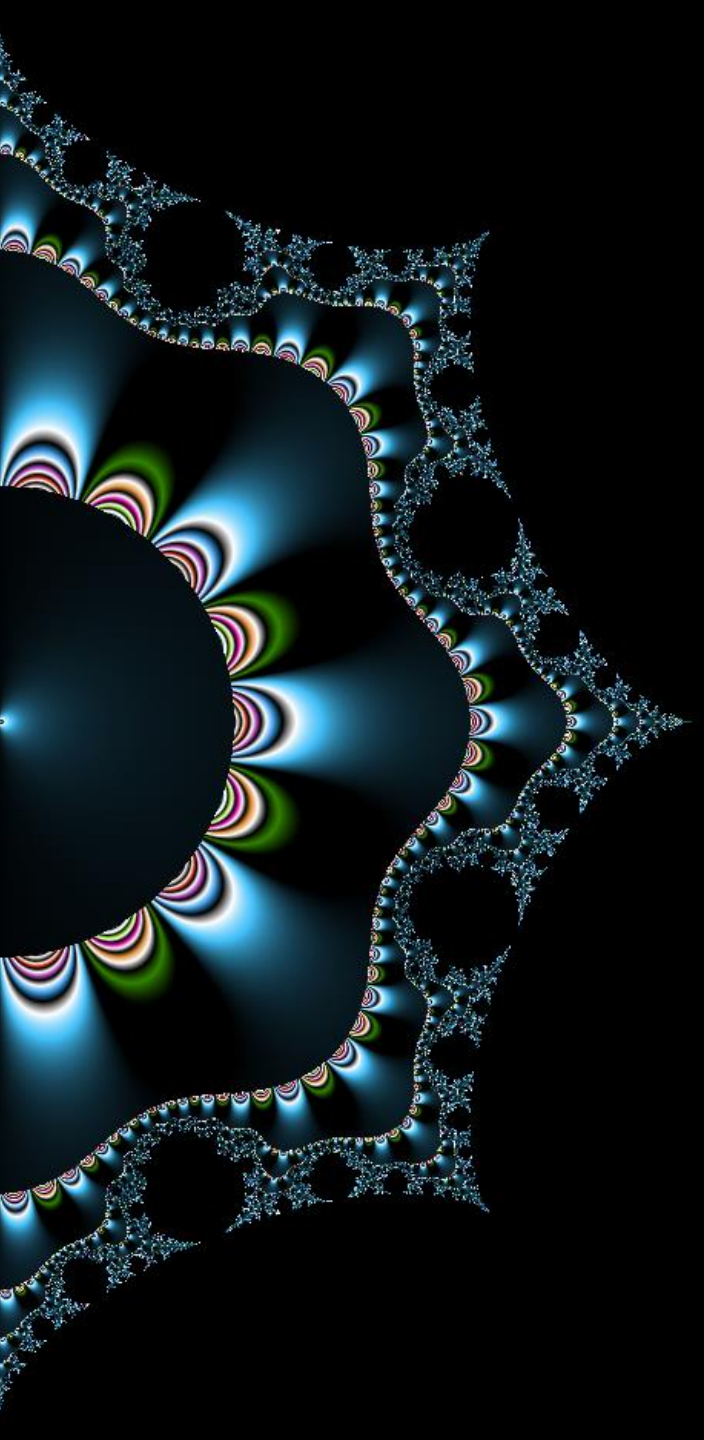
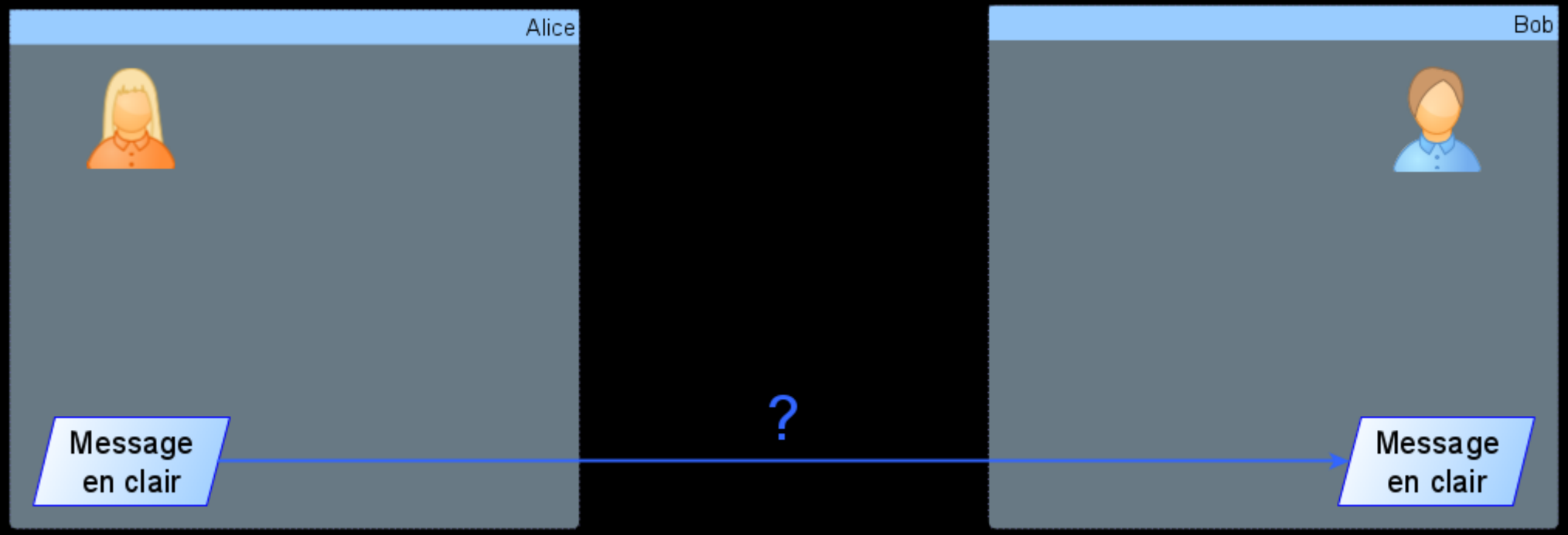


Cryptographie
Éléments d'introduction

Thibaut HENIN

tbowan@arsouyes.org

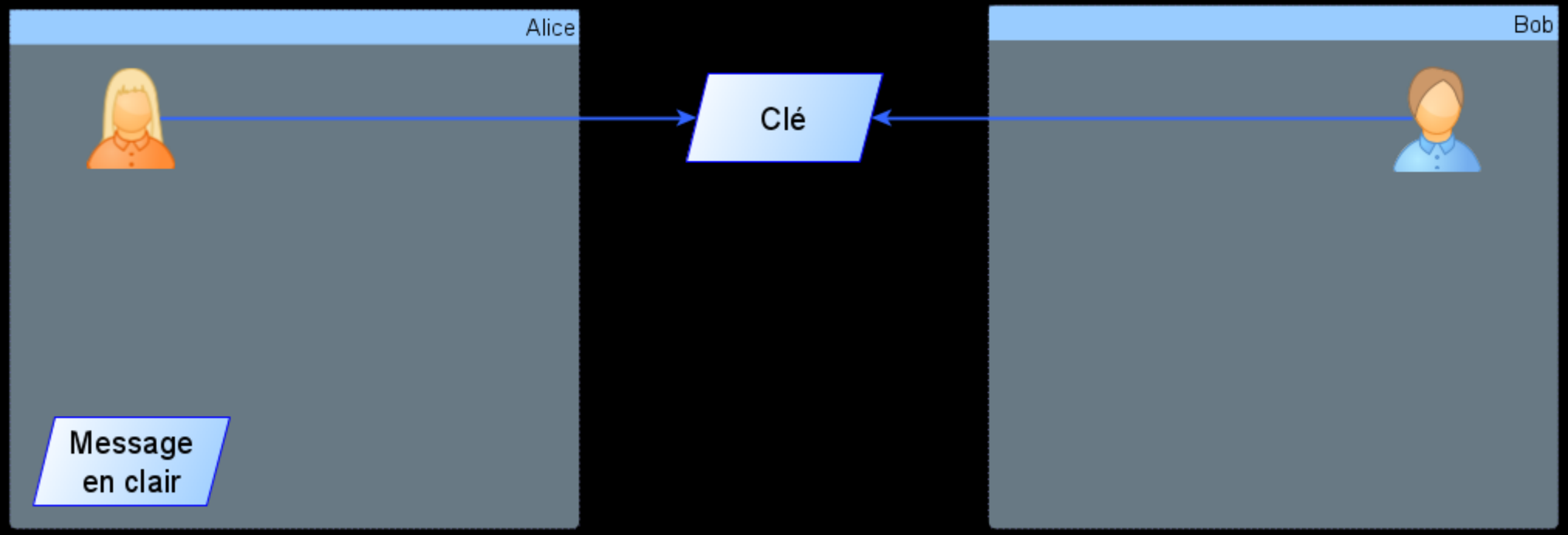
Cryptographie



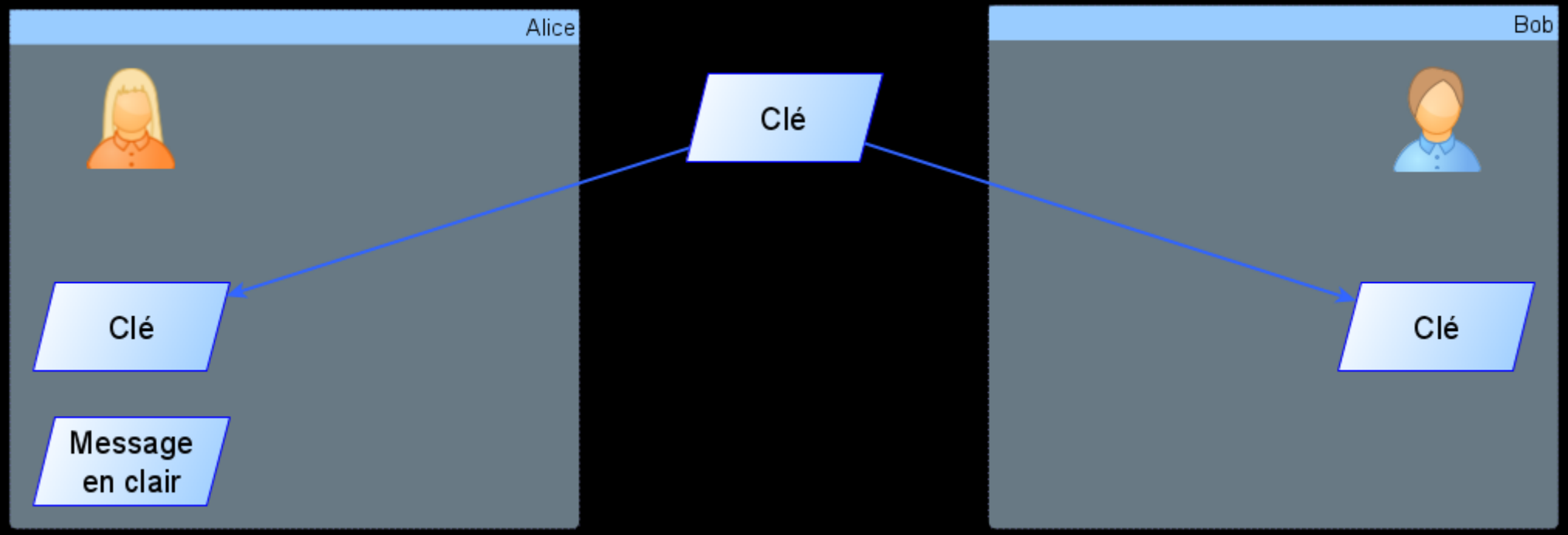
Cryptographie Symétrique

Une clé pour les gouverner tous

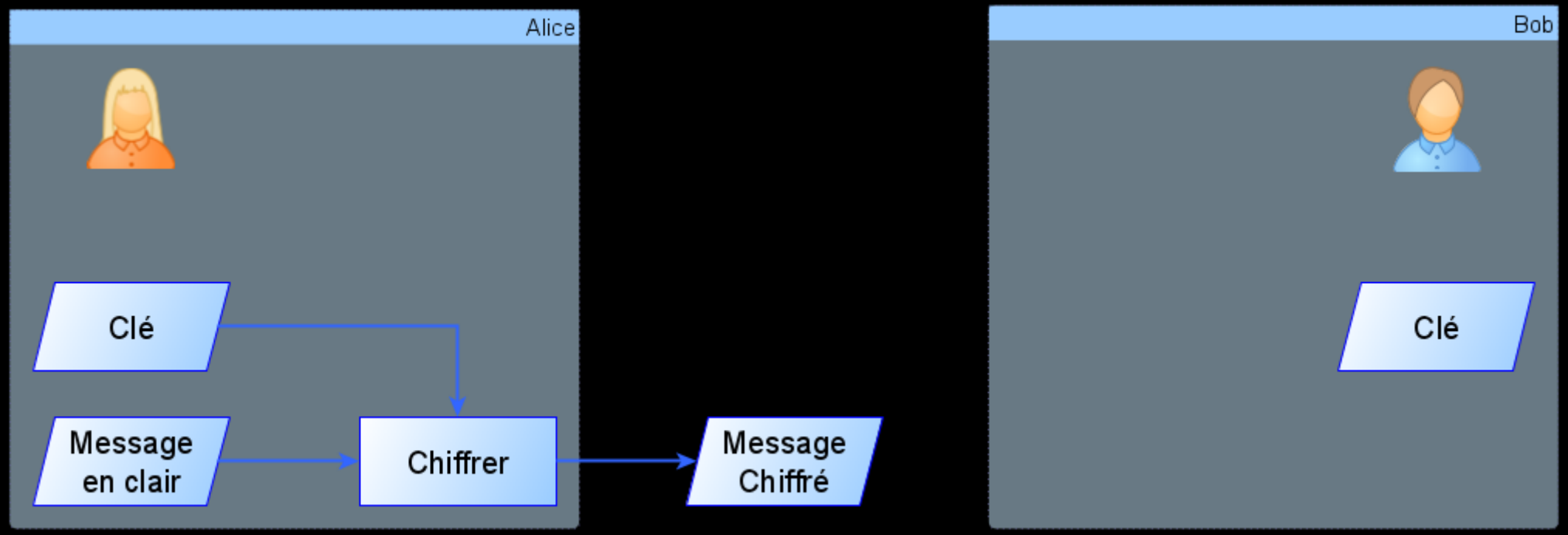
Cryptographie symétrique



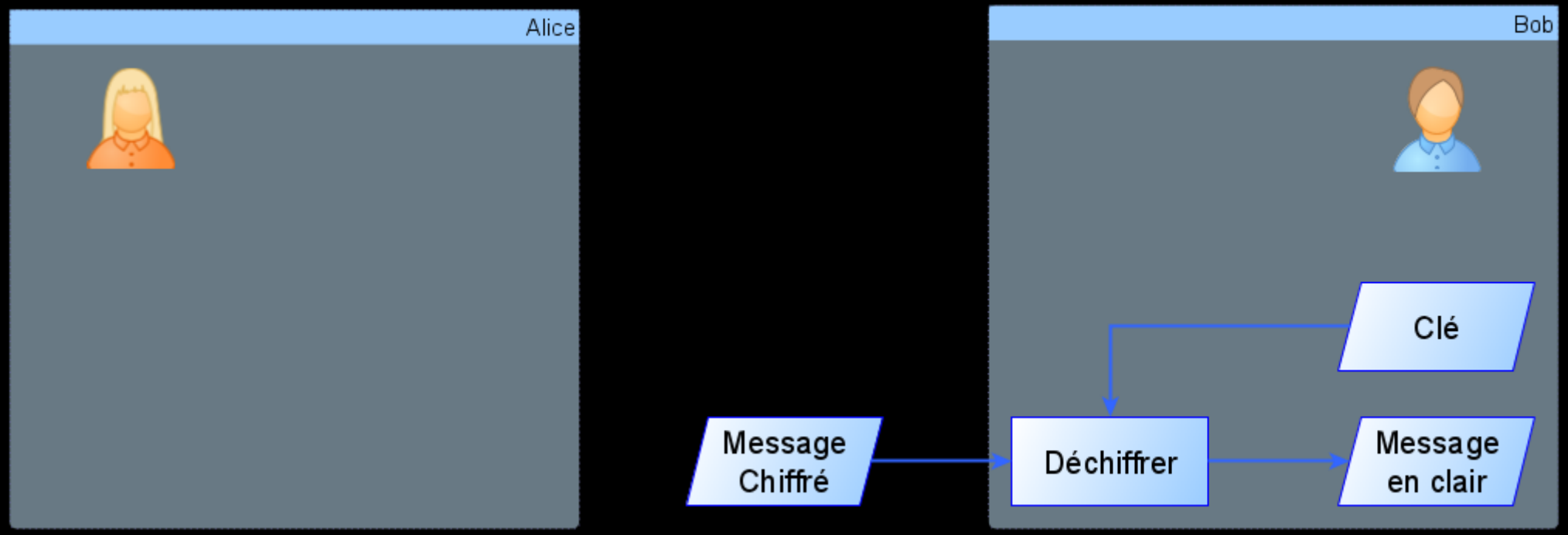
Cryptographie symétrique



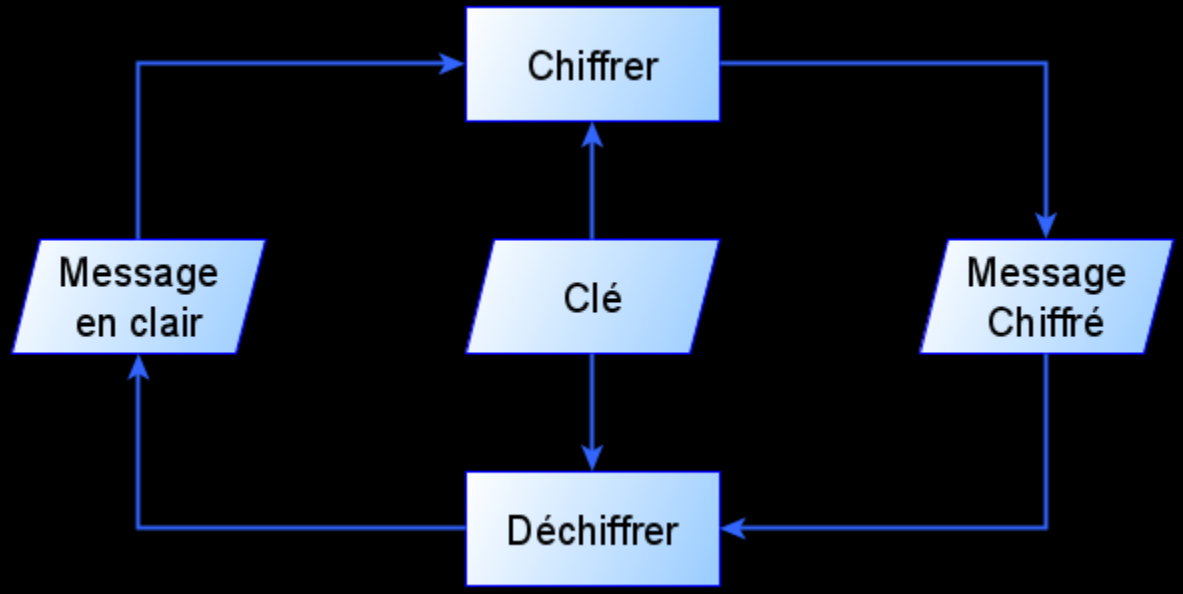
Cryptographie symétrique



Cryptographie symétrique



Cryptographie symétrique



Cryptographie symétrique

Obsolètes

Chiffre de César

4,5 bits

Enigma

67 bits

DES

56 bits

A jour (128 bits)

AES

128 bits

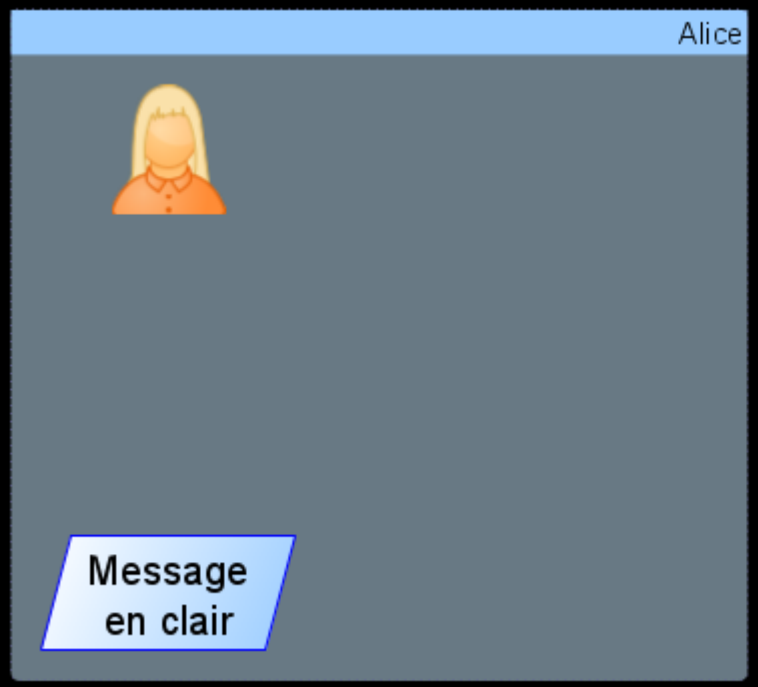
3 DES

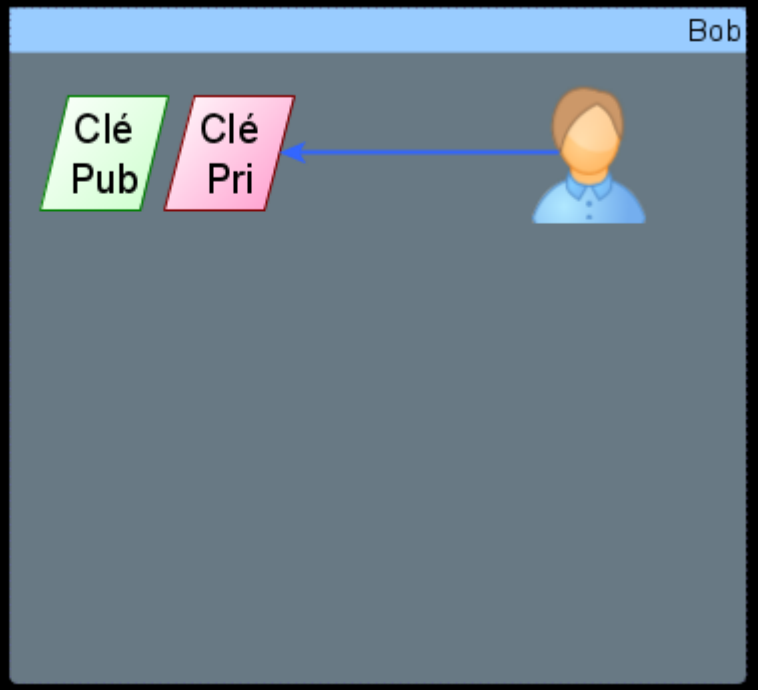
112 ou 168 bits

Cryptographie A-Symétrique

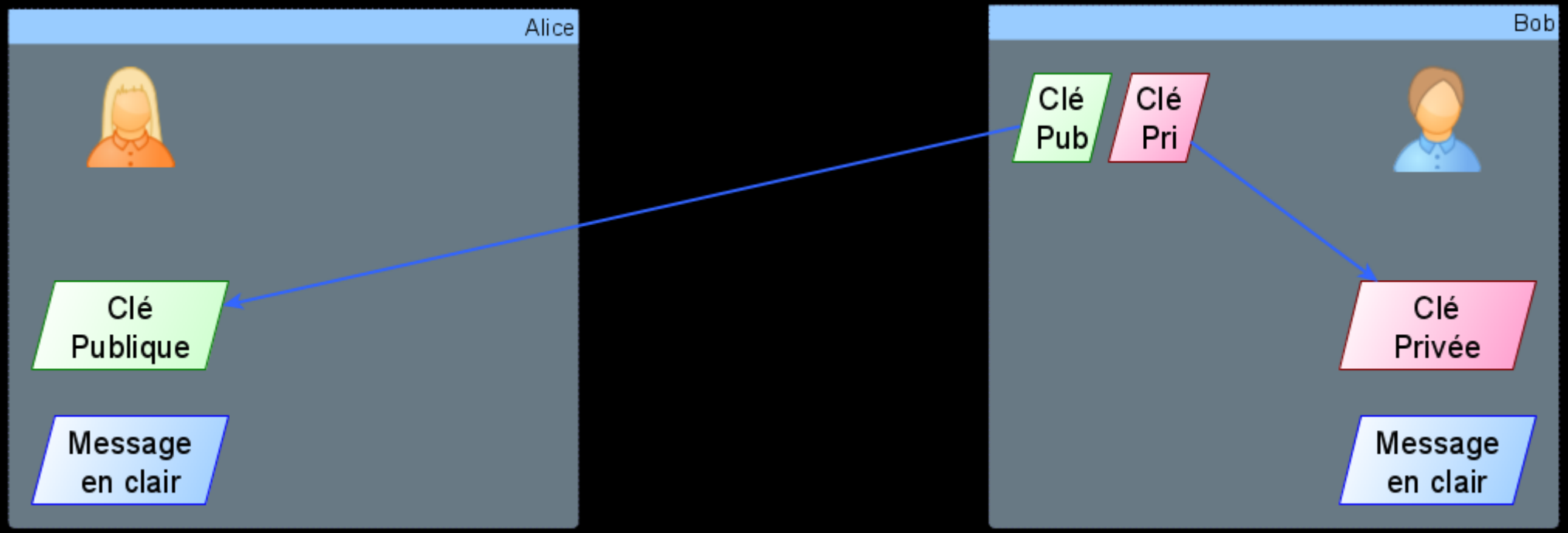
Partenaria Public Privé

Cryptographie asymétrique

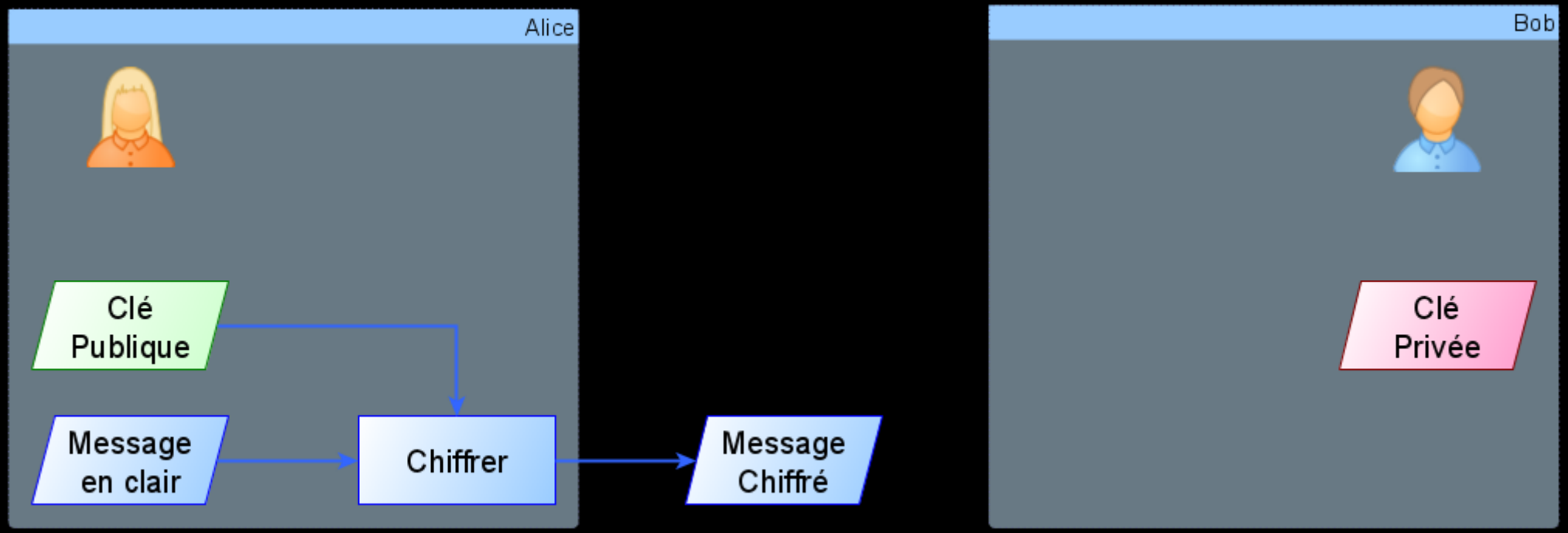




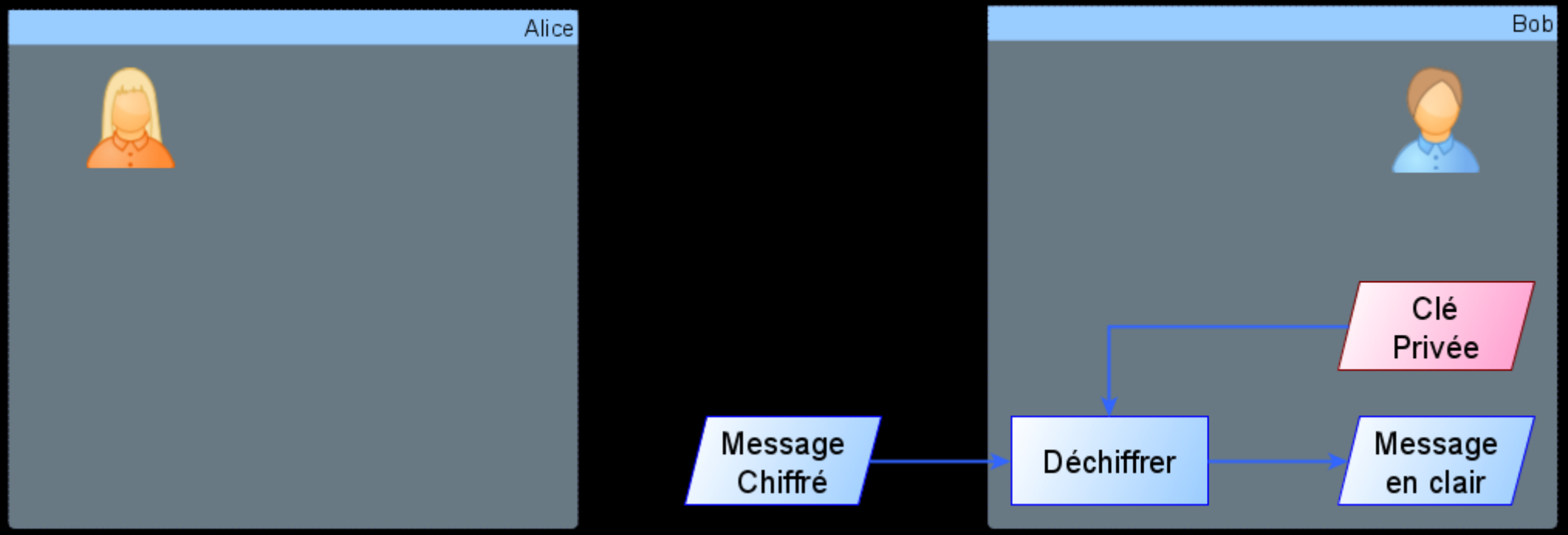
Cryptographie asymétrique



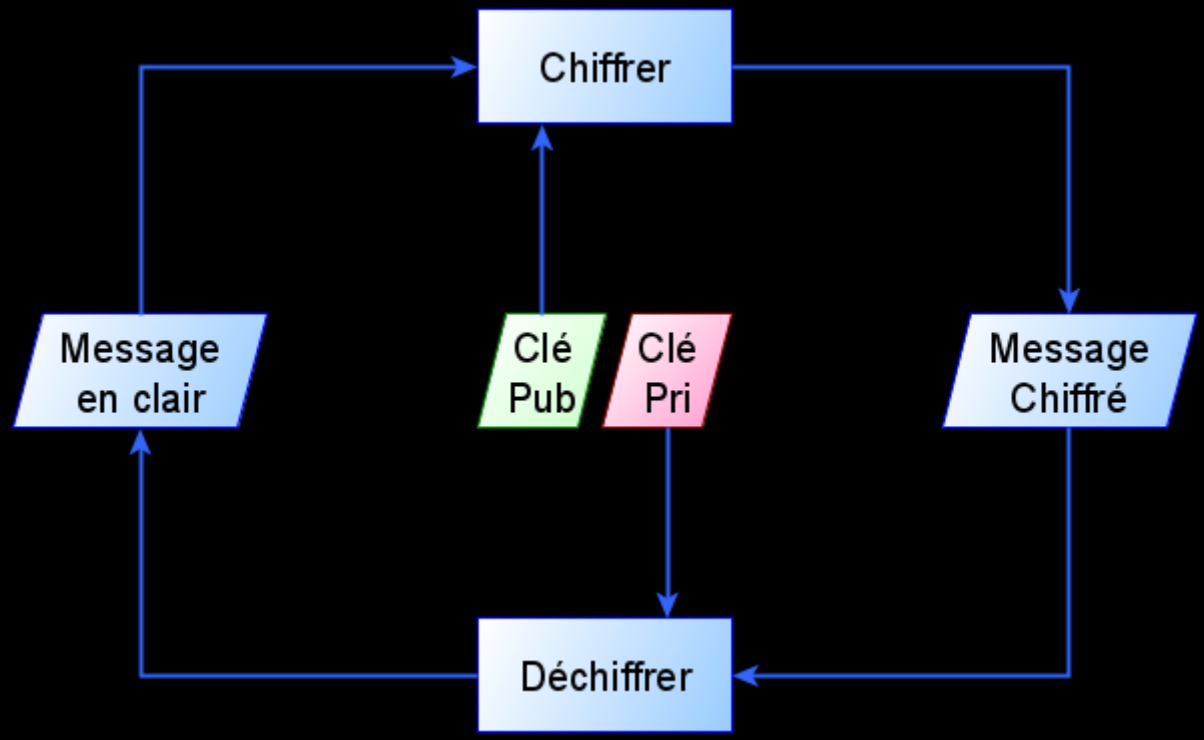
Cryptographie asymétrique



Cryptographie asymétrique



Cryptographie asymétrique



Cryptographie symétrique

Nombres entiers, 3072 bits

RSA

Factorisation de nombres

El Gamal

Logarithme discret

Courbes Elliptiques, 256 bits

El Gamal

Logarithme discret sur EC

Checksum & Hachage

Condenser et oublier

Checksums

https://www.arsouyes.org/blog/2019/50_Hash_Function_Checksum/

Condenser une donnée

Détecter les erreurs

Bits de parité

Ascii 7 bits

Mots de parité

RAID 3, 5, …

Sommes

IPv4, ICMP, TPC

Restes de divisions

Cartes vitales & RIB

CRC-32

Hachage

https://www.arsouyes.org/blog/2019/52_Hash_Function_Cryptography/

Condenser une donnée

Interdire les erreurs

Irreversible

ne pas trouver la donnée

Infalsifiable

ne pas trouver une autre donnée

Résistante aux collisions

Sert aux preuves formelles

Cryptographie symétrique

Obsolètes

MD5

(obsolète depuis 1993)

SHA1

(obsolète depuis 2012)

A jour (256 bits)

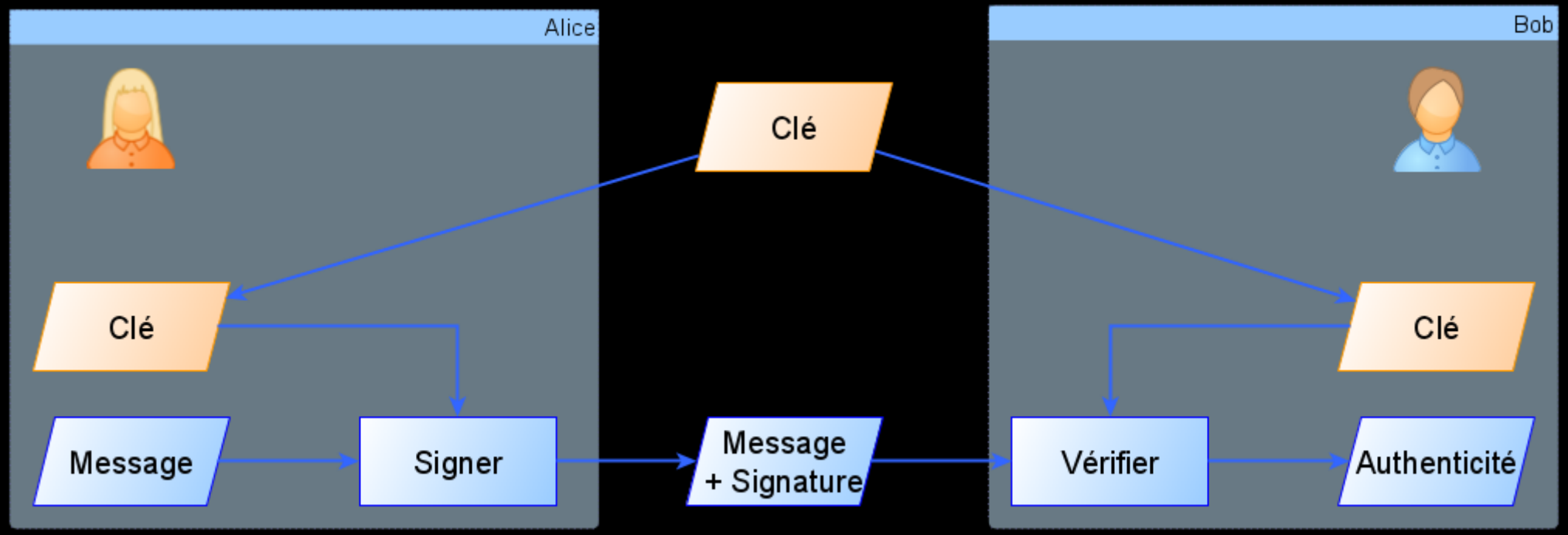
SHA2

(SHA256 et SHA512)

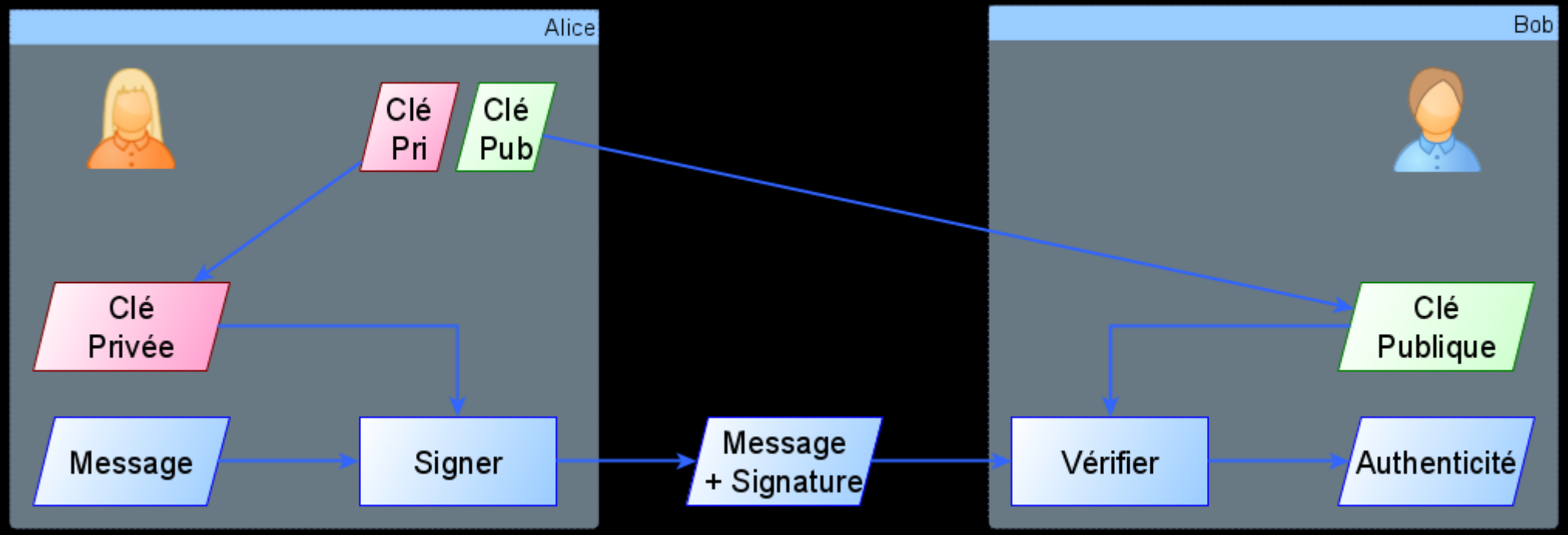
Signature

Pour être sûr

Signature Cryptographique



Signature Cryptographique



Certificats

Carte d’identité numérique

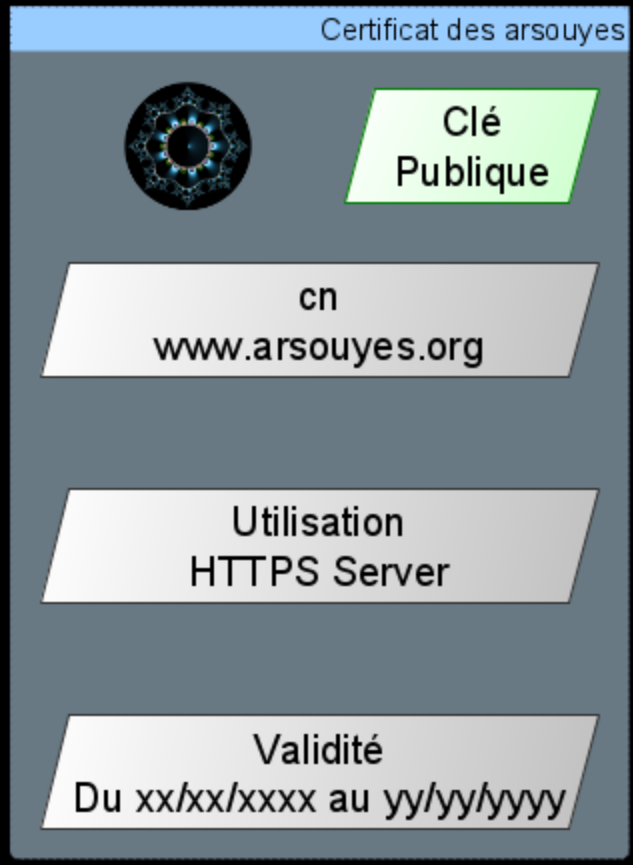
Certificat cryptographique

Clé publique

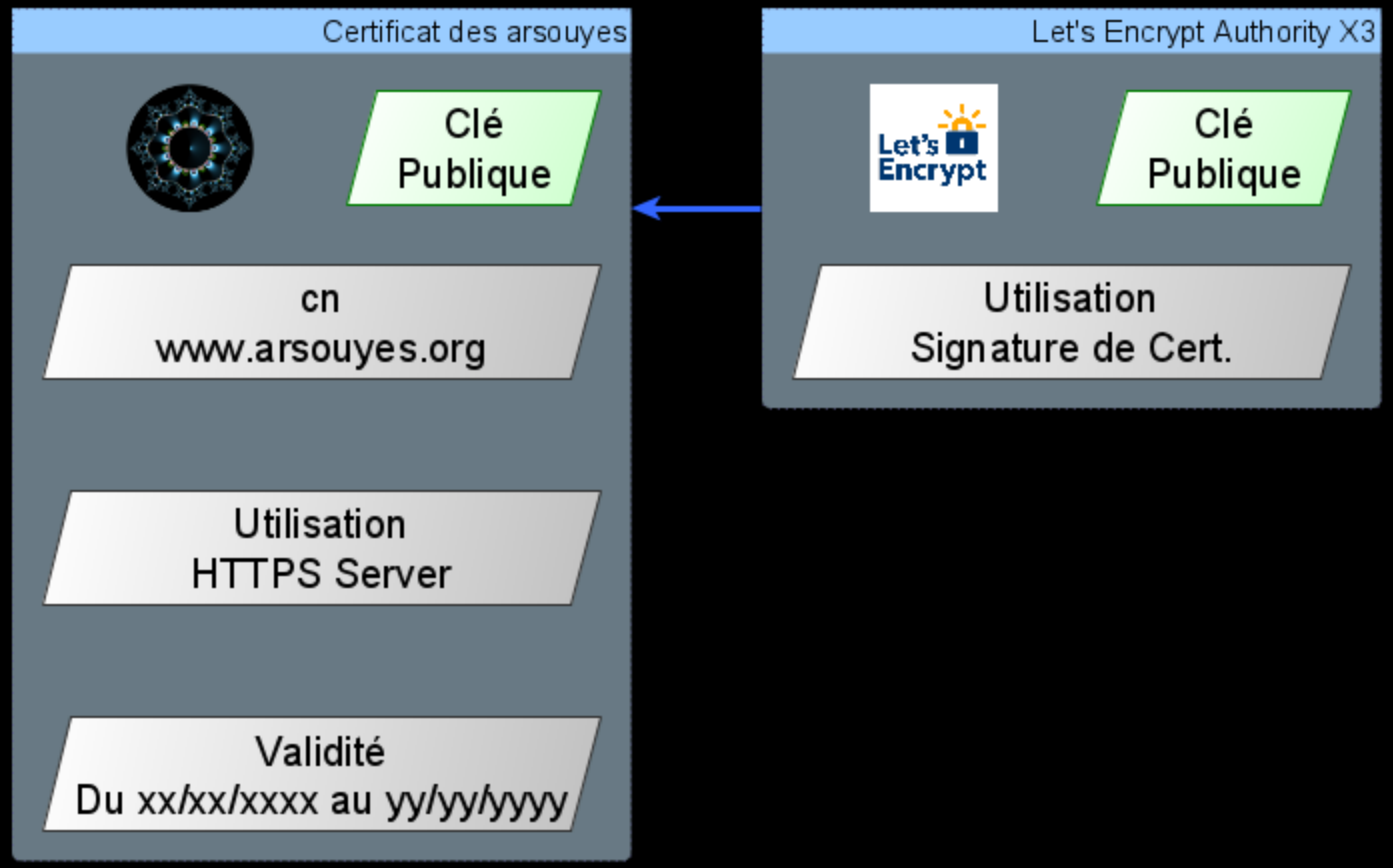
(et algorithme correspondant)

Identité du propriétaire

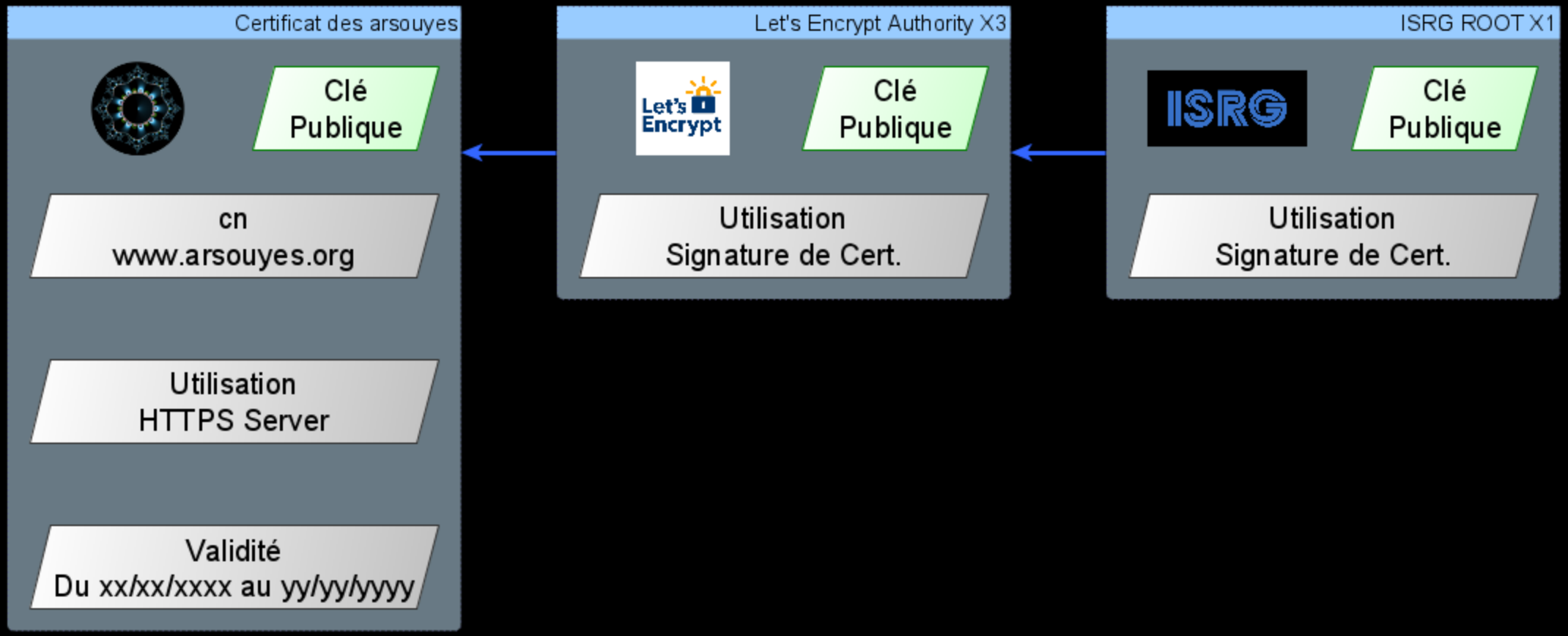
(CommonName, ville, …)



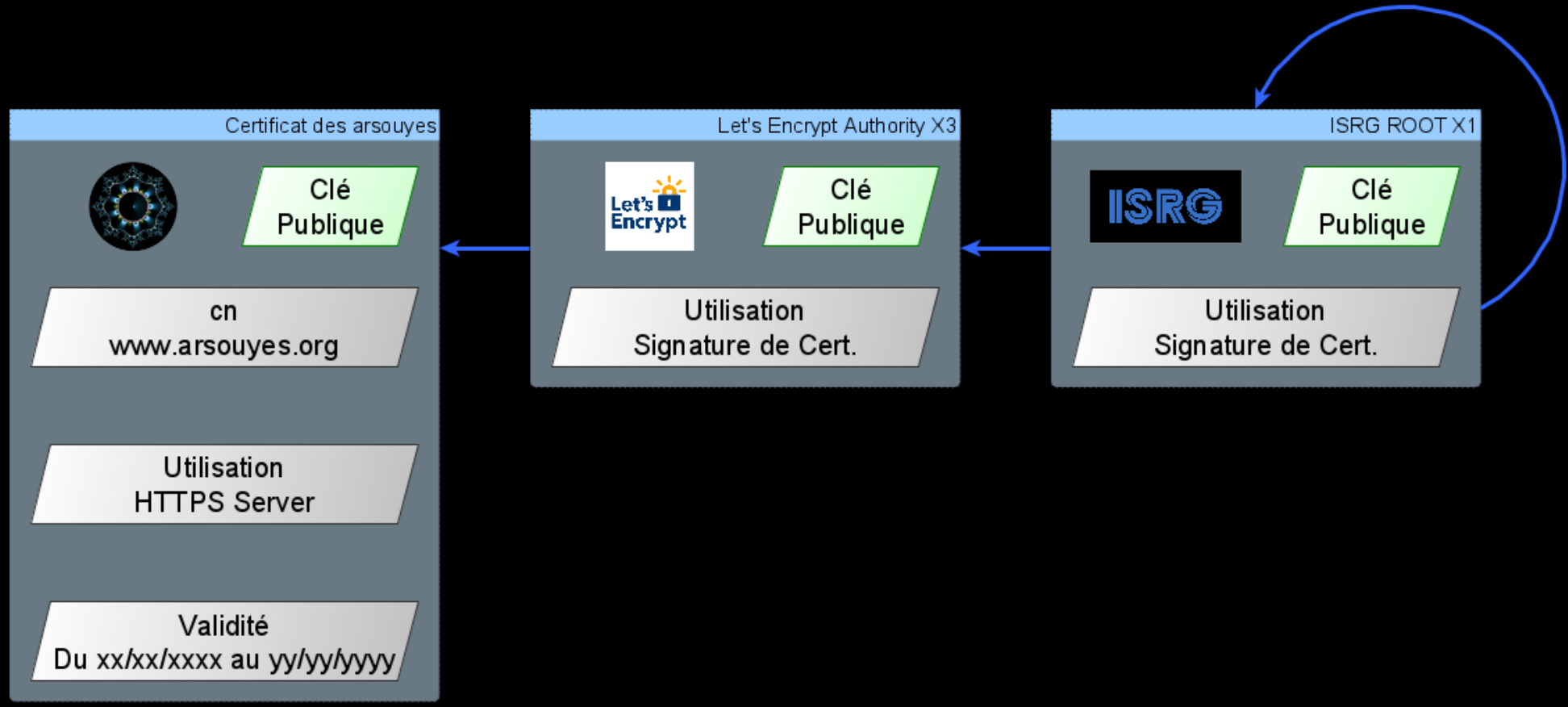
PKI – Signer pour faire confiance



PKI – Chaîne de signatures



PKI – Racine et auto-signé



PKI – Signature croisée