MANUEL Communication sécurisée HTTPS, FTPS, SMTPS





SOMMAIRE

Intro	oduction
1.2	Présentation3
1.3	Les certificats d'authentification4
1.4	Création des certificats d'authentification4
2.	HTTPS5
2.2	Principe
2.3	HTTPS serveur
2.4	HTTPS Customer (client)
3.	FTPS
3.2	Principe
3.3	FTPS serveur
3.4	FTPS client9
	Avec certificat externe
	Sans certificat externe
4.	SMTPS
4.2	Principe11
4.3	SMTPS client
5.	Annexe
5.2	Paramétrage d'un serveur FTPS distant14
5.3	Glossaire



Introduction

1.2 Présentation

L'HyperText Transfer Protocol Secure, plus connu sous l'abréviation HTTPS - littéralement « protocole de transfert hypertexte sécurisé » - est la combinaison du HTTP avec une couche de chiffrement SSL ou TLS.

HTTPS permet au visiteur de vérifier l'identité du site web (REDY) auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable. Il garantit la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur (REDY).

Le File Transfer Protocol Secure, abrégé FTPS est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP, sécurisé avec les protocoles SSL ou TLS. Il permet au visiteur de vérifier l'identité du serveur auquel il accède grâce à un certificat d'authentification. Il permet également de chiffrer la communication.

Il y a deux méthodes pour invoquer le chiffrement SSL/TLS avec FTP : de manière explicite ou implicite ; le **REDY utilise le mode « implicite** ».

Implicite : L'échange est crypté dès que liaison Client / Serveur est établie. Explicite : La connexion se fait en clair, l'échange des données est crypté après l'authentification.

Le Simple Mail Transfer Protocol Secure (SMTPS) est une méthode permettant de sécuriser le protocole SMTP (envoi d'emails) avec la sécurité de la couche de transport. Il est destiné à assurer l'authentification des partenaires de communication, ainsi que l'intégrité et la confidentialité des données.



[**i**]

Ports par défaut :

Les serveurs **HTTPS** utilisent le port TCP **443**.

Les serveurs et clients FTPS utilisent les ports 990 et 989.

Les clients SMTPS utilisent le port TCP 465 (Implicit) ou 587 (Explicit).



Ces protocoles sont disponibles à partir de la version 10.0.0 du REDY.



La version de TLS (Transport Layer Security) utilisée est V1.2.



1.3 Les certificats d'authentification

Les protocoles sécurisés utilisent des certificats d'authentification.

Chaque produit a son certificat personnalisé. Il est donc nécessaire de demander au REDY de créer le sien ; soit pour lui-même soit pour le distribuer à d'autres serveurs.

1.4 Création des certificats d'authentification

Aller à Configuration \rightarrow Gestionnaire \rightarrow Certificats

Cliquer sur le bouton « Création de certificats » :

Gestionnaire
Mise à jour Projets Config.ini Fichiers Certificats
Nom
Création du certificat
Création des certificats en cours

Après quelques secondes, 2 certificats sont créés : Cela permettra au REDY de faire de l'auto-certification.

🤨 Gestionnaire				🗸 🔊 🕹	ه د
Mise à jour Projets Config.ini Fichiers Certificats					
Nom	Expiration	Taille	Date	Exporter	
REDY-02348-00017-CA.crt	Jun 28 14:10:58 2043 GMT	1 Ko	28/06/18 16:10	2	2
ServerREDY.pem	Jun 28 14:11:15 2043 GMT	2 Ko	28/06/18 16:11	2	2
Résultat de la dernière action: Création réussie					

- Le fichier « REDY-xxxxx-yyyyy-CA.crt » est un certificat qu'il est possible d'exporter et d'utiliser sur un appareil tiers qui souhaitera se connecter au REDY *(Exemple : un serveur FTPS)*. Ce certificat est propre au REDY dont le « WID » est xxxxx-yyyyy.
- Le fichier « ServerREDY.pem » est utilisé directement dans le REDY pour ses communications sécurisées en tant que serveur. *(Voir ci-dessous)*.



2. HTTPS

2.2 Principe



Fig.1 – Principe du HTTPS.

2.3 HTTPS serveur

La connexion HTTPS est créée par défaut mais n'est pas valide.

Aller à Configuration \rightarrow Réseau \rightarrow IP \rightarrow HTTPS

IP IP	🗸 🖉 🕃 🖉 🤣 🔌
IP Connexion DNS FTF	FTPS TELNET HTTP HTTPS WOP SMTP WDC
<u></u>	
tonnexion	
Valide	
Etat	Stop, Wait
Libellé	HTTPS
Moniteur	
AutoStart	 Image: A start of the start of
Mode connexion	Serveur Multiple Attente max. (s) 0
Port hôte	443
Port hôte vers Proxy	8080
application	
Protocole	HTTPS
Certificat	ServerREDY.pem V
Time-Out du Keep-Ali	ive (s) 30
URIs Cross-Domain a	utorisées http://appria.wit.fr https://app

Renseigner le certificat créé précédemment puis valider la connexion. Valider la connexion.





Après avoir vérifié le fonctionnement de la liaison, il est possible de dévalider le port 80 de la connexion HTTP.

La connexion au REDY est à présent du type : <u>https://mon-site-REDY.fr</u>

Lors de la première connexion un message de ce type est affiché :



Cliquer sur « Paramètres avancés » :



Ce message apparait car le certificat émis par le REDY n'est pas connu par l'organisme de contrôle.

Il est bien sûr possible d'acheter un certificat auprès d'un organisme de confiance et de l'intégrer dans le REDY depuis le gestionnaire :

🧝 Certificat		
Chargement d'un certificat	Choisir un fichier Aucun fi choisi	Enregistrer



2.4 HTTPS Customer (client)

Le protocole HTTP Customer est également fournit en mode sécurisé, ainsi « eShare » peut aussi partager ses données en mode sécurisé.



Cette possibilité n'est applicable que dans un « domaine eShare » composé uniquement avec des REDY.

🐞 Connexion	
Valide	 Image: A start of the start of
Etat	Stop, Ok
Libellé	eShare sécurisé
Moniteur	
AutoStart	
Mode connexion	Client
Port Destination	443
Adresse Destination	192.68.1.137
Port Destination vers Proxy	1024
Réseau principal	LAN V
🐞 Application	
Protocole	HTTPS Customer
Faire confiance au serveur	
🐞 Lien	
e Share	

L'adresse de destination correspond à l'adresse d'un serveur.

Il n'est pas obligatoire de remplir ce champ, en effet l'adresse est renseignée dynamiquement par la ressource « Domaine eShare » en fonction du site à atteindre.

Le port destination correspond au port du ou des serveur(s).

Par défaut les connexions HTTPS utilisent le port 443.



Tous les REDY qui font partie du réseau « eShare » doivent avoir leur connexion HTTPS serveur validée et posséder le même numéro de port.

Le port de destination vers le Proxy est interne au REDY. Il doit être compris entre 1024 et 65535 et non utilisés sur d'autres connexions au sein du REDY.

 (\boldsymbol{i})

Un contrôle d'unicité est réalisé lors de la saisie :

Mode connexion	Client
Adresse destination	192.68.1.137
Port destination	443
Port destination vers le Proxy	1024 Attention: Ce numéro de Port est déjà utilisé
Réseau principal	Auto.

Liste des sites dans la ressource « Domaine eShare » :

n	ts (1) Schéma Paramètres UTL Etat				
	Logiciel	Adresse	Succès diffusion	Echec diffusion	Dernière diffusion
	REDY 10.0.0 07/08/2018	192.68.1.150:443	13575	140	28/08/2018 16:41:19
	REDY 10.0.1 26/06/2018	192.68.1.137:443	745	12970	28/08/2018 14:18:16



3. FTPS

3.2 Principe

Le protocole FTP permet l'échange de fichiers entre deux machines :



le client établit une seconde connexion pour le trafic de données.

Le protocole **FTPS** propose le même service avec des échanges renforcés par un cryptage des données. Avec le REDY, la connexion FTPS peut être utilisée en mode client et/ou en mode serveur.

3.3 FTPS serveur

La connexion serveur FTPS est créée par défaut mais n'est pas valide. Aller à *Configuration* \rightarrow *Réseau* \rightarrow *IP* \rightarrow *FTPS*

IP Connexion DNS FTP	FTPS TELNET HTTP HTTPS WOP SMTP SMTPS
🗽 Connexion	
Valide	
Etat	Stop, Ok
Libellé	FTPS
Moniteur	
AutoStart	
Mode connexion	Serveur Multiple Attente max. (s)
Port hôte	990
Port hôte avec le Proxy	2121
Port data	989
Port data avec le Proxy	2020
Application	
Protocole FTPS (Implicit)	▼
Certificat ServerREDY.per	n 🔻



Sélectionner le certificat adéquat. Valider la connexion.

(i)

- Le numéro du port hôte est fixé à 990 par défaut.
 - Le numéro du port data est fixé à 989 par défaut.
 - Les ports Proxy hôte et data doivent être compris entre 1024 et 65535 et non utilisés sur d'autres connexion au sein du REDY.

3.4 FTPS client

Avec certificat externe

Le certificat est fourni par le serveur FTPS puis importé dans le REDY depuis le gestionnaire des certificats.

🤨 Gestionnaire
Mise à jour Projets Config.ini Fichiers Certificats
Nom
REDY-02348-00017-CA.crt
ServerREDY.pem
certificate_filezilla.crt
Création du certificat
Certificat
Chargement d'un certificat Choisir un fichier Aucun fi choisi Enregistrer

Créer une nouvelle connexion, sélectionner le protocole « FTPS » en mode Client. Aller à *Configuration* \rightarrow *Réseau* \rightarrow *IP Ajouter une connexion* \rightarrow *FTPS mode Client*

P Connexion DNS FTP FTPS	TELNET HT		WOP SMTP	SMTPS	
该 Connexion					
Valide					
Etat	Stop, Ok				
Libellé	FTPS Client	t in the second s			
Moniteur					
AutoStart					
Mode connexion	Client	T			
Adresse destination	192.68.1.13	7			
Port destination	990]			
Port destination vers le Proxy	7001]			
Port data	989	ĺ			
Port data vers le Proxy	7002	ĺ	🐞 Applicatio	n	
Réseau principal	Auto.	, •	Protocole	-	FTPS
recould principal			Faire con	fiance au serveu	ır 📃
			Certificat		certificate_filezilla.crt
Protocole	PS (Implicit)	•	6		REDY-02348-00017-CA.crt
	, o funknowi	•	🐞 Lien		ServerREDY.crt
Faire contiance au serveur			📻 Server	ILL FTPS PC	certificate filezilla.crt
Certificat	rtificate_filezilla.ort	•	1 10		



Le numéro du port hôte est fixé à 990 par défaut. Le numéro du port data est fixé à 989 par défaut. Les ports Proxy hôte et data doivent être compris entre 1024 et 65535 et non utilisés sur d'autres connexion au sein du REDY. Sélectionner le certificat adéquat. Valider la connexion.

Sans certificat externe

Le serveur est de confiance, le REDY accepte la connexion. Ce choix est à utiliser seulement si l'origine du serveur est connue, et est de confiance.

Créer une nouvelle connexion, sélectionner le protocole « FTPS » en mode Client. Aller à *Configuration* \rightarrow *Réseau* \rightarrow *IP Ajouter une connexion* \rightarrow *FTPS mode Client*

Connexion					
Valide					
Etat	Stop, Ok				
Libellé	FTPS Cli	ente			
Moniteur					
Auto Start					
Mode connexion	Client	¥			
Adresse destination	192.68.1	137			
Port destination	990				
Port destination vers le Proxy	7001				
Port data	989				
Port data vers le Proxy	7002				
Réseau principal	Auto.	T			
Application					
Protocole	TPS (Implicit)		•		

Le numéro du port Destination est fixé à 990.

Le numéro du port data est fixé à 989.

Les ports Proxy Destination et Data doivent être compris entre 1024 et 65535 et non utilisés par d'autres connexion au sein du REDY.

Sélectionner « Faire confiance au certificat ».

Valider la connexion.

Exemple d'utilisation :



Connexion FTPS client

Connexion FTPS serveur

Le REDY transfère ces fichiers à partir de la ressource « FTP Dossier» ou « FTP Ensemble » sur un serveur distant.





4. SMTPS

4.2 Principe

Le protocole SMPTS permet l'envoi d'emails en mode sécurisé.

La connexion SMTPS est utilisée en mode client.

Le REDY utilise les méthodes dites « Implicit » (la méthode de chiffrement utilisée est TLS/SSL (la méthode STARTTLS n'est pas supportée) et « Explicit ».



SSL Implicit : L'échange est crypté dès que liaison Client / Serveur est établie. SSL Explicit : La connexion se fait en clair, l'échange des données est crypté après l'authentification.

Le port par défaut est généralement le port 465 (parfois le port 587 est aussi autorisé).

4.3 SMTPS client

Se rendre dans Configuration \rightarrow Réseau \rightarrow IP \rightarrow SMTPS

IP Connexion SSDP FTP	FTPS HTTP HTTPS SMTPS WOP SMTPs Full	
🐞 Connexion		
Valide	Image: A state of the state	
Etat	Stop, Ok	
Libellé	SMTPs Full	
Moniteur		
Mode de la connexion	Client	
Adresse Destination	smtp.gmail.com	
Port Destination	465	
Réseau principal	LAN ~	
🐞 Application		
Protocole	SMTP-Full	
Le serveur demande ur	ne authentification 🔽	
Utiliser les paramètres	spécifique suivant:	
Nom de l'utilisateur	Test.wit@gmail.com	
Mot de passe		
Mode de transmission	Explicit (STARTTLS)	
Faire confiance au serveur 🗹		

L'Adresse destination correspond à l'adresse du serveur. Ce champ peut contenir une adresse IP ou une URL qui sera résolue lors d'établissement de la connexion.

Le port destination correspond au port du serveur. Par défaut les serveurs SMTPS utilisent le port 465 en mode Implicit et 587 ou mode Explicit.

Le port destination vers le Proxy est interne au REDY. Il doit être compris entre 1024 et 65535 et non utilisé sur d'autres connexions au sein du REDY (mode Implicit).



(i)

Les réseaux SMTP et SMTPs Implicit ont été gardé par soucis de compatibilité ascendante, ils ont été suffixé de « Deprecated » (le fonctionnement reste identique).

Le choix « Utiliser les paramètres » permet de sélectionner automatiquement les informations présentes dans Configuration -> Système, ou de sélectionner ses propres paramètres

Général	Heure et Langue	Gestionnaire des tâches	Journaux du système	
		🗊 Site		
		Identité	Mon REDY	
		Label		
		URL]
		Adresse e-mail	Test.wit@gmail.com	J
		Mot de passe e-mail	•••••	 Montrer

Liste des principaux serveurs SMTP :

FAI	Paramètres	Double authentification
Orange		
Adresse de destination	smtp.orange.fr	
Port de destination	465 et 587	Fonctionne sans double authentification
SFR		
Adresse de destination	smtp.sfr.fr	
Port de destination	465	
Free		
Adresse de destination	smtp.free.fr	
Port de destination	465 et 587	Fonctionne sans double authentification
Bbox		
Adresse de destination	smtp.bbox.fr	
Port de destination	465 uniquement	
Laposte.net		
Adresse de destination	smtp.laposte.net	
Port de destination	465 et 587	Fonctionne sans double authentification
Yahoo*		
Adresse de destination	smtp.mail.yahoo.fr	
Port de destination	465 uniquement	
Aruba		
Adresse de destination	smtp.aruba.it	
Port de destination	465 uniquement	
GMX**		



Adresse de destination	mail.gmx.com	
Port de destination	465 uniquement	
Outlook		
Adresse de destination	smtp-mail.outlook.com	Fonctionne sans double authentification
Port de destination	587 uniquement	
Gmail		
Adresse de destination	smtp.gmail.com	
Port de destination	465 et 587	Demande la double authentification pour fonctionner
Mailo		
Adresse de destination	mail.mailo.com	
Port de destination	465 et 587	Fonctionne sans double authentification

* Dans le compte de messagerie Yahoo, renseigner une « clé de compte » à la place du code d'accès de la boîte mail (« Système → Mot de passe e-mail »). Cette clé est fournie par Yahoo.
** Sur le site GMX, dans le compte de messagerie GMX, il est nécessaire d'activer le protocole SMTP (par défaut il ne l'est pas).



Pour plus d'informations, vous pouvez consulter la FAQ « Comment configurer l'envoi de mails » disponible depuis notre site <u>www.wit.fr</u>.



5. Annexe

5.2 Paramétrage d'un serveur FTPS distant

Le REDY doit transmettre de manière sécurisée un fichier (Journal) vers un serveur FTPS installé sur un ordinateur distant.



Connexion FTPS client

Connexion FTPS serveur

Le logiciel serveur utilisé dans cet exemple est « Filezilla server ». Il est téléchargeable ici : <u>https://filezilla-project.org/</u>

Une fois installé, le serveur se présente sous forme d'un « Service » qu'il convient de démarrer. La fenêtre de paramétrage se présente de cette façon :

🔁 FileZilla S	erver (127.0.0.1)				
<u>File</u> Server	<u>E</u> dit <u>?</u>				
/	💺 £ 🥵 🦿 🔰 /c/ 🕬) 📰 👻			
FileZilla Server 0.9.60 beta Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org) https://filezilla-project.org/ Connecting to server localhost:14147 Connected, waiting for authentication Logged on					
ID 🛆	Account	IP	Transfer		
•		m			•
Ready				0 bytes receiv d 0 E	3/s 0 by

Aller à *Edit* \rightarrow *Settings* \rightarrow *Général settings* \rightarrow *Passive mode settings* Réglage du mode passif.



Appliquer les paramètres tels que ci-dessous :

General settings	Passive mode settings FileZilla Se	rver
···· Welcome message ···· IP bindings		
DF Filter Passive mode settings Security settings Miscellaneous Admin Interface settings Logging Speed Limits Filetransfer compression FTP over TLS settings Autoban	IPv4 specific External Server IP Address for passive mode transfers: Use custom PASV settings if you are operating the server from behind a NAT operating the server from behind a NAT intervention of the server is not accessible from outside of the router, so you should fill in the correct address here. Use the port range to limit the number of ports that will need to be forwarded through the router. ® Betrieve external IP address from: http://p.filezilla-project.org/ip.php (Default: http://p.filezilla-project.org/ip.php) Information for users with dynamic IPs: If your external IP changes, it might take up to 5 minu after the next failed transfer until FileZilla Server recognizes the changed IP. In most cases, the IP is updated within 30s after a failed transfer.	tes
ОК	☑ Don't use external IP for local connections	
Cancel	You can use this site to test that your settings work correctly:	

Indiquer le numéro de port utilisé. Il doit être identique à celui utilisé par le client.

Aller à Edit \rightarrow Settings \rightarrow Général settings \rightarrow FTP over TLS settings

General settings	FTP over TLS settings	FileZilla Serve
 Welcome message IP bindings 	Enable FTP over TLS support (FTPS)	
IP Filter	Disallow plain unencrypted FTP	
- Passive mode settings - Security settings	X.509 Certificate	
Miscellaneous	Private key file:	Browse
- Admin Interface settings - Logging	Certificate file:	Browse
- Speed Limits - Filetransfer compression	Key password:	Password will be stored in plaintext.
FTP over TLS settings Autoban	Generate new certificate	2
	Explicit and implicit FTP over TLS	
	Note: Explicit TF over TLS (default: yes)	r P port configured on the General settings page
	Listen for implicit FTP over TLS connections on the	e following ports (default: 990):
	990	3
	File transfer security	
OK	These settings need to be enabled for file transfer	rs to be secure.
	Force PROT P to encrypt file transfers when us	sing FTP over TLS
Cancel		No. 1 STORTS

- 1. Valider "Enable FTP over TLS support".
- 2. Valider le mode « Explicite ».
- 3. Valider « Force PROT P à l'encrypter les fichiers et dévalider « Require TLS session ».



www.wit.fr

Dans cette même fenêtre cliquer sur le bouton pour générer le nouveau certificat :

Generate new certificate...

La fenêtre suivante s'ouvre :

		87	
		25	
This dialog will self-signed ce connections. Please fill out the requir confuse clients.	I help you to create a new private key and a rtificate, needed by FileZilla Server to accept red information. Wrong or missing information	TLS may	
Key size: () 1280 bit	2048 bit		
2-Digit country code:			
Full state or province:			
Locality (City):			
Organization:			
Organization unit:			
Contact E-Mail:		4	
Common name (Server address):			
Save key and certificate to this file:	Brows	se	
Generating the certifica	te may take some time depending on the key	size.	
Generat	e certificate Cancel		
]	
-		23	
This dialog wil self-signed ce	l help you to create a new private key and a rtificate, needed by FileZilla Server to accept T	ıs	
Please fill out the requir confuse dients.	ed information. Wrong or missing information r	nay	
Key size: 🔘 1280 bit	22 1 0 4096 bit	1	
2-Digit country code:	fr	/	
Full state or province:			
Locality (City):			
Organization:			
Organization unit:			
Contact E-Mail:			
Common name (Server address):			ź
Save key and certificate to this file:	C:\Users\incomei\Deskt Brows	è	
3 the certifica	ite may take some time depending on the key s	size.	
Generat	e certificate Cancel		

- 1. Indiquer l'indicatif du pays (ex : fr).
- 2. Indiquer où sauver le certificat qui va être généré
- 3. Cliquer sur « Generate certificate » : Generate certificate

Le serveur Filezilla est prêt à recevoir les fichiers en mode sécurisé.



5.3 Glossaire

Le numéro des ports généralement utilisés en fonction des protocoles :

Protocol	No encryption Plain port	TLS/SSL Explicit port	TLS/SSL Implicit port
FTP	21	21	990
SMTP	25 or 587	25 or 587	465
POP3	110	110	995
HTTP	80	-	443



Pour tout renseignement complémentaire, notre support technique se tient à votre disposition par e-mail à <u>hot-line@wit.fr</u> ou par téléphone au +33 (0)4 93 19 37 30



www.wit.fr