

# Premiers pas avec WinPT (cryptographie sous Win)

### EITIC

Logiciel : WinPT site : <u>http://www.winpt.org/</u>

Niveau : Débutant

Auteur : EITIC

date de mise en ligne : 21 01 2003

Licence du document : licence libre GNU/FDL



« Partir de Windows pour découvrir le libre... »

www.framasoft.net

WinPT - premiers pas ...

## WinPT : premiers pas ...

WinPT, logiciel de crypto assure la confidentialité de vos échanges. Attention : l'installation et surtout l'utilisation de ce logiciel requièrent une connexion internet.

#### Installation

Après avoir lu le fichier installation.txt cliquer sur l'icône



Cliquer sur next ... ... et suivez le guide d'installation. 腸 winpt-0.5.13-installer.exe

cliquer sur oui



Quand l'installation est terminée, un raccourci s'affiche sur le bureau

#### Génération d'une paire de clés (clé privée et clé publique)

En fait le logiciel fonctionne de la manière suivante : Il génère une paire de clés :

- la clé privée qui sert à lire les documents cryptés
- la clé publique que les correspondants utilisent pour crypter les documents envoyés au titulaire de la clé privée

A la fin de l'installation cette fenêtre s'ouvre

Cliquer sur oui pour générer une clé

NOTE: Key gene	ration can be a lengthy process!	
Please wait until y generation was fi	you get the message that key nished	
Key type	DSA and ELG (delault)	
Subkey length (bi	te) 1536	
User name	nous	
Comment (options	0	
Email address	nous@eitic.info	
Set expiration dat	e	clear
Passphrase		
Repeat passphra		



Remplissez soigneusement les champs requis comme ci-contre

Choisissez un mot de passe qui ne soit pas un mot existant (mélanger lettres et chiffres)

et MEMORISEZ-LE soigneusement vous ne pourrez pas le récupérer en cas d'oubli

Attention, si vous choisissez une date d'expiration votre clé aura une durée limitée

Le logiciel génère votre clé.	Key Summation	Progress Dialog
Cela peut prendre un peu de	temps	
	GnuPG status	7
l a clé est générée	Key Generation completed	Cliquer sur OK
	ОК	

Il est important de sauvegarder les deux clés générées (publique et privée) sur un autre support que le disque dur, pour prévenir tout risque de crash du disque dur par exemple (vos clés seraient alors irrémédiablement perdues). Attention : il ne sert à rien d'imprimer ;o))

WARNING - Import	tant hint	×
It is STRONGLY reco Remember that your I idea to store them on	ommend that you backup your keyrings because they both contain VER' hard disk can crash or the files can be deleted by accident; so it is a goo h a different mass stoarge like a floppy or CDR!	Y important data. od
Backup your keyring:	s now?	
	<u>Uu</u> <u>N</u> on	

Cliquer sur "oui" et choisissez votre destination de sauvegarde (disquette, cdrom, ...) Ici sauvegarde sur une disquette (à archiver soigneusement !)

Destinat	ion for pubring.gpg		? ×
Da <u>n</u> s:	Disquette 3½ (A.)	- 🖻 🜌	
No <u>m</u> :	cles		<u>E</u> nregistrer
<u>T</u> ype :	All files	<b></b>	Annuler

# Utilisation du logiciel

Une icône est installée en bas à droite de la barre d'état du bureau

Cliquer avec le bouton droit de la souris sur cette icône en forme de clé

Un menu contextuel s'ouvre

C'est depuis ce menu que le logiciel se pilote

Selectionner "Key manager" avant de relacher le bouton de la souris

U 🖓 🖾 🔛 🔛 📈 🦓 00:34
---------------------



Key Manager						
<u>File E</u> dit ⊻iew <u>K</u> ey	Groups Keys	erver <u>G</u> PG	à			
UserID	KeylD	Туре	Keylen	Cipher	Valid	Date
nous <nous@eitic.info></nous@eitic.info>	0xBFBD7250	pub/sec	1024/1536	DSA/ELG-E	Ultimate	2003-01-11
Groups						
Default key: BFBD7250						

L'adresse nous@eitic.info est associée à une paire de clés (publique et privée : pub/sec) créée le 11/01/2003. Sa validité n'est pas limitée dans le temps (ultimate)

# Envoi de la clé publique sur un serveur de clés (nécessite d'être connecté à internet)

Pour que les correspondants éventuels puissent envoyer des documents cryptés, il faut qu'ils possèdent la clé publique de leur interlocuteur. D'où l'intérêt des serveurs de clés qui stockent les clés publiques

Il existe deux manières de procéder.

- Méthode directe
- Méthode manuelle

#### Méthode directe

Sélectionner l'adresse mail concernant la clé, cliquer sur le bouton droit de la souris et choisir "Send to keyserver"

Key Manager			×
Do you really want to	o send '0xBFBD7250' t	o the default keyserver h <u>N</u> on	orowitz.surfnet.nl?

Cliquer sur "oui". Un message d'alerte vous prévient de la bonne réalisation de la procédure....

#### Méthode manuelle

Il faut tout d'abord éditer la clé publique

- sélectionner la clé concernée dans le key manager
- cliquer (toujours avec le bouton droit de la souris) sur cette clé et choisir "copy to clipboard"

Un message d'alerte informe de la fin de l'action

Cliquer alors (toujours bouton droit) sur l'icône de la clé en bas à droite du bureau

Le "clipboard" s'ouvre avec la clé sélectionnée

	l	A			
Key	Mana	iger			
<u>F</u> ile	Edit	⊻iew	<u>K</u> ey	Groups	Keys
Use	rID			KeylD	
nous		Copy to Paste I User IE Subke Sign Revok Delete List Sig	o Clipb irom Cl )'s ys e jnature	oard ipboard	
		Refres Send t	h from o Keys	Keyservei erver	r:
		Set as	defaul	t key	

BEGIN P Version Gnu Comment For	GP PJBLIC KEY PG v1 0.6 (Min info see http	BIOCK gW32) - WinPT (//www.gnupg.co	0513 19	
QGiBD4fVagR GGiVtscB3H1 %7GD3j0R2Pp %15XWRc4Rc80 clxCL+9c1DX INf7niSuOGN EwSufScb/7/ IZBbv1kDc81 vacOpmZh4p3 Bm51+AcqQa9 Kjtb1My6A72 becISCVNhDM NTOvc1+aIs7 PhycAhDSAtq YwAnRAJh7Nj ASvF END PGF	BACcTru9q6BcN/ 4:RXF8cDAwENUM O02A3YjcmWaZEI qWsZo12s:OUD/3 zKhG3dPhGP+dI7 ngCff1wuULhDkh BD4fVs80BgC?wd 59tjfEQKdJBrx6 85c0q0WhQpjNWa DI++JN3K1BXYQm pE+c1BfM9EsAAW p2HTKVPk1WZnv2 cAJB5GEuP4M0Ic 3RvBNR1Tdr6JmG VWippxGcYpnP5Y krFanKcLPSj317 PUBLIC KEY EI	+vpItFBVUPB1NH ussrI7MHiXs2VP H1MYopyuY497G5 e16YAeq7vJh5dg 31z4pW+4XCVR7J Oh8O+10vMo1h/z hHjPPej3wM7D95 KaAJTSGir2OqDE RaaUbGX6gwHqHd VNrB46dpwF9B.z UF/052q2601Aj9 07YS+nVCFirit1 EFuXo7EhYFvZy1 FKw7+1KKTHMws6 8CN4hGBBgRAgAG 5YH4f/AJ9PEaXM	if:5bf1e362ML6gu JWSkJyZUVIRsIArs mObpYnjBvJOrsh9 ftyw2A/cQqFEFyZO gixDlP1euNobGHW1 skAnJZzLU2EF6K5 J6pXW7E2B:OI5C/G stgws3CRuPmtU9CU JTH10dV7Skb7L0zD US1XVXLP.Skm6dIW JNA1XzoE+nJne9cc 40SythpLsLgNugmT IZPF6tNifyaPrgSF C/0SDT4GiUGnnYC6 B0I4H1bPAAcJEAH7 Ji0znMtCsNmhIVJC	1VaVvG91 HF1LrBaW +wCguqbW PnZYBJQ *uP062fI tcD62gIT wjqIvOpH wIFTpDEO 6+9VyIr9 7RbcvK87 g2E16t85 71krYEvm tV/OpTZr 7Åi/vKJQ 4rf+2Q==
				Contractor and a line of the

Il faut alors envoyer cette clé sur le serveur

Se connecter à

La fenêtre de ke

	🗯 Welcome to KEYSERVER . NET (PGP Public Keys Server) - Mozilla
	<u>File Edit View Go Bookmarks Tools Window H</u> elp
Serveur de clés	clés   et s'ouvre     Home   Bookmarks   ADD   ADD   ADD   FIND A KEY   CHOOSE ANOTHER   ADD   AKEY   Settings)   Cliquer sur "Add a key" et coller dans la zone de texte la clé publique sélectionnée dans le clipboard
eyserver.net s'ouvre	Ids_         s'ouvre         Image: ADD of the marks         Image: ADD of the ma
	ADD A KEY (more settings) CHOOSE ANOTHER CRYPTO TH
RIND A KEY (more settings)	
A KEY	Cliquer sur "Add a key" et coller dans la zone de texte la clé publique sélectionnée dans le clipboard
	Attention pour copier cette clé il faut bien veiller à ce que la sélection couvre tout le bloc de texte et rien que le bloc de texte,

Paste your key here: pas une ligne vide Uwl81jaTz8EFL7MJixUyeh Cliquer alors sur le bouton "submit this key to the keyserver" cOBlaXRpYy5pbmZvPohXBBI

La réception de la clé est confirmée

AdlkCL+9c1DXngCffjwuOLH



## Chercher une clé publique sur un serveur de clé

Connecté au même serveur : <u>Serveur de clés</u> Cliquer sur "find a key" Entrer l'adresse concernée

Plusieurs options sont proposées

- Short list (liste des clés)
- List with Certificates (liste des clés et adresse des personnes les ayant signées, c'est à dire attestant que la clé présentée appartient bien à l'adresse citée. C'est ce que l'on nomme "un réseau de confiance", nous en parlerons par ailleurs.
- Show the key "Fingerprint" (le "Fingerprint" c'est l'immatriculation de la clé qui identifie précisément cette clé.

Choisir "Short List" et "Show the key "Fingerprint"". Cliquer sur "Get List"



Voici le résultat de la recherche Notre clé publique est donc bien enregistrée sur le serveur de clés

Search Results	belgium.keyserv
Your query on: "nous@eitic.info"	
To get a key, click on its Key Id. Click on <u>Search</u> to make another query.	Primary Name or Identifier Secondary Name or Identifie
Type Key ID Name	Size Created
BFBD7250 nous <nous@eitic.info> Fingerprint = 1D5A 9225 3EAC E344 351E 79F1 0.</nous@eitic.info>	1024 2003/01/10 1D9 6408 BFBD 7250

## Acquérir la clé publique d'un correspondant





1000 Contraction (1000 Contraction)	Key Manager File Manager	
1	Edit clipboard	
1	Clipboard	•
	Current Window	•
	Preferences	•
8	About GPG	
33	About	
	Exit	

Cliquer (toujours bouton droit) sur l'icône de la clé (en bas à gauche du bureau) et choisir "edit clipboard"

#### Clipboard Editor BEGIN PGP PHBLIC KEY BLCCK-Version: OpenKevServer v1.2 Comment: Extracted from belgium keyserver net mQGiBDxT79sRBADFZvZ5WFoVpY2rcPiGx0hV7DXN1Oazn YDCyo76XcrJ0G6KCH3jNEZ+KqtlvW4f4Kps1wflPQSCcc jimoPCZjVTVoHoTIARFA/CSD5aAVFRegENKxxIISdwdgd 5Ie819pvJUvPfMd3rMD/10G0vWRKN4wSjzj JBWAJ962QunqnRfjFBc9F8hfnU4m15CGQLd fxaIRgQCEQIABgUCPV14GwAKCRDfKBBMu6MKtGspaKE fCdgxQCqpVJf?GB0I14N2C9xa99mJxE5NDG0HkNoYW50 YmViZXQub3JnFohMB3ARAgAM3Q\_9eca4BQsHCgMEAAcJE pJZcfUiV81FnBN1V1LCf5fyJAJ9g1CD7k97W2khr8i4D5 BQI9jZKYAAoJEHeRQ9mfGs6c3xaAnaqYo4wU/z3KJxqQc Clear OK Copy

Sélectionner tout le bloc

Cliquer (toujours bouton droit) sur le "Key Manager" (en bas à gauche du bureau) et choisir "paste from clipboard"

La fenêtre "key import" s'ouvre, elle indique les références de la clé à importer



ley impo	rt			
Туре	Keylen	Keyid	Date	UserID
pub	1024	0xA1DBE7CE	2003-01-11	eux <eux@eitic.info></eux@eitic.info>
Imp	ort	Cancel		

Cliquer sur le bouton "import", puis sur "ok" dans le message d'alerte annonçant la fin de la procédure d'importation.

Dans le menu "key" du "Key Management" choisir "Reload key cache", la clé importée apparaît dans le liste des clés (publiques bien évidemment !)

Key Manager						
<u>File E</u> dit <u>V</u> iew <u>K</u> ey Groups Keyserver (	<u>a</u> PG					
UserID	KeylD	Туре	Keylen	Cipher	Valid	Date
eux <eux@eitic.info></eux@eitic.info>	0xA1DBE7CE	pub	1024/1536	DSA/ELG-E	Unknown	2003-01-11
nous <nous@eitic.info></nous@eitic.info>	0xBFBD7250	pub/sec	1024/1536	DSA/ELG-E	Ultimate	2003-01-11

Pour connaître les propriétés de la clé importée et vérifier qu'elle appartient bien au correspondant, faire un clic droit sur la clé et choisir "Propriétés"

Comparer notamment le "Finger Print" de la clé, avec celui qui a été adressé par le correspondant.

Key Propertie:			
Type: Public k Key ID: 0xA1D Algorithm: DSA Size: 1024/15 Created: 2003 Validity: Unkno	5/ 857/03 751/05 95 95 95 95 95 95 95 95 95 95 95 95 95		
Fingerprint			
D981 7580 F3	48 F28F 9CA1	B564 07A8	6FE9A1DB E7CE
Ownertrust			
Unknown			Change
0K	Change par	iswi	

Key owntertrust	
Please decide h verify other users checking fingerp	ow far you trust this s' keys (by looking a print from different s
Don't know I do NOT trust I trust marginally I trust fully	, ,
ОК	Advanced

Si tel est le cas, changer le degré de confiance accodé à la clé en cliquant sur le bouton "change" Choisir le degré de confiance souhaité (traduit en français dans l'ordre d'affichage)

- ne sais pas
- pas confiance
- confiance partielle
- confiance totale

Cliquer sur OK et valider le choix dans le message d'alerte

#### **Crypter un document**

Ouvrir un éditeur de texte, par exemple "note pad" (alias le bloc note de windows) Ecrire le texte souhaité

Avec le bouton droit de la souris, cliquer sur l'icône de la clé (en bas à droite du bureau) et choisir "Current Windows" (fenêtre sélectionnée) et "Sign & Encrypt" (signer et crypter)

Sans titre - Bloc-notes Eichier Edition <u>R</u> echerche <u>?</u>	- <b>D</b> ×	
Bonjour,	<u></u>	
L'anniversaire de grand-Mère sera un é important pour toute la famille. Nous comptons sur les enfants pour pré animations et sur les papas pour confe	vénement parer des ctionner un	Key Manager File Manager
énorme gâteau d'anniversaire.	ccronner un	Edit clipboard
Mais chut. gardez bien le secret !		Clipboard 🕨 🕨
	Encrypt	Current Window 🔸
Tante Esther	Sign & Encrypt Sign	Preferences +
	Decrypt/Verify	About GPG About
	11	Exit

UserID		KeylD
eux <eux@eitic.info></eux@eitic.info>	>	0x84BBB
nous <nous@eitic.in< td=""><td>fo&gt;</td><td>0xCFD79</td></nous@eitic.in<>	fo>	0xCFD79
, 「Select key for Sig	ning	
	ning	

Dans la fenêtre "Sign & Encrypt" qui s'ouvre, choisir la clé du DESTINATAIRE du message crypté

Une fenêtre s'ouvre elle indique l'adresse lié à la clé PRIVEE avec laquelle le message sera signée (donc celle de l'EXPEDITEUR et demande la phrase clé (le mot de passe) pour cette clé.

Jser: nous	<nous@eitic.info></nous@eitic.info>
DSA key ID	0xBFBD7250 (main key ID 0xBFBD7250)
and the second second	
ease enter	your passphrase





Il suffit de l'enregistrer dans le répertoire de son choix pour l'envoyer par mail en pièce jointe (attention comme il a été crypté avec la clé du destinataire il ne pourra pas être décrypté par l'expéditeur ! Ceci dit, vous pouvez égtalement le crypter avec votre propre clé afin d'en garder une copie cryptée)

Il est possible de le coller directement dans le corps d'un mail (attention de bien sélectionner tout le bloc avant de copier).

# Le message s'affiche maintenant crypté

# Décrypter un document

Ouvrir le document dans un éditeur de texte (ici "note pad")

Choisir "Decrypt/Verify" en cliquant avec le bouton droit sur l'icône de la clé (en bas à droite du bureau)

Si le message est dans le corps du mail, utiliser directement la fonction "Current Window" -"Decrypt/Verify" avec la fenêtre du mail.

Le plugin (petit module qui apporte des fonctions supplémentaires) Enigmail permet l'envoi de mails cryptés directement depuis mozilla.



# Le "réseau de confiance"

De même que, sur notre ordinateur, nous pouvons accorder (ou non) notre confiance à la clé publique d'un correspondant, il est possible de porter cette information sur un serveur de clé. Signer la clé d'un correspondant c'est dire "j'atteste que cette adresse mail appartient bien à la personne dont le nom est indiqué". "J'atteste également du sérieux de cette personne dans l'usage qu'elle fait de sa clé.

C'est pour cela qu'il ne faut pas "signer" la clé de tout interlocuteur sans le connaitre vraiment. Ainsi se crée un "réseau de confiance" d'interlocuteurs potentiels.

Il est par ailleurs très facile d'envoyer un mail avec l'adresse d'un autre internaute ... Un mail, signé par clé GPG est garanti envoyé par le propriétaire de l'adresse, sous réserve que le "fingerprint" de la clé signataire corresponde à celui indiqué par le correspondant ... ou, si vous ne connaissez pas ce correspondant, que cette clé soit signée par des personnes de confiance... A vérifier facilement sur le serveur.

#### \*\*\*\*\*

Prochain épisode : intégrer Enigmail dans Mozilla et signer la clé publique d'un correspondant sur un serveur