Importance d'une cryptographie matérielle dans les mobiles

Marc MOUFFRON

CONNEXITY

EADS TELECOM

Approche de la présentation

- Les différentes technologies sans fil
- Exigences de sécurité des technologies sans fil
- Les solutions Logiciel – matériel
- Contrainte et avantage du matériel
- Différentes solutions matérielles
- Exemple TETRAPOL
- Conclusion

Les différentes technologie sans fils

- Réseaux cellulaires (GSM, ...)
- Téléphonie sans fil (DECT, …)
- Professional Mobile Radio (TETRAPOL, TETRA,…)
- Mode direct (talkie walkie, …)
- Téléphone satellite
- Pagers
- Réseau locaux sans fils

La raison d ’être est d ’abord la mobilité

Les menaces sur les réseaux sans fil

- Des menaces de toutes parts dues à :
  - la technologie radio
  - la mobilité
- Ecoute
- Rejeu de transactions
- Intrusion
- Masquarade
- Reprogrammation à distance sur l ’air
- Vol des mobiles

Exemples des Réseaux cellulaires

- Réseaux commerciaux
- S ’appuie sur une infrastructure filaire existante sans sécurité
- Pas de sécurité de bout en bout mais uniquement une sécurité sur le lien radio avec un objectif équivalent à la sécurité d ’un accès filaire

Chiffrement de bout en bout ou d'interface air

Caractéristiques des systèmes radio

- Terminaux de taille de plus en plus réduite avec
  - autonomie limitée
  - puissance limitée
  - débit réduit
- En général une qualité de service faible
- La perte de paquets est fréquente sur la radio
- Délais de transmission élevés et variables dues aux retransmissions au « handover »
- Temps de transit de bout en bout élevé
- Exige des protocoles de communication et de sécurité spécifiques et adaptés

Comparaison de protocoles de sécurité

- Les protocoles internet IPSEC, SSL, SSH sont trop bavards, avec des entêtes trop grandes et des temporisations inadaptées.
- Des adaptations telles que WTLS n ’ont pas réussi
- Seuls des protocoles spécifiques sont réellement opérationnels:
  - Mono-technologie
  - générique : FNBDT

FNBDT:Future Narrow band Data Terminal

- Proposition de standardisation des services de sécurité de bout en bout sur différents réseaux
  - réseaux cellulaires : GSM, TDMA, CDMA
  - réseaux satellitaires
  - réseaux PMR
  - réseaux tactiques
  - tous réseaux offrant une bande passante de 2400 bps
- Spécifie l ’établissement d ’appel
- Spécifie des mécanismes de chiffrement de la voix et des données asynchrones

Sécurité de bout en bout des mobiles

- La confidentialité de bout en bout
- L'authentification et la non-répudiation
- L'intégrité des transactions
- La sécurité de bout en bout doit assurer la protection de la voix et des données avec :
  - un coût minimal,
  - des retards de transmission faibles,
  - une complexité réduite,
  - dans une bande-passante étroite avec peu de signalisation additionnelle.

Terminaux mobiles sécurisés

- Les exigences d ’autonomie impose des restrictions de service
- Principes fondamentaux de la radio : bande-passante, taux d'erreurs, délai de transmission
- LOGICIEL :
  - La puissance de calcul et la capacité de stockage limitée restreint les algorithmes crypto utilisables
- MATERIEL:
  - Peu de place disponible et peu d ’entrées - sorties
  - Puissance de calcul autorise tout type d ’algorithmes

Intérêt d ’un chiffre matériel dans un mobile

- Fournir une sécurité de niveau élevé sans nuire aux services d'utilisateur
  - services de communication
  - durée d'utilisation
  - large gamme de mobiles possible
- Cryptographie de haut niveau
  - la sécurité peut être utilisée dans tous les cas
  - confidentialité des clés (et des algorithmes)
  - consommation très basse selon les solutions
- VRAI générateur de nombres aléatoires matériel
- La distribution des clés à distance avec tous les services de sécurité requis.

Solutions matérielles possibles

- Cartes à puces
- FPGA
  - programmable
  - consommation et surface occupées élevées
- Bloc IP dans un ASIC
  - performant
  - complexité limitée
- ASIC Chiffre dédié
  - solution de sécurité optimale

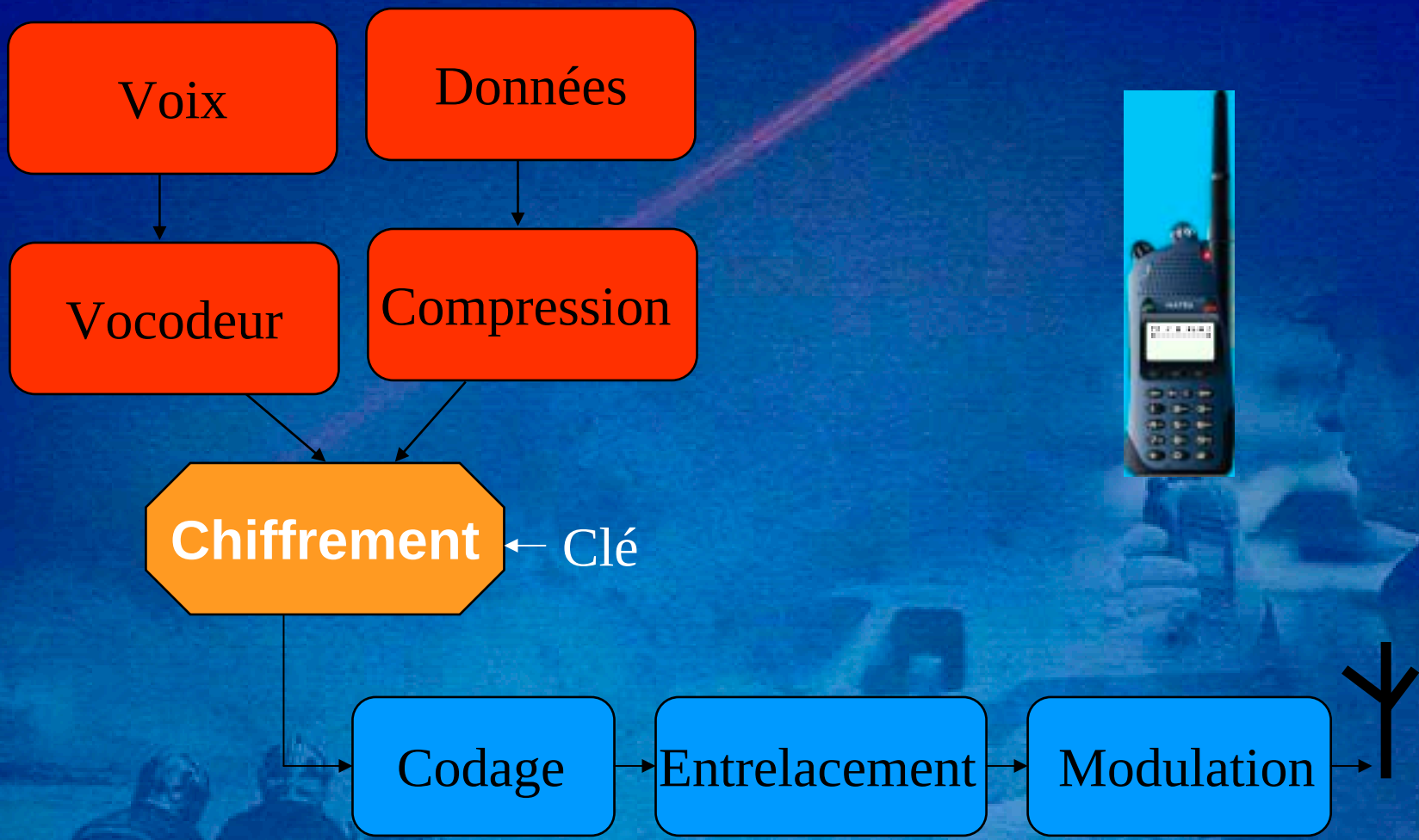
Solution Carte à puce

- Les avantages d ’une carte à puce sont :
  - la standardisation
  - le niveau de sécurité
  - la mobilité
  - le coût
  - la simplicité
- Les inconvénients sont :
  - les performances
  - le débit d ’entrée-sortie
  - la consommation

Terminaux PMR avec carte à puce de sécurité de bout en bout

- En plus des fonctions SIM une carte à puce est utilisée pour des services de sécurité de bout en bout (par exemple le chiffrement)
- La différence fondamentale est l ’utilisation permanente
- Performance des algorithmes symétriques: OK
- Performance des algorithmes asymétriques: insuffisante
- Des contraintes majeures apparaissent:
  - le débit d ’entrée-sortie
  - la consommation

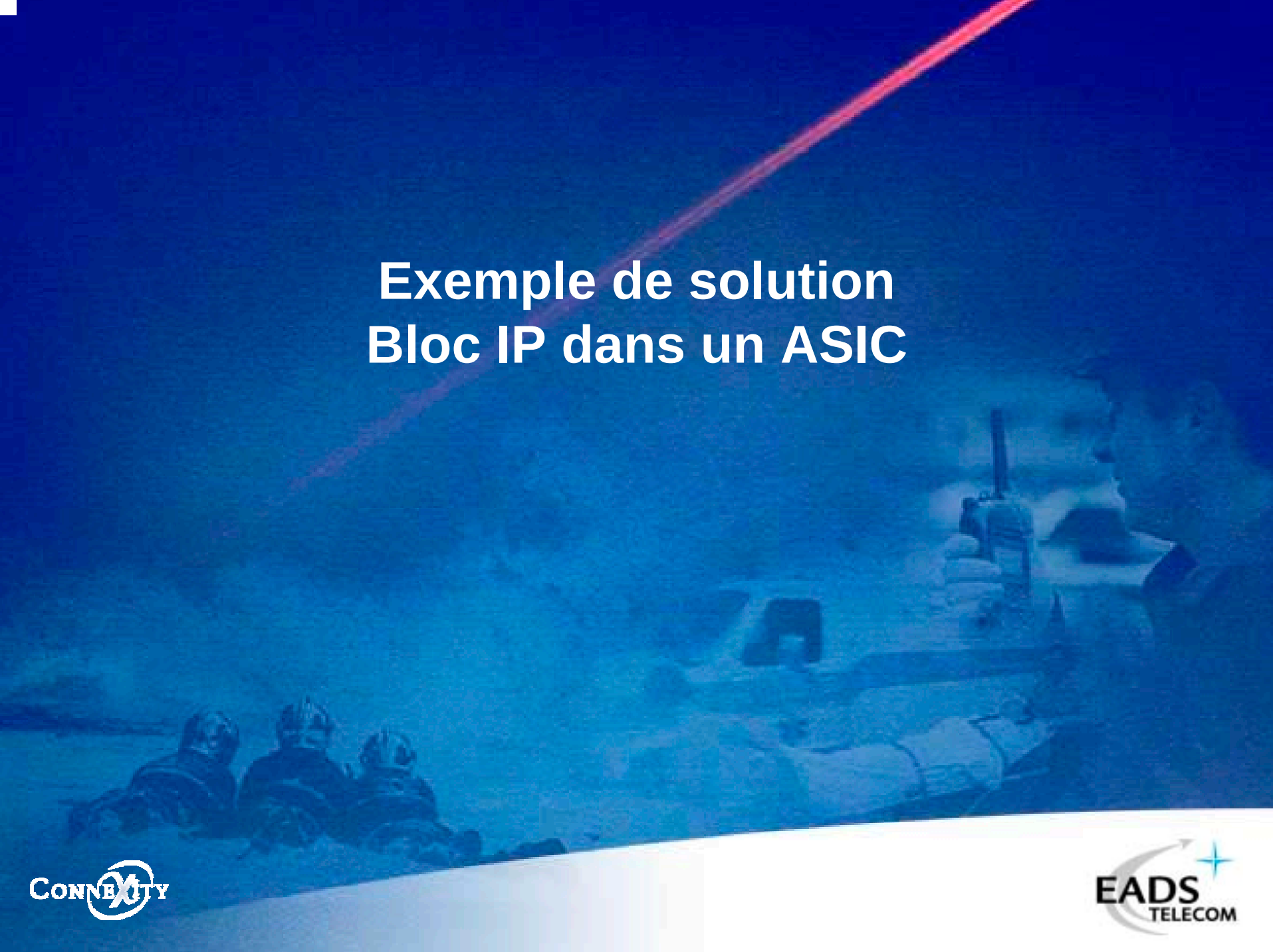
Chiffrement de bout en bout dans un mobile



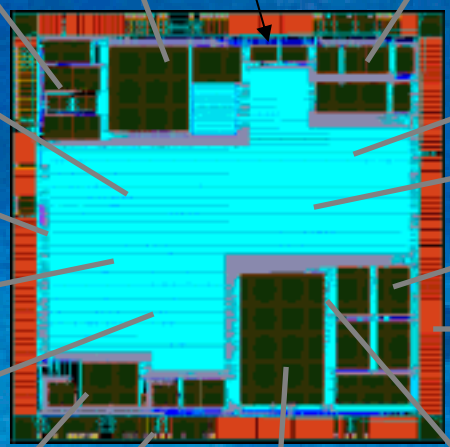
Exemple de limitations d ’une carte à puce

- Le vocodeur fournit des trames de phonie toutes les 20 ms
- L ’entrée d ’une trame claire et la sortie de la trame chiffrée correspondante demande 37,5 ms
- Indépendant de l ’algorithme cryptographique utilisé
- Optimisations possibles :
  - débit d ’entrée - sortie (> 9600 b/s)
  - mode d ’opération crypto
  - compromis sur la sécurité

Exemple de solution
Bloc IP dans un ASIC



Solution « System On Chip » pour la PMR



Security functions

Analog Cells

I-Q Modem

Analog Cells

Custom Cells

Time base, Power gain ctrl, Frequency ctrl, Synthesiser ctrl, Micro-Wire, analog channels.

Low power Sequencing Unit

Power Management

* About 30 clocks under software control.
* Power-down mode for analog cells.

Test Interface

* JTAG.
* TIC for ARM & peripheral.
* Custom 64 IOs Test Port for Digital / Analog cells.

On Chip RAM & ROM

µBGA 256 Package

* Die size area: 85 mm^2
* About 270.000 gates
* CMOS 0.5 µ

IP Cells

I^2C & SMBUS

ARM peripheral cells

Cofidec

PLL

ARM Core

* Low power consumption.
* Code size reduction (Thumb).

AMBA Architecture

* Multi-master high speed bus (3 master on chip).
* Versatile & Low power peripheral bus.

Fonctions de sécurité du SOC

- Algorithme de signature spécifique
- Fonctions de contrôle d ’intégrité du code du terminal mobile
- Fonctions d ’authentification du terminal mobile
- VRAI générateur de nombres aléatoires matériel

Exemple de solution
ASIC chiffre dédié

Fonctions de sécurité d ’un ASIC chiffre

- Fonctions de gestion de clés
- Multi-Algorithmes
- Contrôle d ’intégrité du code du terminal mobile
- Service de chiffrement et déchiffrement des communications
- Authentification du terminal mobile
- Désactivation sécurisée à distance du terminal mobile
- VRAI générateur de nombres aléatoires matériel
- Protection des clés

VRAI générateur de nombres aléatoires

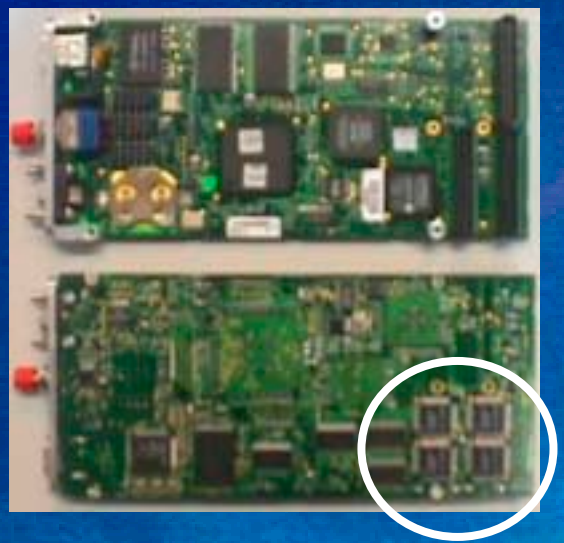
- Beaucoup de mécanismes de sécurité repose sur la disponibilité d ’une source d ’aléa vrai
- Seule une solution matérielle est possible
- Utilisation d ’une source de bruit physique
- Complexité supplémentaire avec une fonction à sens unique
- Validation à la fabrication
- Validation en utilisation par des tests de type FIPS 140-2

Portable sécurisé TETRAPOL

- Conçu pour des utilisateurs PMR
- ASIC chiffre intégré
- Service de chiffrement et déchiffrement des communications de bout en bout
- Services d'authentification
- 2 niveaux de désactivation sécurisée à distance

- Capacités chiffre équivalentes pour d'autres mobiles de la gamme

Sécurité TETRAPOL coté infrastructure



ASIC chiffre

- Carte chiffre TETRAPOL
- Interface au format PMC
- Intègre le même Asic que les terminaux mobiles
- Offre des services d'authentification des terminaux mobiles
- Offre des services de désactivation à distance des terminaux mobiles
- Stockage sécurisé des clés
- Effacement de sécurité

Conclusion

- Un ASIC chiffre permet d ’offrir de la sécurité de bout en bout sur des communications temps réel
- Le coût global est optimisé
- En plus avec un ASIC programmable on retrouve la souplesse du logiciel