SÉCURITÉ DES COMMUNICATIONS SPATIALES

« OU COMMENT NE PAS SE FAIRE RANÇONNER SON SATELLITE »

Mardi 26 janvier 2021

Intervenant : Benoît TRANIER

INP TOULOUSE ENSEEIHT

ThalesAlenia Space
a Thales / Leonardo company

INTERNATIONAL

La France accuse la Russie de tentative d'espionnage par satellite

Selon la ministre de la défense Florence Parly, le satellite russe Louch-Olymp s'est approché d'un peu trop près du satellite franco-italien Athena-Fidus en 2017.

Le Monde avec AFP · Publié le 07 septembre 2018 à 17h42 - Mis à jour le 08 septembre 2018 à 06h42

Lecture 1 min.

AGENDA

1. Introduction
2. Rappels de SSI
3. Rappels de Cryptographie
4. Les systèmes spatiaux
5. Orbitographie
6. Les missions spatiales
7. Les liens spatiaux
8. Menaces et analyse de sécurité
9. Infrastructures de gestion des clés
10. La menace Quantique
10. Conclusion

INTRODUCTION

Dans cette présentation, les sujets sont identifiés selon leur niveau de difficulté avec des pictogrammes dédiés :

Raoul le chat permet d'identifier les sujets faciles à appréhender qui ne font pas intervenir des notions complexes.

Par ailleurs, Raoul interviendra régulièrement dans les planches pour apporter des précisions toujours utiles et pertinentes.

Le disciple permet d'identifier des sujets plus ardus et pour lesquels il faudra être attentif, mais rien d'insurmontable rassurez-vous.

Léonard permet d'identifier des sujets qui, normalement, requièrent des connaissances précises. Mais ici, il faudra faire l'effort de mémoriser quelques postulats afin d'appréhender dans toute leur complexité les sujets présentés. Soyez persévérant ça vaut le coup !

INTRODUCTION

Dans cette partie nous allons parler de 3 personnages : **Alice**, **Bob** et **Eve** :

⇒ **Alice** et **Bob** représentent les « gentil(le)s » qui essaient de communiquer ensemble et à l'abri des regards indiscrets,

⇒ **Eve** qui représente « le(la) méchant(e) » qui essaie d'intercepter ou de perturber les communications entre Alice et Bob (Eve = contraction de "**E**a**VE**sdorpper" qui signifie : « personne qui écoute aux portes »).

Alice et Bob utilisent, pour communiquer, un canal de communication qui leur permet d'échanger leurs messages. Eve s'immiscera dans ce canal pour tenter toutes les actions possibles pour duper Alice et Bob.

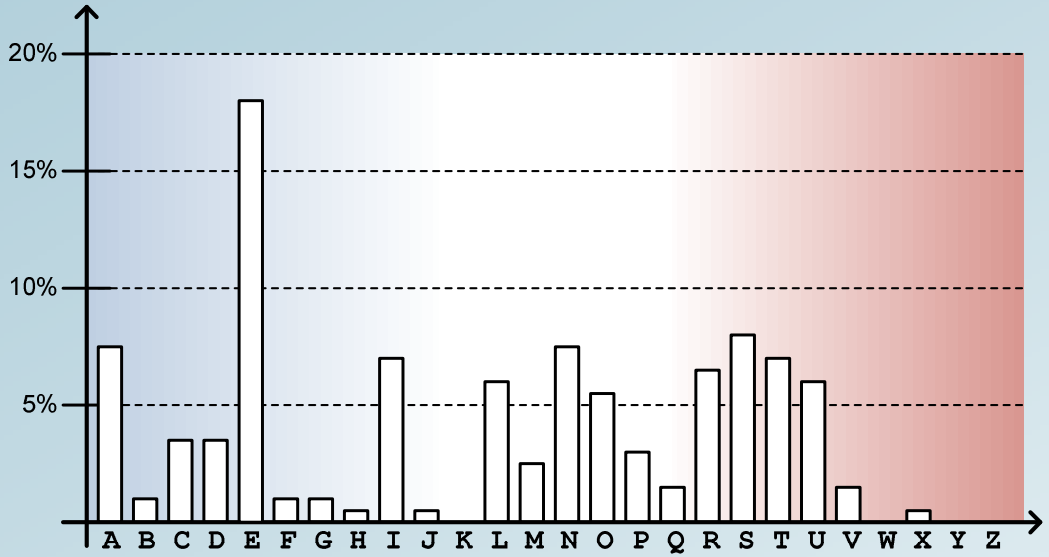
RAPPELS SUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

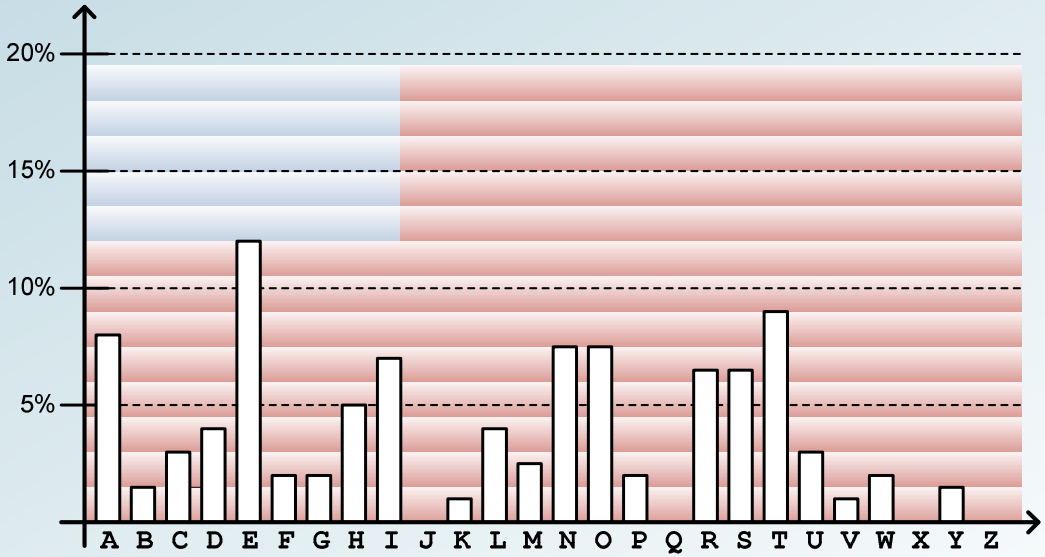
RAPPEL DE SSI

Tout type de message est transcrit aux travers d'un système de codage qui permet d'échanger des informations entre ceux qui partagent ce système de codage.

Pour les langues le "système de codage" repose sur un alphabet et un dictionnaire.

A partir de là, il est possible de faire ressortir des caractéristiques propres à chacun des langages même s'ils sont assez proches (ex: français et anglais).

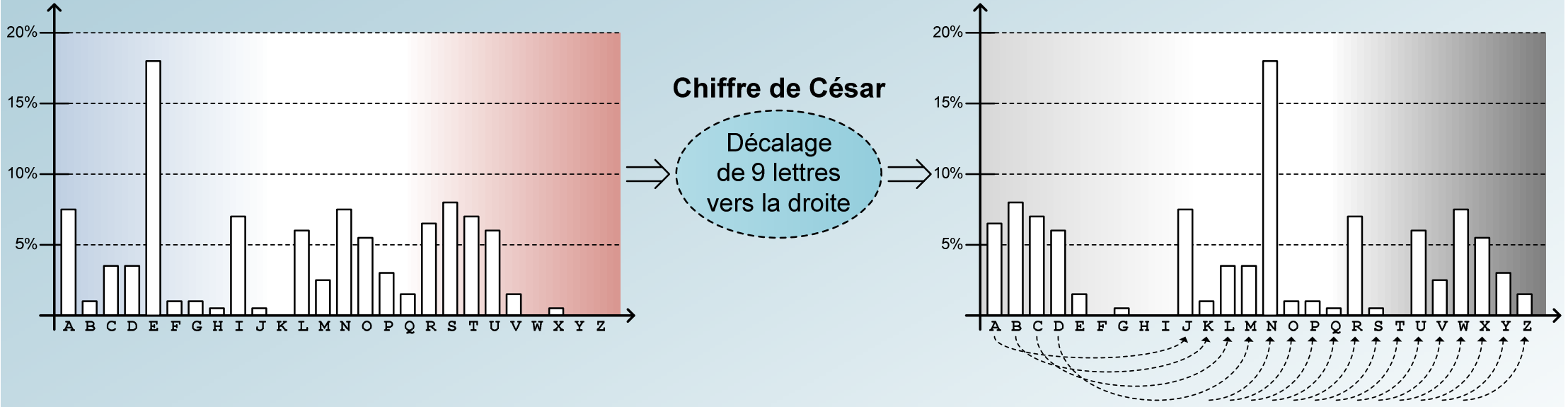




Il est toujours possible, pour l'auteur d'un message, de "tordre" la statistique en choisissant les mots à dessin. L'exemple le plus connu étant le lipogramme en "E", le roman "La Disparition", de Georges Perec pour lequel la lettre "E" n'est pas utilisée une seule fois sur les 300 pages que contient le roman!

RAPPEL DE SSI

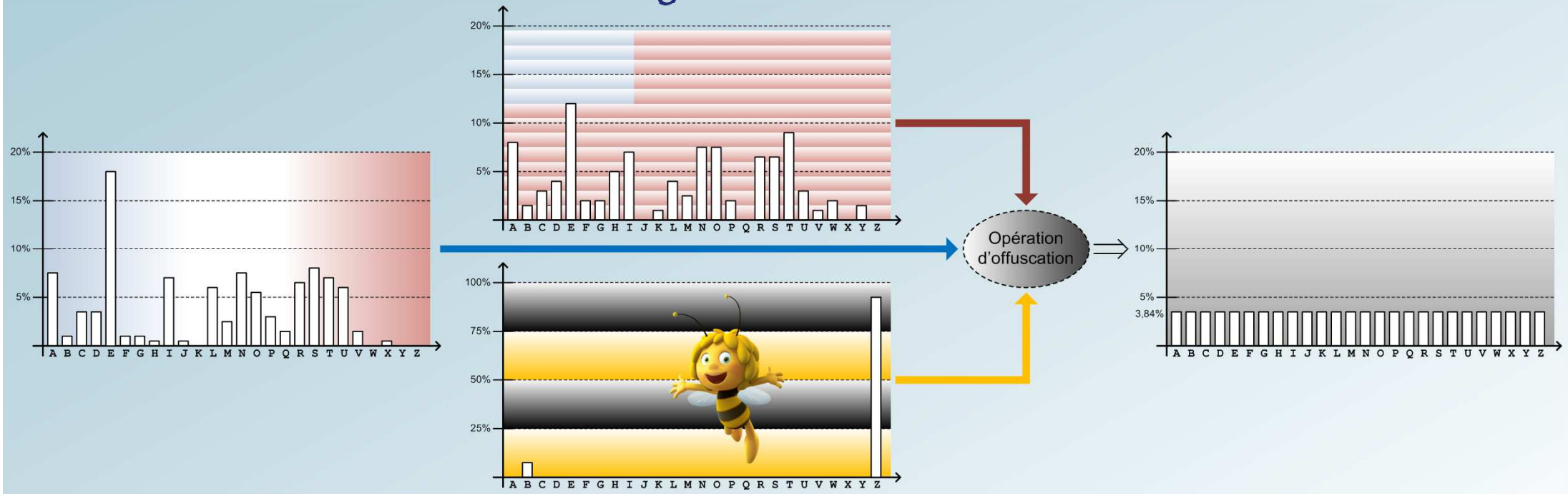
Une cryptographie faible (ex: chiffre de César) ne permet pas de dissimuler complètement les caractéristiques fondamentales des messages clairs initiaux et permet même de remonter à la clé et donc de retrouver les messages clairs!



*"**Je m'appelle Raoul**" donne ➔ "**Sn v'jyynuun Ajxdu**" avec un chiffre de César dont la clé vaut 9.*

RAPPEL DE SSI

Une cryptographie forte doit permettre de dissimuler complètement les caractéristiques fondamentales des messages clairs. Et ce, quels que soient la diversité et le format des messages clairs initiaux.

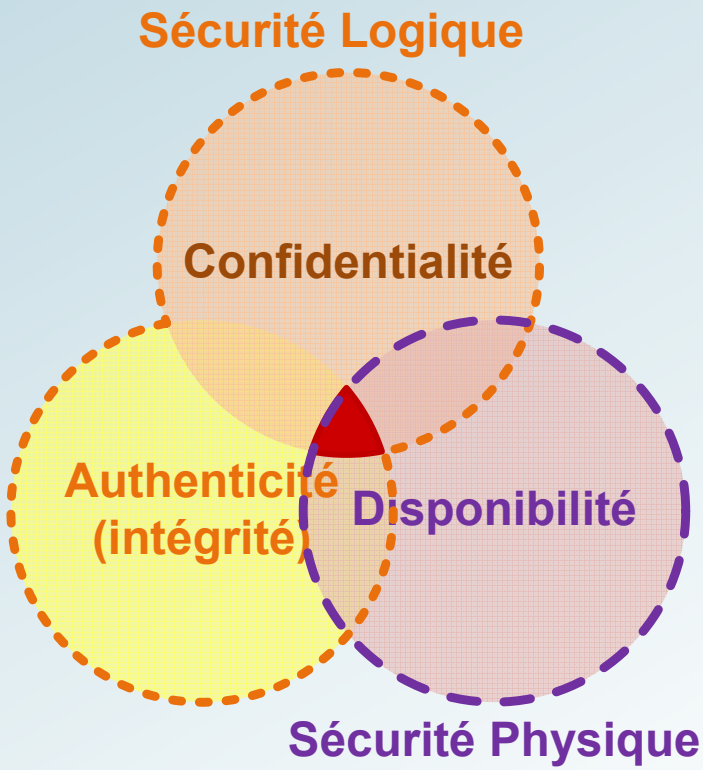


En cryptographie, la sécurité repose sur la capacité du système à produire des messages chiffrés qui ont les exactes caractéristiques d'un message aléatoire.

RAPPEL DE SSI

La sécurité d'un système d'information (ou d'un canal de communication) repose sur 3 principes majeurs :

- La **Confidentialité**, qui garantit que seuls les utilisateurs autorisés auront accès au contenu de l'information,
- **L'Authenticité**, qui garantit que l'information échangé est intègre et de source avérée (elle s'applique à l'intégrité logique de l'information elle-même, mais aussi à l'authenticité de l'émetteur du message dans le cas d'un échange entre deux parties distinctes) ,
- La **Disponibilité**, qui garantit que l'information est accessible ou bien que le canal qui permet d'accéder à l'information est disponible et opérationnel.



*Souvent, il est fait référence aux acronymes suivants : **SSI** pour la **S**écurité des **S**ystèmes d'**I**nformation (très utilisé par l'ANSSI et la DGA) ou **ITS** (son équivalent anglais pour **I**nformation **T**echnology **S**ecurity)*

RAPPEL DE SSI

- La cryptographie permet de garantir les services de sécurité suivants:
  - **La confidentialité**,
  - **L'authenticité**.
- La cryptographie ne permet pas de garantir par elle-même la disponibilité d'une information ou la disponibilité d'un canal de communication/transmission,
- La disponibilité est assurée par des mesures particulières. En général, par des mesures physiques : redondances des chemins/sources, formatage du canal de transmission ou autre.

La cryptographie peut néanmoins être utilisée en support pour l'implémentation d'une fonction de protection en disponibilité, mais elle ne peut la garantir à elle seule.

RAPPEL DE SSI

- Lors d'un échange d'information entre deux parties distinctes, il faut être capable de garantir :
  - L'authenticité des deux parties (ou authenticité de la source et du destinataire) : Alice et Bob sont bien ceux qu'ils prétendent être. Aucune tierce partie n'usurpe l'identité de l'un ou de l'autre,
  - L'authenticité des messages : lorsque Bob reçoit un message d'Alice, le message reçu est **authentique** (ou intègre) et est tel qu'il a été émis par Alice; il n'a pas été modifié en cours de route.
- Afin d'éviter toute confusion par la suite nous utiliserons les termes suivants :
  - **Authenticité** ⇒ pour identifier l'authenticité des parties impliquées dans les échanges,
  - **Intégrité** ⇒ pour identifier l'authenticité des messages échangés.

La non-répudiation est une fonctionnalité dérivée de l'authentification et permet de garantir qu'une donnée a bien été émise et reçue de part et d'autre par les parties authentifiées.

RAPPELS DE CRYPTOGRAPHIE

RAPPELS DE CRYPTOGRAPHIE

- Les systèmes usuels de cryptographie sont fondés sur la complexité algorithmique de leur déchiffrement,
- Un système est considéré comme sûr, si un attaquant a besoin d'une **puissance de calcul déraisonnable** pour déchiffrer le message en un **temps raisonnable**,
- Tout le travail des cryptologues consiste à trouver des algorithmes qui compliquent au maximum la tâche des cryptanalyses et à évaluer leur complexité, en donnant des définitions rigoureuses des termes "déraisonnable" et "raisonnable" mentionnés ci-avant,
- Un système de chiffrement est considéré comme sûr, d'après la théorie de l'information, si sa résistance découle purement de la théorie de l'information sans dépendre des moyens ou des capacités technologiques externes. On considère que l'adversaire ne possède pas assez d'information pour casser le chiffrement même avec une puissance de calcul illimitée.

Reste plus qu'à trouver l'algorithme idéal et théoriquement sûr!

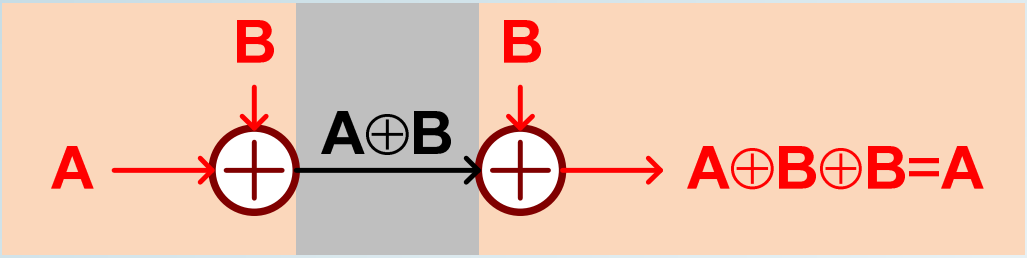
RAPPELS DE CRYPTOGRAPHIE

- La fonction **OU exclusif** (XOR en anglais) est définie de la manière suivante : A⊕B=A./B+/A.B ➔ le résultat du XOR ne vaut "1" que si un seul des deux éléments d'entrée vaut "1", le résultat vaut "0" sinon.
- Voici quelques propriétés remarquables du XOR :

⇨ A ⊕ 1 = /A, A ⊕ 0 = A, A ⊕ A = 0,

⇨ **A ⊕ aléa.x = aléa.y** ⇒ propriété importante du point de vue de la confidentialité,

⇨ **A ⊕ B ⊕ B = A** ⇒ c'est cette dernière propriété qui nous intéresse tout particulièrement et qui est illustrée dans la figure ci-après.



Vous ne voyez pas ce que le OUEX à avoir avec la cryptographie?
Patience ça va venir…

RAPPELS DE CRYPTOGRAPHIE

- Si nous remplaçons maintenant "A" et "B" par des termes plus explicites, nous obtenons la figure ci-après :

- Si les masques sont aléatoires et si, pour chacun des messages, un masque différent (et de même longueur que le message) est utilisé, alors ce type de chiffrement est, selon la théorie de l'information de Shannon, théoriquement sûr,
- Ce type de chiffrement est connu sous les noms suivants : Chiffrement à masques jetables, Chiffre de Vernam ou « **O**ne **T**ime **P**ad cryptography »

Si le chiffrement par XOR est si sûr et si fiable, alors pourquoi s'embêter avec tout un tas d'algorithmes de cryptographie tous plus complexes les uns que les autres?

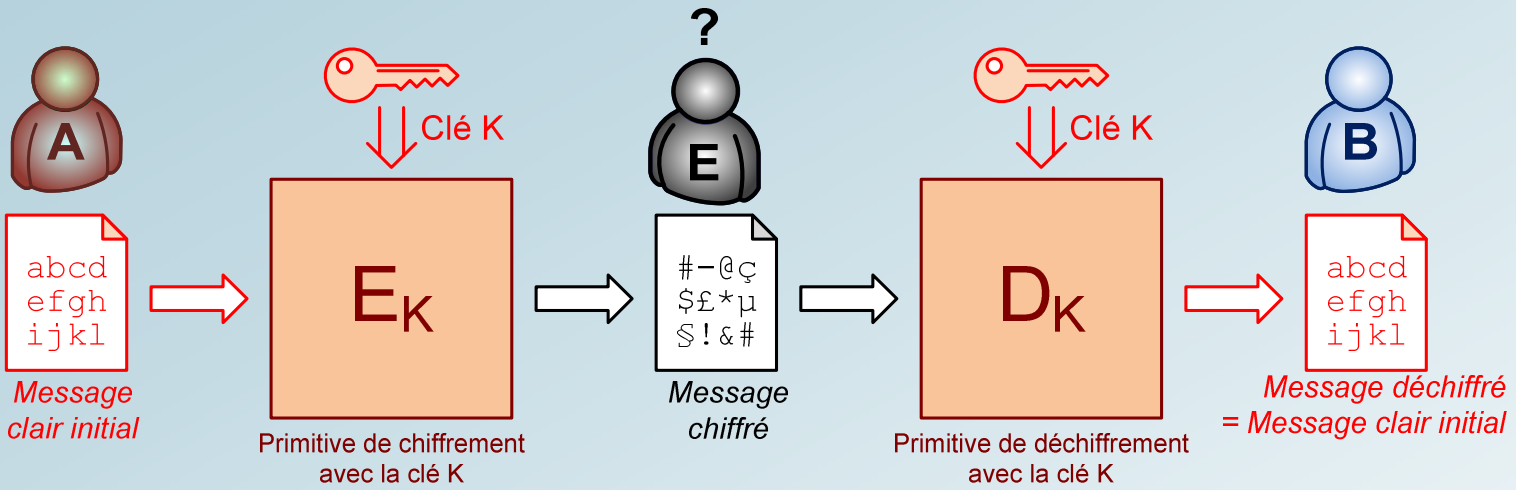
RAPPELS DE CRYPTOGRAPHIE

- Le chiffrement par masque jetable est quand même entaché de quelques limitations majeures,
- Premièrement, il n'assure que la confidentialité des messages. Il ne permet pas d'authentifier l'émetteur du message ni de garantir l'intégrité des messages chiffrés échangés,
- Deuxièmement, il est nécessaire, lors des échanges, qu'Alice et Bob trouvent un moyen d'échanger autant de masques (= clés secrètes) qu'ils ont de messages à échanger. Ce qui est pratiquement impossible compte tenu des besoins actuels en termes de communication,
- Enfin, les masques doivent être issus d'une source aléatoire imprédictible et non reproductible.

Ici, cela soulève un autre point fondamental en cryptographie : celui de la distribution des clés secrètes. Un vrai casse-tête!

RAPPELS DE CRYPTOGRAPHIE

- La cryptographie à clé secrète symétrique repose sur l'utilisation par Alice et par Bob d'une clé identique (i.e. symétrique) connue d'eux seuls !
- La sécurité des données chiffrées échangées repose :
  - Sur la capacité d'Alice et Bob à garantir la confidentialité de la clé secrète,
  - Sur la robustesse de l'algorithme utilisé pour chiffrer/déchiffrer les messages.

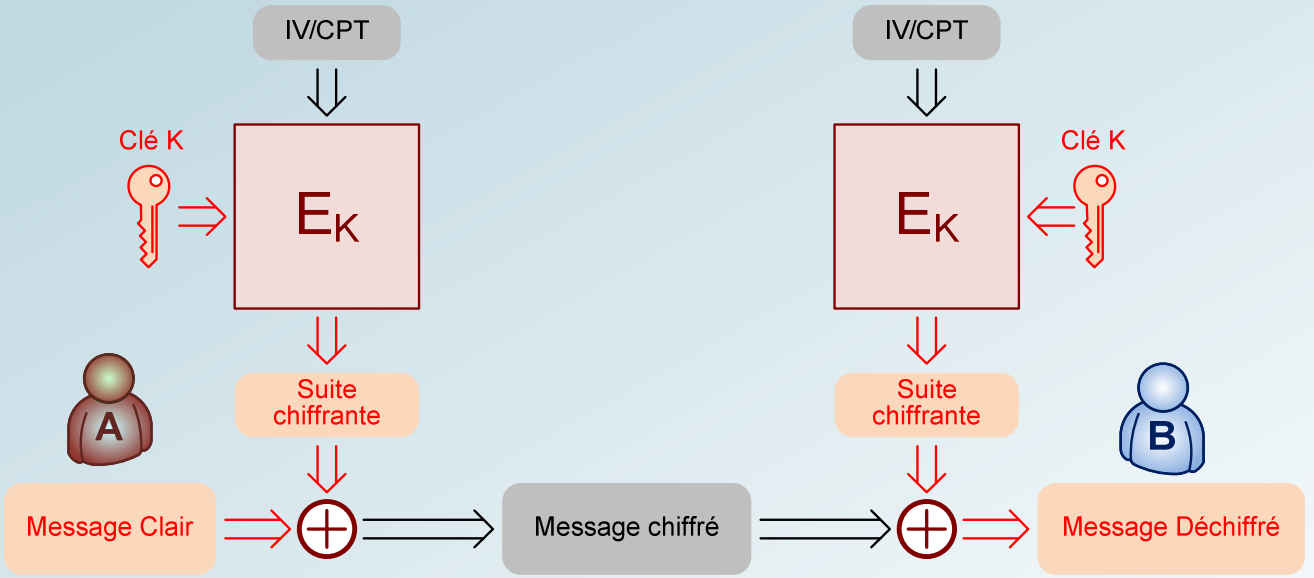


*Lorsque seule la confidentialité est assurée, alors on parle de mode "EO" pour **E**ncryption **O**nly.*

Attention, l'élément le plus sensible ici n'est pas la clé mais le message clair, celui qu'Alice et Bob souhaitent échanger à l'abri des regards indiscrets.

RAPPELS DE CRYPTOGRAPHIE

- Selon les algorithmes utilisés, il peut être nécessaire de modifier l'implémentation afin d'assurer une meilleure sécurité.
- Ici, nous retrouvons notre célèbre XOR,
- Les algorithmes (E_K) servent, sur la base d'une clé secrète commune, à produire une suite chiffrante (pseudo-aléatoire),
- Cette suite chiffrante est utilisée comme masque de chiffrement/déchiffrement mais sans les contraintes d'échange des masques !
- L'algorithme est utilisé en mode compteur.



Attention, la robustesse cryptographique de cette implémentation, même si elle reprend la technique du masque jetable, dépend de la robustesse de l'algorithme qui produit la suite chiffrante (i.e. la séquence des pseudo-aléas issue de E_K).

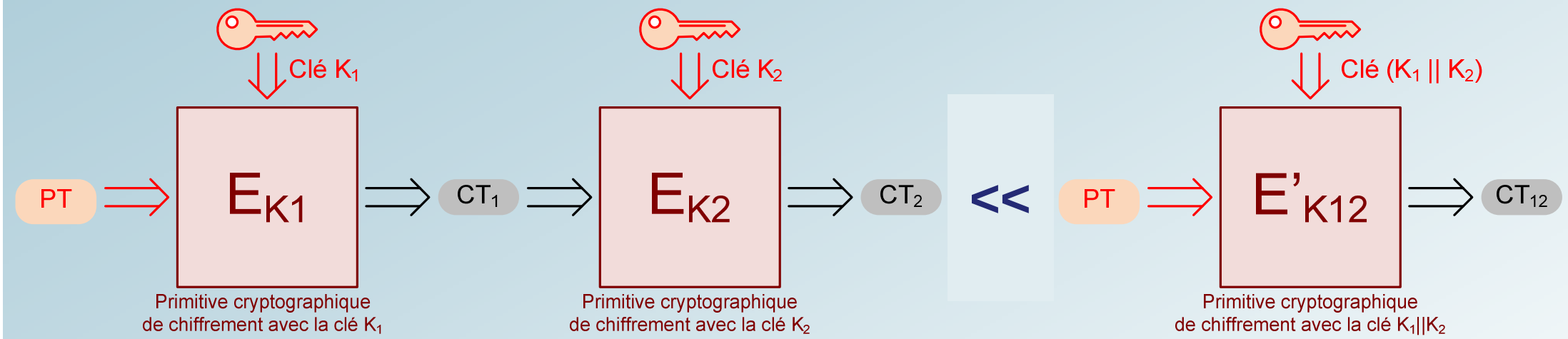
RAPPELS DE CRYPTOGRAPHIE

- L'attaque la plus connue en cryptographie est l'attaque par force brute ou attaque exhaustive. Nous considérons que, si nous essayons 50% des clés possibles, nous avons, en moyenne, une bonne chance de trouver la bonne clé,
- Pour un algorithme avec des clés de 128bits, il faut en moyenne $0.5 * 2^{128}$ soit $2^{127} = 1.7^{E}38$ tentatives pour trouver la clé de chiffrement,
- Plus la clé est longue, plus ce type d'attaque prend du temps. Par exemple : pour un ordinateur capable de mener $1^{E}15$ attaque par seconde (1 toutes les femto secondes!), il faudrait, en moyenne, $1.70^{E}23$ secondes pour trouver la clé soit $5.4^{E}15$ années (plus de 400 000 fois l'âge actuel de l'univers!),
- Il existe de nombreuses autres attaques et méthodes d'analyse: attaque à texte clair choisi, attaque à chiffré connu, cryptanalyse linéaire, cryptanalyse différentielle, etc…

Les algorithmes publiés (AES par exemple) sont préférables aux algorithmes non publiés, car ils sont "cryptanalysés" par toute la communauté. AES n'a toujours pas été cassé d'une manière ou d'une autre après 20 ans de bons et loyaux services. Il est considéré comme sûr.

RAPPELS DE CRYPTOGRAPHIE

- Est-il possible de renforcer le chiffrement à clé secrète symétrique sans créer un nouvel algorithme ?
- Ces deux configurations sont-elles équivalentes ?

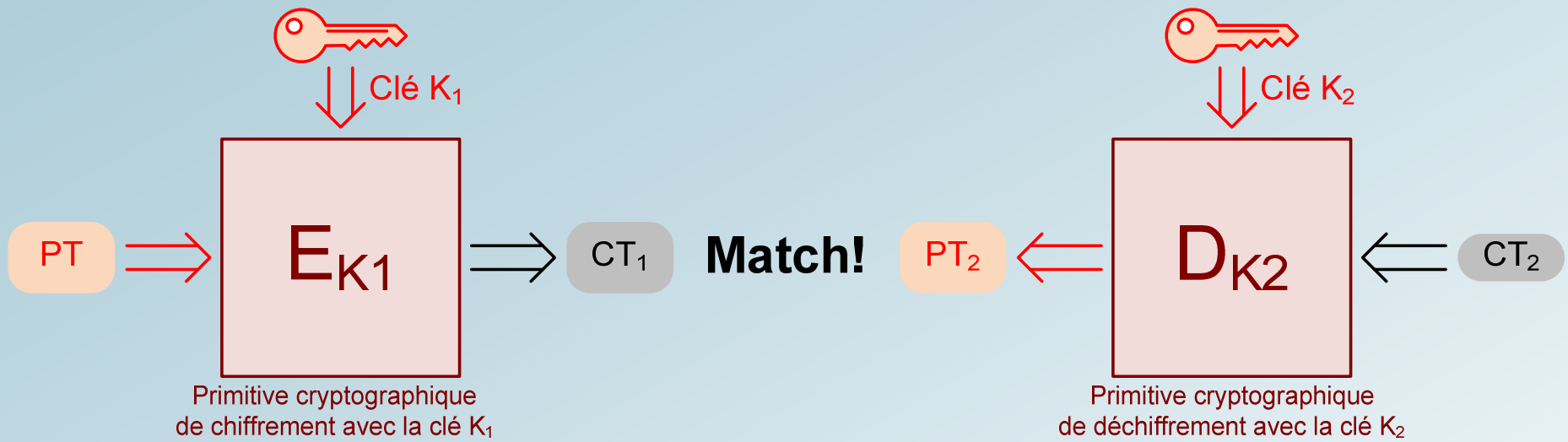


- Nous pourrions le croire, mais elles ne le sont pas!

Il faut être très prudent lorsqu'il s'agit de proposer de nouvelles solutions !

RAPPELS DE CRYPTOGRAPHIE

- Meet-in-the-middle Attack (attaque par rencontre au milieu),

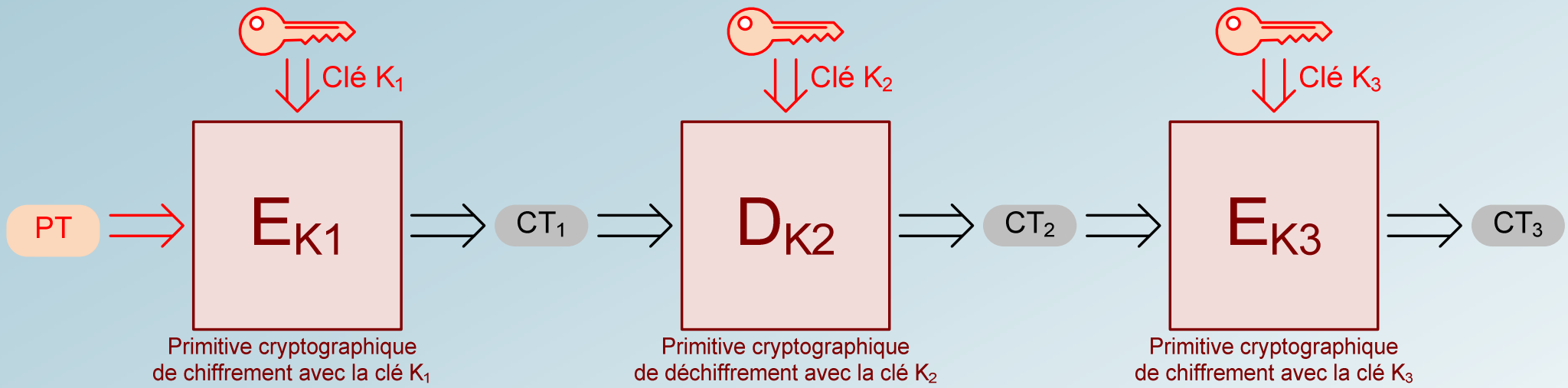


- Il suffit de mener une attaque par force brute simultanée sur le clair initial (PT) et sur le 2ème chiffré (CT_2) ➔ si $CT_1 = PT_2$ alors il y a une très forte probabilité que le couple K_1/K_2 soit le bon !
- Si les 2 clés sont de taille K, alors il suffit de mener $2*2^K$ opérations soit 2^{K+1} et non pas 2^{2*K} opérations!

Il ne faut jamais improviser ou bricoler en cryptographie.
Il faut toujours se référer aux standards!

RAPPELS DE CRYPTOGRAPHIE

- La contre mesure est la suivante ➔ exemple : le Triple DES

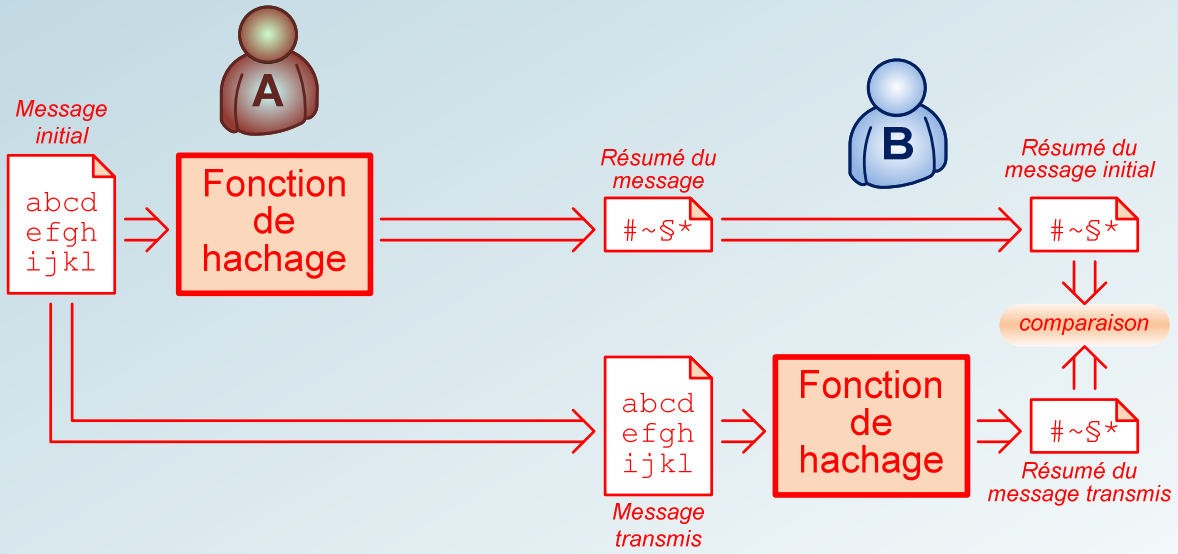


- Attention quand même, car la résistance effective (= taille de la clé effective) ne représente que 2 fois la taille de la clé initiale et non 3 !
- Dans le cas de Triple DES, il faut 168bits de clé pour obtenir une résistance effective équivalente à une taille de clé de 112bits!

Si la primitive cryptographique est bien faite, alors il est possible de chiffrer des données en utilisant la primitive de déchiffrement (D_K), et inversement !
C'est le cas pour le DES et l'AES.

RAPPELS DE CRYPTOGRAPHIE

- L'intégrité des messages échangés au travers d'un canal de communication est assurée par une fonction dite de hachage qui permet de produire des résumés (ou « hash ») qui permettent à celui qui reçoit le message d'en contrôler l'intégrité,
- La fonction de hachage produit des résumés de taille fixe,
- Rien n'interdit d'avoir le même résumé pour deux messages différents (on parle ici de collision),
- Mais il faut que la fonction de hachage produise des résumés suffisamment longs pour minimiser les collisions.



Ici, il existe une attaque qui se base sur le paradoxe des anniversaires, qui vise à produire plusieurs messages dans le but d'obtenir 2 messages pour lesquels le résumé est identique. Le message initial peut être intercepté et remplacé par le message forgé.

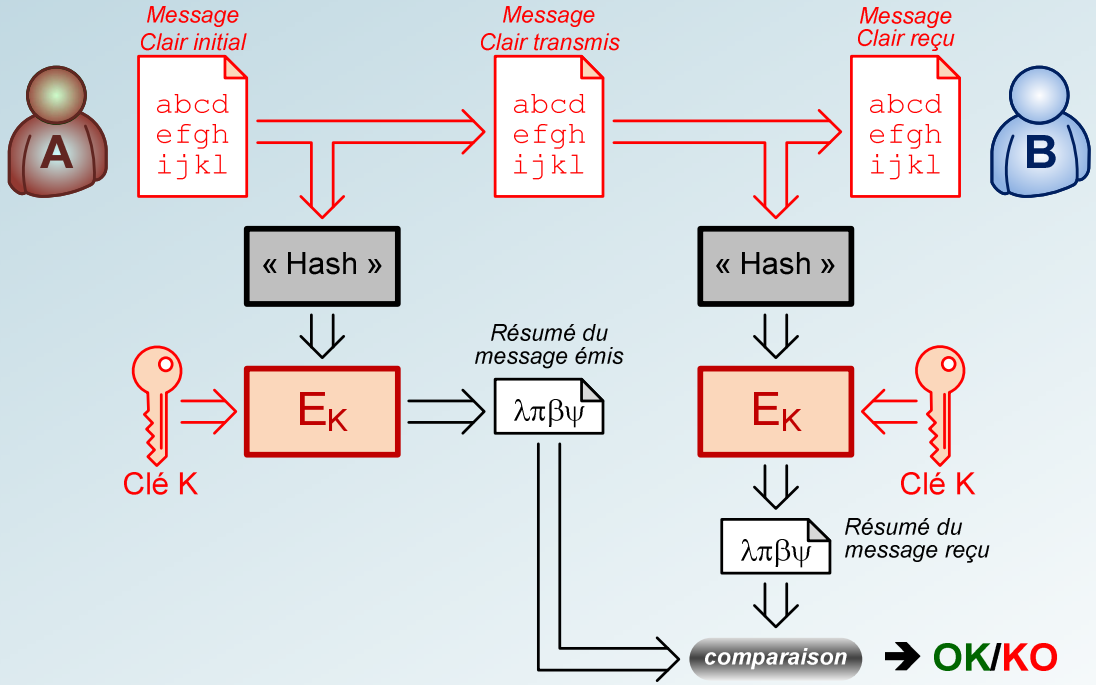
RAPPELS DE CRYPTOGRAPHIE

- Une fonction de hachage est considérée comme sûre si :
  - Il est très difficile (voire impossible) de retrouver le contenu du message initial à partir du "hash". Une fonction à sens unique permet de garantir ce point,
  - Il est très difficile de produire aléatoirement 2 messages différents qui aboutissent au même "hash". Ici, le résumé ou le "hash" doit être suffisamment long (256 bits par exemple),
  - Il est très difficile de produire à dessin (en connaissant le message initial et l'architecture de la fonction de hachage) 2 messages différents qui aboutissent au même "hash". Ici, la fonction de hachage doit être suffisamment complexe pour ne pas intégrer de vulnérabilité. Elle doit être robuste à une cryptanalyse.
- Pour une fonction de hachage cryptographique, les trois points mentionnés ci-avant doivent être garanti impossible au lieu de très difficile. On parle dans ce cas de fonction à sens unique,
- Enfin, le calcul d'un résumé de message doit être très rapide.

Les fonctions de hachage permettent aussi le stockage d'empreinte des mots de passe (ce qui revient au stockage du mot de passe lui-même) mais sans avoir à sauvegarder le mot de passe dans sa totalité.

RAPPELS DE CRYPTOGRAPHIE

- Pour assurer en même temps l'intégrité du message et l'authenticité de la source, il est possible d'utiliser des CAM ou **C**ode d'**A**uthentification de **M**essage (ou MAC pour **M**essage **A**uthentication **C**ode) qui se calculent via une fonction de hachage avec clé (HMAC pour keyed-**H**ash **MAC** par exemple).
- Ici, le résumé du message clair initial est chiffré par Alice avec une clé secrète partagé avec Bob,
- Bob n'aura qu'à effectuer les mêmes opérations qu'Alice (Hash puis chiffrement avec la clé K) sur le message reçu pour vérifier si ce dernier est bien intègre et si c'est bien Alice qui en est à l'origine.
- Ce mode d'opération cryptographique porte le nom d' AO pour "**A**uthentication **O**nly".



Il existe des CAM pour lesquelles la clé est juste "xorée" avec tout ou partie du hash.

RAPPELS DE CRYPTOGRAPHIE

- Modes d'Opération candidats pour le mode AO :
  - **CMAC** : NIST SP800-38B ➔Corrige les vulnérabilités du mode initial CBC-MAC,
  - **HMAC** : NIST FIPS 198a,
  - **UMAC** : RFC 4418 - utilise les fonction Hash Universal-2 de Wegman-Carter
- Le mode **AO GMAC** (NIST SP800-38D) n'est pas retenu en raison de ses défauts & vulnérabilité :
  - impose l'utilisation d'un IV contrairement aux autres modes AO,
  - impact en cas de collision d'IV/clé ➔ compromission possible de la Clé GHASH

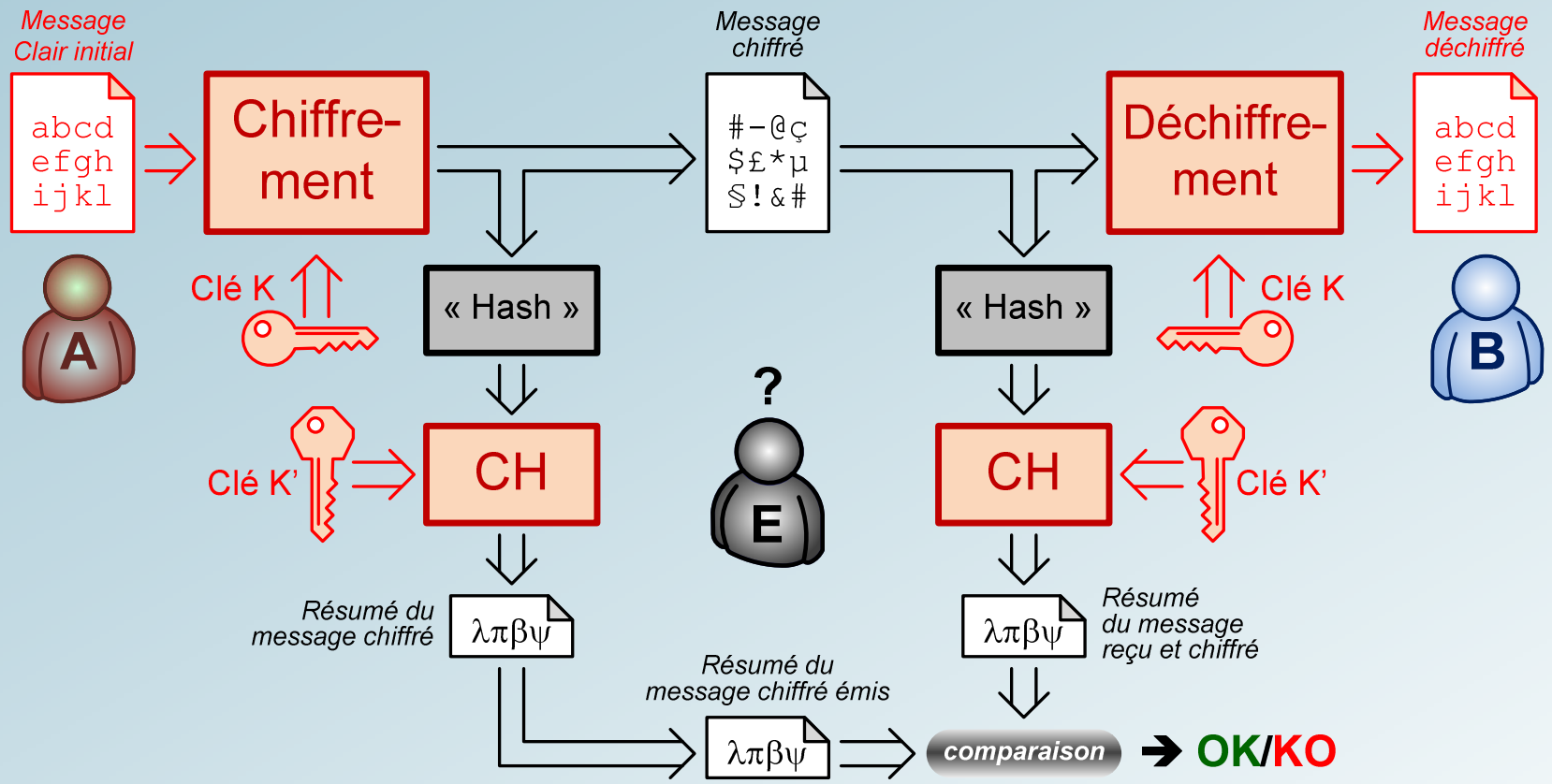
Lorsque la confidentialité n'est pas requise le mode AO est très avantageux car plus efficace en terme de performance et de coût.

RAPPELS DE CRYPTOGRAPHIE

- Mode d'Opération de type AE (Authenticated Encryption)
  - Authenticité, Intégrité et Confidentialité
- L'un des critères majeurs est le niveau de Sécurité en regard des objectifs identifiés dans le document de référence de N. Bellare et N. Namprempreyy
  - "Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm" – 2007
  - **IND** : indistinguishability / **NM** : non-malleability
  - **CPA** : Chosen Plaintext Attack / **CCA** : Chosen Ciphertext Attack
- L'analyse de N. Bellare et N. Namprempreyy montre qu'il est recommandé d'utiliser des modes d'opération AE de type "Encrypt Then MAC" ⇒ critère IND-CCA
- France: confirmé par l'ANSSI qui ne retient que les schémas de type "Encrypt Then MAC".

Ne jamais bâtir par soi-même un mode AE à partir de modes AO et EO existants.

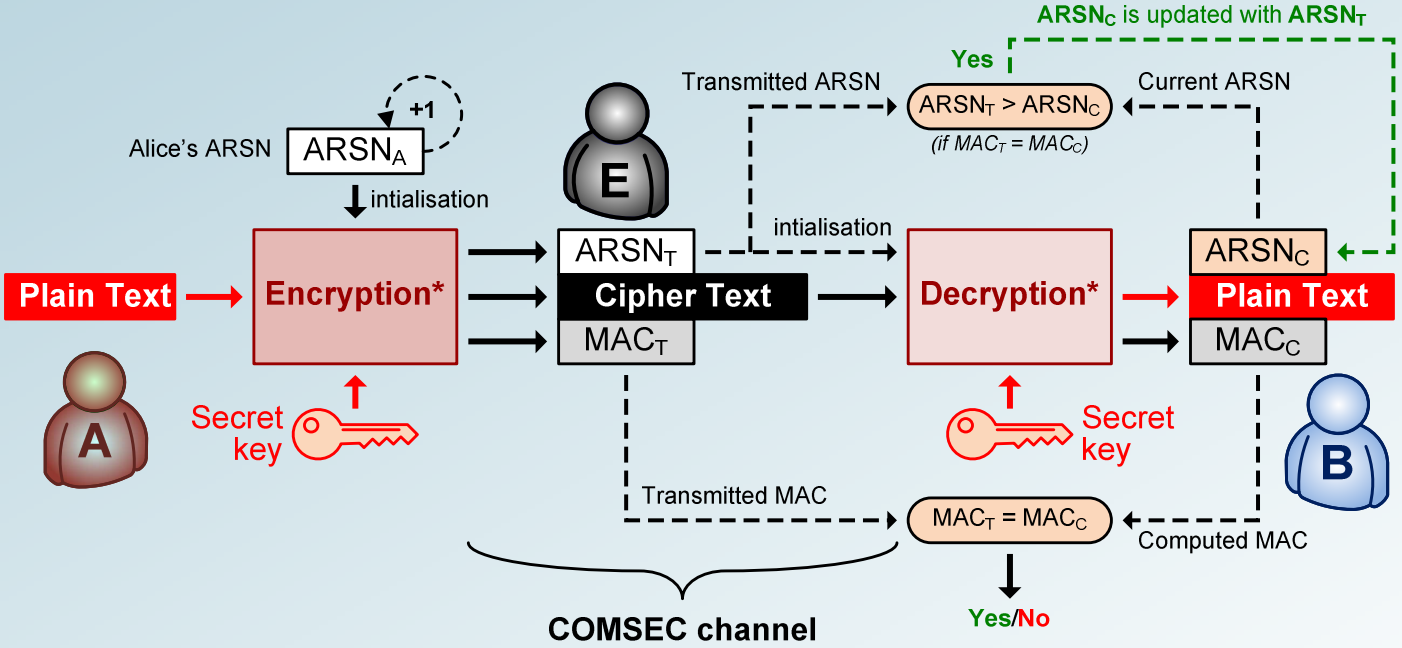
RAPPELS DE CRYPTOGRAPHIE



La clé qui sert pour la confidentialité doit être différente de la clé qui sert pour l'authenticité/intégrité. Comme le résumé dépend d'une clé secrète cela permet d'authentifier la source de chaque message en plus de leur intégrité.

RAPPELS DE CRYPTOGRAPHIE

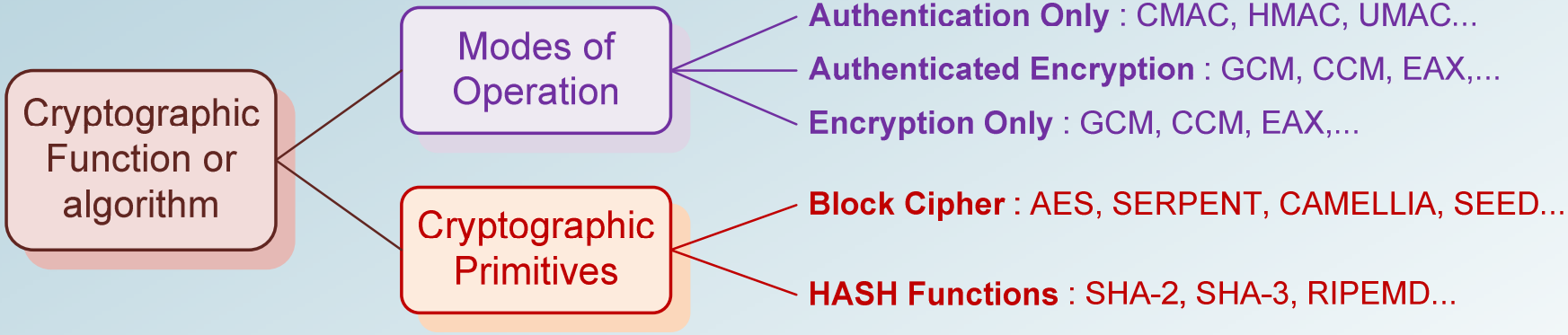
- Une des attaques les plus facile à mener est celle du rejeu des messages déjà joués,
- Il suffit à Eve d'intercepter un message chiffré/authentifié et de le réémettre plus tard pour que Bob l'authentifie et le prennent en compte de nouveau,
- Pour parer ce type d'attaque, il suffit d'implémenter un **C**ompteur d'**A**nti-**R**ejeu (CAR ou ARSN – **A**nti **R**eplay **S**equence **N**umber),
- Le CAR sert à initialiser les fonctions cryptographiques (à minima la fonction de calcul du MAC) pour que Bob puisse reconnaitre un message déjà joué d'un message jamais joué.



Eve pourrait ici modifier le compteur mais ce sera détecté par Bob puisque le MAC dépend de la valeur compteur (et de la clé secrète) qui est rentré dans le calcul du MAC. Le compteur doit absolument être authentifié mais pas forcément chiffré.

RAPPELS DE CRYPTOGRAPHIE

- Nous avons bien vu que la primitive de chiffrement seule ne suffit pas pour assurer tous les services de sécurité,
- Il est nécessaire de séquencer les fonctions cryptographiques selon le mode d'opération de la fonction de sécurité cible,
- La sélection du ou des algorithmes et des modes d'opération doivent s'appuyer sur les recommandations des experts et des organismes dédiés : NIST, ENCRYPT, ENISA etc...



Les standards toujours les standards, ne jamais improviser des modes dans son coin !

RAPPELS DE CRYPTOGRAPHIE

- Critères de sélection des modes d'opération (1 / 2)
  - Type : AO (Authentication Only), EO (Encryption Only, AE (Authenticated Encryption)
  - Standardisation : NIST, RFC/ IETF, ISO…
  - Niveau de déploiement / adoption par l'industrie (spatiale ou non),
  - Soumis ou non à Brevet (ex: RSA, OCB, PMAC),
  - Sécurité vérifiable / démontrable (existence preuve de sécurité)
  - Niveau de Sécurité : IND-CPA, IND-CCA, NM-CPA, INT-CTXT, INT-PTXT,
  - Choix des Primitives Cryptographiques utilisables : Hash / SHA-xxx, Block cipher AES (NIST FIPS 197) ou autres block cipher (ex: CAMELLIA, SEED),
  - Tailles des clés,
  - Nombre de clés utilisées : distinction clés Chiffrement et Authentification (exigence RGS ANSSI),
  - Contrainte sur la taille max des messages.

RAPPELS DE CRYPTOGRAPHIE

- Critères de sélection des modes d'opération (2 / 2)
  - Taille max du MAC / incrémentalité: niveau de Sécurité et "overhead" Sécurité
  - Contraintes relatives aux Counter/IV/Nonce : Unicité, non déterminisme
  - Propagation d'erreur :
    - Ex: avec le mode CBC, 1 bit en erreur dans la séquence chiffrée (CT : **C**ipher**T**ext) impacte 2 PT blocks de 128 bits chacun (PT : **P**lain**T**ext) après déchiffrement,
    - Avec le mode CTR, 1 bit en erreur dans la séquence chiffrée (CT) impacte 1 seul bit d'un PT block après déchiffrement.
  - Padding / Expansion du ciphertext : impact sur overhead sécurité,
  - Nombre d'invocations des primitives cryptographiques pour chaque opération :
    - Impact sur les performances.
  - Capacité de Pré-processing :
    - Ex: pré-calcul des clés dérivées.
  - On-line – Off-line (ex: GCM vs CCM): impact sur les performances,
  - Parallélisation du traitement : impact sur les performances,
  - Performances implémentations matérielles / logicielles (Benchmark).

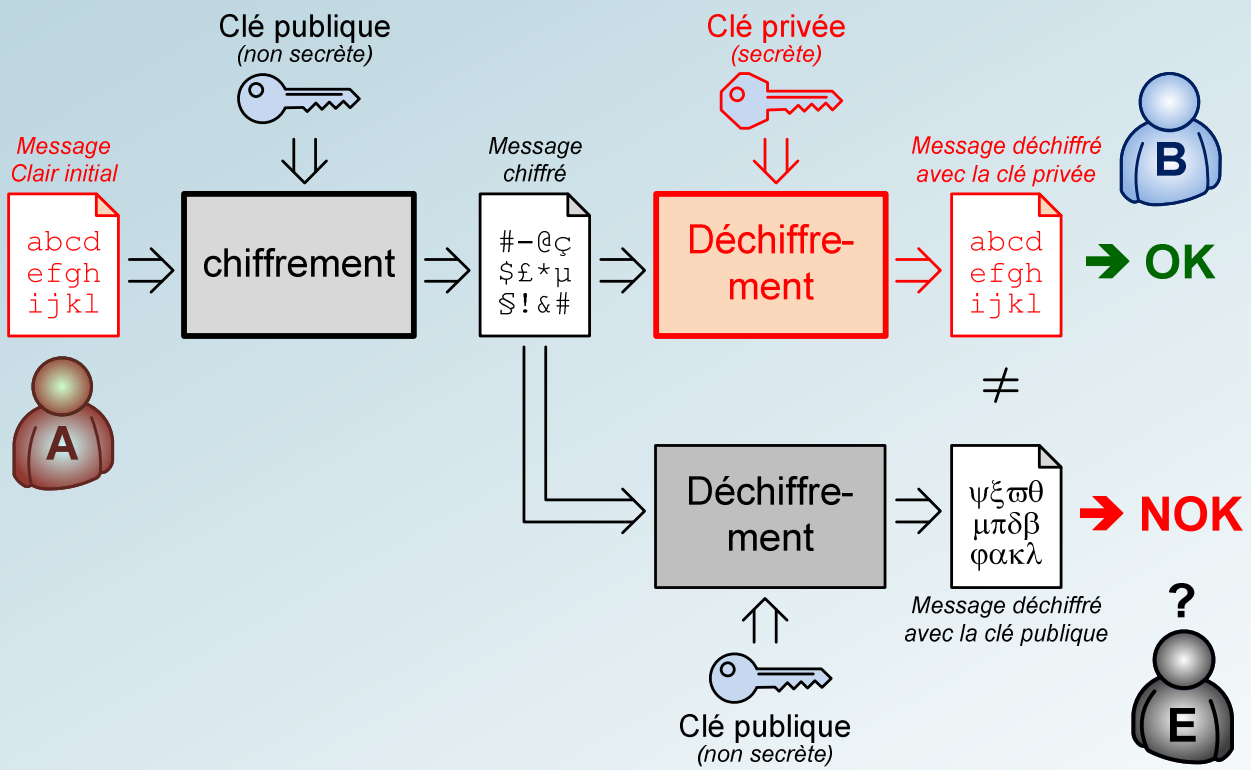
RAPPELS DE CRYPTOGRAPHIE

- La cryptographie asymétrique se base sur :
  - Des mécanismes de chiffrement/déchiffrement construits à partir de fonctions mathématiques,
  - Un couple de clé dites asymétriques appelé aussi bi-clé.
- La bi-clé se compose :
  - D'une **clé publique** non confidentielle et qui peut être diffusée sur un canal clair,
  - D'une **clé privée** confidentielle qui doit rester connue de la seule entité détentrice de cette clé.
- Il existe plusieurs types de cryptographie asymétrique qui ont des objectifs bien précis.

Les mathématiques utilisées en cryptographie asymétrique ne sont pas compliqués. C'est plus l'identification de la clé privée à partir de la clé publique qui est un problème très difficile à résoudre si les clés sont assez grandes.

RAPPELS DE CRYPTOGRAPHIE

- Alice utilise la clé publique que Bob lui a transmise pour chiffrer le message qu'elle souhaite lui transmettre,
- Bob utilise sa clé privée (connue de lui seul) pour déchiffrer le message reçu d'Alice,
- Eve, qui a pu intercepter la clé publique de Bob et le message chiffré d'Alice, ne pourra pas déchiffrer le message en utilisant la clé publique de Bob.



Autant la clé publique peut être diffusée en clair et connue de tous (ici Alice), autant la clé privée doit rester secrète et connue de son seul propriétaire (ici Bob).

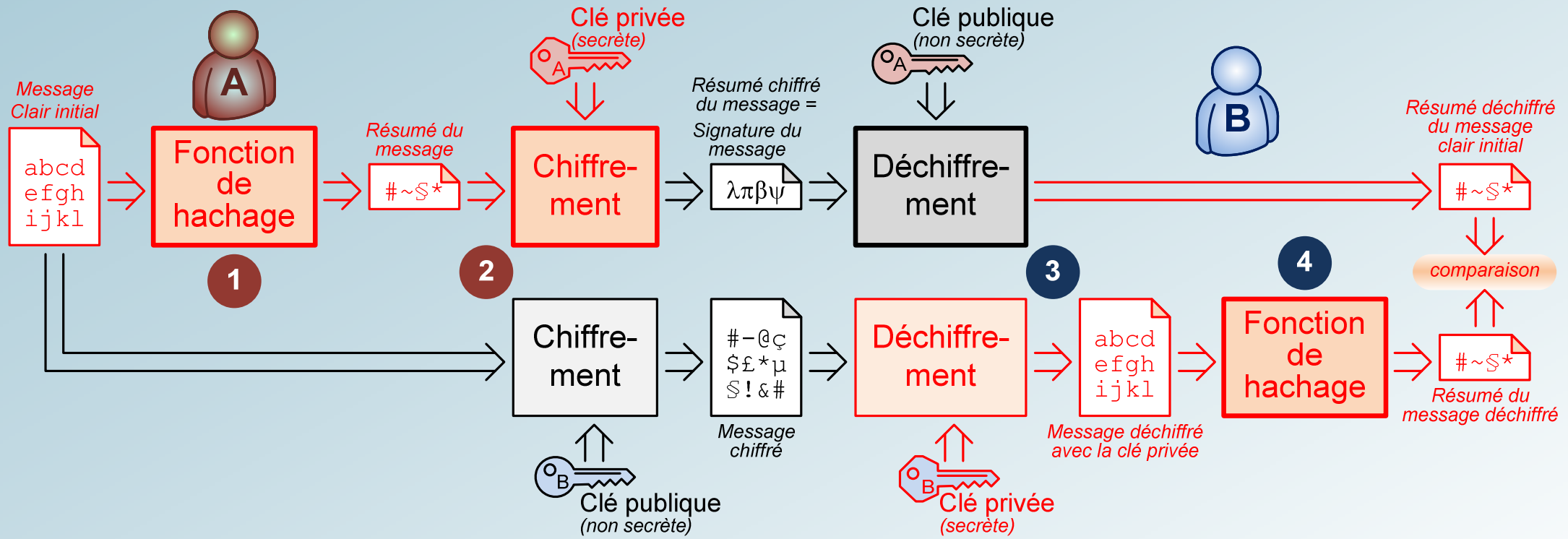
RAPPELS DE CRYPTOGRAPHIE

- Le vrai plus de la cryptographie asymétrique est la signature électronique,
- Si Alice utilise une fonction de hachage sûre sur son message clair initial et qu'elle chiffre le haché avec sa clé privée, alors Bob aura la capacité de vérifier ce haché de la façon suivante :
  - Il déchiffre le message chiffré envoyé par Alice,
  - Il utilise la même fonction de hachage qu'Alice sur le message déchiffré,
  - Il déchiffre le haché chiffré envoyé par Alice,
  - Si le haché déchiffré est identique au haché du message déchiffré alors Bob saura que:
    - Le message vient bien d'Alice ➔ la source est authentifiée,
    - Le message reçu est intègre ➔ le message est reçu tel qu'il a été envoyé par Alice.
- En utilisant sa clé privée, Alice peut signer tous ses messages. Et ceux qui possèdent sa clé publique, peuvent vérifier que les messages ont bien été émis par Alice.

On parle de "signature électronique" lorsque le « hash » est chiffré/déchifré avec un couple de clé privée/publique. On parle de MAC lorsque le « hash » est chiffré/déchiffré avec la même clé secrète symétrique.

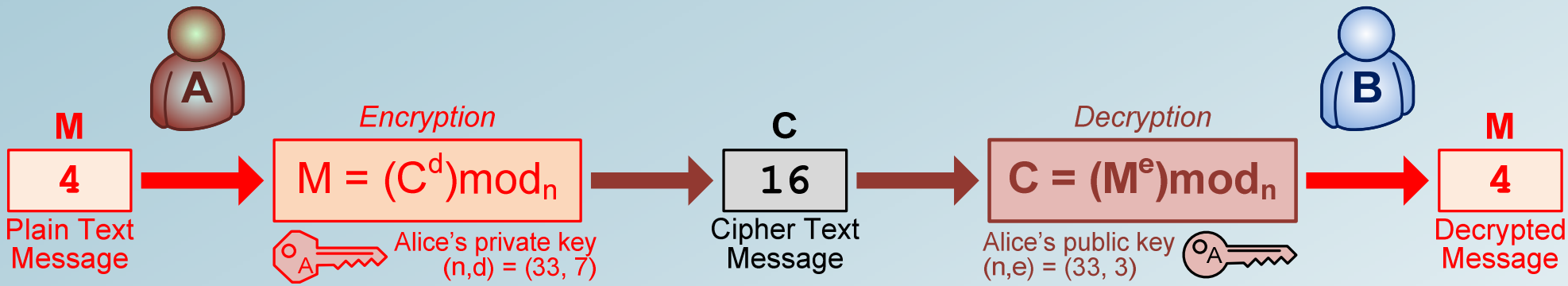
RAPPELS DE CRYPTOGRAPHIE

- La signature électronique se base sur l'emploi de la clé privée pour signer le message et sur l'emploi de la clé publique pour le contresigner.

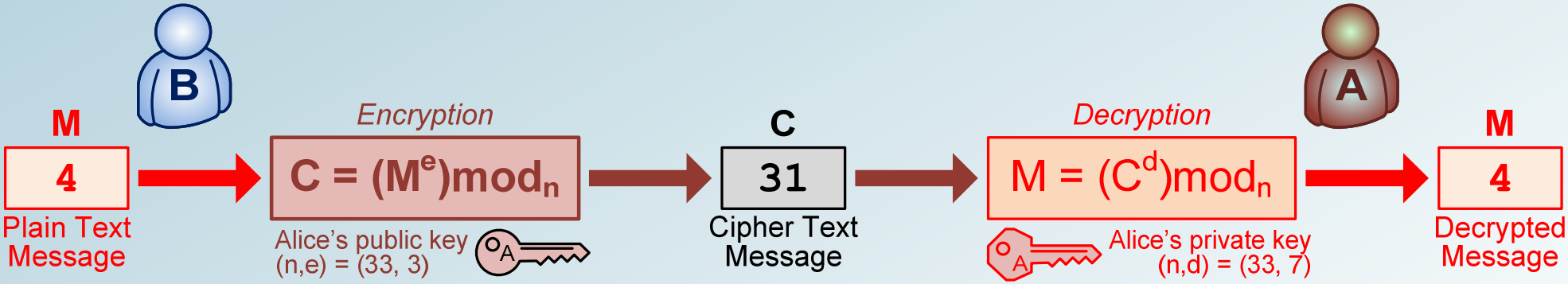


Ici, le chiffrement du résumé de message avec la clé privée d'Alice représente l'opération de signature. Cela permet de garantir l'intégrité du message et aussi l'authenticité de la source du message ➔ ici Alice qui a signé avec sa clé privée.

RAPPELS DE CRYPTOGRAPHIE



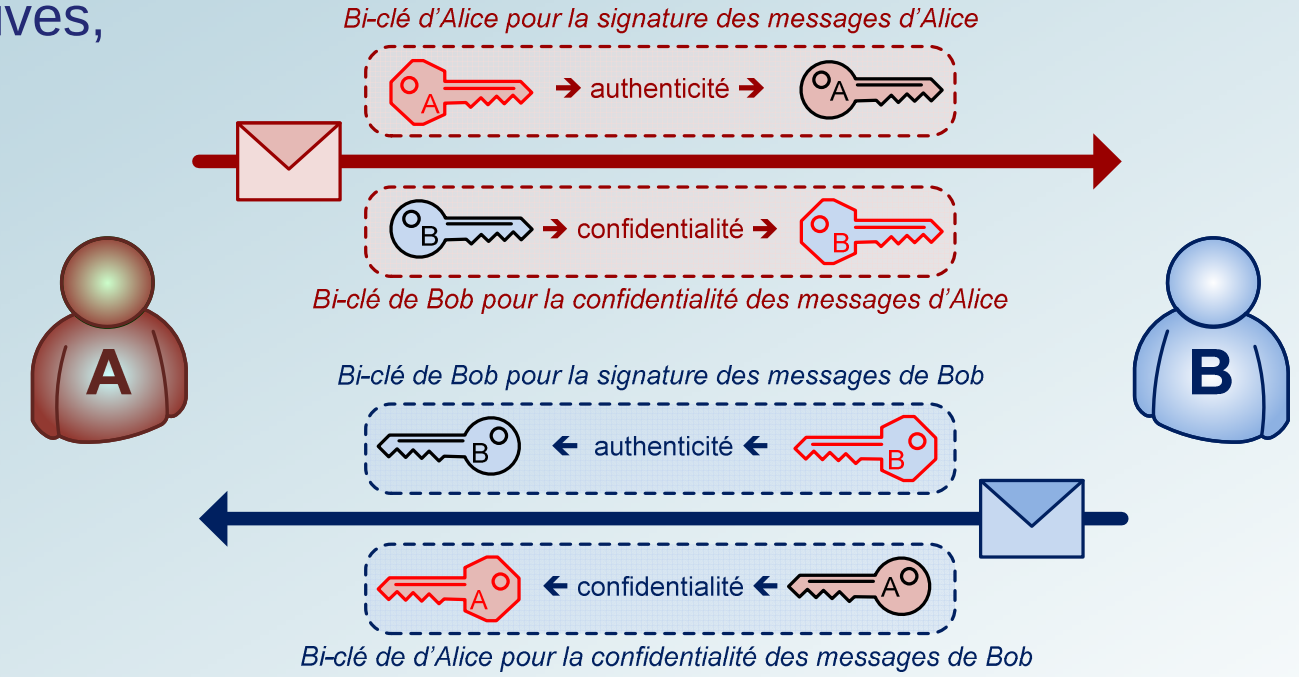
p = 3 et q = 11 (nombres premiers), p.q=33, N=(p-1).(q-1)=20 , e=3 (entier) ➔ $(e.d)mod_N = 1$ ➔ d=7



La cryptographie asymétrique (ici RSA) se base sur l'exponentiation modulaire et sur le produit de grand nombre premiers qu'il est très difficile de factoriser.

RAPPELS DE CRYPTOGRAPHIE

- Pour implémenter une communication bidirectionnelle sécurisée, Alice et Bob devront faire appel à leur bi-clés respectives,
- Les clés publiques devront être échangées,
- Tout message à transmettre devra être chiffré avec la clé publique du destinataire et signé avec la clé privée de l'émetteur.



Les standards recommandent même que la bi-clé pour de chiffrement/déchiffrement soit différente de la bi-clé pour la signature/contre-signature.

RAPPELS DE CRYPTOGRAPHIE

- RSA requière de travailler sur des très grands nombres (2048/3072 bits ➔ 600/900 digits),
- En terme d'implémentation, il est inimaginable de chiffrer de longs messages par le biais de la cette cryptographie asymétrique. Il est impossible de chiffrer des flux à haut débit en temps réels : des flux en streaming par exemple,
- Seule la cryptographie à clé secrète symétrique permet de chiffrer à haut débit des messages très longs,
- Mais sachant qu'une clé secrète n'est finalement pas un gros message en soit (128bits/256bits), il est tout à fait possible d'échanger des clés secrètes par le biais de la cryptographie asymétrique,
- Le message chiffré/authentifié RSA échangé entre Alice et Bob contient la clé secrète symétrique qui sera ensuite utilisée pour chiffrer des messages plus complexes et plus long qu'une simple clé de 128 ou 256 bits,
- Cette technique s'appelle le **K**ey **E**ncapsulation **M**essage (KEM).

La cryptographie asymétrique demande environ 1000 fois plus de ressource calculatoire que la cryptographie symétrique.

RAPPELS DE CRYPTOGRAPHIE

- La technique du **KEM** permet d'échanger des clés secrètes en les encapsulant dans des messages chiffrés authentifié via une cryptographie asymétrique,
- Il est même recommandé que les clés secrètes soient produites au moment où elles sont utilisées et détruites à la fin de la session de communication. On identifie ici les clés secrètes comme des clés dites de session,
- Cette technique fait néanmoins porter sur les clés privées (celles qui doivent rester secrètes) d'Alice et de Bob une lourde responsabilité d'autant plus qu'elles sont persistantes aux sessions,
- Même si la technique du KEM est intéressante elle n'est pas parfaite,
- Heureusement, il existe une autre technique qui porte le nom de **K**ey **E**stablishment (ou **K**ey **E**xchange = **KE**) et qui permet de s'affranchir des clés publiques/privées persistantes d'Alice et de Bob pour se mettre d'accord sur un secret partagé.

Ce qui est redouté ici, c'est le vol du serveur qui héberge les clés privées RSA (celles qui sont persistantes). Et qui pourraient permettre de remonter au clé secrète et de déchiffrer, a postériori, les messages échangés pendant la session de communication.

RAPPELS DE CRYPTOGRAPHIE

choix d'Alice : a, g, p

(ex : a=6 , g=3, p23)

choix de Bob : b

(ex : b=15)

$A = (g^a) \bmod_p$

A, g, p

(ex : A=16, g=3, p=23)

B

B

A

B

(ex : B=12)

$B = (g^b) \bmod_p$

$K = (B^a) \bmod_p$

(ex : K=9)

Secret partagé

$K = (A^b) \bmod_p$

(ex : K=9)

*Il est possible de choisir les paramètres Diffie Hellman en se basant sur les courbes elliptiques qui en réduiront la taille sans en amoindrir la résistance ➔ ECDH : **E**llicptic **C**uvre **D**iffie-**H**ellman*

RAPPELS DE CRYPTOGRAPHIE

- Alice choisit "g" et "p" deux nombres premiers, puis elle effectue un tirage aléatoire pour définir "a" (qui est un entier naturel),
- Bob effectue un tirage aléatoire pour définir "b" (qui est aussi un entier naturel),
- "a" et "b" doivent rester secrets et ne doivent jamais être échangés,
- Alice envoie à Bob, sur un canal clair non sécurisé, les valeurs "g", "p" et le résultat de $(g^{a})\mathrm{mod}_{p} = A$ (sachant qu'il est difficile de retrouver la valeur de "a" à partir de A).
- Bob envoie à Alice, sur un canal clair non sécurisé, le résultat de $(g^{b})\mathrm{mod}_{p} = B$ (sachant qu'il est difficile de retrouver la valeur de "b" à partir de B),
- Alice et Bob calculent la valeur de **K** avec les variables à leur disposition. Alice calculera $K = (B^{a})\mathrm{mod}_{p}$ et Bob calculera le même $K = (A^{b})\mathrm{mod}_{p}$.
- Ce type de protocole permet d'échanger des éléments dits « éphémères » pour établir la clé secrète commune. Tous ces éléments sont propres à une session de communication données et non persistants lorsque la session est close.

Le protocole de KE se base sur un mécanisme asymétrique inventés par Whitfield Diffie et Martin Hellman en 1976.

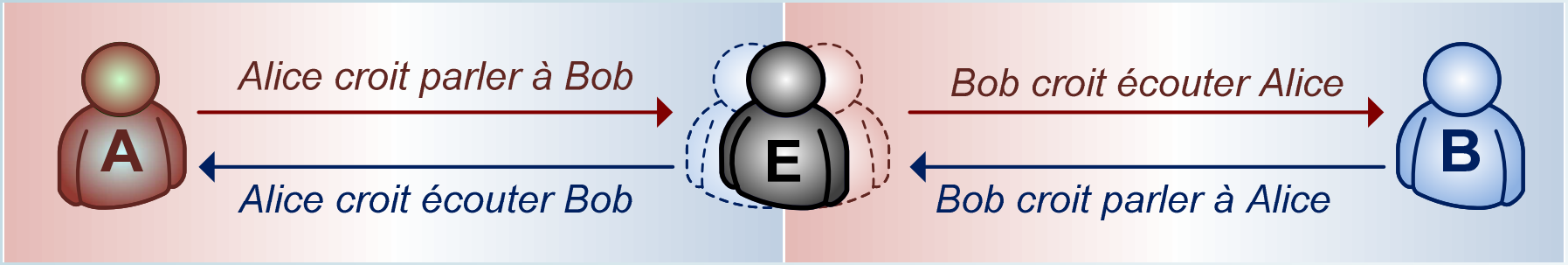
RAPPELS DE CRYPTOGRAPHIE

- Alice et Bob ont donc à leur disposition toutes les briques de base pour mettre en place une communication entièrement sécurisée entre eux deux,
- Des paires de bi-clés pour authentifier leur messages,
- Un protocole d'établissement de clé indépendant des bi-clés d'authentification des messages,
- Cette indépendance entre la phase d'établissement de la clé secrète symétrique et des bi-clés persistantes d'authentification permet de garantir ce que nous appelons la "persistance du secret" ou **P**erfect **F**orward **S**ecrecy : PFS,
- La **PFS** garantie que, si Alice se fait voler son serveur avec la clé privée, personne ne pourra remonter aux clés secrètes qui ont servi à chiffrer les communications antérieures, puisque ces dernières ont été échangés via des éléments éphémères produits pour cette phase et indépendamment de la clé privées d'Alice.

Mais il reste encore un point à assurer : comment Alice prouve à Bob qu'elle est bien Alice et inversement ? Ici ce pose encore le problème d'authentification de la source lors de la phase d'échange des clés publiques.

RAPPELS DE CRYPTOGRAPHIE

- L'attaque la plus connue en SSI est celle appelée : l'attaque de l'Homme Du Milieu (HDM), attaque de l'intercepteur ou **M**an-**I**n-**T**he-**M**iddle **A**ttack (MITM ou MMA),
- Ici, Eve est capable d'intercepter tous les messages échangés entre Alice et Bob,
- Ce qui lui permet, par exemple, d'intercepter la clé publique d'Alice et d'envoyer à Bob la sienne (et inversement avec Alice),
- Il s'agit ni plus ni moins que d'un cas d'usurpation d'identité, Eve se fait passer pour Bob vis à vis d'Alice et inversement.



Pour parer cette attaque, il faut qu'Alice soit capable de prouver son identité à Bob et inversement.

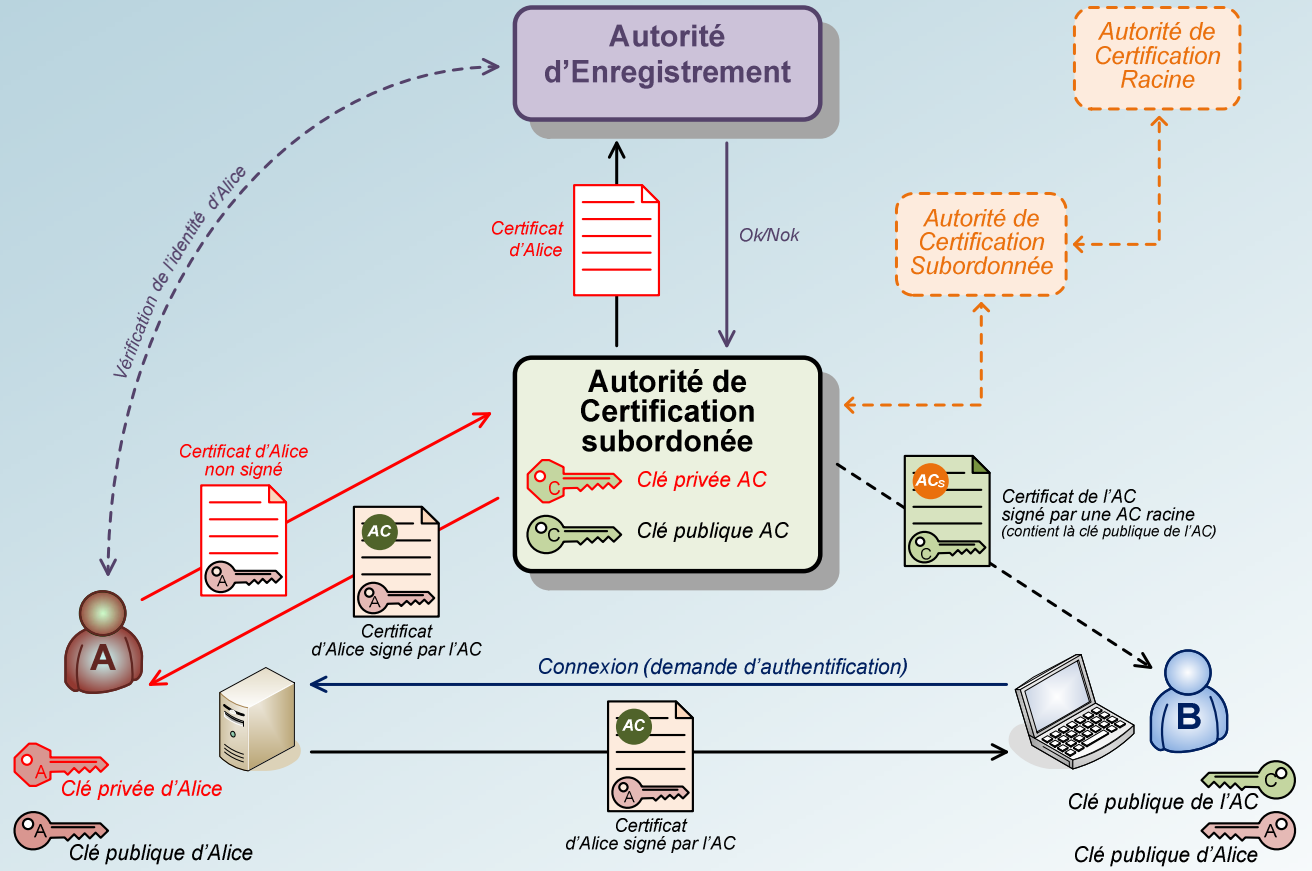
RAPPELS DE CRYPTOGRAPHIE

- La seule et unique solution pour parer ce type d'attaque est : l'authentification de la source des messages !
- Tout message échangé entre deux parties distinctes doit contenir les éléments permettant (en plus de ceux en possession des parties) d'authentifier de façon certaine l'émetteur du message,
- Il n'existe que 2 façons d'authentifier un émetteur :
  - Par le biais de la cryptographie à clé secrète symétrique (qui impose qu'Alice et Bob se rencontrent physiquement pour échanger les clés secrètes en toute discrétion),
  - Par le biais de la cryptographie à clé publique/privée.
- La méthode la plus connue est celle qui vise à s'appuyer sur une entité tierce dite "de confiance" ("trusted thrid party") et qui garantit, par la délivrance de certificats signés électroniquement, l'identité de celui qui en est le possesseur (un peu comme une préfecture qui est habilitée à délivrer des cartes d'identité).

*Les entités autorisées à délivrer des certificats électroniques sont les **A**utorités de **C**ertification (AC) ou **C**ertification **A**uthorities (CA).*

RAPPELS DE CRYPTOGRAPHIE

- Alice qui souhaite ouvrir sa boutique en ligne va produire une bi-clé pour son serveur,
- La clé publique est envoyée à une AC qui vérifiera, via une Autorité d'enregistrement (AE), les bonnes intentions d'Alice avant de lui retourner le certificat signé avec la clé privée de l'AC et qui contient la clé publique d'Alice,
- Lorsque Bob se connectera au serveur d'Alice, le serveur émettra le certificat que contresignera Bob avec la clé publique de l'AC.
- Ce type d'infrastructure permet de parer l'attaque MITM.



Les navigateurs web (ou web browsers) intègrent nativement des certificats qui contiennent les clés publiques de quelques AC de haut niveau. Ce qui permet à tout internaute de ne pas se faire duper lorsqu'il se connecte à un serveur web.

RAPPELS DE CRYPTOGRAPHIE

- Synthèse de la Cryptographie asymétrique : Algorithmes et Protocoles
  - Chiffrement: RSA-OAEP (également EL GAMAL basé sur DLC)
    - Taille de clé (modulus N) : ≥ 3072 bits,
    - Taille du plaintext < taille du modulus N,
    - Taille du ciphertext : taille du modulus,
  - Signature digitale (Authenticité, Intégrité et Non répudiation): DSS, RSASSA
    - Non répudiation: l'auteur d'un message signé ne peut le renier (y compris devant un tribunal) car lui seul est capable d'avoir généré la signature avec sa clé privée (PRK)
  - DSA
    - Taille max de clé : 3072 bits (L = length of prime modulus)
    - Taille max de signature : 256 bits (N = length of q prime divisor of p)
  - RSA
    - Taille max de clé : 3072 bits (L = length of prime modulus)
    - Taille max de signature : 3072 bits (L = length of prime modulus)
  - ECDSA
    - Taille max de clé : 512 bits (n = order of G point)
    - Taille max de signature (r, s) => 2 x 512 bits

RAPPELS DE CRYPTOGRAPHIE

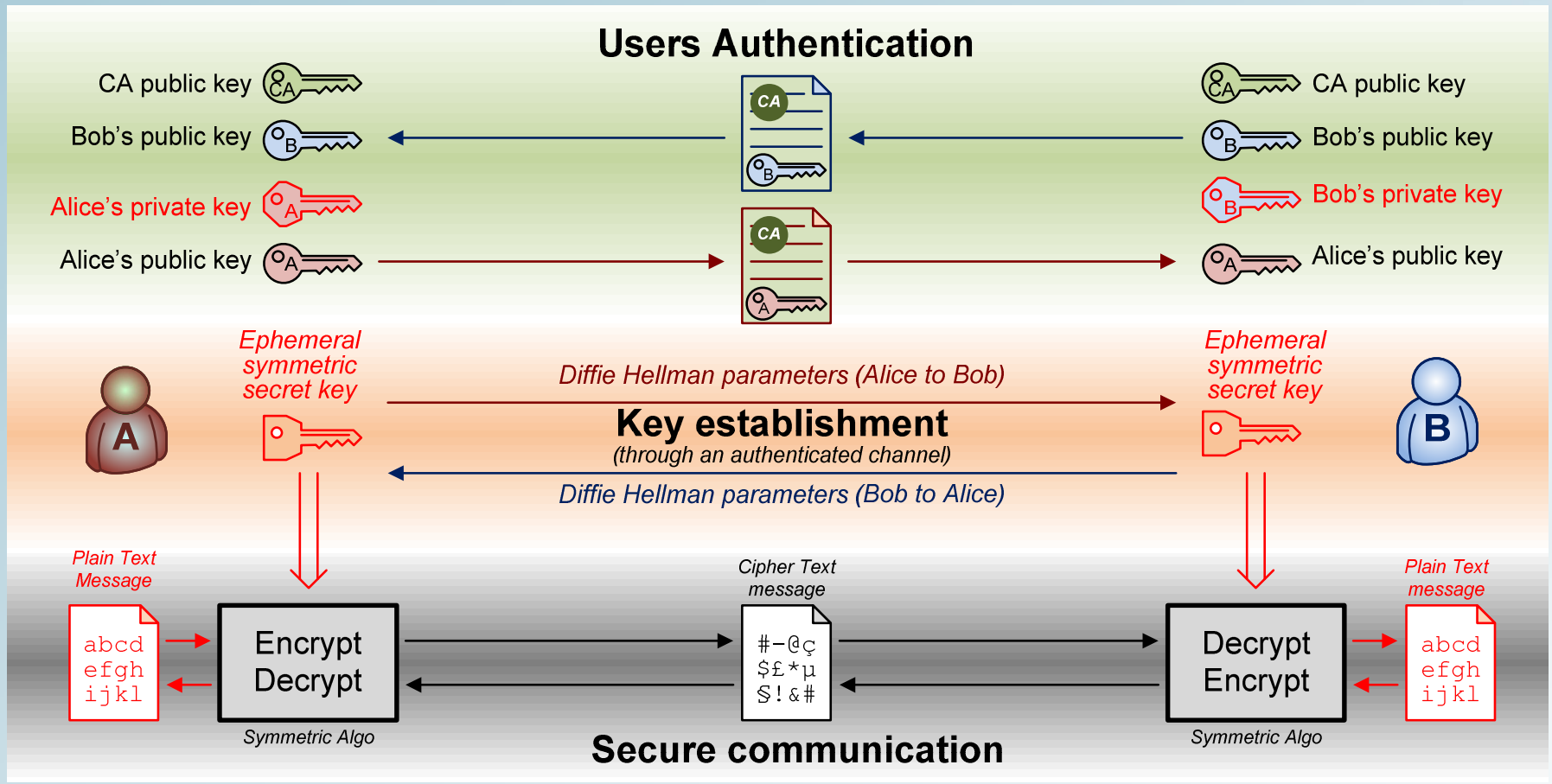
- Synthèse pour le protocole KE (Key Establishment) :
  - KE couvre 2 types de protocoles: Key Agreement (KA) et Key Transport (KT) :
    - KA : Key Agreement : établissement sécurisé de clés secrètes SKI durant la session (KE),
    - KT : Key Transport : établissement durant la session, d'un canal sécurisé puis transport à travers ce canal, des clés secrètes SKI préalablement générées (KEM).
  - Standards KE du NIST :
    - SP800-56 A (DLC) : Discrete Logarithm Cryptography,
    - SP800-56B (IFC) : Integer Factorization Cryptography.
  - Protocole d'établissement de clés (KE) spécifiques :
    - SSL/TLS (TLS 1.2 / TLS 1.3),
    - IPSEC (IKE) : Internet Key Exchange,
    - Protocoles KE : RSA, DSA, DHE-RSA, DSS-RSA, ECDHE-RSA,
    - Seuls les protocoles KE utilisant des clés éphémères garantissent la propriété PFS.

RAPPELS DE CRYPTOGRAPHIE

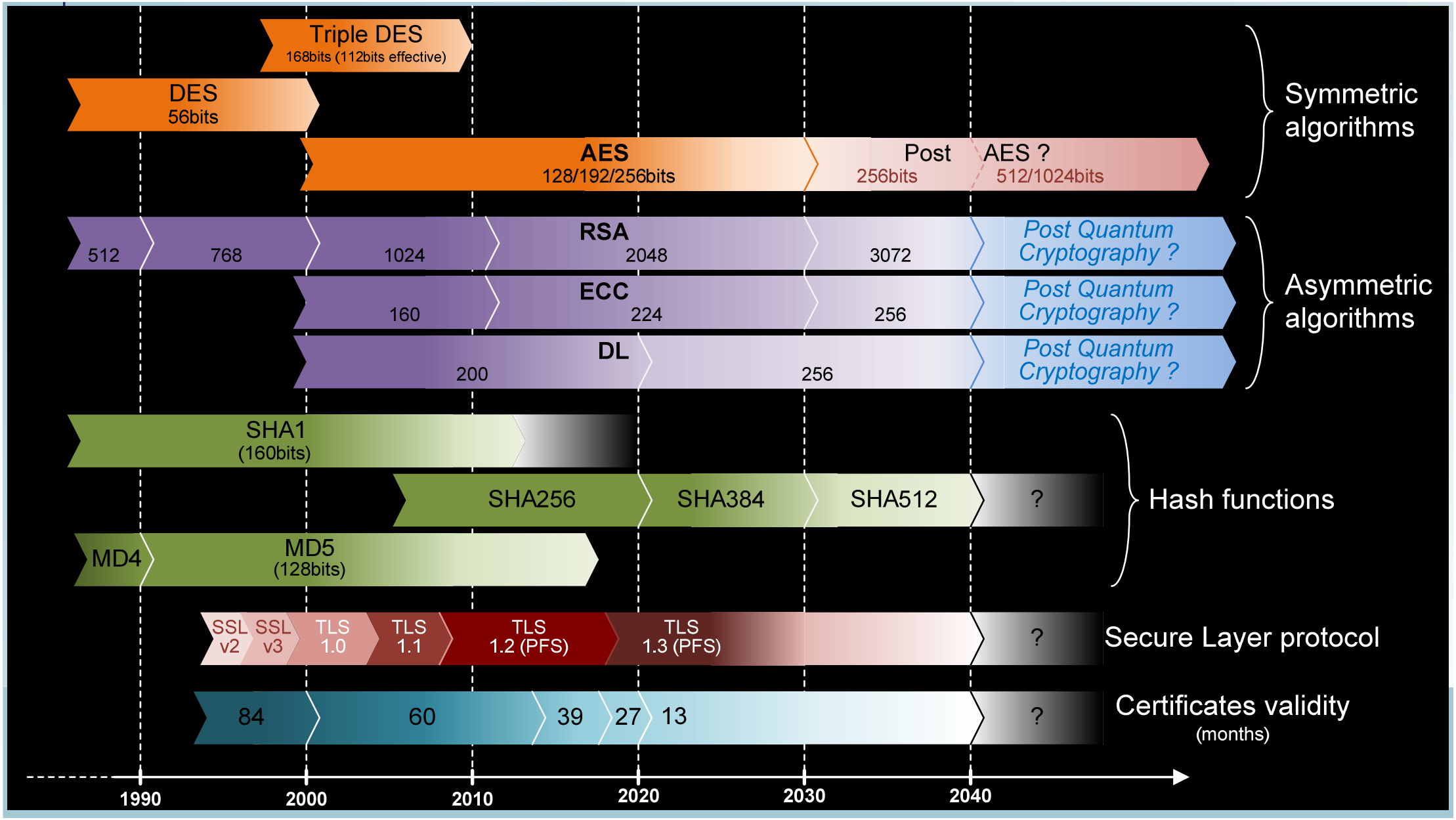
- Pour établir un canal de communication sûr entre deux parties distantes il faut :
  - Des certificats issus d'autorités de certification reconnues et signés par des autorités de certification racines,
  - Des certificats signés par des CA subordonnées reconnues et pour assurer l'authenticité des clés publiques échangées et qui permettront d'authentifier tous les échanges à suivre,
  - Un protocole d'établissement de clé secrète de session au travers de clés asymétriques éphémères qui garantissent la PFS,
  - Un algorithme à clés secrètes symétriques qui assure le chiffrement, l'authentification et l'intégrité des messages échangés avec la clé secrète établie pour la session.

C'est grâce à cet ensemble de mécanismes qu'il est possible à tout un chacun de faire du https:// sur internet en toute sécurité.

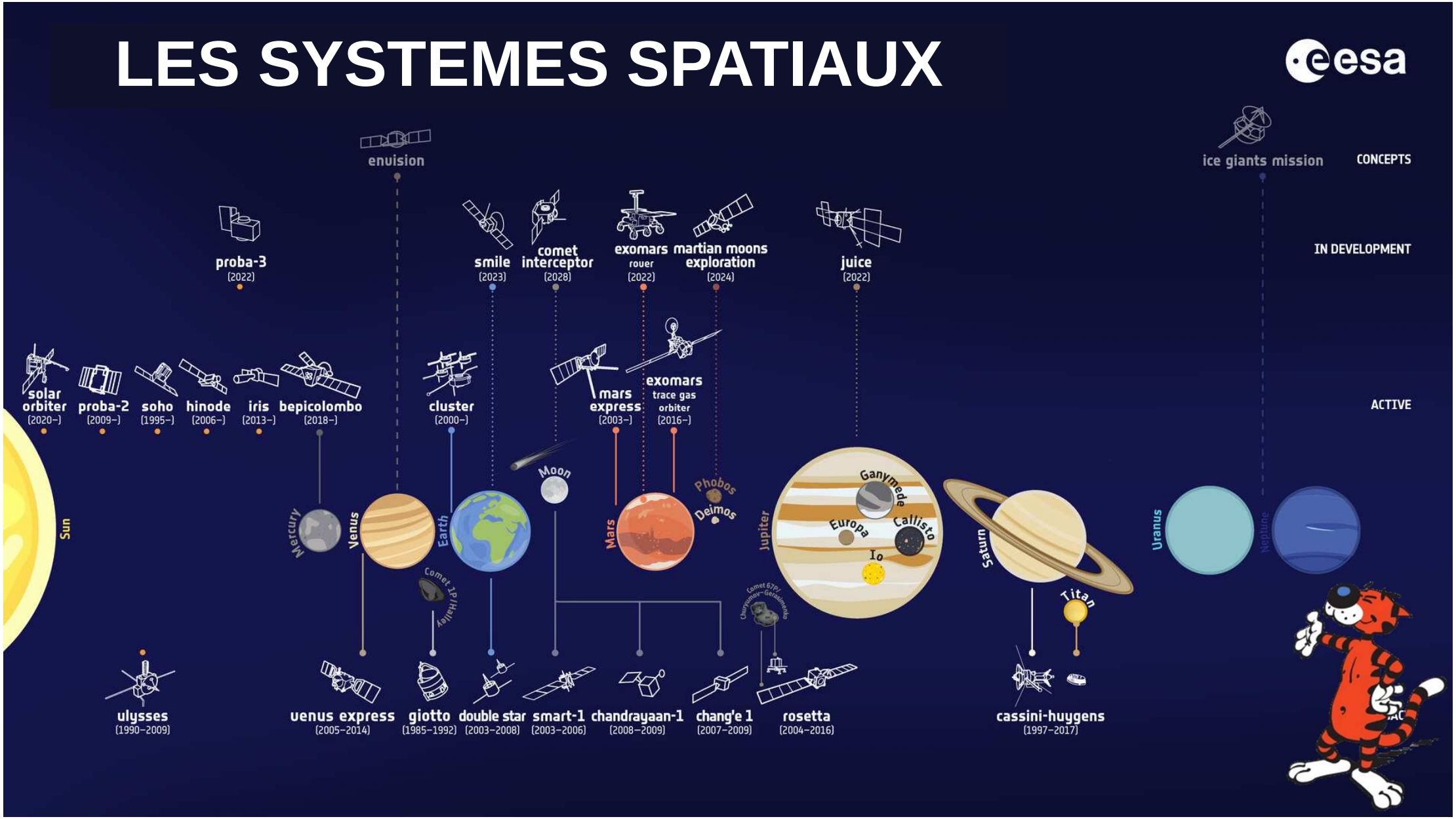
RAPPELS DE CRYPTOGRAPHIE



TLS 1.2 et TLS 1.3, pour l'établissement de connexions sécurisées https://, implémentent la PFS. Ce qui n'était pas le cas des versions antérieures (TLS 1.0/1.1 et SSL).


Triple DES
168bits (112bits effective)
DES
56bits
AES
128/192/256bits
Post
256bits
AES ?
512/1024bits
Symmetric algorithms
RSA
512
768
1024
2048
3072
Post Quantum Cryptography ?
ECC
160
224
256
Post Quantum Cryptography ?
DL
200
256
Post Quantum Cryptography ?
Asymmetric algorithms
SHA1
(160bits)
SHA256
SHA384
SHA512
?
MD4
MD5
(128bits)
Hash functions
SSL v2
SSL v3
TLS 1.0
TLS 1.1
TLS 1.2 (PFS)
TLS 1.3 (PFS)
?
Secure Layer protocol
84
60
39
27
13
?
Certificates validity
(months)
1990
2000
2010
2020
2030
2040

LES SYSTEMES SPATIAUX



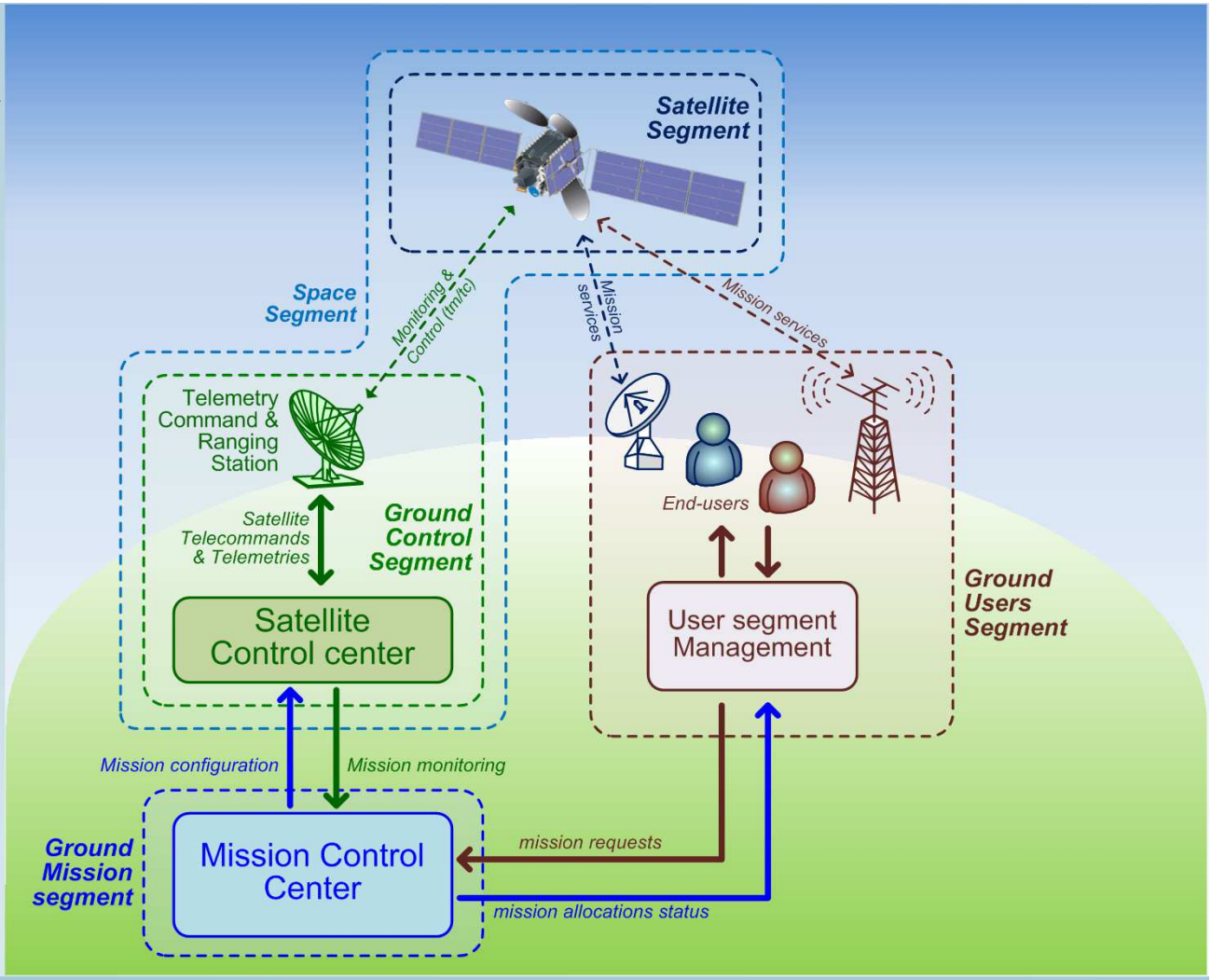
LES SYSTÈMES SPATIAUX

- Un système spatial repose sur le fait qu'une ou plusieurs des composantes de ce système (mais certainement pas toutes) repose(nt) sur un ou plusieurs élément(s) en orbite autour de la Terre ou en déplacement au sein du système solaire,
- Un système spatial intègre forcément une composante terrestre qui représente souvent la majorité du système spatial,
- La composante terrestre communique avec le(s) Spacecraft(s) via des liens bord-sol ou autrement dit : des liens de communication spatiaux.

Les satellites dont il est question ici sont dits « artificiels » car créés et mis en orbite par l'homme.

LES SYSTÈMES SPATIAUX

- Un système spatial se décompose généralement en 4 sous-systèmes appelés segments:
  - Le segment sol de contrôle du ou des satellite(s),
  - Le segment satellite(s),
  - Le segment sol de la mission,
  - Le segment sol des utilisateurs.
- Le satellite se décompose lui-même en :
  - Une Plateforme,
  - Une Charge Utile.

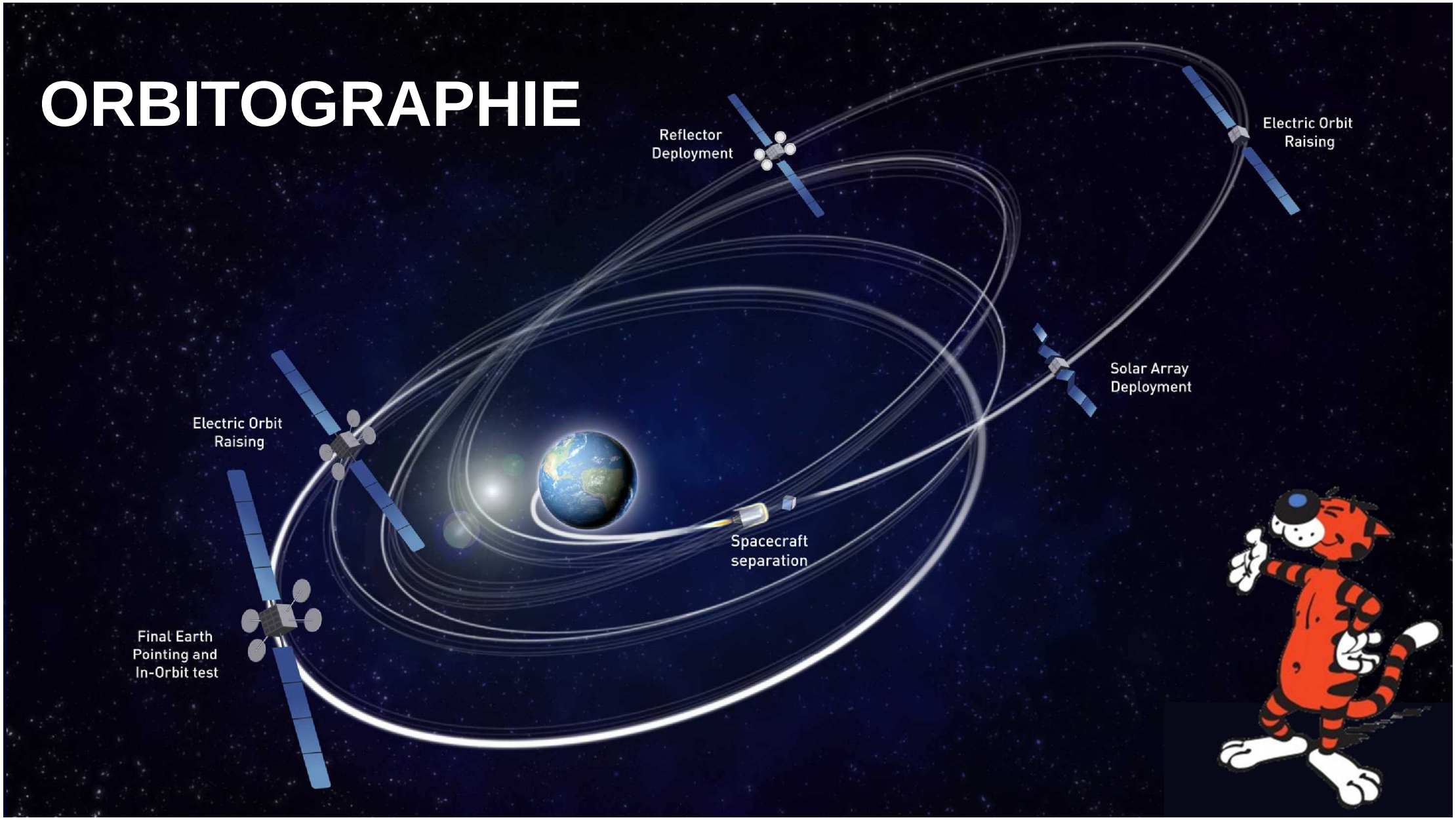


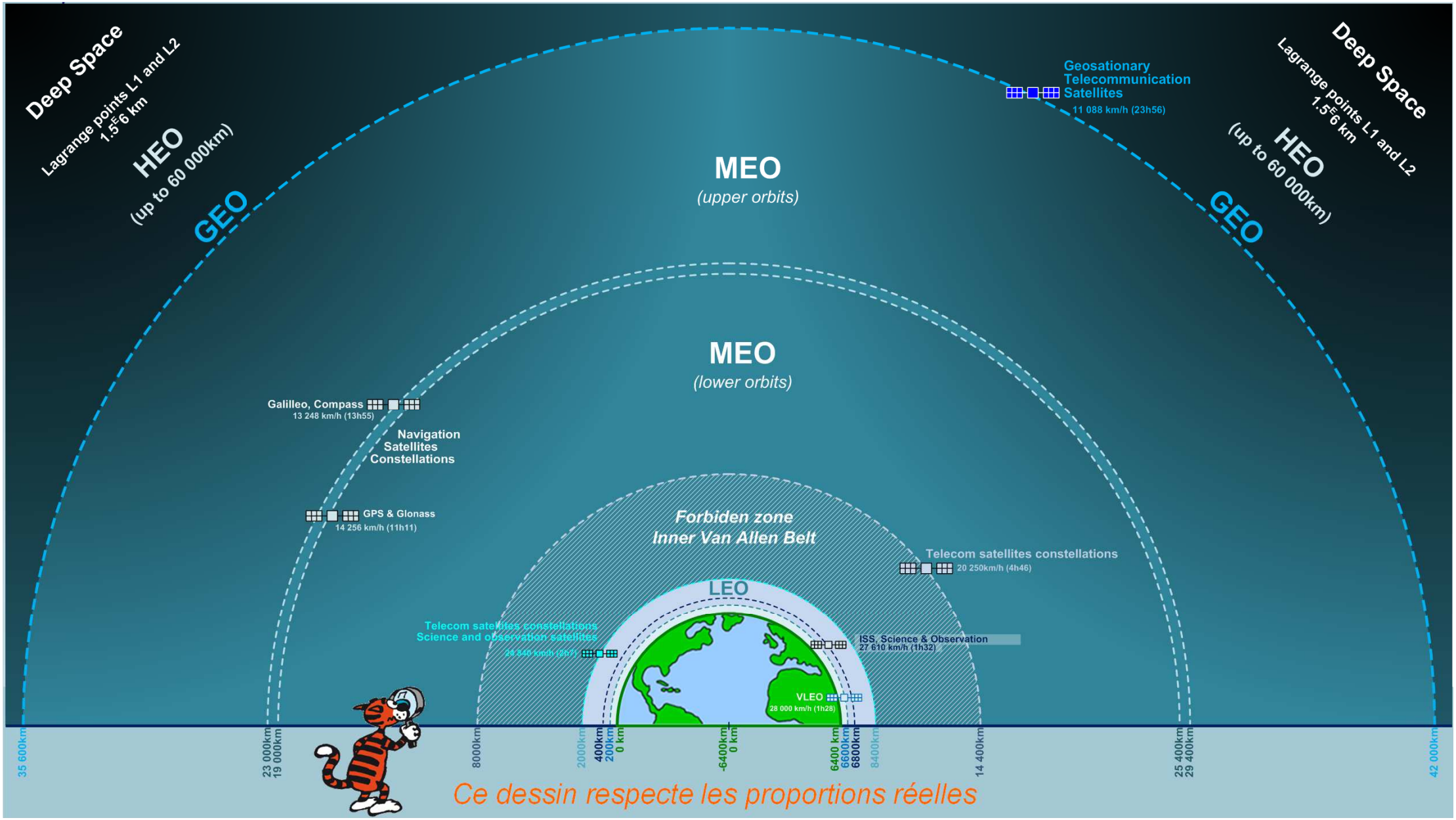
Souvent il est fait référence au « Segment Spatial » qui regroupe le segment sol de contrôle et le segment satellite.

LES SYSTÈMES SPATIAUX

- Le segment satellite contient le ou les satellite(s) qui assure(nt) la mission pour laquelle il(s) a(ont) été placé(s) en orbite,
- Le segment sol de contrôle permet de gérer le(s) satellite(s) en orbite, c.à.d :
  - De maintenir le satellite sur son orbite et dans sa position sur 3 axes (= attitude),
  - D'assurer la gestion des systèmes vitaux et de mettre en œuvre les actions de recouvrement nécessaires en cas d'anomalie à bord,
  - De configurer la charge utile du satellite (conformément aux demande du MCC) pour qu'elle assure les services à destination du segment utilisateur,
- Le segment de contrôle de la mission qui assure l'interface entre le segment utilisateur (requêtes d'entrée d'une nouvel abonné au service par ex.) et le segment de contrôle satellite à qui il envoie les demandes de configuration de la charge utile,
- Le segment sol utilisateur qui regroupe les utilisateurs finaux bénéficiaires de la capacité en orbite (télécommunication, navigation, données d'observation, etc.).

Les termes utilisés ici se retrouvent sur l'ensemble des systèmes spatiaux et chez presque tous les fabricants et opérateurs de ces systèmes.


ORBITOGRAPHIE
Reflector Deployment
Electric Orbit Raising
Solar Array Deployment
Electric Orbit Raising
Spacecraft separation
Final Earth Pointing and In-Orbit test

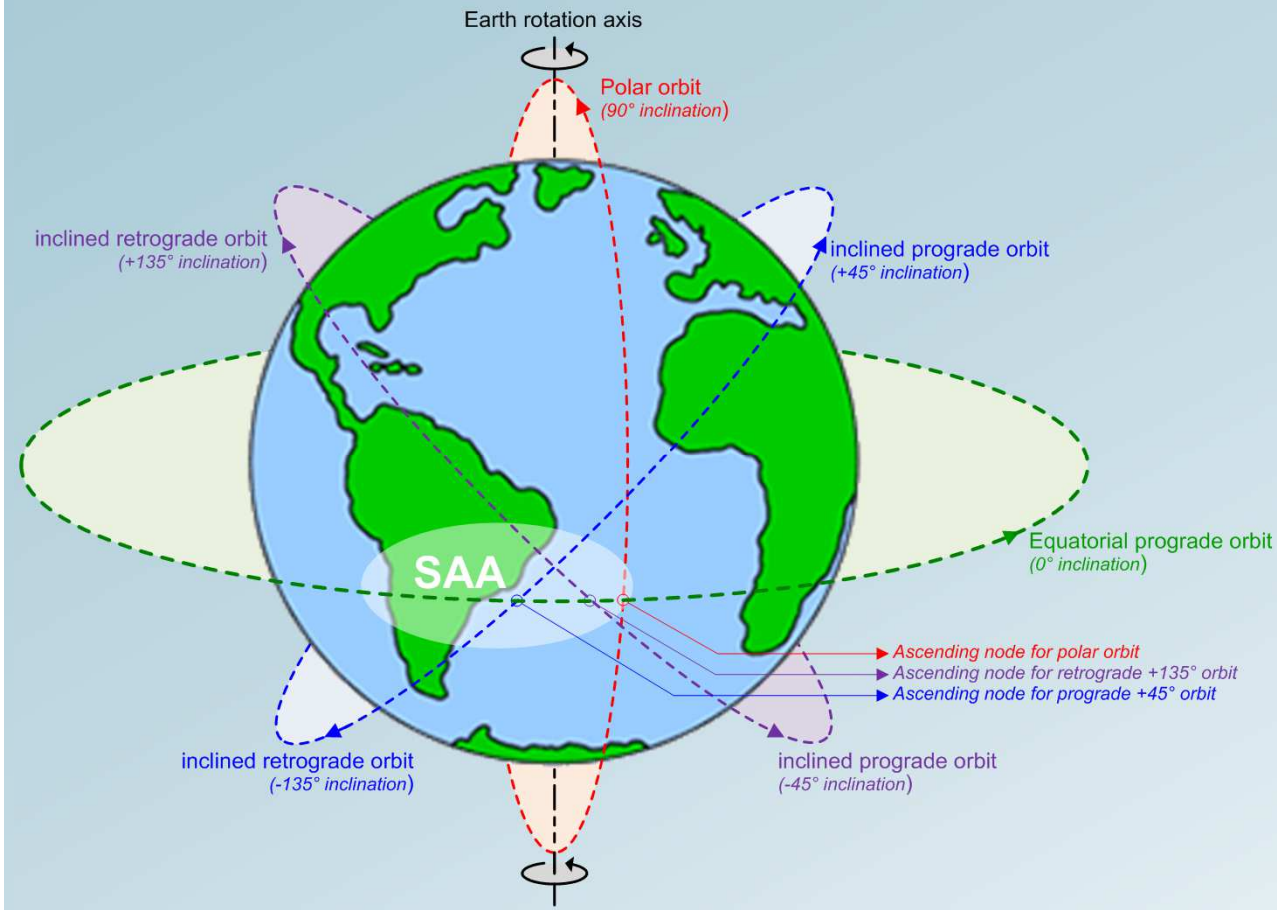

Deep Space
Lagrange points L1 and L2
1,5E6 km
HEO
(up to 60 000km)
GEO
Geosationary
Telecommunication
Satellites
11 088 km/h (23h56)
MEO
(upper orbits)
MEO
(lower orbits)
Galilleo, Compass
13 248 km/h (13h55)
Navigation
Satellites
Constellations
GPS & Glonass
14 256 km/h (11h11)
Forbiden zone
Inner Van Allen Belt
Telecom satellites constellations
20 250km/h (4h46)
LEO
Telecom satellites constellations
Science and observation satellites
ISS, Science & Observation
27 610 km/h (1h32)
VLEO
28 000 km/h (1h28)
35 600km
23 000km
19 000km
8000km
2000km
400km
200km
0 km
-6400km
0 km
6400 km
6600km
6800km
8400km
14 400km
25 400km
29 400km
42 000km
Ce dessin respecte les proportions réelles

ORBITOGRAPHIE

- **L**ow **E**arth **O**rbits [200km à 2000km] : pour les missions scientifiques (ISS), observation de la terre (ou écoute EMC), observation de l'espace (Hubble), Télécommunications (StarLink, OneWeb, IRIDIUM, etc.) et météo,
- **M**edium **E**arth **O**rbits [8000 à 35000km] : 2 zones utilisées, celle des 8000km pour des constellations de télécom et celle des 20 000km pour les systèmes GPS,
- **GEO**stationary orbtit [35 685 km] : Orbite sur le plan équatorial uniquement pour des missions de télécommunication car le satellite se retrouve à la verticale d'un point fixe vis à vis du sol ➔ visibilité continue idéale pour les télécoms et aussi météorologique,
- **H**igh **E**lliptic **O**rbits [périgée < 800km et apogée > 36 000km] : Orbites elliptiques inclinées pour des missions Télécom au niveau des cercles polaires (appelées aussi orbites de Molnya ou orbites « Toundra ») ➔ missions russes ou nord-américaines.

La lune orbite entre 360 000 et 405 000 km de la Terre avec une période de révolution autour de la Terre de 27 jours. Il existe aussi les points de Lagrange pour les missions scientifiques particulières (SOHO, JamesWeb telesope, Hercshel Panck, etc.).

ORBITOGRAPHIE



Les orbites polaires (entre 80° et 100°) offrent une couverture à 100% de la surface de la terre et sont héliosynchrones (**S**un **S**ynchronous **O**rbits – SSO) car les satellites passent toujours à la même heure au-dessus d'un point donné (très utile en observation),

L'orbite GEO ne permet pas de couvrir les pôles au-delà de +80°/-80°,

Les orbites prograde sont privilégiées car elles nécessitent moins de carburant pour la mise à poste des satellites ➔ elles bénéficient de l'effet de fronde de rotation de la Terre.

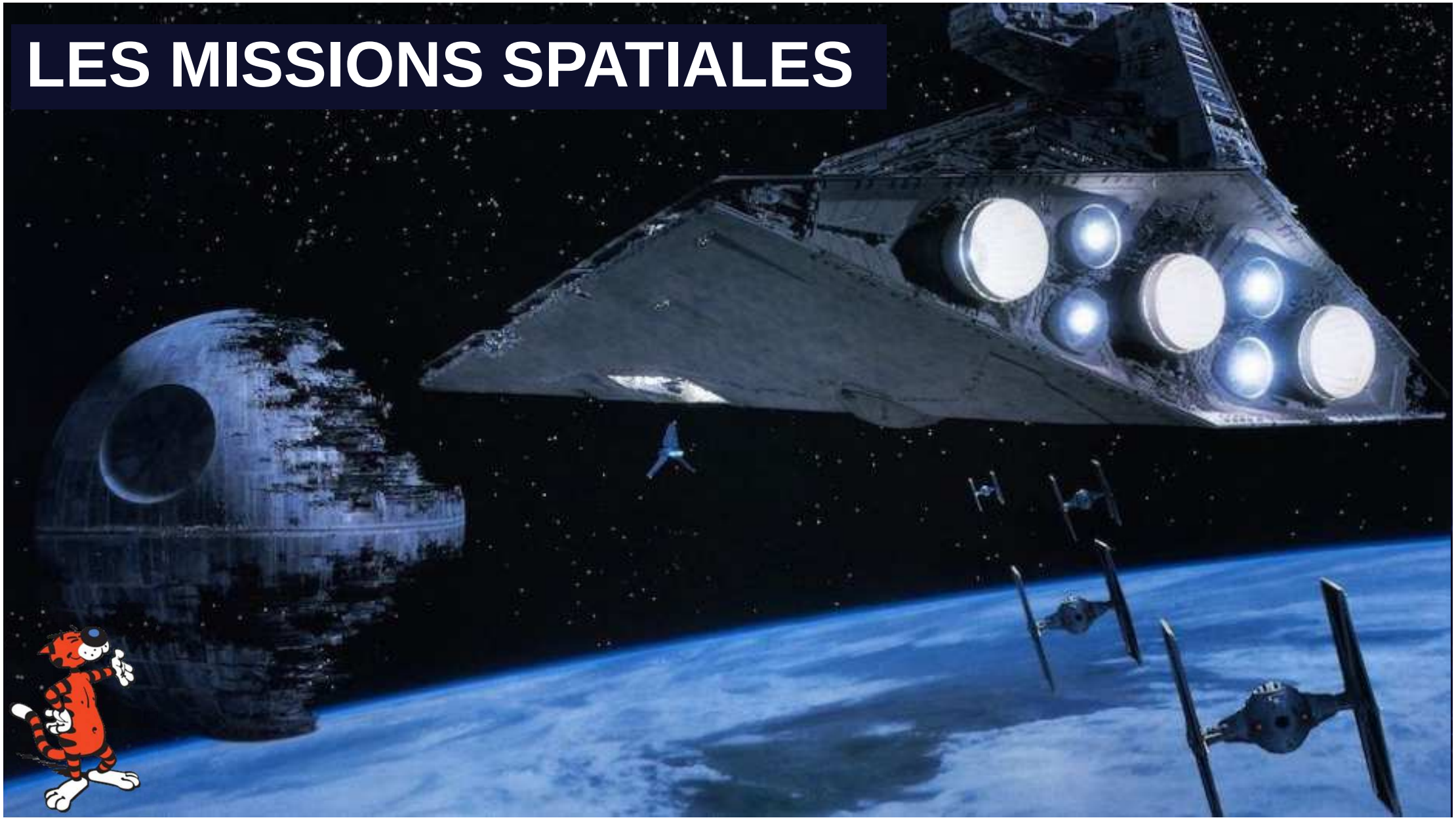
L'orbite équatoriale est forcément prograde et avec une incinaison à 0°.

LES ORBITES

- Il ne suffit pas de mettre un satellite en orbite pour pouvoir l'utiliser dans le cadre de sa mission,
- Durant toute la durée de vie du satellite, il est nécessaire d'effectuer des manœuvres dites de « maintien à poste » (OSK ou "OnStation Keeping" pour les satellites géostationnaires) ou des manœuvres de correction d'orbite pour les satellites LEO/MEO,
- Les satellites sont tous soumis aux fluctuations de gravitation imposées par la lune, par les marées, par les gradients de gravitation terrestres, et par la position de la terre autour du soleil. Ces variations les font dériver de leur position orbitale (GEO) ou de leur orbite initiale (LEO/MEO),
- Les opérations de correction d'orbite et de maintien à poste nécessitent d'envoyer régulièrement des télécommandes et de recevoir les télémesures des satellites . Un satellite qui n'est plus commandé ni "monitoré" est, à terme, perdu!

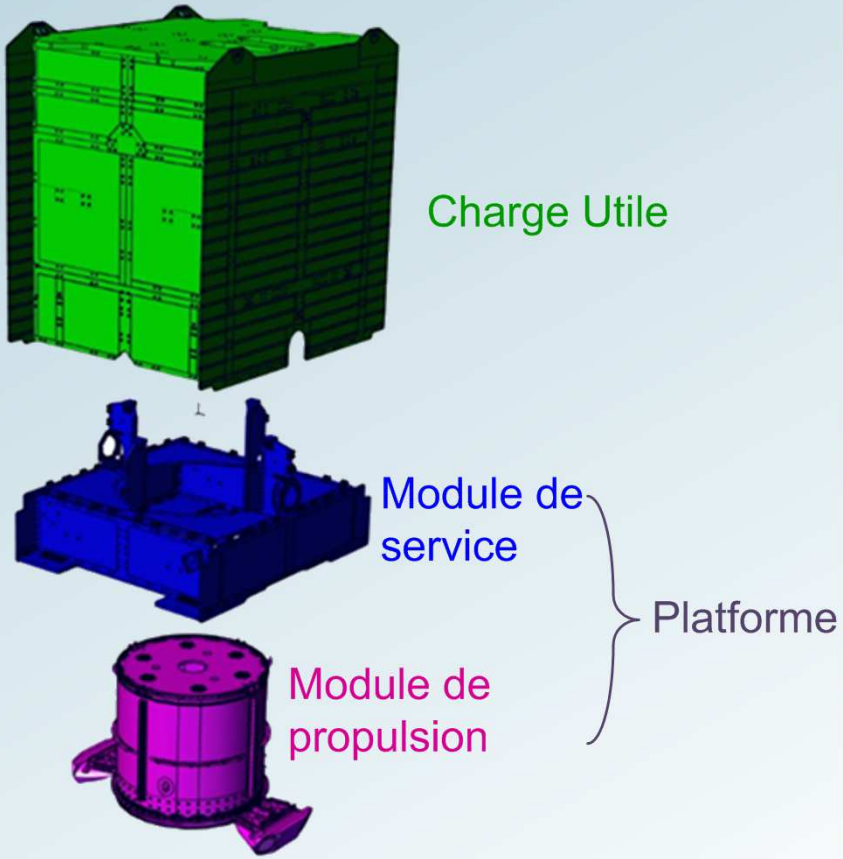
Le lien des Télécommandes et des Télémesures entre le segment sol de contrôle et le(s) satellite(s) est vital pour le système spatial.

LES MISSIONS SPATIALES



LE SATELLITE

- De façon très simplifiée un satellite est généralement constitué de deux éléments principaux :
  - La Plateforme : qui regroupe l'ensemble des éléments qui permet au satellite d'être maintenu sur son orbite et de maintenir les systèmes vitaux (panneaux solaire, batteries, refroidissement, propulsion, avionique etc…),
  - La Charge Utile : qui regroupe les équipements et sous-systèmes relatifs à la mission : communication, observation, navigation, …



La disponibilité est un paramètre fondamental à prendre en compte dans les missions de télécommunication.

LE SATELLITE

Sources RF

Face Terre

Réflecteurs (antennes)

Panneaux ou Générateurs Solaires (GS)

Adaptateur Lanceur

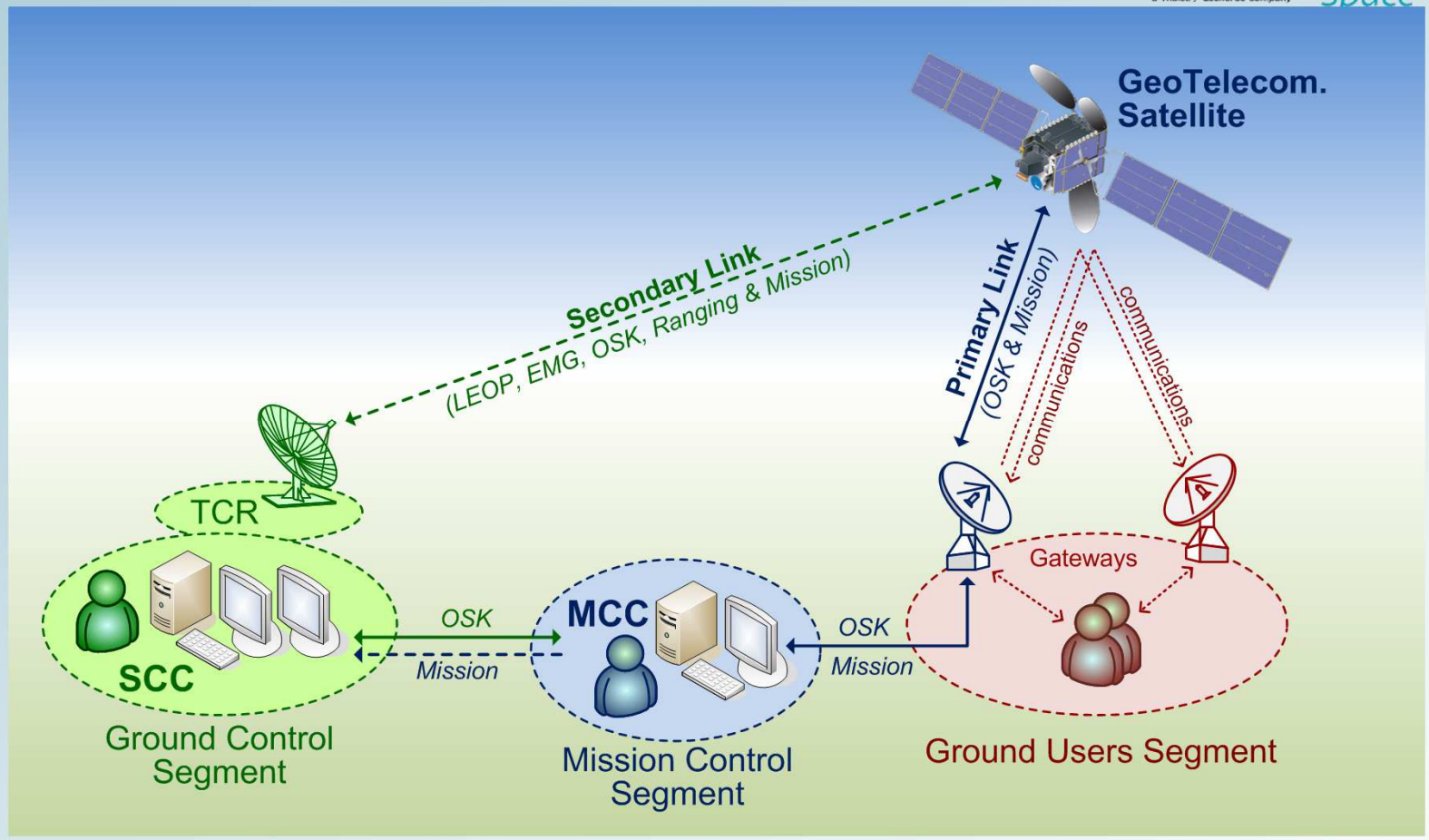
MISSION TÉLÉCOM

- L'ESA et la commission européenne ont défini 3 types de missions de télécommunication par satellites :
- *Les missions **ComSatCom** : qui représentent des missions de télécommunication pour un usage exclusivement civil (Konnect VHTS par exemple) avec un bon niveau de disponibilité,*
- *Les missions **GovSatCom** : qui représentent les missions de télécommunication pour un usage identifié comme critique : les services d'alerte, de secours, d'intervention ou même de télécommunication militaire non sensible (ex: Athena-Fidus). Ce type de mission offre un fort niveau de disponibilité,*
- *Les mission **MilSatCom** : qui représentent les missions de télécommunication pour les armées (SKYNET, SYRACUSE et SICRAL). Ce type de missions garantit un niveau de disponibilité maximal.*

La disponibilité est un paramètre fondamental à prendre en compte dans les missions de télécommunication.
*Le terme **GeoSatCom** désigne un satellite de télécom en position géostationnaire*

MISSION TÉLÉCOM GEO

- Les missions GeoSatCom (à 36 000 Km) couvrent une zone fixe (1/3 de la surface terrestre) et offrent des capacités de télécommunication très large bande avec, néanmoins, une latence assez élevée de l'ordre de 500ms min.



Les missions GéoSatCom ne couvrent pas les zones au-delà des +/- 80° de latitude. Les pôles, bien que peu peuplés, ne sont pas couverts.

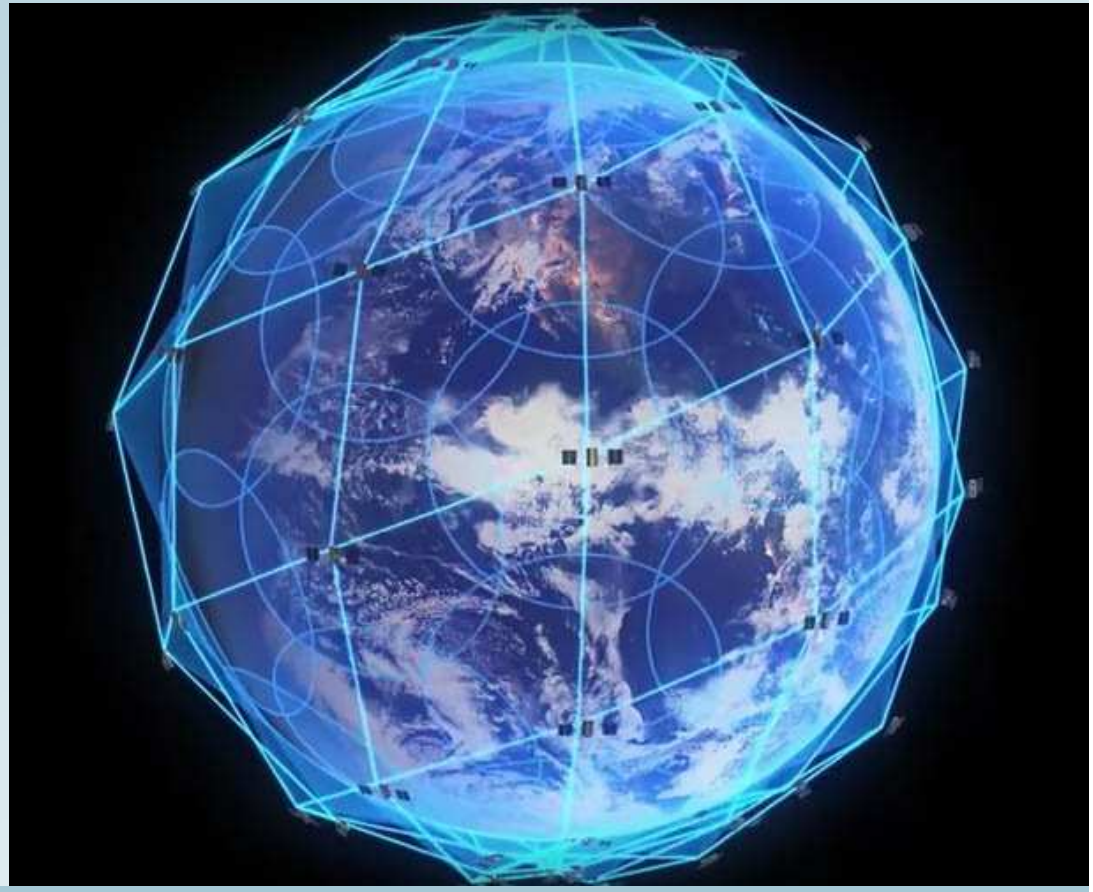
MISSION TÉLÉCOM GEO

- Depuis 2015, les satellites GéoSatCom intègrent plusieurs liens de commande et contrôle bord-sol (= Lien de **T**élése**M**esure et de **T**éle**C**ommande - TM/TC:
  - Le **primary link** (ou High Speed Link) : il est utilisé en phase d'opération nominale et permet de configurer la charge utile (configuration des profils de communication avec le segment sol utilisateur) et la plateforme (manœuvres de maintien à poste essentiellement). Ce lien n'est accessible que lorsque le satellite est pointé Terre (antennes directionnelles),
  - Le **secondary link** (ou Low Speed Link) : il est utilisé pendant la phase de mise à poste (transfert de l'orbite GTO vers l'orbite finale GEO) ou lors de phase de recouvrement du satellite lors d'une défaillance majeure (➔ passage en mode survie). Ce lien est accessible quelle que soit l'orientation du satellite dans l'espace grâce aux antennes omnidirectionnelles.
- Ces deux liens sont les cordons ombilicaux qui permettent "d'ancrer" le satellite géostationnaire sur une position orbitale fixe vis à vis du sol.

*La charge utile d'un GeoSatCom embarque un DTP : **D**igital **T**ransparent **P**rocessor. Les signaux montants sont redescendus sans démodulation de niveau bit, mais avec seulement des transpositions fréquentielles. Le DTP doit être vu comme un répéteur.*

MISSION TÉLÉCOM LEO

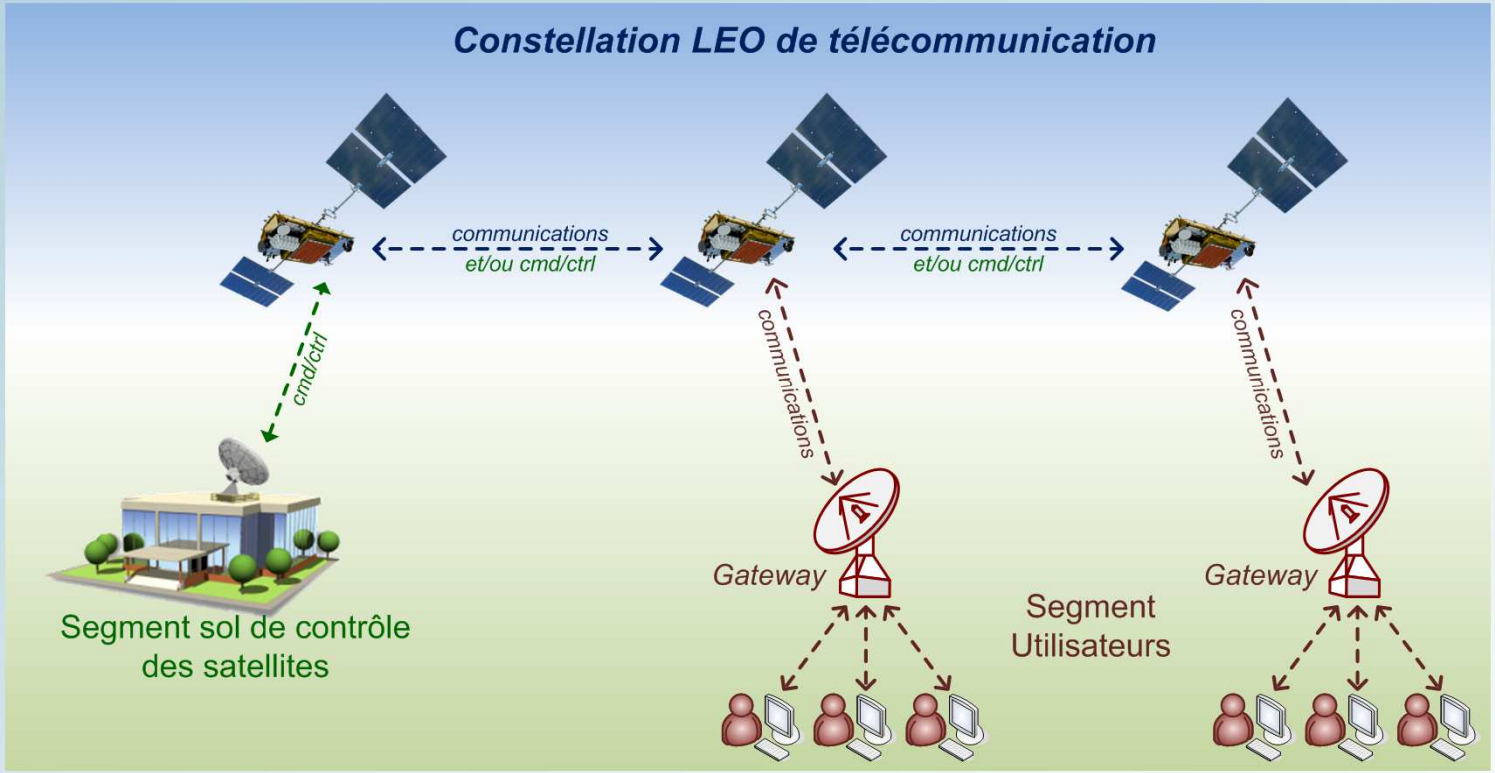
- Les constellations de télécommunication en orbite basse couvrent (selon l'orbite, l'altitude et l'inclinaison choisies) l'ensemble du globe et permettent des communications avec un faible temps de latence (< à 100ms),
- Selon les constellations le nombre de satellites peuvent varier de 60 à 500 voire plus.
- Plus il y a de satellites, plus ils sont petits et moins ils embarquent de capacité.



*La charge utile d'un LeoSatCom embarque un OBP : **O**n**B**oard **P**rocessor. Les signaux montants sont démodulés, traités et remodulés. L'OBP doit être vu comme un routeur. Certaines constellations embarquent même des routeurs IP.*

MISSION TÉLÉCOM LEO

- Les constellations permettent d'implémenter des liens inter-satellites (ISL – Inter Satellite Link),
- Ces liens inter-satellites permettent d'augmenter la disponibilité et les performances du système,
- Chacun des satellites et capable de router des communications (ou même les TM/TC) vers un autre satellite qui les redescendra ensuite vers le destinataire final au sol

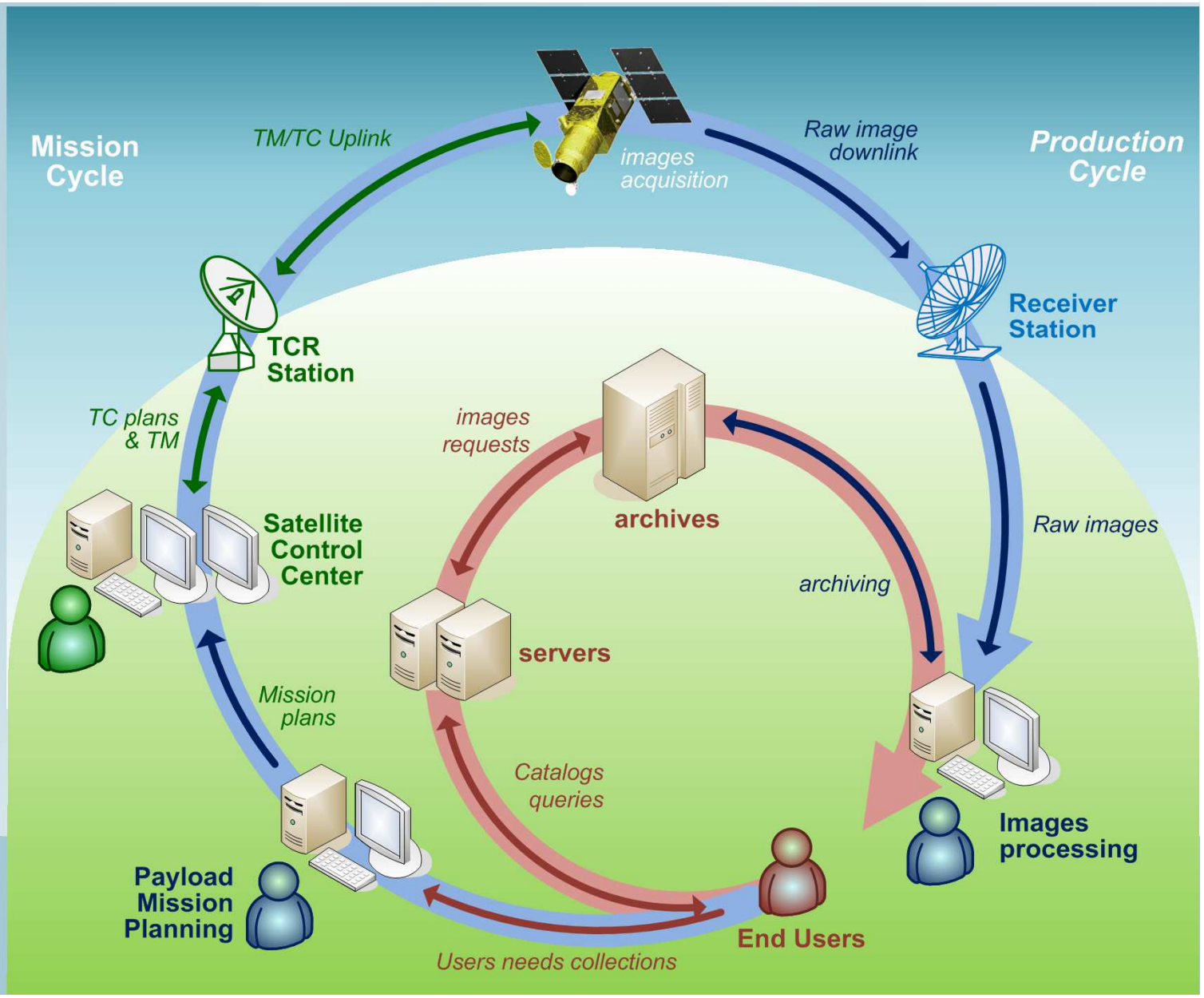


Il existe, dans de plus rares cas, des constellations de télécommunication en orbite MEO. Exemple 03B (Other 3 Billions) avec 20 satellites en orbite à 8063km.

OBSERVATION ET SCIENCE (LEO)

Les systèmes spatiaux d'observation (et les missions scientifiques en général) sont forcément portées par des satellites en orbite basse (< 800km) sur des orbites hellio-synchrones (ou orbites polaires SSO).

Plus on est proche de la Terre, mieux on la voit!



MISSION D'OBSERVATION ET SCIENTIFIQUE

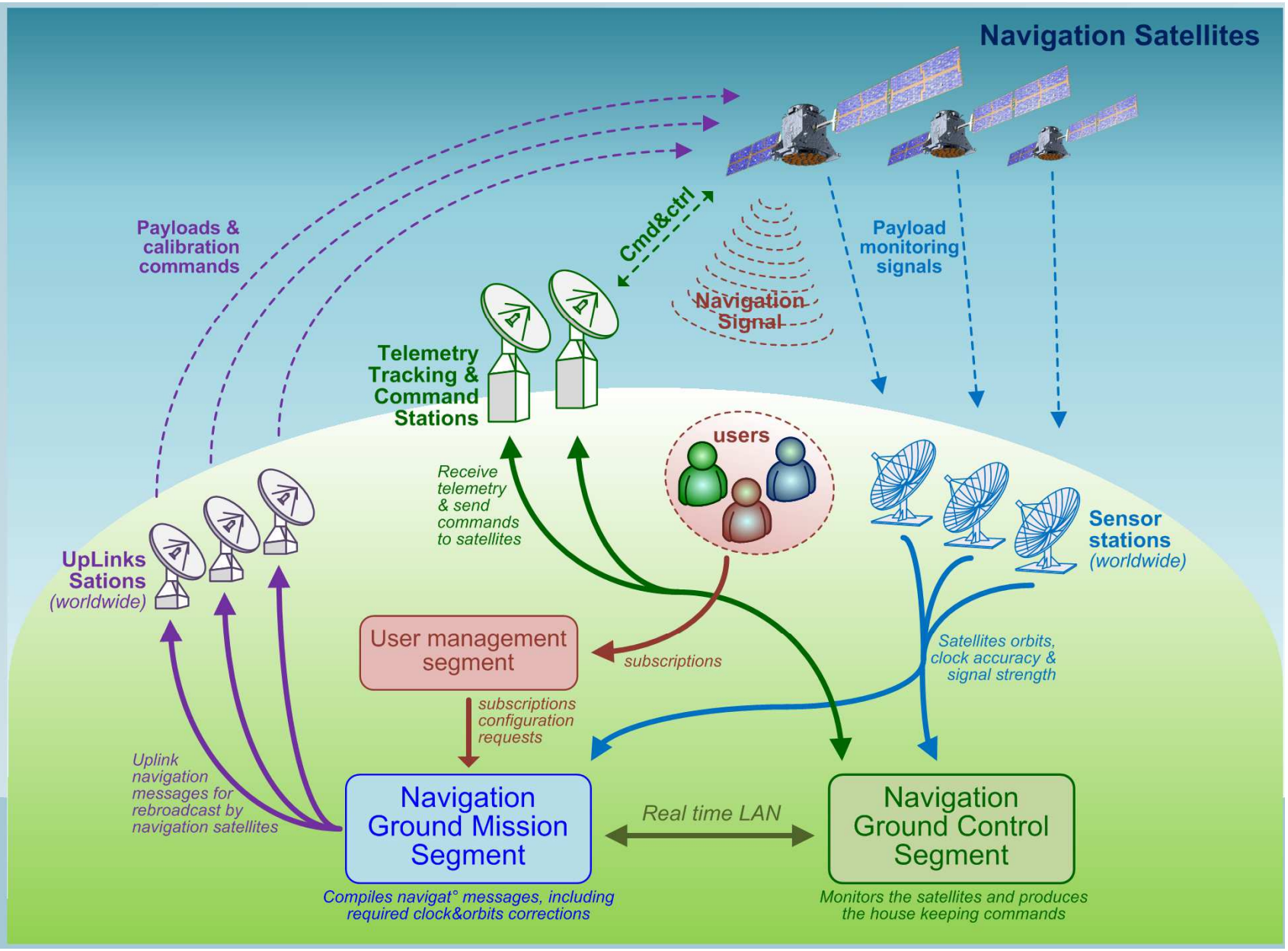
- Ici, ces missions sont en général chargées de récolter des informations d'observation de la terre : imagerie essentiellement,
- Les satellites d'observation embarquent un lien classique de TM/TC qui permet d'opérer le satellite,
- Ils embarquent aussi un lien dédié pour redescendre les images/informations vers les centres au sol ➔ appelé souvent lien TMi (**T**élé**M**esure **I**mage),
- Ce lien est soumis à une double contrainte forte: le temps de visibilité réduit des satellites LEO (3 à 6 minutes selon l'altitude) et au volume des données à redescendre en si peu de temps (de l'ordre du térabit),
- Cela implique des liens TMi avec des débits de l'ordre du Gbits/seconde,

Les missions d'observation peuvent être scientifiques (mission Sentinel) ou bien êtes des missions d'espionnage (observation et écoute radar) comme le sont les missions CERES et CSO pour le compte du ministère des armées.

NAVIGATION

Les systèmes de navigation par satellite fournissent aux utilisateurs au sol (bateaux, voitures etc…) un signal qui leur permet de connaitre exactement leur localisation à la surface de la Terre.

Le GPS est devenu indispensable!

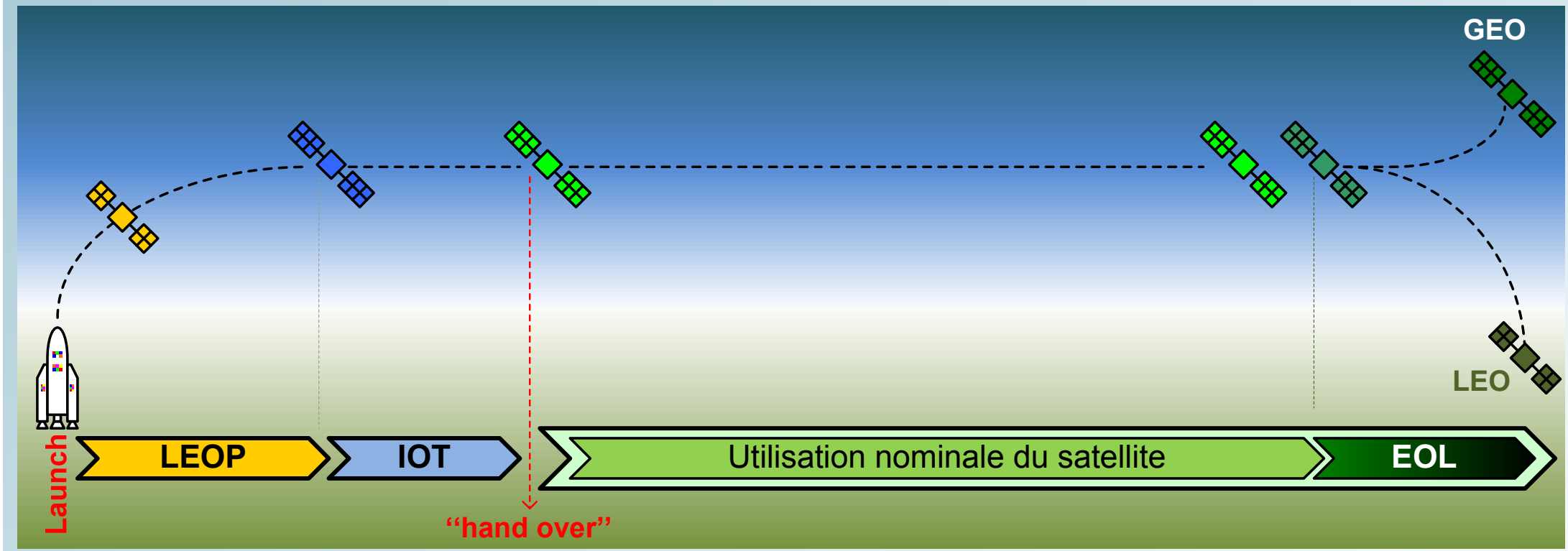


MISSION NAVIGATION

- Ces missions sont exclusivement dédiées à la génération de signaux descendants de positionnement par satellites,
- A l'heure actuelle il existe 4 constellations de 20 à 30 satellites en orbite MEO (20000 km environ) : Le système américain **GPS**, le système européen **Galiléo**, le système Russe **Glonass** et le système Chinois **Compass** (ou Beidou),
- Ces systèmes nécessitent des stations sols réparties autour du globe pour être opérés,
- En plus des liens TM/TC et des liens liées à la mission, il faut prendre en compte le lien descendant de navigation qu'il est important de sécuriser en authenticité et disponibilité,
- Le système Galiléo produit plusieurs signaux de navigation dont le signal PRS (**P**ublic **R**egulated **S**ervice) qui est garanti en authenticité (anti-spoofing), confidentialité et en disponibilité.

Les systèmes de navigation actuels n'intègrent pas de lien inter-satellites.

CYCLE DE VIE DES SATELLITES



Cette figure décrit uniquement le cycle de vie opérationnel du satellite et pas son cycle industriel. La phase de conception/développement/tests n’est pas représentée.

CYCLE DE VIE DES SATELLITES

- Le cycle de vie d'un satellite est propre au satellite et n'est forcément lié au cycle de vie du système spatial qui peut continuer de vivre si les satellites sont renouvelés,
- Le cycle de vie d'un satellite, après le lancement, se décompose en 4 phases :
  - La phase de **LEOP** (**L**ow **E**arth **O**rbit **P**hase) : Cette phase permet de passer d'une orbite de transfert (celle du lanceur) vers l'orbite finale visée. Cette phase est gérée par le concepteur du satellite. Pendant le LEOP, quelques tests permettent de s'assurer que les systèmes vitaux du satellite sont fonctionnels et qu'ils permettent d'opérer le satellite pendant cette phase,
  - La phase **IOT** (**I**n **O**rbit **T**est) : Le satellite est sur son orbite et va être testé par l'industriel du point de vue de sa mission (test de la charge utile). Cette phase ne dure que quelques jours,
  - La phase **OCO** (**O**n-orbit **C**ontrol **O**perations) : c'est la phase principale durant laquelle le satellite est opéré pour remplir sa mission, elle dure plusieurs années,
  - La phase **EOL** (**E**nd **O**f **L**ife) : Cette phase permet de configurer le satellite en vue de sa fin de vie: passivation et désorbitation.
- La sécurité du satellite doit être assurée pour tout son cycle de vie.

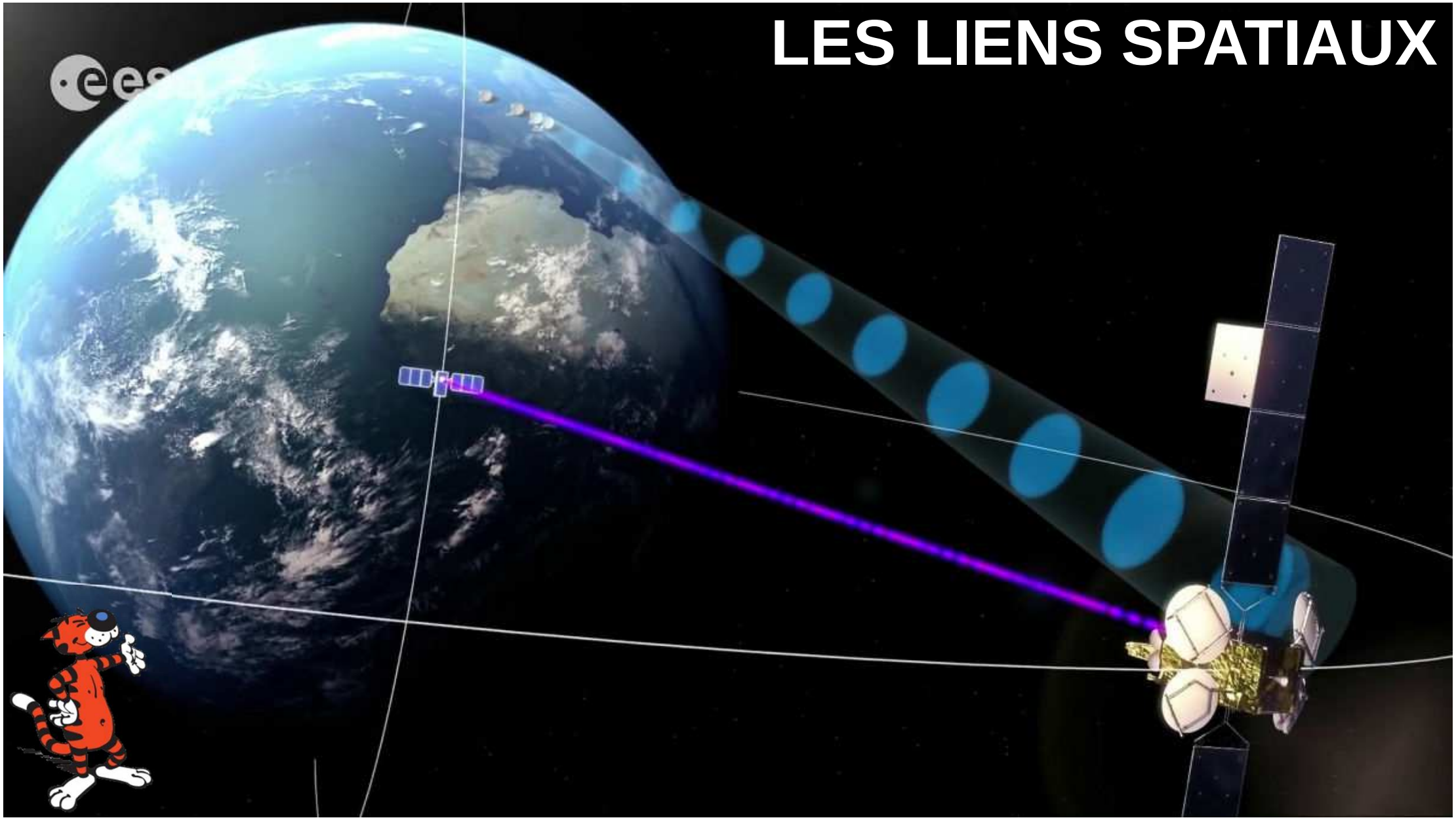
Depuis quelques années, les satellites sont munis de moteurs électriques (en remplacement des systèmes de propulsion chimique) qui leur permettent d'embarquer moins de carburant tout en allongeant leur durée de vie.

DURÉE DE VIE

- La durée de vie d'un satellite en orbite dépend directement de la taille de son réservoir de carburant, mais aussi de l'orbite sur laquelle il se trouve,
- Les gros satellites géostationnaires embarquent beaucoup de carburant et sont conçus pour durer entre 15 et 20 ans,
- Les petits satellites LEO (qui sont plus soumis à l'attraction terrestre) sont conçus pour durer entre 8 et 10 ans, voire beaucoup moins pour les nano-satellites,
- Les satellite MEO eux sont conçus pour une douzaine d'années de durée de vie en orbite,
- En fin de vie, les satellites LEO sont désorbités pour être dirigés vers les couches hautes de l'atmosphère (100km) et pour y être désintégré ou sinon plonger dans l'océan pacifique (au point Némo) pour les plus gros (ex: station Mir),
- Les satellites Géostationnaires en fin de vie sont poussés à 300 kms au-dessus de l'orbite géo, puis passivés et laissés à la dérive. Ils rejoignent les deux puits gravitationnels au-dessus de la Cordillères des Andes et au-dessus de l'Himalaya.

Il est important de bien connaître la durée de vie en orbite afin de dimensionner au mieux des fonctions qui seront encore utilisées pendant 10 ans ou plus. Il faut donc s'assurer que ces fonctions ne seront pas obsolètes en fin de vie.

LES LIENS SPATIAUX

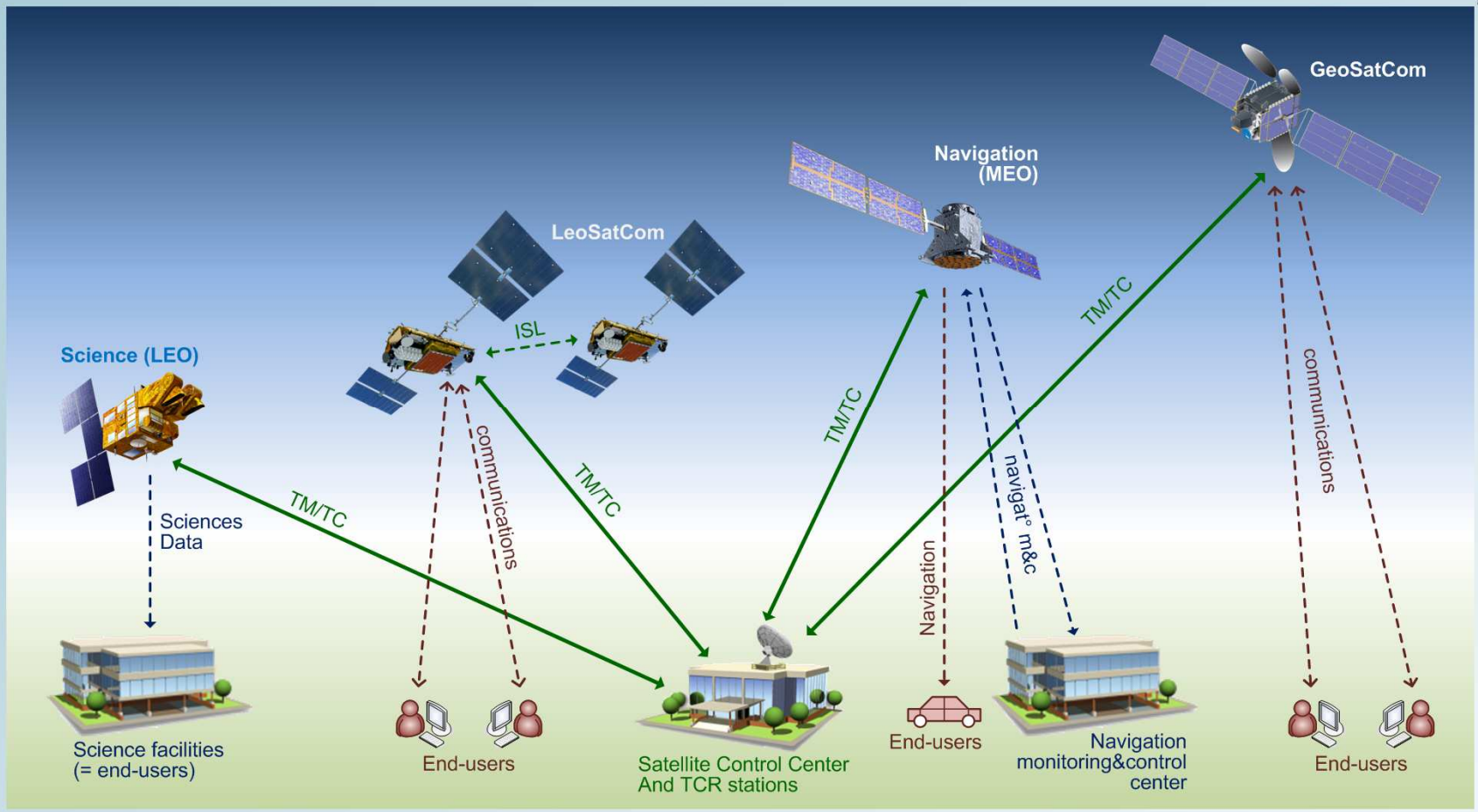


LES LIENS SPATIAUX

- Si nous récapitulons, les liens entre le sol et les satellites en orbite sont de plusieurs natures :
  - Liens TM/TC pour commander et "monitorer" les satellites : plateforme et charge-utile,
  - Liens de télécommunication entre les utilisateurs sol et non démodulé à bord des satellites de télécom (passage par un DTP),
  - Liens de télécommunication entre les utilisateurs au sol et démodulé à bord (passage par un OBP) pour les satellites télécom LEO de type IP,
  - Liens de données missions (images, relevés d'altimétrie, etc.) : charge utile uniquement,
  - Liens de mesure de distance (non protégés),
  - Liens inter-satellites pour véhiculer des communications et/ou des TM/TC.

Cela fait tout un bestiaire de liens (bord-sol ou bord-bord) avec des objectifs différents et donc des protocoles différents.

SYNTHÈSE DES LIENS SPATIAUX



Tous les satellites ont en commun la présence obligatoire d'un lien de TM/TC qui permet de l'opérer depuis le sol.

LES LIENS SPATIAUX

- Un lien identifié comme un lien TM/TC est un lien qui contient :
  - Des télécommandes à destination du satellite, ces télécommandes ont pour seul objet de faire effectuer des actions particulières au satellite (manœuvres) ou de configurer un équipement interne au satellite,
  - Des télémesures issues du satellite pour rendre compte de l'exécution des commandes reçues ou bien de l'état général des fonctions internes du satellite.
- Les données dites missions, celles échangées entre un satellite et un segment sol contiennent des informations relatives à la mission elle-même,
- Ces informations peuvent être : des images, des mesures de la hauteur des océans, des mesures d'écoute en radio fréquence etc.,
- Dans ce cas, les données missions sont identifiées comme des données dites AOS (**A**dvanced **O**rbiting **S**ystem),
- Les TM/TC sont traitées au niveau du centre de contrôle satellite (CCS),
- Les données AOS sont traitées par le centre dédié qui les transmettra aux utilisateurs finaux (universitaire, chercheur, institutionnels, étatiques etc…) qui pourront ainsi les exploiter.

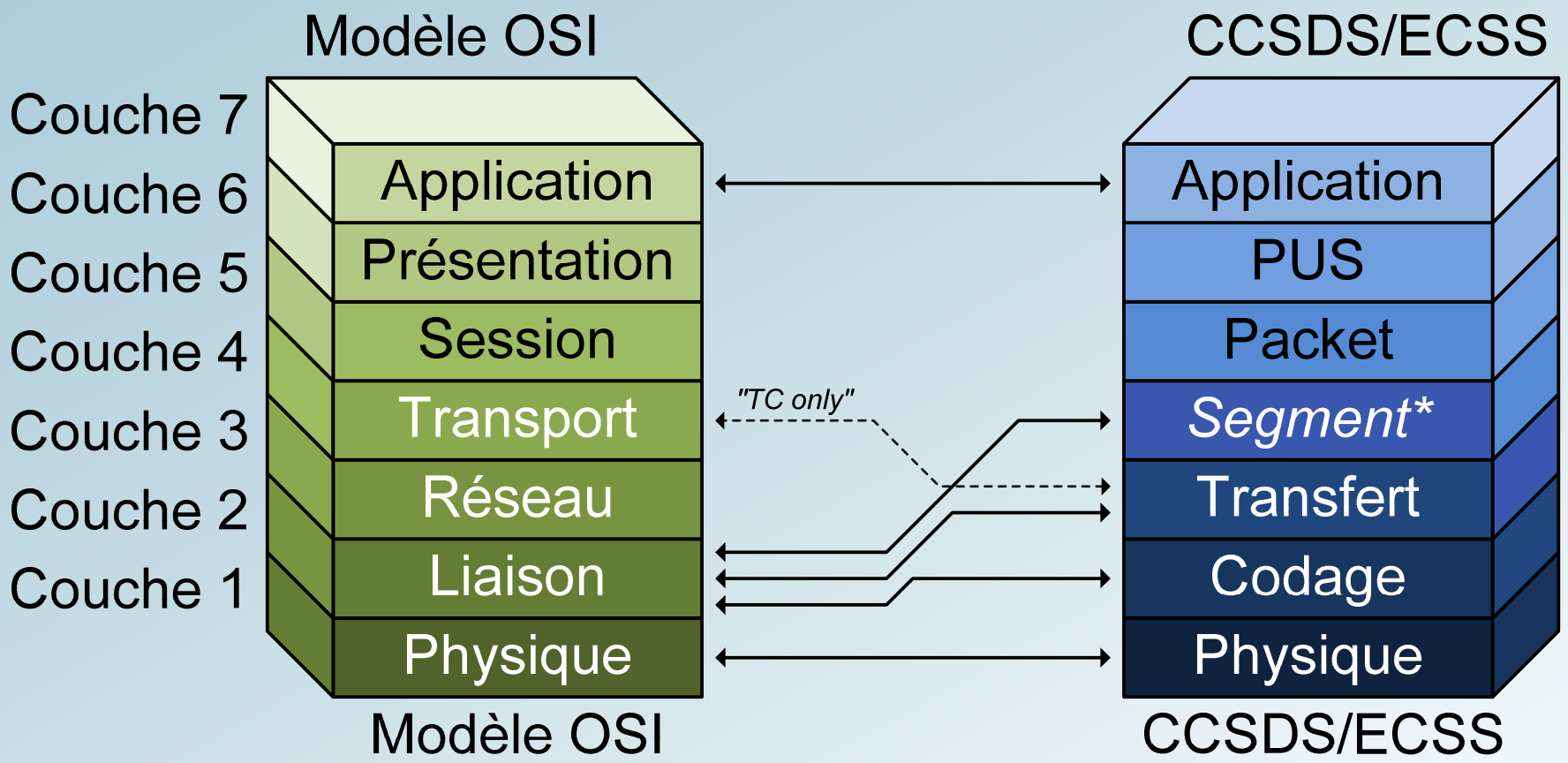
Il existe, plus rarement, des canaux AOS montants, par exemple : les échanges audio et vidéo entre le centre des opérations au sol et la station spatiale internationale.

LES LIENS SPATIAUX

- Les protocoles de communication spatiaux sont standardisés par 2 organismes qui réunissent les agences spatiales internationales et/ou européennes (NASA, ESA, CNES, JAXA, ISRO, DLR, ROSCOSMOS, etc.),
- **CCSDS** : *"The **C**onsultative **Co**mmittee for **S**pace **D**ata **S**ystems (CCSDS) is an international voluntary consensus organization of space agencies and industrial associates interested in mutually developing standard data handling techniques to support space research, including space science and applications."*
- **ECSS** : *"The **E**uropean **C**ooperation for **S**pace **S**tandardization (ECSS) is an initiative established to develop a coherent, single set of user-friendly standards for use in all European space activities."*
- En général les ECSS sont dérivés des CCSDS. On utilise en priorité les ECSS s'ils existent et, sinon, on utilise les CCSDS.

Le CCSDS et l'ECSS couvrent tous les domaines du spatial et bien au-delà des seules communications spatiales.

LES LIENS SPATIAUX



La définition des couches CCSDS/ECSS ne suis pas vraiment le modèle OSI. Et pour cause, certaines des fonctionnalités du modèle OSI ne sont pas toujours applicables (fonctionnalités d'interconnexion de réseaux par exemple).

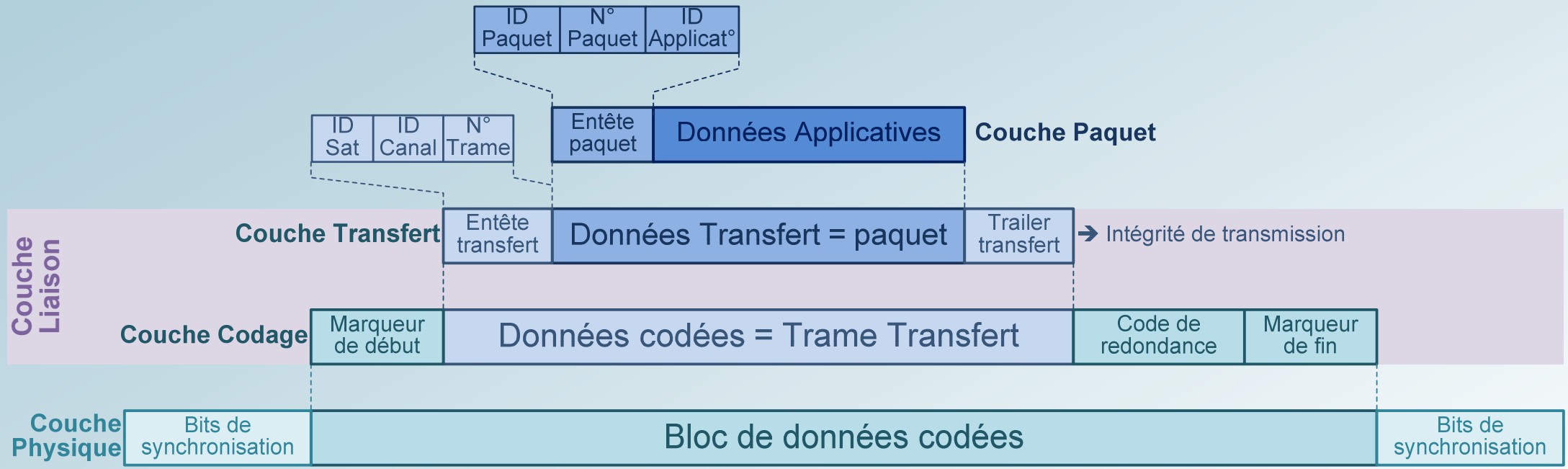
LES LIENS SPATIAUX

- Les standards CCSDS et ECSS ont été mis en place initialement pour faire communiquer un centre de contrôle sol avec un engin spatial en orbite,
- La notion d'interconnexion de réseau locaux (ou inter-network) n'est pas applicable dans ce cas précis ce qui explique que la couche réseau ne soit pas définie,
- Comme les liens bord-sol passent par la voie des airs, les standards CCSDS et ECSS ont introduit au niveau liaison des mécanismes pour garantir un minimum de QoS,
- La couche liaison CCSDS/ECSS intègre des capacités de retransmission de trames qui sont normalement propre à la couche transport du modèle OSI (ex: TCP) ,
- Par ailleurs, certaines missions télécom embarquent des routeurs TCP-IP (StarLink, OneWeb,…) pour interconnecter des réseaux locaux au sol. Dans ce cas précis, il est nécessaire de se conformer au modèle OSI avec les couches réseau (IP) et transport (TCP). Seule les couches physiques et liaison restent propre au spatial.

Il faut voir la couche liaison des systèmes spatiaux comme un mega WiFi super robuste et avec une très grande portée.

LES LIENS SPATIAUX

- La structure des couches selon les standards CCSDS/ECSS permet de mieux comprendre leur utilité et spécificité,



Cette structure de couches est présentée sans sécurité à priori.

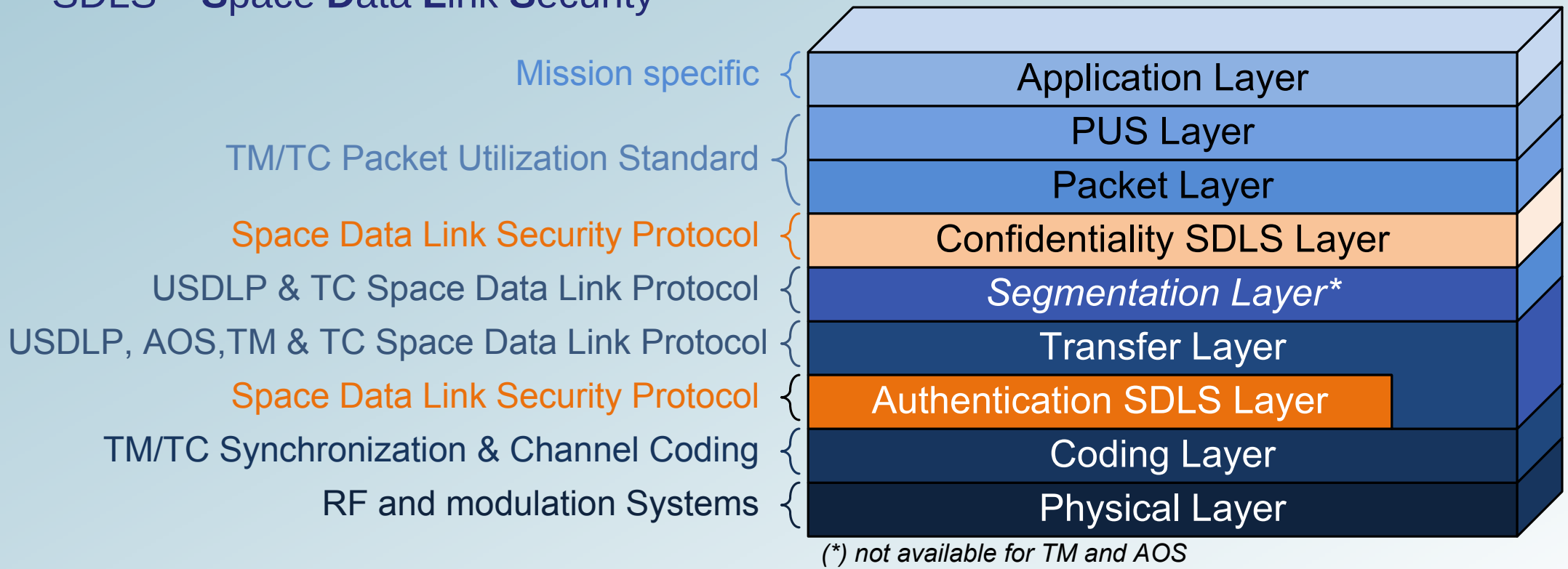
LES LIENS SPATIAUX

- La couche physique porte la modulation des signaux pour la transmission via le lien air, des bits de synchronisation peuvent être nécessaire pour les phases d'accrochage des démodulateurs,
- La couche codage permet de corriger les erreurs de transmission sur le lien en espace libre soumis à toute sorte de turbulences (codes BCH, Viterbi et Reed Solomon),
- La couche transfert permet plusieurs choses :
  - D'identifier le satellite destinataire de la trame,
  - De comptabiliser les trames pour une retransmission éventuelle des trames perdues,
  - De s'assurer que les trames sont intègres du point de vue de la transmission.
- La couche paquet permet d'identifier les processus bord cibles qui utiliserons les données applicatives portées par les paquets.

La couche transfert permet d'identifier le destinataire via l'identifiant du satellite un peu comme l'adresse MAC Ethernet permet d'identifier la machine cible sur un LAN.

LES LIENS SPATIAUX

- CCSDS a récemment édité un standard pour la sécurisation des liens bord-sol: le SDLS – **S**pace **D**ata **L**ink **S**ecurity



(*) not available for TM and AOS

Avant l'arrivée de SDLS, chacun des opérateurs spatiaux définissaient sa propre couche sécurité selon ses besoins et ses contraintes (un beau bazar!).

LES LIENS SPATIAUX

- SDLS se décompose en 2 services complémentaires :
  - Le service de confidentialité des données,
  - Le service d'authenticité de la source et d'intégrité des trames (+ la protection contre le rejeu).
- Les deux services ne sont pas appliqués au même niveau dans la pile des protocoles CCSDS/ECSS :
  - La confidentialité ne couvre que les données liée à la mission (paquets CCSDS)
  - L'authenticité, l'intégrité et l'anti-rejeu couvre les trames jusqu'au niveau transfert,
- Cela signifie que certaine partie des trames sont transmises en clair mais sont quand même protégées en intégrité,
- Cela permet de pouvoir faire du routage de niveau transfert à bord, un peu comme un commutateur Ethernet le fait avec les adresses MAC, mais sans avoir à déchiffrer les trames.

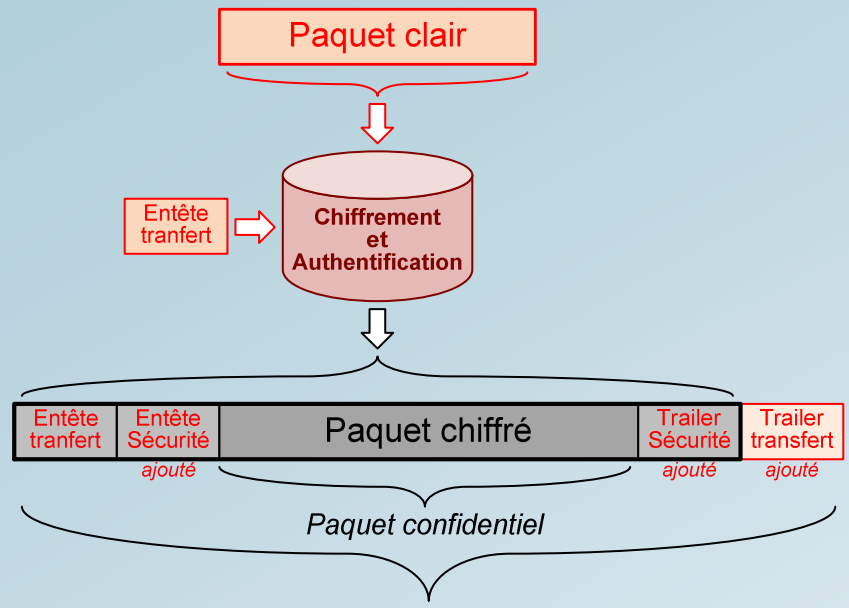
SDLS supporte donc les fonctionnalités d'un service COMSEC complet. Par contre SDLS n'adresse pas les services de sécurité de type TRANSEC pour la protection contre le déni de service.

LES LIENS SPATIAUX

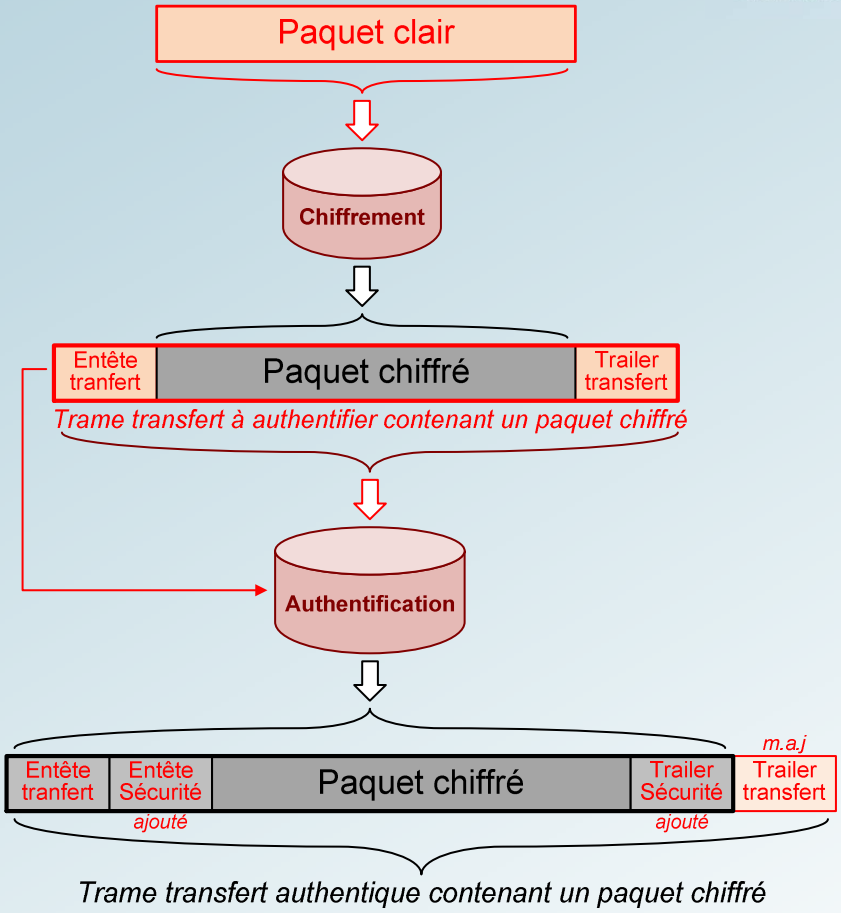
- SDLS, à la manière d'IPSec ou de TLS, introduit la notion d'association de sécurité qui doit permettre à une segment sol et à un segment bord de se mettre d'accord sur les paramètres et sur les algorithmes à utiliser avant de commencer à communiquer ensemble,
- SDLS standardise l'ensemble des commandes permettant de configurer les différents services cryptographiques à bord des satellites,
- SDLS standardise l'ensemble des statuts permettant de "monitorer" les différents services cryptographiques à bord des satellites,
- La prise en compte d'un tel standard reste néanmoins assez lourde compte tenu de sa complexité. Certains aménagement peuvent être nécessaire pour n'embarquer que les services requis pour remplir la mission.

En général, les systèmes spatiaux n'embarquent qu'une seule primitive avec un seul mode d'opération cryptographique. La notion d'association de sécurité de SDLS perd un peu de son intérêt dans le cas des communications spatiales.

LES LIENS SPATIAUX



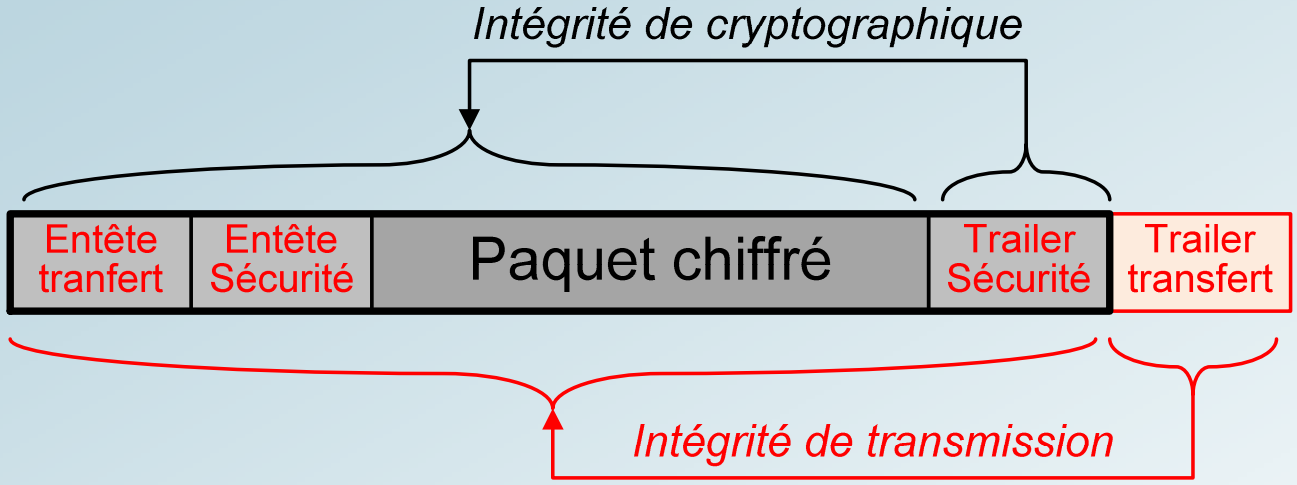
≡



Les opérations de chiffrement et d'authentification sont effectuées simultanément autour de la même fonction cryptographique.

LES LIENS SPATIAUX

- Avant d'authentifier une trame, il est nécessaire de vérifier l'intégrité de transmission pour s'assurer qu'elle n'a pas été corrompue lors de son acheminement sur le canal de transmission (qui n'est jamais parfait),
- C'est seulement après avoir vérifié l'intégrité de transmission (via le CRC de la trame contenu dans le "trailer" de transmission) que la trame peut être vérifiée en intégrité et authenticité (via le MAC contenu dans le "trailer" de sécurité).



Il est important de respecter cet ordre pour ne pas confondre une tentative d'intrusion sur le canal (MAC=KO) d'une simple erreur de transmission (CRC=KO).

LES LIENS SPATIAUX

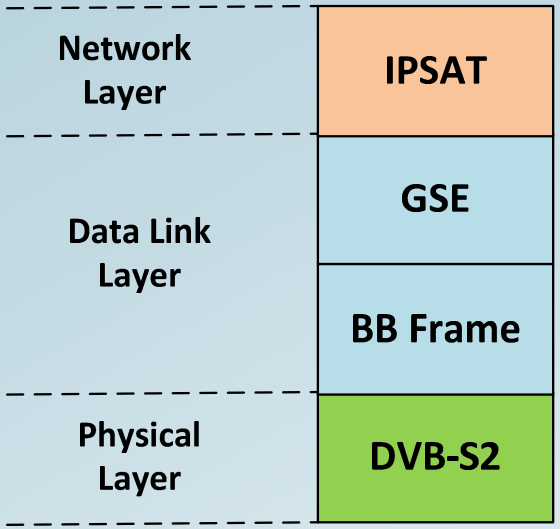
- Voici, et pour information, les standards CCSDS/ECSS les plus utilisés actuellement :
  - CCSDS 232.0-B-1 : TC Space Data Link Protocol (TC SDLP),
  - CCSDS 132.0-B-1 : TM Space Data Link Protocol (TM SDLP),
  - CCSDS 732.0-B-2 : Advanced Orbiting Systems (AOS) Data Link Protocol,
  - CCSDS 355.0-B-1 : Space Data Link Security Protocol (SDLS) Recommended Standard,
  - CCSDS 355.1-B-1 : Space Data Link Security Protocol (SDLS) Extended procedures,
  - CCSDS 732.1-B-2 : Unified Space Data Link Protocol CCSDS (USLP),
  - ECSS-E-ST-50-04C : Telecommand protocols synchronization & channel coding, dérivé du CCSDS 232.0-B-1,
  - ECSS-E-ST-50-03C : Space data links – Telemetry transfer frame protocol, dérivé du CCSDS 132.0-B-1,
  - ECSS-E-ST-50-01 : Space Engineering – Telemetry synchronization & channel coding,
  - ECSS-E-ST-50-05C Rev. 2 : Radio frequency and modulation,
  - ECSS-E-70-41A - Telemetry and telecommand packet utilisation standard (PUS).

La prise en compte de ces standards est obligatoire pour la mise en place de la plus part des liens spatiaux surtout pour les liens de TM et TC.

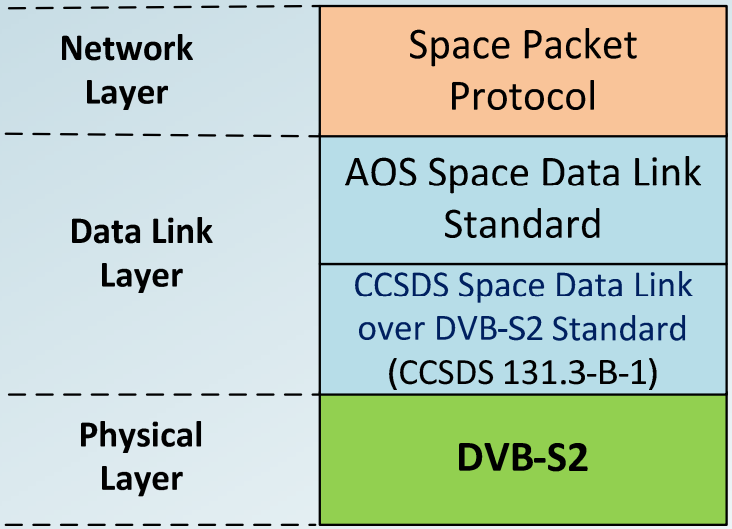
AUTRES STANDARDS

- D’autres standard peuvent être utilisés pour les données charge utile (communication en général),
  - Standard Européens ETSI pour les télécommunication,
  - Standards issus de l’internet (RFC et IETF).

IP / ETSI Hybrid Configuration



CCSCS / ETSI Hybrid Configuration



Les protocoles TCP-IP peuvent, dans certains cas, être portés par une couche liaison dédiée plus adaptée : GSE et BB frames.

C’EST L’HEURE DE LA PAUSE !

Rendez-vous dans 15 minutes…

LES MENACES VS L'ANALYSE DE RISQUE

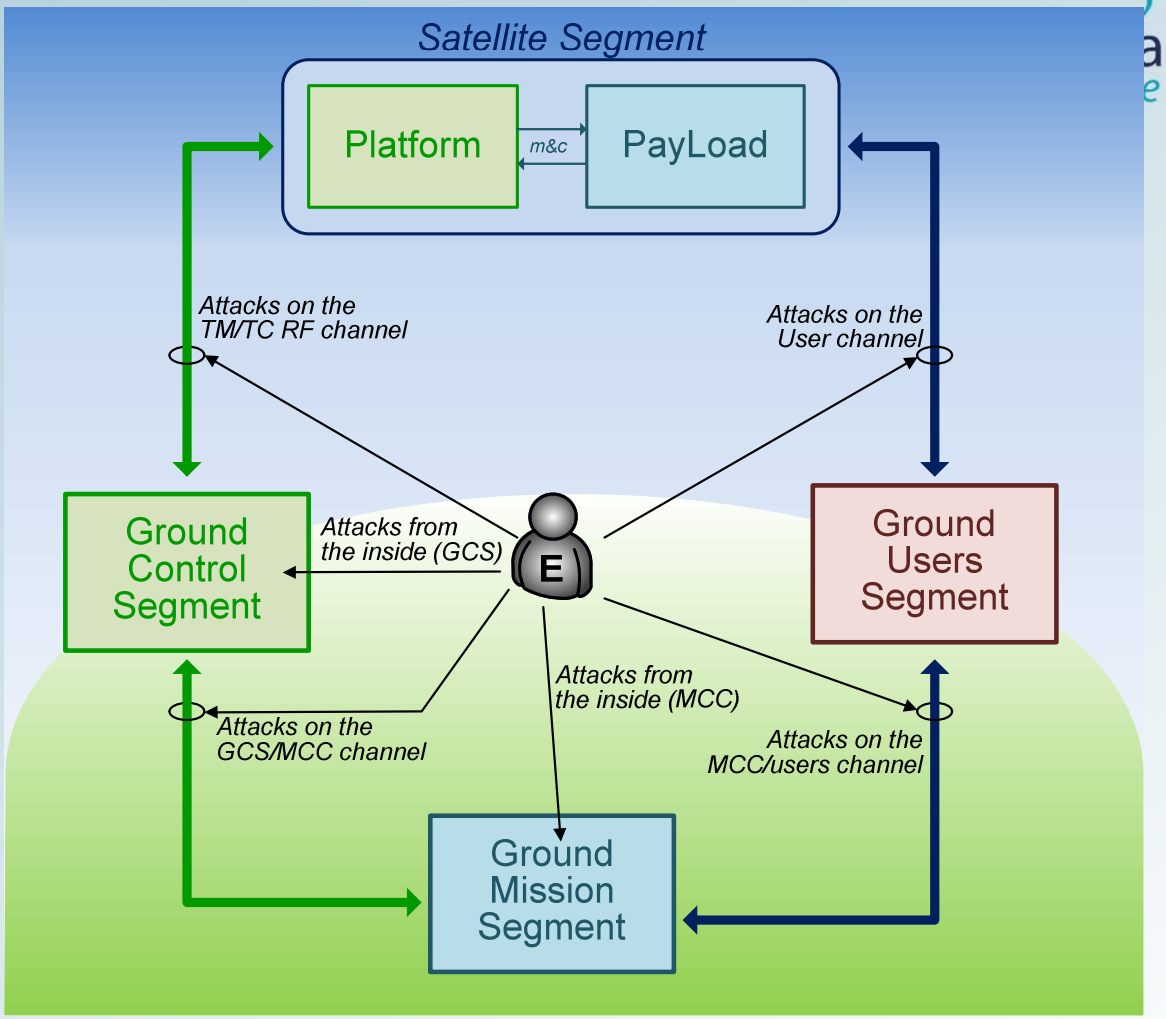
LES MENACES SUR LE SYSTÈME

- D'une manière générale nous devons nous poser la question de ce que peuvent être les motivations d'un assaillant lorsque celui-ci lance son attaque sur un système spatial,
- Il n'y en a finalement pas tant que ça, voici une liste non-exhaustive :
  - L'attaquant cherche à récupérer de l'information sensible (écoute passive, intrusion avec fuite de donnée confidentielle etc.),
  - L'attaquant cherche à prendre le contrôle du système pour nuire physiquement à son intégrité (ex : désorbitation d'un satellite),
  - L'attaquant cherche à s'introduire pour nuire à l'image de marque de celui qui opère le système ou de celui qu'il l'a conçu et développé (ex : réalisation d'un exploit),
  - L'attaquant cherche à prendre le contrôle pour rendre le système indisponible,
  - L'attaquant cherche à prendre le contrôle pour détourner le système à son profit,
  - L'attaquant cherche à tirer un profit pécuniaire en menant une action de rançongiciel,

Nous adressons ici les menaces de niveau logique et non physiques, ce qu' l'on appelle la guerre électronique ou cyber guerre.

LES MENACES

- Les attaques redoutés ici pèsent essentiellement sur le lien des TM/TC entre le sol et le satellite,
- Mais biens d'autres attaques sont possibles sur les autres liens ou partie du système,
- Le satellite lui-même n'est pas directement concerné par des attaques logiques, celles-ci doivent être menée depuis le sol : depuis l'intérieur du centre de contrôle par exemple.



Il ne suffit pas de protéger les liens bord-sol pour protéger un satellite. Les protections contre les cyber-attaques des systèmes au sol sont toutes aussi importantes sinon plus.

LES MENACES SUR LES LIENS SPATIAUX

- Accès non autorisé à la fonction de télécommande (TC) du satellite
  - Intrusion active sur la liaison montante TC (PF ou PL),
  - L'intrus cherche à se faire passer pour le SCC ou le MCC et vise à transmettre des télécommandes à la PF ou la PL,
- Ecoute (Flux TC montant et flux TM descendant)
  - L'intrus écoute la ou les liaisons satellite : l'écoute passive est non contrôlable sur les liaisons RF bord / sol. Tout intrus équipé des moyens adéquats peut écouter sans se faire détecter,
  - L'intrus prend connaissance des données / informations sensibles véhiculées sur ces liaisons
  - Idem avec les flux audio-vidéo véhiculés sur les liaisons AOS.
- Rejeu (Flux TC essentiellement)
  - L'intrus écoute la liaison TC et enregistre les commandes émises par le SCC authentique et qui sont donc valides,
  - L'intrus réémet ensuite ultérieurement les messages de TC enregistrés au satellite pour qu'ils soient de nouveau acceptés par le satellite ➔ perturbe les opérations.

Sur un satellite, le lien montant des télécommandes est certainement le lien le plus critique du point de vue de la sécurité!

LES MENACES SUR LES LIENS SPATIAUX

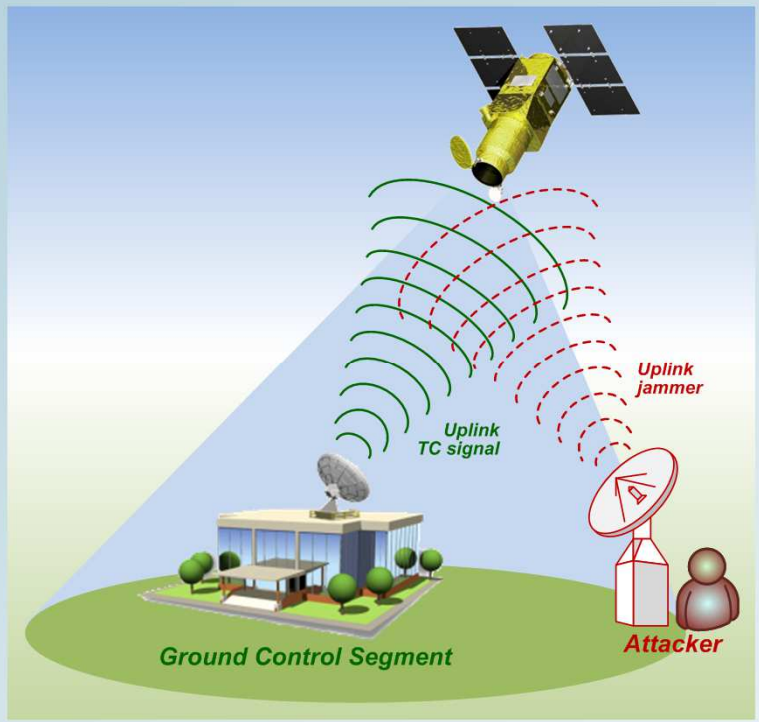
- Modification intentionnelle des données (Flux TC et flux TM)
  - Intrusion active sur la liaison montante ou descendante,
  - Liaison montante Flux TC : L'intrus intercepte le message TC avant émission vers le satellite et modifie son contenu,
  - Liaison descendante TM : L'intrus intercepte le message TM avant acquisition par le SCC/MCC ou le Centre de traitement, et modifie son contenu pour duper l'opérateur.
- Analyse de Trafic
  - L'intrus écoute et enregistre la ou les liaisons satellite (écoute passive),
  - En analysant le contenu des messages enregistrés (header, identifiants, adresses), il peut déterminer qui est l'émetteur (ex: quel satellite ou quel SCC) et le destinataire (ex: équipement / application dans le satellite).
- Brouillage RF (Flux TC)
  - L'intrus utilise un brouilleur RF suffisamment puissant pour rendre la liaison TC inopérante (le SCC n'arrive alors plus à transmettre de TC acceptée par le satellite)
  - Menace de type DoS (Denial of Service) contre la disponibilité de la liaison TC.

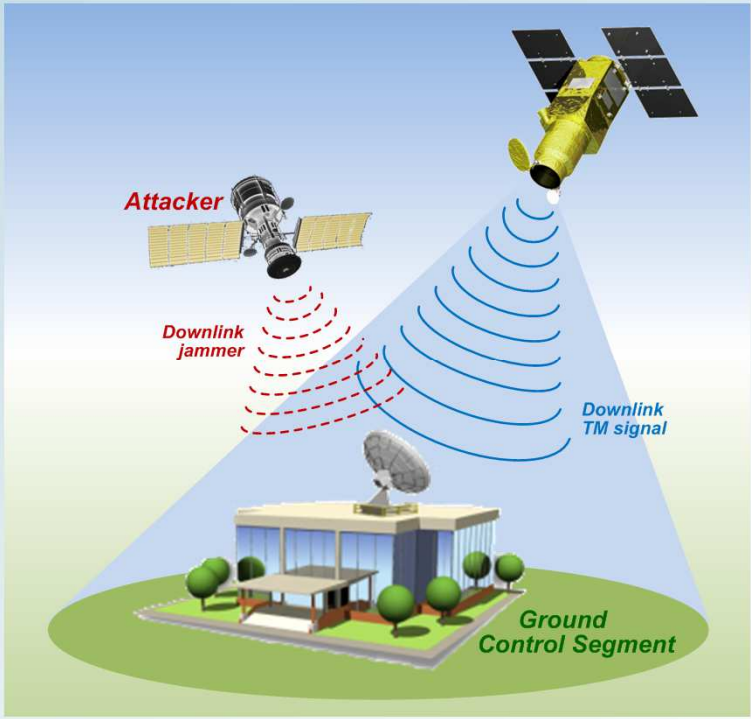
Depuis la mésaventure d'espionnage de Loutch Olymp sur Athena Fidus en 2017, la menace des brouilleurs descendants en TM est de plus en plus considérée sur les GéoSatcom.

LES MENACES SUR LES LIENS SPATIAUX

- La menace en brouillage à pour objectif de rendre indisponible le lien des TC ou le lien des TM selon la position du brouilleur,

- Les attaques sur les liens montants (ex: TC) sont les plus évidentes à mettre en œuvre surtout sur les satellites en position Géostationnaire,
- Les attaques sur les liens descendants (ex : TM), même si elles sont moins probable, doivent être considérée.



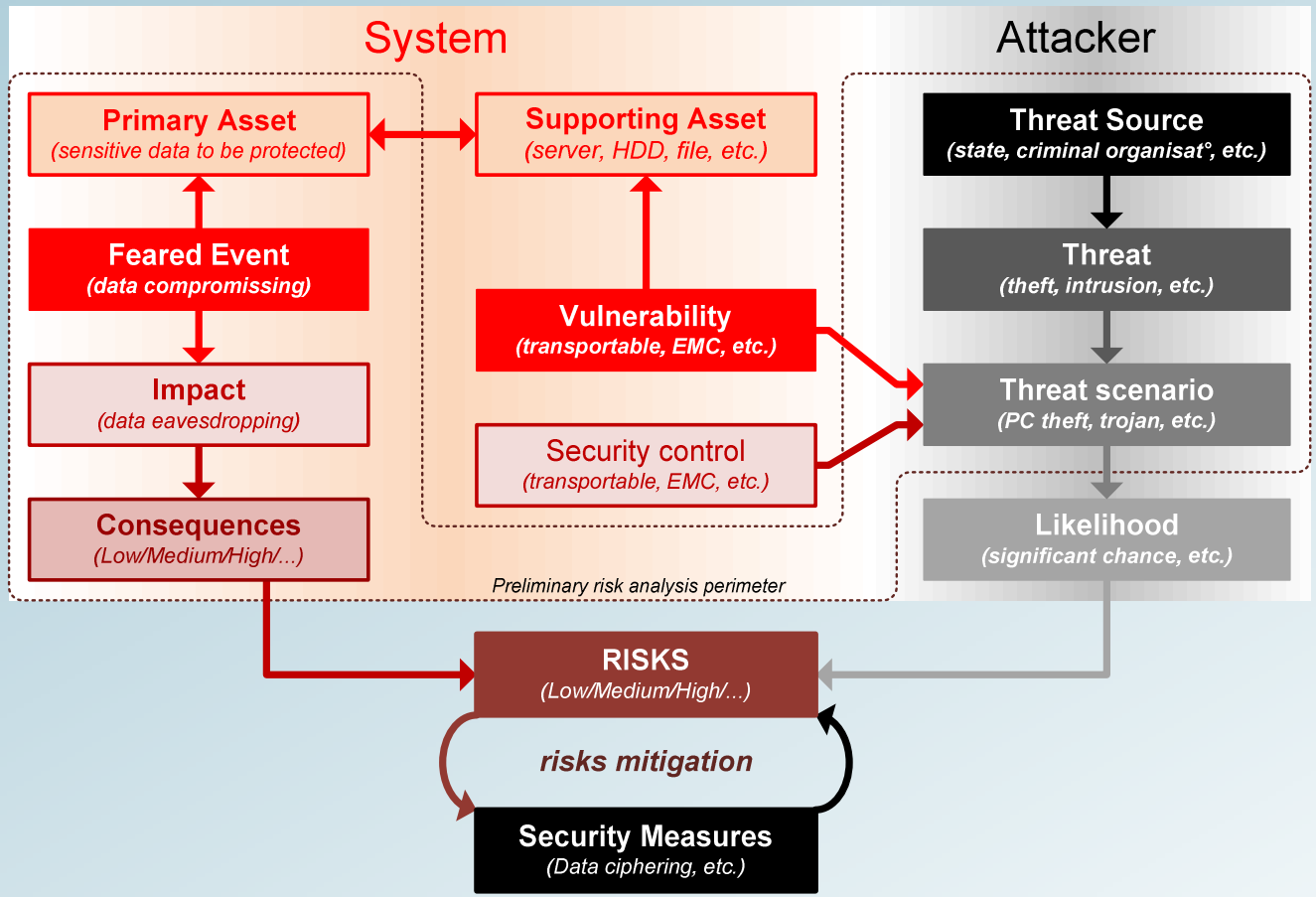


Si l'attaquant brouille assez longtemps le lien TC et/ou TM, cela peut conduire à la perte définitive du satellite.

L'ANALYSE DE RISQUE DE SÉCURITÉ

- Afin de prendre en compte au mieux la sécurité d'un système spatial, il est nécessaire de mener ce que nous appelons une analyse de risque de sécurité,
- Elle permet d'identifier :
  - Les biens essentiels à protéger avec les événement redoutés concernant ces biens,
  - Les menaces qui pèsent sur ces biens essentiels.
- C'est une analyse itérative qui s'affine tout au long de la phase de conception et de développement et qui permet aussi d'identifier :
  - Les biens supports avec leur vulnérabilités : matériel physiques qui stocke des biens essentiels (une serveur réseau par exemple),
  - Les impacts et conséquence liés à la survenue d'un des événements redoutés,
  - Les scénarios d'attaque avec leur probabilité d'occurrence,
- Pour arriver à estimer un risque qui au final est jugé acceptable ou non,
- Afin de minimiser les différents risques, des mesures de sécurité sont mises en place afin qu'ils deviennent acceptables.

L'ANALYSE DE RISQUE DE SÉCURITÉ



En pointillé, est délimité le périmètre couvert par l'analyse de risque de sécurité préliminaire qui est la première étape avant même la phase de conception détaillée du système.

LES OBJECTIFS DE SECURITE

- Pour les système spatiaux le bien essentiel à protéger représente généralement les données qui transitent via les lien bord sol,
- Chacun des risques identifie si les données sont menacées en confidentialité, en intégrité et en disponibilité,
- En conséquence, les données échangées via un lien bord-sol (montant ou descendant) doivent prendre en compte les objectifs suivants:
  - En **confidentialité** : toute partie externe ne peut interpréter le contenue des données
  - En **intégrité** : Les données reçues n'ont pas été modifiée en chemin
  - En **authenticité** de la source : Les données sont bien produites par une source autorisée et de confiance,
  - En **non-rejeu** : les données reçues sont nouvelles et ne sont pas une réémission de données déjà traitées antérieurement,
  - En **disponibilité** : Le canal qui véhicule les données est toujours disponible.

Ces objectifs sont applicables à tous les liens bord-sol. Mais attention, ce ne sont que des objectifs, cela ne veut pas dire qu'ils sont appliqués tout le temps et partout, cela dépend fortement des sorties de l'analyse de risque de sécurité du système.

LES OBJECTIFS DE SECURITE

- La protection des liaisons spatiales (TC, TM, AOS) couvre deux familles de services de sécurité,
- Service de Sécurité de type COMSEC (**COM**munication **SEC**urity) :
  - Implémenté au niveau de la couche Liaison de Données (Data Link) du modèle CCSDS,
  - Opère sur les messages numériques transportés sur les liaisons TC/TM/AOS,
  - Couvre les services d'Authentification et de Chiffrement,
  - L'authentification répond aux objectifs suivant : Authenticité, Intégrité et Anti-rejeu,
  - Le chiffrement répond à l'objectif de Confidentialité.
- Service de Sécurité de type TRANSEC (**TRAN**smission **SEC**urity) :
  - Implémenté au niveau de la couche Physique/Radio (Physical Layer) du modèle CCSDS,
  - Répond à l'objectif de Disponibilité,
  - Protection contre le brouillage RF / menaces de type DoS (Denial of Service),
  - A pour objet de garantir la disponibilité de la liaison sous certaines conditions dégradées.

SSL/TLS, IPSEC et MACSec sont des protocoles de sécurité qui portent le service COMSEC pour les réseaux sol. Pour le spatial c'est le CCSDS-SDLS.
Il n'existe pas de standard pour le service TRANSEC.

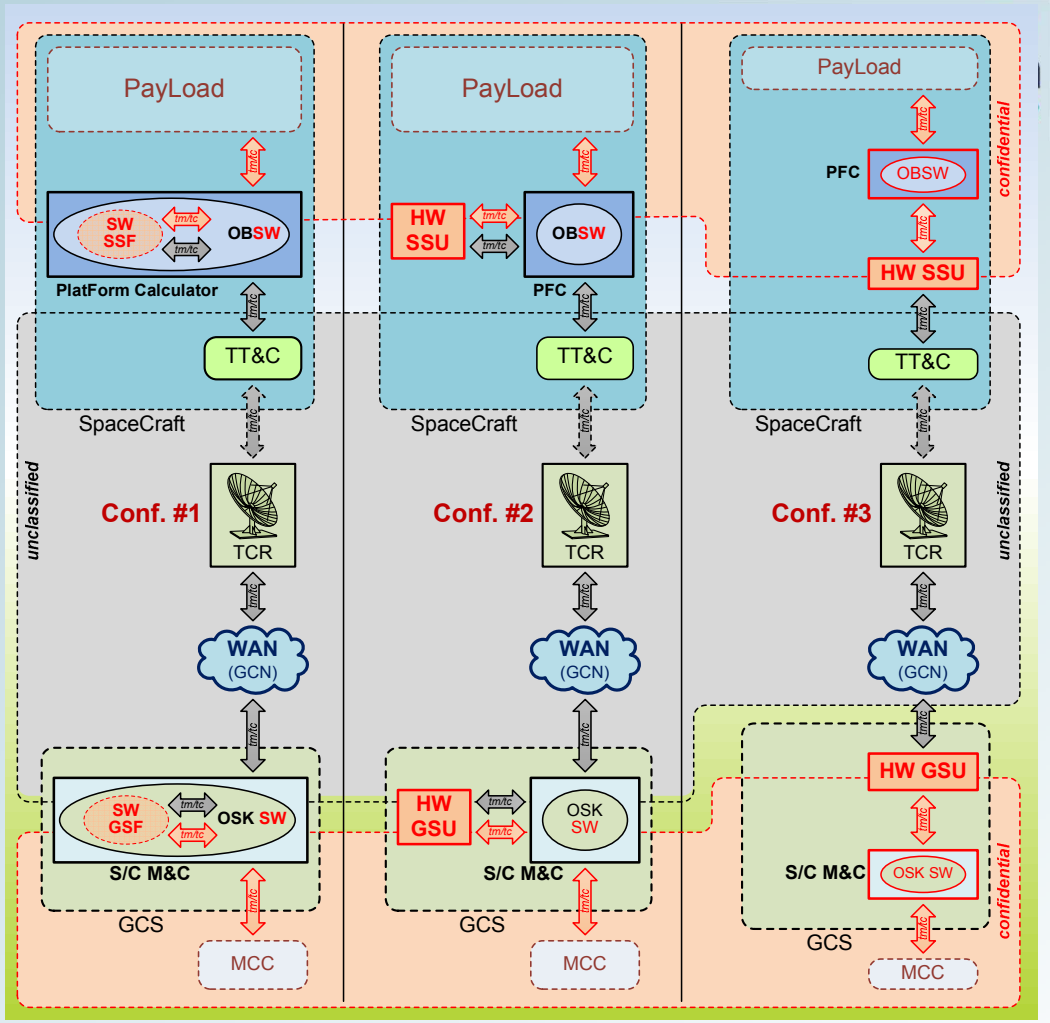
LES OBJECTIFS DE SECURITE

Type de lien/donnée	Orbite et type de mission	Confidentialité des messages	Authenticité de la source	Intégrité des messages	Anti-rejeu des message	Disponibilité du canal
TC Satellite	Militaire GEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Obligatoire
	Civil GEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Optionel
	Militaire LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Optionel
	Civil LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Pas necessaire
TM Satellite	Militaire GEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Optionnel
	Civil GEO	Obligatoire	Obligatoire	Obligatoire	Optionnel	Pas necessaire
	Militaire LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Pas necessaire
	Civil LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Optionnel	Pas necessaire
TC Payload Haut débit	Militaire GEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Obligatoire
	Civil GEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Optionnel
TM Payload Haut débit	Militaire GEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Optionnel
	Civil GEO	Obligatoire	Obligatoire	Obligatoire	Optionnel	Pas necessaire
Flux IP Charge utile montant	Militaire LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Optionnel
	Civil LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Pas necessaire
Flux IP Charge utile descendant	Militaire LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Optionnel
	Civil LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Optionel	Pas necessaire
Flux AOS Images et science	Militaire LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Obligatoire	Pas necessaire
	Civil LEO/MEO	Obligatoire	Obligatoire	Obligatoire	Optionnel	Pas necessaire
Flux AOS (audio/video)	ISS LEO	Obligatoire	Pas necessaire	Pas necessaire	Pas necessaire	Pas necessaire

De tous les objectifs de sécurité, c'est celui de la disponibilité qui est le moins requis, soit car il n'est pas pertinent (orbite LEO/MEO); mais aussi parce que la mise en place d'un service TRANSEC est très compliqué et très coûteux (et donc très risqué).

LES SERVICES COMSEC TM/TC

- Un service COMSEC peut être positionné de différentes façons dans un système :
  - Conf #1: Intégré dans les équipements émetteurs/destinataires des flux à protéger (option la moins coûteuse),
  - Conf #2 : En ressource des équipements émetteurs/destinataires des flux à protéger.
  - Conf #3 : En coupure physique des flux qu'il protège (option la plus sécurisé).
- L'option d'une fonction HW en coupure est privilégiée pour les missions étatiques,
- L'option intégrée est privilégiée pour les missions civiles/commerciales,
- L'option en ressource n'est pas très pertinente et est à éviter.



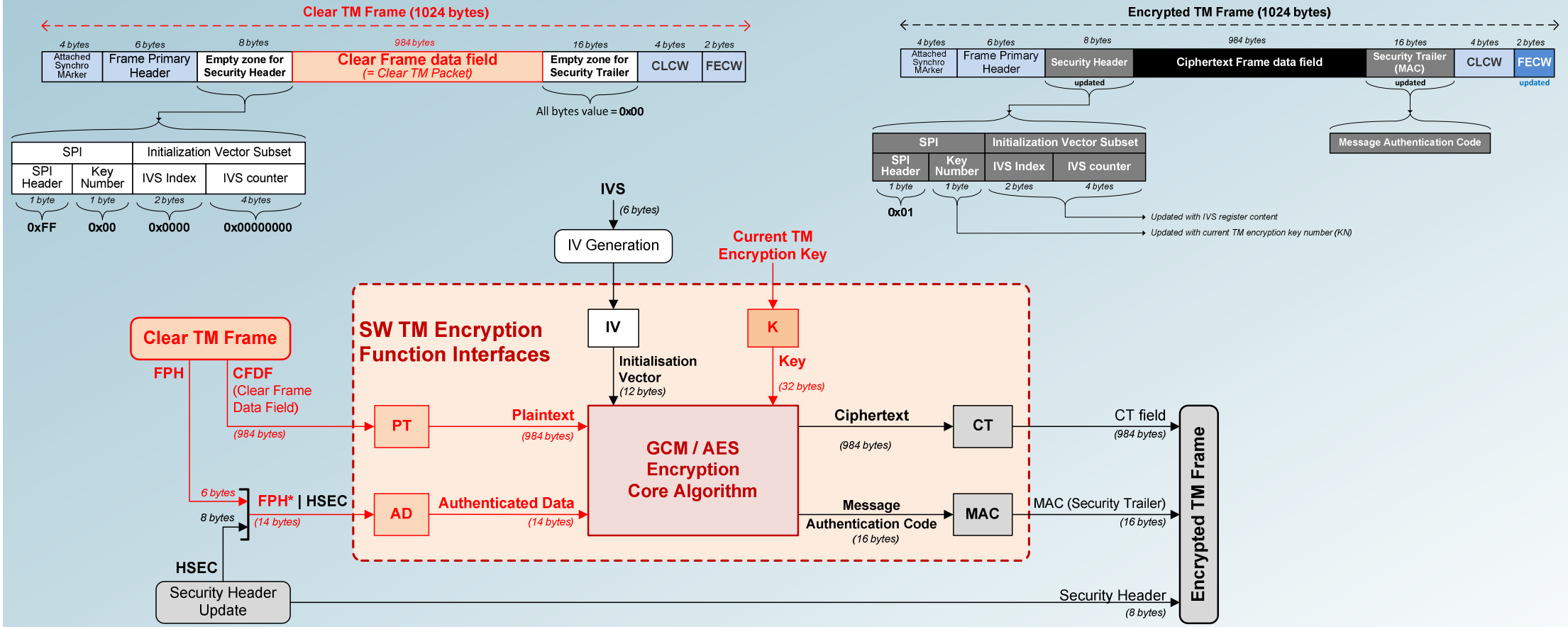
*Les équipements de sécurité implémentés dans des modules matériels dédiés sont souvent appelés HSM : **H**ardware **S**ecurity **M**odule.*

LES SERVICES COMSEC TM/TC

- Pour les services COMSEC TM et TC implémentés pour des missions civiles et commerciale, nous utilisons systématiquement l'algorithme AES séquencé en mode compteur selon le standard du NIST AES-GCM (**NIST SP800-38D**). Ce mode est aussi celui proposé sur TLS pour la sécurisation *https://*,
- AES n'est pas vraiment adapté pour du chiffrement de trames en continu, c'est pourquoi il est séquencé en mode compteur avec quelques contraintes liées au mode GCM,
- Voici une recommandation du NIST liée à la partie de calcul du MAC de GCM : "*The probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data shall be no greater than* 2^{-32}*.*"
- En termes simples, cela signifie qu'il ne faut jamais utiliser deux fois le même couple IV/Clé pour chiffrer des trames, sans quoi, il pourrait être possible à l'attaquant de remonter à la clé!

Avant d'implémenter une fonction cryptographique, il faut attentivement lire les standards applicables afin de ne pas introduire de vulnérabilité.

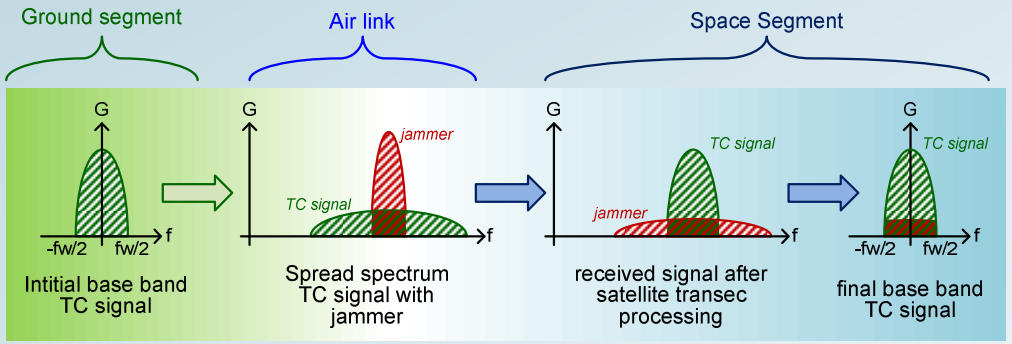
LES SERVICES COMSEC TM/TC



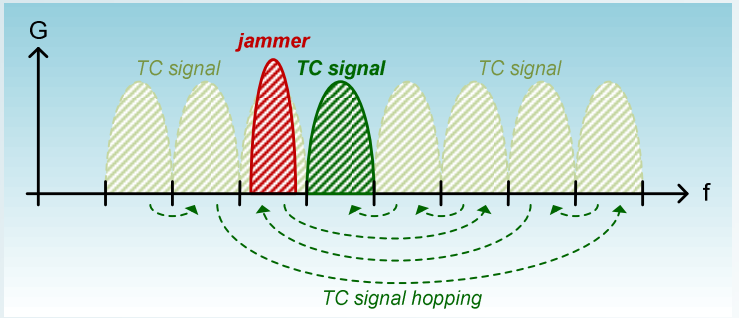
Il ne suffit pas d'implémenter AES-GCM pour garantir la sécurité, il faut correctement l'initialiser et bien choisir le périmètre des données qui seront protégées en confidentialité et le périmètre de celles qui seront protégées en authenticité.

LES SERVICES TRANSEC

- Il existe deux techniques de protection contre les brouilleurs RF (montants ou descendants) :
  - La technique DSSS (**D**irect **S**equence **S**pread **S**pectrum) : il s'agit ici de convoluer en fréquence une séquence pseudo-aléatoire avec le signal à moduler. Au final, cela revient à étaler le signal sur un plus large spectre au niveau du canal de transmission,



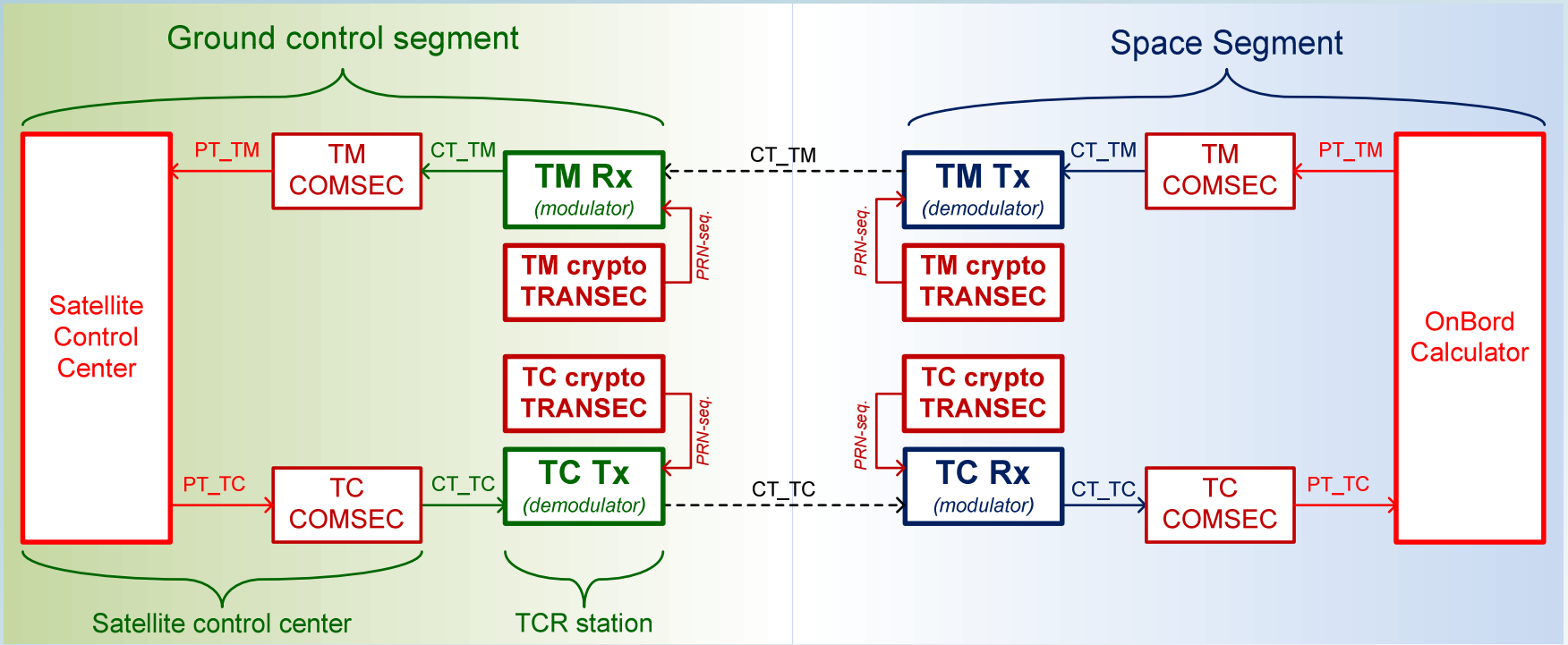
  - La technique FHSS (**F**requency **H**opping **S**pread **S**pectrum) : il s'agit de faire faire des sauts de fréquence au signal modulé sur un spectre assez large. Sachant que les données sont répétées entre plusieurs canaux.



Il est aussi possible de mixer les deux techniques pour rendre le lien encore moins sensible à tous les types de brouilleurs. La séquence pseudo-aléatoire de saut ou la d'étalement est délivrée par une algorithme cryptographique à clé secrète symétrique.

LES SERVICES TRANSEC

- La sécurisation en TRANSEC nécessite d'ajouter les générateurs pseudo-aléatoires (les équipements crypto TRANSEC) en support des modulateurs/démodulateurs qui portent la fonction de modulation DSSS ou FHSS.



La mise en place d'un service TRANSEC ajoute de la complexité et donc du coup sur le système.

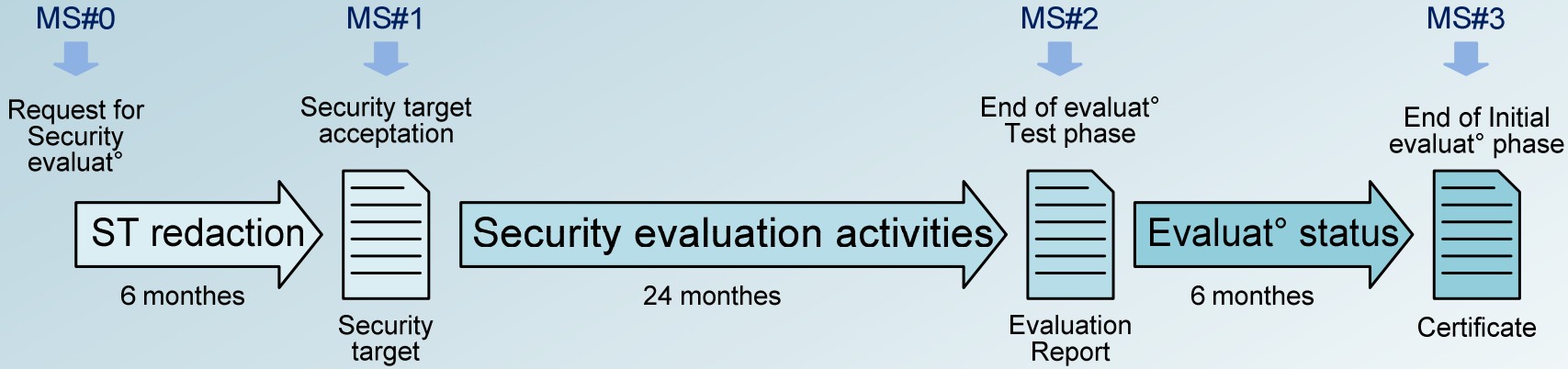
CERTIFICATION DE SECURITE

- Comme nous l'avons vu précédemment, c'est pas parce qu'un ingénieur implémente une fonction cryptographique que celle-ci est exempte de vulnérabilité (Cf. mode AES-GCM). La seule bonne fois de l'ingénieur ou de l'industriel n'est pas suffisante comme preuve de sécurité,
- C'est pourquoi, il existe des processus dits de certification des équipements de sécurité,
- Ces processus sont conduits sous la férule des agences nationales de sécurité (NSA, ANSSI, BSI, NCSC, etc.) et sont exécutés par des **C**entres de **S**écurité des **T**echnologies de l'**I**nformation agréés (CESTI ou ITSEF de l'anglais pour **I**nformation **T**echnology **S**ecurity **E**valuation **F**acility),
- Les deux processus les plus connus sont :
  - La certification FIPS,
  - La certification Critères Communs.
- Ces processus donnent des garanties objectives de sécurité des fonctions certifiées.

En France, il existe quelques laboratoires certifié FIPS et/ou CC comme : SERMA, OPPIDA, le CESTI LETI et le CESTI Thales.

CERTIFICATION DE SECURITE

- Globalement un processus de certification, quel qu'il soit, se déroule comme suit :
  - Le soumissionnaire rédige une Cible de Sécurité (ou ST : **S**ecurity **T**arget) qui identifie les objectif de sécurité, les hypothèses d'environnement et les fonctions de sécurité à évaluer,
  - La ST sert de base de référence au CESTI pour mener son activité d'évaluation sécurité, à la fin de laquelle, il délivre un rapport d'évaluation,
  - Le rapport est analysé par l'agence nationale de sécurité qui décide alors d'octroyer ou non la certification du produit évalué.



Il est rare qu'une certification soit refusée, l'agence préfère délivrer les certificats avec des limitations et des recommandations d'usage pour limiter la portée des vulnérabilités résiduelles lorsqu'il y en a.

CERTIFICATION DE SECURITE

- Processus de certification **FIPS 140-3** :
  - Ce processus remplace le **FIPS 140-2** qui est encore applicable jusqu'en septembre 2021,
  - Il permet de s'aligner sur les autres standards internationaux dont les critères communs,
  - Ce standard identifie les exigences de sécurité applicables à la fonction cryptographique certifiée,
  - Il intègre 4 niveaux d'évaluation/certification : Level 1 (le plus bas) à Level 4 (le plus haut),
  - Depuis la version 140-3, les exigences couvrent aussi d'autres domaines connexes (la documentation, les polices de sécurités, etc.)
  - La listes des annexes applicables est la suivante :
    - SP 800-140, FIPS 140-3 Derived Test Requirements (DTR),
    - SP 800-140A, CMVP Documentation Requirements,
    - SP 800-140B, CMVP Security Policy Requirements,
    - SP 800-140C, CMVP Approved Security Functions,
    - SP 800-140D, CMVP Approved Sensitive Parameter Generation and Establishment Methods,
    - SP 800-140E, CMVP Approved Authentication Mechanisms,
    - SP 800-140F, CMVP Approved Non-Invasive Attack Mitigation Test Metrics.

La certification FIPS est surtout demandée pour les produits destinés au marché nord-américain (USA et Canada).

CERTIFICATION DE SECURITE

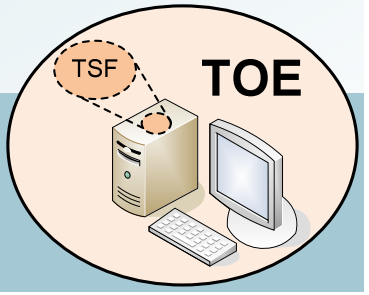
- Processus de certification **C**ritères **C**ommuns ou CC :
  - Ce processus est un processus partagé par bon nombre d'agences de sécurité,
  - Il se divise en 2 sous-ensembles :
    - Les guides pour la définition des exigences de sécurité : Ces guides contiennent toute une liste d'exigences regroupées en classe de composants fonctionnels qui seront choisis pour faire partie des fonctions de sécurité du produit à évaluer (TSF : **T**arget **S**ecurity **F**unctions),
    - Les guides pour la définition des exigences liées aux activités l'évaluation de sécurité du produit : ce guides identifies l''ensemble des tâches que doit effectuer l'évaluateur ainsi que le support que devra fournir l'équipementier. Il existe 7 niveaux d'évaluation de sécurité dont découle le niveau de certification : du niveau EAL 1 (le plus bas) au niveau EAL 7 (le plus élevé). Un HSM classique s'évalue en EAL3 ou EAL 4 (rarement plus).
  - Les agences nationales de sécurité peuvent décider d'augmenter les niveaux de sécurité pour créer les leurs. En France l'ANSSI a créée les niveaux EAL3+ et EAL4+, ils représentent respectivement des niveaux intermédiaires entre EAL3/EAL4 ou EAL4/EAL5,
  - Les CC sont surtout utilisés en Europe.

*EAL signifie : **E**valuation **A**ssurance **L**evel.*

CERTIFICATION DE SECURITE

- Pour certains systèmes, il peut être exigé que les équipements/fonctions de sécurité soit certifiés,
- C'est toujours l'industriel qui finance le CESTI pour qu'il mène l'activité d'évaluation,
- Une certification Critère Commun EAL3+ coûte environ 200 00 euros et 400 000 euros pour une certification EAL4+,
- L'évaluation se délimite sur le périmètre physique de l'équipement qui porte les fonctions de sécurité à évaluer : TOE ou **T**arget **O**f **E**valuation,
- C'est pourquoi, il est recommandé d'avoir des HSM (des équipements physiques de sécurité) distincts des autres équipements du système,
- Il faut proscrire les fonctions de sécurité SW intégrées dans des équipements dont la sécurité n'est pas la vocation principale (difficile à évaluer).

*TOE = **T**arget **O**f **E**valuation*
*TSF = **T**arget **S**ecurity **F**unctions*



LA CYBER DEFENSE

- La sécurisation des liaisons spatiales ne permet pas de protéger, à elle seule, le système qui est pourvu de nombreuses composantes interconnectées entre elles au sol,
- Le développement très important des attaques au sol contre les systèmes d'information utilisant des réseaux de communication (Internet, réseaux mobiles, ..), a conduit à développer le concept de Cyber-Sécurité destiné à adresser toutes les menaces et contre-mesures associées, ainsi que la détection et la supervision des systèmes à implémenter :
  - USA / NSA : Executive order 13636 (2013) : Improving Critical Infrastructure Cybersecurity - Preliminary CyberSecurity framework - Energy, Transport, Telecommunication, Finance,
  - NIST framework for improving critical infrastructure cybersecurity [2014],
  - NIST roadmap for improving critical infrastructure cybersecurity [2014],
  - EU : Network and Information Security Directive of the 7th February 2013 ,
  - Autres initiatives : NATO, ENISA, National (BSI, ANSSI, etc.).

*La mise en place de mesures de cyber défense (ou LID – **L**utte **I**nformatique **D**éfensive) pour les systèmes au sol est primordiale pour assurer la sécurité du système spatial dans son ensemble.*

INFRASTRUCTURES DE GESTION DE CLÉ

INFRASTRUCTURE DE GESTION DE CLÉ

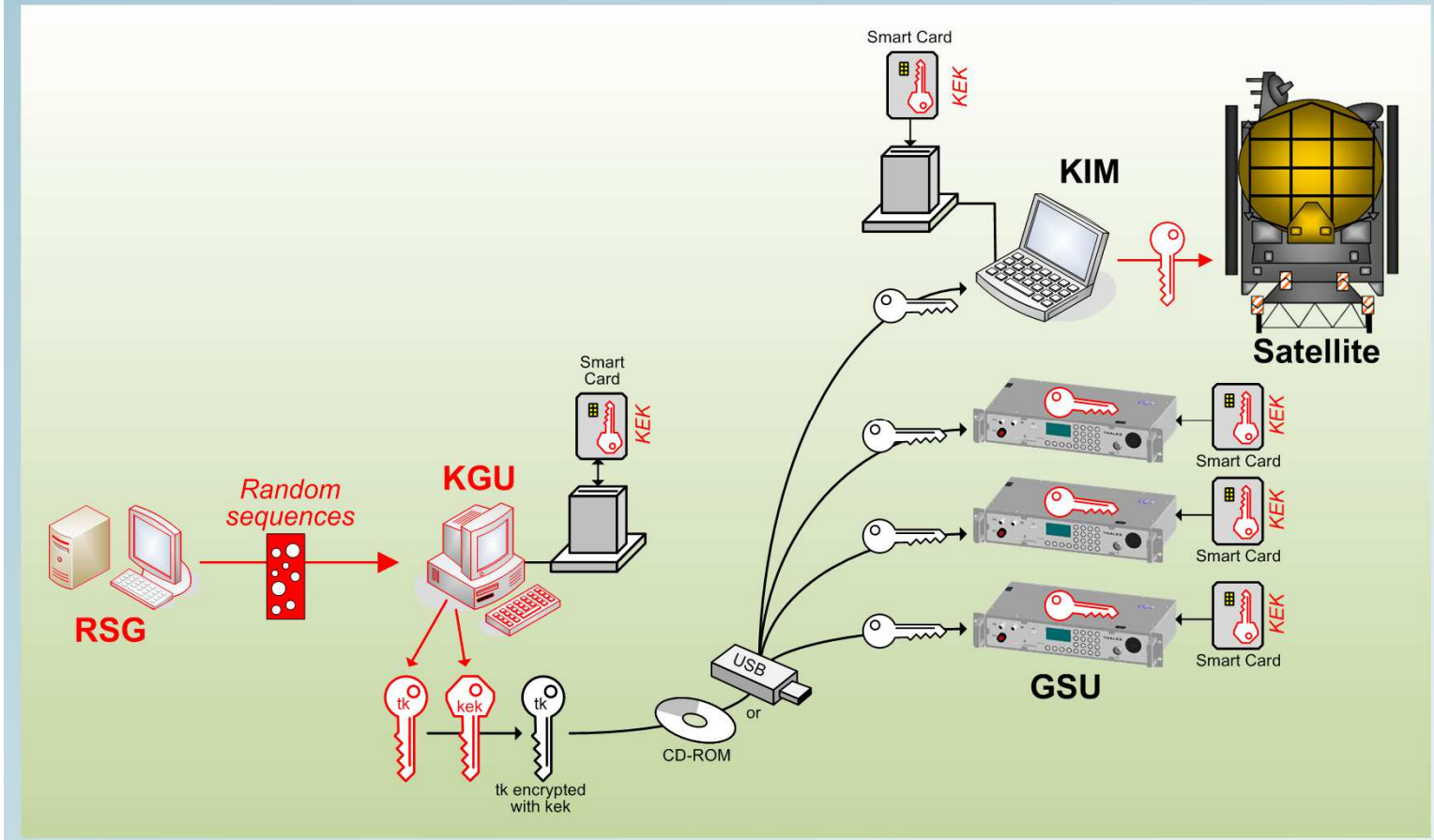
- La distribution des clés secrètes, celles utilisées pour sécuriser les canaux de communication, a toujours été un véritable casse-tête pour les architectes des systèmes spatiaux supportant de tels mécanismes,
- A ce jour, il existe 2 types d'infrastructure de gestion de clé (IGC) :
  - Les infrastructures à clé secrète (ou SKI ➔ **S**ecret **K**ey **I**nfrastructure)
  - Les infrastructures à clé publique (ou PKI ➔ **P**ublic **K**ey **I**nfrastructure)
- Au final, les deux infrastructures ont exactement les mêmes objectifs de sécurité:
  - Permettre l'authentification des utilisateurs eux-mêmes,
  - Permettre la distribution des clés entre les utilisateurs,
- Pour remplir ces objectifs, les infrastructures doivent permettre de produire et de sécuriser le transport de l'ensemble des éléments nécessaires à ces actions.

INFRASTRUCTURE DE GESTION DE CLÉ

- Les infrastructures à clés secrètes se basent exclusivement sur l'échange de clés secrètes qui peuvent, elles-mêmes, être chiffrées via d'autre clés secrètes : les clés de chiffrement de clés ➔ KEK ou **K**ey **E**ncryption **K**ey,
- Les fonctions de chiffrement de clé, lorsqu'il y en a, sont basées sur des algorithmes à clés secrètes symétrique uniquement,
- On parle ici de la technique du "**K**ey **W**rapping",
- Les SKI se basent sur une chaine de confiance qui permet de les acheminer depuis l'équipement de génération jusqu'aux équipements de sécurité finaux,
- Les SKI sont très peu rependues car elle ne sont pas adaptées à la majorité des configurations.

Attention, la technique de "Key Wrapping", décrite ici, est différente de la technique du "Key Encapsulation Mechanism" qui se base sur une cryptographie asymétrique.

INFRASTRUCTURE DE GESTION DE CLÉ



- Des séquences aléatoires sont produites par un générateur d'aléa (Random Sequences Generator),
- Ces aléas sont affectés en clés de trafic ou en Key Encryption Key ➔ elles sont numérotés,
- Les clés de trafic sont chiffrées et distribuées aux équipements cibles (Ground Security Unit et satellite).

Ce type d'infrastructure devient vite ingérable dans les cas des constellations avec plusieurs dizaines de satellites.

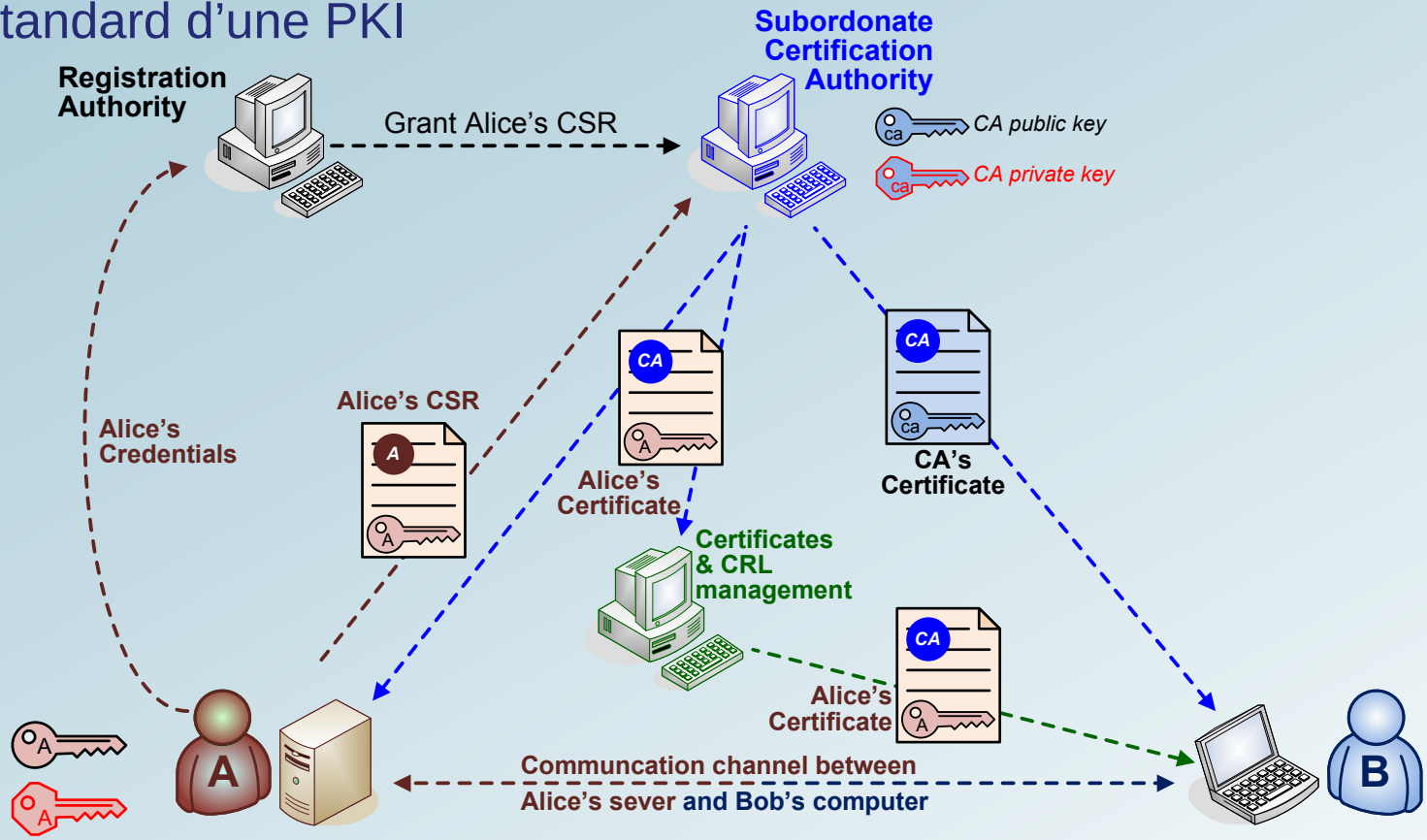
LE INFRASTRUCTURE DE GESTION DE CLÉ

- Les infrastructures à clés publique/privée (PKI) se basent sur des mécanismes d'authentification et d'établissement de clés basés sur des algorithmes de cryptographie asymétrique (RSA, Diffie-Hellman, etc.),
- Il existe plusieurs façons d'implémenter les PKI :
  - Sans PFS : authentification par certificat signé DSA et chiffrement de clé via RSA par exemple (**K**ey **E**ncapsulation **M**echanism - KEM),
  - Avec PFS : authentification par certificat signé DSA et établissement des clés via Diffie-Hellman (**K**ey **E**stablishment – KE).
- Les PKI s'articulent autour d'une entité tierce dite de confiance : l'**A**utorité de **C**ertification ou CA : **C**ertification **A**uthority, qui délivre les certificats signés.

*La "**P**erfect **F**orward **S**ecrecy" est de plus en plus la norme dans les communications actuelles surtout depuis TLS1.2 et TLS1.3.*

INFRASTRUCTURE DE GESTION DE CLÉ

- Architecture standard d'une PKI



Cette figure dévoile toute la complexité des PKI. C'est le prix à payer pour assurer la sécurité des échanges sur internet !

INFRASTRUCTURE DE GESTION DE CLÉ

- Les PKI reposent donc sur la notion de certificat de clé publique,
- Le but des certificats est de lier officiellement une clé publique à l'entité de son propriétaire (qui est le seul détenteur de la clé privé) via l'utilisation d'une cryptographie forte (RSA),
- Le certificat contient donc la clé publique mais aussi des informations qui garantissent l'authenticité du détenteur de la clé publique :
  - La version du certificat (SSL/TLS etc…),
  - Le nom de l'entité ou organisation à qui est associé le certificat,
  - Le numéro de série attribué par la CA,
  - Le nom de la CA,
  - La date de début et de fin de validité du certificat,
  - La clé publique,
  - Les algorithmes pour la signature et l'intégrité,
  - La signature de la CA.

INFRASTRUCTURE DE GESTION DE CLÉ

- Lorsqu'un certificat est échangé il est en plus signé par l'émetteur avec sa clé privée. Celle-là même qui est appariée avec la clé publique contenue dans le certificat
- Celui qui reçoit le certificat doit vérifier :
  - L'authenticité et l'intégrité du message en utilisant à priori la clé publique contenue dans le certificat
  - L'authenticité et l'intégrité du certificat en lui-même est vérifié en utilisant la clé publique de la CA déjà connu de Bob.

*Un certificat dont la date de validité n'est plus utilisable. Cela est tracé au travers de la CRL : **C**ertificate **R**evocation **L**ist.*

LE INFRASTRUCTURE DE GESTION DE CLÉ

- Les 3 entités qui constituent la PKI sont :
  - L'Autorité d'enregistrement : (**R**egistration **A**uthority - RA) Son principal rôle est de vérifier la demande d'enregistrement (**C**ertificate **S**igning **R**equest - CSR) d'un nouvel utilisateur dans l'infrastructure.
  - Une Autorité de Certification : (**C**ertification **A**uthority - CA) Son principal rôle est de générer un certificat pour l'utilisateur. Le certificat contiendra des informations personnelles sur l'utilisateur mais surtout sa clef publique et la date de validité. L'autorité de certification signera ce certificat avec sa clef privée, ainsi ce certificat sera certifié authentique par lui même.
  - Un Annuaire (**C**ertificate **M**anagement **S**ystem) : Son rôle est de stocker les certificats révoqués (**C**ertificate **R**evocation **L**ist - CRL), les certificats en cours de validité afin d'avoir un accès rapide à ces certificats. De plus, l'annuaire peut stocker les clefs privées des utilisateurs dans le cadre du recouvrement de clef. L'annuaire doit accepter le protocole X.509 pour le stockage des certificats révoqués et le protocole LDAP pour les échanges associés.

Cette architecture varie en fonction des besoins, du type de réseau (public/privé) et des objectifs de sécurité.

INFRASTRUCTURE DE GESTION DE CLÉ

- Représentation d'un Certificat PBK: PEM (ASCII file) or DER (Binary file)
- Format PEM (ci-dessous): encodage BASE 64 appliqué au codage ASN1 du Certificat

```
-----BEGIN CERTIFICATE-----
MIICiTCCAi6gAwIBAgICIAAwCgYIKoZIzj0EAwIwbzELMAkGA1UEBhMCRlIxFjAU
BgNVBAgMDUhhdXRlLUdhcm9ubmUxETAPBgNVBAcMCFRvdWxvdXNlMQ0wCwYDVQQK
DARDTkVTMRMwEQYDVQQLDApHTkQtTk9ERS0wMREwDwYDVQQDDAhLTVMtTy1DQTAe
Fw0xODA5MTcxMzI1MTdaFw0xOTA5MTcxMzI1MTdaMFkxCzAJBgNVBAYTAkZSMRYw
FAYDVQQIDA1IYXV0ZS1HYXJvbm5lMQ0wCwYDVQQKDARDTkVTMRMwEQYDVQQLDApH
TkQtTk9ERS0wMQ4wDAYDVQQDDAVLSU0tMDBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABE6l48XhHt9KRdfBVB/iL3OD73AIGcHuFasjwIBAhHeIETpKn5qUfUkjKlqN
7s42DfsD8Dd5cKhSHlvzQZ7KQRGjgc8wgcwwCQYDVR0TBAIwADARBglghkgBhvhC
AQEEBAMCBeAwMwYJYIZIAYb4QgENBCYWJE9wZW5TU0wgR2VuZXJhdGVkIENsaWVu
dCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUy4scTBwWHY6kIKJSGNGhAsCGlE8wHwYD
VR0jBBgwFoAUIbH8c2fbbLIsdhLCckPbpUVvmAAwDgYDVR0PAQH/BAQDAgXgMCcG
A1UdJQQgMB4GCCsGAQUFBwMCBggrBgEFBQcDAQYIKwYBBQUHAwQwCgYIKoZIzj0E
AwIDSQAwRgIhAPymY067HSZ7hV1F73Llhhtqjor8moKP7iH531Af5jEDAiEAodJR
QXGFyA7/Hnr2PQwoQpNTN5UjTmfsT79J9uFmoCM=
-----END CERTIFICATE-----
```

Openssl x509 –in user.cert –text - noout

Commande Open SSL pour décoder le certificat

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8192 (0x2000)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=FR, ST=Haute-Garonne, L=Toulouse, O=CNES, OU=GND-NODE-0, CN=KMS-O-CA
        Validity
            Not Before: Sep 17 13:25:17 2018 GMT
            Not After : Sep 17 13:25:17 2019 GMT
        Subject: C=FR, ST=Haute-Garonne, O=CNES, OU=GND-NODE-0, CN=KIM-0
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:4e:a5:e3:c5:e1:1e:df:4a:45:d7:c1:54:1f:e2:
                    2f:73:83:ef:70:08:19:c1:ee:15:ab:23:c0:80:40:
                    84:77:88:11:3a:4a:9f:9a:94:7d:49:23:2a:5a:8d:
                    ee:ce:36:0d:fb:03:f0:37:79:70:a8:52:1e:5b:f3:
                    41:9e:ca:41:11
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, SSL Server, S/MIME
            Netscape Comment:
                OpenSSL Generated Client Certificate
            X509v3 Subject Key Identifier:
                CB:8B:1C:4C:1C:16:1D:8E:A4:20:A2:52:18:D1:A1:02:C0:86:94:4F
            X509v3 Authority Key Identifier:
                keyid:21:B1:FC:73:67:DB:6C:B2:2C:76:12:C2:72:43:DB:A5:45:6F:98:00

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication, E-mail Protection
    Signature Algorithm: ecdsa-with-SHA256
         30:46:02:21:00:fc:a6:63:4e:bb:1d:26:7b:85:5d:45:ef:72:
         e5:86:1b:6a:8c:ea:fc:9a:82:8f:ee:21:f9:df:50:1f:e6:31:
         03:02:21:00:a1:d2:51:41:71:85:c8:0e:ff:1e:7a:f6:3d:0c:
         28:42:93:53:37:95:23:4e:67:ec:4f:bf:49:f6:e1:66:a0:23
```

Certificat PBK décodé et lisible

INFRASTRUCTURE DE GESTION DE CLÉ

- Le point faible des PKI repose sur la chaine de confiance constituée par la CA racine (CA root) et les CA subordonnées. Si jamais une des clés privées d'une des CA est compromise, cela remet en cause la validité des certificats qui ont été générés à partir de cette chaine de confiance. Le pire étant la compromission de la clé privée de la CA racine,
- Celui qui récupère la clé privée d'une CA peut émettre des faux certificats et usurper facilement l'identité de n'importe quel serveur étant associé à la CA compromise,
- Pour minimiser ce risque, il existe plusieurs CA racines avec des ramifications de CA subordonnées (structure pyramidale),
- Les certificats ont aussi une durée de vie limitée dans le temps ce qui limite aussi le risque d'une compromission ➔ la durée des attaques sur les clés publiques contenues dans les certificats est limité dans le temps.

La compromission de la clé privée d'un utilisateur final ne remet pas en cause la sécurité de la chaine de confiance des CA.

INFRASTRUCTURE DE GESTION DE CLÉ

- Nous allons maintenant voir, via un exemple concret, comment nous pouvons appliquer les mécanismes de PKI aux systèmes spatiaux qui en sont dépourvus nativement,
- Sur un de nos programmes (une petite constellation de télécommunication) un client avait initialement commandé 12 satellites avec seulement une protection en authenticité/intégrité (avec anti-rejeu) des TC montantes via un algorithme de hachage CCSDS basé sur des clés de 64bits de long… un peu juste,
- Une fois que les satellites ont été mis en orbite, et une fois que le client a commencé à avoir du retour sur son investissement, il nous a demandé si nous pouvions upgrader la sécurité du lien TM/TC en implémentant un service complet COMSEC TM/TC basé sur de l'AES 256.

Il faut savoir que, jusqu'en 2010 environ, les processeurs embarqués sur les satellites n'était pas assez puissant pour effectuer les calculs requis pour prendre en charge des algorithmes de cryptographie asymétrique.

INFRASTRUCTURE DE GESTION DE CLÉ

- Les hypothèses de départ étaient les suivantes :
  - Nous avions la capacité de "patcher" le logiciel de vol du calculateur du satellite pour "ajouter" les fonctions logicielles de chiffrement et déchiffrement des TM/TC,
  - Toute les TC montantes étaient, du point de vue du satellite, garanties en authenticité de la source, en intégrité et en rejeu,
  - Les données de TM descendantes n'étaient pas protégées en confidentialité et en authenticité,
  - La fonction de hachage utilisait des clés secrètes stockées en dur qui n'étaient pas modifiable et pas directement accessibles au software du calculateur embraqué (elle ne pouvait donc pas être réutilisées en clé de confidentialité).
- Nos objectifs pour répondre au besoin du client étaient les suivants :
  - Etre capable de télécharger un nouvel applicatif qui prendrait en compte :
    - un service COMSEC TC basé sur AES-GCM avec des clés secrètes de 256bits,
    - un service COMSEC TM basé sur AES-GCM avec des clés secrètes de 256bits.
  - Trouver un moyen de télécharger à bord des clés secrètes symétriques TM/TC garanties en authenticité et surtout en confidentialité sachant qu'initialement toutes les TC montent en clair.

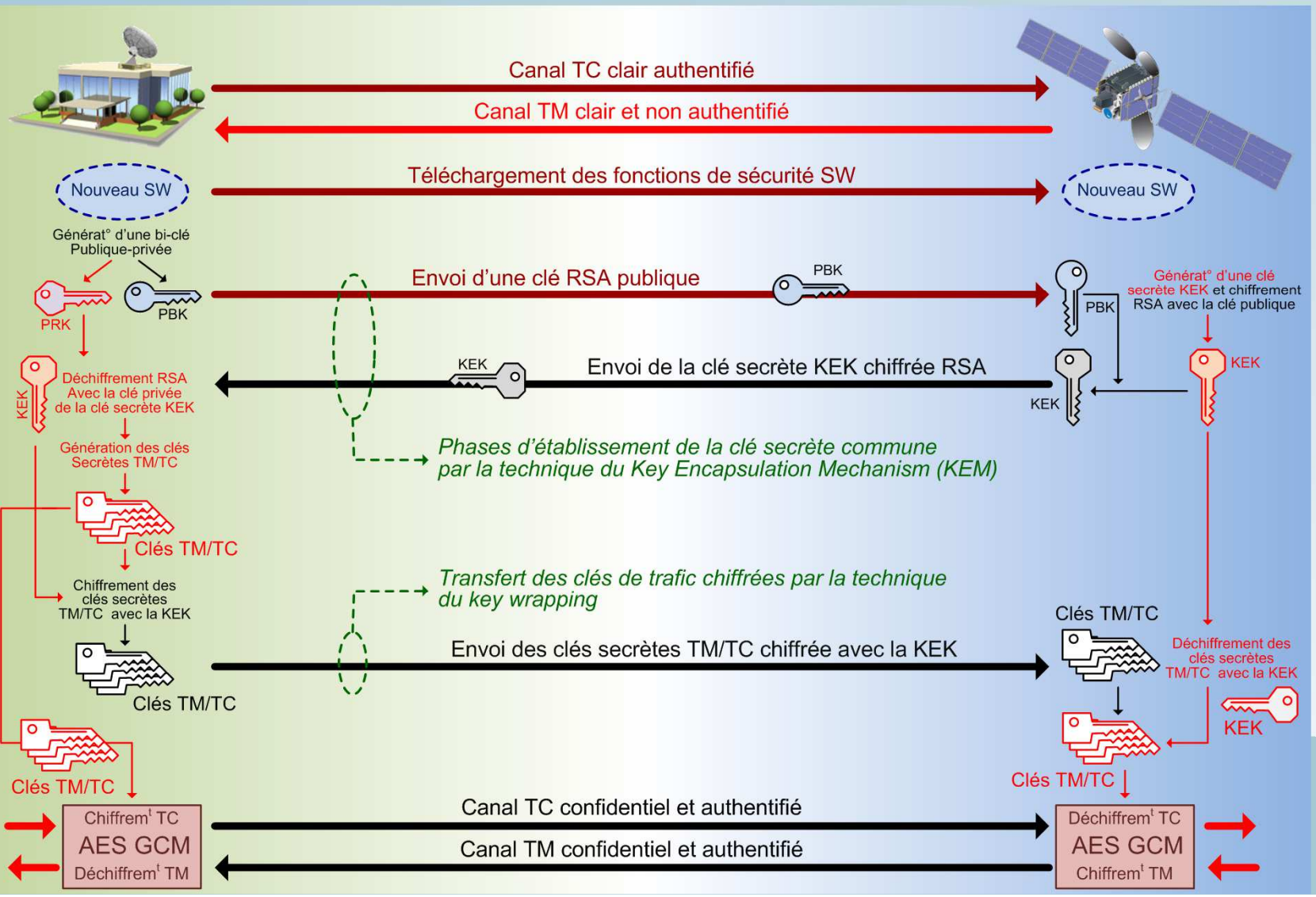
Comment faire monter une clé secrète, si, au préalable, il n'y a pas une première clé secrète de disponible pour assurer la confidentialité?

INFRASTRUCTURE DE GESTION DE CLÉ

- La solution a été d'avoir recours à la cryptographie asymétrique,
- Puisque nous avions un canal clair authentifié montant entre le sol et le bord, rien ne nous empêchait :
  - De "patcher" le logiciel de vol à bord. Il ne contenait rien de confidentiel, juste des fonctions cryptographiques publiées. Il suffisait juste de garantir l'authenticité des commandes de "patch" envoyées au satellite,
  - D'envoyer à bord, toujours via le lien montant clair et authentifié, une clé publique (non sensible) afin que le bord et le sol puissent échanger une clé secrète commune,
  - De générer au sol les jeux des clés de trafic TM/TC qui seraientt chiffrées avec la clé secrètes commune et envoyée au satellite pour qu'il les déchiffre,
- Le bord et le sol partagerait ainsi des clés de trafic confidentielles et authentiques qui pourraient être utilisées pour sécuriser les liens TM et TC entre le sol et le bord.

Fallait y penser !

INFRASTRUCTURE DE GESTION DE CLÉ



Ceci n'est pas une PKI, car il n'y a ni certificat ni autorité de certification!

Il s'agit juste d'une gestion de clé basée sur des mécanismes de cryptographie asymétrique et symétrique.

INFRASTRUCTURE DE GESTION DE CLÉ

- La mise en place de ce "protocole" d'échange de clé repose sur une hypothèse forte que nous n'avons pas mentionné jusqu'ici,
- Le satellite n'a pas de possibilité de s'authentifier du point de vue du sol. Lorsque le centre de contrôle au sol reçoit des messages du satellite, rien, dans les messages, ne permet d'en authentifier la source (= le satellite),
- Ici, nous nous appuyons sur le fait que la position exacte du satellite à un instant « t » est connue à l'avance et que cette position ne peut pas être usurpée par un autre satellite,
- L'authentification du satellite est donc garantie par son seul positionnement qui est connu et qui peut être déterminé à chaque instant,
- Donc, tous les messages émis par le satellite sont garantis en authenticité par le seul fait qu'il respecte bien ses éphémérides!

Les éphémérides d'un satellite correspondent aux données d'orbitographie qui permettent de connaître avec exactitude sa position et sa vitesse tout instant.

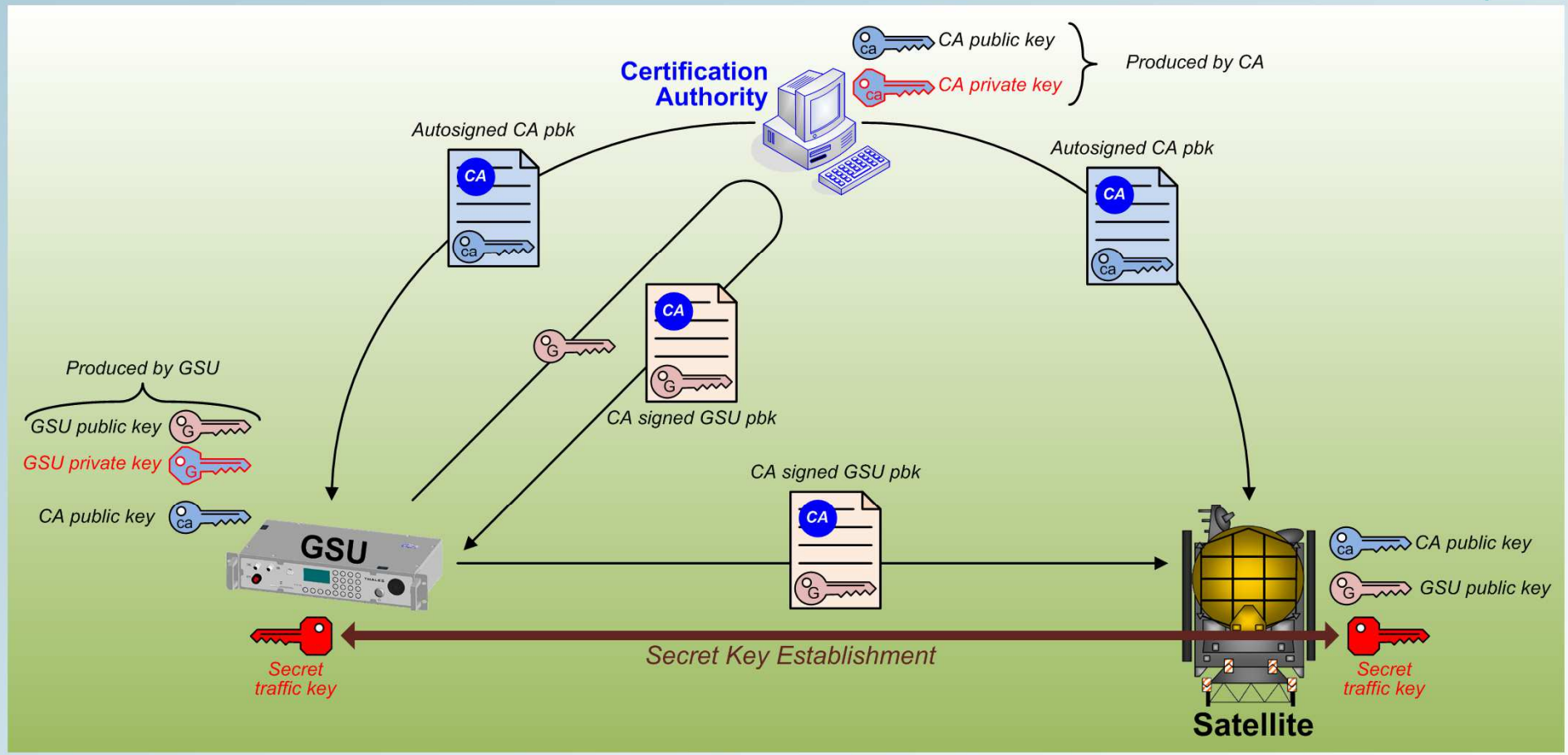
INFRASTRUCTURE DE GESTION DE CLÉ

- La solution que nous venons de voir nous a donc permis d'implémenter une primitive de chiffrement asymétrique pour sécuriser complètement un lien TM/TC bord sol (service COMSEC TM/TC : Confidentialité, authenticité et anti-rejeu),
- Nous n'avons pas, dans cet exemple, implémenté de PKI au sens propre du terme, car à aucun moment un certificat n'a été produit, signé et échangé,
- Mais sur la base de cette expérience concluante, nous pouvons maintenant envisager de déployer sur nos satellites une PKI plus complète qui nous permettrait :
  - De ne plus avoir à charger au sol (juste avant le tir des clés secrètes symétriques),
  - De n'avoir à charger dans le satellite que le certificat signé qui contient la clé publique de la station de contrôle (plus besoin d'injecter un secret dans le satellite avant le tir),
  - D'effectuer les opérations d'établissement de clé via des protocoles qui garantissent la PFS (ex: ECDH).

Les opérateurs satellites redoutent toujours la phase d'injection des clés secrètes dans le satellite, c'est pourquoi nous devons leur proposer une solution qui permet de s'affranchir de cette étape toujours jugée comme critique et risquée!

INFRASTRUCTURE DE GESTION DE CLÉ

Exemple de PKI envisagée pour un lien TM/TC satellite



Dans le cas des systèmes spatiaux une authentification semi-mutuelle est suffisante. Cela permet de ne pas avoir à gérer de clé privée dans le satellite.

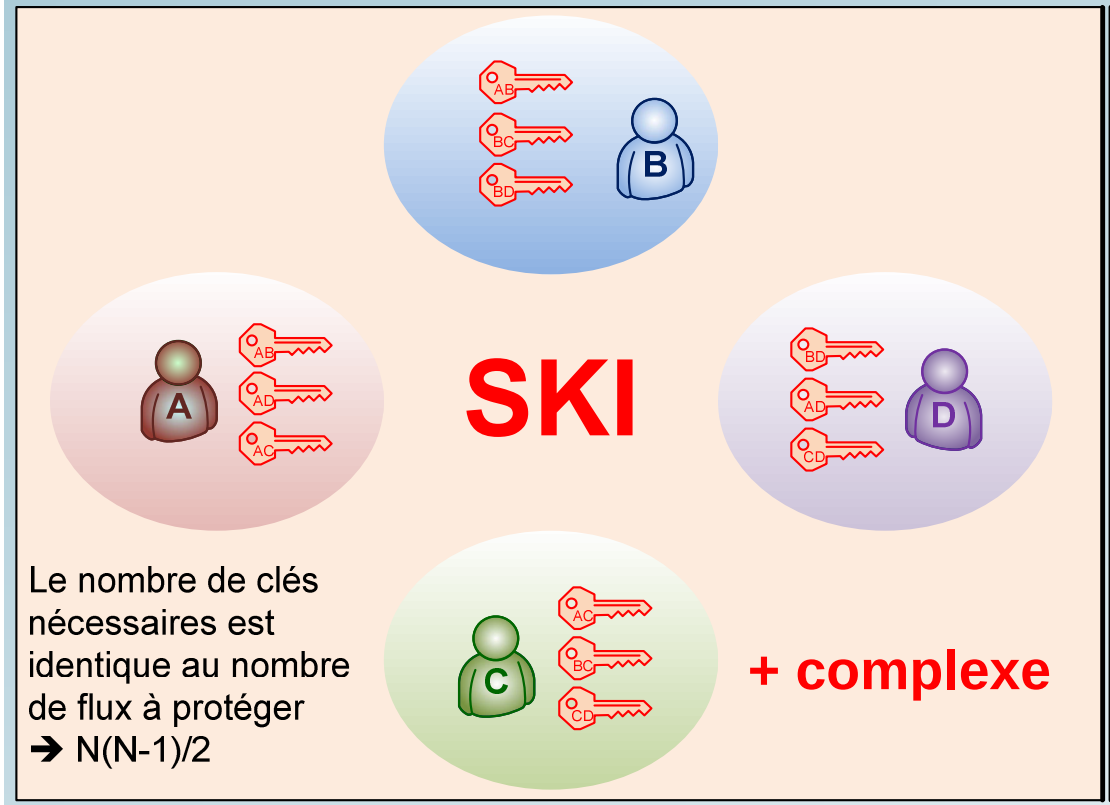
INFRASTRUCTURE DE GESTION DE CLÉ

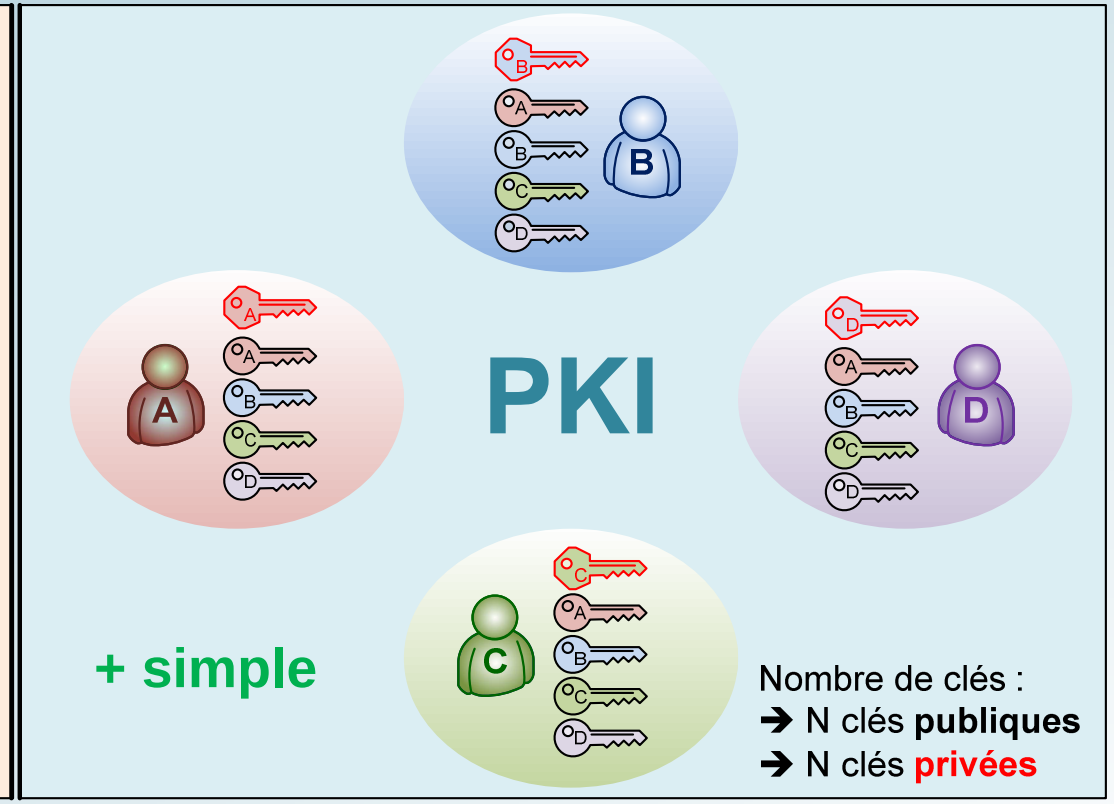
- Dans l'architecture présentée, le choix est fait de laisser les fonctions utilisatrices générer elles-mêmes leur propre couple de clé publique/privée. Ce qui nécessite l'implémentation de très bons générateurs d'aléas,
- Le certificat contenant la clé publique de la CA est auto-signé avec la clé privée de la CA (qui est donc une CA Root ou AC racine),
- Le certificat contenant la clé publique du GSU est signé avec la clé privé de la CA,
- Le certificat contenant la clé publique de la CA est inséré dans le GSU et dans le satellite (durant la phase de développement chez l'industriel),
- Le certificat contenant la clé publique du GSU sera fourni au satellite qui pourra le contre signer avec la clé publique de la CA,
- Le satellite utilisera la clé publique du GSU pour établir avec le GSU une clé secrète symétrique qui servira de clé de session pour sécuriser les communications,
- L'authentification du satellite vis à vis du centre de contrôle sol lors de la phase d'établissement de clé est garantie via les éphémérides.

Cette configuration permet de ne pas avoir à injecter de secret initial dans le satellite. La clé secrète symétrique est établie au moment où elle est nécessaire.
Cette PKI est une PKI privée sans autorité d'enregistrement.

INFRASTRUCTURE DE GESTION DE CLÉ

- Quel type d'IGC est la plus simple à implémenter et à administrer?





Si N vaut 100, alors il faudra 100 paires de bi-clés pour une PKI et 4950 clés secrètes pour une SKI ! Au-delà de 5 éléments interconnectés, il faut plus de clés secrètes que de clés asymétriques.

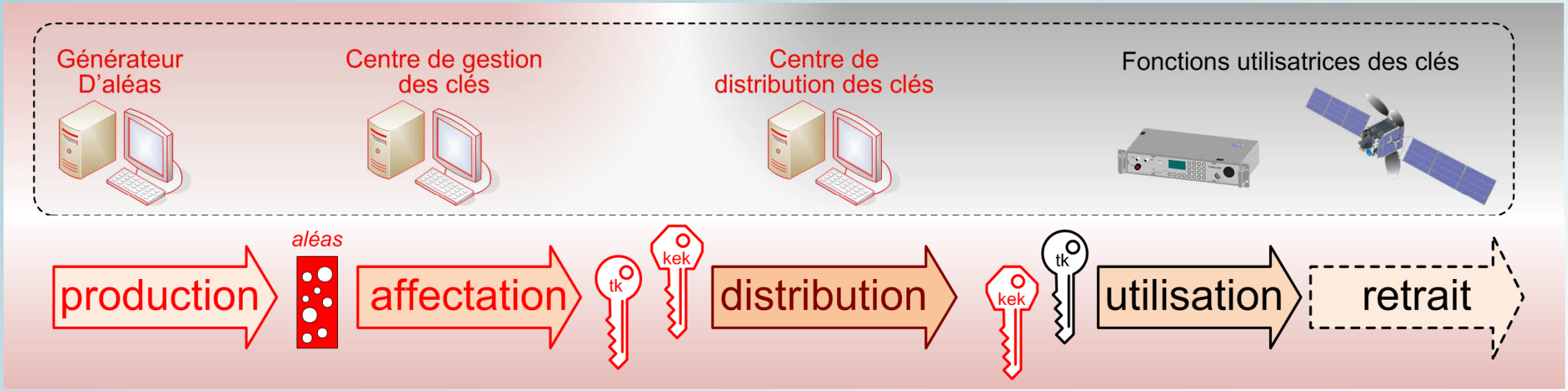
INFRASTRUCTURE DE GESTION DE CLÉ

- Alors pour nos système spatiaux quelle IGC utiliser ? SKI ou PKI.
- Jusqu'en 2015 nous utilisions exclusivement des SKI quels que soit les systèmes.
- Les SKI sont assez contraignantes et sont plus adaptées pour les systèmes qui ont un nombre réduit d'éléments à mettre à la clé (mission télécom GEO ou mission scientifique),
- Les PKI nécessitent la mise en place d'une CA privée dédiée et sont adaptées pour les systèmes qui ont un nombre d'éléments importants à mettre à la clé : constellation de satellites (télécom ou navigation),
- Enfin, sur les programmes militaire/étatiques, ce sont les IGC à base de SKI qui sont, encore privilégiée. Il est plus facile de détecter une compromission sur ce type d'IGC que sur une PKI,
- Nous commençons à envisager de déployer des solutions à base de PKI sur nos futurs systèmes spatiaux.

*"**Mettre à la clé un équipement**" signifie introduire des clés cryptographiques dans l'équipement.*

CYCLE DE VIE DES CLÉS

- Les clés ont un cycle de vie qui leur est propre et qu'il faut respecter afin de ne pas induire de vulnérabilité dans le système,
- Le cycle de vie des clés se décompose en 5 étapes : la génération, l'affectation, la distribution, l'utilisation et le retrait.



CYCLE DE VIE DES CLES

- **Production** : Une clé doit être basée sur une séquence aléatoire non prédictible et non reproductible. Elle doit être produite par un générateur d'aléa vrai,
- **Affectation** : Une clé donnée ne doit être affectée qu'une seule fois à un service de sécurité donné. Elle doit porter un identifiant unique,
- **Distribution** : Une clé doit être acheminée vers la fonction utilisatrice de façon sûre, en garantissant sa confidentialité et son intégrité de bout en bout,
- **Utilisation** : Une clé doit être utilisée dans le respect des recommandations relative à son usage et à son contexte. Elle ne jamais déroger aux règles en vigueurs,
- **Retrait** : Une clé « usée » doit être effacée et ne plus jamais être utilisable.

Les back-doors de certains systèmes reposent sur la génération de clé par une source d'aléa maitrisée et prédictible pour celui qui la connait.

CYCLE DE VIE DES CLES

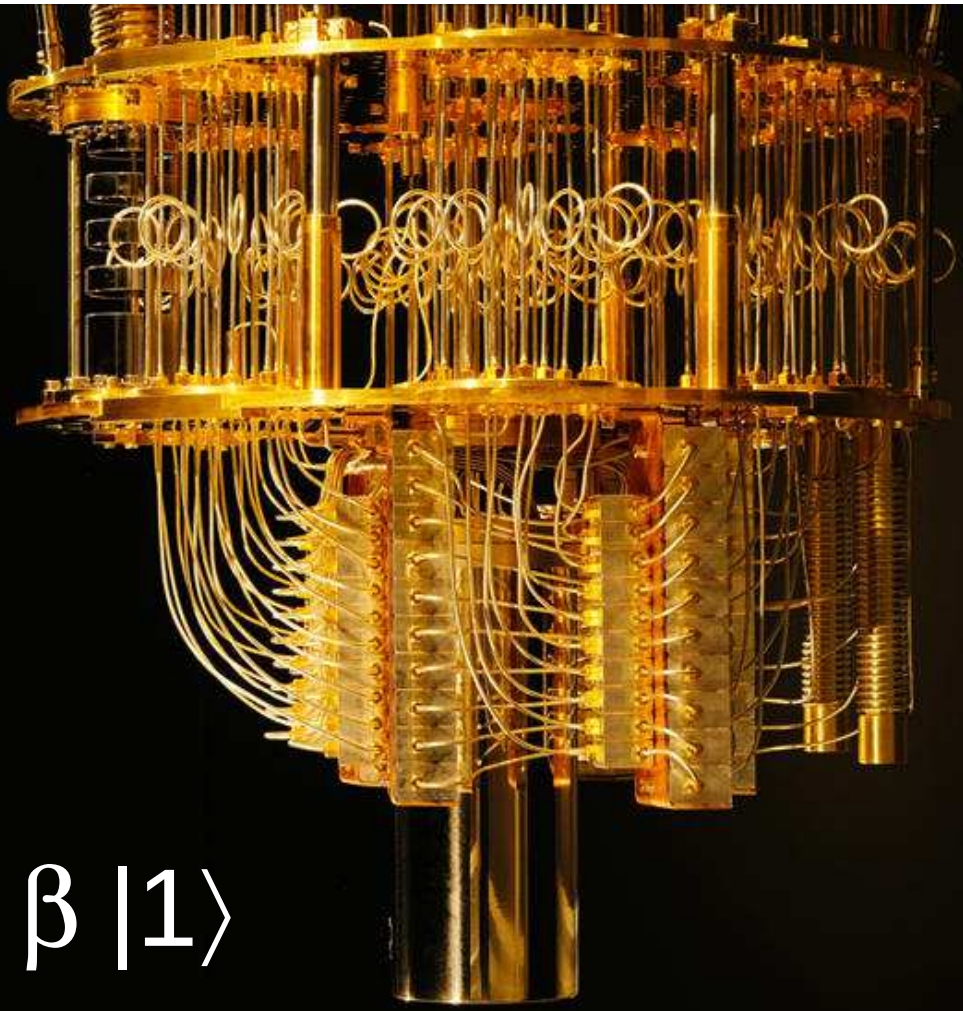
- Il existe quelques standards sur la gestion des clés :
  - NIST SP800-57 : Modèle de référence de cycle de vie des clés,
  - NIST SP800-133 : Modèle de référence pour la génération des clés,
  - NIST SP800-135 : Standard de référence pour la dérivation des clés,
  - NIST SPI-800-22 : Suite de test statistique pour les générateurs d'alea,
  - CCSDS 350.6-G-1 : Modèle de référence pour la gestion des clés,
  - RGS Annexe B2 (ANSSI) : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques.
- Des clés peuvent être dérivées à partir d'une clé dite maître. Par exemple une clé maître peut servir (via un algorithme) à chiffrer un IV (**I**nitialisation **V**ector) pour produire une clé pour la confidentialité et une clé pour l'intégrité.

CYCLE DE VIE DES CLES

- En fonction des algorithmes et des modes d'opération cryptographiques utilisés, il est nécessaire de respecter quelques points précis :
  - Changer régulièrement les clés :
    - 1 fois par mois pour les clés secrètes sur les liens satellites,
    - A chaque session de communication pour les systèmes interconnectés (ex : TLS),
    - Tous les ans pour les clés asymétriques (renouvellement des certificats).
  - Respecter les périodes cryptographiques induites par les IV ou les compteurs d'anti-rejeu;
  - Dans le cas d'AES pas plus de 2^{64} appels à la même clé (l'ANSSI recommande 2^{48});
  - Ne pas utiliser la même clé trop longtemps (moins d'un mois par exemple) afin de limiter la durée d'exposition dans les équipements au sol.
- Il faut pouvoir renouveler des clés en vol : service OTAR (**O**ver **T**he **A**ir **R**ekeying) pour couvrir tous les cas :
  - Compromission des clé au sol,
  - Corruption ou effacement accidentel des clé à bord,
  - Utilisation de clé « fraiches » qui sont toujours moins exposées.

ENCORE UN DERNIER EFFORT ET C'EST TERMINÉ

LA MENACE QUANTIQUE



$$|Q_{bit}\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

LA MENACE QUANTIQUE

- Quantum Computer is coming !
- Les développements récents en physique appliquée ont permis de développer les premiers vrais ordinateurs quantiques avec quelques dizaines de Qubits logiques effectifs (les deux notation Qubit et Qbit sont valables),
- L'ordinateur quantique manipule des Qubits qui sont une combinaison linéaire des deux état possibles d'un bit classique : $|Q_{bit}\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- α et β appartiennent à l'ensemble des nombres complexes,
- Les ordinateurs quantiques permettent d'implémenter certains algorithmes qui permettront de casser (Algorithme de Shor pour la cryptographie asymétrique) ou d'affaiblir (algorithme de Grover pour la cryptographie symétrique) les cryptographies actuelles,
- Selon les projections actuelles, nous estimons à 50% la probabilité qu'un ordinateur quantique assez puissant soit disponible à l'horizon 2035 pour casser des clés RSA de 2048bits voire plus.

2035 n'est pas si loin que ça si on considère que la durée de vie en orbite d'un satellite géostationnaire peut atteindre 20ans ! Les satellites conçus en ce moment doivent prendre en compte la menace quantique !

LA MENACE QUANTIQUE

- Une des attaques sur les systèmes cryptographiques repose sur ce qu'il s'est passé en 1998 lorsque les ordinateurs assez puissants ont pu mener des attaques exhaustives sur DES (clé de 56 bits),
- Imaginons que si tous les messages échangés avant 1998 et chiffrés avec DES avaient été enregistrés, il aurait été alors possible de les déchiffrer à postériori et de récupérer des informations suffisamment sensibles pour être exploitables,
- Avec l'avènement proche des ordinateurs quantiques et avec les capacités de stockage décuplées actuelles, il est possible de faire du "**data harvesting**" afin de mener la "**store-now-and-decrypt-later attack**",
- Le but de cette attaque est de stocker les données chiffrées échangées aujourd'hui sur les réseaux pour les déchiffrer plus tard lorsque les technologies quantiques le permettront.

Ces attaques sont actuellement mises en œuvre par les agences de sécurité gouvernementales (USA, Chine, Russie…) et sont encore dans la phase « store-now ».

LA MENACE QUANTIQUE

- Quelles sont les solutions vis à vis de cette menace?
- Là maintenant, et lorsque c'est possible, il y a deux actions qui permettent de s'affranchir de la menace liée à l'attaque "**store-now-decrypt-later**" :
  - Passer sur des clés symétriques de 256bits (protection effective = 128bits après attaque par algorithme de Grover),
  - Utiliser une infrastructure de gestion de clés de type SKI, mais cela n'est applicable que dans de très rares cas (ex: systèmes spatiaux avec peu de satellites).
- Ces deux solutions ne permettent pas de couvrir la sécurité des communications sur internet par exemple (réseau trop complexe pour une SKI),
- A plus long terme, il y a deux axes de recherche très actifs :
  - La cryptographie post quantique (PQC – **P**ost **Q**uantum **C**ryptography),
  - La distribution des clés par des canaux quantiques (QKD – **Q**uantum **K**ey **D**istribution).

La PQC et la QKD sont à l'étude depuis quelques années et seront bientôt assez matures pour pouvoir être utilisés à grande échelle.

LA CRYPTOGRAPHIE POST-QUANTIQUE

- Le NIST a initiée une compétition depuis 2017 pour développer les nouveaux algorithmes asymétriques (PQC) résistants aux ordinateurs quantiques :
  - 1er round: 69 candidats,
  - 2ème (depuis Janvier 2019): 26 candidats sélectionnés par le NIST,
  - 3ème round (depuis Juillet 2020) : 7 candidats finalistes avec 8 solutions alternatives,
  - Délai global : 6/7 années pour aboutir à un standard NIST PQC.
- 5 familles d'algorithmes PQC considérées :
  - Code-based cryptography,
  - Multivariate cryptography,
  - Isogeny based cryptography.
  - Lattice-based cryptography,
  - Hash-based signatures,
- Les applications PKI adressées par les algorithmes PQC sont : Asymmetric encryption, Key Exchange et Digital Signature,
- Les nouveaux standards de PQC sont attendus pour 2024.

Ces nouveaux algorithmes remplaceront les algorithmes actuellement utilisés (RAS, DH, EC,DL). Sans eux pas de sécurité sur internet lorsque la menace quantique deviendra effective!

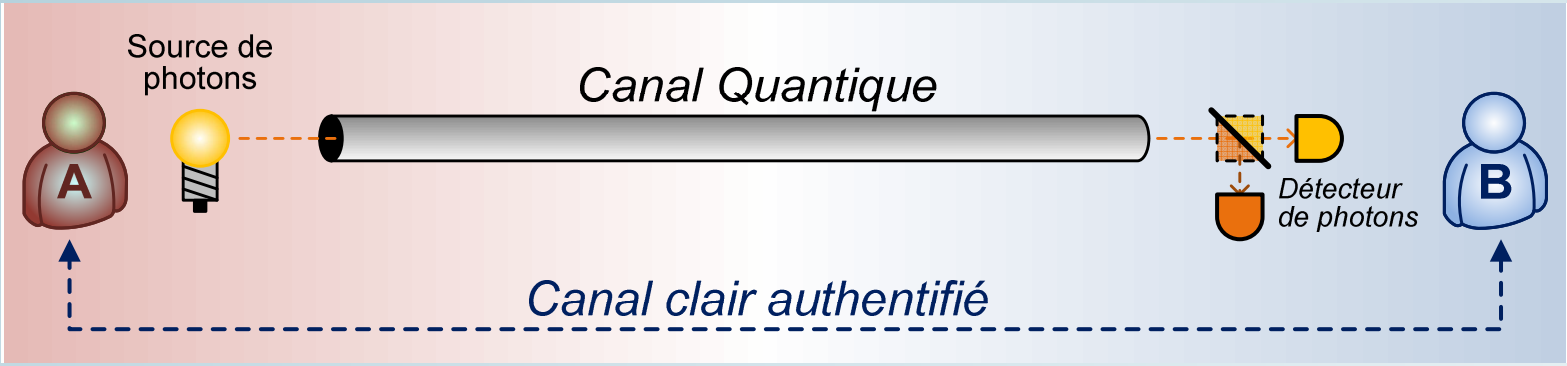
LA CRYPTOGRAPHIE POST-QUANTIQUE

- Les futurs algorithmes de cryptographie asymétrique seront, pour certains, beaucoup plus complexes que les précédents,
- A ce jour, et tant que la menace quantique n'est pas effective et que les algorithmes actuels sont jugé sûrs, l'ANSSI recommande que, lorsque les nouveaux algorithmes seront disponibles, qu'ils soient hybridés avec les anciens,
- L'hybridation consiste à signer les messages avec DSA, mais aussi avec le nouvel algorithme de PQC qui aura été retenu pour la signature,
- L'idée est de s'assurer que, si les nouveaux algorithmes ont des vulnérabilités, il y ait quand même la deuxième barrière de protection via les anciens algorithmes jugés sûrs face aux menaces actuelles,
- Après quelques années d'hybridation, il sera possible de basculer sur les nouveaux algorithmes de PQC et d'abandonner définitivement les anciens.

Ça promet quelques belles années de travail dans le domaine des PKI! La technique d'hybridation permet de faire de la défense en profondeur, c'est à dire de cumuler les protections pour rendre plus difficile les attaques.

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

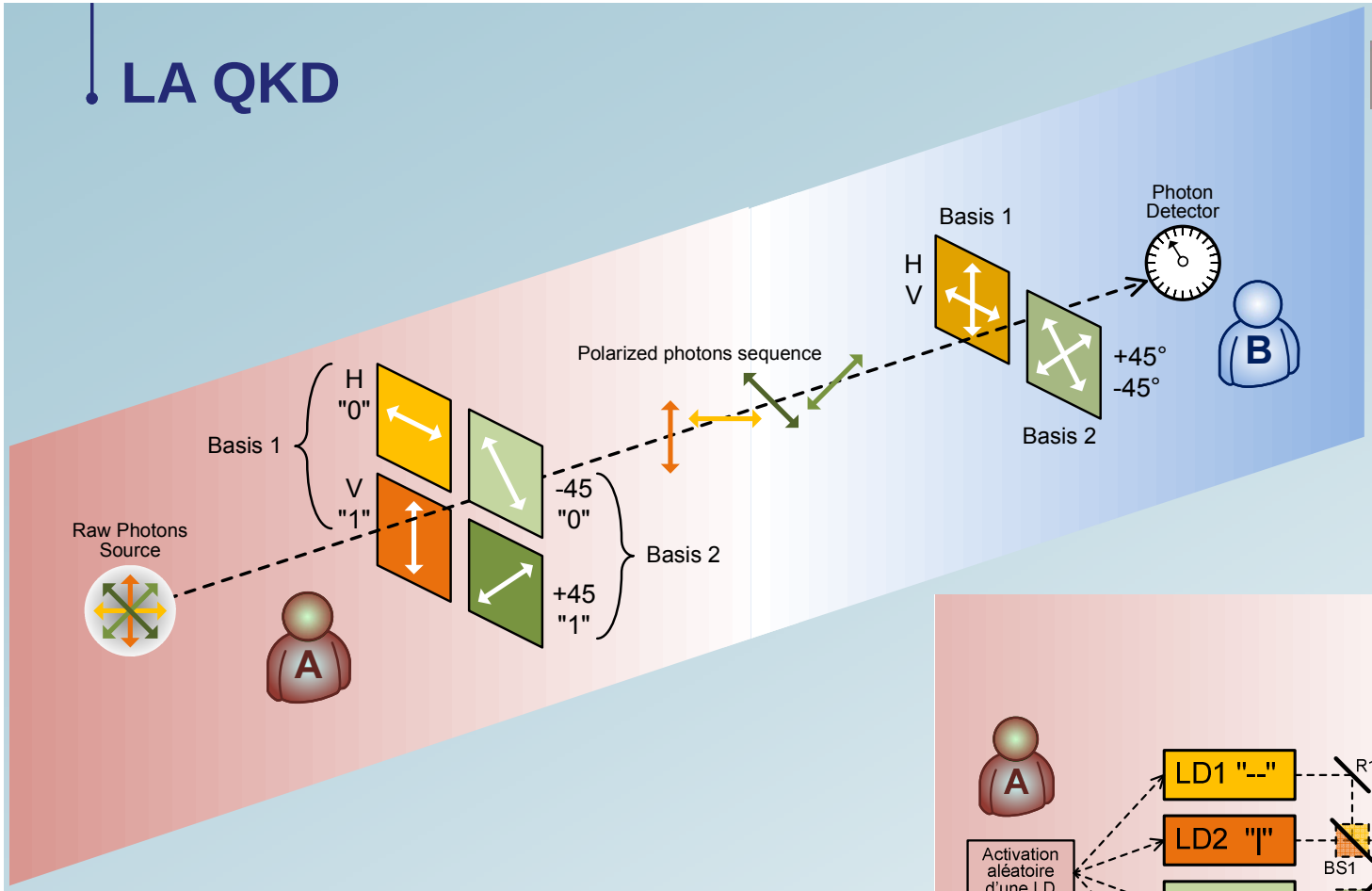
- La QKD, elle, est plus radicale dans ce qu'elle apporte,
- La QKD permet dans la phase d'établissement d'une connexion sécurisée de remplacer la phase Diffie-Hellman d'établissement de clé par une phase d'établissement de clé basée sur l'échange de particules quantiques,



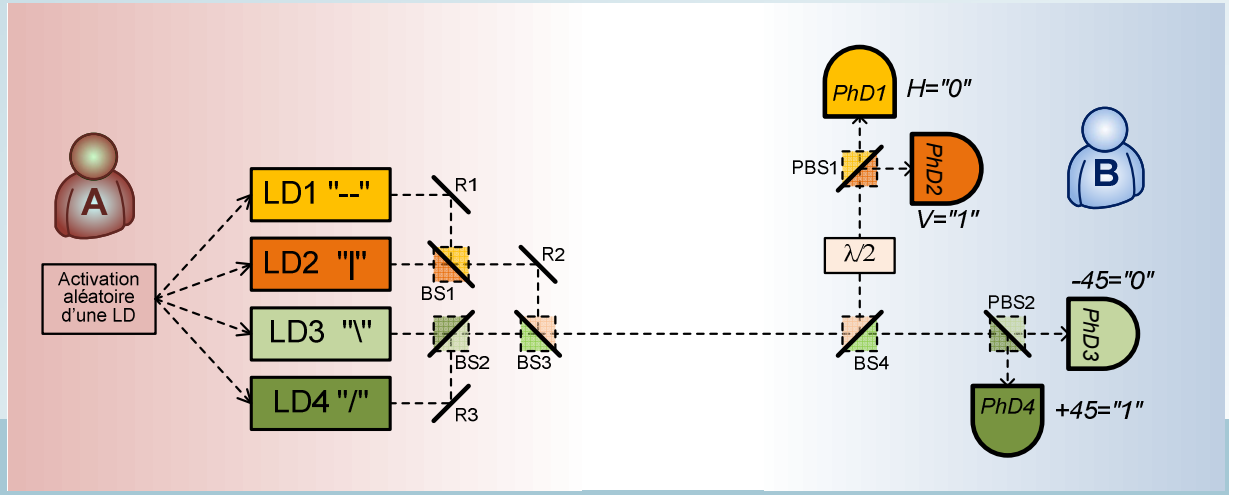
- Alice et Bob échangent des photons (via une fibre optique) et communiquent, sur un canal non confidentiel mais authentifié, les résultats des mesures pour se mettre d'accord sur une clé secrète commune.

La clé secrète commune établie au travers du protocole de QKD servira ensuite à chiffrer/authentifier les communications entre Alice et Bob.

LA QKD



BS : **B**eam **S**pliter ou séparateur de faisceau 50/50
PBS : **P**olarised **B**eam **S**pliter ou séparateur de photons polarisé



Pour faire de la QKD, il faut maitriser la mécanique quantique et l'optique !

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- Alice détermine à l'avance une séquence aléatoire de bits (1),
- Elle choisit ensuite d'encoder les bits en Qubits en utilisant des photons qui sont polarisés selon une des deux bases de polarisation possibles (base n°1 = H/V et base n°2 = +45/-45) puis envoyés à Bob (2),
- Bob, "choisit aléatoirement" et indépendamment d'Alice, une base pour la détection des photons et il notera la valeur détectée et la base de détection (3)(4),
- Bob transmet à Alice la séquence des bases qu'il a "choisi" pour la détection (5),
- Alice compare la séquence de Bob avec la sienne et indique à Bob les endroits de la séquence où les bases ne correspondent pas aux siennes (6),
- Alice et Bob peuvent éliminer les bits qui n'ont pas été émis/détectés selon la même base pour obtenir une séquence secrète commune : la clé brute (raw key) (7).

Les phases (5), (6) et (7) sont regroupés sous le terme de phase de « sifiting » qui signifie tamisage.

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

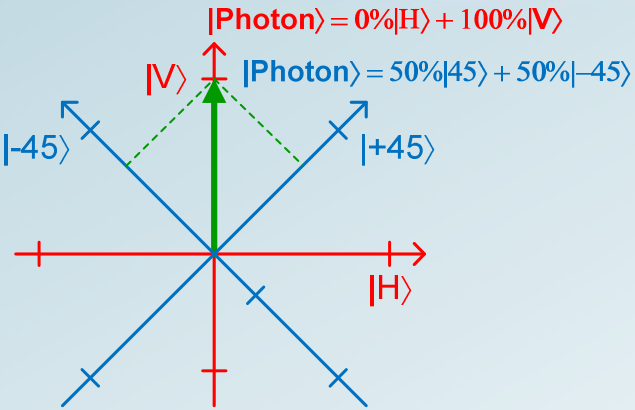
Séquence binaire initiale d'Alice	0	1	1	0	0	1	0	0	0	0	1	0	1	1	0	0	0	0	1	1	1	0	0	1	
Choix du mode de polarisation par Alice	+	+	X	+	X	X	X	X	X	X	X	+	X	X	+	+	X	X	+	X	+	+	+	2	
Photons envoyé par Alice	-	|	/	-	\	/	\	\	\	\	/	-	/	/	-	-	\	\	|	/	|	-	-		
Choix du mode de détection par Bob	+	+	+	X	X	X	X	+	+	+	+	+	X	+	+	+	X	+	+	X	+	X	X	3	*Génération, transmission et détection de la séquence initiale d'Alice par Bob*
Mesure de polarisation de Bob	-	|	|	/	\	/	\	-	|	-	-	-	/	|	-	-	\	-	|	/	|	\	/	4	
Séquence binaire résultante de Bob	0	1	1	1	0	1	0	0	1	0	0	0	1	1	0	0	0	0	1	1	1	1	0		

⇓

Bob transmet à Alice son tirage de detection	+	+	+	X	X	X	X	+	+	+	+	+	X	+	+	+	X	+	+	X	+	X	X	5	*Echanges entre Alice et Bob pour identifer les bits valides*
Alice indique à Bob lesquels sont conformes	O	O	N	N	O	O	O	N	N	N	N	O	O	N	O	O	O	N	O	O	O	N	N	6	
Séquence binaire sûre reconstituée par Alice & Bob	0	1			0	1	0					0	1		0	0	0		1	1	1			7	

La séquence de préparation/envoi des photons, de détection des photons et d'échange des bases est commune à tous les protocoles de QKD.

LA CRYPTOGRAPHIE QUANTIQUE (QKD)



- Du point de vue quantique les choses fonctionnent comme suit :
- Alice a polarisé verticalement un photon, dans la base des vecteurs états vertical/horizontal que nous notons |V⟩ / |H⟩, vis à vis de cette base des états, l'état du photon s'exprime comme suit :
  - |Photon⟩ = 0% |H⟩ + 100% |V⟩
- Cela signifie que le photon est polarisé verticalement et que si ce photon est envoyé vers un filtre polarisant vertical, il aura 100% de chance de passer et d'être détecté comme d'un "1",
- Un photon qui aura été polarisé horizontalement (préparé dans l'état |Photon⟩ = 100% |H⟩ + 0% |V⟩) sera systématiquement réfléchi par le filtre polarisant vertical et sera détecté comme un "0" de façon certaine,
- Par contre, un photon polarisé verticalement aura 50% de chance de passer le filtre polarisant à +45° et 50% de chance d'être rejeté. Dans ce cas les photons |V⟩ seront détectés aléatoirement soit comme un "1" soit comme un "0".

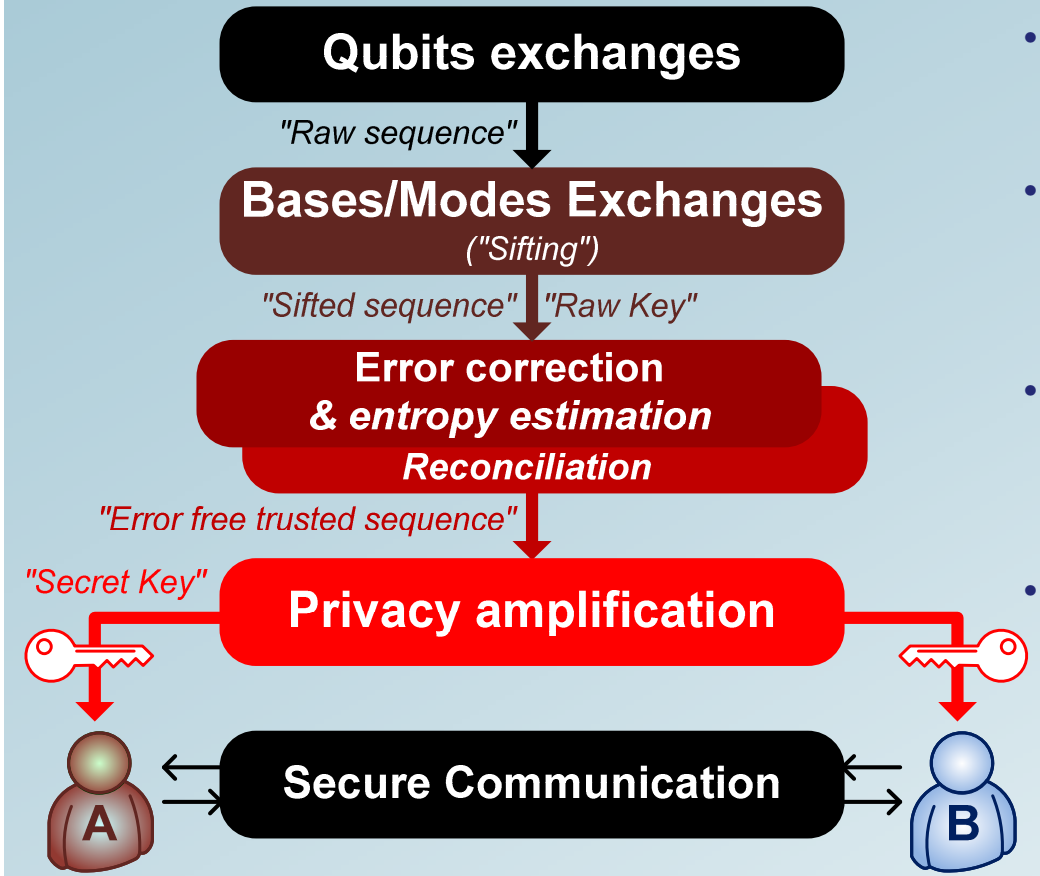
C'est pour cela qu'Alice et Bob doivent échanger le choix des bases de polarisation pour ne conserver que les photons préparés et mesurés selon la même base.

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- Le protocole présenté jusqu'ici a été inventé, en 19**84,** par Charles **B**ennet et Gilles **B**rassard, il se nomme : **BB84** (pas très original mais explicite),
- Il existe toute une variété de protocoles de QKD dérivé de BB84 qu'on regroupe sous la famille des protocoles **P&M** : "**P**repare and **M**easure" car Alice prépare l'état quantique du photon et Bob mesure cette état quantique préparé,
- Il existe 2 autres techniques d'établissement de clé par des canaux quantique :
  - Emission par une source unique de paires de photons intriqués qui sont détecté simultanément par Alice d'un côté et Bob de l'autre. Ce type de protocole est du type **EB** (**E**ntanglement **B**ased) et le plus connus d'entre eux est le protocole E91 inventé par Arthur Ekert en …1991!
  - Emission simultanée de deux photons à destination d'un détecteur (Charlie). Alice émet un photon en même temps que Bob et, au milieu se trouve, Charlie le détecteur. Charlie indique ensuite à Alice et à Bob quel est le résultat des détections. Ce type de protocole, encore peu répandu, est connu sous le nom de **MDI** : "**M**easurement **D**evice **I**ndependant".

Tout ça c'est bien beau mais comment on utilise la QKD dans les communications classiques?

LA CRYPTOGRAPHIE QUANTIQUE (QKD)



- La séquence pour l'établissement comprend des phases supplémentaires en plus de l'échange quantique et de l'échange des bases,
- Il y a une phase de correction des erreurs dues aux imperfections du canal de transmission, un trop grand nombre d'erreur peut indiquer que quelqu'un écoute le canal,
- Il y a ensuite une phase d'échange de quelques bits (sacrifiés) de la clé brute et qui permet à Alice et Bob de s'assurer qu'ils n'ont pas été écouté ou victime d'une attaque MITM (= réconciliation),
- Il y a enfin une phase d'amplification du secret qui consiste à appliquer une fonction de hachage à sens unique sur la clé brute de sorte à obtenir une clé finale raffinée qui n'a plus grand chose à avoir avec la clé brute initiale. Cette phase s'appelle l'amplification du secret.

Pour essayer d'intercepter la clé, il est nécessaire de s'intercaler physiquement sur le canal quantique pour exploiter les vulnérabilités des sources/canal/détecteurs lorsqu'il y en a. La QKD est donc hors de portée de la menace des ordinateurs quantiques!

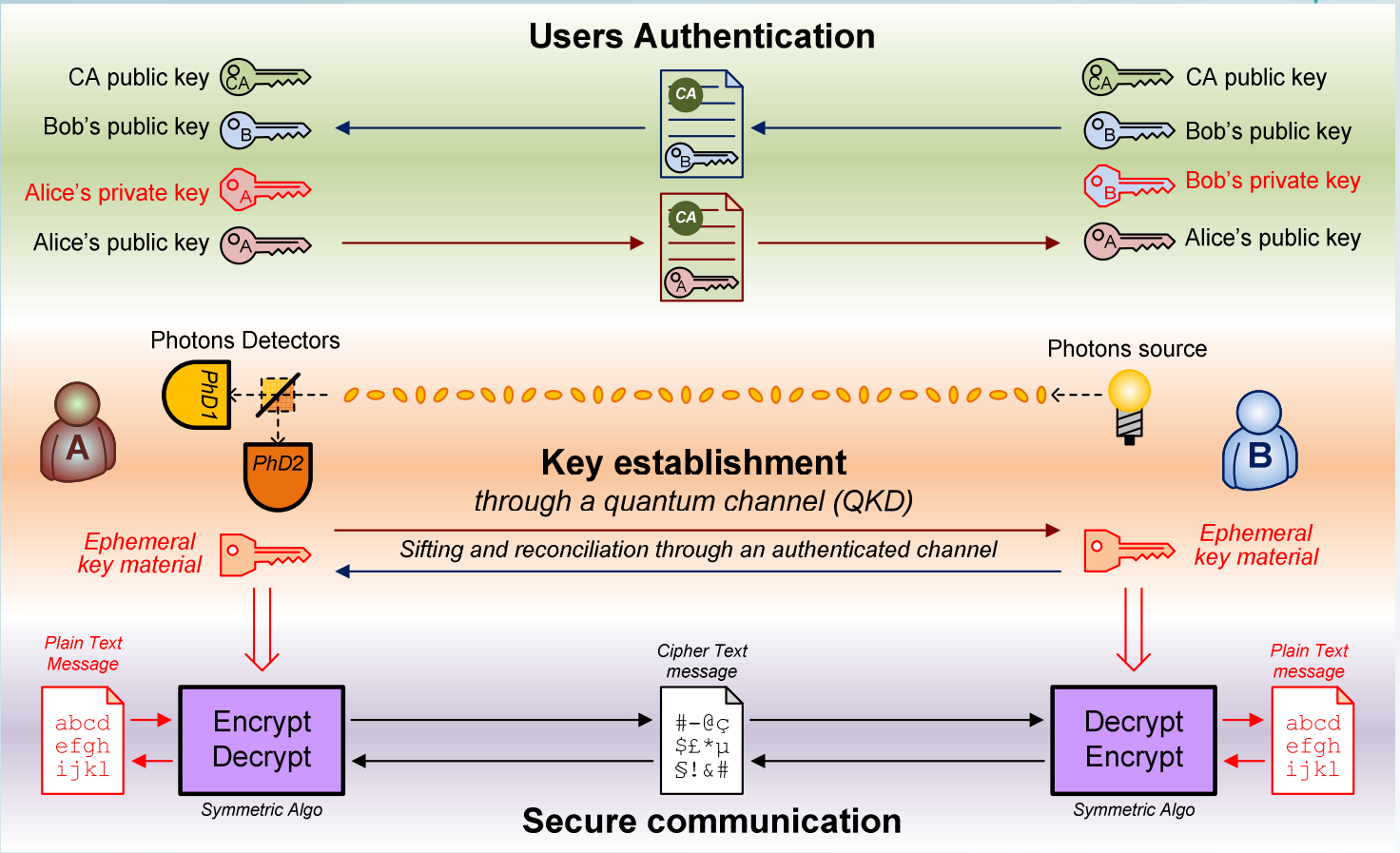
LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- La sécurité des protocoles d'établissement de clé par des canaux quantiques repose sur les lois de la mécanique quantiques qui stipulent :
  - Que toute mesure effectuée sur une particule affecte son état quantique et que cela sera décelable par celui qui devait la détecter initialement,
  - L'état d'une particule quantique est non "clonable", il est strictement impossible de dupliquer un photon par exemple (il faudrait pouvoir le mesurer sans affecter son état ce qui est impossible!).
- De fait, Bob est capable, avec Alice, et lors de la phase de réconciliation, de savoir si un espion a intercepté ou a tenté de mener une attaque de l'homme du milieu sur le canal quantique;
- Les lois de la mécanique quantique garantissent donc la confidentialité du Qubit porté par le photon et l'intégrité de celui-ci,
- Par contre, elles ne permettent pas de garantir l'authenticité de la source. Lorsque Bob reçoit un photon, rien ne lui dit que ce photon a bien été émis par Alice. C'est ce qui justifie ici la nécessité d'avoir recours à un canal clair authentifié pour échanger les bases!

Authentification de la source sur un canal clair? Ca nécessite la mise en place d'une SKI ou d'une PKI avec certificats signés!

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- La QKD s'insère dans le processus de communication en remplaçant la phase d'établissement de clé Diffie-Hellman
- Cependant, l'authenticité des sources et le chiffrement des communication est toujours assuré par de la cryptographie asymétrique et de la cryptographie symétrique



Pour être cohérent, il faut coupler la QKD avec des algorithmes asymétriques post quantiques de sorte à offrir un lien complètement résilient face à la menace des ordinateurs quantiques.

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- La QKD apporte l'avantage suivant : elle permet de mettre en place un mécanisme physique pour l'échange des clés qui nécessite des attaques bien particulières et très sophistiquées,
- La sécurité de la QKD ne repose pas sur la résolution de problèmes mathématiques complexes,
- Utiliser la QKD, c'est donc ajouter une barrière supplémentaire de défense, ce qu'on appelle de la défense en profondeur,
- Néanmoins, la QKD souffre de quelques désavantages :
  - La portée d'un canal optique sur fibre optique n'est que de 100km max, il n'est pas possible de faire de la QKD entre Paris et New York via la fibre!
  - Les équipements de QKD coûtent à l'heure actuelle extrêmement chers, autour de 200 000 euros!
- Même si nous savons que les prix vont baisser, la limitation des 100km va être difficile à surmonter pour implémenter des WAN en QKD,
- Le seul moyen pour surmonter cette limitation est de faire de la QKD en champ libre (free space) ou même depuis l'espace!

Les photons sont beaucoup moins sensibles au phénomène d'absorption dans l'atmosphère et encore moins dans le vide de l'espace.

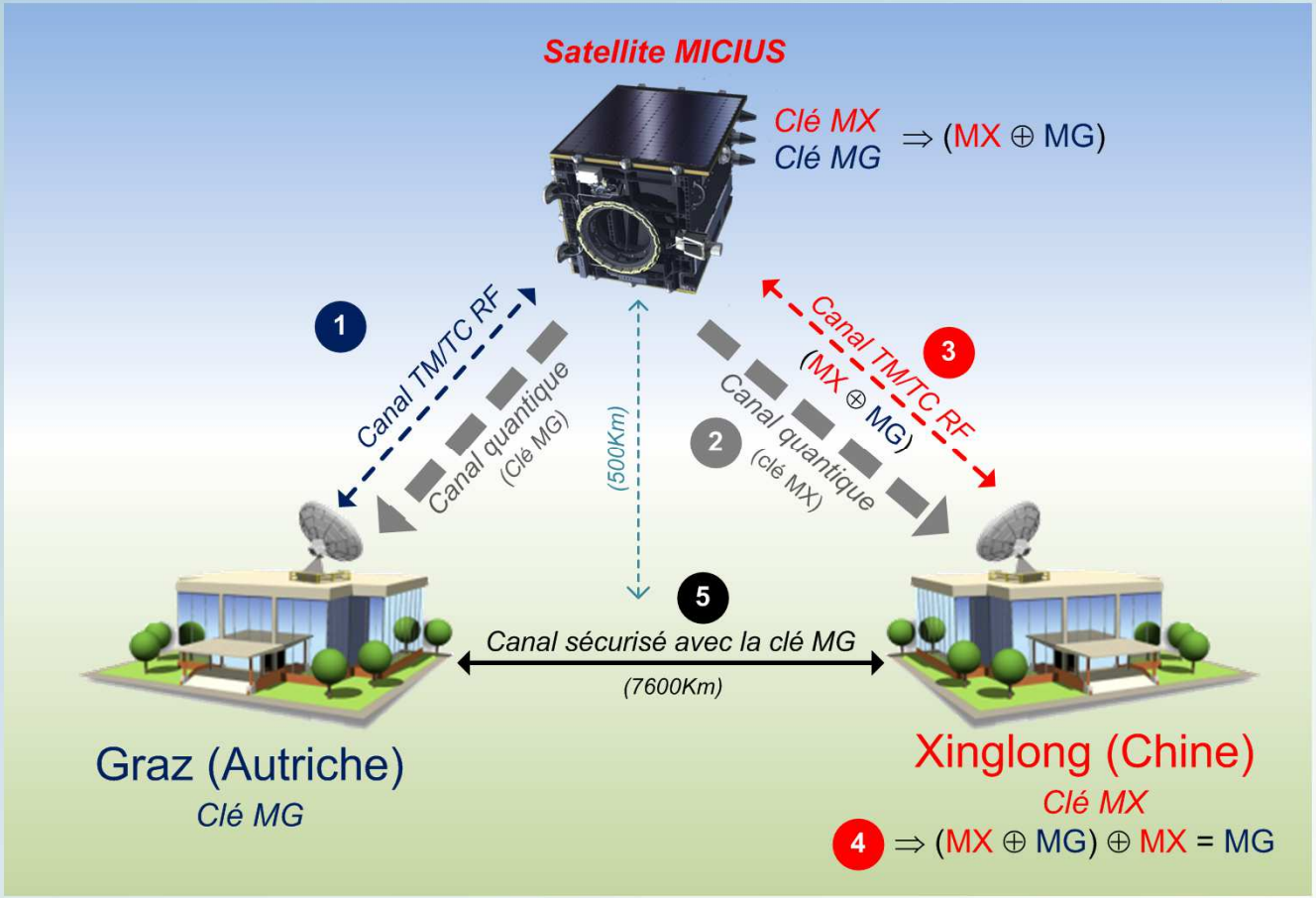
LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- Et le spatial dans tout ça?!
- La mise en place d'un canal quantique pour établir des clés secrètes en vue de sécuriser spécifiquement un lien TM/TC bord sol n'est pas envisageable car le matériel nécessaire est extrêmement couteux, complexe et lourd par rapport aux solutions actuelles,
- Pour le satellite il faudrait embarquer : une source de photon, un télescope (20 à 30cm de diamètre), des systèmes de pointage optiques avec lasers, etc,
- Par contre, il est tout à fait imaginable qu'un satellite puisse depuis l'espace distribuer des clé à des utilisateurs distants au sol (Alice à Paris et Bob à New York pat exemple),
- Les chinois l'ont fait en 2016! En lançant le satellite MICIUS qui est le tout premier du genre et qui permet de distribuer des clés à des utilisateurs au sol via des canaux quantiques,
- Depuis cette époque, les agences occidentales, dont l'ESA, ont décidé de relever le défi !

C'est bien beau mais comment cela fonctionne?

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

1) Le satellite MICIUS établit une clé MG avec la station de Gratz,
2) Lorsque le satellite passe au-dessus de la station de Xinglong, il établit une clé MX avec cette station,
3) Le satellite transmet ensuite à la station de Xinglong le XOR entre MX et MG (one-time pad),
4) La station de Xinglong reconstitue la clé MG en « xorant » sa clé MX avec la séquence (MX ⊕ MG) précédemment reçue,
5) La station de Gratz peut établir une communication sécurisée avec la station de Xinglong en utilsant la clé secrète commune MG.



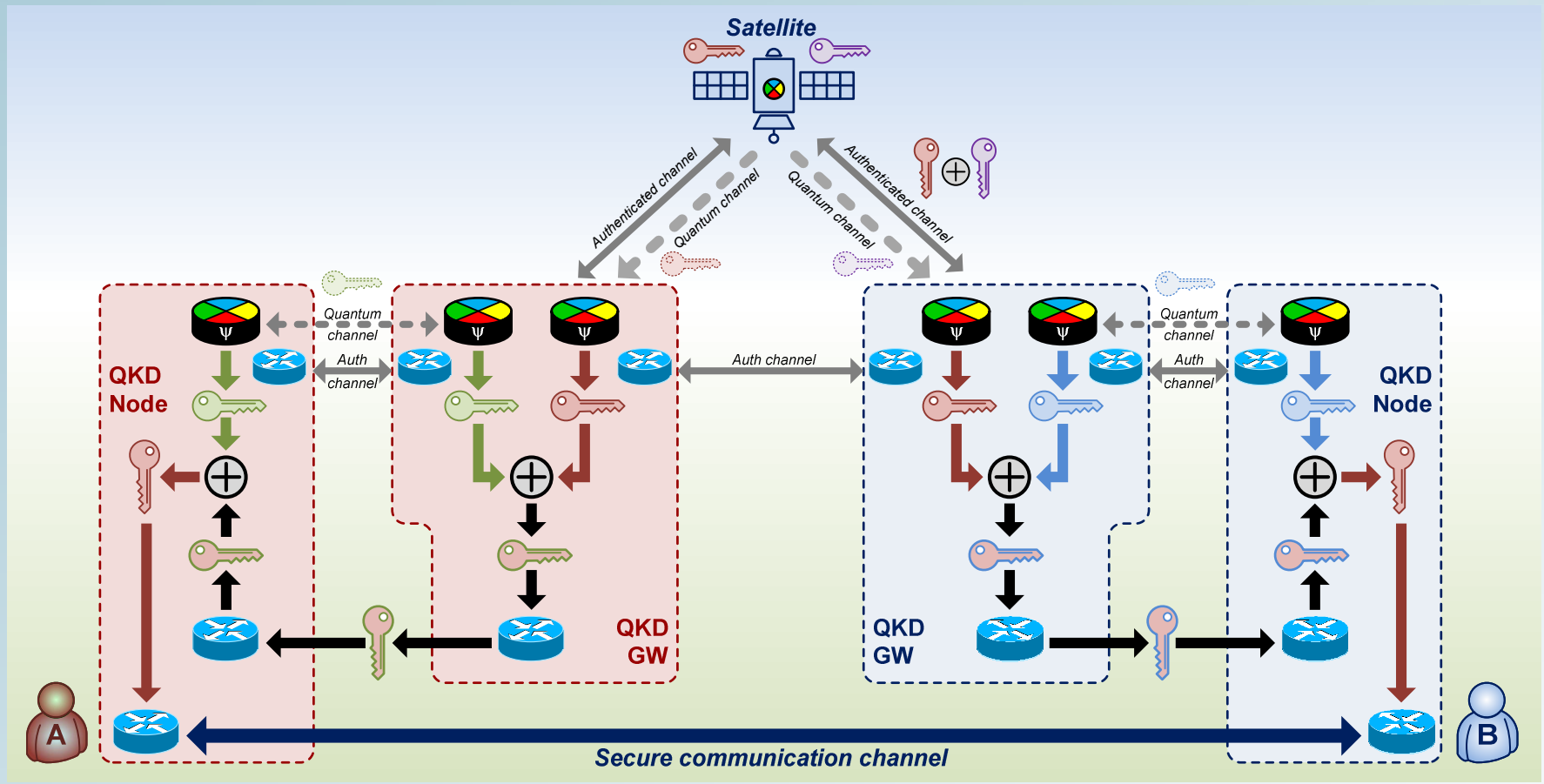
Ici l'emploi du satellite (en orbite LEO) permet d'outre passer la limitation sol des 100km imposée par la fibre optique au sol. Avec l'usage des satellites, il n'y a plus de limite pour la QKD !

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- L'idée est donc de prévoir au sol des sortes de « portes d'entrée » (ou QKD GateWays) en relation avec les satellites et avec les réseaux locaux de QKD au sol pour pouvoir les interconnecter entre eux sur de longue distances,
- Un utilisateur quelconque peut alors établir une clé via des techniques de QKD avec un autre utilisateur, même très éloigné à la condition que les deux aient localement accès à une QKD Gateway,
- Du coup, le réseau mondial de QKD est une collection de réseaux de QKD fibrés locaux qui sont interconnectés entre eux par l'entremise des satellites et des QKD GateWays,
- A noter que les futurs réseaux de QKD ne permettent pas de remplacer toutes les configurations réseau qui requièrent de l'établissement de clés,
- La QKD reste une technique lourde et complexe à mettre en œuvre qui sera exclusivement réservée à la sécurisation de réseau critique : infrastructures d'énergie, agences gouvernementales, agences bancaires etc.

La QKD ne remplacera pas les protocoles d'établissement de clé par des techniques de cryptographie asymétrique (classique ou post quantique) qui représentent la majorité des cas d'emploi.

LA CRYPTOGRAPHIE QUANTIQUE (QKD)



Cette figure montre toute la complexité d'un réseau mondial basé sur de la QKD.

LA CRYPTOGRAPHIE QUANTIQUE (QKD)

- La menace que font peser les futurs ordinateurs quantiques sur la sécurité des communication doit donc nous obliger à repenser nos algorithmes et nos architectures,
- La QKD et la PQC permettront de contrer la menace quantique :
  - Les nouveaux algorithmes post-quantiques seront, lorsqu'ils seront disponibles, déployés sur l'ensemble des machines et serveurs connecté à internet,
  - La QKD restera une solution de niche et sera mise en place seulement pour les réseaux identifiés comme à très fort risque cyber ou jugés critique,
- Dans ces deux domaines les choses évoluent très vite et il faut toujours être en veille technologique afin de prendre en compte les nouveautés dès qu'elles se présentent,
- Une solution qui était sûre il y a quelques mois, n'est pas garantie sûre à vie, cela est d'autant plus vrai pour des systèmes dont la durée de vie peut dépasser 15 ans,
- C'est toute la difficulté de nos systèmes.

CONCLUSION

CONCLUSION

- Compte tenu du contexte d'augmentation des menaces cyber dans tous les secteurs, la sécurisation des liens de communications spatiaux qui avant, était une option, est devenue obligatoire,
- La mise en place de service de sécurité sur des liens spatiaux doit toujours prendre en compte les sorties de l'analyse de sécurité système,
- La mise en place de service de sécurité sur des liens spatiaux doit toujours prendre en compte les standards applicables,
- L'évolution des technologies et des menaces nécessite de toujours rester vigilent et de ne jamais être prisonniers de solutions établies,
- Il faut toujours être capable de se remettre en cause pour adapter les solutions lorsque de nouvelles menaces apparaissent.

MERCI POUR VOTRE PATIENCE ET VOTRE ATTENTION !

LES LIENS UTILES

- Les Critères Communs :
  https://www.commoncriteriaportal.org/
- Certification FIPS 140-2/140-3 :
  https://csrc.nist.gov/publications/detail/fips/140/2/final
  https://csrc.nist.gov/publications/detail/fips/140/3/final
- Recommandation sur les tailles des clés :
  https://www.keylength.com
- Orbitographie :

  https://upload.wikimedia.org/wikipedia/commons/b/b4/Comparison_satellite_navigation_orbits.svg
- Les référentiels généraux de sécurité de l'ANSSI :
  https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/
- Point de contact :
  benoit.tranier@thalesaleniaspace.com