Centre de Calcul - accès depuis windows : Génération clé publique/clé privée pour ssh Paramétrage des utilitaires PUTTY

Objet et contexte:

Pour accéder au Centre de Calcul de l'Université, il faut une paire de clés pour s'authentifier. Cette paire de clés est nécessaire pour toute connexion vers ce serveur; ce qui nécessite un paramétrage des outils que vous utiliserez notamment pour la connexion.

Ce document décrit les étapes nécessaires pour :

- générer une clé publique et privée à l'aide de l'utilitaire PUTTYGEN
- se connecter au centre de calcul avec l'utilitaire PUTTY

Étapes pour la génération de la paire de clé :

- (1) Il vous faut d'abord installer l'utilitaire puttygen puis le démarrer : <u>http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html</u>
- (2) Sélectionner SSH-2-DSA et cliquer sur le bouton « Generate »

le Key Conversions He	In			
Kau	P .			
No key.		<	1	Etape 3
Actions		-		
Actions Generate a public/private key pa	air	C	Generate	
Actions Generate a public/private key pa Load an existing private key file	air		Generate Load	
Actions Generate a public/private key pa Load an existing private key file Save the generated key	air Save	public key	Generate Load Save private key	
Actions Generate a public/private key pa Load an existing private key file Save the generated key Parameters	air Save	public key	Generate Load Save private key	
Actions Generate a public/private key pa Load an existing private key file Save the generated key Parameters Type of key to generate: O SSH-1 (RSA)	air Save) SSH-2 RSA	public key	Generate Load Save private key	

- (3) Bouger la souris afin d'introduire un aléa dans la génération de la clé (cf. indication cidessus)
- (4) Saisir un commentaire dans le champ « Key Comment » puis une passphrase dans le champ « Key Passphrase » et cliquer sur « Confirm »

Key		deal from the	
Public key for pasting ssh-dss AAAAB3NzaC1kc3M xEmLfP3bcZC2KREj b1zFwzWogssBNulb FQC/rm4sM+S99BZI	Into UpenSSH autho IAAACBALOc1wJw9n he28/XeyCaosm4q4Y HjQTC+VEXt+ZNjAgg pazddTS07yogP7wA4	rizea_keys rile: 1xqW5Xns9fPwrRTnk5Jsl '3nFjtKF7PwQ//NReHlda jdqE/lblGvLwSFE5EobqC AlBmsUK2ABx65WpPrl2	E+XN358phZHvm zDhlDfp11wPgmtZ)NcnckQnlDAAAA 8oCUwcHf0rfEDb
Key fingerprint:	ssh-dss 1024 9a:81	:af:e6:29:9c:5d:13:36:e8:	cb:60:2a:82:8a:bb
Key <u>c</u> omment:	delpine@pc-portab	le	
Key p <u>a</u> ssphrase:			
C <u>o</u> nfirm passphrase:			
Actions			
Generate a public/pri	vate key pair		<u>G</u> enerate
Load an existing priva	ate key file		Load
Save the generated k	.ey	Save p <u>u</u> blic key	Save private key
Parameters			
1 aramotoro			
Type of key to genera SSH- <u>1</u> (RSA)	ate: O SSH-2 <u>B</u>	SA 💿 SS	H-2 <u>D</u> SA

(5) Sauvegarder la clé publique SSH2 en cliquant sur « Save public Key » et lui donner un nom avec le suffixe « .pub », généralement utilisé pour les clés publiques.

Public key for pasting	into OpenSSH autho	nrizert_keys file:			
ssn-ass AAAADONzaC1kcOM xEmLfP3bcZC2KREji h1zFwzWnjssRNulhi FQC/rm4sN+S99BZt	AAACDALOc1wJw0i he28/XeyCaosm4q4 HjQTC+VFXI+ZNjAg bazddTS07yoqP7wA	mxqv/5Xns9fPw Y3rFjtKF7PwQ/. gdqF/lblGvLwSI AAl3msUK2ABx	r∏Tnk5JsE+> /NReHidazDi FE5EobqΩNc 65WpPri28oC	(NO50phZHvm hDfp11wPgmtZ nckQnDAAAA (UwcHf0rfEDb	< >
Key fjngerprnt:	ssh-dss 1024 9a:8	1:afe6:29:9c:5d	:13:36:e8:cb:	60:2a:82:8a:bb	
Key <u>c</u> omment.	delpine@pc-portat	ole			_
Key p <u>a</u> ssphiase:					
C <u>o</u> nfini passphrase.					
Jerierate a Jobilic/pin Jave the generated k Parameters Sype of key to genera SSH-1 (RSA) Number of <u>L</u> its in a ge	te key file ey ate: O SSH-2 F merated key:	Save put	Jickey (Load Save pivate kr DSA 1024	зу
		gen Warr Ara you sure wihout a pas	you want t ssphrase to	o save this ki protect it?	∋у

- (6) Sauvegarder la clé privée en cliquant sur « Save private Key » et lui donner un nom avec le suffixe « .ppk », généralement utilisé pour les clés privées.
- (7) Faites un copier coller de l'encadré « Public key to paste into OpenSSH ... » dans un fichier type Notepad au format ANSI au nom de id_dsa_win.pub (pas d'extension .txt)

Étapes pour le paramétrage de PUTTY :

- (1) Il faut installer l'utilitaire putty.exe puis le démarrer : <u>http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html</u>
- (2) Créer la nouvelle session en remplissant le champ « Host Name » par « titan.univ.run » ou « ccur.univ-reunion.fr » et 22 pour le Port

🕱 PuTTY Con	figu	iration	X	
Category:				
🖃 Session	~	Basic options for your PuTTY se	ession	
Logging Terminal Keuboard		 Specify the destination you want to connect the second seco	ect to Port	
Bell		titan.univ.run	22	
Features		Connection type: Raw Telnet Rlogin SSH Serial		
- Appearance - Behaviour - Translation		Load, save or delete a stored session Saved Sessions		
Selection		ccur		
Colours Connection Data Proxy Telnet Rlogin SSH Kex Auth TTY X11		Default Settings ccur	Load Save Delete	
	>	Close window on exit: Always Never Only on o	clean exit	
About		Open	Cancel	

(3) Dans le menu de gauche, aller dans : Connection/SSH/Auth

	ngu	
Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex <u>Auth TTY X11 Turneth </u>	· · · · · · · · · · · · · · · · · · ·	Options controlling SSH authentication Bypass authentication entirely (SSH-2 only) Authentication methods Authentication methods Attempt authentication using Pageant Attempt TIS or CryptoCard auth (SSH-1) Attempt "keyboard-interactive" auth (SSH-2) Authentication parameters Allow agent forwarding Allow attempted changes of username in SSH-2 Private key file for authentication: Browse
About	~	Open Cancel

(4) Parcourir vos dossiers pour indiquer le chemin du fichier contenant la clé privée (le .ppk) en cliquant sur « Browse »

т	(1000)	0-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6
I erminal		Uptions controlling SSH authentication
- Bell		Bypass authentication entirely (SSH-2 only)
Features		Authentication methods
window		Attempt authentication using Pageant
- Appealance Rehaviour		Attempt TIS or CryptoCard auth (SSH-1)
Translation		Attempt "keyboard-interactive" auth (SSH-2)
Selection Colours Data Proxy Telnet Rlogin		Authentication parameters Allow agent forwarding Allow attempted changes of username in SSH-2 Private key file for authentication: C:\Documents and Settings\cri-974\Bur Browse
E SSH ─ Kex ─ Auth		
TTY		
Tunnel		
- I unnels	1000	

- (5) Revenir dans la Session via le menu de gauche
- (6) Entrer un nom comme « titan » ou « CCUR » dans le champ « Saved sessions » puis cliquer sur « Save » pour enregistrer les paramètres pour les prochaines connexions

Session	~	Basic options for your PuT 1	'Y session	
- Logging ⊒ Terminal - Keyboard		 Specify the destination you want to on Host Name (or IP address) 	onnect to Port	
Bell Features		Connection type:		
window Appearance Behaviour Translation		Load, save or delete a stored session Saved Sessions ccur		
Colours Connection Data Proxy Telnet Rlogin		Default Settings ccur	Load Save Delete	
Kex Auth		Close window on exit: Always Never Only	on clean exit	

(7) Cliquer enfin sur « Open »

contributeurs :

Nom	Date	type modifications	version
Delphine Ramalingom	05/05/10	Première version	1.0