", then click on "OK".



Sélection d'u	ın certificat	x
Certificat : Détails du c	Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID [39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:B0:C0:21] ertificat sélectionné :	•
Émis pour : Numéro d Valide de Sujets: Cl Émis par : (Stocké dan	E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft ID,O=TEST,C=FR e série: 39:2D:6B:2A:16:28:90:33:D3:DE:86:49:0B:80:C0:21 28/10/2005 02:00:00 pour 29/10/2007 00:59:59 ient,Signature,Chiffrement ZN=RTE Autorite de Certification,O=RESEAU DE TRANSPORT D ELECTRICITE s : Sécurité personnelle	
	OK Annule	,

All your emails destined for RTE applications sent from this account will now be encrypted and signed.

6.3.2 User Guide

6.3.2.1 When to use the certificate

By using your certificate, you can:

- authenticate yourself to RTE applications;
- sign and encrypt emails destined for RTE applications;
- decrypt electronic messages that have been sent to you by RTE applications.

The encryption and signature of a message are two distinct processes: you sign a message with your own certificate whereas you encrypt it with the recipient's certificate. The recipient's certificate can be obtained in several ways. The RTE applications send you their certificates by sending you a signed message: this is the way that you obtain a copy of their certificates.

To do this, when you receive a signed message, use the "Add to contacts" function to save its certificate as you read it, and you can then use it later to send the application encrypted messages.

The decryption of a message is done in an automatic manner when you already have the email sender's certificate and if you open that message with a message client that supports S/MIME format secured messages, which Mozilla Thunderbird does.

IMPORTANT NOTE

The encryption of a message is dependent on the possession of a valid certificate corresponding to the recipient's email address.

6.3.2.2 Application certificates

The installation of an application certificate is done automatically when the first email signed and encrypted sent by that application is read.



Nevertheless, you can add the application's email address to your address book by clicking on "Add this address to the address book".

💐 Courrier entrant pour client	.rte@services.rte-france.com - Thunderbird		_ 0	×
Eichier Edition Affighage Al	lerà <u>M</u> essages Ou <u>t</u> ils Ai <u>d</u> e			
Relever Écrire Adresses	Répondre Rép. à tous Transférer Supprimer Indésirable			0
Dossiers	Voir : Tous	,		
🗉 🥔 Client RTE	🗨 🕖 Sujet 😽 Expéditeur	0	Date 🛆	EŞ.
Courrier entrant (3)	🔀 RTE - Ouverture de service (hotline : 01 58 79 50 50) 🔹 RTE - ENVOI-NEB-SITES-RPD	• 1	7:30	
Brouillons	🖄 RTE - Ouverture de service (hotline : 01 58 79 50 50) 🔹 RTE - REFERENTIEL GRD	· 1	7:30	
-La Modèles	🖄 RTE - Ouverture de service (hotline : 01 58 79 50 50) 🔹 RTE - DIAPASON TEST	• 1	7:29	
Envoyés	RTE - Ouverture de service (hotline : 01 58 79 50 50) • RTE - DIAPASON	• 1	7:29	
Corbeille	RTE - Ouverture de service (hotline : 01 58 79 50 50) • RTE - PUBLICATION	· 1	7:29	
🛿 🥪 Dossiers locaux	RTE - Confirmation de prise de rendez-vous	• 1	7:27	
Messages en attente	RTE - Accusé de réception de dossier d'inscription RTE Hotline 	• 1	7:24	
Brouillons				
Envoyes	Sujet : RTE - Ouverture de service (hotline : 01 58 79 50 50)			<u>^</u>
Corbelle	De: RTE - DIAPASON <diapason@services.rte-france.com></diapason@services.rte-france.com>		. 6	
	Date: 17:29 diapason@services.rte-france.com		6	5
	Pour : client.rte@services.rte-france.com Ajouter l'adresse au carnet d'adresse	es .	1	
	Envoyer un courrier à	5		_
	Madame, Monsieur, Copier l'adresse			
	Pour accéder au service DIARASON veuillez Crégunfiltre			
	message au carnet d'adresses de votre client de messagerie.			
	Cette procédure est décrite au chapitre 5 du Manuel Utilisateur PKI auquel vous pouvez vous reporter (voir sur le CD-ROM d'installation)			
	En cas de difficulté, n'hésitez pas à contacter la Hotline RTE (tél. Ol 58 79 50 50, jours ouvrés de 9h à 18h), qui saura vous assister.	. :		
	Cordialement,			
	 Service DIAPASON			
2	Non lus : 3	3 T	otal : 7	
0				14

Whenever you see the window "New file for [RTE - DIAPASON]" appearing, just click on "OK".

To verify that the application certificate (e.g. "RTE - DIAPASON") is correctly installed, open the "Tools > Options..." menu, select the "Confidentiality" section and the "Security" tab, then click on "View the certificates" and finally click on the "Other people" tab.

🥞 Gestionnaire de certifica	Gestionnaire de certificats				
Vos certificats Autres pers Vous possédez des certific	onnes Sites Web Autorités ats enregistrés identifiant ces p	ersonnes :			
Nom du certificat	Sujets	Adresse électronique	E.		
E RESEAU DE TRANSP					
RTE-DIAPASON	Client, Signature, Chiffrement	diapason@services.rte-france.com			
RTE-PUBLICATION	Client, Signature, Chiffrement	publication-comptage@services.rte-france.com	י		
Voir Modifie	r Importer Suppr	imer			
			ОК		

6.3.2.3 Message encryption and signing

To encrypt and sign a message with Mozilla Thunderbird, first create a new message by clicking on "Write" (or Ctrl+M),



Click on the "Security" button to make sure the two options "**Encrypt this message**" and "**Digitally sign this message**" have been selected (these options ought to be selected by default).

🥳 Réda	ction : Su	ıjet						<u> </u>
Eichier	<u>E</u> dition	Affi <u>c</u> hage	Options	<u>O</u> utils	Ai <u>d</u> e	s de la companya de l		
Envoyer	Con	J tacts O	ABC rthographe	÷.	Ooindre -	Sécurité 📐	Enregistrer	
Expédite	ur : Cli	ent RTE <cli< td=""><td>ent.rte@ser</td><td>vices.rt</td><td>e-france.c</td><td>Ne <u>p</u>as chift • Chiff<u>r</u>er ce</td><td>frer ce message message</td><td></td></cli<>	ent.rte@ser	vices.rt	e-france.c	Ne <u>p</u> as chift • Chiff <u>r</u> er ce	frer ce message message	
H	Pour	: 🛃 RIE- : 🔝	DIAPASON	IESI <	alapason-	✓ Signer num	ériquement ce message	
<u> </u>	, oai					Voir les info	rmations de sécurité	
<u>S</u> ujet :	Sujet							
Conte	Contenu							
]]	🖉 🌽 //,
								††

6.4 Lotus Notes

Please refer to the document titled: "PKI User Manual - digital certificates - Windows XP Notes".



7. SSL VPN

7.1 Foreword

Connection via SSL VPN is a service which offers the establishment of a secured communications channel to RTE FrontOffice through the Internet. This channel is established after authentication of your certificate with a dedicated site.

The use of SSL VPN requires the installation of a special tool which is installed during your first connection to the site. This application is called **Windows Secure Application Manager** (WSAM).

The SSL VPN makes it possible to access email folders hosted in RTE FrontOffice.

The connection URL for the SSL VPN is:

https://secure.iservices.rte-france.com

7.2 Initial configuration

7.2.1 Prerequisites

Even before making your first connection, you must have:

- configured your workstation (§2),
- configured your browser and retrieved your certificate:
 - o §5 for Mozilla Firefox (max version: 2.0.0.14),
 - §3 for Internet Explorer 6,
 - §4 for Internet Explorer 7,

You must also verify that your workstation is able to resolve and access the address: **secure.iservices.rte-france.com**. To do this, open your Start menu and click on Run. In the window that appears, enter this command:

cmd /k ping secure.iservices.rte-france.com

	Entrez le nom d'un programme, dossier, document ou d'une ressource Internet, et Windows l'ouvrira pour vous.
Ouvrir :	cmd /k ping secure.iservices.rte-france.com
	OK Annuler Parcourir

Click on the "**OK**" button.

A window will appear containing some information:

• If the first line starts with "Sending a ping request to secure.iservices.rte-france.com", then the address



secure.iservices.rte-france.com has been resolved. Your workstation is correctly configured.

• If the first line starts with "The ping request could not locate the server secure.iservices.rte-france.com", then the address secure.iservices.rte-france.com has not been resolved. Please contact your IT support desk so that they can make the necessary changes to enable the ping/address resolution.

IMPORTANT

For your first connection, you must have an account with administrative rights so that the WSAM application installation can be made.

7.2.2 First connection

7.2.2.1 Internet Explorer

Start your browser and enter the following URL:

https://secure.iservices.rte-france.com

This window will be displayed:

	Authentification du client
	Identification Le site Web que vous voulez visiter requiert une identification. Sélectionnez le certificat à utiliser pour vous connecter.
→	Client RTE 2
	<u>Plus d'infos</u> Affic <u>h</u> er le certificat
	OK Annuler

Select your certificate, then click on the "OK" button.

If necessary, this window will ask you for the store password for your certificate.



Copyright RTE. This document is the property of RTE. All communication, reproduction or publication, even partial, is prohibited without written authorisation from the Electricity Transport Network Operator (RTE)



Then the WSAM application installation will start:

RTE		
Veuillez patienter		
Lancement de Secure Application Manager.	L'opération peut demander plusieurs minutes.	
Installati	on	[
	Téléchargement de l'application. Patientez	
	Téléchargement de 131056 sur 792000	
Si une erreur ne permet pas le chargeme • <u>vérifier la compatibilité de votre systèn</u> • <u>poursuivre</u> . Il est possible que toutes le	Annuler	

Please be patient through the entire installation procedure.

If your Internet access requires authentication with a proxy, a window will appear asking you for your connection identification credentials. Enter them and validate.

Once the installation has completed, the following page will be displayed:

RTE			Déconnexion
		Page d accuell	Deconnexion
	Bienvenue dans l'espace sécurisé RTE - Accès Messagerie Espace sécurisé RTE.		
	Signets Web	Þ	
	Sessions des applications clientes	-	
	A Windows Secure Application Manager	émarrer	

Finally, the 🚵 icon will appear in your task bar,

Click on the **Disconnect** button (on the top right of the page) to terminate the session:







7.2.2.2 Mozilla Firefox

Start your browser and enter the following URL:

https://secure.iservices.rte-france.com

This window will be displayed:

	mande que vous vous identifiiez avec un certificat de sécurité :			
portail.serv	ices.rte-france.com			
Organisation : « RTE »				
Émis sous :	« RSA Data Security, Inc. »			
Choicir u	cartificat à présenter comme identification :			
Client RTI	1's RESEAU DE TRANSPORT DEI ECTRICITE ID [39:20:68:24:16:28:90:33:D3:DE:86:49:08:80:C0:21]			
Détails du	ertificat sélectionné :			
Émis pour	E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft			
ID,O=TES Numérou	,C=FR e série: 39:2D:6B:2∆:16:28:9D:33:D3:DE:B6:49:0B:80:C0:21			
Valide de	28/10/2005 02:00:00 pour 29/10/2007 00:59:59			
Sujets: C	ent, Signature, Chiffrement			
Emis par :	INERTE Autorité de Certification, OERESEAU DE TRANSPORT D'ELECTRICITE s : Sécurité dersonnelle			
Stocké da				
Stocké da				

Select your certificate from the dropdown list labelled "Choose a certificate to present as identification" and click on "OK". If necessary, this window will ask you for the password to the Mozilla Firefox certificate store.

Invite	×
i	Veuillez saisir le mot de passe principal de Sécurité personnelle.

	OK Annuler

Then the following page will be displayed:

	1	
	Page d'accueil	Déconnexion
Bienvenue dans l'espace sécurisé RTE - Accès Messagerie Espace sécurisé RTE.		
Signets Web		
Sessions des applications clientes	-	
🐴 Windows Secure Application Manager	Démarrer	

Click on the "Start" button to commence the installation.



If this window below appears, just click on Yes.



Please be patient through the entire installation procedure:

Création du dossier : C:\Documents and Sett	ings\All Users\Start Menu\Proç
Extraction : dsWinClentResource_E5.dl 100% Extraction : dsWinClentResource_F1.dl 100% Extraction : dsWinClentResource_J7.dl 100% Extraction : dsWinClentResource_J7.dl 100% Extraction : dsWinClentResource_J7.dl 100% Extraction : dsWinClentResource_J7.dl 100% Extraction : estranginfi.nl 100% Extraction : semspi.dl 100% Extraction : estranginfi.nl 100% Crédetion du dosein : c.(3)Program Files/Jun Crédetion du dosein : c.(3)Program Files/Jun	% s(Secure Application Ma iper Networks(Secure

If your Internet access requires authentication with a proxy, a window will appear asking you for your connection identification credentials. Enter them and validate.

Once the installation has finished, the welcome page will be shown again:



In addition, the 🚨 icon will appear in your task bar,



Click on the **Disconnect** button (on the top right of the page) to terminate the session:



Bienvenue dans l'espace sécurisé RTE Espace Sécurisé RTE

Votre session est terminée.

7.3 User Guide

7.3.1 Establishing a connection

7.3.1.1 Internet Explorer

Start your browser and enter the following URL:

https://secure.iservices.rte-france.com

This window will be displayed:

Authentification du client
Identification Le site Web que vous voulez visiter requiert une identification. Sélectionnez le certificat à utiliser pour vous connecter.
 Client RTE 2
<u>Plus d'infos</u> <u>Afficher le certificat</u>
OK Annuler

Select your certificate, then click on the "**OK**" button.

If necessary, this window will ask you for the store password for your certificate.



Copyright RTE. This document is the property of RTE. All communication, reproduction or publication, even partial, is prohibited without written authorisation from the Electricity Transport Network Operator (RTE)


The WSAM application automatically starts and the following page is displayed:

Page d'accueil	Déconnexion
Þ	
-	
Démarrer	
	Þ Démarrer

In addition, the 🚨 icon will appear in your task bar,

Notes:

- The certificate is only used to establish the SSL VPN connection.
- To close the SSL VPN session, click on the Disconnect button (on the top right of the page).





7.3.1.2 Mozilla Firefox

Start your browser and enter the following URL:

https://secure.iservices.rte-france.com

This window will be displayed:

	mande que vous vous identifiiez avec un certificat de sécurité :
portail.serv	ices.rte-france.com
Organisati	n : « RTE »
Émis sous :	« RSA Data Security, Inc. »
Choicir u	cartificat à présenter comme identification :
Client RTI	1's RESEAU DE TRANSPORT DEI ECTRICITE ID [39:20:68:24:16:28:90:33:D3:DE:86:49:08:80:C0:21]
Détails du	ertificat sélectionné :
Émis pour	E=client.rte@services.rte-france.com,CN=Client RTE 1,OU=ISO 6523 - 0000 0000,OU=Soft
ID,O=TES Numérou	,C=FR e série: 39:2D:6B:2∆:16:28:9D:33:D3:DE:B6:49:0B:80:C0:21
Valide de	28/10/2005 02:00:00 pour 29/10/2007 00:59:59
Sujets: C	ent, Signature, Chiffrement
Emis par :	INERTE Autorité de Certification, OERESEAU DE TRANSPORT D'ELECTRICITE s : Sécurité dersonnelle
Stocké da	
Stocké da	

Select your certificate from the dropdown list labelled "Choose a certificate to present as identification" and click on "OK". If necessary, this window will ask you for the password to the Mozilla Firefox certificate store.

Invite	×
j	Veuillez saisir le mot de passe principal de Sécurité personnelle.

	OK Annuler

Then the following page will be displayed:

	1	
	Page d'accueil	Déconnexion
Bienvenue dans l'espace sécurisé RTE - Accès Messagerie Espace sécurisé RTE.		
Signets Web		
Sessions des applications clientes	-	
🐴 Windows Secure Application Manager	Démarrer	

Click on the "Start" button to start the WSAM application.



If this window below appears, just click on **Yes**.

Avertis	sement - Sécurité
0	Acceptez-vous le certificat du site Web "secure iservices rte-france.com" en vue d'un échange d'informations cryptées ?
	Authenticité de l'éditeur vérifiée par "VeriSign, Inc."
	Le certificat de sécurité a été émis par une société qui n'est pas digne de confiance.
	Le certificat de sécurité n'a pas expiré et est encore valide.
	Attention : "secure iservices rte-france.com" atteste que ce contenu est sûr. Vous ne devriez accepter ce contenu que si vous estimez que "secure iservices ite-france.com" est digne de conflance.
	<u>P</u> lus de défails
	Qui Non Toujours

If your Internet access is protected by a proxy, a window will appear asking you for your connection identification credentials. Enter them and validate.

Once the application has started, the 🚵 icon will display in your task bar.

Notes:

- The certificate is only used to establish the SSL VPN connection.
- To close the SSL VPN session, click on the Disconnect button (on the top right of the page).

7.3.2 Using SSL VPN to access hosted email folders

SSL VPN can be used to access email folders hosted in FrontOffice with the use of a standard email client.

Access to the hosted email folders requires that the SSL VPN connection has been established (see §7.3.1).

The configuration of the email account in your email client software is made in the normal fashion with the following parameters:

- Email server type: POP server
- POP server address: pop.services.rte-france.com
- SMTP server address: smtp.services.rte-france.com

When your access to RTE FrontOffice is supplied to you, you will receive your login identifier, your password and your email address.

NOTE

Given that the messages are being forwarded through a secure channel, the sending and receipt of emails does not require the use of a certificate for message encryption.



8. Renewal of certificates

Certificates have a validity of two years so that a high level of security can be delivered with them.

Forty days before the expiry of a certificate, an electronic message is sent to the certificate holder to inform him of the renewal of his digital certificate.

If modifications need to be made relating to the certificate holder's details, then the certificate holder's representative contacts the RTE customer relations officer to tell him what those changes are.

Otherwise an email is sent to the certificate holder with the information necessary for the retrieval of his new certificate.



9. Revocation of certificates

9.1 The revocation scenario

The customer must issue a revocation request whenever one of the following circumstances arises:

- change of the certificate holder;
- loss, theft, compromise, or suspicion of possible, probable or certain compromise of the private key associated with the holder's certificate;
- death or discontinuation of employment of the certificate holder;
- loss of the activation data, or defective or lost removable media.

9.2 The revocation request

To revoke your certificate, you should call the RTE Hotline and supply your **PKI User Authentication**, such as was provided in the forms for requesting access to the RTE IT systems.



10. Incident handling and support

In the event of a problem, the customer contacts the RTE Hotline (see §10.2), who will diagnose the problem and forward it to the corresponding technical expert concerned. The Hotline will forward the solution to the customer and assist them where necessary to apply the procedures indicated to regain access to the RTE IT systems.

10.1 Error codes returned by email

During an exchange of electronic messages. it is possible that a functionality error may occur. In such events, the component (e.g. a server, a router) in question returns an error code by email.

The subjects of the error messages returned by the cryptographic router are of the form:

<err:nnn!!<fr< th=""><th>Description>!!<en< th=""><th>Description>></th><th><subject-of-the-< th=""></subject-of-the-<></th></en<></th></err:nnn!!<fr<>	Description>!! <en< th=""><th>Description>></th><th><subject-of-the-< th=""></subject-of-the-<></th></en<>	Description>>	<subject-of-the-< th=""></subject-of-the-<>
	original-	message>	

nnn	Description	Possible cause
001	The email sent by the customer has not been signed nor encrypted	You have not checked the signing and encrypting boxes in your email software when you sent the email
002	The email sent by the customer has only been encrypted	You did not check the signing box in your email software
003	The email sent by the customer has only been signed	You did not check the encrypt box in your email software
004	The email sent by the customer has only been signed and the signature used is incorrect	You did not check the encrypt box in your email software and the certificate that you used to sign the message is invalid or unknown
005	The email sent by the customer has been signed and encrypted, but the signature used is incorrect	The signature certificate that you used is invalid or unknown
006	The email sent by the customer could not be decrypted by RTE	That certificate that you used to encrypt the email is invalid
007	The email sent by RTE did not reach the customer because of a security problem	This is an internal RTE problem





<fr-description></fr-description>	Description of the error in French.
<en-description></en-description>	Description of the error in English.
<subject-of-the-original-message></subject-of-the-original-message>	The subject header of the original message that caused the error in question.

10.2 Support

For any information or assistance, the customer can contact the RTE Hotline at:

+800 80 50 50 50

or from within France at:

01 55 69 79 52



11. Appendix A – Importing and exporting certificates

The export of your digital certificate, from the navigator under which you downloaded it, with the associated private key and the RTE CA root certificate, constitutes a backup of these elements. The result will be a file in the PKCS*12 standard format, that you will be asked to protect with a password, and that will be required to be put on a removable media and stored in a physically protected location.

This PKCS#12 file can then be imported into the browser of your choice, or into Lotus Notes, in order to either change browser, email client or PC, or to restore your certificate, your key pair and the root certificate in the event of a disk *crash*.

IMPORTANT

When re-importing into Internet Explorer, do not check the checkbox labelled "Mark the key as being exportable", so that no one can later perform an export of your private key without your knowledge from this workstation.

11.1 Exporting a certificate under Mozilla Firefox

Under Mozilla Firefox, export of a certificate with the private key and the root certificate. Once finished, generation of a file in the PKCS#12 (.p12) format protected with a password.

From the **"Tools > Options...**" menu:

Op	otions						X
	1	•	(<u> </u>	No.	
	Général	Vie privée	Contenu	Onglets	Téléchargements	Avancé	
	Général N	1ises à jour	Sécurité				
	rotoco	les ———					
	🔽 Uti	iser SSL <u>2</u> .0			🔽 Utiliser SSL	<u>3</u> .0	
	🔽 Uti	iser TLS <u>1</u> .0					
	Certifica	ats —					
	Lorsqui	un site wed n	ecessite un c	ertiricat :	•	and faile	
		sel <u>e</u> ctionner i	un automatiq	uement (•	Me demander a ch	ague rois	
	Affich	er les certifica	ts Listes	; de révocati	on Vérification	Périphériques de sécurité	
	T						
							_
					ОК	Annuler Aide	1

Select "Advanced" > "Security", and click on "Display the certificates".



🕹 Gestionnaire de certificats	
Vos certificats Autres personnes Sites Web Autorités	
Nom du certificat Périphérique de Sujets Numéro de Expire le I RESEAU DE TR 	Ę
Client RTE 1 Sécurité personnelle Client, Signature, Chiffr 39:2D:6B:2A 29/10/2007	
Voir Exporter Tout exporter Importer Supprimer	
ОК	

Select your certificate and click on "Export".

Choose a location and a name for the generated file in the PKCS#12 (.p12) format:

Nom de fichier à	sauvegarder				<u>? ×</u>
Enregistrer <u>d</u> ans :	Certificats		- 🔾 💋	i 📂 🛄 -	
Mes documents					
récents					
Bureau					
6					
Mes documents					
					
Poste de travail					
S	<u> </u>				
Favoris réseau	Nom du fichier :	RTE_client.rte@servi	ces.rte-france.com	.p12 💌	Enregistrer
	Type:	Fichiers PKCS12		i	Annuler
	— ·	1			///

Click on the "Save" button.

If necessary, this window will ask you for the password to the Mozilla Firefox certificate store:

Invite	×
?	Veuillez saisir le mot de passe principal de Sécurité personnelle.

	OK Annuler



Access to the IT system with digital certificates
under Microsoft Windows XP
PKI user manual

	_
Choix d'un mot de passe de sauvegarde du certificat	×
Le mot de passe de sauvegarde du certificat que vous venez de définir protège le fichier de sauvegarde que vous allez créer. Vous devez donner le mot de passe pour commencer cette sauvegarde.	
Mot de passe de sauvegarde du certificat : *******	
Mot de passe de sauvegarde du certificat (encore) : *******	
Important : si vous avez oublié votre mot de passe de sécurité, vous ne pourrez plus importer cette sauvegarde plus tard. Veuillez le conserver en un lieu sûr.	
Mesure de la qualité du mot de passe :	
OK Annuler	

Enter a password to restrict access to the PKCS#12 (.p12) file, then click on "OK".

Alerte		×
<u>.</u>	Sauvegarde des certificats et clés privées réussie.	
	OK	

Your certificate, your private key, and the CA root certificate are exported to the generated file with the ".**p12**" extension.



11.2 Exporting a certificate under Internet Explorer (Windows)

Under Internet Explorer, export of a certificate with the private key and the root certificate. Once finished, generation of a file in the PKCS#12 (.p12) format protected with a password.

Under Internet Explorer, open up: "Tools > Internet options..." and click on the "Contents" tab, then on the "Certificates..." button:

Certificat <i>s</i>						? ×
Rôle prév <u>u</u> :	<	(Tout>				•
Personnel	Autres pers	onnes Auto	prités intermédiaire	es 🛛 Autorités pr	incipales de cor	ifiance
Délivré à	RTE 2	Délivré par RTE Autori	te de Certification	Date d'expira 01/11/2007	tion Nom.con <aucun)< th=""><th>vivial ></th></aucun)<>	vivial >
	1 [1			
Importer	Export	er	upprimer			<u>A</u> vancé
<pre></pre>	ertificat					
		۱. I			Af	fic <u>h</u> age
						Eermer

Select your certificate, then click on "Export...".

Assistant Exportation de certifi	icat	Assistant Exportation	ion de certificat	×
	Bienvenue I Cet Assistant vous aide à copier des certificats, des letes de certificats de contiance et des letes de révocation de cettificats depuis le magasin de certificates vers votre disque dur. Un certificat, émis par une Autorité de certification, est une confirmation de votre identité et contient des informations comersions réseau sécurisées. Le magasin de certificate et la acore système où les certificats vont conservés. Pour continuer, cliquez sur Suivant.	Exportation de l Vous pouvez c Les clés privée avec le certific Voulez-vous e: C Non, r	la clé privée choisir d'exporter la clé privée avec le certificat. es sont protégées par mot de passe. Pour pouvoir exporter la clé privée cat, vous devez entrer son mot de passe dans une des pages suivantes. exporter la clé privée avec le certificat ? exporter la clé privée ne pas exporter la clé privée	
	< Précédent Suivant > Annuler		< Précédent Suivant > Annuler	

Click on the "Next" button.

Select "Yes, export the private key", then click on the "Next" button.





Assistant Exportation de certificat	Assistant Exportation de certificat
Format de fichier d'exportation Les certificats peuvent être exportés sous plusieurs formats de fichier.	Mot de passe Pour maintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de passe.
Sélectionnez le format à utiliser :	Entrez et confirmez le mot de passe.
C Binaire codé DER X.509 (.cer)	Mot de passe :
C Codé à base 64 <u>X</u> .509 (.cer)	An and a second s
${f C}$ Standard de syntaxe de message cryptographique - Certificats PKC5 #7 (.p7b)	<u>⊂</u> onfirmer le mot de passe :
🔲 Indure tous les certificats dans le chemin d'accès de certification si possible	Academic and a second
Échange d'informations personnelles - PKCS #12 (.pfx)	
Inclure tous les certificats dans le chemin d'accès de certification si possible	
Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur)	
Supprimer la clé privée si l'exportation s'est terminée correctement	
< <u>Précédent</u> <u>Suivant</u> Annuler	< Précédent Suivant > Annuler

Select the first two checkboxes, then click Enter a password to restrict access to on the "Next" button.

the PKCS#12 (.p12) file, then click on "Next".

Assistant Exportation de certificat	×	Assistant Exportation de certificat
Fichier à exporter Spécifiez le nom du fichier à exporter Nom du fichier : C:\Certificats\RTE2_client.rte@services.rte-france.com.pfx Pargourir		Fin de l'Assistant Exportation de certificat Vous avez terminé correctement l'Assistant Exportation de certificat. Vous avez spécifié les paramètres suivants : Vous avez spécifié les paramètres suivants : Vous du fichier Exporter les clés Inclure tous les certificats dans le chemin d'accès de ce Format de fichier
< Précédent Suivant > Annuler		< <u>P</u> récédent Terminer Annule

Enter the name of the PKCS#12 file, then Lastly, click on the "Finish" button. click on the "Next" button.

You have just exported into a password protected PKCS#12 standard format file, a combination of your certificate, its private key, and the certificate of the CA root. These elements have therefore been exported, but are still present in the Internet Explorer store.





11.3 Importing a certificate into Mozilla Firefox

With Mozilla Firefox, import of a complete PKCS#12 file with the root certificate.

In the "Tools > Options..." menu, select the "Advanced" section and the "Security" tab:

Options							X
	•	$\langle \langle \rangle$		<u> </u>	Ser and a series of the series		
Général	Vie privée	Contenu	Onglets	Téléchargements	Avancé		
Général	Mises à jour	Sécurité					1
Protoc	oles ———						— I I
🔽 Ut	iliser SSL <u>2</u> .0			🔽 Utiliser SSL	<u>3</u> .0		
🔽 Ut	iliser TLS <u>1</u> .0						
Certific Lorsqu C Er	tats 'un site Web n n sél <u>e</u> ctionner (ner les certifica	écessite un c un automatiq ats Listes	ertificat : uement () : de <u>r</u> évocat	● Me demander à ch ion <u>V</u> érification	ague fois Périphé	rique <u>s</u> de sécurité	
				ОК	Ar	nuler Aid	e

Click on "Display the certificates".

Č	Gestionnaire de cer	tificats			_ 🗆 ×
	Vos certificats Autres Vous possédez des ce	personnes Sites We	b Autorités ations qui vous identifient	:	
	Nom du certificat	Périphérique de	Sujets	Numéro de	Expire le 🖽
	Voir Exp	oorter Tout expo	orter Importer	Supprimer	
			1		ОК

Click on "Import".

Select the PKCS#12 file (with a ".p12" or ".pfx" extension):



Nom de fichier à	mporter				? ×
Regarder <u>d</u> ans :	Certificats		. 🖸 🔊	 •	
Mes documents récents	RTE_client.rte@service	s.rte-france.com.p12			
Mes documents					
Doste de travail					
Tavoris réseau	Nom du fichier :	E_client.rte@services.rte	e-france.com.p12		ivrir 🔤
	Fichiers de <u>type</u> : Fic	chiers PKCS12		▼ Anr	nuler

Enter the password to access the Mozilla Firefox certificate store:

Invite	×
?	Veuillez saisir le mot de passe principal de Sécurité personnelle.

	OK Annuler

Click on "OK".



Enter the password restricting access to the PKCS#12 (.p12) file, then click on "OK".



The holder's certificate is now in the Mozilla Firefox certificate store.



Č	Gestionnaire de certificats
	Vos certificats Autres personnes Sites Web Autorités
	Vous possédez des certificats de ces organisations qui vous identifient :
	Nom du certificat Périphérique de Sujets Numéro de Expire le 🖽
	RESEAU DE TR
•	Client RTE 1 Sécurité personnelle Client, Signature, Chiffr 39:2D:6B:2A 29/10/2007
	Voir Exporter Tout exporter Importer Supprimer
	ОК

Check that it's the right one by clicking on the "View" button.

Détails du certificat :"Client I	RTE 1'S RESEAU DE TRANSPORT D ELECTRICITE ID"	Détails du certificat :"Client RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID"
Général Détails		Général Détails
Ce certificat a été vérifi	é pour les utilisations suivantes :	Hiérarchie des certificats
Certificat client SSL		RTE Autorite de Certification
Certificat de signature de o	courrier	
Certificat de réception de o	ourrier	
Émis pour		Champs du certificat
Nom commun (CN) Organisation (O) Unité d'organisation (OU) Numéro de série	Client RTE 1 TEST 50f: ID 39:2D:68:2A:16:28:90:33:D3:DE:86:49:08:80:C0:21	Clent RTE I'S RESEAU DE TRANSPORT D ELECTRICITE ID Certificat Version Muméro de cérie
Émis par Nom commun (CN) Organisation (O) Unité d'organisation (OU)	RTE Autorite de Certification RESEAU DE TRANSPORT D ELECTRICITE «Ne fait pas partie du certificat»	- Algorithme de signature des certificats Émetteur ⊖ Validté -Pas avant
Validité Émis le Expire le	28/10/2005 29/10/2007	Pas après Valeur du champ
Empreintes numériques Empreinte numérique SHA1 Empreinte numérique MD5	B2:98:A5:48:24:50:CD:D5:D1:68:5C:2F:3E:E3:18:49:B7:07:98:FC 49:2F:C8:E1:2F:76:0C:67:19:D1:60:86:CC:49:E5:1C	CN = RTE Autorite de Certification O = RESEAU DE TRANSPORT D ELECTRICITE
	Fermer	Fermer

The RTE CA certificate is also in the Mozilla Firefox store:

Vos certificats Autres personnes Sites Web Autorités	
Vous possédez des certificats enregistrés identifiant ces autorités de certifica	tion :
Nom du certificat Périphérique de sécurité	E.
RESEAU DE TRANSPORT D'ELECTRICITE	
ⁱ RTE Autorite de Certification Sécurité personnelle	
🖃 RSA Data Security, Inc.	
Verisign/RSA Secure Server CA Builtin Object Token	
Secure Server OCSP Responder Builtin Object Token	-
Voir Modifier Importer Supprimer	

Copyright RTE. This document is the property of RTE. All communication, reproduction or publication, even partial, is prohibited without written authorisation from the Electricity Transport Network Operator (RTE)



11.4 Importing a certificate into Internet Explorer (Windows)

With Internet Explorer, import of a password protected PKCS#12 file with the root certificate.

Under Internet Explorer, open up: "Tools > Internet options..." and click on the "Contents" tab, then on the "Certificates..." button:

Certificats			?
Rôle prév <u>u</u> :	<tout></tout>		
Personnel Autres	personnes 🛛 Autorités intermédiaire	es Autorités principa	ales de confiance
Délivré à	Délivré par	Date d'expiration	Nom convivial
Importer	xporter Supprimer		<u>A</u> vancé
Détails de certifica	t		
			Affic <u>h</u> age
			Former

Click on the "Import" button.



Click on the "Next" button.

Click on the "Browse" button to locate the **PKCS#12 file** (ext. ".p12" or ".pfx"), then click on "Next".



< Précédent Suivant > Annuler

Enter the PKCS#12 file password, check Select the first box, then click on "Next". the 2 boxes, then click on "Next".

Assistant Importation de certific	at	×						
Fin de l'Assistant Importation de certificat Vous avez terminé correctement l'Assistant Importation de certificat.								
	Yous avez spécifié les paramètres su Magasin de certificats sélectionné Contenu Nom du fichier	ivants : Déterminé automatiq. PFX C:\Certificats\RTE2_c						
	<pre>< Précédent []</pre>	Terminer Annuler						

< Précédent Suivant > Annuler

Lastly, click on "Finish".

Select the security level of the private key that you are importing with the certificate.



Click on the "Define the security level" Select the "High" option, then click on button.

the "Next" button.



Access to the IT system with digital certificates under Microsoft Windows XP PKI user manual

Importation d'une nouv	elle clé d'échange privée	X Impo	rtation d'une nou
<u>a</u>	Créer un mot de passe pour protéger cet élément.		Une ap
	Créer un nouveau mot de passe pour cet élément. Mot de passe pour : Clé privée CryptoAPI		Clé priv
	Mot de passe : ••••••• Confirmer : ••••••		Niveau Élevé
	< Précédent Ierminer Annuler		



Enter a name for the "key pair" element to Click on the "**OK**" button. protect and a password, then click on the "Finish" button.

A dialogue box appears showing the elements of the CA root certificate that you are importing with your certificate.

Magasin	de certificats principal 🔀	Assistant	Importation de certificat 🛛 🔀
1	Voulez-vous ajouter le certificat suivant au magasin principal ? Objet : RTE Autorite de Certification, RESEAU DE TRANSPORT DELECTRICITE Émetteur : auto-émis Limite de validité : de mercredi 29 mai 2002 à marid 29 mai 2012 Numéro de série : 75220902 54AEC749 81042703 8CCC21EB Empreinte numérique (sha) : A29AFA1 L'1742/S67 FA302D60 8F2C0237 37C7AE37 Empreinte numérique (md5) : S3426A2E AS10AE2A 2109EE88 1367A031 Qui Non	į)	L'importation s'est terminée correctement.

Click on the "Yes" button.

Click on the "OK" button.

Your certificate, your private key and the root certificate of the RTE CA have been imported into Internet Explorer.

Certificats	? × Certifica	t		<u>?</u> ×
Rôle prév <u>u</u> : <pre></pre>	Généra	Détails Chemin d	d'accès de certification	
Délivré à Délivré par Date d'ex… Nom convivia ⊡Client RTE 2 RTE Autorite de Certif… 01/11/2007 <aucun></aucun>		Informations certificat est cons outes les stratégies c	sur le certificat çu pour les rôles suivants : d'application	-
Importer Exporter Supprimer	<u>A</u> vancé	Délivré à :	Client RTE 2	-
<tout></tout>	Affichage	Délivré par : Valide à partir d	RTE Autorite de Certification	
	<u>E</u> ermer	Vous avez une clé	privée qui correspond à ce certificat.	
The image on the right shows that	the		Déclaration de l'émetteur	

private key is indeed present.



11.5 Importing a certificate into Mozilla Thunderbird

With Mozilla Thunderbird, import of a complete PKCS#12 file with the root certificate.

Open the "Tools > Options..." menu, the "Confidentiality" section and then the "Security" tab:

Options						×
W	2			Ø	 	
Général	Affichage	Rédaction	Confidentialité	Pièces joint	es Avancé	
Général	Courrier fraudu	leux Antiviru	s Mots de passe	Sécurité		
Gérer les sécurité.	certificats, les	listes de révoc	ation, la vérificatio	n des certifica	ats et les périphériques d	e
Vo	įr les certificats	List <u>e</u> s de	révocation V	érification	<u>P</u> ériphériques de sécur	ité
	Î.					
	•					
					OK Anr	uler

Click on the "View the certificates" button.

4	Gestionnaire de certificats							
	Vos certificats Autres	personnes Sites Web Autori	tés					
	Vous possédez des certificats de ces organisations qui vous identifient :							
	Nom du certificat	Périphérique de sécurité	Sujets	Numéro de série	Expire le	E.		
	Voir Exp	orter Tout exporter	Importer	Supprimer				
			1			ок		

Click on the "Import" button:

Select the **PKCS#12** file (with a ".p12" or ".pfx" extension):



Nom de fichier à	importer						? ×	1
Regarder <u>d</u> ans :	Certificats		•	G	1 🖻	•		
	BRTE_client.rte@sei	rvices.rte-france.com.p	012					
Mes documents								
Bureau								
								I
mes documents								I
								I
Poste de travail								I
Favoris réseau	<u>N</u> om du fichier :	RTE_client.rte@servi	ices.rte-fra	nce.cor	n.p12	•	<u>O</u> uvrir	
	Fichiers de <u>type</u> :	Fichiers PKCS12				•	Annuler	

Setting up the protection password for the Enter the password restricting access certificate store.

Définir le mot de passe principal	<u>×</u>
Périphérique de sécurité : Sécurité	é personnelle
Ancien mot de passe	(non défini)
Entrez le nouveau mot de passe	****
Entrez-le à nouveau	****
Mesure de la qualité du mot de pa:	sse :
	OK Annuler

to the PKCS#12 (.p12) file, then click on "OK".

Fenêtre d'entrée du mot de passe	×
Veuillez entrer le mot de passe portable de sécurité protégear ce certificat de sécurité et la clé privée.	nt
Mot de passe : 🛛 ******	
OK Annuler	
Alerte	×
Récupération des certificats et clés privées réussie	
OK	

Click on "OK".

Note: if this password already exists, a field entry form will appear.

The holder's certificate is now in the Mozilla Thunderbird certificate store:

2	Gestionnaire de certifi	icats				
	Vos certificats Autres pe	ersonnes Sites Web Autor	ités			
	Vous possédez des certif	icats de ces organisations qu	i vous identifiei	nt:		
	Nom du certificat	Périphérique de sécurité	Sujets	Numéro de série	Expire le	E.
	E RESEAU DE TRAN					
	ⁱ Client RTE 1	Sécurité personnelle	<ne fait<="" td=""><td>39:2D:6B:2A:16:28</td><td>29/10/2007</td><td></td></ne>	39:2D:6B:2A:16:28	29/10/2007	
	Voir Expor	rter Tout exporter	Importer	Supprimer		
						OK

Check that it's the right one by clicking on the "View" button.



Détails du certificat :"Client F Général Détails	RTE 1'S RESEAU DE TRANSPORT D ELECTRICITE ID"	Détails du certificat :"Elient RTE 1's RESEAU DE TRANSPORT D ELECTRICITE ID"
Incossible de vérifier co Émis pour Nom commun (CN) Organisation (O) Unité d'organisation (OU) Numéro de série Émis par Nom commun (CN) Organisation (O) Unité d'organisation (OU) Validité Émis le Expre le Empreintes numérique SHA1 Empreinte numérique MD5	e certificat car son émetteur n'est pas digne de confiance. Clent RTE 1 TEST Soft ID 39:20:68:24:16:28:90:33:D3:DE:86:49:08:80:C0:21 RTE Autorite de Certification RESEAU DE TRANSPORT D ELECTRICITE «Ne fait pas partie du certificat> 28/10/2005 29/10/2007 82:98:A5:48:24:50:CD:05:D1:68:5C:2F:SE:E3:18:49:87:07:98:FC 49:2F:C8:E1:2F:76:0C:67:19:D1:6D:86:CC:49:E5:1C	Hiérarchie des certificats RETE Autorite de Certification Champs du certificat Sujet Fundo de publique du sujet Agorithme dé publique du sujet Agorithme dé publique du sujet Champs du champ E = client.rte@services.rte=france.com CN = client RTE 1 OU = ISO 6523 - 0000 0000 OU = Soft ID O = TEST
	Fermer	C = FR

The RTE CA certificate is also in the Mozilla Thunderbird store:

🥞 Gestionnaire de certificats		
Vos certificats Autres personnes Sites Web	Autorités	
Vous possédez des certificats enregistrés identi	fiant ces autorités de certification :	
Nom du certificat	Peripherique de securite	
RTE Autorite de Certification	Sécurité personnelle	
🖻 RSA Data Security, Inc.		
-Verisign/RSA Secure Server CA	Builtin Object Token	
Secure Server OCSP Responder	Builtin Object Token	▼
Voir Modifier Importer	Supprimer	
		ОК

Click on the "Modify" button.

Édition des paramètres de confiance de l'autorité de certification (CA) 🛛 🔀
Le certificat « RTE Autorite de Certification » représente une autorité de certification.
Modifier les paramètres de confiance :
Ce certificat peut identifier des sites Web.
Ce certificat peut identifier des utilisateurs de courrier électronique.
 Ce certificat peut identifier des créateurs de logiciels.
OK Annuler

Check the three boxes shown above, then click on "OK".



You have now declared your trust in the RTE root certificate as shown below:

ŝ,	Gestionnaire de certificats	<u> </u>
	Vos certificats Autres personnes Sites Web Autorités	
	Vous possédez des certificats de ces organisations qui vous identifient :	
	Nom du certificat Périphérique de Sujets Numéro de Expire le 	E
	Client RTE 1 Sécurité personnelle Client, Signature, Chiffrement 39:2D:6B:2A: 29/10/2007	
	Voir Exporter Tout exporter Importer Supprimer	
		ок

Certificat de signature de (courrier
Certificat de réception de o	courrier
Émis pour	
Nom commun (CN)	Client RTE 1
Organisation (O)	TEST
Unite d'organisation (UU) Numéro de série	39:2D:6B:2A:16:28:90:33:D3:DE:86:49:0B:80:C0:21
Émic nor	572576524716267575757575757575757567575757575757575
Nom commun (CN)	RTE Autorite de Certification
Organisation (O)	RESEAU DE TRANSPORT D ELECTRICITE
Unité d'organisation (OU)	<ne certificat="" du="" fait="" partie="" pas=""></ne>
Validité	
Émis le	28/10/2005
Expire le	29/10/2007
Empreintes numériques	,
Empreinte numérique SHA1	B2:98:A5:4B:24:50:CD:D5:D1:68:5C:2F:3E:E3:18:49:B7:07:9B:F0
Empreinte numérique MD5	49:2F:C8:E1:2F:76:0C:67:19:D1:6D:86:CC:49:E5:1C



12. Appendix B – (PKI) secured environment

This appendix describes the secured environment in which the PKI system is implemented. It specifically addresses:

- the concepts of the secured environment and the corresponding computing objects managed by the PKI,
- the role of the different entities taking part in the PKI operational processes.

12.1 Concepts and objects generated by a PKI

This appendix presents the principal concepts needed to understand the role of the objects generated by a PKI:

- a presentation of the structural principles of a secured process,
- the role of the key pair,
- and the certificates.

12.1.1 What is a secured process?

12.1.1.1 Definition of a PKI

With a PKI (Public Key Infrastructure, or IGC in French for Infrastructure de Gestion de Clés), every certificate holder has a pair of keys – a private key, known only to its sole owner, and a public key – inter-connected with a complex mathematical relationship, which makes it almost impossible to determine the private key with only the public key. This means that the probability of determining the private key based on the public key in a **reasonable** period of time is **very low**.

Data encrypted with one key (typically the public key) can only be decrypted using the other one (typically the private key). This is the basis which forms the core operation that ensures the confidentiality of the exchanged messages.

12.1.1.2 The four pillars of information communication security

This electronic identity card is designed to establish a trust environment based on the four following fundamental pillars:

- **authentication** confirms that the participant parties are indeed who they claim to be;
- confidentiality prevents non-recipients from reading the data;
- integrity ensures that the data have not been altered in transit;
- **non-repudiation** makes it impossible for either party to deny that the information has been transmitted.

12.1.1.3 The cryptographic solution

Because of the inherent nature of the technology used (i.e. public protocols, architectures, etc.), information circulating on the Internet is not



confidential. Neither do the technologies currently employed respond to the other three security requirements mentioned above.

In order to maintain the confidentiality of communications made over the Internet, the data must be rendered incomprehensible to anyone except the intended recipients. Encryption is a solution that meets these demands.

The encryption of the data is naturally accompanied by the authentication of the system users. In reality, if certain data are confidential, it is necessary that the senders and receivers of that data can authenticate each other in a certain and unambiguous manner in order to proceed with secured communications.

Authentication relies on the possession of a certificate. This certificate is delivered by a Certification Authority to which the participating parties of a transaction both assign confidence (in our case, the Certification Authority is the RTE). In addition, certificate holders can trust the information supplied to them, and RTE knows that only the assigned certificate holders have access to the information.

NOTE

Following an analogy in normal life, it is necessary to supply an identity document provided by an approved authority in order to have access to certain privileges reserved for citizens of a country (e.g. very expensive purchases, exercising voting rights, etc.).

12.1.2 The role of the key pair

Each certificate holder has a public key as well as a corresponding private key:

- The **private key** is the key that the certificate holder must keep confidential. He is the only person to **have that key** and **be able to use it**. He may not necessarily know it himself (for example, it might be stored on a card with a computer chip, from which it can be extracted, but access to the card is protected with a PIN code known only by its owner).
- The **public key**, as its name indicates, is public and may be communicated to everyone. The public keys of certificate holders are only used to encrypt messages intended for the certificate's holder. If an encrypted message is intercepted, there are no significant impacts to confidentiality because the message can not be decrypted (in a reasonable period of time) by a person who does not have the private key.

The private key enables its owner to sign messages that he sends out and to decrypt messages that are sent to him.

12.1.2.1 Encryption and decryption of a message

Each message is encrypted with the public key of its recipient, who will decrypt that message with his private key.

When RTE sends a message to its customer A:



- 1. RTE knows the public key of customer A (from his certificate).
- 2. RTE automatically encrypts the message using customer A's public key and sends it to him using RTE's electronic email services.
- 3. Customer A receives the message and automatically decrypts it with his private key.



Encryption and decryption with a key pair

12.1.2.2 Use of the keys for signing messages

Each message is signed with the private key of the sender. The source (i.e. the signature) of a message can be checked thanks to the sender's public key being openly available through his certificate.

To prove to customer A that the message he has received actually does come from RTE, RTE automatically signs its messages with its own private key before sending them to customer A.



Signing and signature verification with a key pair

When customer A receives the message from RTE, he automatically verifies the signature on the received message with RTE's public key.



12.1.3 The certificates

12.1.3.1 Objectives of the digital certificate

Because the public keys are used to verify the electronic signatures and to encrypt messages, it is critical for every certificate holder to be certain about the identity of the owner of a public key: this is the role of the **certificate**.

12.1.3.2 Properties of a certificate

The certificate is an electronic proof of identity:

- which guarantees the identity of its holder,
- which contains data facilitating identification,
- which is resistant to counterfeits and is issued by a trusted third party: the Certification Authority.

A Certification Authority is an entity which creates and manages certificates. It defines the rules for registration in the PKI of the various certificate holders.

12.1.3.3 Structure of a certificate

A digital certificate contains:

- the **public key** of the owner,
- the **name of the owner** and other identification information (the email address of the person if it is a certificate to be used to sign emails),
- the validity period of the certificate,
- the **name of the certification authority** which generated this certificate,
- a unique serial number,
- and the **signature** of the certification authority.



12.1.3.4 Certificate examples

informations	s sur le certificat
Ce certificat est de	stiné à :
• Garantit Indentite du Garantit votre identit • Assure que le logiciel • Protége le logiciel cor • Protége le courrier él • Permet aux données • Vous permet de signe	A ordinateur distant cé auprès d'un ordinateur distant provenait d'un éditeur de logiciels htre toute modification après sa publication lectronique d'être signées avec l'heure en cours er numériquement une liste de certificats de
Délivré à :	Evariste Akouegnon
Délivré par :	RTE Autorite de Certification
¥alide à partir (du 01/08/2002 jusqu'au 02/08/2003

A digital certificate in Internet Explorer

J Certificat de signature de courrier Certificat de réception de courrier Émis pour Nom commun (CN) Client RTE 1 Organisation (O) TEST Unité d'organisation (OU) Soft ID Numéro de série 39:20:68:2A:16:28:90:33:D3:DE:B6:49:0B:BC	
Émis pour Kom commun (CN) Client RTE 1 Organisation (O) TEST Unité d'organisation (OU) Soft ID Numéro de série 39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:BC	
Émis pour Client RTE 1 Nom commun (CN) Client RTE 1 Organisation (O) TEST Unité d'organisation (OU) Soft ID Numéro de série 39:2D:6B:2A:16:28:90:33:D3:DE:B6:49:0B:BC	
	:CD:21
Émis par RTE Autorite de Certification Nom commun (CN) RTE Autorite de Certification Organisation (O) RESEAU DE TRANSPORT D ELECTRICITE Unité d'organisation (OU) <ne certificat="" du="" fait="" partie="" pas=""></ne>	
Validité Émis le 28/10/2005 Expire le 29/10/2007	
Empreintes numériques Empreinte numérique SHA1 B2:98:A5:48:24:50:CD:D5:D1:68:5C:2F:3E:E3 Empreinte numérique MD5 49:2F:C8:E1:2F:76:0C:67:19:D1:6D:86:CC:49	8:18:49:87:07:98:FC 9:E5:1C

A digital certificate in Mozilla Firefox



12.2 Documentation

Reference documents:

- The RTE Certification Policy,
- The subscription contract for the RTE's secured IT system.

Web sites:

- http://www.legifrance.gouv.fr/
- Legislation from March 13th 2000 bearing modifications on legal proofs of information technologies relative to electronic signatures:

http://www.assemblee-nat.fr/

• Directive 1999/93/CE from December 13th 1999 concerning an EU community framework for electronic signatures:

http://europa.eu.int/

• The regulatory working group on electronic signatures:

http://www.internet.gouv.fr/

• Keynectis:

http://www.keynectis.com/



13. Appendix C – Glossary

When certificate holders approach their new secure environment, they will be confronted with specific terminology, the terms of which are explained in this section.

Authentication

Verification of the validity of identity as declared by a user, by a device or by another entity in an information or communications system.

• Certification Authority

A Certification Authority (CA) is an entity which issues digital certificates for use by other parties as electronic equivalents of identity documents. In distributing digital certificates, the Certification Authority or Trust Authority serves as an ethical guarantor by asserting a person's identity through the certificate provided to that person. According to the scope accorded to the Certification Authority, this certificate will have a field of application of varying range: limited to internal communications in a company (like a company security badge) or for use in communications with other organisations and administrative bodies (like a national identity card or passport).

• Certificate

A digital certificate plays the role of an electronic ID card (electronic passport). It guarantees the identity of its owner in electronic transactions and contains all the information required to permit such identification (surname, first name, possibly company, address, etc.). A digital certificate consists of a public key and personal information about the holder, all signed by a Certification Authority.

• Confidentiality

A property of data or information which are neither actively nor passively available nor disclosed to unauthorised persons.

• Cryptography

The practice, study and techniques of transforming data with the aim of hiding its semantic content, establishing its authenticity, preventing its unobserved modification, warning of its repudiation, and preventing its unauthorised use.

• Private Key

A secret digital value assigned to one person, allowing that person to either successfully decipher messages encrypted with the corresponding public key or to affix an authenticating signature to the foot of messages sent.

• Public key

A digital value, assigned to one person, but distributed to others so that these others are able to either securely send the person encrypted data or to verify that person's signature.

• Encryption / Decryption



The transformation of data through cryptographic techniques to make that data unintelligible in order to ensure its confidentiality / The inverse transformation of encrypted data.

• Integrity

The assurance that the data or information have not been modified or altered in an unauthorised manner.

• Non-repudiation

A property obtained with cryptographic methods to prevent a person from denying having performed a particular action on the data (for example, source non-repudiation; attestation of obligations, intentions or commitments; establishment of ownership).

Revocation

Revocation is the procedure which leads to the deletion of the guarantee provided by the Certification Authority for a given certificate, made upon the request of the subscriber or any other suitably authorised person. The request may be the consequence of various types of events, such as the compromise or destruction of the private key, the modification of information contained in the certificate, or non-respect of the certificate's usage rules.

• Electronic signature

The electronic signature of a document consists of signing a digital "summary" of that document with one's private key, which can then not be modified without such modification being visible. As with a handwritten signature, it commits the signatory to certain responsibilities.

END OF DOCUMENT