AIRBUS DEFENCE & SPACE

General information

AIRBUS DS SLC (Secure Land Communication)

Christophe CALVEZ

christophe.calvez@airbus.com

+33 1 61 38 78 81

Area of interest	**Choose Y or N**
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	Y
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	N
○ Authenticated encrypted token research for mobile payment solution	N
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	N
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	Y
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	Y

Competencies

- *Organisation competencies*
  - Professional Mobile Radio manufacturer for more than 20 years (TETRA/TETRAPOL/P25),
  - Develop network infrastructure and radio terminal products with secured communications needs *(End to End encryption, authentication, HW crypto module …),*
  - Several Public Safety nationwide networks installed all over the world,
  - Competences in security, algorithm/cryptography design and implementation.

- *Organisation experience in the European project*
  - Involved in projects like : SALUS, SOAPS, ISITEP, EPISECC, SECINCORE

- *The skills you can bring*
  - Crypto expertise and implementation
  - Security and cryptography use cases
  - Secured communications solutions and expertise

Project idea

- *Describe your project idea*

⇒ *(can also be a use case attached to another project).*

  - The PMR network are going to migrate from narrowband (TETRA/TETRAPOL) to broadband (LTE/3GPP MCxx) technology (*under standardisation*)
  - New broadband solution and Mission Critical services are based on IBE cryptography mechanisms (*MIKEY-SAKKE*) for key distribution and symmetric algorithm for media encryption,
  - Project / use cases could be to :
    - Analyse and propose security/crypto improvement for the future standardisation releases
    - Analyse, propose and perform feasibility studies for a quantum safe solution

- *List of the complementary skills you need for your consortium*
  - To be discussed
    - HW crypto module provider
    - Academic cryptography experts