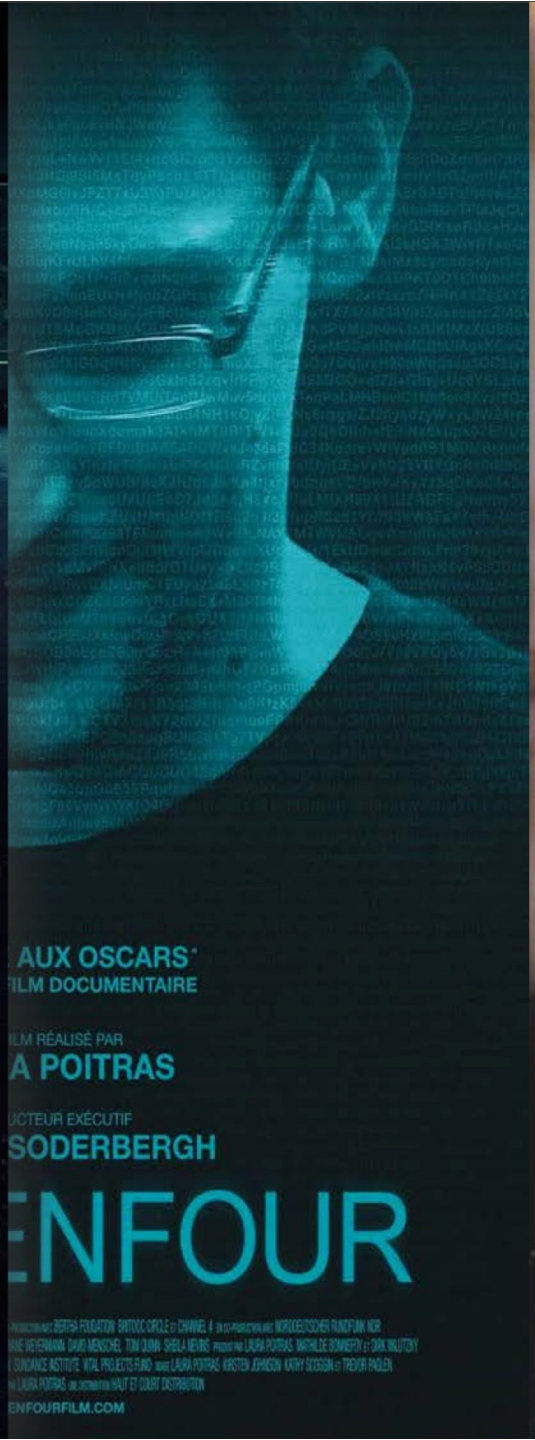

X GIBNEY OSCAR® WINNING DIRECTOR OF GOING CLEAR AND TAXI TO THE DARK SIDE
WORLD WAR 3.0
"A WHITE KNUCKLE THRILLER.
Clear, urgent, and positively terrifying at times."
-Peter Debruge, Variety
ZERO DAYS
COMING JULY 8


AUX OSCARS®
ILM DOCUMENTAIRE
A POITRAS
SODERBERGH
ENFOUR
ENFOURFILM.COM

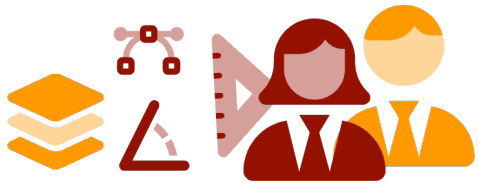
La signature électronique sécurisée


```
F96DE8C227A259C87EE1DA2AED5
7C93FE5DA36ED4EC87EF2C63AAE
5B9A7EFFD673BE4ACF7BE8923CA
B1ECE7AF2DCF7AE29A3DA44F235
A24C963FF0DF3CA3599A70E5DA3
6BF1ECE77F8DC34BE129A6CF4D1
26BF5B9A7CFEDF3EB850D37CF0C
63AA2509A76FF9227A55B9A6FE3
D720A850D97AB1DD35ED5FCE6BF
0D138A84CF8DC34BE129F8DC34B
```

Voilà … c’est fini !

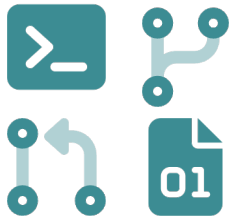
Ingénieur(e)s

- scientifiques
- design



Code

- préhistoire
- tout à inventer



Stage

- pas très grave
- management

1ère page du rapport le 1er jour + répétitions

Offre de stage

candidats à voir

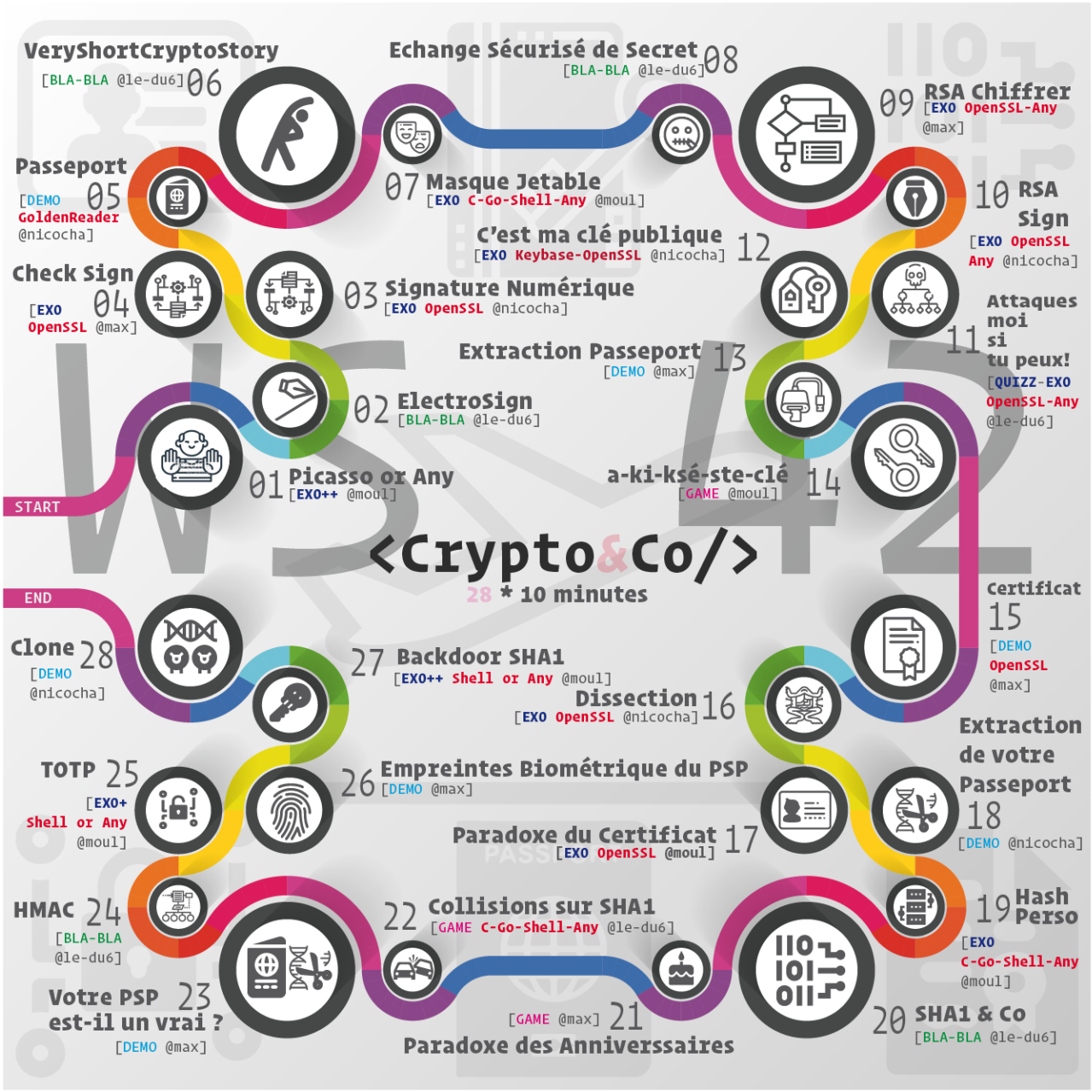
excellents stages

missions formatrices

rémunération +++

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU


VeryShortCryptoStory
[BLA-BLA @le-du6] 06
Echange Sécurisé de Secret
[BLA-BLA @le-du6] 08
09 RSA Chiffrer
[EXO OpenSSL-Any @max]
Passeport
[DEMO GoldenReader @nicocha] 05
07 Masque Jetable
[EXO C-Go-Shell-Any @moul]
10 RSA Sign
[EXO OpenSSL Any @nicocha]
C'est ma clé publique
[EXO Keybase-OpenSSL @nicocha] 12
Check Sign
[EXO OpenSSL @max] 04
03 Signature Numérique
[EXO OpenSSL @nicocha]
Attaques moi si tu peux!
[QUIZZ-EXO OpenSSL-Any @le-du6] 11
Extraction Passeport
[DEMO @max] 13
02 ElectroSign
[BLA-BLA @le-du6]
START
01 Picasso or Any
[EXO++ @moul]
a-ki-ksé-ste-clé
[GAME @moul] 14
<Crypto&Co/>
28 * 10 minutes
END
Certificat
15
[DEMO OpenSSL @max]
Clone 28
[DEMO @nicocha]
27 Backdoor SHA1
[EXO++ Shell or Any @moul]
Dissection 16
[EXO OpenSSL @nicocha]
Extraction de votre Passeport
18
[DEMO @nicocha]
TOTP 25
[EXO+ Shell or Any @moul]
26 Empreintes Biométrique du PSP
[DEMO @max]
Paradoxe du Certificat 17
[EXO OpenSSL @moul]
HMAC 24
[BLA-BLA @le-du6]
22 Collisions sur SHA1
[GAME C-Go-Shell-Any @le-du6]
19 Hash Perso
[EXO C-Go-Shell-Any @moul]
Votre PSP est-il un vrai ? 23
[DEMO @max]
[GAME @max] 21
Paradoxe des Anniverssaires
20 SHA1 & Co
[BLA-BLA @le-du6]

[01] - Picasso or Any Tool => Vous avez 8 minutes pour signer ces 4 trucs ? Démmerdez-vous !

[02] - ElectroSign => Qu'est-ce que la signature électronique ?

[03] - Signature Numérique => 10 minutes pour votre première signature de A à Z ?

[04] - Vérification de Signature Numérique => 10 minutes pour votre première vérification de signature ?

[05] - Signature du Passeport => Qui qui signe le passeport ?

[06] - VeryShortCryptoStory => RSA & Co

[07] - Masque Jetable => Le Cryptosystème Incassable : Masque Jetable / One Time Pad

[08] - Echange sécurisé de secret => Pas si facile

[09] - RSA pour chiffrer => Chiffrement Asymétrique

[10] - RSA pour signer => Chiffrement Asymétrique

[11] - Attaques-moi si tu peux ? => Chiffrement asymétrique attention aux usages

[12] - C'est ma clé publique à moi-Modèle Wanacry => Chiffrement Asymétrique

[13] - Extraction Passeport 1/2 => Comment y extraire vos informations

[14] - a-ki-ksé-ste-clé => Memory de bi-clés RSA

<Crypto&Co/>

Do Not Implement Crypto Yourself !

Dan Boneh

Si vous n'êtes pas d'accord ?

Venez vérifier avec votre passeport

Le WS-42 <Crypto&Co/> vous plongera dans les mécanismes de la sécurité cryptographique du passeport électronique au travers de 28 katas de 10 minutes chacun.

28 katas * 10 minutes

niveau requis: aucun

WS 42

[15] - Certificat Electronique => Récupérer un certificat depuis internet

[16] - Dissection du Certificat => Que contient le certificat ? pas-à-pas

[17] - Paradoxe du certificat de Signature => Pour signer, il doit être signé

[18] - Extraction Passeport 2/2 + BAC => 8 minutes pour extraire vos informations de votre passeport

[19] - Hash => Fabriques ton hash crypto en 8 minutes

[20] - SHA1 & Co => Les fonctions de hachage crypto

[21] - Paradoxe des Anniversaires => A combien veut-on jouer ?

[22] - Collisions sur SHA1 => Recherche de la plus grande collision sur SHA1 en 8 minutes

[23] - Votre passeport est-il un vrai ? => 8 minutes pour vérifier le signataire et l'intégrité de votre passeport

[24] - HMAC => Finauderie bien utile

[25] - TOTP => 8 minutes pour le réimplémenter

[26] - Empreintes biométriques du PSP => Où sont vos empreintes biométriques ?

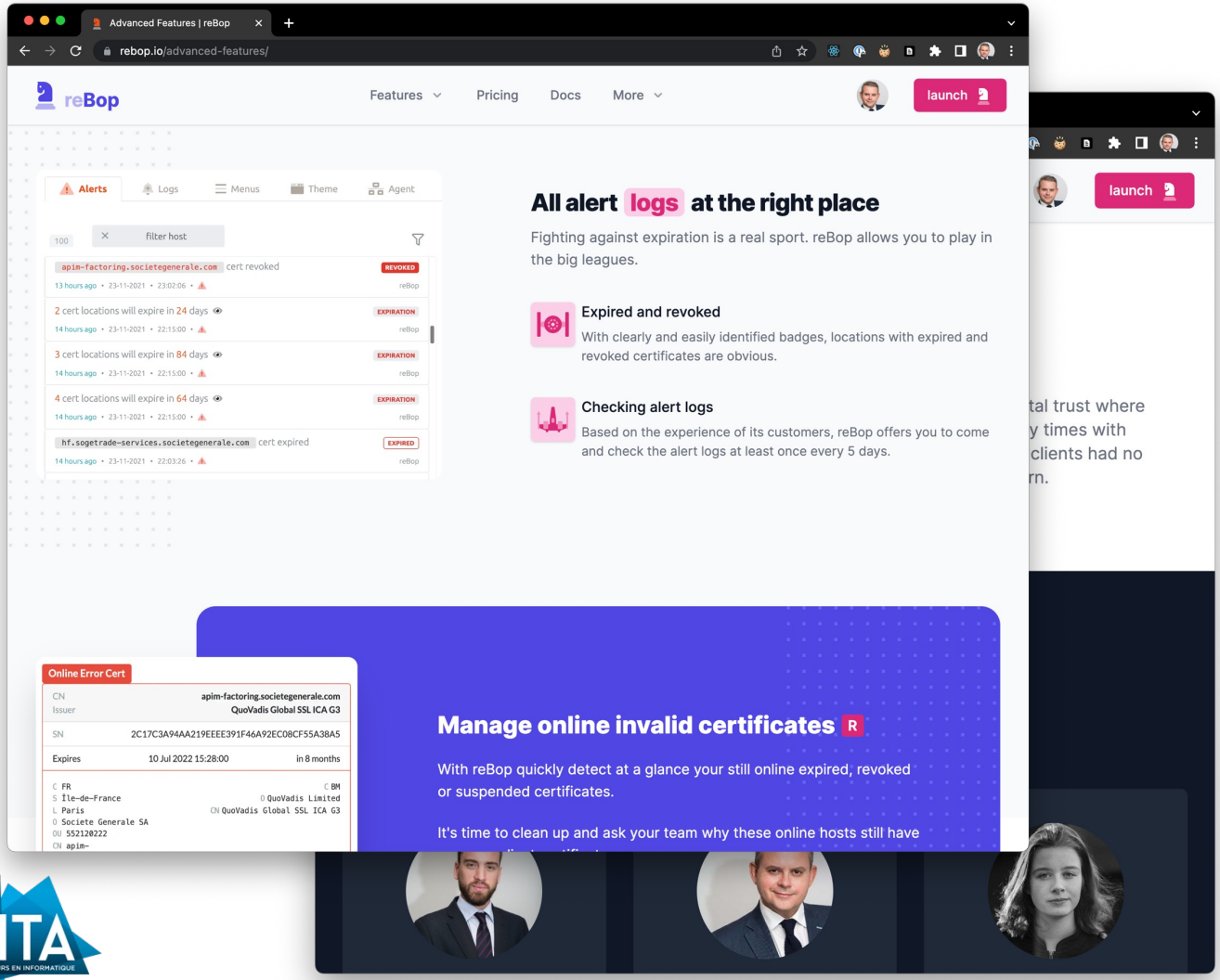
[27] - Backdoor SHA1 => Introduction d'une paille dans l'algo SHA1

[28] - PARAF et Clonage du passeport => 8 minutes pour cloner un passeport

reBop.io

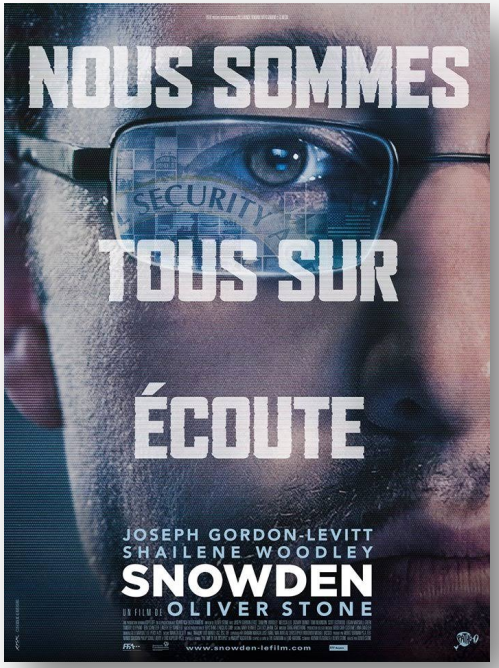
Certificate Lifecycle Managment

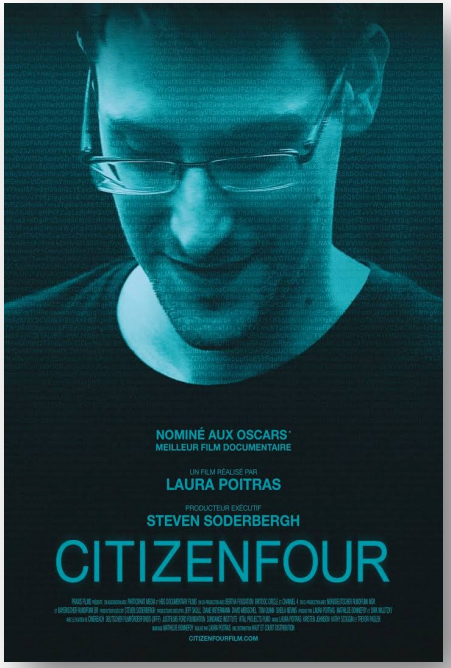
reBop



EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU





EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

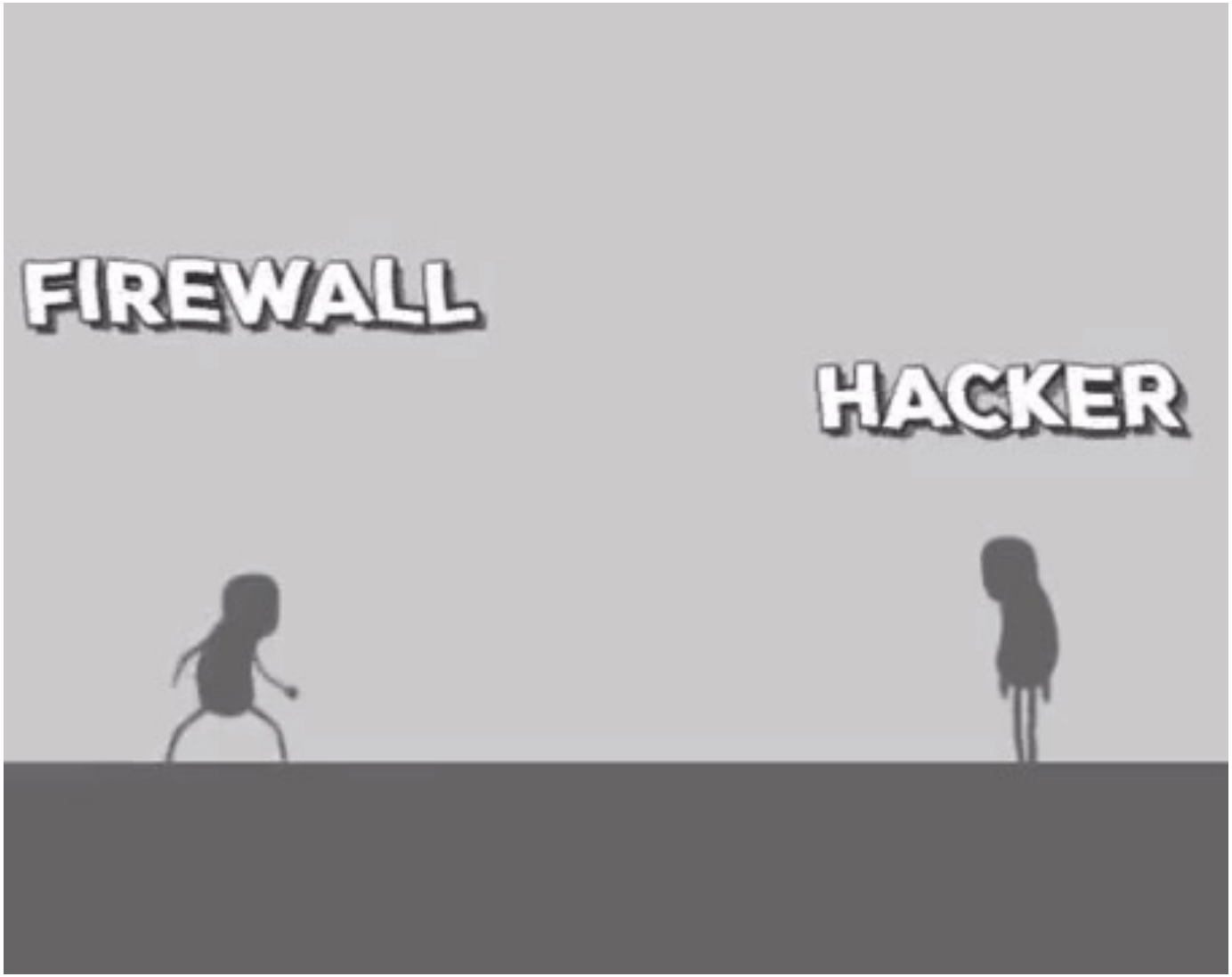
STELAU

le hacking

facile

le hacker

direct



Historique

rien n'a vraiment changé

il y a 26 ans,
le 11 aout 1996 un
certain **aleph_one** publie

"Smashing The Stack For Fun And Profit »

dans une revue de hackers
(phrack n°49).


Elias Levy

```
                    .oO Phrack 49 Oo.

                Volume Seven, Issue Forty-Nine

                        File 14 of 16

              BugTraq, r00t, and Underground.Org
                        bring you

     XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
     Smashing The Stack For Fun And Profit
     XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

                        by Aleph One
                    aleph1@underground.org

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

                        Introduction
                        ~~~~~~~~~~~~

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

   Basic knowledge of assembly is required.
memory concepts, and experience with gdb
We also assume we are working with a
system is Linux.
```

UaF + dF
RUST

```
testsc2.c
-------------------------------------------------------------------------------
char shellcode[] =
        "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
        "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
        "\x80\xe8\xdc\xff\xff\xff/bin/sh";

void main() {
   int *ret;

   ret = (int *)&ret + 2;
   (*ret) = (int)shellcode;

}
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
[aleph1]$ gcc -o testsc2 testsc2.c
[aleph1]$ ./testsc2
$ exit
[aleph1]$
-------------------------------------------------------------------------------


                        Writing an Exploit
                        ~~~~~~~~~~~~~~~~~~
                    (or how to mung the stack)
                    ~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Aujourd'hui

web => OWASP

CRLF Injection
CSV Injection by Timo Goosen, Albinowax
Catch NullPointerException
Covert storage channel
Deserialization of untrusted data
Directory Restriction Error
Doubly freeing memory
Empty String Password
Expression Language Injection
Full Trust CLR Verification issue Exploiting
Passing Reference Types by Reference
Heartbleed Bug
Improper Data Validation
Improper pointer subtraction
Information exposure through query strings in url by Robert Gilbert (amroot)
Injection problem
Insecure Compiler Optimization
Insecure Randomness
Insecure Temporary File

Buffer Overflo

débo

Depuis 1996, il existe de nombreuses parades …

… mais les techniques de hacking se sont aussi perfectionnées !

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

Table of Contents

- Introduction to Memory
  - X86 Assembly Language
  - Linkers & Loaders
  - **ELF Demonstration**
- Dynamic Linux Memory
- Introduction to Shellcode
- Smashing the Stack
  - **Exercise: Got Root?**
  - **Exercise: ret2libc**
  - Return Oriented Programming
- Advanced Stack Smashing
  - Defeating Stack Protection
  - Hacking ASLR
  - Hacking ASLR: Another Technique
- **Bootcamp Exercise One – Hacking MBSE**
- **Bootcamp Exercise Two – Brute Forcing ASLR**

A Note on OS Versions

- Why do we jump around OSs, some older and some newer?
  - To learn math, would you start with calculus?
  - Techniques are often the same; however, we must learn how to defeat controls
    - OS: ASLR, LFH, DEP
    - Compiler: Canaries, SafeSEH
    - Programs can opt-in or out of some controls
  - Windows 7/8 & 2008/2012 exploitation often involves overwriting C++ vtable pointers on the heap
    - Complex attacks requiring advanced programming skills

Winning the Lottery

- Making the right address guess is unlikely
  - Let us look at the registers when we hit a segmentation fault

ESP is pointing to our NOPs…

```
(gdb) info reg
eax            0x0      0
ecx            0x17     23
edx            0x0      0
ebx            0xbfb03cc0       -1078969152
esp            0xbfb03c90       0xbfb03c90
ebp            0x41414141       0x41414141
esi            0xb7f2dce0       -1208820512
edi            0x0      0
eip            0xbffff644       0xbffff644
```

```
x/6x $esp -16
0:   0x44444444   0xff0a0000   0x41414141   0xbffff644
0:   0x90909090   0x90909090   0xe983c929   0xd9eed9f4
0:   0x5bf42474   0x35137381   0x83c4b8b0   0xf4e2fceb
0:   0x5de0bb5f   0xe9d0d667   0xac5f3956   0xc4d0c31a
```


Searching for Trampolines

- What if we could find an instruction that would cause execution to jump to the address held in ESP?
  - jmp esp is "FF E4" in hex
  - call esp is "FF D4" in hex
- Wait, isn't everything randomized?
  - Not Always …
  - Let us discuss one method

SANS Security 660

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Cyber-attaque

modus operandi

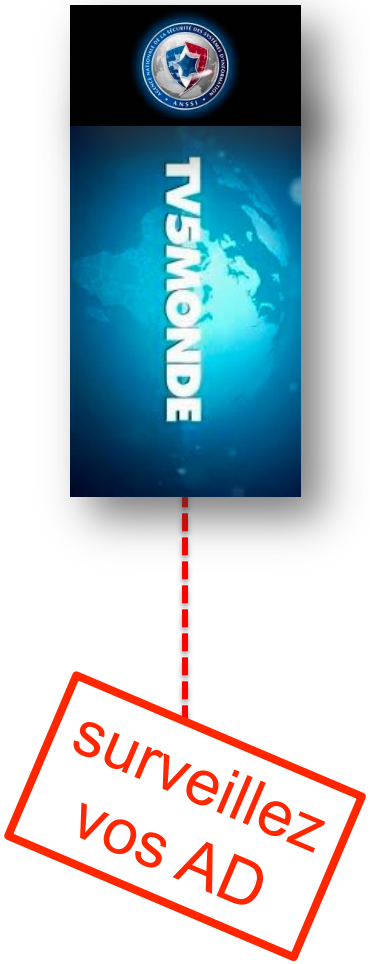
« *On a les attaques que l'on mérite !* »

ANSSI Luc Delsalle

L'attaquant se place toujours au niveau optimal de vos défenses.

Il ne cherche pas la difficulté si une faille évidente apparait.

Dans presque toutes les attaques les AD sont compromis.



Attaques actualités

OpenSSL

- buffer overrun
- X.509 certificate verification
- malicious email address to overflow
- 4 attacker-controlled bytes on the stack

```
183  183
184       -        if (written_out > max_out)
     184  +        if (written_out >= max_out)
185  185              return 0;
186  186
```

Pegasus & Co

- Asset Panda, eFORCE Software Suite, Resolver Investigations & Incident, CIS, Nuance, Adashi Systems, VCS Employee Scheduling, CrimeSoft, On Duty and IWS Law Enforcement.

Google Pixel TitanM Quarkslab

- attacking Titan M with Only One Byte
- fuzzing with AFL++ in Unicorn mode
- code execution on the chip

EPITA ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Attaques actualités

UBER

- vole de creds
- notif microsoft
- exploitant dit « non »
- message Whatspp => « oui »

MacronLeaks

- lundi : consigne de sensibilisation
- mardi : phishing + exploit

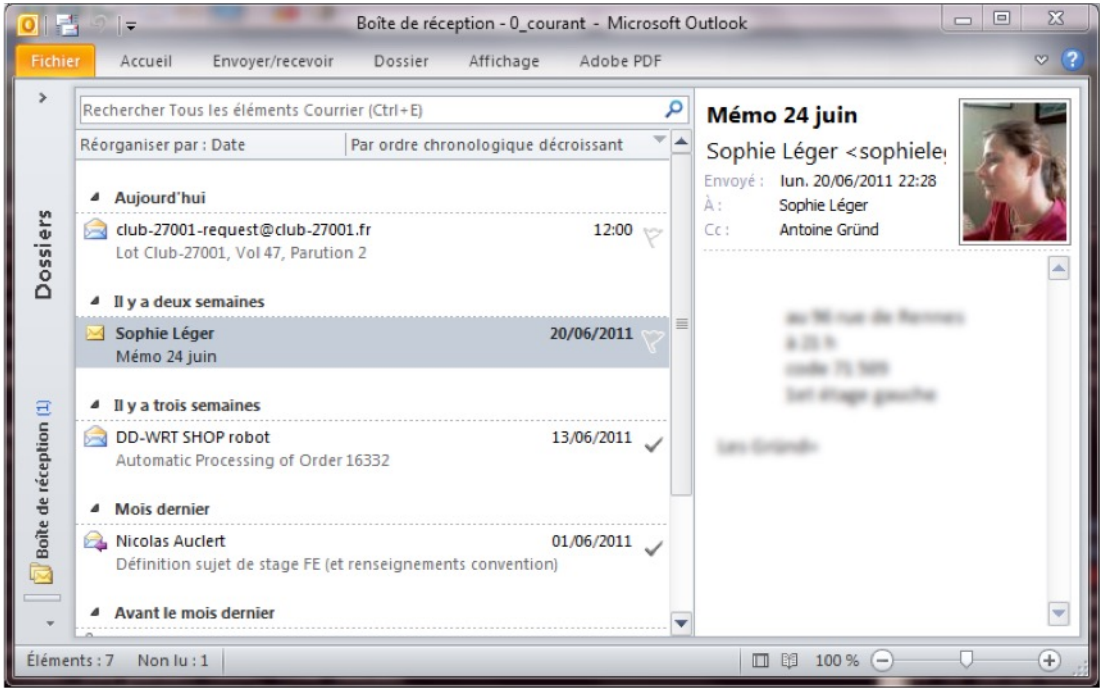
Ransomware

- chiffrement partiel
- en-têts + magic numbers
- bypass des EDR ☺

Le mail

- usurpation de l'adresse mail de mes proches
- usurpation de mon adresse mail
- usurpation de l'adresse mail de mes collaborateurs

Qui s'est préparé psychologiquement ?

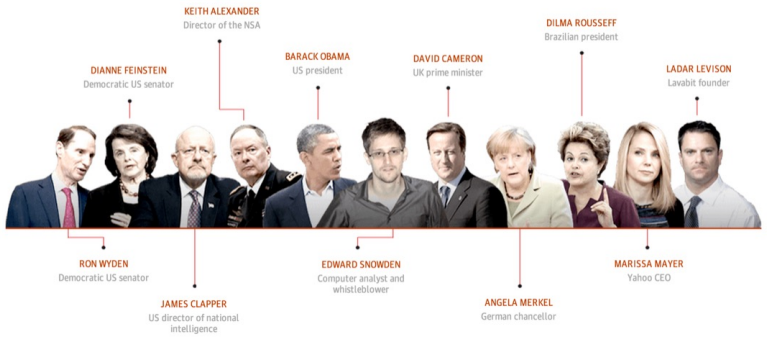


US-984XN

http://goo.gl/SNEXRo

2:17 Former CIA Director: 'We Kill People Based On Metadata'
www.youtube.com/watch?v=ZLX--i7EjzM
12 mai 2014 - Ajouté par DAHBOO77
More info at link: http://rt.com/usa/158460-cia-director-metadata-kill-people/

PRISM

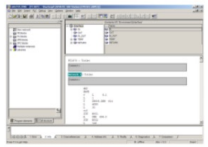


STELAU

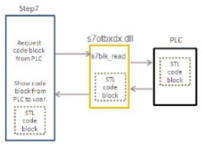
Stuxnet – Juin 2010

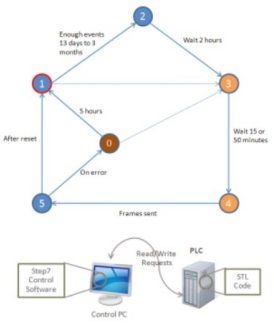
Un avant et un après Stuxnet ?

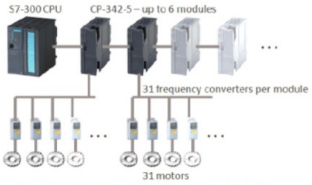
Objectif : ralentir le programme d'enrichissement nucléaire Iranien
Moyen : saboter le fonctionnement des centrifugeuses d'enrichissement
Cible : atteindre la centrale de *Bushehr* et les centrifugeuses nucléaires de *Natanz*
Prise en compte de 33 types de convertisseurs de fréquences de 2 fabricants par le protocole Profibus



Step7 et PCL avec s7otbxdx.dll





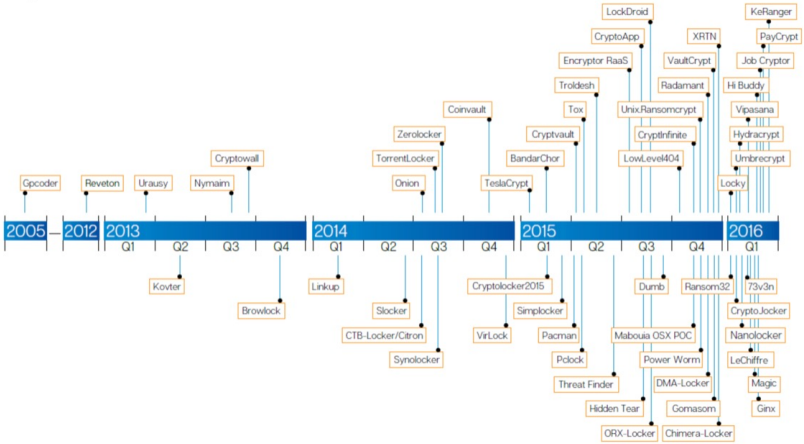


http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

STELAU

2016 année des ransomwares

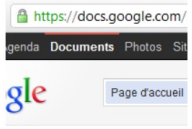
explosion des cas



STELAU

DigiNotar – Juillet-Août 2011

Affaire grave ou très grave



Objectif : politico-idéologico-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

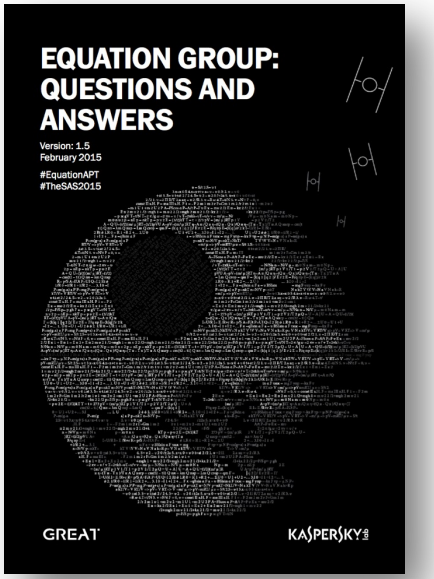
Conséquences: 500 certificats frauduleux fabriqués et un certificat *.google.com ayant permis l'espionnage d'utilisateurs Iraniens du 10 juillet au 29 aout 2011

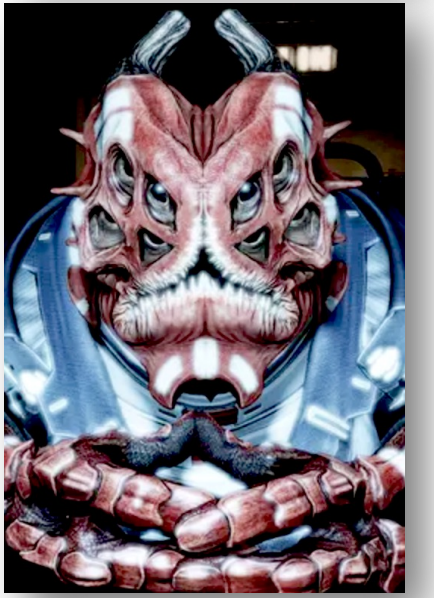
Correctifs / Réactions : MAJ de tous les navigateurs et OS
+ audits de 54 autorités de certification

STELAU

Equation Group

and the Shadow Brockers





PIXPOCKET

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[vv]  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 uninitialised 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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Outils NSA

suite et fin

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 (p 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, V 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
- **ENGLISHMANSDENTIST** sets Outlook Exchange WebAccess rules to trigger execut 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 Serv
- **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 domai
- **ESTEEMAUDIT** is an RDP exploit and backdoor for Windows Server 2003
- **ECLIPSEDWING** is an RCE exploit for the Server service in Windows Server 2008 an
- **ETRE** is an exploit for IMail 8.10 to 8.22
- **ETCETERABLUE** is an exploit for IMail 7.04 to 8.05

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

MS17-10

quand la NSA perd ses outils

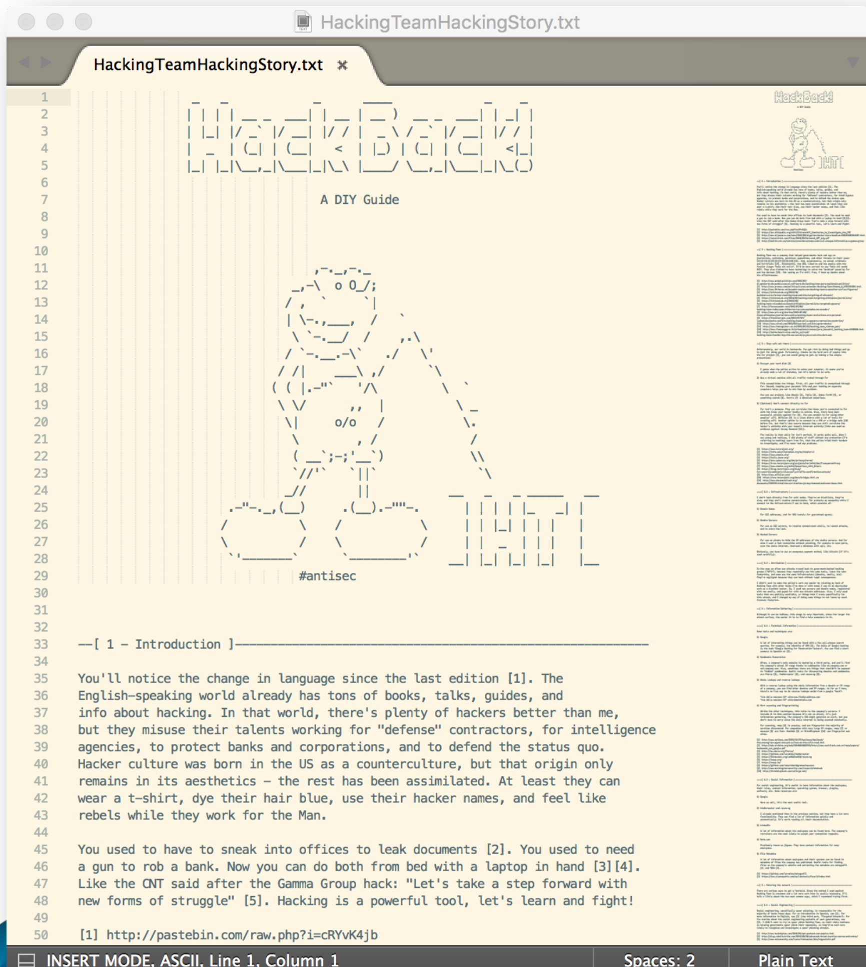
```
msf auxiliary(smb_ms17_010) > options

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
   RPORT      445              yes       The SMB service port (TCP)
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   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
```

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Hacking Team hacked

Phineas Fisher – avril 2016



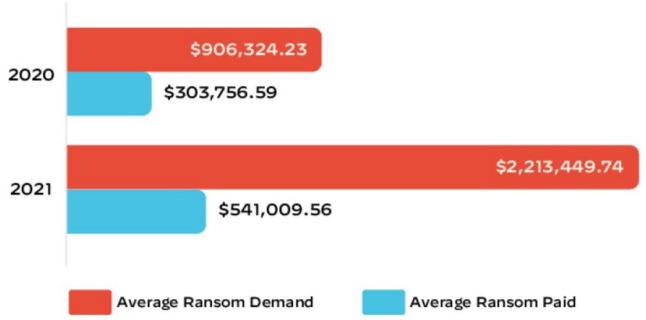
⇒ pas d'APT
⇒ pas d'aide mafieuse

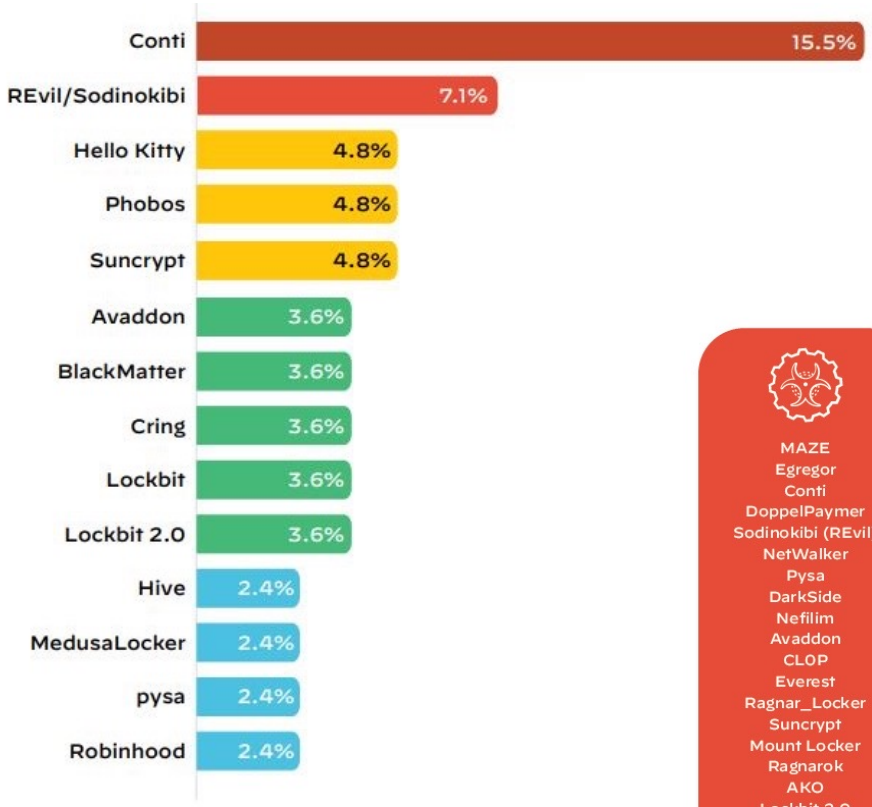
⇒ du travail d'orfèvre
⇒ de haut niveau
⇒ véritable ontologie
⇒ tout y est
⇒ une leçon
⇒ mieux qu'une formation

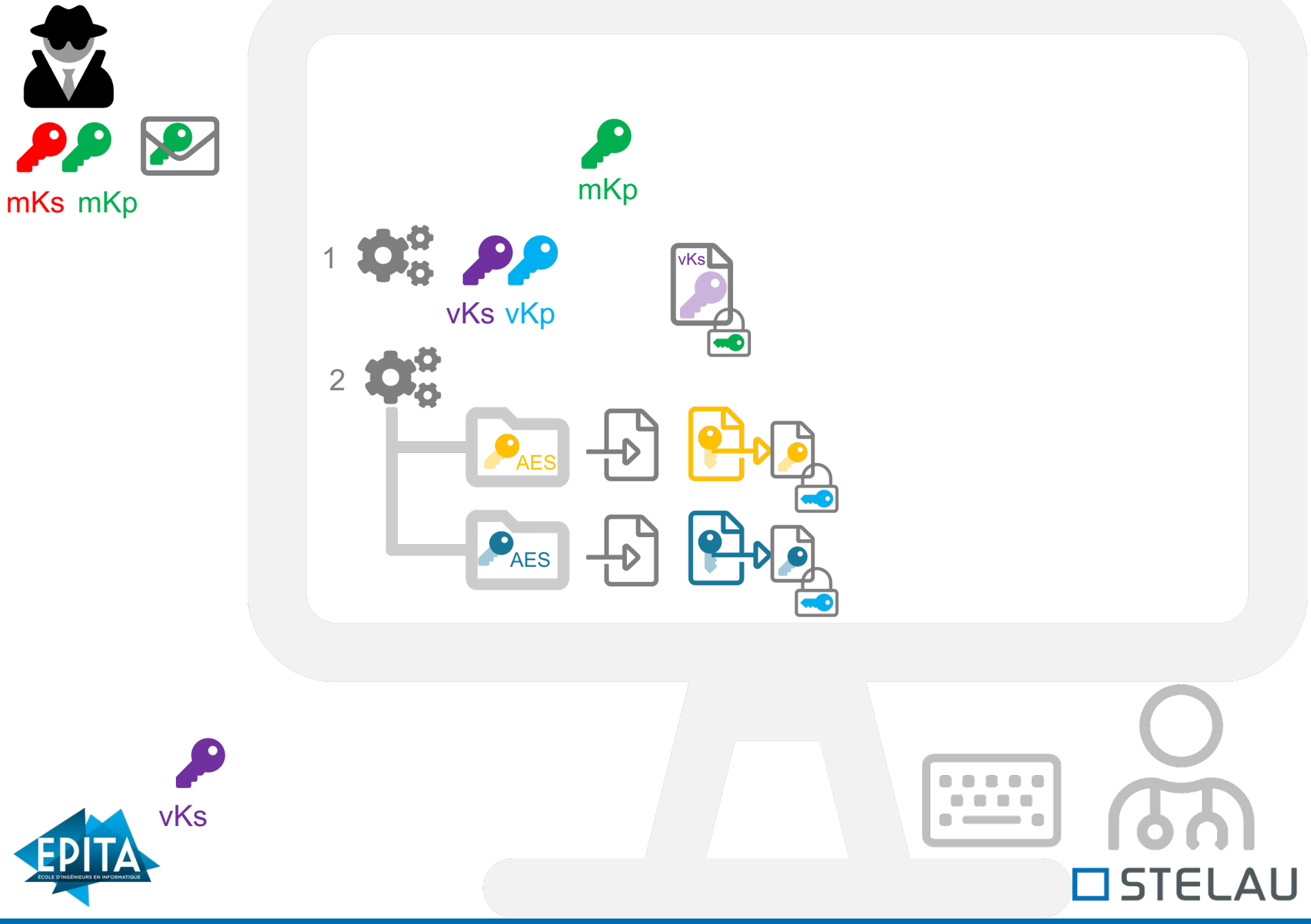
⇒ à lire ici :
http://pastebin.com/0SNSvyjJ

Ransomwares

Unit 42 - Latest Cyber Security Research
Palo Alto Networks






mKs mKp
mKp
1
vKs vKp
vKs
2
AES
AES
vKs

ELSI - jeudi matin 09:00-12:00

#1 : Hacking - Crypto 101

#2 : Crypto 101 - Signature - IGC

#3 : TP noté : OpenSSL + XAdES

#4 : Signature - IGC - Certificats

#5 : Loi - Textes - Règlements - Audits

#6 : Révisions + Examen

JEUDI 10 NOVEMBRE 2022

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

JEUDI 17 NOVEMBRE 2022

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

JEUDI 24 NOVEMBRE 2022

[EPITA] - TP Cours E... 09:00 12:00

JEUDI 1 DÉCEMBRE 2022

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

JEUDI 8 DÉCEMBRE 2022

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

JEUDI 15 DÉCEMBRE 2022

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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

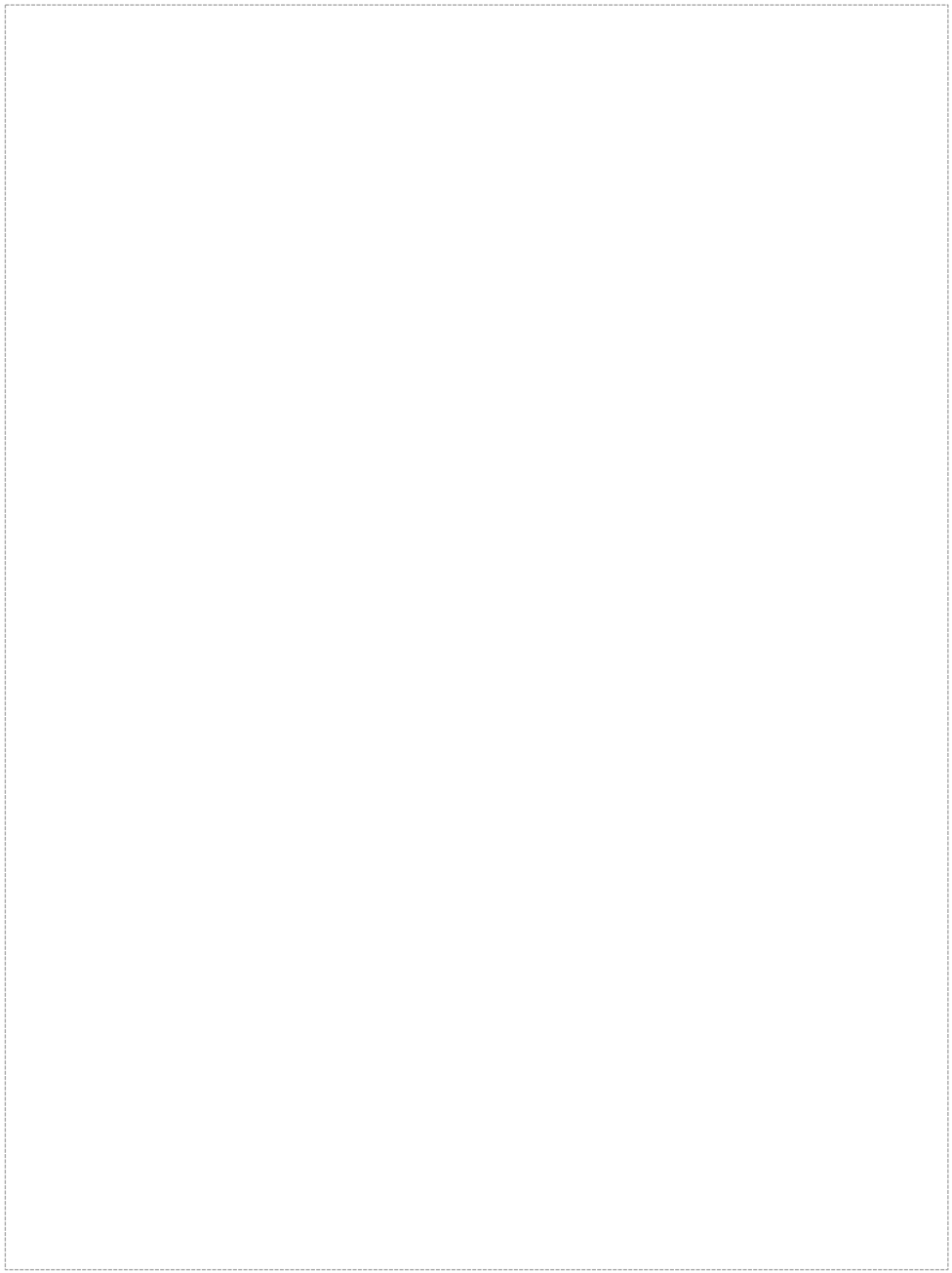
⏸ de 15 min

La signature électronique sécurisée

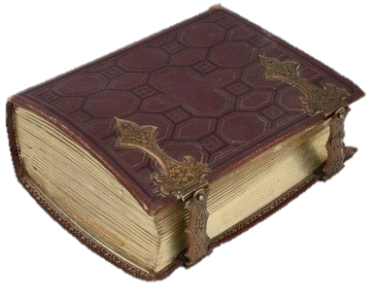

```
F96DE8C227A259C87EE1DA2AED5
7C93FE5DA36ED4EC87EF2C63AAE
5B9A7EFFD673BE4ACF7BE8923CA
B1ECE7AF2DCF7AE29A3DA44F235
A24C963FF0DF3CA3599A70E5DA3
6BF1ECE77F8DC34BE129A6CF4D1
26BF5B9A7CFEDF3EB850D37CF0C
63AA2509A76FF9227A55B9A6FE3
D720A850D97AB1DD35ED5FCE6BF
0D138A84CF8DC34BE129F8DC34B
```

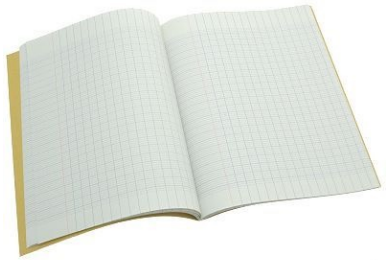
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

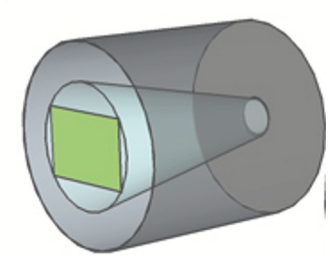
STELAU

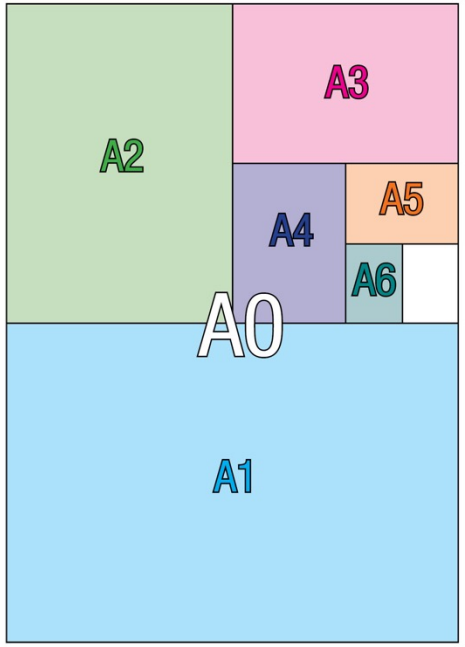


Conditions de perception / acquisition







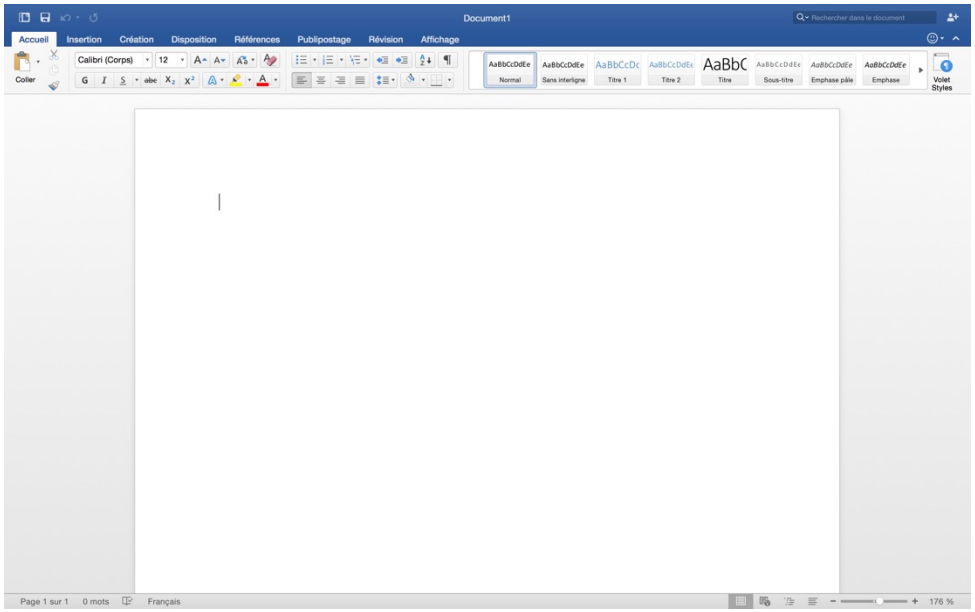


EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Toujours plat et rectangulaire

Evolutions


Document1
Accueil
Insertion
Création
Disposition
Références
Publipostage
Révision
Affichage
Page 1 sur 1
0 mots
Français

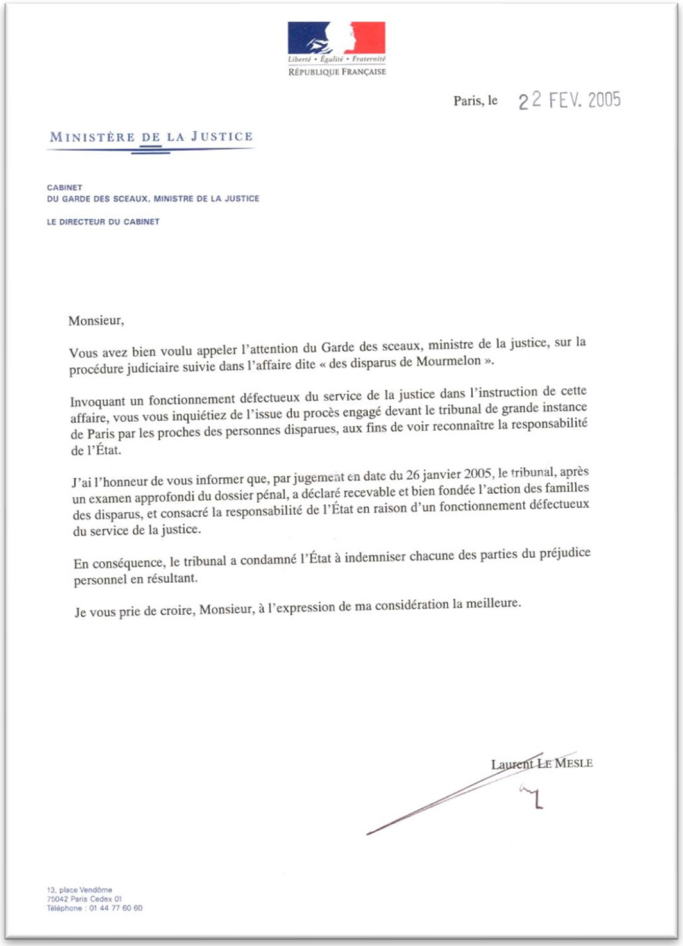

EPSON

Codes & Machines

Sommes-nous des machines ?

- Sommes-nous rectangulaires ?
- Pourquoi tabulons-nous ?
- Notre cerveau est-il tabulé ?
- Nouvelles IHM ?
- Sommes-nous du code ?

Soulagement



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Paris, le 22 FEV. 2005

MINISTÈRE DE LA JUSTICE

CABINET
DU GARDE DES SCEAUX, MINISTRE DE LA JUSTICE

LE DIRECTEUR DU CABINET

Monsieur,

Vous avez bien voulu appeler l'attention du Garde des sceaux, ministre de la justice, sur la procédure judiciaire suivie dans l'affaire dite « des disparus de Mourmelon ».

Invoquant un fonctionnement défectueux du service de la justice dans l'instruction de cette affaire, vous vous inquiétiez de l'issue du procès engagé devant le tribunal de grande instance de Paris par les proches des personnes disparues, aux fins de voir reconnaître la responsabilité de l'État.

J'ai l'honneur de vous informer que, par jugement en date du 26 janvier 2005, le tribunal, après un examen approfondi du dossier pénal, a déclaré recevable et bien fondée l'action des familles des disparus, et consacré la responsabilité de l'État en raison d'un fonctionnement défectueux du service de la justice.

En conséquence, le tribunal a condamné l'État à indemniser chacune des parties du préjudice personnel en résultant.

Je vous prie de croire, Monsieur, à l'expression de ma considération la meilleure.

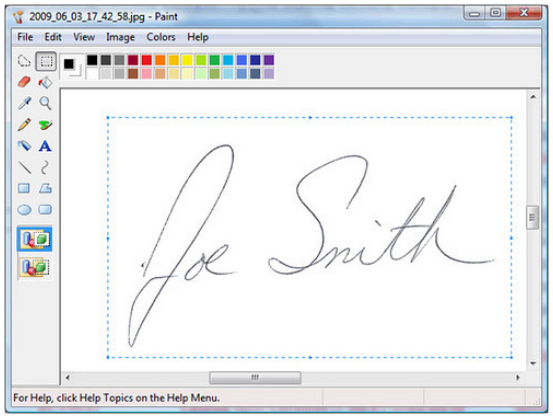
Laurent LE MESLE

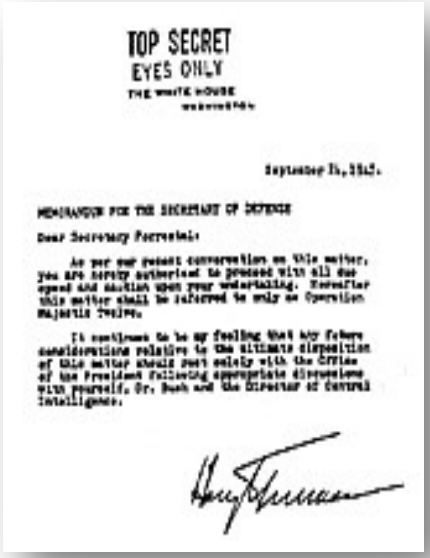
13, place Vendôme
75042 Paris Cedex 01
Téléphone : 01 44 77 60 60

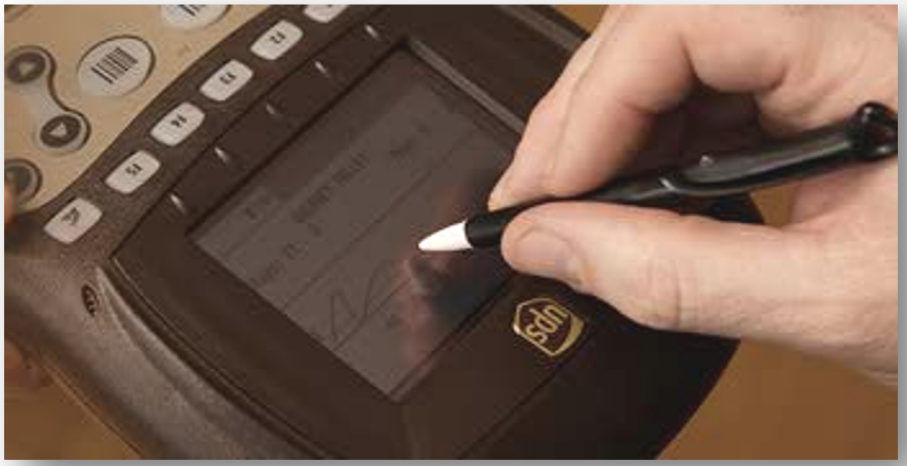
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Introduction

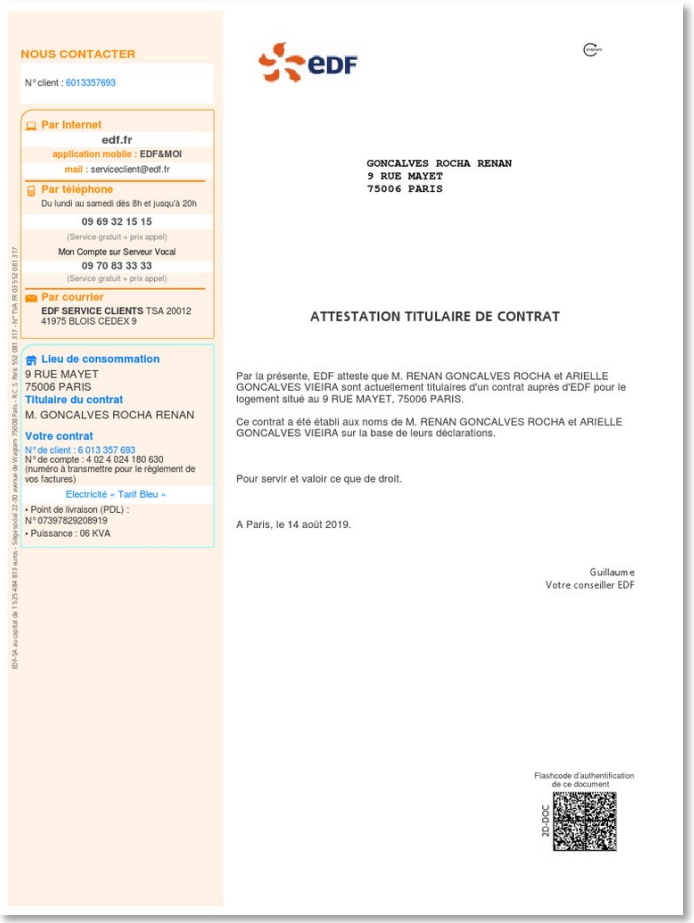






Introduction

Signature Electronique ?



NOUS CONTACTER

N° client : 6013357693

Par Internet
edf.fr
application mobile : EDF&MOI
mail : serviceclient@edf.fr

Par téléphone
Du lundi au samedi dès 8h et jusqu'à 20h
09 69 32 15 15
(Service gratuit + prix appel)
Mon Compte sur Serveur Vocal
09 70 83 33 33
(Service gratuit + prix appel)

Par courrier
EDF SERVICE CLIENTS TSA 20012
41975 BLOIS CEDEX 9

Lieu de consommation
9 RUE MAYET
75006 PARIS
Titulaire du contrat
M. GONCALVES ROCHA RENAN

Votre contrat
N° de client : 6 013 357 693
N° de compte : 4 02 4 024 180 630
(numéro à transmettre pour le règlement de vos factures)
Electricité « Tarif Bleu »
• Point de livraison (PDL) :
N° 07397829208919
• Puissance : 06 KVA

EDF

GONCALVES ROCHA RENAN
9 RUE MAYET
75006 PARIS

ATTESTATION TITULAIRE DE CONTRAT

Par la présente, EDF atteste que M. RENAN GONCALVES ROCHA et ARIELLE GONCALVES VIEIRA sont actuellement titulaires d'un contrat auprès d'EDF pour le logement situé au 9 RUE MAYET, 75006 PARIS.

Ce contrat a été établi aux noms de M. RENAN GONCALVES ROCHA et ARIELLE GONCALVES VIEIRA sur la base de leurs déclarations.

Pour servir et valoir ce que de droit.

A Paris, le 14 août 2019.

Guillaume
Votre conseiller EDF

Flashcode d'authentification de ce document
2D-DOC

Spécifications ?

AC: ANTS

La signature électronique sécurisée #2


```
F96DE8C227A259C87EE1DA2AED5
7C93FE5DA36ED4EC87EF2C63AAE
5B9A7EFFD673BE4ACF7BE8923CA
B1ECE7AF2DCF7AE29A3DA44F235
A24C963FF0DF3CA3599A70E5DA3
6BF1ECE77F8DC34BE129A6CF4D1
26BF5B9A7CFEDF3EB850D37CF0C
63AA2509A76FF9227A55B9A6FE3
D720A850D97AB1DD35ED5FCE6BF
0D138A84CF8DC34BE129F8DC34B
```

Questions ?

1. Dans le doc « zer0days » quel est le nom du projet de la NSA ?
2. Quelle est notamment l'une des capacités attendue d'un ingénieur ?
3. Quel pays écoute la planète ? [*cryptographiquement*]
4. On signe avec quoi ?
5. Quels sont les deux piliers de la crypto symétrique ?
6. De quand date l'agrégation externe d'informatique ?
7. Connaissez-vous ces personnes ?




Questions ?

1. NitroZeus
2. Capacité à CONCEVOIR
3. La Belgique
4. Une clé privée *et jamais rien d'autre*
5. Confusion et Diffusion *(substitution et transposition)*
6. 2021
7. Connaissez-vous ces personnes ?

Yann Lecun

Mars 2019 :
Prix Turing
l'équivalent du
« **Prix Nobel** »
en informatique.

Christopher Chedeau

React Native
Prettier
Excalidraw

Floriane Alixe

https://www.harfanglab.io/

Luc Delsalle

Alsid => Tenable

Crypto Asymétrique

Crypto Asymétrique

Concept de signature numérique

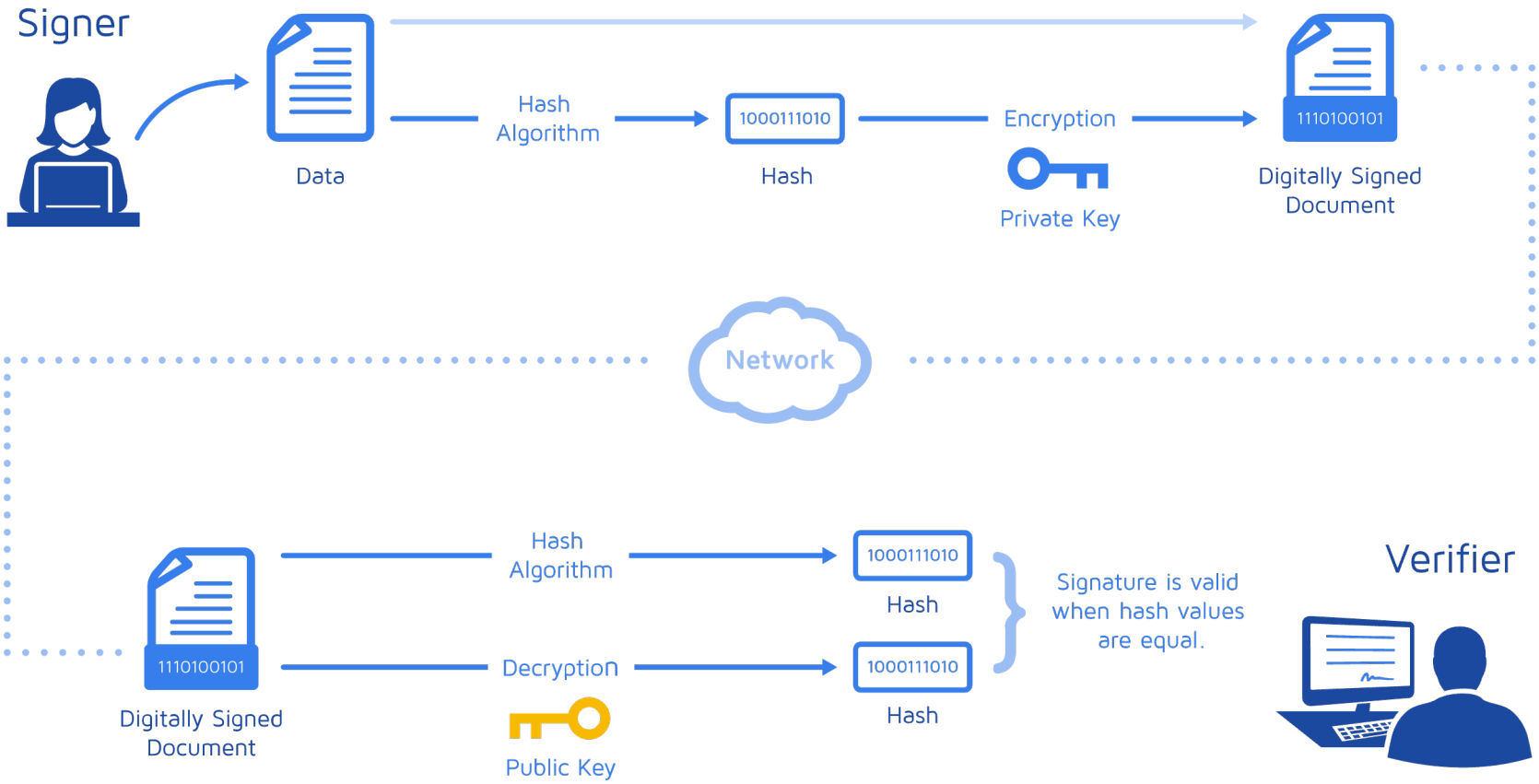
Signature manuscrite

- 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*

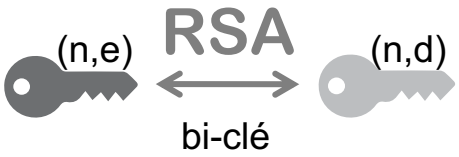
- approbation
- vérifiable
- non forgeable
- non répudiable
- transférable

Processus de Signature



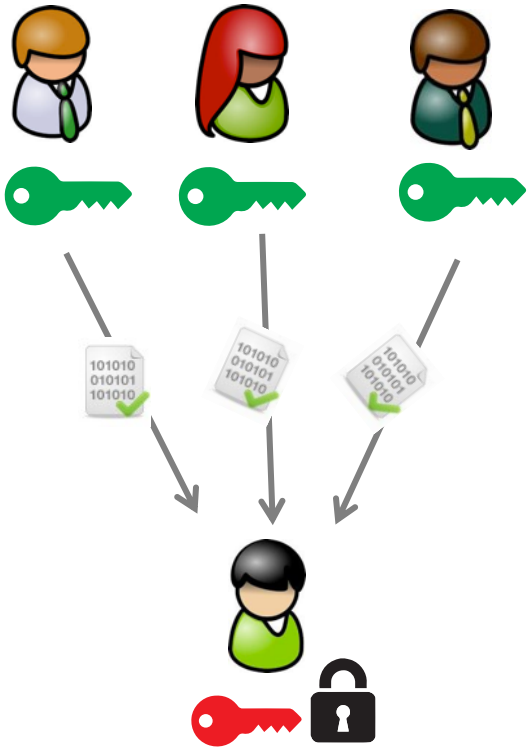
Crypto asymétrique

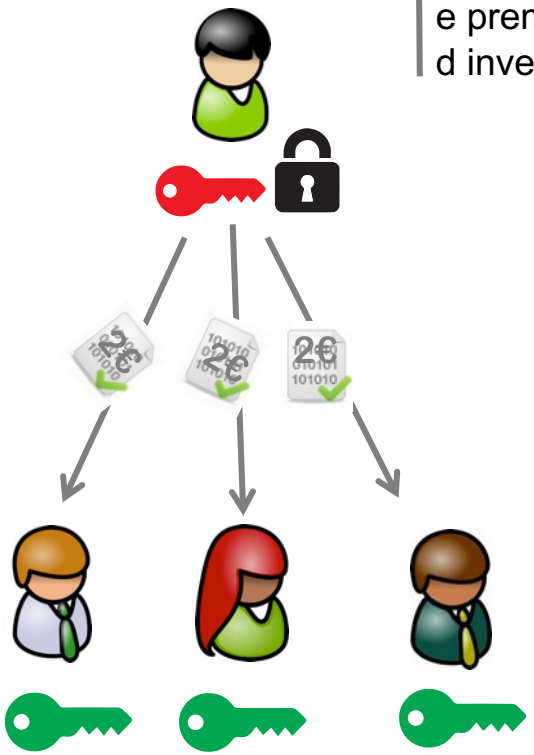
Usage : chiffrement vs signature



p et q premiers
n=p.q
φ(n) = (p - 1)(q -1)

e premier avec φ(n)
d inverse de e modulo φ(n)

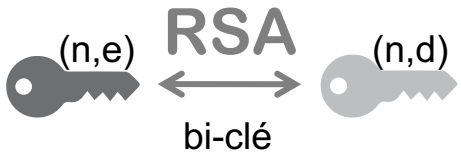




Signature

Standard PKCS#1 v2.2 (PSS)

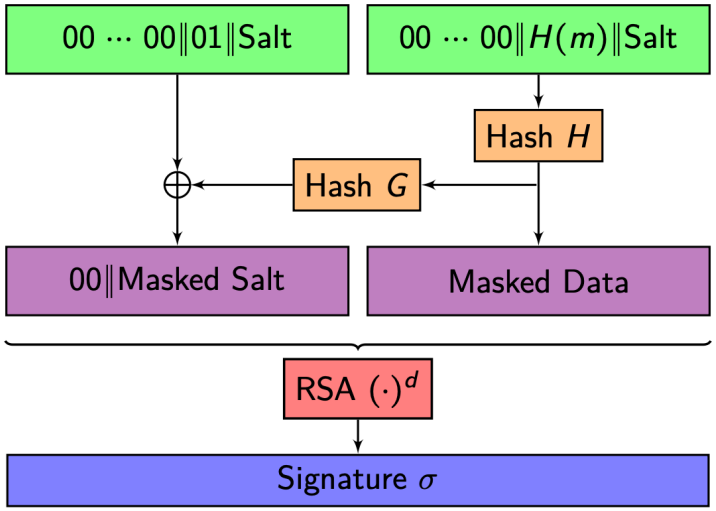
PKCS #1: RSA Cryptography Specifications
Version 2.2 – RFC 8017

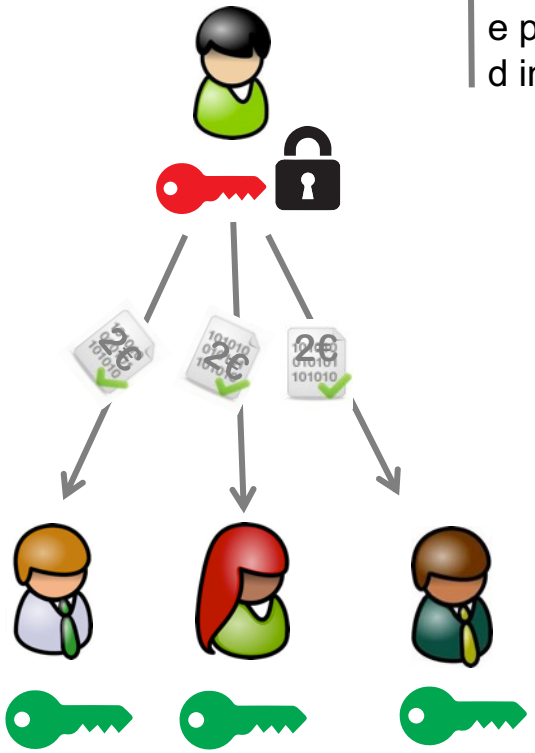


p et q premiers
n=p.q
φ(n) = (p - 1)(q -1)

e premier avec φ(n)
d inverse de e modulo φ(n)

Hash-and-Sign





VeryShortCryptoStory

Réagir après avoir cassé le code de son adversaire

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)

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

VeryShortCryptoStory

3000 ans de **crypto** **symétrique**

recettes militaro-diplomatiques de confusion et de diffusion

100 ans de **crypto** **moderne**

de Kerckhoffs ... au crypto-système parfait / incassable

50 ans de **crypto** **asymétrique**

la petite révolution ?

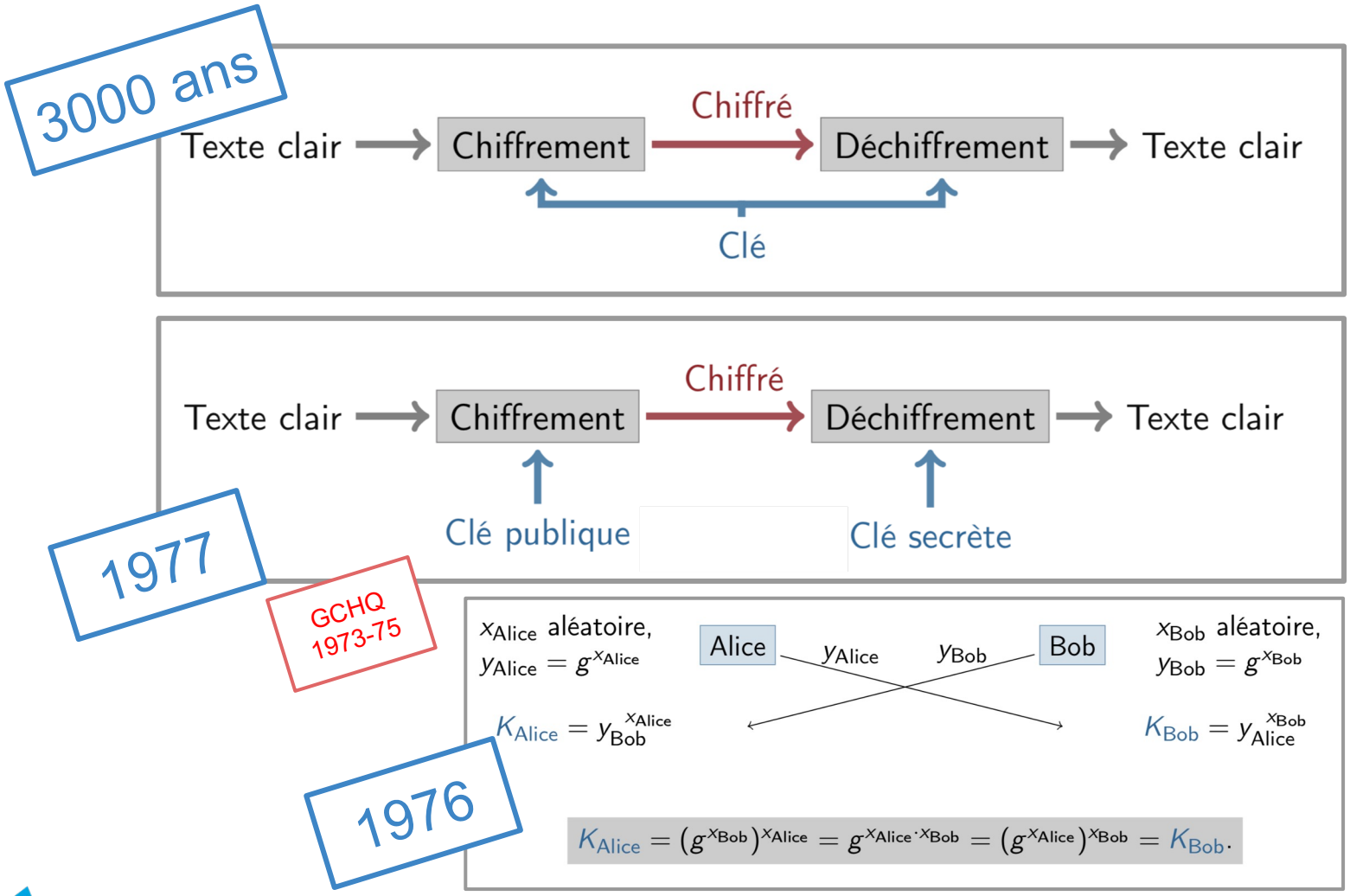
20 ans de **crypto** **quantique**

la grande révolution ?

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

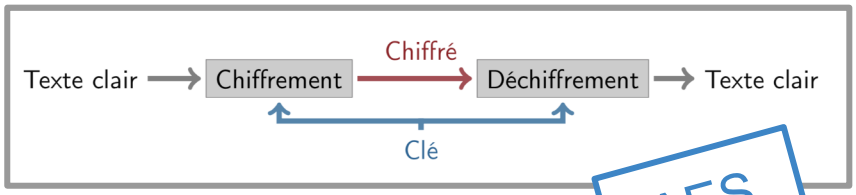
STELAU

Echange sécurisé de secret



4 primitives Crypto

Chiffrement Symétrique



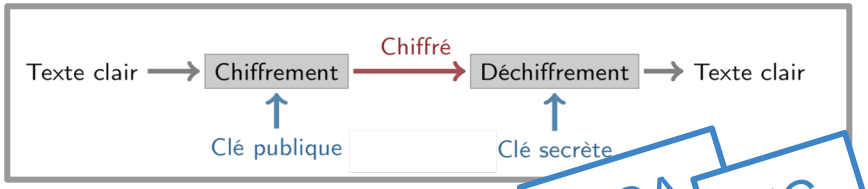
AES

Hachage crypto

```
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)
}
```

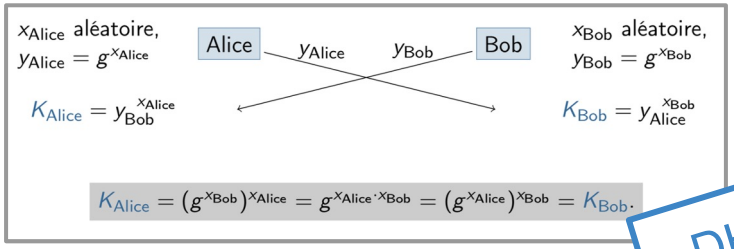
SHA3

Chiffrement Asymétrique



RSA EC

Key establishment

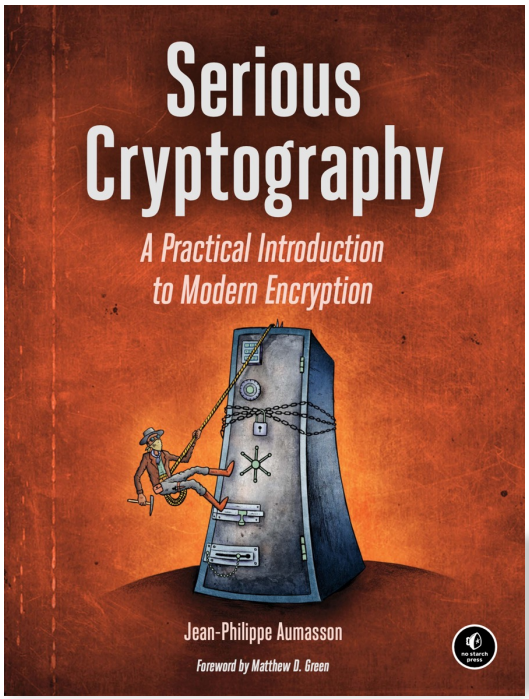


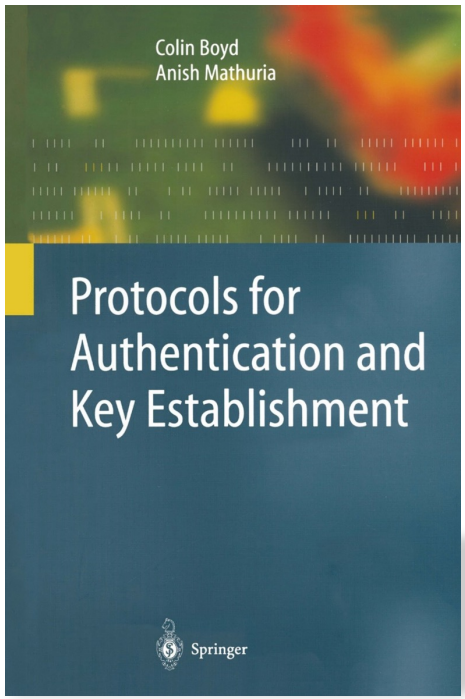
DH

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Deux ouvrages `Crypto`





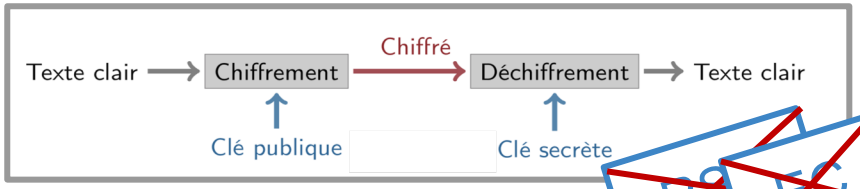
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

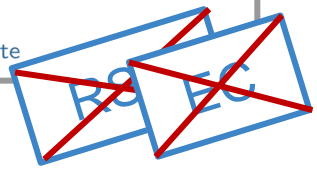
STELAU

Post quantique

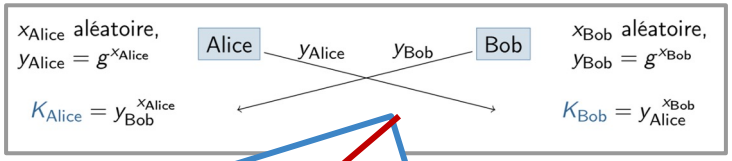
Résultats NIST 2022

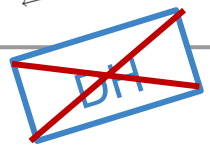
Chiffrement Asymétrique





Key establishment





CRYSTALS-KYBER

t.ly/_HRW

6qD-T1gjtKw

Digital Signature Algorithms

CRYSTALS-DILITHIUM

FALCON

SPHINCS+

3000 ans de crypto symétrique

Cryptographie Symétrique => Confusion et Diffusion

Confusion par substitution

A<=>U C<=>H Y<=>M Z<=>P ...

Diffusion par permutation / transposition

JESUISPASLA => UEISJASSPAL

<Crypto&Co/> => @HEMZOT+HT?@ => Z@H@?TM+TOEH

100 ans de crypto symétrique moderne

Crypto symétrique moderne => Auguste Kerckhoffs - 1883

1. Le système doit être matériellement, sinon mathématiquement indéchiffrable.

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

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

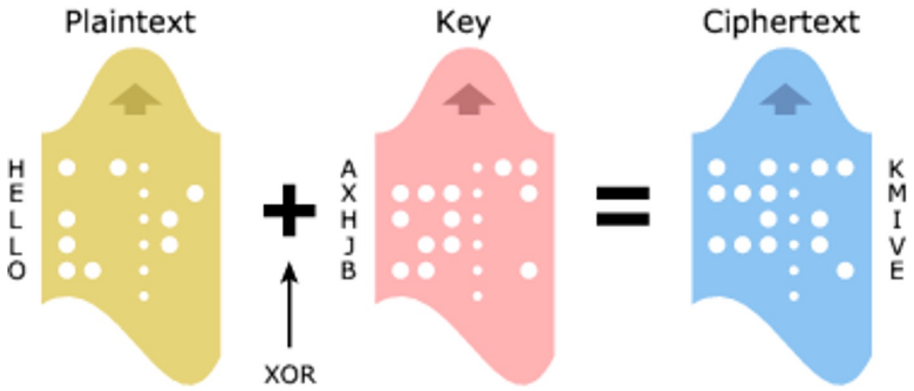
4. Il faut qu'il soit applicable à la correspondance télégraphique.
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
6.Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Le crypto-système inviolable existe



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**

Cryptographie Symétrique => Le Masque Jetable ou One Time Pad

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 totalement aléatoire.

Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de masque jetable).

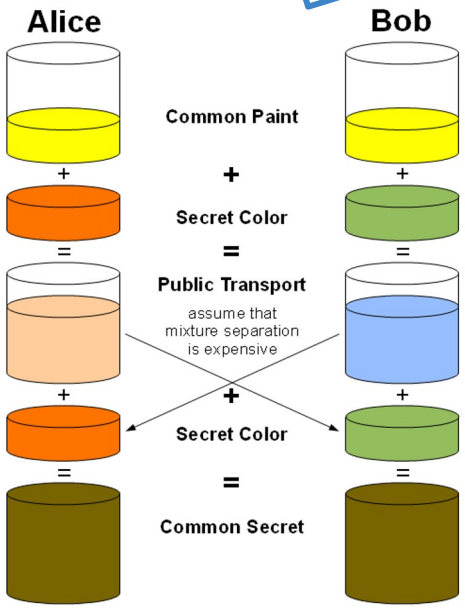
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

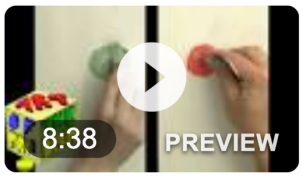
STELAU

Crypto asymétrique révolutionnaire 1

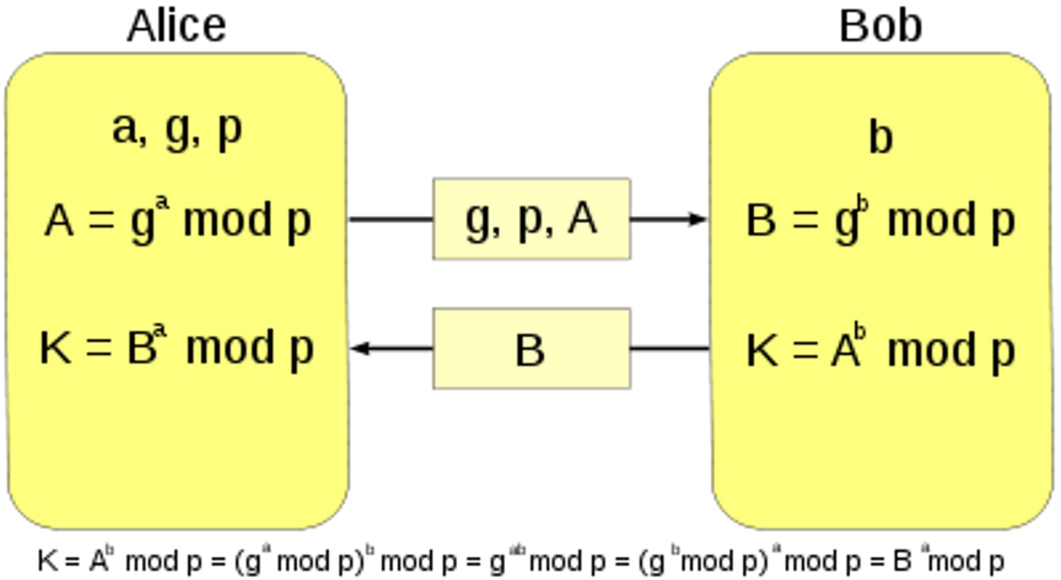
DH
Diffie-Hellman

Problème : établissement d'un secret commun entre deux entités Alice et Bob, ne pouvant communiquer que par un canal public.





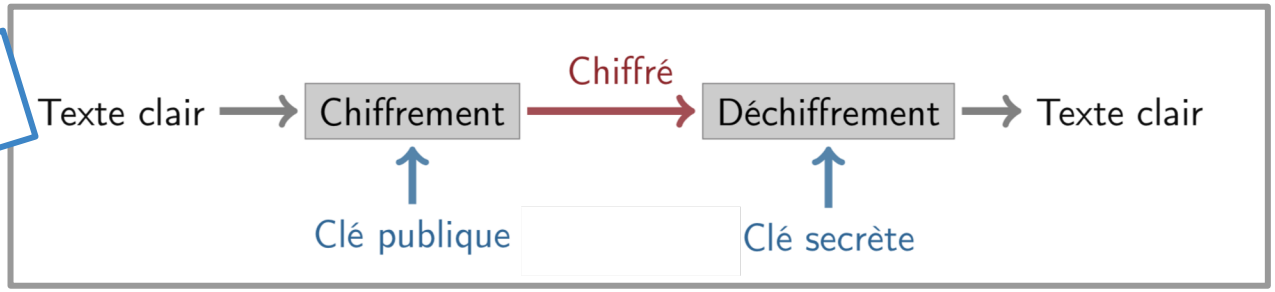
YEBfamv-_do



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Crypto asymétrique révolutionnaire 2

RSA



Echange sécurisé de secret

Clé secrète : deux nombres premiers p, q, un nombre d

Clé publique : $n = pq$ et $e = d^{-1} \pmod{(p-1)(q-1)}$

Chiffrement :

$$E(m) = m^e \pmod{n}$$

Déchiffrement :

$$D(c) = c^d \pmod{n}$$

Propriété mathématique :

$$D(E(m)) = m^{ed} \equiv m \pmod{n}$$

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

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

RSA

DH

Construction Hachage Crypto

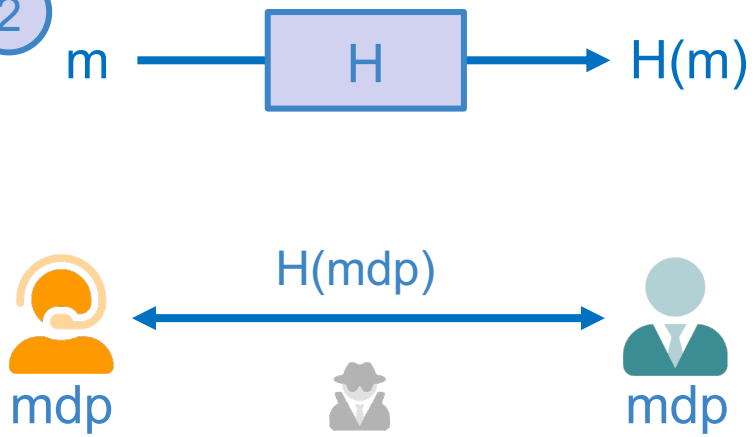
1

Hachage crypto

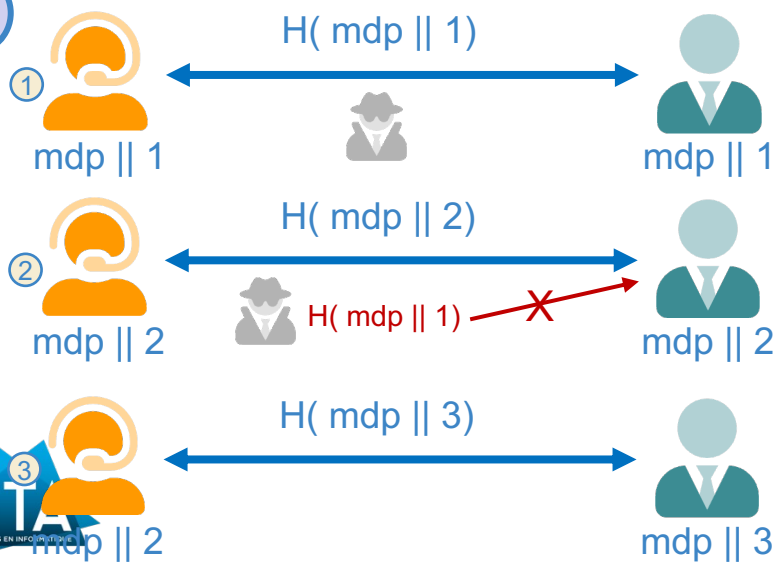
```
SHA1-blockcipher(a, b, c, d, e, M) {
    W = expand(M)
    for i = 0 to 79 {
        new = (a <<< 5) + f(i, b, c, d) + e + K[i] + W[i]
        (a, b, c, d, e) = (new, a, b >>> 2, c, d)
    }
    return (a, b, c, d, e)
}
```

SHA3

2



3



4

A function meeting these criteria may still have undesirable properties. Currently, popular cryptographic hash functions are vulnerable to *length-extension* attacks :

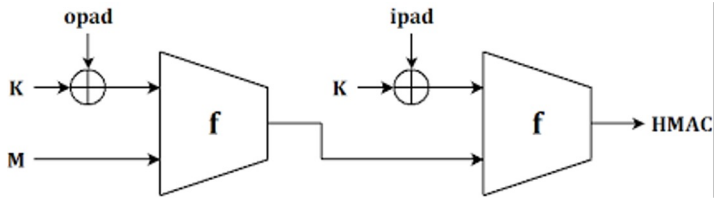
=> given hash(*m*) and len(*m*) but not *m*, by choosing a suitable *m′* an attacker can calculate hash(*m* ‖ *m′*), where ‖ denotes concatenation.[6] This property can be used to break naive authentication schemes based on hash functions. The HMAC construction works around these problems.

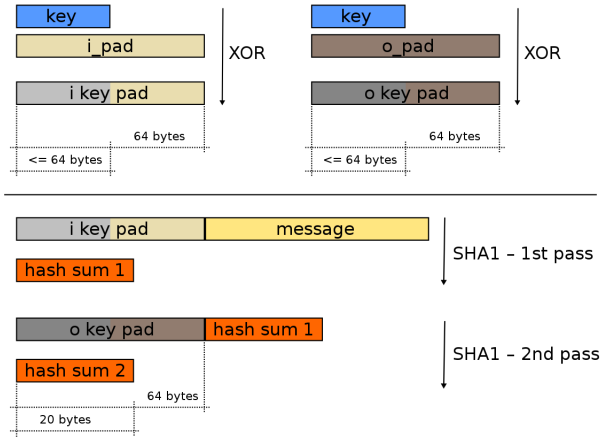
EPITA ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

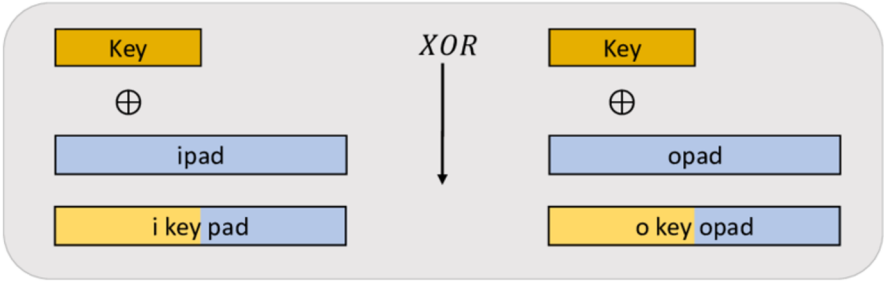
STELAU

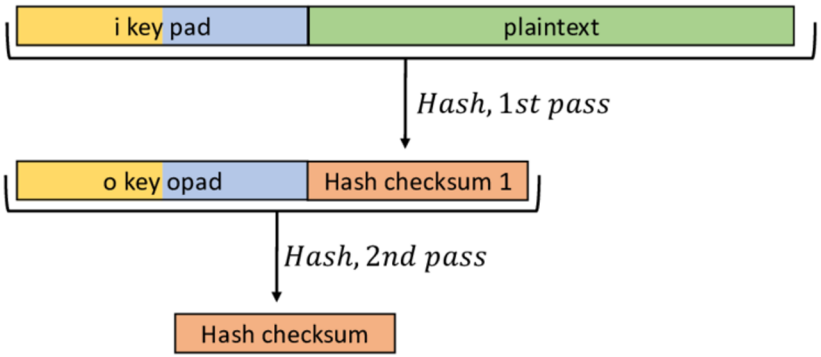
Construction du HMAC

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

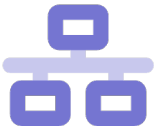








Ce que n'est pas un HMAC



	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 ?

N'oubliez pas que l'authentification sans confiance dans les clés utilisées est inutile.

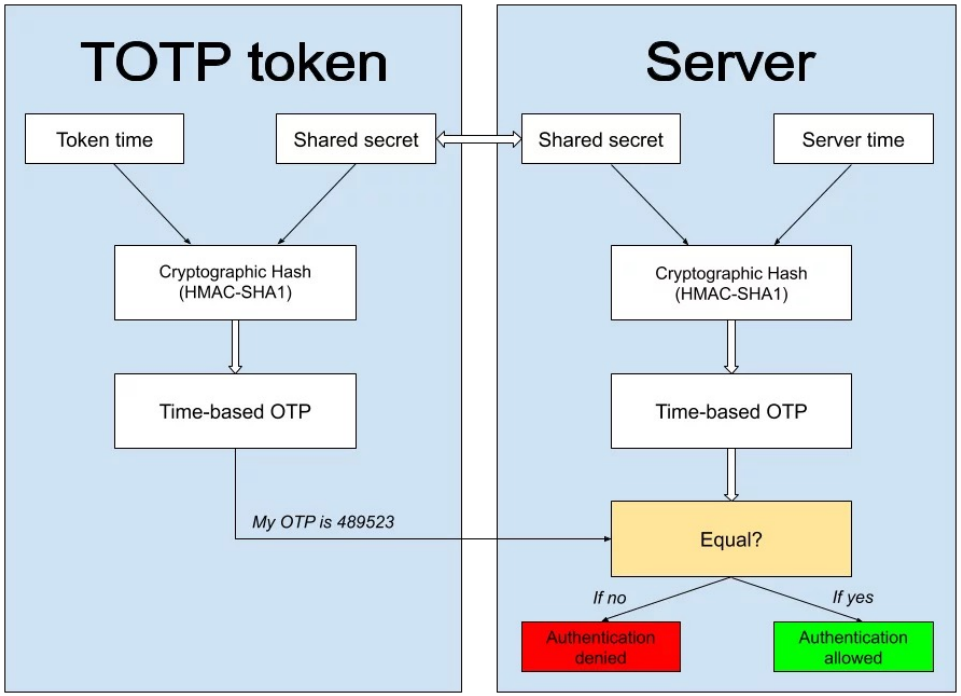
Pour les signatures un vérificateur doit être sûr que la clé de vérification appartient réellement au signataire.

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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Construction Hachage Crypto: TOTP



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

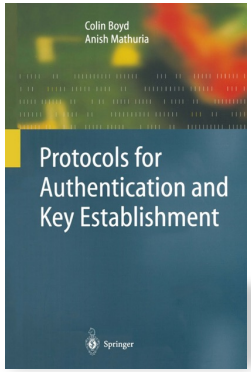
* The last byte (byte 19) has the hex value 0x5a.
* The value of the lower 4 bits is 0xa (the offset value).
* The offset value is byte 10 (0xa).
* The value of the 4 bytes starting at byte 10 is 0x50ef7f19, which is the dynamic binary code DBC1.
* The MSB of DBC1 is 0x50 so DBC2 = DBC1 = 0x50ef7f19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

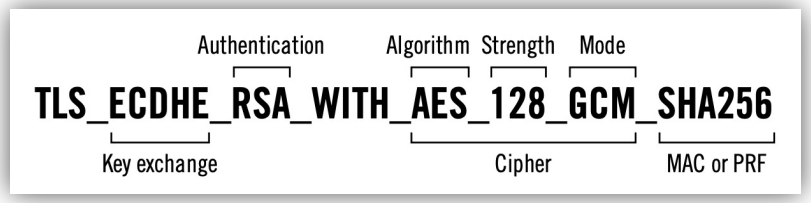
We then take this number modulo 1,000,000 (10^6) to generate the 6-digit HOTP value 872921 decimal.

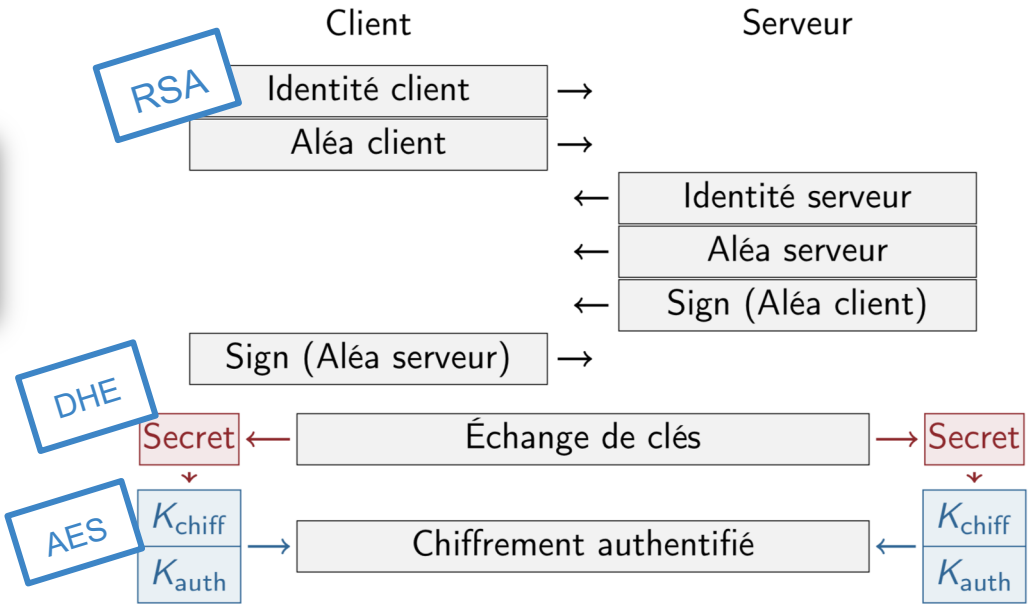
Où utilise-t-on cela ?

SSL/TLS
2D-DOC
message d'infraction
SSH
S/MIME
marchés publics
PGP
GPG
.pdf
.docx
eID Card
ePasseport
ordinateur
navigateur
carte bancaire
smartphone
navigo



Assemblage Crypto





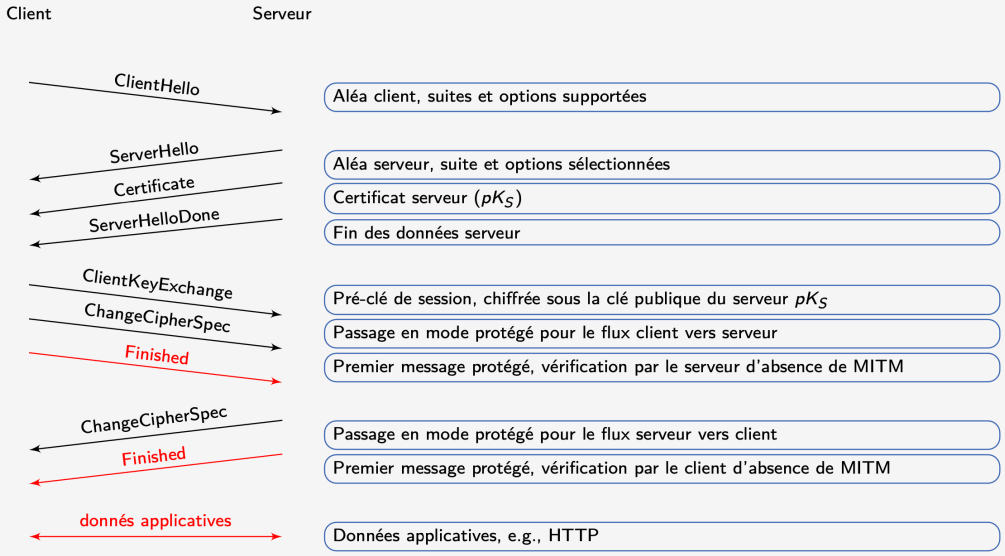
Cipher Suite Name	Auth	KX	Cipher	MAC	PRF
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	RSA	ECDHE	AES-128-GCM	-	SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDSA	ECDHE	AES-256-GCM	-	SHA384
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DHE	3DES-EDE-CBC	SHA1	Protocol
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES-128-CBC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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

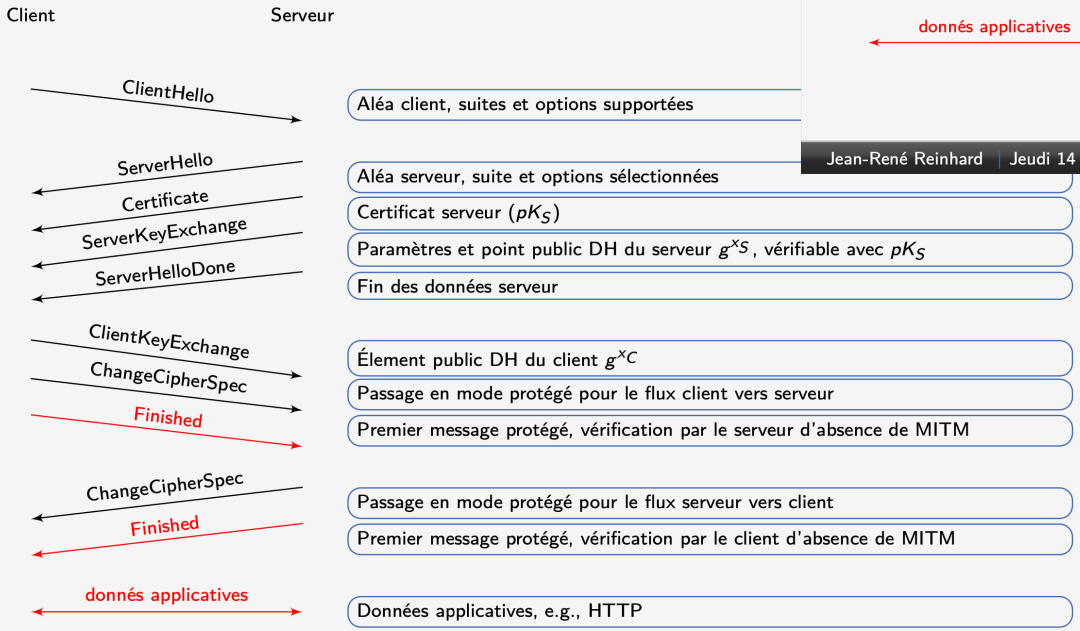
STELAU

Assemblage Crypto

SSL/TLS : établissement de clé RSA



SSL/TLS : établissement de clé DHE



STELAU

La signature électronique sécurisée #3


```
F96DE8C227A259C87EE1DA2AED5
7C93FE5DA36ED4EC87EF2C63AAE
5B9A7EFFD673BE4ACF7BE8923CA
B1ECE7AF2DCF7AE29A3DA44F235
A24C963FF0DF3CA3599A70E5DA3
6BF1ECE77F8DC34BE129A6CF4D1
26BF5B9A7CFEDF3EB850D37CF0C
63AA2509A76FF9227A55B9A6FE3
D720A850D97AB1DD35ED5FCE6BF
0D138A84CF8DC34BE129F8DC34B
```

Question?

Mon hébergeur m'a fournit un certificat électronique TLS (SSL) pour le serveur du site de ma société dont le Common Name est www.foobar.fr.

Je peux m'en servir pour signer électroniquement car j'en suis le gérant.

- ❑ Oui, toujours
- ❑ Oui, si le certificat comporte également le key usage approprié
- ❑ Non, jamais
- ❑ Non, sauf si cela ne dérange pas mon hébergeur

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

REX TP OpenSSL

> Signer au moins une fois ... et avec ?

> Qu'est ce que l'on signe exactement ?

données binaires ou autre format

> Quel format de signature ?

à l'arraché
XAdES
PKCS#7
S/MIME
autre

> Comment vérifie-t-on une signature ?

la signature cryptographique elle-même
certificat
chaine de signature
LCR (CRL)
OCSP

7e0950bb938539162d268b379595
44efb87b718950bf4721dd5c94f5f7
d12fc4efac9d9b5f0c81bbc1555c3d7
6610ef3080a354e60b625f5c50a23
a6bfd13ec024239ddc0b47706c9a23
11fc38e37161e87501236542732797
2469b3985721cc0feca3b04047a9c5
b559e3471a736f5e4c7b473b2e86b1
b21dd8a829828d f8d6

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
  - 1ère pré-image
  - 2de pré-image
  - collision

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

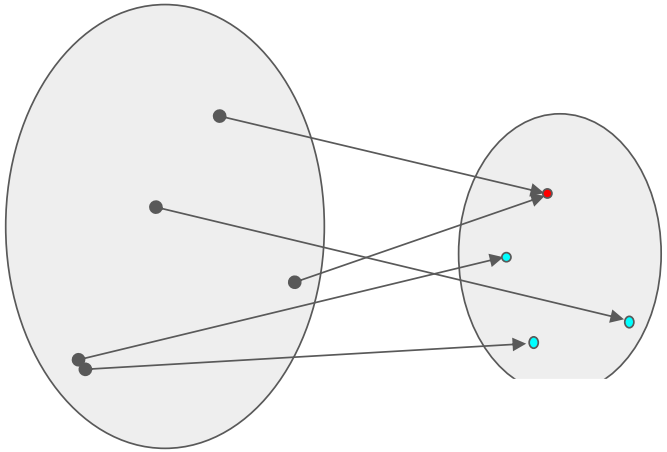
STELAU

Hash

fonctions de hachage cryptographiques

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

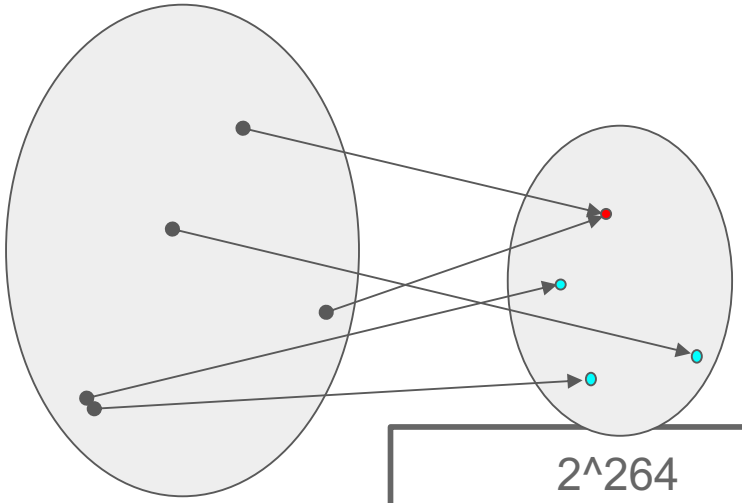
- Résistantes aux attaques
  - 1ère pré-image
  - 2de pré-image
  - collision



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
  - 1ère pré-image
  - 2de pré-image
  - collision

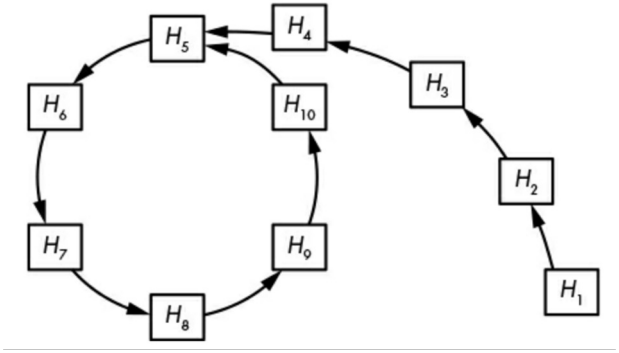


2^264
2^(80*3,3)
10^80
nb. atomes univers

Hash

fonctions de hachage cryptographiques

- Résistantes aux attaques
  - 1ère pré-image
  - 2de 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)

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

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 m1 donné, trouver m2 tel que H(m1) = H(m2)

- Résistance aux collisions

  Attaque : trouver m1 et m2 tel que H(m1) = H(m2)

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Hash

5baa61e4c9b93f3f0682250b6f8331b7ee68fd8

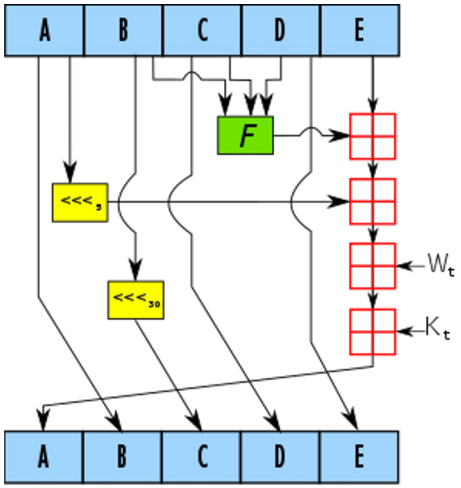
fonctions de hachage cryptographiques

```
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)
}
```

```
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)
}
```




```
275         x[6] = byte(s >> 8)
276         x[7] = byte(s)
277 }
278
279 func putUint32(x []byte, s uint32) {
280         _ = x[3]
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
```

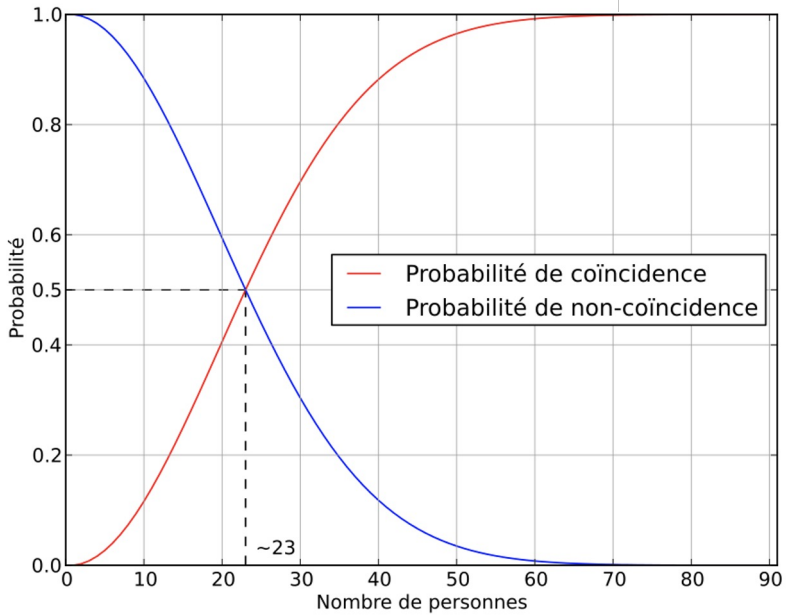
Source : Serious Cryptography

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 :

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



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.

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

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

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

```
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
```

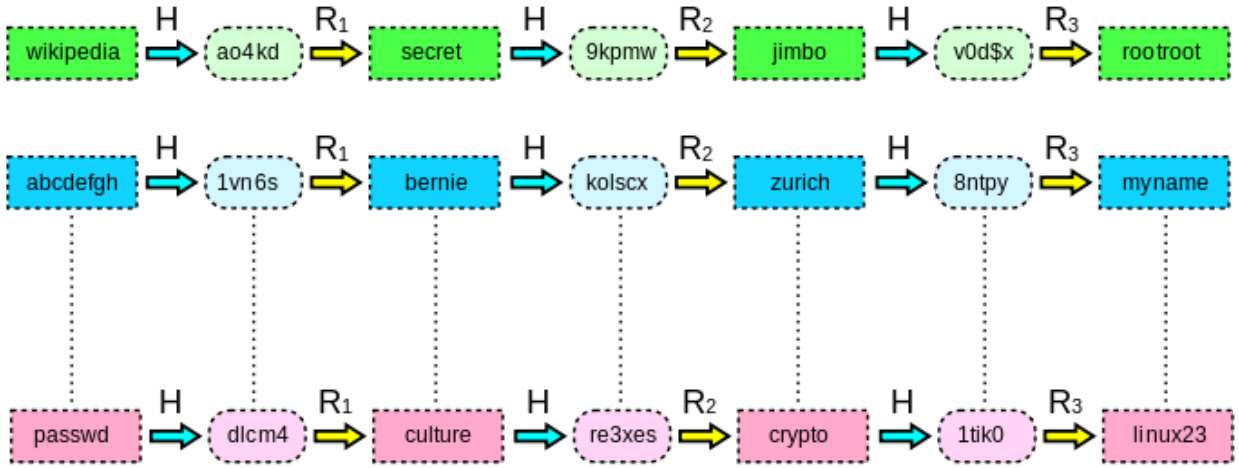
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

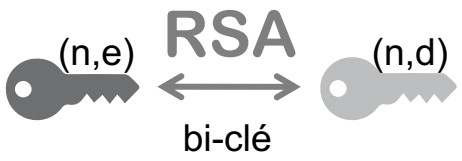
STELAU

Signature

Cryptosystème RSA

$$C \equiv M^e \ (mod\ n)$$

$$M \equiv C^d \ (mod\ n)$$



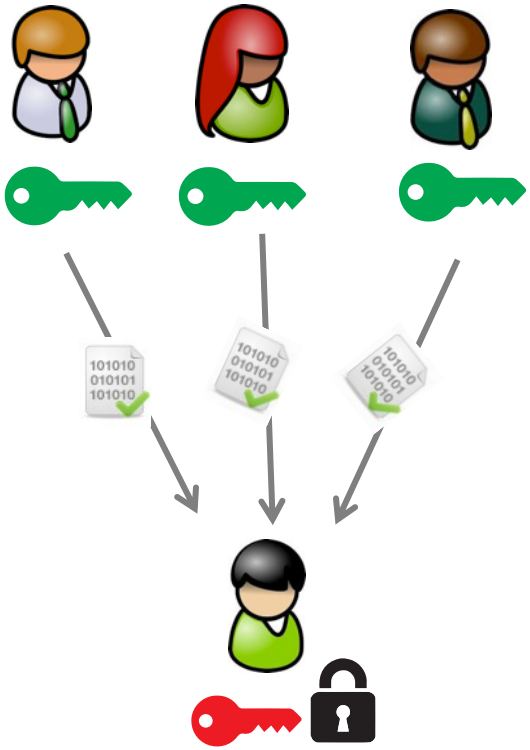
p et q premiers
n=p.q
φ(n) = (p - 1)(q -1)

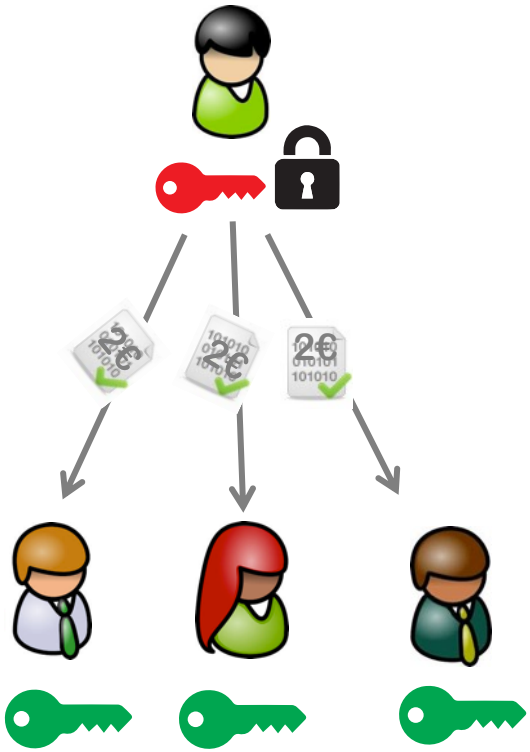
e premier avec φ(n)
d inverse de e modulo φ(n)

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

Crypto asymétrique

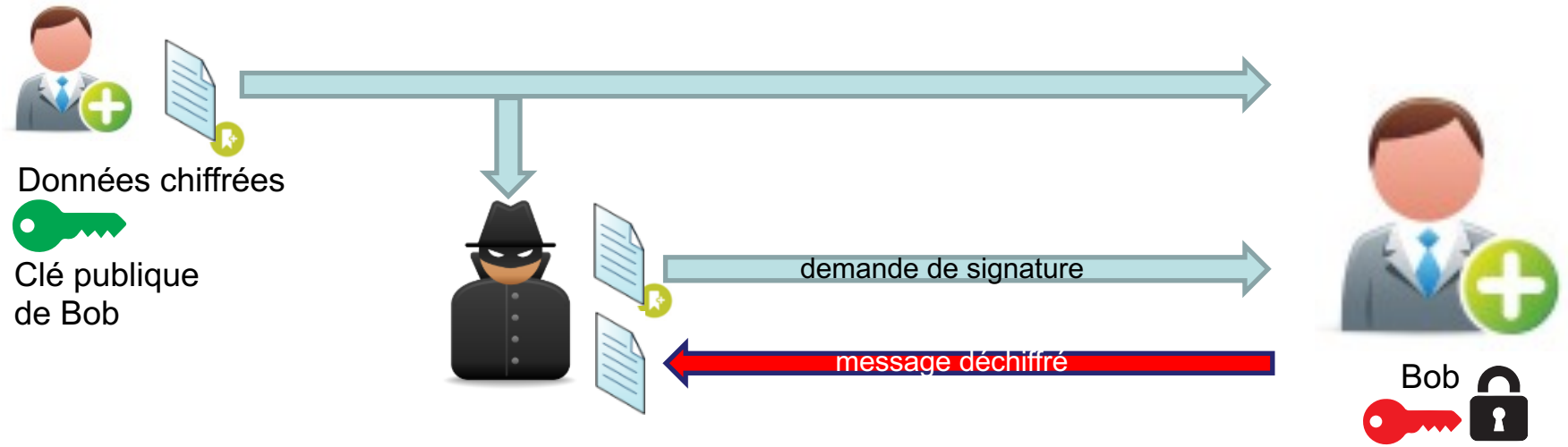
Usage : chiffrement vs signature





Rappels

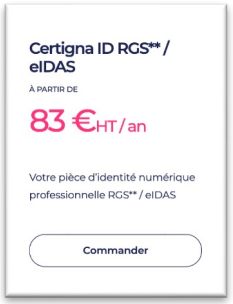
Certificat – Séparation des Key Usage

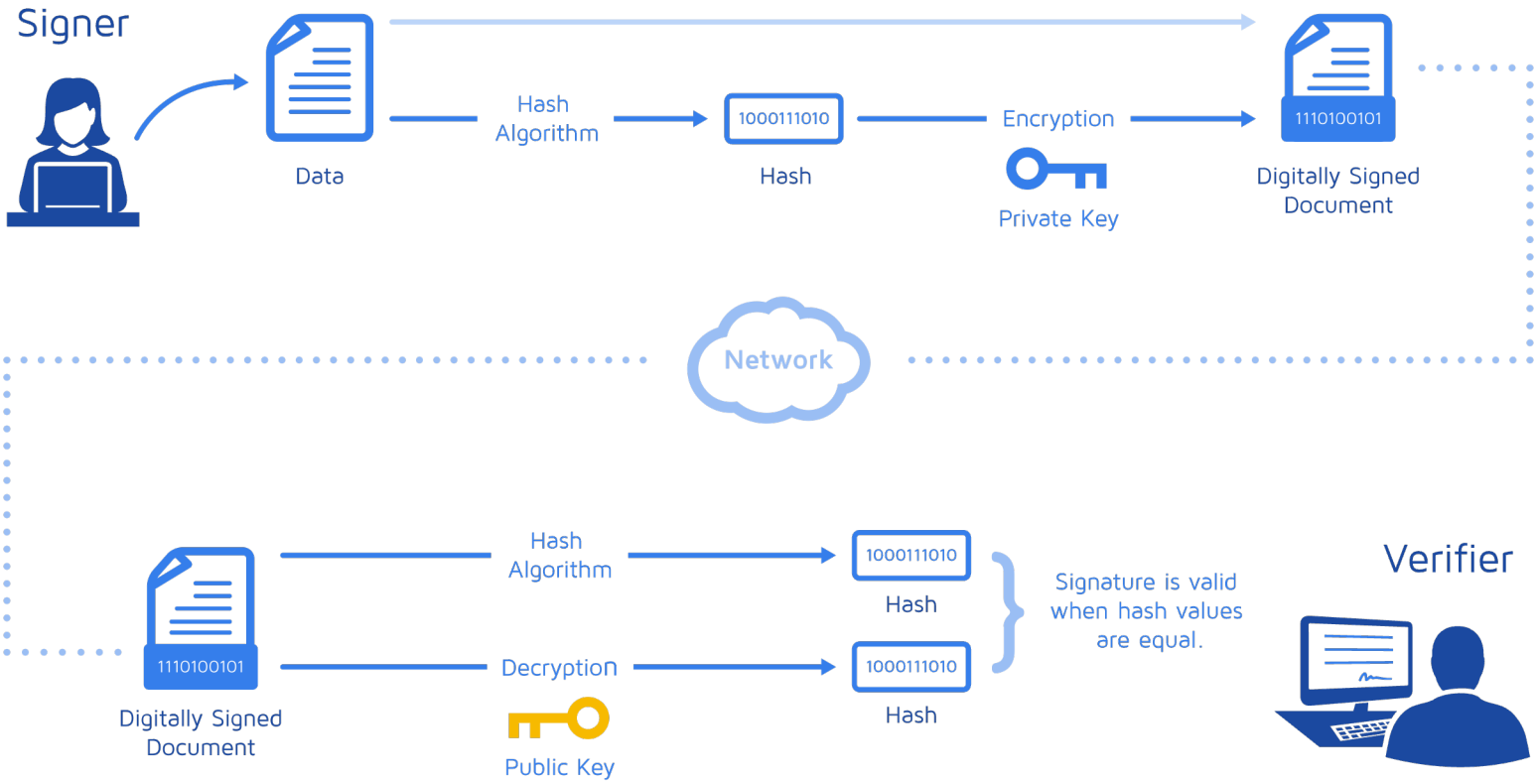


Cryptographie : utilisation de sa clé privée
déchiffrement = signature

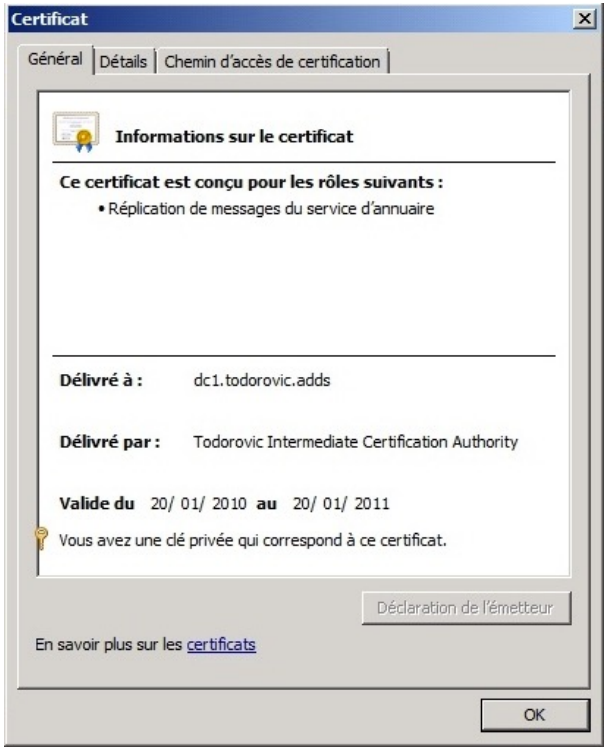
Exemple de Signature

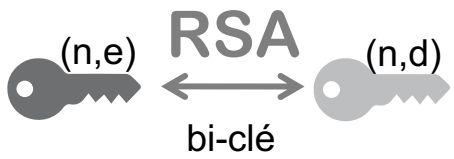
bi-clé de signature Certigna

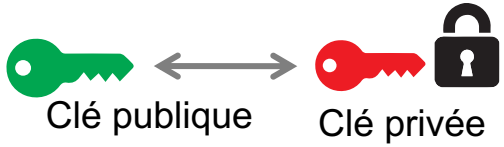




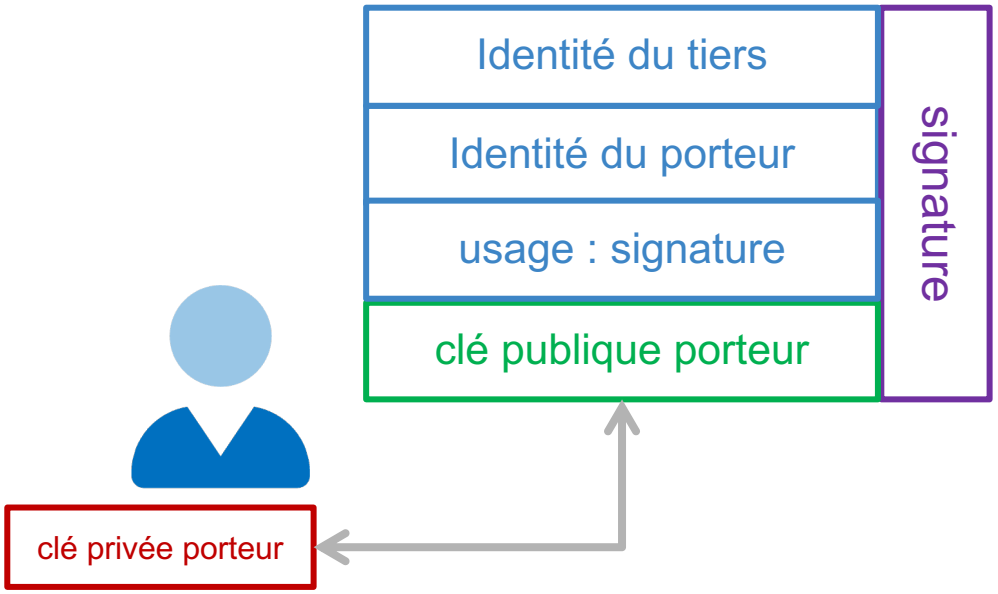
Certificat


Certificat
Général
Détails
Chemin d'accès de certification
Informations sur le certificat
Ce certificat est conçu pour les rôles suivants :
• Réplication de messages du service d'annuaire
Délivré à : dc1.todorovic.adds
Délivré par : Todorovic Intermediate Certification Authority
Valide du 20/ 01/ 2010 au 20/ 01/ 2011
Vous avez une clé privée qui correspond à ce certificat.
Déclaration de l'émetteur
En savoir plus sur les certificats
OK


(n,e)
RSA
(n,d)
bi-clé

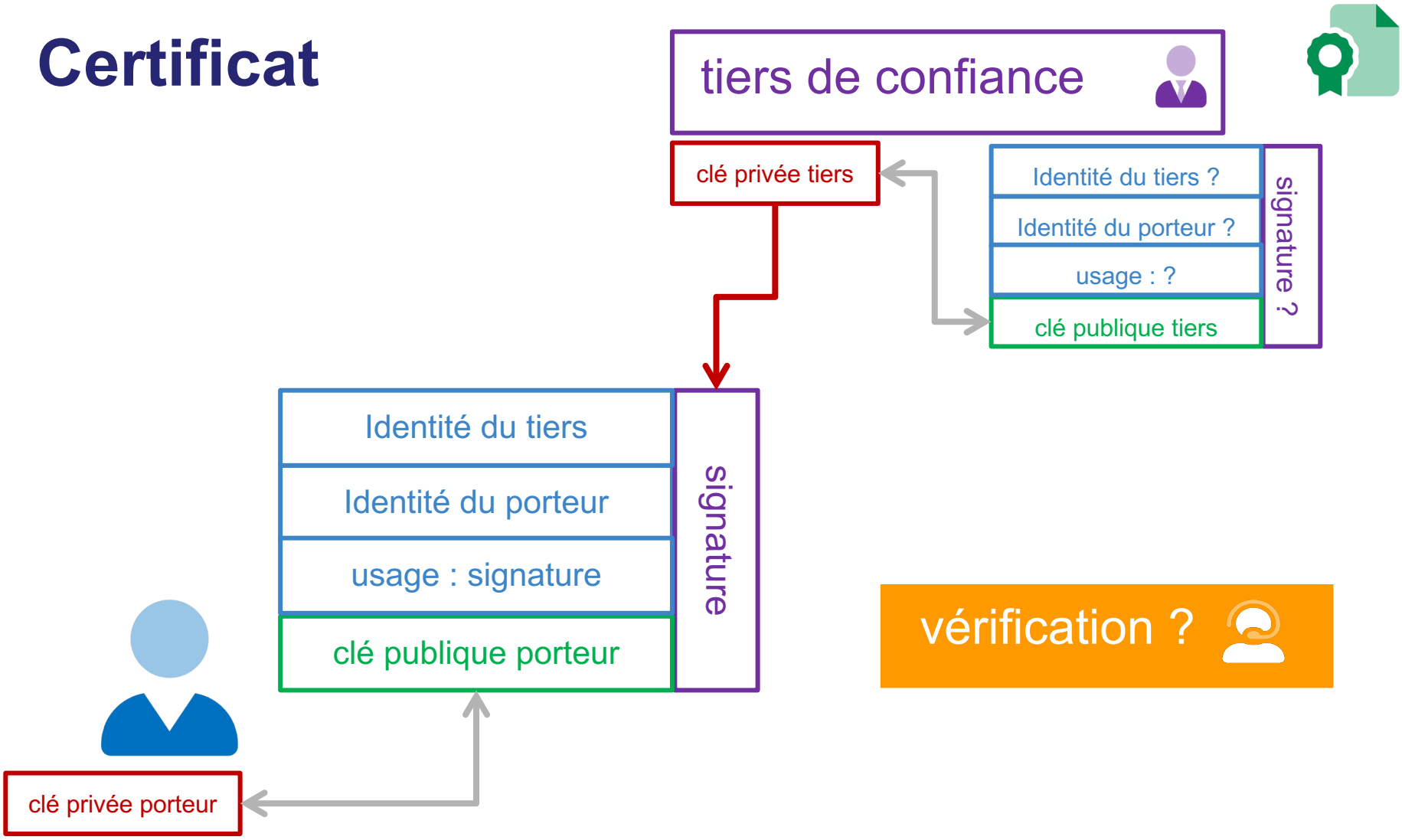

Clé publique
Clé privée

Certificat



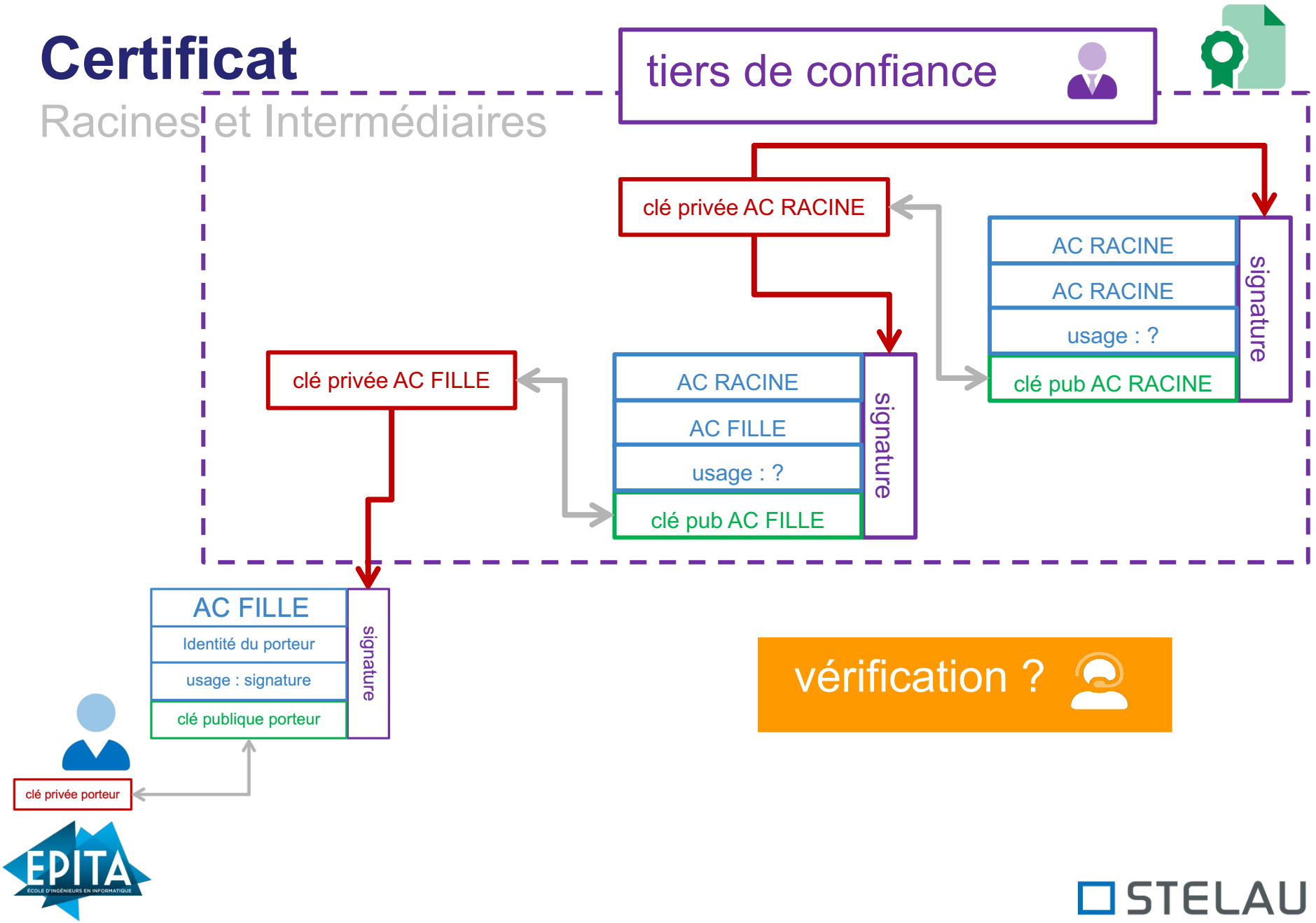
vérification ?

Certificat


tiers de confiance
clé privée tiers
Identité du tiers ?
Identité du porteur ?
usage : ?
clé publique tiers
signature ?
Identité du tiers
Identité du porteur
usage : signature
clé publique porteur
signature
vérification ?
clé privée porteur

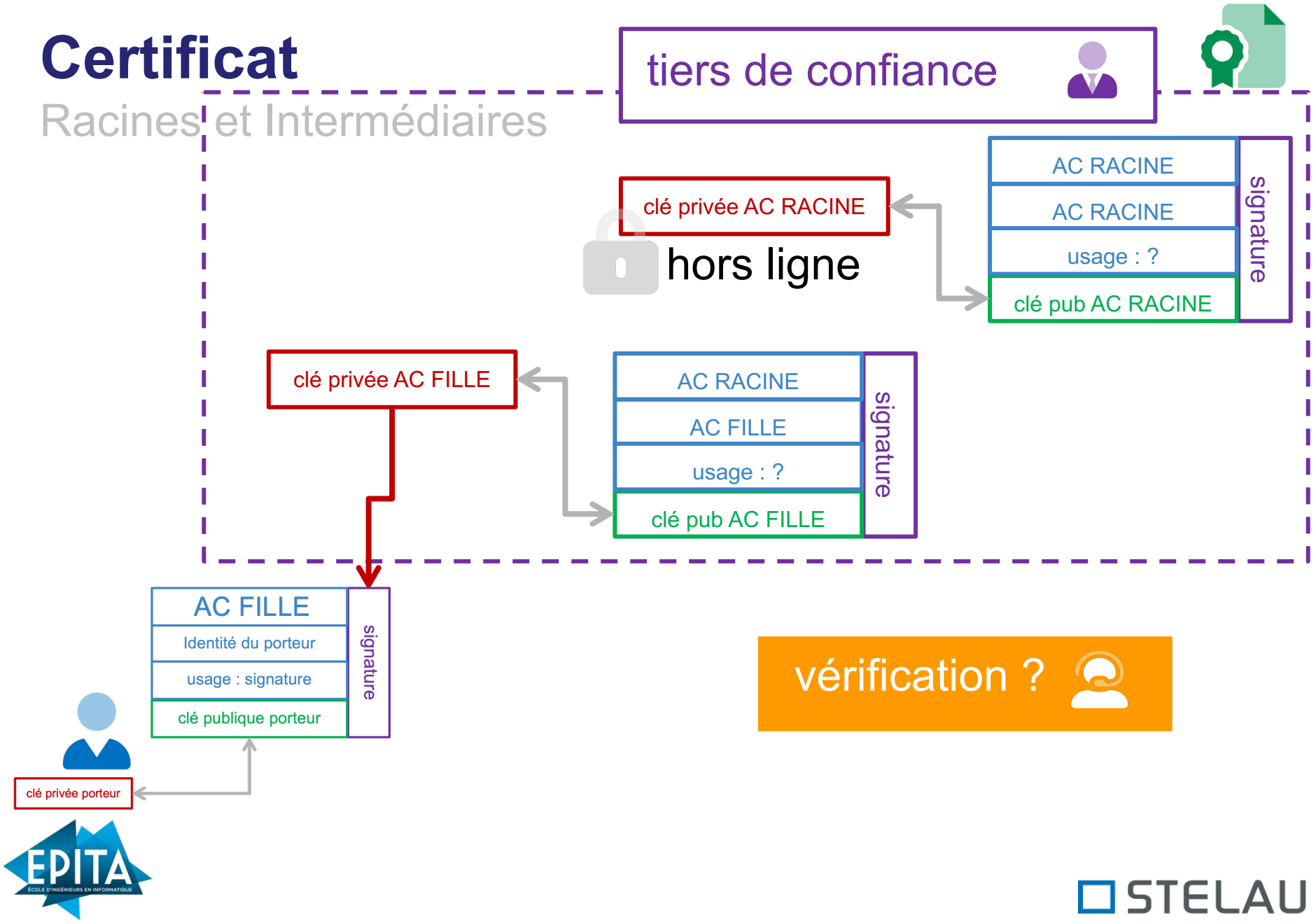
Certificat

Racines et Intermédiaires



Certificat

Racines et Intermédiaires



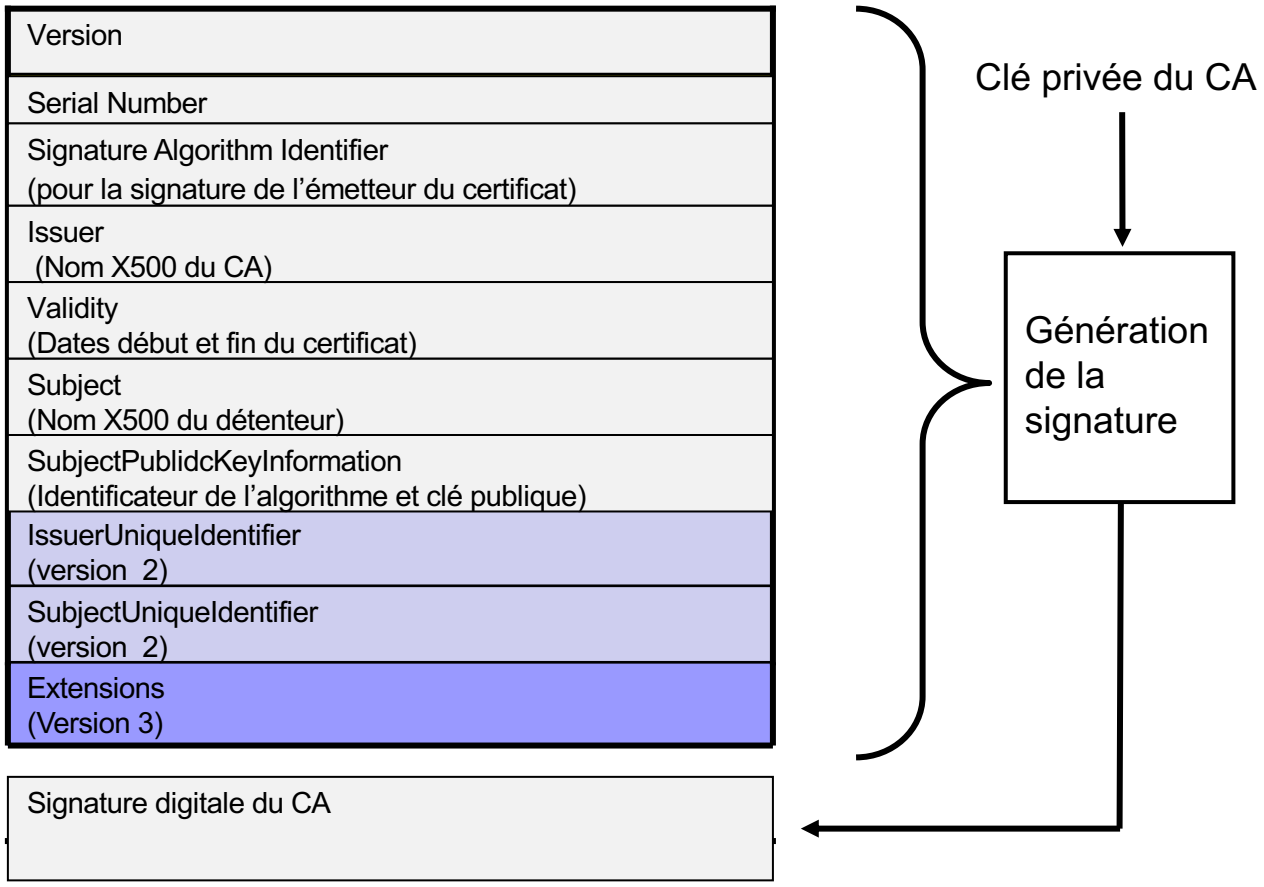
Certificat

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:e7:74: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:b0: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:e7:88:6d: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:e4: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
```

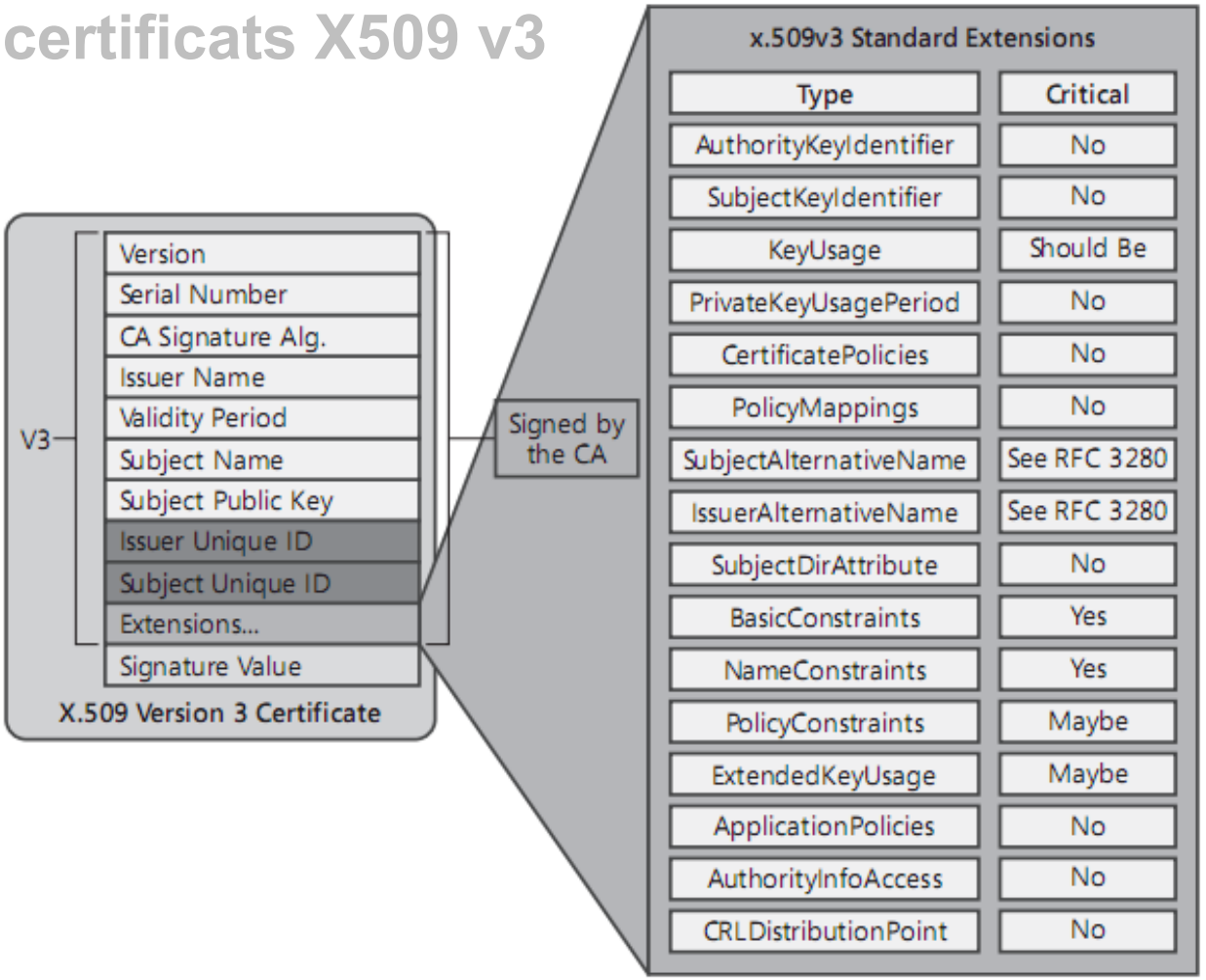
Certificat

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 ...
Extension	Utilisation de la clé (2 5 29 15)
Critique	NON
Utilisation	Signature numérique, Non répudiation
Extension	Contraintes élémentaires (2 5 29 19)
Critique	OUI
Autorité de certification	NON

Authentification (Vérification de signature)

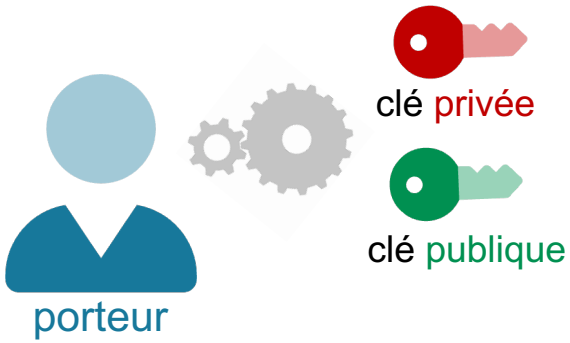
Signature électronique

IGC - PKI

IGC – Demande de certificat

IGC - PKI

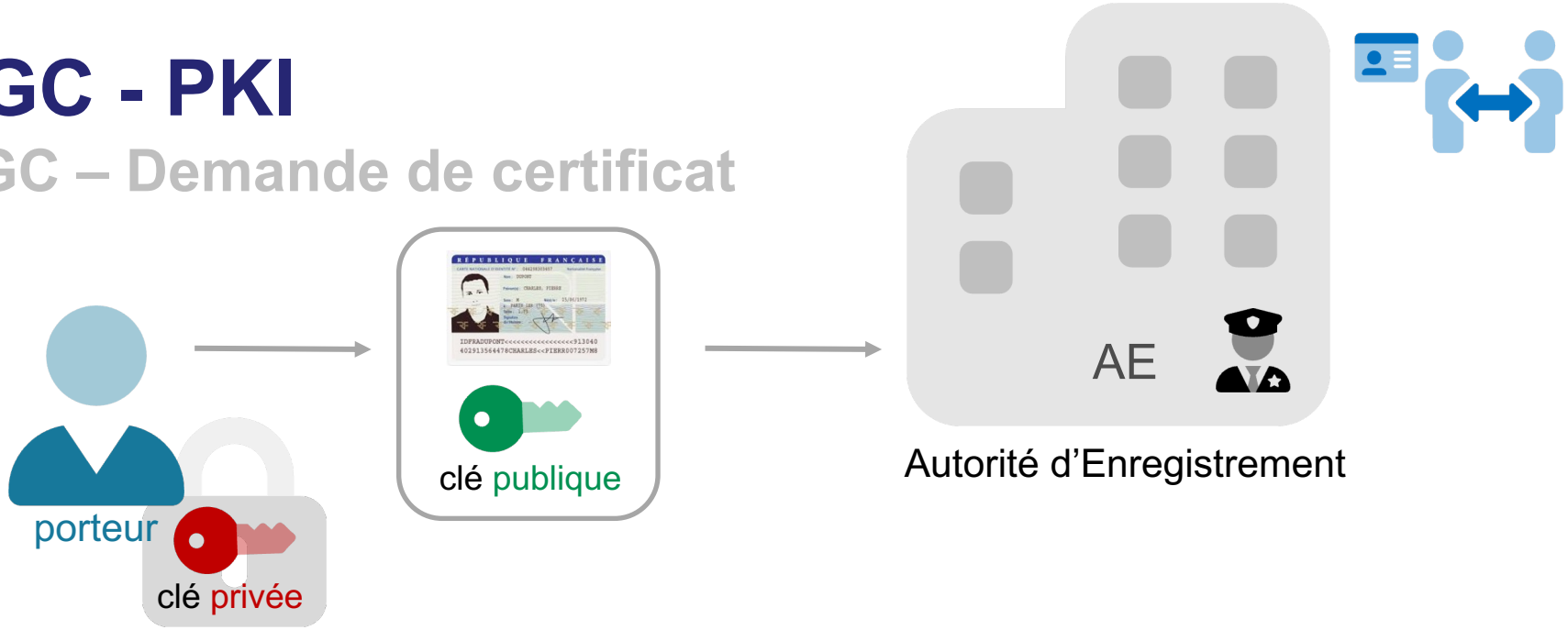
IGC – Demande de certificat



génération du bi-clés

IGC - PKI

IGC – Demande de certificat

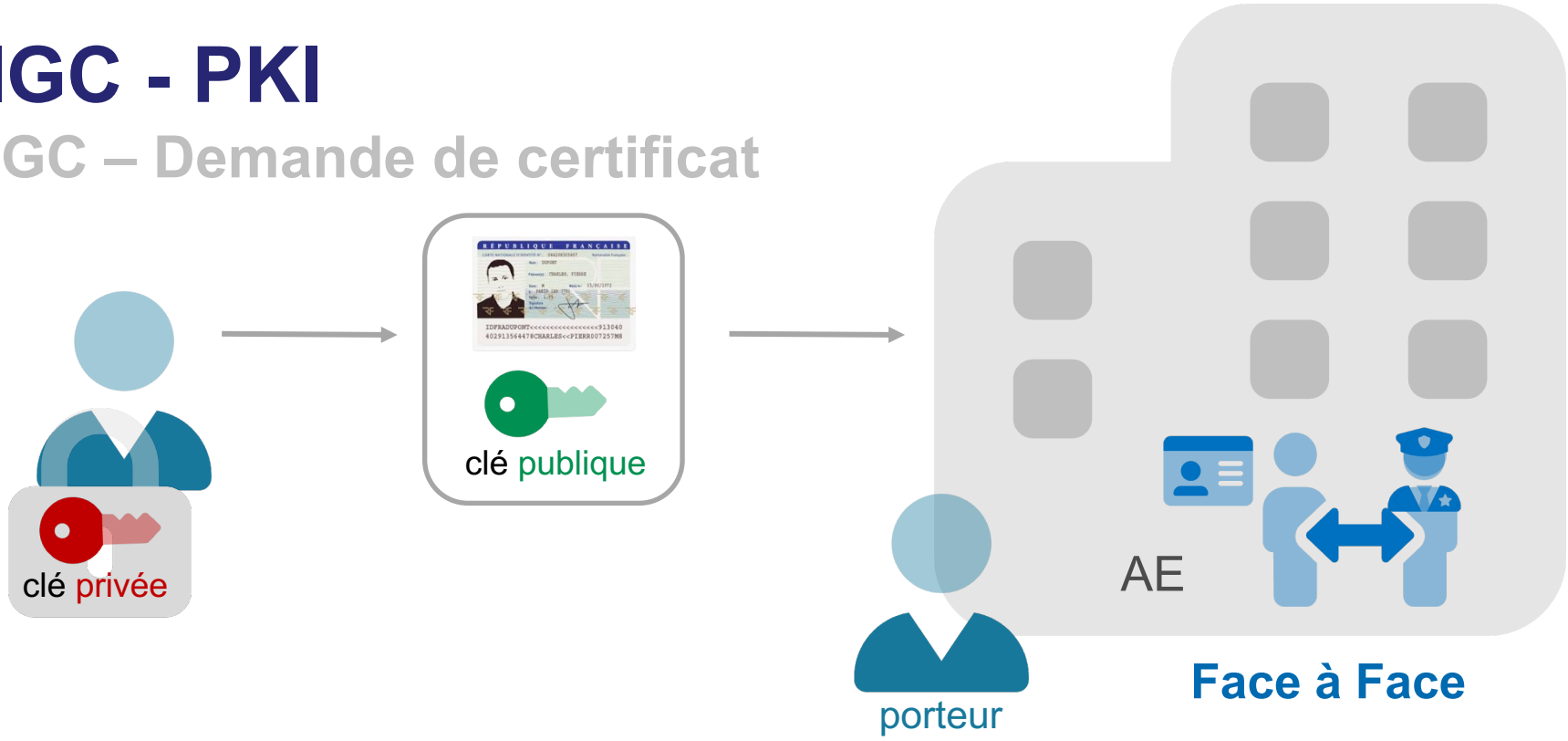


1. Sécurisation de la clé privée

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

IGC - PKI

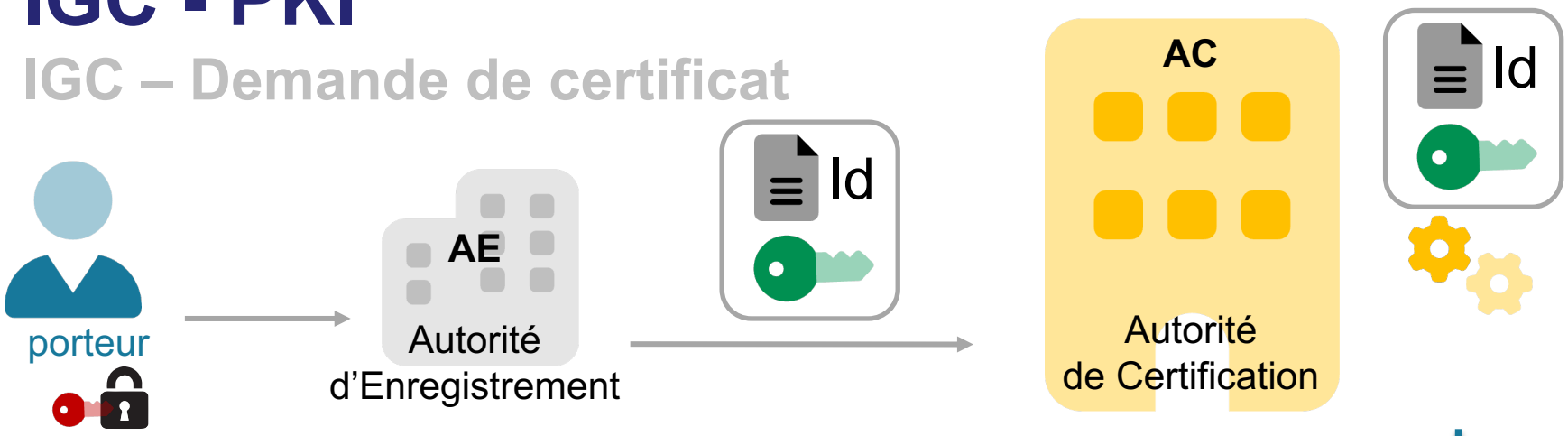
IGC – Demande de certificat



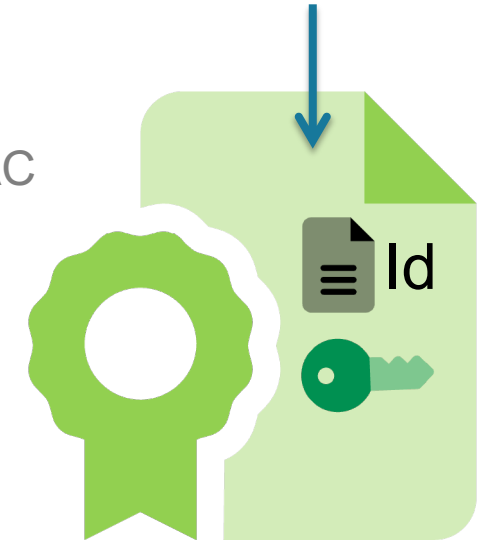
3. Vérification des informations d'identité du porteur par l'Autorité d'Enregistrement

IGC - PKI

IGC – Demande de certificat

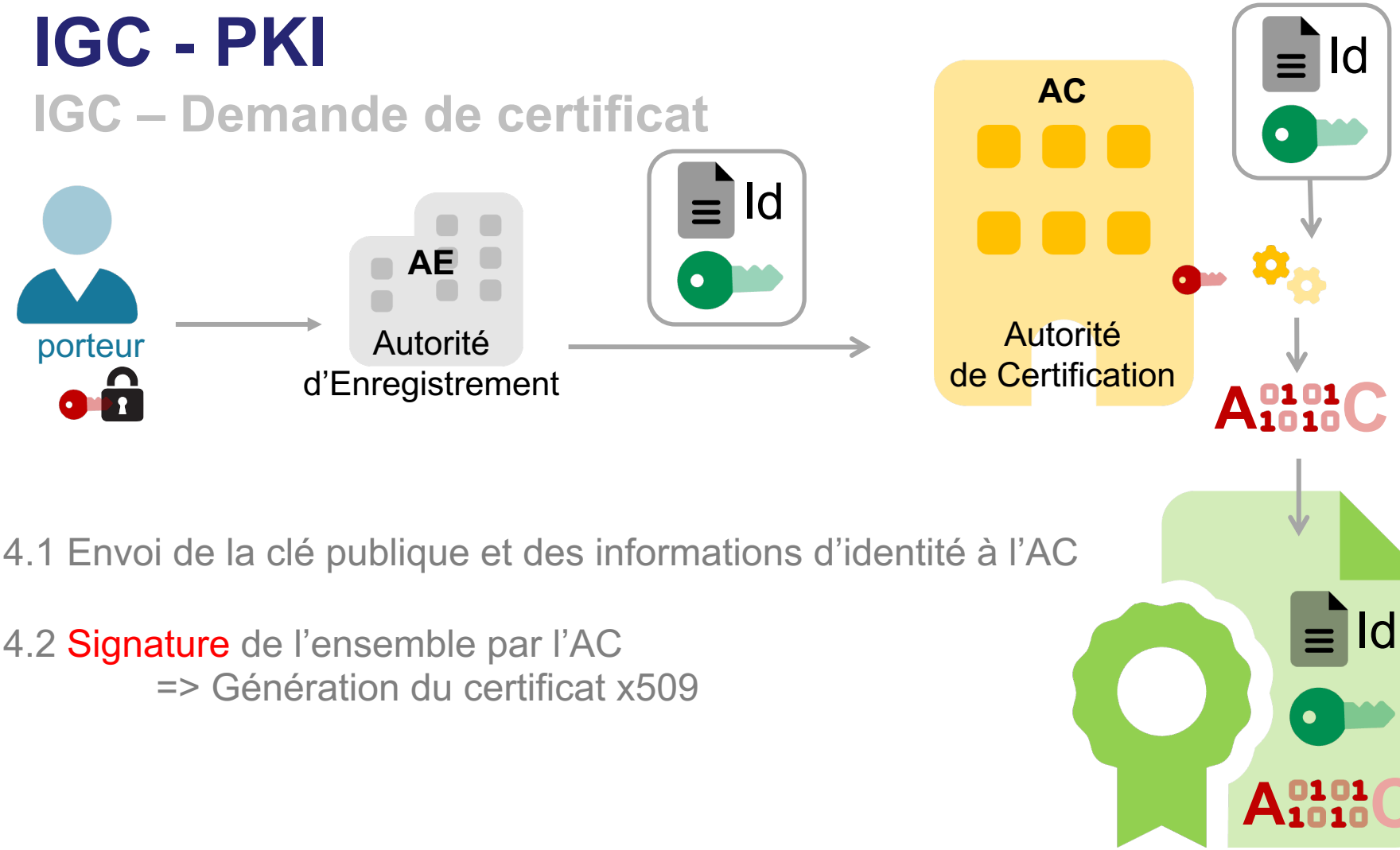


4.1 Envoi de la clé publique et des informations d'identité à l'AC



IGC - PKI

IGC – Demande de certificat

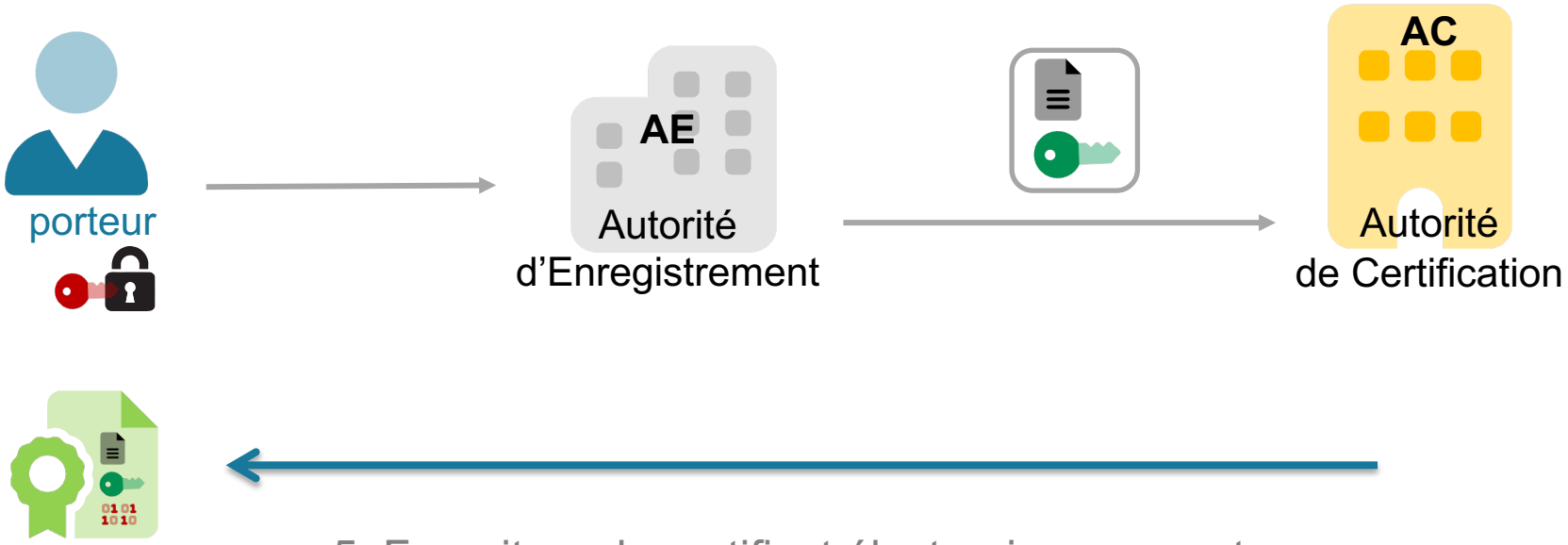


4.1 Envoi de la clé publique et des informations d'identité à l'AC

4.2 Signature de l'ensemble par l'AC
=> Génération du certificat x509

IGC - PKI

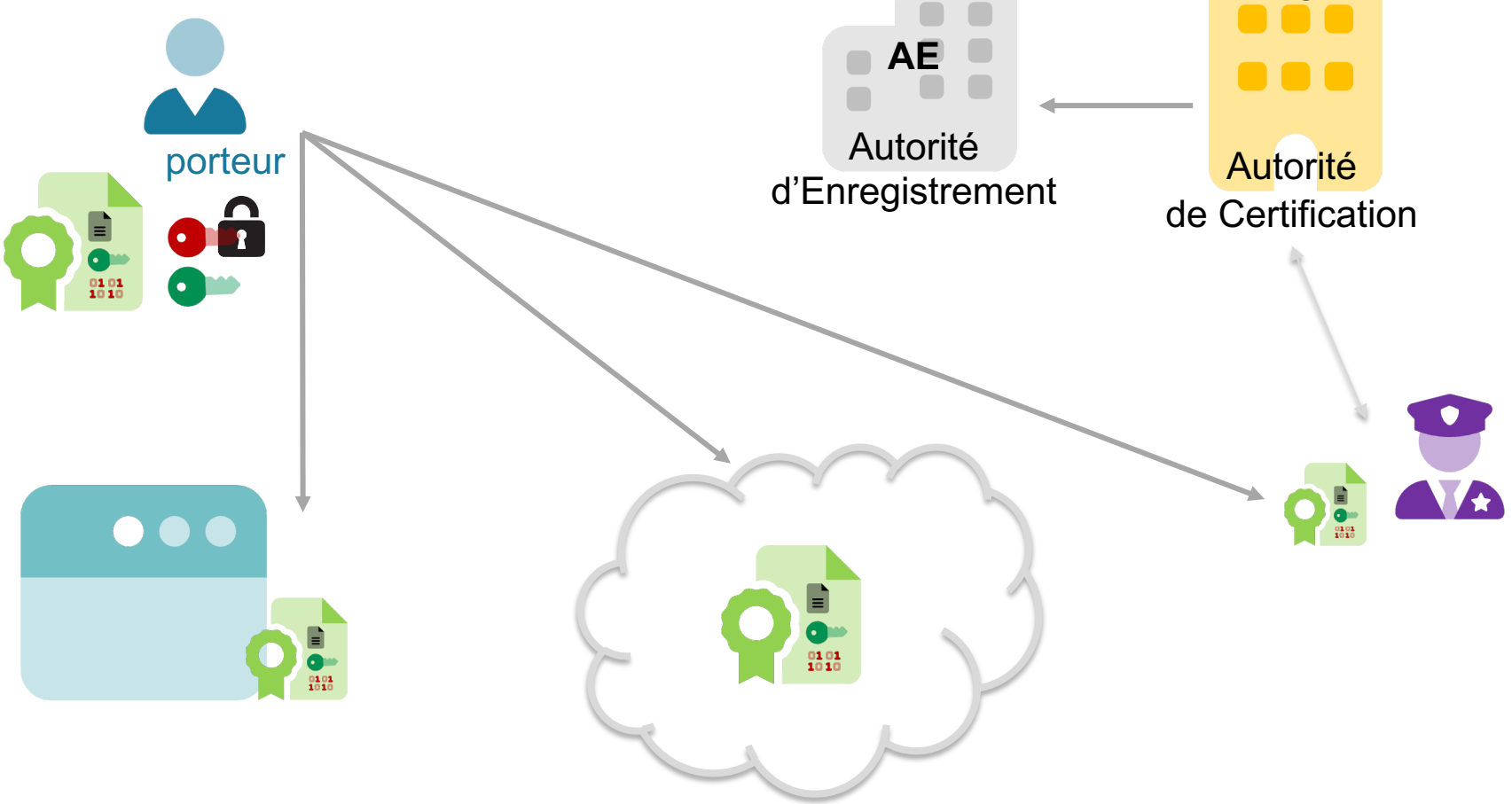
IGC – Demande de certificat



5. Fourniture du certificat électronique au porteur

IGC - PKI

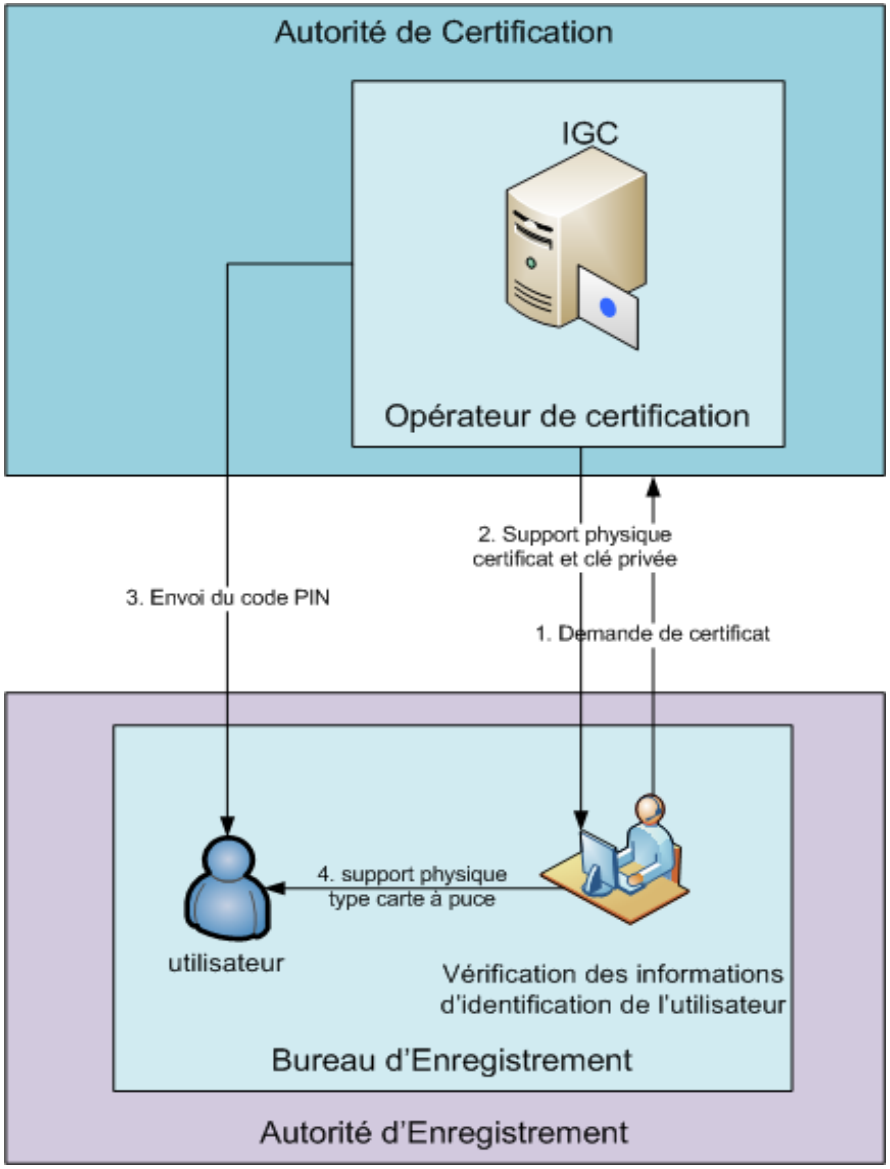
IGC – Demande de certificat



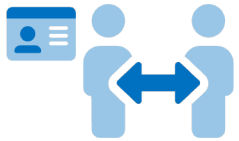
6. Utilisation des éléments

IGC - PKI

AC - OC - AE



Question ?



Une Autorité de Certification émettant des certificats qualifiés doit :

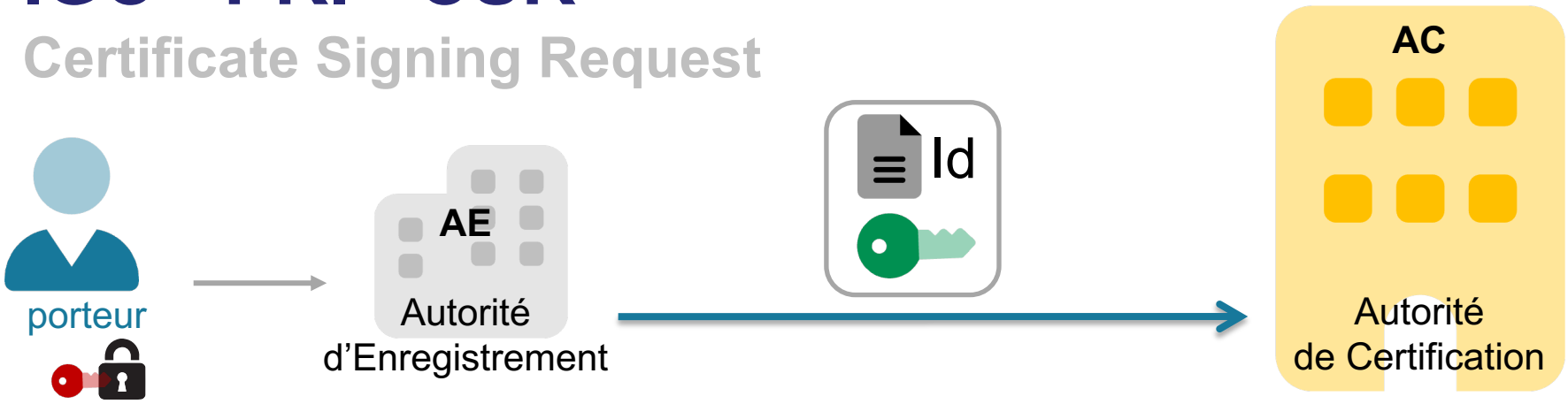
- ❑ Garantir que les clés de signature privées de l'AC stockées par le matériel cryptographique sont détruites lorsque que le dispositif n'est plus utilisé
- ❑ Vérifier par des moyens appropries conformes au droit national l'identité de la personne à qui est délivré un certificat qualifié
- ❑ Conserver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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

IGC - PKI - CSR

Certificate Signing Request

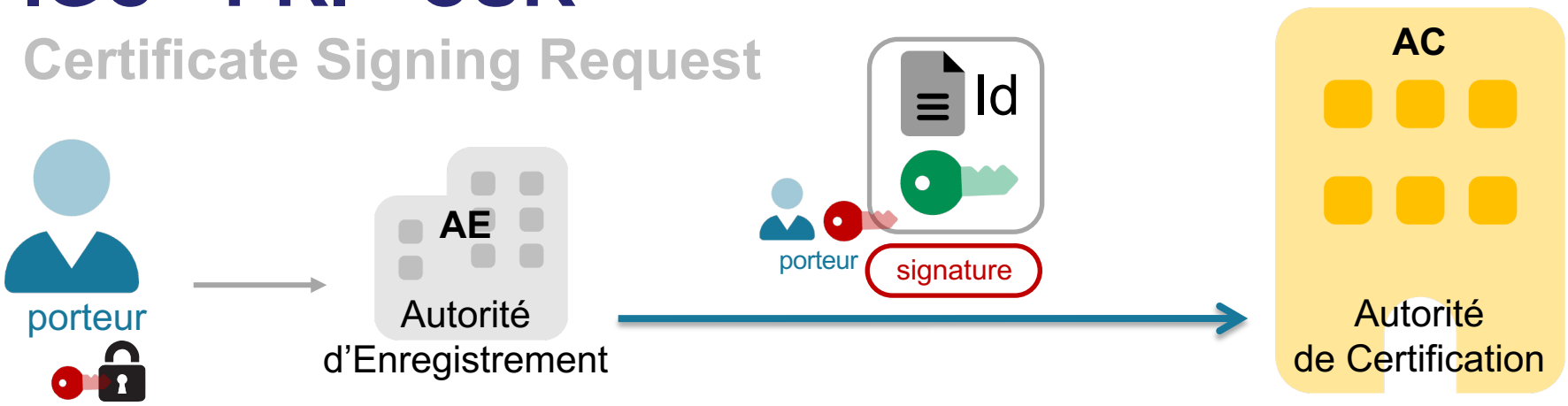


Comment assurer la preuve de **possession** de la **clé privée** du porteur ?

- 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

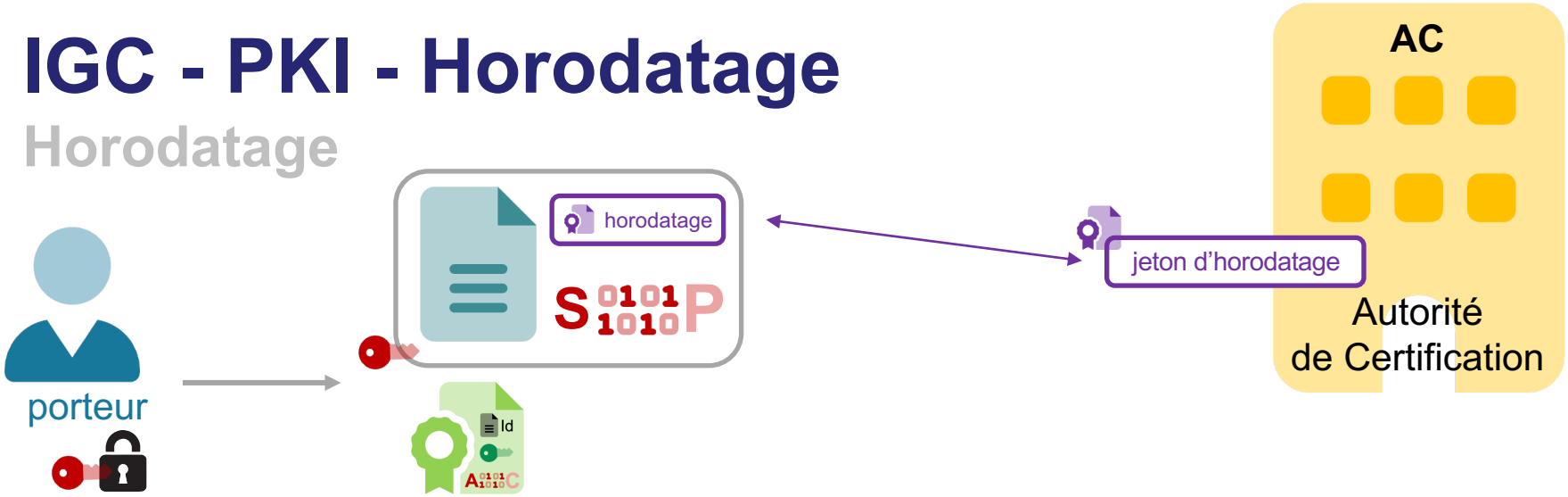
Question

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

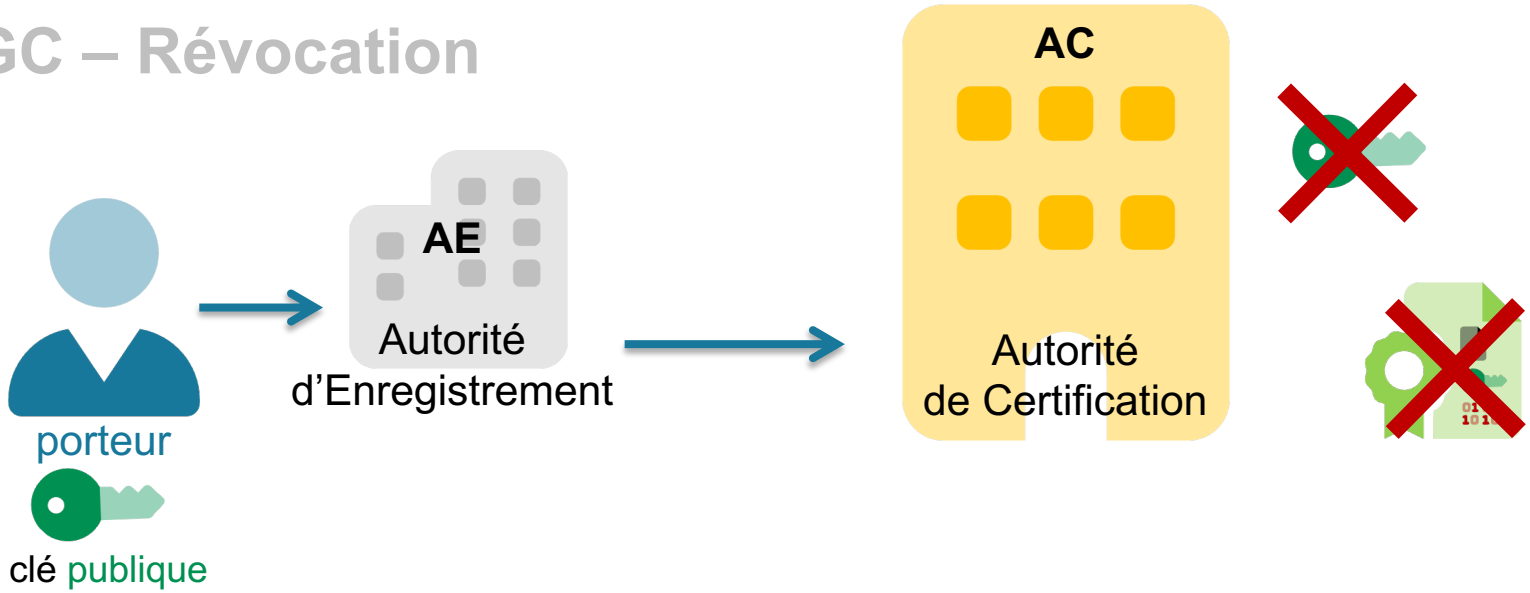
IGC - PKI

IGC – Révocation

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

IGC - PKI

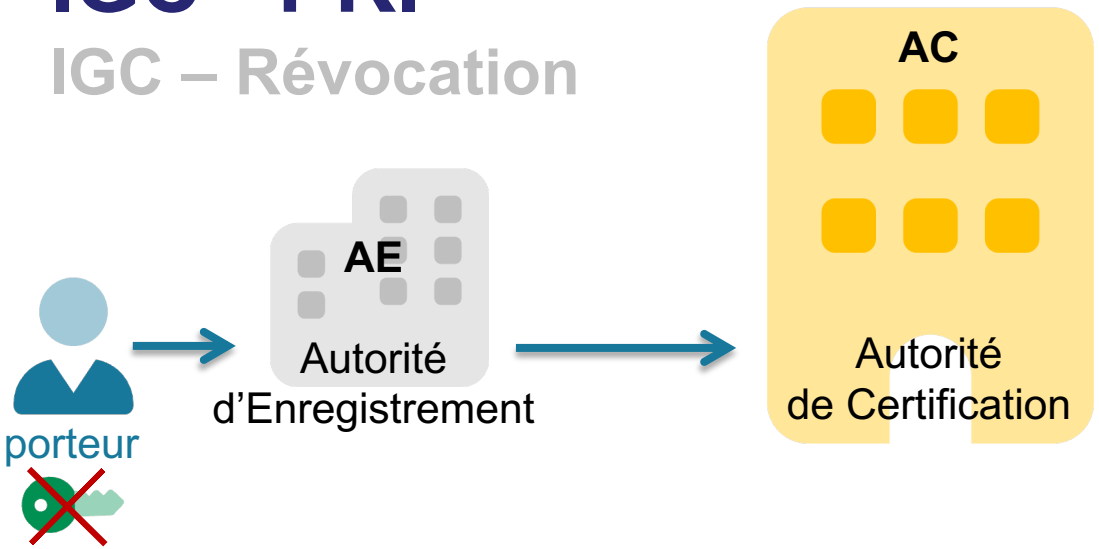
IGC – Révocation



- 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

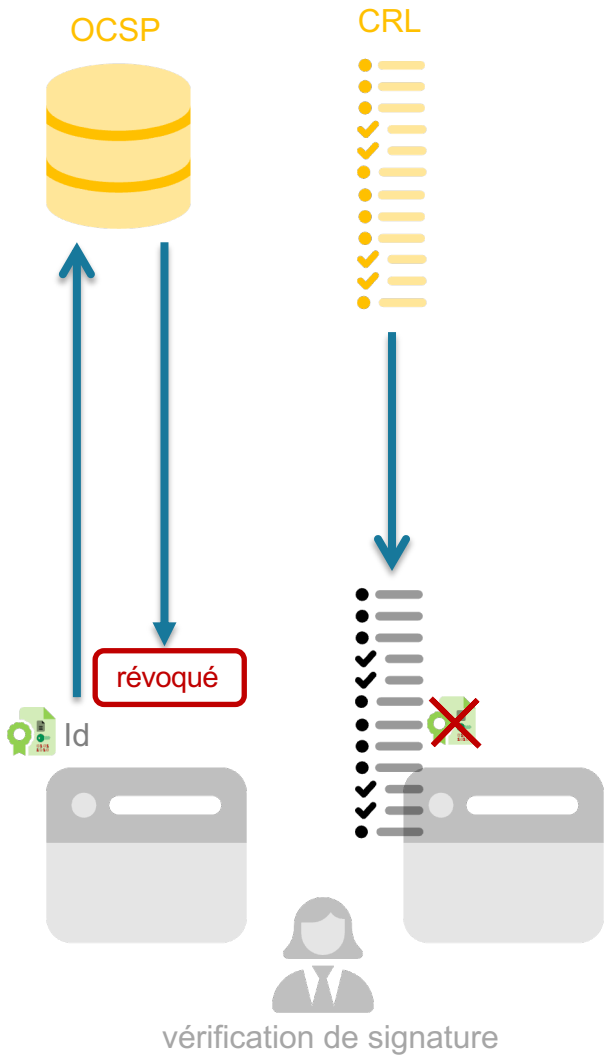
IGC – Révocation



- mise à jour de la liste de révocation
  CRL: Certificate Revocation List

- mise à jour de la base OCSP
- Online Certificate Status Protocol

  OCSP fournit des informations fraiches sur le statut du certificat
  - pas de récupération de CRL : allègement de trafic
  - pas de traitement de CRL : allégement de parsing
    - possibilité de de facturation au « vendeur » et non pas à « l'acheteur »
    - les CRL peuvent être vues comme des "listes de mauvais clients »
    - divulgation d'information non souhaitable



La signature électronique sécurisée #4


```
F96DE8C227A259C87EE1DA2AED5
7C93FE5DA36ED4EC87EF2C63AAE
5B9A7EFFD673BE4ACF7BE8923CA
B1ECE7AF2DCF7AE29A3DA44F235
A24C963FF0DF3CA3599A70E5DA3
6BF1ECE77F8DC34BE129A6CF4D1
26BF5B9A7CFEDF3EB850D37CF0C
63AA2509A76FF9227A55B9A6FE3
D720A850D97AB1DD35ED5FCE6BF
0D138A84CF8DC34BE129F8DC34B
```

La signature électronique sécurisée

sécurisée = avancée et/ou qualifiée


```
F96DE8C227A259C87EE1DA2AED5
7C93FE5DA36ED4EC87EF2C63AAE
5B9A7EFFD673BE4ACF7BE8923CA
B1ECE7AF2DCF7AE29A3DA44F235
A24C963FF0DF3CA3599A70E5DA3
6BF1ECE77F8DC34BE129A6CF4D1
26BF5B9A7CFEDF3EB850D37CF0C
63AA2509A76FF9227A55B9A6FE3
D720A850D97AB1DD35ED5FCE6BF
0D138A84CF8DC34BE129F8DC34B
```

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Complexité

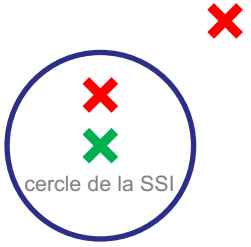
- la signature
  - Compréhension facile
  - Mise en œuvre facile

- la signature électronique
  - Compréhension difficile
  - Mise en œuvre délicate

7e0950bb938539162d268b379595
44efb87b718950bf4721dd5c94f5f7
d12fc4efac9d9b5f0c81bbc1555c3d7
6610ef3080a354e60b625f5c50a23
a6bfd13ec024239ddc0b47706c9a23
11fc38e37161e87501236542732797
2469b3985721cc0feca3b04047a9c5
b559e3471a736f5e4c7b473b2e86b1
b21dd8a829828d f8d6

- la signature électronique sécurisée
  - Compréhension difficile
  - Mise en œuvre très difficile

7e0950bb938539162d268b379595
44efb87b718950bf4721dd5c94f5f7
d12fc4efac9d9b5f0c81bbc1555c3d7
6610ef3080a354e60b625f5c50a23
a6bfd13ec024239ddc0b47706c9a23
11fc38e37161e87501236542732797
2469b3985721cc0feca3b04047a9c5
b559e3471a736f5e4c7b473b2e86b1
b21dd8a829828d f8d6



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.

https://www.legifrance.gouv.fr/loda/id/JORFTEXT000035676246

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/

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

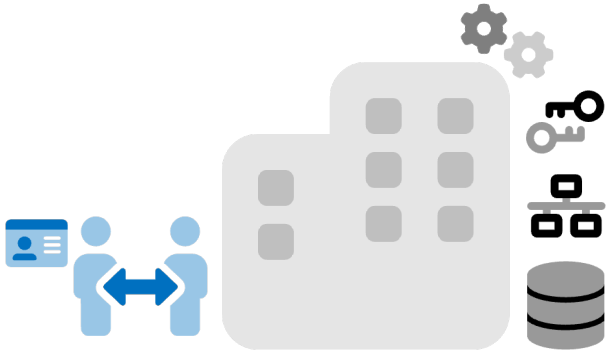
- ETSI
  - EN 319 411-1 – AC non qualifiée
  - EN 319 411-2 – AC qualifiée
  - EN 319 122 – CAdES (CMS)
  - EN 319 132 – XAdES (XML)
  - EN 319 142 – PAdES (ISO-32000 / PDF)
- CEN
  - CWA 14167 : Trustworthy systems / PP des HSM
  - CWA 14169 : PP SSCD
  - CWA 14170 : Application de création de Signature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

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Entités et vocabulaire

les termes et leurs synonymes

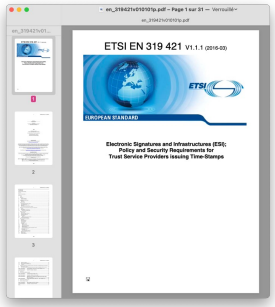


- AE et AC
  - PSCe – PSCo – TSP

- HSM – SSCD – QSCD – Carte à puce

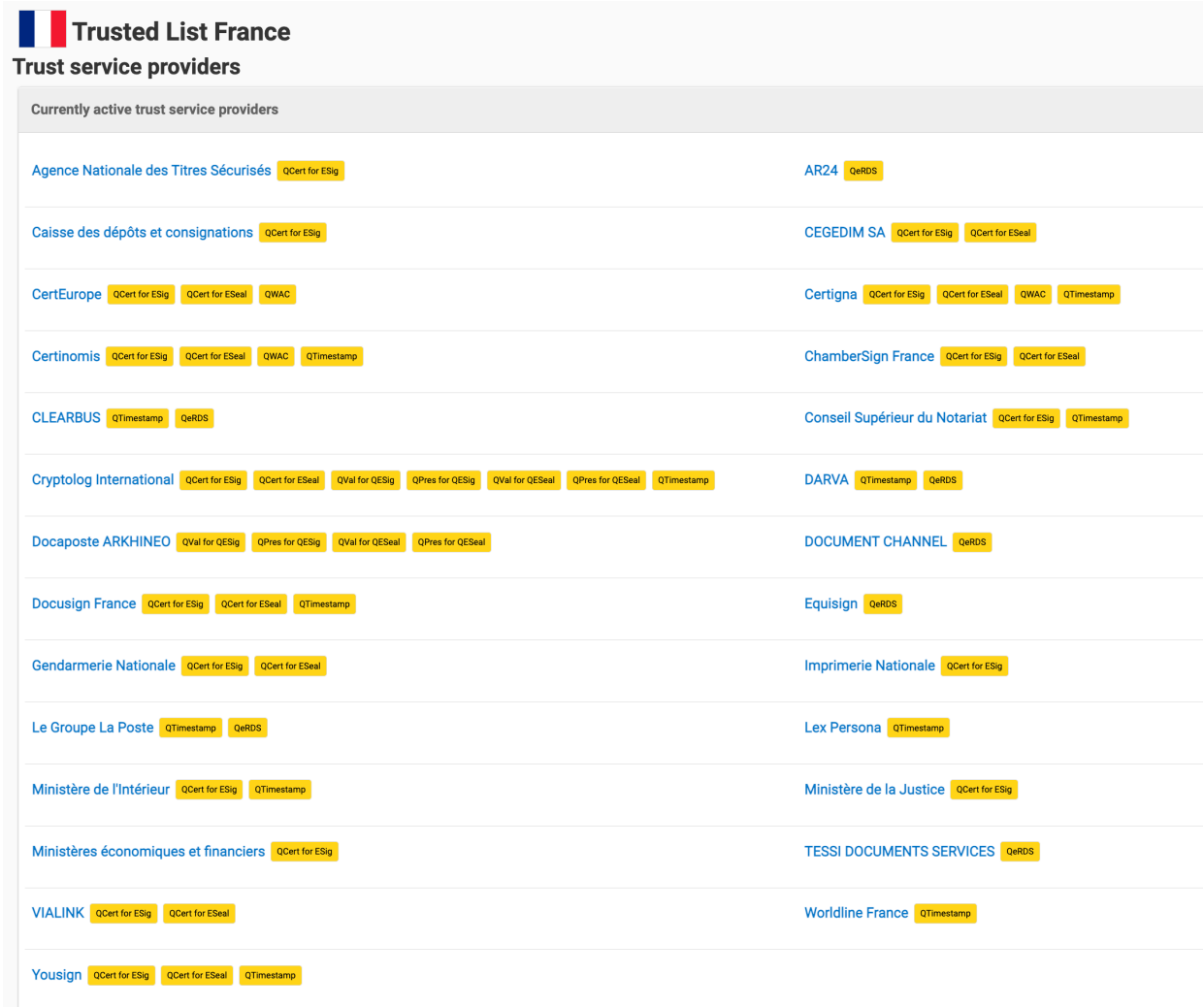
On entend par **SSCD** [Secure-Signature-Creation Device] ou **QSCD** [Qualified-Signature-Creation Device] un Dispositif Sécurisé de Création de Signature. Un SSCD correspond à une « carte à puce » contenant un crypto-système hardware sécurisé, ou encore à un **HSM** (Hardware Security Module), ou encore un « **Secure Element** » ou **TPM** (Trusted Plateform 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	AR24 QeRDS
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 QCert for ESig QCert for ESeal
CLEARBUS QTimestamp QeRDS	Conseil Supérieur du Notariat QCert for ESig QTimestamp
Cryptolog International QCert for ESig QCert for ESeal QVal for QESig QPres for QESig QVal for QESeal QPres for QESeal QTimestamp	DARVA QTimestamp QeRDS
Docaposte ARKHINEO QVal for QESig QPres for QESig QVal for QESeal QPres for QESeal	DOCUMENT CHANNEL QeRDS
Docusign France QCert for ESig QCert for ESeal QTimestamp	Equisign QeRDS
Gendarmerie Nationale QCert for ESig QCert for ESeal	Imprimerie Nationale QCert for ESig
Le Groupe La Poste QTimestamp QeRDS	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 QeRDS
VIALINK QCert for ESig QCert for ESeal	Worldline France QTimestamp
Yousign QCert for ESig QCert for ESeal QTimestamp	

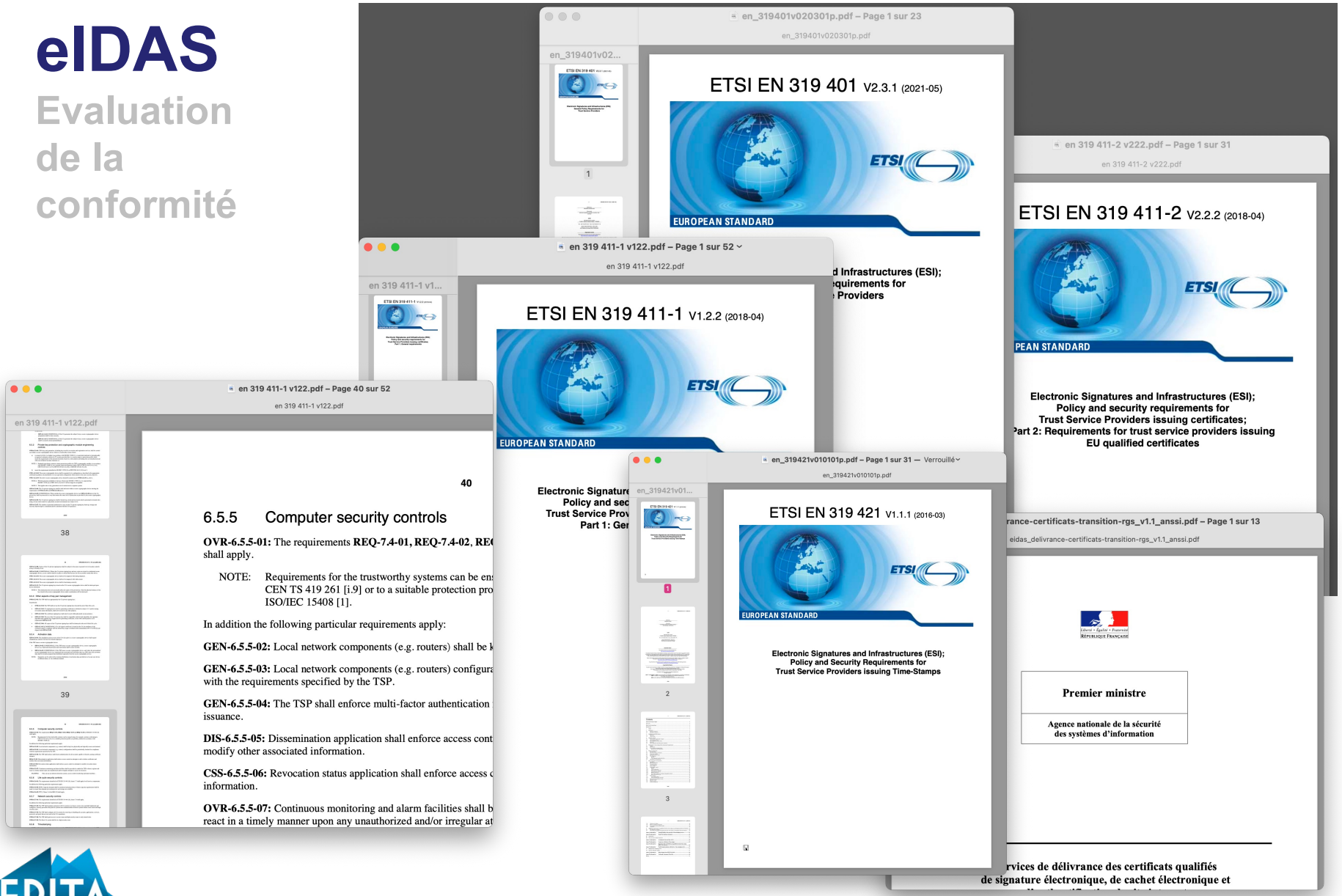
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

STELAU

Audit PSCo/TSP eIDAS - RGS

eIDAS

Evaluation de la conformité



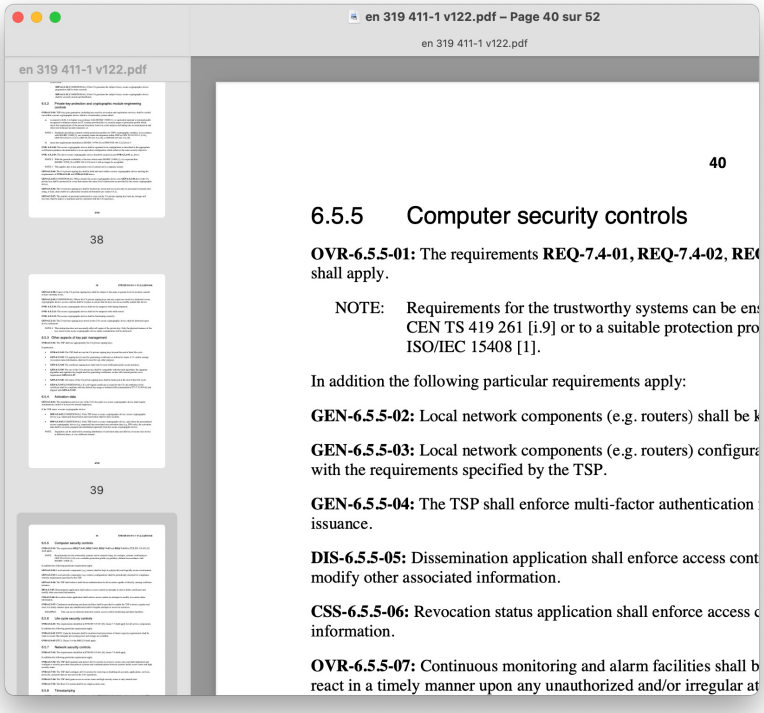
eIDAS

ETSI EN 319 401
Politique générale

ETSI EN 319 411-1
Délivrance de certificats

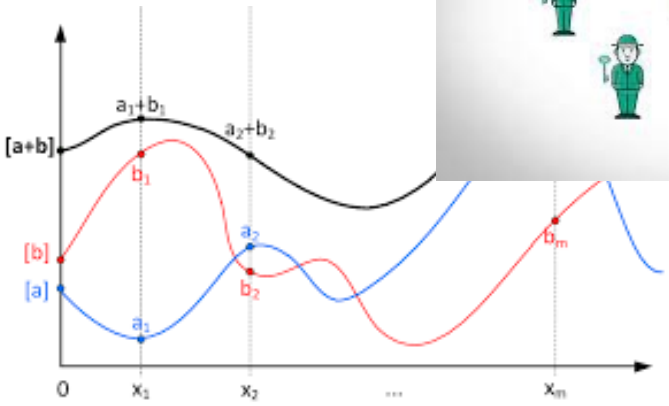
ETSI EN 319 411-2
Délivrance de certificats qualifiés EU

ETSI EN 319 421
Horodatage qualifiés EU



KC : Key Ceremony

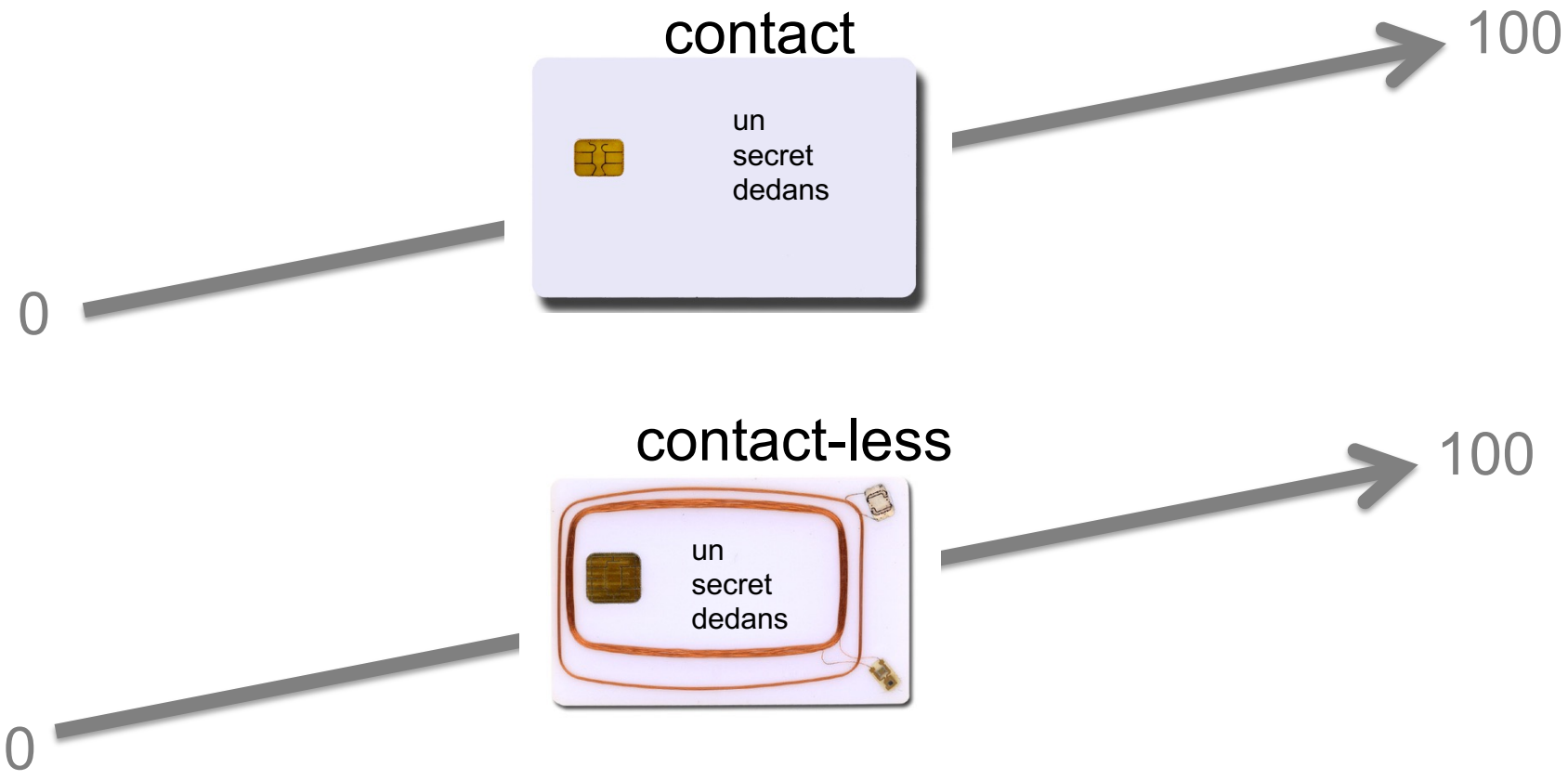
Audit des parts de secrets



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 V1.11
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.

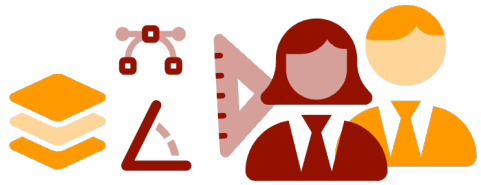
Attention : « c'est (*pas*) sécurisé » ne veut rien dire



Voilà … c'est fini !

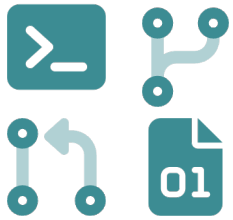
Ingénieur(e)s

- scientifiques
- design (capacité à concevoir)



Code

- préhistoire
- tout à inventer



Stage

- pas très grave
- management

1ère page du rapport le 1er jour + répétitions

Stelau
Hack different.