Protocole d'authentification CrypTonAuth

Monika Trimoska

Gaël Le Mahec

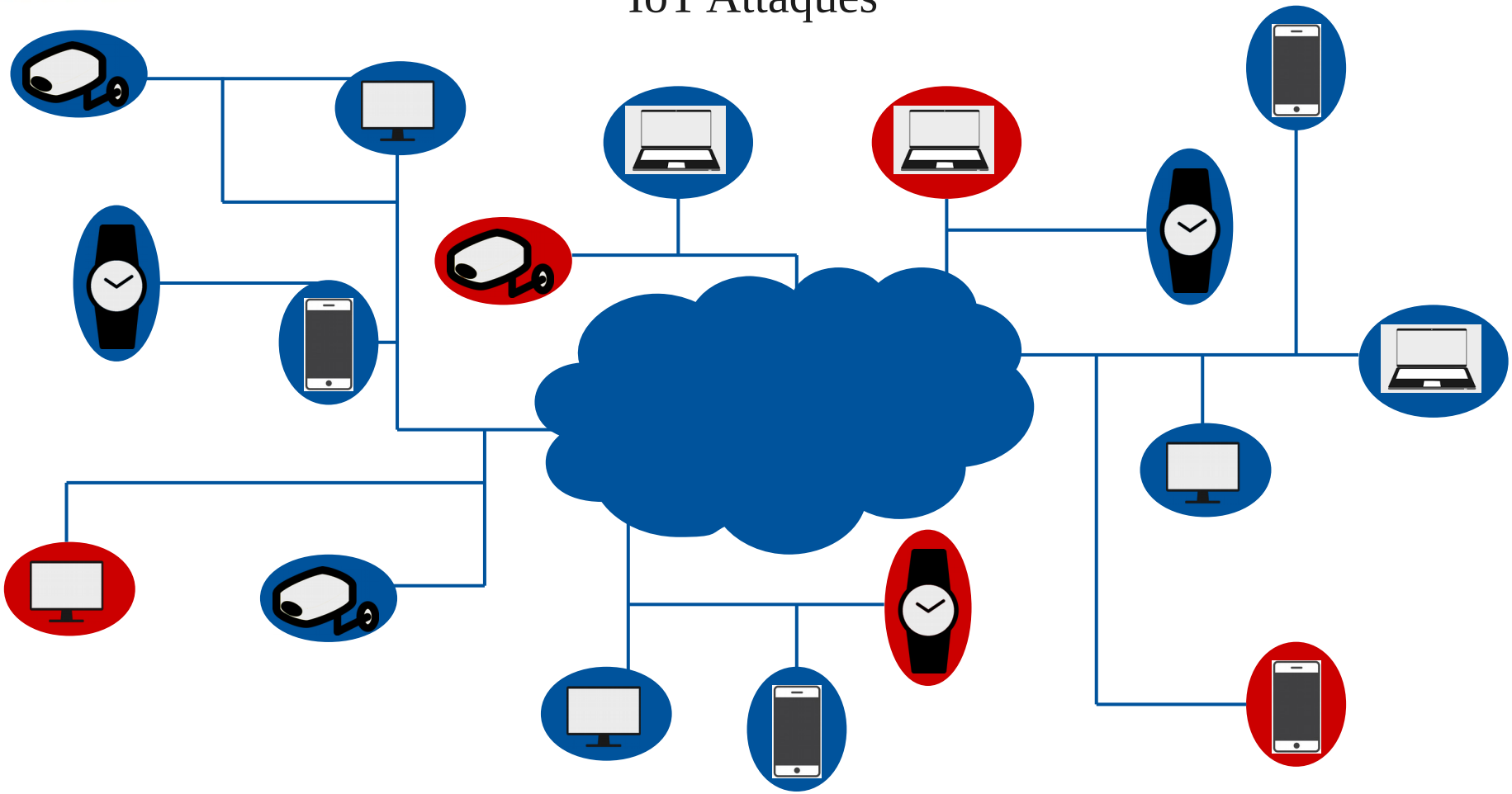
Gilles Dequen

Laboratoire MIS, Université de Picardie Jules Verne

Amiens, 2017

- Authentification classique
-
  - Faire confiance aux procédures de sécurisation
  - Couple identifiant, mot de passe
  - L’enregistrement d’une empreinte du mot de passe sur le serveur

IoT Attaques



21 octobre 2016, une attaque DDoS contre le DNS du fournisseur Dyn, à partir de centaines de milliers d'objets connectés.

IoT Attaques

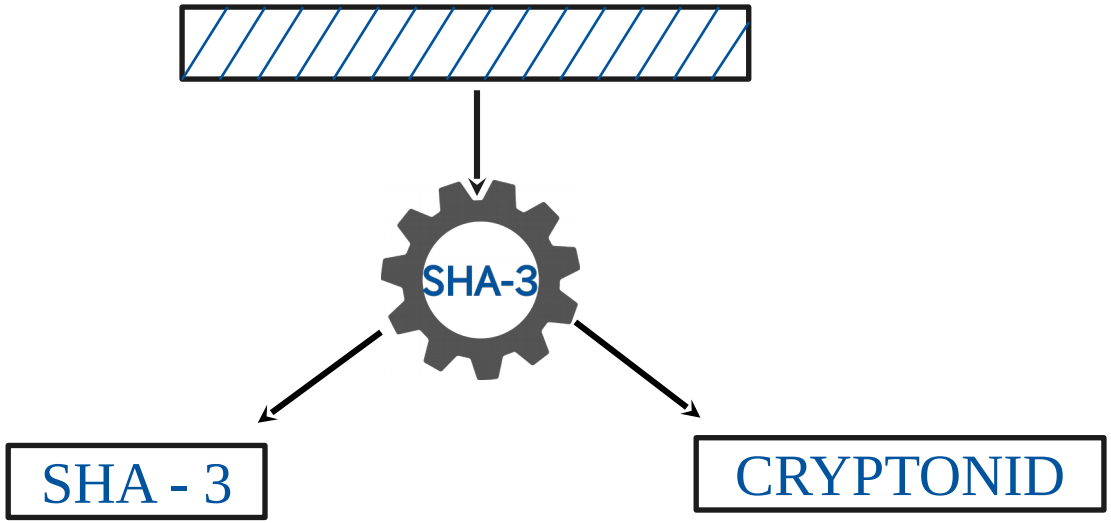
- 20 septembre 2016, KrebsOnSecurity
- Janvier 2017, Fournisseurs de services en Asie
- 10 mai 2017, Le Monde et Le Figaro
- Faiblesses ?
  - Mot de passes par défaut
  - Faible capacités énergétique et limitations matérielles

IoT Attaques

- 20 septembre 2016, KrebsOnSecurity
- Janvier 2017, Fournisseurs de services en Asie
- 10 mai 2017, Le Monde et Le Figaro
- Faiblesses ?
  - Mot de passes par défaut
  - Faible capacités énergétique et limitations matérielles

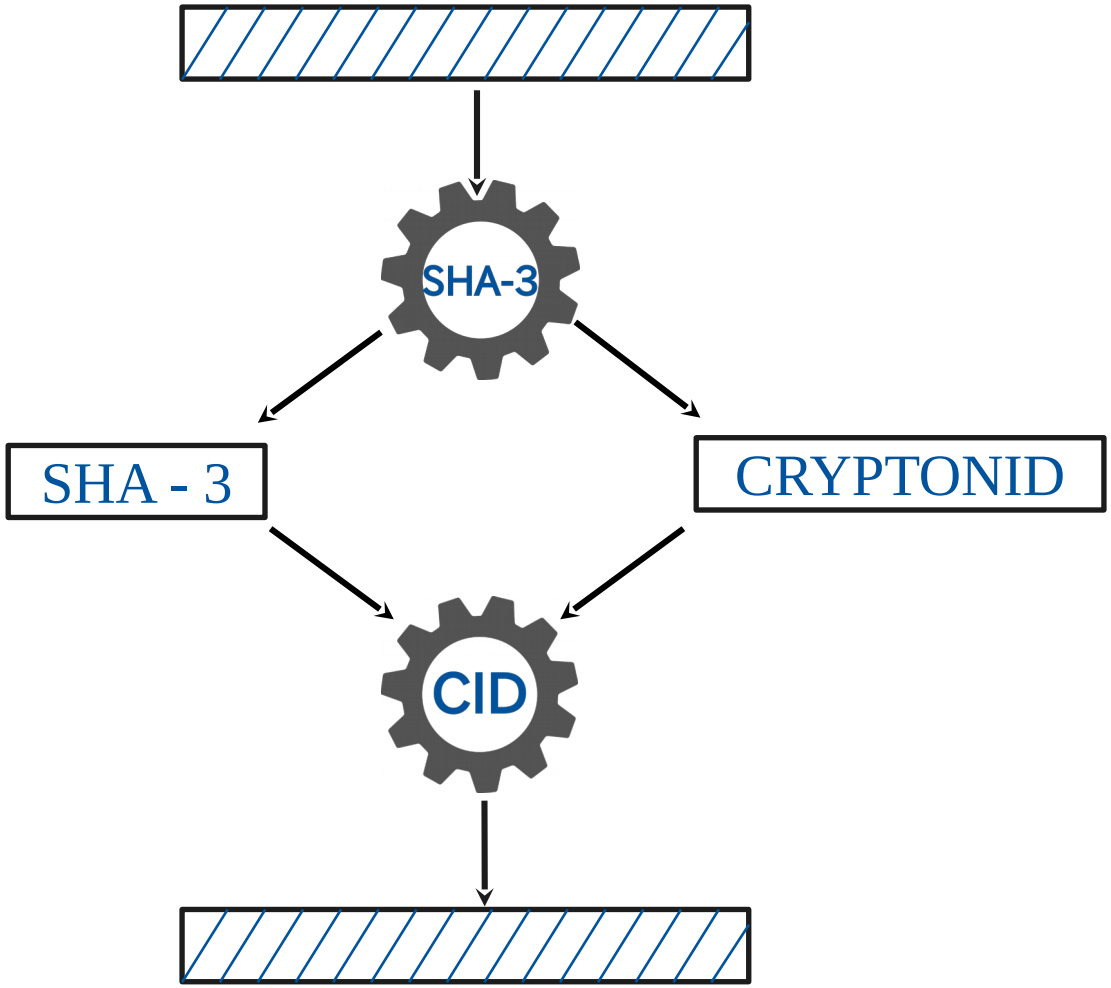
CrypTonID

Reconstitution de données hachées



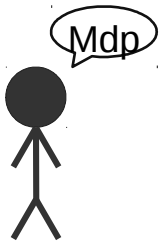
CrypTonID

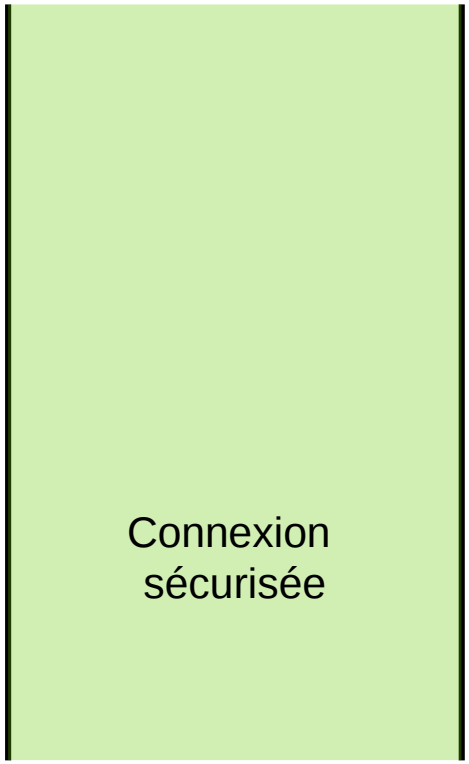
Reconstitution de données hachées

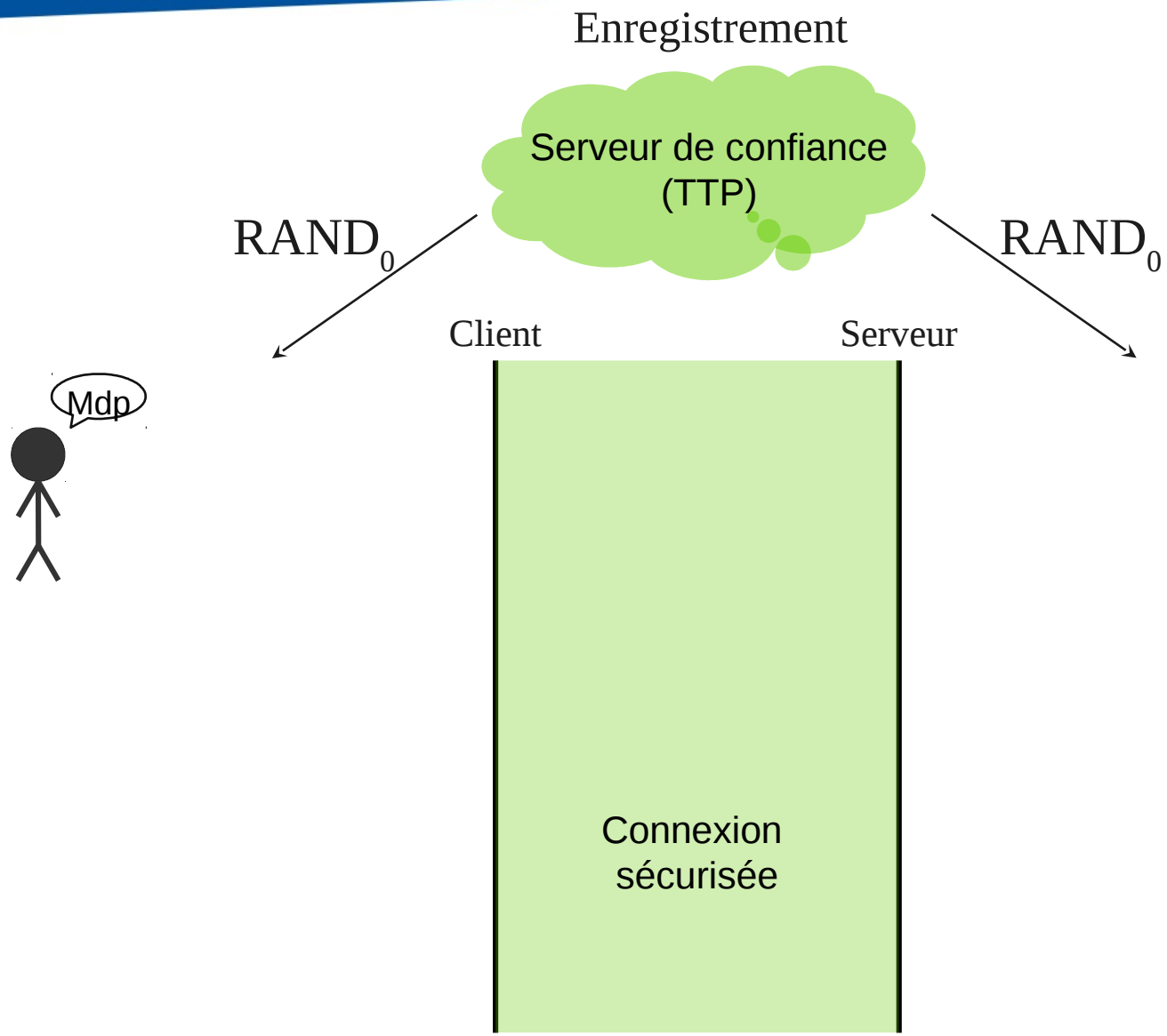


Enregistrement

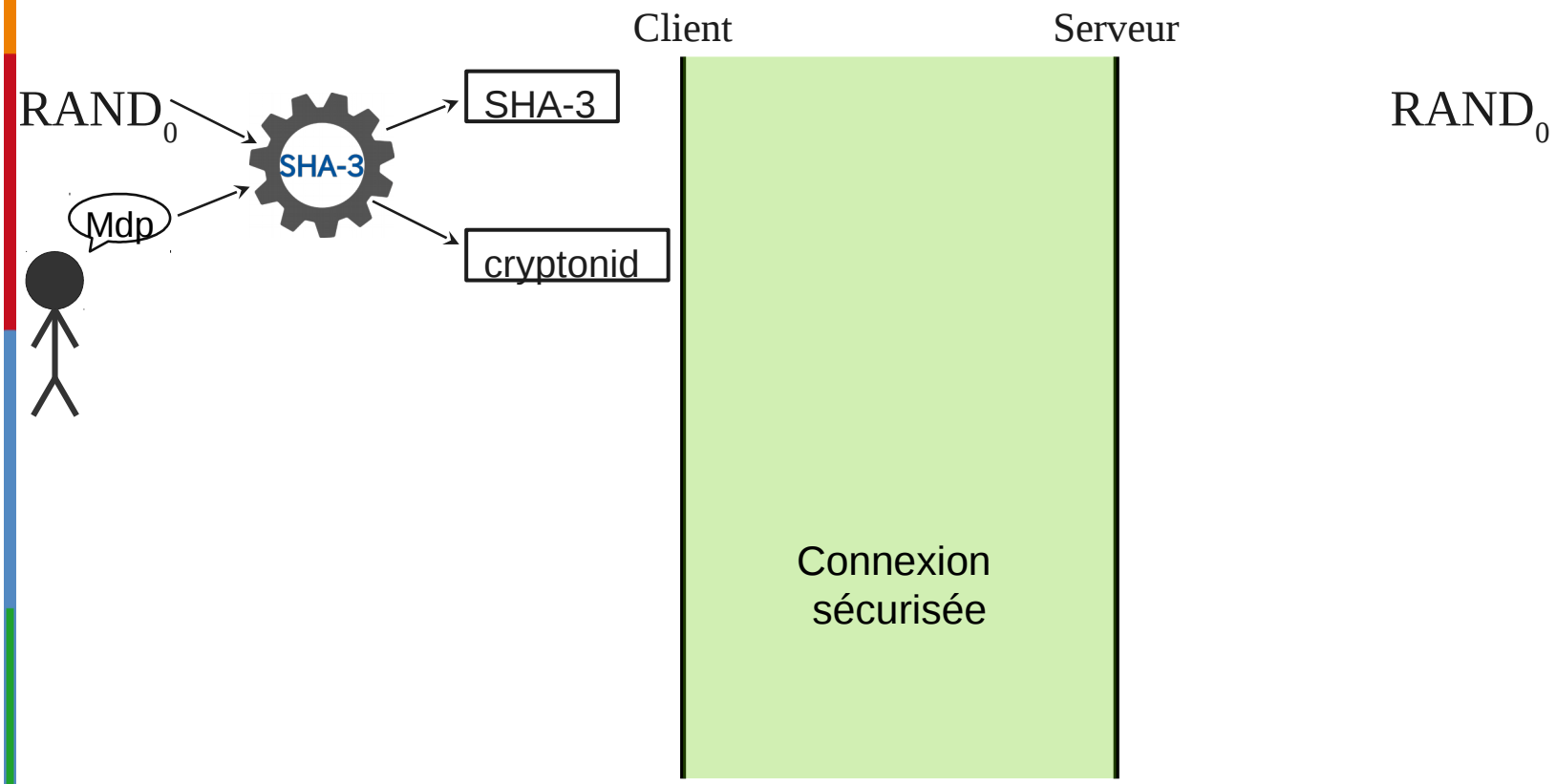
Client Serveur



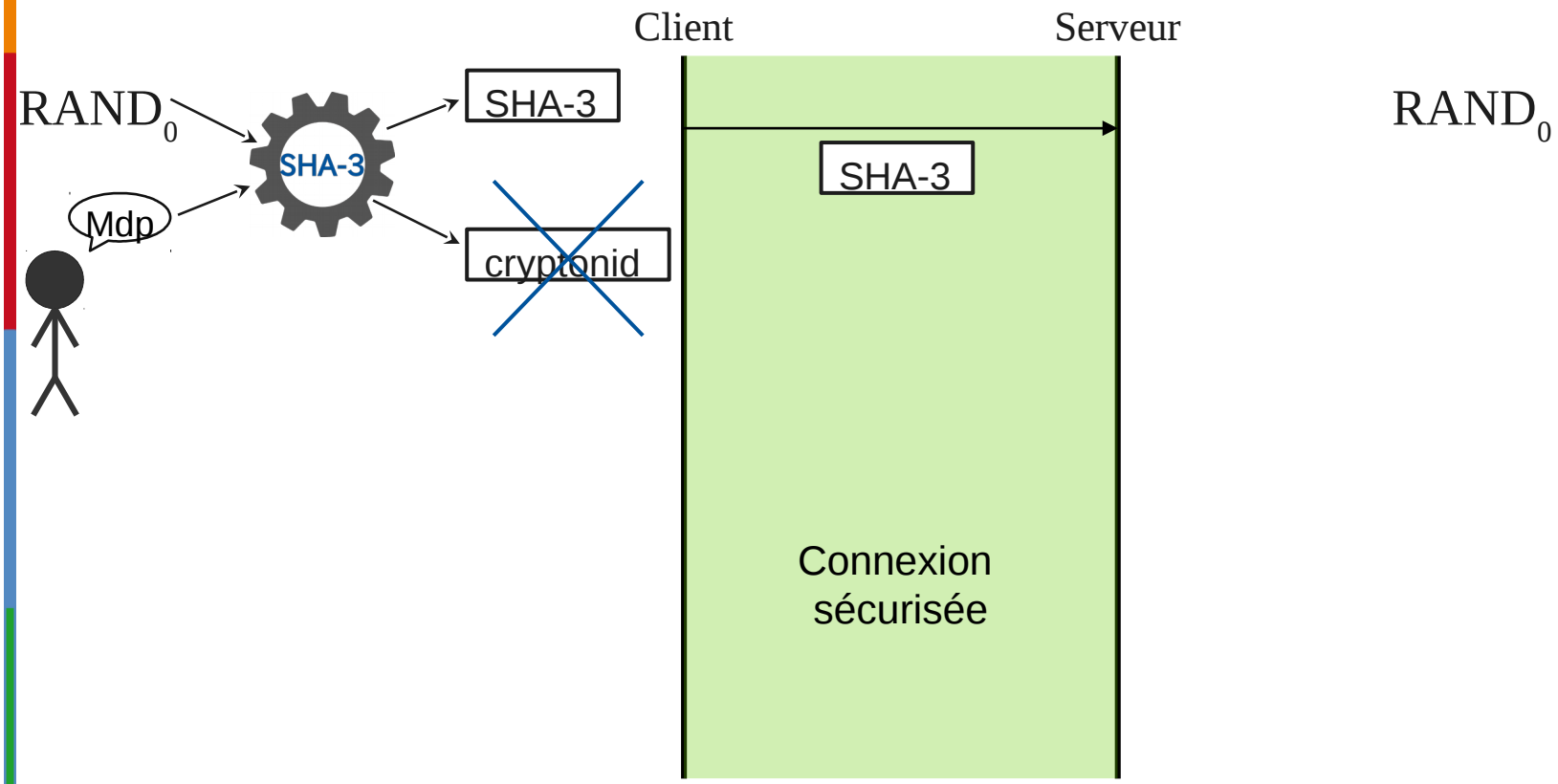



Enregistrement
Serveur de confiance
(TTP)
RAND0
RAND0
Client
Serveur
Mdp
Connexion
sécurisée

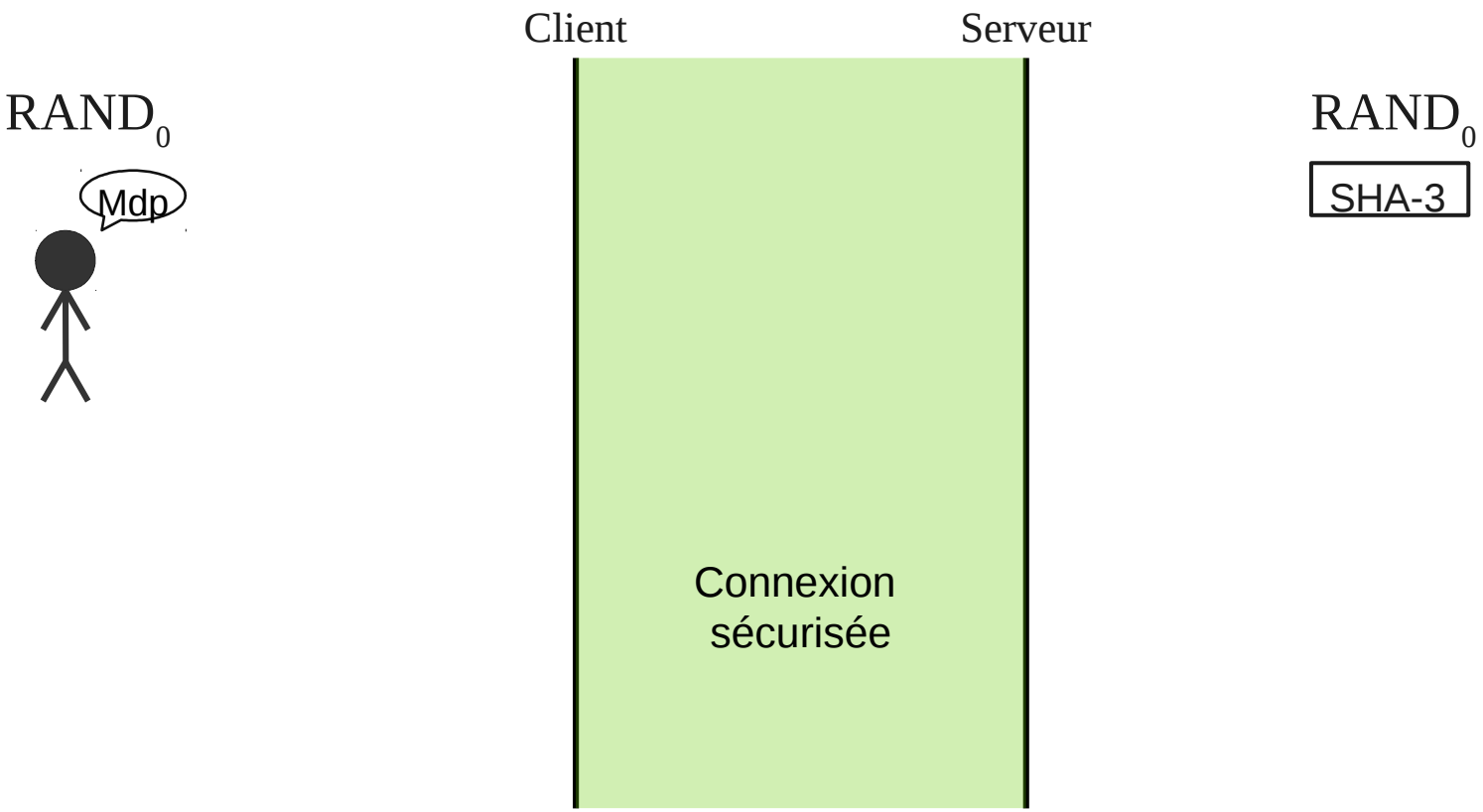
Enregistrement



Enregistrement



Enregistrement

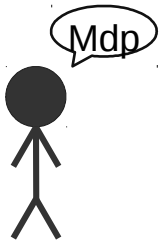


Authentification

Client

Serveur

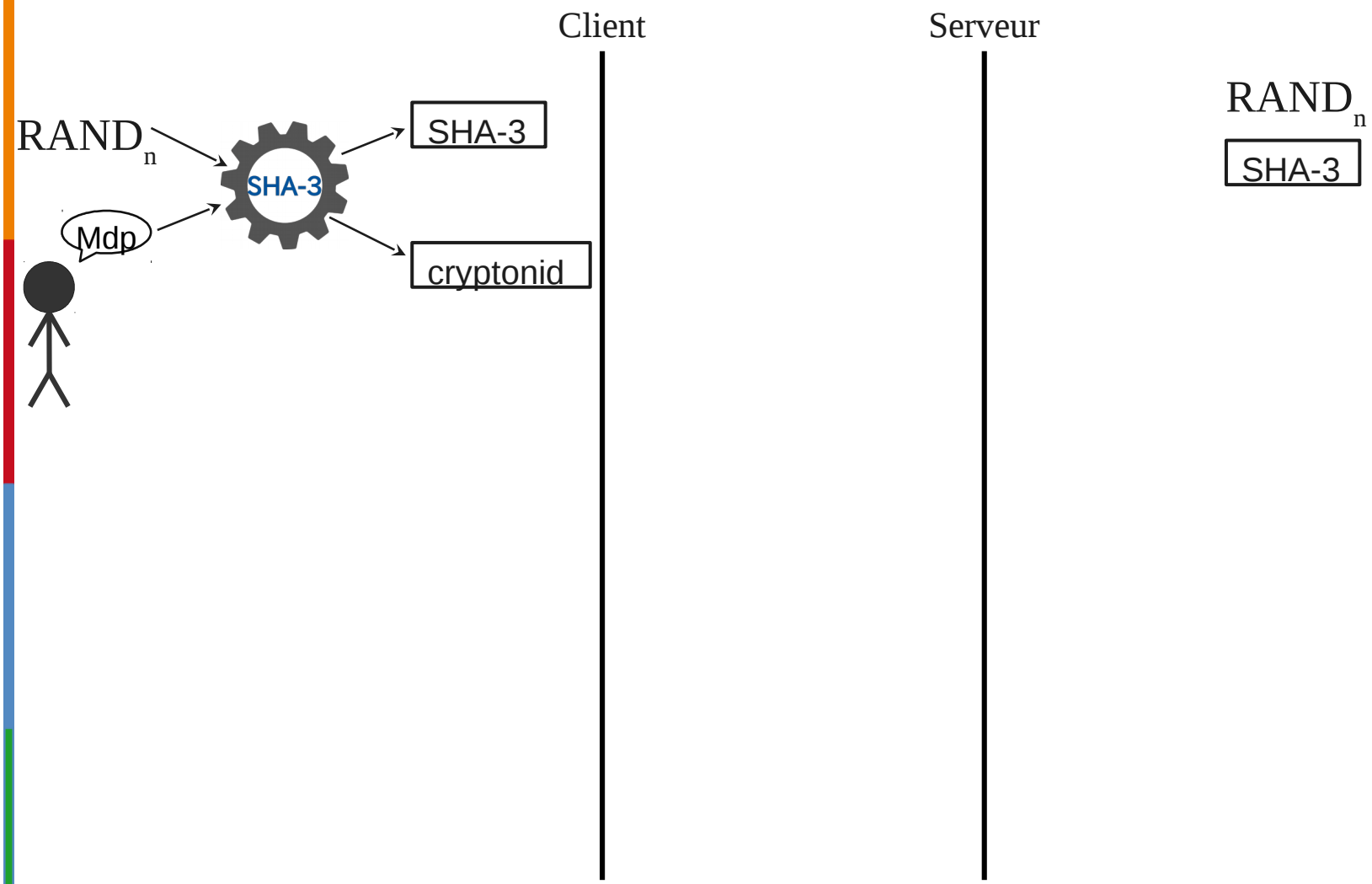
$RAND_n$



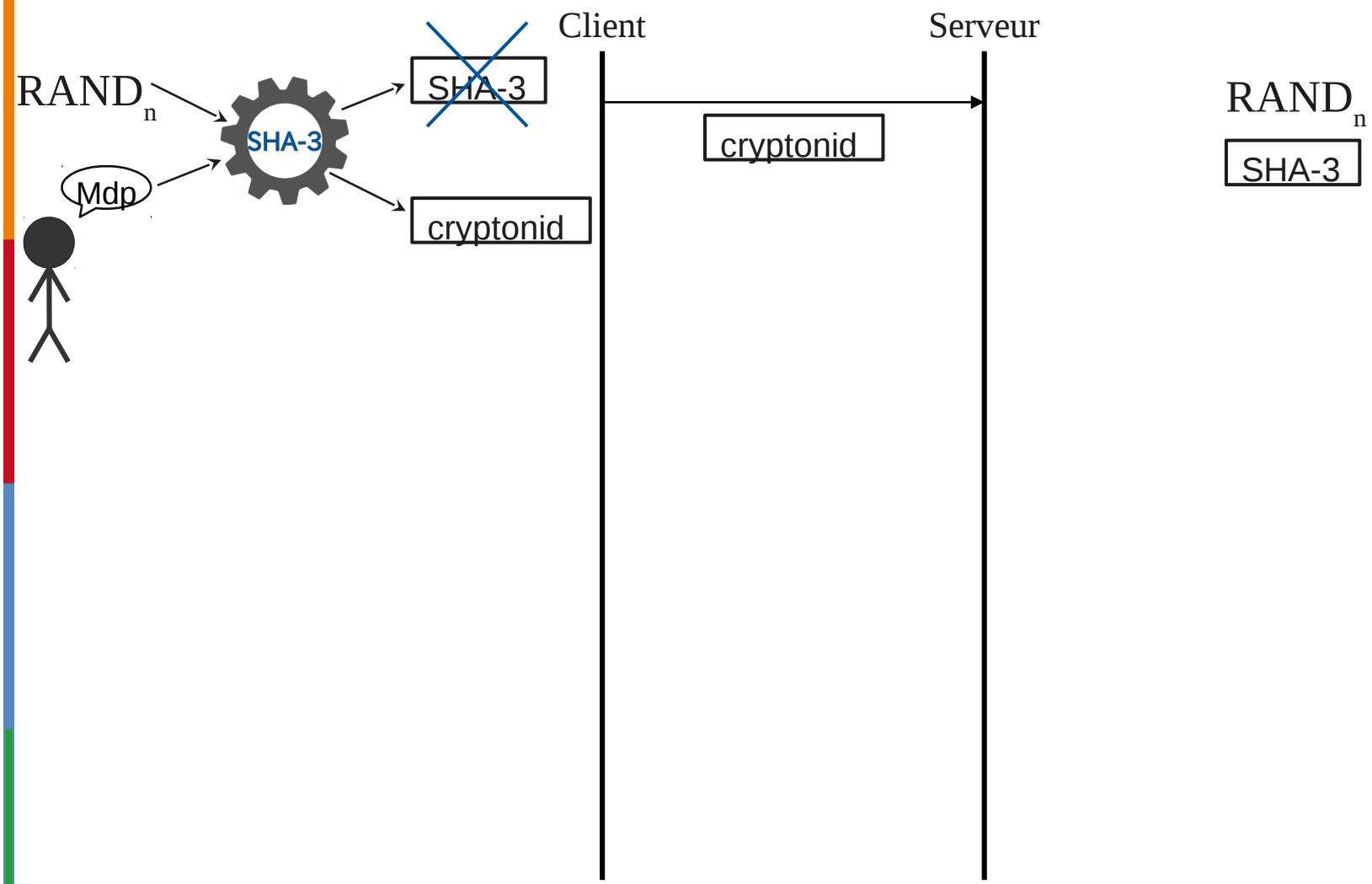
$RAND_n$

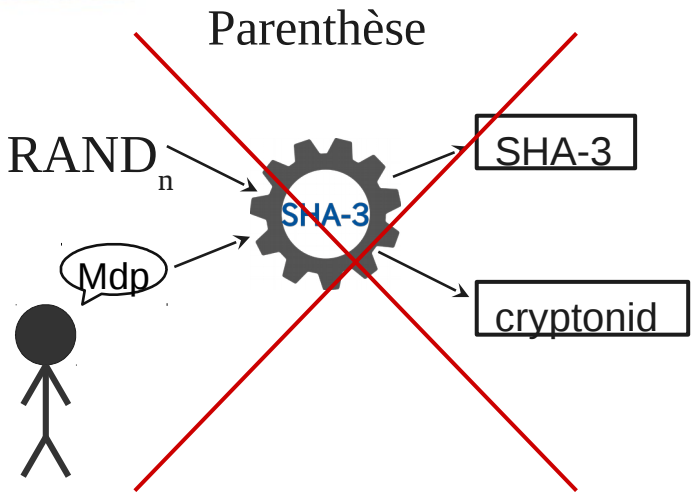
SHA-3

Authentification

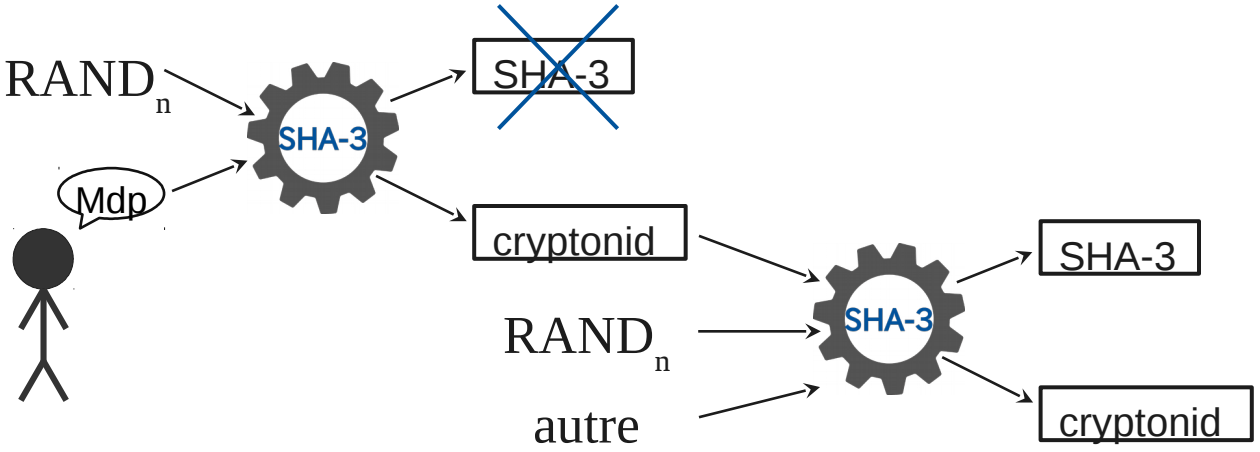


Authentification

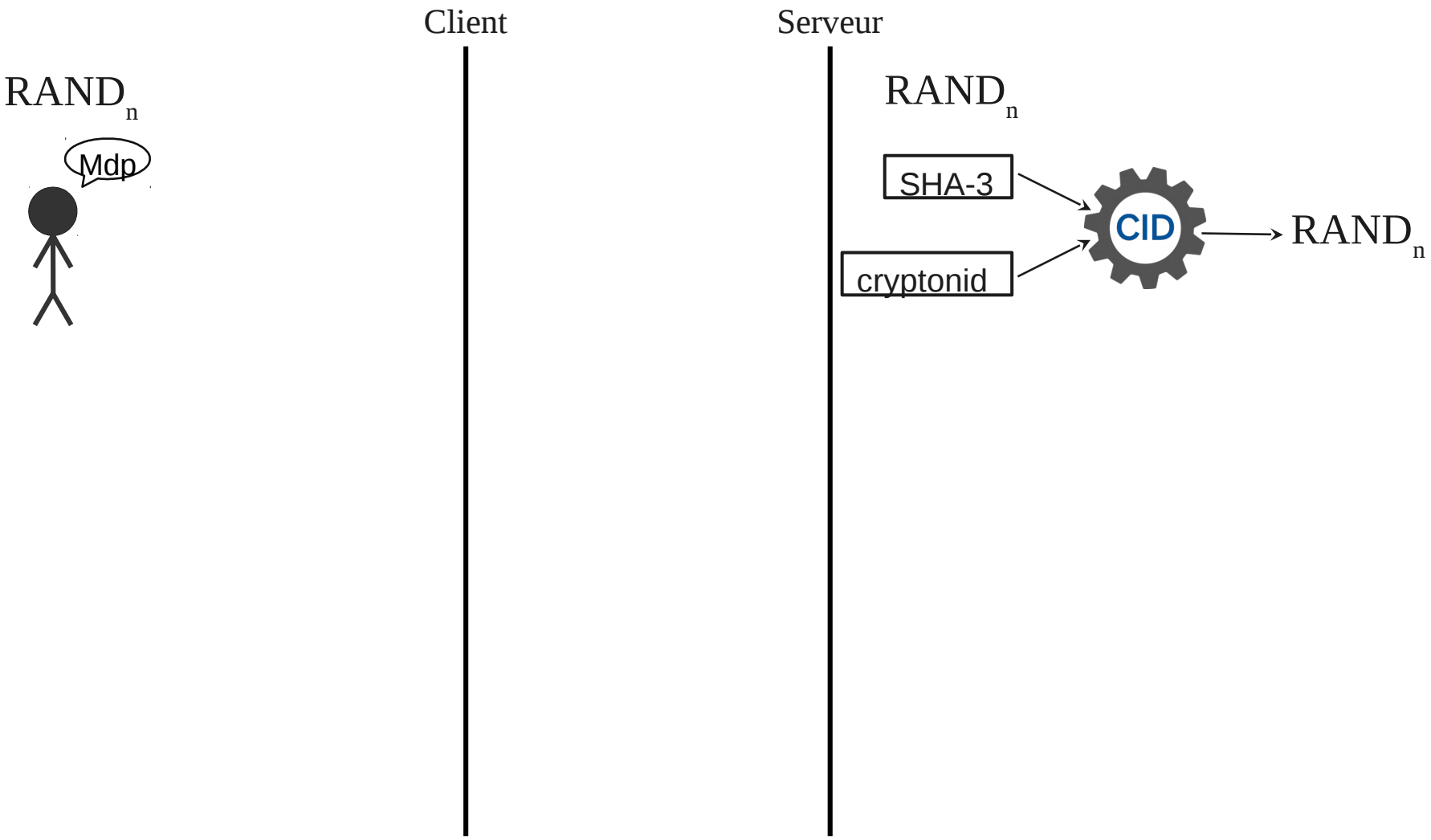



Parenthèse
RAND n
SHA-3
SHA-3
Mdp
cryptonid

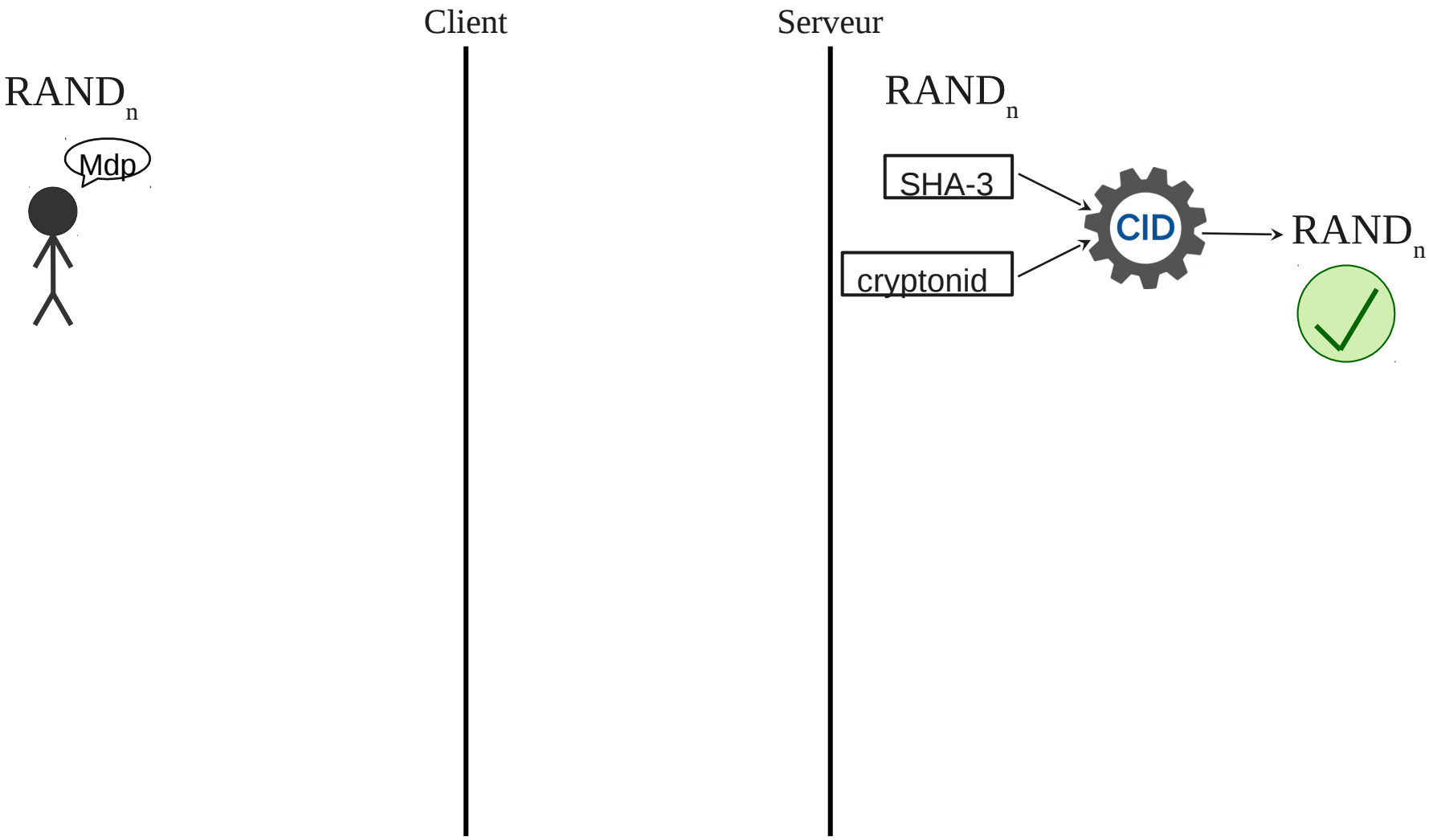
Réellement


RAND n
SHA-3
SHA-3
Mdp
cryptonid
RAND n
autre
SHA-3
SHA-3
cryptonid

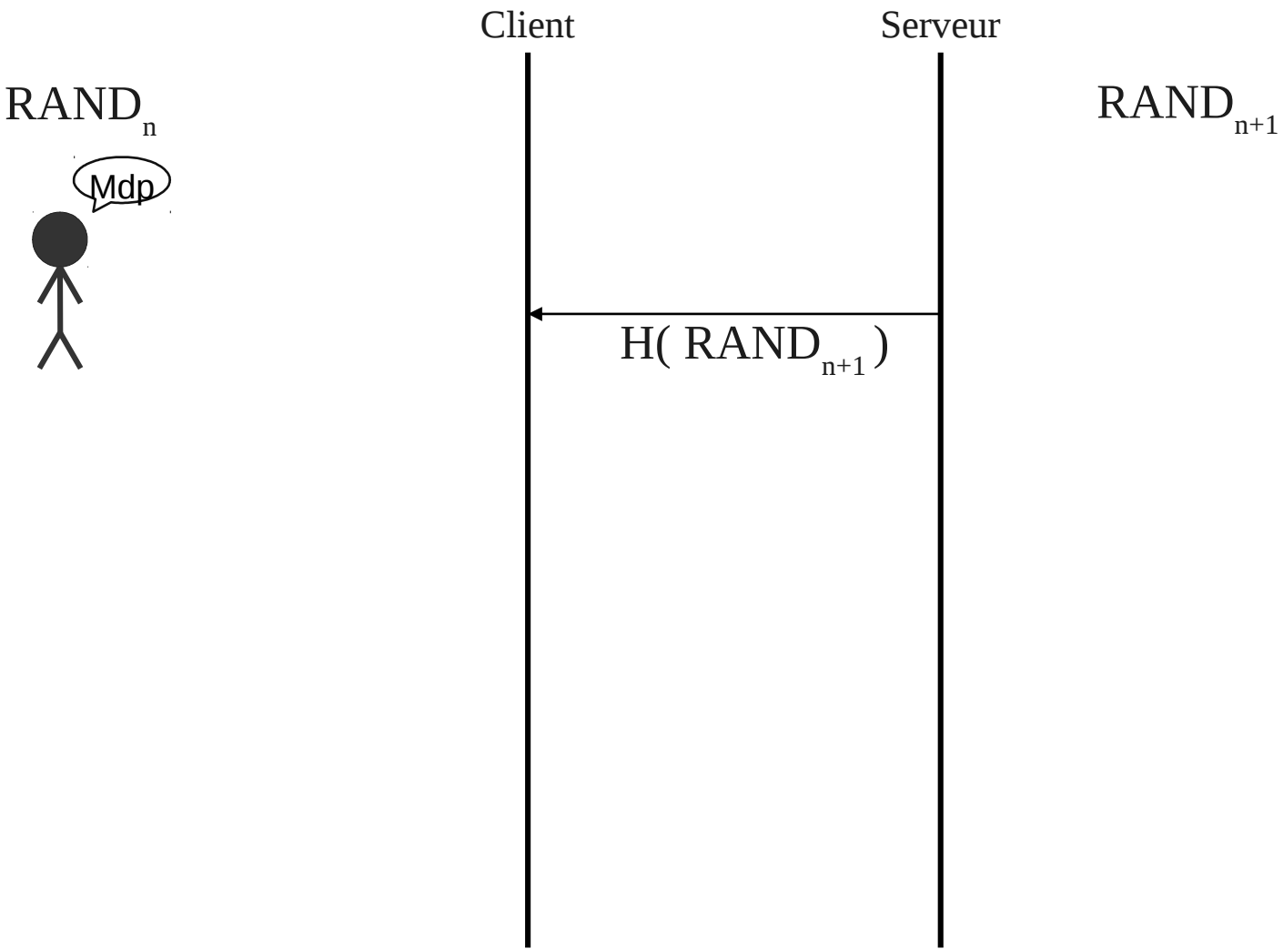
Authentification



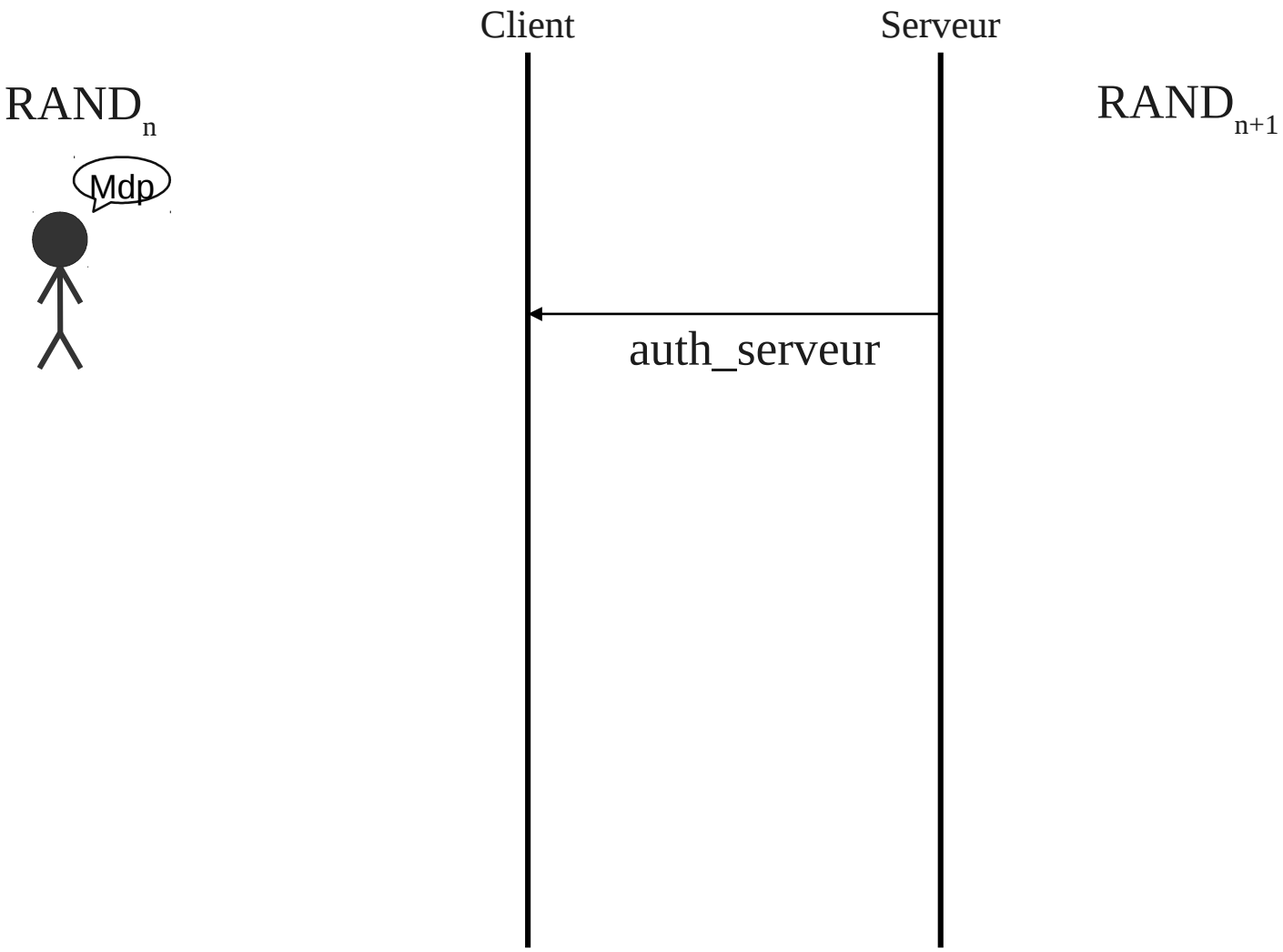
Authentification



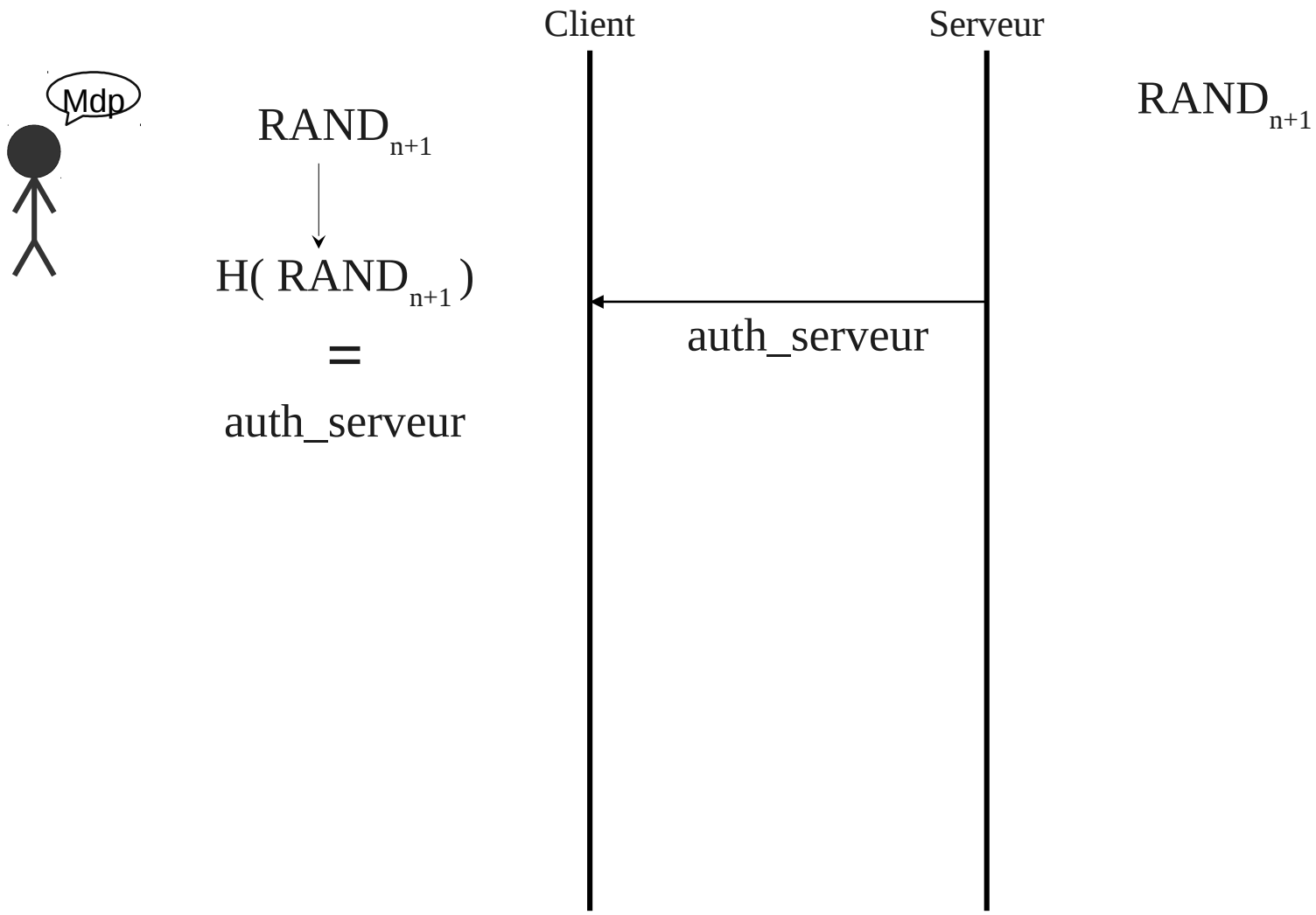
Authentification



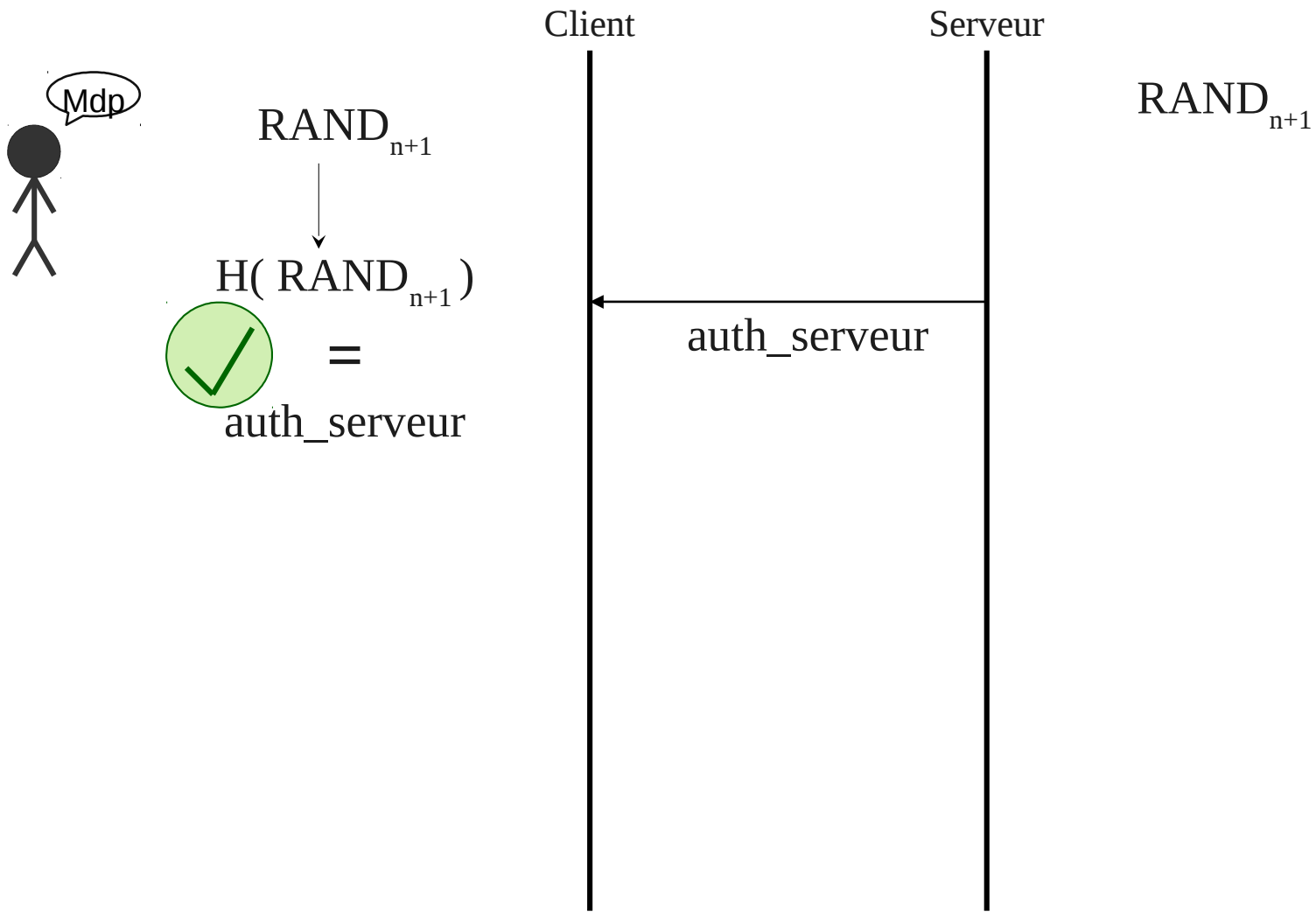
Authentification



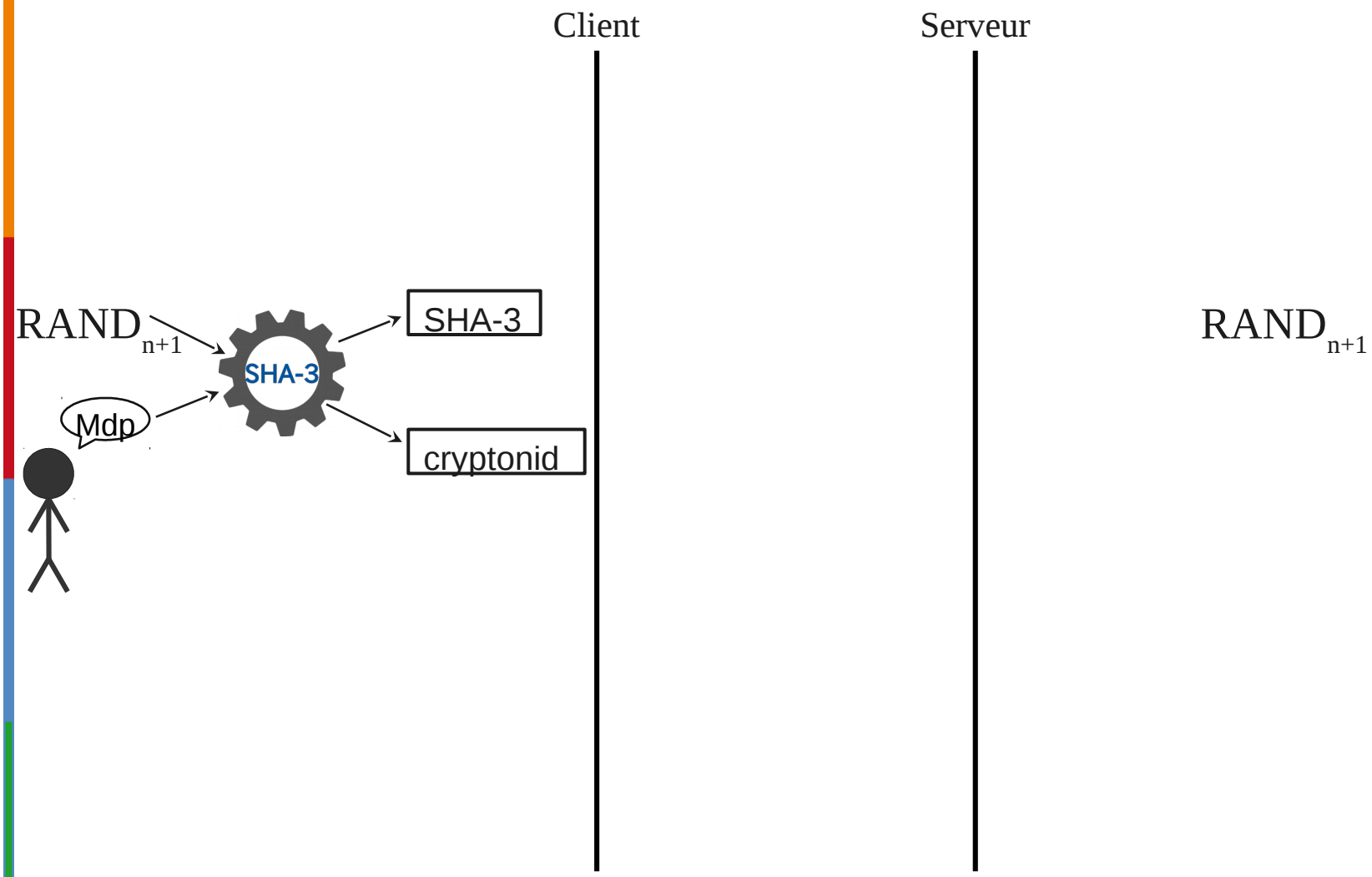
Authentification



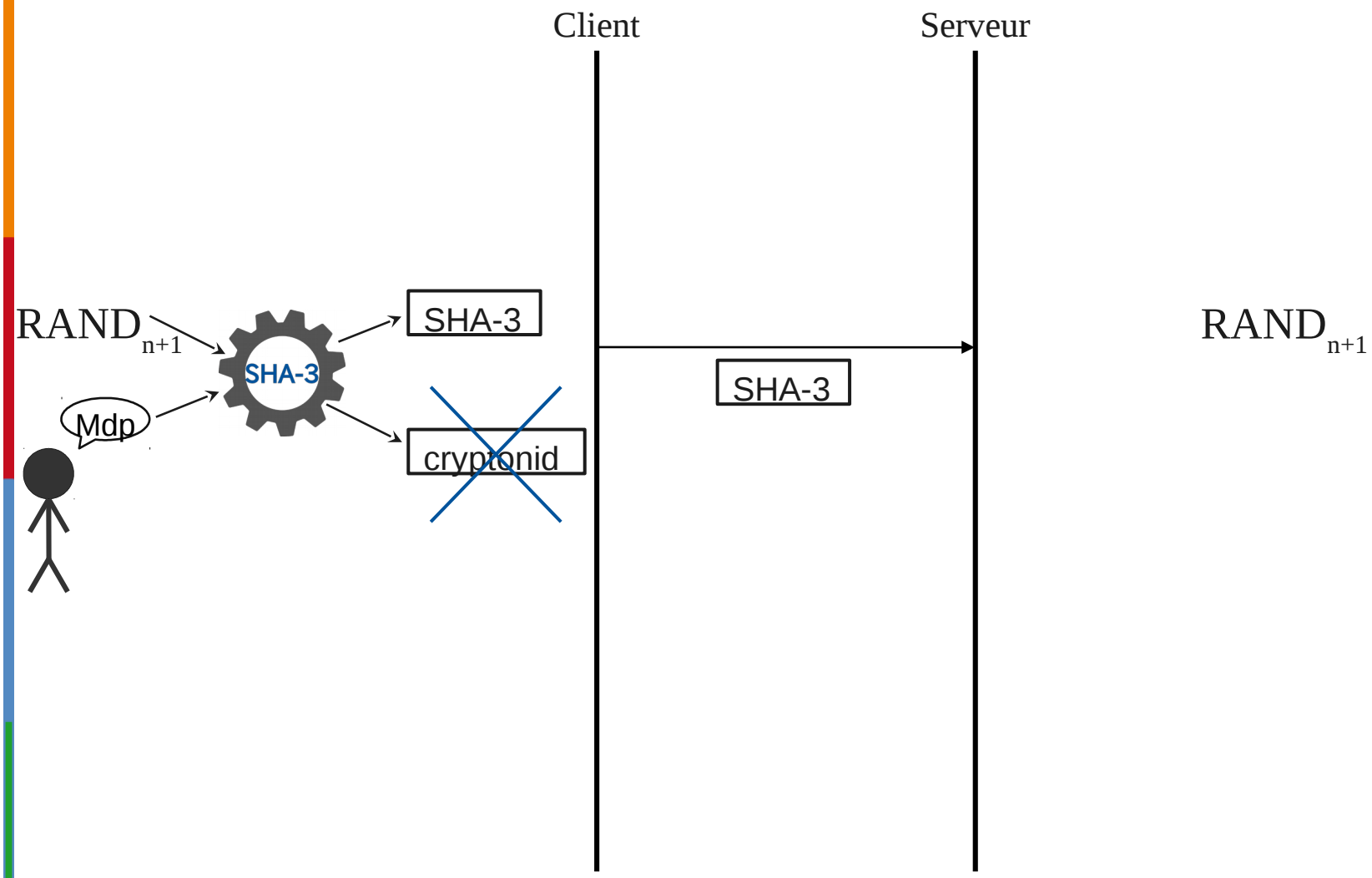
Authentification



Authentification



Authentification

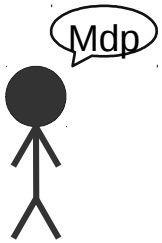


Authentification

Client

Serveur

$RAND_{n+1}$



$RAND_{n+1}$

SHA-3

Points forts

- Compatible avec l’authentification biométrique
- Usurpation d’identité détectée à la reconnexion
- Changement de mot de passe transparent pour le serveur
- L’usage de mots de passe « faibles » n’est plus une faille de sécurité
- Authentification du serveur intégrée
- Faible besoin de ressources et faible consommation d’énergie

Points forts

- Compatible avec l'authentification biométrique
- **Usurpation d'identité détectée à la reconnexion**
- Changement de mot de passe transparent pour le serveur
- L'usage de mots de passe « faibles » n'est plus une faille de sécurité
- Authentification du serveur intégrée
- Faible besoin de ressources et faible consommation d'énergie

Points forts

- Compatible avec l'authentification biométrique
- Usurpation d'identité détectée à la reconnexion
- **Changement de mot de passe transparent pour le serveur**
- L'usage de mots de passe « faibles » n'est plus une faille de sécurité
- Authentification du serveur intégrée
- Faible besoin de ressources et faible consommation d'énergie

Points forts

- Compatible avec l’authentification biométrique
- Usurpation d’identité détectée à la reconnexion
- Changement de mot de passe transparent pour le serveur
- **L’usage de mots de passe « faibles » n’est plus une faille de sécurité**
- Authentification du serveur intégrée
- Faible besoin de ressources et faible consommation d’énergie

Points forts

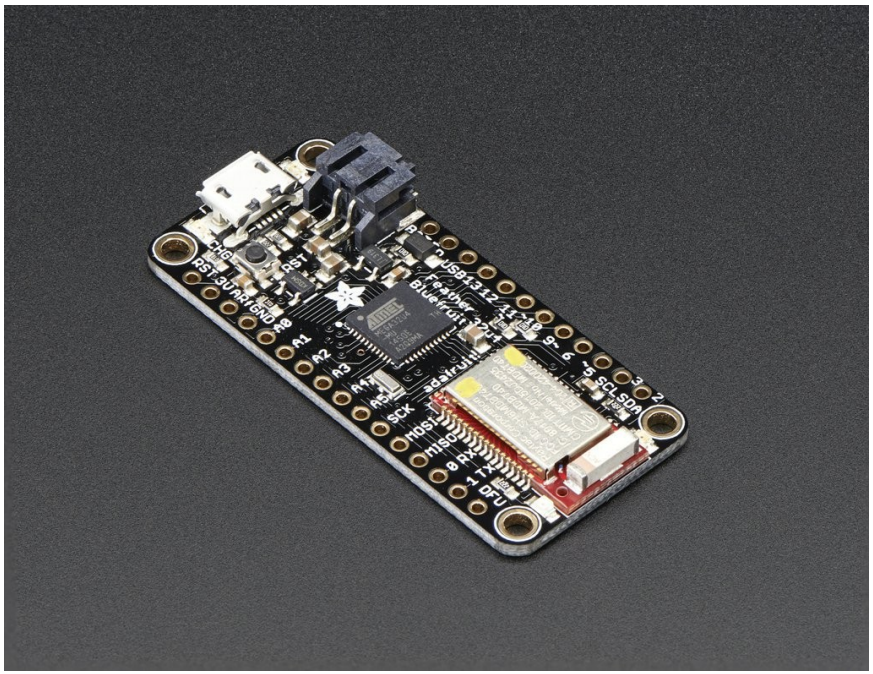
- Compatible avec l’authentification biométrique
- Usurpation d’identité détectée à la reconnexion
- Changement de mot de passe transparent pour le serveur
- L’usage de mots de passe « faibles » n’est plus une faille de sécurité
- **Authentification du serveur intégrée**
- Faible besoin de ressources et faible consommation d’énergie

Points forts

- Compatible avec l'authentification biométrique
- Usurpation d'identité détectée à la reconnexion
- Changement de mot de passe transparent pour le serveur
- L'usage de mots de passe « faibles » n'est plus une faille de sécurité
- Authentification du serveur intégrée
- Faible besoin de ressources et faible consommation d'énergie

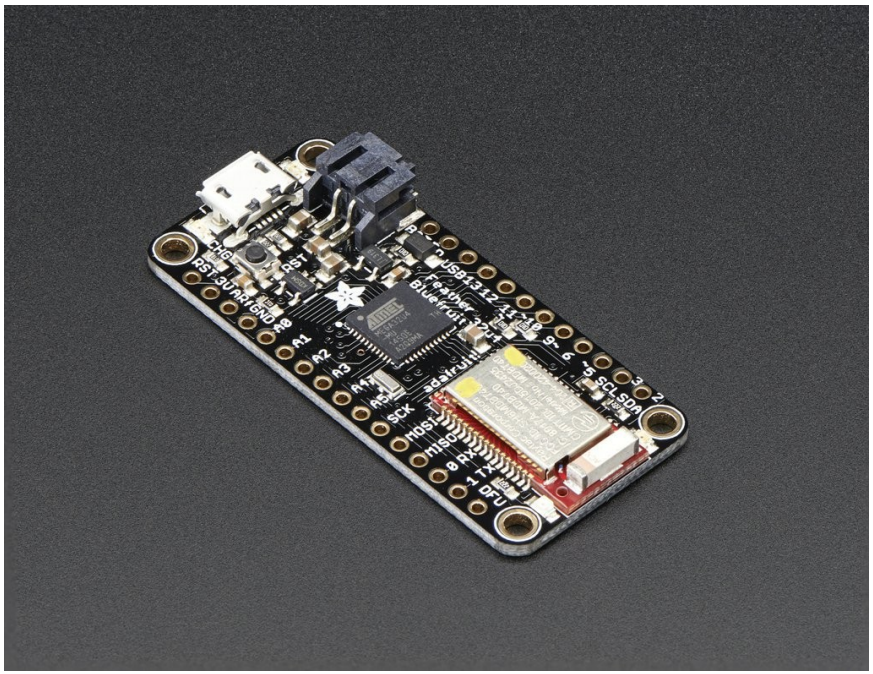
Prototype

Microcontrôleur



Prototype

Microcontrôleur



Utilisation

- ► Remplacer les clés de voiture
- ► Ouvrir des portes
- ► Déverrouiller des stations de travail
- ► Servir comme un deuxième facteur d'authentification (2FA)
- ► Autoriser une transaction bancaire
- ► etc.

Perspectives

- Certification ANSSI
- Intégration dans des objets de la vie quotidienne
- Implémentation sur smartphone iOS et Android
- Intégration de la biométrie comme donnée secrète d'identification

Perspectives

- Certification ANSSI
- Intégration dans des objets de la vie quotidienne
- Implémentation sur smartphone iOS et Android
- Intégration de la biométrie comme donnée secrète d'identification