DS-06-2017 Cryptography

Paris – 05/09/16

Agenda

TIC Sécurité
PCN - Horizon2020 PCN - Horizon2020

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*

HORIZON
LE PROGRAMME DE RECHERCHE D'INNOVATION DE L'UNION EUROPÉENNE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

HORIZON 2020: UN PROGRAMME MAJEUR AU NIVEAU NATIONAL

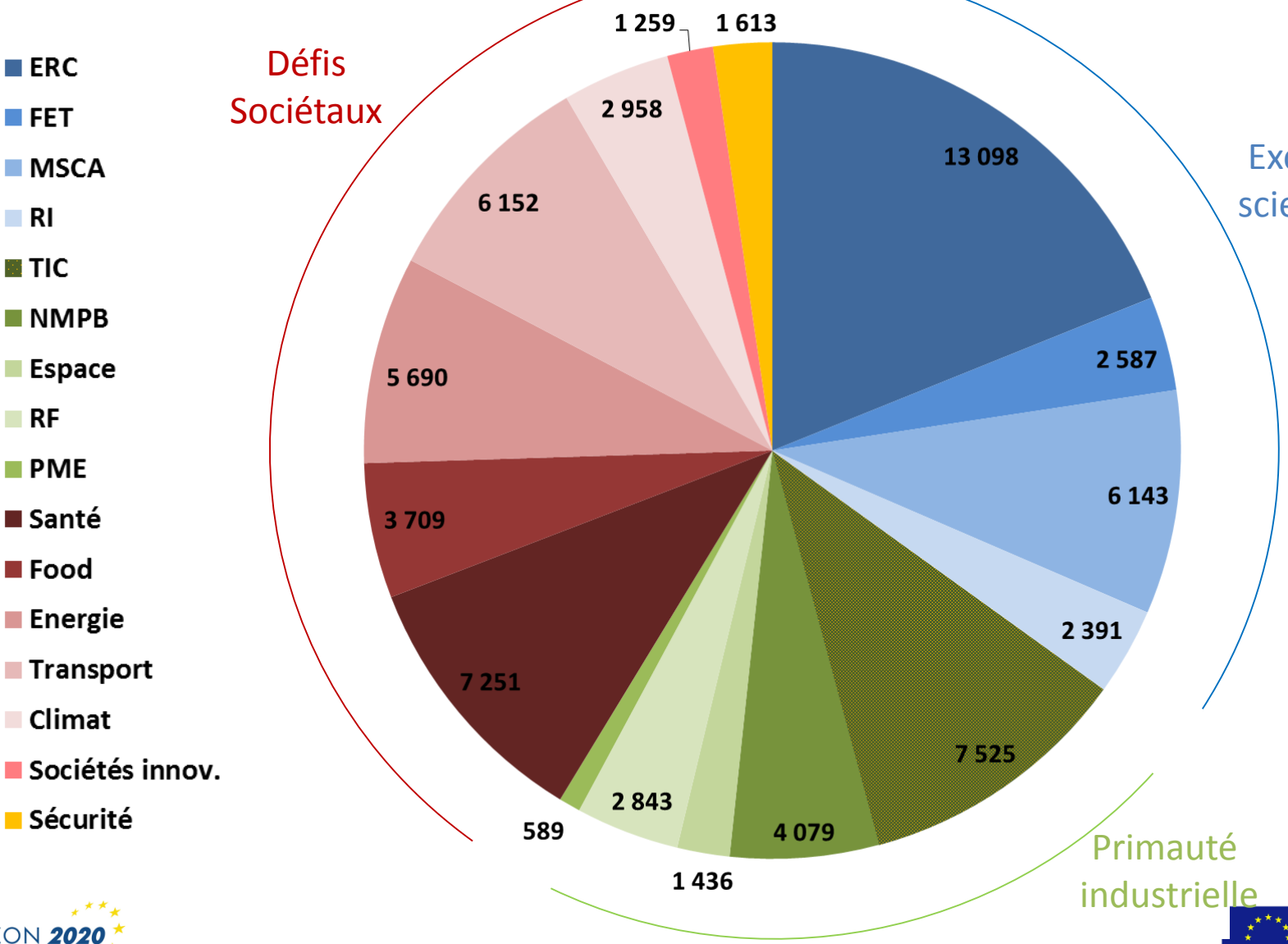
TIC PCN - Horizon2020 Sécurité PCN - Horizon2020

Financement non-récurrent des équipes nationales de RDI en 2014

77,2 Md€ dont ~1,8 Md€ pour la sécurité

TIC PCN - Horizon 2020

Sécurité PCN - Horizon 2020



HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MISE EN ŒUVRE H2020:
LE MÉCANISME DES APPELS À PROPOSITIONS

TIC PCN - Horizon2020 Sécurité PCN - Horizon2020

6 mois – 1 an *3 mois – 10 mois* *Max. 8 mois* *2 - 4 ans*

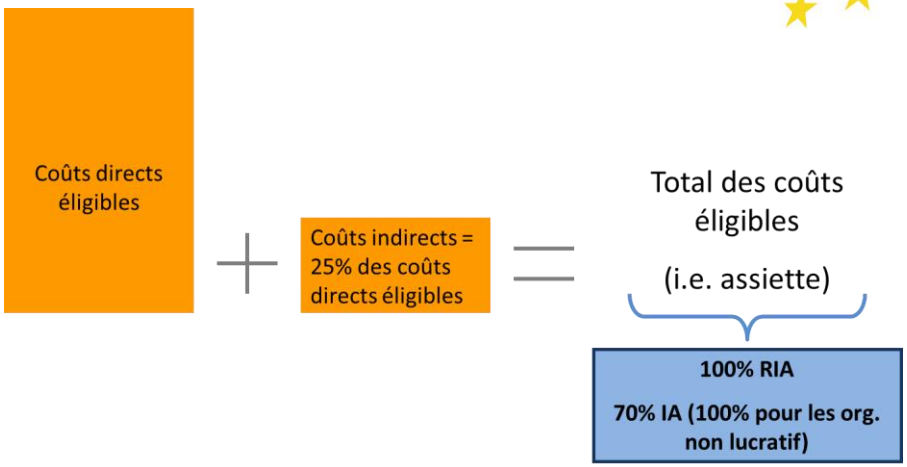
HORIZON 2020 LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

LES PRINCIPALES RÈGLES D'HORIZON 2020

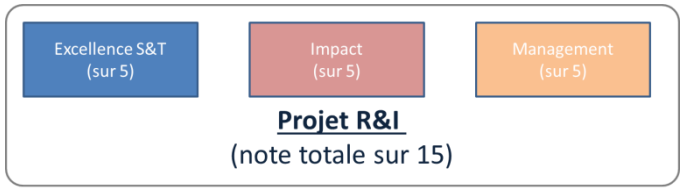
TIC PCN - Horizon2020 Sécurité PCN - Horizon2020

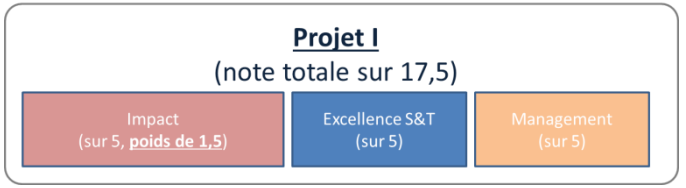
1. Des taux de subvention modifiés



A comparer aux taux nationaux !

2. Une pondération des critères modifiée





3. Une gamme d'« instruments » plus larges :

- De plus en plus en de PCP
- L'instrument PME
- L'instrument *Fast Track to innovation (FTI)*

4. Un « *time-to-grant* » de 8 mois max.

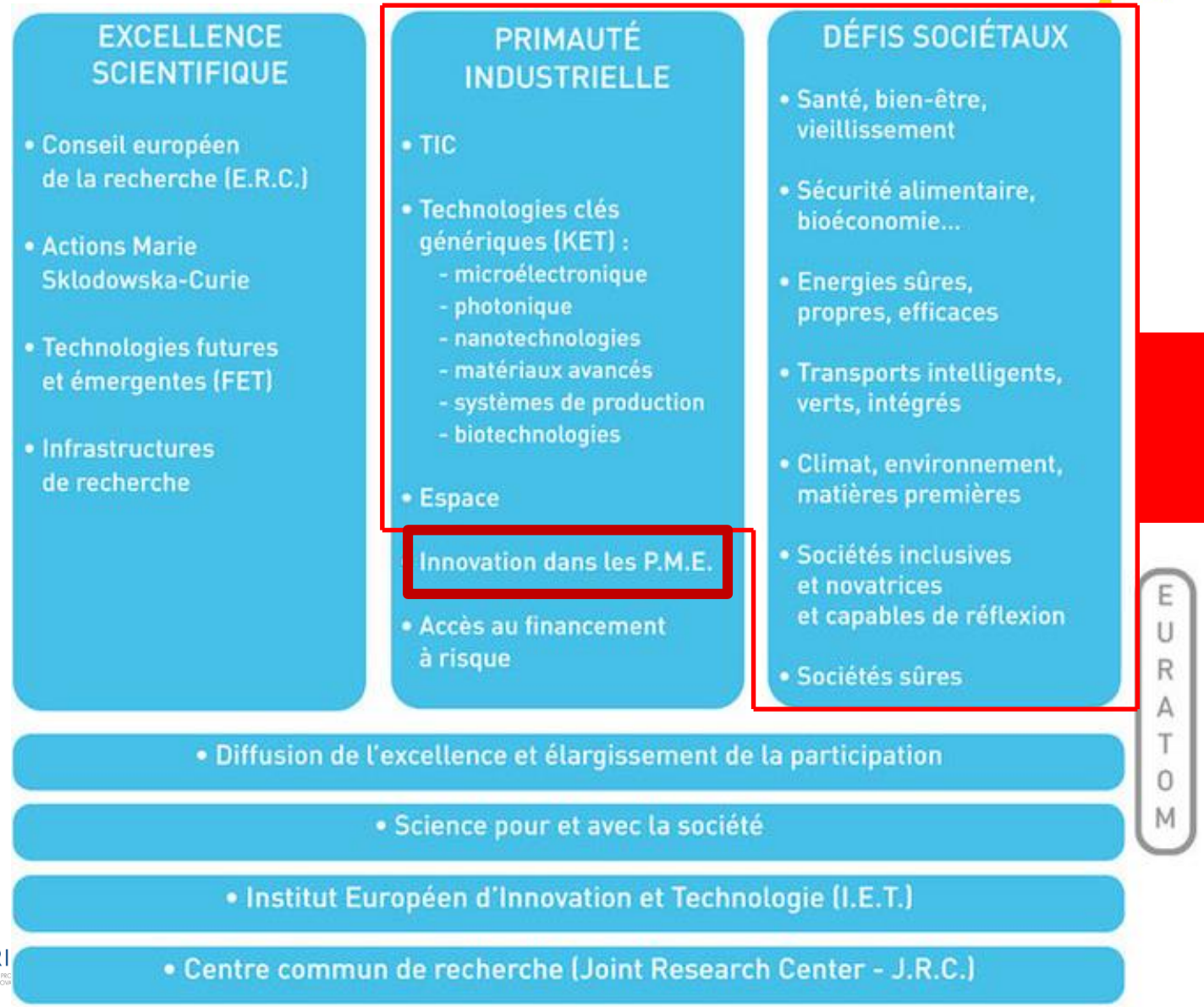
HORIZON 2020 LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

ATTENTION ACCRUE PORTÉE AUX PME

TIC PCN - Horizon2020

Sécurité PCN - Horizon2020



Objectif politique d'allouer 20% du budget aux PME

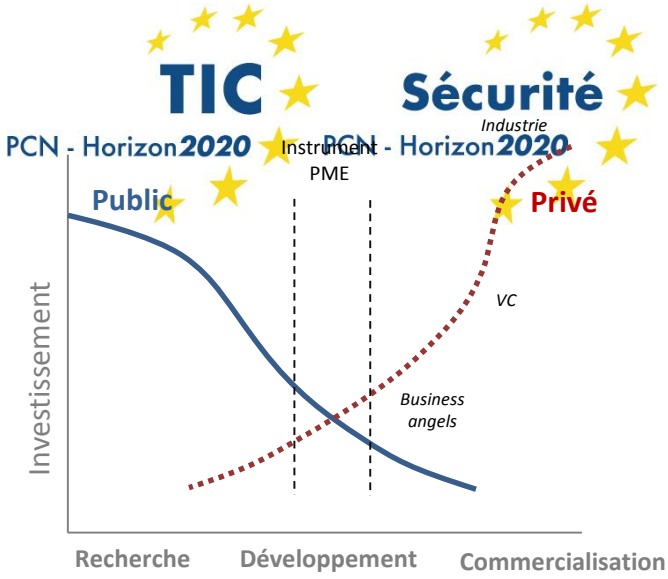
A terme, 7% du budget alloué au nouvel instrument PME

HORI

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

INSTRUMENT PME

- Phase 1: idée/concept,
  - Input: Business plan I (10 p.)
  - Activités: faisabilité, analyse risques, IP, recherche partenaires, pilote…
  - Output: Business plan II
  - 50 k€, ~ 6 mois
- Phase 2: R&D, démonstration, *market replication*
  - Input: Business plan II et description des activités de la phase 2 (30 p.)
  - Activités: développement, prototypes, test, pilotes, miniaturisation, scale-up…
  - Output: investor ready Business plan III
  - 1-3 M€, 12-24 mois
- Phase 3: Commercialisation
  - Coaching sur l'accès aux financements, formation, IP management…



Concept & Etude de faisabilité (50 k€)

R&D Démonstration (1-3 M€)

Commercialisation (Coaching)

IDEE → MARCHE

10%

30-50%

Taux de succès envisagé

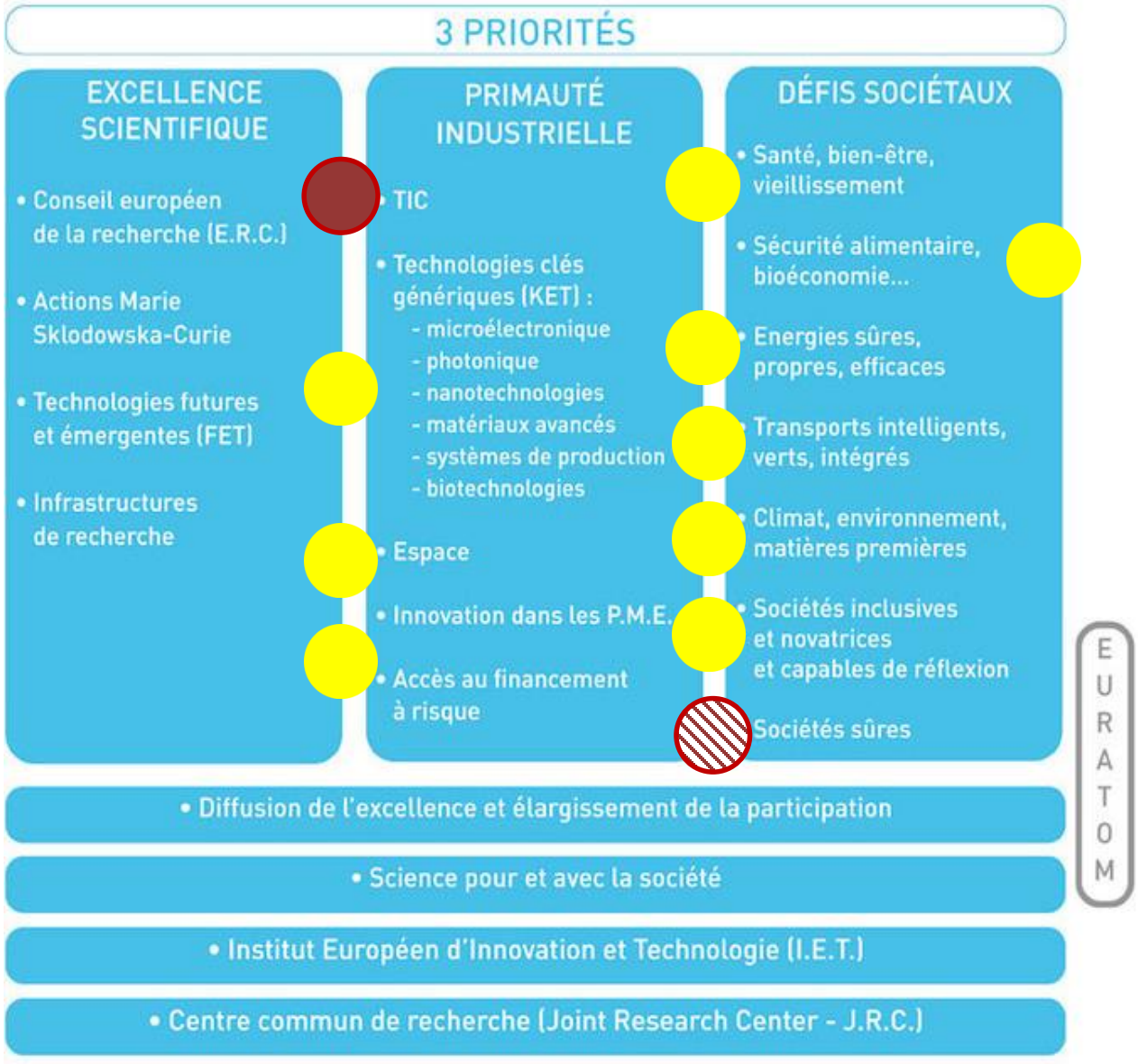
HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ATTENTION: IL Y A DE LA CRYPTO AILLEURS

TIC PCN - Horizon2020

Sécurité PCN - Horizon2020



HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Cybersecurity cPPP
and
European Cyber Security Association - ECSO

L.REBUFFI
ECSO Secretary General and (interim) Chairman of the Board

European Brokerage Event
DS-06-2017: Cybersecurity PPP: Cryptography

Paris - September 5th 2016

SIGNATURE CEREMONY – July 5, 2016

EUROPEAN CYBER SECURITY ORGANISATION

Commissioner Oettinger

46 ORGANISATIONS
14 DIFFERENT COUNTRIES
MORE THAN 300 TWEETS
180 TWITTER FOLLOWERS
1,610 WEBSITE VIEWS

"Cybersecurity needs trust and confidence We have to invest in cybersecurity. This means financial investment, technological investment and human investment"

"This PPP is the beginning of a team work"

"It is our ambition to stabilise cybersecurity in our digital infrastructure and to leverage upon our industries to develop a European culture of cybersecurity"

"Cybersecurity is a shared responsibility we need your economic and technical competence"

"We are expecting from your side advise on what should be done from our side"

Budget

- Commission contribution to the cPPP for R&I initiatives (from H2020 budget): **€450 mln for the 2017-2020 calls (4 years)**
- **Leverage factor = 3**

  The cPPP should demonstrate that the €450mln will trigger investments linked to R&I for 3*450= € 1350mln in the next (typically) 10 years
- Contributions are expected from private investments (users/operators, suppliers, RTOs/Universities, national R&I funds, other EU funds: regional / structural, capital venture, insurances, etc.) and public funding

Key Performance Indicators - KPIs

Industrial Competitiveness

KPI 1: **MARKET DEVELOPMENT**

- Evolution of cybersecurity revenues in the European and global market, including positioning and market share of the EU industry

KPI 2: STANDARDS, TESTING, CERTIFICATION AND TRUST LABELLING

- Contribution to standards, use of testing, validation, certification infrastructures as well as EU trust labelling procedures, best practices and pilots for innovative elements of the supply chain

KPI 3: USERS AND APPLICATIONS

- Increased use of cybersecurity solutions in the different markets / applications

KPI 4: PRODUCTS and SERVICES SUPPLY CHAIN

- Development of the EU cybersecurity industry and of the European digital autonomy.

KPI 5: SMEs

- Support the creation and development of start-ups having products / services that effectively reach the market.

Key Performance Indicators - KPIs

Socio-Economic Security

KPI 6: EMPLOYMENT

- Develop employment in cybersecurity sectors (supply and users / operators)

KPI 7: ECOSYSTEM: EDUCATION, TRAINING, EXERCISES

- Development of education, training and skills on cybersecurity products and safe use of IT tools in European countries for citizens and professionals

KPI 8: PRIVACY & SECURITY BY DESIGN

- Development and implementation of European approaches for cybersecurity, trust and privacy by design

KPI 9: DATA / INFORMATION EXCHANGE & RISK MANAGEMENT

- Facilitate process for information sharing between MS, CERTs and Users to increase monitoring and advising on threats; better understanding risk management and metrics

KPI 10: IMPLEMENTATION OF LEGISLATIONS

- Implementation of the NIS Directive and market driving Regulations / Guidelines

Key Performance Indicators - KPIs

Implementation and operational aspects of the cPPP

KPI 11: **INVESTMENTS**

- Investments (R&I, capability, competence and capacity building) in the cybersecurity sectors defined by the cPPP objectives and strategy

KPI 12: cPPP MONITORING

- Efficiency, openness and transparency of the PPP Consultation Process

KPI 13: COORDINATION WITH THE EU and THIRD COUNTRIES

- Coordination of the cPPP implementation with EU Member States, Regions and Third Countries

KPI 14: DISSEMINATION & AWARENESS

- Dissemination and Awareness making the cPPP action and results visible in Europe and internationally, to a broad range of public and private stakeholders

THE INDUSTRY PROPOSAL:
Cybersecurity challenges in Europe

ECS
EUROPEAN CYBER SECURITY ORGANISATION

- Global cybersecurity and ICT market dominated by global suppliers from North America.
- Mature commodity market.
- Market fragmentation.
- Innovation led by imported ICT products.
- Innovation: strong in Europe but not always properly funded due to a lack of a consistent transnational approach. Results of Research and Innovation are hardly reaching the market. There is still a lack of strategy in European research
- Financial. Weak entrepreneurial culture, lack of venture capital.
- European industrial policies not yet addressing specific cybersecurity issues.
- Human factor.
- Sovereignty.
- Strategic supply chain dependency.

Overall long term vision of the PPP

Main strategic objectives for an industry led European Cybersecurity cPPP:

- The protection from cyber threats of the growth of the European Digital Single Market
- The creation of a strong European-based offering and an equal level playing field to meet the needs of the emerging digital market with trustworthy and privacy aware solutions
- The growth and the presence of European cybersecurity industry in the global market

THE INDUSTRY PROPOSAL:
Operational / Strategic Objectives

- Protecting critical infrastructures from cyber threats.
- Use of massive data collection to increase overall security.
- Increased European digital autonomy.
- Security and trust of the whole supply chain.
- Investments in areas where Europe has a clear leadership.
- Leveraging upon the potential of SMEs.
- Increase competitiveness.

Cybersecurity: a different cPPP

- Cybersecurity: a transversal issue, pervasive in all sector (economic, societal, …): large number of stakeholders, of interests, of constraints…
- Security: a national prerogative. Stronger participation of representatives from the national administrations, also at decision making level (not just a "mirror group")
- Interest from national Public Administrations: Representatives to the two PCs + Ministries (Interior, Economy, etc.) + Regulatory Bodies + Public users

- cPPP: leveraging upon H2020 rules
- Open to any entity eligible under H2020 (EU MS + EEA / EFTA countries)

- **The cPPP will focus on R&I, developing a SRIA and supporting its implementation in the H2020 Work Programme**

- **The ECSO Association will tackle other industry policy aspects for the market and the industrial / economic development**
- **ECSO will support the development of the European cybersecurity industry and EU trusted solutions, including cooperation with Third Countries.**

European Cybersecurity Council
(High Level Advisory Group: EC, MEP, MS, CEOs, …)

ECS - cPPP Partnership Board
(monitoring of the ECS cPPP - R&I priorities)

EUROPEAN COMMISSION

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Governance

ECSO - Board of Directors
(management of the ECSO Association: policy / market actions)

INDUSTRIAL POLICY
Coordination / Strategy Committee

R&I
Scientific & Technology Committee

- WG Standardisation Certification / Labelling / Supply Chain Management
- WG Market development / Financing Export
- WG Sectoral demand (market applications)
- WG Support SME, East EU, …
- WG Education, training, awareness, exercises
- WG SRIA Technical areas Products Services areas

- SME solutions / services providers; local / regional SME clusters and associations Startups, Incubators / Accelerators
- Others (financing bodies, insurance, etc.)
- Large companies Solutions / Services Providers; National or European Organisation / Associations
- Regional / Local administrations (with economic interests); Regional / Local Clusters of Solution / Services providers or users
- Public or private users / operators: large companies and SMEs
- NATIONAL PUBLIC AUTHORITY REPRESENTATIVES COMMITTEE R&I Group
  Policy Group / GAG
- Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO
General Assembly

ECSO Membership (152 from 23 countries)

To be admitted as a Member, the party should be:

a) Legal Entity established at least in an EU Member State, an EEA / EFTA country or an associated country (called: "ECSO Countries")

b) A public body from an ECSO Country.

CATEGORIES OF MEMBERS

a) Large companies : cybersecurity solutions / services providers;

b) National and European Organisation / Associations (gathering large companies and SMEs) representing interests at national or European / International level.

c) SME solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators.

d) Users / Operators (where cybersecurity technology / solutions / services provision is not one their business activities): National public administrations or private companies (large or SMEs) directly represented.

e) Regional / Local public administrations (with economic interests); Regional / Local Clusters of public / private Legal Entities with local economic / ecosystem development interests.

f) Public Administrations at national level (national strategy / regulatory / policy issues, incl. R&I coordination).

g) Research Centers, Academies / Universities; Associations composed only by Research Centers, Academies or Universities.

h) Others (financing bodies, insurances, consultants, etc.).

	2017	2018	2019	2020	TOTAL	%
CYBER PILLARS	10	13	14	14	51	6.0%
Trustworthy Innovation Ecosystem					15	
Technical Experimentation Ecosystem					36	
RESEARCH & INNOVATION ACTIONS (technical projects based on technical priorities	44	107	98	90	339	39.9%
3.1.1 Priority "Fostering assurance and security and privacy by design"					42	
identity, access and trust management					36	
3.1.2 Priority "Identity and Access Management"						
3.1.3 Priority "Trust Management"						
data protection, including encryption					63	
3.1.4 Priority "Data security"						
Protecting the ICT Infrastructure and enabling secure execution:					150	
3.1.5 Priority "Cyber Threats Management"						
3.1.6 Priority "Network Security"						
3.1.7 Priority "System Security"						
3.1.8 Priority Cloud Security"						
3.1.9 Priority "Trusted hardware/ end point security/ mobile security"						
Security services					48	
3.1.10 Priority "Auditing, compliance and certification"						
3.1.11 Priority "Risk Management"						
3.1.12 Priority "Managed/management security services"						
3.1.13 Priority "Security training services"						
CYBER INFRASTRUCTURE (produts / services used in different applications)						50.9%
Integration Projects (validation of existing technology solutions)	*20*	*63*	*71*	*70*	*224*	
A) digital citizenships (including identity management)					22	
B) risk management for managing SOC, increasing cyber risk preparadness plans for NIS etc.					45	
C) information sharing and analytics For CERTs and ISACs (includes possibly trusted SIEM, cyber intelligence)					40	
D) Secure Networks and ICT (Secure and trusted Routers, Secure and Trusted Network IDS, Secure Integration, Open source OS)					117	
Demonstration / Pilot projects (solutions in different applications)	*20*	*45*	*50*	*50*	*165*	
Energy, including smart grids					18	
Transport					22	
Finance					18	
Healthcare					22	
Smart & Secure Cities					22	
Public Services / eGovernment					31	
Industrial Critical Systems / Industry 4.0					32	
Bottom up track on innovation	0	13	14	17	*44*	
COORDINATION (Stakeholder cooperation for Roadmapping Dissemination & Communication; KPI monitoring activities; MS cooperation; International Relationship; EU observatory; Governance, …)	6	7	7	7	27	3.2%
	100	248	254	248	850	100.0%

ECS
EUROPEAN CYBER SECURITY ORGANISATION

ECSO Suggestions for future Work Programmes with a global strategy

ECSO WG6 - SRIA (Strategic Research and Innovation Agenda) First meeting: September 12 and 14

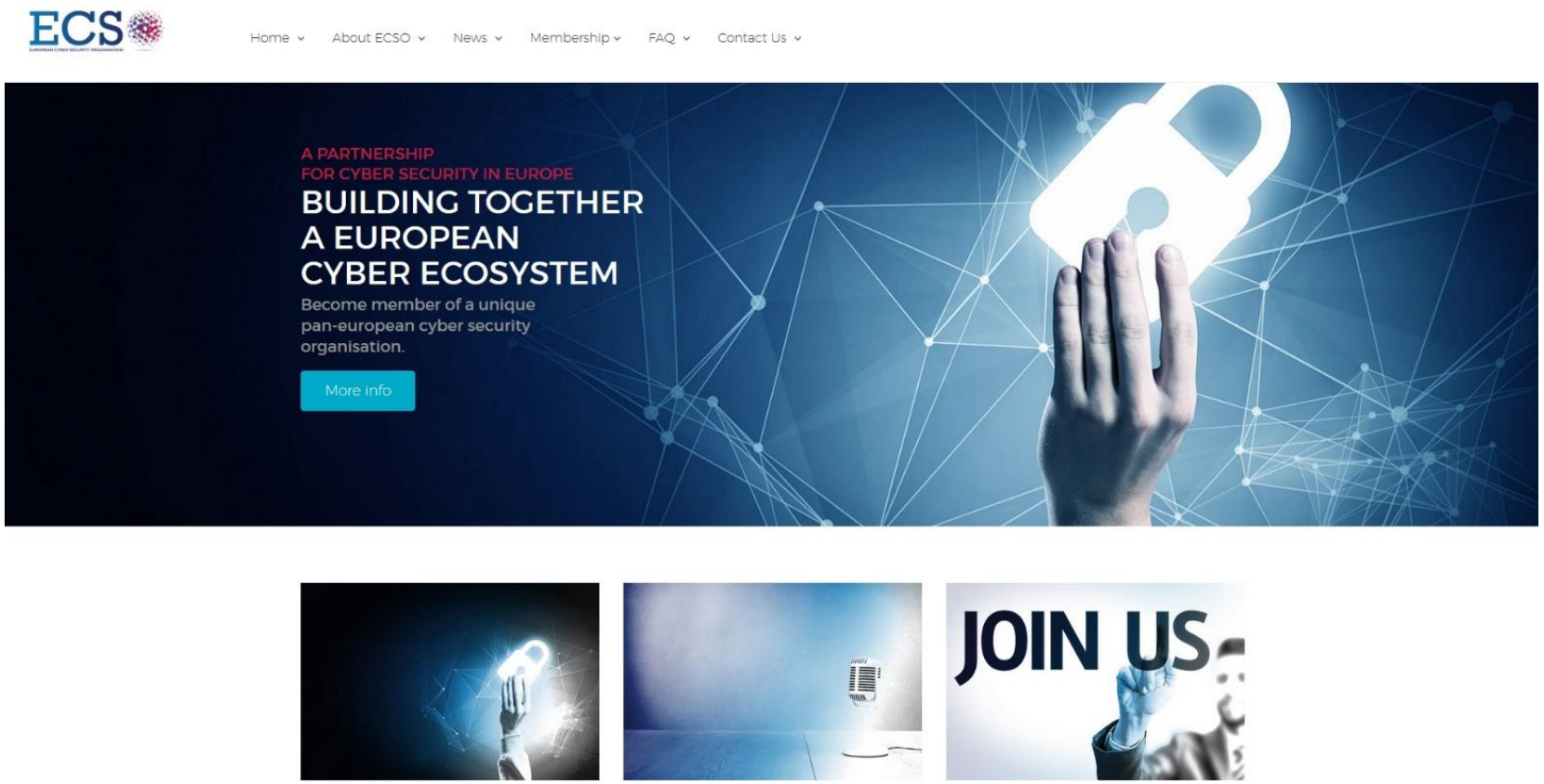
Segmentation

- **WG 6.1: Coordination and support activities at several levels**
  - Market and stakeholders update,
  - Link across R&I projects and other cPPP / EC initiatives (5G, Cloud, IoT, Big Data, etc.)
  - Dissemination & awareness, events etc.

- **WG 6.2: Technical priority areas**
  - Assurance / risk management and security / privacy by design
  - Identity, access and trust management (including Identity and Access Management, Trust Management)
  - Data security
  - Protecting the ICT Infrastructure (including Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
  - Security services

- **WG 6.3: Trustworthy infrastructures**
  - Digital citizenships (including identity management)
  - Risk management for managing SOC, increasing cyber risk preparedness plans for NIS etc.
  - Information sharing and analytics for CERTs and ISACs (includes possibly trusted SIEM, cyber intelligence)
  - Secure Networks and ICT (Secure and trusted Routers, Secure and Trusted Network IDS, Secure Integration, Open source OS).

More info at: www.ecs-org.eu



For any contact: luigi.rebuffi@ecs-org.eu

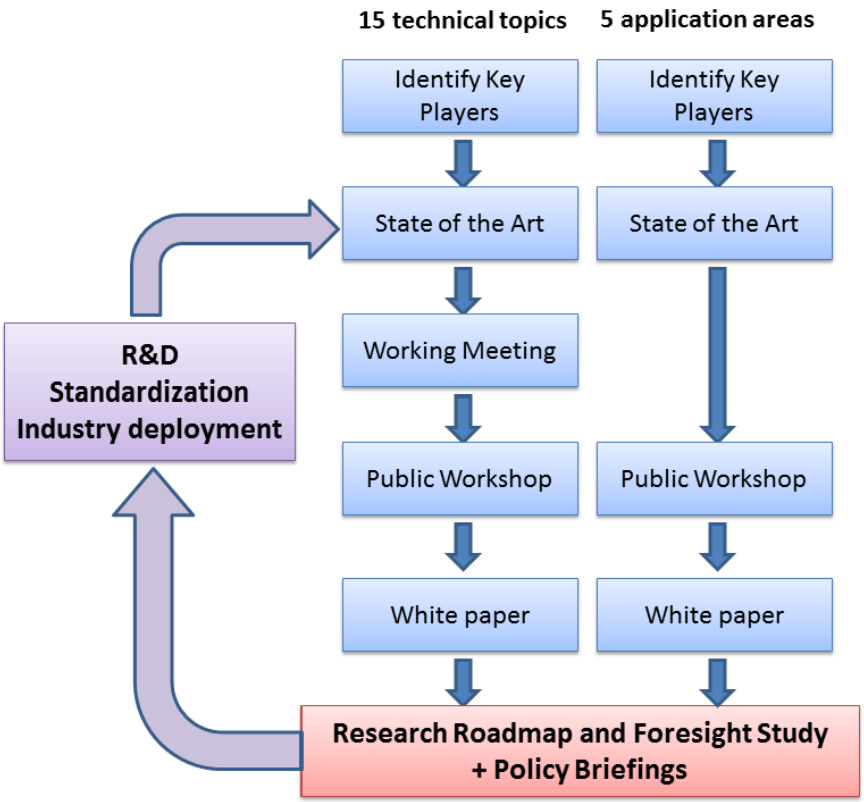
Current activities in cryptology and the DS-06-2017 call

Dr. Florent Frederix
Trust and Security Unit
DG Communications Networks, Content and Technology
European Commission

Content

- Current activities
  - **H2020 LEIT Encryption Projects**
  - **H2020 SC7 Research Executive Agency projects**
- Next H2020 Encryption call
  - **H2020 SC7 in WP 2017**
  - **DS-07-2017 Cryptography call**

H2020 LEIT: ECRYPT_CSA



Workshops and summer schools on encryption covering

- Authentication
- Low energy and small devices
- Symmetric standards
- Asymmetric cryptanalysis
- Random number generation
- Side channel fault resistance
- Modelling tools and proofs
- Cryptocurrencies
- Quantum cryptography
- PETs

H2020-ICT-645421

European Commission

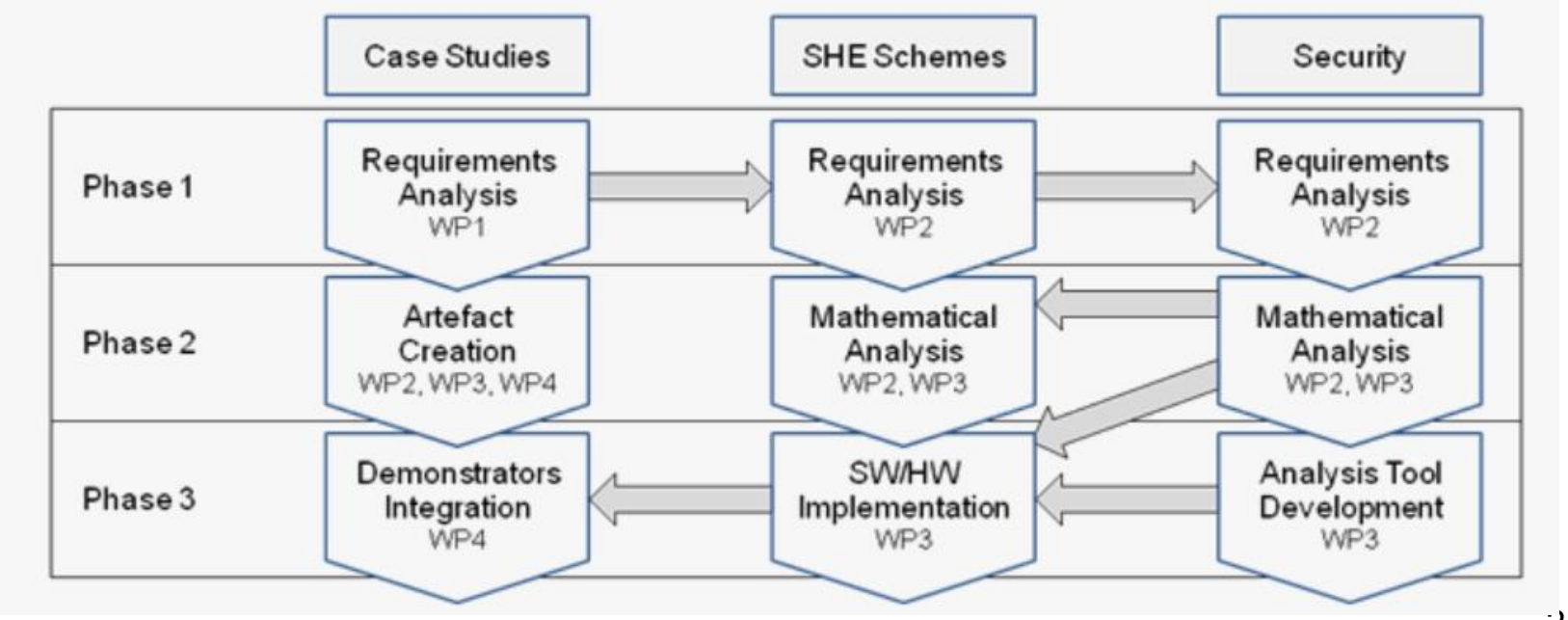
H2020 LEIT: HEAT

HEAT

Homomorphic Encryption Applications and Technology

H2020-ICT-644209

Objective: An **open source software library** to support applications that wish to use **homomorphic cryptography**



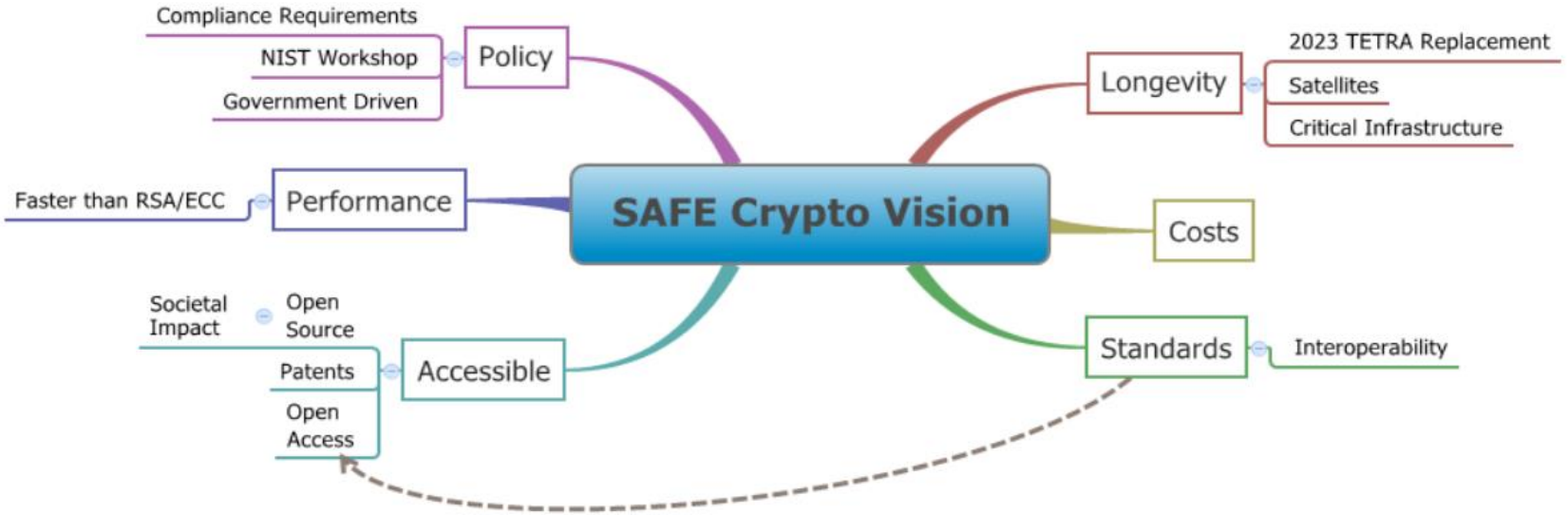
European Commission

H2020 LEIT: SAFEcrypto

Secure Architectures of Future Emerging cryptograpny

H2020-ICT-644729

Objective: a new generation of practical, robust and physically secure **post-quantum cryptographic solutions**



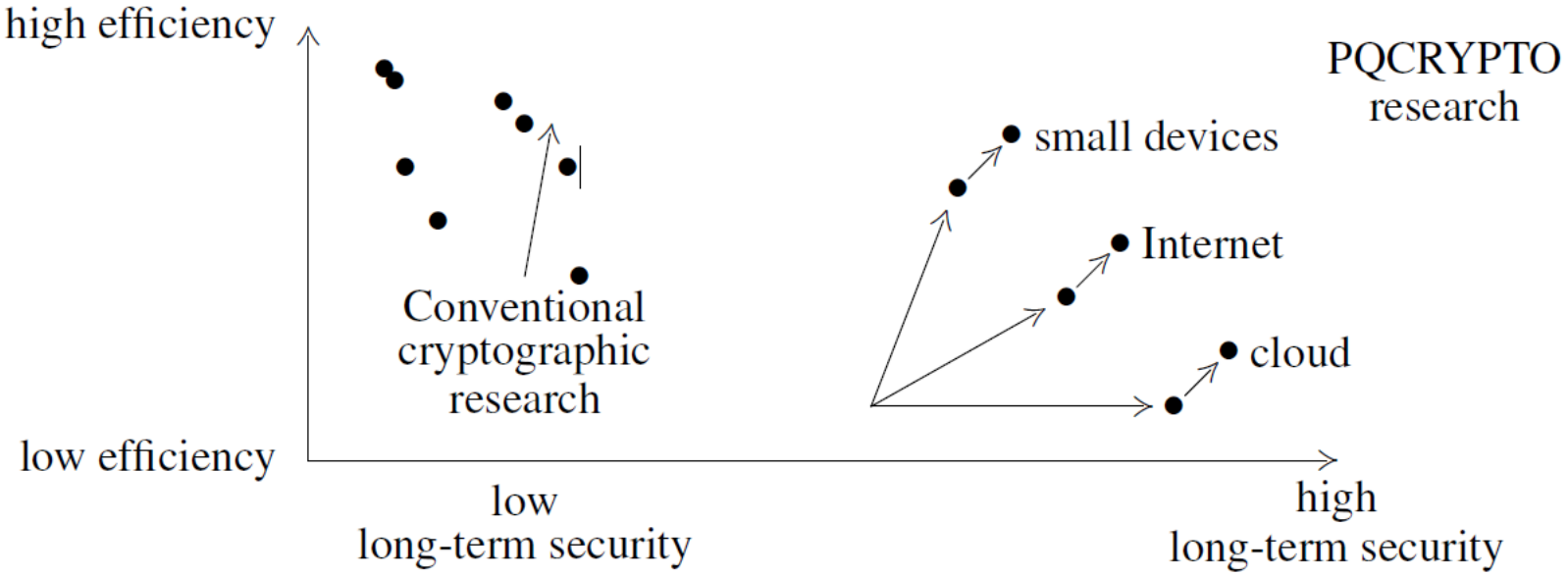
European Commission

H2020 LEIT: PQcrypto

Secure Architectures of Future Emerging cryptography

H2020-ICT-645622

The primary objective of the PQCRYPTO project is **to switch real-world applications to postquantum cryptography**

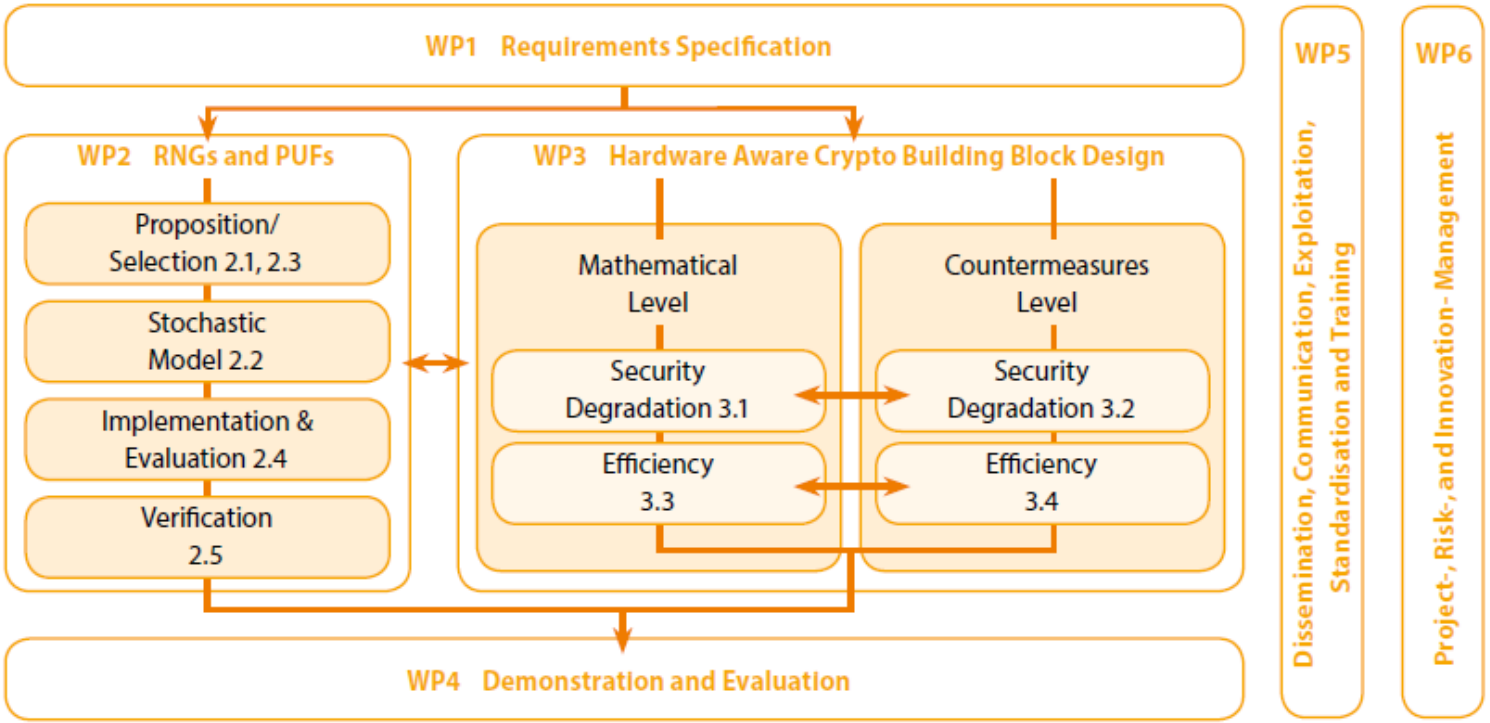


H2020 LEIT: Hector

HARDWARE ENABLED CRYPTO AND RANDOMNESS

H2020-ICT-644052

The mission is to close the gap between the mathematical heaven of cryptographic algorithms and their secure hardware implementations.



H2020 SC7 REA call projects

RIA IA CSA

European Commission

Current Activities

Resilience, Secure Network Infrastructures, Critical Infrastructures, Threat Detection/CyberSecurity

MITIGATE (1)
DOGANA (1)
WISER (1)
RECRED
CREDENTIAL
PROTECTIVE
SISSDEN
CIPSEC
CISP
SHIELD
DISIEM
CANVAS
ATENA
CITADEL (1)

Privacy, Biometrics, Identity management, Authentication

OCTAVE (1)
RECRED (1)
PRIVACY FLAG (1)
TYPES (1)
LIGHTest
FutureTrust
CREDENTIAL (1)
PANORAMIX (1)
Speech XRays (1)
VISION (1)
SAFECLOUD (1)
OPERANDO (1)

Trustworthy Service Infrastructure, Secure Software Engineering, Cryptography

CREDENTIAL https://credential.eu/
LIGHTest (1)
FutureTrust(www.futuretrust.eu)

Certification, Cloud Computing

PRIVACY FLAG
MITIGATE
SAFECLOUD
CITADEL

(1) Shows the main category where the project belongs

2014 — Research Executive Agency — 2015

European Commission

Digital Security Focus Area in H2020 SC7 WP 2016-2017

- **Situation:** ICT-driven transformations bring opportunities across many important sectors.
- **Complication**: "Smart", "Connected", "Digital" also introduce vulnerabilities...
- **R&D&I challenge:** Innovative and multidisciplinary actions addressing cyber security, data protection and privacy across individual H2020 pillars and calls.

European Commission

Call – Digital Security Focus Area – Topics

- **DS-01-2016**: Assurance and Certification for Trustworthy and Secure ICT systems, services and components;
- **DS-02-2016**: Cyber Security for SMEs, local public administration and Individuals;
- **DS-03-2016**: Increasing digital security of health related data on a systemic level;
- **DS-04-2016**: Economics of Cybersecurity;
- **DS-05-2016**: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation;
- **DS-06-2017**: Cryptography;
- **DS-07-2017**: Addressing Advanced Cyber Security Threats and Threat Actors;
- **DS-08-2017**: Privacy, Data Protection, Digital Identities;

European Commission

DS-06-2017: Cryptography (1)

- Research beyond the partial homomorphic encryption algorithms under development. Additionally, means to reduce data leakage
- IoT ultra-lightweight cryptology and means to protect privacy in these applications
- Ultra-high-speed cryptographic algorithms that are fully parallelizable and energy efficient
- Physical cryptanalysis, including tampering, side channel- and faults injection attacks
- Automated proof techniques for cryptographic protocols

DS-06-2017: Cryptography (2)

- Toolkits that seamless integrate encryption
- Authenticated encrypted token research. The proposals should aim to create a real e-currency without compromising security.
- Innovative cryptographic and complementary non-cryptographic privacy-preserving mechanisms.
- Quantum computer safe cryptography
- Improved quantum key distribution schemes with validation by end-users in realistic and relevant scenarios

DS-06-2017: Cryptography - Impact

- Proposals should lead to Technology Readiness Level 3 to 5 prototyping
- Increase the competitiveness of the European ICT, cryptography and smart card industry.
- Increased trust in ICT and online services.
- Protect European Rights of Privacy and Data Protection.
- Improvement in performance and efficiency of cryptography beyond state of the art.
- Protection against emerging threats such as quantum computation

References

Draft work programmes 2016-17

http://europa.eu/!Dh67Gk

CNECT-H4@ec.europa.eu
@EU_TrustSec