

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

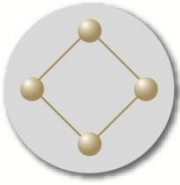
General information

Company name : Oppida

Contact name : Sylvain Ruhault

Contact details : sylvain.ruhault@oppida.fr / 0628566638

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



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Competencies

- *Organisation competencies*

Security testing of IT systems and products

- **Common Criteria (ISO 15408) evaluations (100 evaluations performed)**
- **CSPN evaluations (> 50 evaluations performed)**
- **Cryptographic assessments ((> 50 assessments performed)**

Licensed by



- *Research projects*

- **Industrial systems security (SCADA)**
- **Attack detection (IDS)**
- **Cryptography (PRNG analysis)**

- *The skills you can bring*

- **Common Criteria / code source analysis / reverse / pen tests**

Project idea

- *Describe your project idea*
- *List of the complementary skills you need for your consortium*