

X GIBNEY OSCAR® WINNING DIRECTOR OF GOING CLEAR AND TAXI TO THE DARK SIDE



WORLD WAR 3.0

"A WHITE KNUCKLE THRILLER.
Clear, urgent, and positively terrifying at times."
-Peter Debruge, Variety

ZER0 DAYS

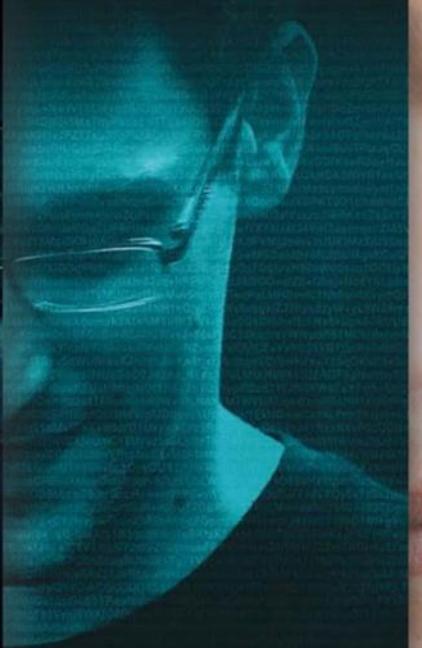
© 2013 CIRQUE PICTURES and PARTICIPANT MEDIA, Inc. in association with ZERODAY DOCUMENTARY FILMS & GLOBAL PRODUCE / OSCAR® nominee "ZERODAYS"
by ANDY GREENE
PRODUCED BY ANDREW REISS and BRETT WILLEY
DIRECTED BY ANDREW REISS and BRETT WILLEY
WRITTEN BY ANDREW REISS and BRETT WILLEY
EDITED BY ANDREW REISS and BRETT WILLEY
MUSIC BY DAVID HORNBERG and REX SAWAYNE
CINEMATOGRAPHY BY ANDREW REISS and BRETT WILLEY

REMASTERED BY ANDREW REISS and BRETT WILLEY

DISTRIBUTED BY VINTAGE

IN SELECTED CINEMAS

COMING JULY 8



AUX OSCARS®
HOMMAGE
AU FILM DOCUMENTAIRE

PAR
A POITRAS

CO-AUTEUR EXÉCUTIF:
STEVEN SODERBERGH

ENFOUR

© 2013 CIRQUE PICTURES and GLOBAL PRODUCE / OSCAR® nominee "ZERODAYS"
by ANDREW REISS and BRETT WILLEY
PRODUCED BY ANDREW REISS and BRETT WILLEY
DIRECTED BY ANDREW REISS and BRETT WILLEY
WRITTEN BY ANDREW REISS and BRETT WILLEY
EDITED BY ANDREW REISS and BRETT WILLEY
MUSIC BY DAVID HORNBERG and REX SAWAYNE
CINEMATOGRAPHY BY ANDREW REISS and BRETT WILLEY



ONCE YOU'RE IN, THERE'S NO WAY

TEHRA

La signature électronique sécurisée



F96DE8C227A259C87EE1DA2AED57C93
FE5DA36ED4EC87EF2C63AAE5B9A7EFF
D673BE4ACF7BE8923CAB1ECE7AF2DCF
7AE29A3DA44F235A24C963FF0DF3CA3
599A70E5DA36BF1ECE77F8DC34BE129
A6CF4D126BF5B9A7CFEDF3EB850D37C
F0C63AA2509A76FF9227A55B9A6FE3D
720A850D97AB1DD35ED5FCE6BF0D138
A84CF8DC34BE129F8DC34B

EX_MACHINA



Bitcoin as Frankenstein creature ?

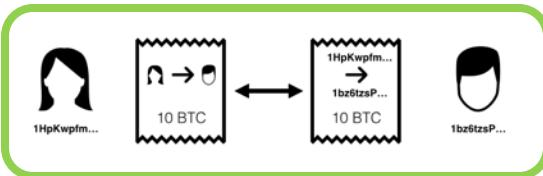
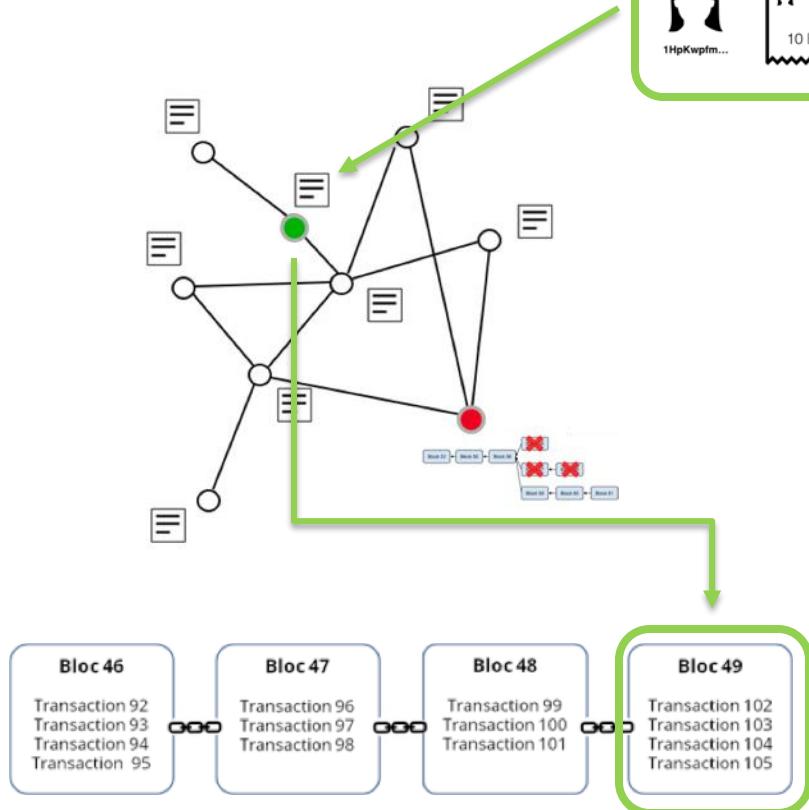


Bitcoin





Bitcoin



preuve de possession - imputabilité

anonymat - pseudonymat

tracabilité - intégrité - non répudiation

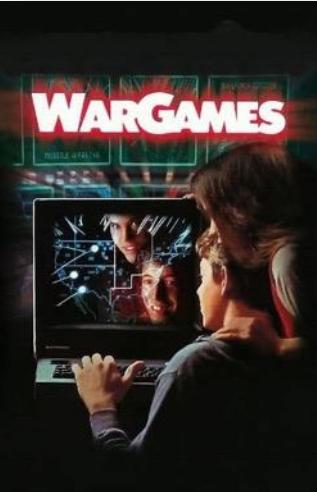
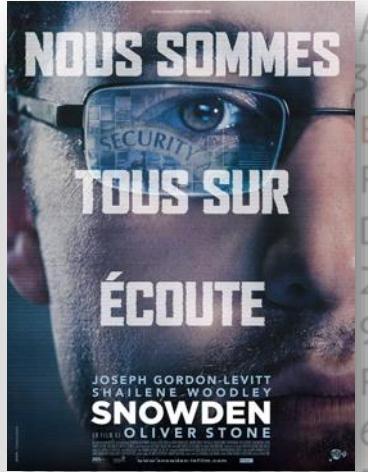
disponibilité - accessibilité

évolutivité - adaptabilité - scalability

autonomie et pérennité de fonctionnement

consensus décentralisé et automatisé

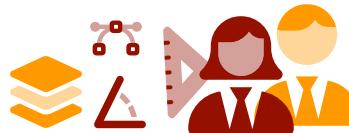
unicité de la dépense (anti double spending)



Voilà ... c'est fini !

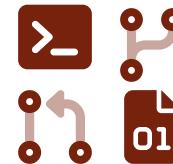
Ingénieur(e)s

- scientifiques
- design



Code

- préhistoire
- tout à inventer



Stage

- pas très grave
- management

1^{ère} page du rapport le 1^{er} jour + répétitions



Cabinet d'Experts Cybersécurité



reBop.io

Certificate Lifecycle Management



The screenshot shows the reBop web application interface. At the top, there's a navigation bar with links for 'Features', 'Pricing', 'Docs', 'More', and a user profile. Below the navigation is a search bar and a 'launch' button. The main area has tabs for 'Alerts' (selected), 'Logs', 'Menus', 'Theme', and 'Agent'. The 'Alerts' tab displays a list of certificates with their status (e.g., 'RENEWED', 'EXPIRATION', 'EXPIRED') and expiration dates. A modal window titled 'Online Error Cert' provides detailed information about a specific certificate, including its CN (apm-factoring.societe generale.com), issuer (QuoVadis Global SSL ICA G3), SN (2C17C3A94AAZ19E7EE391F46A92EC08CF55A38A5), and expiration date (10 Jul 2022 15:28:00). It also lists locations: C: FR, S: Ile-de-France, L: Paris, O: Societe Generale SA, and SSID: 28222. Logos for QuoVadis Limited and QuoVadis Global SSL ICA G3 are shown. A large blue callout box highlights the 'Manage online invalid certificates' feature.

All alert logs at the right place

Fighting against expiration is a real sport. reBop allows you to play in the big leagues.

Expired and revoked

With clearly and easily identified badges, locations with expired and revoked certificates are obvious.

Checking alert logs

Based on the experience of its customers, reBop offers you to come and check the alert logs at least once every 5 days.

Manage online invalid certificates

With reBop quickly detect at a glance your still online expired, revoked or suspended certificates.

It's time to clean up and ask your team why these online hosts still have

Offre de stage

candidats à voir

1. **Expertise SSI** : Consulting, analyse technique Cyber/SSI/Crypto, Lecture/rédaction de cible de sécurité labo CESTI, Lecture de spécifications (Passeport biométrique et Carte d'Identité électronique), Rédactions de notes techniques

=> Objectif n° 1 :

devenir **Consultant(e) Expert Cyber**
+ à terme Auditeur MIE / PVID / eIDAS / 27K1

2. **Code** : Développement d'outils internes et commerciaux Stelau
(IdCheck, IdFod, reBop, Lib CEV et VDS Verify)

=> Objectif n° 2 :

Connaitre et **maitriser** l'assemblage des primitives cryptographiques de cybersécurité

3. **Conception** : Participation à l'élaboration et au maintien des Cours EPITA et EGE (renouvellement et adaptation des TP, TD et jeux cryptographiques).

=> Objectif n° 3 :

Apprendre et enseigner

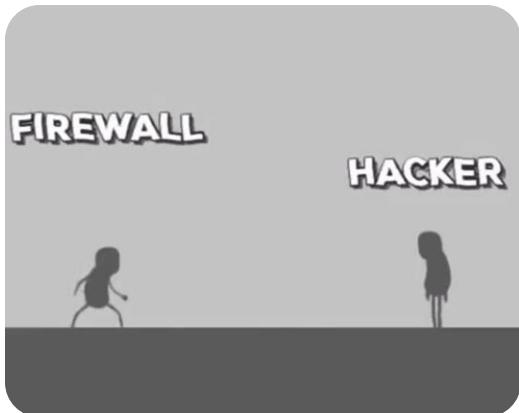
excellents stages
missions formatrices
rémunération ++



A screenshot of the France Identité mobile application. The top navigation bar includes the logo, "France Identité", and tabs for "Accueil", "En savoir plus", "Questions fréquentes", "Actualité", "Justificatif d'identité", "Contact", and "Votre compte". Below the navigation is a large image of a smartphone displaying a digital French ID card (Carte Nationale d'Identité). The card shows a photo of a person named MARTIN, born on 13.07.1990 in Paris, with a validity date of 11.02.2030. Buttons for "Scanner un QR Code", "Créer un justificatif d'identité", and "Télécharger la version Web de l'application" are visible. The main slogan "Gardez la maîtrise de vos données d'identité" is prominently displayed on the right side.



le hacking facile



Historique

rien n'a vraiment changé

.00 Phrack 49 Oo.

Volume Seven, Issue Forty-Nine

File 14 of 16

BugTraq, r00t, and Underground.org
bring you

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Smashing The Stack For Fun And Profit
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

by Aleph One
aleph1@underground.org

'smash the stack' [C programming] n. On Many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trashing the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See span; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.

Introduction

Over the last few months there has been a large increase of buffer overflow vulnerabilities being both discovered and exploited. Examples of these are syslog, splittv, sendmail 8.7.5, Linux/FreeBSD mount, Xt library, at, etc. This paper attempts to explain what buffer overflows are, and how their exploits work.

Basic knowledge of assembly is required. An understanding of memory concepts, and experience with gdb are very helpful. We also assume we are working with an Intel x86 CPU. Our system is Linux.

UaF + dF
RUST

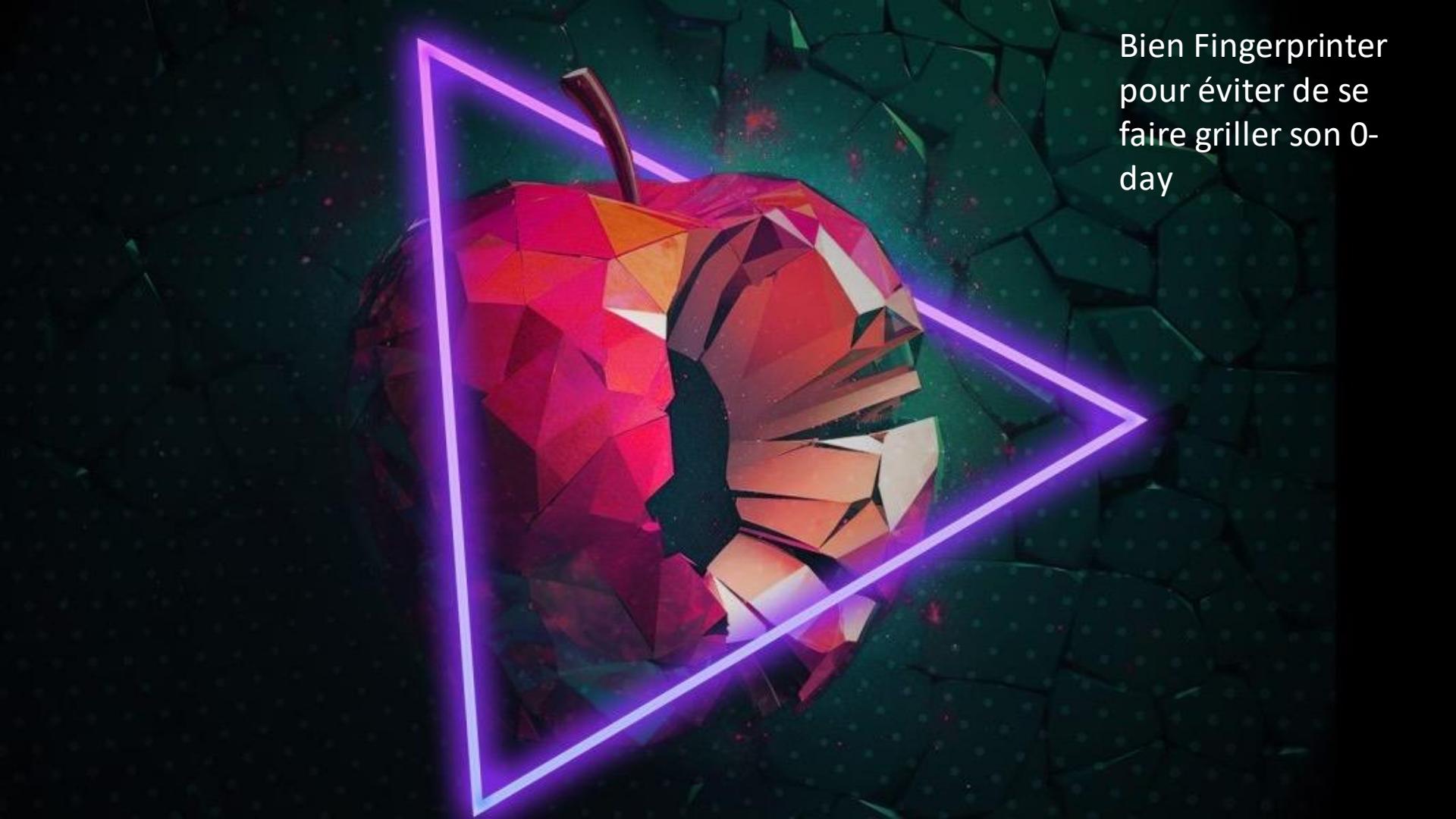
il y a 27 ans,
le 11 août 1996 un certain aleph_one publie
"Smashing The Stack For Fun And Profit" »
dans une revue de hackers (*phrack* n°49).



- Ce qu'il faut retenir :
 - o N'importe quel appareil équipé d'un CPU qui fait tourner du code est potentiellement vulnérable

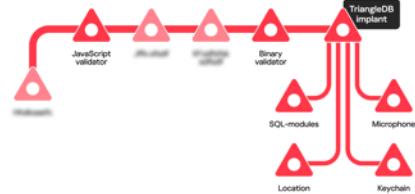
Writing an Exploit

(or how to mung the stack)



Bien Fingerprinter
pour éviter de se
faire griller son 0-
day

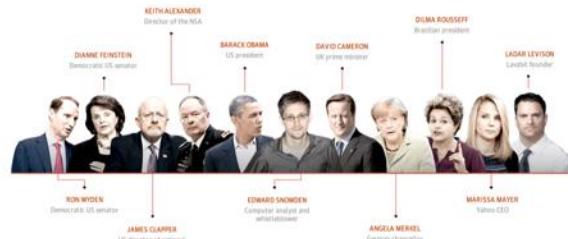
Operation Triangulation



- JavaScript Validator
- Binary Validator
- Looking for traces in logs
- Microphone recording
- Keychain exfiltration
- SQLite stealing modules
- Location-monitoring module

US-984XN

<http://goo.gl/SNEXRo>

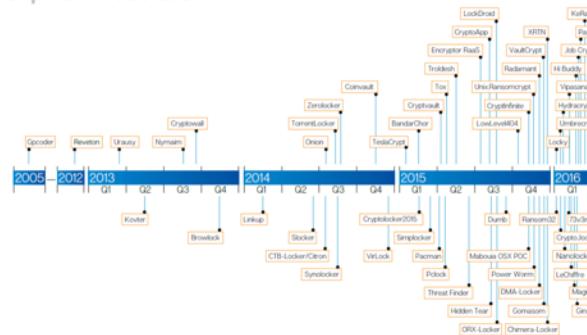


12

□ STELAU

2016 année des ransomwares

explosion des cas



□ STELAU

11

Stuxnet – Juin 2010

Un avant et un après Stuxnet ?



Objectif : ralentir le programme d'enrichissement nucléaire Iranien

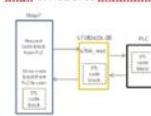
Moyen : saboter le fonctionnement des centrifugeuses d'enrichissement

Cible : atteindre la centrale de **Busher** et les centrifugeuses nucléaires de **Natanz**

Prise en compte de 33 types de convertisseurs de fréquences de 2 fabricants par le protocole **Profibus**



Siemens et PCL avec **7softbox**



13

□ STELAU

DigiNotar – Juillet-Août 2011

Affaire grave ou très grave



<https://docs.google.com/>
Google Documents Photos Site

Page d'accueil



14

Objectif : politico-ideologico-religio...
hacker iranien **ComodoHacker**

Moyen : prise de contrôle totale du HSM de DigiNotar
(autorité de certification reconnue et importante
émettant certains certificats du gouvernement Hollandais)

Cible : le HSM de DigiNotar ? un simple PC hébergeant tous
les systèmes de génération de certificats ... très mal protégé

Conséquences : 500 certificats frauduleux fabriqués et un
certificat *.google.com ayant permis l'espionnage d'utilisateurs
Iraniens du 10 juillet au 29 aout 2011

Correctifs / Réactions : MAJ de tous les navigateurs et OS
+ audits de 54 autorités de certification

□ STELAU

Equation Group and the Shadow Brockers



The first step is executing `bc-genpkt`, which generates an IKE packet of arbitrary size and fills some of it with arbitrary data.

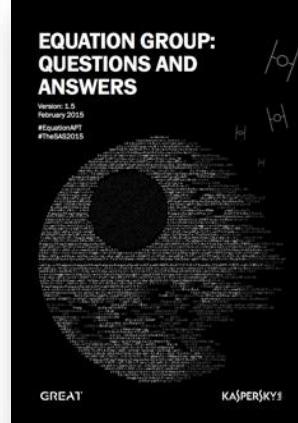
```
Usage: ./bc-genpkt [-h] [-o <file>] [-f <X>] [-r] [-s] [-v[vv]] size
-h help/usage
-o file write data to named file
-f X fill remainder of large packets with character 'X'
-r randomize the initiator cookie
-s randomize the SPI
-v[v] verbosity - show lengths, packet dumps, etc
size size of new packet, should be 96 <= size <= 65536 bytes

Packets larger than 2528 bytes will be filled with random data
unless the -f option is used.
```

This generates a packet file which can be used as input to the binary `bc-id`, which sends the packet to the victim host. Hector Martin notes that it sends a IKE packets with a large Group-Prime option, and speculates that if the victim host is replying using the request length but only filling in the requested 768 bit prime, then it returns a buffer of uninitialized data following it.

```
Usage:
./bc-id -t <dest IP> []
Options:
-t <dest IP>
-l <local port>
-p <remote port>
-I <infile name> [defaults to sendpacket.raw]
-O <outfile name> [defaults to ".raw"]
-f <packetfile name> Reads in packet from a file.
-h print this message
-q quiet mode. Doesn't print hex of response pack
```

The strings in the `bc-id` binary shows that the program seems to patch some memory and look for a start string in the response. However Hector Martin



Outils NSA

quand la NSA perd ses outils

GitHub, Inc. [US] https://github.com/misterch0c/shadowbroker

- EARLYSHOVEL RedHat 7.0 - 7.1 Sendmail 8.11.x exploit
- EBBISLAND (EBBSHAVE) root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (pentium and x86).
- ECHOWRECKER remote Samba 3.0.x Linux exploit.
- EASYBEE appears to be an MDaemon email server vulnerability
- EASYFUN EasyFun 2.2.0 Exploit for WDaemon / IIS MDaemon/WorldClient pre 9.5.6
- EASYPi is an IBM Lotus Notes exploit that gets detected as Stuxnet
- EWOKFRENZY is an exploit for IBM Lotus Domino 6.5.4 & 7.0.2
- EXPLODINGCAN is an IIS 6.0 exploit that creates a remote backdoor
- ETERNALROMANCE is a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 2008 R2, and gives SYSTEM privileges (MS17-010)
- EDUCATEDSCHOLAR is a SMB exploit (MS09-050)
- EMERALDTHREAD is a SMB exploit for Windows XP and Server 2003 (MS10-061)
- EMPHASISMINE is a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2
- ENGLISHMANDENTIST sets Outlook Exchange WebAccess rules to trigger execution to send an email to other users
- EPICHERO 0-day exploit (RCE) for Avaya Call Server
- ERRATICGOPHER is a SMBv1 exploit targeting Windows XP and Server 2003
- ETERNALSYNERGY is a SMBv3 remote code execution flaw for Windows 8 and Server 2012
- ETERNALBLUE is a SMBv2 exploit for Windows 7 SP1 (MS17-010)
- ETERNALCHAMPION is a SMBv1 exploit
- ESKIMOROLL is a Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domains
- ESTEEMAUDIT is an RDP exploit and backdoor for Windows Server 2003
- ECLIPSEDWING is an RCE exploit for the Server service in Windows Server 2008 and 2012
- ETRE is an exploit for iMail 8.10 to 8.22
- ETCETERABLUE is an exploit for iMail 7.04 to 8.05



les Shadow Brokers fournissent la clé PGP

```
msf auxiliary(smb_ms17_010) > options
Module options (auxiliary/scanner/smb/smb_ms17_010):
=====
Name      Current Setting  Required  Description
-----  -----
RHOSTS    192.168.1.177   yes       The target address range or CIDR identifier
REPORT    445              yes       The SMB service port (TCP)
SMBDomain .
SMBPass   .
SMBUser   .
THREADS   1               yes       The number of concurrent threads

msf auxiliary(smb_ms17_010) > exploit
[*] 192.168.1.177:445  - Connected to \\192.168.1.177\IPC$ with TID = 2048
[*] 192.168.1.177:445  - Received STATUS_INSUFF_SERVER_RESOURCES with FID = 0
[!] 192.168.1.177:445  - Host is likely VULNERABLE to MS17-010!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

WannaCry

Mai 2017

ETERNALBLUE

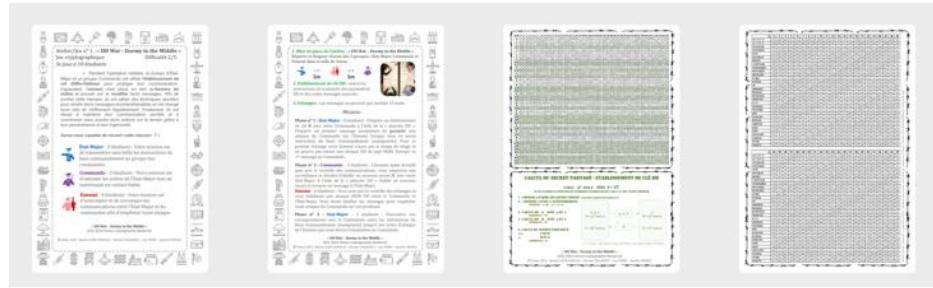
MS17-10



Ateliers/jeux Cryptographie Moderne

<https://github.com/stelaucconseil/EPITA-ELSI>

Atelier 1 : DH War- Ennemy in the Middle



4 groupes
de 10 étudiants

4 groupes
de 5 étudiants

Atelier 2 : Wannacry Nightmare Puzzle



« We kill people based on metadata »



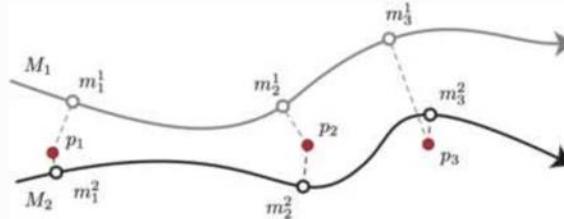
NSA Director Michael Hayden - "We Kill People Based on Metadata"

1,1 k vues • il y a 6 ans

 The Silentist

Published on Apr 7, 2014 The Price of Privacy: Re-Evaluating the NSA, A Debate This year's Presidential

Figure 1



Trajectory-based identification. Two traces M_1 (grey) and M_2 (black) along with a set of three points (red) sampled from M_2 . These points are classified as belonging to M_2 because the average distance to the corresponding nearest points in M_2 is lower than the average distance to the nearest points in M_1 .

ELSI - jeudi matin 09:00-12:00

JEUDI 16 NOVEMBRE 2023

#1 : Hacking - Crypto 101

EPITA - Cours ELSI - ...
09:00
12:00

#2 : Crypto 101 - Signature - IGC

JEUDI 23 NOVEMBRE 2023

EPITA - Cours ELSI - ...
09:00
12:00

#3 : TP noté : OpenSSL + XAdES

JEUDI 30 NOVEMBRE 2023

EPITA - Cours ELSI - ...
09:00
12:00

#4 : Signature - IGC - Certificats

JEUDI 7 DÉCEMBRE 2023

EPITA - Cours ELSI - ...
09:00
12:00

#5 : Loi - Textes - Règlements - Audits

JEUDI 14 DÉCEMBRE 2023

EPITA - Cours ELSI - ...
09:00
12:00

#6 : Révisions + Examen

Les 3 objectifs

- La cryptographie moderne c'est 5 primitives à connaître
 - PRNG
 - DH
 - AES
 - RSA
 - SHA
- Essayer de comprendre l'aspect « révolutionnaire » de la cryptographie **asymétrique**
- En déduire le concept de **signature** cryptographique



Les vraies difficultés de la cryptographie moderne

1. **THEORIE** : Cryptologie

- failles théoriques = **mathématiques**
- cryptologue est un métier

2. **CODE** : Implémentations

- erreurs/failles/vuln. = **informatique**
- « *Do not implement cryptography yourself !* »

3. **UX** : Usages

- mauvais usages = **ignorance/pusillanimité**
- bons usages = **formation**



Poncifs cybersécuritaires

- la faille c'est l'humain ☺
- le filtre d'écran 🧐
- les cookies du RGPD 🍪
- « c'est sécurisé ... » 😎
- « c'est crypté, c'est sécurisé » 😎 😎

STOP SVP



Sondage ?

Chiffrement symétrique



Chiffrement asymétrique



Vocabulaire cryptographique

- Cryptologie - science (λόγος) du secret (κρυπτός) :
 - cryptographie
 - cryptanalyse
- « *Do not implement crypto yourself* »
- Le bureau du chiffre du quai d'Orsay
- « *crypter* » est un néologisme
- Cybersécurité = sécurité informatique = SSI
- SSI : sécurité des systèmes d'information
- C'est *crypté* chiffré donc c'est sécurisé ... ne veut rien dire en SSI.

La cryptologie ne se limite plus aujourd'hui à assurer la confidentialité des secrets



Algo. de chiffrement	Avec Clé	Sans Clé
message clair	chiffrer	<i>crypter</i>
message chiffré	déchiffrer	décrypter

La Cryptographie Moderne

F96D E8C2 27A2 59C8 7EE1 DA2A
ED57 C93F E5DA 36ED 4EC8 7EF2
C63A AE5B 9A7E FFD6 73BE 4ACF
7BE8 923C AB1E CE7A F2DC F7AE
29A3 DA44 **F235** A24C 963F F0DF
3CA3 599A 70E5 DA36 BF1E CE77
F8DC 34BE **129A** 6CF4 D126 BF5B
9A7C FEDF 3EB8 50D3 **7CF0** C63A
A250 9A76 FF92 27A5 5B9A 6FE3
D720

Modern
Cryptography

é c3 a9
f0 9f 94 a5

Cryptographie

F96D E8C2 27A2 59C8 7EE1 DA2A
ED57 C93F E5DA 36ED 4EC8 7EF2
C63A AE5B 9A7E FFD6 73BE 4ACF
7BE8 923C AB1E CE7A F2DC F7AF
29A3 DA44 **F235** A24C 963F F0DF
3CA3 599A 70E5 DA36 BF1E CE77
F8DC 34BE **129A** 6CF4 D126 BF5B
9A7C FEDF 3EB8 50D3 **7CF0** C63A
A250 9A76 FF92 27A5 5B9A 6FE3
D720

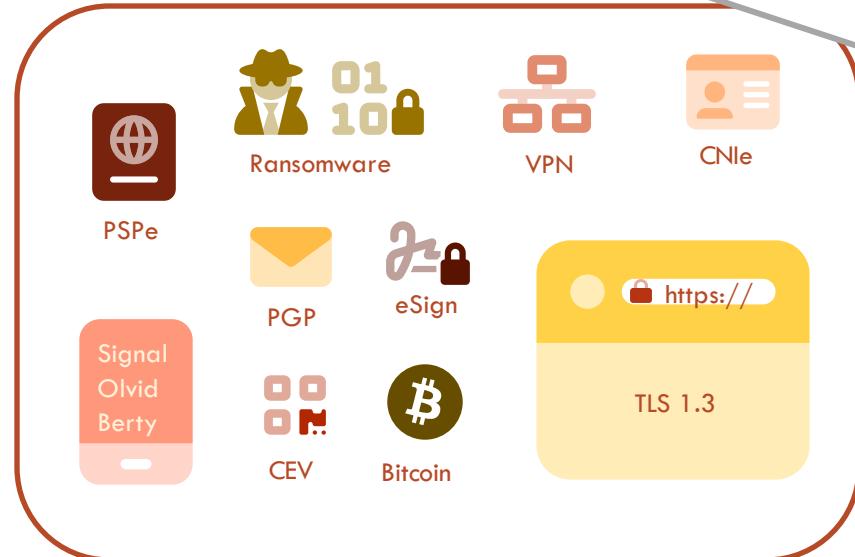
9A 7E
1001 1010 0111 1110
8 bits 8 bits
= =
1 octet 1 octet

Bonjour
42 6f 6e 6a 6f 75 72
01000010 01101111 01101110 01101010 01101111 01110101 01110010

Cryptographie

F96D E8C2 27A2 59C8 7EE1 DA2A
ED57 C93F E5DA 36ED 4EC8 7EF2
C63A AE5B 9A7E FFD6 73BE 4ACF
7BE8 923C AB1E CE7A F2DC F7AE
29A3 DA44 **F235** A24C 963F F0DF
3CA3 599A 70E5 DA36 BF1E CE77
F8DC 34BE **129A** 6CF4 D126 BF5B
9A7C FEDF 3EB8 50D3 **7CF0** C63A
A250 9A76 FF92 27A5 5B9A 6FE3
D720

La cryptographie ne se limite plus aujourd'hui à assurer la confidentialité des secrets



Cryptographie

La cryptographie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets



1. Confidentialité
2. Intégrité
3. Authenticité

4. Disponibilité
5. Originalité
6. Non-réputation

7. Traçabilité
8. Preuve à divulgation nulle (zero-knowledge)

originalité authenticité intégrité confidentialité non réputation traçabilité



✓ ✓ ✓



✓ ✓ ✓



✓ ✓



✓ ✓ ✓



✓ ✓



✓ ✓ ✓



✓ ✓ ✓



✓

Les 5 primitives cryptographiques

Chiffrement Symétrique



Chiffrement Asymétrique



Fonctions de hachage



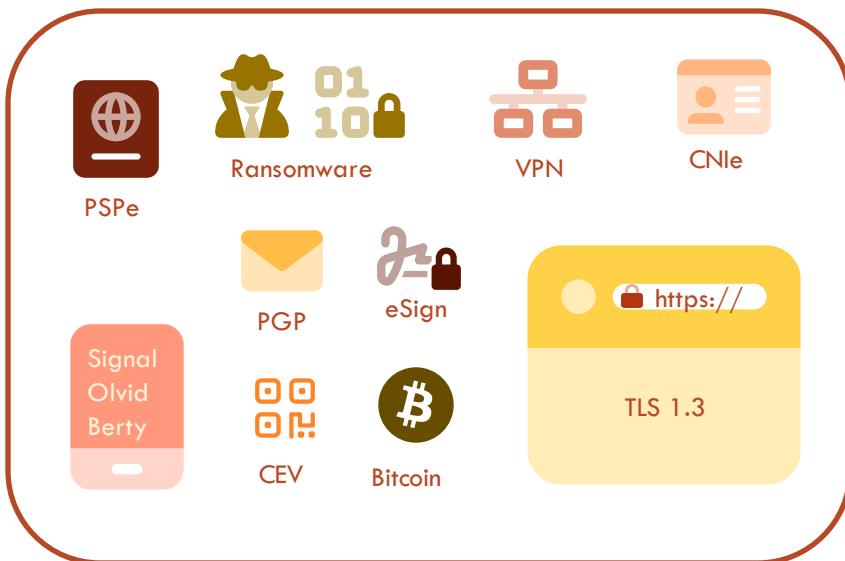
Établissement de clé



Générateurs d'aléa



Cryptographie moderne

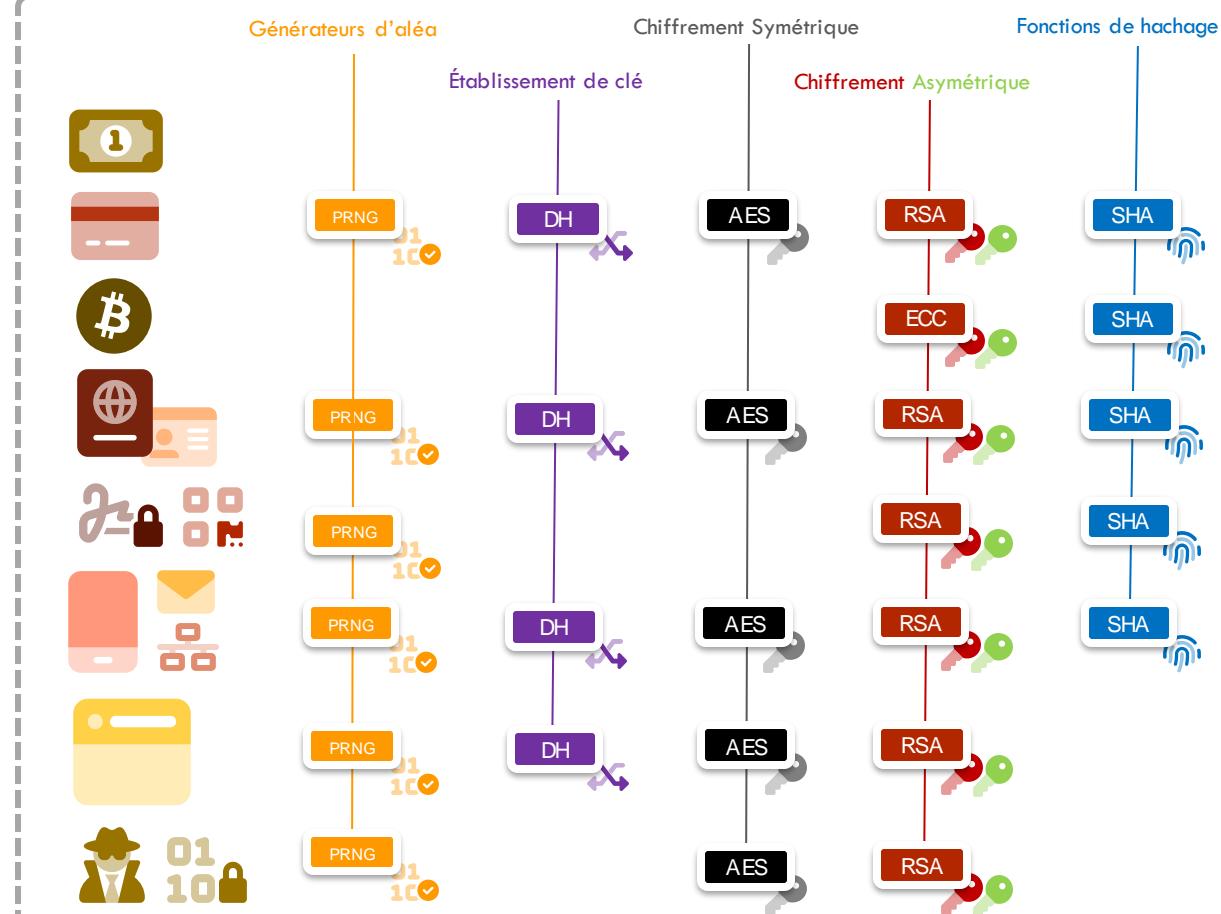


Cryptographie

La cryptographie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets



1. Confidentialité
2. Intégrité
3. Authenticité
4. Disponibilité
5. Originalité
6. Non-répudiation
7. Traçabilité
8. Preuve à divulgation nulle (zero-knowledge)



Les 5 primitives cryptographiques

Chiffrement Symétrique



Chiffrement Asymétrique



Fonctions de hachage



Établissement de clé



Générateurs d'aléa



Hello !

AES



Hello !

SHA



26, 47, 10

DH



91690410bec9
graine

PRNG

11
10 ✓

798

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

+

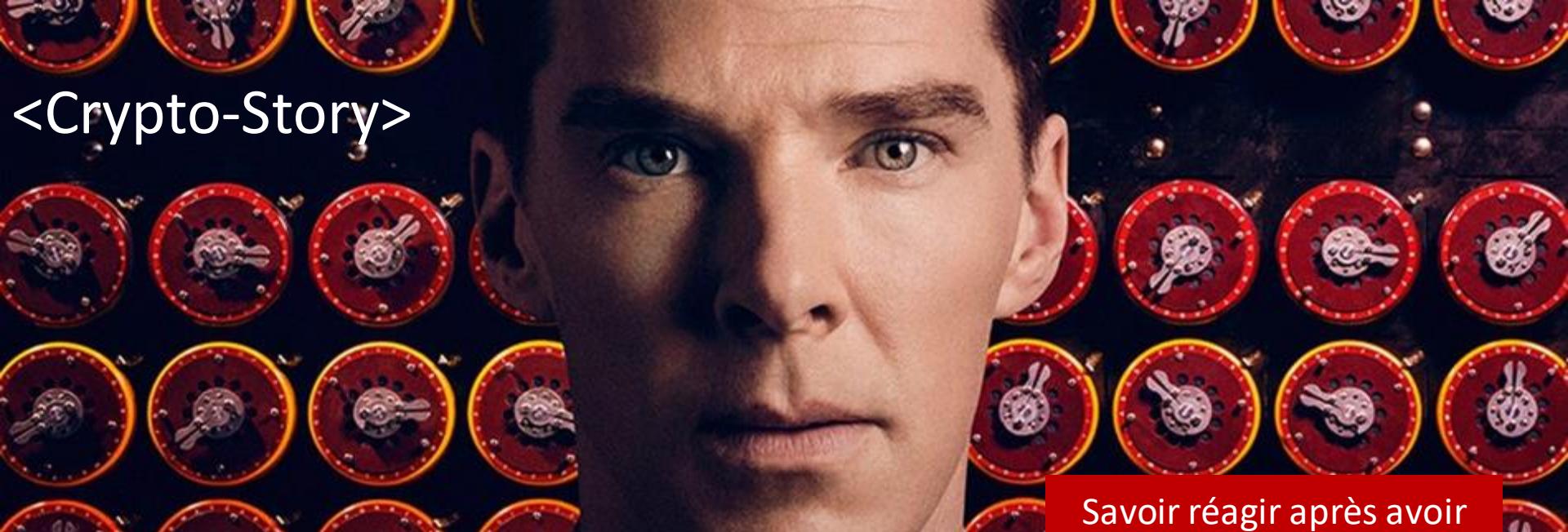
Permet l'usage du
principe de **Signature**

20 ans de crypto. post quantique

révolution ? (ou pas)



<Crypto-Story>



Feindre d'ignorer ce qu'on sait,
de savoir tout ce qu'on ignore, ...
avoir souvent pour grand secret
de cacher qu'il n'y en a point, ...

Beaumarchais - Le Mariage de Figaro (1778)

Savoir réagir après avoir
cassé le code de son
adversaire

Confusion et Diffusion

Substitution et Permutation

Cryptographie Symétrique => Confusion et Diffusion

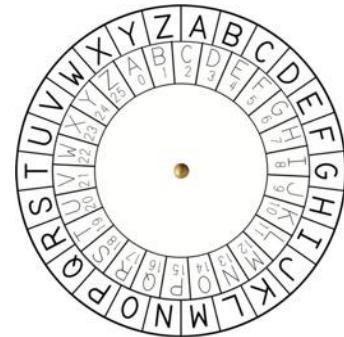
Confusion par Substitution

A → E L → T L → T O → Y ...

Diffusion par Permutation / Transposition

J E S U I S P A S L A => S I U S E J A L S A P

A	E
B	K
C	M
D	F
E	L
F	G
G	D
H	Q
I	V
J	Z
K	N
L	T
M	O
N	W
O	Y
P	H
Q	X
R	U
S	S
T	P
U	A
V	I
W	B
X	R
Y	C
Z	J



Principes de Kerckhoffs - 1883

Crypto symétrique moderne

Auguste Kerckhoffs - 1883

1. Il faut qu'il n'exige **pas le secret**, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.

2. La clef doit pouvoir **en être communiquée** et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.

=> ce qui est gardé secret doit être ce qui est le moins coûteux à changer si le secret s'avérait divulgué

Notion de clé secrète

Algorithme connu de tous :

- Substitution
 - Permutation

mais basées sur la clé secrète

Nulles $\text{ff} = -\infty$ Dowbleth ∞

and for with that if but where as of the from by
2 3 4 4 4 3 7 n M 8 X 0

so not when there this in wic h is what say me my wyrt
x ++ he g x t h m n m m d

send Iſe receave bearer I pray you Mte your name myne

Chiffrement Symétrique

cryptosystème parfait : « incassable »



Le Masque Jetable - One Time Pad

1917

- La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer
- Les caractères composant la clé doivent être choisis de façon aléatoire
- Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois
 - d'où le nom de masque jetable

One-Time Pad

• Plain text: H O W A R E Y O U
7 14 22 0 17 4 24 14 20

+

OTP: 13 2 1 19 25 16 0 17 23
N C B T Z Q A R X

Initial total: 20 16 23 19 42 20 24 31 43

Mod 26: 20 16 23 19 16 20 24 5 17

Ciphertext: U Q X T Q U Y F R

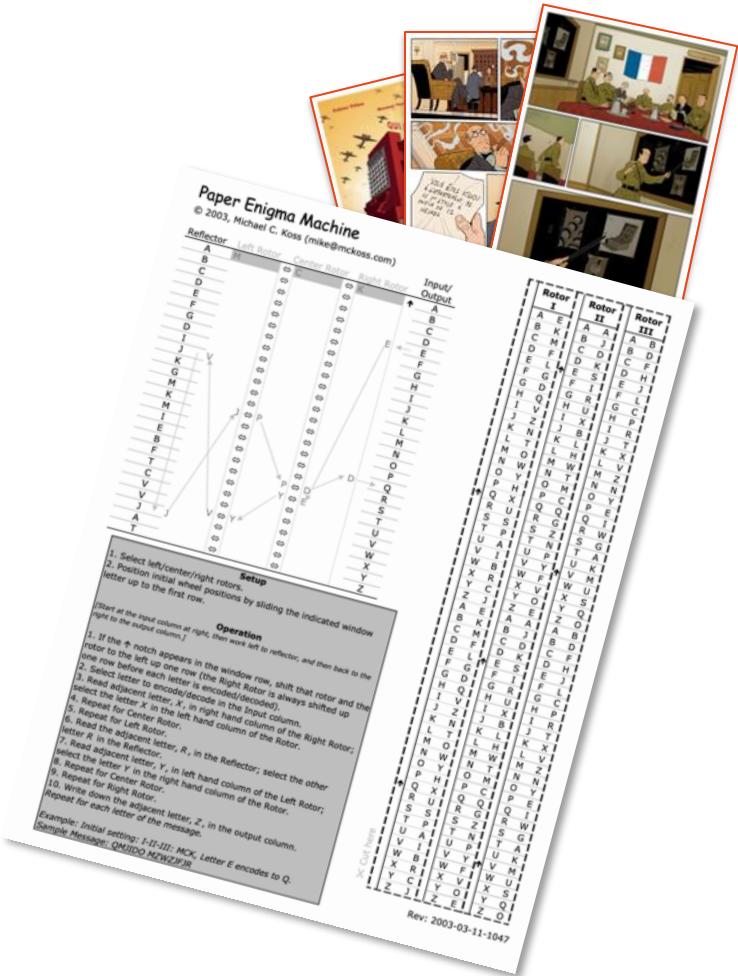
« Qui a cassé Enigma ? »

1932. Dans la salle de bains d'un hôtel bruxellois, un espion français photographie les premiers documents décrivant une nouvelle machine à coder *a priori* inviolable : Enigma. Une machine que s'apprêtent à adopter les services secrets allemands. Quelques mois plus tard, avec l'aide des Français, un groupe de mathématiciens polonais entreprend de percer à jour le fonctionnement complexe de la machine.

1940. Après la défaite française face aux nazis, les Français et les Polonais transmettent leurs trouvailles aux Britanniques. À Bletchley Park se déploie une gigantesque entreprise de décodage dont va dépendre l'issue de la guerre.

1942. Sous le nez des Allemands, à Vichy même, Français et Polonais continuent leurs efforts de décodage. La Gestapo est à leurs trousses et le MI-6 a pour priorité absolue de les exfiltrer. Pendant ce temps dans l'Atlantique, les U-Boote allemands mènent une traque dévastatrice contre les navires américains qui ravitaillent la Grande-Bretagne en armes, vivres et marchandises. Si on ne réussit pas très vite à décoder les messages de la Marine allemande, le Royaume-Uni ne tiendra pas.

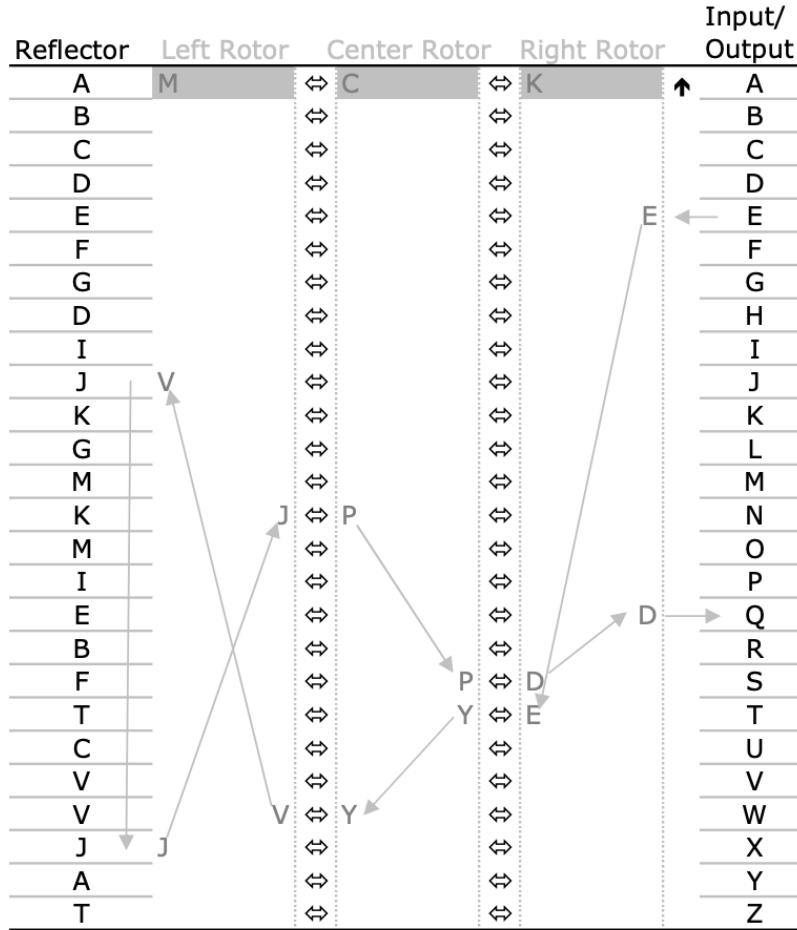
À Bletchley Park, un des cerveaux les plus brillants de l'histoire scientifique, **Alan Turing**, va apporter une contribution décisive...





Paper Enigma Machine

© 2003, Michael C. Koss (mike@mckoss.com)



Rotor I	Rotor II	Rotor III
A E	A A	A B
B K	B J	B D
C M	C D	C F
D F	D K	D H
E L	E S	E J
F G	F I	F L
G D	G R	G C
H Q	H U	H P
I V	I X	I R
J Z	J B	J T
K N	K L	K X
L T	L H	L V
M O	M W	M Z
N W	N T	N N
O Y	O M	O Y
P H	P C	P E
Q X	Q Q	Q I
R U	R G	R W
S S	S Z	S G
T P	T N	T A
U A	U P	U K
V I	V Y	V M
W B	W F	W U
X R	X V	X S
Y C	Y O	Y Q
Z J	Z E	Z O
A E	A A	A B
B K	B J	B D
C M	C D	C F



Very Short Crypto Story

3000 ans de crypto. symétrique

*recettes militaro-diplomatiques
de confusion et de diffusion*

100 ans de crypto. moderne

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

50 ans de crypto. asymétrique

LA véritable révolution



DH

1976



RSA

1977

20 ans de crypto. quantique

révolution ? (ou pas)



https://fr.wikipedia.org/wiki/Histoire_de_la_cryptographie

Les dates clefs de la cryptographie

Hachage

Hachage cryptographique

SHA



Secure
Hash
Algorithm



Alice



Une fonction de hachage cryptographique est une fonction sans clé qui permet de transformer une donnée de taille arbitraire en une chaîne de bits de taille h fixe, appelée haché.

SHA



empreinte cryptographique

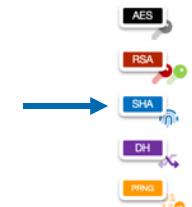
1. Confidentialité
2. Intégrité
 - Très rapide
 - Gros volume
3. Authenticté
4. Disponibilité
5. Originalité
6. Non répudiation
7. Traçabilité

R3

Fonctions de hachage

Les fonctions de hachage de la famille SHA-2 [FIPS180] et de la famille SHA-3 [FIPS202] dont la taille de sortie est supérieure ou égale à 256 bits sont recommandées.

Primitive	Taille de paramètre	R/O	Notes
SHA-2 [FIPS180, ISO10118-3]	$h = 256$ bits (SHA-256)	R	
	$h = 384$ bits (SHA-384)	R	
	$h = 512$ bits (SHA-512)	R	
	$h = 256$ bits (SHA-512/256)	R	
SHA-3 [FIPS202]	$h = 256$ bits	R	
	$h = 384$ bits	R	
	$h = 512$ bits	R	



1. BLAKE
2. RIPEMD
3. WHIRLPOOL

Hachage

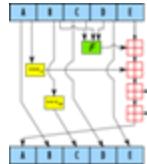
Hachage cryptographique

SHA



Secure
Hash
Algorithm

```
SHA1-compress(H, M) {
    (a0, b0, c0, d0, e0) = H    // parsing H as five 32-bit big endian words
    (a, b, c, d, e) = SHA1-blockcipher(a0, b0, c0, d0, e0, M)
    return (a + a0, b + b0, c + c0, d + d0, e + e0)
}
```



```
SHA1-blockcipher(a, b, c, d, e, M) {
    W = expand(M)
    for i = 0 to 79 {
        new = (a <<< 5) + f(i, b, c, d) + e + K[i] + W[i]
        (a, b, c, d, e) = (new, a, b >>> 2, c, d)
    }
    return (a, b, c, d, e)
}
```

```
expand(M) {
    // the 512-bit M is seen as an array of sixteen 32-bit words
    W = empty array of eighty 32-bit words
    for i = 0 to 79 {
        if i < 16 then W[i] = M[i]
        else
            W[i] = (W[i - 3] ⊕ W[i - 8] ⊕ W[i - 14] ⊕ W[i - 16]) <<< 1
    }
    return W
}
```

```
f(i, b, c, d) {
    if i < 20 then return ((b & c) ⊕ (~b & d))
    if i < 40 then return (b ⊕ c ⊕ d)
    if i < 60 then return ((b & c) ⊕ (b & d) ⊕ (c & d))
    if i < 80 then return (b ⊕ c ⊕ d)
}
```

b1e9feb2d6015f3fa4bfac79788cb21f03560984

SHA1



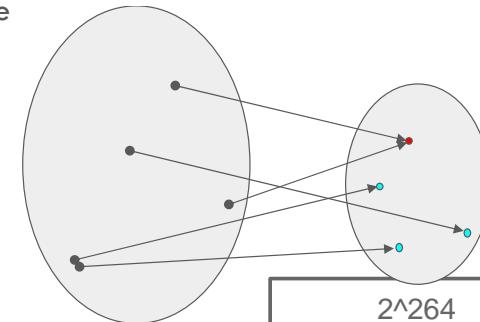
- Fonctions à sens unique

d'un espace infini vers un espace fini
de :

128, 160, 224, 256 ou 512 bits

- Résistantes aux attaques

- 1^{ère} pré-image
- 2^{de} pré-image
- collisions



2^{264}
 $2^{(80*3,3)}$

10^{80}

nb. atomes univers

Hachage

Hachage cryptographique

SHA



Secure
Hash
Algorithm

SHA256

f9dcc621fcb8ac6a172c40fd3ffcbfcf20fa400e3b216d3777362ee7c22965ea

SHA256("Guess #0") =
1101000101011001000101011010001
0111100101100000011100100000111
11101100101001100101110111101100
0001001110100011101111000101011
10000001001111000011001100100111
10001101011011101001000110000101
1110101111101011000101011011000
100011101000000110000110100000000

Hachage

Hachage cryptographique

SHA
Secure
Hash
Algorithm

La cryptographie moderne est une branche de la cryptologie qui utilise des algorithmes mathématiques pour protéger et sécuriser les informations. Elle est devenue essentielle dans le monde numérique pour garantir la confidentialité, l'intégrité et l'authenticité des données échangées. Les principaux objectifs de la cryptographie moderne sont de garantir la confidentialité, l'authenticité et l'intégrité des données. Elle est utilisée dans de nombreux domaines tels que les transactions financières, la communication en ligne, la sécurité des réseaux informatiques, et la protection des données personnelles.



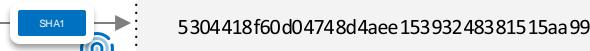
Benoit LEGER-DERVILLE

12 mars 1974

5 rue de la Villa
65432 Bourg-la-Ville



ba81264aba b6e296cc48838ebb9df78db1970267



5304418f60d04748d4aee15393248381515aa993

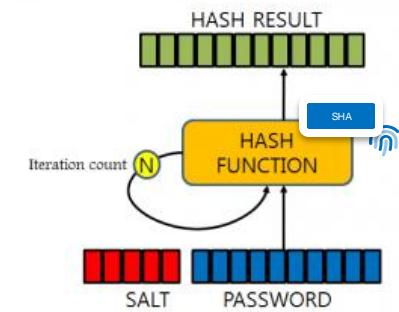
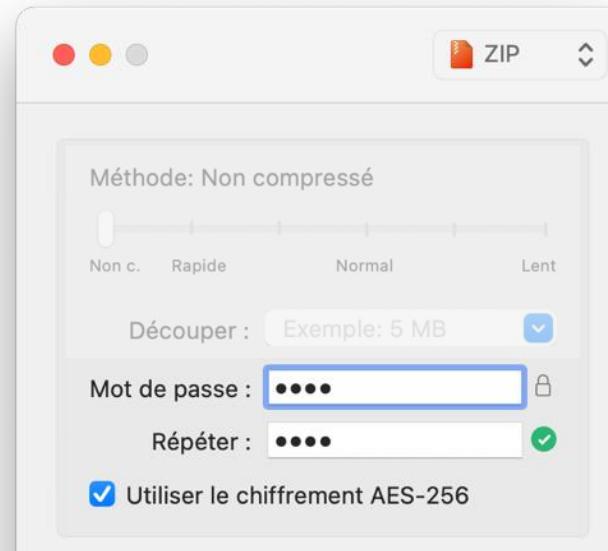


194a0023224bf8db193346aa8b09cdfc0689f1fd

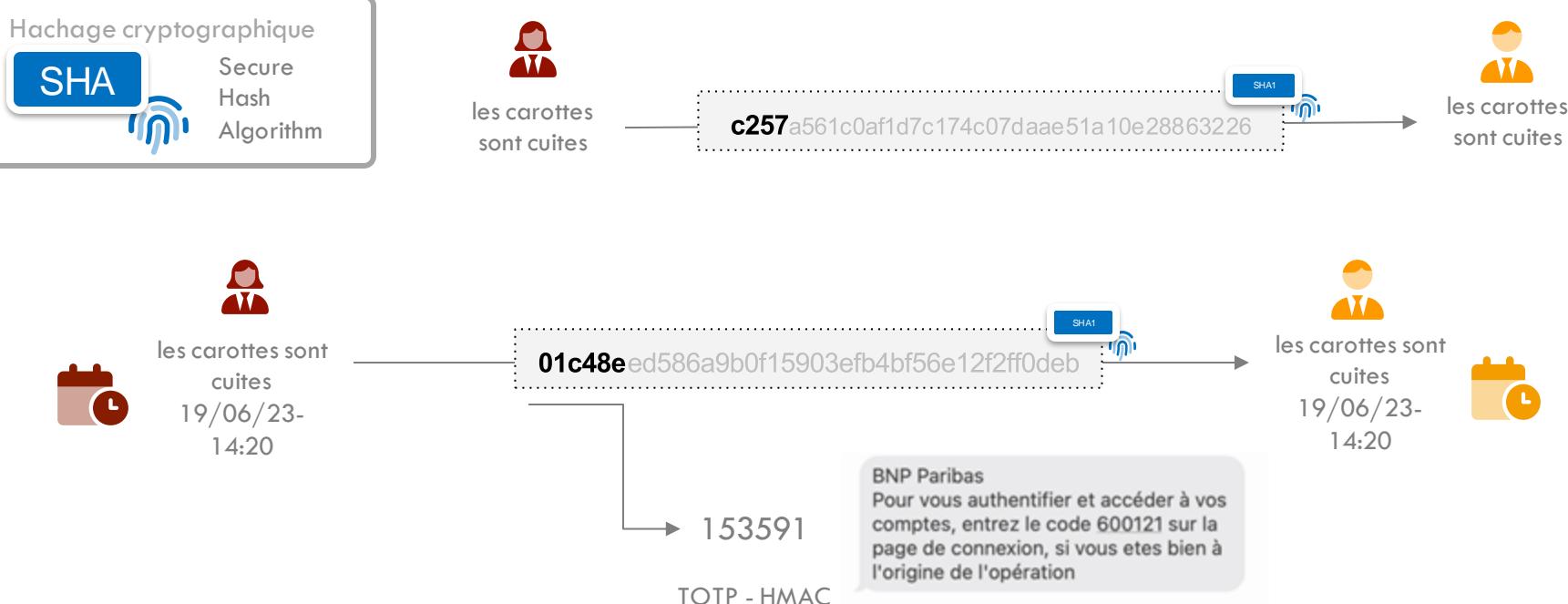
Hachage

Hachage cryptographique
SHA
Secure
Hash
Algorithm

P@55w0rD/2023 → SHA → 6967e32dfaafdde85d7d40db50cd906c9200caeef



Hachage



Hachage

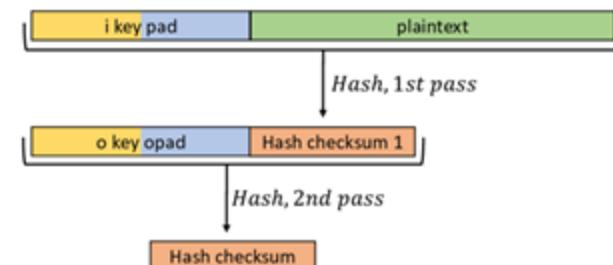
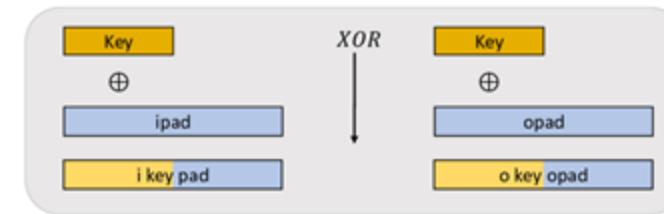
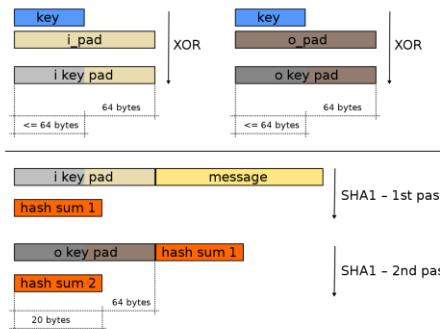
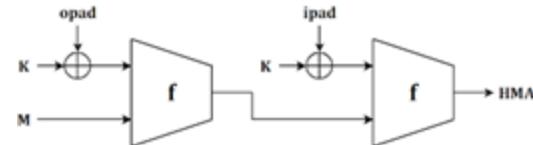
Hachage cryptographique

SHA



Secure
Hash
Algorithm

$$\text{HMAC}_K(m) = h\left((K \oplus opad) \parallel h\left((K \oplus ipad) \parallel m\right)\right)$$



Construction du HMAC

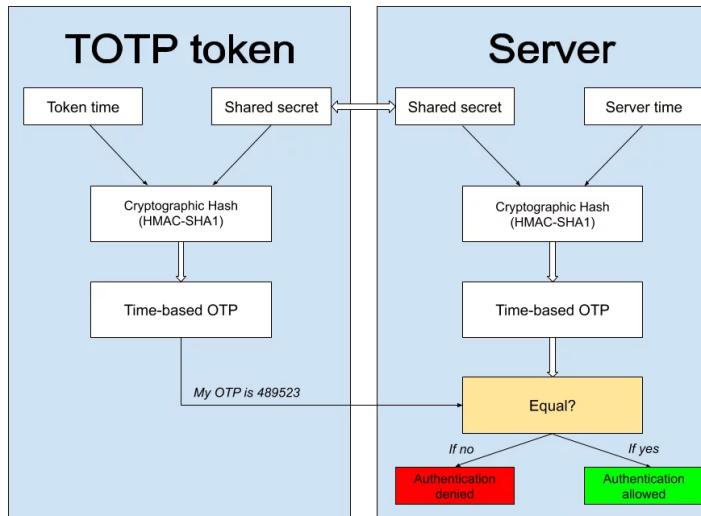
Construction Hachage Crypto: TOTP

Hachage cryptographique

SHA



Secure
Hash
Algorithm



5.4. Example of HOTP Computation for Digit = 6

The following code example describes the extraction of a dynamic binary code given that `hmac_result` is a byte array with the HMAC-SHA-1 result:

```

int offset  = hmac_result[19] & 0xf ;
int bin_code = (hmac_result[offset]  & 0x7f) << 24
| (hmac_result[offset+1] & 0xff) << 16
| (hmac_result[offset+2] & 0xff) << 8
| (hmac_result[offset+3] & 0xff) ;
  
```

SHA-1 HMAC Bytes (Example)

Byte Number	
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19	
Byte Value	
1f 86 98 69 0e 02 ca 16 61 85 50 ef 7f 19 da 8e 94 5b 55 5a	***** -----++

M'Raihi, et al.

Informational

[Page 7]

RFC 4226

HOTP Algorithm

December 2005

- * The last byte (byte 19) has the hex value 0x5a.
- * The value of the lower 4 bits is 0xa (the offset value).
- * The offset value is byte 10 (0xa).
- * The value of the 4 bytes starting at byte 10 is 0x50ef7f19, which is the dynamic binary code DBC1.
- * The MSB of DBC1 is 0x50 so DBC2 = DBC1 = 0x50ef7f19 .
- * HOTP = DBC2 modulo 10^6 = 872921.

We treat the dynamic binary code as a 31-bit, unsigned, big-endian integer; the first byte is masked with a 0x7f.

We then take this number modulo 1,000,000 (10^6) to generate the 6-digit HOTP value 872921 decimal.

Hachage

Hachage cryptographique

SHA



Secure
Hash
Algorithm

Ce que n'est pas un HMAC

	Hash	MAC	Digital signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudiation	No	No	Yes
Kind of keys	None	Symmetric	Asymmetric

Intégrité : Le destinataire peut-il être sûr que le message n'a pas été modifié accidentellement ?

Authentification : Le destinataire peut-il être sûr que le message provient de l'expéditeur ?

Non-répudiation : Si le destinataire transmet le message et la preuve à une tierce partie, cette dernière peut-elle être certaine que le message provient de l'expéditeur ?

Pour les signatures un vérificateur doit être sûr que la clé de vérification appartient réellement au signataire.

Pour les MAC, un destinataire doit être sûr que la clé symétrique partagée n'a été partagée qu'avec l'expéditeur.

Hachage

Hachage cryptographique

SHA

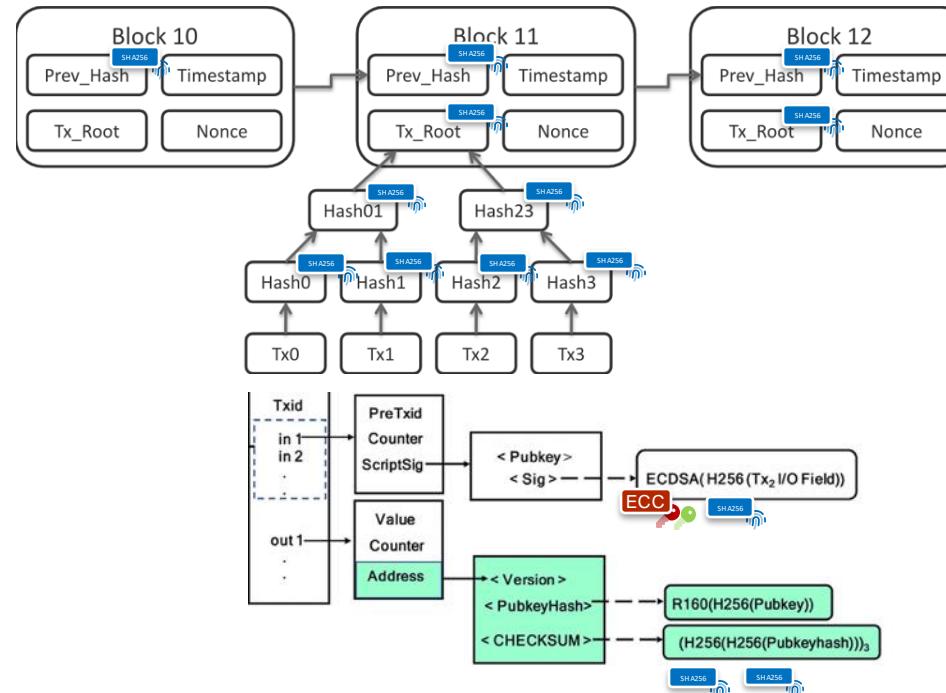


Secure
Hash
Algorithm

SHA256

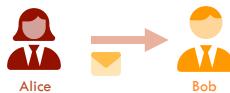


f9dcc621fcb8ac6a172c40fd3ffcbfcf20fa400e3b216d377736ee7c22965ea

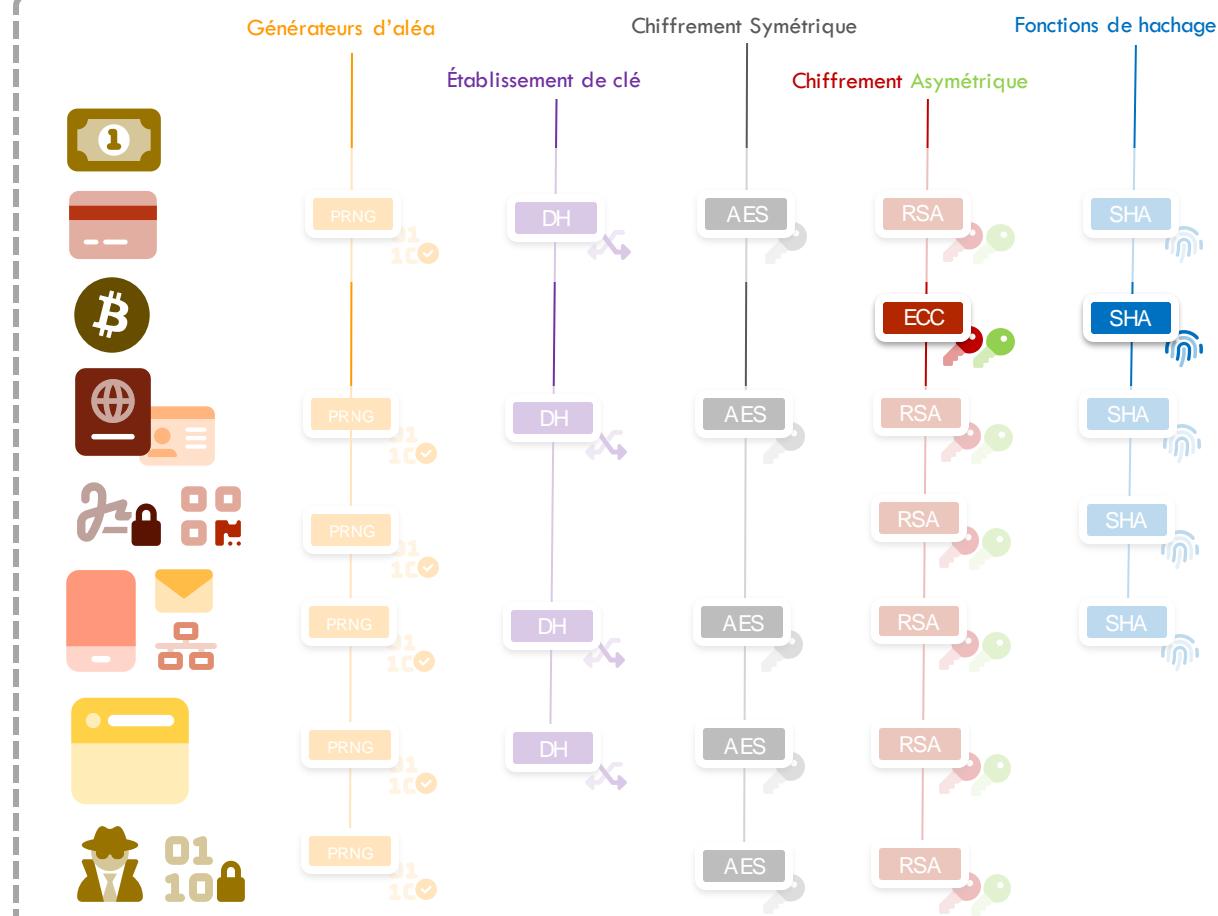


Cryptographie

La cryptographie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets



1. Confidentialité
2. Intégrité
3. Authenticité
4. Disponibilité
5. Originalité
6. Non-répudiation
7. Traçabilité
8. Preuve à divulgation nulle (zero-knowledge)



Génération d'Aléa

Pseudo Aléatoire

PRNG



Pseudo
Random
Number
Generator



Alice

s



1. Confidentialité
2. Intégrité
3. Authenticité
4. Disponibilité
5. Originalité
6. Non-répudiation
7. Traçabilité

91690410bec9
graine

PRNG



798

aléa

Une source d'aléa est un processus probabiliste duquel on peut extraire une séquence de bits aléatoires. Il est difficile de s'assurer de la qualité des sorties d'une source d'aléa.

Deux approches : 1. Réaliser des tests statistiques sur les sorties de la source ;
2. Modéliser le processus stochastique de la source.

R23

Générateur d'aléa déterministe

HMAC-DRBG, Hash-DRBG et CTR-DRBG [FIPS197, ISO18033-3] sont recommandés.

Schéma	R/O	Notes
HMAC-DRBG [SP800-90A, ISO18031]	R	
Hash-DRBG [SP800-90A, ISO18031]	R	
CTR-DRBG [SP800-90A, ISO18031]	R	

AES

RSA

SHA

DH

PRNG



1. Test de primalité : Miller-Rabin
2. RSA : $|p - q| \geq 2^{n/2 - 100}$

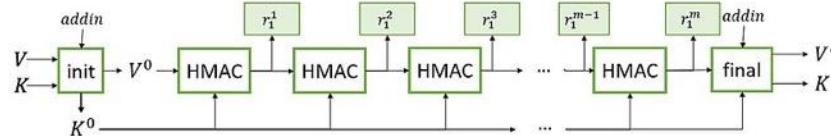
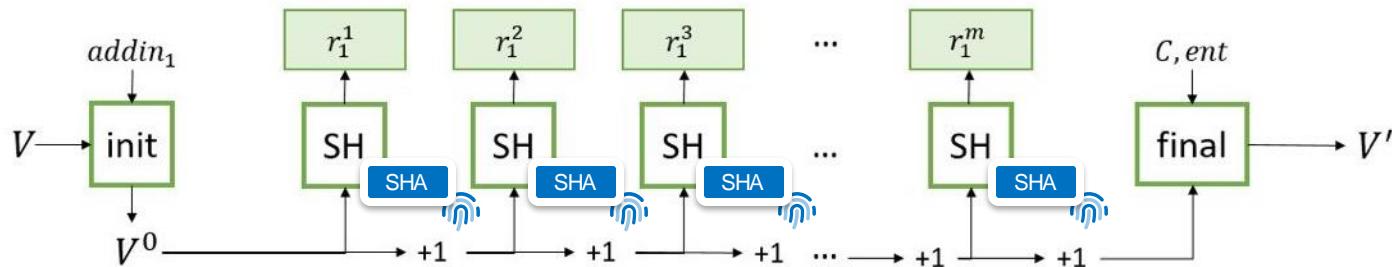
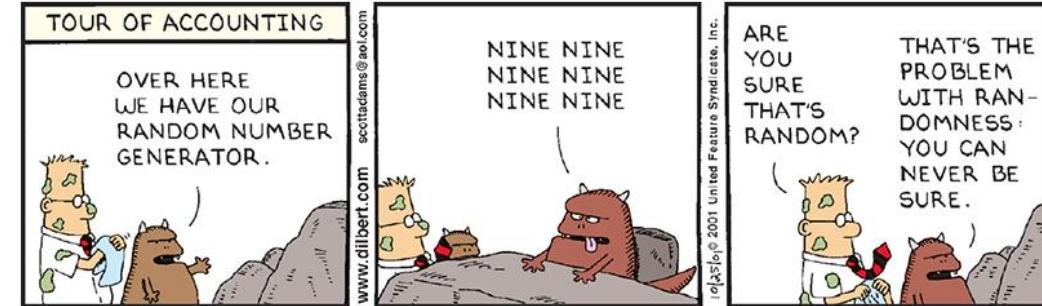
Génération d'Aléa

Pseudo Aléatoire

PRNG

01
10

Pseudo
Random
Number
Generator

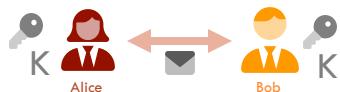


Symétrique

Chiffrement Symétrique

AES

Advanced
Encryption
Standard



1. Confidentialité
 - Très rapide
 - Gros volume
2. Intégrité
3. Authenticté
4. Disponibilité
5. Originalité
6. Non-répudiation
7. Traçabilité

Hello !

AES



K



Un mécanisme de chiffrement symétrique permet, à l'aide d'une clé secrète K, de transformer un message clair M en un message chiffré C

R1

Algorithmes de chiffrement par bloc

AES [FIPS197, ISO18033-3] est recommandé pour ses trois tailles de clés (128, 192 et 256 bits).

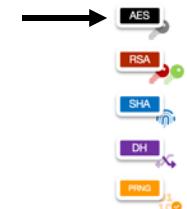
Primitive	Taille de clé	Taille de bloc	R/O	Notes
AES [FIPS197, ISO18033-3]	k = 128 bits	n = 128 bits	R	
	k = 192 bits		R	
	k = 256 bits		R	
Triple-DES [SP800-67, ISO18033-3]	k = 112 bits	n = 64 bits	O	3.1.a, 3.1.b
	k = 168 bits		O	3.1.b

R2

Algorithmes de chiffrement par flot

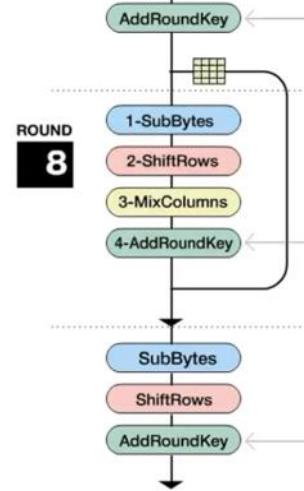
L'algorithme de chiffrement par flot ChaCha20 [RFC8439] est recommandé.

Primitive	R/O	Notes
ChaCha20 [RFC8439]	R	



1. AES
2. Blowfish
3. DES
4. 3DES
5. IDEA
6. RC4
7. RC5
8. Serpent
9. Twofish

Symétrique



Symétrique

Chiffrement Symétrique

AES



Advanced
Encryption
Standard

Qui écoute la planète ?

Les USA



Rijndael

Joan Daemen et Vincent Rijmen

Les Chinois



Keccak

Les Belges



Etablissement de clé

Partage de secret

DH

Diffie
Hellman



1. Confidentialité
 - Rapide
 - vuln. MitM
2. Intégrité
3. Authenticité
4. Disponibilité
5. Originalité
6. Non-répudiation
7. Traçabilité

26, 47, 10

DH



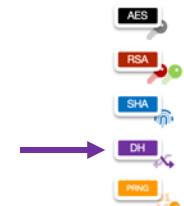
Un mécanisme d'établissement de clé permet à deux entités (ou plus) de se mettre d'accord sur une valeur de clé secrète.

R22

Mécanismes d'établissement de clé

Les mécanismes d'établissement de clé DH et EC-DH sont recommandés.

Primitive	Mécanisme	R/O	Notes
FF-DLOG	DH [SP800-56A, ISO11770-3]	R	6.4.a
EC-DLOG	EC-DH [SP800-56A, ISO11770-3]	R	6.4.a



1. ECDH

Discrete Log Problem

$$2^n = 16$$

$$2^n \bmod 17 = 16$$

Partage de secret

DH



Diffie
Hellman

Alice

$$A = g^a \bmod p$$

$$K = B^a \bmod p$$

$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p =$$

$$3 \bmod 17 \equiv$$

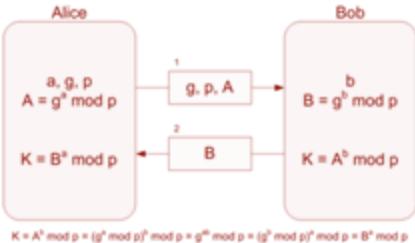
Etablissement de clé

Partage de secret

DH



Diffie
Hellman



1. Confidentialité
2. Attaque MitM
Man in the Middle
3. Intégrité
4. Authenticité
5. Disponibilité
6. Originalité
7. Non-répudiation
8. Traçabilité

G:	11124136727432308918812736531716408346878332998901256519320663274861933580804712151 00797237775771467149894260123512660136402158406998369481252844452718796		
N:	77818714124031252720819944202374984988485179601906368139945936248931661607804455138 87821412313009361625936687452586174696909303141691170346568788390764347		
Next Bob and Alice will generate two random numbers (X and Y), calculate an X value and a Y value, respectively:			
Bob's X Value	39	Alice's Y value	86
	Bob's random value		Alice's random value
Bob's A value	156437054090510643708213487397359650 653706600103085237076814872023455692 501938943883924390306994339326651518 339656294271164634334019120166300414 0138530961	Alice's B value	867562183713756921586080163515215184 994404228948268998120566392949664779 371069184674731003959263884633988486 672884899488683959430851633340784964 621708228
	A=G^x mod N		B=G^y mod N
and Bob will send his A value to Alice, and Alice will send her B value to Bob, and they now re-calculate the values to generate the same shared key :			
Bob's Key	8444217310575129445600473794887733095 7898956649193468344758061625930880277 3327317656211099035659946951701937245 2044286993289357313115568251376348740 50285	Alice's Key	8444217310575129445600473794887733095 7898956649193468344758061625930880277 3327317656211099035659946951701937245 2044286993289357313115568251376348740 50285
	Key=B^x mod N		Key=A^y mod N

Etablissement de clé

Partage de secret

DH

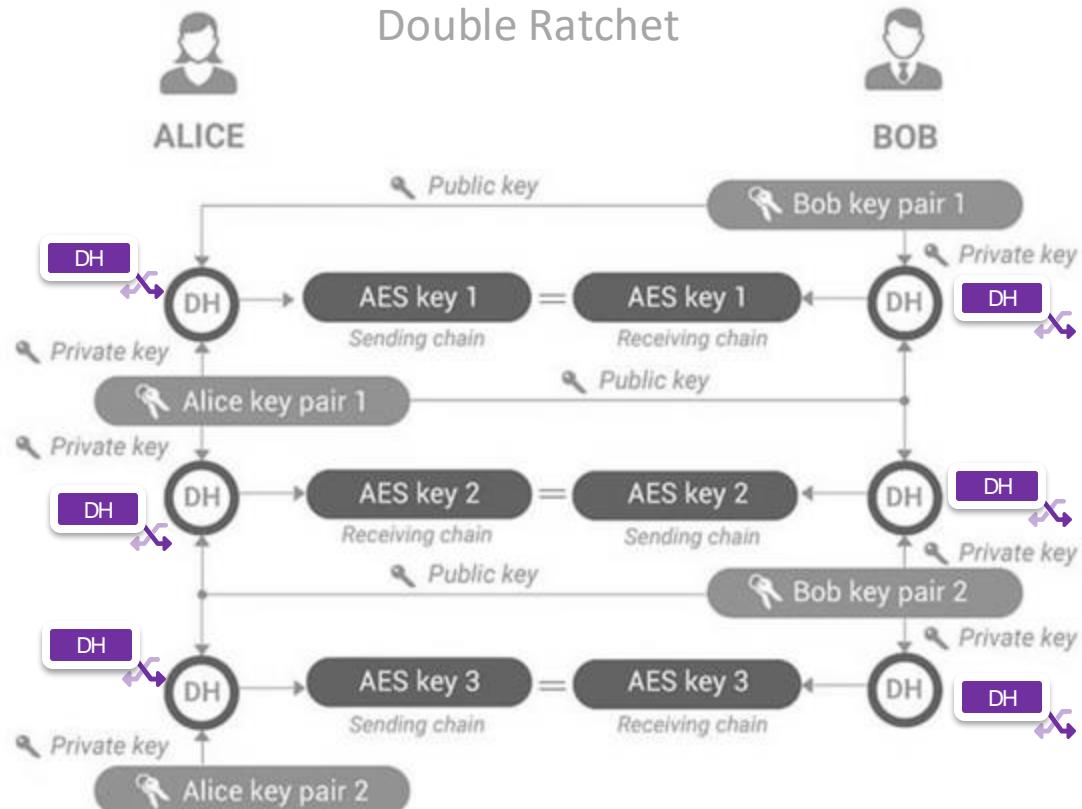


Diffie
Hellman



- **Symmetric end-to-end encryption.** Message decrypted on all recipients' ends with the same exchange.
- **Forward secrecy.** Unique ephemeral keys are compromised, all your other messages remain therefore safe.
- **Independent key renewal.** The algorithm does not get new keys. It uses key derivation function
- **Plausible deniability.** If a message gets intercepted, who has sent it.
- **No lost or out-of-order messages.** Each message has a header. This way, if a message gets lost or is delayed.

Double Ratchet



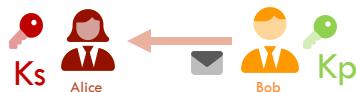
Asymétrique

Chiffrement Asymétrique

RSA



Rivest
Shamir
Adleman



le secret

RSA

M



RSA

C



M

L'opération publique de chiffrement transforme à l'aide de la clé publique K_p un message clair M en un message chiffré C . L'opération privée de déchiffrement permet de recalculer M à partir de C et de la clé privée K_s . Le chiffrement asymétrique permet donc à toute personne ayant accès à la clé publique de chiffrer des messages à l'intention du détenteur de la clé privée.

1. Confidentialité
 - Lent
 - Petit volume

2. Intégrité

3. Authenticité

4. Disponibilité

5. Originalité

6. Non-réputation

7. Traçabilité

R18

Paramètres de courbes elliptiques pour le DLOG

Les paramètres de courbes elliptiques P256r1, P384r1 et P512r1 de la pool, les paramètres de courbes elliptiques P-256, P-384 et P-521 du paramètres de courbes Curve25519 et Curve448 sont recommandés.

Familles de courbes	Courbes	R/O	Notes
Brainpool [RFC5639]	BrainpoolP256r1	R	
	BrainpoolP384r1	R	5.3.a
	BrainpoolP512r1	R	
NIST [FIPS186] (voir Annexe D.1.2)	NIST P-256	R	
	NIST P-384	R	5.3.a
	NIST P-521	R	
IETF [RFC7748]	Curve25519	R	
	Curve448	R	5.3.b

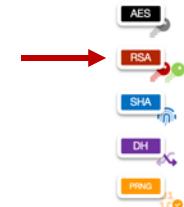
R16

Dimensionnement du schéma asymétrique RSA

On recommande d'utiliser des modules RSA d'au moins 3072 bits publics e de taille strictement supérieure à 2^{16} .

Primitive	Taille des paramètres	R/O	Notes
RSA	$n \geq 3072, \log_2(e) > 16$	R	
	$n \geq 2048, \log_2(e) > 16$	O	

1. ECC
2. Post Quantique
 - FALCON
 - SPHINCS+
 - CRYSTALS-KYBER
 - CRYSTALS-DILITHIUM



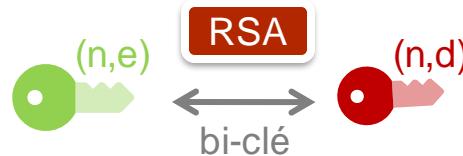
Asymétrique

Chiffrement Asymétrique

RSA



Rivest
Shamir
Adleman



$$C \equiv M^e \pmod{n}$$

$$M \equiv C^d \pmod{n}$$

p et q premiers

$$n=p \cdot q$$

$$\phi(n) = (p - 1)(q - 1)$$

e premier avec $\phi(n)$

d inverse de e modulo $\phi(n)$

- Comme $c = m^e \pmod{n}$, $c^d \pmod{n} = m^{ed} \pmod{n}$
- Comme $ed = 1 \pmod{(p-1)(q-1)}$ il existe un entier k tel que $ed = 1 + k(p-1)(q-1)$
- Par conséquent $c^d \pmod{n} = m^{1+k(p-1)(q-1)} \pmod{n}$
- Or (théorème de Fermat) $m^{(p-1)} \pmod{p} = 1$ si m n'est pas multiple de p . Par élévation à la puissance $k(q-1)$ puis multiplication par m on obtient : $m^{1+k(p-1)(q-1)} \pmod{p} = m$ égalité qui reste vraie (2 membres=0) si m est multiple de p
- Par symétrie $m^{1+k(p-1)(q-1)} \pmod{q} = m$ donc $m^{1+k(p-1)(q-1)} - m$ est divisible par p et q donc par pq (p et q premiers et différents)
- Par conséquent $c^d \pmod{n} = m^{1+k(p-1)(q-1)} \pmod{pq} = m$

Asymétrique

Chiffrement Asymétrique

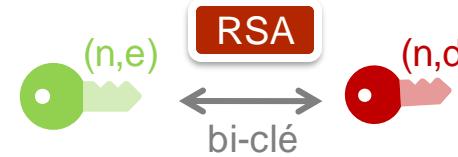
RSA



Rivest
Shamir
Adleman

$$C \equiv M^e \pmod{n}$$

$$M \equiv C^d \pmod{n}$$



Message=hello

p=1780731609485571264810668272791995899914711193175875151378804
074228378407969900390762278303079206056838884626265923868792218
367632557891163061154753567325103171346019724100725958290999956
638624959629388394207924641815440071623570127595625788276627675
2937990502678061624633628703093952827543039555774118880861

q=1659131989902429311320647733356628360786681694637180433412560
894004052610620886878487919454167845518159615723611150571927731
077520725426964037514349809386962699556220313541603209708580761
255180830815503806133227993555854257708408662876270644910978887
84189682166960030796126554428589177031865285035399557919043

e=65537

d=7541588446120496966253234620344712333501069795303049916555478
181024739612748768714849307670020087520498050753853969336769842
721963177053759904513002332911786096655412117391051494984460634
179886021618010916184586203664729878176106218580539243017832573
064752374135639173722301872742910212929520185645517211756292260
442337408227686415915940057868098542605732388150060822257263017
768153073048470043906529305219251168471687810973059378400133633
64431841434819869871137449204223710920038333030466757157771841
088217670969580298385949540902819878485019509485570883603413467
234108699097821896589722966999532605527832607563513

p et q premiers

n=p.q

$\phi(n) = (p - 1)(q - 1)$

e premier avec $\phi(n)$

d inverse de e modulo $\phi(n)$

N=2954468778727951519381542455099117772733932758531747159909715903
818628489453739346434808277662182293208684035240167304823272057321
422288076172288054479598539813596184732724354963397672285147033236
886721151377782449815143774439760136571897904056785781223890706818
86176417142983940340406627783874748342767092341923727807298159971
873503674156291633101481940976644619125965267514073300546813320042
580729928081378915771201586619482771747482544538290338600642244942
010670574478156402877487966789398331122247930143951606695548203913
045284760438130510844259880483102317018508493449083312299070937455
1035113290128717200136023

Public key (e,n) Private key (d,n)

cipher=273743492279956537274854241317285273489687949926990383595577
818303469365389369383595210177750765405360365710781579824329830305
899759170691700224655572029292953466922904049974236228138933712837
677798511174101407776261740120993841843494109034252357715708754150
858729358036738829777908947650774051399543308967832986991616410972
346874156044067581889268723764995402779650371468342794857706752356
242882149636133999260072349301958518578960262847313752426012359065
189237744326344835963663284896710050292993953459275970081116400819
06499050426803485874451895899128806555366663122851343001665872030
55372566737379510918409870253

Decipher=hello

Les 5 primitives cryptographiques

Chiffrement Symétrique



Chiffrement Asymétrique



Fonctions de hachage



Établissement de clé

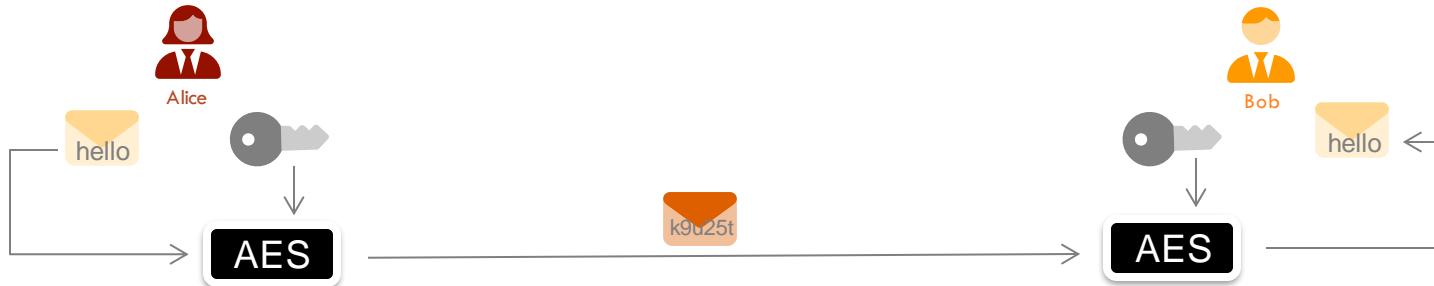


Générateurs d'aléa



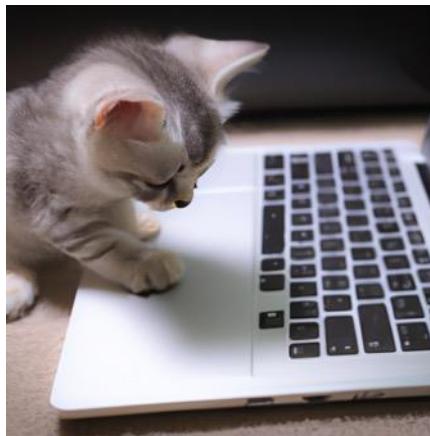
Chiffrement symétrique

AES



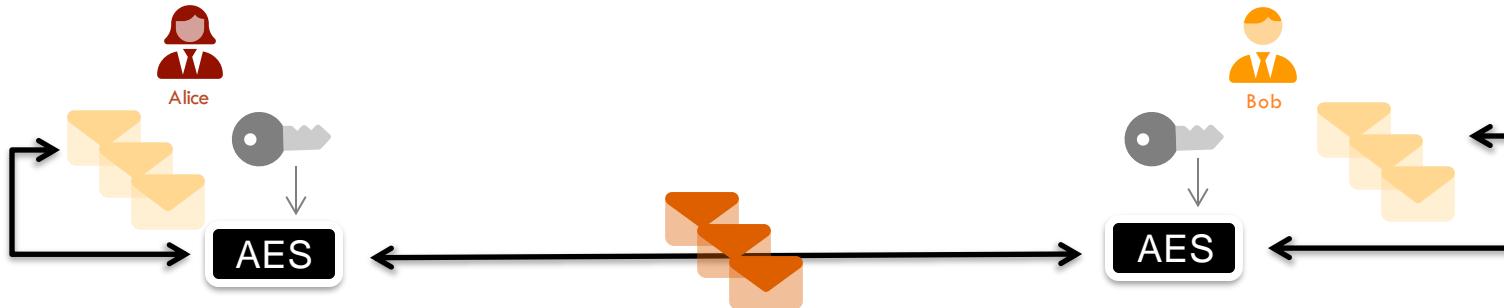
Chiffrement symétrique

AES



Chiffrement symétrique

AES

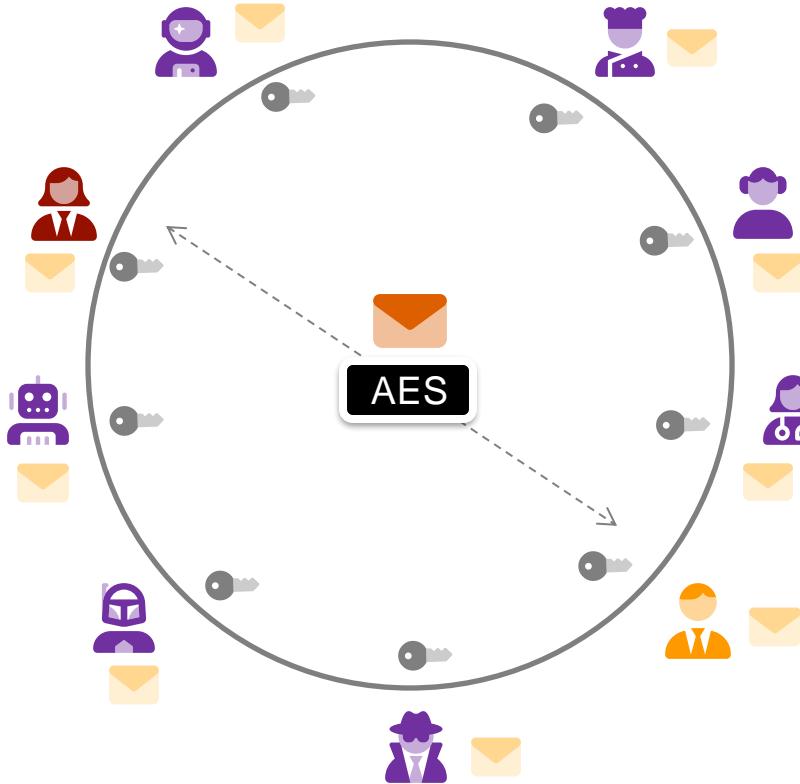


- rapide et optimisé
- chiffrement de larges volumes
- usage simple et direct (dans les 2 sens : A<=>B)
- d'où vient cette unique clé symétrique ?
- établissement de la clé
- partage/échange de la clé

Chiffrement symétrique

AES

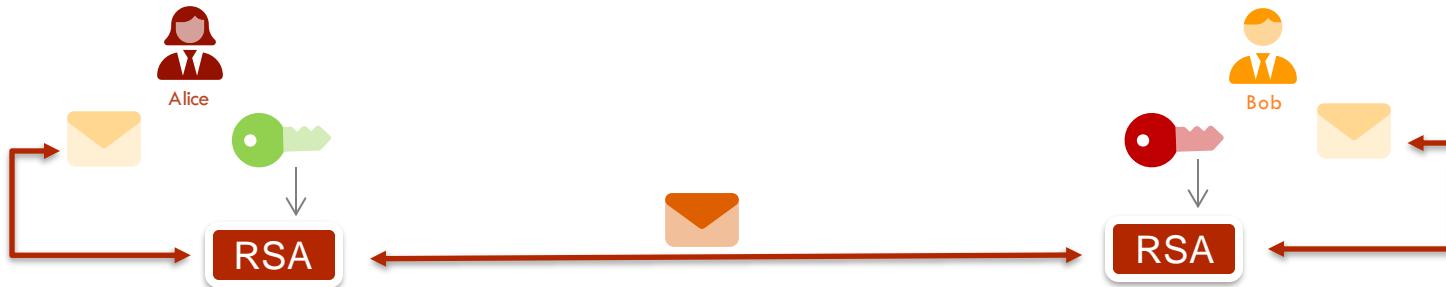
le partage et le maintien confidentiel de la clé est une difficulté



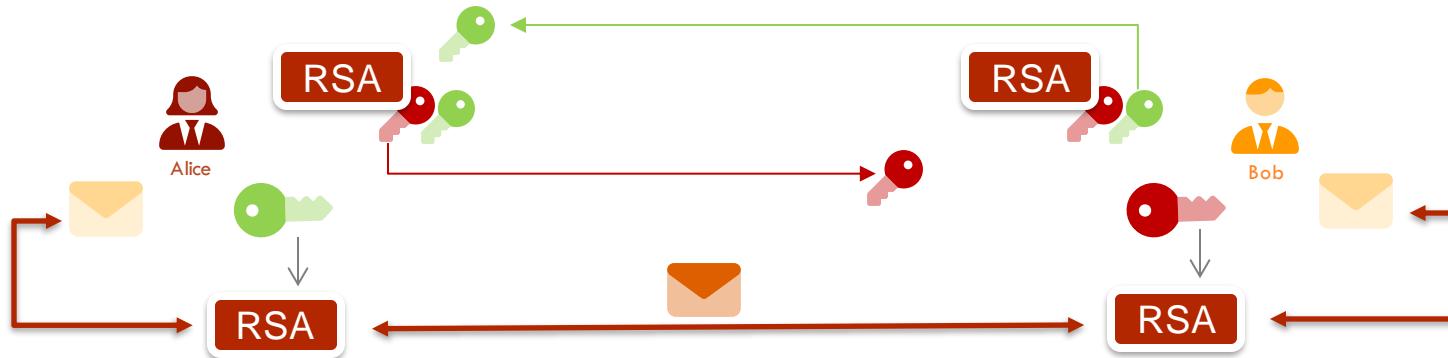
Chiffrement asymétrique



bi-clé
issu du
même
algorithme



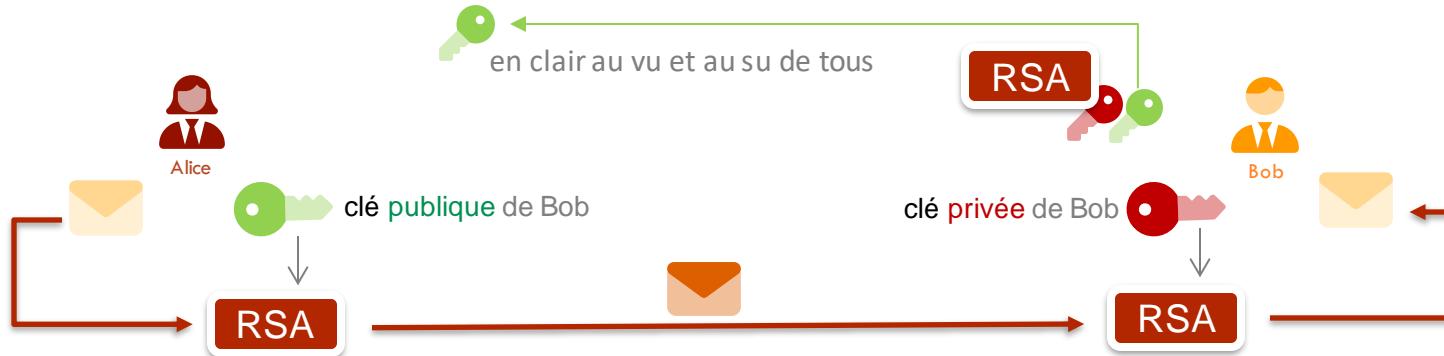
Chiffrement asymétrique



- génération du bi-clé par celui qui déchiffre
- une des bi-clés est nommée **clé privée**
- l'autre bi-clé est nommée **clé publique**

- la **clé publique** est envoyée en claire au vu et au su de tous

Chiffrement asymétrique

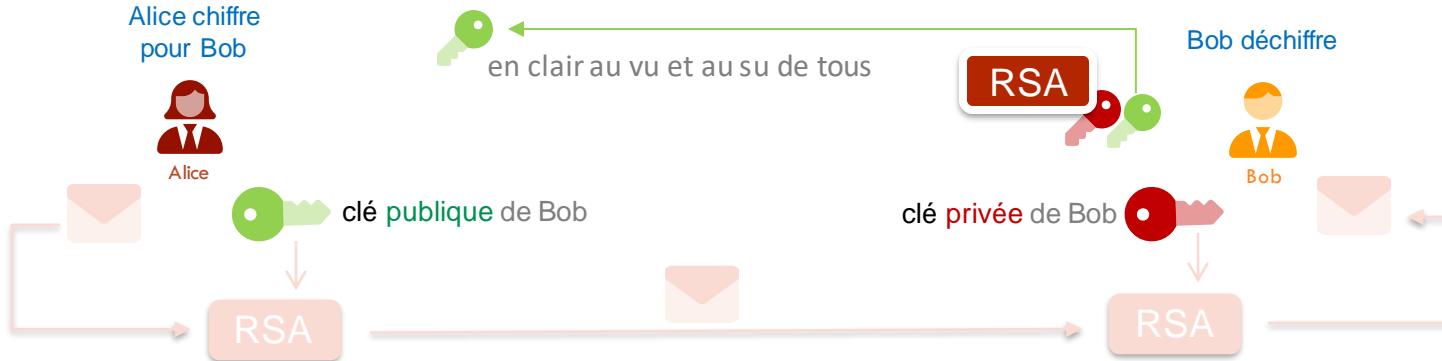


- génération du bi-clé par celui qui déchiffre
- une des bi-clé est nommée **clé privée**
- l'autre bi-clé est nommée **clé publique**

- la **clé publique** est envoyée en clair au vu et au su de tous
- seule la **clé publique** permet de chiffrer
- seule la **clé privée** permet de déchiffrer

Chiffrement asymétrique

RSA



Analogie Chiffrement asymétrique

RSA



WARNING

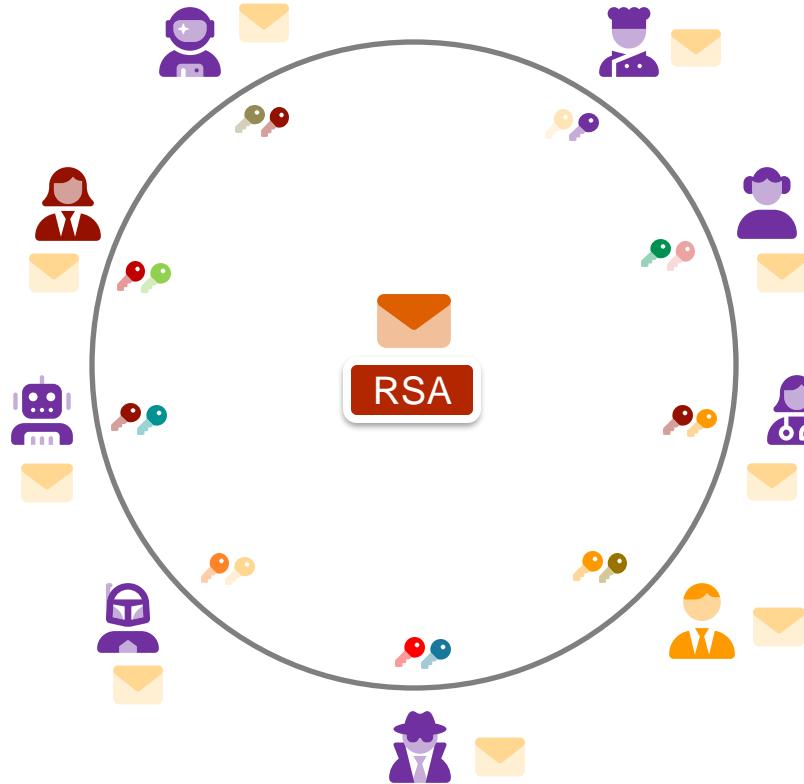


Chiffrement asymétrique

RSA



des pairs de clé avec des clés publiques partagées et diffusées



Chiffrement asymétrique

RSA



des pairs de clé avec des clés publiques partagées et diffusées

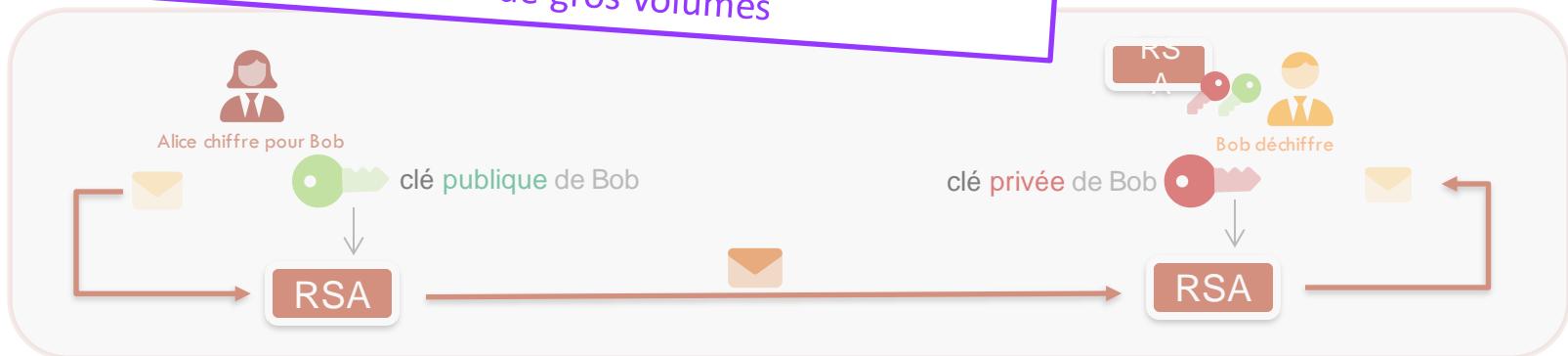


Chiffrement asymétrique

RSA



1. Beaucoup plus lent que la crypto. symétrique
2. Difficile de chiffrer de gros volumes



Chiffrement réel



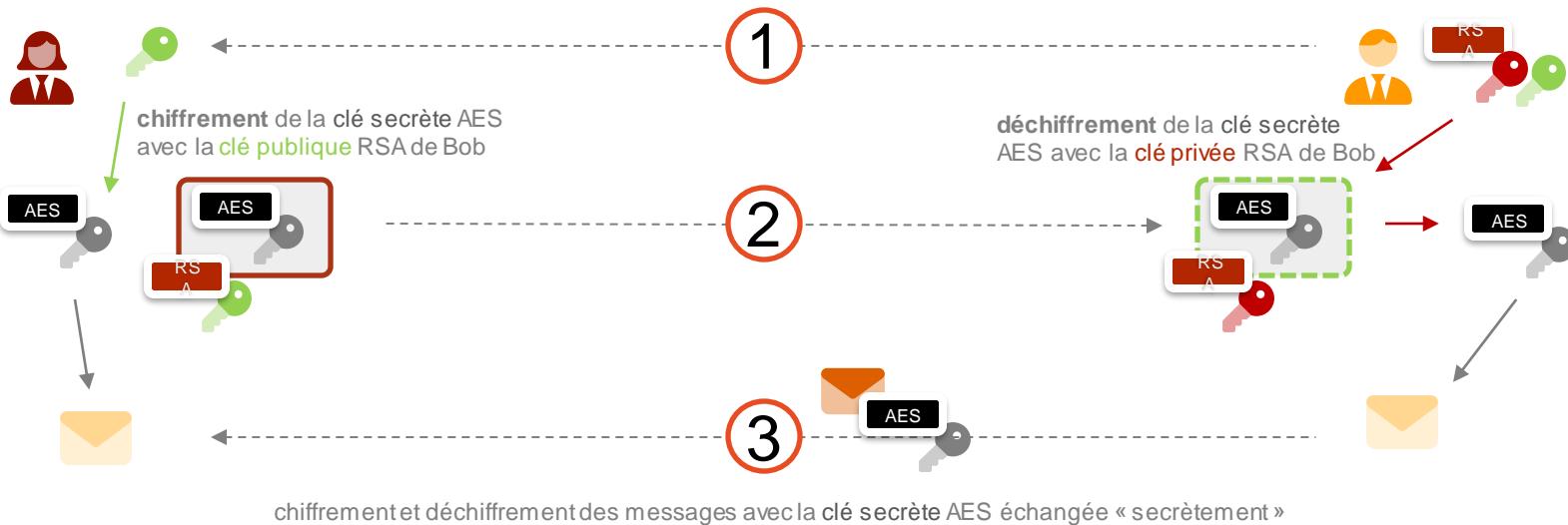
1. Chiffrement de la clé symétrique
2. avec la clé publique asymétrique



Chiffrement robuste



1. Chiffrement de la clé symétrique
2. avec la clé publique asymétrique



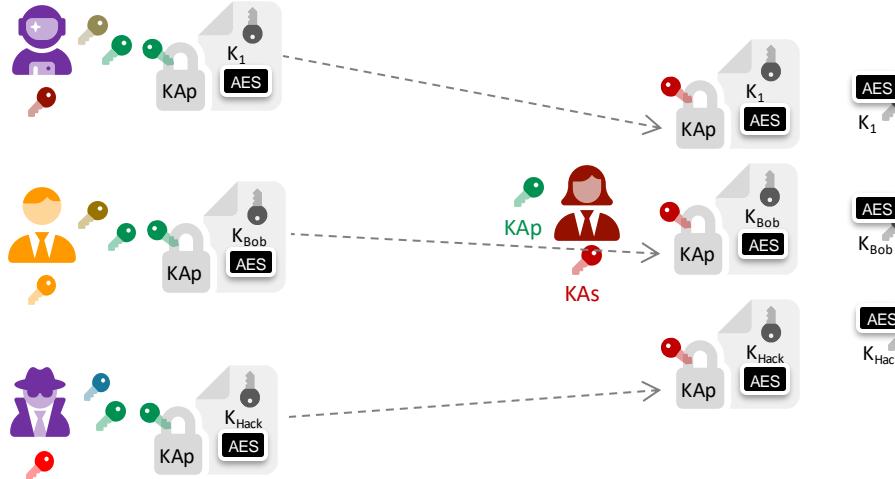


Usage: chiffrement pour la Confidentialité

RSA



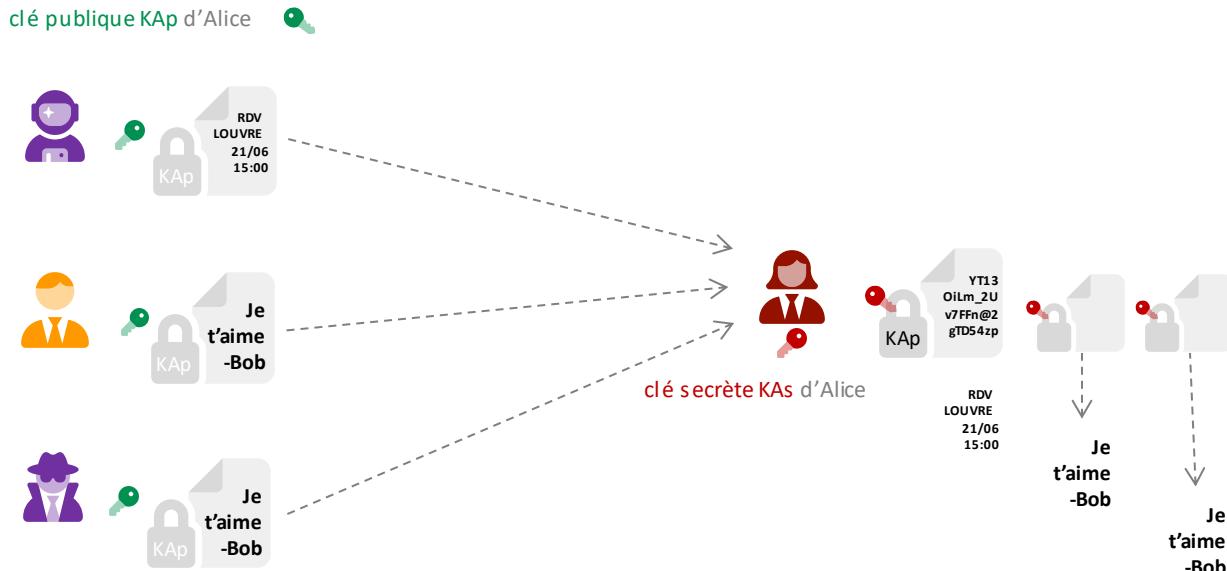
clé publique d'Alice



Type	Nom
pub	Loïc PERRY
pub	
sec/pub	Benoit LEGER
pub	stratia

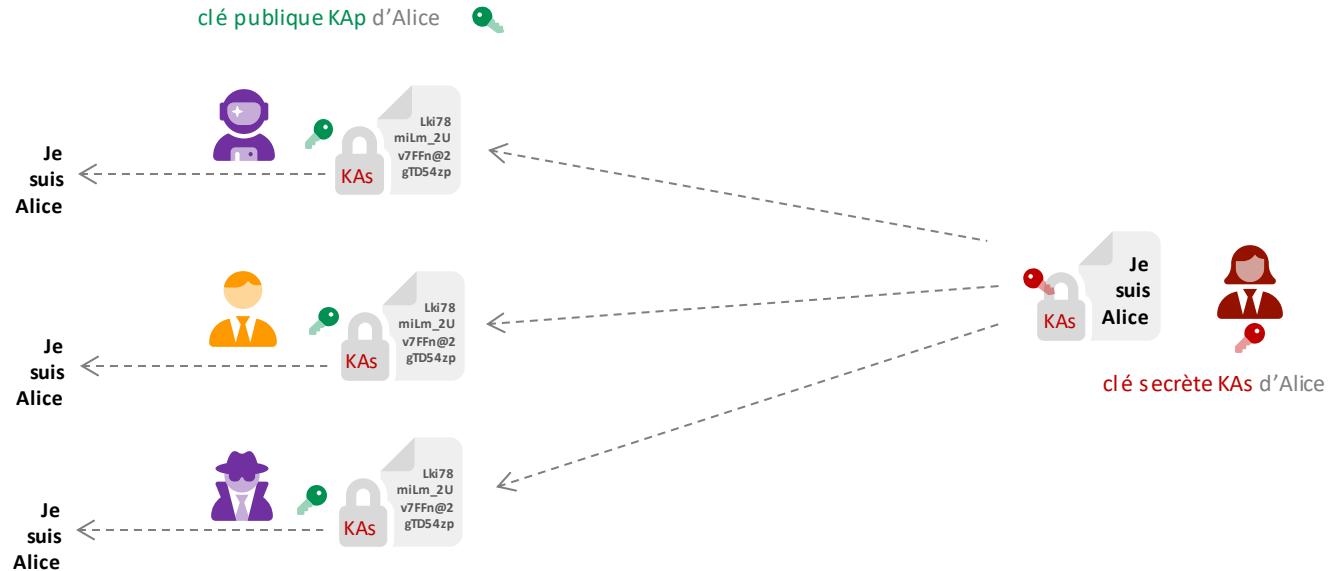


Usage: Chiffrement/Déchiffrement pour confidentialité



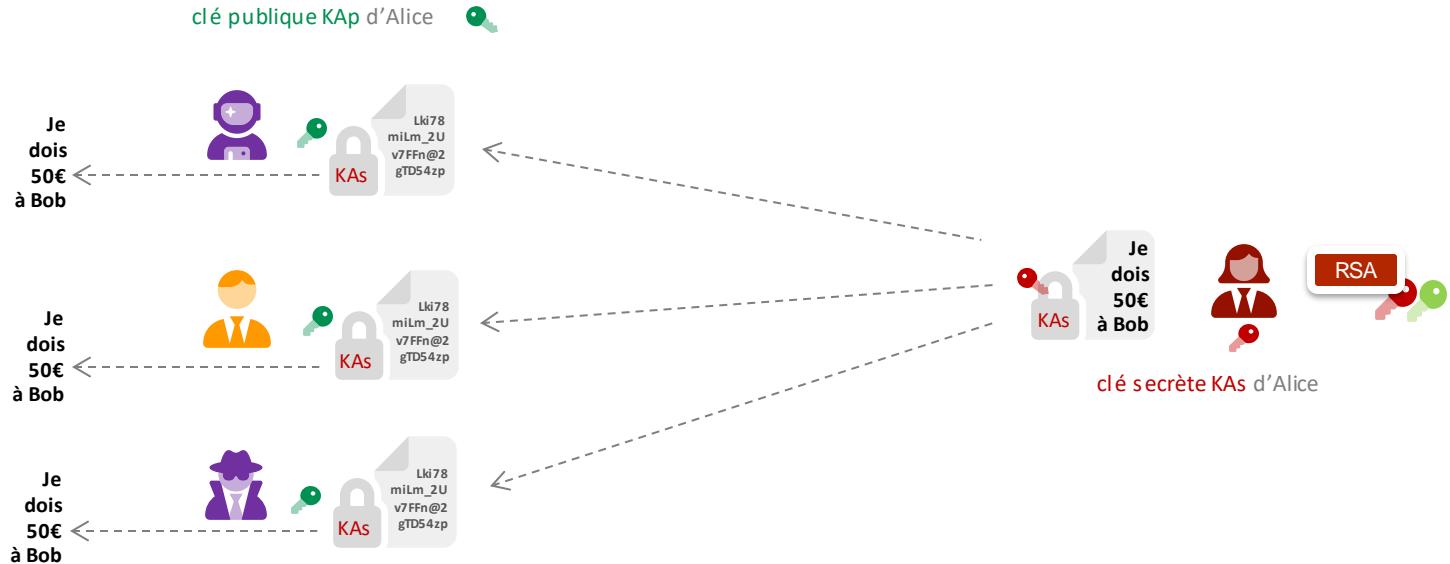


Usage: ? / ? pour ?



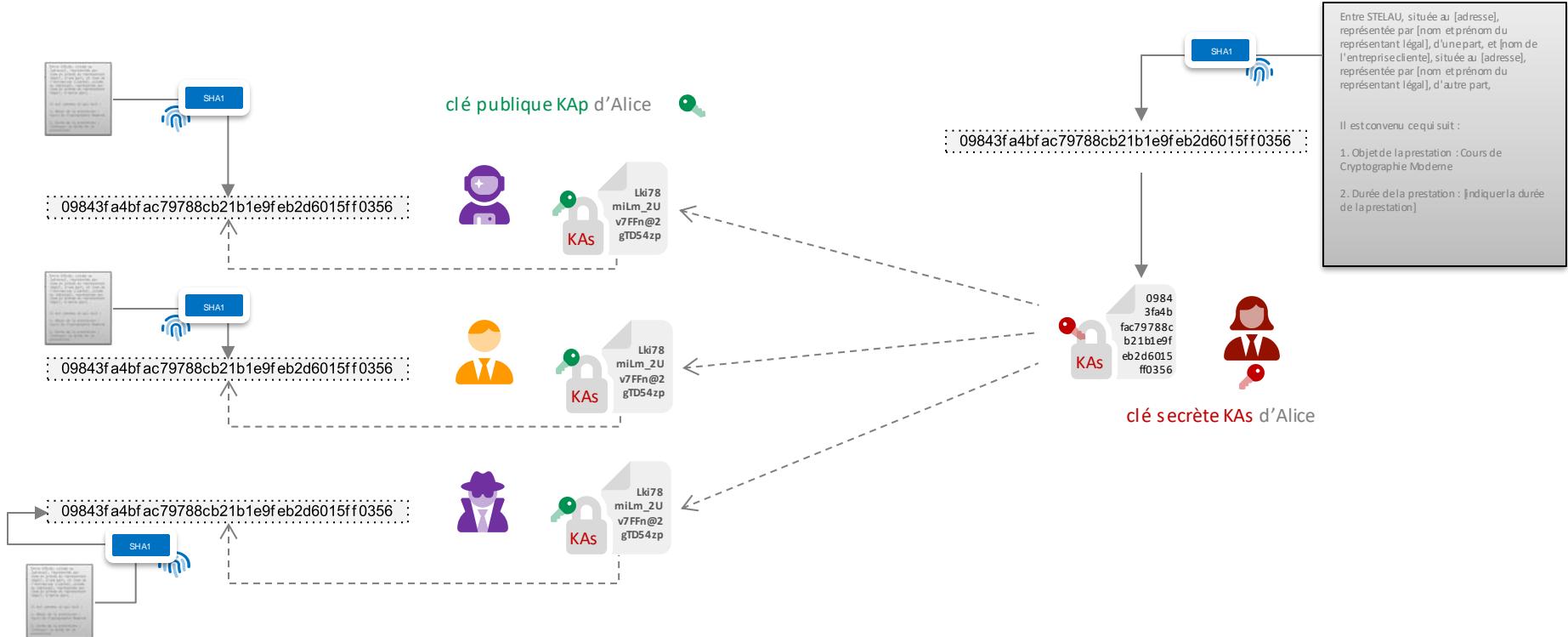


Usage: Signature / Vérification pour non-répudiation





Usage: Signature / Vérification pour non-répudiation



Deux usages différents



clé privée

clé publique

chiffrement

déchiffrer

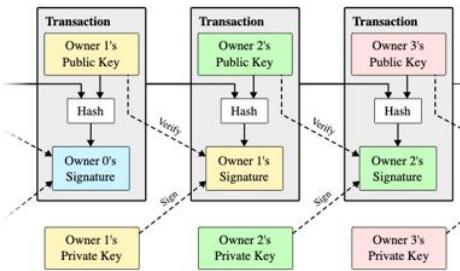
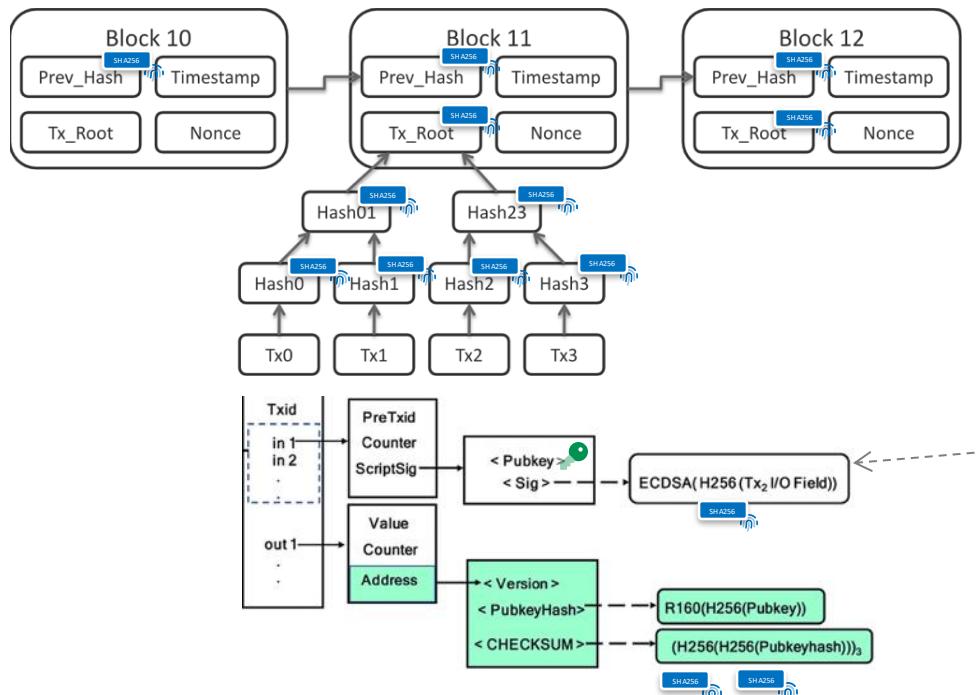
chiffrer

signature

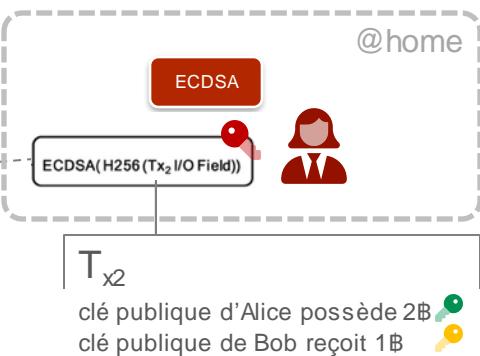
signer

vérifier

Bitcoin : hashes et signature



La clé privée de l'expéditeur est utilisée pour signer le hachage SHA-256 de toutes les données de la transaction, y compris les entrées, les sorties et les montants.



Un Tx (ou transaction) en Bitcoin est une opération dans laquelle une ou plusieurs entrées de Bitcoin sont utilisées pour créer une ou plusieurs sorties de Bitcoin. Les entrées de Bitcoin sont des sorties de transactions antérieures qui ont été envoyées à l'adresse Bitcoin du destinataire et qui sont maintenant disponibles pour être dépensées. Les sorties de Bitcoin sont des montants de Bitcoin qui sont envoyés à une adresse Bitcoin.

CEV : Cachet Electronique Visible



r9zNN1c/+Btc
6nhaLUfe0wCk
bNFwjq2l1hus
nlk

RSA

@EDF



SHA



NOUS CONTACTER

N° client : Identifiant Internet

Par Internet et Mobile
edf.fr sur Smartphone et Tablette
Télécharger l'app mobile EDF&MOI

Par téléphone
Du lundi au vendredi de 8h et jusqu'à 21h
09 69 32 18 15 (appel gratuit, prix appel)

Par courrier
EDF-SERVICE CLIENT
TBS 20012
41975 Billaud Cedex

Non boutiques
Retrouvez la boutique la plus proche de chez vous sur [boutiques.edf.com](#)

Lieu de consommation

M. LEGER BENOIT
[Votre contrat](#)



LEGER BENOIT
2 rue d'ici
1^{er} Etage
75001 PARIS

ATTESTATION TITULAIRE DE CONTRAT

Par la présente, EDF atteste que M. BENOIT LEGER est actuellement titulaire auprès d'EDF pour le logement situé au

Ce contrat a été établi au nom de M. BENOIT LEGER sur la base de ses décl

Pour servir et valoir ce que de droit.

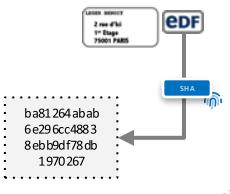


@home

RSA



r9zNN1c/+Btc
6nhaLUfe0wCk
bNFwjq2l1hus
nlk

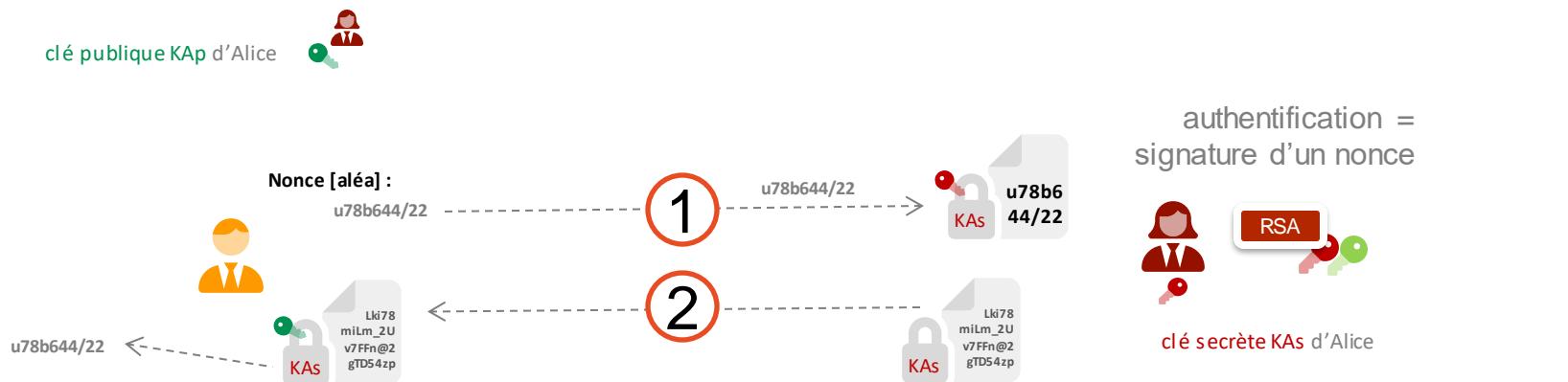


SHA

ba81264abab
6e296c4883
8eb9df78db
1970267

Usage: Authentification

RSA



~ 100% des authentifications
sont établies sur une signature

Trois usages différents



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

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'**Authentification**

Fonctions de hachage



Établissement de clé



Générateurs d'aléa



S/MIME (Secure/Multipurpose Internet Mail Extensions)	Azure Active Directory (gestion des identités et des accès)	Trezor (autre portefeuille matériel pour cryptomonnaies)
e-Passport (Passport électronique)	OAuth 1.0a (protocole d'autorisation)	Knox de Samsung (solution de sécurité pour dispositifs mobiles de Samsung)
Smartphones modernes (sécurisation des données et communications)	Keepass (gestionnaire de mots de passe open-source)	3CX (système de téléphonie IP qui sécurise les communications VoIP)
HTTPS (SSL/TLS)	Samsung Knox (sécurité pour les appareils mobiles)	FortiClient (client VPN de Fortinet)
IPsec (Internet Protocol Security)	Android Keystore System (sécurité pour les clés de chiffrement sur les appareils Android)	Zix (solutions de chiffrement des emails pour les entreprises)
PGP (Pretty Good Privacy) / GPG (GNU Privacy Guard)	Cisco AnyConnect Secure Mobility Client (VPN)	CryptoWall (malware de type ransomware utilisant le chiffrement, mentionné ici à titre informatif)
TOTP (Time-Based One-Time Password)	Fortinet FortiGate (solutions de sécurité réseau et de pare-feu)	Onavo Protect (VPN propriété de Facebook, controversé pour des raisons de confidentialité)
Bitcoin et autres cryptomonnaies	s2n (Signal to Noise), bibliothèque de cryptographie implémentée par AWS	Apache SSL/TLS (module mod_ssl pour le chiffrement avec le serveur web Apache)
SSH (Secure Shell)	Keybase (sécurité des équipes et collaboration)	Check Point VPN (technologies de virtualisation de réseau et de sécurité)
TLS (Transport Layer Security)	OpenPGP (cryptage des emails et des fichiers)	Code42 (logiciel de sauvegarde et de récupération des données).
IKE (Internet Key Exchange)	Secure Enclave (sécurisation des données sur les appareils Apple)	
HSM (Hardware Security Modules)	Thales nShield HSMs (Hardware Security Modules pour la protection des clés)	
Kerberos (protocole d'authentification réseau)	CyberArk (protection des priviléges et gestion sécurisée des sessions)	
OTR (Off-the-Record Messaging)	Silent Circle (communications chiffrées)	
Signal Protocol (messagerie chiffrée)	Wickr (messagerie chiffrée et appels sécurisés)	
Tor (The Onion Router)	Dust (messagerie sécurisée avec auto-destruction des messages)	
Wi-Fi Protected Access (WPA2 et WPA3)	Duo Security (solutions d'authentification à deux facteurs)	
YubiKey (dispositif d'authentification)	Microsoft Encrypting File System (EFS) pour NTFS	
Zoom (chiffrement de communications vidéo)	Ghostery (protection de la vie privée et bloqueur de trackers pour navigateurs)	
Apple Pay / Google Pay (paiements sécurisés)	EFF's HTTPS Everywhere (extension de navigateur pour forcer le chiffrement HTTPS)	
Z RTP (Zimmermann Real-Time Transport Protocol)	Mullvad VPN (réseau privé virtuel axé sur la confidentialité)	
OpenSSL (bibliothèque de cryptographie)	NordVPN (VPN avec fonctionnalités de sécurité avancées)	
VPNs utilisant OpenVPN ou WireGuard	Let's Encrypt (fournisseur d'autorité de certification pour HTTPS)	
ECC (Elliptic Curve Cryptography) utilisé dans divers protocoles et produits	Yubico YubiHSM (module de sécurité matériel pour la protection des clés)	
Let's Encrypt (autorité de certification utilisant ACME)	OpenSSH (implémentation sécurisée du protocole SSH)	
RDP (Remote Desktop Protocol) sécurisé	DigiCert (fournisseur d'autorités de certification SSL/TLS)	
LUKS (Linux Unified Key Setup) pour le chiffrement de disque	Okta (gestion de l'identité et de l'accès)	
Signal (application de messagerie)	Authy (authentification à deux facteurs)	
WhatsApp (chiffrement bout en bout pour la messagerie)	Symantec VIP (Validation and ID Protection Service)	
Telegram (mode "Secret Chat" pour la messagerie sécurisée)	SignalR (bibliothèque pour les communications en temps réel sécurisées)	
X.509 certificats (pour SSL/TLS)	Cloudflare WARP (service VPN pour utilisateurs finaux)	
TrueCrypt et VeraCrypt (chiffrement de disque)	CAC (Common Access Card) pour l'identification militaire et gouvernementale	
RSA SecureID (tokens d'authentification)	Trusted End Node Security (TENS, autrement nommé Lightweight Portable Security)	
LDAPS (LDAP over SSL)	Magic Leap (réalité augmentée avec des caractéristiques de sécurité)	
DKIM (DomainKeys Identified Mail)	Blackphone (smartphone orienté vers la sécurité et la vie privée)	
DMARC (Domain-based Message Authentication, Reporting & Conformance)	SwissSign (fournisseur d'autorité de certification pour la signature numérique)	
SPF (Sender Policy Framework)	Tresorit (service de stockage cloud avec chiffrement bout en bout)	
SCCP (Stream Control Transmission Protocol) avec DTLS (Datagram Transport Layer Security)	CyberGhost VPN (service VPN axé sur la confidentialité)	
SCADA systems (pour sécuriser les systèmes de contrôle industriel)	ExpressVPN (service VPN avec de multiples fonctionnalités de sécurité)	
EMV (Europay, MasterCard et Visa) pour la sécurité des transactions par carte	pfSense (pare-feu open source et routeur)	
Microsoft BitLocker (chiffrement de disque)	I2P (Invisible Internet Project pour une communication sécurisée)	
Apple FileVault (chiffrement de disque)	Lastline (protection avancée contre les menaces)	
Docker Content Trust (signature et vérification d'image)	Silent Circle's Blackphone (smartphone axé sur la vie privée)	
Secure Boot et Trusted Platform Module (TPM) dans les systèmes modernes	OpenKeychain (implémentation Android de PGP)	
HCE (Host Card Emulation) pour paiements mobiles	Telegram Passport (identification sécurisée pour les services en ligne)	
1Password, LastPass (gestionnaires de mots de passe)	Hushmail (service email sécurisé)	
ProtonMail (service de courriel sécurisé)	VMware Horizon (virtualisation de postes de travail sécurisée)	
Brave (navigateur avec des fonctionnalités de sécurité améliorées)	Crypto.com (plateforme de paiement et d'échange de cryptomonnaies)	
Matrix (protocole de communication décentralisé)	EncroChat (service de communication crypté, désormais fermé)	
Monero, Zcash (cryptomonnaies axées sur la confidentialité)	PureVPN (service VPN avec chiffrement sécurisé)	
IPFS (InterPlanetary FileSystem) avec libp2p (sécurité pour les systèmes de fichiers distribués)	Line (application de messagerie avec option de chiffrement bout en bout)	
RIPEMD, Whirlpool (autres fonctions de hachage utilisées)	Signal Private Messenger (messagerie sécurisée et privée)	
StartTLS (amélioration de la sécurité pour les protocoles de communication en texte clair)	Auth0 (plateforme d'authentification et d'autorisation)	
BGPSEC (sécurité pour le protocole de routage BGP)	Keycloak (gestion de l'identité et des accès avec support SSO)	
STIX/TAXII pour le partage d'informations sur les menaces cybernétiques	Cloudflare Access (sécurisation des applications internes)	
Zero Trust Networks	AxCrypt (logiciel de chiffrement de fichiers pour Windows)	

Crypto asymétrique : attention

Echange sécurisé de secret

Clarification

► Key exchange :

- Sender generates a key and encrypts it using receiver's public key
- Receiver does not participate in key generation. Only sender.
- RSA is typically used for key exchange.

RSA

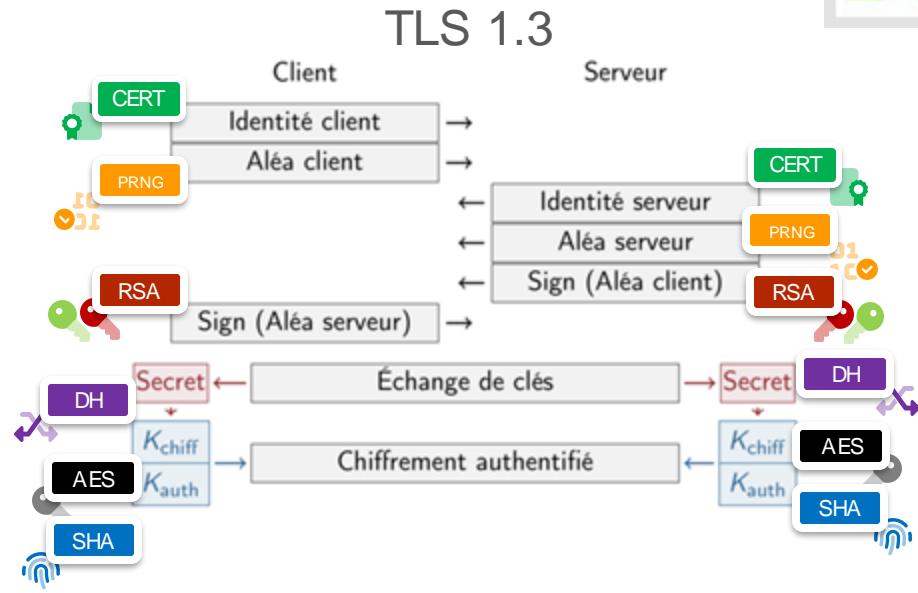
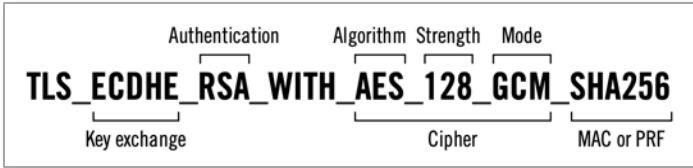
► Key agreement :

- Sender and receiver work together to generate a key.
- This is what DH provides.

DH

Assemblage Crypto

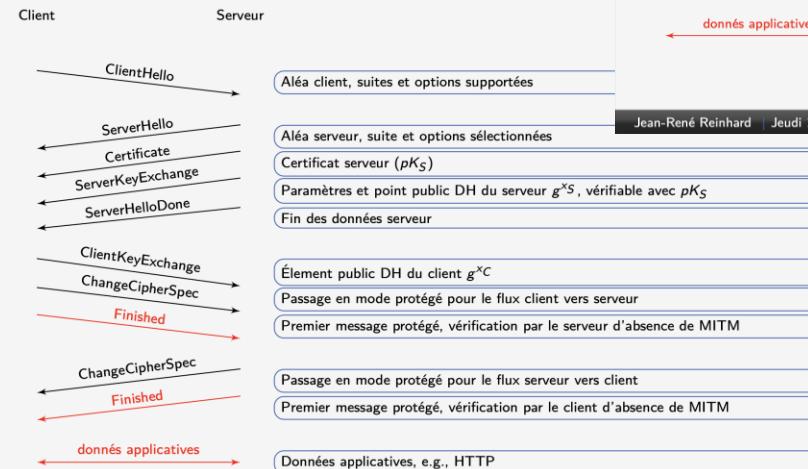
https://



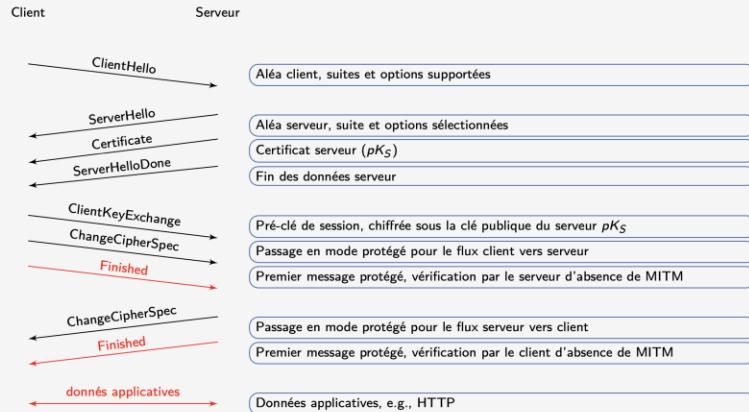
Cipher Suite Name	Auth	KX	Cipher	MAC	PRF
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	RSA	ECDHE	AES-128-GCM	-	SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDSA	ECDHE	AES-256-GCM	-	SHA384
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DHE	3DES-EDE-CBC	SHA1	Protocol
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES-128-CBC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

Assemblage Crypto

SSL/TLS : établissement de clé DHE



SSL/TLS : établissement de clé RSA



Certificat électronique

Ce n'est pas une primitive cryptographique

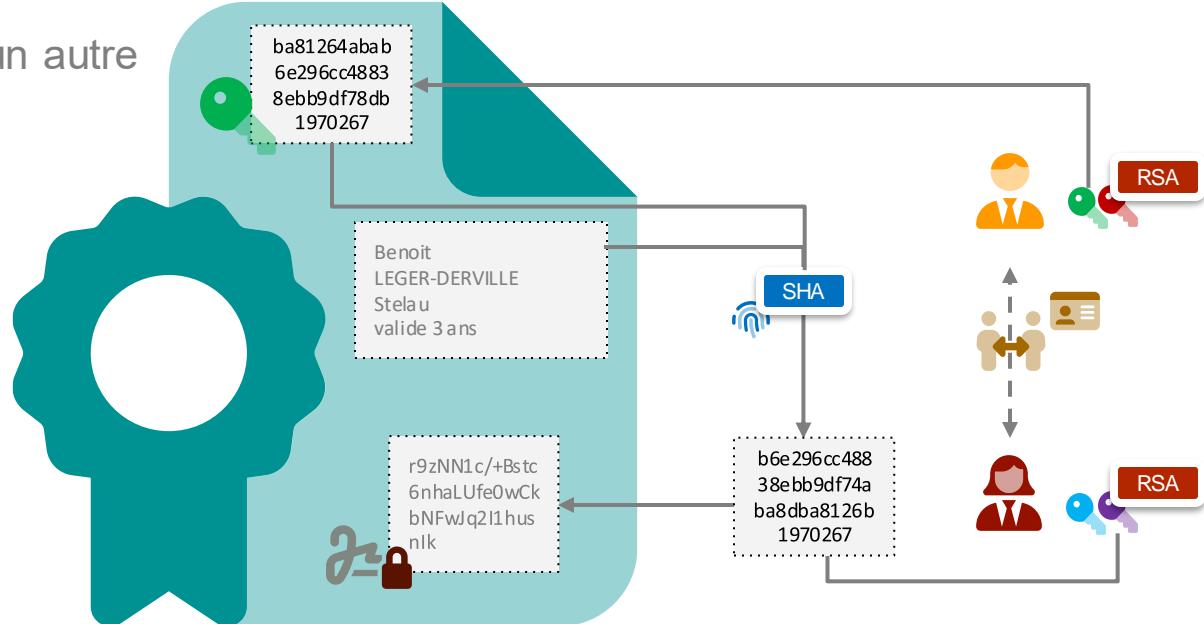
C'est un assemblage

C'est un fichier comme un autre

1. identité

2. clé publique

3. signature
de l'identité
par un tiers



Very Short Crypto Story

3000 ans de crypto. **symétrique**

recettes militaro-diplomatiques
de confusion et de diffusion

100 ans de crypto. **moderne**

de Kerckhoffs ...
au crypto-système incassable



50 ans de crypto. **asymétrique**

LA véritable révolution



20 ans de crypto. **quantique**

révolution ? (ou pas)



Confusion et Diffusion

« tant bien que mal »
de César à Enigma

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

Résout la difficulté de
l'échange de clé

+

Permet l'usage du
principe de **Signature**

Les vrais difficultés de la cryptographie moderne

1. THEORIE : Cryptologie

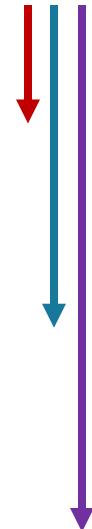
- failles théoriques = **mathématiques**
- cryptologue est un métier

2. CODE : Implémentations

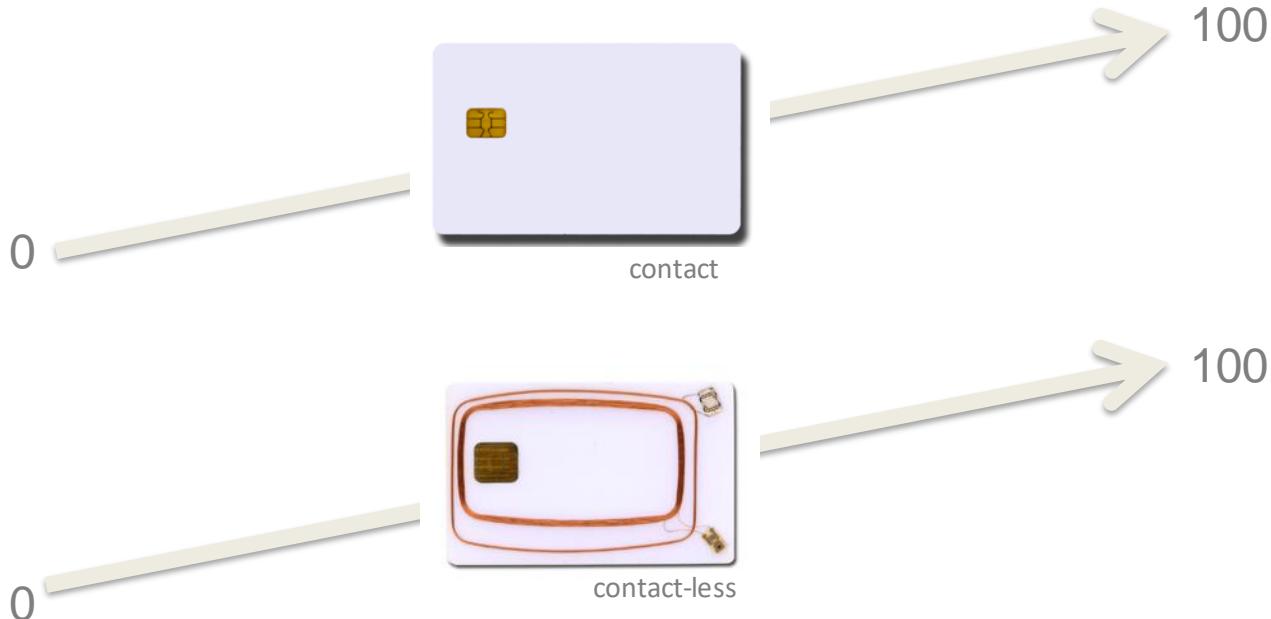
- erreurs/failles/vuln = **informatique**
- « Do not implement cryptography yourself ! »

3. UX : Usages

- mauvais usages = **ignorance/pusillanimité**
- bons usages = **formation**

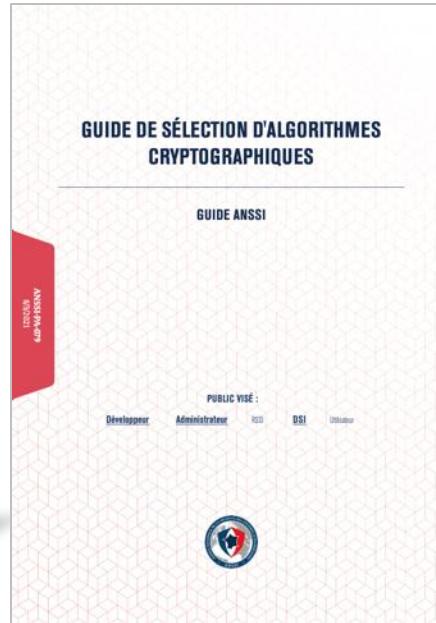
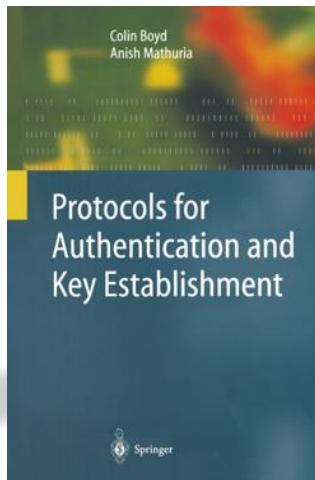
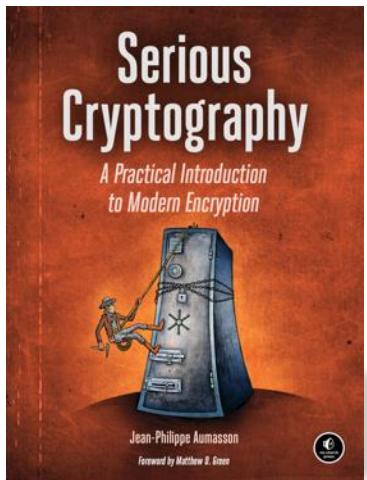


Attention : « C'est (pas) sécurisé ! » ne veut rien dire



Fin

Ouvrages Cryptographiques



Ateliers/jeux Cryptographie Moderne

Atelier 1 : DH War- Ennemy in the Middle



4 groupes
de 10 étudiants

4 groupes
de 5 étudiants

Atelier 2 : Wannacry Nightmare Puzzle



Hello !

AES



Hello !

SHA



26, 47, 10

DH



91690410bec9
graine

PRNG

101
100

798

aléa



7e0950bb938539162d268b379595
44efb87b718950d4f721dd5c945f7
d12fcfe4ca9d9b5f0c81bbc1555c3d7
6610ef3080a354e60b625f5c50a23
a6ffd13ec024239dd0e47706c9a23
11fc38e37161e87501236542732797
2469b3985721cc0fea3b04047a9c5
b559e3471a736f5e4c7b473b2e86b1
b21dd8a829828d8f6

Rappels

hash crypto – RSA - certificats – IGC/PKI



Hash



fonctions de hachage cryptographiques

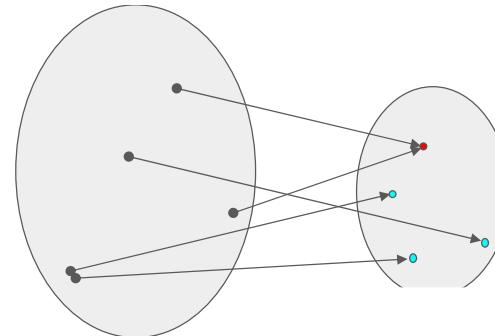
- Fonctions à sens unique
 - d'un espace infini vers un espace fini
 - 128, 160, 224, 256 ou 512 bits
- Résistantes aux attaques
 - 1^{ère} pré-image
 - 2^{de} pré-image
 - collision

Hash



fonctions de hachage cryptographiques

- Fonctions à sens unique
 - d'un espace infini vers un espace fini
 - 128, 160, 224, 256 ou 512 bits
- Résistantes aux attaques
 - 1^{ère} pré-image
 - 2^{de} pré-image
 - collision



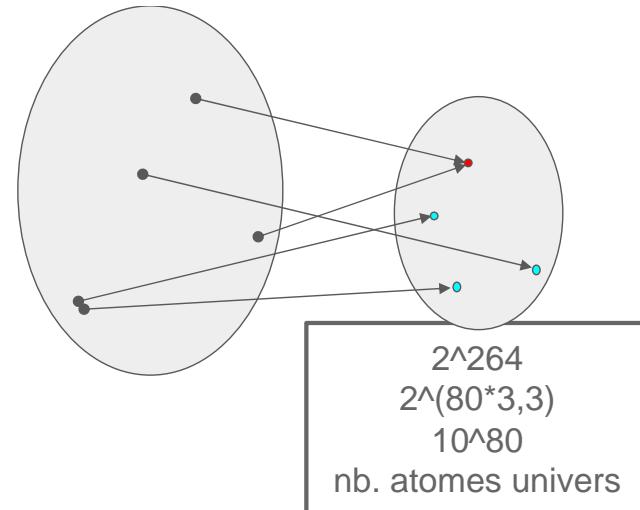
Hash



fonctions de hachage cryptographiques

- Fonctions à sens unique
 - d'un espace infini vers un espace fini
 - 128, 160, 224, 256 ou 512 bits

- Résistantes aux attaques
 - 1^{ère} pré-image
 - 2^{de} pré-image
 - collision



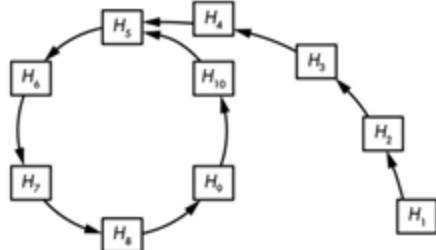
Hash



fonctions de hachage cryptographiques

- Résistantes aux attaques

- 1^{ère} pré-image
- 2^{de} pré-image
- collision



1. il est très difficile de trouver le contenu du message à partir de son condensat
2. à partir d'un message donné et de son condensat (et de la fonction de hachage), il est très difficile de générer un autre message qui donne le même condensat
3. il est très difficile de trouver deux messages aléatoires qui donnent un même condensat (résistance aux collisions)



Hash

fonctions de hachage cryptographiques

- Résistance aux préimages

Attaque : avec x donné, trouver m tel que $H(m) = x$

- Résistance aux secondes préimages

Attaque : avec m_1 donné, trouver m_2 tel que $H(m_1) = H(m_2)$

- Résistance aux collisions

Attaque : trouver m_1 et m_2 tel que $H(m_1) = H(m_2)$

Hash

5baa61e4c9b93f3f0682250b6f8331b7ee68fd8



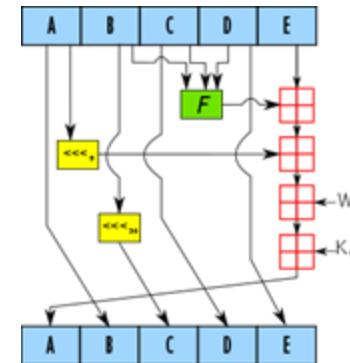
fonctions de hachage cryptographiques

```
SHA1-compress(H, M) {
    (a0, b0, c0, d0, e0) = H // parsing H as five 32-bit big endian words
    (a, b, c, d, e) = SHA1-blockcipher(a0, b0, c0, d0, e0, M)
    return (a + a0, b + b0, c + c0, d + d0, e + e0)
}
```

```
expand(M) {
    // the 512-bit M is seen as an array of sixteen 32-bit words
    W = empty array of eighty 32-bit words
    for i = 0 to 79 {
        if i < 16 then W[i] = M[i]
        else
            W[i] = (W[i - 3] ⊕ W[i - 8] ⊕ W[i - 14] ⊕ W[i - 16]) <<< 1
    }
    return W
}
```

```
SHA1-blockcipher(a, b, c, d, e, M) {
    W = expand(M)
    for i = 0 to 79 {
        new = (a <<< 5) + f(i, b, c, d) + e + K[i] + W[i]
        (a, b, c, d, e) = (new, a, b >>> 2, c, d)
    }
    return (a, b, c, d, e)
}
```

```
f(i, b, c, d) {
    if i < 20 then return ((b & c) ⊕ (~b & d))
    if i < 40 then return (b ⊕ c ⊕ d)
    if i < 60 then return ((b & c) ⊕ (b & d) ⊕ (c & d))
    if i < 80 then return (b ⊕ c ⊕ d)
}
```



```
275     x[2] = byte(s >> 24)
276     x[1] = byte(s >> 16)
277     x[0] = byte(s >> 8)
278     x[7] = byte(s)
279   }
280   func putUInt32(x []byte, s uint32) {
281     x[0] = byte(s >> 24)
282     x[1] = byte(s >> 16)
283     x[2] = byte(s >> 8)
284     x[3] = byte(s)
285   }
286 }
```

Source : Serious Cryptography
Copyright © 2018 by Jean-Philippe Aumasson

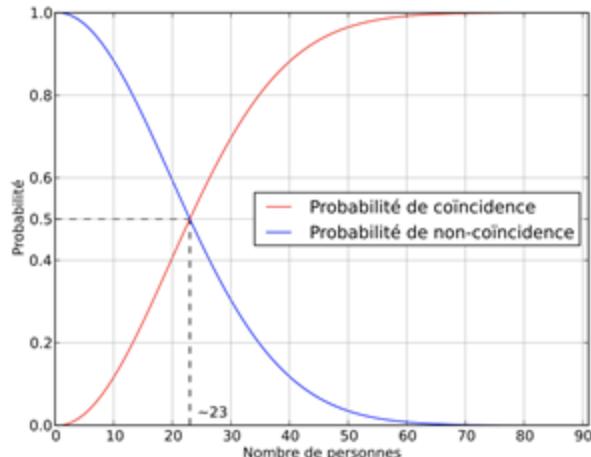
Hash



le paradoxe des anniversaires

Soit E un ensemble fini. La probabilité $p(n)$ que, parmi n éléments de E , chaque élément étant tiré uniformément dans tout l'ensemble E , deux éléments au moins soient identiques vaut :

$$\bar{p}(n) = \frac{365!}{(365 - n)!} \cdot \frac{1}{365^n}$$



n	$p(n)$
5	2,71 %
10	11,69 %
15	25,29 %
20	41,14 %
23	50,73 %
25	56,87 %
30	70,63 %
40	89,12 %
50	97,04 %
60	99,41 %

Hash



le paradoxe des anniversaires

Si une fonction de hachage a une sortie de n bits (**n grand**) alors l'ensemble d'arrivée possède 2^n éléments et il faut **environ** $2^{(n/2)}$ hachés d'éléments distincts pour produire une collision avec 50 % de chance.

$$n(p) \approx \sqrt{2 \cdot |E| \ln\left(\frac{1}{1-p}\right)}$$

$$p(n) = 1 - \frac{|E|!}{(|E|-n)!} \cdot \frac{1}{|E|^n}$$

```
for j in $(seq 1 100); do
    for i in $(seq 1 █); do
        empreinte=$(head -c 142 /dev/urandom | shasum5.18 -b)
        Bits8=$(echo $empreinte | head -c 2)
        echo $Bits8
        # echo $empreinte " " $(echo $empreinte | head -c2)
        # echo $(echo $empreinte | head -c 2)
    done | sort | uniq -c | grep -v '1 ' | head -n 1
    # echo $j
done | wc -l
```

4b5171fcc7dcb79851a0471bf65bc012	4b
581bff7d931ac867fb7e1ed5c2d303c7	58
643504d90e1236b6f63feffe33ca4fe4	64
7a940a030cfb822565abd2d93f30369c	7a
7defce06508bc9e3a227e1267bc91d3b	7d
80eef2c533d0efc1d20d3b498d7aec8a	80
a0286479a5d60986fcac43d3d863b21e	a0
ab2d4b8df2e6ade91fc39bdbe1a6a22a	ab
c617bdee475a7221864ec7535aa46b9f	c6
f12f395b4c4a3c3d0d43b6224e875aeb	f1
fb7c125c99ee3f897a23b95081b18f9a	fb

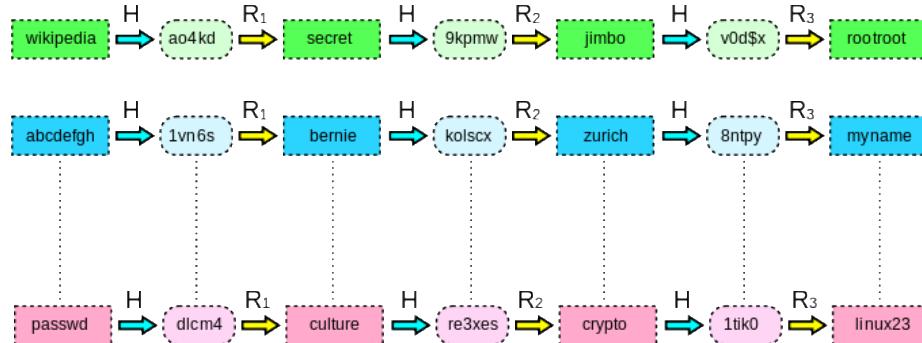
Hash



compromis temps-mémoire

- Rainbow Tables

- génération longue délicate



```
empreinte = h(mot_de_passe + sel)
```



Rappel : Signature numérique

Signature manuscrite

- atteste de l'approbation du contenu d'un document par le signataire
- vérifiable à l'aide d'une signature de référence
- difficile à imiter sur un autre document (**forge**)
- non-répudiable : le signataire ne peut nier avoir signé le document
- transférable : Bob peut convaincre un juge qu'Alice a bien signé un document portant sa signature

Signature numérique *on souhaite conserver les mêmes propriétés*

- approbation
- vérifiable
- non forgeable
- non répudiable
- transférable

Signature numérique

Crypto Asymétrique



- Fonctions à sens unique
 - à trappe (RSA)
 - ou pas (DSA, ECDSA)
- Bi-clés
 - une privée, connue du seul signataire
 - une publique, connue de tous

Signature

Cryptosystème RSA



$$C \equiv M^e \pmod{n}$$

$$M \equiv C^d \pmod{n}$$



p et q premiers

$$n=p \cdot q$$

$$\varphi(n) = (p - 1)(q - 1)$$

e premier avec $\varphi(n)$

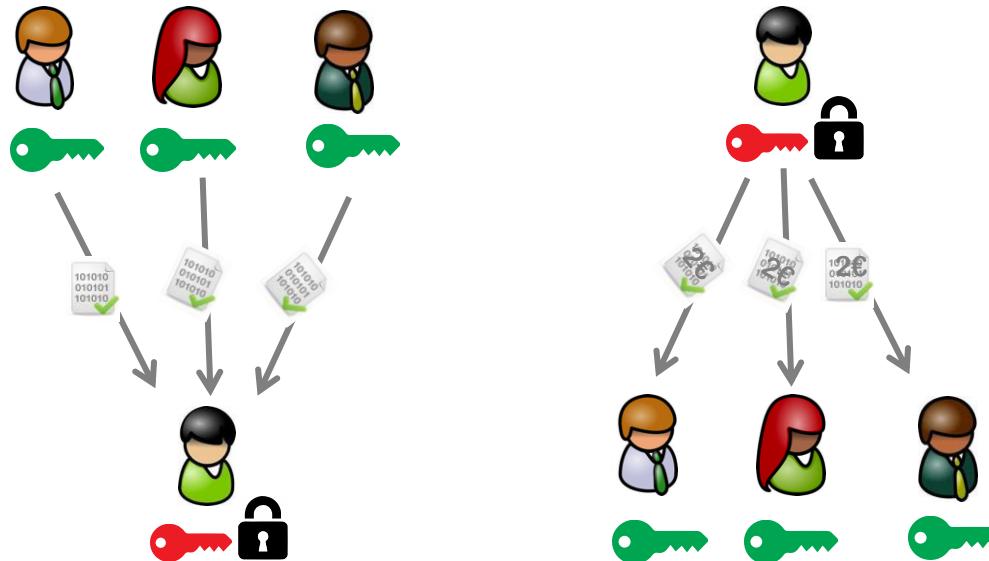
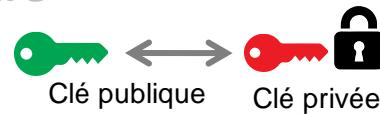
d inverse de e modulo $\varphi(n)$

- Comme $c \equiv m^e \pmod{n}$, $c^d \pmod{n} = m^{ed} \pmod{n}$
- Comme $ed \equiv 1 \pmod{(p-1)(q-1)}$ il existe un entier k tel que $ed \equiv 1 + k(p-1)(q-1)$
- Par conséquent $c^d \pmod{n} = m^{1+k(p-1)(q-1)} \pmod{n}$
- Or (théorème de Fermat) $m^{(p-1)} \pmod{p} = 1$ si m n'est pas multiple de p. Par élévation à la puissance $k(q-1)$ puis multiplication par m on obtient : $m^{1+k(p-1)(q-1)} \pmod{p} = m$ égalité qui reste vraie (2 membres=0) si m est multiple de p
- Par symétrie $m^{1+k(p-1)(q-1)} \pmod{q} = m$ donc $m^{1+k(p-1)(q-1)} - m$ est divisible par p et q donc par pq (p et q premiers et différents)
- Par conséquent $c^d \pmod{n} = m^{1+k(p-1)(q-1)} \pmod{pq} = m$

Crypto asymétrique



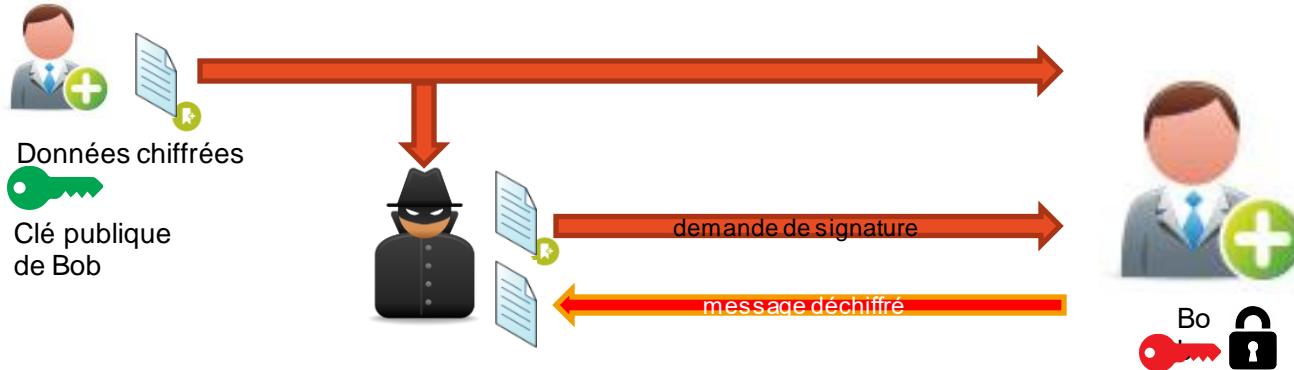
Usage : chiffrement vs signature



Rappels

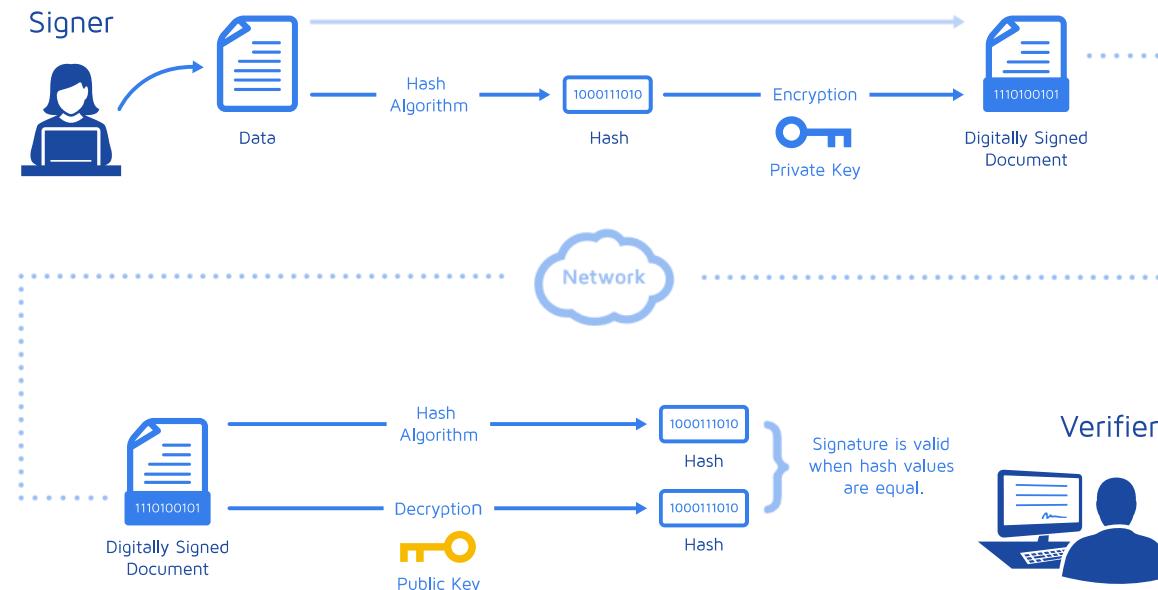


Certificat – Séparation des Key Usage

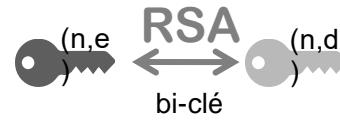


Cryptographie : utilisation de sa clé privée
déchiffrement = signature

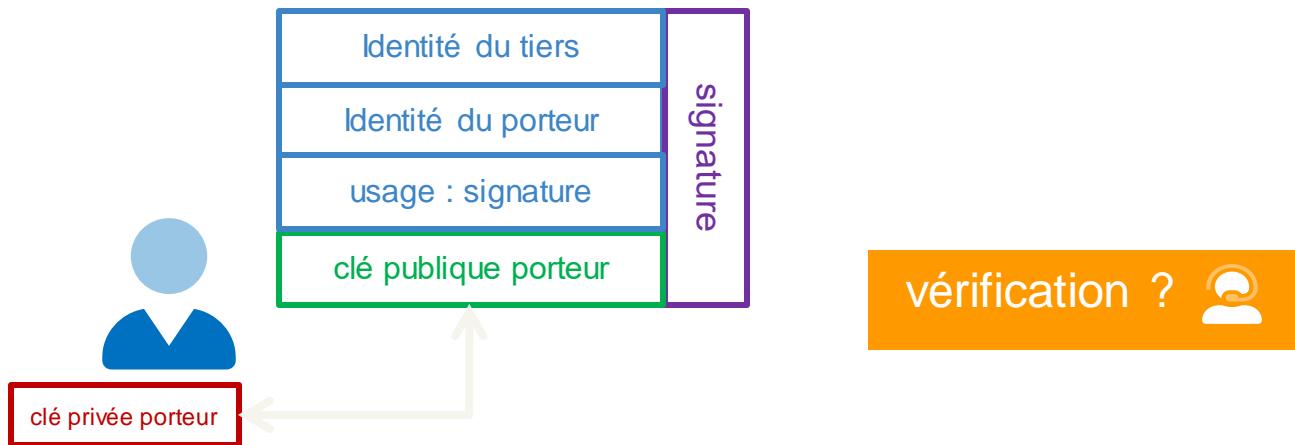
Exemple de Signature bi-clé de signature Certigna



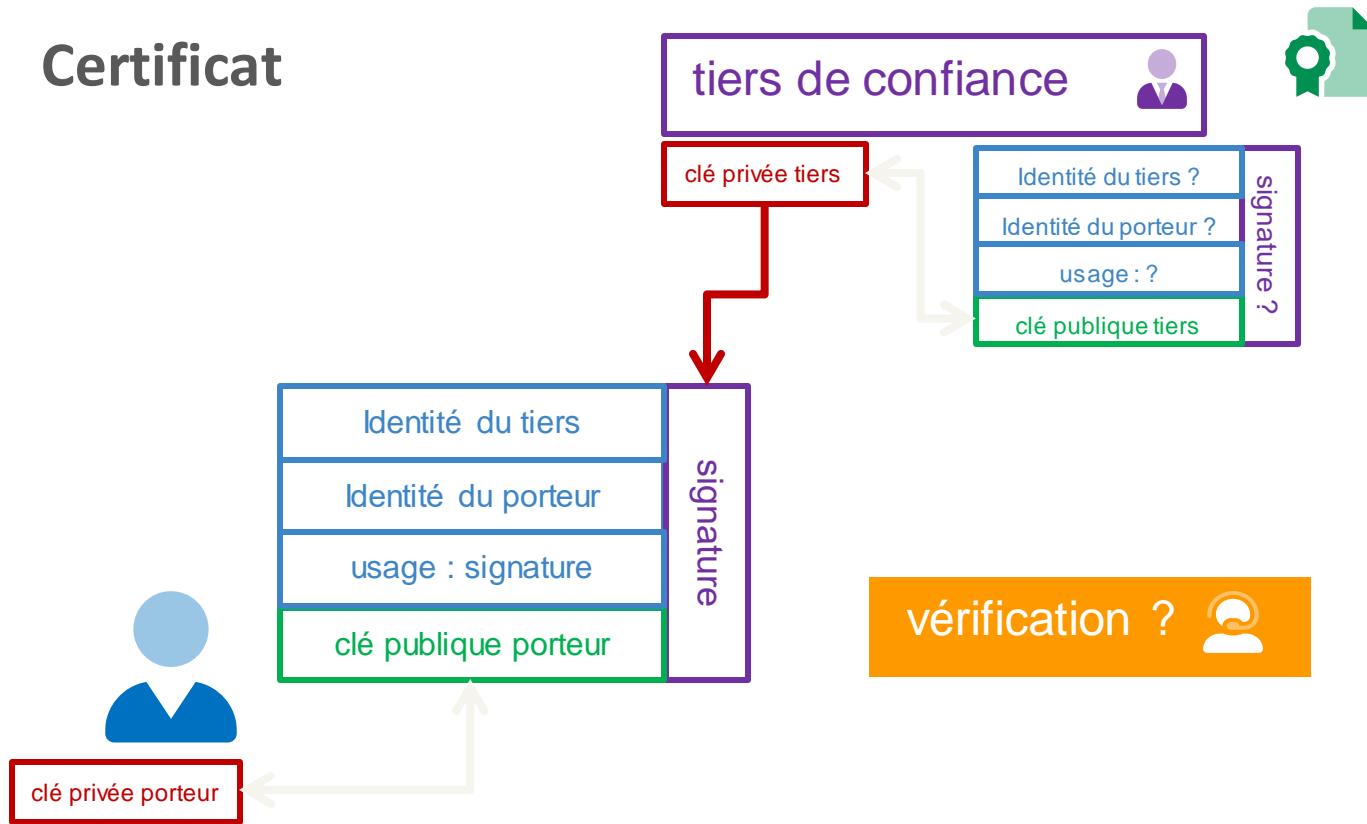
Certificat



Certificat

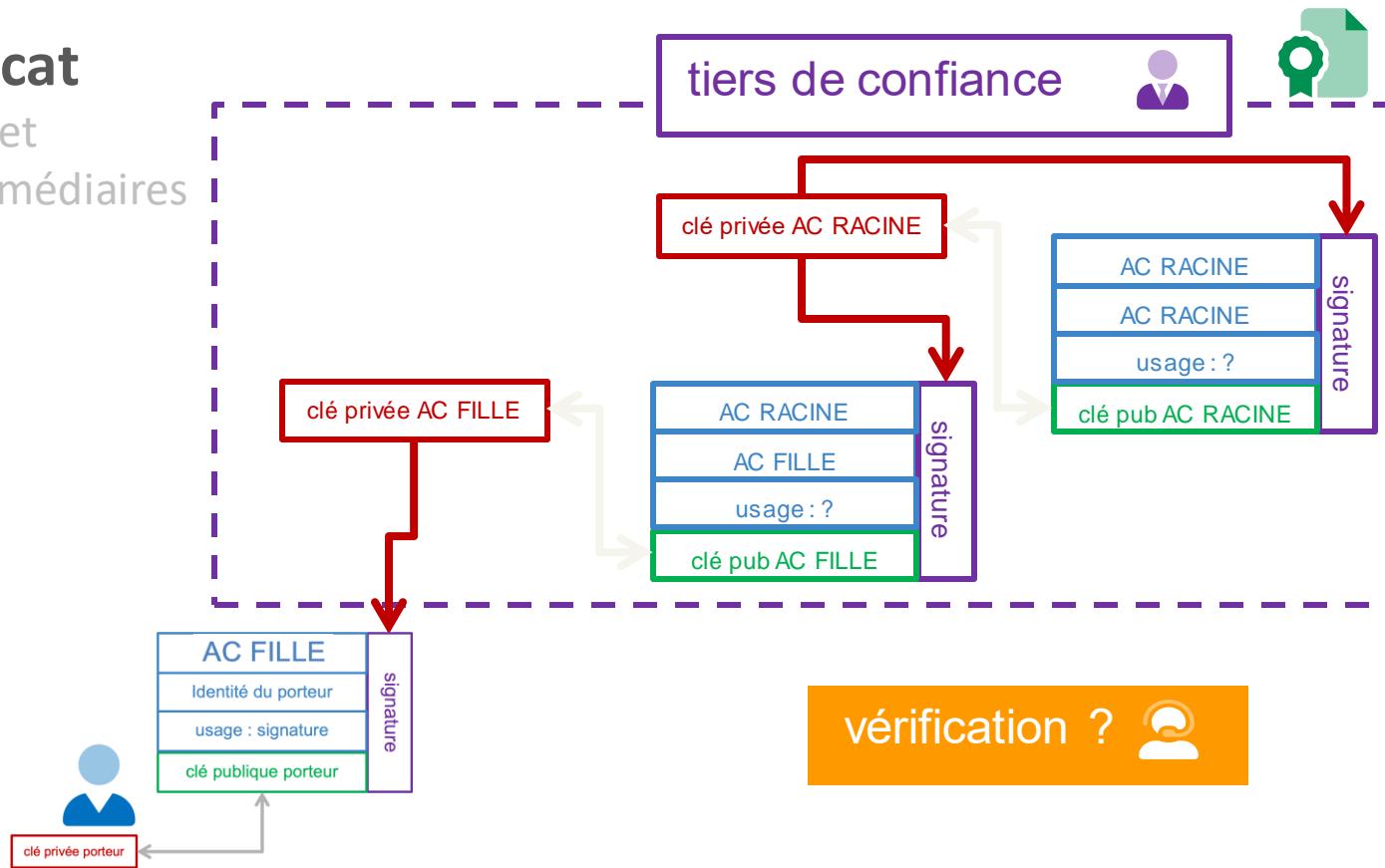


Certificat



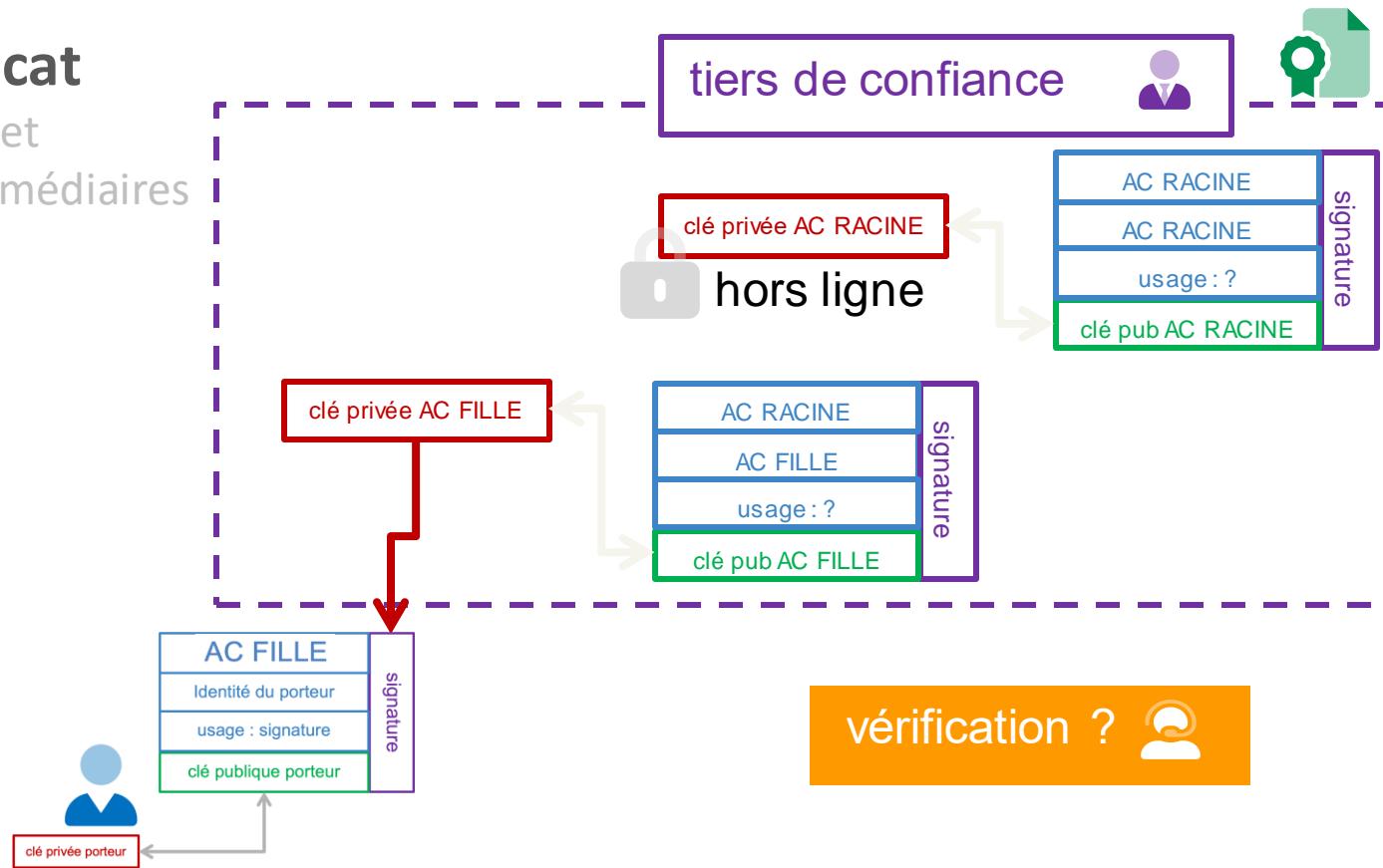
Certificat

Racines et
AC Intermédiaires



Certificat

Racines et
AC Intermédiaires



Certificat

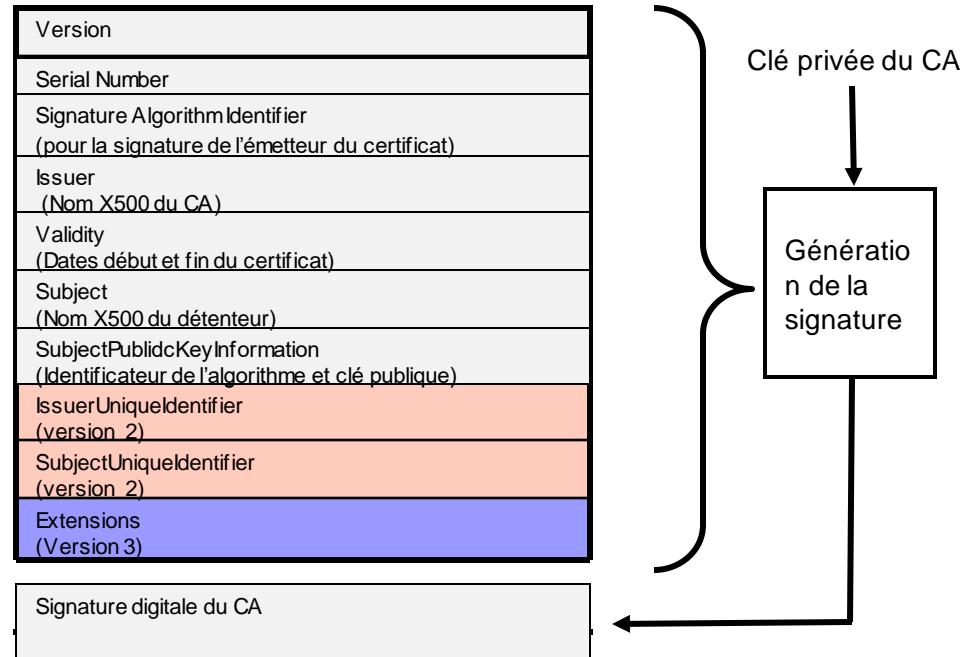
Gabarits des certificats X509 v3



```
$ openssl x509 -in pierre_dupond.crt -noout -text
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=FR, O=EPITA, OU=OOO2 12345678912345,
              CN=Cours SigElec
    Validity
        Not Before: Nov 24 17:48:27 2009 GMT
        Not After : Nov 23 17:48:27 2014 GMT
    Subject: CN=Pierre Dupond
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
          Modulus:
            00:d1:ea:2a:f8:b1:c6:86:fc:2c:0c:ed:c1:d4:0d:
            49:9c:bb:2b:3d:ce:58:84:ae:30:59:86:18:05:2b:
            f8:83:d6:bf:c0:ee:0d:5f:cb:1c:a0:9b:73:2c:ea:
            67:9b:f6:62:d4:07:33:a5:c4:60:3a:0f:73:85:44:
            98:75:c3:1d:6c:9e:fe:03:99:38:88:12:56:d8:eb:
            67:05:43:ae:c3:09:38:cc:9e:14:d5:a9:62:88:15:
            18:27:f8:8b:5d:ef:ac:cf:db:fb:ab:04:9b:eb:b4:
            27:0c:67:74:a7:7c:f9:46:6a:af:c1:7a:92:93:67:
            b5:3e:7a:c1:c7:27:a4:47:7b:0a:97:4c:49:c8:51:
            de:91:ce:c3:28:21:b3:d5:d2:d8:bd:38:96:e0:98:
            b4:ae:7f:72:56:a6:70:b3:71:fc:f7:e4:bd:6e:aa:
            ed:21:6a:b5:f2:bo:e2:94:54:44:0e:a6:80:30:af:
            15:9e:61:ae:47:cd:a9:cf:e8:7d:c7:09:fe:98:1c:
            22:a3:db:38:be:5b:66:dc:c3:52:74:9a:c8:89:de:
            44:3c:40:59:aa:0f:00:a0:09:8c:b3:f5:37:b4:76:
            4e:43:d1:99:24:3e:b5:6c:69:c4:1f:eb:b6:6e:2f:
            1d:5d:fb:66:f7:77:d4:16:ff:1b:a1:83:9a:ba:e6:
            1b:79
Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:FALSE
    X509v3 Authority Key Identifier:
        keyid:0C:88:C2:D1:10:E6:72:D0:7C:63:30:4A:E8:8D:3D:D6:9D:FB:BD
        :9C
        DirName:/C=FR/O=EPITA/OU=OOO2
        12345678912345/CN=Cours SigElec
        serial:8A:5D:41:8A:CA:49:B3:39
    X509v3 Subject Key Identifier:
        76:97:32:8F:65:62:33:8A:EA:8E:E3:C4:E5:2A:85:73:7E:7A:78:93
X509v3 Key Usage:
    Non Repudiation
Signature Algorithm: sha256WithRSAEncryption
    1c:80:dc:93:50:24:04:5a:dd:c9:6f:95:3d:78:4c:0f:5c:8e:
    79:ef:d9:f8:32:35:3f:f3:da:2f:ae:35:4d:c0:1b:17:f0:6a:
    3b:31:14:26:46:a3:61:ed:c4:dd:77:98:86:93:2d:65:78:e3:
    6d:21:70:23:b0:d3:ce:7:88:6d:83:ea:85:d6:d8:cf:77:54:
    6f:78:ee:9a:e9:db:4c:cd:3f:1f:20:b5:2f:bd:43:cd:22:fc:
    41:fd:52:ab:4b:a4:16:57:61:95:52:8b:9b:e2:69:c2:b8:ec:
    8f:da:2e:5b:ed:f4:d3:0a:23:4e:07:ff:db:e7:25:dd:38:12:
    30:d6:3c:9f:9e:e5:bc:99:8f:bc:df:ba:b0:d9:a0:82:05:a2:
    2b:b6:39:2c:7e:20:4b:b6:a7:b1:ae:ce:cf:06:ab:62:c9:b0:
    98:62:0d:94:b5:b9:d1:62:01:a4:4f:56:63:c1:89:67:4e:f8:
    85:2d:c7:6a:5f:b2:a1:3c:61:2a:b2:6c:2b:92:f3:d6:62:ac:
    69:84:3d:73:ef:ce:da:0b:a6:92:1d:2d:b5:60:04:59:b2:51:
    9b:5e:69:24:f5:91:29:b4:06:e2:19:7d:0c:12:b0:87:cc:41:
    84:36:7b:e1:df:bc:e4:29:9e:2d:b8:b3:70:74:66:f7:3d:a6:
    50:6a:0b:4c
```

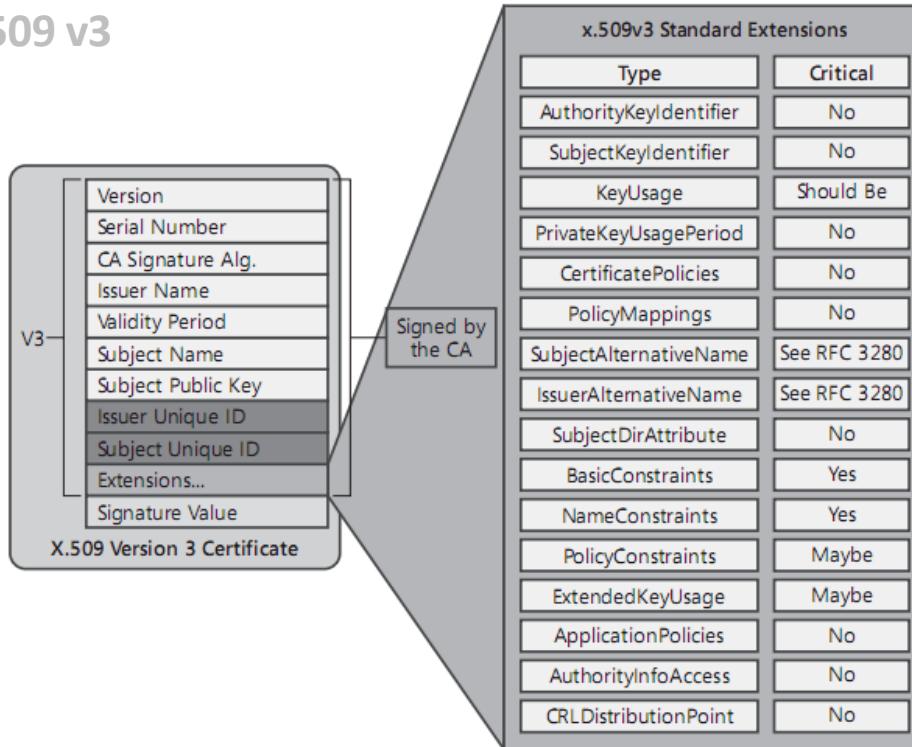
Certificat

Gabarits des certificats X509 v3



Certificat

Gabarits des certificats X509 v3



Certificat

Key Usages (RFC 5280)



```
KeyUsage ::= BIT STRING {
    digitalSignature          (0),
    nonRepudiation          (1), -- recent editions of X.509 have
                                -- renamed this bit to contentCommitment
    keyEncipherment           (2),
    dataEncipherment          (3),
    keyAgreement              (4),
    keyCertSign                (5),
    cRLSign                   (6),
    encipherOnly               (7),
    decipherOnly                (8)  }

id-kp-serverAuth            OBJECT IDENTIFIER ::= { id-kp 1 }
id-kp-clientAuth             OBJECT IDENTIFIER ::= { id-kp 2 }
id-kp-codeSigning             OBJECT IDENTIFIER ::= { id-kp 3 }
id-kp-emailProtection        OBJECT IDENTIFIER ::= { id-kp 4 }
id-kp-timeStamping            OBJECT IDENTIFIER ::= { id-kp 8 }
id-kp-OCSPSigning             OBJECT IDENTIFIER ::= { id-kp 9 }
```

Certificat

Gabarits des certificats X509 v3



Nom de l'émetteur _____

Organisation DIRECTION GENERALE DES IMPOTS

Nom AC SERVICES INDIVIDUELS IAS1 C

Numéro de série 02 06 45 B3 F5 63 DE 72 FB B1 15 CC 68 10 48 7A

Version 3

Algorithme de signature SHA-1 avec chiffrement RSA (1 2 840 113549 1 1 5)

Paramètres aucun

Non valide avant samedi 7 février 2009 18:09:51 HEC

Non valide après mardi 7 février 2012 18:09:51 HEC

Infos de clé publique _____

Algorithme Chiffrement RSA (1 2 840 113549 1 1 1)

Paramètres aucun

Clé publique 256 octets : C9 73 CB 76 B8 8A DF E6 ... ⓘ

Exposant 65537

Dimension de la clé 2048 bits

Utilisation de la clé Vérification

Signature 128 octets : 06 63 F3 08 9C E4 6B D7 ... ⓘ

Authentification (Vérification de signature)

Extension Utilisation de la clé (2 5 29 15)

Critique NON

Utilisation Signature numérique, Non répudiation

Signature électronique

Extension Contraintes élémentaires (2 5 29 19)

Critique OUI

Autorité de certification NON

IGC - PKI

IGC – Demande de certificat



IGC - PKI



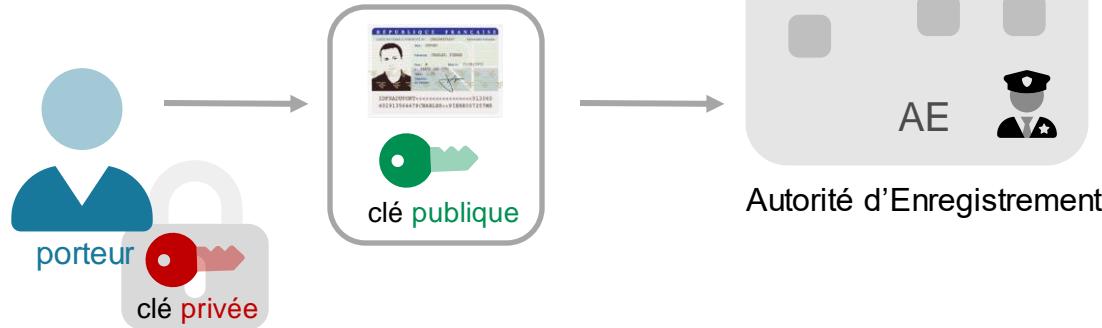
IGC – Demande de certificat



génération du bi-clés

IGC - PKI

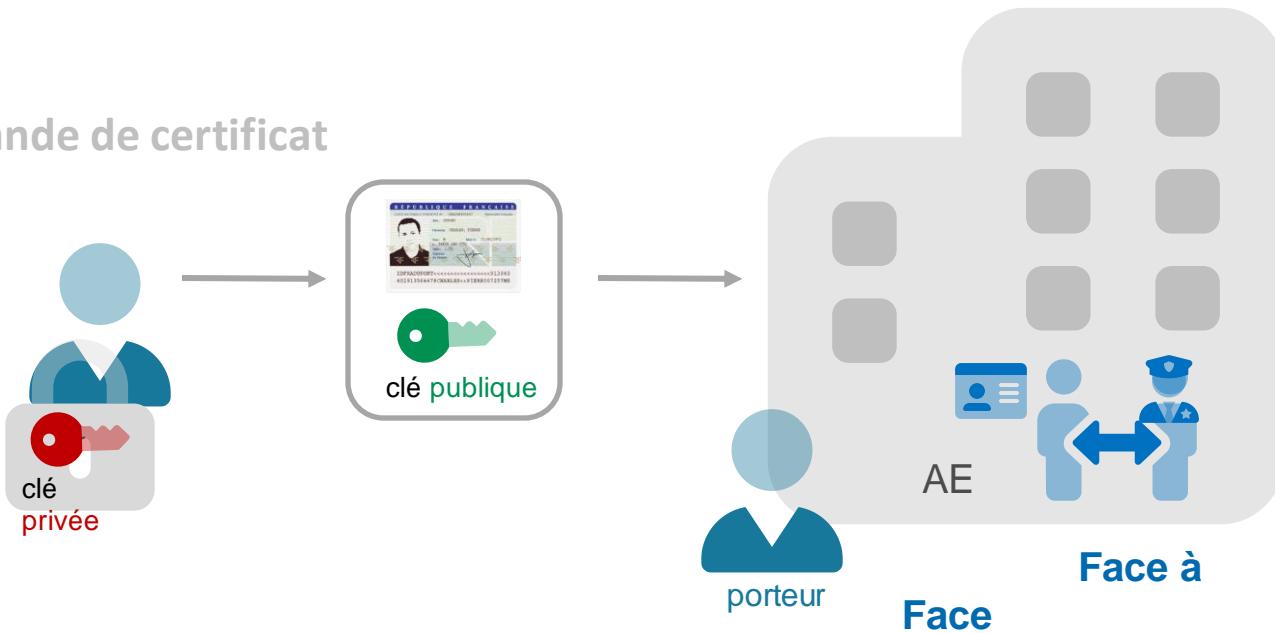
IGC – Demande de certificat



1. Sécurisation de la clé privée
2. Envoi de la clé publique et des informations d'identité

IGC - PKI

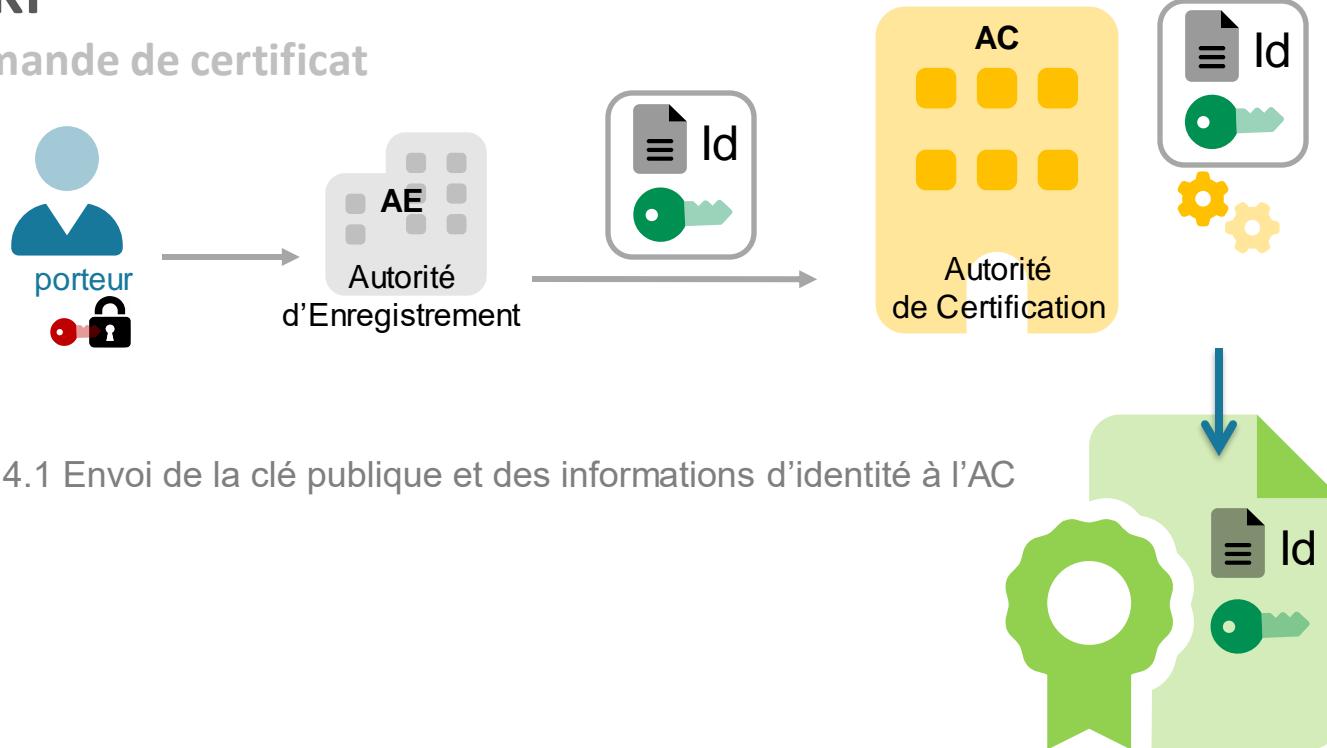
IGC – Demande de certificat



3. Vérification des informations d'identité du porteur par l'Autorité d'Enregistrement

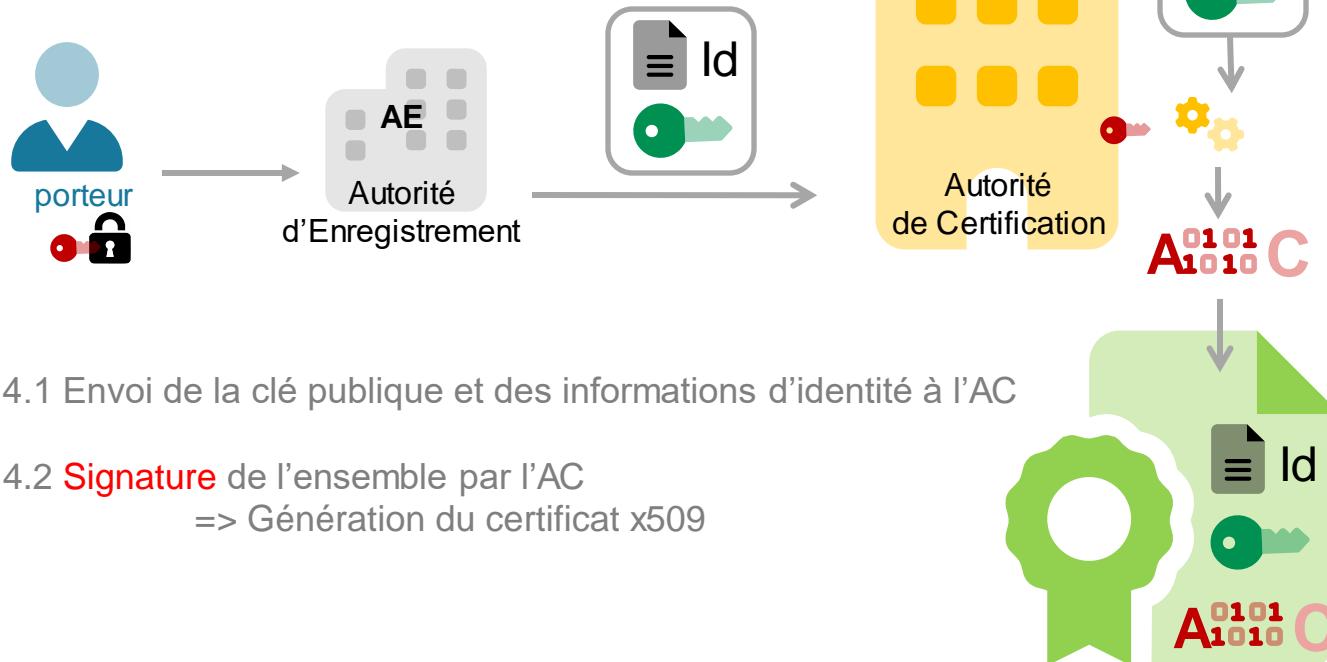
IGC - PKI

IGC – Demande de certificat



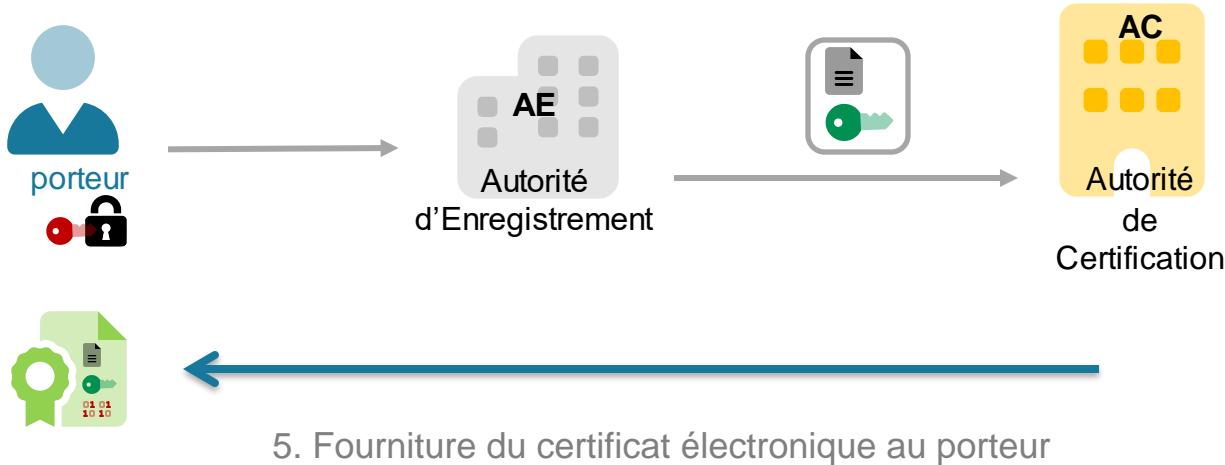
IGC - PKI

IGC – Demande de certificat



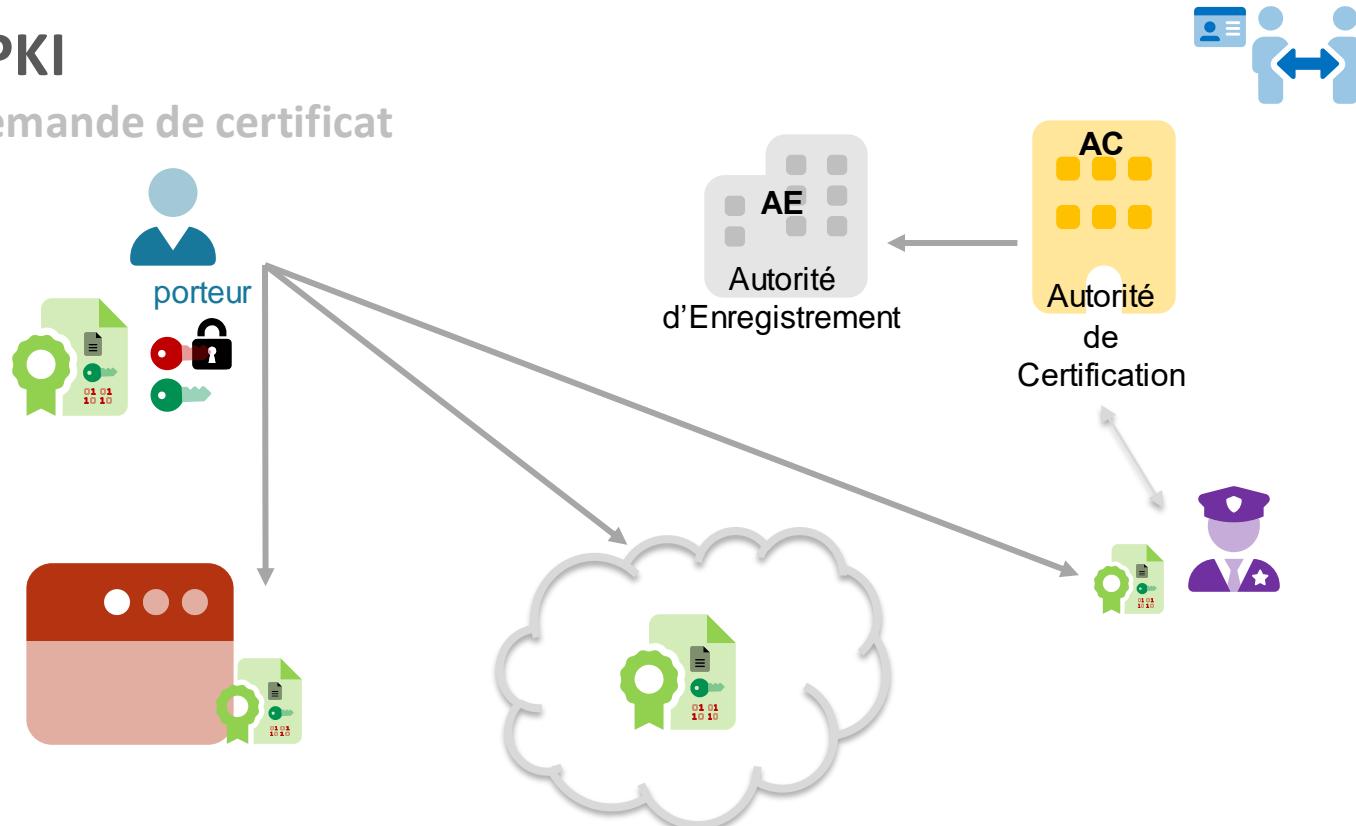
IGC - PKI

IGC – Demande de certificat



IGC - PKI

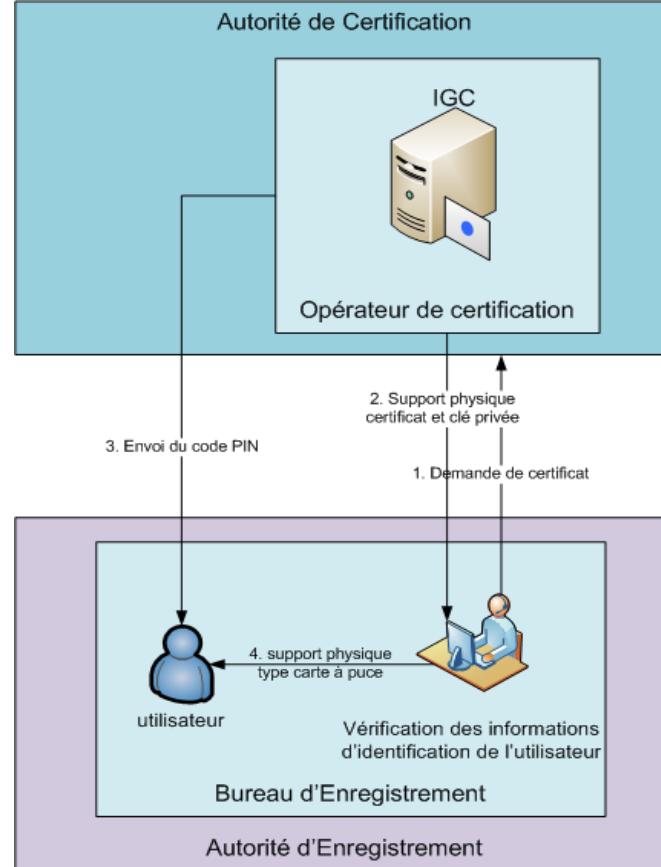
IGC – Demande de certificat



6. Utilisation des éléments

IGC - PKI

AC - OC - AE



Question ?

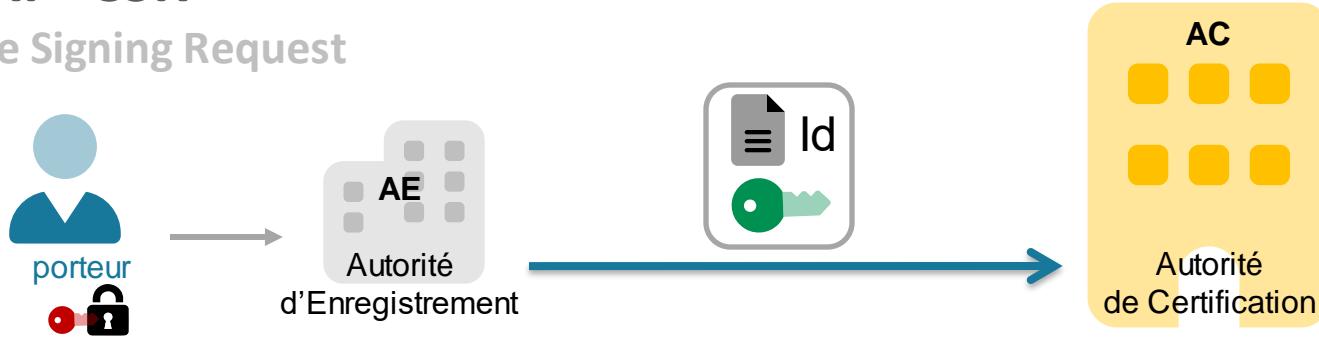


Une Autorité de Certification émettant des certificats qualifiés doit :

- Garantir que les clés de signature privées de l'AC stockées par le matériel cryptographique sont détruites lorsque que le dispositif n'est plus utilisé
- Vérifier par des moyens appropriés conformes au droit national l'identité de la personne à qui est délivré un certificat qualifié
- Conserver les informations du porteur aussi longtemps que nécessaire pour faire la preuve de la certification en justice
- Toutes ces réponses

IGC - PKI - CSR

Certificate Signing Request

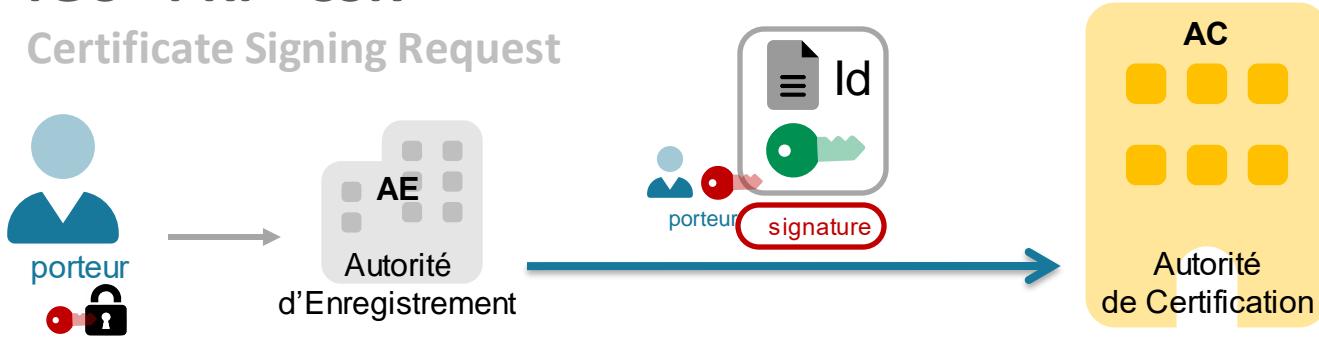


Comment assurer la preuve de **possession** de la **clé privée** du porteur ?

- cela permet d'assurer le principe de **non répudiation** de la signature
- très simple avec une seule requête

IGC - PKI - CSR

Certificate Signing Request



Comment assurer la preuve de **possession** de la **clé privée** du porteur ?

=> CSR est la spécification **PKCS#10 v1.7 - RFC 2986**

IGC - PKI - Horodatage

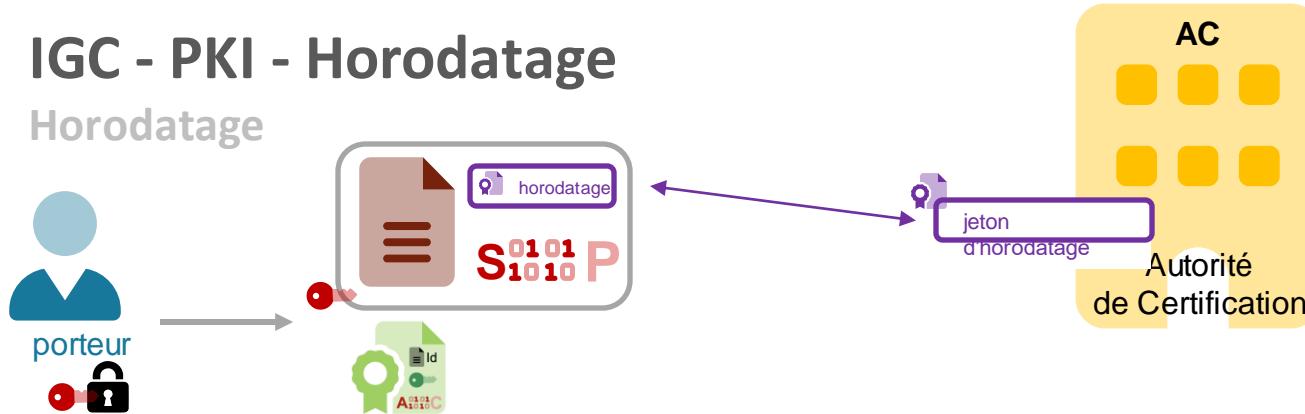
Question

41. En cas de compromission de sa clé privée, peut-on répudier une signature électronique qui n'a pas d'horodatage et n'a pas encore été vérifiée ?

- A. Oui, dans tous les cas
- B. Oui, uniquement pour les signatures créées après la révocation de la clé privée
- C. Non, jamais
- D. Non, sauf si le format de signature est XAdES-EPES

IGC - PKI - Horodatage

Horodatage



41. En cas de compromission de sa clé privée, peut-on répudier une signature électronique qui n'a pas d'horodatage et n'a pas encore été vérifiée ?

- A. Oui, dans tous les cas
- B. Oui, uniquement pour les signatures créées après la révocation de la clé privée
- C. Non, jamais
- D. Non, sauf si le format de signature est XAdES-EPES

IGC - PKI

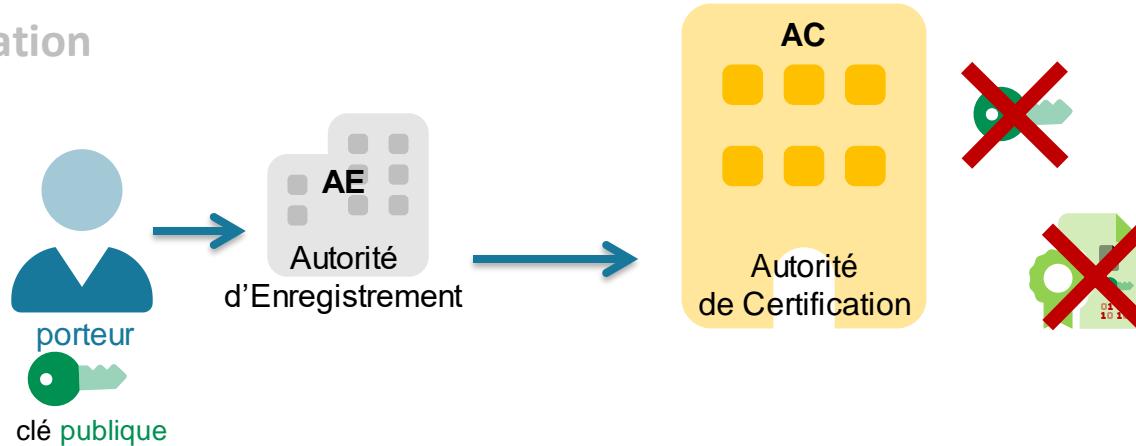
IGC – Révocation



- Porteur demandeur d'une révocation
- Compromission et/ou perte de la clé privée

IGC - PKI

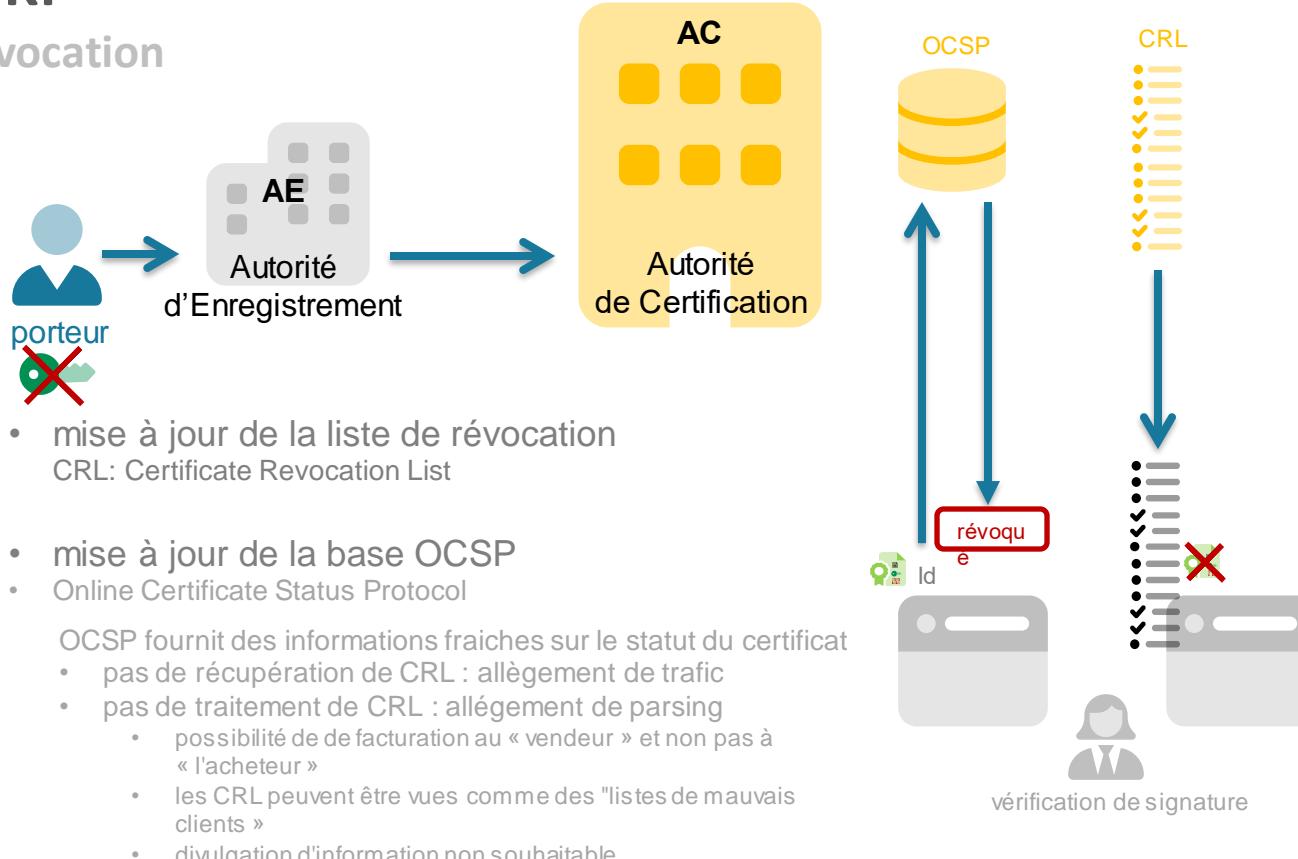
IGC – Révocation



- Demande de révocation par le porteur
- Validation de la demande de révocation par l'AE
- Révocation de la clé publique par l'Autorité de Certification

IGC - PKI

IGC – Révocation



La signature électronique sécurisée #4



F96DE8C227A259C87EE1DA2AED
57C93FE5DA36ED4EC87EF2C63A
AE5B9A7EFFD673BE4ACF7BE892
3CAB1ECE7AF2DCF7AE29A3DA44
F235A24C963FF0DF3CA3599A70
E5DA36BF1ECE77F8DC34BE129A
6CF4D126BF5B9A7CFEDF3EB850
D37CF0C63AA2509A76FF9227A5
5B9A6FE3D720A850D97AB1DD35
ED5FCE6BF0D138A84CF8DC34BE
129F8DC34B

La signature électronique sécurisée

sécurisée = avancée et/ou qualifiée



F96DE8C227A259C87EE1DA2AED
57C93FE5DA36ED4EC87EF2C63A
AE5B9A7EFFD673BE4ACF7BE892
3CAB1ECE7AF2DCF7AE29A3DA44
F235A24C963FF0DF3CA3599A70
E5DA36BF1ECE77F8DC34BE129A
6CF4D126BF5B9A7CFEDF3EB850
D37CF0C63AA2509A76FF9227A5
5B9A6FE3D720A850D97AB1DD35
ED5FCE6BF0D138A84CF8DC34BE
129F8DC34B

Complexité

- **la signature**

- Compréhension facile
- Mise en œuvre facile





- **la signature électronique**

- Compréhension difficile
- Mise en œuvre délicate

7e0950bb938539162d268b379595
44efb87b718950bf4721dd5c94f5f7
d12fc4efac9d9b50c81bbc1555c3d7
6610ef3080a354e60b625f5c50a23
a6bfd13ec024239ddcb47706c9a23
11fc38e37161e87501236542732797
2469b3985721cc0fea3b04047a9c5
b559e3471a736f5e4c7b473b2e86b1
b21dd8a829828d f8d6



- **la signature électronique sécurisée**

- Compréhension difficile
- Mise en œuvre très difficile



Statut légal d'une signature électronique

Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique

Le Premier ministre,

Sur le rapport de la garde des sceaux, ministre de la justice,

Vu le règlement (UE) n° 910/2014 du Parlement européen (eIDAS) et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

Vu l'article 1367 du code civil dans sa rédaction issue de l'article 4 de l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Article 1

La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique **qualifiée**.

Est une signature électronique **qualifiée** une signature électronique **avancée**, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de signature électronique **qualifié** répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat **qualifié** de signature électronique répondant aux exigences de l'article 28 de ce règlement.

Règlement eIDAS

Périmètre

Le Règlement « eIDAS » n° 910/2014 du 23 juillet 2014 a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

Le règlement eIDAS concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE. L'ANSSI est l'un des organismes nationaux chargés de la mise en œuvre de ce règlement.



[https://www.ssi.gouv.fr/entreprise/reglementation/
confiance-numerique/le-reglement-eidas/](https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/)

Règlement RGS

Pour les Autorités Administratives

- **RGS 2.0**

« Règles auxquelles les systèmes d'information mis en place par les **autorités administratives** doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs ».



Contexte légal

RGS

- RGS 2.0

Documents applicables concernant l'utilisation de certificats électroniques

 RGS A1 PDF - 453.6 ko Règles relatives à la mise en oeuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques, version 3.0	 RGS A2 PDF - 1.3 Mo Politique de Certification Type « certificats électroniques de personne », version 3.0	 RGS A3 PDF - 1.1 Mo Politique de Certification Type « services applicatifs », version 3.0	 RGS A4 PDF - 458.8 ko Profils de certificats, CRL, OCSP et algorithmes cryptographiques, version 3.0	 RGS A5 PDF - 740 ko Politique d'Horodatage Type, version 3.0
--	--	---	--	--

Normalisation Européenne

CEN : Comité Européen de Normalisation – cen.eu
ETSI : European Telecommunications Standards Institute -
etsi.org

CWA : CEN Workshop Agreement
TS : Technical Specification
EN : European standard

- ETSI
 - EN 319 411-1 – AC non qualifiée
 - EN 319 411-2 – AC qualifiée
 - EN 319 122 – CAdES (CMS)
 - EN 319 132 – XAdES (XML)
 - EN 319 142 – PAdES (ISO-32000 / PDF)
- CEN
 - CWA 14167 : Trustworthy systems / PP des HSM
 - CWA 14169 : PP SSCD
 - CWA 14170 : Application de création de Signature électronique
 - CWA 14171 : Application de vérification de Signature électronique

Entités et vocabulaire

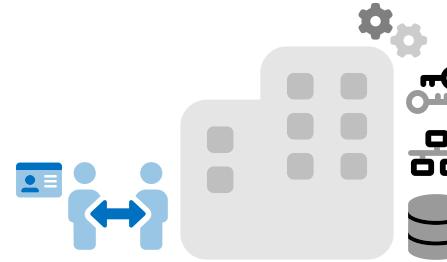
les termes et leurs synonymes

- AE et AC
 - PSCe – PSCo – TSP
- HSM – SSCD – QSCD – Carte à puce

On entend par **SSCD** [Secure-Signature-Creation Device] ou **QSCD** [Qualified-Signature-Creation Device] un Dispositif Sécurisé de Création de Signature. Un SSCD correspond à une « carte à puce » contenant un crypto-système hardware sécurisé, ou encore à un **HSM** (Hardware Security Module), ou encore un « **Secure Element** » ou **TPM** (Trusted Platform Module) dans un smartphone ou sur une carte mère d'ordinateur.



- eIDAS - RGS 2.0
 - eIDAS : Délivrance de certificats qualifiés - Audit ETSI 319 401 / 411-1&2 / 412
 - RGS : Délivrance de certificats qualifiés - Audit RGS – Annexes A2 / A3 / etc.



EU Trusted List

26 PSCe - PSCo – TSP en France – Services diverses

Trusted List France Trust service providers	
Currently active trust service providers	
Agence Nationale des Titres Sécurisés	QCert for ESig QCert for ESeal AR24 QRDS
Caisse des dépôts et consignations	QCert for ESig CEGEDIM SA QCert for ESig QCert for ESeal
CertEurope	QCert for ESig QCert for ESeal QWAC
Certigna	QCert for ESig QCert for ESeal QWAC QTimestamp
Certinomis	QCert for ESig QCert for ESeal QWAC QTimestamp
ChamberSign France	QOpen for ESig QCert for ESeal
CLEARBUS	QTimestamp QRDS Conseil Supérieur du Notariat QCert for ESig QTimestamp
Cryptolog International	QCert for ESig QCert for ESeal QVal for QESig QPtes for QESig QVal for QESeal QPtes for QESeal QTimestamp
Docaposte ARKHINEO	QVal for QESig QPtes for QESig QVal for QFSeal QPtes for QFSeal
DOCUMENT CHANNEL	QRDS
Docusign France	QCert for ESig QCert for ESeal QTimestamp
Equisign	QRDS
Gendarmerie Nationale	QCert for ESig QCert for ESeal
Imprimerie Nationale	QOpen for ESig
Le Groupe La Poste	QTimestamp QRDS Lex Persona QTimestamp
Ministère de l'Intérieur	QCert for ESig QTimestamp
Ministère de la Justice	QCert for ESig
Ministères économiques et financiers	QCert for ESig
TESSI DOCUMENTS SERVICES	QRDS
VIALINK	QCert for ESig QCert for ESeal
Worldline France	QTimestamp
Yousign	QCert for ESig QCert for ESeal QTimestamp

Audit PSCo/TSP eIDAS - RGS



eIDAS

Evaluation de la conformité

The image displays a collage of screenshots from various ETSI EN 319 documents and a section from a computer security control document.

Top Left: A screenshot of a computer screen showing multiple windows of ETSI EN 319 documents. One window shows the title "ETSI EN 319 401 V2.3.1 (2021-05)" and another shows "ETSI EN 319 411-1 v122.pdf – Page 1 sur 52".

Top Right: A screenshot of a computer screen showing the title "ETSI EN 319 411-2 V2.2.2 (2018-04)" and the subtitle "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

Middle Left: A screenshot of a computer screen showing the title "ETSI EN 319 411-1 v122.pdf – Page 40 sur 52" and the subtitle "Electronic Signature Policy and security requirements for Trust Service Providers issuing Time-Stamp Part 1: General".

Middle Right: A screenshot of a computer screen showing the title "ETSI EN 319 421 V1.1.1 (2016-03)" and the subtitle "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamp".

Bottom Left: A screenshot of a computer screen showing the title "eidas_delivrance-certificats-transition-rgs_v1.1_anssi.pdf – Page 1 sur 13" and the subtitle "Agence nationale de la sécurité des systèmes d'information".

Bottom Right: A screenshot of a computer screen showing the title "Services de délivrance des certificats qualifiés de signature électronique, de cachet électronique et".

Bottom Center: A screenshot of a computer screen showing the title "6.5.5 Computer security controls".

Text:

OVR-6.5.5-01: The requirements REQ-7.4-01, REQ-7.4-02, REQ-7.4-03 shall apply.

NOTE: Requirements for the trustworthy systems can be ensured by CEN TS 419 261 [i.9] or to a suitable protection profile according to ISO/IEC 15408 [1].

In addition the following particular requirements apply:

GEN-6.5.5-02: Local network components (e.g. routers) shall be secured.

GEN-6.5.5-03: Local network components (e.g. routers) configurations shall be secured in accordance with the requirements specified by the TSP.

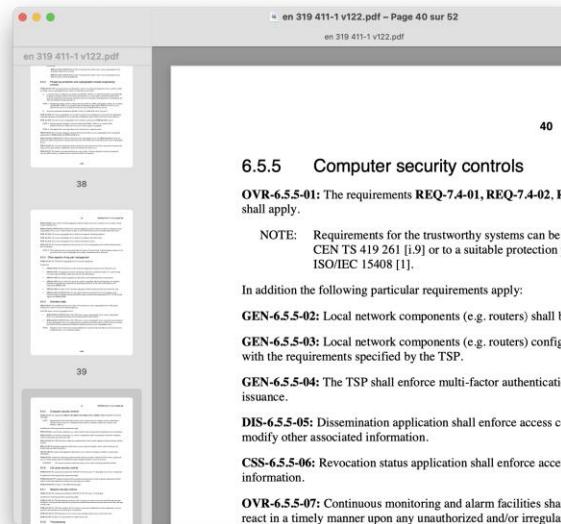
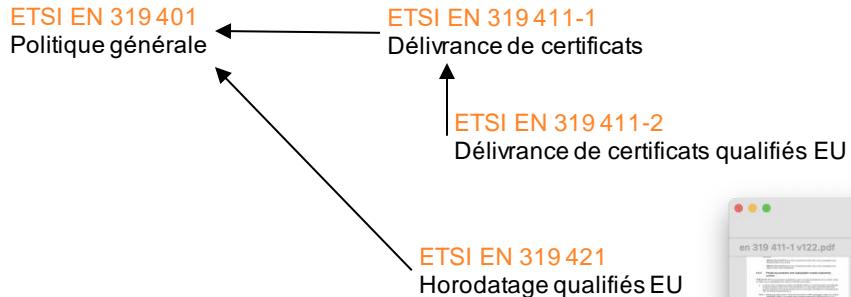
GEN-6.5.5-04: The TSP shall enforce multi-factor authentication issuance.

DIS-6.5.5-05: Dissemination application shall enforce access control and shall not modify other associated information.

CSS-6.5.5-06: Revocation status application shall enforce access control and shall not modify other associated information.

OVR-6.5.5-07: Continuous monitoring and alarm facilities shall be implemented so that the system reacts in a timely manner upon any unauthorized and/or irregular attempt.

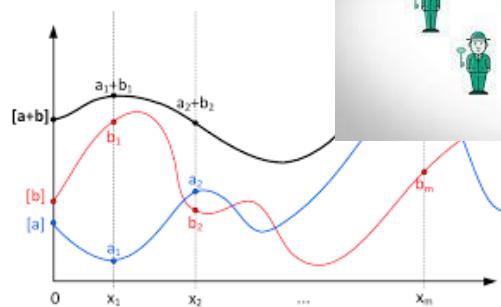
eIDAS



KC : Key Ceremony



Audit des parts de secrets



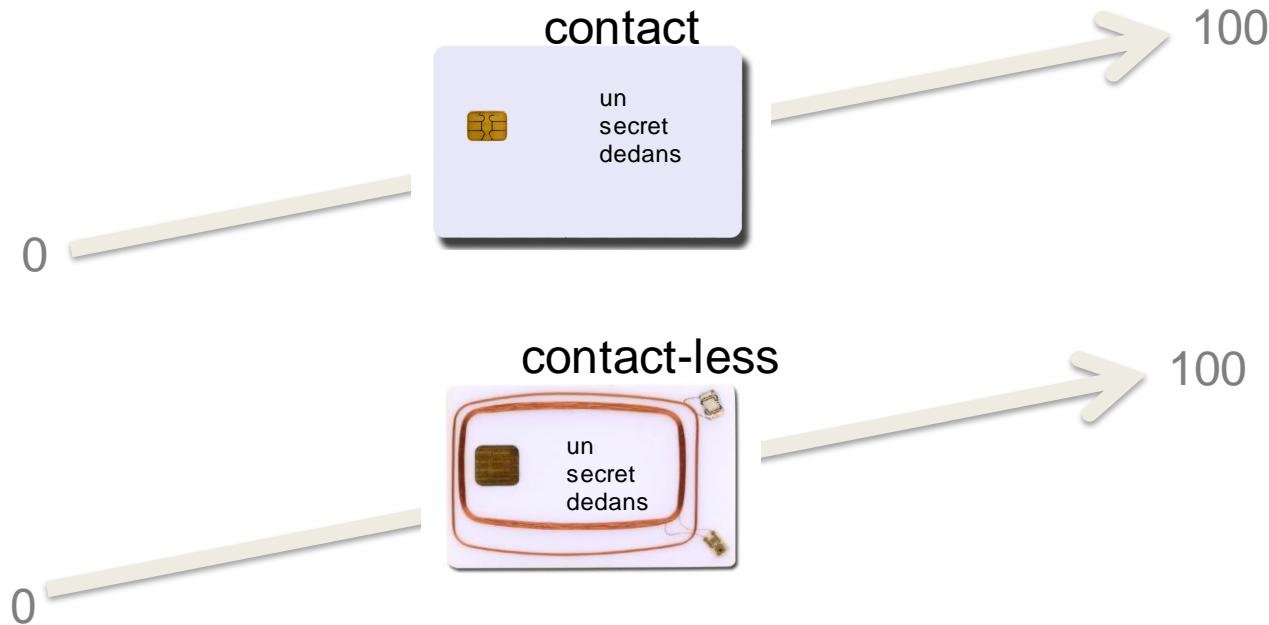
le dernier sanctuaire des petits secrets et autres clés privées ?



MultiApp ID IAS ECC Combi complies with the following international and European standards:

Java Card 2.2.1
Global Platform 2.1.1
ISO 7816 parts 1, 2, 3, 4, 5, 6, 8 & 9
ISO14443 type-A and type B
CEN TS 15480 part 1 and 2
E-SingK EN 14890 part 1 and 2
ICAO EAC V.1.1
ICAO Doc 9303 Sixth Edition
ICAO Machine Readable Travel Document ?
RF Protocol and Application Test Standard for e-Passport.
Pre-loaded applets in ROM
IAS ECC applet
ICAO applet
One time password applet
Mifare emulation upon request.
Security
MultiApp ID IAS ECC Combi includes multiple hardware and software countermeasure against various public & non-public attacks as:
Side channel attacks (SPA, DPA, Timing attacks etc)
Invasive attacks
Advanced fault attacks.

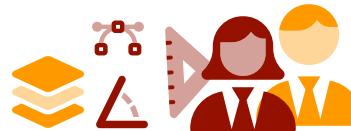
Attention : « c'est (pas) sécurisé » ne veut rien dire



Voilà ... c'est fini !

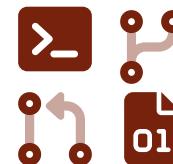
Ingénieur(e)s

- scientifiques
- design (capacité à concevoir)



Code

- préhistoire
- tout à inventer



Stage

- pas très grave
- management

1^{ère} page du rapport le 1^{er} jour + répétitions

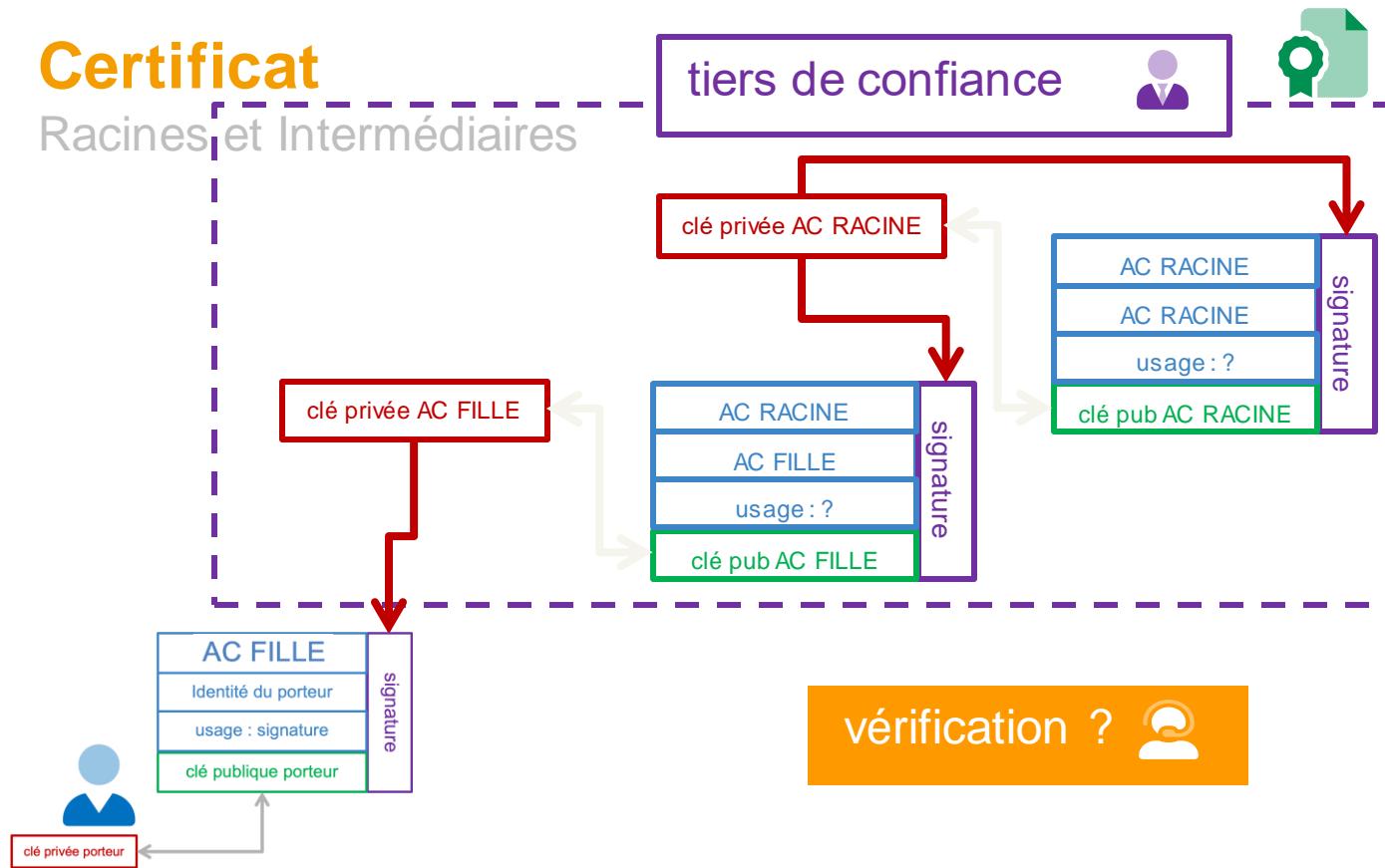




Stelau
Hack different.

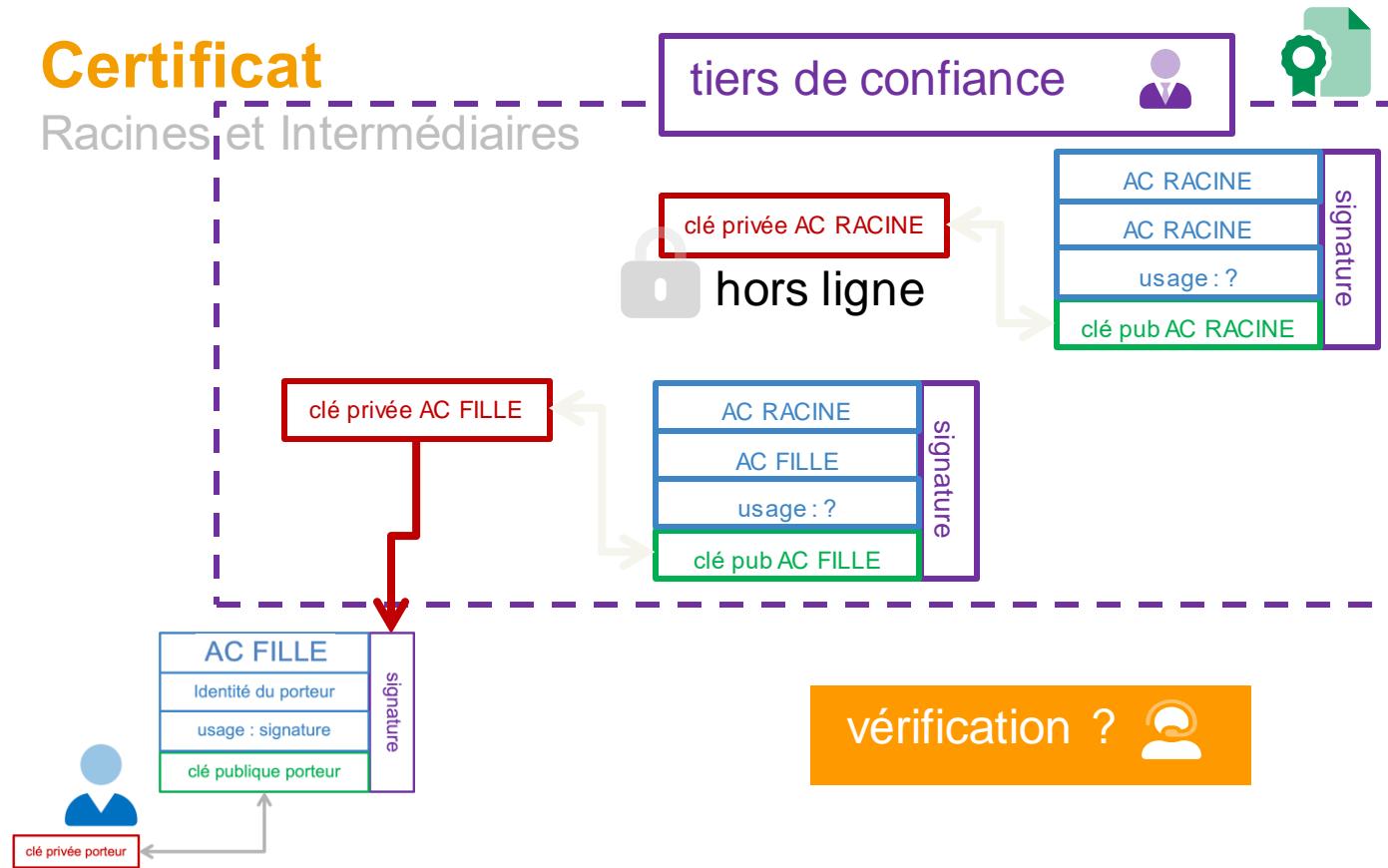
Certificat

Racines et Intermédiaires



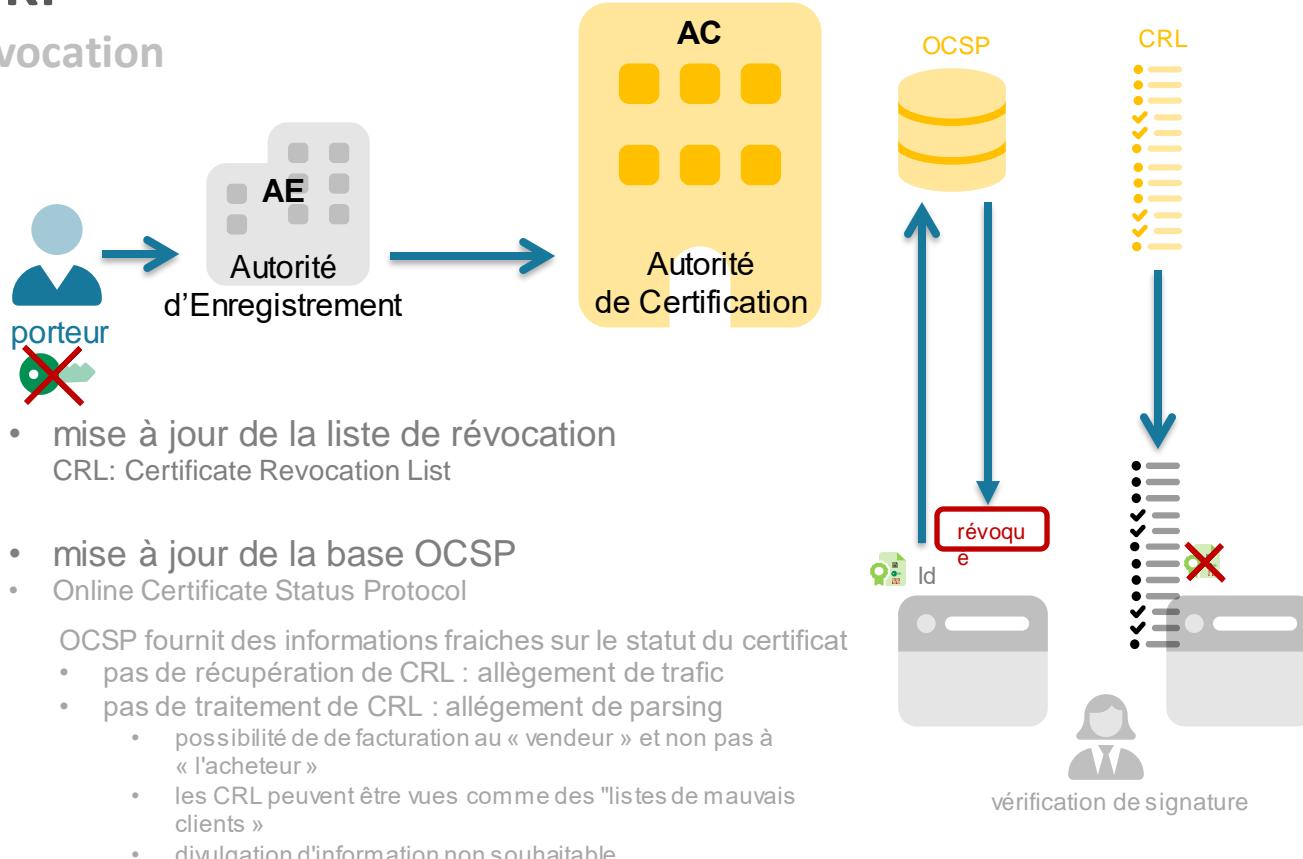
Certificat

Racines et Intermédiaires



IGC - PKI

IGC – Révocation



Règlement eIDAS

signature

Article 25

Effets juridiques des signatures électroniques

1. L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.
2. L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.
3. Une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les autres États membres.

Article 26

Exigences relatives à une signature électronique avancée

Une signature électronique avancée satisfait aux exigences suivantes:

- a) être liée au signataire de manière univoque;
- b) permettre d'identifier le signataire;
- c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et
- d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Règlement eIDAS

à distance

Article 24

Exigences applicables aux prestataires de services de confiance qualifiés

1. Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie, par des moyens appropriés et conformément au droit national, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié.

Les informations visées au premier alinéa sont vérifiées par le prestataire de services de confiance qualifié directement ou en en ayant recours à un tiers conformément au droit national:

- a) par la présence en personne de la personne physique ou du représentant autorisé de la personne morale; ou
- b) à distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfont aux exigences énoncées à l'article 8 en ce qui concerne les niveaux de garantie substantiel et élevé; ou
- c) au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a) ou b); ou
- d) à l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité.

Règlement eIDAS

remote signing

- (52) La **création de signatures électroniques à distance**, système dans lequel l'environnement de création de signatures électroniques est géré par un prestataire de services de confiance au nom du signataire, est appelée à se développer en raison de ses multiples avantages économiques. Toutefois, afin que ces signatures électroniques reçoivent la même reconnaissance juridique que les signatures électroniques créées avec un environnement entièrement géré par l'utilisateur, les prestataires offrant des services de signature électronique à distance devraient appliquer des procédures de sécurité spécifiques en matière de gestion et d'administration et utiliser des systèmes et des produits fiables, notamment des canaux de communication électronique sécurisés, afin de garantir que l'environnement de création de signatures électroniques est fiable et qu'il est utilisé sous le contrôle exclusif du signataire. Dans le cas de la création d'une signature électronique qualifiée à l'aide d'un dispositif de création de signature électronique à distance, les exigences applicables aux prestataires de services de confiance qualifiés énoncées dans le présent règlement devraient s'appliquer.

Examen ESLI

QCM

- pas de point négatif
- 40 min

Conception

- pertinence – granularité – cohérence - clarté
- 50-60 minutes

Barème

- 50/50
rééquilibrage possible suivant la meilleure moyenne