🔑 Gestion des Clés SSH

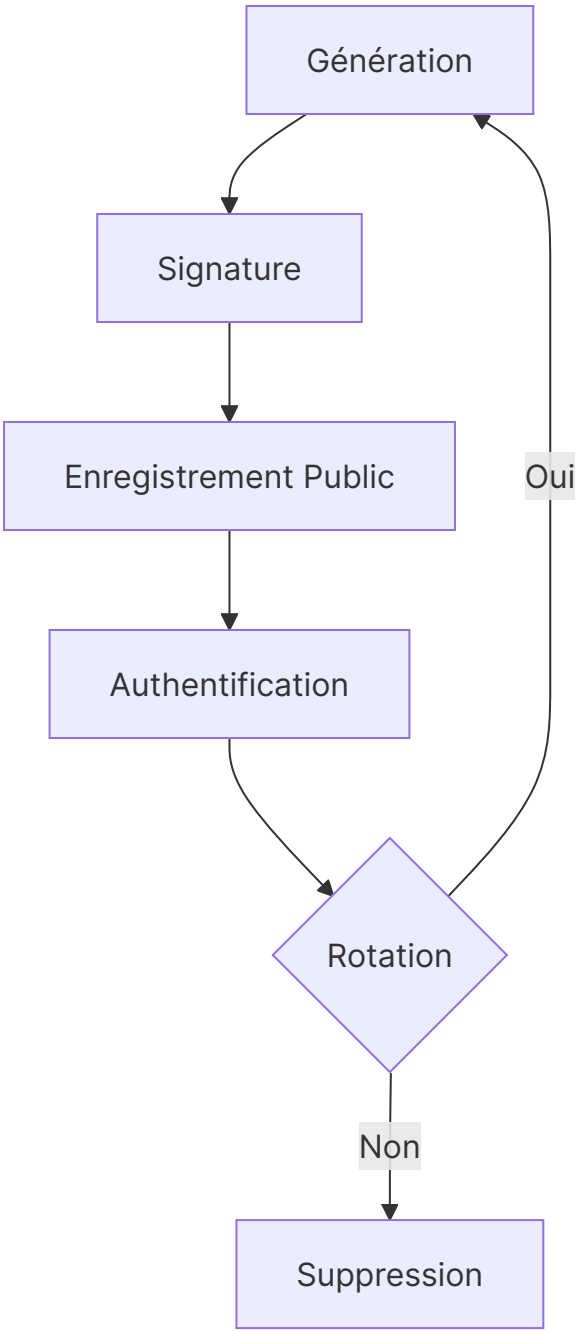
📃 **Abstract**

En Bref :
Cycle de vie complet des clés SSH :

- Génération sécurisée
- Déploiement contrôlé
- Rotation périodique
- Révocation d'urgence

🗝️ Types de Clés

Algorithme	Sécurité	Compatibilité
ED25519	★★★★★	OpenSSH 6.5+
RSA 4096	★★★★☆	Universelle
ECDSA 521	★★★★☆	Linux/BSD



🛠️ Workflow de Gestion

1. Génération Sécurisée

```
# Avec protection par passphrase
ssh-keygen -t ed25519 -a 100 -f ~/.ssh/prod_key -N "s3cr3tP@ss!"
```

2. Déploiement

```
# Copie contrôlée (pas de ssh-copy-id !)
cat prod_key.pub | ssh user@host "mkdir -p ~/.ssh && chmod 700 ~/.ssh && cat
```

```
>> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys"
```

3. Configuration Client

```
# ~/.ssh/config
Host production
    HostName 192.168.1.100
    User admin
    IdentityFile ~/.ssh/prod_key
    IdentitiesOnly yes
```

🔒 Bonnes Pratiques

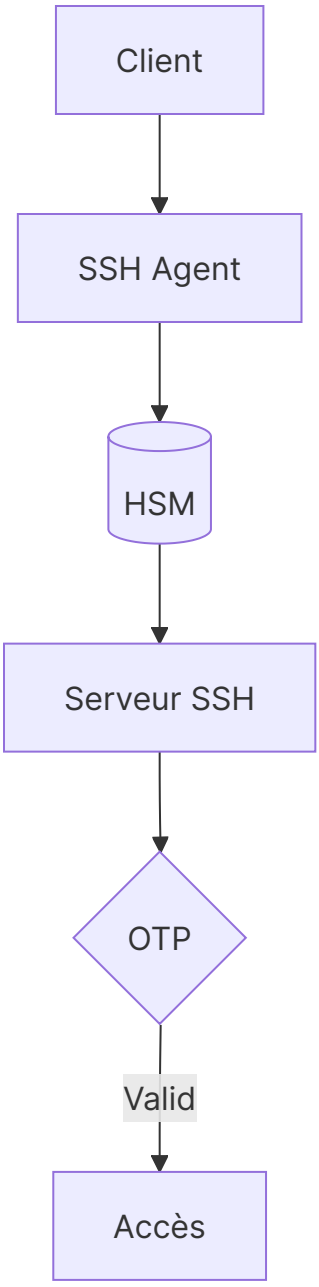
- [x] Utiliser un agent SSH (`ssh-agent`)
- [ ] Stocker les clés privées dans un coffre sécurisé
- [ ] Limiter les clés par serveur avec `from="10.0.0.*"` dans `authorized_keys`
- [ ] Audit trimestriel via `ssh-keygen -l -f authorized_keys`

🚨 Révocation d'Urgence

```
# Serveur compromis
sed -i '/user@host/d' ~/.ssh/authorized_keys

# Client
ssh-keygen -R production  # Supprime l'empreinte connue
```

🧩 Intégration Avancée



Authentification Multiple

```
# Require key + MFA
AuthenticationMethods publickey,keyboard-interactive
```

❌ Erreurs Courantes

1. **Permissions trop ouvertes**

   ```
   chmod 600 ~/.ssh/authorized_keys  # Doit être 600
   ```

2. **Clés zombie**

```
# Trouver les clés inutilisées
lastlog | grep -v "Never logged in"
```

3. **Agent SSH persistants**

```
eval $(ssh-agent -k)  # Tue l'agent après utilisation
```

📚 Ressources

- SSH-Serveur → Configuration associée
- NIST IR 7966 → Standards cryptographiques
- `man ssh-keygen` → Documentation complète