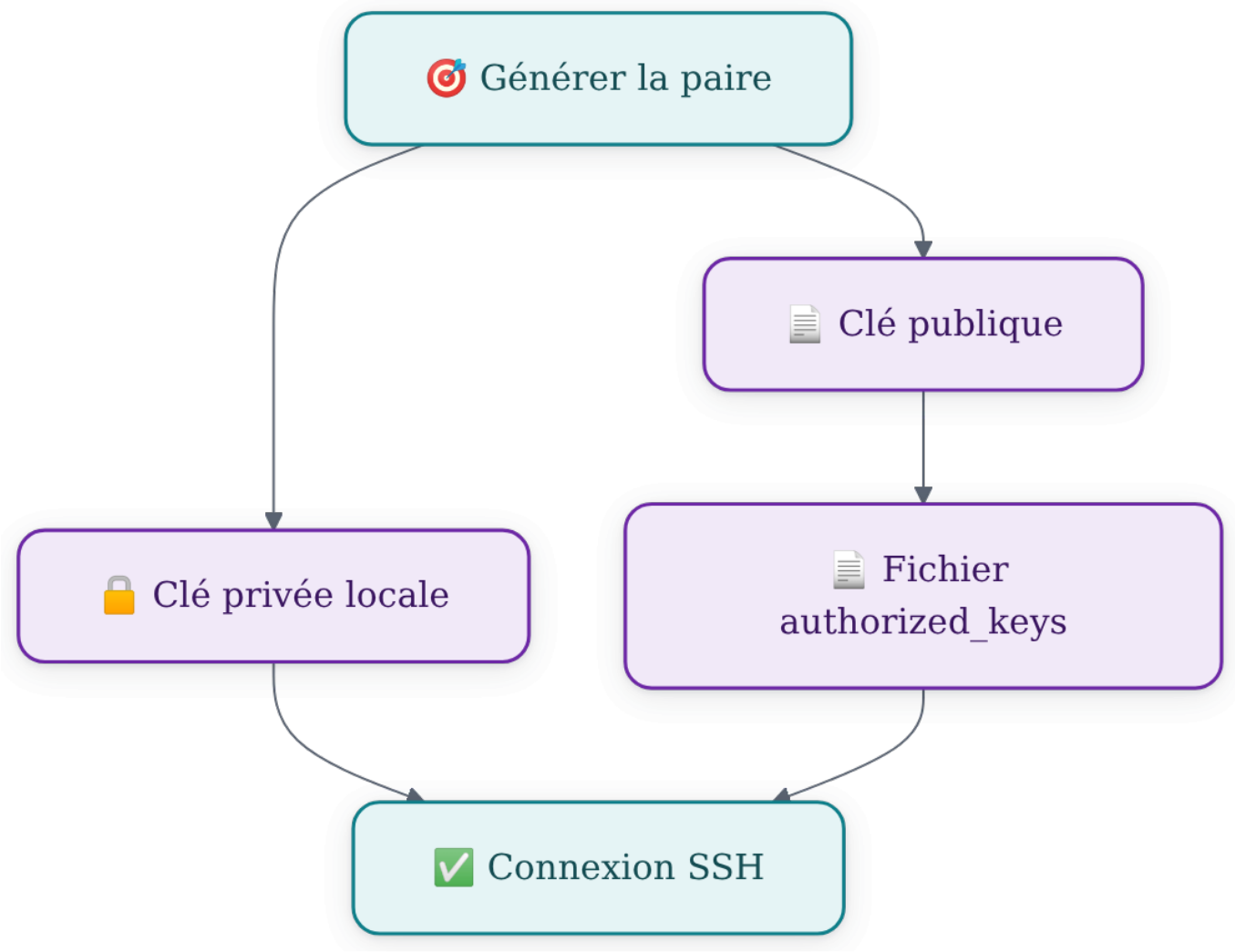
Votre clé SSH Linux : créer, déployer, vérifier, sécuriser

Suivez ce parcours pour mettre en place une connexion SSH par clé depuis votre poste Linux, sans exposer votre clé privée. Cochez chaque étape avant de renforcer l'accès au serveur.

Au sommaire

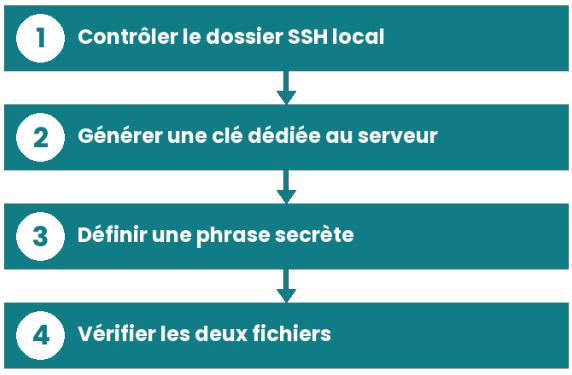
Avant de commencer

- [ ] **Vérifier que le client OpenSSH est disponible**
  Lancez : ssh -V
- [ ] **Identifier le nom d'utilisateur du compte distant**
  Exemple : alice
- [ ] **Préparer l'adresse du serveur**
  Nom de domaine, adresse IP ou alias réseau correct
- [ ] **Noter le port SSH si le serveur n'utilise pas le port habituel**
- [ ] **Conserver l'accès actuel par mot de passe jusqu'au test réussi de la clé**



INFOGRAPHIE *Schéma de création d'une clé SSH Linux et ajout de la clé publique sur un serveur*

1. Créer une paire Ed25519 sur votre poste Linux



1 **Contrôler le dossier SSH local**
Affichez son contenu avec : ls -la ~/.ssh. Son absence n'empêche pas la génération de la clé.

2 **Générer une clé dédiée au serveur**
Utilisez un nom explicite pour ne pas écraser une clé existante : ssh-keygen -t ed25519 -f ~/.ssh/id_ed25519_serveur -C "acces-serveur"

3 **Définir une phrase secrète**
Choisissez une phrase secrète longue et mémorisable : elle protège la clé privée si votre poste est perdu ou compromis.

4 **Vérifier les deux fichiers**
Contrôlez avec : ls -l ~/.ssh/id_ed25519_serveur*. Le fichier sans extension est privé ; celui qui se termine par .pub est public.

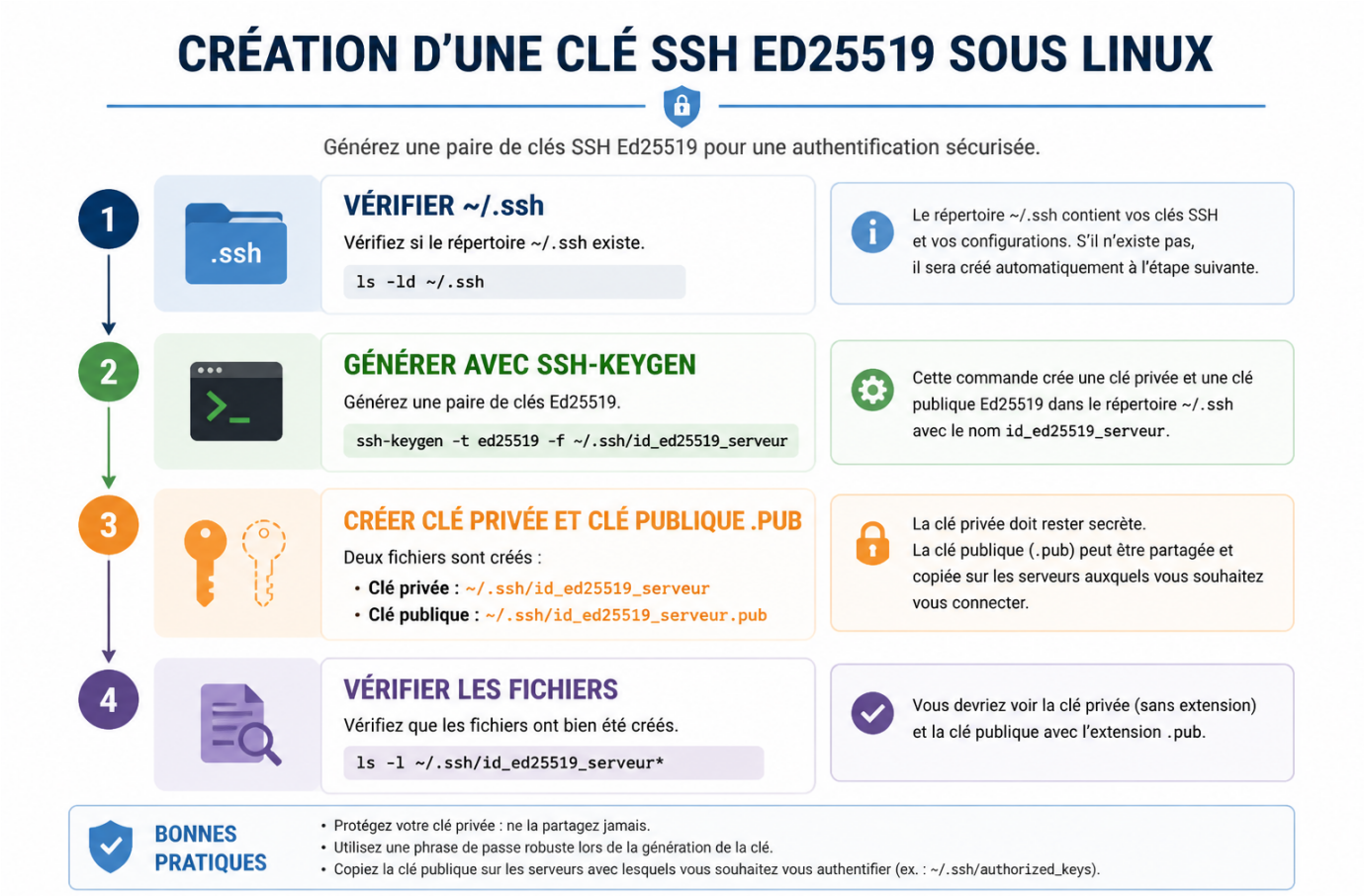
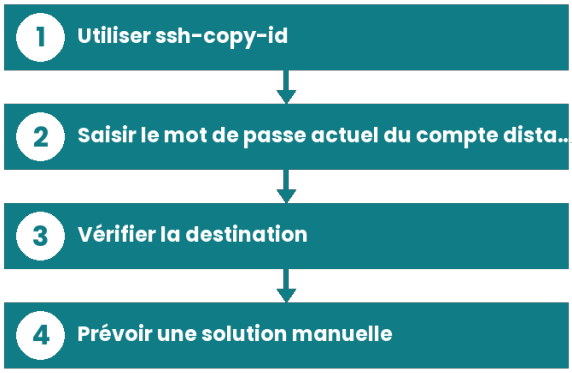


SCHÉMA *Une paire Ed25519 est créée localement : clé privée à conserver, clé publique à déployer.*

2. Installer uniquement la clé publique sur le serveur



1 **Utiliser ssh-copy-id**
Depuis votre poste Linux, installez la clé publique sur le compte concerné : ssh-copy-id -i ~/.ssh/id_ed25519_serveur.pub alice@serveur.exemple.net

2 **Saisir le mot de passe actuel du compte distant**
Cette authentification est généralement nécessaire pour le premier déploiement de la clé.

3 **Vérifier la destination**
La clé publique doit être ajoutée au fichier ~/.ssh/authorized_keys du bon utilisateur sur le serveur.

4 **Prévoir une solution manuelle**
Si ssh-copy-id est indisponible, affichez la clé publique avec cat ~/.ssh/id_ed25519_serveur.pub et ajoutez sa ligne complète dans authorized_keys sur le serveur.

Repère essentiel : quel fichier va où ?

Élément	Emplacement habituel	Règle de sécurité
Clé privée	~/.ssh/id_ed25519_serveur sur votre poste	Ne jamais partager, envoyer ni déposer sur le serveur
Clé publique	~/.ssh/id_ed25519_serveur.pub sur votre poste	À copier seulement vers les serveurs concernés
Clés autorisées	~/.ssh/authorized_keys sur le serveur	Contient les clés publiques acceptées pour ce compte

3. Tester avant de durcir la configuration

- [ ] **Ouvrir une nouvelle session de terminal**
Gardez votre session existante ouverte comme solution de secours.
- [ ] **Tester la connexion**
Exemple : ssh alice@serveur.exemple.net
- [ ] **Confirmer que la connexion utilise bien la clé**
La connexion ne doit pas demander le mot de passe du compte distant si tout est correctement configuré.
- [ ] **Contrôler les permissions si la clé est refusée**
Vérifiez notamment le dossier ~/.ssh et le fichier authorized_keys du compte distant.
- [ ] **Ne modifier l'authentification par mot de passe qu'après un test concluant**

! **Règle non négociable**
La clé privée reste sur votre ordinateur. Ne la copiez jamais dans un e-mail, une messagerie, un dépôt Git, un presse-papiers partagé ou sur le serveur. Seule la clé publique peut être installée dans authorized_keys.

Une connexion SSH par clé ne supprime pas la nécessité de protéger la clé privée : utilisez une phrase secrète et testez toujours l'accès avant de désactiver l'authentification par mot de passe.