

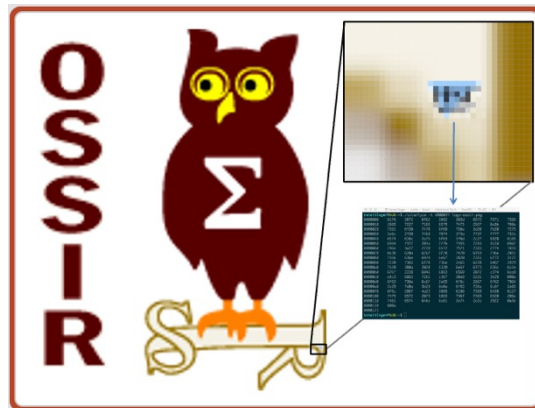
7 avril 2009 [ENSAM]

- Sécurité du passeport biométrique français (*Benoit LEGER, Nicolas CHALANSET / Stelau Conseil*) [\[PDF\]](#)
- Retour d'expérience après une intrusion (*François MORRIS / CNRS*) [\[PDF\]](#)
- Revue d'actualité [\[PDF\]](#)

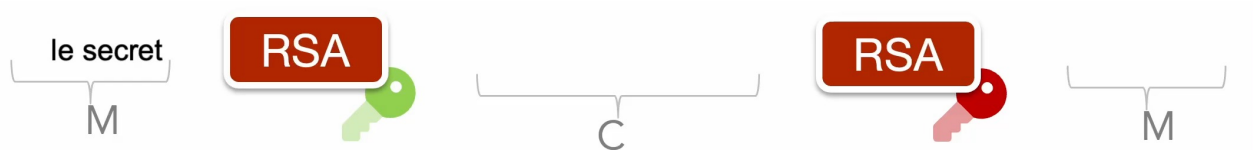
27 janvier 2015

Sécurité des passeports biométriques [\[PDF\]](#)

Nicolas Chalanset, Stelau



Hello !



Hello !



Les 5 primitives cryptographiques

Chiffrement Symétrique



Chiffrement Asymétrique



Résout la difficulté de
l'échange de clé
+
Permet l'usage
du principe de **Signature**
et d'**Authentication**

Fonctions de hachage
cryptographiques



Établissement de clé



Générateurs d'aléa



Very Short Crypto Story

3000 ans de crypto. **symétrique**

*recettes militaro-diplomatiques
de confusion et de diffusion*

Confusion et Diffusion
« tant bien que mal »
de César à Enigma

100 ans de crypto. **moderne**

*de Kerckhoffs ...
au crypto-système incassable*

1. Principes de Kerckhoffs - 1883
2. One Time Pad - 1917



50 ans de crypto. **asymétrique**

LA véritable révolution

Résout la difficulté de
l'échange de clé
+
Permet l'usage du
principe de **Signature**



20 ans de crypto. **post quantique**

révolution ? (ou pas)



Qu'est ce qui a changé depuis 2009/2015 ?

RF

Prénoms / Given names
Maëlys-Gaëlle, Marie

SEXE / Sex **F** NATIONALITÉ / Nationality **FRA** DATE DE NAISS. / Date of birth **13 07 1990**

LIEU DE NAISSANCE / Place of birth
PARIS

NOM D'USAGE / Alternate name
NOM D'USAGE

N° DU DOCUMENT / Document No.
X4RTBPFW4

DATE D'EXPIR. / Expiry date
11 02 2030

Signature

384213

Identité Numérique d'État

Qu'est-ce que l'identité numérique ?

... des usages :

- Justificatifs d'identité
- Signatures CEV + PAdES
- Vérification en ligne
- Authentification Services
- Permis de conduire
- Prouver certains attributs
- Procuration de vote
- Attestations Tiers
- « device engagement » avec photo
- ...



fin 2023: 17M détenteurs d'une CNIe

france-identite.gouv.fr

France Identité
Gardez la maîtrise de vos données d'identité

Accueil En savoir plus Questions fréquentes Actualité Justificatif d'identité Contact Votre compte

Gardez la maîtrise de vos données d'identité

- 👤 Prouver votre identité sans divulguer toutes vos données
- 🛡️ Éviter l'usurpation de votre identité
- 🔑 Remplacer vos identifiants et mots de passe

DISPONIBLE SUR Google Play

Télécharger dans l'App Store

France Identité permet de



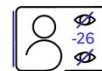
Fournir un justificatif d'identité à usage unique

Facilement, en toute sécurité, et à usage unique. Terminés les scans de carte d'identité !



Accéder à plus de 1400 services en ligne

Un compte unique pour accéder à tous vos services.




Prouver votre identité ou de certains attributs...

En ligne ou pour des usages de proximité avec ou sans partage de vos données



ou encore de votre droit à conduire

Lors d'un contrôle routier ou pour louer un véhicule




RÉPUBLIQUE FRANÇAISE
*Liberté
Égalité
Fraternité*

Justificatif d'identité à usage unique


N° Z6KZAAT76UI2TXC

CADRE D'UTILISATION	
DESTINÉ À 072c immo	NOTIF Location d'appartement
GÉNÉRÉ LE 06/09/2023	DATE LIMITE D'UTILISATION 11/12/2023

ÉMETTEUR	
NOM Martin	
PRÉNOMS Maëlys-Gaëlle, Marie	
SEXE F	NATIONALITÉ FRA
DATE DE NAISSANCE 13/07/1990	
LIEU DE NAISSANCE Paris	



Vérifier ce justificatif sur france-identite.gouv.fr/justificatif



Une signature électronique du ministère de l'Intérieur

Un destinataire

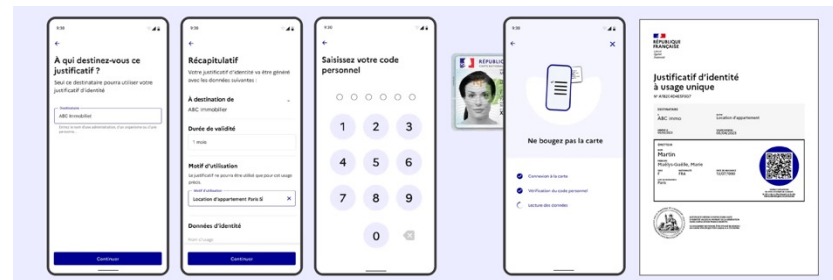
Un motif (facultatif)

Une date limite d'utilisation

Un QR code sécurisé vérifiable en ligne

Un émetteur

Une signature électronique du ministère de l'Intérieur



Parcours SSI complexe

SSI : AdRs - Audits – Certifications

1. Analyses de risques
2. CSPN / CESTI
3. Qualification Elémentaire / ANSSI
4. MIE élevé / ANSSI
5. Guide d'Hygiène / ANSSI
6. 27K1
7. PASSI
8. SHFD
9. Bug Bounty
10. Red Team
11. Analyse de la fraude

Service

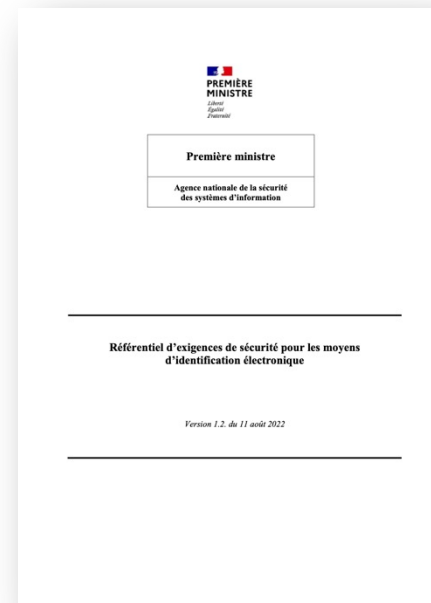
Mis à jour le 26 Avril 2024

France Identite

Type de service: MIE Nom du fournisseur: Ministère de l'Intérieur et des Outre-mer Date de début de certification: 07/02/2024

Date de fin de certification: 07/02/2026

Niveau de recommandation: ✓ - Optimal



Les 5 primitives cryptographiques

Chiffrement Symétrique



Chiffrement Asymétrique



Résout la difficulté de
l'échange de clé
+
Permet l'usage
du principe de **Signature**
et d'**Authentication**

Fonctions de hachage
cryptographiques












Établissement de clé



Générateurs d'aléa



Normes	Mécanismes de sécurité	Objectifs de sécurité	Fonctions Cryptographiques	Obligatoire / Facultatif	France
OACI 9303	BAC	contrôle d'accès confidentialité des échanges	authentification (symétrique) échange de clés de session	facultatif	✗
	Passive Auth.	Intégrité et Authenticité	Vérification de signature [~ <i>certificaf</i>]	obligatoire	X
	Active Auth.	Originalité du composant	Signature électronique [<i>défi-réponse</i>]	facultatif	
OACI 9303	PACE (SAC)	Contrôle d'accès Confidentialité des échanges	Diffie-Hellman éphémère [<i>secret partagé</i>]	obligatoire	X (depuis décembre 2014)
EAC TR03110 V 2.20	Chip Auth. v1	Originalité du composant Contrôle d'accès Confidentialité des échanges	Diffie-Hellman éphémère [<i>bi-clé composant/puce</i>]	obligatoire	X (depuis juin 2009)
	Term Auth. v1	Contrôle d'accès (authentification du lecteur)	Vérification de signature Chaine de certificats Signature électronique [<i>défi-réponse</i>]	obligatoire	X (depuis juin 2009)

Normes	Mécanismes de sécurité	Objectifs de sécurité	Fonctions Cryptographiques	Obligatoire / Facultatif	France
OACI 9303	BAC	contrôle d'accès confidentialité des échanges	   authentification (symétrique) échange de clés de session	facultatif	X
	Passive Auth.	Intégrité et Authenticité	Vérification de signature [~ <i>certificat</i>] 	obligatoire	X
	Active Auth.	Originalité du composant	Signature électronique [<i>défi-réponse</i>] 	facultatif	
OACI 9303 TR 03110	PACE (SAC)	Contrôle d'accès Confidentialité des échanges	Diffie-Hellman éphémère [<i>secret partagé</i>] 	obligatoire	X (depuis décembre 2014)
EAC TR 03110 V 2.20	Chip Auth. v1	Originalité du composant Contrôle d'accès Confidentialité des échanges	Diffie-Hellman éphémère [<i>bi-clé composant/puce</i>] 	obligatoire	X (depuis juin 2009)
	Term Auth. v1	Contrôle d'accès [<i>authentification du lecteur</i>]	Vérification de signature Chaine de certificats Signature électronique [<i>défi-réponse</i>]  	obligatoire	X (depuis juin 2009)

OACI



Passport

PACE

Passive Authentication

Benoit
LEGER-DERVILLE
29-02-77
à BourgLaVille

S_{0D}
r9zNN1c/+B
stc6nhaLuf
e0wCkbNFwJ
q2I1husnIk

CERT
France

P<NLDDE<BRUIJN<WILLEKE<LISELOTTE<<<<
SPECI20142ND6503101F2403 TCEILOTTE<<<< 84

PAYS SIGNATAIRE

RSA

Active Authentication

GTFFYSHJSU
SHA
b6e296cc48
838ebb9df7

RSA
stc6nhaLuf
r9zNN1c/+B

GTFFYSHJSU
PRNG
r9zNN1c/+B
stc6nhaLUf

RSA

Chip Authentication

DH
 K_{CA}
AES

AES
 K_{CA}
DH

Terminal Authentication

PRNG
OKN0NCE009
RSA
 K_p
Ufm/+A56/+
Bstc6nhako

OKN0NCE009
SHA
b6e296cc48
838ebb9df7
r9zNN1c/+B
stc6nhaLuf
RSA
 K_s

Benoit
LEGER-DERVILLE
29-02-77
à BourgLaVille

SHA
b6e296cc48
838ebb9df7
4aba8dba81
26b1970267

RSA
r9zNN1c/+B
stc6nhaLuf
e0wCkbNFwJ
q2I1husnIk

S_{0D}
Security
Object
document

Assemblage
riche et
complexe
mais sans
surprise !

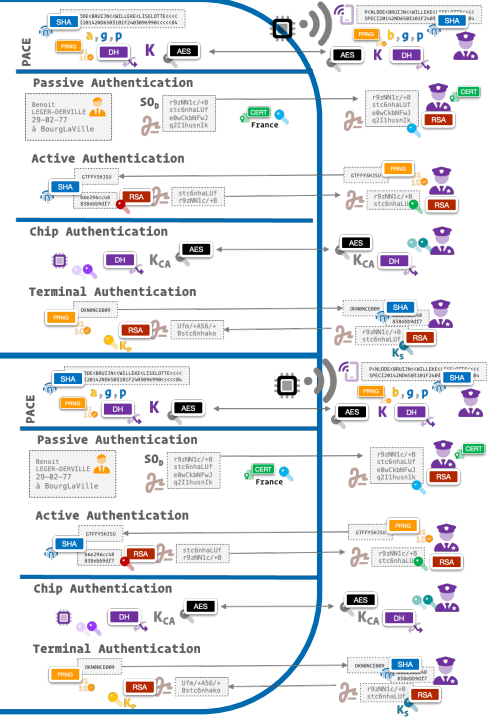


ICAO

- PACE
- Passive Authentication
- Active Authentication
- Chip Authentication
- Terminal Authentication

eID

- PACE
- Passive Authentication
- Active Authentication
- Chip Authentication
- Terminal Authentication



CNIe

PACE



Passive Authentication

Benoit
LEGER-DERVILLE
29-02-77
à BourgLaVille

$S0_D$
r9zNN1c/+B
stc6nhaLUf
e0wCkbNFwJ
q2I1husnIk

CERT
France

r9zNN1c/+B
stc6nhaLUf
e0wCkbNFwJ
q2I1husnIk

CERT
RSA
Police Officer icon

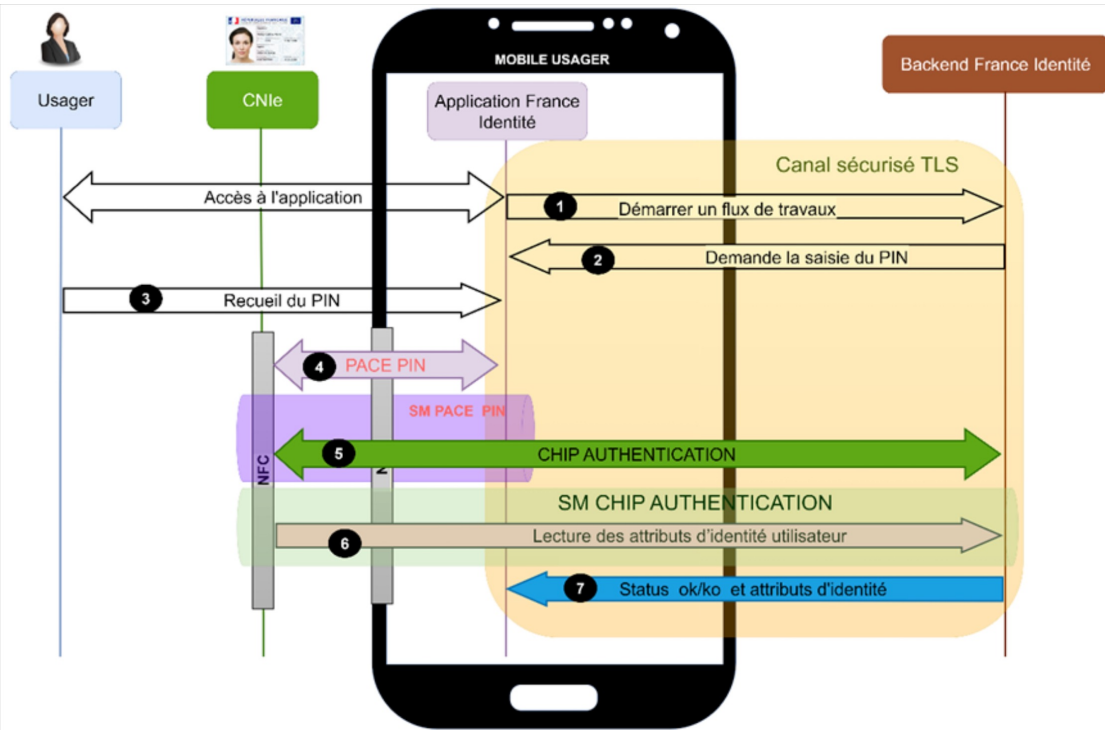
Active Authentication

Chip Authentication



Terminal Authentication





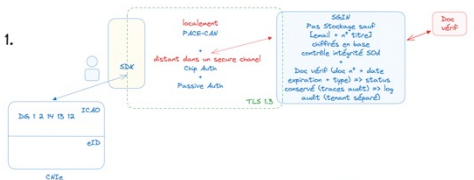
1. Récupération par le Produit, depuis le Backend, du scénario de lecture ;
2. Le Produit demande le code PIN ;
3. Le Produit recueille le code PIN via un clavier sécurisé ;
4. Le Produit initie le PACE-PIN puis le *Secure Messaging* correspondant ;
5. Le Produit permet l'établissement entre le Titre et le Backend du canal de « *Chip Authentication* » et du « *Secure Messaging* » correspondant ;
6. Le Backend lit les données d'identité de l'utilisateur dans l'application « *eID* » de la CNIe ;
7. Le Backend retourne au Produit le statut de validité du titre et le cas échéant les attributs d'identité de l'utilisateur.

Les obligations du MIE

II.2.1. Inscription

II.2.1.2. Preuve et vérification d'identité (personne physique)

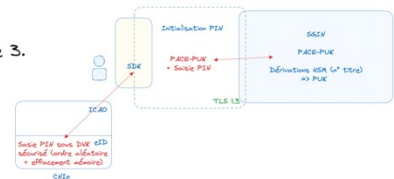
Etape 1.



Etape 2.



Etape 3.



Bilan :

Trois Facteurs :
App/Mobile avec les DG stockés
+ PIN
+ CNIe

=> multi-device via le compte S&SIN (n-mobilité)

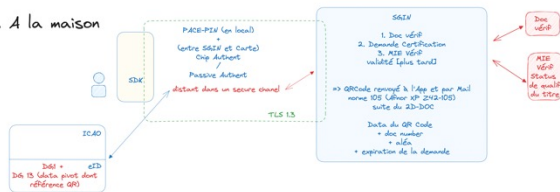


II.2.2. Gestion des moyens d'identification électronique

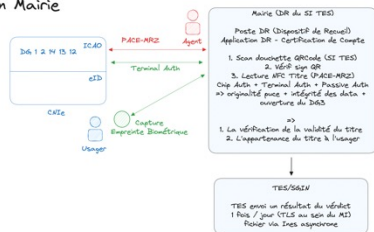
II.2.2.2. Délivrance, mise à disposition et activation

II.2.2.2. MIE Elevée = Certification de Compte

1. A la maison



2. En Mairie



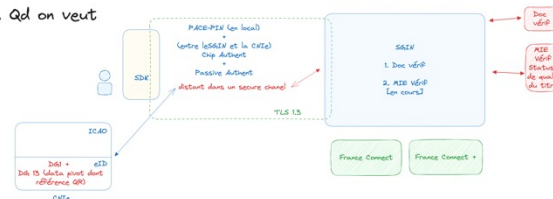
- 24h plus tard - hors Mairie



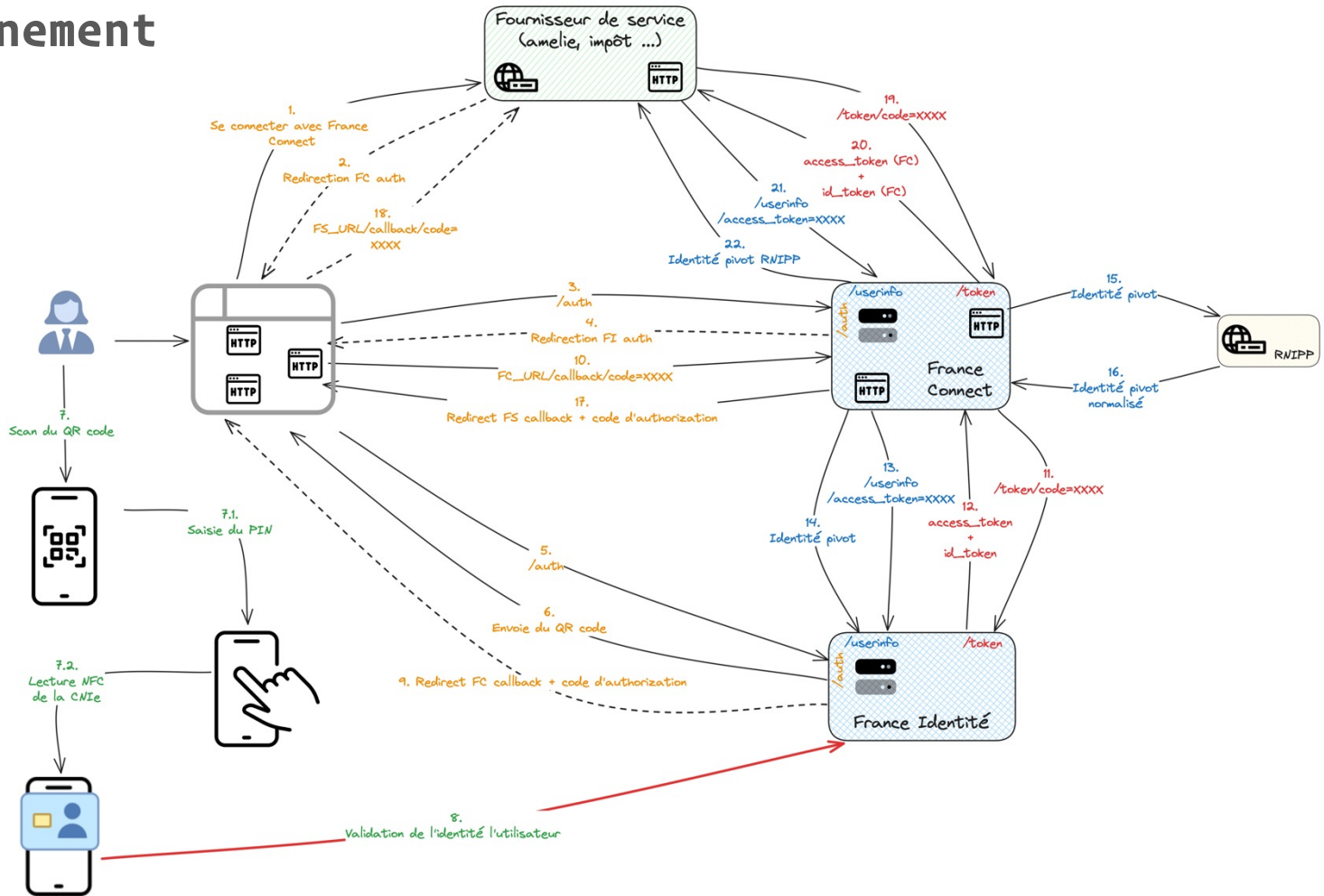
II.2.3. Authentification

II.2.3.1. Mécanisme d'authentification

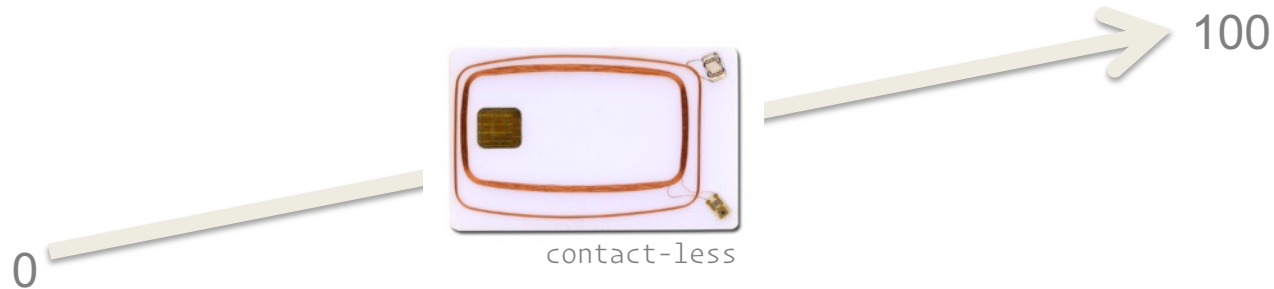
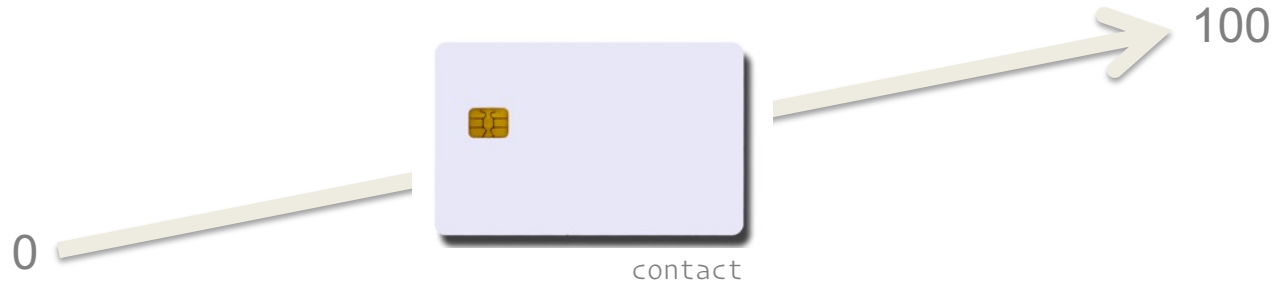
1. Qd on veut



Fonctionnement



Attention : « C'est (*pas*) sécurisé ! » ne veut rien dire



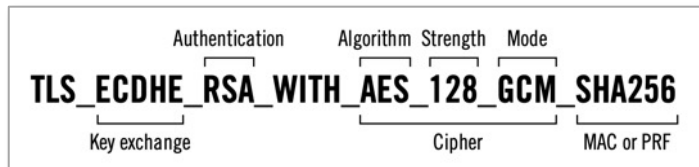
Trois usages différents

RSA

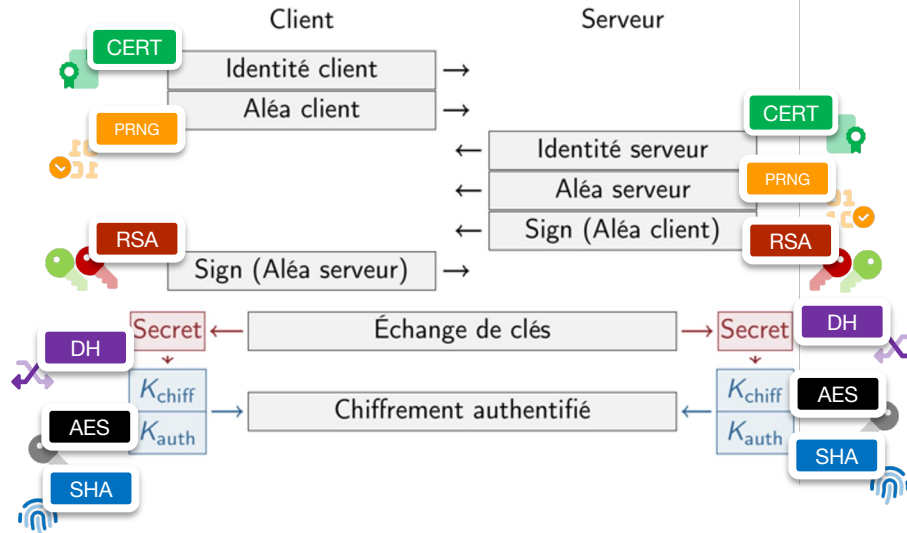


	clé privée	clé publique
chiffrement	déchiffrer	chiffrer
signature	signer	vérifier
authentification	signer	vérifier

Assemblage Crypto

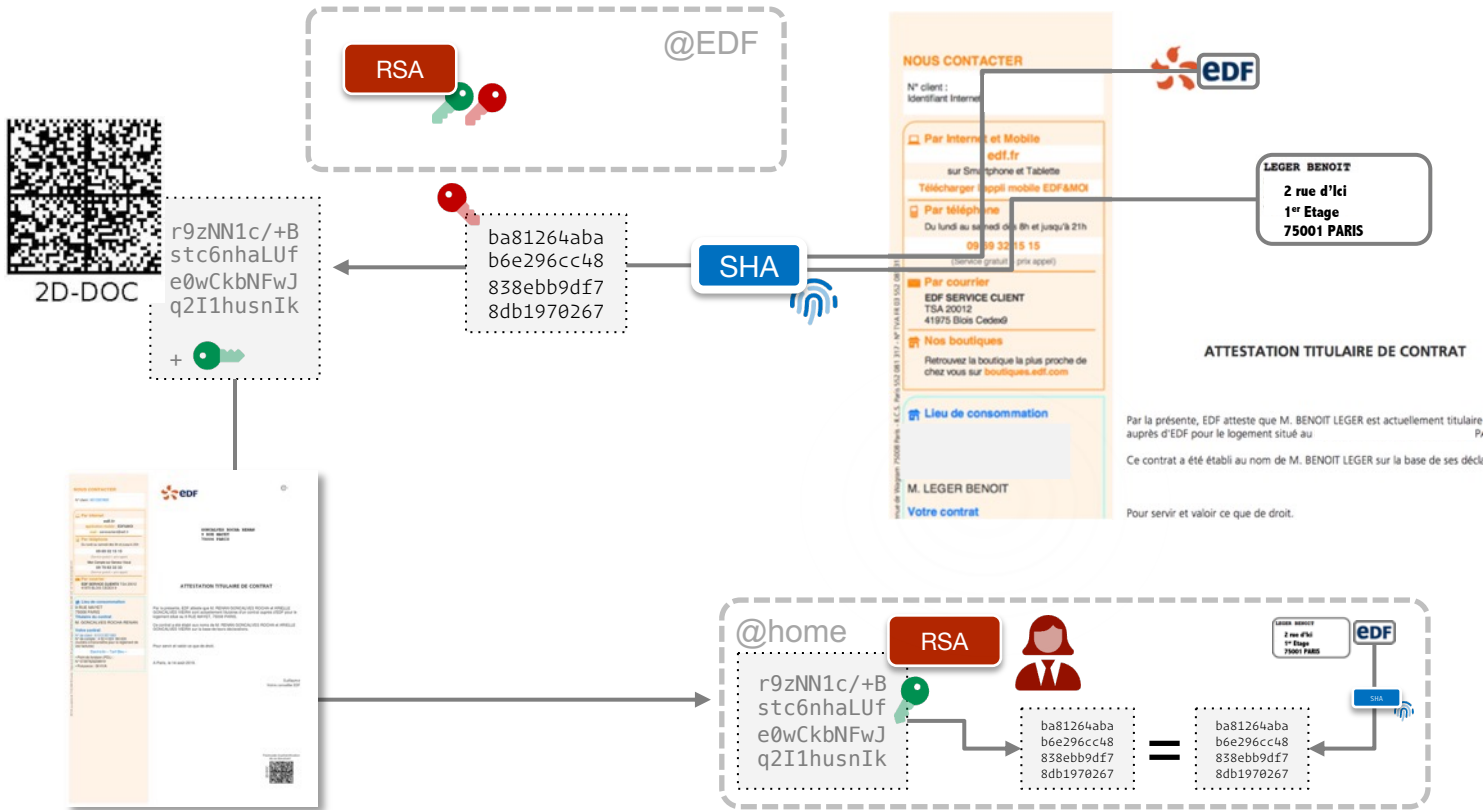


TLS 1.3



Cipher Suite Name	Auth	KX	Cipher	MAC	PRF
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	RSA	ECDHE	AES-128-GCM	-	SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDSA	ECDHE	AES-256-GCM	-	SHA384
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DHE	3DES-EDE-CBC	SHA1	Protocol
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES-128-CBC	SHA1	Protocol
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	ECDSA	ECDHE	AES-128-CCM	-	SHA256

CEV : Cachet Electronique Visible



Certificat électronique



Ce n'est pas une primitive cryptographique

C'est un assemblage

C'est un fichier comme un autre

1. Clé publique
2. Identité
3. Signature du hash de la clé publique et de l'identité par un tiers

