



Enable S³ : Touch And Go Assistant

Gavin Crosmarie, January 12, 2019

This project has received funding from the ECSEL Joint Undertaking under grant agreement No 692455. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Norway.

Enable S3 – Qui ?

- 68 partenaires
- 16 pays
- Industriels & chercheurs

Enable S3 – Quand ?

- Mai 2016 – Mai 2019
- Plusieurs expositions au public
 - Dublin juillet 2018
 - Graz mai 2019

Enable S3 – Qu'est-ce ?

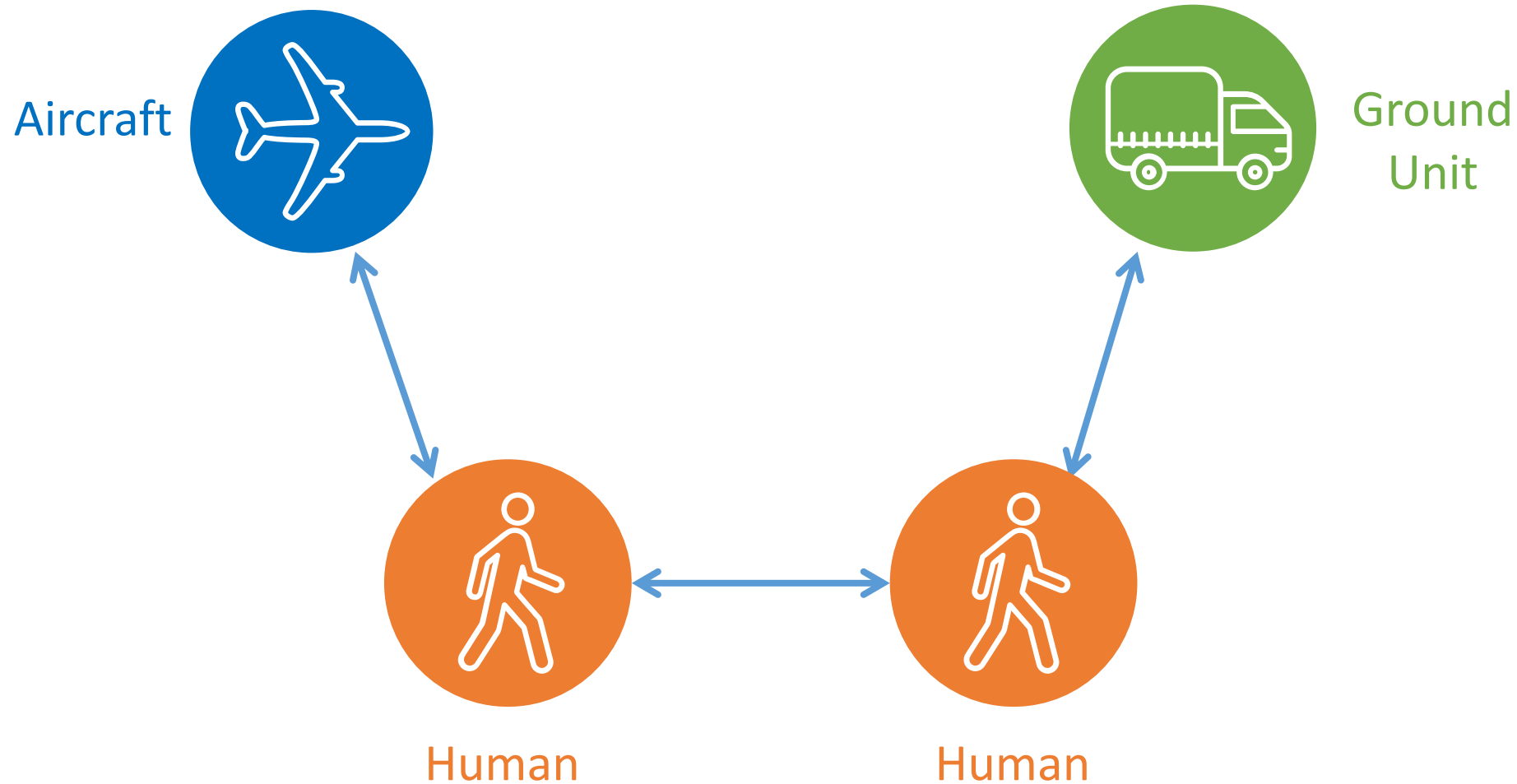
- La validation de systèmes hautement autonomes surs et sécurisés
- Réduire le coût de la validation et des vérifications
- 6 domaines



Aéronautique - Touch And Go Assistant

- 1 des 12 sujets d'Enable S3
- Faciliter et optimiser les turn-arounds des avions
- Peu importe l'aéroport
- Sans accroître les risques

Un ravitaillement aujourd'hui



Exemples typiques

- Ravitaillement en fioul
 - Ravitaillement initial
 - Ravitaillement d'ajustement

- Climatisation
 - Refroidissement lors du turn-around
 - Ajustement du flux d'air

TAGA : Touch And Go Assistant



Goals



Réduire la durée du Turn-around



Fonctionner localement sans infrastructure



Conserver le processus de ravitaillement



Réduire les coûts

Contraintes

- Climat hostile : Pluie, Neige, Désert...
- Aéroport sans connexion internet
- Sur un parking d'avion
- Entités de companies différentes

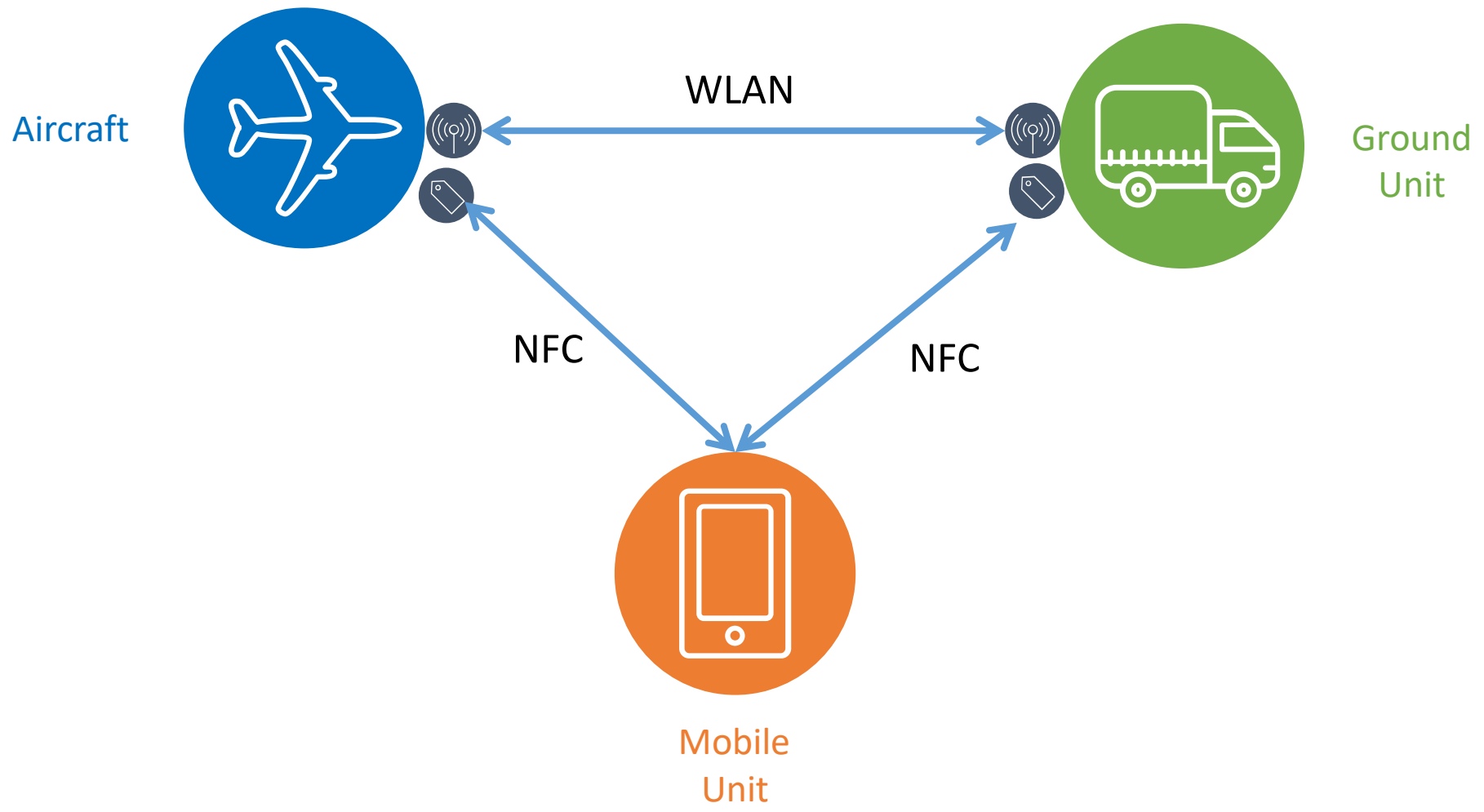
TAGA : Touch And Go Assistant



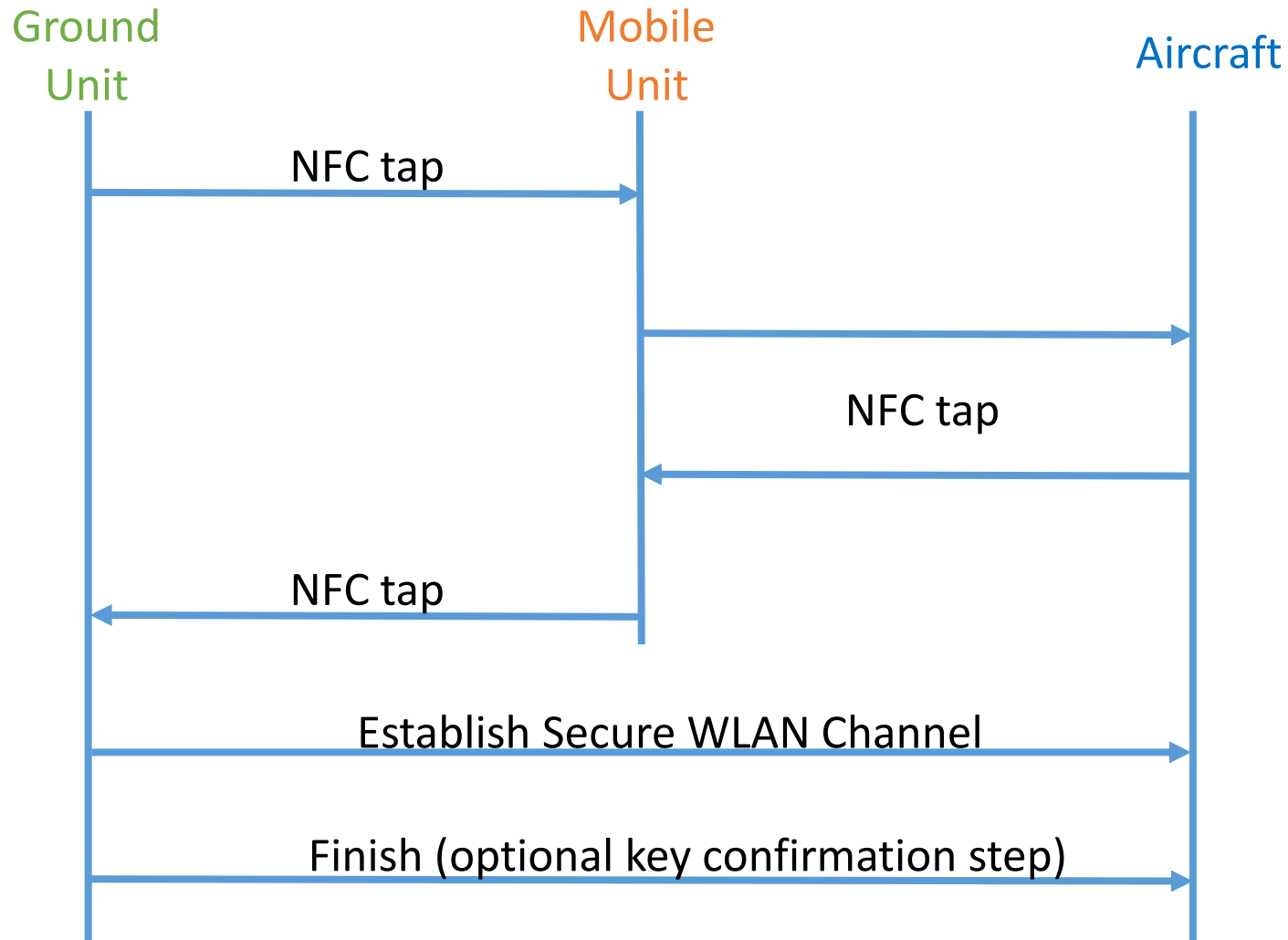
Wait a second...

- Pourquoi pas un simple câble ?
 - Le poids
 - Le nombre de connexions possibles
 - Le type de service que l'on peut connecter
 - Le côté pratique et rapide

TAGA : Concept



Le fonctionnement



Deux canaux

Par le Mobile Unit – Le pairing

Etablir la connexion

Echanger des identifiants et des clés

S'assurer de l'interlocuteur

WLAN – La communication

Pour l'échange de données utiles

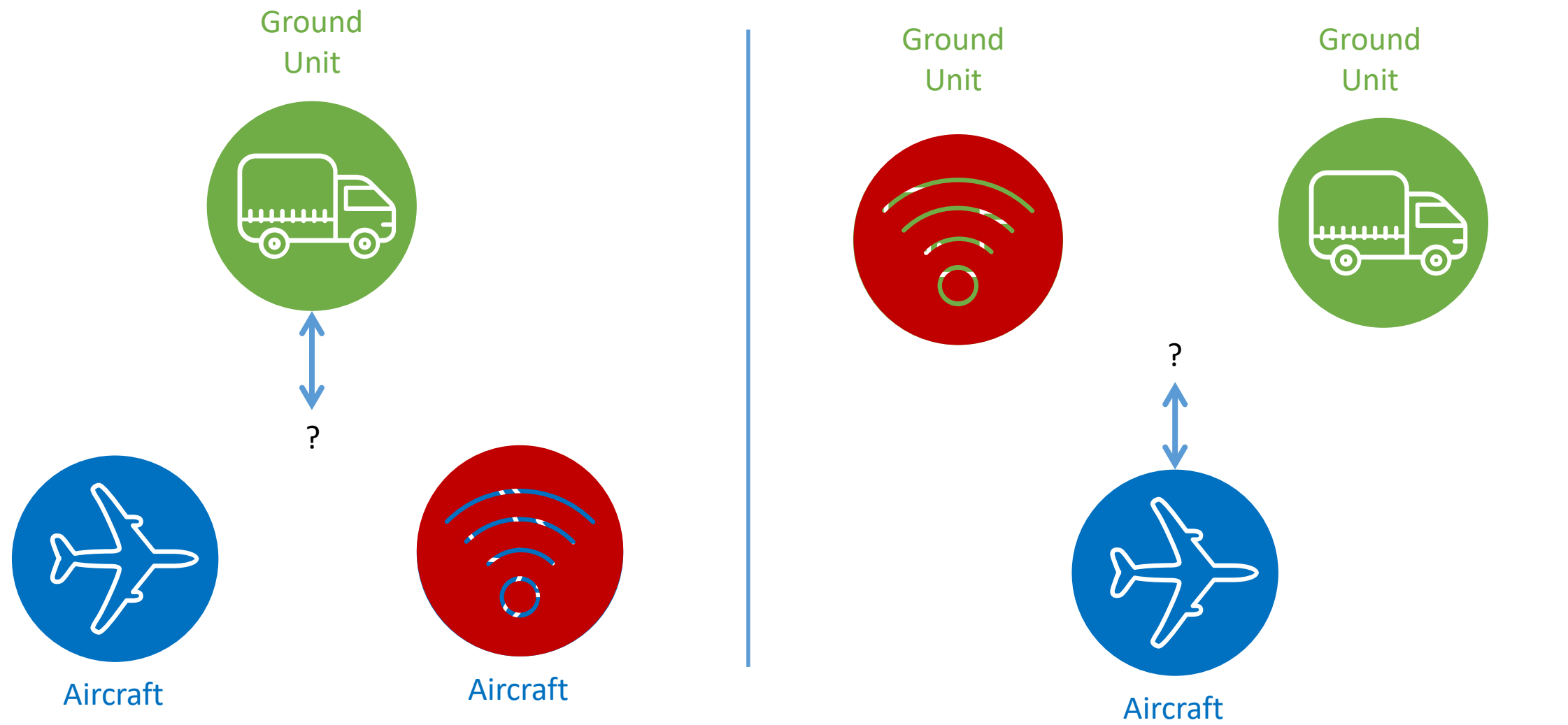
Pourquoi le NFC ?

Etablir une connexion avec la bonne machine

Sans information préalable

Sans infrastructure

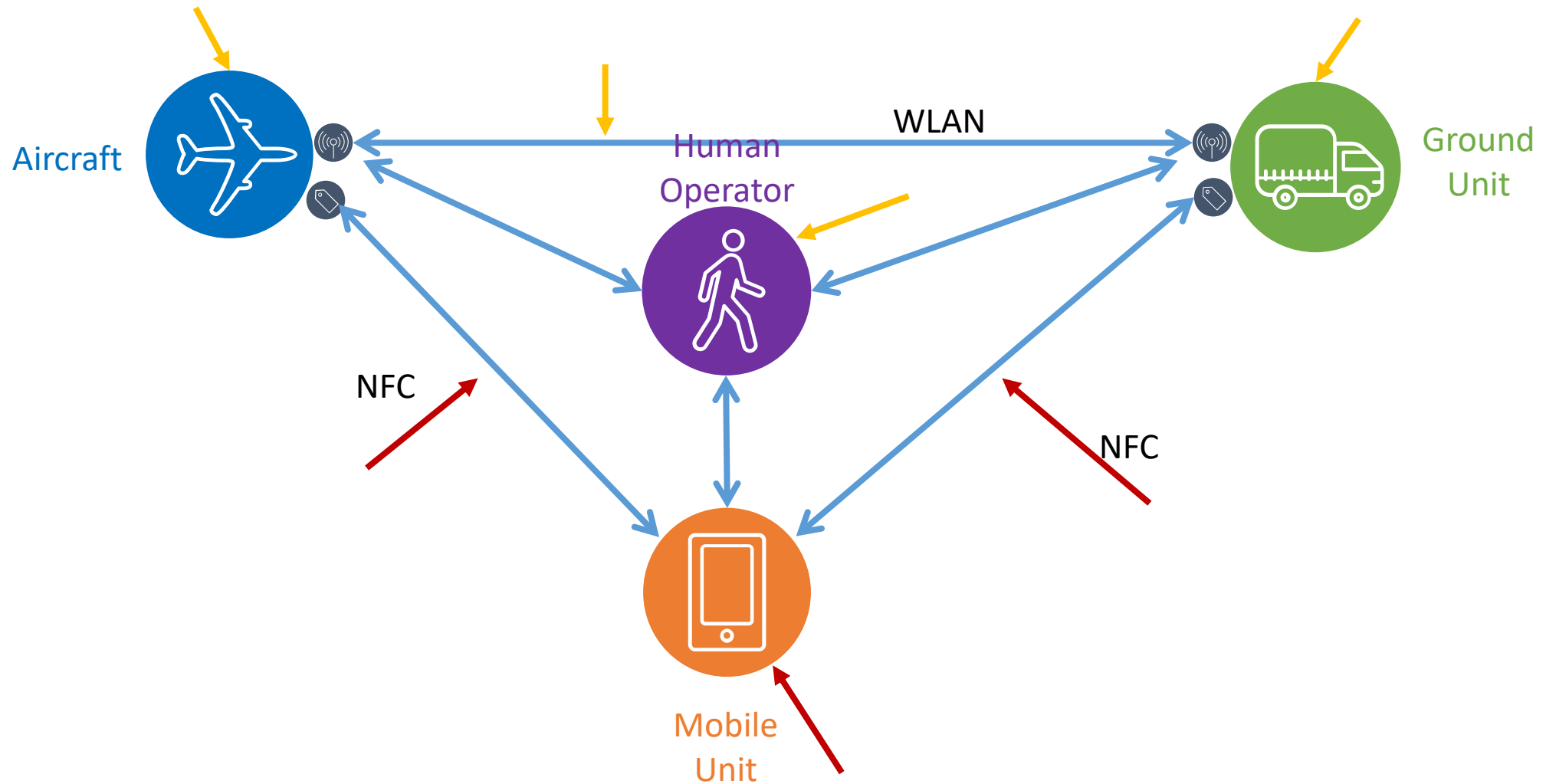
Ce qu'on veut protéger



Menaces

- Un contact NFC
 - Périmètre contrôlé (hostile)
 - Processus à respecter
 - Dénis de service possible
- Mobile Unit compromis
 - Attaque extensible
 - Nécessite une protection
- Avions ou équipement au sol compromis
 - Hors champs
- WLAN
 - Protocol sûr
 - Dénis de service possible

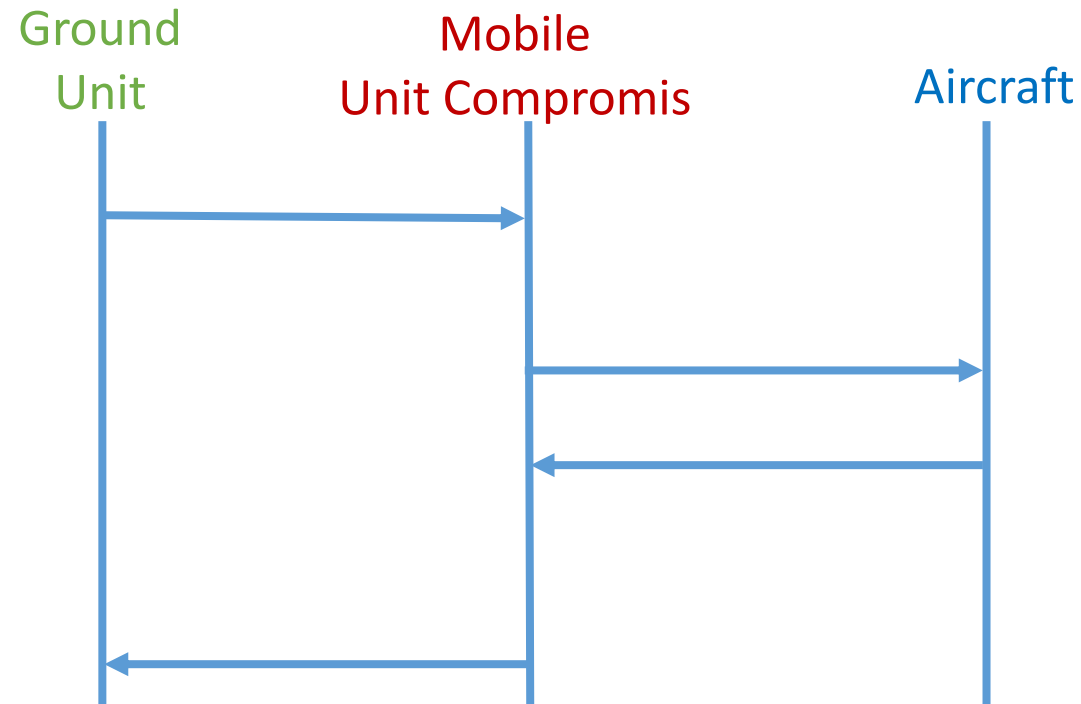
Menaces



Sécurité du canal NFC (état de l'art)

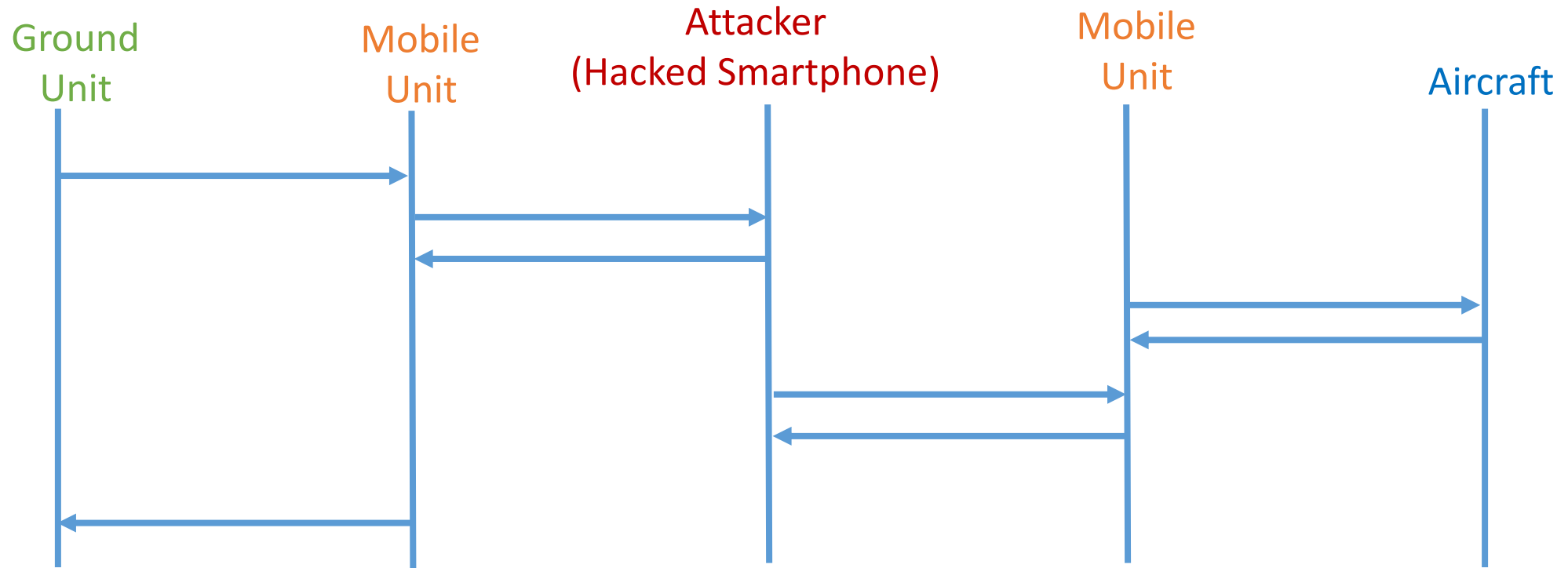
- La portée pour l'écoute illicite :
 - 10m en actif
 - 1m en passif
- Avec NFC pas d'attaque de l'homme du milieu
- Un canal sécurisé sur du NFC protège
 - de l'écoute
 - de la modification de données

Scenario : Mobile Unit (1)



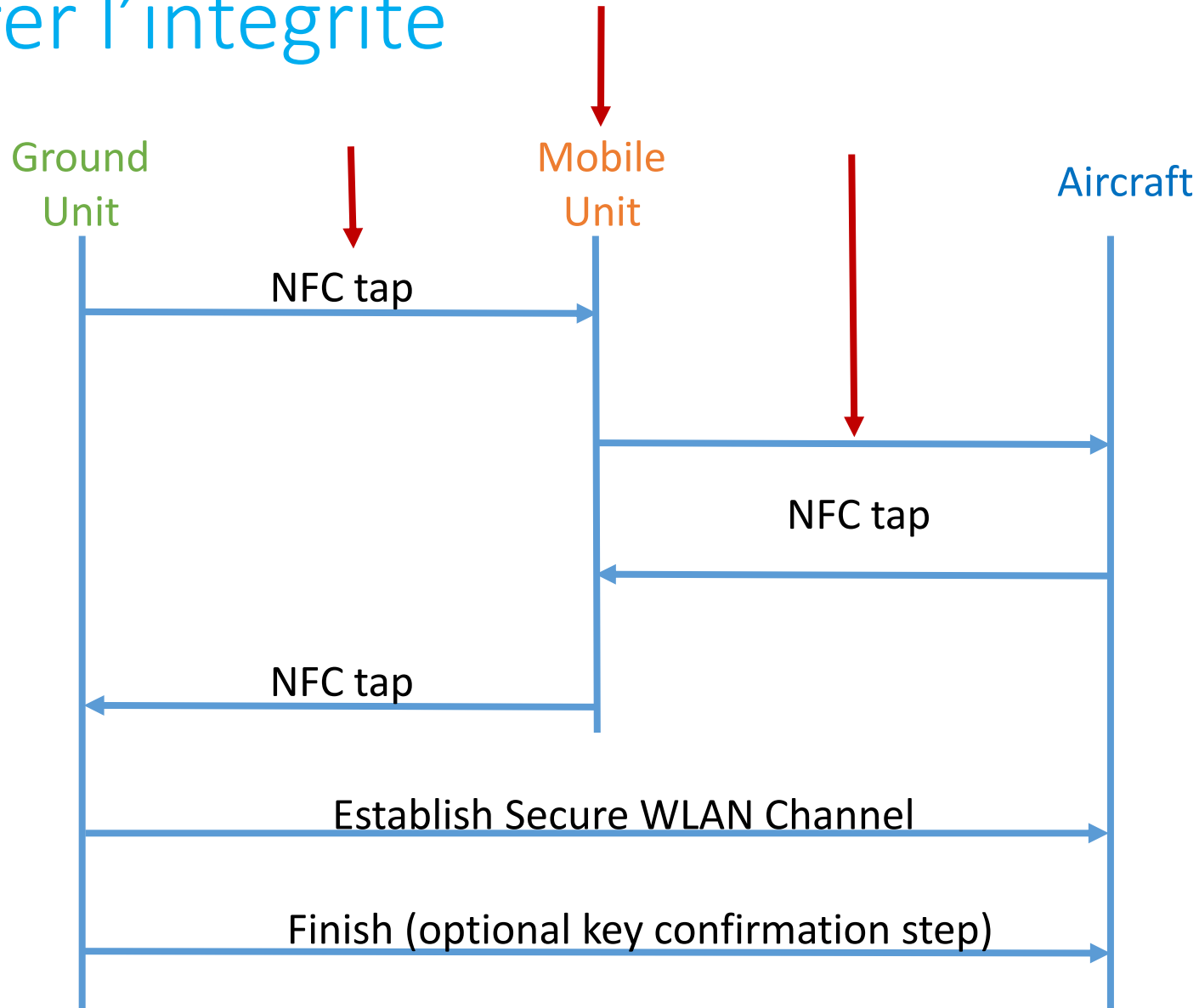
Attaque de l'homme du milieu par compromission du médium

Scenario : Mobile Unit (2)



Attaque de l'homme du milieu par modification du médium

Assurer l'intégrité



Solution « Plain TAGA »

1. Carte NFC avec une contrainte de distance
2. Carte NFC lié cryptographiquement au Ground Unit
3. Confirmation par clé physique

2 et 3 résistants contre des attaques extensibles

La suite...

- Une solution « Authenticated TAGA »
- Pour assurer une résilience complète contre les attaquants actifs

Avez-vous des questions ?

Les points clés :

- Solution d'authentification
- Contraintes particulières
- Canal spécial pour le pairage

Merci pour votre écoute

Pour plus d'information sur le projet : <https://www.enable-s3.eu/>



THANK YOU

ECSEL JU

The research leading to these results has received funding from the H2020-ECSEL-2015-2-IA-two-stage-Master/H2020-ECSEL-2015-2-IA-two-stage for ENABLE-S3 – European Initiative to Enable Validation for Highly Automated Safe and Secure Systems Joint Undertaking under grant agreement n° 692455 and from specific national programs and / or funding authorities.