Trust Security

European Commission
Communications Networks, Content and Technology

The newsletter about Trust & Security in the Information Society

JULY 2012

- ✓ INFSO changes to CONNECT
- ✓ Work Programme 2013 and ICT Call 10
- ✓ Horizon 2020
- ✓ European strategy for Cyber security

EVENT'S CORNER

ICT Proposers' Day 2012
26-27 September 2012
Warsaw, Poland
(http://ec.europa.eu/information_society/events/ictproposersday/2012/index_en.htm)

Trust & Security Infoday 2012
9 October 2012
DG CONNECT, Brussels

- Information about the new Call 10
- opportunity to meet new POs
- discussion
- networking

Annual Privacy Forum 2012
10-11 October 2012
Limassol, Cyprus
(http://privacyforum.eu/)
(invitation in this issue)

~~INFSO~~ changes to CONNECT

As of the 1st July 2012 we will all be working in a new DG called **DG CONNECT** (*Communications Networks, Content and Technology*). The new name better represents the range of topics where our DG is active, and our new structure better aligns the work of the DG with key EU policies for the coming decade: ensuring that digital technologies can help deliver the growth which the EU needs.
The DG helps to harness information & communications technologies in order to create jobs and generate economic growth; to provide better goods and services for all; and to build on the greater empowerment which digital technologies can bring in order to create a better world, now and for future generations.

To help achieve this, DG CONNECT:

1. Supports the kind of high-quality research & innovation which delivers imaginative, practical and value-enhancing results;
2. Fosters creativity through a European data value-chain in which anyone can share knowledge;
3. Promotes greater use of, and public access to, digital goods and digital services, including "cloud" computing, in order to boost the European single market;
4. Ensures that those goods and services are more secure, that people can trust the rapidly evolving technologies which surround them, and that people have the right skills and confidence to use them as part of everyday life;
5. Works with partners globally to support an open Internet.

INFSO Trust & Security changes to CONNECT Trust & Security

This change affects also DG INFSO Unit **Trust & Security**. The unit leaves the former INFSO Directorate F "Emerging Technologies and Infrastructures" and becomes a part of CONNECT Directorate H **"Sustainable and Secure Society"**. Directorate's main goals are to address selected ICT challenges for a sustainable,

Continue to next page >>

Goodbye message from Jesús Villasante (former Head of INFSO T&S)

Dear Friends,

Following the European Commission reorganisation of the Directorate-General Information Society and Media to the new DG CONNECT, I started work in the Net Innovation Unit on 1st July. My colleague, Giuseppe Abbamonte will take over the actions on Trust and Security.

It has been a pleasure to work with you over the last two years in the area of Trust and Security. My interactions with researchers, academics, industrialists and policy-makers from all areas of the Privacy and Cyber security community who are so passionate about the subject have been very rewarding.

With so many social and human implications, we are all aware of the importance of Trust and Security in the future. Our projects have been well perceived and there is high interest and expectation for the Commission activities in this field to provide a strong technological and research base in Europe, develop industrial competencies and support the creation of policy.

Stakeholders from outside our community have commented positively on your project achievements and contributions. I encourage you to continue your work with the same enthusiasm.

I wish you success and will be pleased to meet you again in my new function.

Jesús Villasante

~~INFSO~~ changes to CONNECT

healthy and secure society, and to develop a full-cycle roadmap to get the output into the EU economy, through innovation tools such as pilot-lines, pre-commercial procurement, and standards. Directorate H is the leader for Horizon 2020/Societal Challenges.

Trust & Security priorities:

- Elaborate a European strategy on Internet security and remove Cyber security related obstacles to the proper functioning of the Internal Market.
- We will manage implementation of the e-privacy Directive and follow-up of all issues related to the protection of privacy on-line.
- Manage the various financial programmes (FP7, CIP, H2020) supporting the Internet and ICT security.
- Promote a better coordinated and coherent approach on cyber incident management worldwide.

To find out more information about the transition follow http://ec.europa.eu/dgs/information_society/connect_en.htm

Message from Giuseppe ABBAMONTE
Head of CONNECT Trust & Security

The concern for security is as old as humankind. What is "new" is its extension to our digital environment. Indeed, our economy and society are now highly dependent on Information and Communication Technology (ICT). We have grown accustomed to the benefits brought by the Internet, smartphones, and the visible and invisible computing power around us. ICT services and devices have become an integral part of our way of life, and even of our culture.

The Digital Agenda for Europe (DAE) recognises that the Internet has proved to be remarkably secure, resilient and stable. However, the extensive usage of ICT brings not only benefits but also carries risks. IT networks and end users' terminals still remain vulnerable to a wide range of evolving threats. Therefore, the DAE has defined a number of objectives in the field of trust and security, namely security of networks; fight against cybercrime and cyber attacks; trust in technology and safety of children online.

To keep our society secure and provide citizens with trust in ICT services and devices, a twofold approach is needed:

- The definition of *legal frameworks* to protect us from any disruption of, or attack on, our services and devices;
- The investment in research and development of *secure, trustworthy and privacy protecting ICT*, this entails creation of a market for secure and trustworthy ICT products and services and other measures to stimulate the take-up of secure ICT solutions.

ICT PSP Call 6
Fighting botnets

As part of the ICT PSP Competitiveness and Innovation Programme (CIP) Call 6 interested stakeholders were invited to participate with project proposals addressing measures to establish a European-wide pilot platform for detecting, measuring, analysing, mitigating and eliminating botnets. In this way, a European toolbox for fighting botnets but also of other emerging cyber threats should be made accessible to European stakeholders.

The received proposals for a Pilot B were evaluated in June and the retained proposal will now be invited for negotiation. It is expected that the Pilot B on fighting botnets will start by the end of 2012.

Martin Muehleck

ICT Work programme 2013 and ICT Call 10

The emphasis in WP2013 is put on ICT innovations which are driver and support for transforming our society. With regards to our unit, these innovations include **Internet and cloud computing** technologies and **Mobile services** which will radically impact how citizens and businesses use technology and individuals live their lives.
In addition to R&D activities, to boost future productivity and growth, it is critically important to generate breakthrough technologies and to translate them into innovations (new products, processes and services) which are taken up by the wider economy.
On the top of these priorities, WP2013 will serve as a bridge to activities in Horizon 2020.

Work programme 2013:
http://ec.europa.eu/research/participants/portalplus/static/docs/calls/fp7/common/32767-annex_6_to_the_decision_ict_for_cap_en.pdf

Objective ICT-2013.1.5 Trustworthy ICT

- Security and privacy in Cloud computing
- Security and privacy in Mobile services
- Development, demonstration and innovation in Cyber security
- Technologies and methodologies to support European Trust and security policies
- EU-Australia cooperation on building user trust in broadband delivered services

Funding schemes: IP, STREP, CSA
Total budget: 36,5M€
Date of publication: 10 July 2012
Deadline: 15 January 2013

Expected impacts are demonstration of secure and privacy-preserving technical solutions in clouds, mobile services and management of cyber incidents. Activities will cover R&D and innovation activities, including the adaptation and integration of technology and demonstration in real life environments, from the design to the implementation stage. This objective also aims at supporting trust and security policies.

More information can be found on our webpages.

Call coordinator and contact point:

Mr. Rodrigo MENDES (rodrigo.mendes@ec.europa.eu)

Don't miss: ICT Proposers' Day, 26-27 September, Warsaw, Poland
Trustworthy ICT Information Day, 9 October, Brussels

Annual Privacy Forum 2012 (invitation)

When: 10-11 October 2012
Where: Limassol, Cyprus

The European Network and Information Security Agency (ENISA) is organising in collaboration with the Trust and Security Unit of DG CONNECT the Annual Privacy Forum (APF'2012) aiming to establish an annual forum that addresses the links between the advances made by research in the area of privacy and the relevant policy initiatives. This first edition of the APF will take place in Cyprus and is endorsed by the Cyprus Presidency of the Council of the EU.

In June, the call for papers has closed and the Trust and Security research community has submitted a number of scientific papers related research projects funded by the EC in this area. The Forum also invites European stakeholders contributing to EU privacy policies to present and discuss these policies with the research community, in order to strengthen the links between the research in privacy and data protection with European policies in this field.

For more information please consult the AFP website: http://privacyforum.eu/

Horizon 2020 – new Framework Programme

Horizon 2020 is the European Union Framework Programme (FP) for Research and Innovation for the period 2014-2020. It represents the challenge named "Smart & inclusive growth", the overall target for all the challenges is to stabilise the financial and economic system while taking measures to create economic opportunities.

Earlier this year the European Commission had presented its proposal for a Regulation on H2020 and the H2020 Specific Programs. The discussions on both are currently underway in the European Council and the European Parliament. It is expected to have an adoption by the end of this year. In parallel the Trust & Security unit is starting its consultations on the content and scope of the H2020 components it is responsible for, i.e. the research, development and innovation activities addressing, cyber security, privacy and trust in the Societal Challenge on Secure Societies and the ICT Key Enabling Technology of the Leadership in Enabling Industrial Technologies Program. After the summer break the Trust & Security unit will start the public consultations where all interested stakeholders will be invited to contribute to the shaping of the research directions beyond 2014. More details about the consultations will be made available on the unit's website.

The launch of first Calls for Horizon 2020 is scheduled on 1st January 2014. For more information and updates follow also the link to the homepage of Horizon 2020: (http://ec.europa.eu/research/horizon2020/index_en.cfm?pg=home&video=none)

Call for Tender (SMART 2012/0010)

Feasibility study and preparatory activities for the implementation of a **European early warning and response system against cyber-attacks and disruptions.**

Identifier: 2012/S 108-178433
Publication date: 8 June 2012
Deadline: 10 August 2012

The Digital Agenda highlights the need to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks. The pillar on trust and security includes measures to allow faster responses in the event of disruptions or attacks against information systems.

More information can be found on our webpages (see Calls)

European Strategy for Cyber security

Every day, the digital ecosystem boosts productivity, drives innovation and positive societal developments. At the same time, threats are growing and so is the vulnerability of our networks. Therefore, Cyber security is of vital importance for the Commission, the Member States and the EU as a whole. In the coming months, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy will adopt a European Strategy for Cyber security to achieve our core objectives. The legislation will aim at strengthening security at national and EU level, by establishing appropriate mechanisms for cross-border and public-private cooperation and information exchange. We need to make sure that there are no weak links across the EU. From the policy side, the vision will be hinged on improving the overall resilience of networks and information systems, stepping up the fight against cybercrime, and developing an external EU Cyber security policy. The Member States should acknowledge the importance of Cyber security at the highest political level and treat it as a priority, just like some of our main partners have done already.

Main elements of the Strategy:
DG CONNECT will ensure full continuity with the policy it has undertaken in the past years and make a step forward including on EU level initiatives on Fighting botnets, Cyber security of Industrial control systems and Smart grids, security standards as well as on R&D, awareness raising and international cooperation. The Strategy will include actions to stimulate the competitiveness of the European ICT industry and stimulate user demand to provide security functionalities in ICT products and services. Horizon 2020 will support the goals of the Strategy.

Regarding the proposal for Regulation, its main focus will be on ensuring a high level of security across the EU. This will entail:

- Ensuring a **high level of security at national level**, in terms of preparedness and capabilities. Each Member State will be required to, among the other things, nominate an agency/competent body responsible for Cyber security and ensure it has the necessary capabilities.
- Ensuring **cooperation at EU level**, via a Network composed by national competent authorities that will exchange key information relevant to security (on threats and risks as well as on incidents)
- Ensuring that private operators/providers falling under specific categories (in particular Information Society Services providers) **adopt risk management practises** according to the state of the art and report major incidents to the national competent authorities.

The European Strategy for Cyber security will help Europe make its own house in order. Making Europe the most secure place in the world for ICT is a key element to our future competitiveness that will strongly contribute to better place the EU also at the international level. As we still need to do more, a European Strategy for Cyber security will be presented later this year. In September, a proposal for a Regulation on a common high level of security across the Union will be adopted.

Report from Security and Privacy Forum 2012
(24-25 April, Berlin)

The main objective of the event was to work to actively promote the outputs and potential innovation coming from research projects active in the Cyber Security and Privacy domain. By having such an event it provides an opportunity for like-minded experts in the domain to come together to network, collaborate, learn from each others' experiences, and discuss current and future gaps and challenges, working to ensure that this domain remains a top research priority.

The mixture of the type of session between Day 1 (plenary sessions, tutorials, demos) and Day 2 (project specific and cluster specific workshops), was deemed a successful approach to take when detailing and planning the programme for such an event. The attendees found the layout and choice of parallel sessions appropriate to their needs and interests.

The subjects addressed by the speakers referred to: the key issues for security and trust in the context of current trends like cloud, mobile, and "digital natives", the challenges related to ensuring privacy (including in the context of the new European data protection regulation), privacy by design, the challenges for ICT security research and innovation (e.g. the influence of policy, regulation, educational systems, the lack of communication across communities, the need to foster synergies between industry and academic research).

ICT Call 8 – Stats and facts

Objective ICT 2011.1.4 "Trustworthy ICT" with the following target outcomes:

a) Heterogenous networked, service and computing environments
b) Trust, eIdentity and Privacy management infrastructures
c) Data policy, governance and socio-economic systems
d) Networking and coordination activities

Funding schemes: IP, STREP, CSA. NoE

Total budget allocated: 80 M€

A total of 110 proposals were received for this objective, requesting a total grant of 424 M€. They were evaluated in three panels (IP, STREP, CSA+NoE)

Funding scheme	Proposals received	Grant requested (M€)	No. above threshold	Retained	Req. grant received proposals (M€)
IP	19	169	9	5	43,2
STREP	81	240	39	9	29,3
CSA	9	11	6	6	7,5
NoE	1	4	0	0	0
Total:	**110**	**424**	**54**	**20**	**80**

At the end of the day 20 most successful projects, covering all the objectives, were promoted to the phase of negotiations which takes place these days. The estimated start of the projects is by the end of year 2012.

Trust & Security – Project Officers

Although the change from INFSO to CONNECT brought also many personnel changes to unit Trust & Security, there is no need to make worries about the projects that are either active or in the phase of negotiations. Trust & Security wants to ensure all partners that transfer of the agenda to new Project Officers will be smooth and will not have negative consequences for the projects.

This is the new team of Trust & Security Project Officers:

- Valerie ANDRIANAVALY (valerie.andrianavaly@ec.europa.eu)
- Olivier BRINGER (olivier.bringer@ec.europa.eu)
- Florent FREDERIX (florent.frederix@ec.europa.eu)
- Rodrigo MENDES (rodrigo.mendes@ec.europa.eu)
- Martin MUEHLECK (martin.muehleck@ec.europa.eu)
- Aristotelis TZAFALIAS (aristotelis.tzafalias@ec.europa.eu)
- Ainhoa URIARTE URRUTIA (ainhoa.uriarte-urrutia@ec.europa.eu)