



H2020 "Secure Societies" Work Programme

Digital Security 2015

Rafael Tesoro

Trust and Security Unit H.4

DG Communications Networks, Content and Technology

European Commission

Rafael.TESORO-CARRETERO@ec.europa.eu

Agenda

- The role of research to innovation (RTI) in the EU cybersecurity strategy.
- Past developments in cybersecurity RTI co-funded by the EU.
- Calls for proposals within H2020 in Digital Security
- What next?

- The role of research to innovation (RTI) in the EU cybersecurity strategy.
- Recent developments in RTI on cybersecurity.
- Calls for proposals under H2020.
- What next?

Cybersecurity Trends



- Cyber security still a young and immature field***
- Attackers more innovative than defenders***
- Defenders need to share information and cooperate***



⇒ Digital Security is a focus area for Horizon 2020

⇒ Cyber security will never be “solved” but will be “managed”

⇒ User centric perspective of cybersecurity

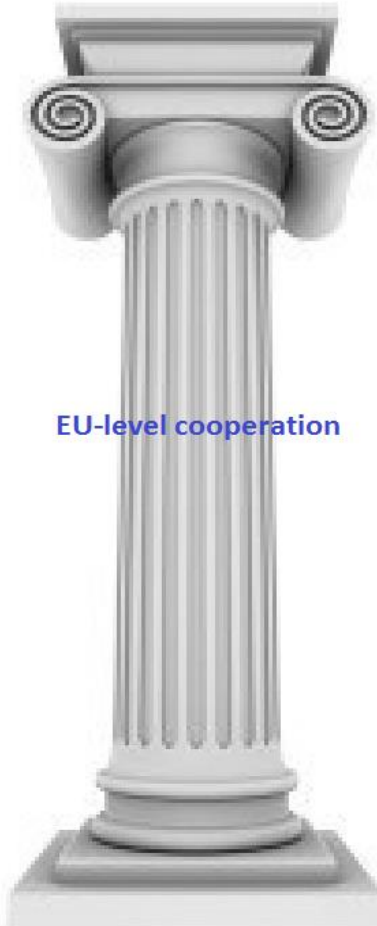


European
Commission

Proposal for a directive on Network and Information Security (NIS)



Common requirements
across the Member States



EU-level cooperation



Risk management
and reporting
across sectors

EU Cybersecurity Strategy

Promoting a single market for cybersecurity products

Developing industrial and technological resources for cybersecurity



Foster R&D investments

- **Use H2020 to address ICT privacy and security**
- **Better coordination of research agendas**
- **Member States invited to develop good practices to leverage public procurement**



- The role of research to innovation (RTI) in the EU cybersecurity strategy.
- Past developments in cybersecurity RTI co-funded by the EU.
- Calls for proposals under H2020.
- What next?

The big picture – Calls in FP7 & CIP (I)

- **FP7-ICT-2007-1 (90M€) :**
 - Identity management and privacy enhancing tools
 - Security and resilience in network infrastructures
 - Security and trust in dynamic and reconfigurable service architectures
 - Trusted computing infrastructures
- **FP7-ICT-SEC-2007-1 (20 M€) - Critical Infrastructure Protection**
- **CIP-ICT-PSP-2008-2 (2,5 M€) - Biometrics + Identity Management**
- **FP7-ICT-2009-5 (90M€)**
 - Technology & Tools, Mobile Devices and Smartphones
 - Trustworthy Network Infrastructures, Cloud Security
 - Trustworthy Service infrastructures, Privacy Management
- **FP7-ICT-2011-8 (80 M€)**
 - Data policy, governance and socio-economic ecosystems
 - Heterogeneous networked, service and computing environments
 - Trust, e-identity and privacy management infrastructure



The big picture – Calls in FP7 & CIP (II)

- **CIP-ICT-PSP-2012-6** – Fighting Botnets (7,8 M€)
- **FP7-ICT-2013-10 (35,8 M€)**
 - Security and privacy in cloud computing
 - Security and privacy in mobile services
 - Development, demonstration and innovation in cyber security
- **CIP-ICT-PSP-2013-7** – Website Security and Biometrics (4 M€)
- **Joint Calls** with Brazil (2011), Japan (2013) and Australia (2013) – (5,5 M€)



In total:



101 R&D Projects for 334 M€ EU funding

Some statistical data...

(excluding FP7-ICT-SEC-2007-1 and FP7-ICT-2007-1)



Top recipients countries (above 1M€)

1. Germany – 49.4 M€
2. France – 28.9 M€
3. Italy – 22.2 M€
4. United Kingdom – 18.2 M€
5. Spain – 18.1 M€
6. Austria – 12.4 M€
7. Netherlands – 12.0 M€
8. Switzerland – 11.8 M€
9. Norway – 9.9 M€
10. Belgium – 9.5 M€
11. Greece – 7.7 M€
12. Denmark – 5.6 M€
13. Sweden - 4.5 M€
14. Portugal – 3.5 M€
15. Estonia – 3.2 M€
16. Israel – 3.1 M€
17. Ireland – 3.0 M€
18. Hungary – 1.7 M€
19. Finland – 1.6 M€

Total: 232 M€



The top private sector recipients:

1. SAP (Germany/France) – 9.8 M€
2. IBM (Israel/Switzerland) – 7.3 M€
3. ATOS (Spain) – 4.6 M€
4. Infineon (Germany/Austria) – 3.5
5. Technicon (Austria) – 3.2 M€
6. HP (UK/Italy) – 2.7 M€
7. THALES (France) – 1.9 M€
8. Bicore (Netherlands) - 1.5 M€
9. Microsoft (France) – 1.5 M€
10. Siemens (Germany) – 1.4 M€
11. Gemalto (France) – 1.4 M€
12. NEC (UK) – 1.3 M€
13. Cybernetica (Estonia) – 1.2 M€
14. Cloud Security Alliance (CSA) - 1.1 M€



Ca. 19% of total EC funding (232 M€)

The top academic/public recipients:

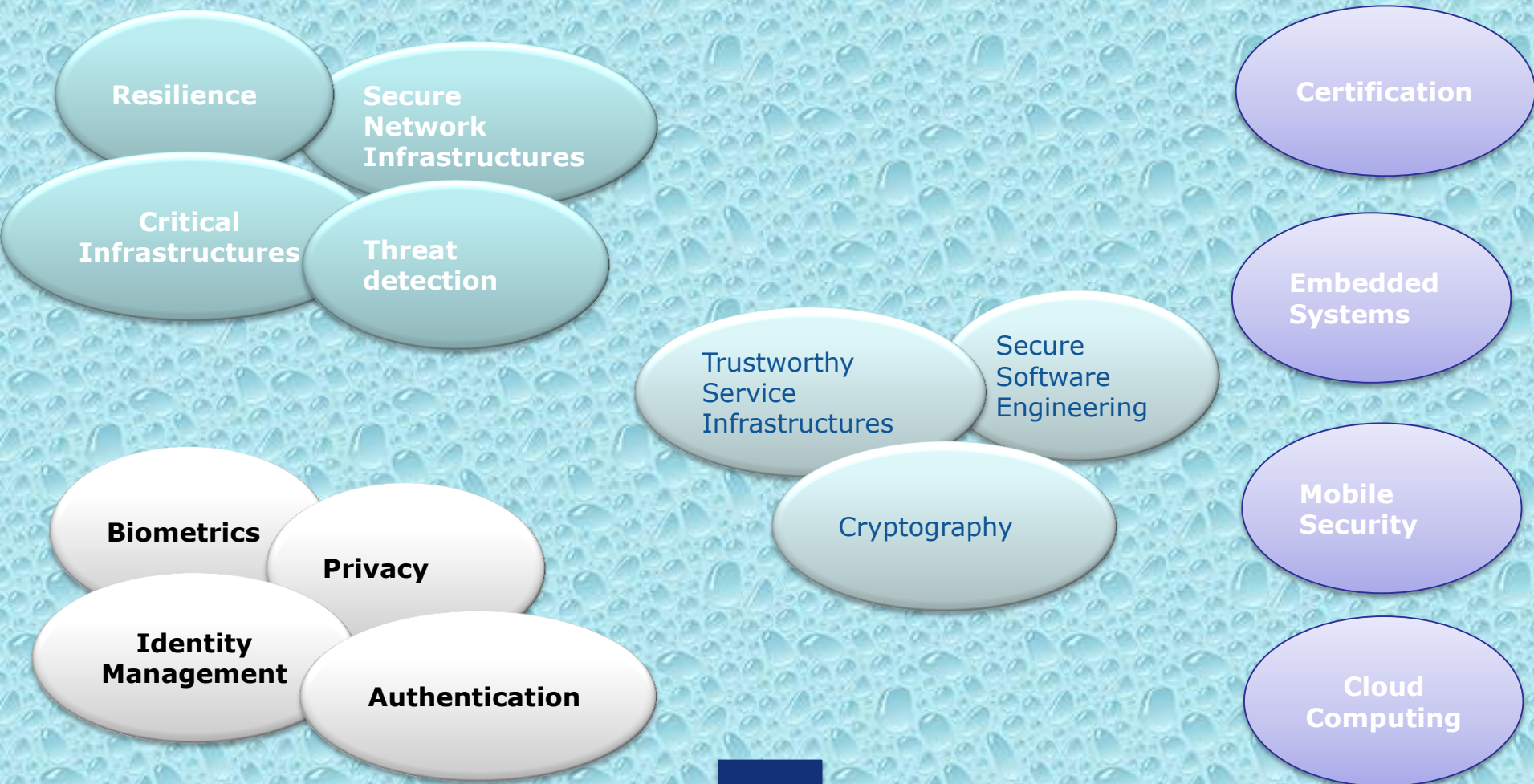
1. SINTEF (Norway) – 6.0 M€
2. Fraunhofer (Germany) – 5.9 M€
3. KU LEUVEN (Belgium) – 3.4 M€
4. TU Darmstadt (Germany) – 2.8 M€
5. TU Graz (Austria) – 2.3 M€
6. Frankfurt University (Germany) – 2.2 M€
7. Unabh. Landeszentr. für Datenschutz (Germany) – 1.9 M€
8. CNR (Italy) - 1.8 M€
9. University Malaga (Spain) – 1.8 M€
10. Poli. Torino (Italy) – 1.7 M€
11. Eurecom (France) – 1.5 M€
12. Danmarks TU (Denmark) - 1.3 M€
13. TU Eindhoven (Netherlands) – 1.2 M€
14. University Lisbon (Portugal) – 1.2 M€

Ca 18% of total EC funding (232 M€)



Structuring the Portfolio

(one way of doing it)



Critical Infrastructure Protection

(security for networked infrastructures)

- **Efficiency gains**
- **Being "smart"**
(grid, city, transport)
- **Legacy systems**
- **Complexity increases vulnerabilities**
- **Increased target surface**



Critical Infrastructure Protection

(enabling secure solutions for CIP using ICT)

Identification of emerging threats: FORWARD – SysSec

ICT to increase resilience of CIP: Tclouds, OPTET, Euro-MILS

Support networked-linked CIP: MICIE, SERSCIS

Identifying attacks: Trespass

Follow-up: DS-3-2015



SMEs

Percentage of overall funding: ca. 10-12 %

Percentage of participating entities: below 20%

Examples of success:



3 projects since 2012, 1.2 M€ funding



***CIP Project securing websites: 5 SMEs out
11 partners, 41% of budget***



***FP7 IP Project: 5 SMEs out 15 partners,
41% of budget***

But still need to address obstacles for SMEs in H2020

What remains to be done – challenges for H2020

**From world-class research to market
innovation**

Europe competing globally

Industrial Policy

User trust in ICT

Linking the threads



- The role of research to innovation (RTI) in the EU cybersecurity strategy.
- Recent developments in RTI on cybersecurity.
- Calls for proposals within H2020 in Digital Security
- What next?

THE EU FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

HORIZON 2020

THE EU FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

HORIZON 2020

**Societal
Challenges**

**Three
Pillars**

THE EU FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

HORIZON 2020

**Industrial
Leadership**

THE EU FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

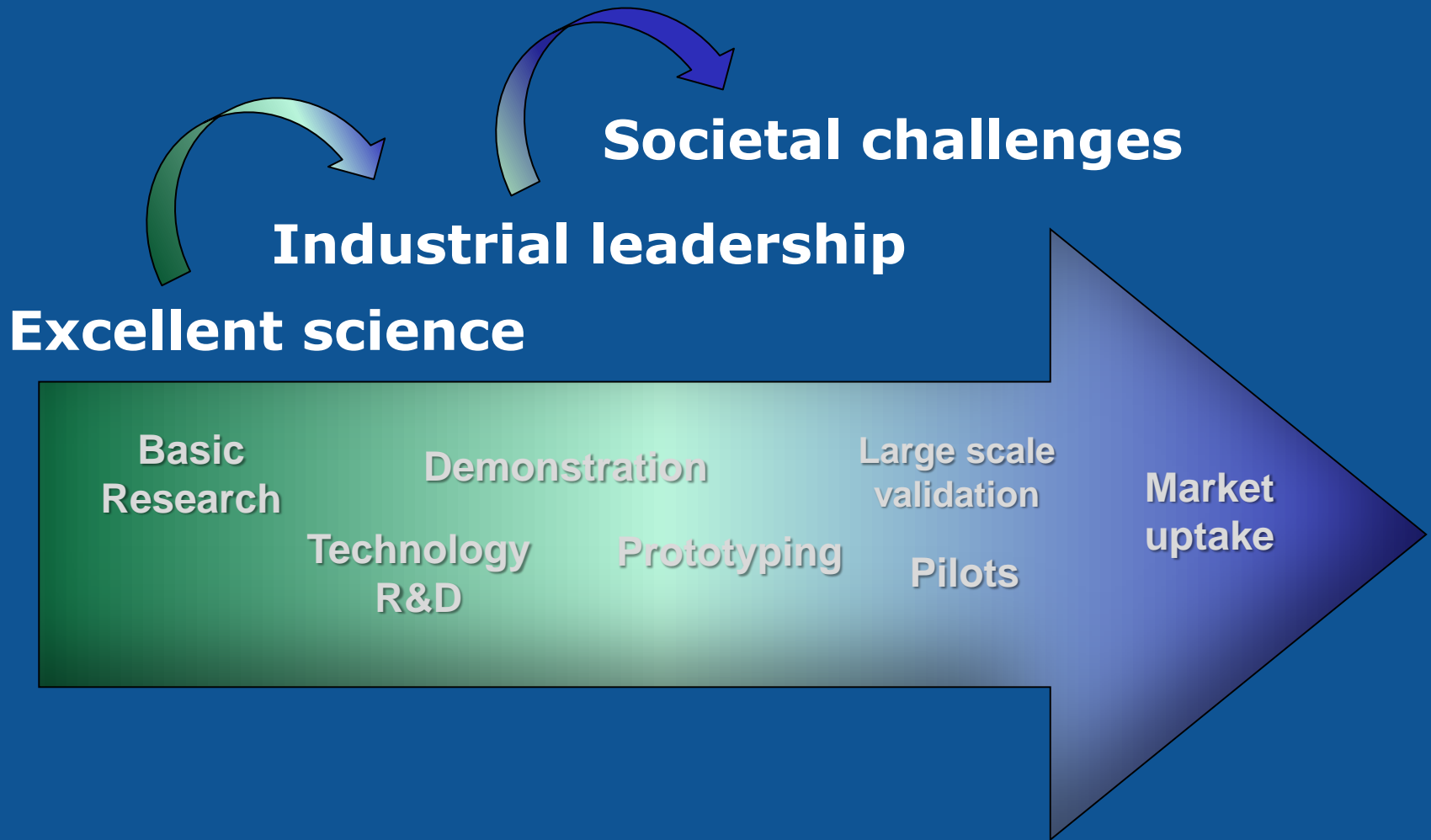
HORIZON 2020

EXCELLENCE

Excellent Science

**€70
bn**

Coverage of the full innovation chain



Policy Driven

*Finance,
Banking,
Payment*

Smart Cities

*Connected
Cars*

*Smart
Grids*

*Intelligent
Transport
Systems*

*eHealth
mHealth*

**Securing
Present &
Future
Critical
Market
Functions**

3. Mainstreaming Cybersecurity

Technology Driven

IoT

Big
Data

Cloud

5G

Embedded
Systems

Computing

**Securing Data
Processing,
Storage and
Transmission**

THE EU FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

HORIZON 2020



ICT in the Societal Challenges



Key principles for ICT R&I in the Societal Challenges

- Interoperability and security-by-design
- Re-use and economies of scale
- Breakthroughs leveraging the transformative power of ICT
- Preparation for market deployment

+ Information for future digital policies

H2020 SC7 Secure societies - Four key concepts

- Secure societies – Protecting freedom and security of Europe and its citizens.
- Address the economic and societal dimension of security and privacy in the digital ecosystem.
- Secure and increase trust in the digital society.
- Demonstrate the viability and maturity of state-of-the-art solutions.

Calls in 2014/15

LEIT (40 M€) Technology Building blocks in Security - 2014:

- Cryptography
- Security-by-Design

Societal Challenge 7: Digital Security (97M€):

2014:

- Privacy
- Access Control
- Risk management and assurance models

2015:

- The role of ICT in Critical Infrastructure Protection
- Information driven Cyber Security Management
- Trust eServices
- Value-sensitive technological innovation in Cybersecurity

Four Topics in 2015

- DS-03-2015: The role of ICT in Critical Infrastructure Protection (IA)
- DS-04-2015: Information driven Cyber Security Management (IA)
- DS-05-2015: Trust eServices (IA)
- DS-07-2015: Value-sensitive technological innovation in Cybersecurity (CSA)

Other Topics in SC7

- **DRS: Disaster-resilience**
 - Crisis Management
 - Disaster Resilience & Climate Change
 - Critical Infrastructure Protection
 - Communication technologies and interoperability
- **FCT: Fight against Crime and Terrorism**
 - Forensics
 - Urban Security
 - Ethical / Societal Dimension
- **BES: Border Security and External Security**
 - Supply Chain Security
 - External Security
 - Border Security



The role of ICT in Critical Infrastructure Protection

DS-3-2015

The role of ICT in Critical Infrastructure Protection

- **Challenge:**

- Despite strong connection between ICT systems and Operational Technology (OT) environment running critical infrastructures, there is only little awareness regarding IT risks that can affect OT control systems.
- ICT systems are deployed in an environment or for an application that was not designed with security in mind.
- [...]

- **Scope:**

- Investigate dependencies [...], monitor cascading effects of incidents, [...] develop self-healing mechanisms.
- Plans of how to retrofit state-of-the-art security into networks can also be addressed.
- The investigated concepts have to be tested in a field trial.

The role of ICT in Critical Infrastructure Protection

- **Scope (cont.):**
 - ICT should be protected or re-designed at the software level, but also at the physical level [...]
 - ICT operators experience [...] can be applied to [...] smart grids
 - In relation to the protection of legacy IACS, SMEs are particularly encouraged to provide specific and very focused security solutions adapting current ICT security technology to IACS environments on topics such as [...]:
 - [...]
- **Impact:**
 - Resilient networks [...], increased preparedness, reduced response time and coordinated response in case of a cyber-incident.
 - Reduced possibilities to misuse ICT as a vehicle to commit cybercrime or cyber-terrorism.
 - [...]

Budget and schedule

- Call identifier: H2020-DS-2015-1
- Topic: DS-3-2015
- Instrument: Innovation Action (TRL 7)
- Indicative budget: 17,50 million EURO
- Indicative project size: 3-8 million EURO
- Opening date: 25/03/2015
- Deadline: 27 August 2015, 17.00.00 CET



Information driven Cyber Security Management

DS-4-2015

Information driven Cyber Security Management

- **Challenge:**

- Effective defence against [...] threats requires the addition of a balancing, outward focused approach, on understanding the adversary's behaviour, capability, and intent.
- Those [...] responsible for managing cyber security programmes are often faced with an overwhelming amount of information, often raw and unstructured [...]
- SMEs face a particular challenge [...] they often do not have the capacity [...] or the [...] expertise [...] in order to address the cyber security threats they face.
- [...]

- **Scope:**

- [...] tools and techniques that enable organisations to efficiently process the flow of information from both internal and external sources, through improved information processing, analysis and, where necessary, exchange.

Information driven Cyber Security Management

- **Scope (cont.):**
 - [...] should leverage the state-of-the-art in areas such as SIEM, data analytics (including Big Data) and visualisation, threat intelligence, malware analysis and cyber security information exchange.
 - [...] promote interoperability through [...] open standards
 - Several pilots [...] for different application areas [...]
 - Proposals are encouraged to include security end-users.
 - [...] address the needs of those entities whose mission it is to assist others such as [...] Cyber Security Centres or similar.
 - [...]
- **Impact:**
 - [...] effective vulnerability remediation, enhanced prevention and detection capabilities and faster response to incidents.
 - [...] increase the level of awareness and preparedness.

Budget and schedule

- Call identifier: H2020-DS-2015-1
- Topic: DS-5-2015
- Instrument: Innovation Action (TRL 6+)
- Indicative budget: 14,31 million EURO
- Indicative project size: 3-5 million EURO
- Opening date: 25/03/2015
- Deadline: 27 August 2015, 17.00.00 CET



Trust eServices

DS-5-2015

Trust eServices

- **Challenge:**

- The [...] adoption of [...] eServices is hampered by the lack of globally interoperable solutions, mutually recognized or compatible trust models and the absence of solid business cases for the reliance on electronic signatures, e-seals, timestamps or certified electronic delivery.
- [...] assessing the security assurance and trustworthiness of [...] eServices, in particularly when coming from third countries

- **Scope:**

- Comparison and interoperability of electronic trust services covering aspects such as security assurance levels, operational security audits, state supervision systems, data protection regimes or liability of trust service providers.
- [...] assessment of technical and organisational standards for trust services, [...] development of a framework for 'global trust lists'.

Trust eServices

- **Scope (cont.):**
 - Validation platforms able to handle the specificities of various jurisdictional or national systems could be created [...]
 - Proposals are encouraged to include security end-users.
 - [...]
- **Impact:**
 - Demonstrate a positive business case and the economic value for the use of and reliance upon trust eServices.
 - [...] empower and protect users in their digital experiences like e-contracting, e-bidding, e-invoicing, accessing social networks, or accessing the services of local or national administrations.
 - [...] ease the dematerialisation of processes, reduce administrative overhead for citizens and businesses and [...] facilitate higher availability of eGov services.

Budget and schedule

- Call identifier: H2020-DS-2015-1
- Topic: DS-5-2015
- Instrument: Innovation Action (TRL 7)
- Indicative budget: 17,40 million EURO
- Indicative project size: 3-8 million EURO
- Opening date: 25/03/2015
- Deadline: 27 August 2015, 17.00.00 CET



Value-sensitive technological innovation in Cybersecurity

DS-7-2014

Value-sensitive technological innovation in Cybersecurity

- **Challenge:**

- [...] to ensure a flourishing information society which offers safety and security and at the same time respects Europe's fundamental values and rights.
- cybersecurity technologies [...] incorporate European values and fundamental rights, [...] autonomy, equality, privacy, [...] fairness and accountability and ensure the 'right' level of control individuals can exercise over their actions [...].
- The role of public and private sectors [...] to allow citizens to make informed and responsible choices regarding innovative products and services leading to a strong European market for [...] effective cybersecurity technology.

- **Scope:**

- facilitate community building and [...] understanding involving relevant stakeholders from civil society, research, industry and public bodies

Value-sensitive technological innovation in Cybersecurity

- **Scope (cont.):**

- Drafting standards and guidelines for industry and the public sector to enable consumers to exert a high level of control over devices and services [...]
- Identifying the key factors for promoting a secure and innovative ecosystem [...] in line with European values
- [...]

- **Impact:**

- [...] insight into how networked ICT, autonomous system [...] devices [...] services influence the perception of citizens with respect to security and [...] values [e.g.] freedom and autonomy
- New approaches for users to exercise control over their data and maintain the desired autonomy of their actions in the digital domain [...]
- [...]

Budget and schedule

- Call identifier: H2020-DS-2015-1
- Topic: DS-7-2015
- Instrument: Coordination & Support Action
- Indicative budget: 1 million EURO
- Opening date: 25/03/2015
- Deadline: 27 August 2015, 17.00.00 CET

- The role of research to innovation (RTI) in the EU cybersecurity strategy.
- Recent developments in RTI on cybersecurity.
- Calls for proposals under H2020.
- What next?

Cybersecurity & Privacy Innovation Forum 2015

- 28-29th April 2015
- Venue: MCE, Brussels
- This event will include DG CNECT informational sessions relating to 'Digital Security: Cybersecurity, Privacy & Trust' calls in 2015
 - **DS-03-2015, DS-04-2015, DS-05-2015, DS-07-2015.**
 - <https://www.cspforum.eu/2015>

H2020 SC7 Digital Security 2015 calls:

<http://europa.eu/!fY78Nu>

Network of National Contact Points (NCPs)

<http://europa.eu/!up97Wv>

Digital Agenda for Europe - Cybersecurity

<http://ec.europa.eu/digital-agenda/en/cybersecurity>

Follow us on Twitter

https://twitter.com/EU_TrustSec