4. Autenticació amb claus i agent SSH

Dos parells de claus amb funcions diferents

Element	On es troba	Per a què servix
Clau privada de host	Servidor, habitualment en `/etc/ssh/`	Acreditar la identitat del servidor
Clau de host coneguda	Client, en `known_hosts`	Detectar canvis en la identitat del servidor
Clau privada de l'usuari	Client	Demostrar la identitat de l'usuari
Clau pública autoritzada	Servidor, en `~/.ssh/authorized_keys` del compte remot	Reconéixer una clau d'usuari autoritzada

En l'autenticació amb clau pública, el client demostra que posseïx la clau privada mitjançant una signatura. **La clau privada no s'envia al servidor.**

Generar i autoritzar una clau

En el client Linux es pot generar una clau Ed25519:

```
ssh-keygen -t ed25519 -C "alumne-sx"
ssh-copy-id -i ~/.ssh/id_ed25519.pub alumne@192.168.0.1
ssh -i ~/.ssh/id_ed25519 alumne@192.168.0.1
```

Si cal RSA per compatibilitat o per la pràctica prevista:

```
ssh-keygen -t rsa -b 3072 -C "alumne-sx-rsa"
```

En generar-la es tria una ruta que no sobreescriga claus necessàries. El fitxer sense `.pub` és privat; el fitxer amb `.pub` és públic. `ssh-copy-id` necessita una via d'accés inicial al compte, habitualment la contrasenya.

Una frase de pas protegix la clau privada emmagatzemada. Per tant, entrar amb claus no sempre significa entrar sense cap petició de secret: es pot demanar la frase de pas de la clau.

Permisos

En el client:

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/id_ed25519
chmod 600 ~/.ssh/config
```

L'última ordre s'aplica si el fitxer `config` existix. En el servidor, el directori `.ssh` i `authorized_keys` han de pertànyer al compte remot i disposar de permisos restrictius, habitualment `700` i `600`, respectivament.

Agent local i reenviament

`ssh-agent` permet utilitzar una clau desbloquejada sense tornar a escriure'n la frase de pas en cada connexió. Molts escriptoris ja proporcionen un agent. Si no n'hi ha cap disponible, es pot iniciar i carregar una clau:

```
eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_ed25519
ssh-add -l
```

El **reenviament de l'agent** permet que una màquina intermèdia sol·licite signatures a l'agent local:

```
ssh -A alumne@bastio
```

El servidor ha de permetre `AllowAgentForwarding yes`. La clau privada no es copia al bastió, però un equip intermediari compromés pot utilitzar l'agent mentre estiga disponible. Per a arribar a un servidor passant per un bastió, sovint és suficient `ProxyJump`, sense reenviar l'agent.

Referències

- ssh-keygen.
- ssh-agent i ssh-add.
- Autenticació SSH — RFC 4252.