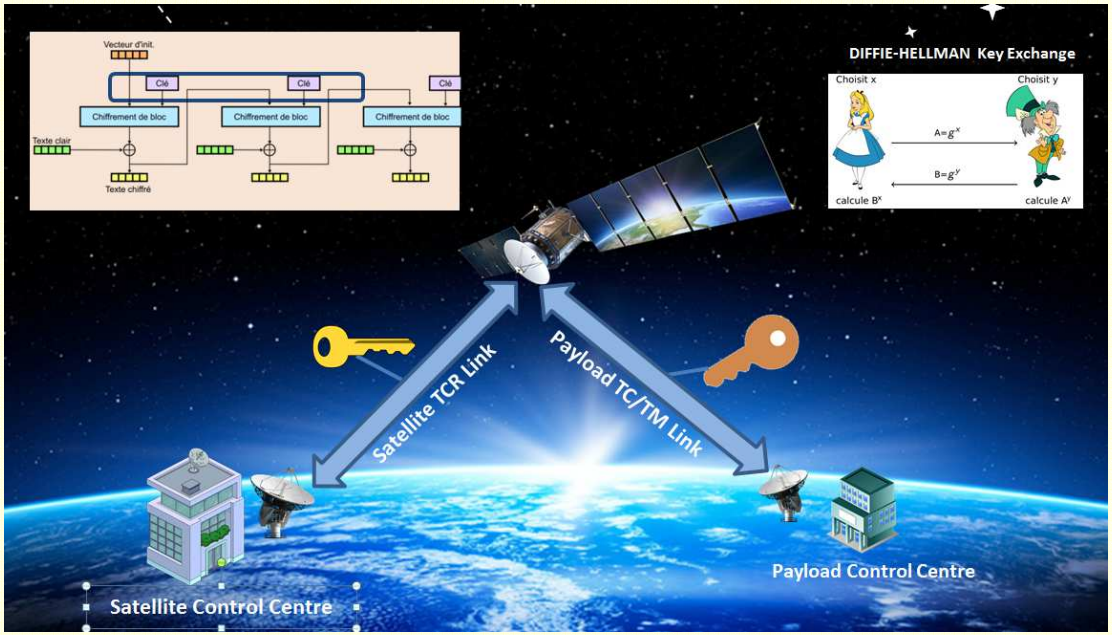
Formation TLS-SEC

Sécurité des Communications Spatiales



Intervenant : William HALIMI - THALES ALENIA SPACE France

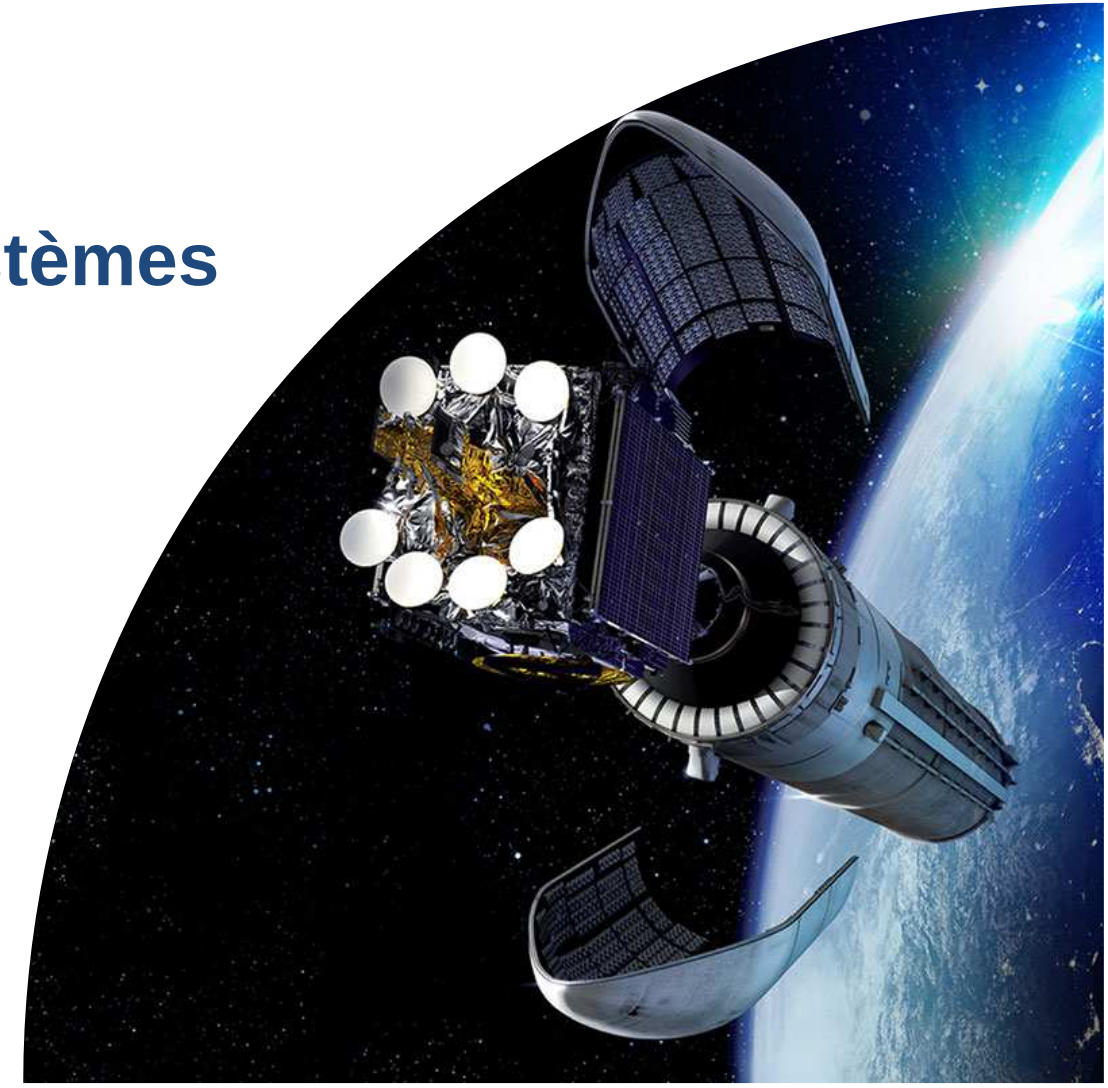
ENSEEIHT Toulouse – Le 8 Janvier 2020

Ref : TAS-FORM-TLS-SEC-PR-001
Issue : 1
Date : 08 Janv 2020

Plan de la Présentation

TLS-SEC – Sécurité des Communications Spatiales

1 – Missions et Systèmes Spatiaux Cibles



1.1 – Missions et Systèmes Spatiaux Cibles

Type de Mission

- Télécommunication
- Observation / Environnement / Sécurité civile
- Scientifique
- Navigation

Profil Mission applicable à chaque type

- Commerciale : ex EUTELSAT / INTELSAT(Télécom), SPOT (Observation)
- Défense : Ex SYRACUSE (Télécom), HELIOS (Observation)
- Duale : Commerciale et Défense : ex PLEIADES (Observation), SGDC (Télécom)

1.2 – Systèmes Spatiaux

Orbite

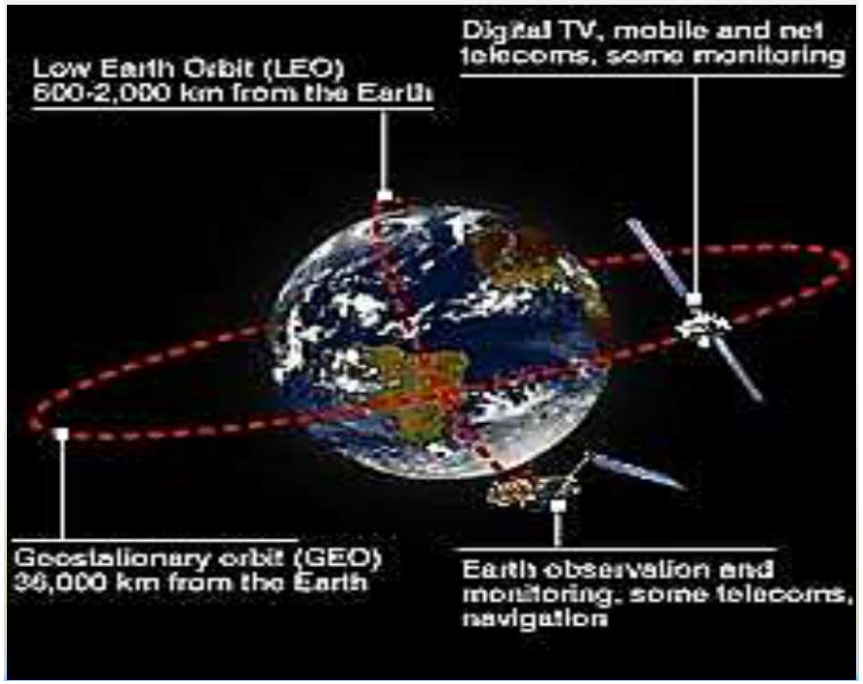
- Géostationnaire : 36000 km
- LEO (Low Earth Orbit) : orbite circulaire 500 à 1500 km
  - Période orbitale : environ 90 mn – Durée de visibilite / passage : 10 à 15 mn
- MEO (Medium Earth Orbit) / HEO (Highly Elliptical Orbit): 2000 à 30000 km
  - Ex: GLONASS, GPS, GALILEO, IRIDIUM
  - Période orbitale : 2h à 12h

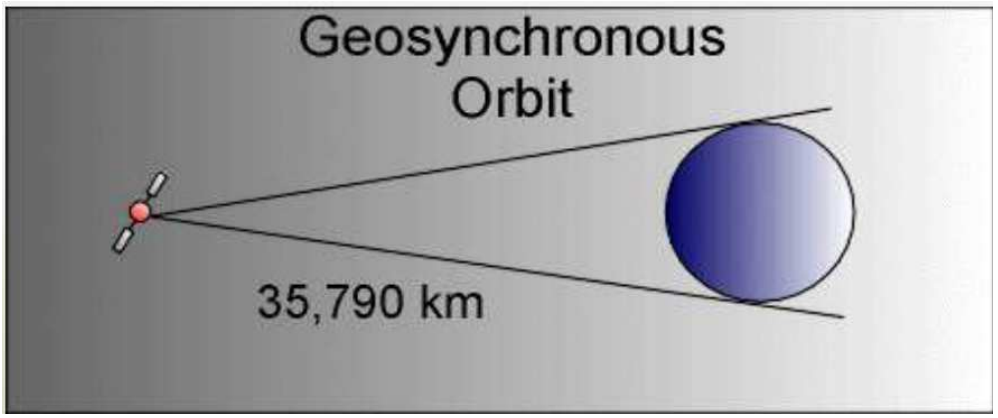
Configuration

- Mono / Multi satellites
- Constellation :
  - Telecom : IRIDIUM, O3B, GLOBALSTAR
  - Navigation : GPS, GALILEO, GLONASS
  - Avec ou non liaison inter satellites (ISL: Inter satellite Link) : exemple IRIDIUM

1.2 – Systèmes Spatiaux => Orbites

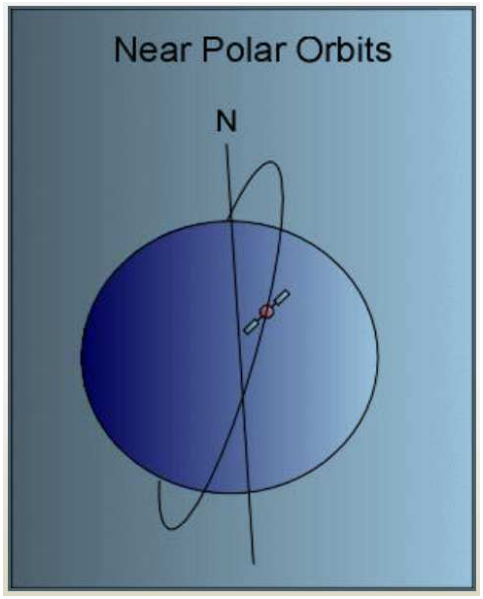
Orbite GEO

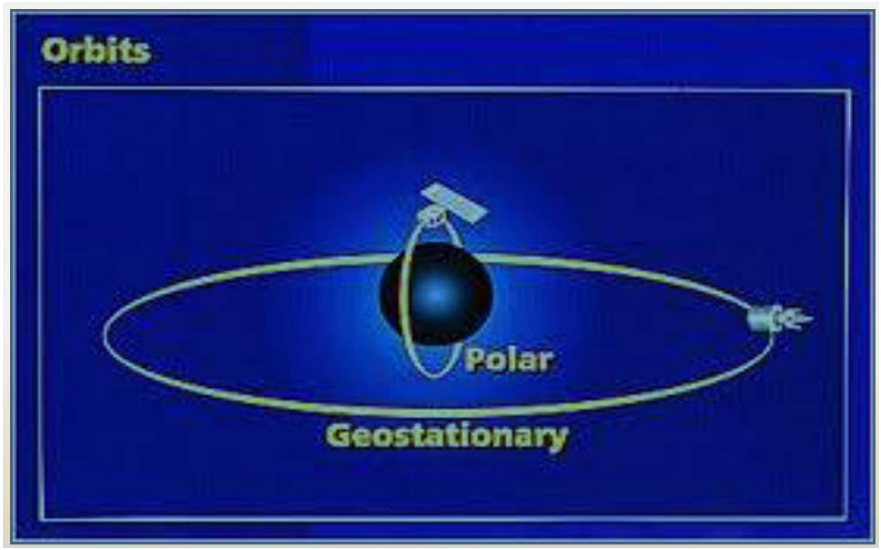


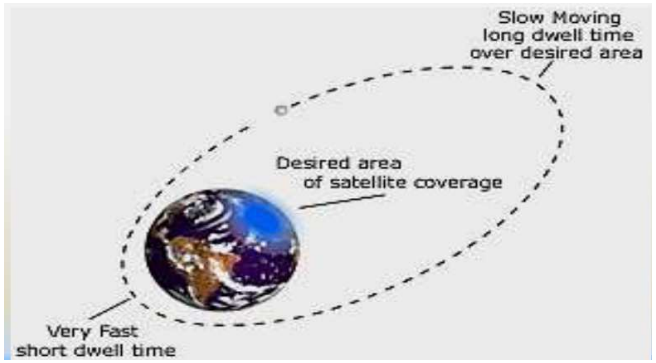


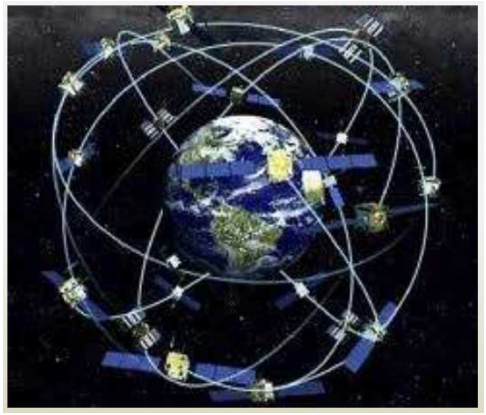
1.2 – Systèmes Spatiaux => Orbites

Orbites LEO / MEO / HEO



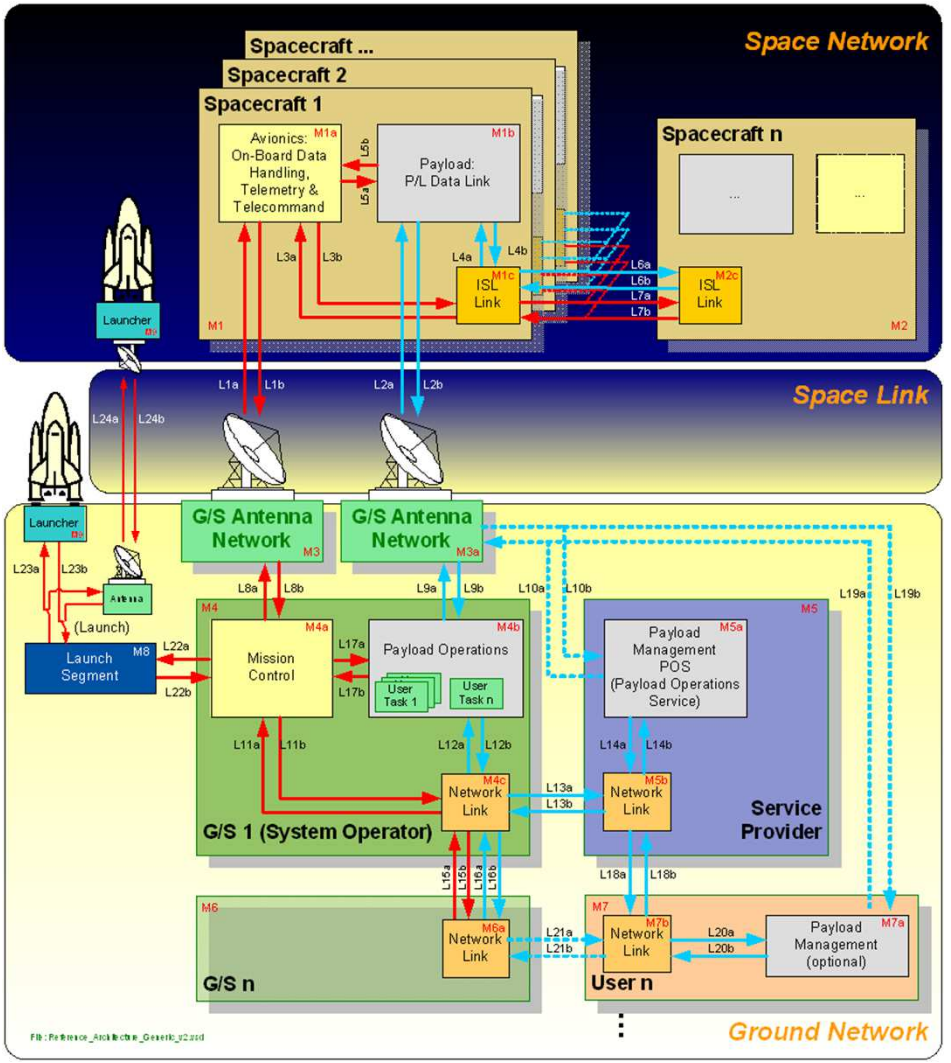






1.3 – Configuration Générale des Systèmes Spatiaux

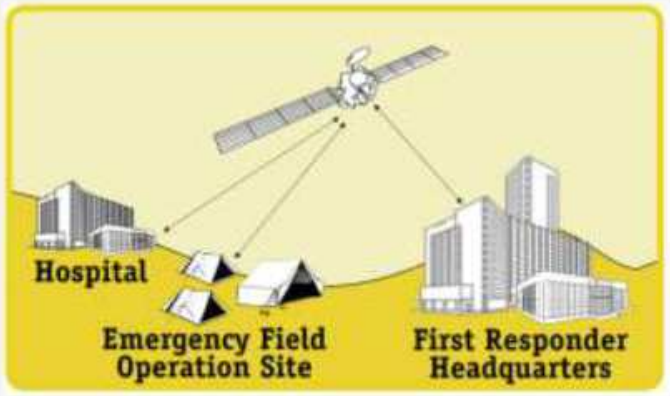
- Segments Sol
  - Segment Sol de Contrôle
  - Segment Sol de Mission
  - Segment Sol Utilisateur
- Segment Spatial
  - Satellite(s)
- Segment Lanceur
  - Ex: Fusée Ariane5, SpaceX, Proton



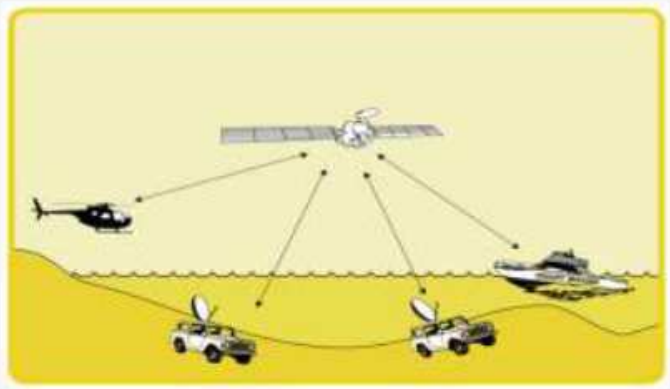
1.4 – Missions Télécommunications

Capacité des Communications par Satellites

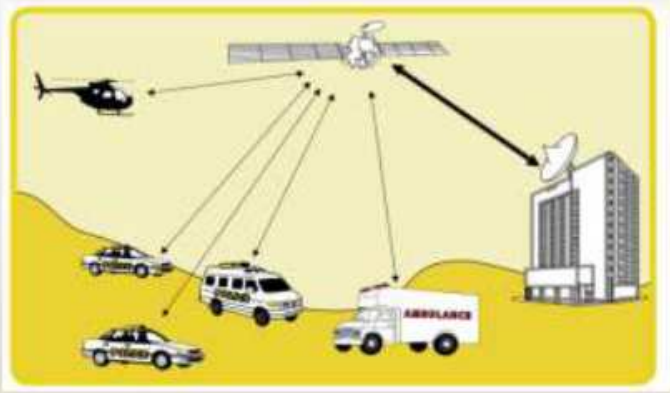
- FIXED-TO-FIXED



- Mobile to mobile



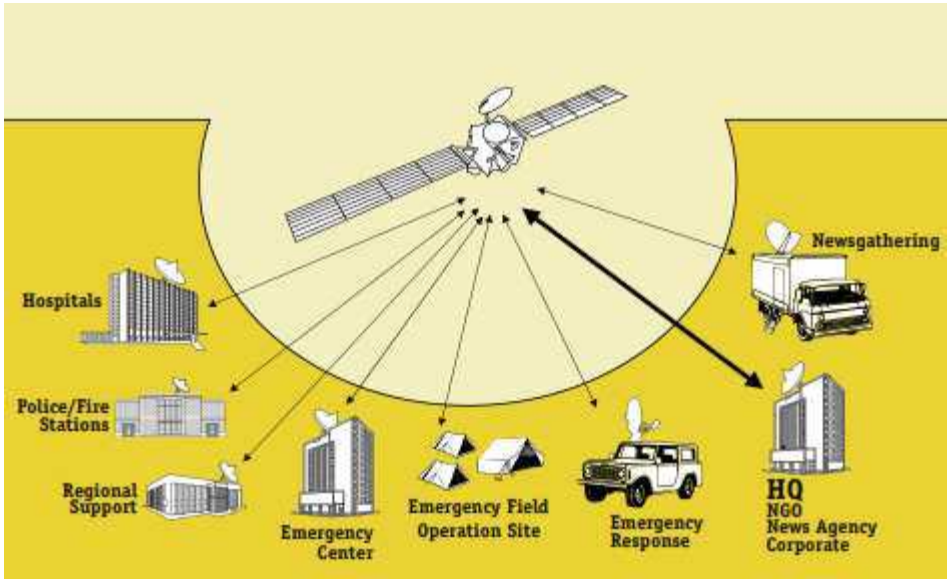
FIXED-TO-MOBILE

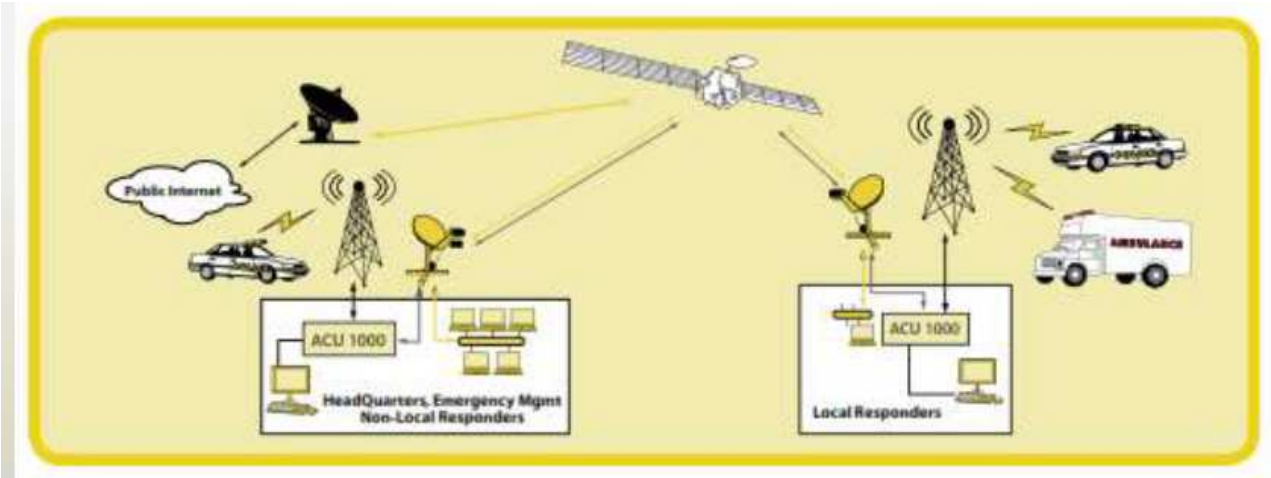


POINT-TO-MULTIPOINT

1.4 – Missions Télécommunications

- Communications fixes par Satellites (GEO) : Audio / Vidéo / Données





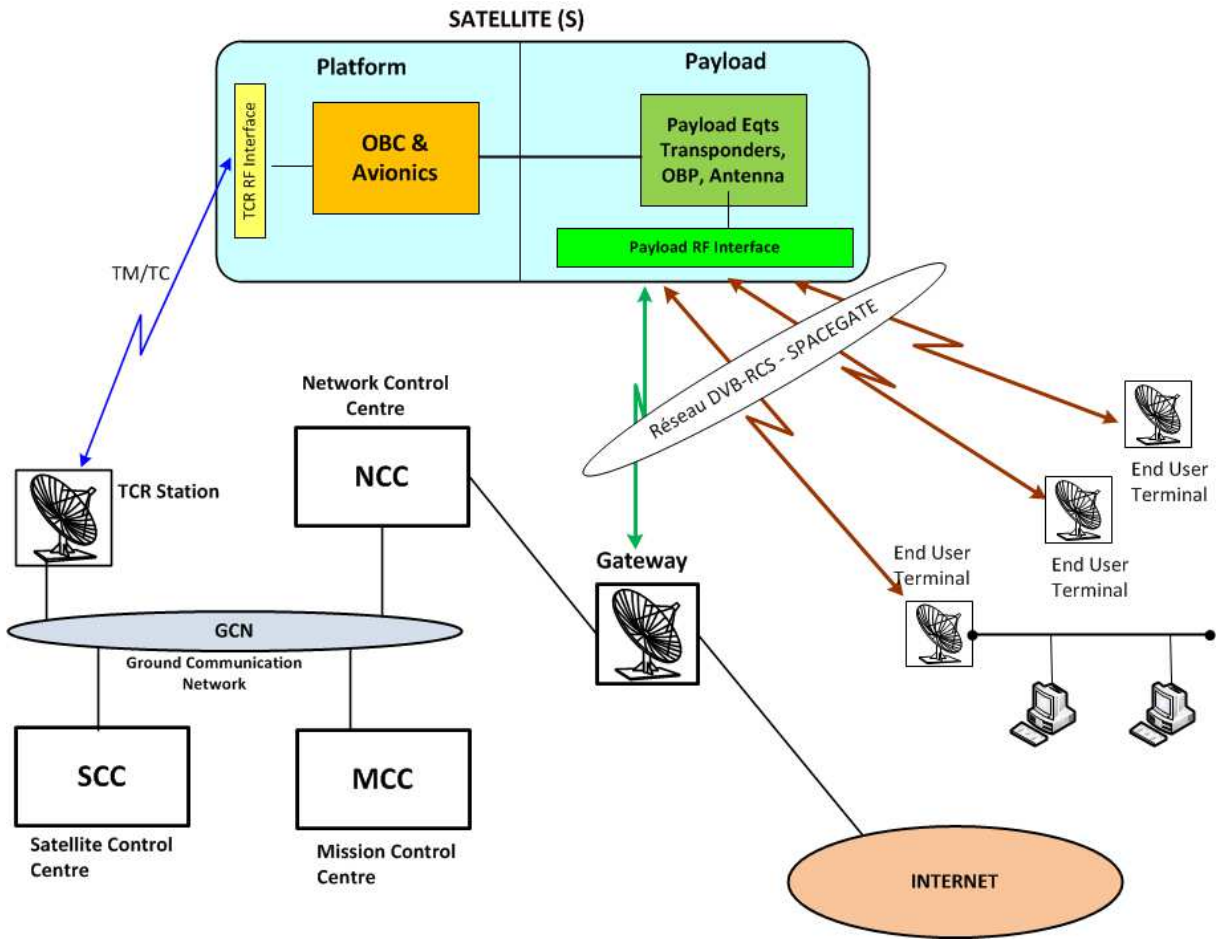
1.4 – Missions Télécommunications

Communications mobiles par Satellites (LEO/MEO) : IRIDIUM

- Constellation MEO
- 6 * plans de 11 satellites

1.4 – Missions Télécommunications

Exemple de Configuration de Mission Télécommunication (1/2)



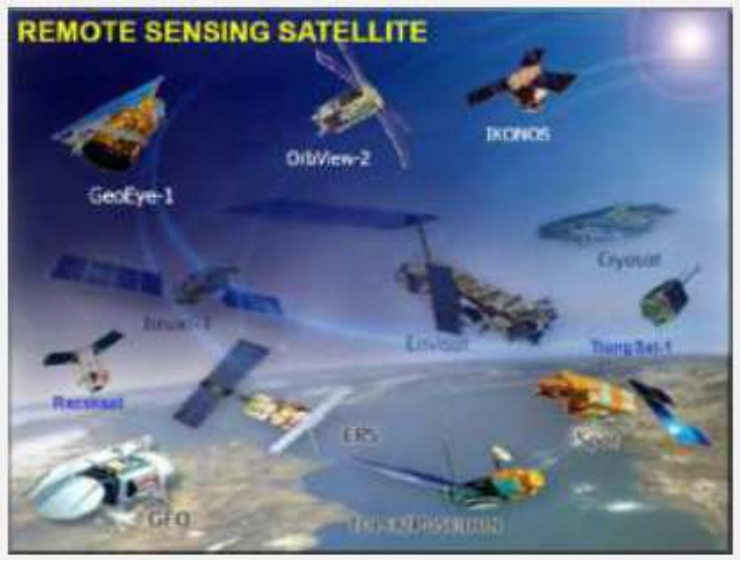
1.4 – Missions Télécommunications

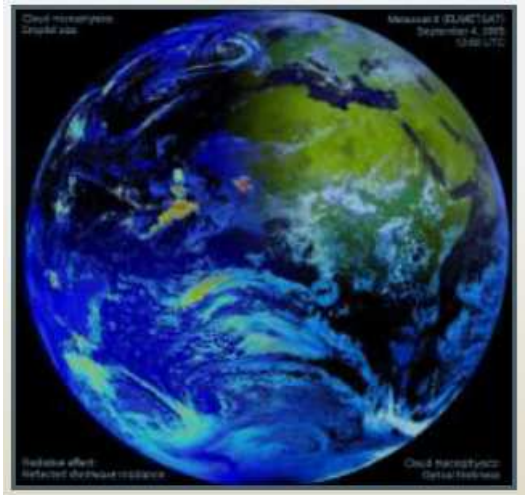
Exemple de Configuration de Mission Télécommunication (2/2)

- SCC : en charge du contrôle et monitoring du satellite (maintien à poste)
- Station TCR (Telemetry Command Ranging) :
  - Assure l'interface Radio-Fréquence (RF) entre le SCC et le satellite
  - Gère les liaisons TC (Télécommande/montante), TM (Télémesure/descendante) et assure la fonction mesure de distance (Ranging) pour la localisation du satellite.
- MCC : gère la mission (Charge utile) du satellite
- NCC : gère le Segment Sol Utilisateur (SSU) et en particulier les Stations Gateways et ressources RF associées
- Terminaux : équipement des Utilisateurs finaux et assurant l'accès au service fourni par l'Opérateur satellite
  - Ex: Récepteur TV numérique / DVB, Accès à Internet via les Gateways ou Interconnexion de sites

1.5 – Missions Observation

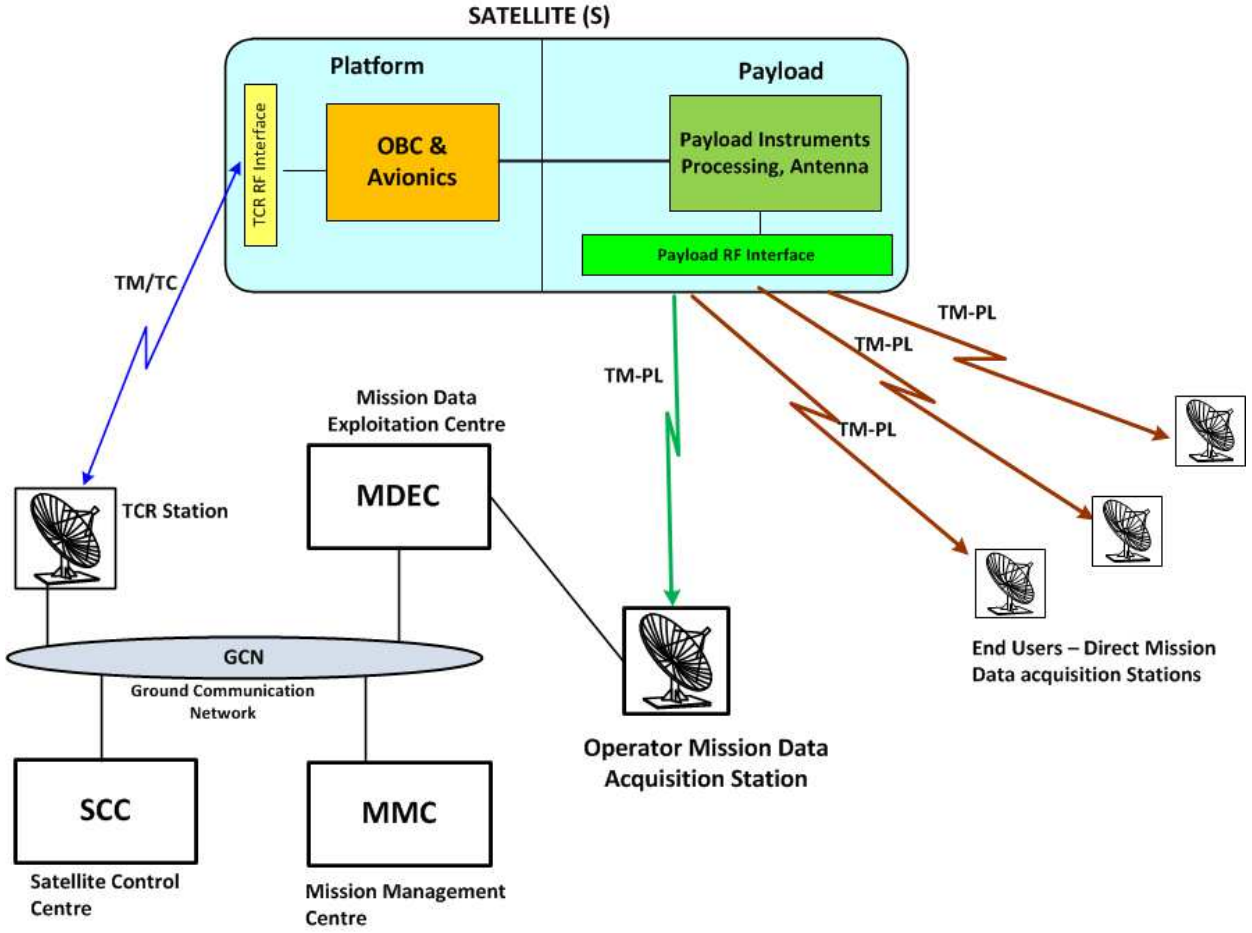
- Exemple : Imagerie – Application Environnement, Surveillande, Google Earth





1.5 – Missions Observation

Exemple de Configuration de Mission Observation (1/2)



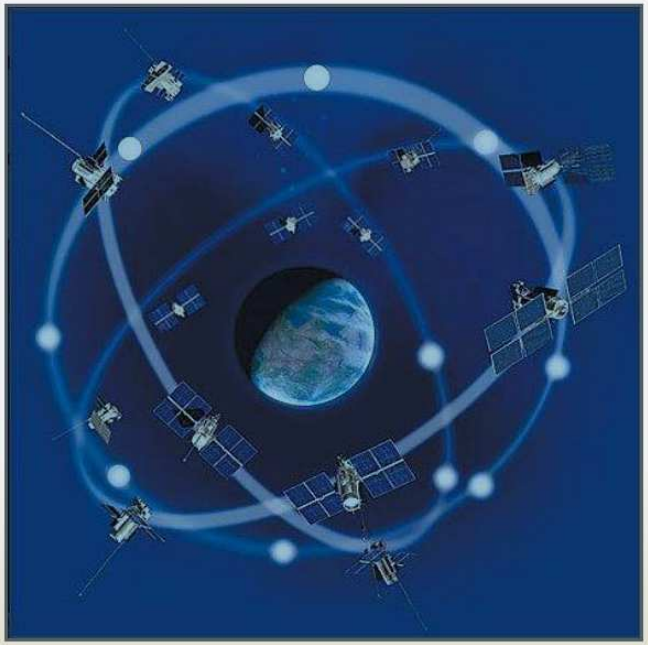
1.5 – Missions Observation

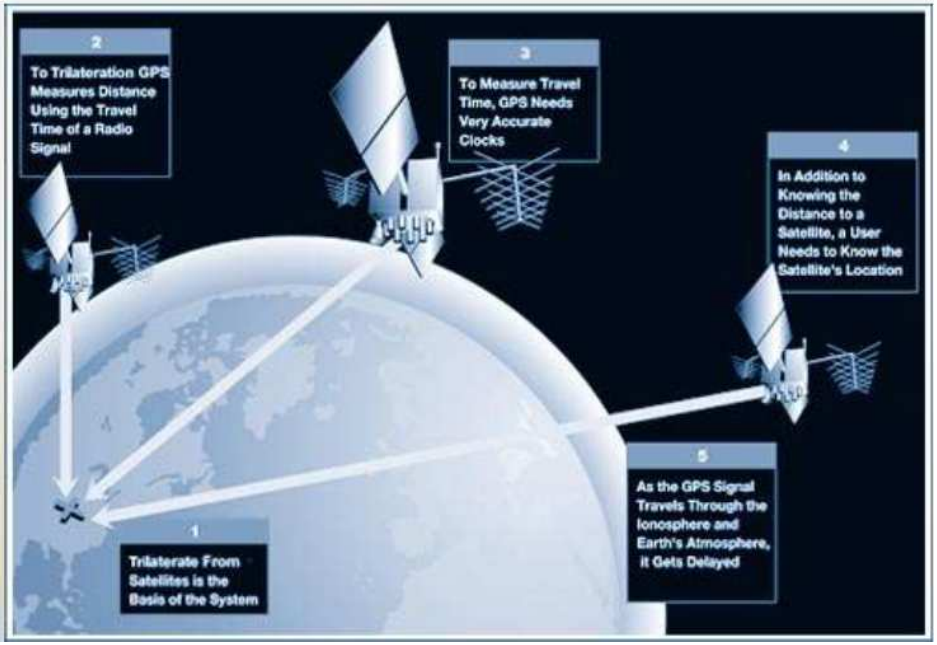
Exemple de Configuration de Mission Observation (2/2)

- SCC : en charge du contrôle et monitoring du satellite (maintien à poste)
- Station TCR (Telemetry Command Ranging) : idem Mission Telecom
  - Acces RF au satellite (liaison TM/TC) et ranging (localisation)
- MMC : assure la plannification de la Mission
  - Réception des démandes des Utilisateurs (ex: images / prises de vue)
  - Generation des plans de travail de la Charge utile du satellite (Instrument)
- MDEC : recoit les données instruments via la station d'acquisition dédiée de l'opérateur satellite , et génère les produits (ex: images) commandés par les Clients (acces indirect aux données Instruments bord)
- Stations d'acquisition des Utilisateurs : équipement des Utilisateurs finaux et assurant l'accès direct aux données instruments du satellite

1.6 – Missions Navigation=> Constellation GPS

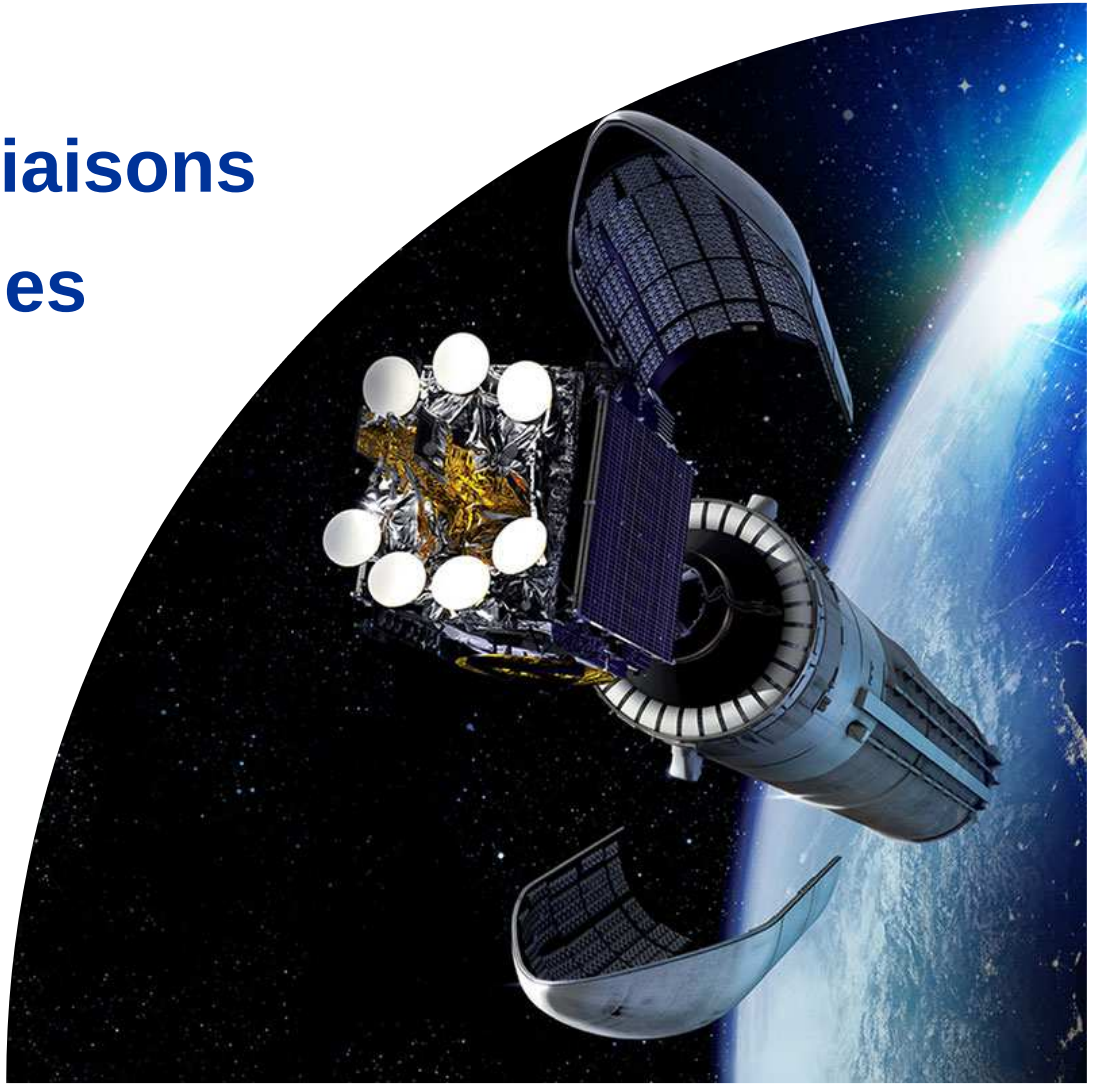
- Constellation de 24 satellites Global Positioning System
- Sol : un récepteur GPS recoit des signaux de 3 à 4 satellites pour déterminer sa position avec précision
  - Information : Longitude, Lattitude, Altitude, Temps





TLS-SEC – Sécurité des Communications Spatiales

2 – Définition des Liaisons de Données Spatiales



2.1 - Liaisons de Données Spatiales – Standards CCSDS

CCSDS : Consultative Committee of Space Data Systems

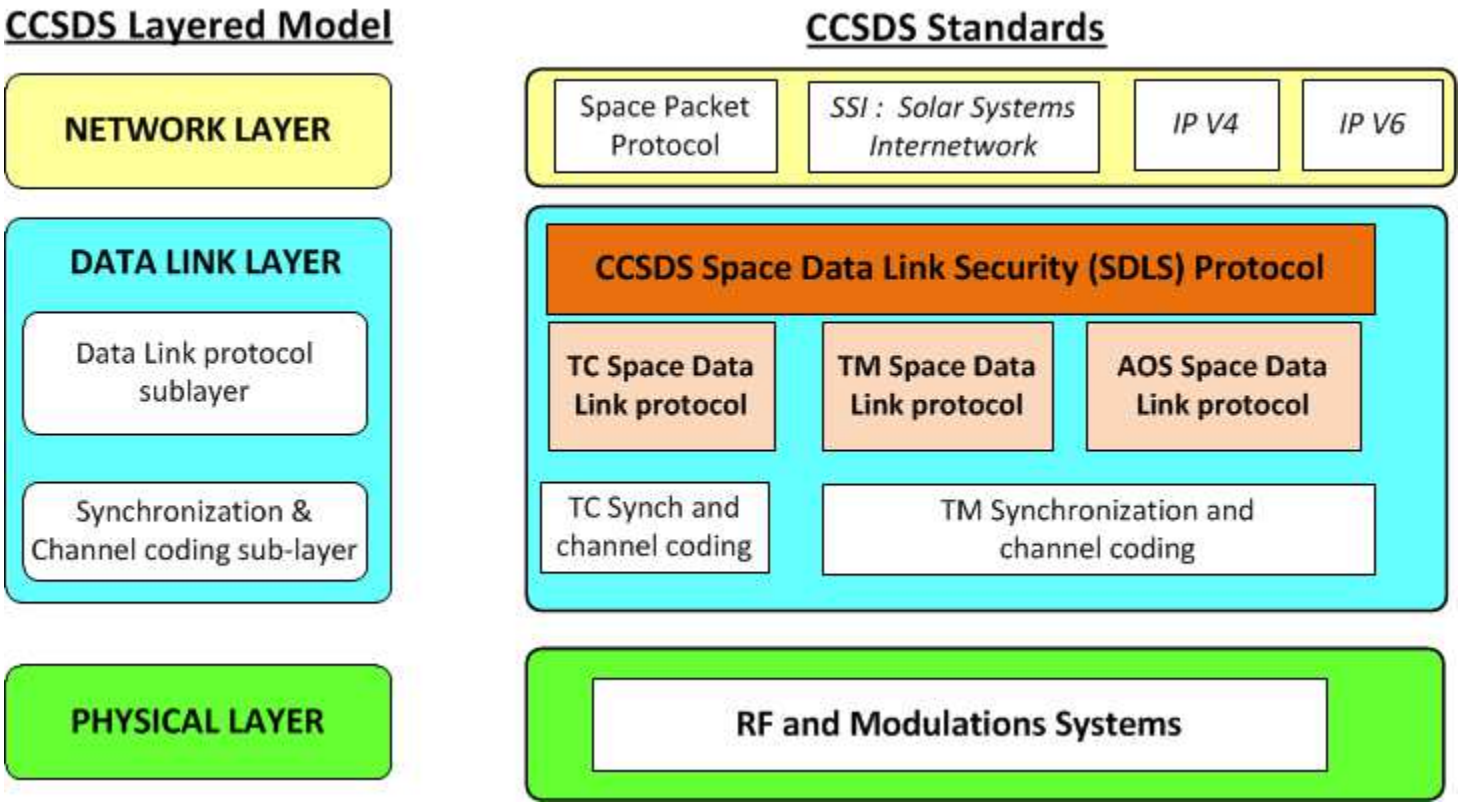
- Organisme regroupant toutes les agences spatiales et éditant les standards spatiaux
- Ex: ESA, NASA, CNES, DLR, ISRO, JAXA, ROSCOSMOS

Principaux standards CCSDS relatifs aux liaisons spatiales : TC, TM, AOS

- TC Space Data Link Protocol : CCSDS 232.0-B-1
- TM Space Data Link Protocol : CCSDS 132.0-B-1
- Advanced Orbiting Systems (AOS) Data Link Protocol : CCSDS 732.0-B-2
- Space Data Link Security Protocol (SDLS) : 355.0-B-1
  - Standard Sécurité COMSEC pour data links TC / TM / AOS
  - Issue 1 sortie en Sept 2015

2.1 - Liaisons de Données Spatiales – Standards CCSDS

Standards CCSDS – Modèles en couches => 3 couches

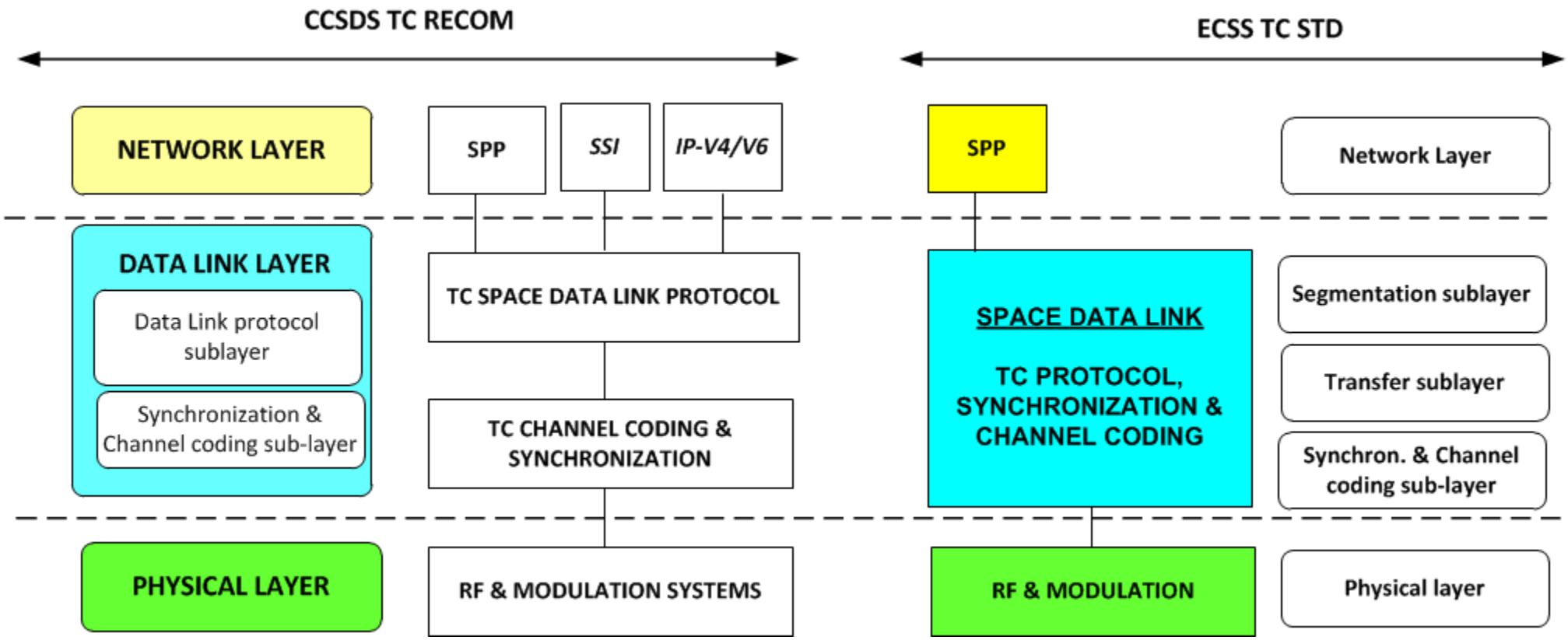


2.2 - Liaisons de Données Spatiales – Standards ECSS

- ECSS: European Cooperation for Space Standardization
- Standards Européens dérivés des standards CCSDS
- Standards ECSS soutenus par l'ESA et l'industrie spatiale européenne
- Principaux standards ECSS relatifs aux liaisons spatiales : TC, TM
  - ECSS TC Space data link standard
    - ECSS-E-ST-50-04C - Telecommand protocols synchronization & channel coding
  - ECSS TM Space data link standard
    - ECSS-E-ST-50-03C - Space data links – Telemetry transfer frame protocol
    - ECSS-E-ST-50-01 - Space Engineering – Telemetry synchronization & channel coding

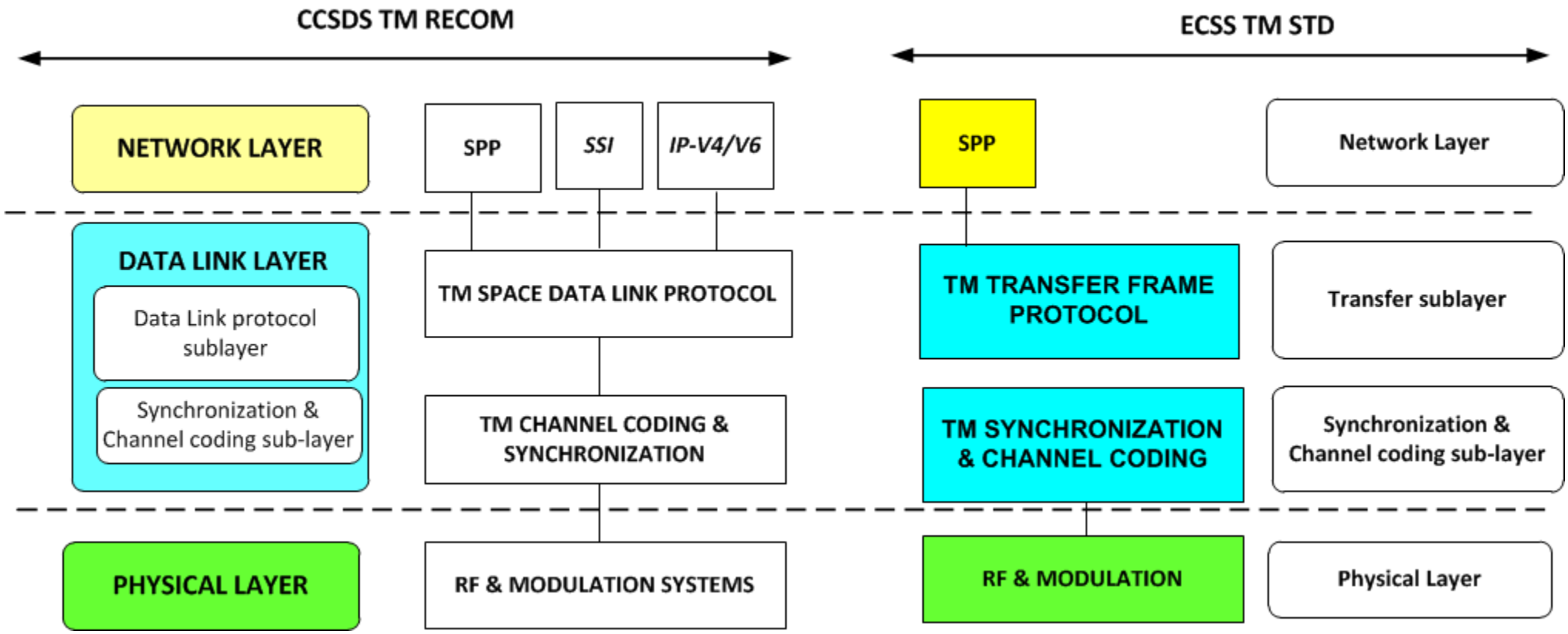
2.2 - Liaisons de Données Spatiales – Standards ECSS

Standards CCSDS vs Standards ECSS : Liaison TC



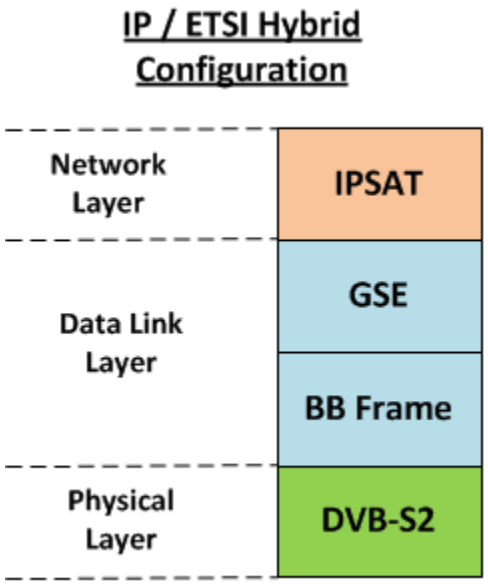
2.2 - Liaisons de Données Spatiales – Standards ECSS

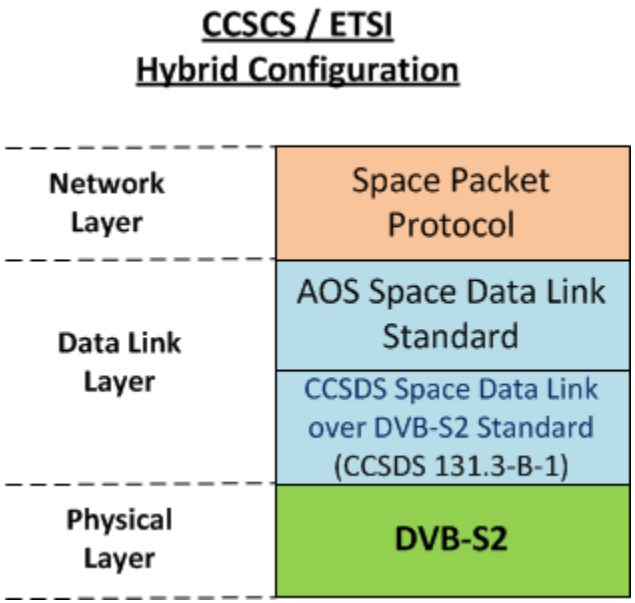
Standards CCSDS vs Standards ECSS : Liaison TM



2.3 - Liaisons de Données Spatiales – Autres Standards: ETSI/IETF

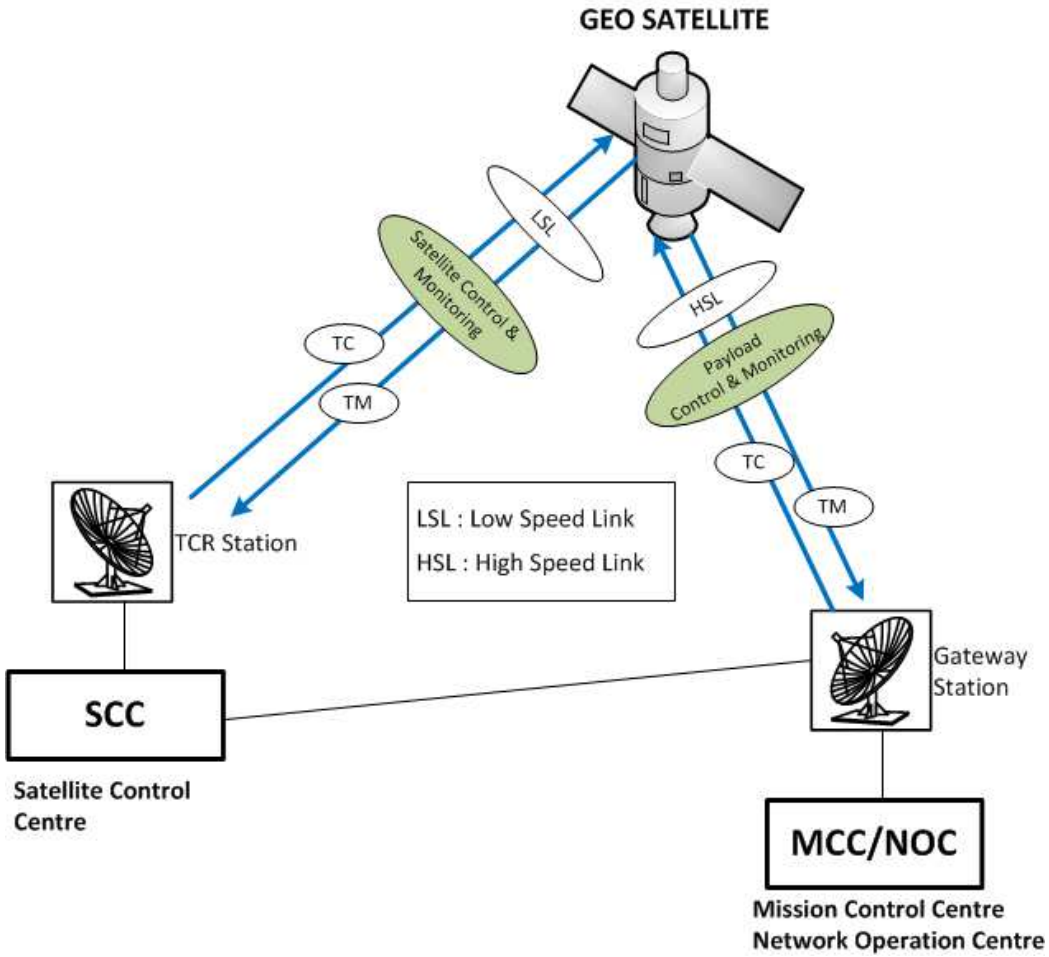
- D'autres standards non spécifiquement CCSDS ou spatiaux sont utilisés
  - Standards Europeens ETSI pour les Télécommunications
  - Standards issus de l'Internet (RFC / IETF)





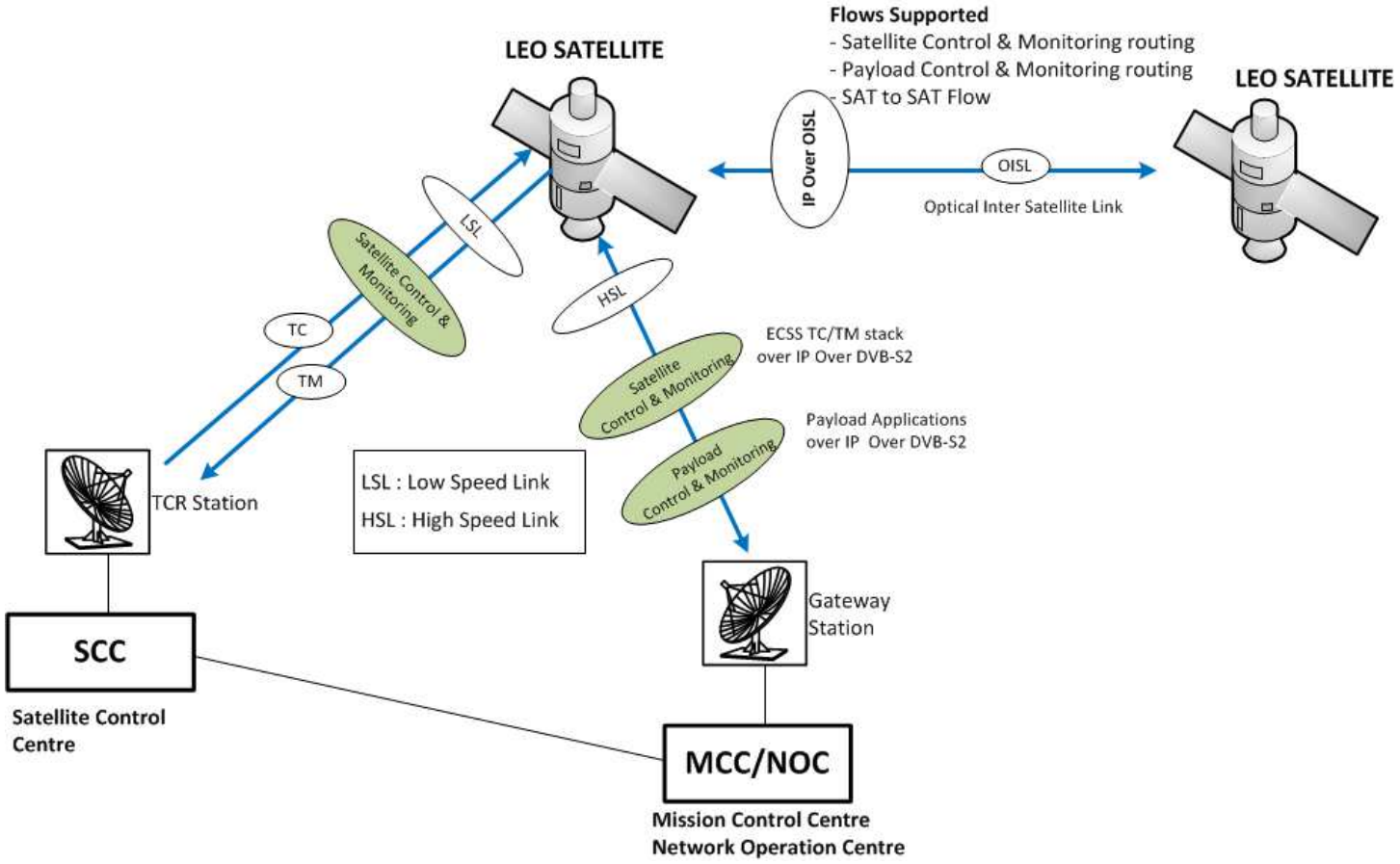
2.4 - Domaines d'application des standards de liaison de données spatiales

- Mission Télécom avec satellite GEO
- Utilisation des standards CCSDS/ECSS



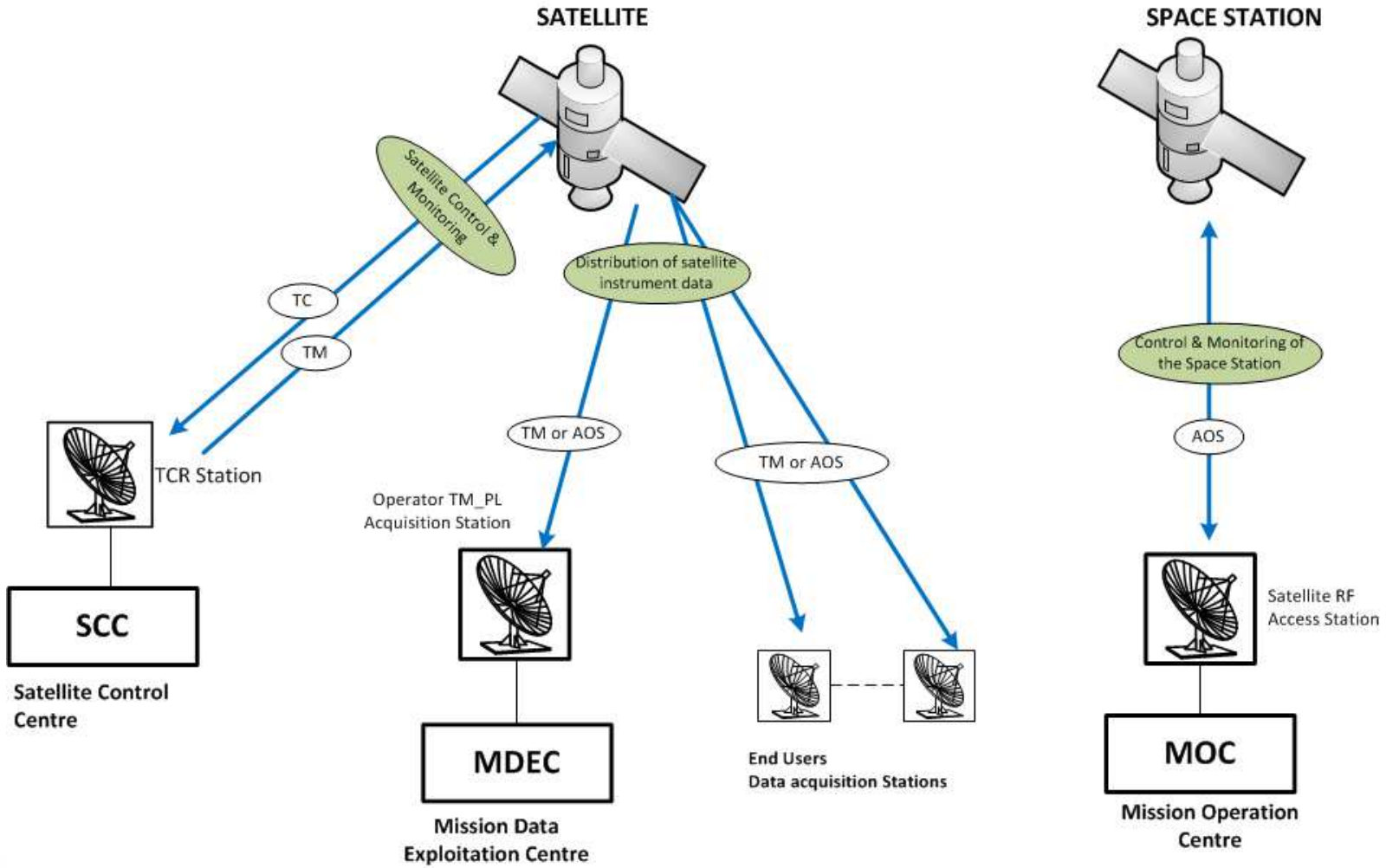
2.4 - Domaines d'application des standards de liaison de données spatiales

- Mission Télécom avec Constellation + Liens inter-satellite
- Configuration Hybride : CCSDS / ETSI / IP



2.4 - Domaines d'application des standards de liaison de données spatiales

- Mission 3 : Observation avec satellite LEO
- Mission 4 : Station Spatiale Européenne (ISS)



2.5 - Caractéristiques des liaisons de données spatiales

Standard TC (Télécommande)

- Liaison montante dédiée au contrôle du satellite / charge utile
- Flux de données asynchrone et bas débit (< 100 kb/s) et haut débit (1 Mb/s)
- Associée à un protocole COP-1 assurant le séquencement et la retransmission des TC (Sequenced Controlled Service)

Standard TM (Télémesure)

- Liaison descendante
- Flux de données continu – liaison synchrone
- Utilisée pour le monitoring du satellite / charge utile: Flux TM-HK (Télémesure de servitude)
  - Flux bas débit (< 100 kbs) à haut débit (10 Mb/s)
- Standard utilisé également pour le transport des données Instruments : Flux TM-PL pour les satellites Observation / Environnement / Scientifiques
  - Flux moyen débit jusqu'à très haut débit (1 Gb/s)

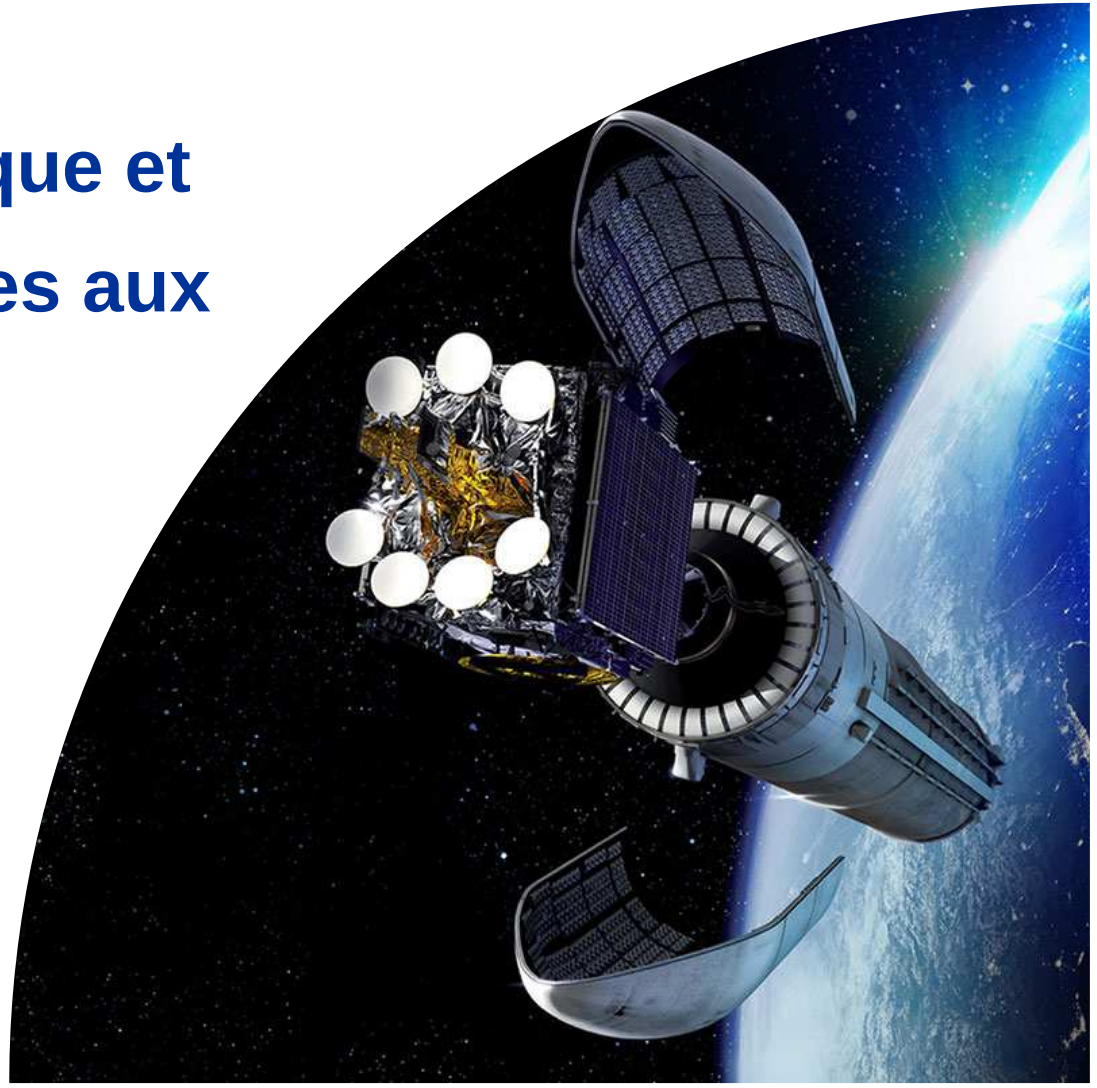
2.5 - Caractéristiques des liaisons de données spatiales

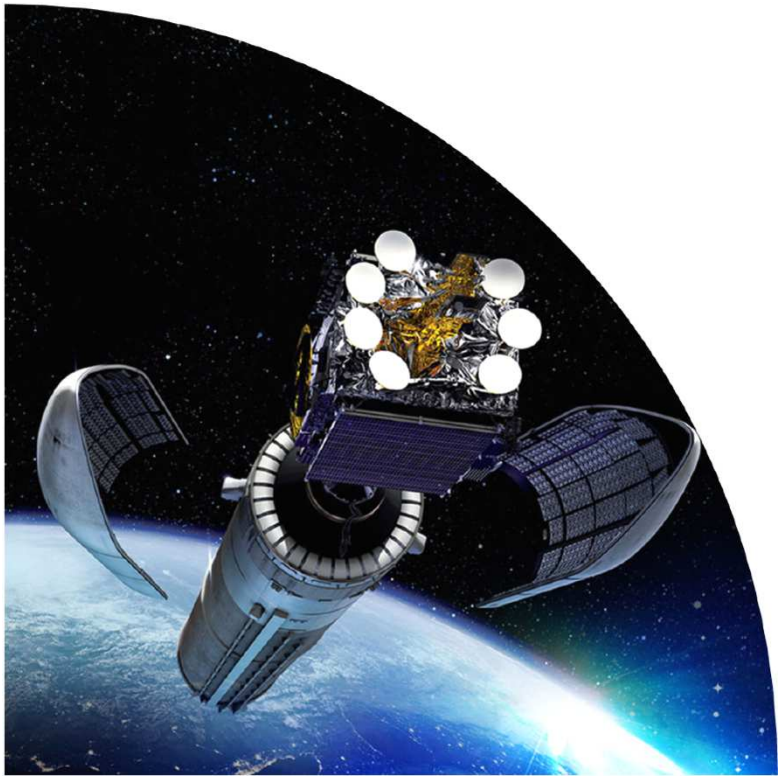
Standard AOS (Advanced Orbiting Systems)

- Couvre une liaison bidirectionnelle
- Flux multimedia : données, audio, video – liaison synchrone
- Utilisation multiple
  - Contrôle et monitoring d'une station spatiale (ex: station spatiale ISS)
  - Transport des données Instruments (liaison AOS seule) et alternative à la liaison TM pour le flux TM-PL
  - Echanges Audio / Vidéo avec équipage (ex: station spatiale ISS)

TLS-SEC – Sécurité des Communications Spatiales

3 – Analyse de Risque et Menaces applicables aux Liaisons spatiales





3.1 – Analyse de Risque et Certification Sécurité

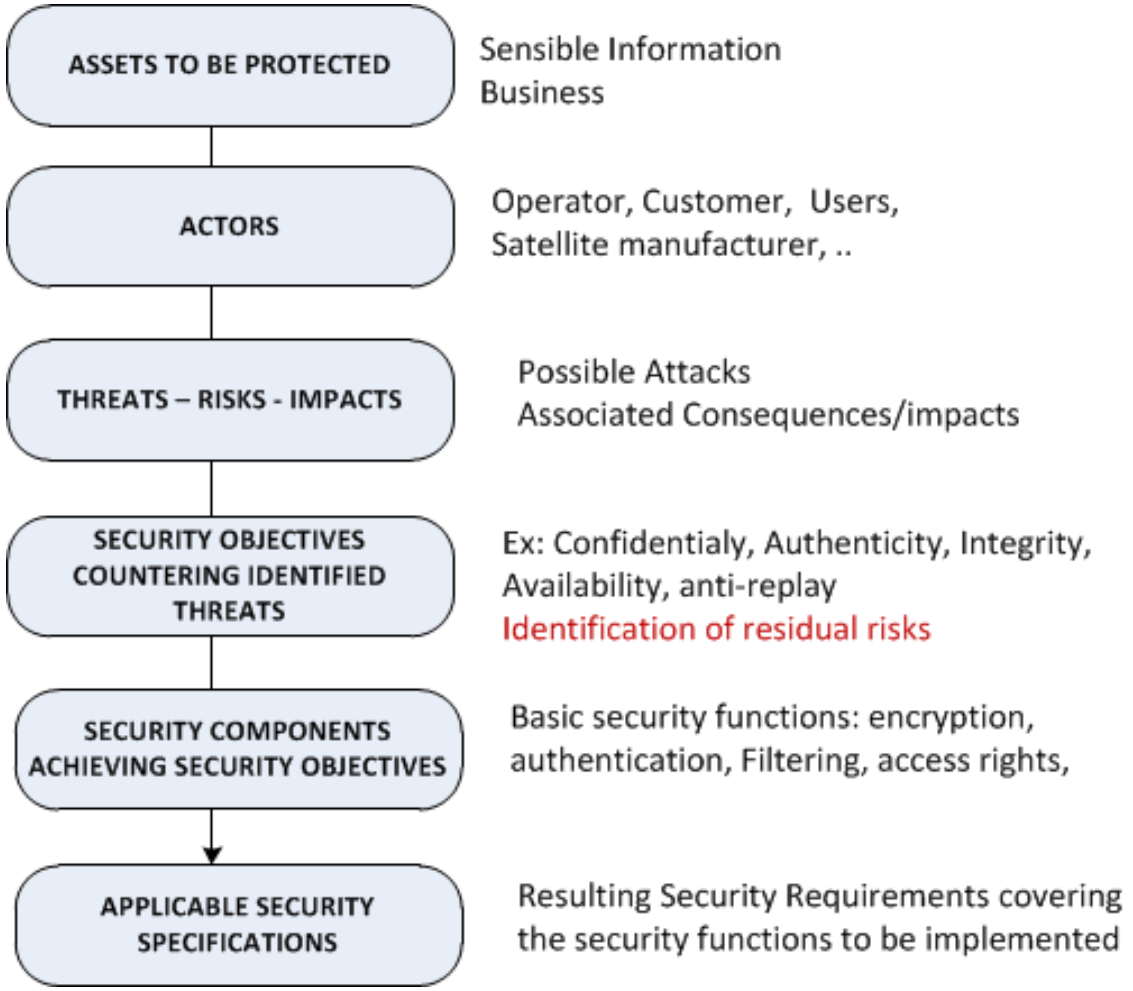
3.1- Analyse de Risques – Généralités

- L'Analyse de Risque constitue la première étape de l'activité Sécurité (pour tout système)

- Différentes méthodologies existent et peuvent être appliquées dans le spatial
  - Critères Communs
  - NIST – Risks Analysis
  - EBIOS (ANSSI) : Identification des Besoins et Identification des Objectifs de Sécurité

- La logique d'analyse de risques illustrée ci-joint est issue de la méthodologie Critères Communs

- Sortie : Exigences de Sécurité applicables au système spatial à déployer



3.1 – Analyse de Risques : Certifications CC / NIST

Certification Critères Communs (CC)

- 7 niveaux d'Assurance Sécurité : EAL (Assurance Evaluation Level)
- Evaluation par un organisme agréé dit CESTI (en France agréé par l'ANSSI)
- Pour chaque équipement, l'évaluation se fait sur la base d'un document **Cible de Sécurité (ST : Security Target)** de la fonction cible (TOE : Target of Evaluation) incluant l'ensemble des exigences de sécurité à vérifier
- Inclut des tests de vulnérabilité poussés suivant le niveau EAL
- Certains tests de vulnérabilité (Classe AVA) peuvent être destructifs

Certification NIST

- Basé sur les exigences définies dans le document NIST FIPS 140-3
- 4 niveaux d'assurance sécurité
- Evaluation par un organisme / laboratoire agréé par le NIST

3.1 – Analyse de Risques : Certifications CC / NIST

Certification Critères Communs (CC) : Méthodologie

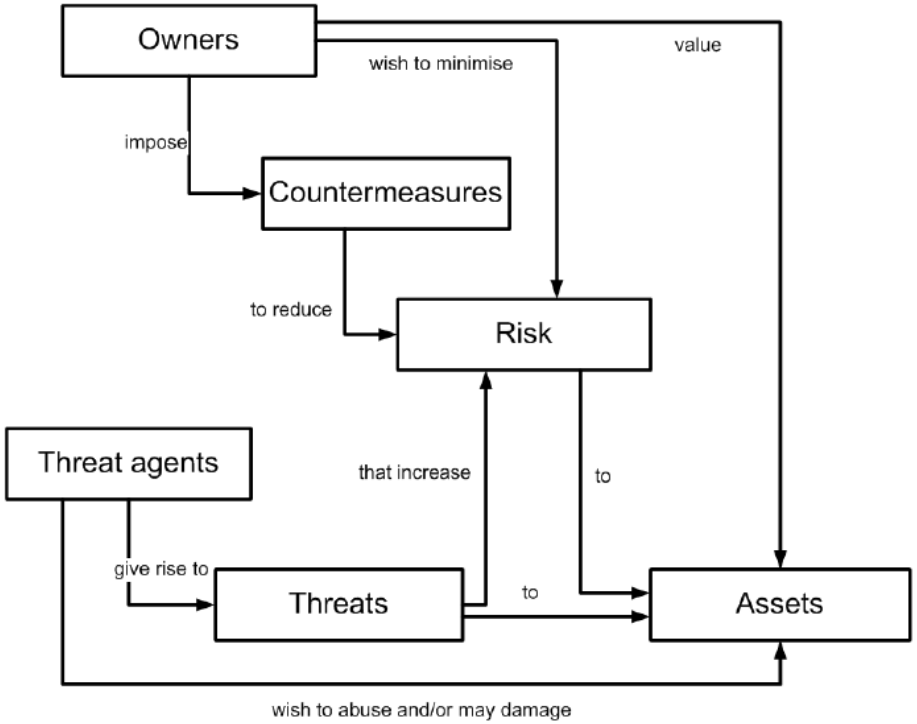


Figure 2 - Security concepts and relationships

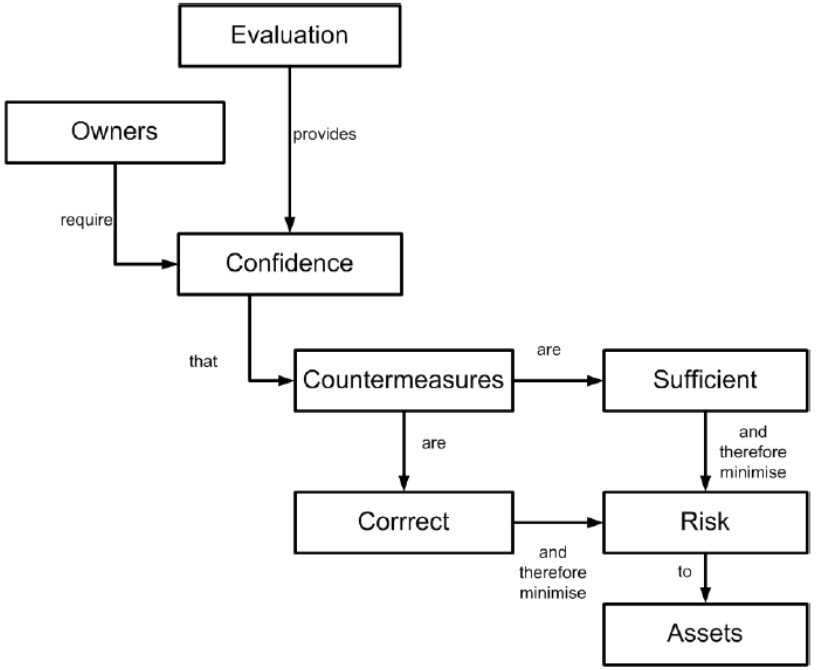
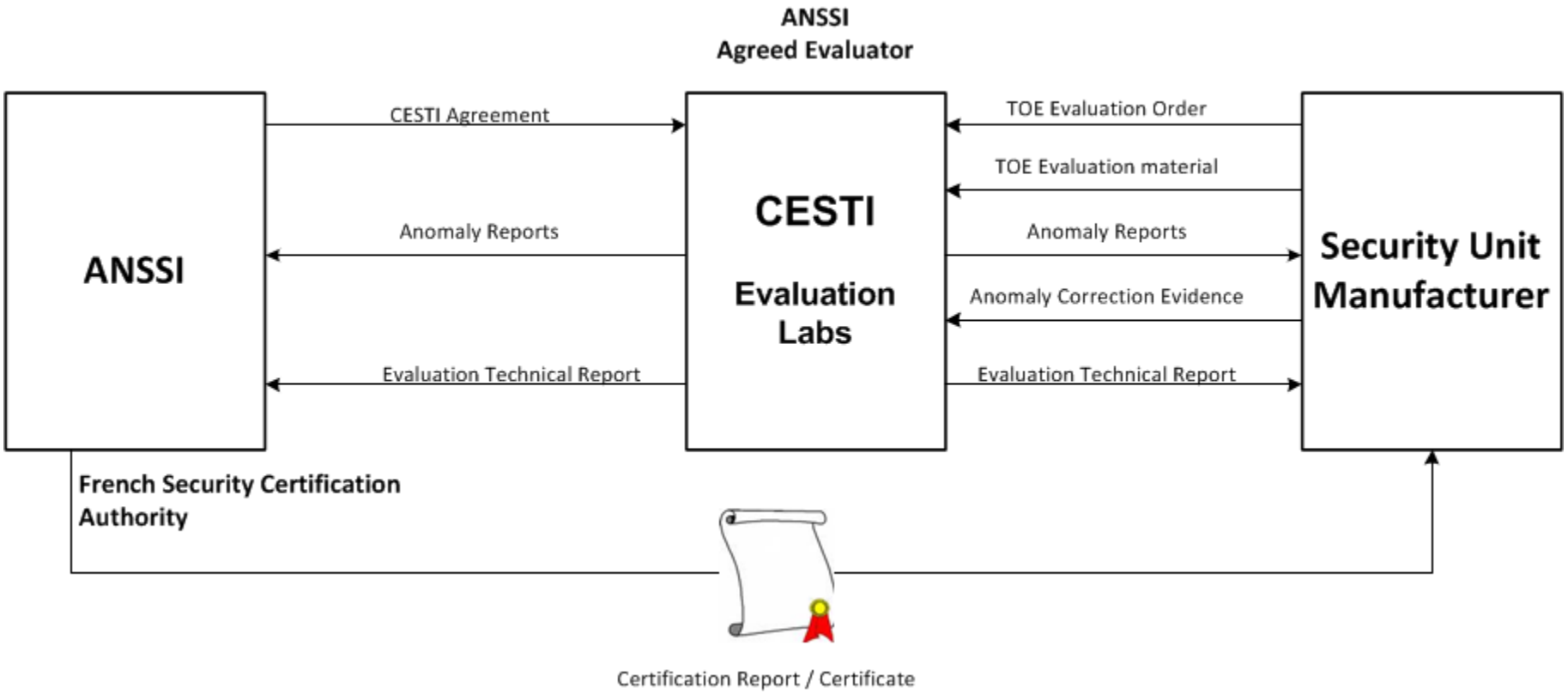


Figure 3 - Evaluation concepts and relationships

3.1 – Analyse de Risques : Certifications CC / NIST

Certification Critères Communs (CC) : Processus



3.1 – Analyse de Risques : Certifications CC / NIST

Certification Critères Communs

- Cible de Sécurité (ST Security Target)
- ST = Spécification applicable d'entrée pour l'évaluation Sécurité par le CESTI

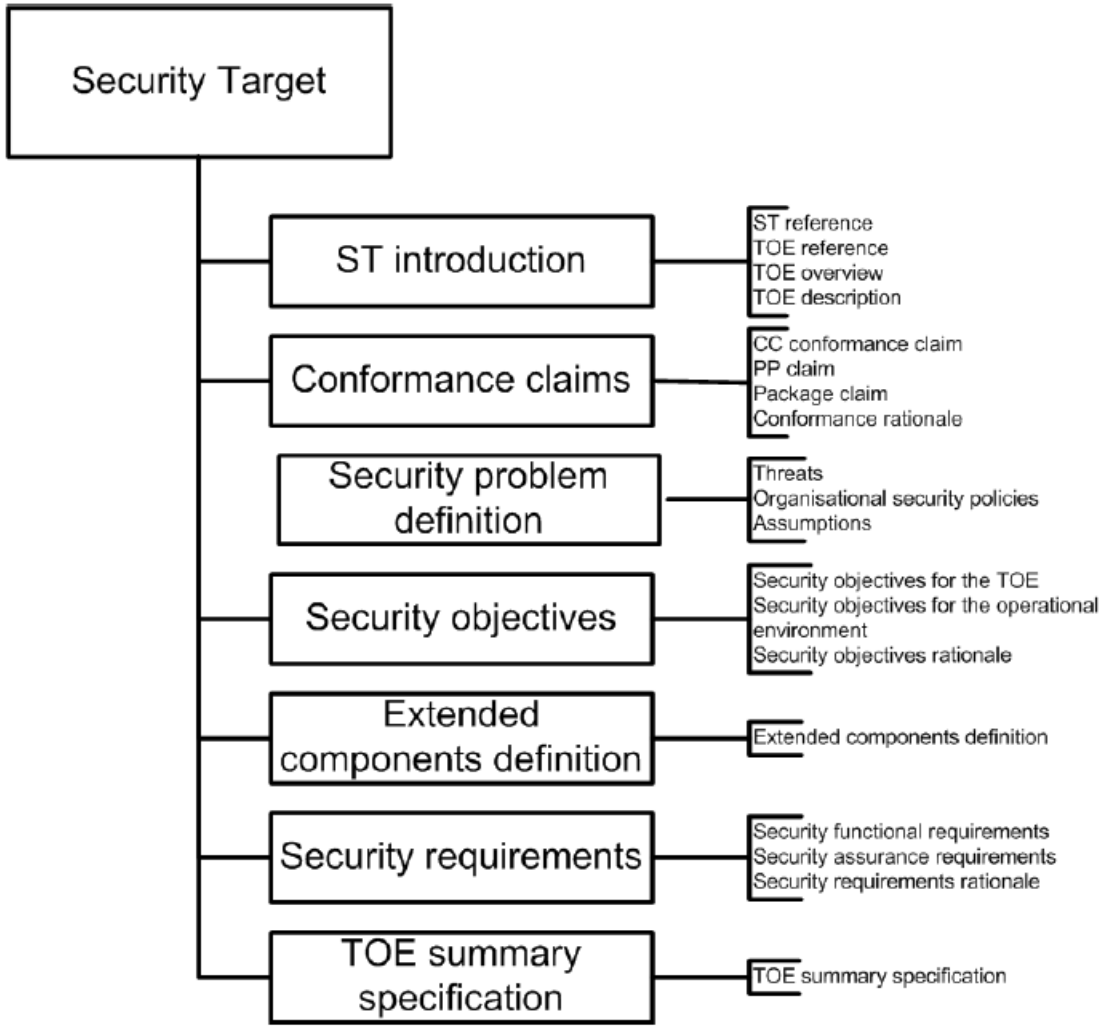
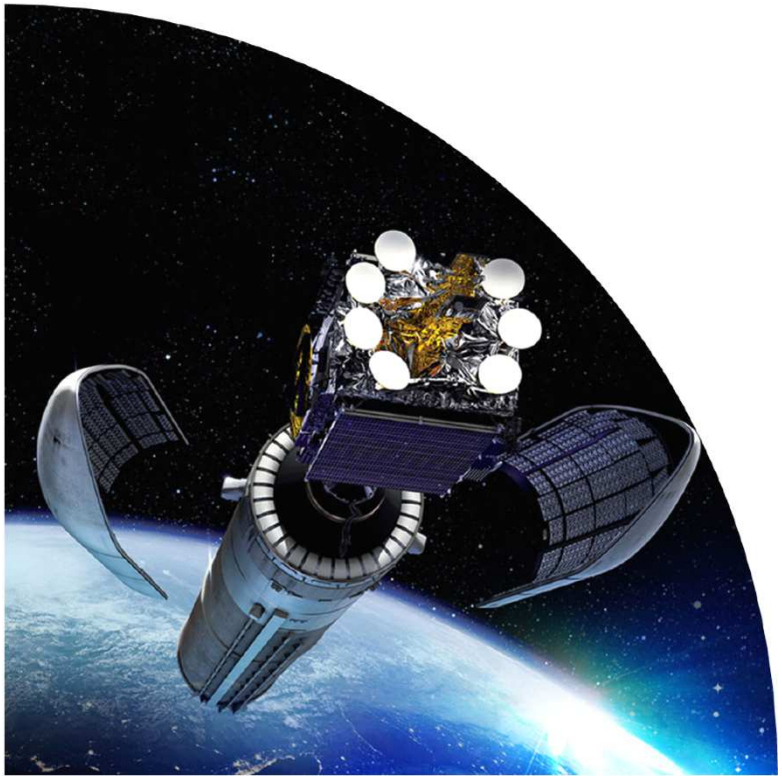


Figure 5 - Security Target contents



3.2 – Menaces Applicables aux Liaisons Spatiales

3.2 – Menaces Applicables aux Liaisons Spatiales

- Accès non autorisé à la fonction de commande (TC) du satellite
  - Intrusion active sur la liaison montante TC
  - L'intrus cherche à se faire passer pour le SCC et vise à transmettre des télécommandes au satellite
- Ecoute (Flux TC, TM-HK, TM-PL)
  - 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
  - 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)
  - L'intrus écoute la liaison TC et enregistre les commandes émises par le SCC authentique et qui sont donc valides
  - l'intrus re-émet ensuite ultérieurement les messages TC enregistrés au satellite en visant à ce qu'ils soient à nouveau acceptés par le satellite

3.2 – Menaces Applicables aux Liaisons Spatiales

Modification intentionnelle des données (Flux TC, TM-HK, TM-PL)

- 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-HK, TM-PL : L'intrus intercepte le message TM avant acquisition par le SCC ou le Centre de traitement, et modifie son contenu

Analyse de Trafic

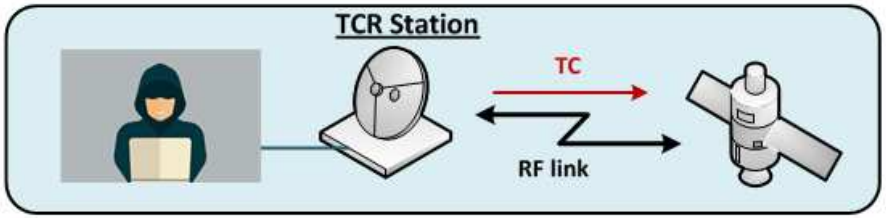
- L'intrus écoute et enregistre la ou les liaisons satellite (écoute passive)
- En analysant le contenu des messages enregistrés (header, identifiants, adresses), il peut déterminer qui est l'émetteur (ex: quel satellite ou quel SCC) et le destinataire (ex: équipement / application dans le satellite)

Brouillage RF (Flux TC)

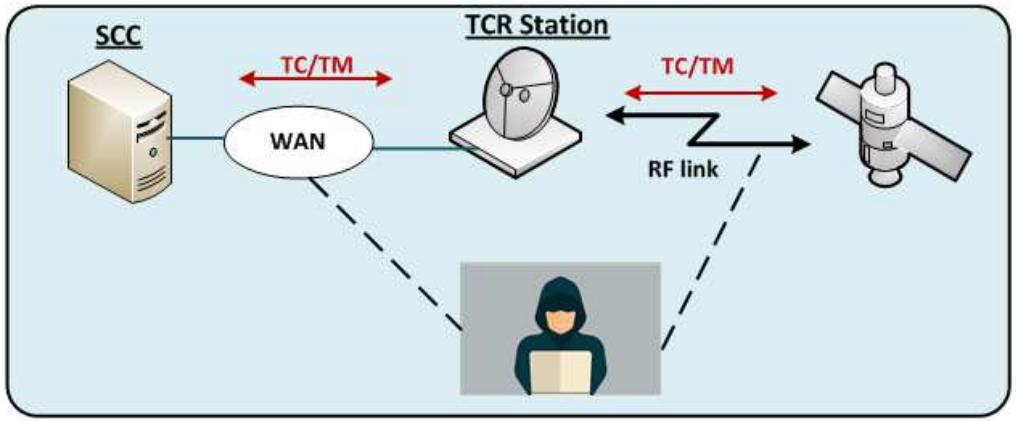
- L'intrus utilise un brouilleur RF suffisamment puissant pour rendre la liaison TC inopérante (le SCC n'arrive alors plus à transmettre de TC acceptée par le satellite)
- Menace de type **DoS** (Denial of Service) contre la disponibilité de la liaison TC

3.2 – Menaces Applicables aux Liaisons Spatiales

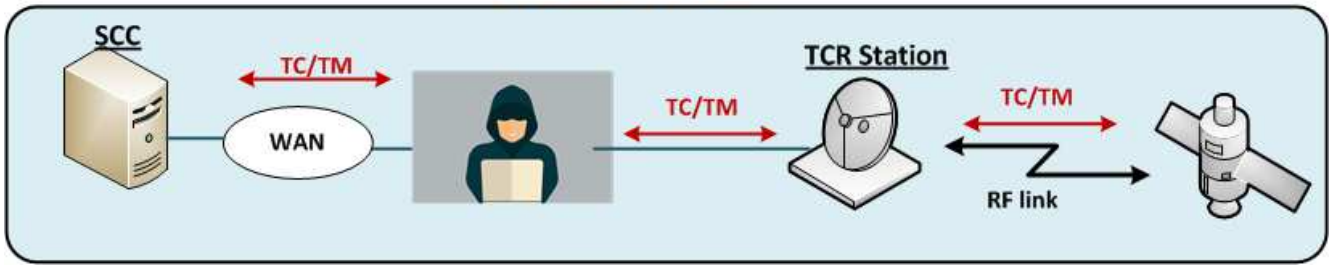
Unauthorized Access to Satellite Commanding Function



Data Interception

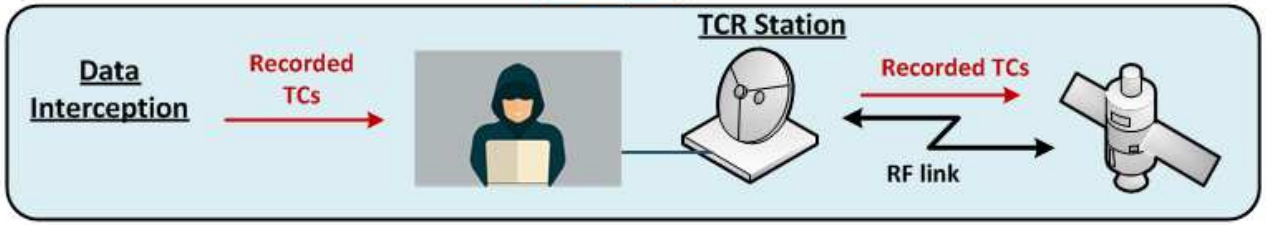


Data Modification

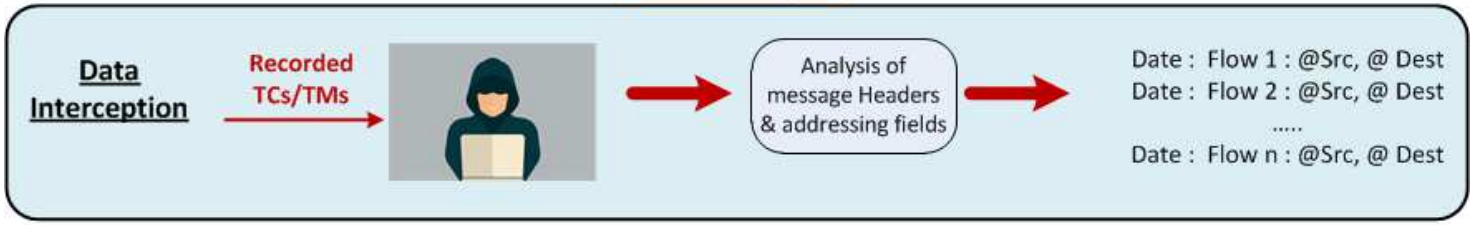


3.2 – Menaces Applicables aux Liaisons Spatiales

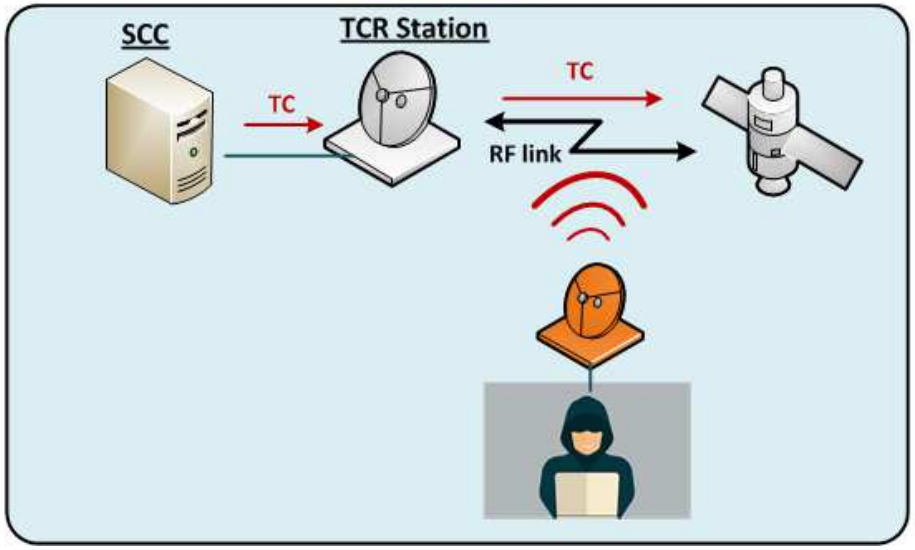
TC Replay



Traffic Analysis



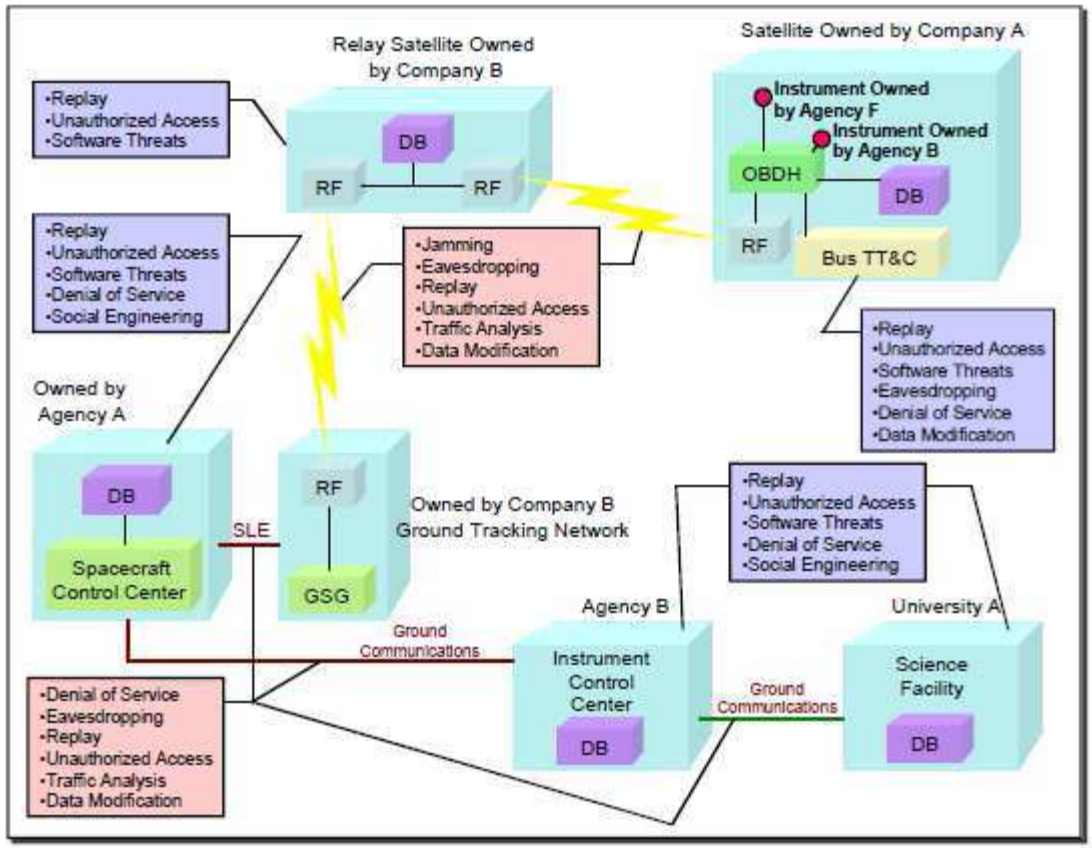
RF Jamming

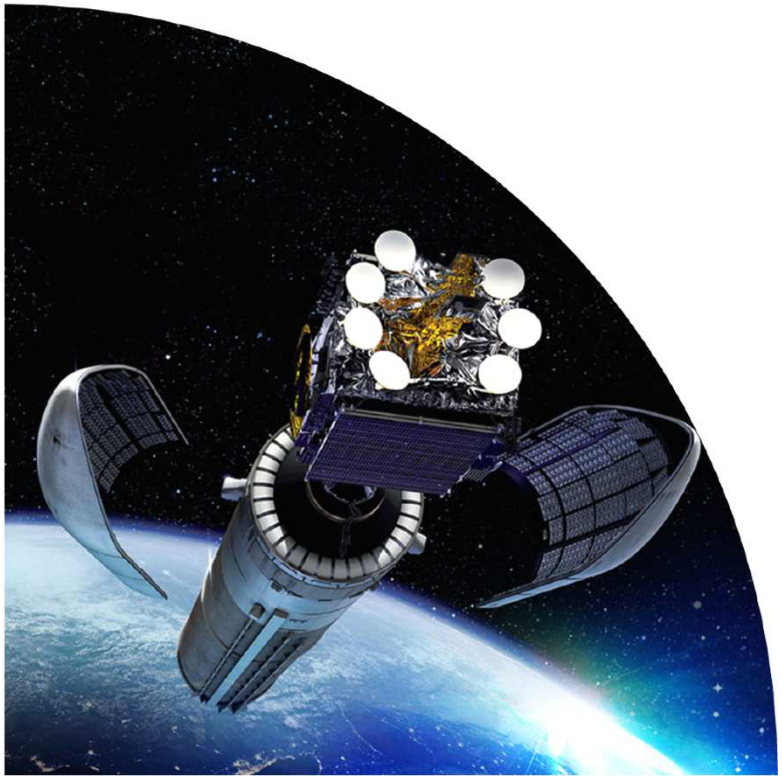


3.2 – Menaces Applicables aux Liaisons Spatiales

Principales Menaces (référence CCSDS)

- Document CCSDS 350.1-G-1 : Security Threats against Space Missions





3.3 – Cyber Sécurité et Systèmes Spatiaux

3.3 – Cyber Sécurité et Systèmes Spatiaux

- Le développement très important des attaques au sol contre les systèmes d'information utilisant des réseaux de communication divers (Internet, réseaux mobiles, ..), a conduit durant la derniere decennie à développer le concept nouveau de Cyber-Securité destiné à adresser toutes les menaces et contre-mesures associées, ainsi que la détection / supervision des systèmes à implémenter

- USA / NSA : Executive order 13636 (2013) :
  - Improving Critical Infrastructure Cybersecurity - Preliminary CyberSecurity framework- Energy, Transport, Telecommunication, Finance

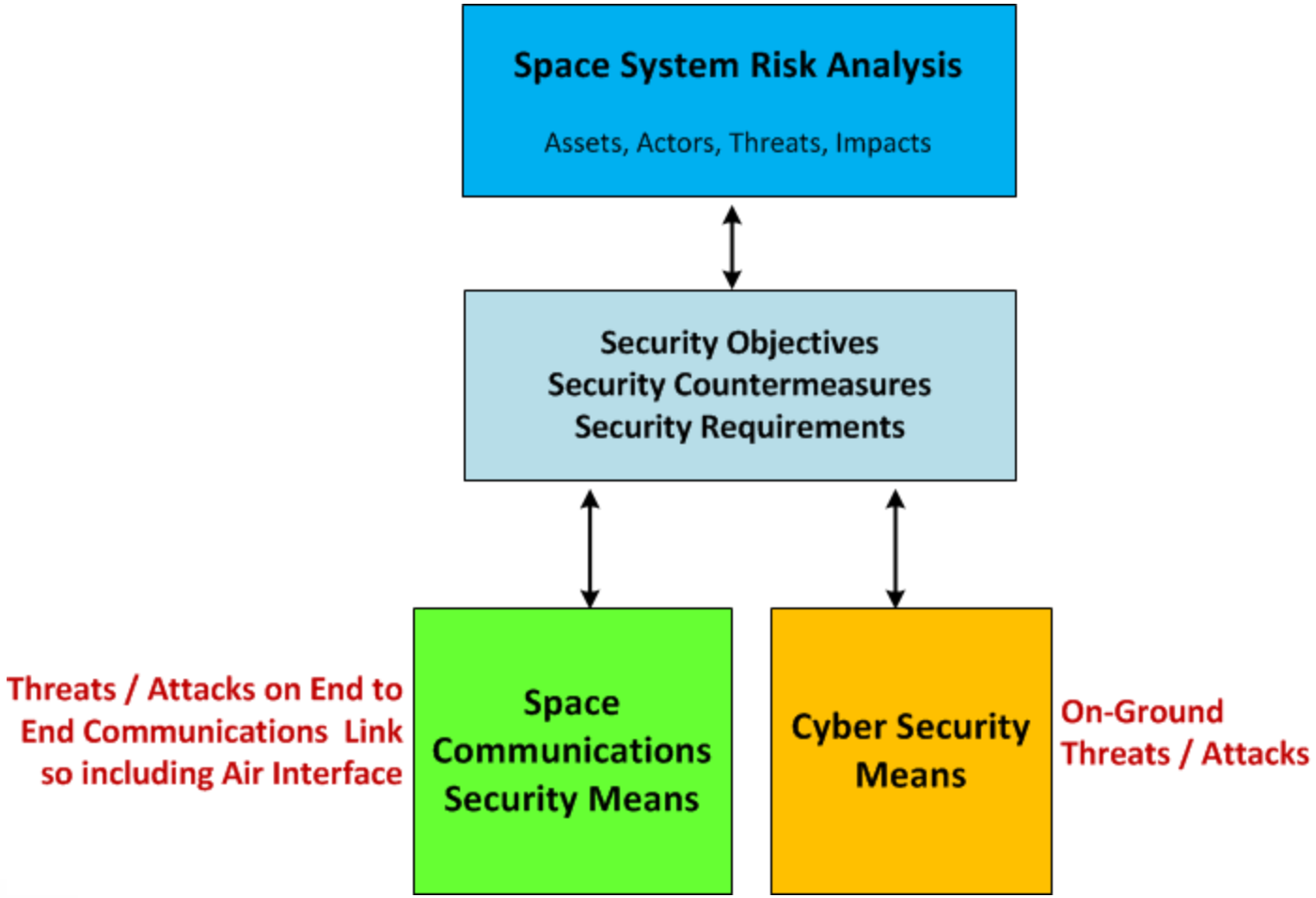
- NIST
  - NIST framework for improving critical infrastructure cybersecurity [2014]
  - NIST roadmap for improving critical infrastructure cybersecurity [2014]

- EU : Network and Information Security Directive of the 7th February 2013

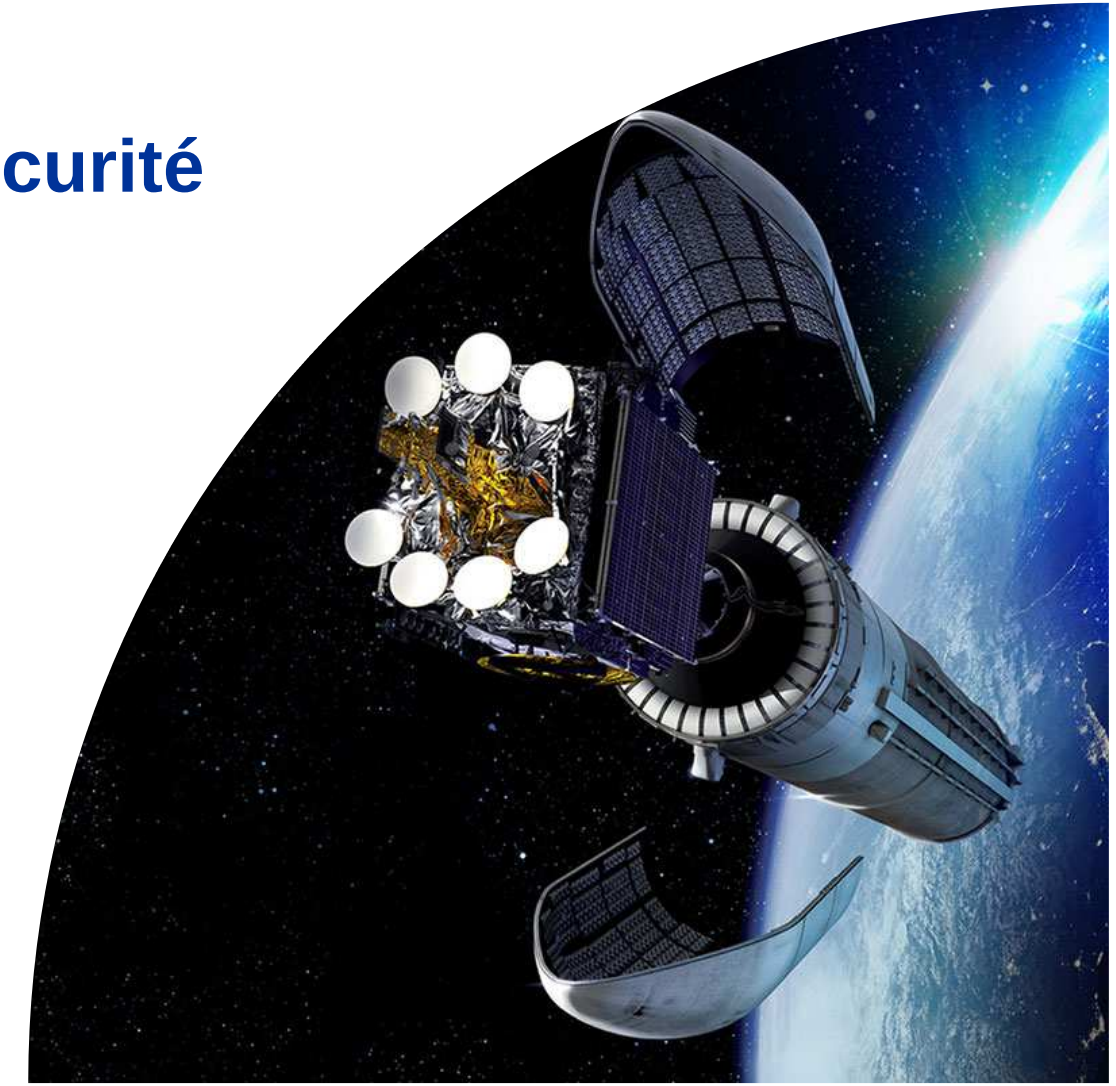
- Autres initiatives : NATO, ENISA, National (BSI, ANSSI, ..)

3.3 – Cyber Sécurité et Systèmes Spatiaux

- Rôles distincts et complémentaires de la Cyber Sécurité et de la Sécurité TCR (Sécurite bord / sol) dans un système spatial



4 – Objectifs de Sécurité Résultants



4 – Objectifs de Sécurité résultants

Liaison TC / Flux TC (Commande du Satellite)

- Authenticité de la source
  - Le satellite ne doit accepter des TCs que si l'authenticité de la source (SCC légitime) est vérifiée
- Intégrité des messages
  - Le satellite ne doit accepter des TCs que si leur intégrité (aucune modification intentionnelle ou non du message source) est vérifiée
- Anti-rejeu
  - Le satellite doit rejeter toute TC déjà transmise antérieurement
- Confidentialité des messages
  - Les données contenues dans un message TC ne doivent être accessibles qu'au satellite légitime
- Disponibilité
  - La liaison TC doit rester disponible (avec si besoin des performances réduites) même en cas d'attaque de type brouillage / DoS (Denial of Service)

4 – Objectifs de Sécurité résultants

Liaison TM / Flux TM-HK (Télémesure de Servitude)

- Authenticité de la source
  - Le SCC ne doit accepter des messages TM que si l'authenticité de la source (satellite légitime) est vérifiée
- Intégrité
  - Le SCC ne doit accepter des messages TM du satellite que si l'intégrité (aucune modification intentionnelle ou non du message source) est vérifiée
- Confidentialité
  - Les données contenues dans un message TM ne doivent être accessibles qu'au SCC légitime

Liaison TM / Flux TM-PL (Télémesure Instrument)

- Idem TM-HK entre satellite et Centre Sol d'acquisition et de traitement des données TM-PL
- Authenticité de la source
- Intégrité
- Confidentialité

4 – Objectifs de Sécurité Résultants

Flux AOS Audio / Vidéo

- Seule la Confidentialité est requise
- Authenticité / Intégrité non requis

Remarque 1: Authenticité vs Non Répudiation

- Pour les liaisons TC comme TM, l'objectif de Non Répudiation n'est pas retenu comme besoin réel, l'authenticité de la source étant considérée comme suffisant
- Ceci permet notamment pour la protection du Trafic TC / TM de s'affranchir du besoin de **signature digitale** réquérant l'utilisation de la cryptographie asymétrique (ex: DSA, RSA-PSS, ECDSA)

Remarque 2 : Protection contre l'Analyse de Trafic

- Couvert par l'objectif de Confidentialité
- Les champs d'adressage sensibles sont alors considérés comme faisant partie des données confidentielles à chiffrer

5 – Services de Sécurité Cibles

5 - Services de Sécurité Cibles

- La protection des liaisons spatiales TM/TC/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 en couches CCSDS
    - Opère sur les messages numériques transportés sur les liaisons TC/TM/AOS
    - Couvre les Services Authentification et Chiffrement
    - **Authentification** : répond aux objectifs => Authenticité , Intégrité, Anti-rejeu,
    - **Chiffrement** : répond à l'objectif => Confidentialité
  - Service de Sécurité de type TRANSEC (**TRAN**smission **SEC**urity)
    - Implémenté au niveau de la couche Physique Radio-Fréquence (Physical Link) du modèle en couches 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 TC sous certaines conditions dégradées

5 - Services de Sécurité Cibles

Services de Sécurité applicable aux liaisons spatiales

- TC-COMSEC-1 - (Flux : TC)
  - Service de sécurité implémenté : Authentification (AO : Authentication Only)
    - Protection : Authenticité , Intégrité, Anti-rejeu
    - Pas de besoin de confidentialité (missions commerciales / scientifiques)
- TC-COMSEC-2 (Flux : TC)
  - Services de Sécurité implémentés : Authentification + Chiffrement (AE : Authenticated Encryption)
    - Protection : Authenticité , Intégrité, Anti-rejeu , Confidentialité
- Note : Le service Authentification est obligatoire en TC (service minimal)
- TC TRANSEC (Flux : TC)
  - Services de Sécurité implémenté : Anti-brouillage

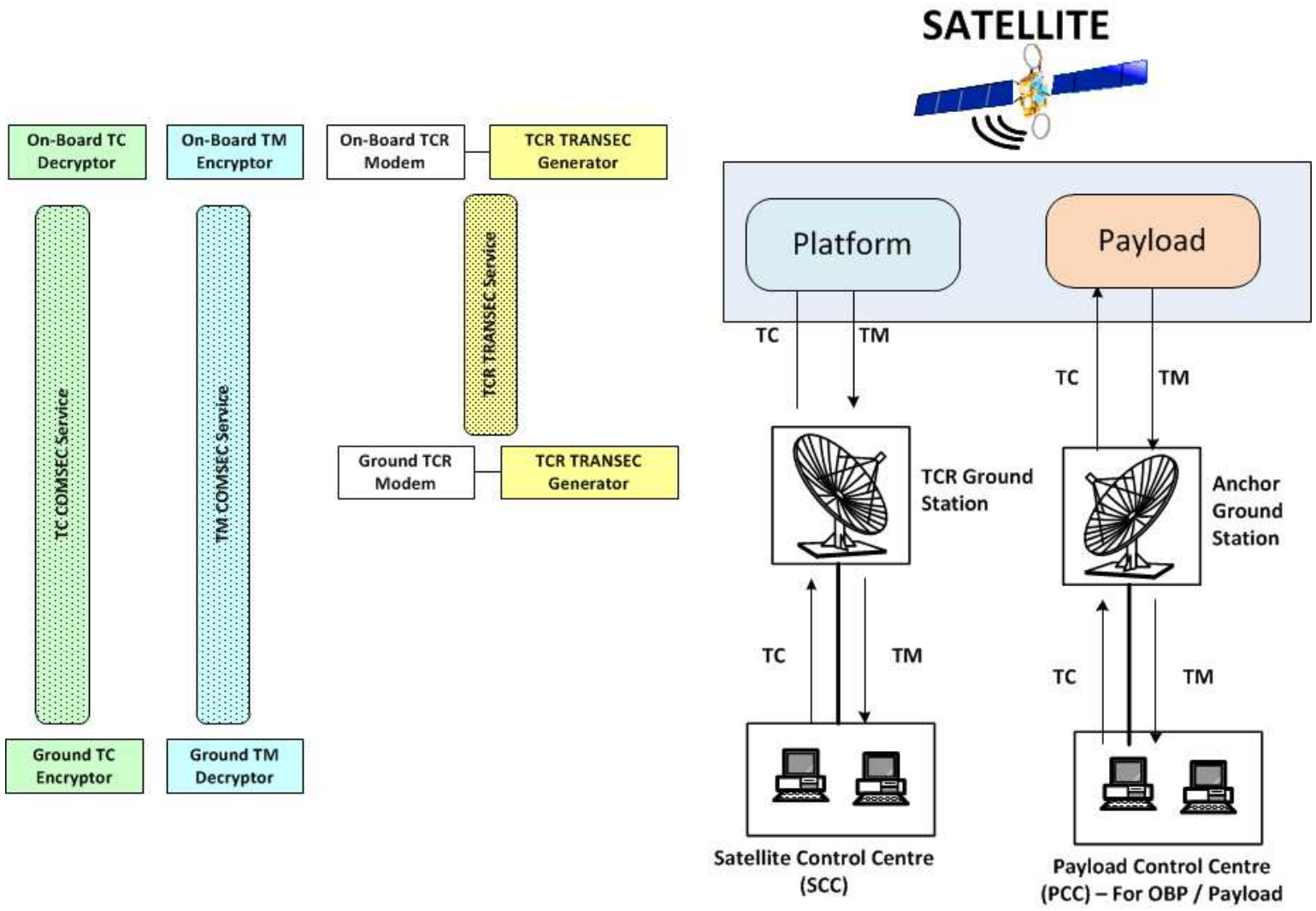
5 - Services de Sécurité Cibles

Services de Sécurité applicable aux liaisons spatiales

- TM COMSEC (Flux : TM-HK ou TM-PL)
  - Services de Sécurité implémentés : Authentification + Chiffrement (AE : Authenticated Encryption)
    - Protection : Authenticité , Intégrité, Confidentialité
- AOS COMSEC (Flux AOS Audio-Vidéo)
  - Service de Sécurité implémenté : Chiffrement (EO : Encryption Only)

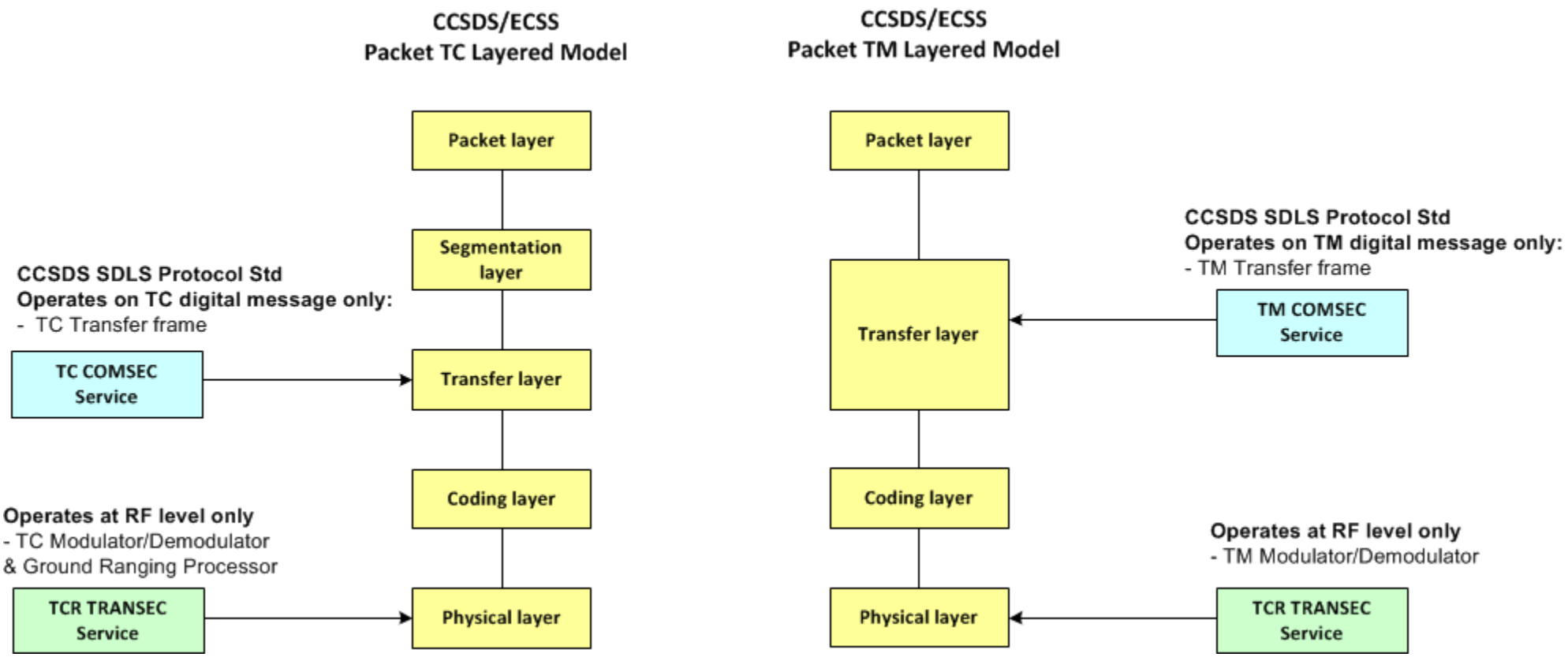
5 - Services de Sécurité Cibles

Exemple de localisation des fonctions de Sécurité COMSEC & TRANSEC



5 - Services de Sécurité Cibles

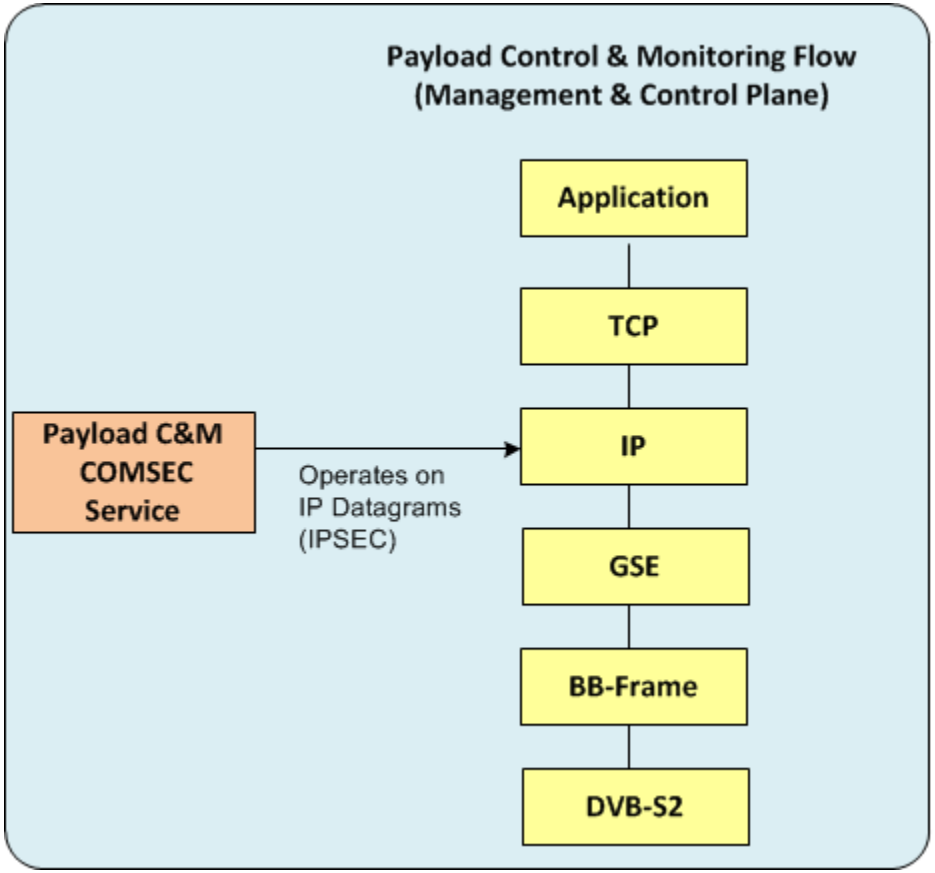
Position des Couches Sécurité dans le modèle en couches CCSDS

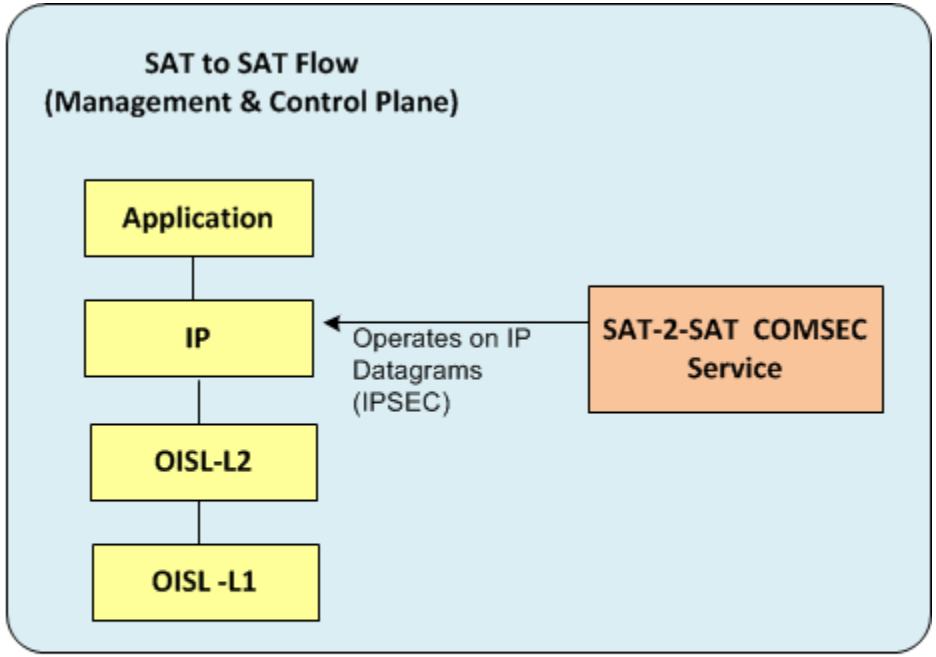


5 - Services de Sécurité Cibles

Utilisation IPSEC dans un réseau spatial

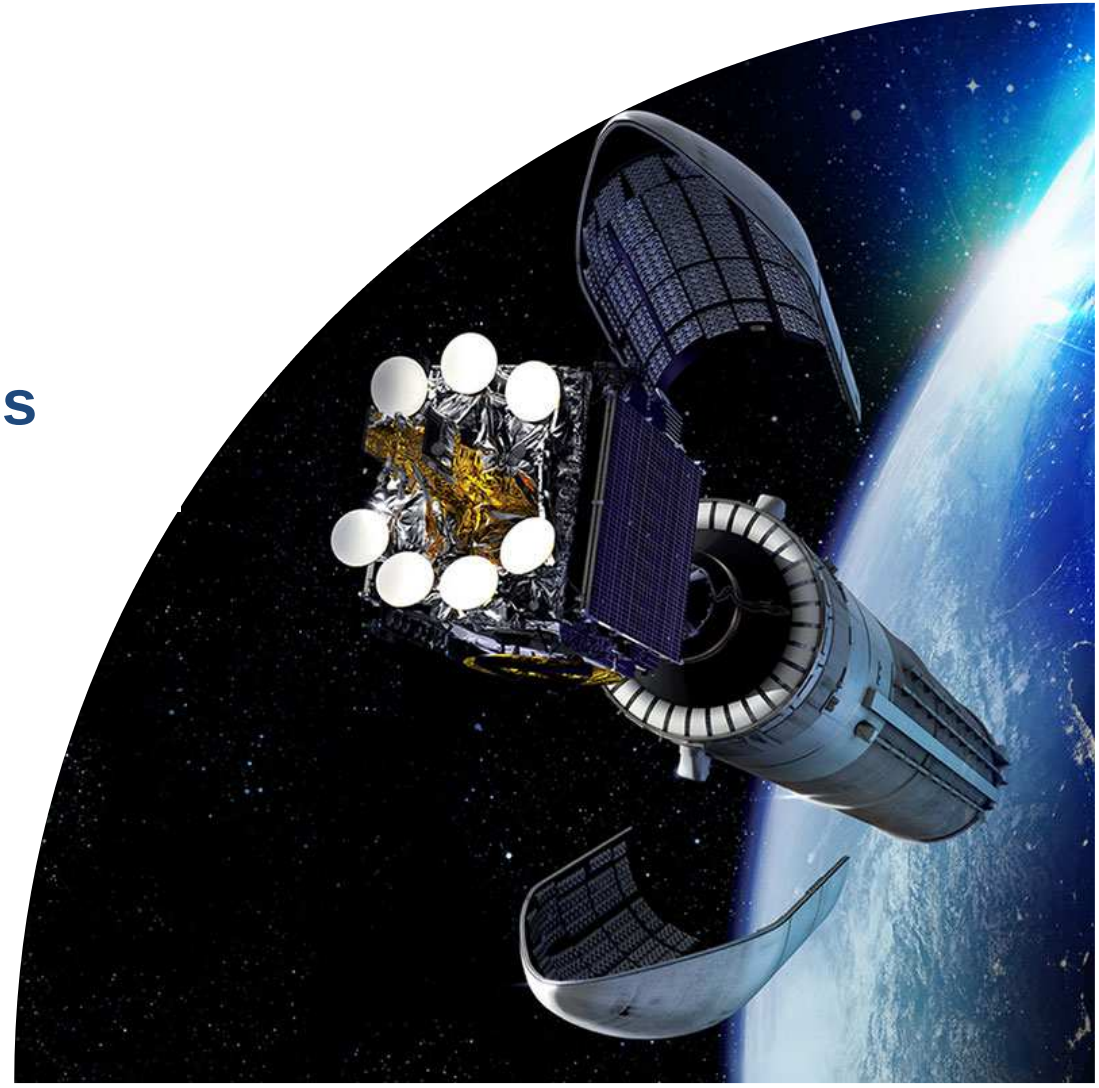
- Constellation de satellites avec lien inter-satelite (ISL)
- Plan de management/contrôle Payload basé sur le stack de protocoles TCP/IP

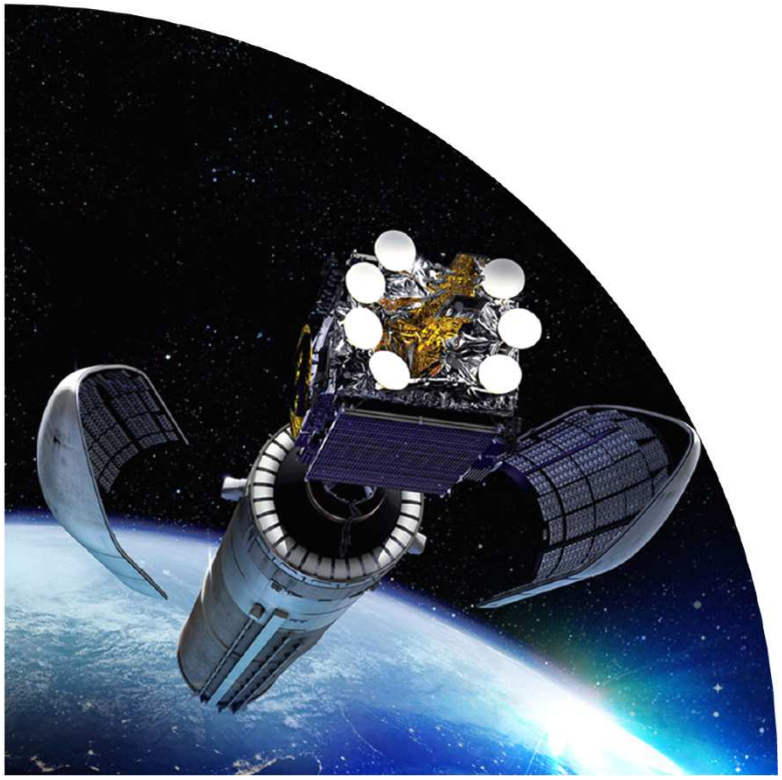




TLS-SEC – Sécurité des Communications Spatiales

6 – Cryptographie : Algorithmes, Modes d'Opérations et Protocoles





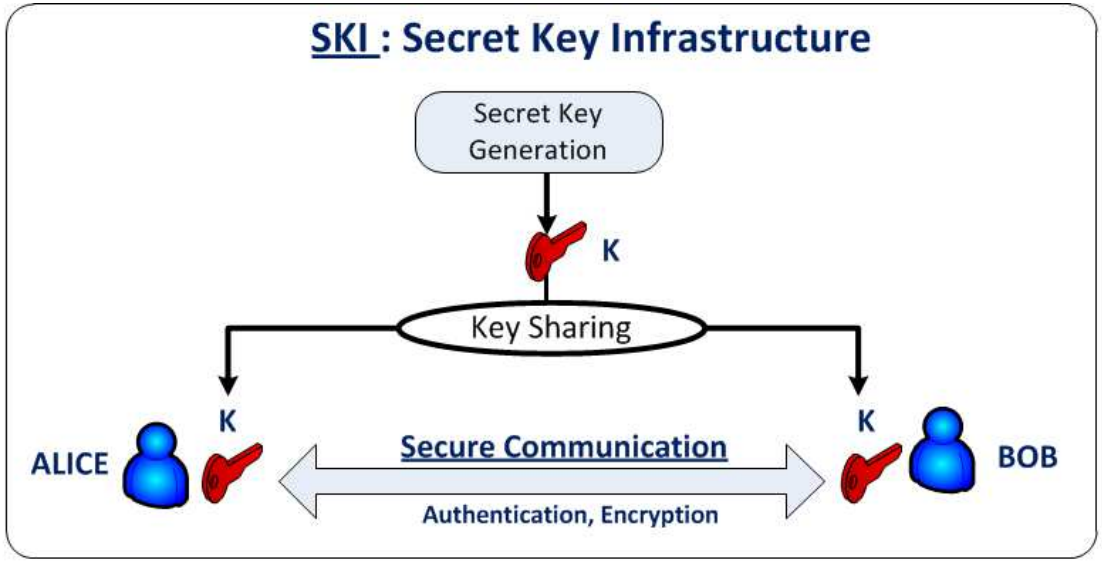
6.1 – Généralités sur la Cryptographie SKI et PKI

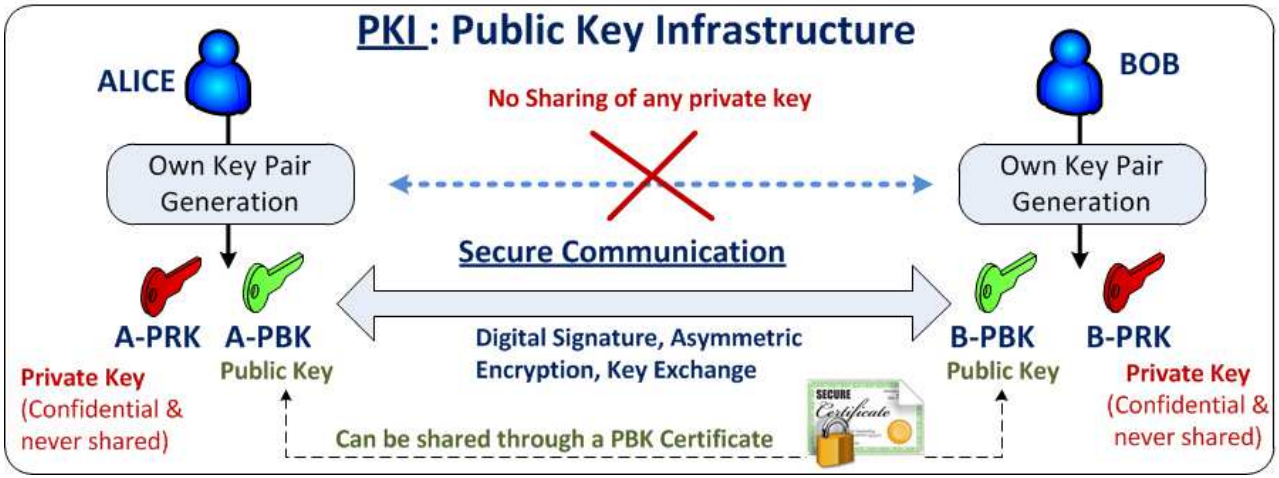
6.1 - Généraliteés sur la Cryptographie SKI et PKI

- La Cryptographie est une technologie basée sur les mathématiques et destinée à garantir la sécurité des communications à travers un canal de communication public
- La Cryptographie vise à atteindre deux objectifs essentiels:
  - Confidentialité : l'information n'est accessible qu'aux parties autorisées
  - Authentification: les parties communiquantes sont légitimes
- Techniques actuelles utilisées en cryptographie
  - Cryptographie **symétrique** basée sur le partage préalable de clés secrètes entre les 2 utilisateurs communiquant
    - **SKI** : Secret Key Infrastructure
  - Cryptographie **asymétrique** basée sur l'allocation d'un couple de clés Privée / Publique (PRK/PBK) à chaque utilisateur et sans aucun partage préalable d'éléments secrets
    - **PKI** : Public Key Infrastructure
    - La PRK est la propriété exclusive d'un utilisateur unique (pas de partage)
    - La PBK est diffusée via un certificat la liant formellement à l'identité de son propriétaire

6.1 - Généralités sur la Cryptographie SKI et PKI

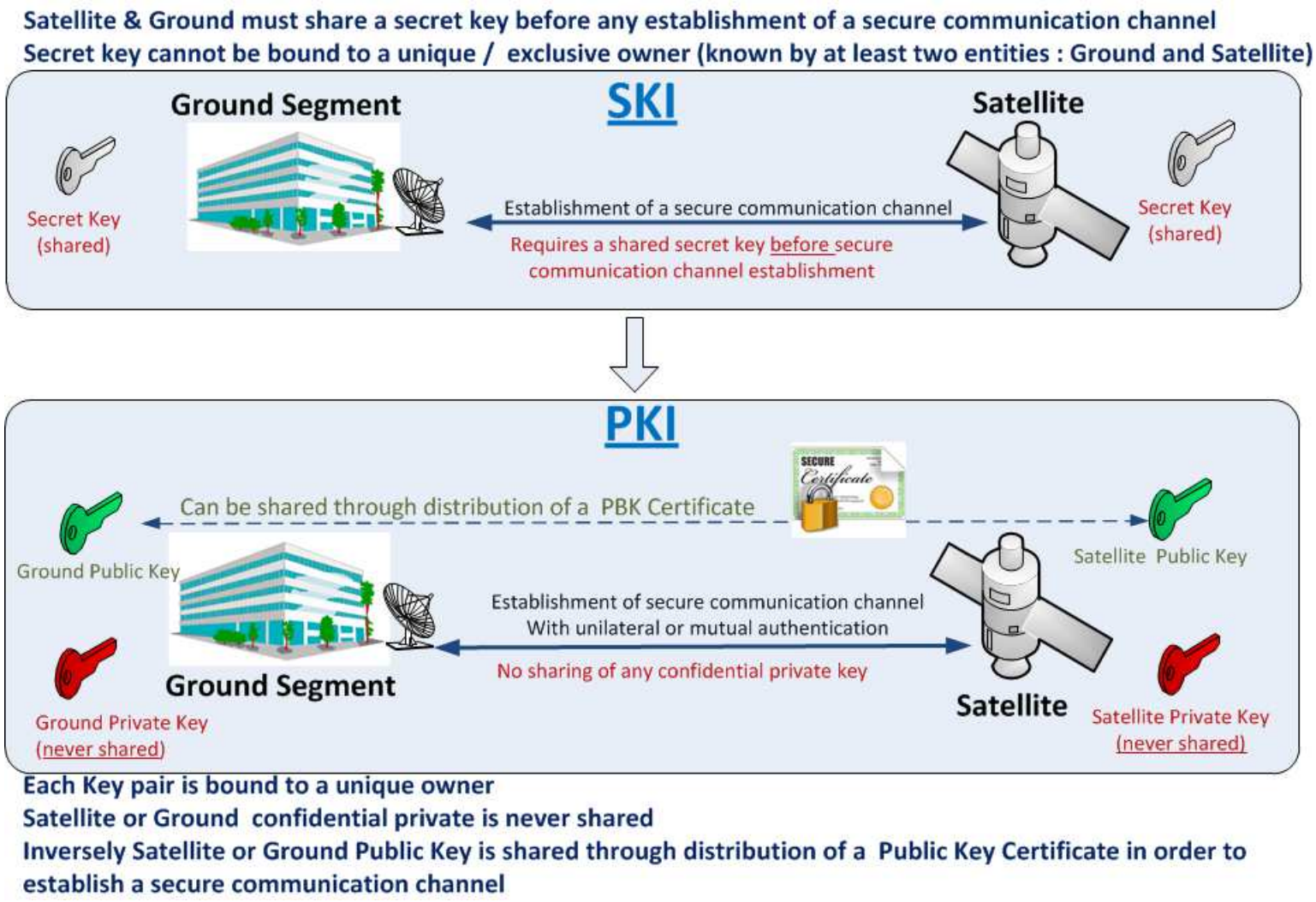
Cryptographie SKI vs PKI : Cas Général





6.1 - Généralités sur la Cryptographie SKI et PKI

Cryptographie SKI vs PKI : Application aux Systèmes Spatiaux



6.1 - Généralités sur la Cryptographie SKI et PKI

Utilisation de la SKI vs PKI dans le spatial

- La protection du Trafic bord / Sol TC, TM, AOS (services COMSEC / TRANSEC) n'utilise que la cryptographie symétrique
  - Le standard CCSDS Space Data Link Security (CCSDS 355.0-B-1) recommande principalement l'utilisation de la cryptographie symétrique pour la protection COMSEC du trafic TC / TM
  - Aucun besoin de sécurité imposant la cryptographie PKI (ex: Non Répudiation)
- La Gestion des clés
  - Utilise encore largement la cryptographie symétrique
  - Evolue vers la cryptographie asymétrique

SKI vs PKI : Application aux Systèmes Spatiaux

Space Communication Links Traffic Protection	⟺	**Symmetric Cryptography (SKI)**
Key Management	⟺	**Symmetric Cryptography (SKI) and/or Asymmetric Cryptography (PKI)**

6.1 - Généralités sur la Cryptographie SKI et PKI

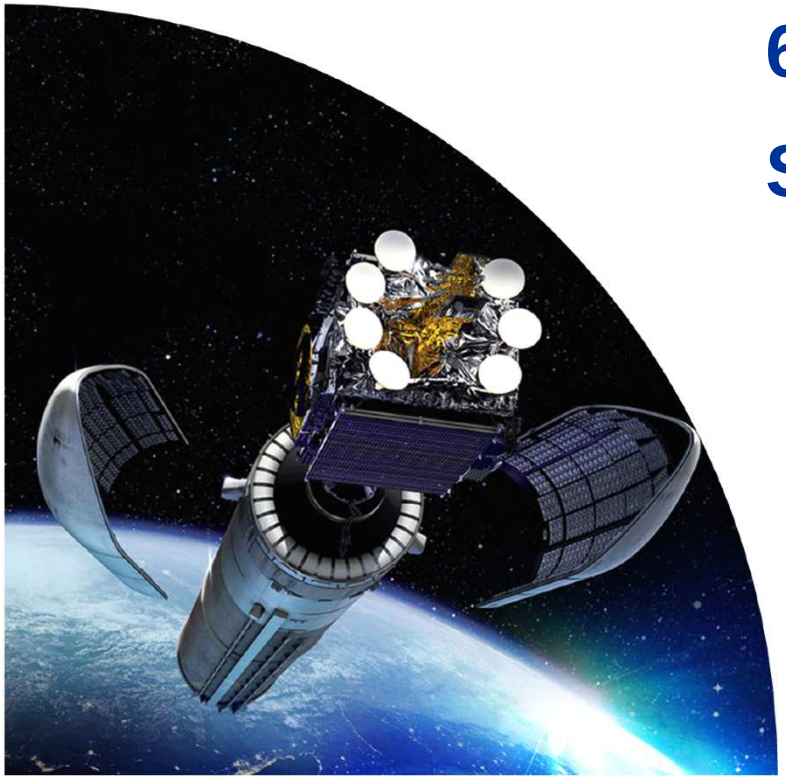
Techniques émergentes en cryptographie

❑ Cryptographie post-quantique

- ➢ Algorithmes PKI résistant aux attaques utilisant des ordinateurs quantiques (algorithme de SHOR)

❑ Cryptographie quantique / QKD (Quantum Key Distribution)

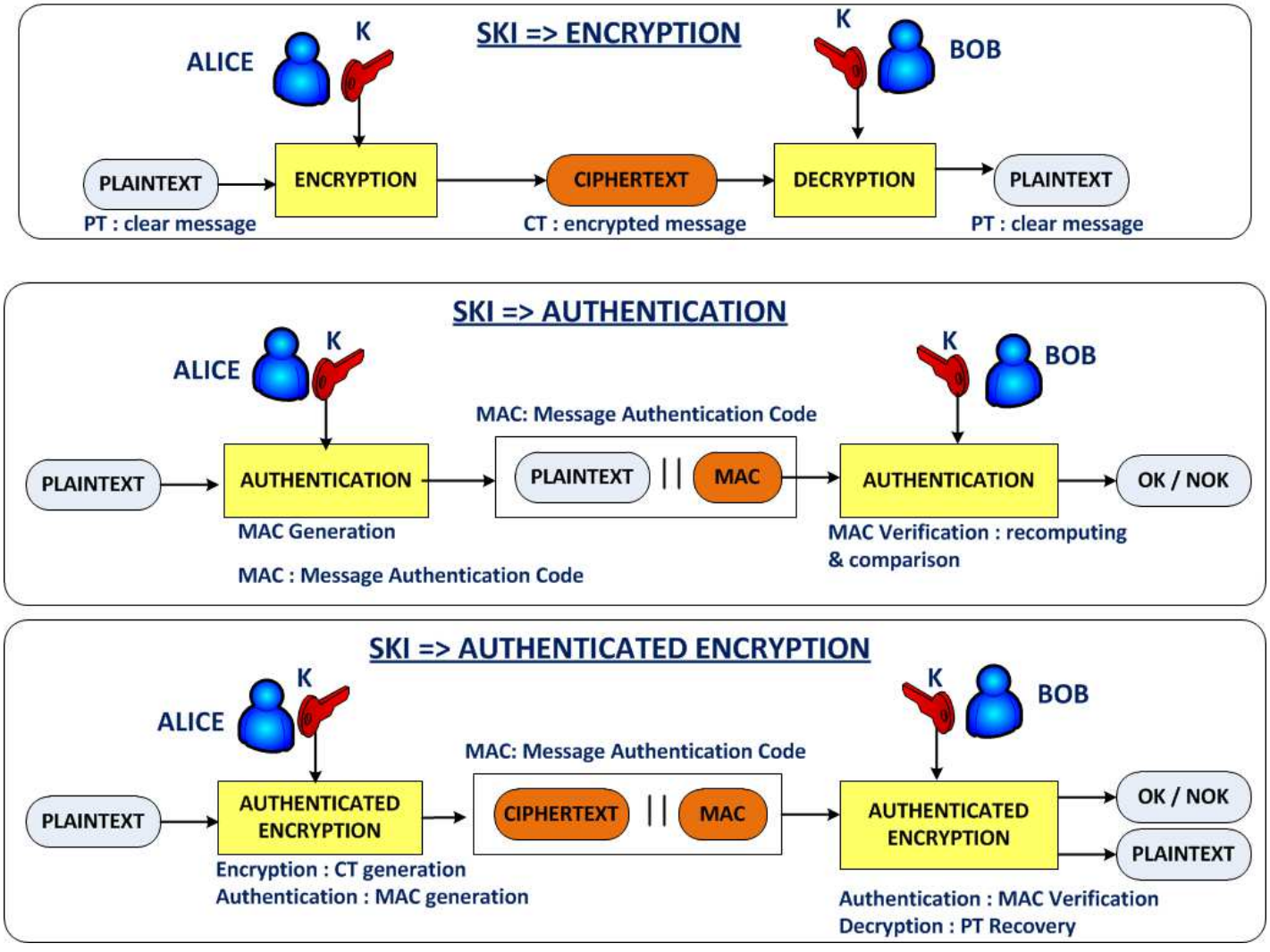
- ➢ Utilisation de liaisons optiques quantiques pour distribuer des clés de manière inviolable car reposant exclusivement sur les lois de la physique quantique



6.2 – Cryptographie Symétrique (SKI)

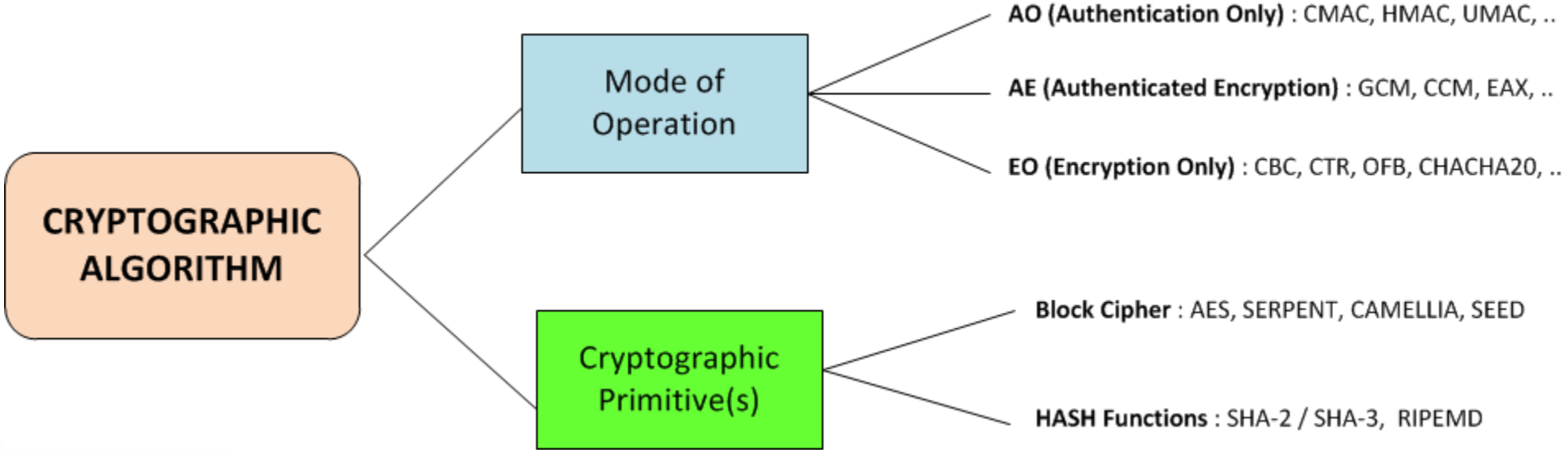
6.2 - Cryptographie Symétrique (SKI)

Cryptographie SKI : Opérations



6.2 - Cryptographie Symétrique (SKI)

- Un Algorithme cryptographique est composé:
  - D'un Mode d'opération : supporte le service de sécurité cible (AO, AE, EO)
  - D'une ou plusieurs primitives cryptographiques
- Sélection: impératif de suivre les recommandations d'experts / veille crypto
  - Ex: organismes ECRYPT, ENISA, ..
  - Emettent des recommandations à jour pour les algorithmes cryptographiques, les protocoles cryptographiques ou la taille des clés



6.2 - Cryptographie Symétrique (SKI)

Avantages de la Cryptographie Symétrique pour la protection du Trafic

- Algorithmes et modes d'opération parfaitement connus et maîtrisés
- Fort héritage en vol
- Implémentation aisée et optimisée
  - Logicielle (ex: calculateurs bord) , matérielle (FPGA / ASIC)
- Solutions peu gourmandes en ressources bord / satellite (CPU, mémoire, ..)
- Performances très élevées en débit
  - Compatibles de débits allant jusqu'à 1 Gb/s pour les données Instruments (Flux TM-PL)
  - Ratio de perfs allant de 1 jusqu'à 1000 entre SKI et PKI pour une opération de chiffrement
- Performances très honorables au niveau implémentation logicielle avec l'AES
  - Emergence d'algorithmes Stream Ciphers performants (Service EO)
  - Ex: CHACHA20 = 3 x plus rapide que l'AES

6.2 - Cryptographie Symétrique (SKI)

Sélection des Modes d'opération : Critères (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

6.2 - Cryptographie Symétrique (SKI)

Sélection des Modes d'opération : Critères (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 : Ciphertext) impacte 2 PT blocks de 128 bits chacun (plaintext) apres déchiffrement
  - Avec le mode CTR, 1 bit en erreur dans la séquence chiffrée (CT : Ciphertext) impacte 1 seul bit d'un PT block (plaintext) apres déchiffrement
- Padding / Expansion du ciphertext : impact sur overhead sécurité
- Nombre d'invocations des primitives cryptographiques pour chaque opération
  - Impact sur les performances
- Capacité de Preprocessing
  - Ex: pré-calcul des clés dérivées
- On-line – Off-line (ex: GCM vs CCM): impact sur les performances
- Parallèlisation du traitement : impact sur les performances
- Performances implémentations matérielles / logicielles (Benchmark)

6.2 - Cryptographie Symétrique (SKI)

Mode d'Opération de type AO (Authentication Only)

- Utilisation typique : service TC COMSEC-1
  - Authenticité et Intégrité requises
  - Pas de Confidentialité requise
- Modes d'Opération candidats
  - 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
- Remarque
  - Le mode AO GMAC (NIST SP800-38D) non retenu dû à ses défauts & faiblesses
    - impose l'utilisation d'un IV contrairement aux autres modes AO
    - impact en cas de collision d'IV => compromission possible de la Clé GHASH

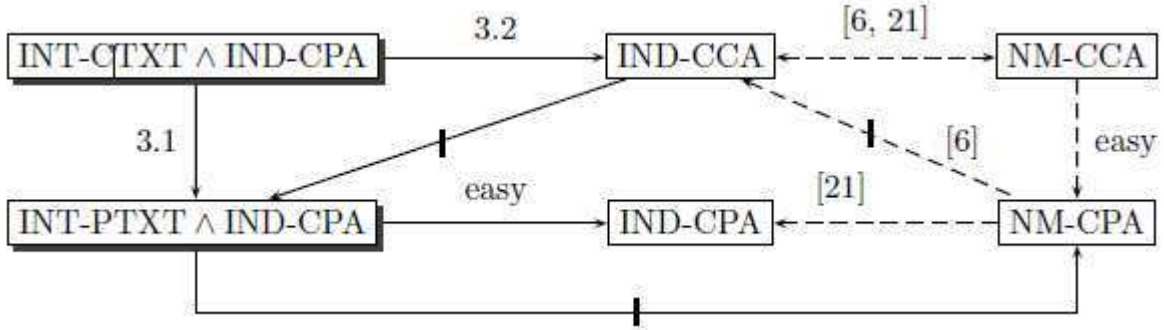
Extrait Rapport ECRYPT 2018

Scheme	Classification Legacy	Classification Future	Building Block
CMAC	✓	✓	Any block cipher as a PRP
EMAC	✓	✓	Any block cipher as a PRP
AMAC	✓	✓	Any block cipher
HMAC	✓	✓	Any hash function as a PRF
UMAC	✓	✓	An internal universal hash function
GMAC	✓	✗	Finite field operations
Poly1305	✓	✗	Finite field operations

6.2 - Cryptographie Symétrique (SKI)

Mode d'Opération de type AE (Authenticated Encryption)

- Service TC COMSEC-2
  - Authenticité, Intégrité et Confidentialité
- Règle d'Or : ne jamais bâtir par soi-même un mode AE à partir de modes AO et EO existants
- 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. Namprempprey
  - "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



6.2 - Cryptographie Symétrique (SKI)

Mode d'Opération de type AE (Authenticated Encryption)

- L'analyse de N. Bellare et N. Namprempprey montre qu'il est recommandé d'utiliser des modes d'opération AE de type "Encrypt Then MAC" => critère IND-CCA
- France: confirmé par l'ANSII qui ne retient que des schémas type "Encrypt Then MAC"

Composition Method	Privacy			Integrity	
	IND-CPA	IND-CCA	NM-CPA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	insecure	secure	insecure
MAC-then-encrypt	secure	insecure	insecure	secure	insecure
Encrypt-then-MAC	secure	secure	secure	secure	secure

- Modes AE Candidats (Rapport ECRYPT 2018)

Scheme	Legacy	Future	Notes
Authenticated Encryption			
Generic Composition	✓	✗	Encrypt-then-MAC, and other variants
CCM	✓	✗	Superseded by EAX
CWC	✓	✗	Superseded by GCM
OCB	✓	✓	
EAX	✓	✓	
GCM	✓	✓	
ChaCha20+Poly1305	✓	✓	

6.2 - Cryptographie Symétrique (SKI)

Remarques sur les modes AE candidats

GCM

- Très large déploiement et adoption (Réseaux, Internet, Banques, incluant les système spatiaux..)
- Faiblesse liée aux impacts d'une collision d'IV : risque de compromission de la clé GHASH
  - Impact opérationnel (Sol) important . L'IV Sol est contrôlé par l'Opérateur SCC via l'IHM
  - Une erreur humaine / Opérateur (rejeu valeur IV antérieure) est toujours possible
- Taille effective du MAC réduite à 96 bits dû à la découverte de clés GCM faibles
- Performant , mais 75% du processing est dû à la fonction Authentification / GHASH
  - 25 % pour la fonction Chiffrement (CTR)

EAX / EAX2

- Combinaison de 2 modes sûrs et performants : CTR et UMAC
- EAX2: seul mode AE permettant l'utilisation de 2 clés distinctes : Authentification et Chiffrement
  - Séparation des clés (1 fonction = 1 clé) recommandé par l'ANSSI (RGS)
- Standard ISO - Mode non standardisé NIST

6.2 - Cryptographie Symétrique (SKI)

- Compétition CAESAR Competition: emergence d'une nouvelle génération de modes AE (Authenticated Encryption)
  - Objectif: Disposer d'alternatives performantes et sures au mode GCM
  - Compétition démarrée en 2014 and cloturée en février 2019
  - Le portfolio final CAESAR est organisé suivant 3 Use Cases
    - Use Case 1: Lightweight applications (resource constrained environments)
      - ASCON, ACORN
    - Use Case 2: High Performance Applications
      - AEGIS-128, OCB
    - Use Case 3: Defence in Depth (ex: tolerance to IV collision)
      - DEOXYS-II, COLM, COPA
    - Note: ces algorithmes sélectionnés à la suite de la compétition CAESAR ne sont pas encore standardisés

6.2 - Cryptographie Symétrique (SKI)

Mode d'Opération de type EO (Encryption Only)

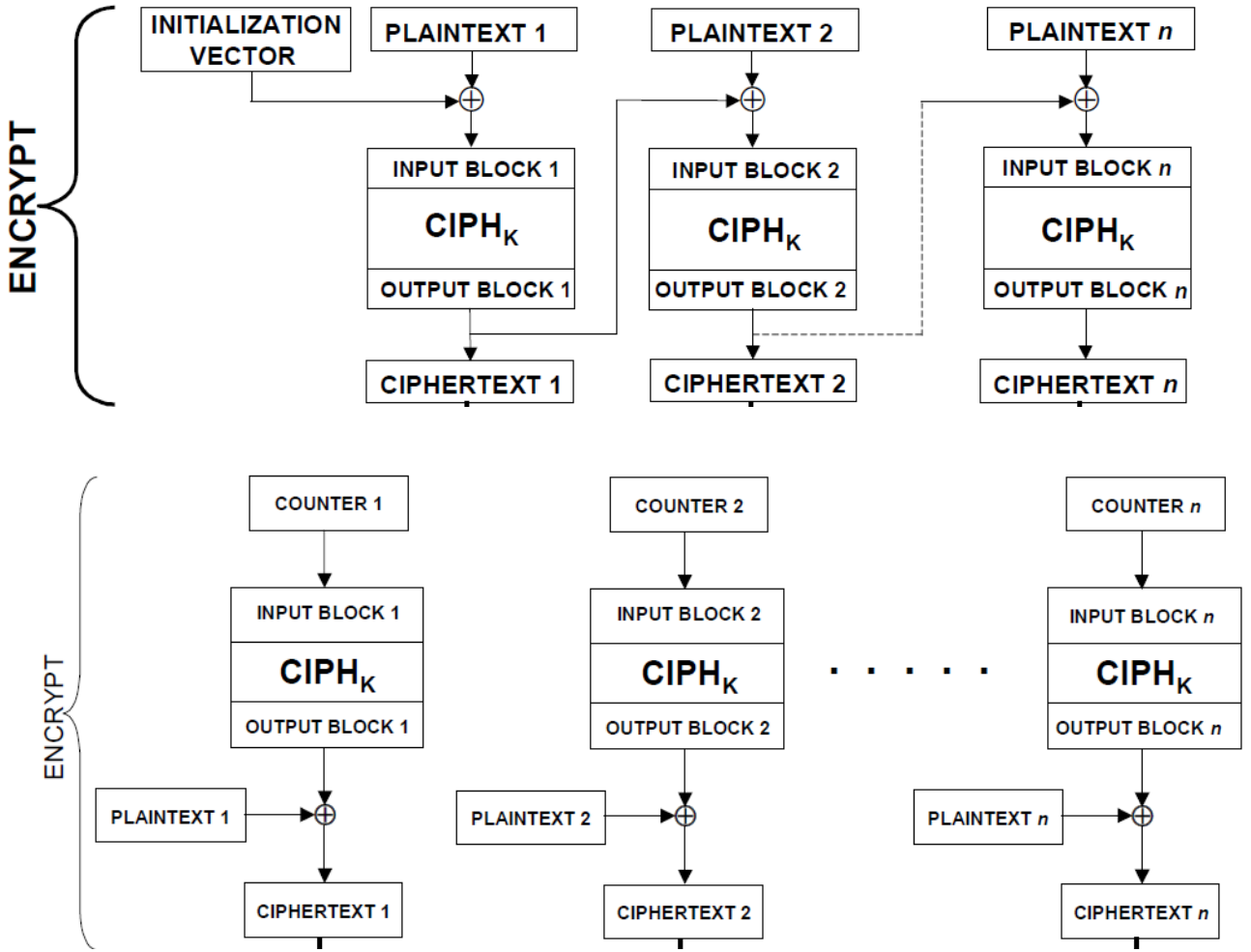
- Service : AV COMSEC (protection de flux Audio-Vidéo / liaisons de type AOS)
  - Confidentialité Requise / Authenticité / Intégrité non requises
- Modes EO candidats (NIST SP800-38A)
  - CTR : Counter Mode / CBC : Cipher Block Chaining Mode – en version sans padding
    - Note il existe des versions de CBC sans padding => CBC-CTS : ciphertext stealing
  - CFB: Cipher Feedback Mode / OFB : Output Feedback Mode
- Nouveau modes EO candidats : EME; FFX
  - Mais soumis à brevet
- Rapport ECRYPT 2018 sur les modes EO

Table 5.1: Symmetric Key Encryption Summary Table

Scheme	Legacy	Future	Notes
Block Cipher Modes of Operation			
OFB	✓	✗	No padding required
CFB	✓	✗	No padding required
CTR	✓	✗	No padding required
CBC	✓	✗	
ECB	✗	✗	
XTS	✓	✗	
EME	✓	✓	
FFX	✓	✓	

6.2 - Cryptographie Symétrique (SKI)

- Le standard NIST SP800-38A permet l'utilisation de primitives Block Cipher (ex: AES) pour réaliser les opérations EO en mode Block Cipher (Fig haut) ou Stream Cipher (Fig bas)

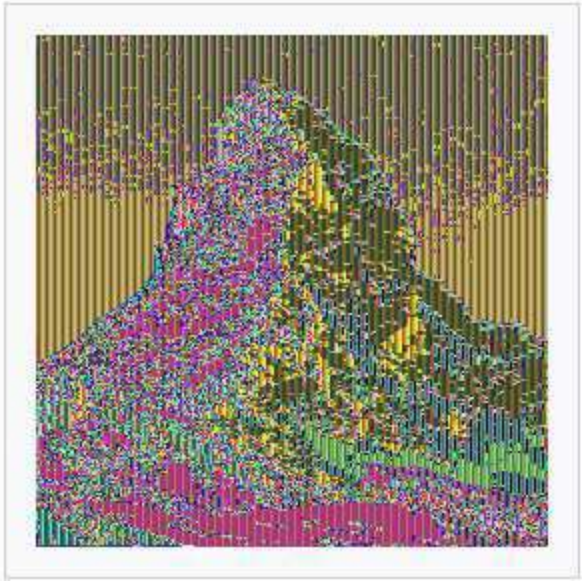


6.2 - Cryptographie Symétrique (SKI)

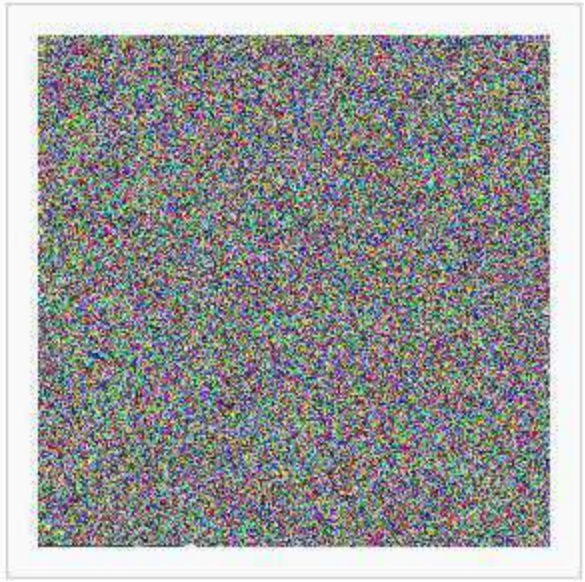
Mode EO: Pourquoi le mode ECB est à prohiber

- Pas d'IV (Initialization Vector) permettant de différencier chaque chiffrement bloc éléméntaire
- Conséquence: pour une clé donnée, le meme plaintext donnera toujours le meme ciphertext
- IV requis pour tous les modes EO retenus

Plaintext



Ciphertext avec ECB



Ciphertext avec CTR ou CBC

6.2 - Cryptographie Symétrique (SKI)

Sélection des primitives cryptographiques pour modes AO, AE, EO

- Mode d'Opération HMAC : utilisation des primitives SHA-xxx (SHA-2 / SHA-3)
  - Donc taille MAC minimale = 256 bits
- Tous les autres modes d'opération sont basés sur une primitive Block Cipher
  - Aujourd'hui AES (NIST FIPS 197) est la primitive recommandée et utilisée
  - Autres primitives Block Cipher 128 bits: CAMELLIA ou SERPENT => alternatives envisageables
- Consultation d'avis issus d'organismes effectuant un survey / rapport annuels
  - ECRYPT 2018

Table 4.2: Block Cipher Summary

Primitive	Classification Legacy	Future
AES	✓	✓
Camellia	✓	✓
Serpent	✓	✓
Three-Key-3DES	✓	✗
Two-Key-3DES	✓	✗
Kasumi	✓	✗
Blowfish$^{\geq 80\text{-bit keys}}$	✓	✗
DES	✗	✗

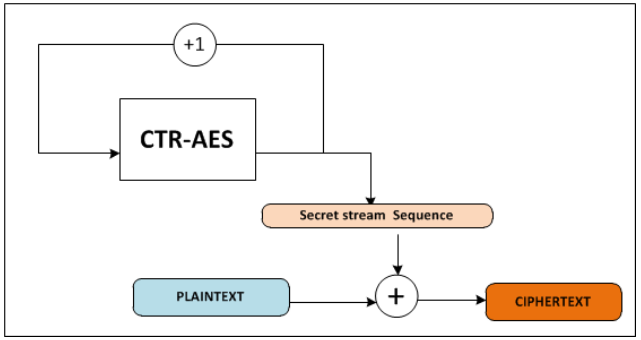
Table 4.3: Hash Function Summary

Primitive	Output Length	Classification Legacy	Future
SHA-2	256, 384, 512, 512/256	✓	✓
SHA-3	256, 384, 512	✓	✓
SHA-3	SHAKE128, SHAKE256	✓	✓
Whirlpool	512	✓	✓
BLAKE	256, 384, 512	✓	✓
RIPEMD-160	160	✓	✗
SHA-2	224, 512/224	✓	✗
SHA-3	224	✓	✗
MD5	128	✗	✗
RIPEMD-128	128	✗	✗
SHA-1	160	✗	✗

6.2 - Cryptographie Symétrique (SKI)

Cas des algorithmes natifs Stream Cipher

- Application:
  - Service COMSEC => mode Encryption Only (EO) : XOR entre Plaintext et une stream sequence secrete générée
  - Service TRANSEC =>: generation des séquences TRANSEC pilotant l'étalement de spectre (voir §9)
- 8 algorithmes candidats Stream Cipher: voir Table
  - ECRYPT Report 2018
- Rappel: l'utilisation de Block Cipher constitue une alternative aux Stream Cipher (ex: modes CTR, CFB, OFB, ..)



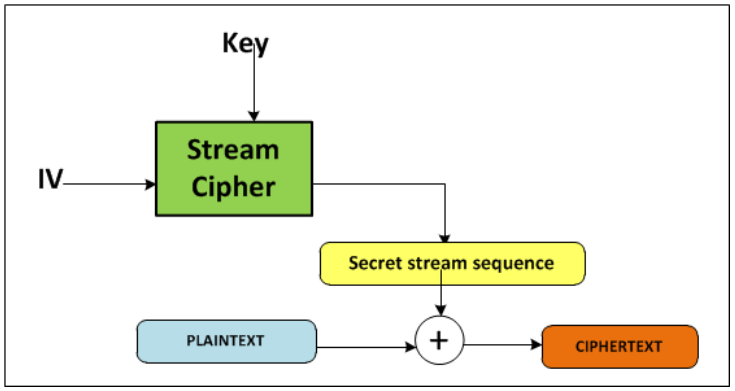


Table 4.4: Stream Cipher Summary

Primitive	Classification	
	Legacy	Future
HC-128	✓	✓
Salsa20/20	✓	✓
ChaCha	✓	✓
SNOW 2.0	✓	✓
SNOW 3G	✓	✓
SOSEMANUK	✓	✓
Grain 128a	✓	✓
Grain	✓	✗
Mickey 2.0	✓	✗
Trivium	✓	✗
Rabbit	✓	✗
A5/1	✗	✗
A5/2	✗	✗
E0	✗	✗
RC4	✗	✗

6.2 - Cryptographie Symétrique (SKI)

Taille Clés et MAC

- Taille de clé de 128 bits convient en théorie à toutes les missions
  - Mais pour les Clients exigeants (Opérateurs majeurs) ou Gouvernementaux, il n'y a pas de débat
    - La taille de clé de 256 bits est exigée de-facto
    - Indépendamment des analyses et démonstrations de robustesse de systèmes utilisant une clé de 128 bits
  - À terme taille 256 bits pour l'AES imposée par la menace des ordinateurs quantiques
- Taille de MAC : 128 bits acceptable – Evolution future à 256 bits requise
- Extrait Rapport ECRYPT 2018

	Parameter	Legacy	Future System Use	
			Near Term	Long Term
Symmetric Key Size	k	80	128	256
Hash Function Output Size	m	160	256	512
MAC Output Size*	m	80	128	256
RSA Problem	$\ell(n) \geq$	1024	3072	15360
Finite Field DLP	$\ell(p^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512
ECDLP	$\ell(q) \geq$	160	256	512
Pairing	$\ell(p^{k \cdot n}) \geq$	1024	6144	15360
	$\ell(p), \ell(q) \geq$	160	256	512

6.2 - Cryptographie Symétrique (SKI)

Taille Clés et MAC : Autres Sources

- Voir notamment le site : www.keylength.com
- ANSII

Date	Symétrique	Factorisation Module	Logarithme discret Clef	Logarithme discret Groupe	Courbe elliptique GF(p)	Courbe elliptique GF(2^n)	Hash
2014 - 2020	100	2048	200	2048	200	200	200
2021 - 2030	128	2048	200	2048	256	256	256
> 2030	128	3072	200	3072	256	256	256

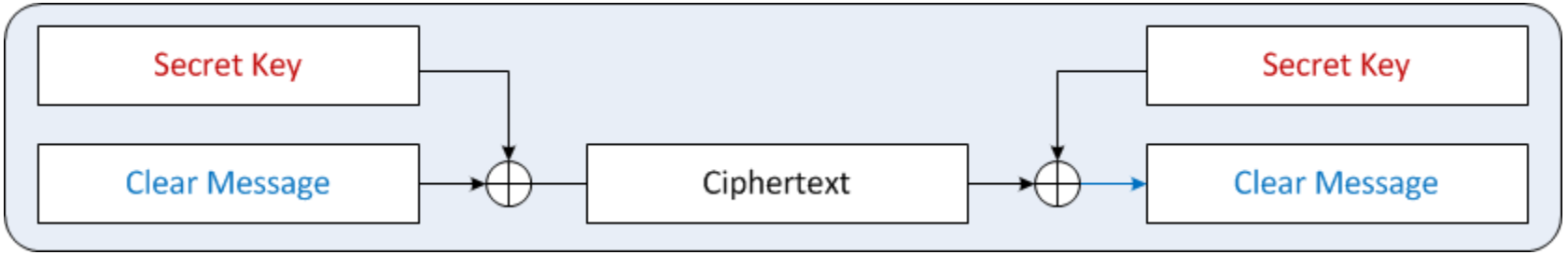
- NIST

Date	Résistance minimale	Algorithme symétrique	Factorisation Module	Logarithme discret Clef	Logarithme discret Groupe	Courbe elliptique	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 et au-delà	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 et au-delà	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 et au-delà	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

6.2 - Cryptographie Symétrique (SKI)

SKI : Chiffrement parfait : OTP (One Time Pad)

- Méthode de chiffrement inventée par Vernam (1917)
- 1 clé aléatoire, différente pour chaque message et de la taille du message à chiffrer
- Démonstration par Shannon en 1949 : Sécurité théorique absolue
  - Sécurité inconditionnelle
- Très rarement utilisé : complexité de la gestion associée des clés

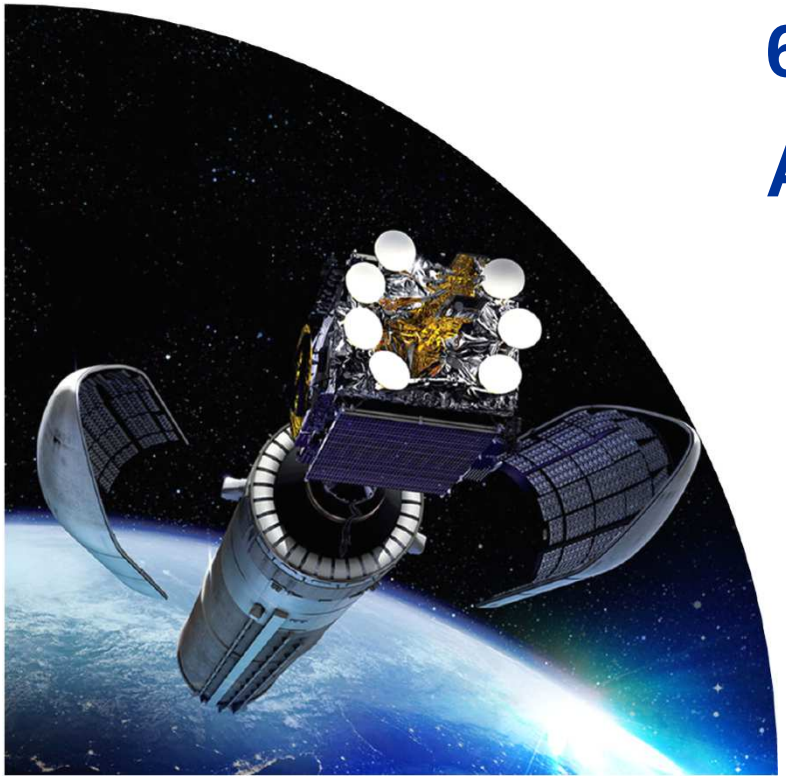


6.2 - Cryptographie Symétrique (SKI)

NIST : Programme de validation AES / AES Validation List

- Objectif : Validation de l'implémentation de l'algorithme cryptographique
- Note : Il ne s'agit pas d'une validation ou certification Sécurité mais uniquement de vérifier le respect de la spécification NIST (mode d'opération, primitive cryptographique) par l'implémentation
- Process courant NIST avec l'algorithme AES
- Validation réalisée par un Labo agréé NIST
- Verification du Code (code source logiciel / VHDL)
- Exécution de Test patterns complets
- À la fin (tests OK) : inscription dans l'AES Validation List officielle du NIST (voir site web dédié)
- Ex: Couche logicielle GCM-AES développée par TAS

4023	THALES ALENIA SPACE 26 avenue JF Champollion - BP 33787 Toulouse, Toulouse 31037 France -HALIMI William TEL: + 33 5 34 35 52 98 FAX: + 33 5 34 35 61 69	**GCM-AES software module for TAS Satellites Telemetry link encryption** Version 01.00.00	The targeted satellite on-board computer is based on a Leon3FT processor (SPARCv8 family). w/ OSTRALES	7/31/2016	**ECB** (e only; 128 , 256); **GCM (KS: AES_128**( ) Tag Length(s): 128) **(KS: AES_256**( ) Tag Length(s): 128) **PT Lengths Tested:** (7808 , 7808 , 7872 , 7872) ; **AAD Lengths tested:** (112 , 176) ; **IV Lengths Tested:** (8 , 1024) ; **96BitIV_Supported** **GMAC_Not_Supported** "The target GCM-AES software crypto module (gcm-aes-encrypt function) is implemented as part of the so-called On-board-Software (OBSW) of THALES ALENIA SPACE (TAS) GEO / LEO satellites involved in Telecommunication and Observation space missions."



6.3 – Cryptographie Asymétrique (PKI)

6.3 – Cryptographie Asymétrique (PKI)

Cryptographie Asymétrique : fondations par DIFFIE & HELLMAN en 1976

- Article IEEE: « New Directions in Cryptography » introduisant la notion de paire de clés publique/privée et le tout premier protocole d'échange de clés DH (Diffie-Hellman)

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. Introduction

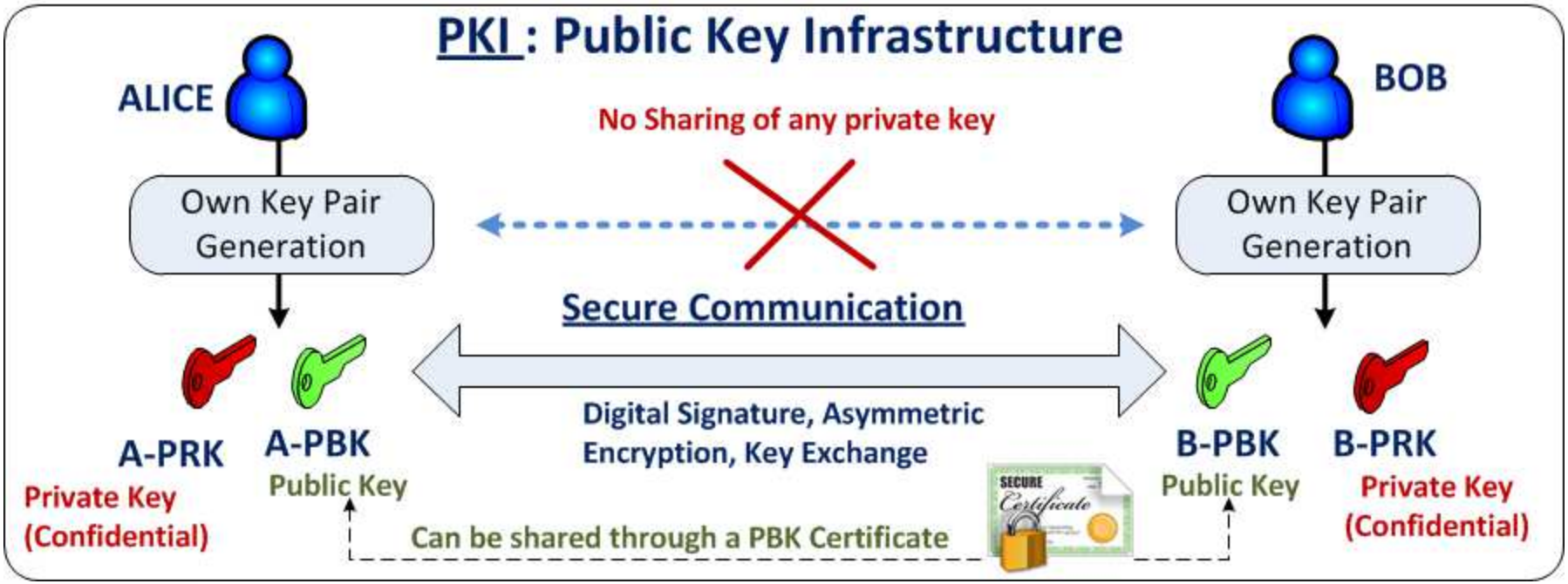
WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of me-

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

6.3 – Cryptographie Asymétrique (PKI)

Rappel des concepts de base de la Cryptographie asymétrique

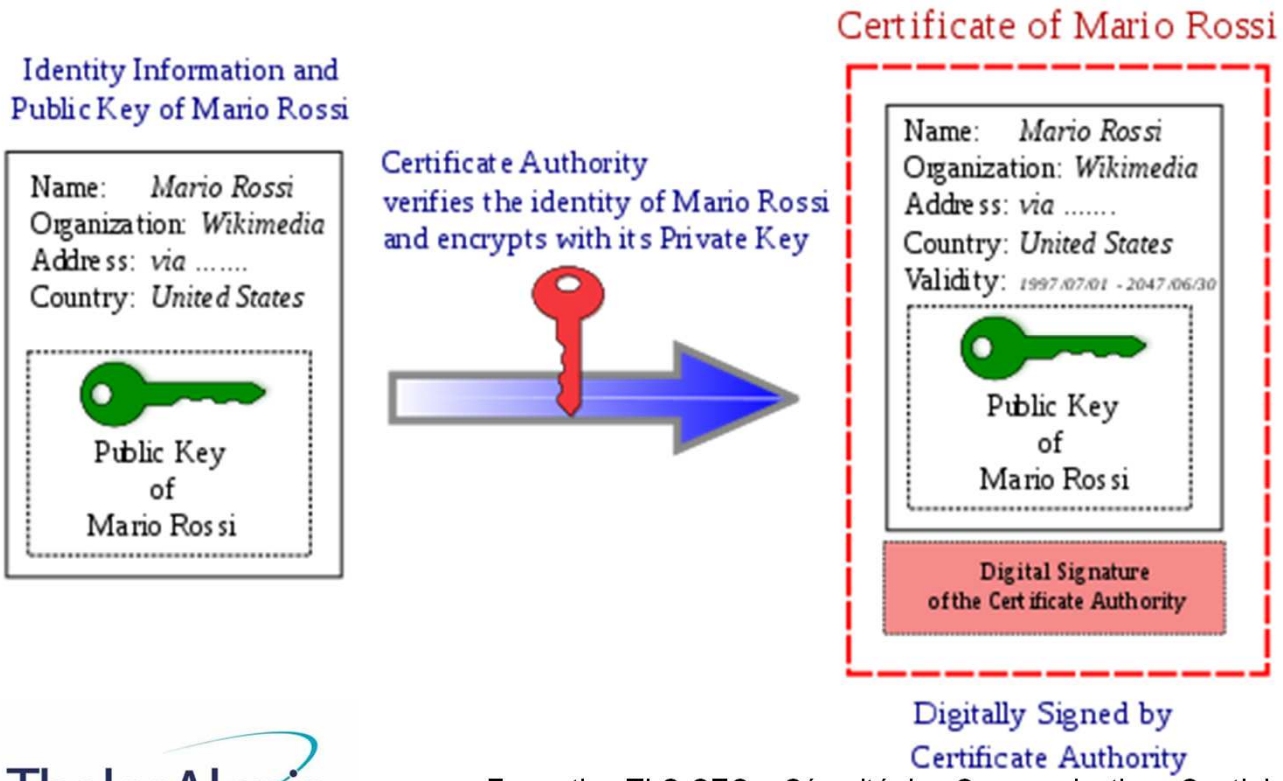
- Chaque entité possède sa propre paire de clés : clé privée (PRK) et clé publique (PBK)
  - Chaque paire de clé est liée à un propriétaire unique
- La clé privée est confidentielle et jamais partagée: utilisée par son seul propriétaire
- La clé publique n'est pas confidentielle: elle peut être partagée via la distribution d'un Certificat de clé publique afin d'etablir une communication sécurisée avec un tiers

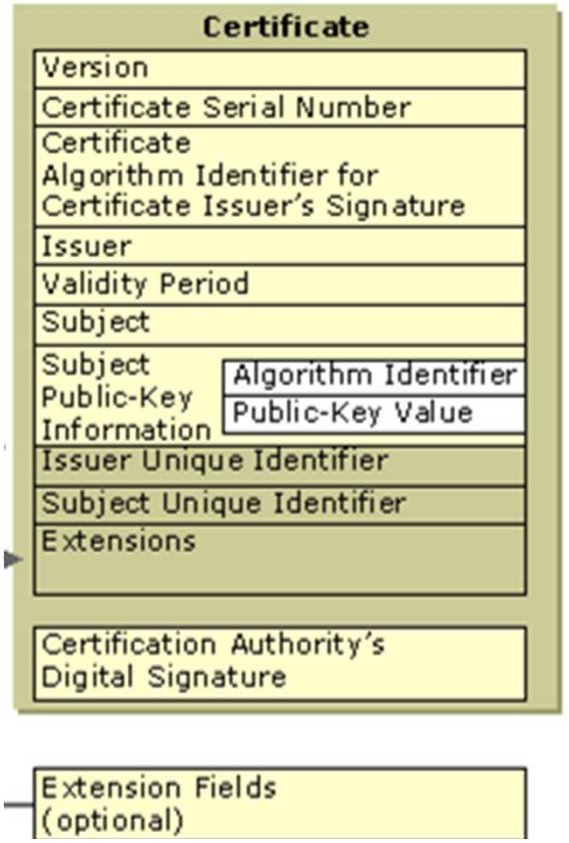


6.3 – Cryptographie Asymétrique (PKI)

PKI: notion fondamentale de Certificat de clé publique

- Role: Lier officiellement une PBK à l'identité de son propriétaire via l'utilisation d'une cryptographie forte
- Contenu: information PBK (ID propriétaire, usage, algorithme, validité, valeur PBK, ..) associé à une signature digitale couvrant le contenu du certificat
- Autorité: Certificat signé par une Certification Authority (CA)
  - Signé avec la PRK de la CA





6.3 – Cryptographie Asymétrique (PKI)

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
A0IABE6148XhHt9KRdfBVB/iL3OD73AIGcHuFasjwIBAhHeIETpKn5qUfUkjKlqN
7s42DfsD8Dd5cKhSHlvzQZ7KQRGjgc8wgcwwCQYDVR0TBAIwADARBglghkgBhvhC
AQEEBAMCBeAwMwYJYIZIAYb4QgENBCYWJE9wZW5TU0wgR2VuZXJhdGVkIENsaWVu
dCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUy4scTBwWHY6kIKJSGNGhAsCGlE8wHwYD
VR0jBBgwFoAUIbH8c2fbbLIsdhLCckPbpUVvmAAwDgYDVR0PAQH/BAQDAgXgMCcG
A1UdJQQgMB4GCCsGAQUFBwMCBggrBgEFBQcDAQYIKwYBBQUHAwQwCgYIKoZIzj0E
AwIDSQAwRgIhAPymY067HSZ7hV1F73Llhhtqj0r8moKP7iH531Af5jEDAiEAodJR
QXGFyA7/Hnr2PQwoQpNTN5UjTmfsT79J9uFmoCM=
-----END CERTIFICATE-----
```

OPENSSL command for PBK Certificate decoding

openssl x509 -in user.cert -text -noout

Decoded PBK Certificate

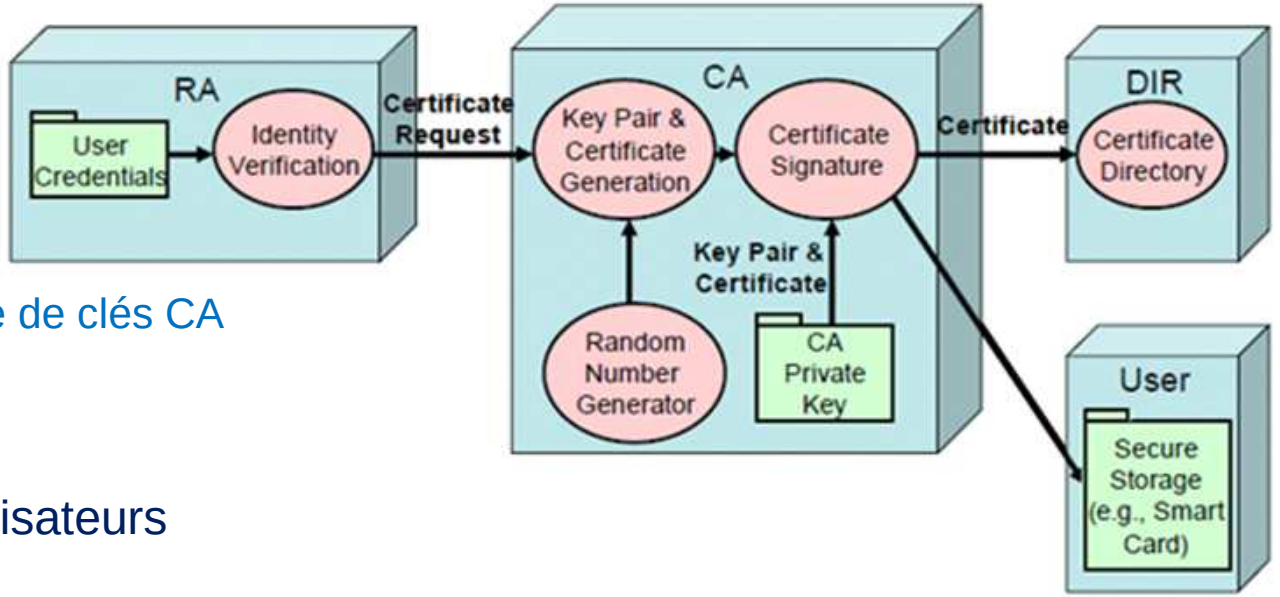
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8192 (0x2000)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=FR, ST=Haute-Garonne, L=Toulouse, O=CNES, OU=GND-NODE-0, CN=KMS-O-CA
        Validity
            Not Before: Sep 17 13:25:17 2018 GMT
            Not 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
```

6.3 – Cryptographie Asymétrique (PKI)

Infrastructure PKI : Architecture

- RA: Registration Authority
- CA: Certification Authority
  - Equippé de sa propre paire de clés CA

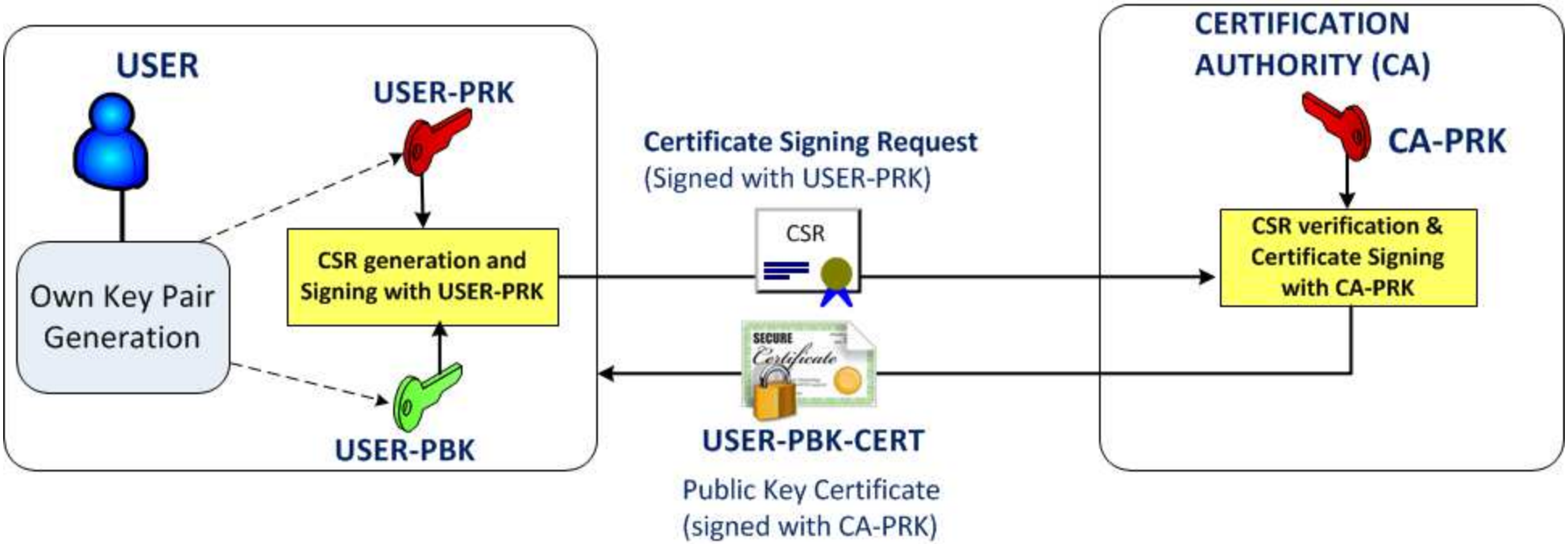


Roles

- RA: Enregistrement des Utilisateurs
- CA: Signature des Certificats PBK
  - Via le traitement d'une CSR (Certificate Signing Request) – voir slide suivant
- CA: Révocation des Certificats PBK
  - Création et mise à jour d'une CRL (Certificate Revocation List) signée avec la PRK CA et distribution ("CRL PUSH").

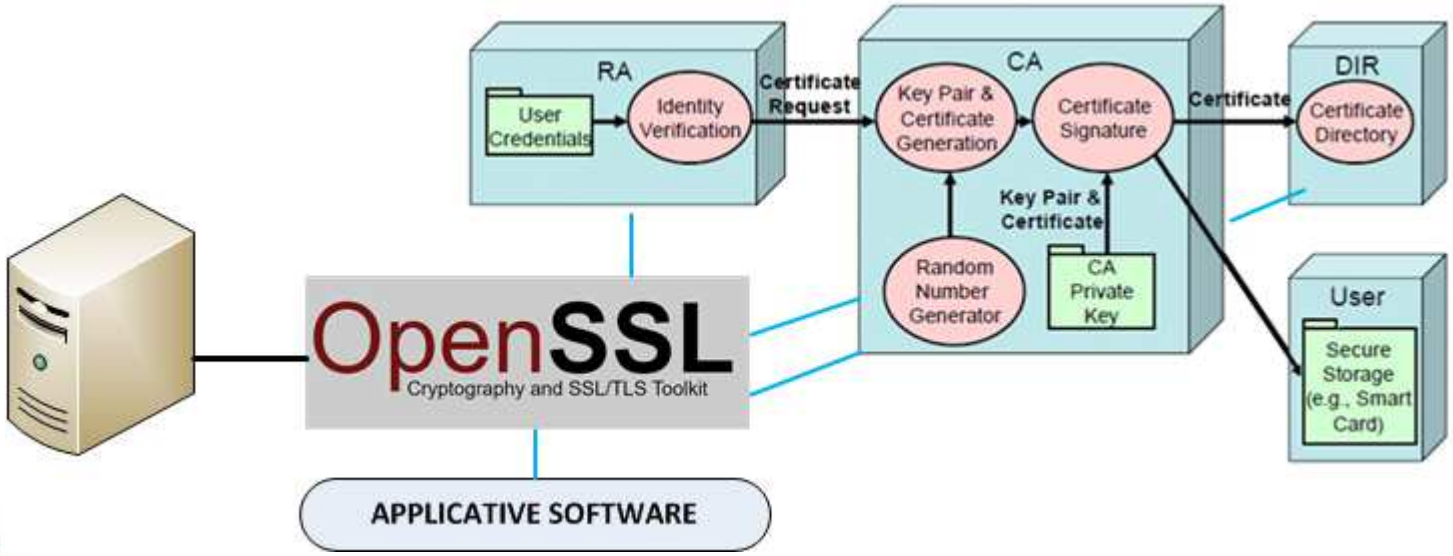
6.3 – Cryptographie Asymétrique (PKI)

Illustration de la génération d'un Certificat PBK



6.3 – Cryptographie Asymétrique (PKI)

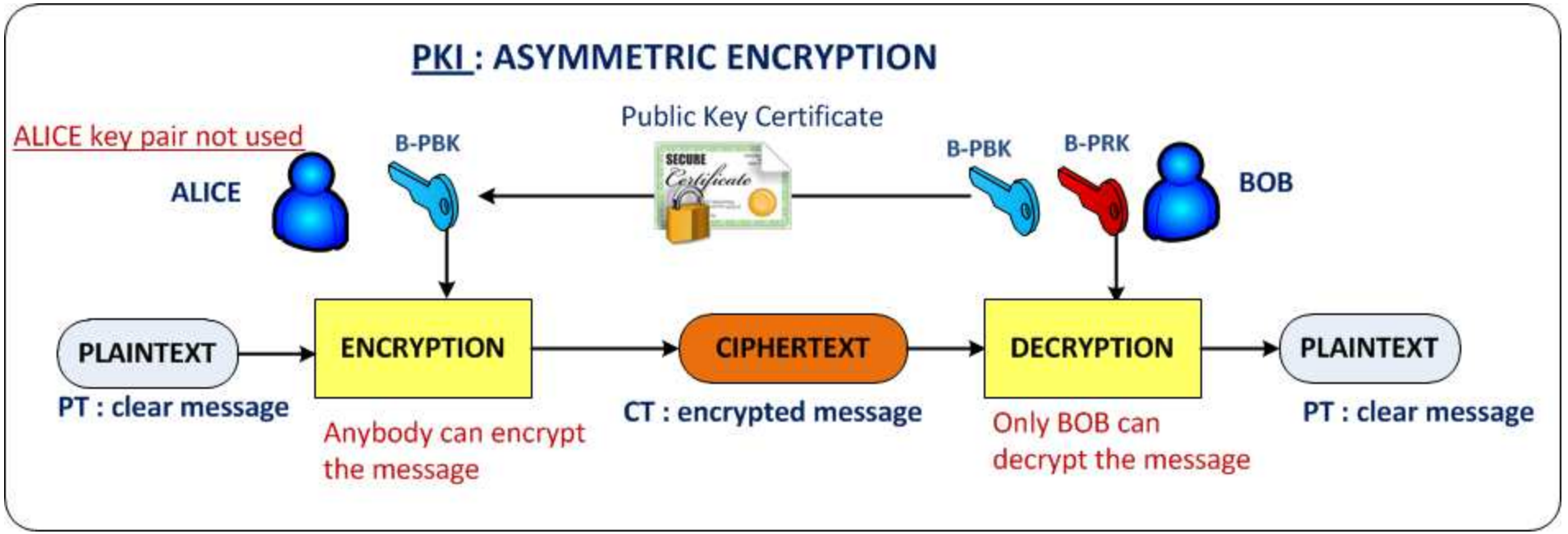
- Une CA peut être publique ou privée.
- Au niveau des applications PKI considérées pour les missions spatiales, la CA est privée (créée et gérée par l'Opérateur Satellite)
  - RA/CA = Opérateur Satellite
- Optimisation de l'infrastructure PKI pour une CA privée PKI
  - Implémentation RA/CA dans une station de travail dédiée chez l'Opérateur Satellite
  - Utilisation d'une librairie cryptographique type OPENSSL (nombre d'opérations peuvent etre realisées par de simples lignes de commande)



6.3 – Cryptographie Asymétrique (PKI)

Cryptographie PKI : Opérations => Chiffrement asymétrique

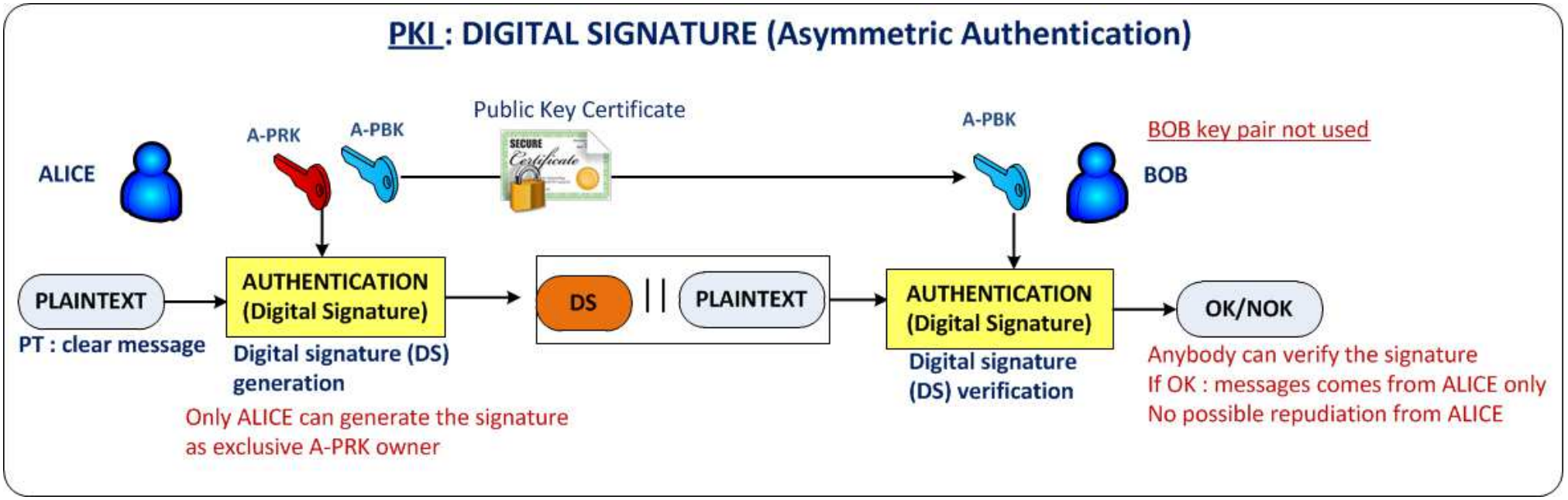
- Entité Emetteur: chiffrement avec la PBK de l'Entité Réceveur
  - Obtenue via le CERT PBK
- Entité Réceveur : déchiffrement avec sa propre PRK
- La paire de clés de Entité Emetteur n'est pas utilisée



6.3 – Cryptographie Asymétrique (PKI)

Cryptographie PKI : Opérations => Signature Digitale

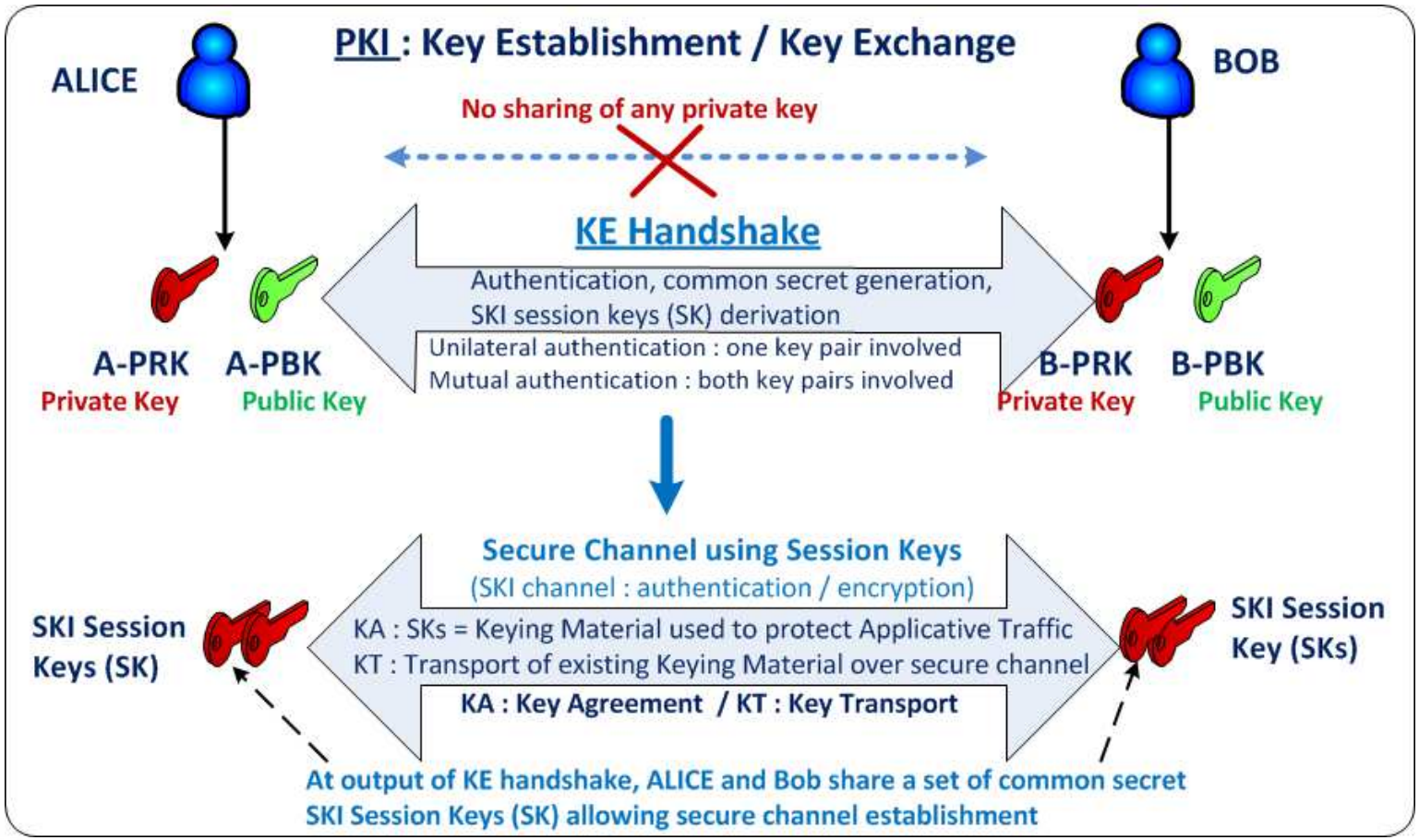
- Entité Emetteur: signature avec sa propre PRK
- Entité Receveur : vérification signature avec la PBK de l'Entité Emetteur
  - Obtenue via le CERT PBK
- La paire de clés de l'Entité Receveur n'est pas utilisée



6.3 – Cryptographie Asymétrique (PKI)

Cryptographie PKI : Opérations => Etablissement de Clés (= Echange de Clés)

- Objectif: Partage sécurisé d'un jeu de clés SKI (Keying Material) entre 2 entités en vue de leur utilisation pour une communication sécurisée (authentification / chiffrement)

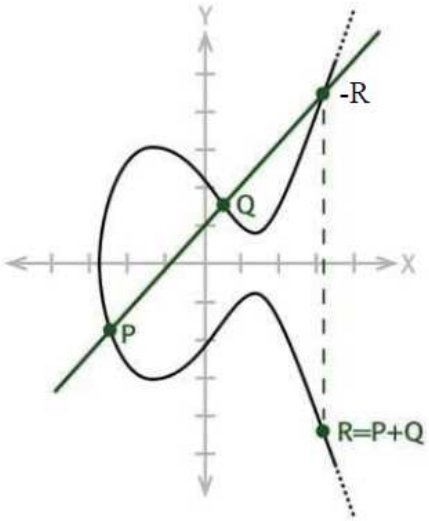


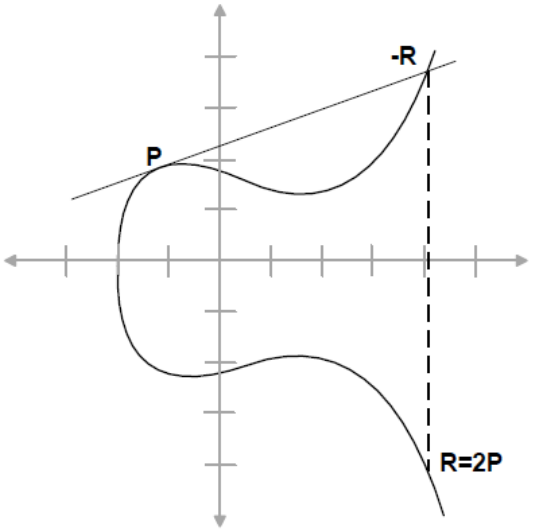
6.3 – Cryptographie Asymétrique (PKI)

Cryptographie PKI: trois systèmes

- IFC: Integer Factorization Cryptography (ex: RSA)
- DLC: Discrete Logarithm Cryptography (ex: DH Exchange)
- ECC: Elliptic Curves Cryptography (ex: ECDSA, ECDH)
- Note: pour chaque système la sécurité est liée à un “problème mathématique réputé difficile” (voir Annexe: “Hard Problems”)

ECC: Illustration des opérations addition & multiplication avec les courbes elliptiques





6.3 – Cryptographie Asymétrique (PKI)

Cryptographie PKI : 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

6.3 – Cryptographie Asymétrique (PKI)

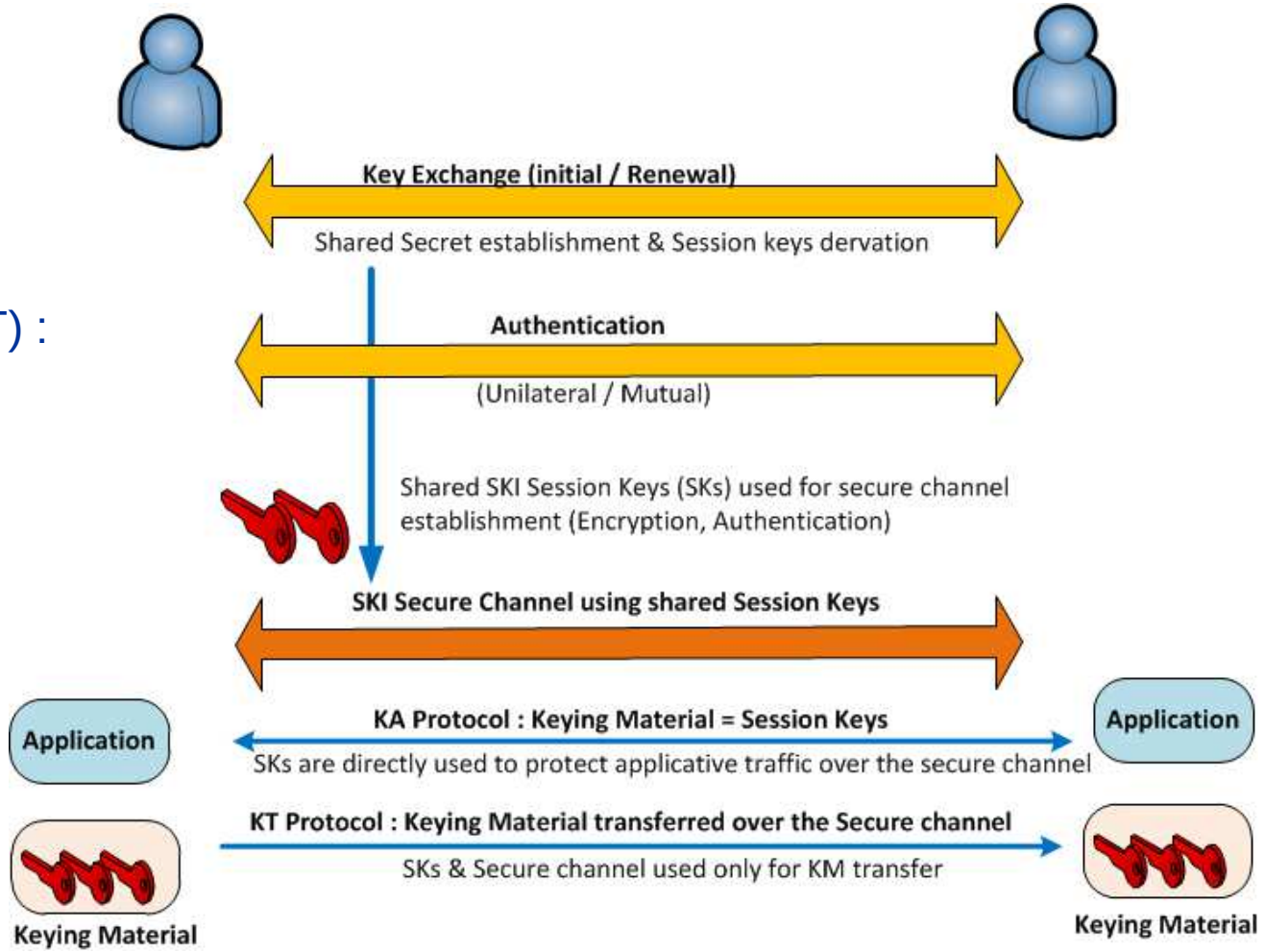
Protocole KE (Key Establishment)

- Procédure cryptographique réalisant le partage sécurisé d'un jeu de clés SKI (Keying Material) entre 2 entités en vue de leur utilisation ultérieure pour une communication sécurisée (authentification / chiffrement)
- 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
  - KT : Key Transport : établissement durant la session, d'un canal sécurisé puis transport à travers ce canal, des clés secrètes SKI préalablement générées
- 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 éphémeres garantissent la propriété PFS

6.3 – Cryptographie Asymétrique (PKI))

- Une session KE inclut 2 étapes principales
  - Génération des clés de session SKI pour la protection du Trafic
  - Authentification (mutuelle ou unilatérale)

Protocole KE (KA/KT) :
Logique générale



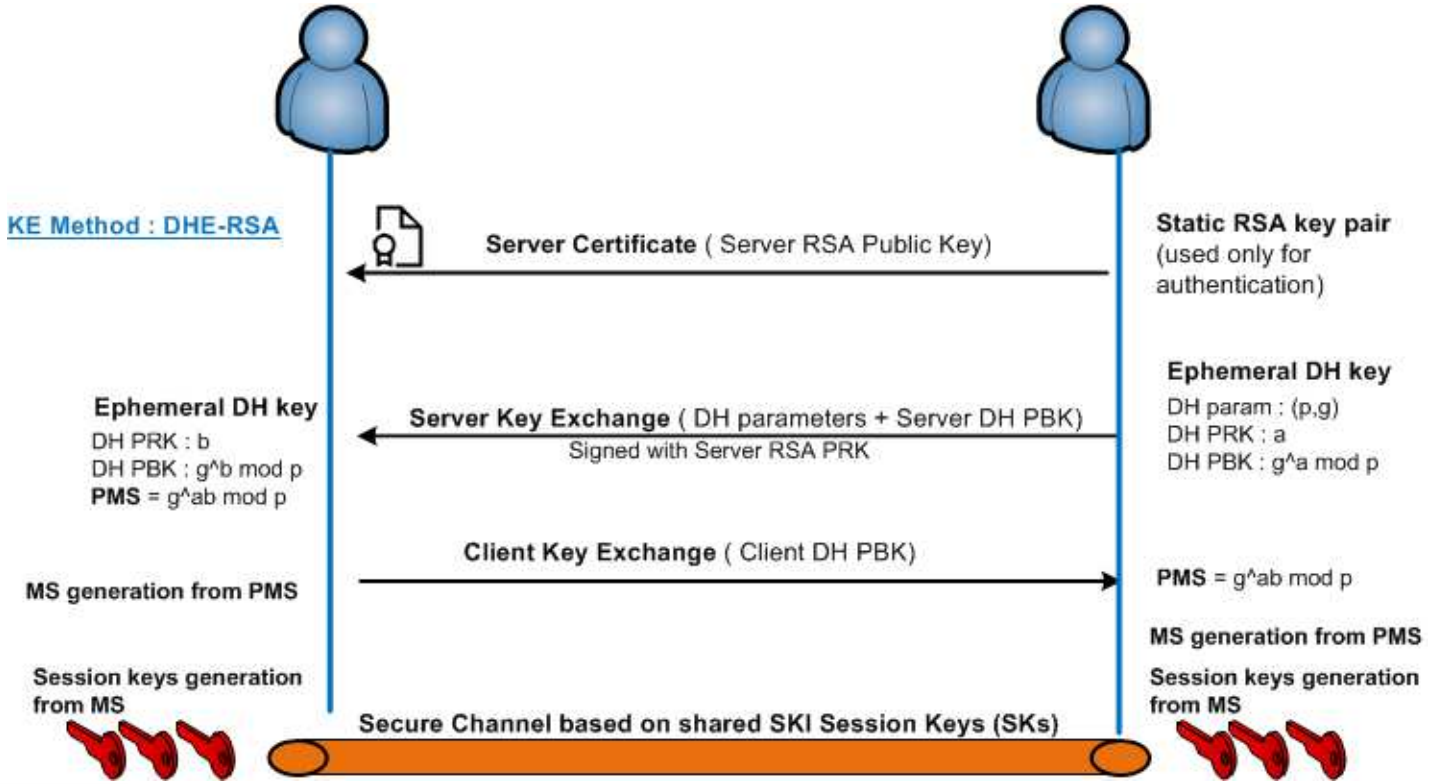
6.3 – Cryptographie Asymétrique (PKI)

- Authentification (mutuelle ou unilatérale)
  - Echange de certificats PBK, et authentification des échanges via la vérification de la signature digitale (ex: algorithme RSA, DSA ou ECDSA)
- Génération des Clés de session (SKI)
  - Etablissement d'un secret commun, puis dérivation des clés de session à partir du secret commun via une fonction de dérivation KDF (Key Derivation Function)
- Critère Majeur pour la selection d'un protocole KE
  - Respect de la propriété PFS (Perfect Forward Secrecy)
  - Definition: la compromission d'un secret lié à une session KE actuelle ne doit pas compromettre la confidentialité des communications passées (sessions KE antérieures)
  - De ce fait l'établissement du secret commun ne peut en aucun cas se baser exclusivement sur des clés statiques / longue durée mais doit mettre en œuvre des clés ephémères
  - Cas du standard SSL-TLS
    - Protocole KE RSA : ne garantit pas la PFS (basé uniquement sur la paire de clés statique RSA)
    - Protocoles DHE-RSA, ECDHE-RSA, DHE-DSS : garantissent la PFS

6.3 – Cryptographie Asymétrique (PKI)

Exemple de Session KE avec PFS : TLS avec protocole KE DHE-RSA

- Secret commun (PMS : pre-master secret) via algorithme DHE : Ephemeral Diffie Hellman
  - Garantit la PFS
- Authentification des échanges DH via algorithme RSA 'signature digitale) et paire de clés statique / longue durée
  - La compromission de la PRK RSA n'impacte pas la PFS



6.3 – Cryptographie Asymétrique (PKI)

Protocoles et Primitives KE du NIST

- C(ne, ps) : nombre de paires de clés PBK / PRK statiques / éphemères

NIST SP800-56A => Key Agreement Protocols		
	KA Protocols	**Primitives**
C(2e, 2s)	dhHybrid1	FFC-DH
	Full Unified Model	ECC-CDH
	MQV2	FCC-MQV
	Full MQV	ECC-MQV
C(2e, 0s)	dhEphem	FFC-DH
	Ephemeral Unified Model	ECC-CDH
C(1e, 2s)	dhHybridOneFlow	FFC-DH
	One-Pass Unified Model	ECC-CDH
	MQV1	FFC-MQV
	One-Pass MQV	ECC-MQV
C(1e, 1s)	dhOneFlow	FFC-DH
	One-Pass Diffie-Helmann	ECC-CDH
C(0e, 2s)	dhStatic	FFC-DH
	Static Unified Model	ECC-CDH

NIST SP800-56A => Key Transport Protocols		
	Protocol	**Primitives**
One KT defined	KA scheme : subset of C(2e, 2s), C(1e, 2s), C(1e, 1s), C(0e, 2s)	Subset of primitives listed above

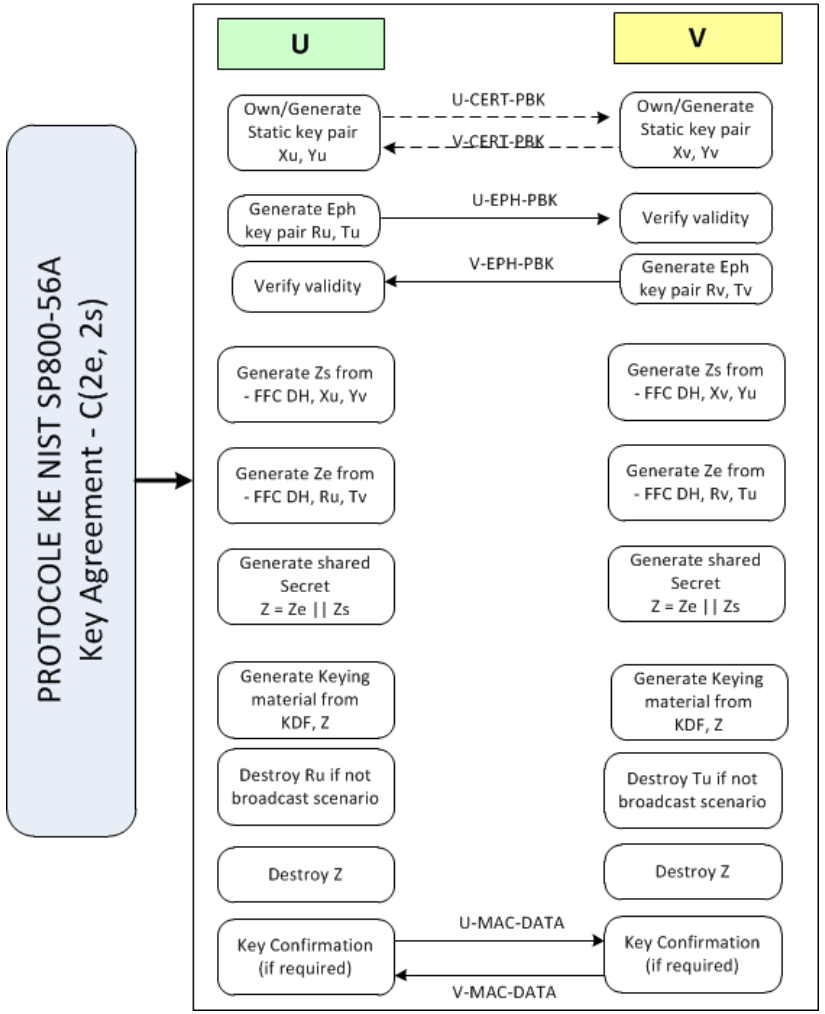
NIST SP800-56B => Key Agreement Protocols	
KA Protocols	**Primitives**
KAS1-basic	RSASVE (RSA EP/DP)
KAS1- key confirmation – Party V	RSASVE
KAS2-basic	RSASVE (RSA EP/DP)
KAS2-key confirmation – Party V	RSASVE
KAS2-key confirmation – Party U	RSASVE
KAS2-key confirmation – Bilateral	RSASVE

NIST SP800-56B => Key Transport Protocols	
KT Protocols	**Primitives**
KTS-OAEP-basic	RSA-OAEP
KTS-OAEP-key-confirmation – Party V	RSA-OAEP
KTS-KEM-KWS-basic	RSA-KEM-KWS
KTS-KEM-KWS-key-confirmation – Party V	RSA-KEM-KWS

6.3 – Cryptographie Asymétrique (PKI)

Example de session KE basée sur le standard NIST SP800-56A Standard (DLC)

- Exemple de Session KE basée sur un protocole KE du NIST
  - Standard SP800-56A (DLC)
  - Protocole KA (Key Agreement)
  - Protocole C(2e, 2s) avec authentification mutuelle et confirmation de clé
- Note: Nombre limité de messages échanges dans le handshake
- Impacts sur les opérations satellite



6.3 – Cryptographie Asymétrique (PKI)

Ski/PKI: Recommandations sur les tailles de clé

- Court terme
  - SKI: 128 bits – PKI: 3072 bits (RSA, DH) et 256 bits (ECC)
- Long Terme (menace des ordinateurs quantiques)
  - SKI: 256 bits – PKI: 15360 bits (RSA, DH) et 512 bits (ECC)

Extrait of Rapport ECRYPT 2018

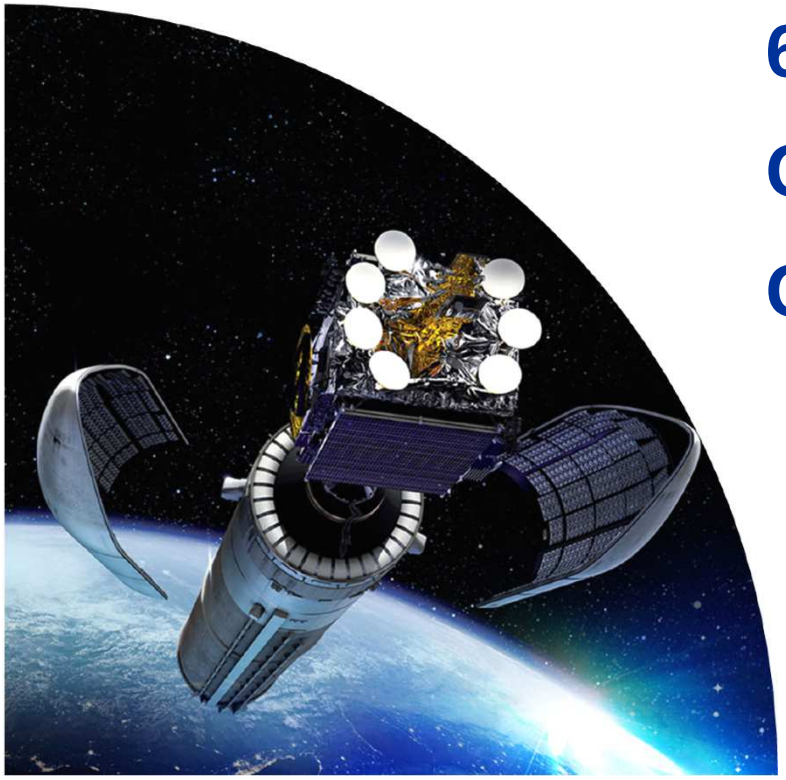
	Parameter	Legacy	Future System Use	
			Near Term	Long Term
Symmetric Key Size	k	80	128	256
Hash Function Output Size	m	160	256	512
MAC Output Size*	m	80	128	256
RSA Problem	$\ell(n) \geq$	1024	3072	15360
Finite Field DLP	$\ell(p^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512
ECDLP	$\ell(q) \geq$	160	256	512
Pairing	$\ell(p^{k \cdot n}) \geq$	1024	6144	15360
	$\ell(p), \ell(q) \geq$	160	256	512

6.3 – Cryptographie Asymétrique (PKI)

- Importance cruciale du respect des spécifications pour les algorithmes et protocoles cryptographiques (PKI / SKI) lors de leur implémentation

- Cas de la vulnérabilité de la PS3 SONY (2011)
  - Fonction: Signature Digitale pour la vérification des logiciels / jeux installés
    - PBK installée dans chaque PS3 and PRK gerée chez / par SONY
  - Incorrecte implémentation de la specification ECDSA : non respect de la génération du pattern k aléatoire
    - PRK SONY compromise : permit à tout Utilisateur d'installer un logiciel avec la PRK compromise

- **Source ci-dessous: "**PS3 hacked through poor cryptography implementation_ Ars Technica.htm"
  - *A group of hackers called fail0verflow claim they've figured out a way to get better control over a PlayStation 3 than ever before. After they worked through a number of Sony's security measures, they found the keystone to gaining access to the system's innards was the PS3's poor use of public key cryptography.*
  - *After beating several other security measures, the group was able to locate the PS3's ECDSA signature, a private cryptographic key needed to sign off on high-level operations. Normally, these kinds of keys are difficult to figure out, and require running many generations of keys to crack.*
  - *But when fail0verflow worked backwards from generated keys*
    - *They found out that a parameter that **should have been randomized** for each key generation **wasn't being randomized at all.***
    - *Instead, the PS3 was **using the same number for that variable**, every single time, making it easy to work out acceptable keys.*



6.4 – Techniques émergentes : Cryptographie quantique et Cryptographie post-quantique

6.4 : Cryptographie Quantique et Post Quantique

Menaces sur la cryptographie liées à l'avènement des ordinateurs quantiques

- La cryptographie asymétrique **(PKI)** est basée sur une sécurité **conditionnelle**
  - Les algorithmes PKI reposent sur des problèmes mathématiques réputés « difficiles »
    - DLC : Logarithme discret (Diffie Hellman, Courbes elliptiques)
    - IFC : Factorisation des grands nombres (RSA)
  - La sécurité de la cryptographie asymétrique (PKI) se base sur l'hypothèse (difficulté calculatoire) que ces problèmes ne peuvent être résolus avec les moyens actuels et dans des délais suffisamment courts pour menacer la mission concernée
  - Cette hypothèse va progressivement être battue en brèche avec l'avènement des ordinateurs quantiques utilisant l'algorithme de Shor
- La cryptographie symétrique (SKI) est également basée sur une sécurité **conditionnelle**
  - Cependant de par le design des algorithmes cryptographiques SKI, elle n'est pas considérée comme fortement menacée par l'avènement des ordinateurs quantiques
  - Sous réserve d'utiliser des clés de 256 bits au minimum (ex: avec AES)
- 2 solutions pour contrer la menace sur la PKI conventionnelle
  - Cryptographie quantique
  - Cryptographie post-quantique

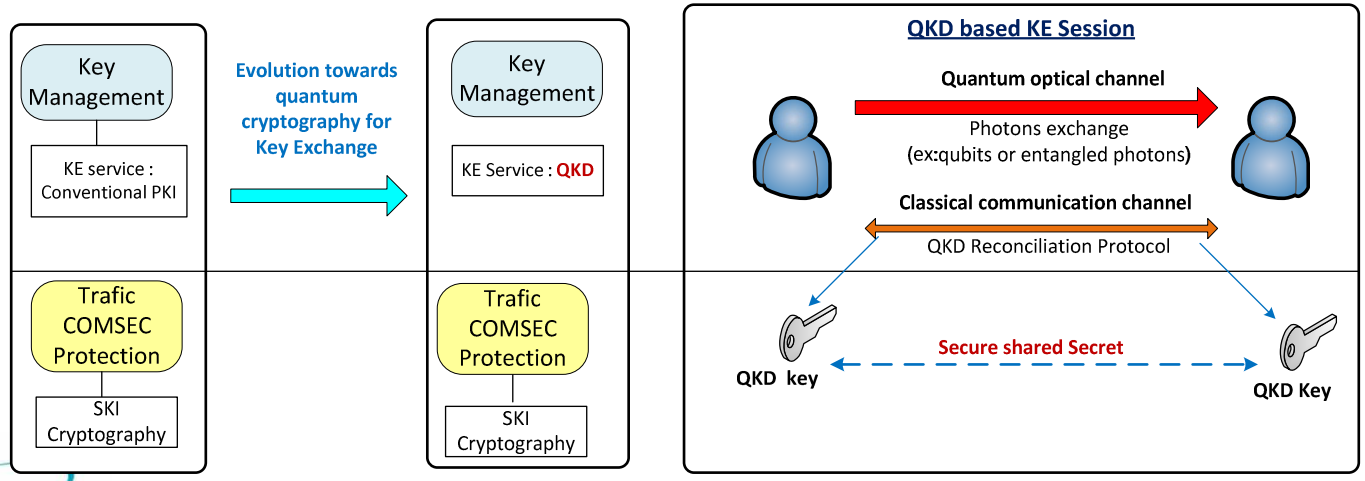
6.4 : Cryptographie Quantique et Post Quantique

Cryptographie post-quantique / Post Quantum Cryptography (PQC)

- Compétition NIST initiée depuis 2017 pour développer de nouveaux algorithmes PKI résistant aux ordinateurs quantiques (algorithme de SHOR)
  - Premier round: 69 candidats
  - Second round (Annonce Janvier 2019): 26 candidats sélectionnés par le NIST
  - Délai global : 5-7 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
- Applications PKI adressées par les algorithmes PQC
  - Asymmetric encryption
  - Key Exchange
  - Digital Signature

Cryptographie Quantique / QKD (Quantum Key Distribution)

- La cryptographie quantique est une alternative en plein développement, pour laquelle la sécurité repose sur des postulats physiques (physique quantique), par principe inviolables .
  - Elle permet au niveau de la génération et distribution des clés d'offrir une sécurité inconditionnelle se basant sur des impossibilités imposées par les lois de la physique quantique , et non plus sur la puissance supposée des moyens de calcul d'un tiers mal intentionné
  - Garantie absolue de la confidentialité et de l'intégrité des clés échangées sur un canal optique non protégé, avec détection systématique de toute intrusion sur ce canal optique
- La cryptographie quantique définit une nouvelle fonction d'établissement des clés dite QKD (Quantum Key Distribution) garantissant une sécurité inconditionnelle des clés générées
- Elle se traduit au niveau des architectures de sécurité, par l'introduction d'une nouvelle primitive KE (QKD) au sein de la fonction de Gestion des Clés



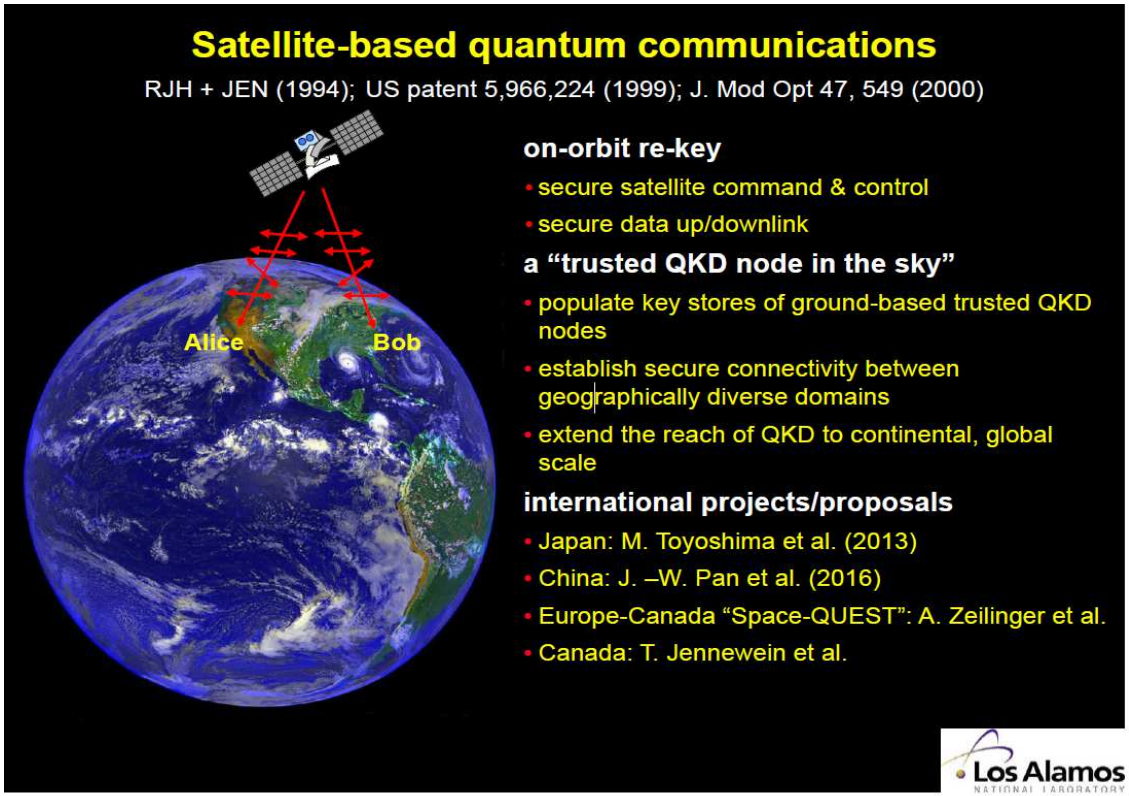
6.4 : Cryptographie Quantique et Post Quantique

Introduction de la Cryptographie Quantique dans le spatial

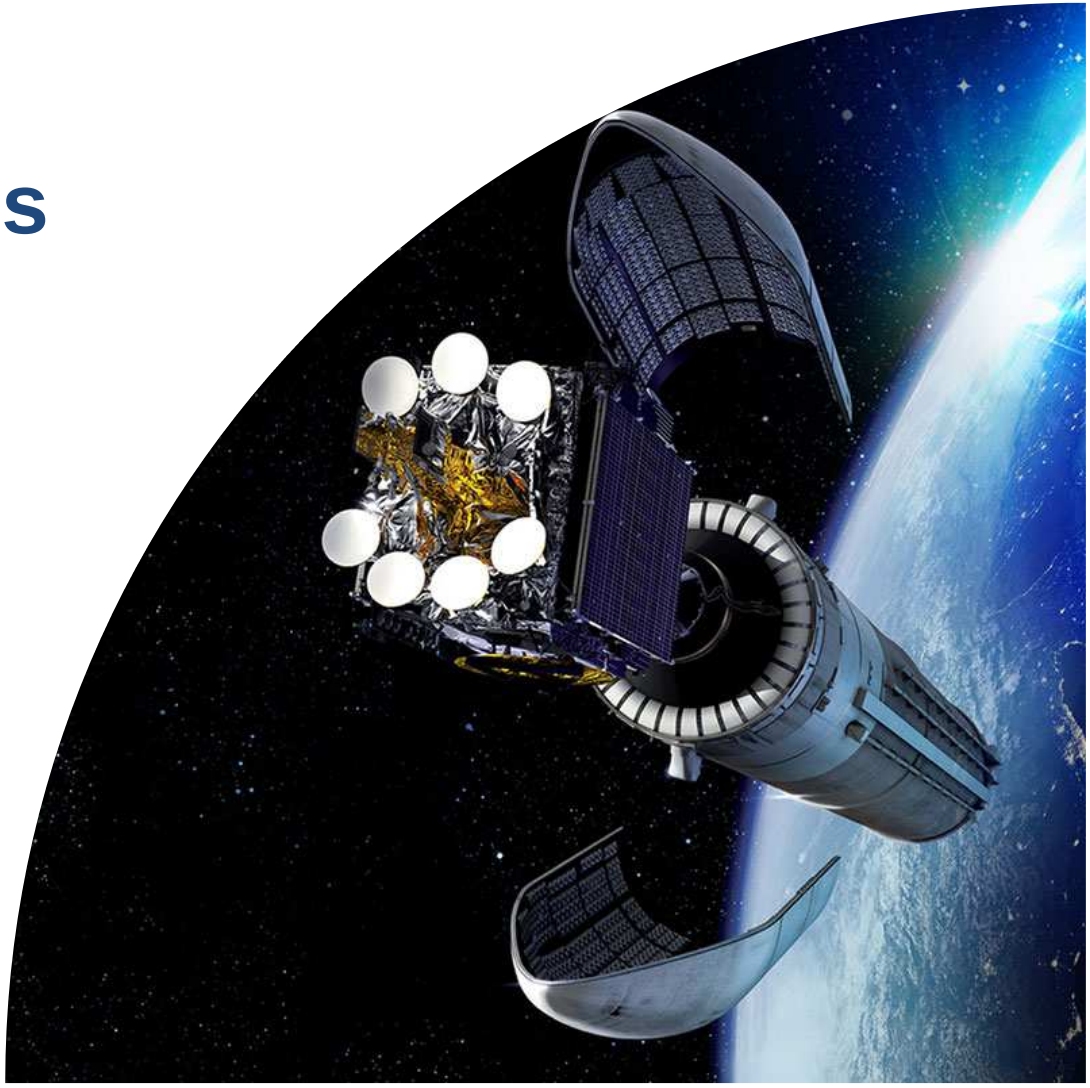
- Application à l'établissement de clés en temps réel par liaison optique quantique entre un satellite et des stations Sol
- De nombreux projets / démonstrateurs en cours (Ex: ESA SCYLIGHT program)
- Buzz suite au lancement du premier satellite quantique par la Chine en juillet 2016

Exemple d'application

- Le satellite passe au-dessus de la station A et établit une clé KA via la QKD
- Le satellite passe au-dessus de la station B et établit une clé KB via la QKD
- Le satellite repasse au-dessus de la station A et transmet KA XOR KB
- Les Sites A et B peuvent alors établir une communication sol sécurisée par la clé commune KB et considérée comme inviolable par la QKD



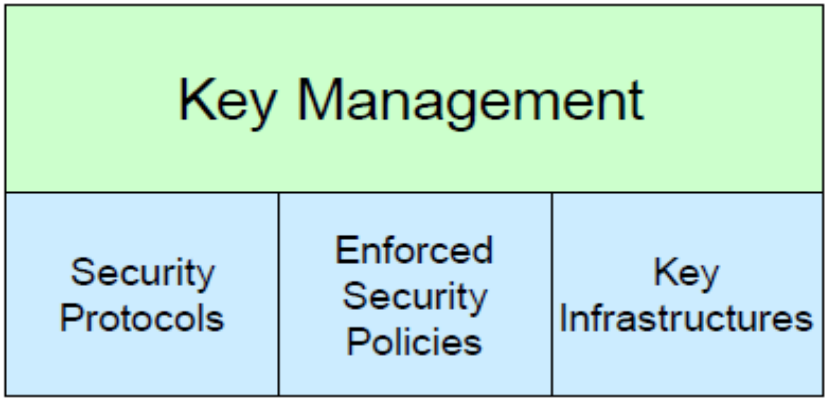
7 – Gestion des Clés



7 - Gestion des Clés

Modèle de référence CCSDS pour la Gestion des Clés

- Ref: CCSDS 350.6-G-1

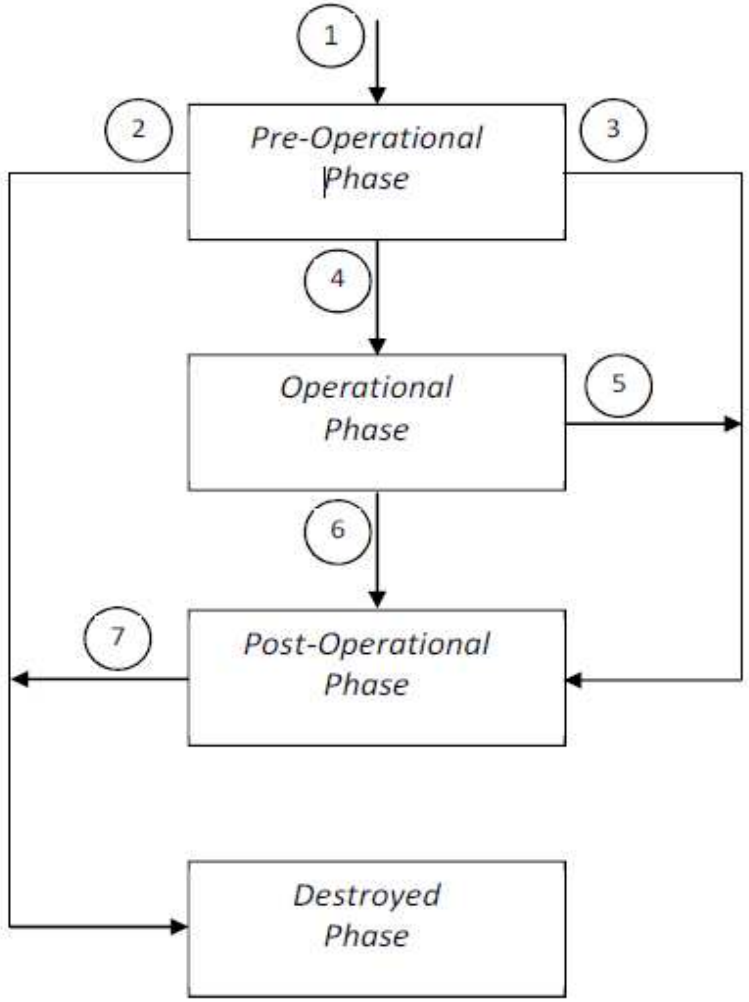


Trois blocs fonctionnels principaux

- Security Protocols
  - Authentification unilatérale/ mutuelle
  - Etablissement de Clés (KE)
  - Ex: protocoles NIST KE, IKE / IPSEC, SST-TLS, SSH
- Security Policies
  - Procédures opérationnelles relatives à la gestion des clés
  - Couvrent notamment la génération & distribution des clés
- Key Infrastructures
  - Secret Key infrastructure (SKI)
  - Public Key Infrastructure (PKI)

Cycle de Vie des Clés : Modèle de Référence NIST : SP800-57

- Pre-Operational Phase
  1. System and User Initialization;
  2. Entity Registration;
  3. Keying-Material Installation;
  4. Key Establishment;
  5. Key Registration.
- Operational Phase
  1. Normal Operational Storage Function;
  2. Continuity of Operations Function;
  3. Key Change Function;
  4. Key Derivation Function.
- Post-Operational Phase
  1. Key Archive;
  2. Key Recovery;
  3. Entity De-registration Function;
  4. Key De-registration Function;
  5. Key Destruction Function;
  6. Key Revocation Function.
- Destroyed Phase

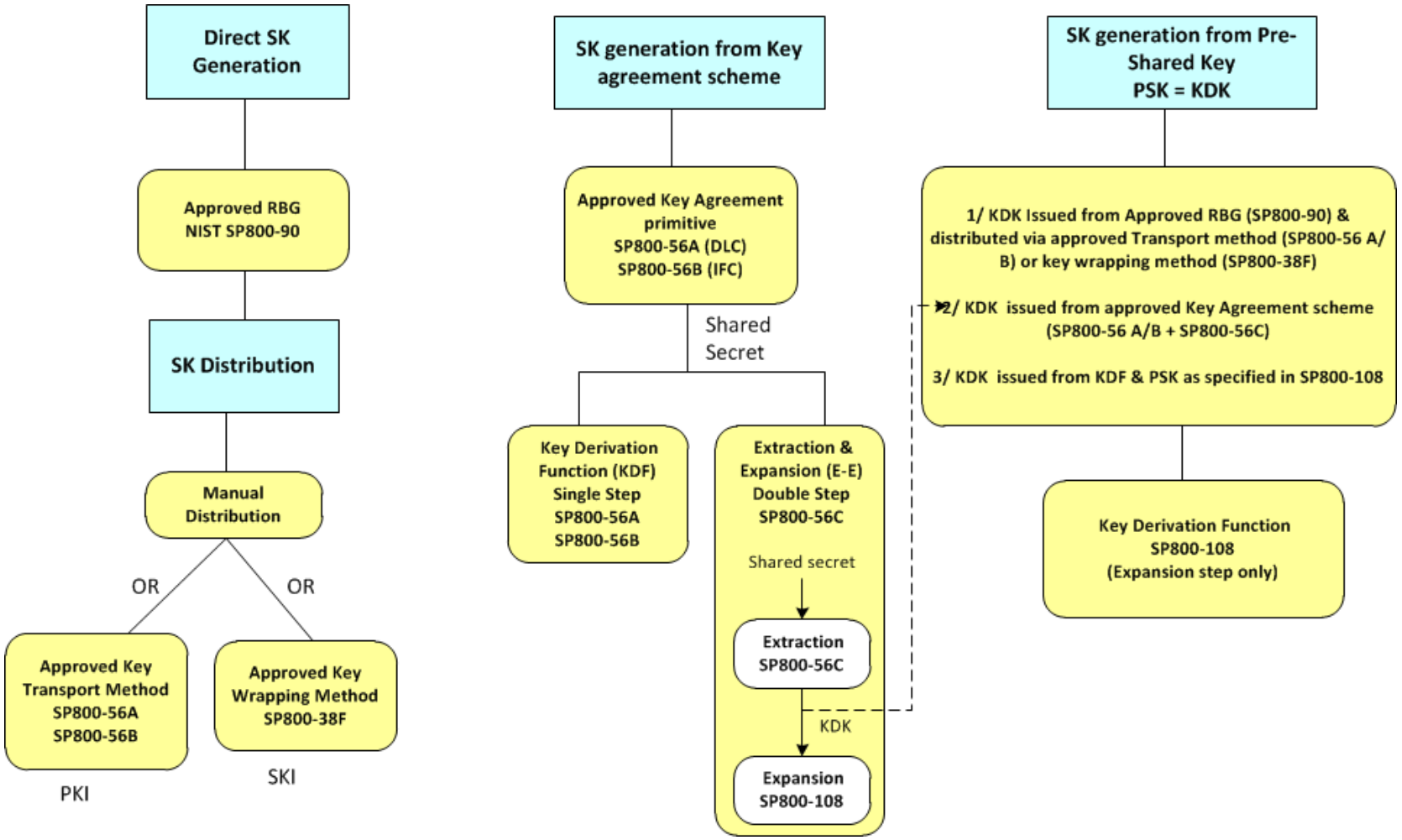


7 - Gestion des Clés

- La Gestion des Clés relatives à la protection des communications spatiales inclut les phases suivantes
  - Génération des clés COMSEC ou TRANSEC
    - Clés de Trafic, Clés de wrapping (KEK : Key Encryption Key) pour le renouvellement en Vol
    - Fonction OTAR : Over The Air Rekeying
  - Distribution sécurisée des Clés au Sol
    - Protection par une clé de wrapping Sol (GPK : Ground Protection Key)
  - Chargement des Clés dans le satellite avant le Tir (Injection des clés)
  - Gestion des clés durant la mission / exploitation du satellite
    - Changement régulier de clé : suivant la crypto-période choisie
    - Renouvellement en vol (OTAR)
    - Invalidation / Effacement de Clé
      - Clé obsolète – crypto période expirée ou clé compromise

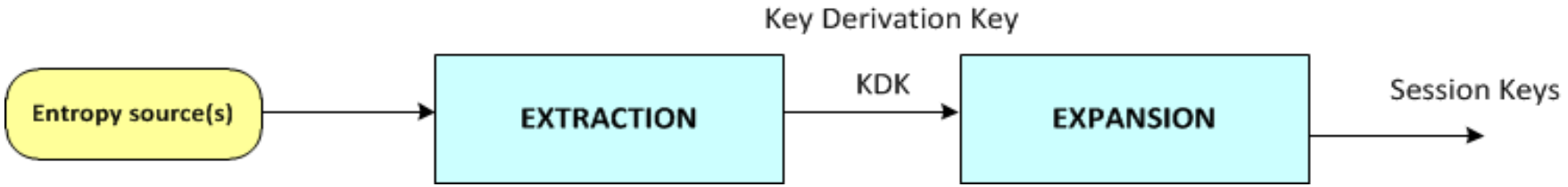
7 - Gestion des Clés

NIST – Standard de référence pour la génération des clés: NIST SP800-133



7 - Gestion des Clés

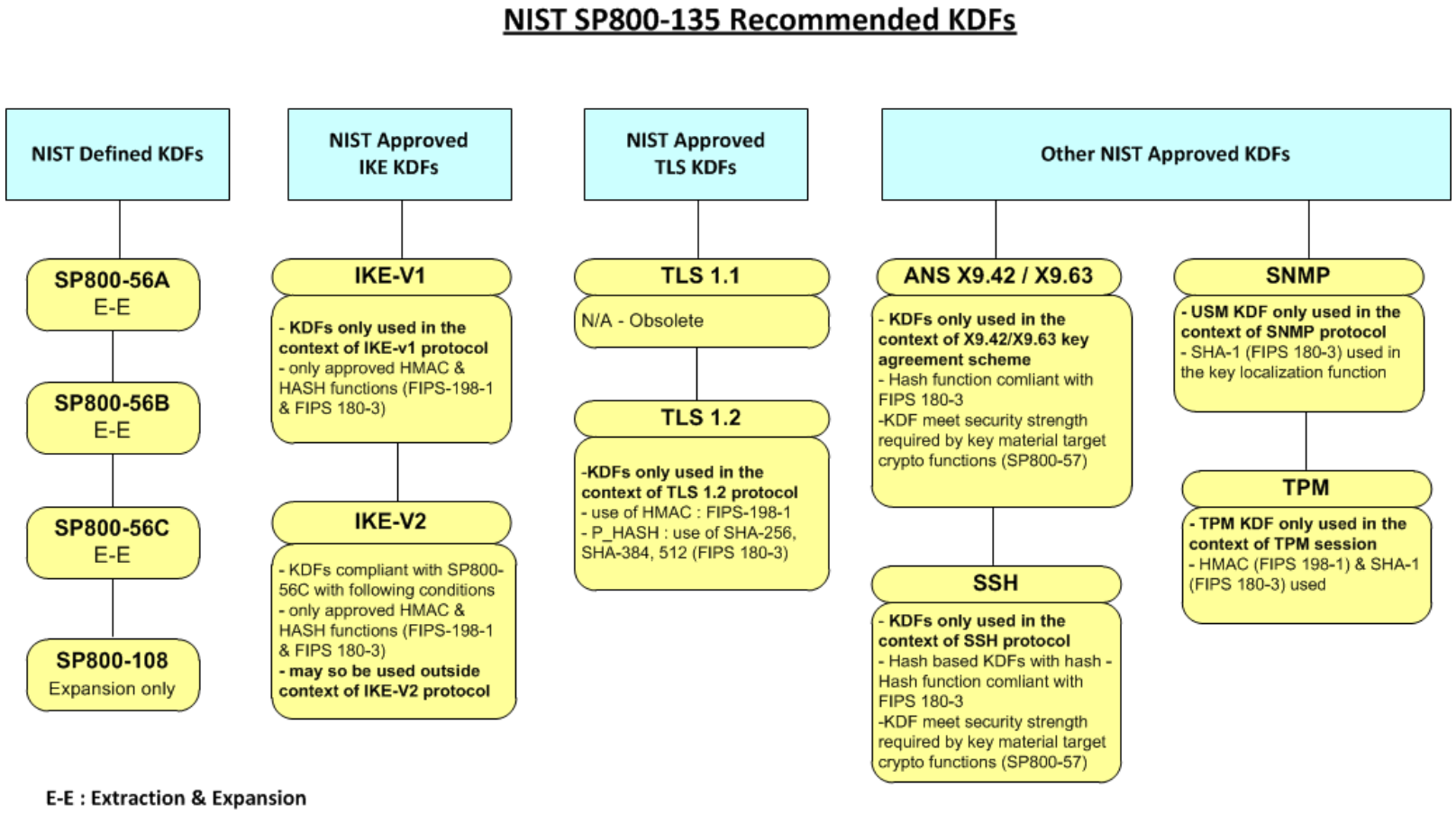
- Dans les solutions actuelles les clés de trafic COMSEC / TRANSEC (SKI) sont générées par un PRNG
  - Pseudo-Random Number Generator
- Modèle E-E
  - **E**xtraction de l'Entropie & génération d'une KDK (Key Derivation Key)
  - **E**xpansion : dérivation des clés de trafic à partir de la KDK



- Les clés de trafic SKI sont protégées par une clé de wrapping
  - Ex standard NIST SP800-38F pour algorithme Key Wrapping
  - Pas de distribution de clés rouges (claires) au sol

7 - Gestion des Clés

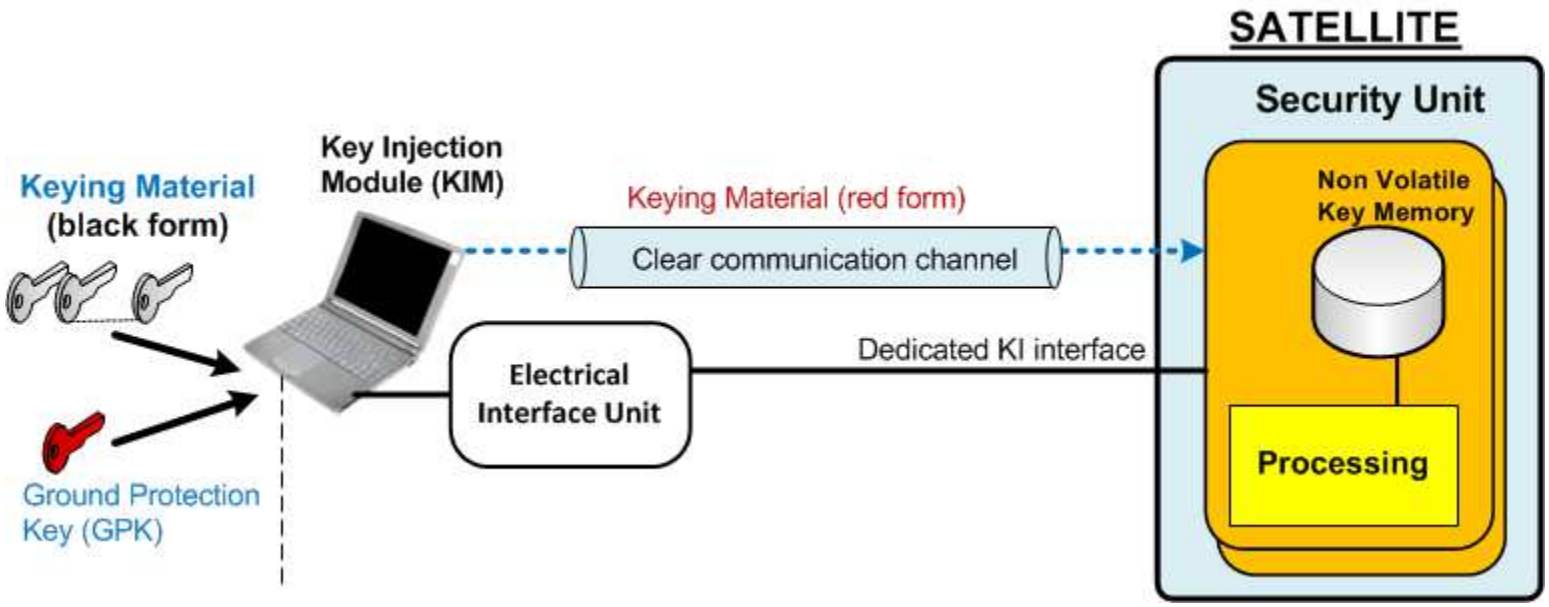
NIST - Standard de référence pour la dérivation des Clés : NIST SP800-135



7 - Gestion des Clés

Chargement des clés dans le satellite : Injection des Clés

- Opération effectuée au Sol juste avant le Tir du satellite
- Chargement des Clés SKI de trafic : TPK (Trafic Protection Key)
- Chargement des Clés SKI OTAR de protection des clés de trafic : KEK (Key Encryption Key)



7 – Gestion des Clés

Gestion des Clés de Trafic (SKI) en Vol

- Changement régulier de clé : selon une crypto-période à définir (ex: 1 mois)
  - La crypto-période est davantage liée aux risques d'exposition et de compromission de clés au Sol que liée aux exigences cryptographiques
  - Avec un mode AO ou AE utilisant l'AES, la limite théorique est définie par le nombre d'appels AES qui pour une clé donnée ne doit pas dépasser 2^64
    - Recommandation ANSSI : nombre d'appels < 2^48
  - Autres contraintes cryptographiques
    - crypto période < période du compteur anti-rejeu
    - crypto période < période de l'IV
- Renouvellement des Clés en Vol : service OTAR
  - Téléchargement d'un jeu de clés protégées par une Clé de wrapping / KEK
  - Intérêt : génération et téléchargement de clés fraiches le plus tard possible durant la mission – limitation de la compromission
  - Remplacement de clés bord corrompues (ex: Radiations / SEU)

7 – Gestion des Clés

Limites de la technologie SKI pour la Gestion des Clés

❑ Impacts de la compromission des clés su Sol

- ➢ Pas de recouvrement en vol possible des clés satellite si compromission des clés au Sol
- ➢ KEK bord compromises => Utilisation de la fonction OTAR impossible pour télécharger un nouveau jeu de clés

❑ Limites de l'Injection des clés dans le satellite

- ➢ Chargement des clés en clair car état initial = pas de clé secrète / partagée à bord
- ➢ Canal d'injection non protégé : confidentialité / intégrité non garantis
  - Protection par des mesures radio-fréquence (protection TEMPEST)
- ➢ Pas d'authentification possible de l'équipement d'injection des clés par le satellite
  - On ne peut par design, garantir à un Client qu'il est le seul capable de charger des clés dans le satellite
- ➢ Protection par des mesures classiques (ex: scellé, vidéo) et organisationnelles

7 – Gestion des Clés

Limites de la technologie SKI pour la Gestion des Clés

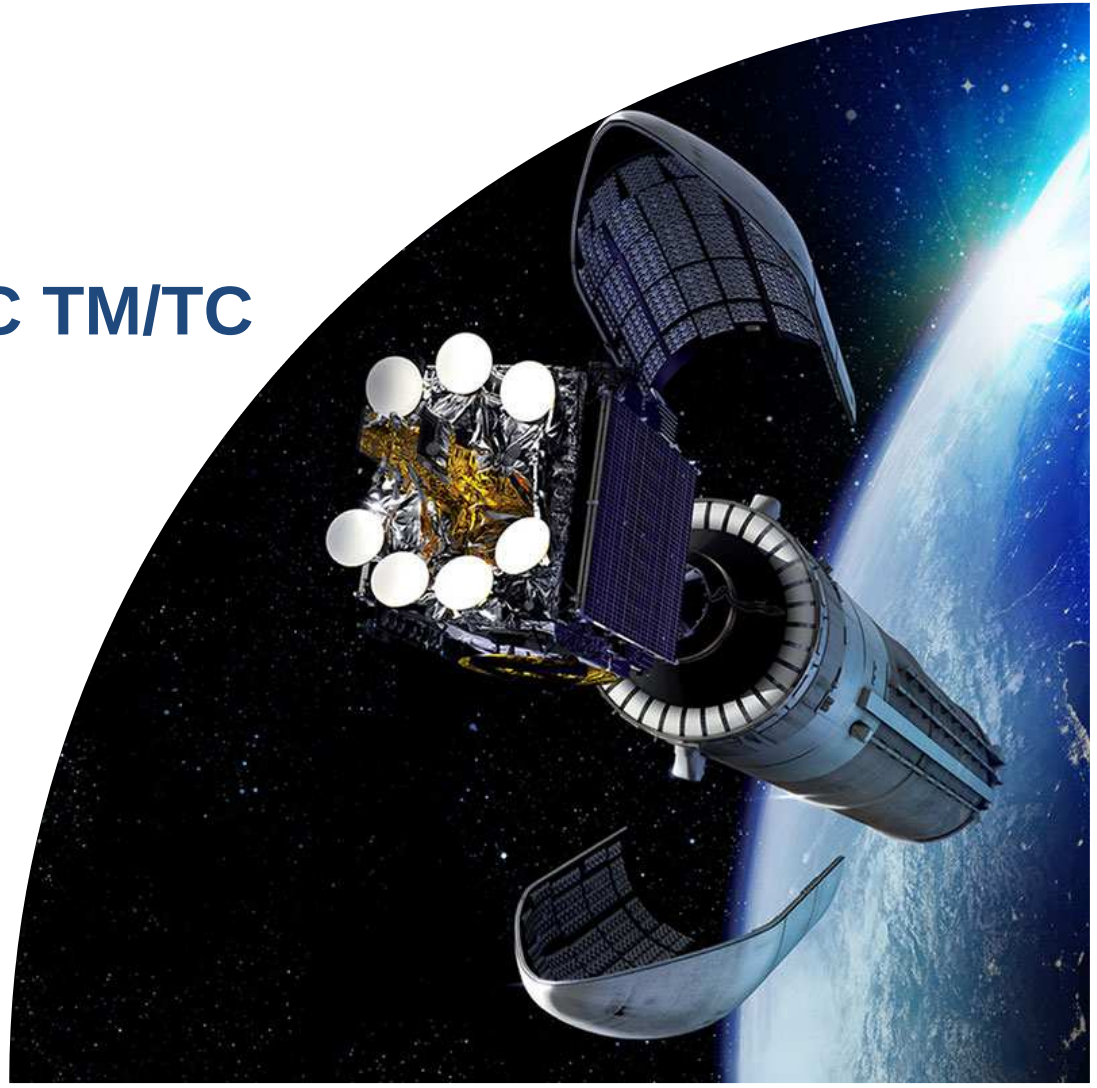
- Complexité de la Gestion des Clés Multi-Utilisateurs
  - Mission Observation : jusqu'à 1000 utilisateurs Sol
  - La gestion des clés TM-PL COMSEC obéit à des contraintes de nature dynamique (enregistrement, début / Fin du service, révocation)
  - Avec les solutions SKI, l'utilisation de clés partagées ne permet pas de lien formel possible entre l'Identité d'un Utilisateur et une Clé donnée
  - Faible flexibilité

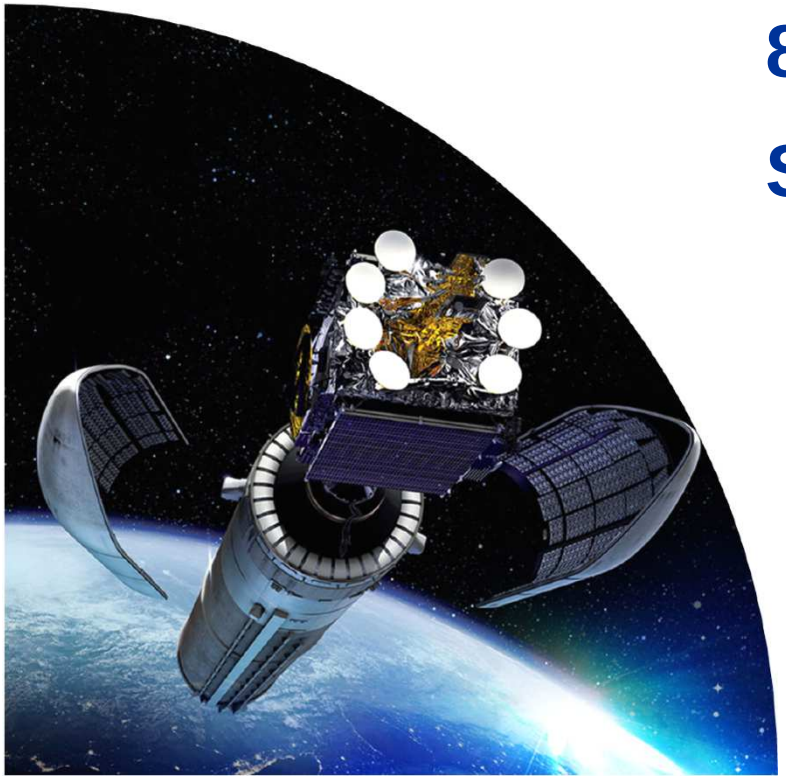
Evolution naturelle vers la Technologie PKI pour la Gestion des Clés Satellite

- Mise en oeuvre de protocoles PKI de type KE (Key Establishment) pour le chargement / renouvellement des clés
- Permet de s'affranchir des principaux défauts / contraintes des systèmes conventionnels / SKI
- Plus grande complexité d'implémentation (ex: matérielle) liée à la cryptographie KI

8 – Application aux Systèmes Spatiaux

Protection COMSEC TM/TC

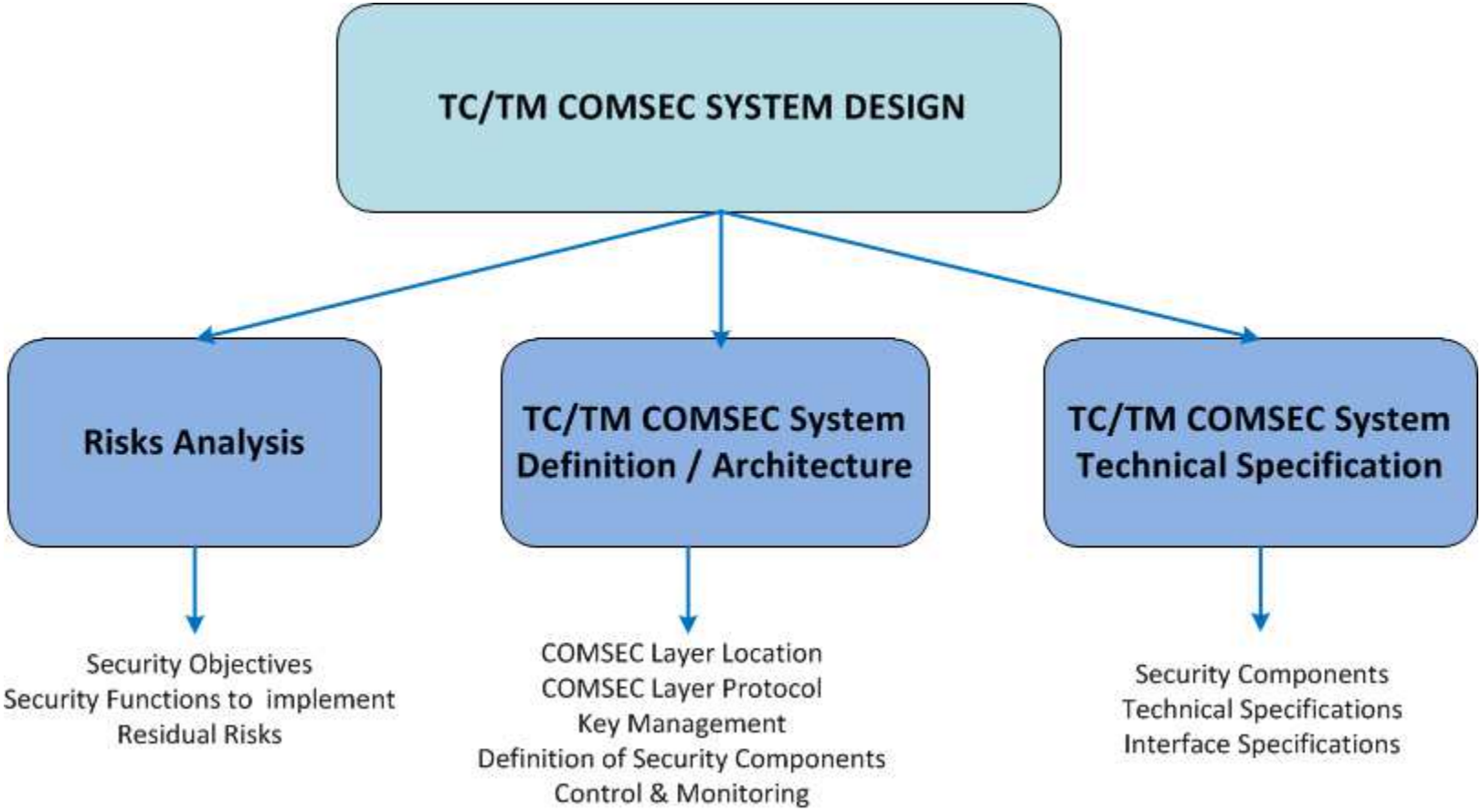




8.1 – Conception d'un Système COMSEC TM/TC

8. 1 – Conception d'un système COMSEC TM/TC

Activités de Conception d'un Système COMSEC TC/TM



8.1 – Conception d'un Système COMSEC TM/TC

Conception d'un Système COMSEC TM/TC

- Analyse de Risque - les sorties principales sont:
  - Les fonctions / mesures de sécurité à implémenter (Authentification et/ou Chiffrement)
  - Les vulnérabilités résiduelles : vulnérabilités non couvertes par les fonctions de sécurité identifiées, mais considérées comme acceptables
- Architecture du Système COMSEC (1/2)
  - Position de la couche Sécurité : couches basses (transmission/transport) / couches hautes (applicatives)
  - Le protocole de la couche Sécurité définit les interactions / échanges (handshake), et le format détaillé des messages échangés
    - Ex: le standard CCSDS Space Data Link Protocol, définit le format des champs Sécurité à appliquer aux trames TC / TM / AOS sécurisées
  - Composants Sécurité : Equipements ou Fonctions logicielles Bord & Sol résultant de l'allocation des fonctions de sécurité
    - Eqt Chiffreur / Déchiffreur matériel bord ou Sol
    - Couche Logicielle Chiffreur / Déchiffreur bord ou Sol

Architecture du Système COMSEC (2/2)

- La Gestion des Clés traite l'ensemble des fonctions à implémenter pour couvrir le cycle de vie des clés :
  - Génération, distribution, changement, renouvellement en vol, invalidation, stockage, protection, ..
- Le Contrôle et Monitoring définit
  - Les commandes de contrôle et configuration de la fonction Sécurité bord
    - Activation de la sécurite (Secure mode), désactivation (Clear mode)
    - Changement de la clé courante
    - Modification / Reset du compteur anti-rejeu
    - Téléchargement d'une clé en vol (OTAR : over the air rekeying)
  - Les informations de configuration / status / alarmes redescendues vers le sol et permettant une observabilité de la fonction Sécurité bord
- Specification Techniques
  - Elaboration des exigences techniques des différents composants Sécurité Bord & Sol ainsi que des interfaces associées, afin de permettre leur développement

8.1 – Conception d'un Système COMSEC TM/TC

Protocole : Couche TC / TM COMSEC

- Avant 2015:
  - Seul standard existant : TC Authentification ESA (ESA PSS-05-151)
  - Toutes les solutions TC/TM Encryption (avec chiffrement) sont forcément propriétaires
- Depuis Sept 2015
  - Le standard CCSCS SDLS est sorti officiellement en Issue 1
  - Les principaux Clients / Opérateurs sont fortement intéressés à s'appuyer sur un standard garantissant l'interopérabilité entre satellites et segments sol issus de fournisseurs différents
  - Le protocole de la couche définit les interactions / échanges (handshake), et le format détaillé des messages échangés

Secured Message Format with CCSDS SDLS Protocol Standard

Message Authentication Code (MAC)

8.1 – Conception d'un Système COMSEC TM/TC

Standard CCSDS SDLS Fonction de Sécurité vs Paramètres Sécurité

- Authenticité : MAC
- Intégrité : MAC
- Anti-rejeu : Compteur ARSN
  associé à une fenêtre anti-rejeu incluse dans le calcul du MAC
- Confidentialité : Chiffrement

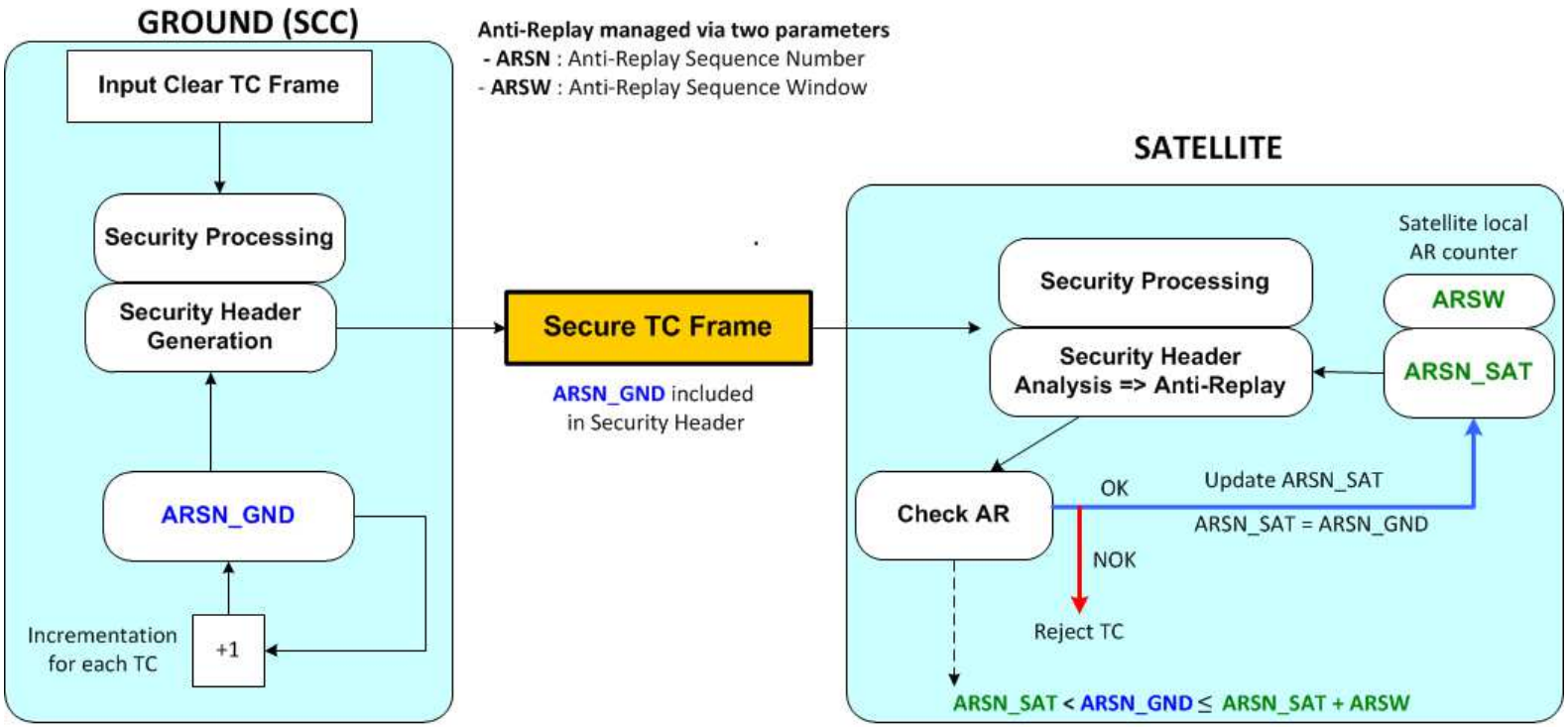
Role des Paramètres / champs Sécurité

- SPI : Security Parameter Index - Identifie une Security Association (SA)
- IV : Initialization Vector utilisé par l'algorithme (ex: GCM, CBC, CTR)
- ARSN : Anti Replay Sequence Number - compteur anti-rejeu
- Pad length : taille des octets de bourrage si padding requis par l'algorithme
  - Ex: algorithme CBC-AES requiert du padding car il ne travaille que sur des blocs de données de 128 bits
- MAC : Message Authentication Code

8.1 – Conception d'un Système COMSEC TM/TC

Protocole CCSDS SDLS : Mécanisme Anti-Rejeu

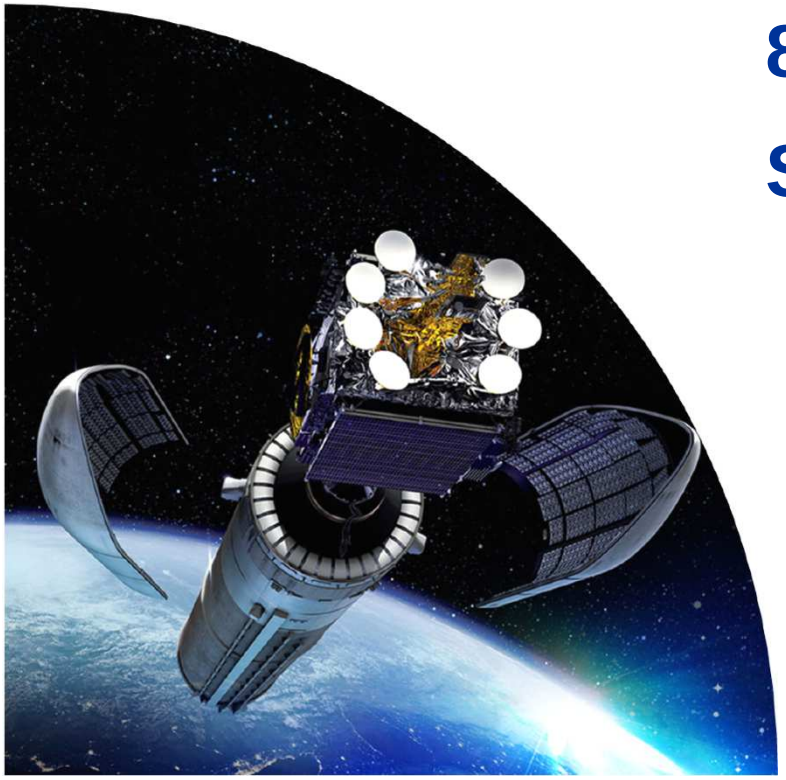
- Basé sur un compteur AR dédié et associé à une fenêtre AR



CCSDS SDLS Protocol can support both AR schemes

- Scheme A : 1 unique Anti-Replay counter per secured channel

- Scheme B : 1 Anti-Replay counter per key (with key number defined by SPI)

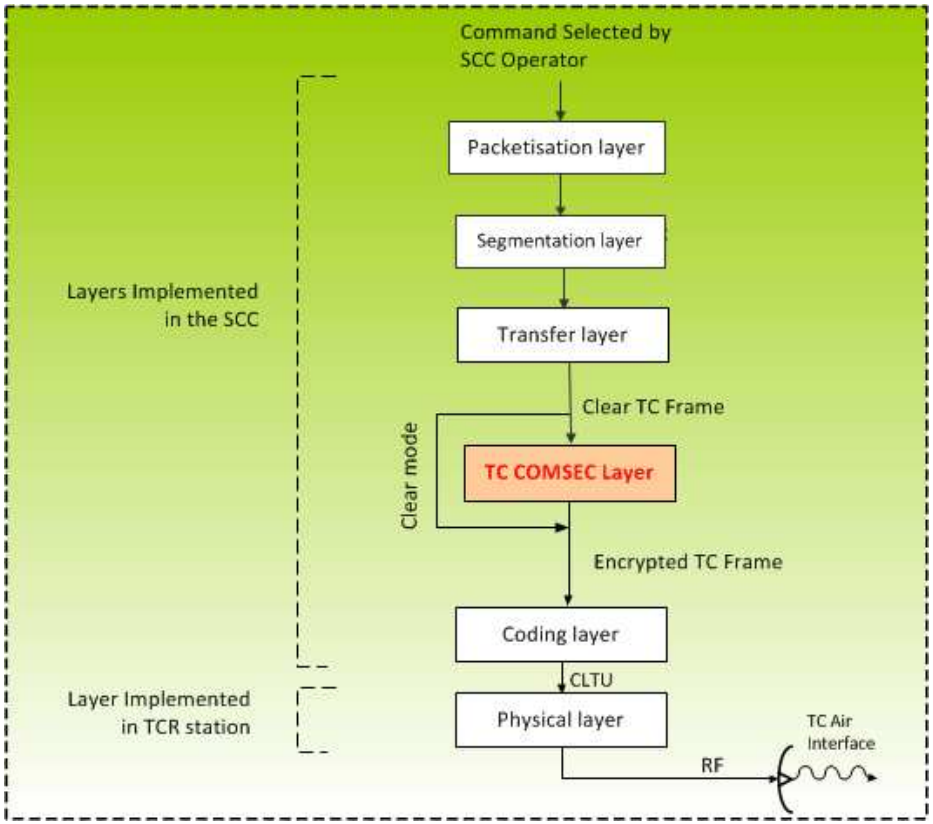


8.2 – Exemple d'Architecture de Systèmes COMSEC TM/TC

8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

Positionnement de la Couche Sécurité (TC COMSEC)

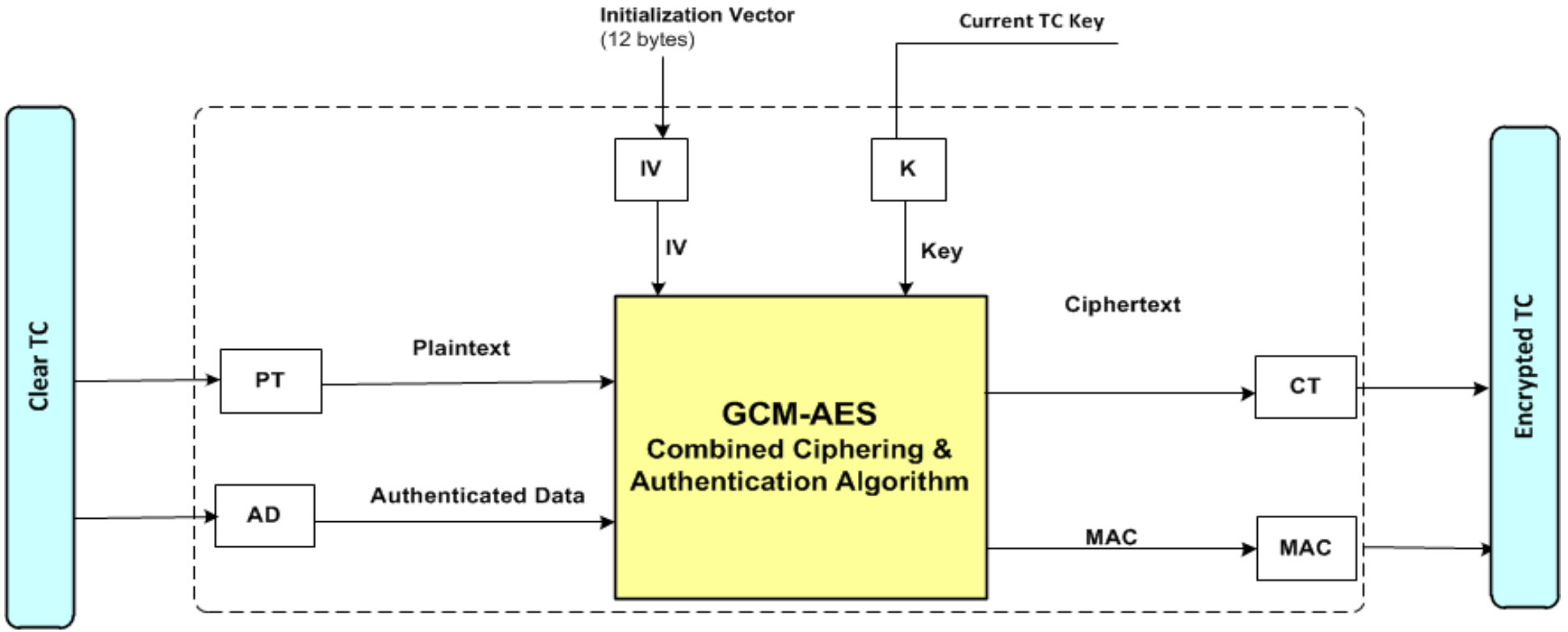
- Exemple : Opération sur des Trames de Transfert
- Note : Plus basse est positionnée la couche Sécurité plus sa couverture est élevée



8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

Cryptographie

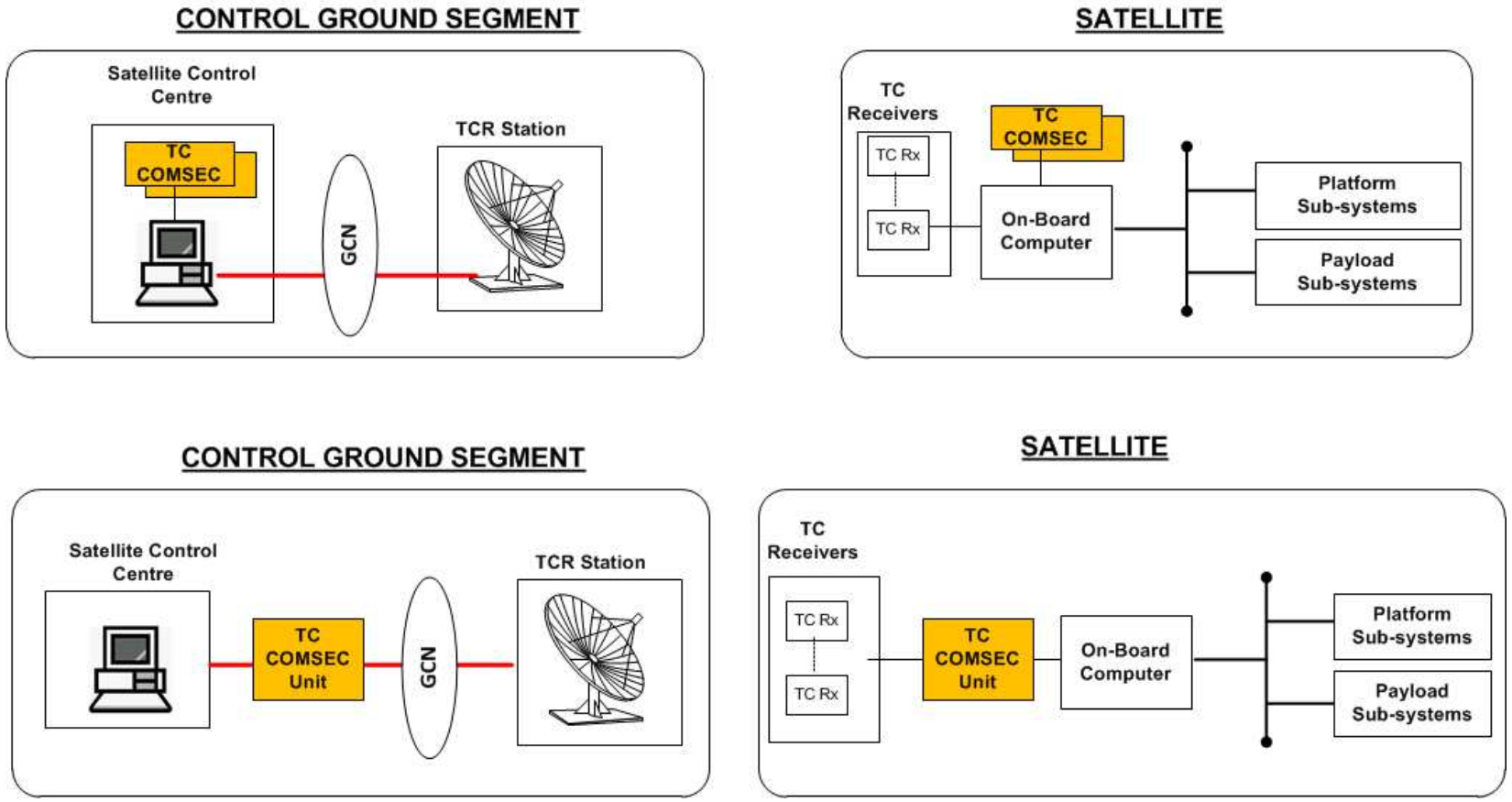
- Définition de la fonction Chiffrement d'un message TC
- Ex : Chiffrement Authentifié avec GCM-AES (NIST SP800-38D)



8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

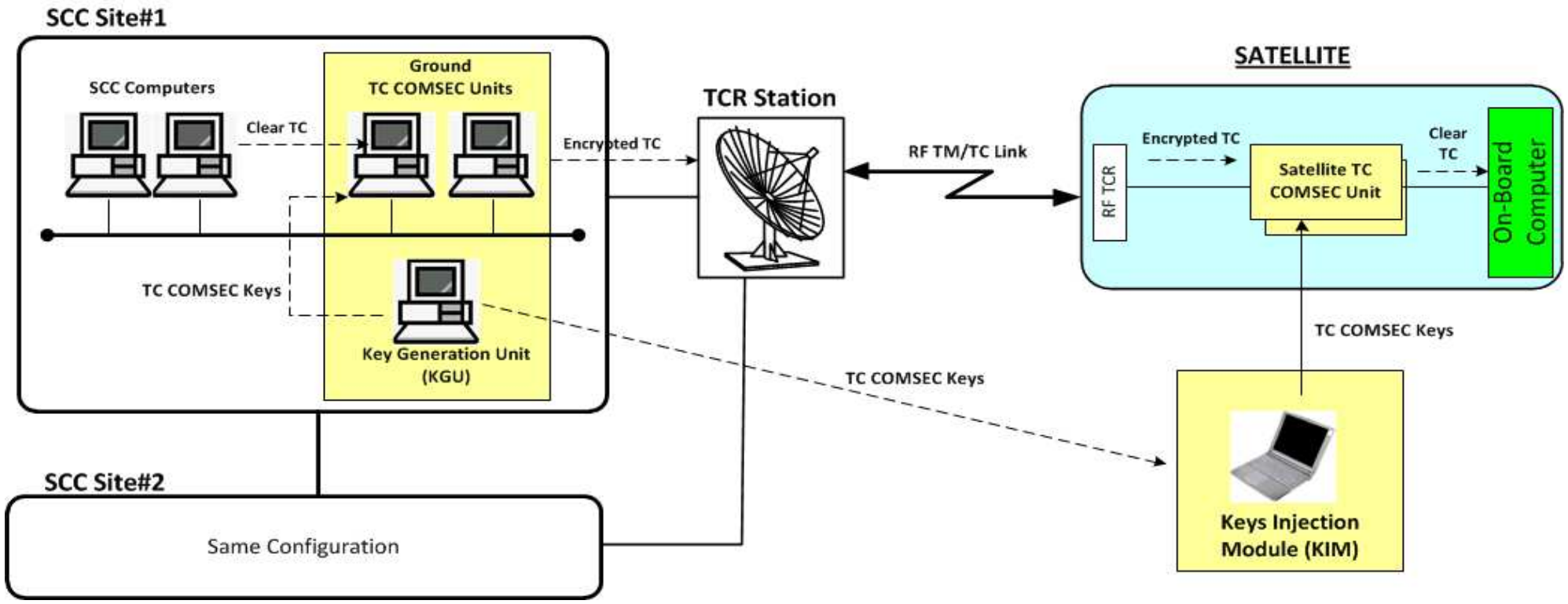
Architecture vs Niveau de Sécurité

- Haute Sécurité : Eqt Sécurité en coupure physique du flux à protéger
- Sécurité Standard : Eqt Sécurité en coupure logique du flux à protéger



8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

Système COMSEC TC – Configuration Système typique



8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

Architecture Générale du Système COMSEC TC

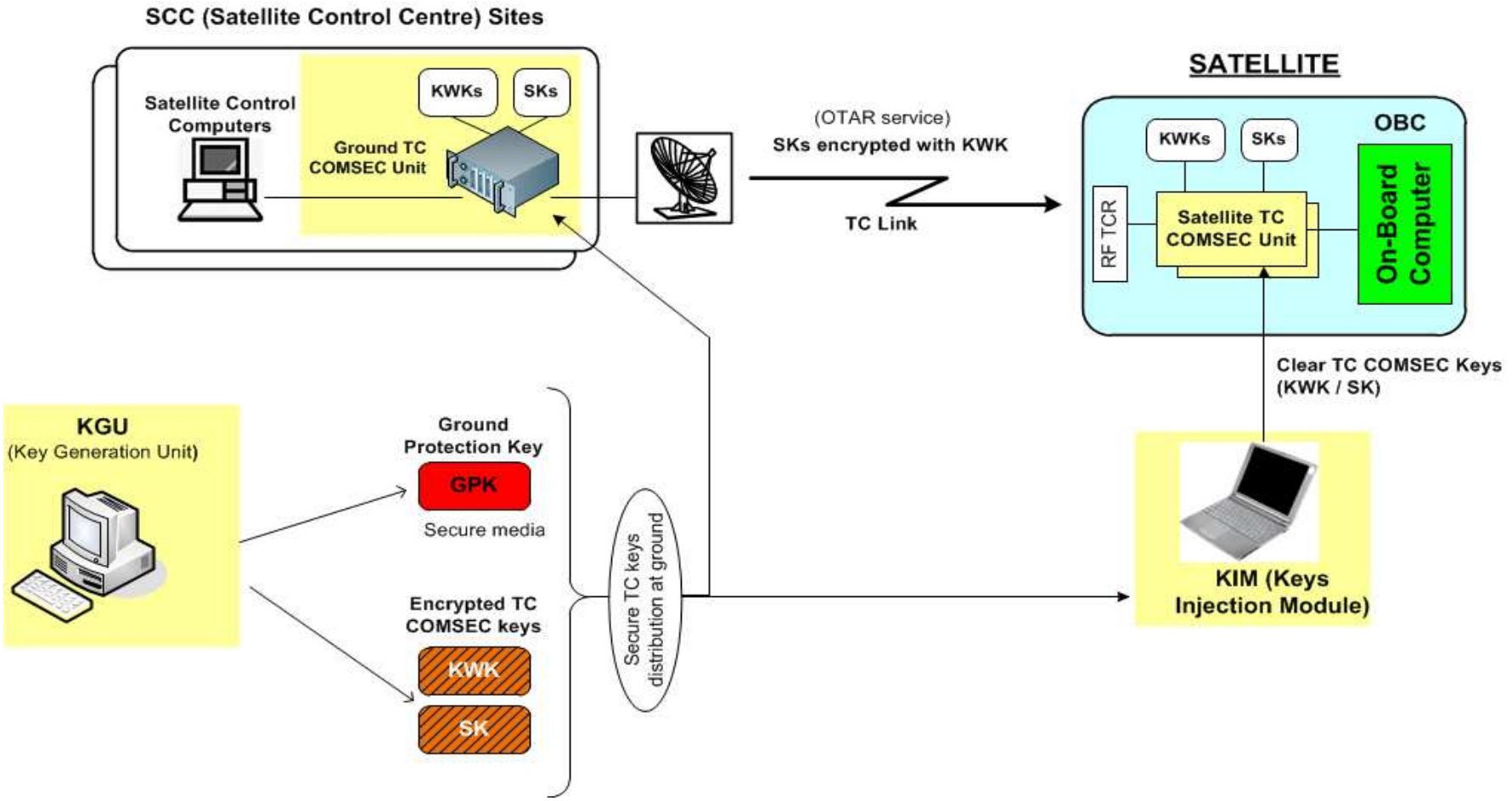
- Composants Sol
  - Key Generation Unit : génération des clés (Clés de Traffic, KEK)
  - Ground TC COMSEC Unit : Chiffrement et Authentification des TC
  - Key Injection Module : Chargement des clés dans le satellite avant le Tir
- Composants Bord / Satellite
  - Satellite TC COMSEC Unit : Déchiffrement et Authentification des TC
- La conception des composants varie très fortement suivant le niveau de Sécurité applicable et la certification ou non des équipements concernés
  - Equipement Sécurité en coupure des flux à protéger
  - Séparation physique des ports E / S pour les données claires /chiffrées
  - Cloisonnement interne en zones rouges (manipulation des données claires) / noire (rouges (manipulation des données chiffrées)
  - Detection anti-intrusion
  - Gestion des Clés
  - Implémentation des fonctions cryptographiques

8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

- Certification Sécurité (pour Systèmes avec niveau de Sécurité : Haut)
  - Certification Critères Commun (CC)
    - 7 niveaux d'Assurance Sécurité : EAL (Assurance Evaluation Level)
    - Evaluation par un organisme agréé dit CESTI (en France agréé par ANSSI)
    - Pour chaque équipement, l'evaluation se fait sur la base d'un document Cible de Sécurité (TOE : Target of Evaluation) incluant l'ensemble des exigences de sécurité à verifier
  - Certification NIST
    - Basé sur les exigences définies dans le document NIST FIPS 140-3
    - 4 niveaux d'assurance sécurité
    - Evaluation par un organisme / laboratoire agrée par NIST
- Validation de l'implémentation de l'algorithme cryptographique
  - Process courant NIST avec l'algorithme AES
  - Validation réalisée par un Labo agréé NIST
  - Verification du Code, Execution de Test patterns complets
  - À la fin : inscription dans l'AES Validation List officielle du NIST

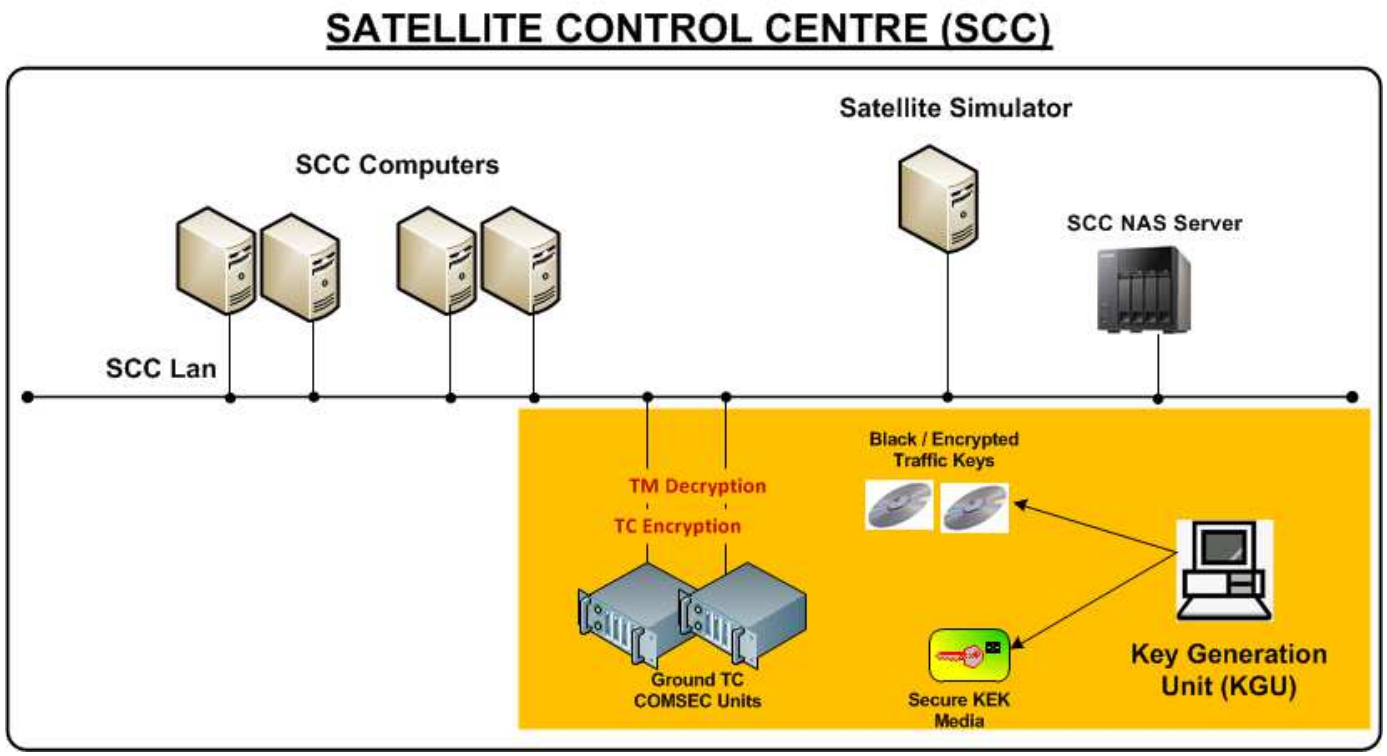
8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

Exemple 1 : Système TC COMSEC => Gestion des Clés



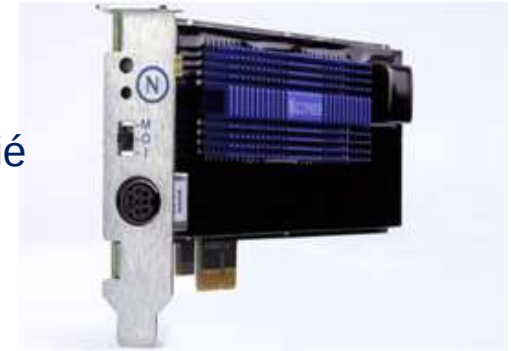
8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

Système TC COMSEC => Gestion des Clés au Sol (SCC)



Cas des Système Haute Sécurité :

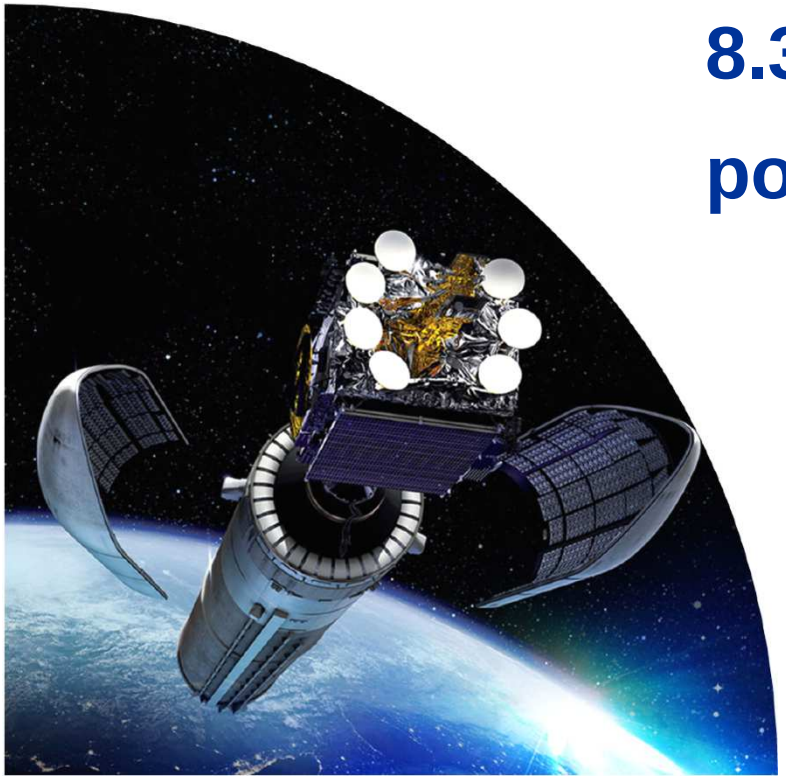
- Utilisation possible d'un HSM (Hardware Security Module) certifié



8.2.1 – Exemples d'Architecture - Cas des Systèmes COMSEC TC

Gestion des Clés => Génération des Clés

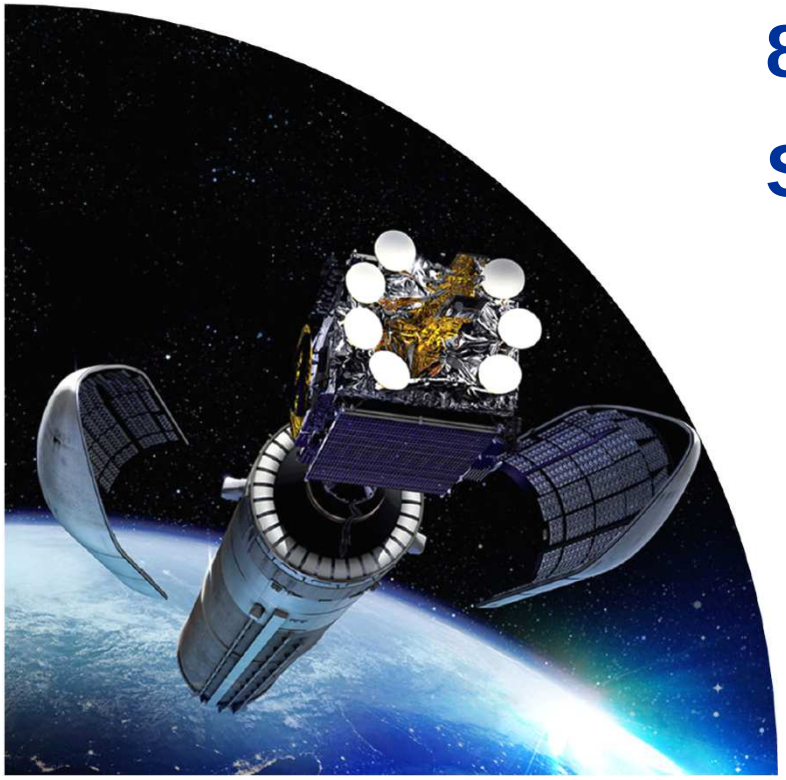
- L'un des points délicats est la génération des clés de vol
  - Pattern de clé aléatoires et non déterministes garantissant leur confidentialité
- Sélection d'un générateur PRNG robuste et standard
  - Ex: le standard NIST SP800-90A spécifie 3 * générateurs pseudo aléatoires utilisant un DRBG (Deterministic Random Bit Generator)
    - HASH_DRBG : basé sur fonctions HASH (SHA_xxx)
    - HMAC_DRBG : basé sur algorithme HMAC-SHAxxx
    - CTR_DRBG : basé sur algorithme CTR-AES
  - Note : le dernier générateur EC_DRBG basé sur des courbes elliptiques a été retiré par le NIST, car fortement mis en cause par la communauté des experts en cryptographie (backdoor NSA)
- L'élément critique est la source d'entropie
  - Source logicielle : bruit dans le noyau Unix **(/dev/random ou dev/urandom**), compilation (random pool) des divers evènements materiels / logiciels captables par l'OS (souris, clavier, écran, E/S, acces disques, heure, ..)
  - Source matérielle : générateur hardware (modules USB) , générateur DRNG intégré dans les circuits INTEL (i5 / i7)



8.3 – Selection de la Cryptographie pour une mission donnée

8.3 – Sélection de la Cryptographie pour une mission spatiale

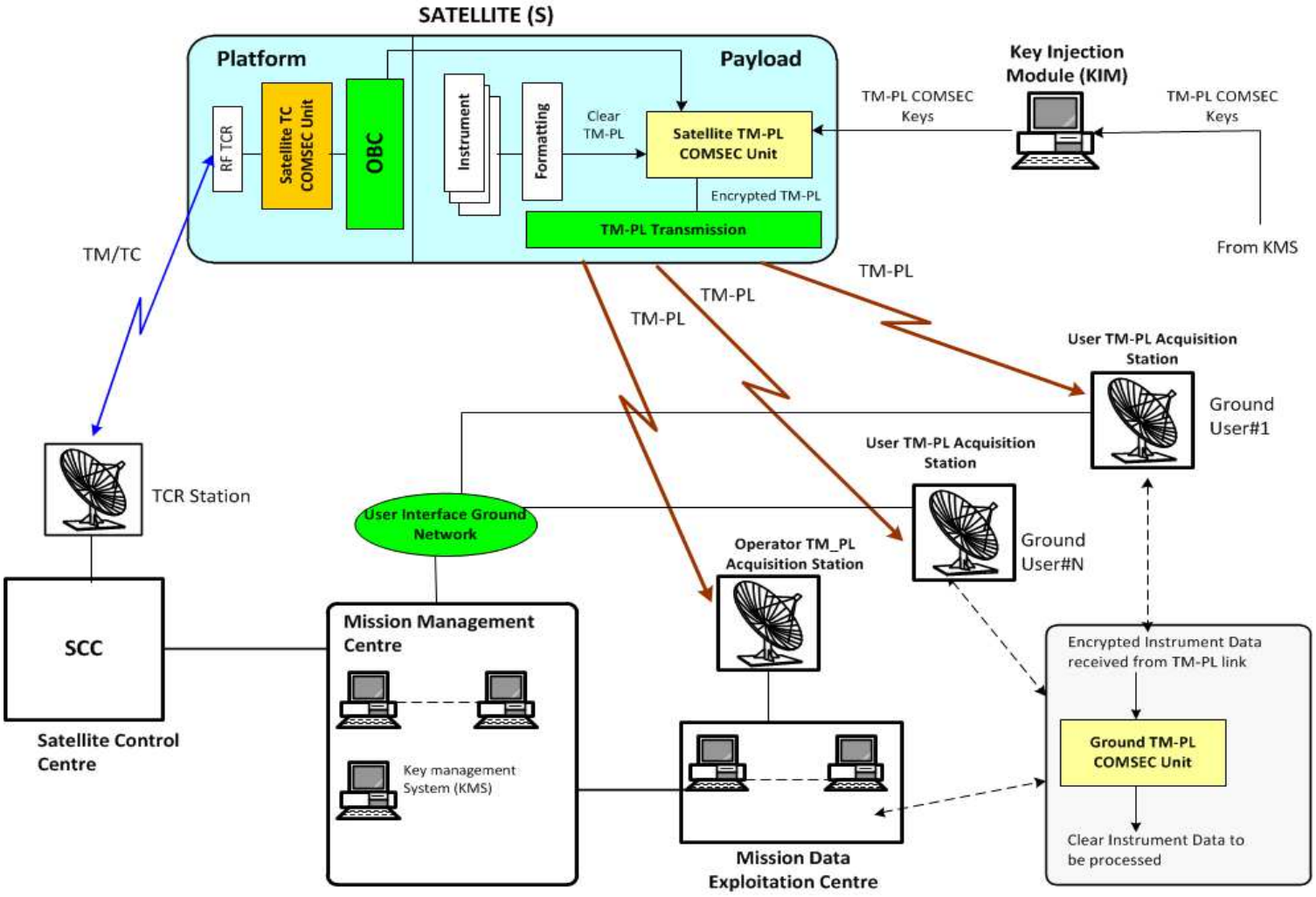
- La cryptographie peut suivant le Client ou la Mission être imposée
- Trois cas généralement rencontrés
  - Cryptographie domaine publique : sélection par le fournisseur satellite (ex: AES)
  - Cryptographie propriétaire / nationale exigée par un Client : boite noire / algorithme confidentiel
  - Cryptographie Certifiée NSA (“NSA Approved Cryptography”) imposée par le Gouvt US
    - Document applicable : CNSSP-12 Information Assurance
- La Cryptographie Certifiée NSA impose
  - l’implémentation d’équipements COMSEC certifiés par la NSA et fabriqués par des industriels US agréés
  - La génération des clés par la NSA
  - Des contraintes de sécurité très fortes : ex Eqts de sécurité COMSEC surveillés 24/24 par des gardes US agréés lorsque ceux-ci sont transférés hors des USA
    - Ex: tests en France sur site satellite ou sur le pas de tir (ex: Kourou)



8.4 – Exemple d'Architecture de Systèmes COMSEC TM-PL

8.4 – Exemples d'Architecture - Cas des Systèmes COMSEC PL-TM

Système TM-PL COMSEC : Exemple d'Architecture

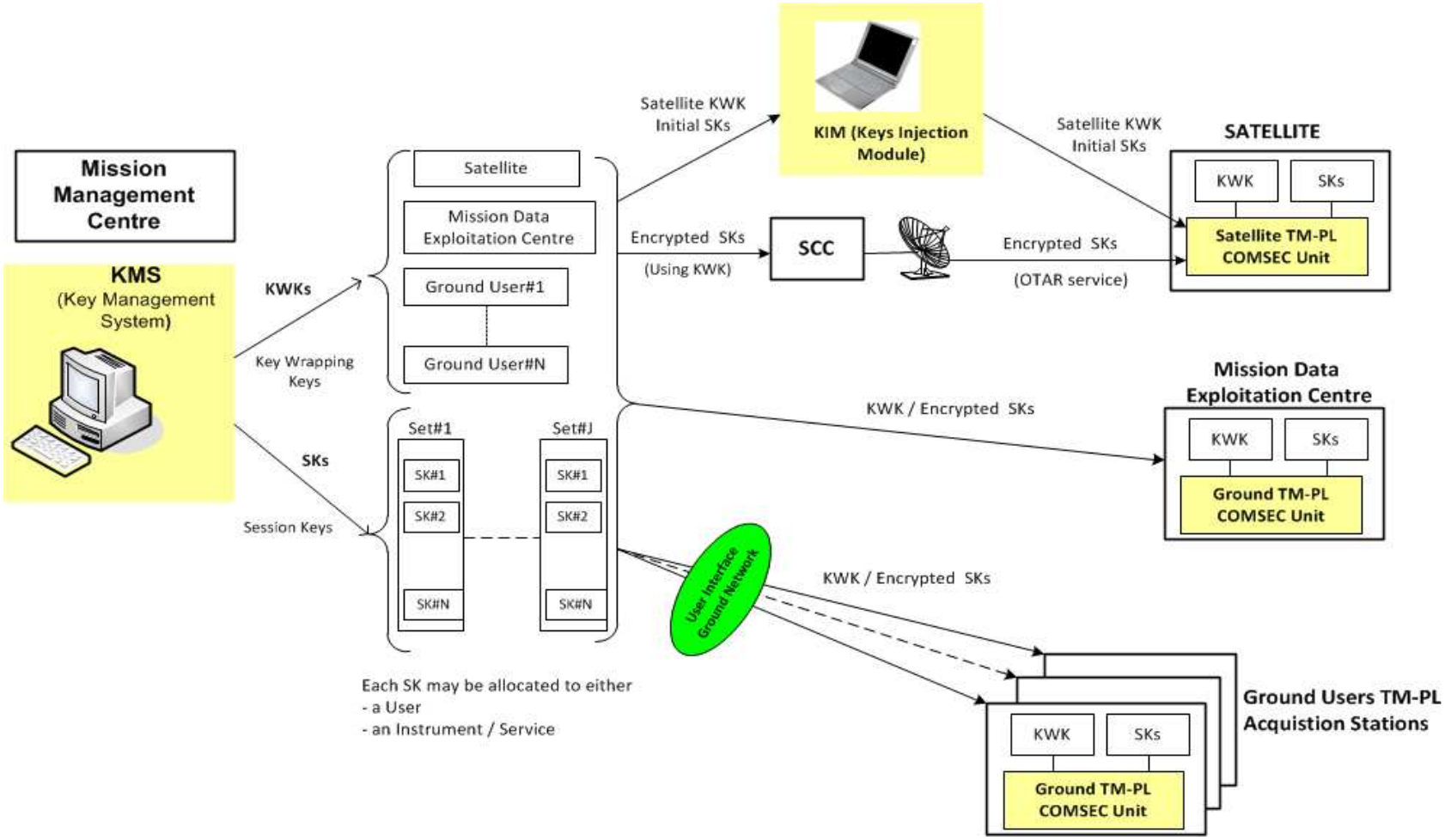


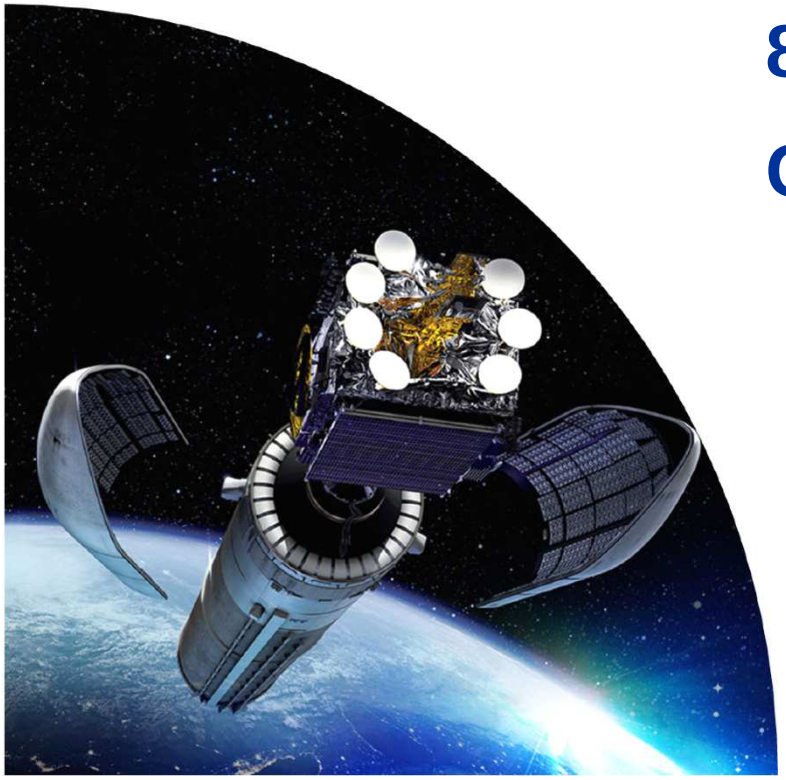
8.4 – Exemples d'Architecture - Cas des Systèmes COMSEC PL-TM

- Composants Sol
  - Key Management System : génération et distribution des clés (Clés de Traffic, KEK)
  - Ground TM-PL COMSEC Unit : Déchiffrement et Authentification des Trames TM-PL
  - Key Injection Module : chargement des clés dans le satellite
- Composants Bord / satellite
  - Satellite TM-PL COMSEC Unit : chiffrement et authentification des Trames TM-PL
- La gestion des Clés est le point le plus delicat d'un système TM-PL COMSEC
  - Distribution des Produits instruments : jusqu'à 1000 Utilisateurs Sol
  - La Gestion des clés TM-PL COMSEC doit obéir à des contraintes de nature dynamique (enregistrement d'un Utilisateur, début / fin du service, révocation)
  - La distribution d'un produit Instrument, est très diverse et impacte la Gestion des Clés
    - Broadcast : accès à tous les utilisateurs enregistrés et autorisés
    - Multicast : accès à un sous-ensemble des utilisateurs enregistrés et autorisés
    - Unicast : accès à un seul utilisateur enregistré et autorisé (ex demande prise de vue images au-dessus d'une région donnée)

8.4 – Exemples d'Architecture - Cas des Systèmes COMSEC PL-TM

Exemple 2 : Système TM-PL COMSEC => Gestion des Clés

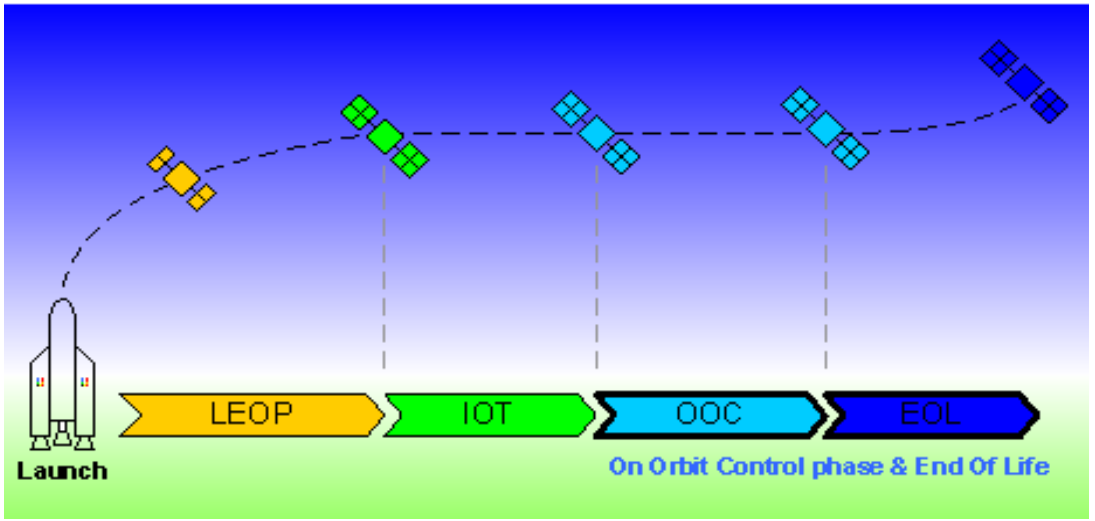




8.5 – Opération d'un Système COMSEC TM/TC

8.5 – Opération d'un Système COMSEC TC/TM

Phases relatives à l'Opération d'un satellite



Avant le tir : Campagne de tir (ex: CSG / Kourou)

- Chargement des clés de Vol dans le satellite (injection des clés)

Tir du satellite et LEOP phase (Launch & Early Orbit Phase)

- Pas d'opération sécurité
- les fonctions de sécurité sont désactivées – Mode "Clair"

8.5 – Opération d'un Système COMSEC TC/TM

- IOT : In-Orbit-Test
  - Validation du système en Vol
  - Test des fonctions de sécurité à partir du Sol (SCC)
- OOC : Orbit Control Phase : Phase d'exploitation du satellite
  - Initialisation Sécurité
    - Activation des fonctions de Sécurité
    - Initialisation des paramètres: compteur anti-rejeu, clé courante
  - Opération nominale
    - Changement périodique de clé courante
    - Génération et téléchargement de nouveaux jeux de clés (clés fraiches) - OTAR
  - Opérations non nominales
    - Investigations sur pannes, reset, switch sur la redondance, ..

8.5 – Opération d'un Système COMSEC TC/TM

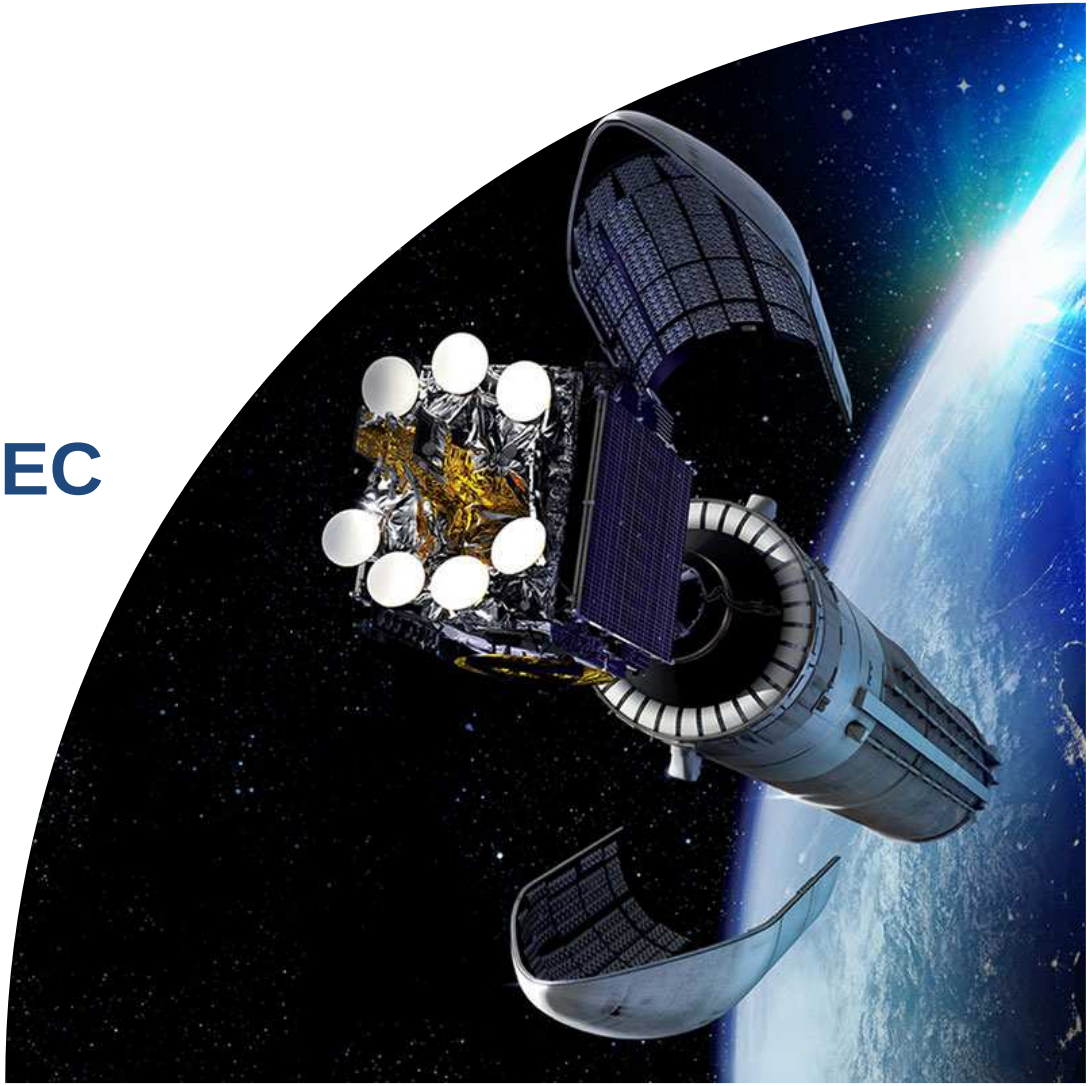
Changement Périodique de Clé

- Selon la crypto-période définie dans les Procédures Sécurité
- Ex ci-dessous: crypto-période de 1 mois

	1rst Month	2nd Month		11th Month	12th Month
1st Year	key#17	key#18	…	key#26	key#28
2nd Year	key#29	key#30	…	key#38	key#40
3rd Year	key#41	key#42	…	key#50	key#52
4th Year	key#53	key#54	…	key#62	key#64
5th Year	key#65	key#66	…	key#74	key#76
6th Year	key#77	key#78	…	key#86	key#88
7th Year	key#89	key#90	…	key#98	key#100
8th Year	key#101	key#102	…	key#110	key#112
9th Year	key#113	key#114	…	key#122	key#124
10th Year	key#125	key#126	…	key#134	key#136
11th Year	key#137	key#138	…	key#146	key#148
12th Year	key#149	key#150	…	key#158	key#160
13th Year	key#161	key#162	…	key#170	key#172
14th Year	key#173	key#174	…	key#182	key#184
15th Year	key#185	key#186	…	key#194	key#196
16th Year	key#197	key#198	…	key#207	key#208

9 – Application aux Systèmes Spatiaux

Protection TRANSEC



9 – Cas des Systèmes TRANSEC

Définition - Un système TRANSEC

- Assure une protection des données à transmettre contre le brouillage et l'interception
- Opère au niveau de la couche physique
  - Couche modulation / transmission Radio-Fréquence des données à transmettre
- Utilise la technologie de Spectre étalé (Spread Spectrum / SS)
  - Séquence Directe : système DSSS (Direct Sequence Spread Spectrum)
  - Saut de Fréquence: système FHSS (Frequency Hopping Spread Spectrum)
- Met en oeuvre des mécanismes cryptographiques
  - Génération des séquences dites TRANSEC pilotant les fonction d'étalement de spectre et assurant leur qualité et confidentialité

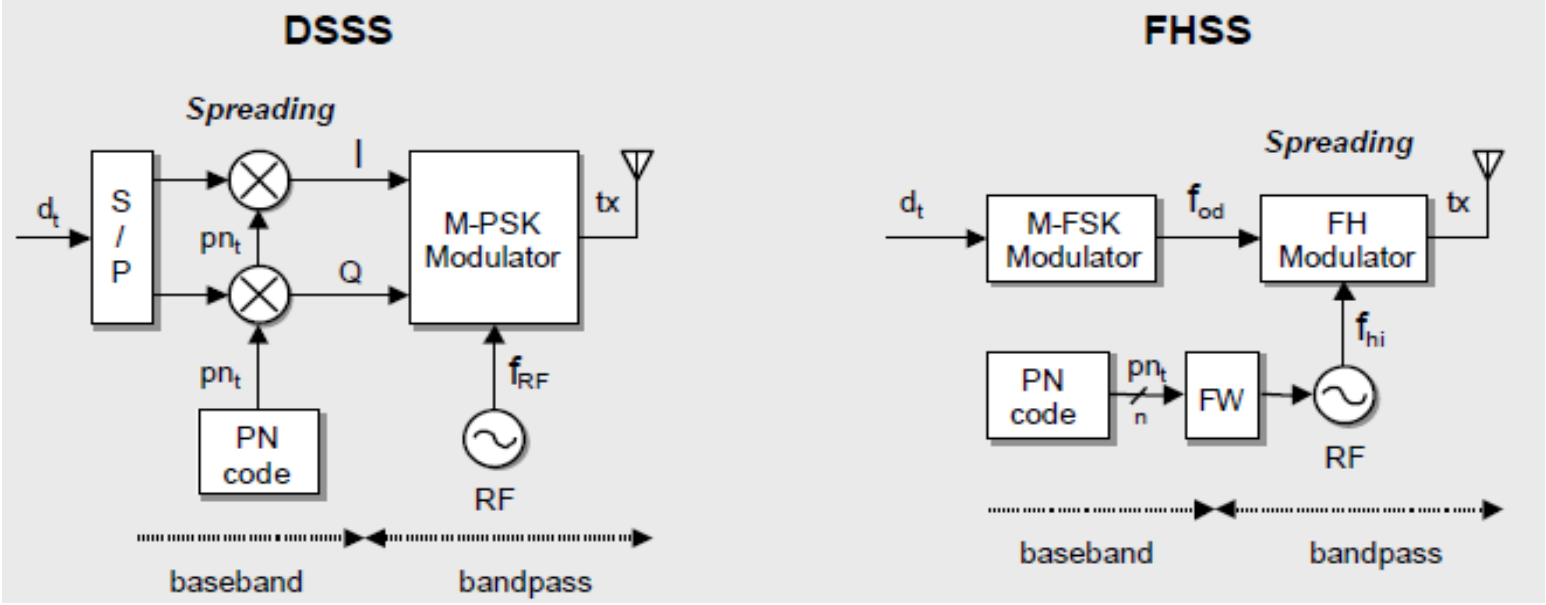
- Affiche des performances (anti-brouillage) compatible des besoins / exigences de niveau Gouvernemental / Défense
  - Principaux utilisateurs des systèmes spatiaux TRANSEC

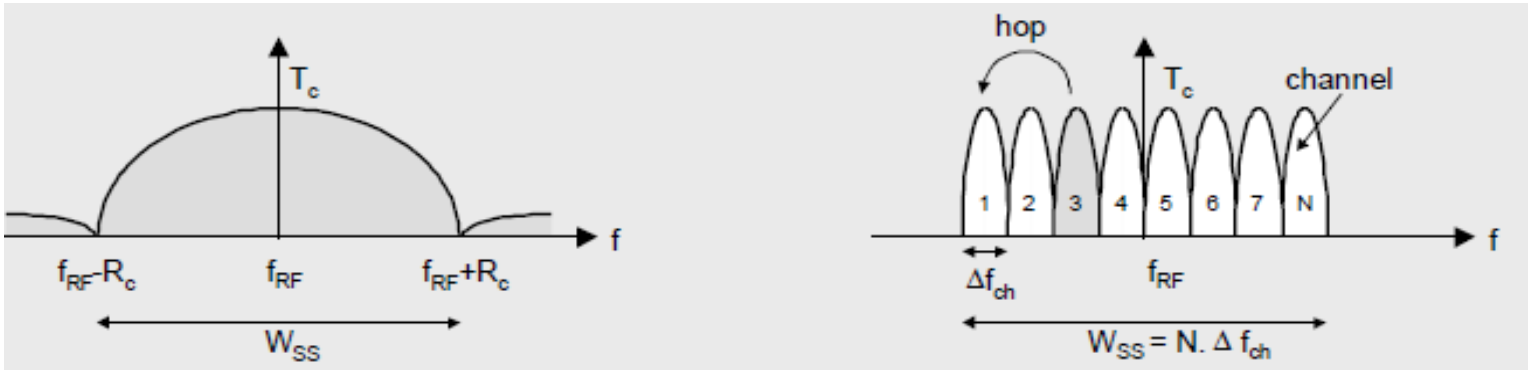
9 – Cas des Systèmes TRANSEC

Principe d'un système TRANSEC

- Le principe consiste à transforrmer le signal contenant les données utiles à transmettre (signal occupant une bande étroite), en un signal occupant une bande beaucoup plus étendue (large-bande) et semblable à du bruit
  - La bande de fréquence résultante peut-etre 100 à 1000 fois plus étendue que la bande étroite utile nécessaire à la transmission des données d'entrée
- Comme la puissance de transmission du signal large-bande est identique à celle du signal à bande etroite, la densité spectrale du signal (W/Hz) s'en trouve proportionnellement réduite
- Du fait que le signal utile à transmettre est réparti sur bande de fréquence nettement plus large et qu'il est difficilement distinguable du bruit:
  - Il est nettement plus difficile à intercepter => LPI : Low Probability to Intercept
  - Il est nettement plus resistant au brouillage => AF anti-jamming
- Les lois d'étalement de spectre sont basées sur des sequences pseudo-aléatoires dites PN (pseudo Noise) , générées par un algorithme cryptographique
  - Elles deviennent alors des séquences TRANSEC

Principe d'un système TRANSEC DSSS et FHSS



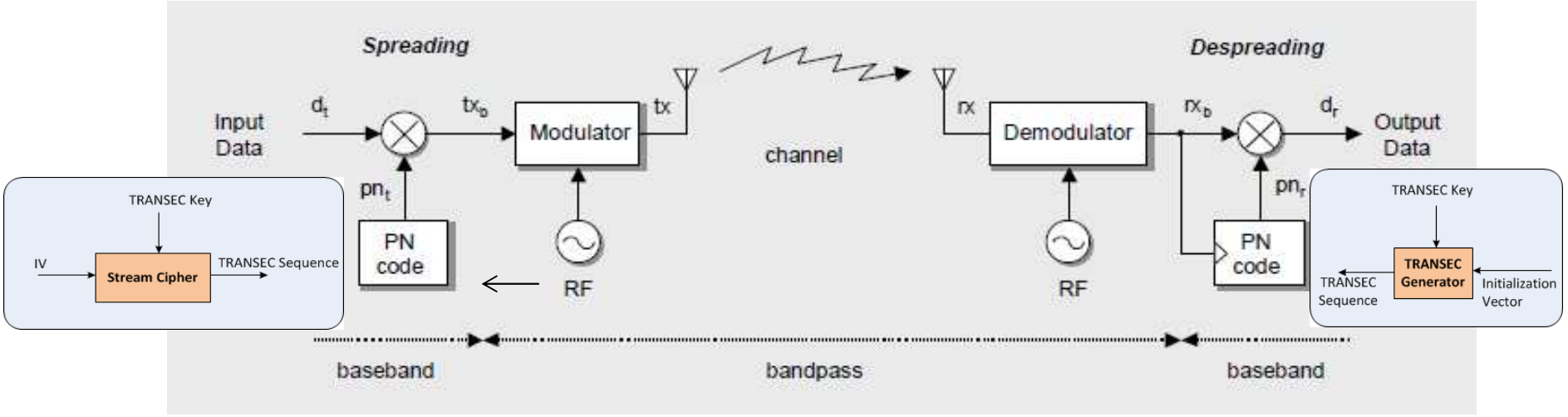


9 – Cas des Systèmes TRANSEC

Role des fonctions cryptographiques dans un système TRANSEC

❑ Système DSSS

- ➢ Génération de la sequence pseudo-aléatoire (PN Code dans la figure) haut-débit additionnée (XOR) avec la séquence utile d'entrée
- ➢ Implémentation d'une fonction PRNG (pseudo-random number generator) basée sur un stream cipher et des clés secrètes
  - Ex: OFB-AES, CTR-AES, RABBIT, SNOW, SALSA_20



9 – Cas des Systèmes TRANSEC

Role des fonctions cryptographiques dans un système TRANSEC

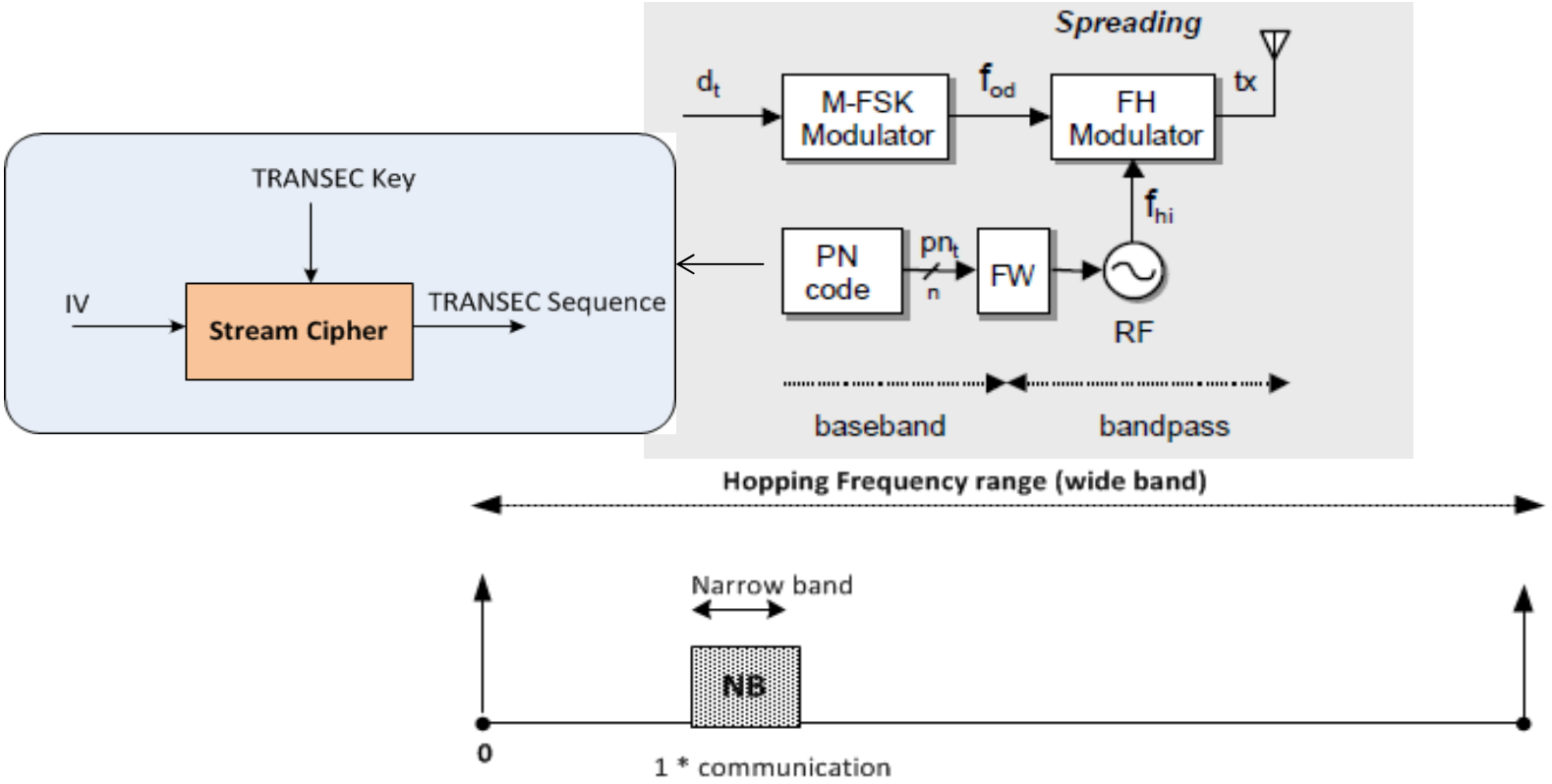
Caractéristique des séquences TRANSEC

- Pseudo aléatoires : doivent paraitre parfaitement aléatoires à ceux qui écoutent le signal RF large bande sans connaître la loi TRANSEC
  - Caractéristiques statistiques : moyenne , écart type, ..
- Déterministes : la loi TRANSEC doit être connue de l'emetteur et du Récepteur (Sol et Satellite)
- Non linéaire
- Longue crypto-période rendant plus difficile l'analyse
  - Typiquement une période superieure à la durée d'une mission spatiale (10 à 20 ans) repond à ce besoin
- Génération par une cryptographie forte
  - Algorithme, mode d'opération, taille de clé

Role des fonction cryptographiques dans un systéme TRANSEC

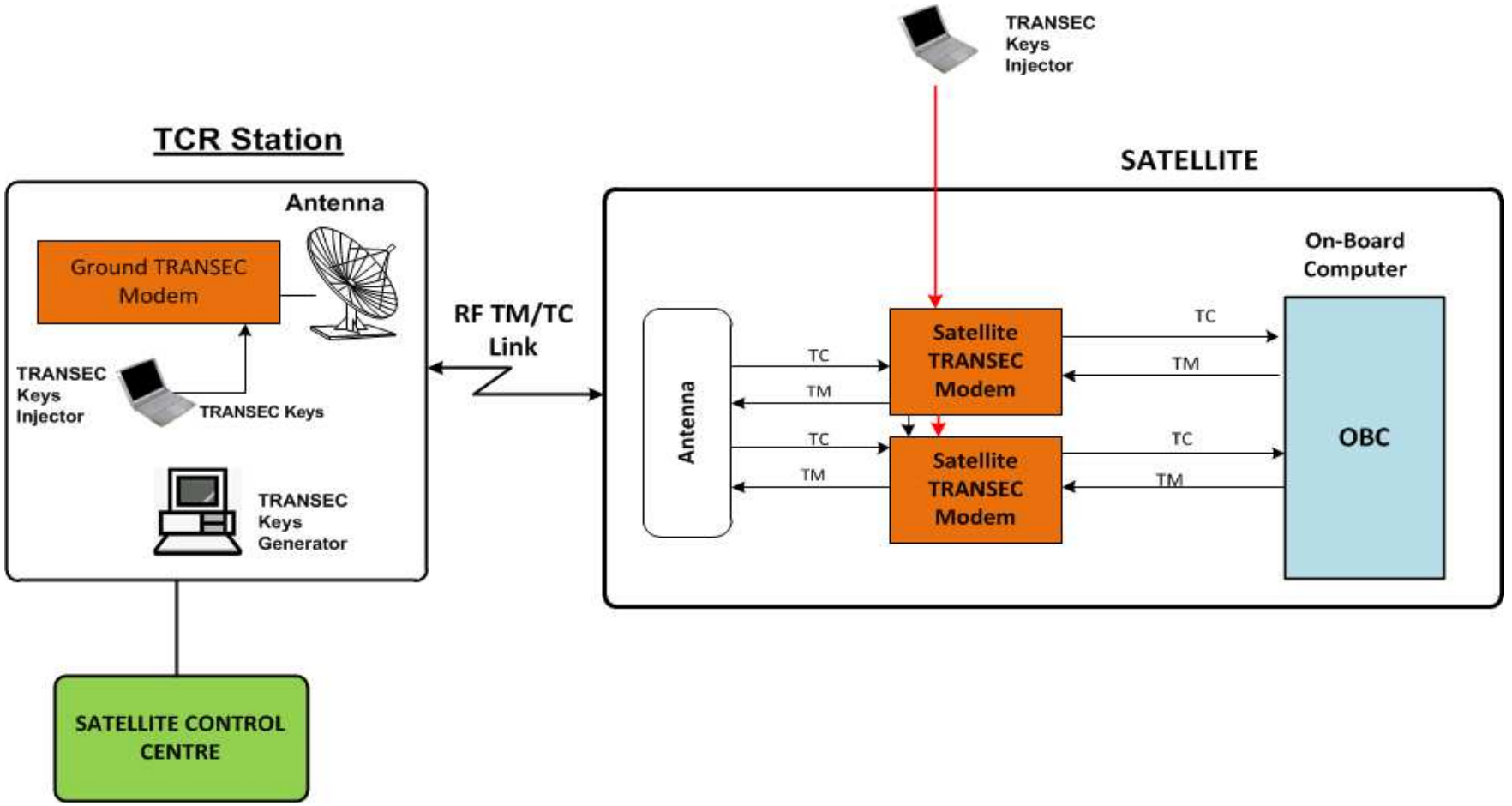
❑ Système FHSS

- Génération de la sequence pseudo-aléatoire déterminant la position de la bande de fréquence étroite transportant la communication en cours à l'instant T , dans la bande de fréquence globale (large bande)



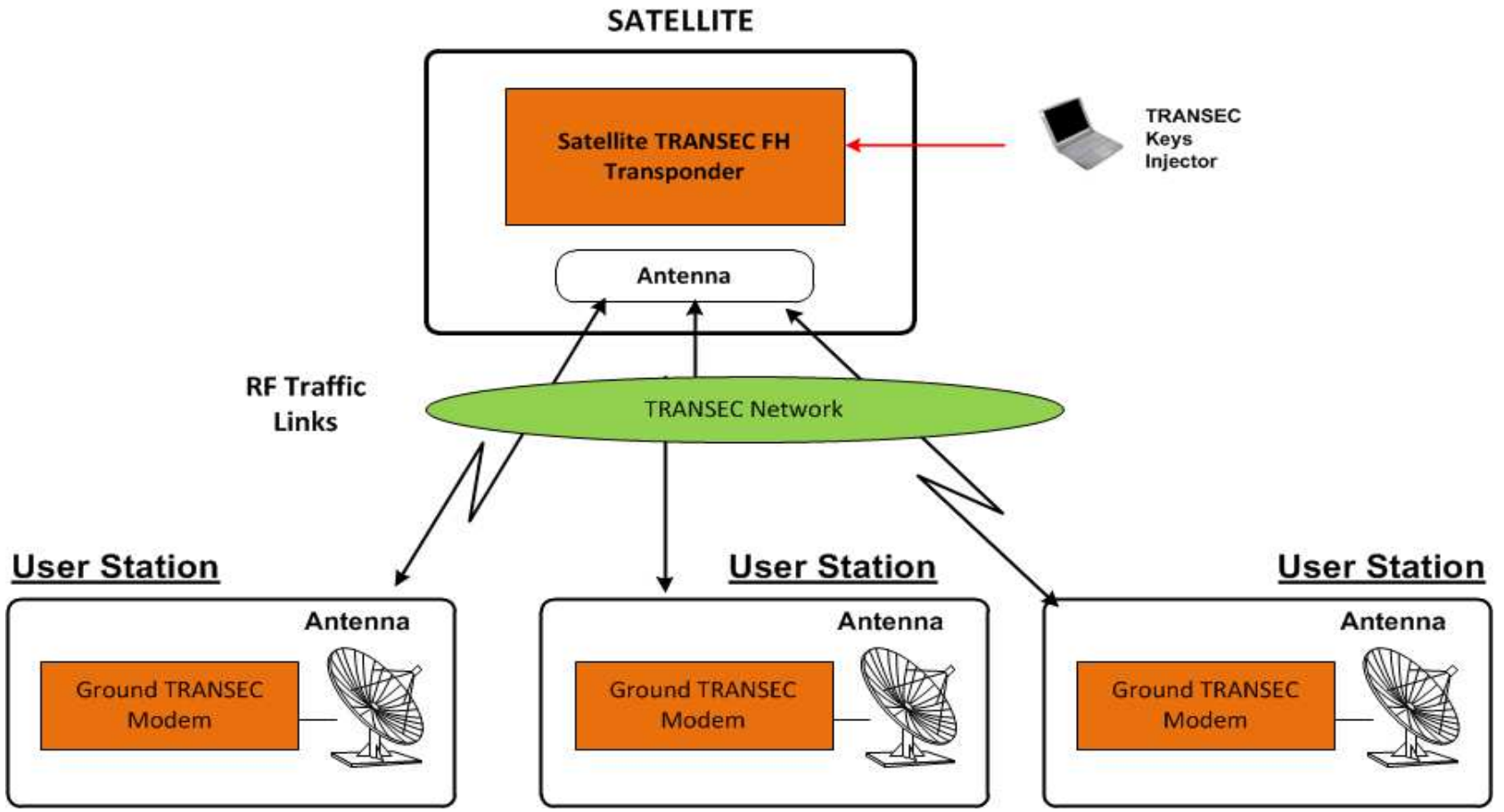
9 – Cas des Systèmes TRANSEC

Exemple : Configuration d'un Système TRANSEC TC (DSSS)

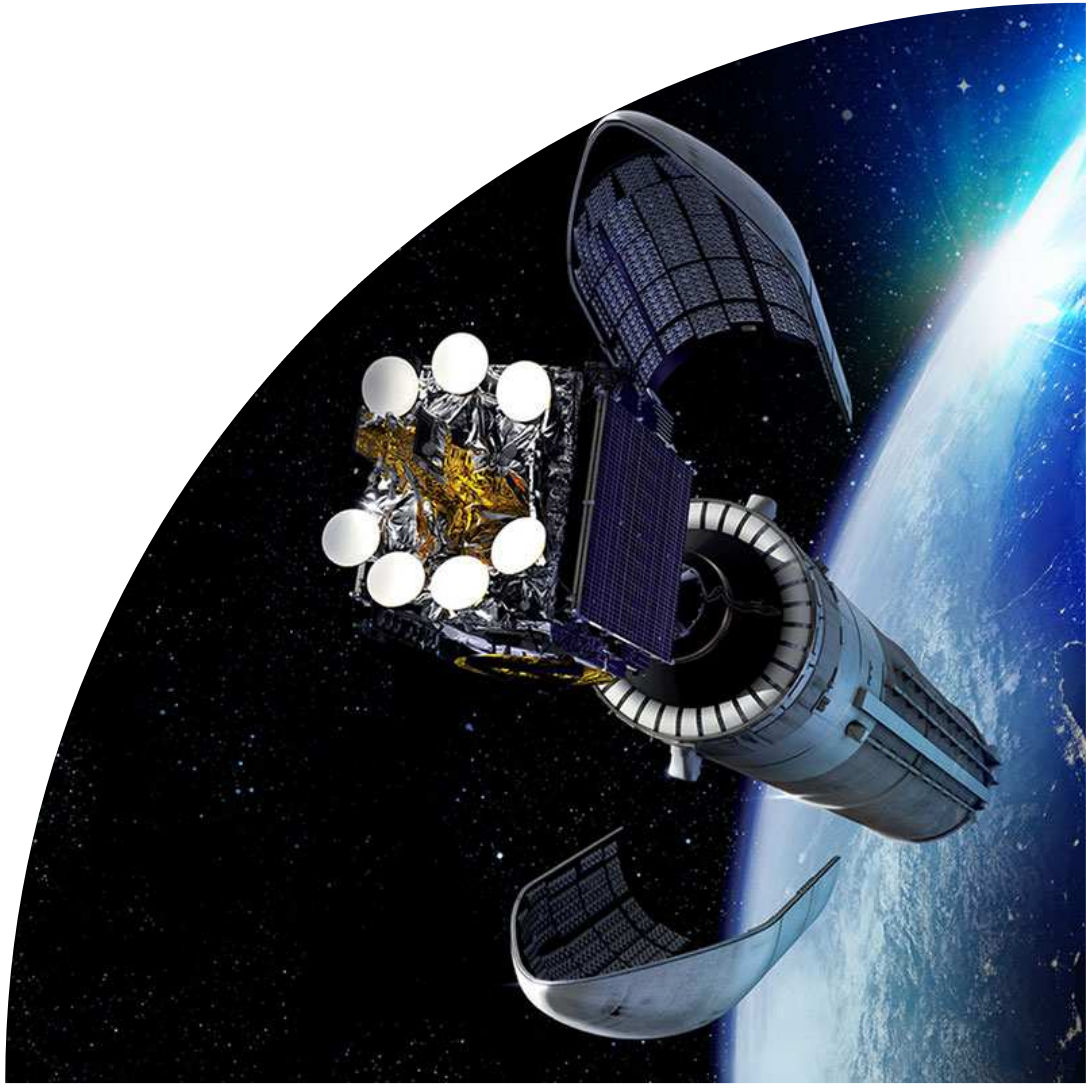


9 – Cas des Systèmes TRANSEC

Exemple : Configuration d'un Système TRANSEC Payload (FHSS)



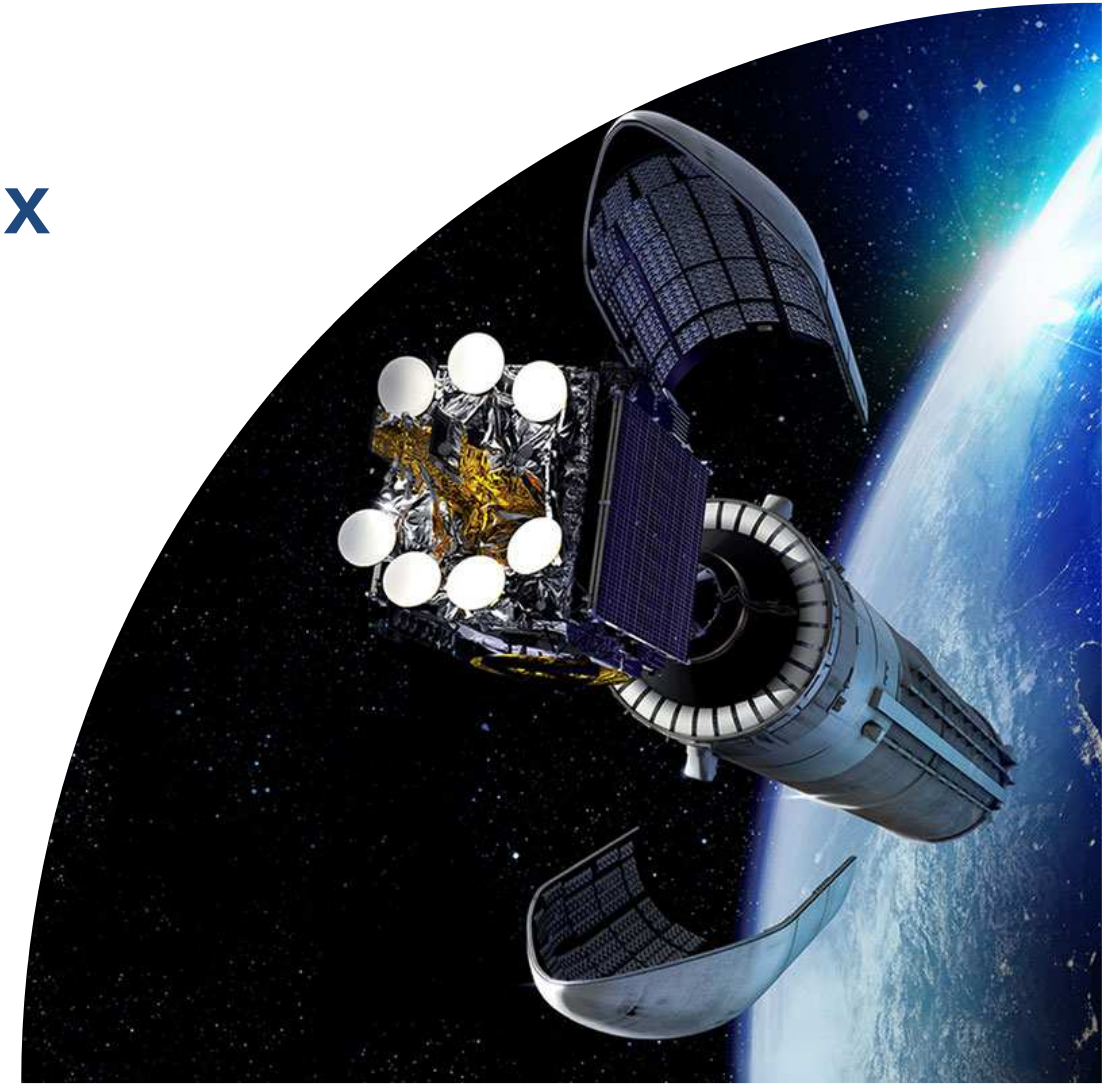
10 – Conclusion



10 – Conclusion

- La sécurité des communications spatiales est un domaine très riche et en permanente évolution
- Exigences en Sécurité accrues des Clients et Opérateur satellites, avec l'accroissement des menaces (Cyber attaques, ordinateurs quantiques)
- Emergence de standards de sécurité (CCSDS) matures pour la protection des liaisons spatiales
- Met en oeuvre les différentes technologies disponibles et futures en cryptographie : SKI, PKI, cryptographie quantique, cryptographie post quantique
- Les solutions de sécurité impactent les segments sols, les satellites, les interfaces bord / sol
  - Centre de contrôle satellite, réseaux sol, sous-systèmes TM / TC satellite, Data handling satellite (Avionique), Charge utile satellite
- De ce fait les Ingénieurs Sécurité sont impliqués aussi bien dans les architectures Sol que les architectures satellites
- Bref , métier passionnant , je conseille….

Annexe : Principaux “Hard Problems” Cryptographiques



ANNEX - PKI Cryptography Relevant ‘’Hard Problems’’ => RSA

RSA key pair generation.

- Randomly select two large primes p and q, and p≠q
- Compute n=pq and ø=(p-1)(q-1)
- Select an arbitrary integer e with 1<e<ø and gcd (e,ø)=1.
- Compute the integer d satisfying 1<d<ø and ed ≡ 1 mod (ø)
- **The public key is (n,e), and the private key is d.**

Factorization problem

- **Definition**: given a positive integer *n*, find its two prime factorization *p* and *q*.
- For RSA: If one can derive the primes p and q from n, ø = (p-1)(q-1) can be computed
- The enables the determination of the private key $d \equiv e^{-1} \pmod{ø}$.
- The best published solution to the factoring problem is the general number field sieve (**GNFS**) algorithm

ANNEX - PKI Cryptography Relevant ‘’Hard Problems’’ => DH

DH (DIFFIE-HELLMAN) key pair generation.

- G is finite group with generator g, p is a prime and q is a prime divisor of p-1.
- Randomly select x from [1, q-1]
- Compute $y=g^x \pmod p$
- **The public key is y, and private key is x.**

Note

- $x=\log_g y \pmod p$, x is called the **discrete logarithm** of y to the base g.
- Given g,x, and p, it is trivial to calculate y. However, given y, g,and p it is difficult to calculate x.

Discrete Logarithm Problem

- Given a prime p, generator g, and an element y in group G, find the integer x, such that $y=g^x \pmod p$.
- The fastest algorithm known for solving discrete logarithm is still **GNFS** (as for RSA)

ANNEX - PKI Cryptography Relevant ‘’Hard Problems’’ => ECC

ECC (Elliptic Curves Cryptograph) key pair generation.

- Randomly select d∈ [1, n-1].
- Compute Q=dP, P, Q is a point on the curve
- **Public key is Q, private key is d**

Note

- The naive algorithm to recover d from Q is the computation of a sequence of points P, 2P, 3P, 4P, until Q=dP
- According to d size (≥ 256 bits) it is computationally infeasible to solve d from Q by using the naive algorithm.

Elliptic Curve Discrete Logarithm Problem (ECDLP)

- Given an elliptic curve E defined over a finite field $\mathbb{F}_q$, a point P∈E($\mathbb{F}_q$) of order n, and a point Q ∈E, find the integer d ∈ [0,n-1] such that Q=dP.
- The fastest algorithm to solve ECDLP is **Pollard’s rho** algorithm

TLS-SEC – Sécurité des Communications Spatiales

Fin de la Présentation

Merci de votre Attention