European Brokerage Event

5th September 2016
BUSINESS FRANCE
77 Boulevard Saint Jacques
75014 Paris

DS-06-2017

Cryptography

Horizon 2020

The French NCP's for ICT and Secure Societies, the Security Research NCP Network (SEREN3), IDEAL-IST, UPMC, INRIA, Systematic, and Safe Cluster are pleased to invite you to the brokerage event dedicated to the topic: **DS-06-2017: Cryptography**, that will take place on Monday 5th September 2016 in Paris.

At this event, supported by the European Commission, you will have the opportunity to share with the participants an overview of your company products, services, and competencies in the cryptography area. You can also present your own proposal concepts. Then, you can meet representatives from SMEs and other organisations, in order to exchange ideas with the aim of paving the way for future cooperation.

Participation in the brokerage event is *free of charge*. However, *registration is mandatory.*
Please register online by 30 August 2016 at the following link:
http://www.horizon2020.gouv.fr/cryptography-5th-september-2016
Seats will be allocated on a first come, first serve basis due to the *limited capacity* of the meeting room.

AGENDA

Time	Session
09:30 - 10:15	**Welcome, registration, coffee, and networking**
10:15 - 10:30	**Cyber security PPP,** *Dr. Luigi Rebuffi, EOS*
10:30 - 10:50	**Presentation of current activities in cryptology and of the DS-06-2017 topic,** *Dr. Florent Frederix, DG CNCT*
10:50 - 11:10	**Automated proof techniques for cryptographic assurance,** *Dr. Bruno Blanchet, INRIA*
11:10 - 11:30	**Ultra-lightweight cryptology,** *Dr. Francois-Xavier Standaert, UC Louvain*
11:30 - 11:50	**Quantum safe cryptography,** *Dr. Jean-Charles Faugère, INRIA & Dr. Ludovic Perret UPMC*
11:50 - 12:10	**Quantum key distribution,** *Dr. Bruno Huttner, ID Quantique*
12:10 - 12:30	**Cryptography, Encryption and Big Data,** *Dr. Hoeteck Wee, ENS-Ulm, Paris*
12:30 - 13:30	**Networking Lunch**
13:30 - 13:40	**Presentations of the networks: IDEAL-IST & SEREN 3,** *Claire Ferté, Business France & Gabriella Quaranta, APRE*
13:40 - 15:00	**Participants' presentations (2 minutes per presentation)** *A presentation will include your organization key figures, products, services, and competencies, and possibly your proposal suggestions*
15:00 - 15:10	**Short break**
15:10 - 16:00	**8 potential parallel working groups** *Each work group will elaborate informal proposal(s)*
16:00 - 16:15	**Q&A session and conclusion,** *Dr. Florent Frederix, DG CNCT*

Brokerage session	Room	Number of registered participants
o Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	Amphithéâtre	25
o Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	DSS 101	16
o Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	DSS 106	10
o Authenticated encrypted token research for mobile payment solution	DSS 104	12
o Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	Mezzanine	25
o New techniques, such as quantum safe cryptography, which are secure from quantum computers	DSS 103	22
o Quantum key distribution	ASS 101	13
o Automated proof techniques for cryptographic protocols	DSS 105	14
o Not decided yet	DSS 102	13