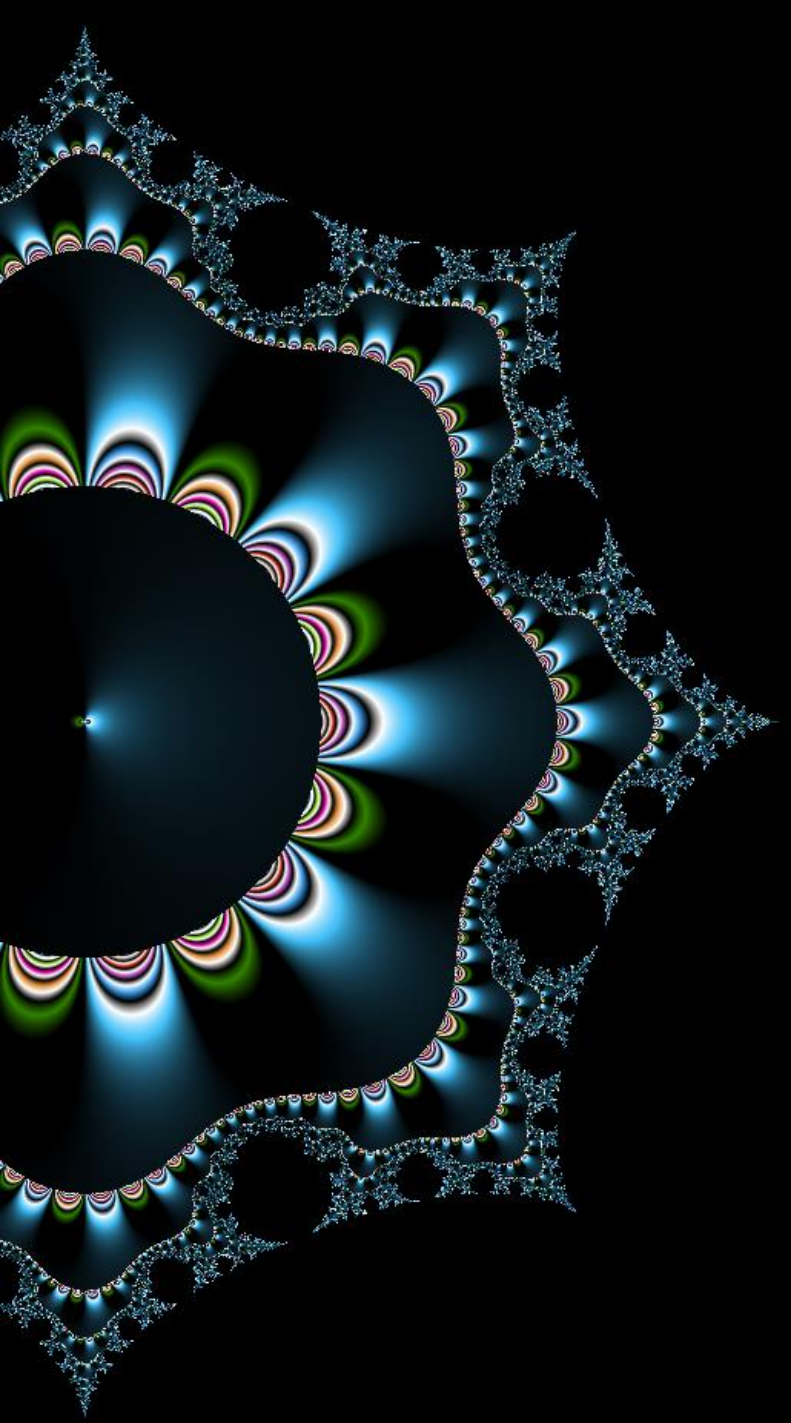


08 Cryptographie

Algorithmes asymétriques

Corinne HENIN

www.arsouyes.org

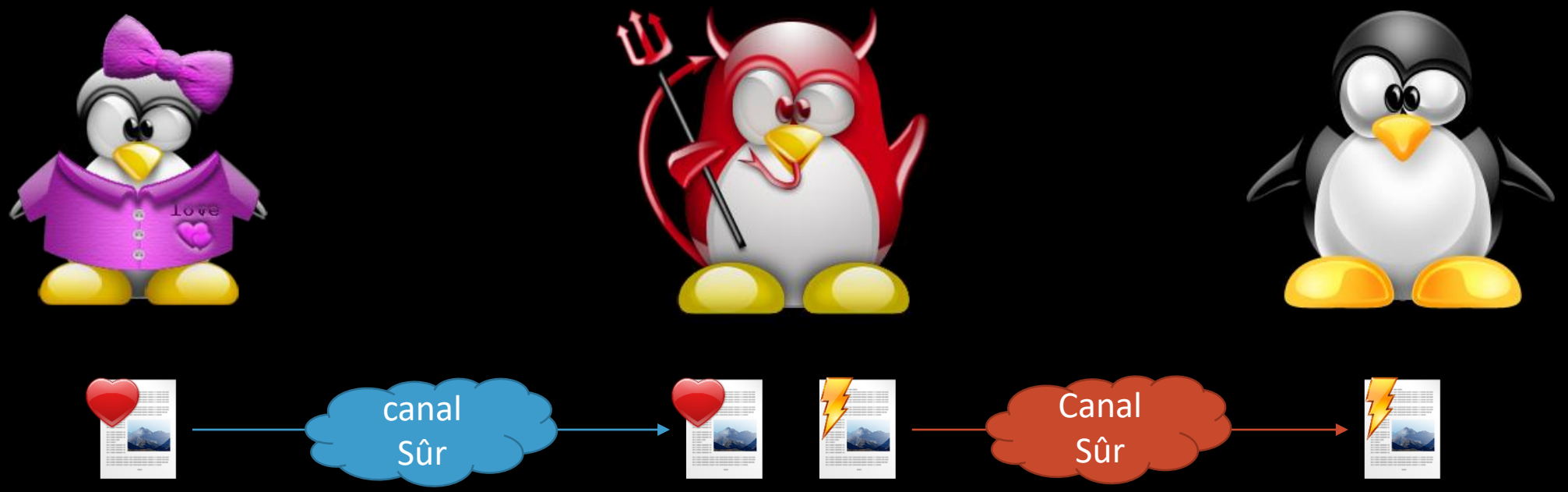
Quel est le problème

Méthodes symétriques

Eve écoute mais ne comprend plus

Et si Eve intercepte ?

Et usurpe les parties ?



Problème d’authenticité

Authentifier les extrémités

(Alice et Bob se reconnaissent)

Algorithmes a-symétriques

Chiffrer et signer les messages

Principe

Deux clés 🔑

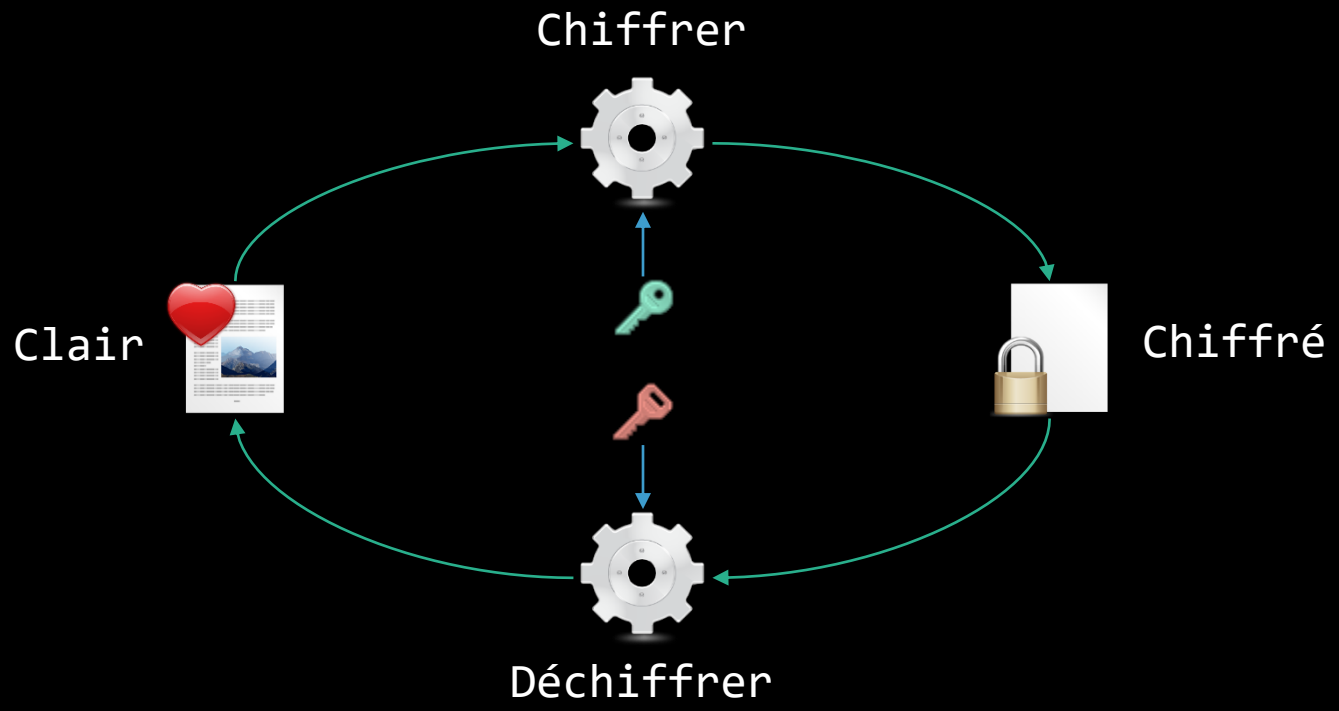
publique 🔑 privée 🔑

Inversent l’une de l’autre

(annulent leurs effets)

Chiffrer avec la clé publique

déchiffrer avec la clé privée

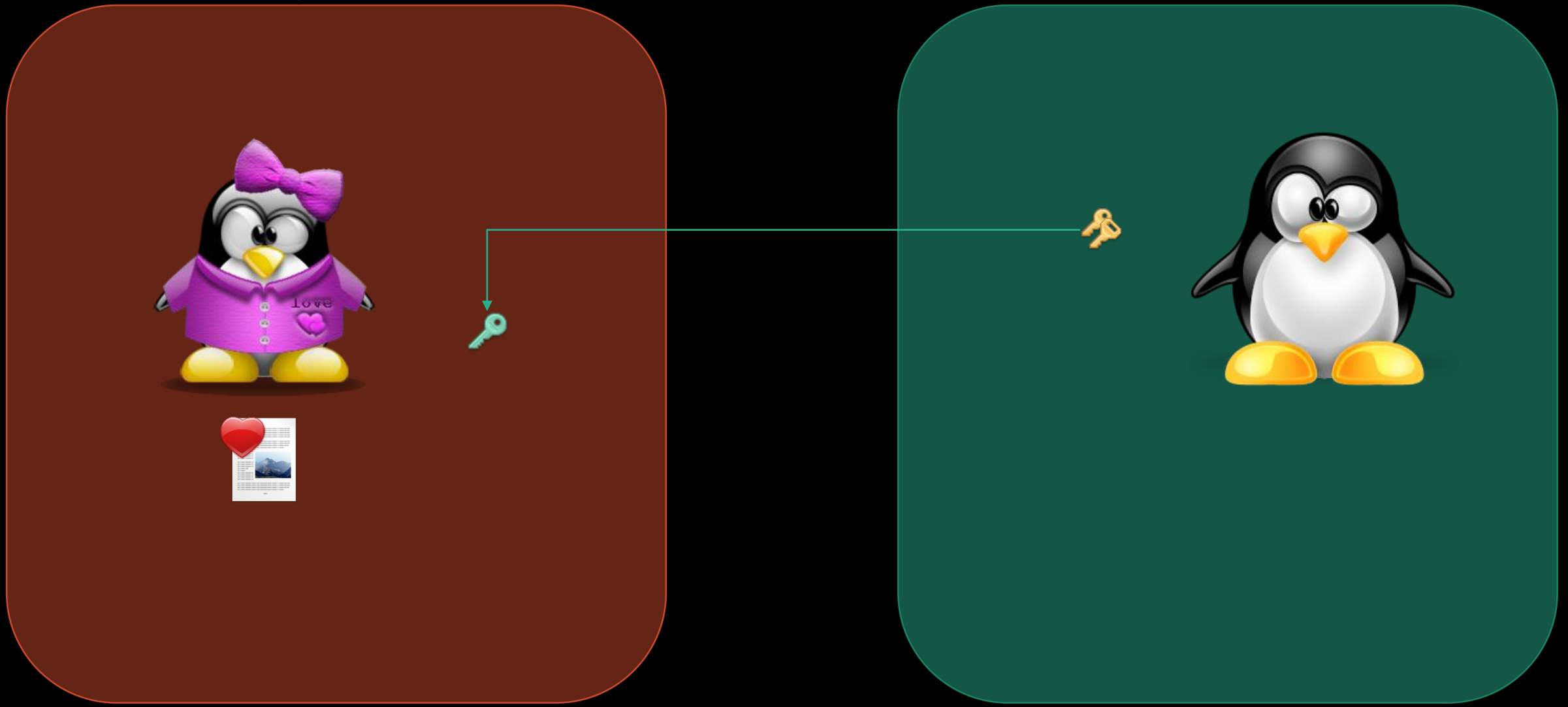


Chiffrer un message

Seul bob peut le lire

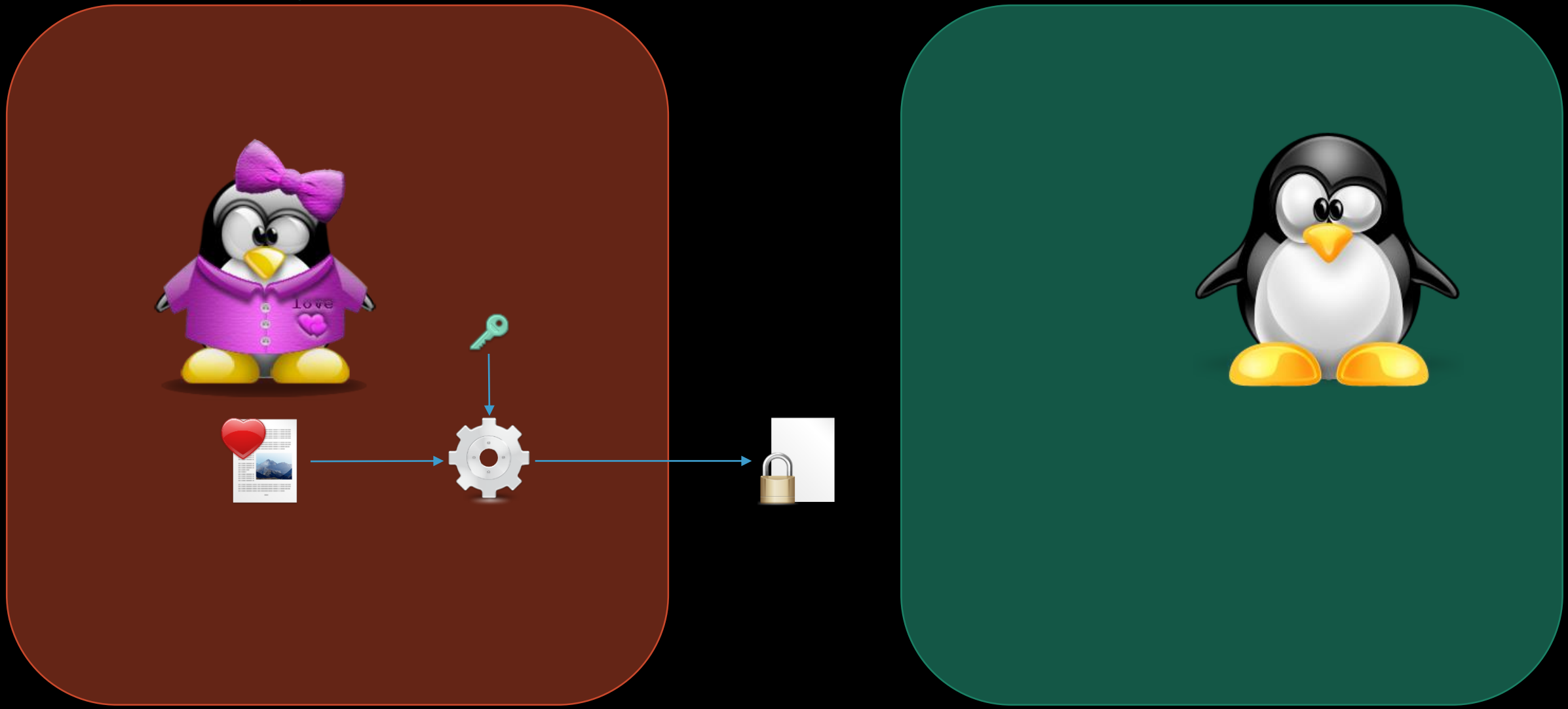
Chiffrer un message

Seul bob peut le lire



Chiffrer un message

Seul bob peut le lire

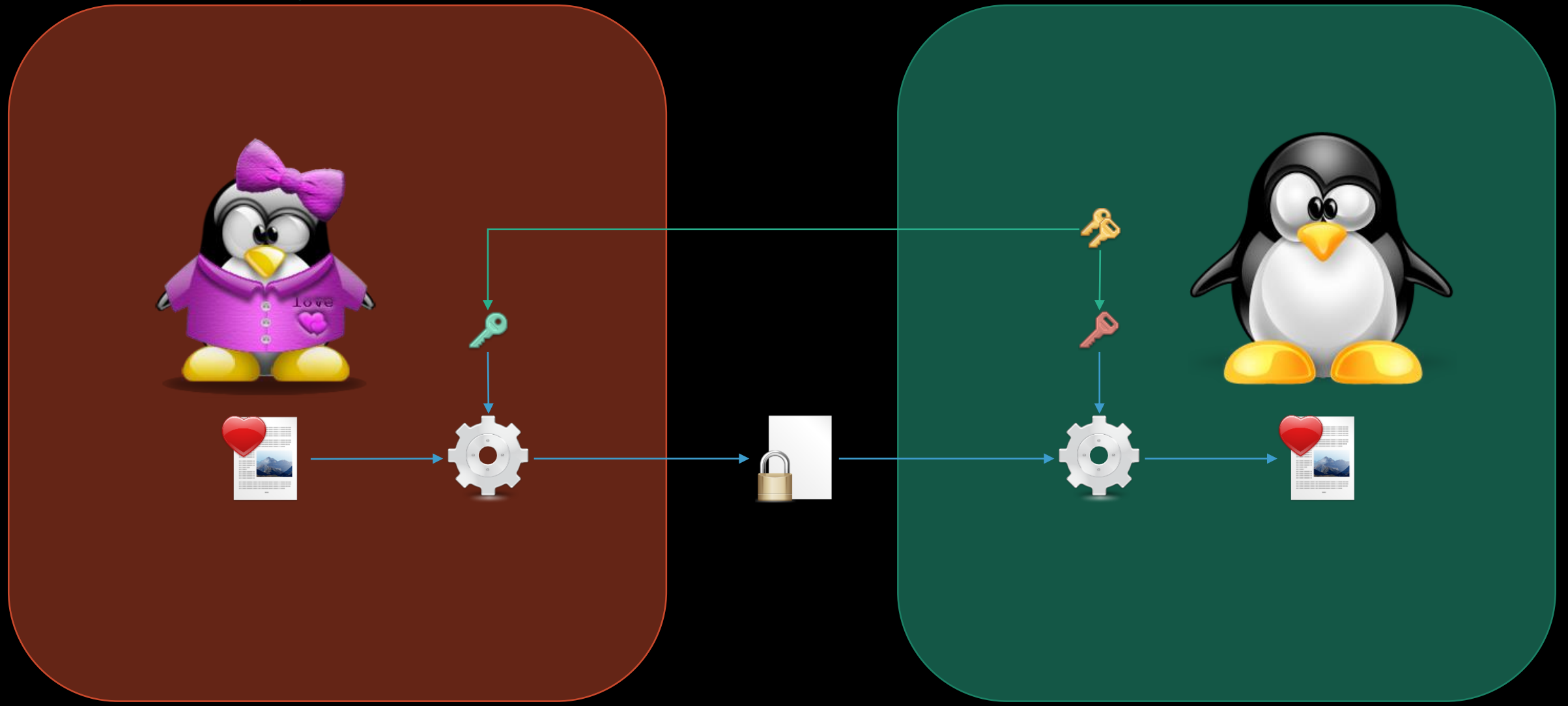


Chiffrer un message

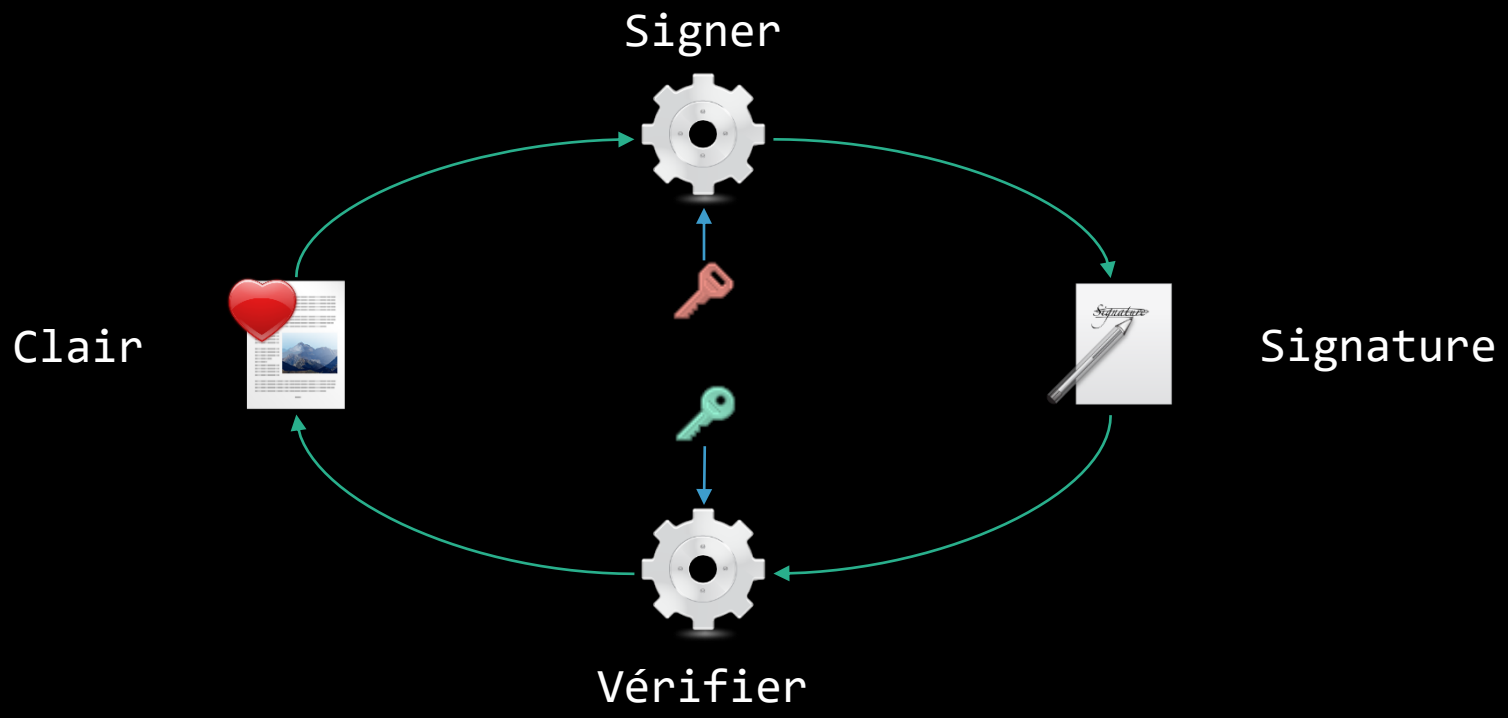
Seul bob peut le lire

Chiffrer un message

Seul bob peut le lire



Signer avec la clé privée
vérifier avec la clé publique

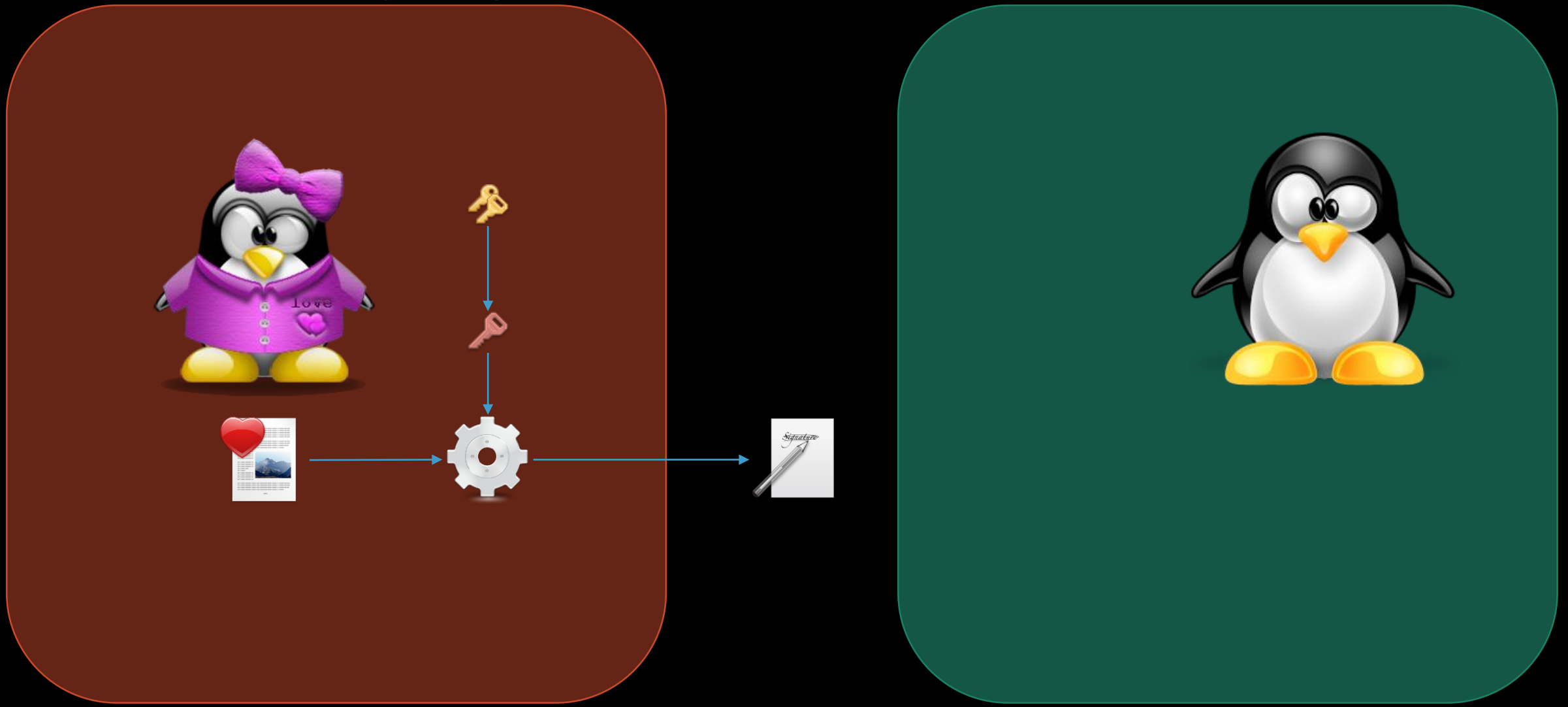


Signer un message

Seule Alice a pu signer

Signer un message

Seule Alice a pu signer

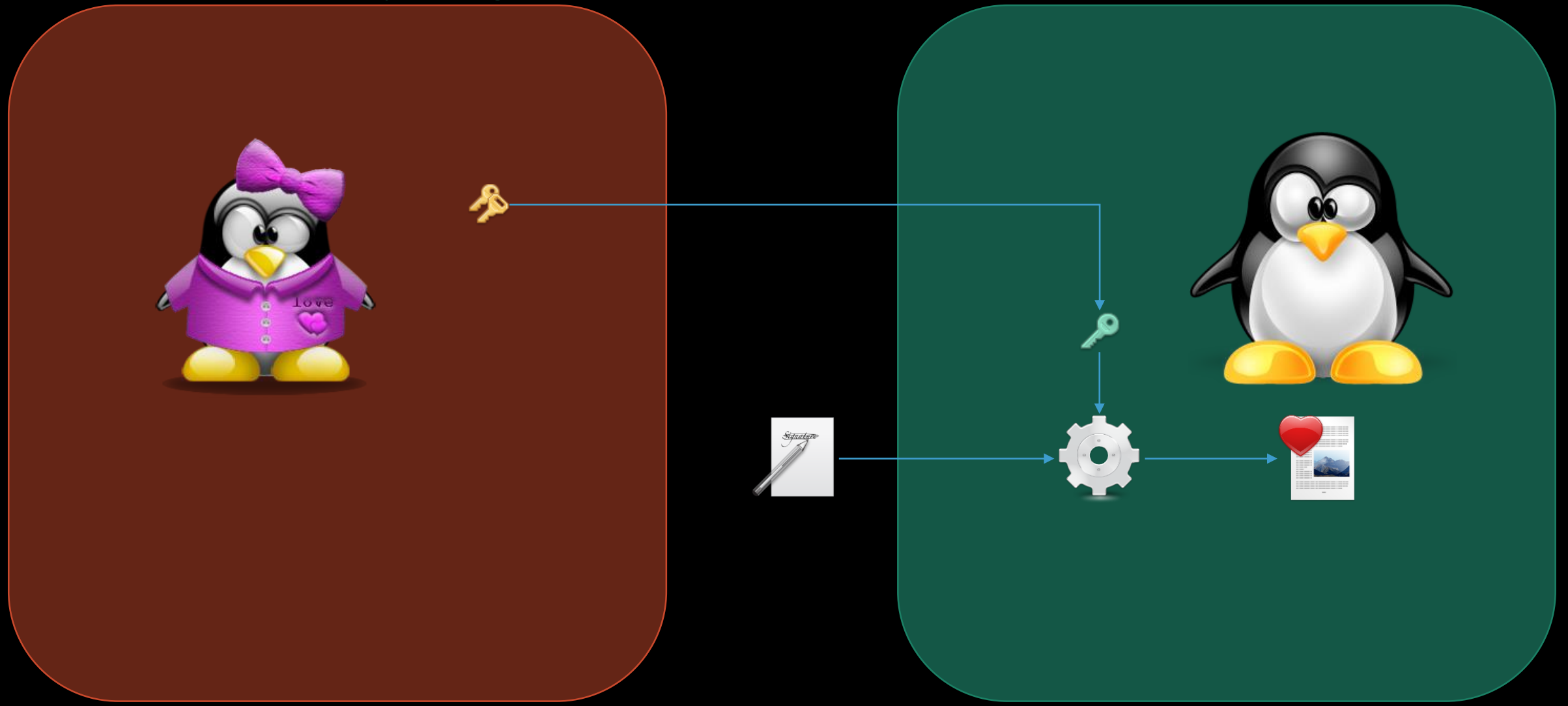


Signer un message

Seule Alice a pu signer

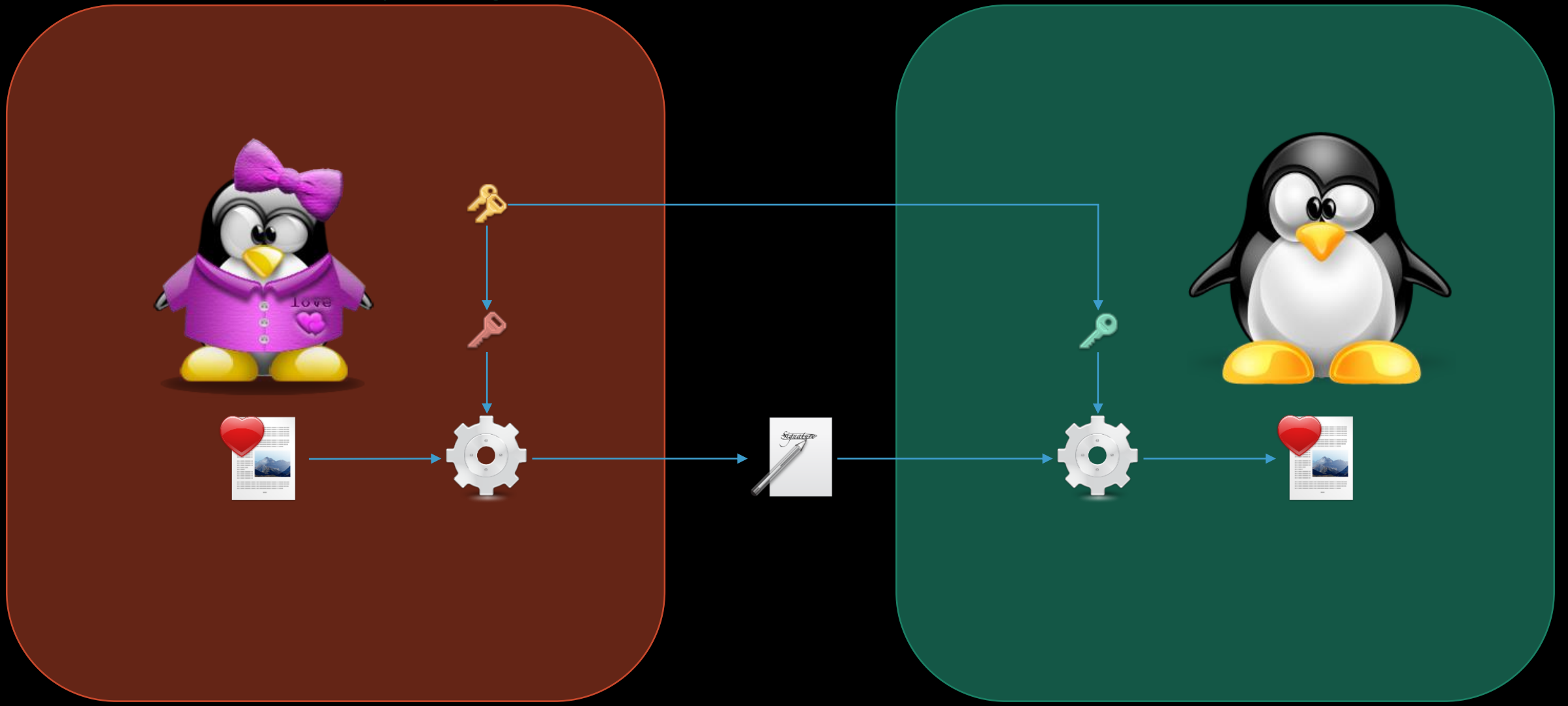
Signer un message

Seule Alice a pu signer



Signer un message

Seule Alice a pu signer

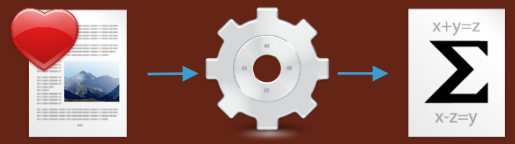


Signer un condensat de message

Seule Alice a pu signer

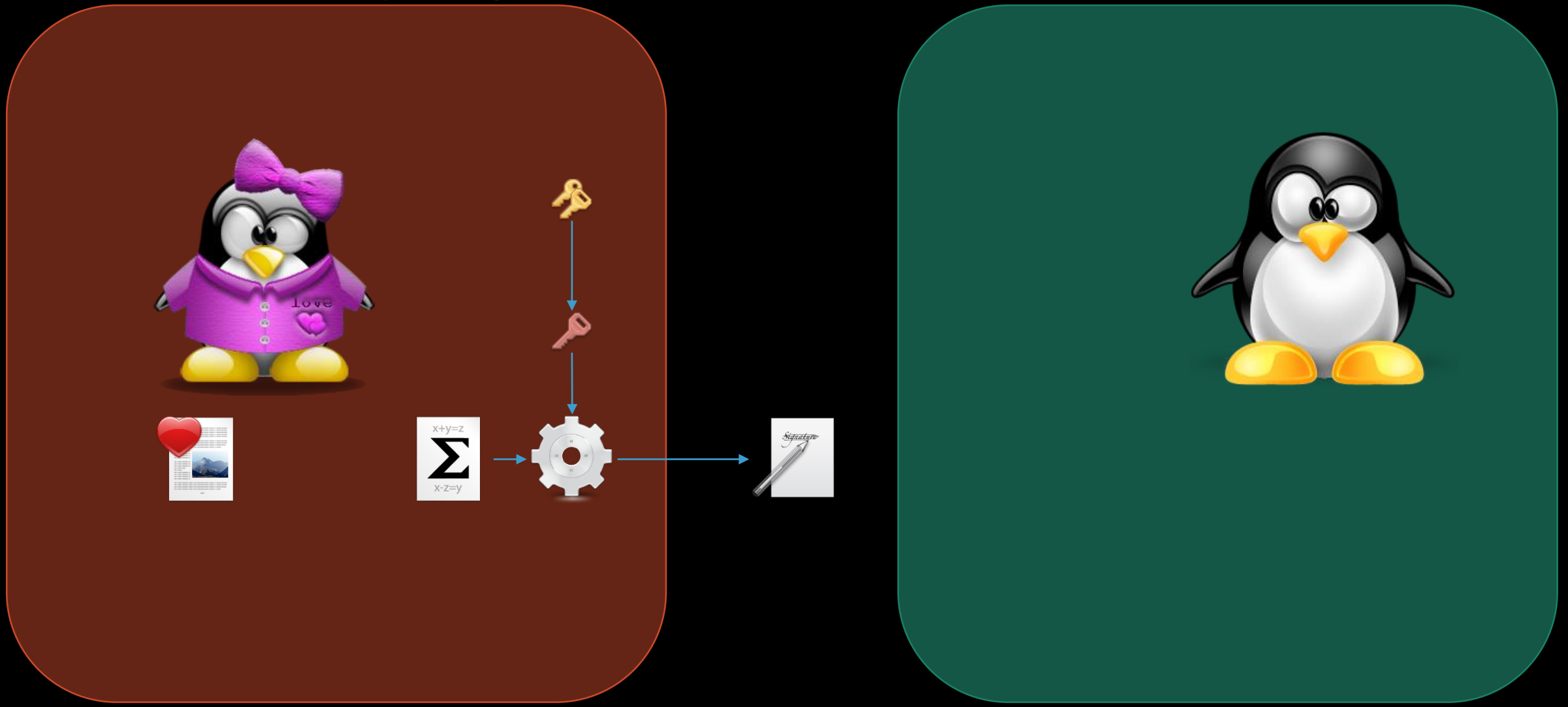
Signer un condensat de message

Seule Alice a pu signer



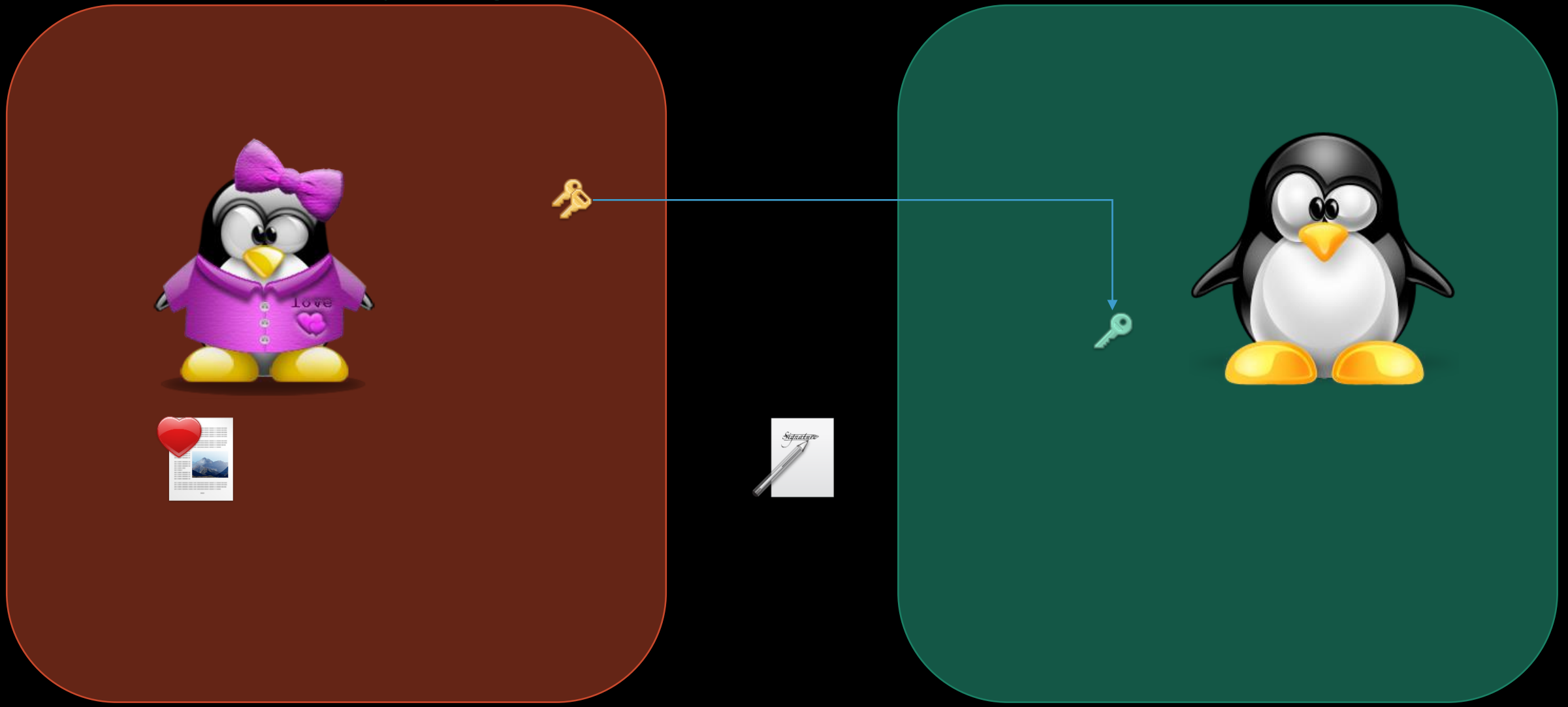
Signer un condensat de message

Seule Alice a pu signer



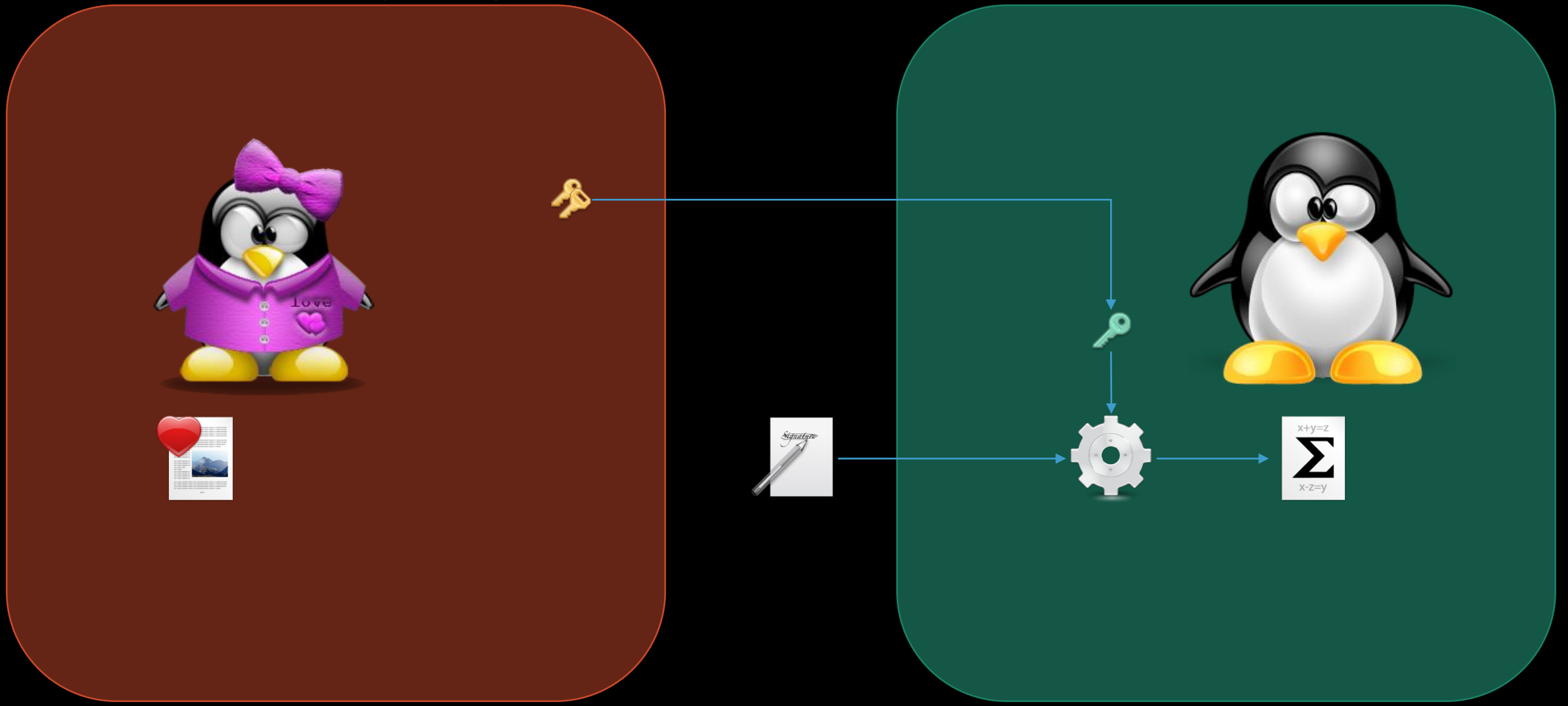
Signer un condensat de message

Seule Alice a pu signer



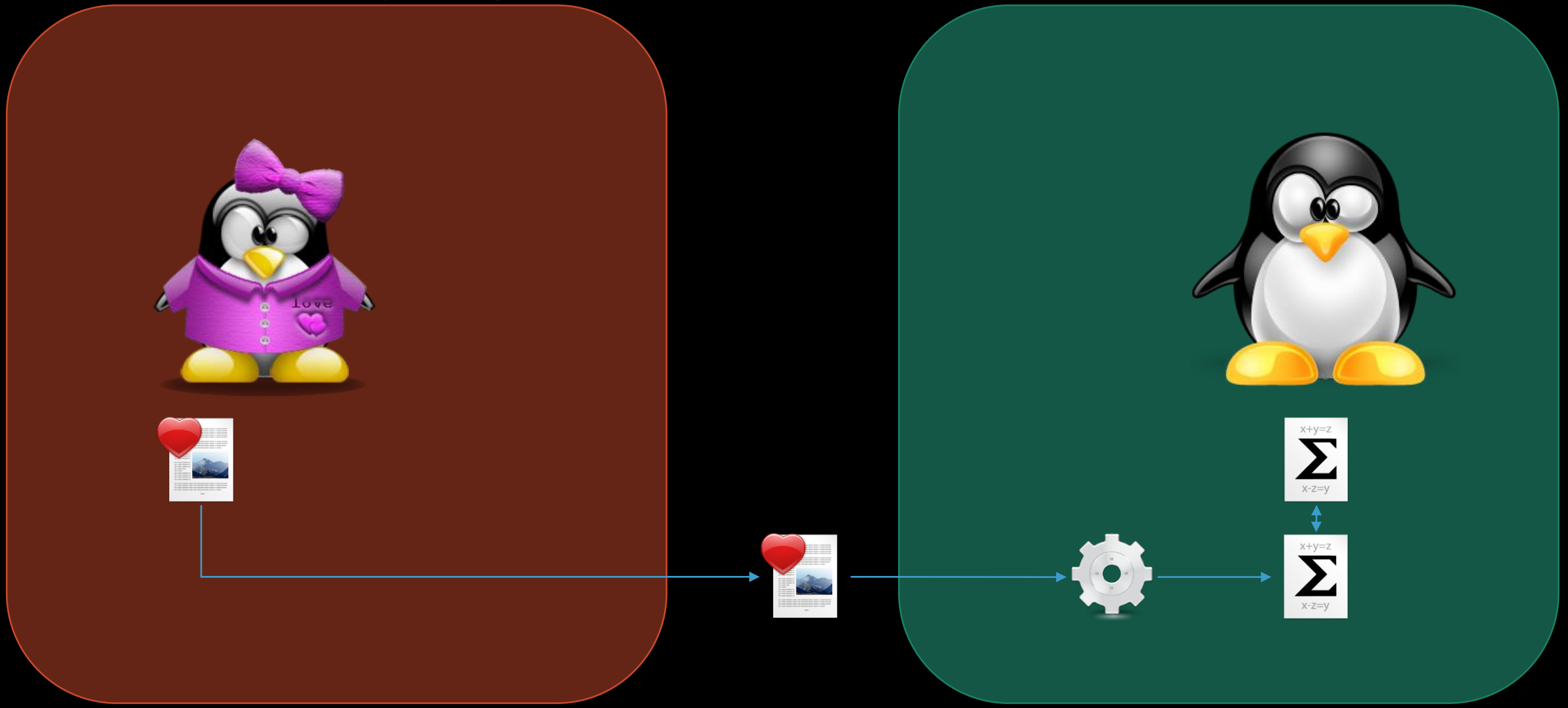
Signer un condensat de message

Seule Alice a pu signer



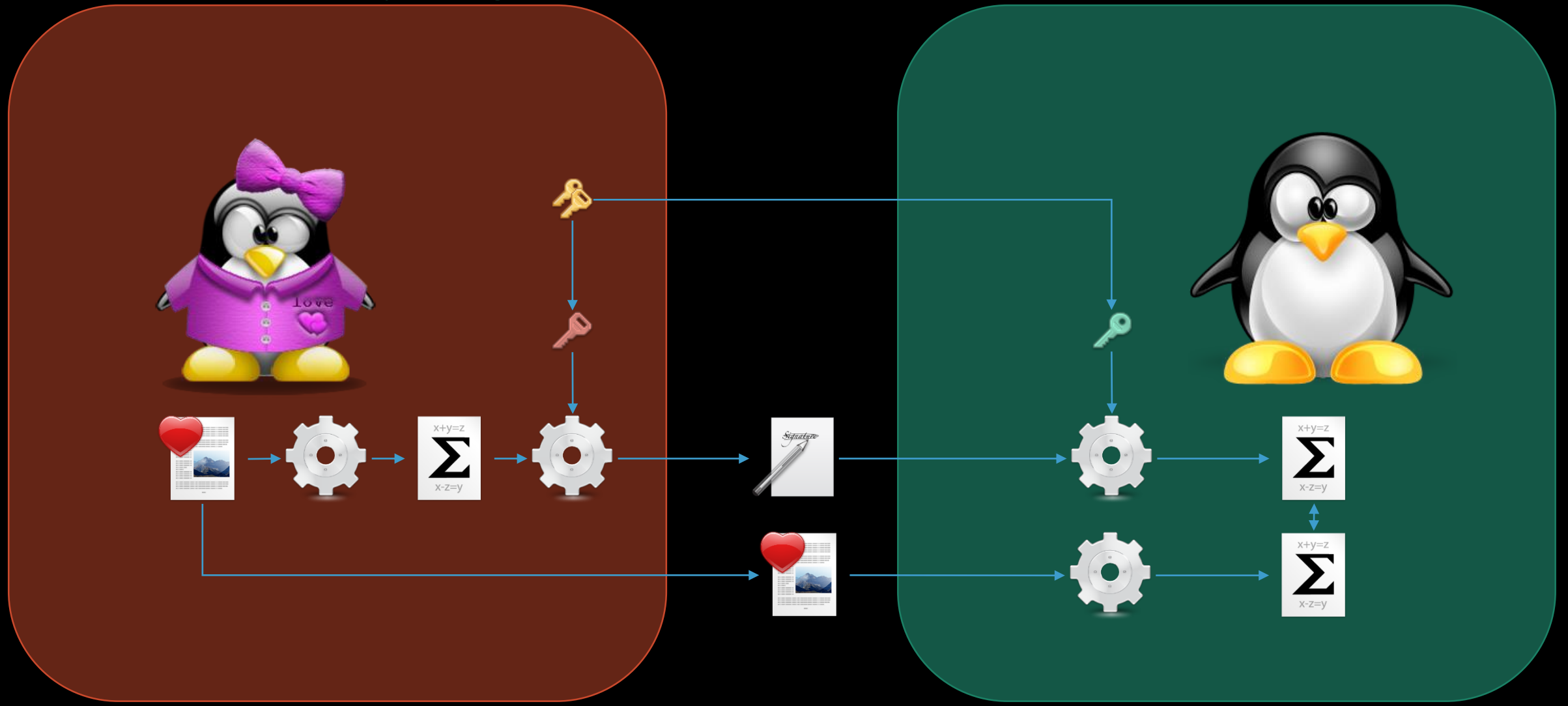
Signer un condensat de message

Seule Alice a pu signer



Signer un condensat de message

Seule Alice a pu signer



Signer ET Chiffrer

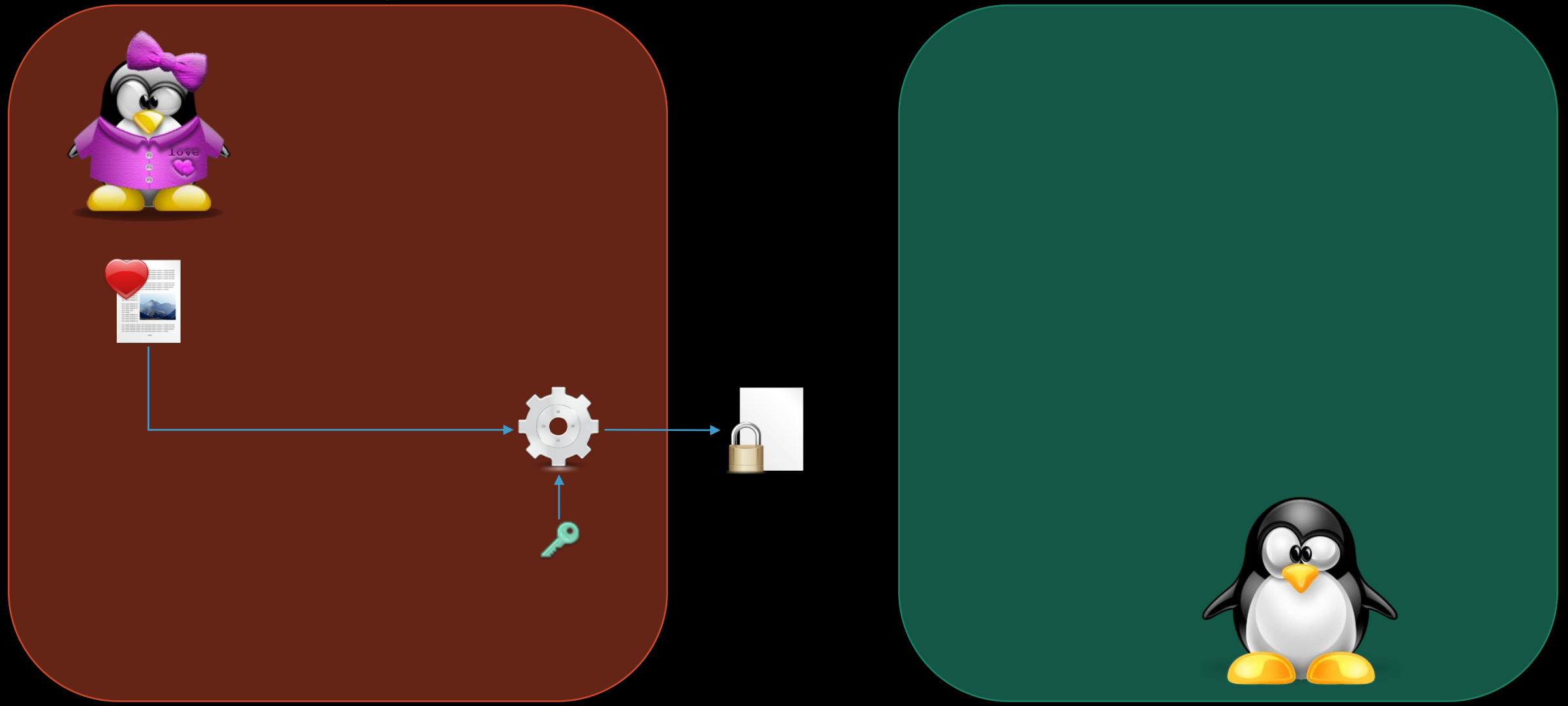
Seule Alice a pu écrire, et bob le lire

Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire

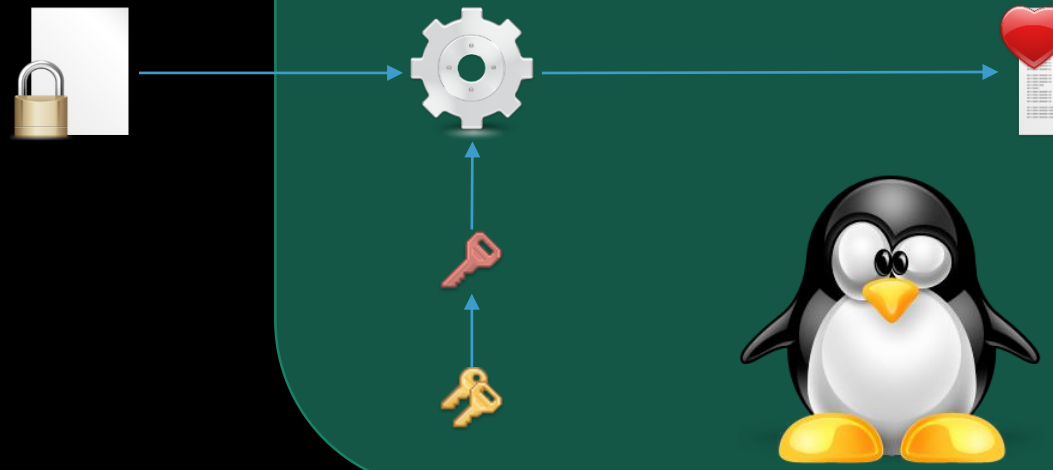
Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire



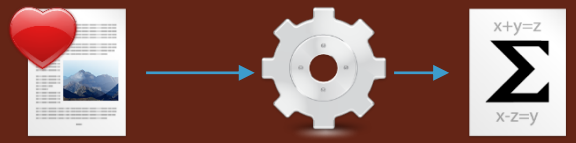
Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire



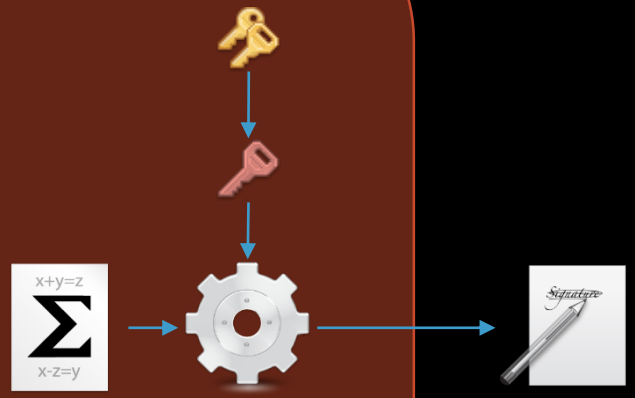
Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire



Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire

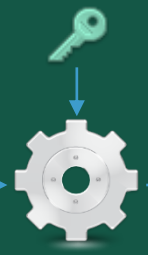


Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire

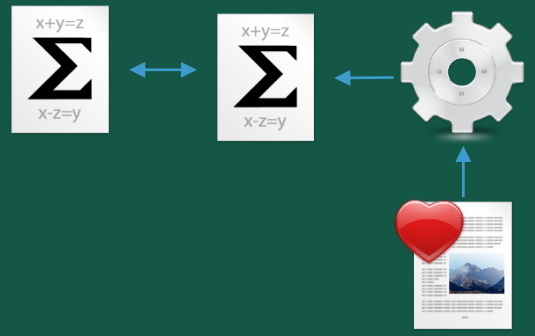
Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire



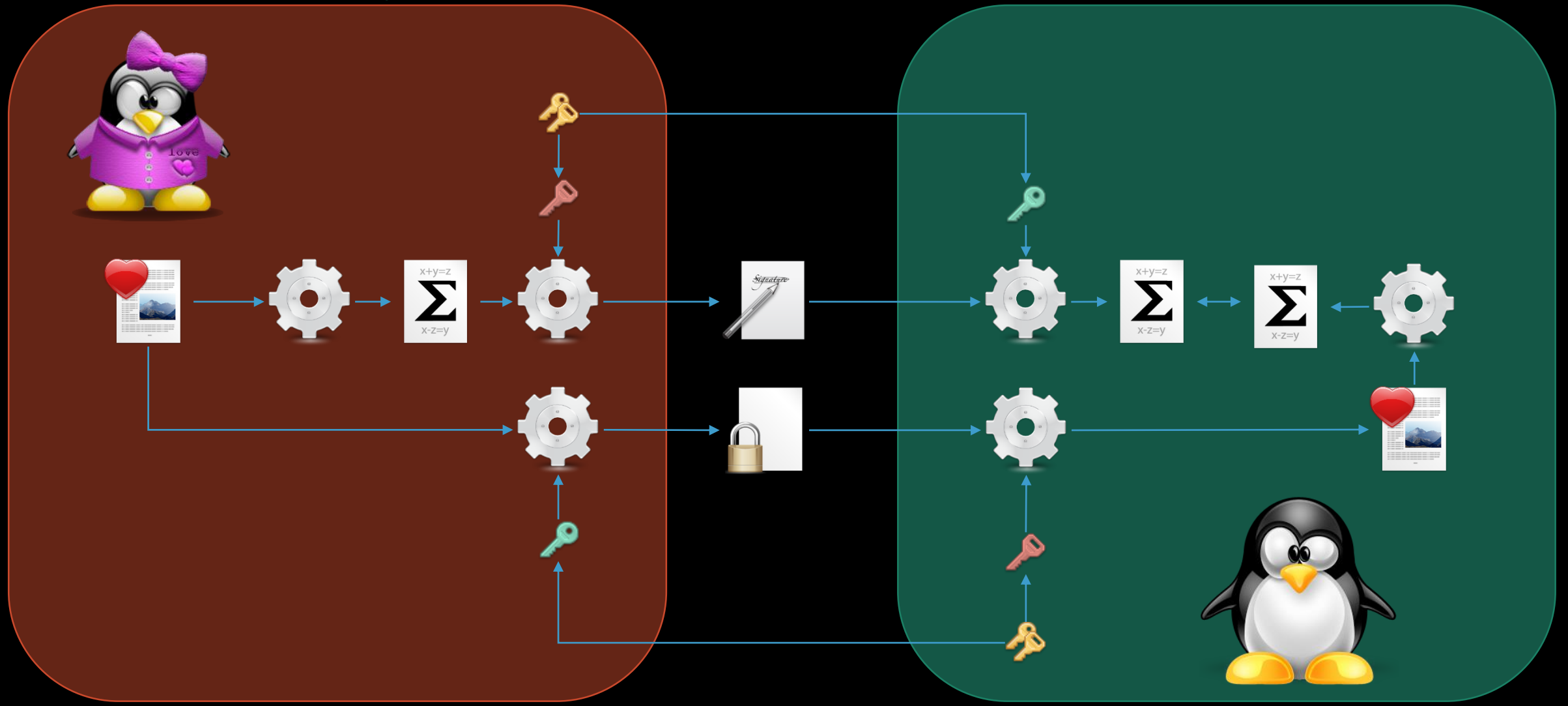
Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire



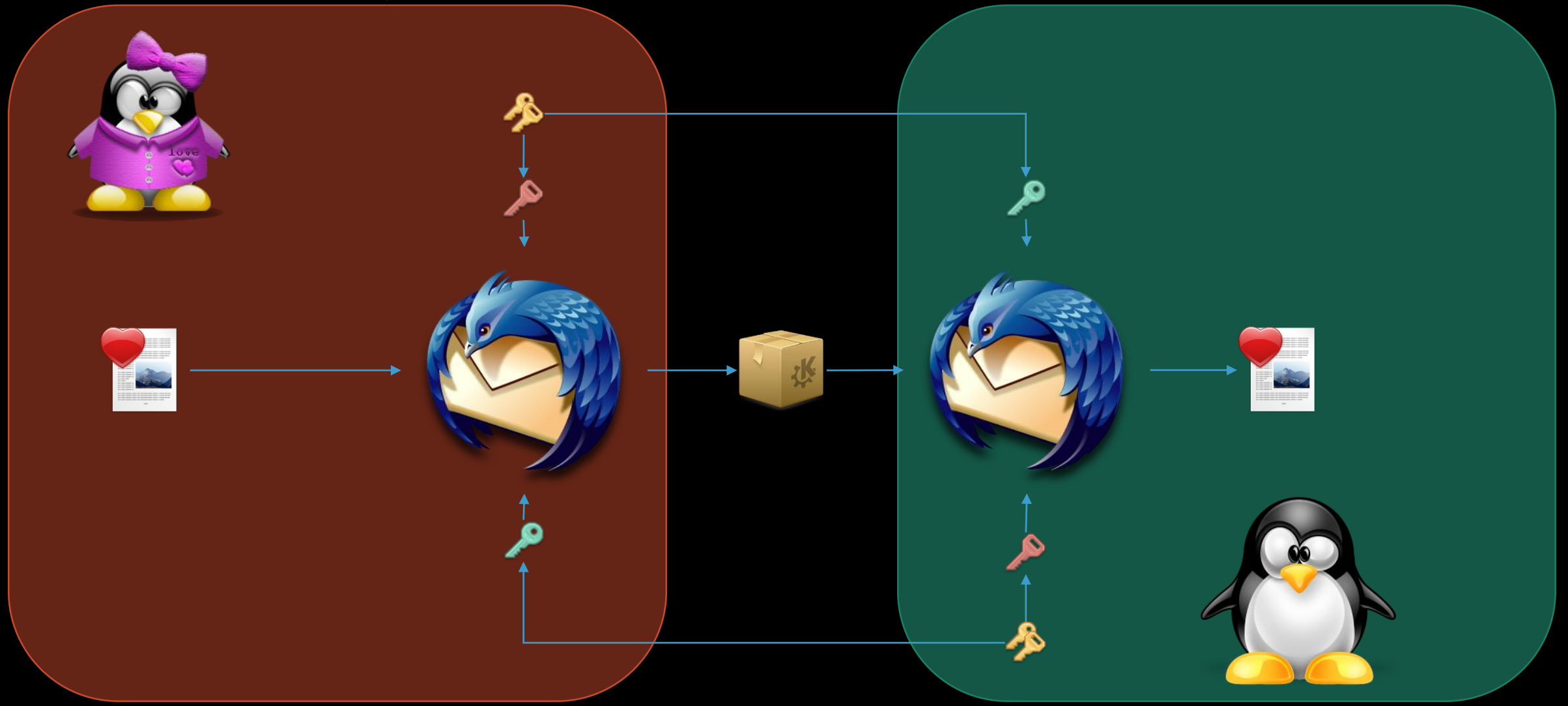
Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire



Signer ET Chiffrer

Seule Alice a pu écrire, et bob le lire



Quelques algorithmes

Nombres entiers, ≥ 3072 bits

RSA

Factorisation de nombres

El Gamal

Logarithme discret

Courbes Elliptiques, ≥ 256 bits

El Gamal

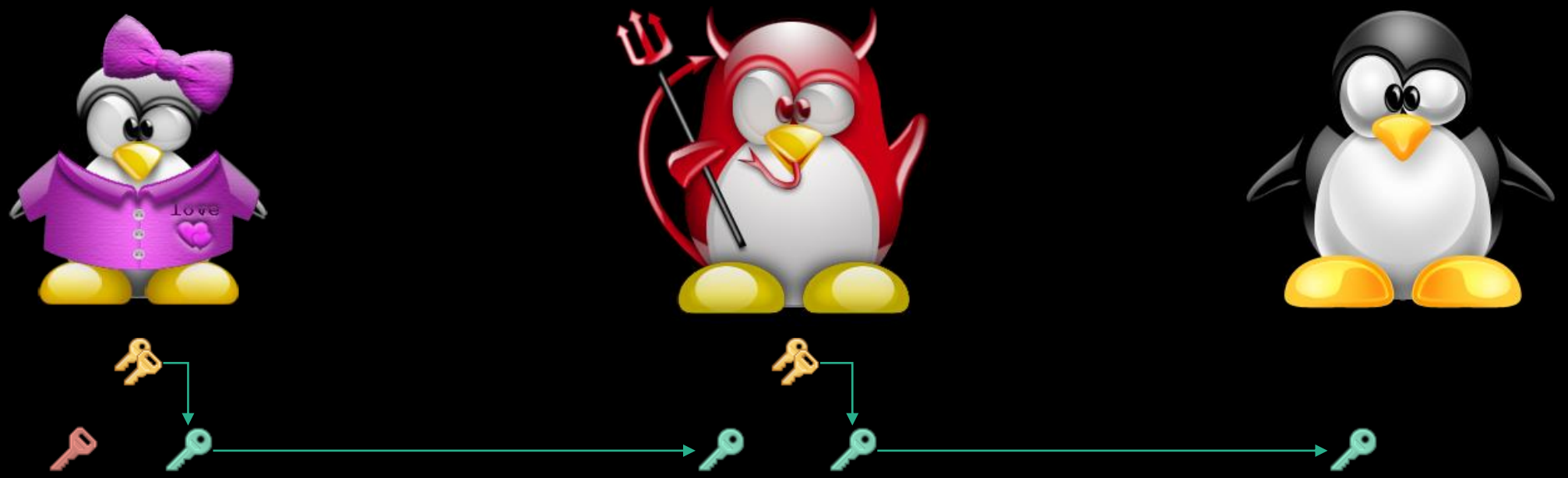
Logarithme discret sur EC

Distribuer les clés

S’assurer de l’identité des propriétaires

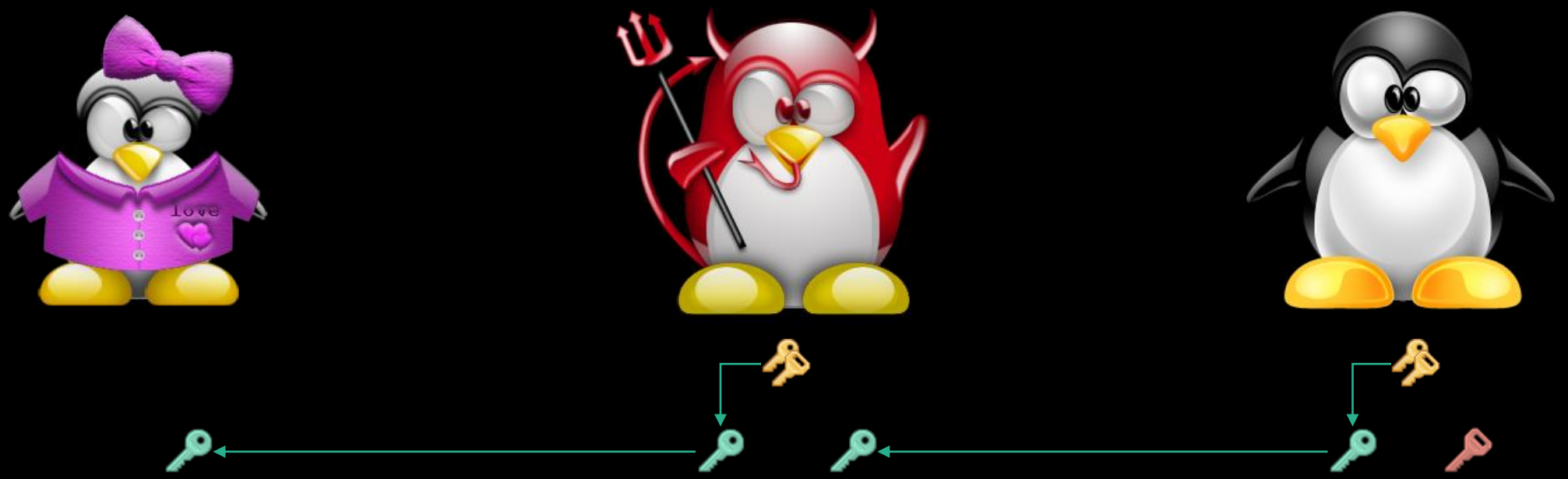
Et si Eve intercepte ?

Et usurpe les parties ?



Et si Eve intercepte ?

Et usurpe les parties ?



Et si Eve intercepte ?

Et usurpe les parties ?

Public Key Infrastructure

Infrastructure à clé publique

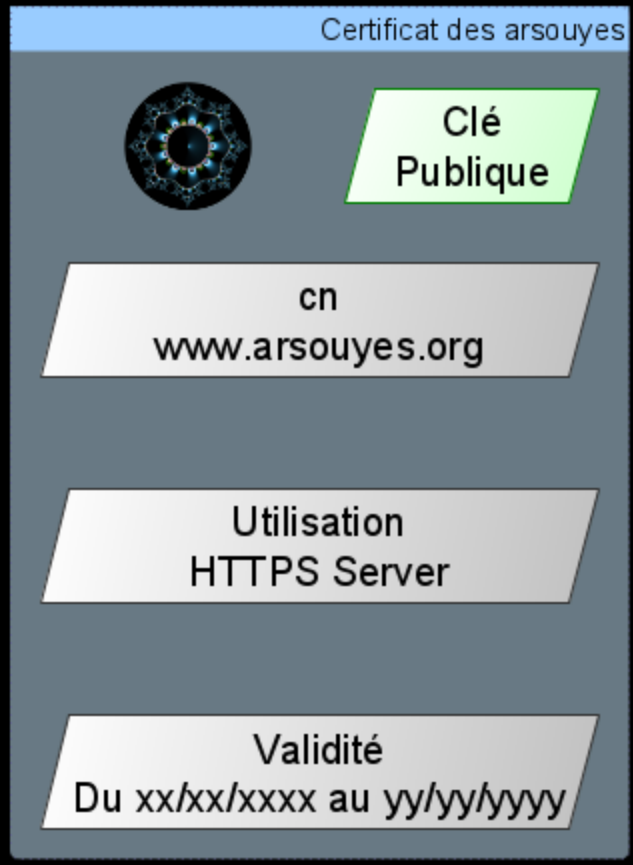
Certificat cryptographique

Clé publique

(et algorithme correspondant)

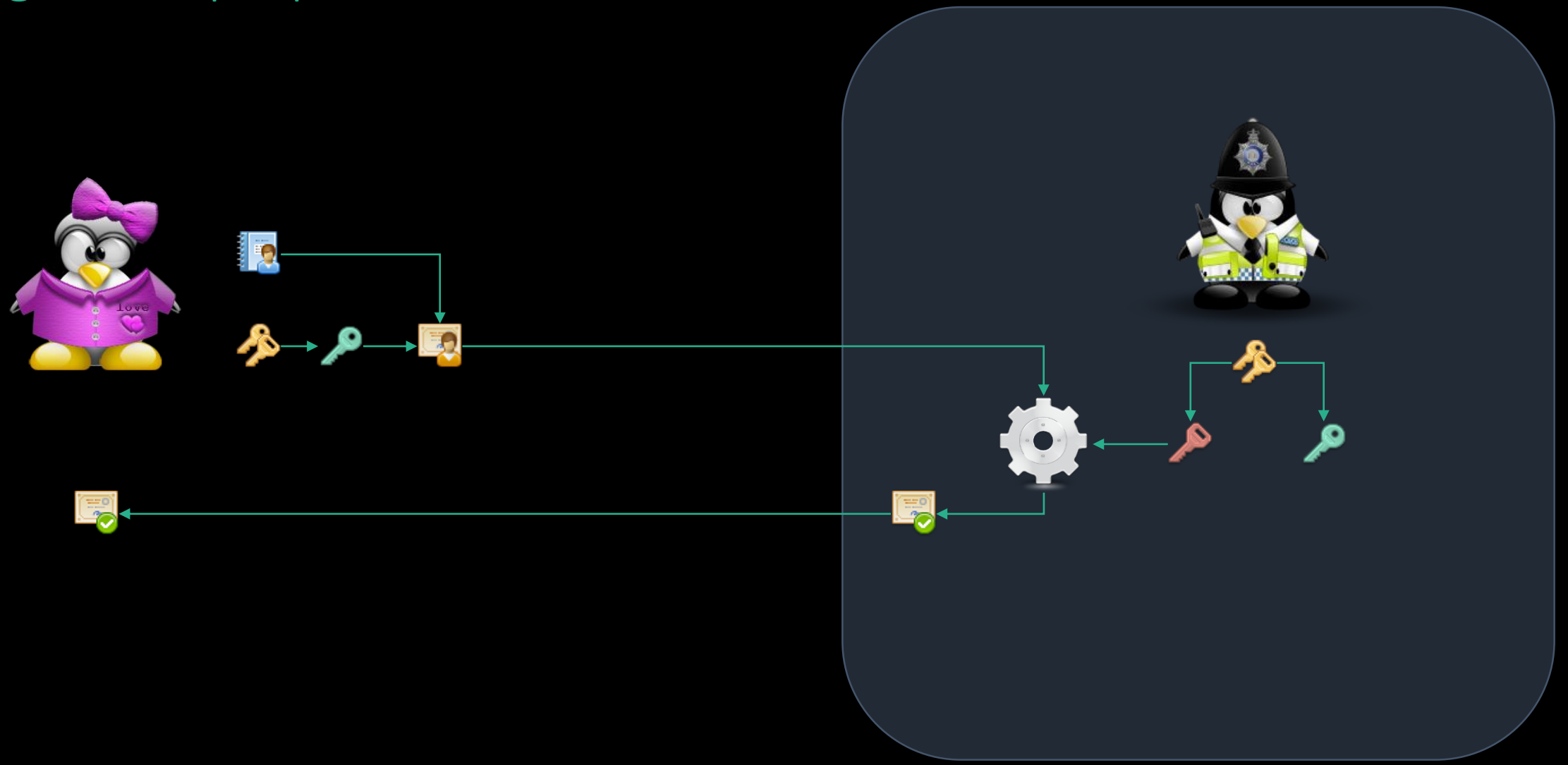
Identité du propriétaire

(CommonName, ville, …)

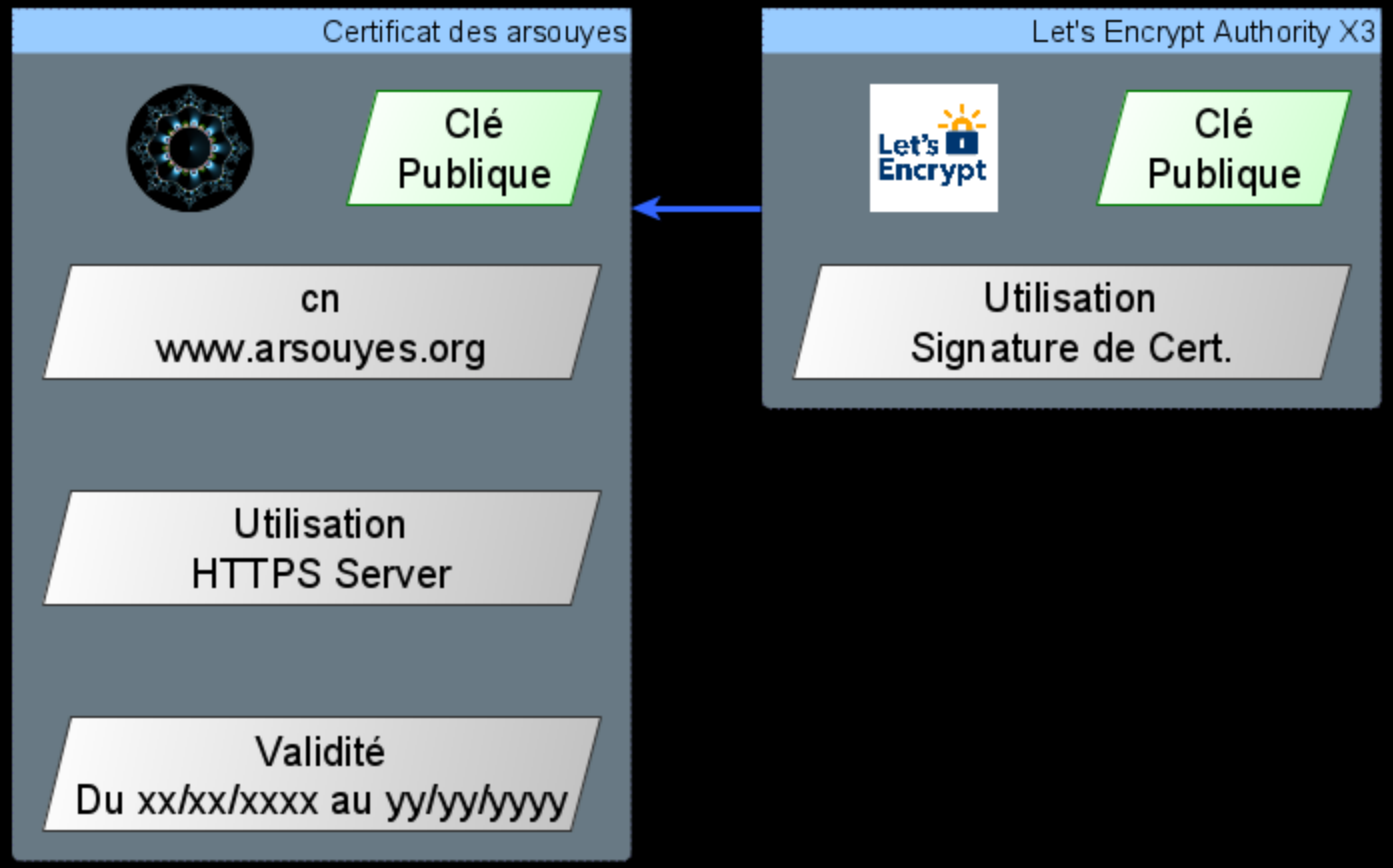


Autorité de confiance

Signe la « propriété »



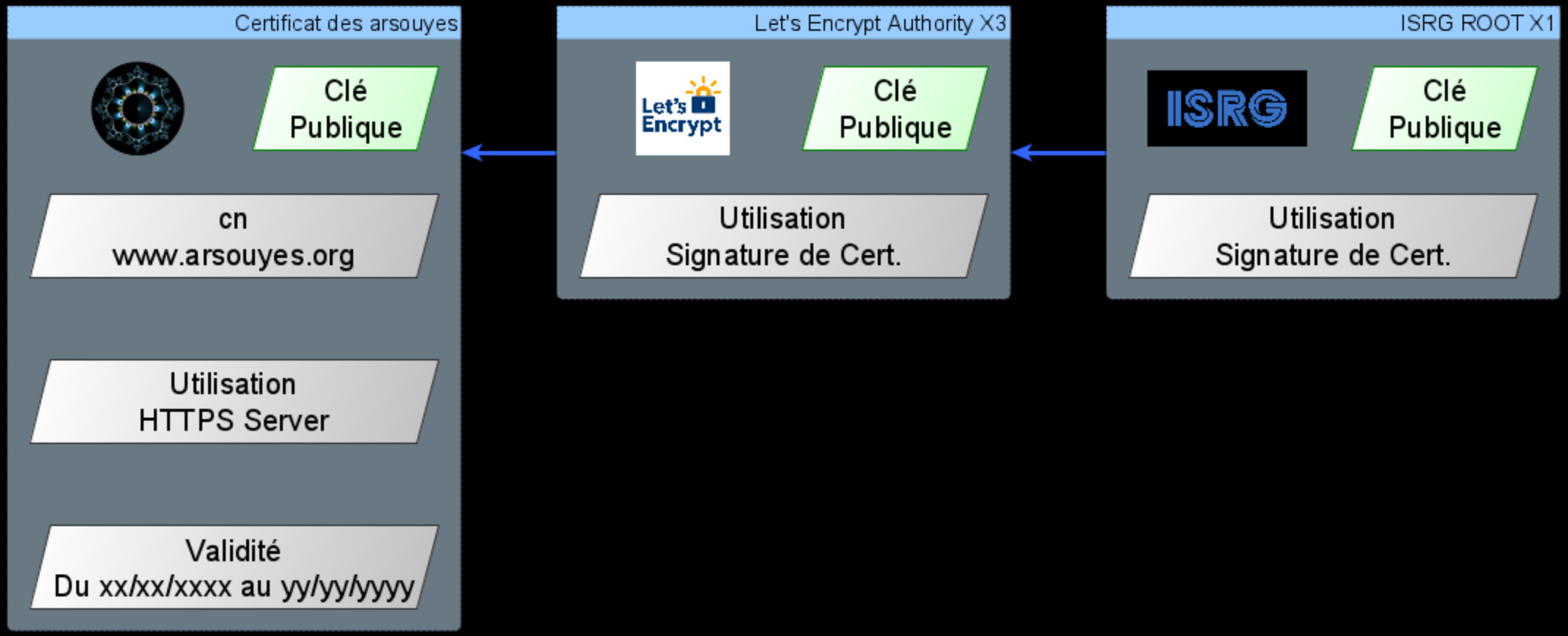
PKI – Signer pour faire confiance



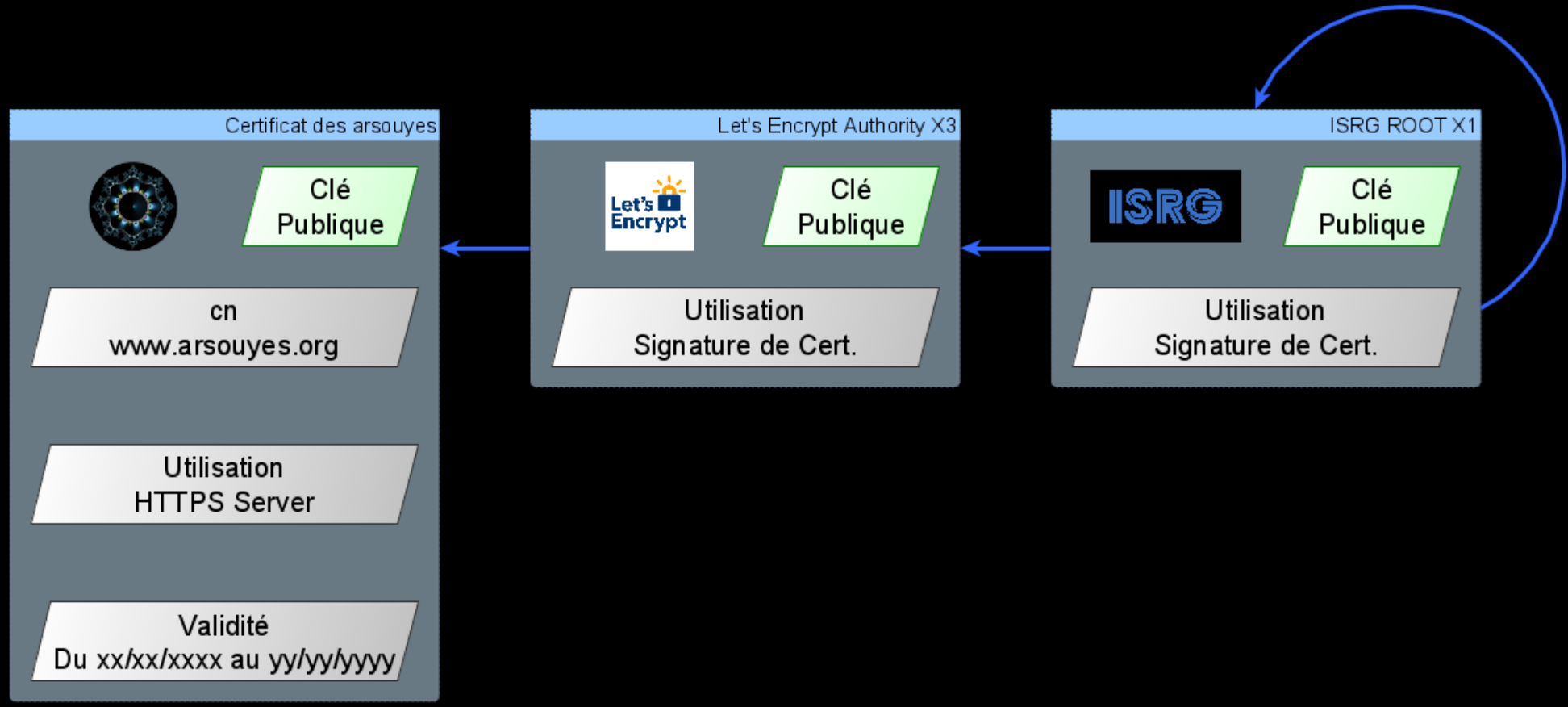
Autorité de confiance

Vérifier la « propriété »

PKI – Chaîne de signatures



PKI – Racine et auto-signé



PKI – Signature croisée