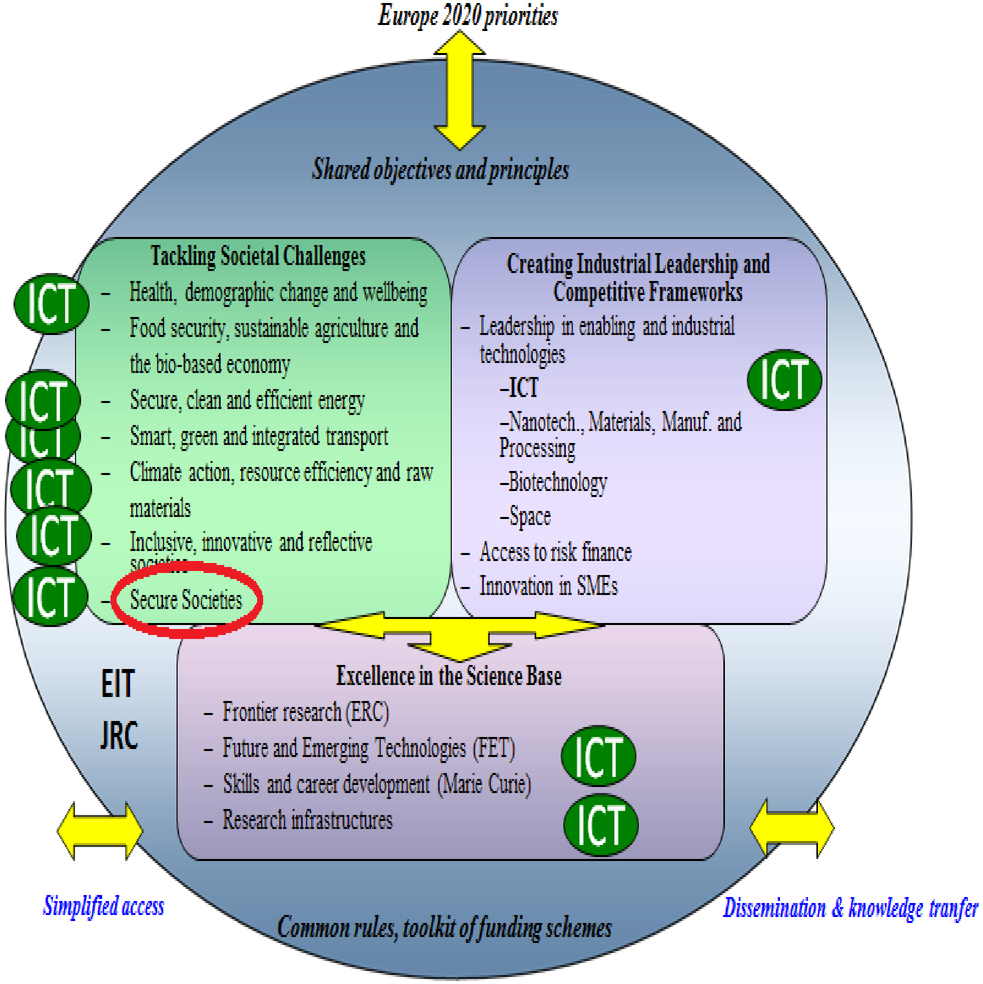
SC7: Secure Societies – Protecting Freedom and Security of Europe and Its Citizens

SSH and RRI contents

Aristotelis Tzafalias

European Commission



Europe 2020 priorities

Shared objectives and principles

Tackling Societal Challenges
- Health, demographic change and wellbeing
- Food security, sustainable agriculture and the bio-based economy
- Secure, clean and efficient energy
- Smart, green and integrated transport
- Climate action, resource efficiency and raw materials
- Inclusive, innovative and reflective societies
- Secure Societies

Creating Industrial Leadership and Competitive Frameworks
- Leadership in enabling and industrial technologies
  - –ICT
  - –Nanotech., Materials, Manuf. and Processing
  - –Biotechnology
  - –Space
- Access to risk finance
- Innovation in SMEs

Excellence in the Science Base
- Frontier research (ERC)
- Future and Emerging Technologies (FET)
- Skills and career development (Marie Curie)
- Research infrastructures

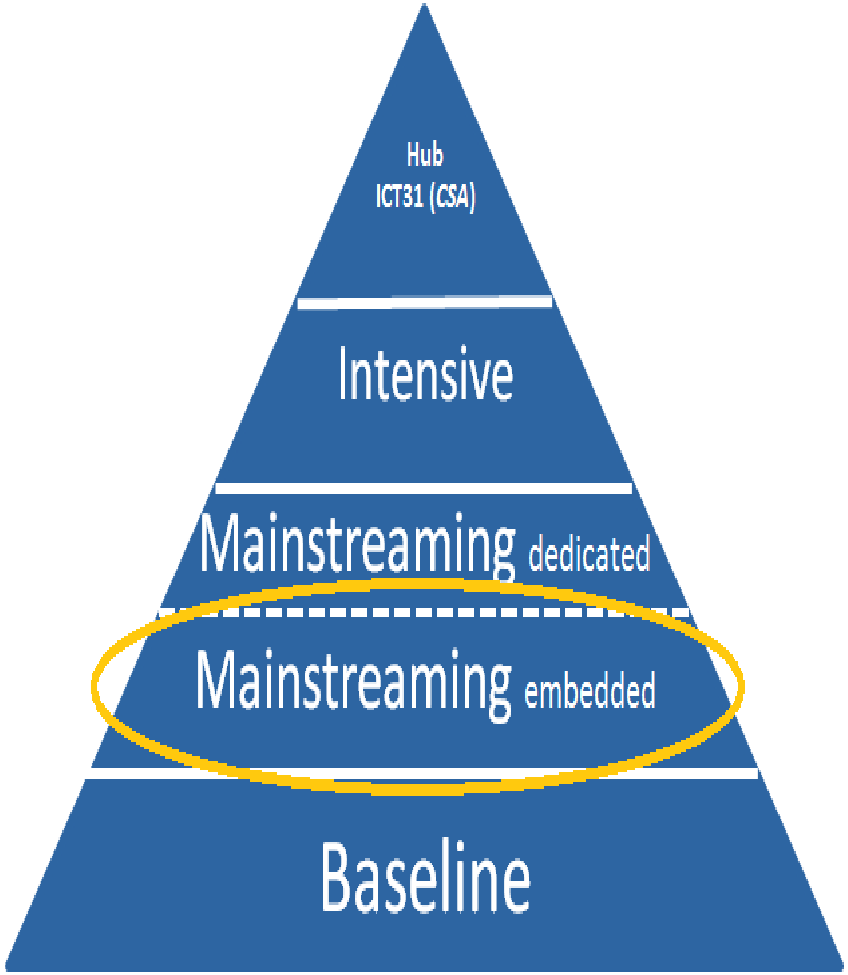
EIT

JRC

Simplified access

Common rules, toolkit of funding schemes

Dissemination & knowledge tranfer



Hub
ICT31 (CSA)

Intensive

Mainstreaming dedicated

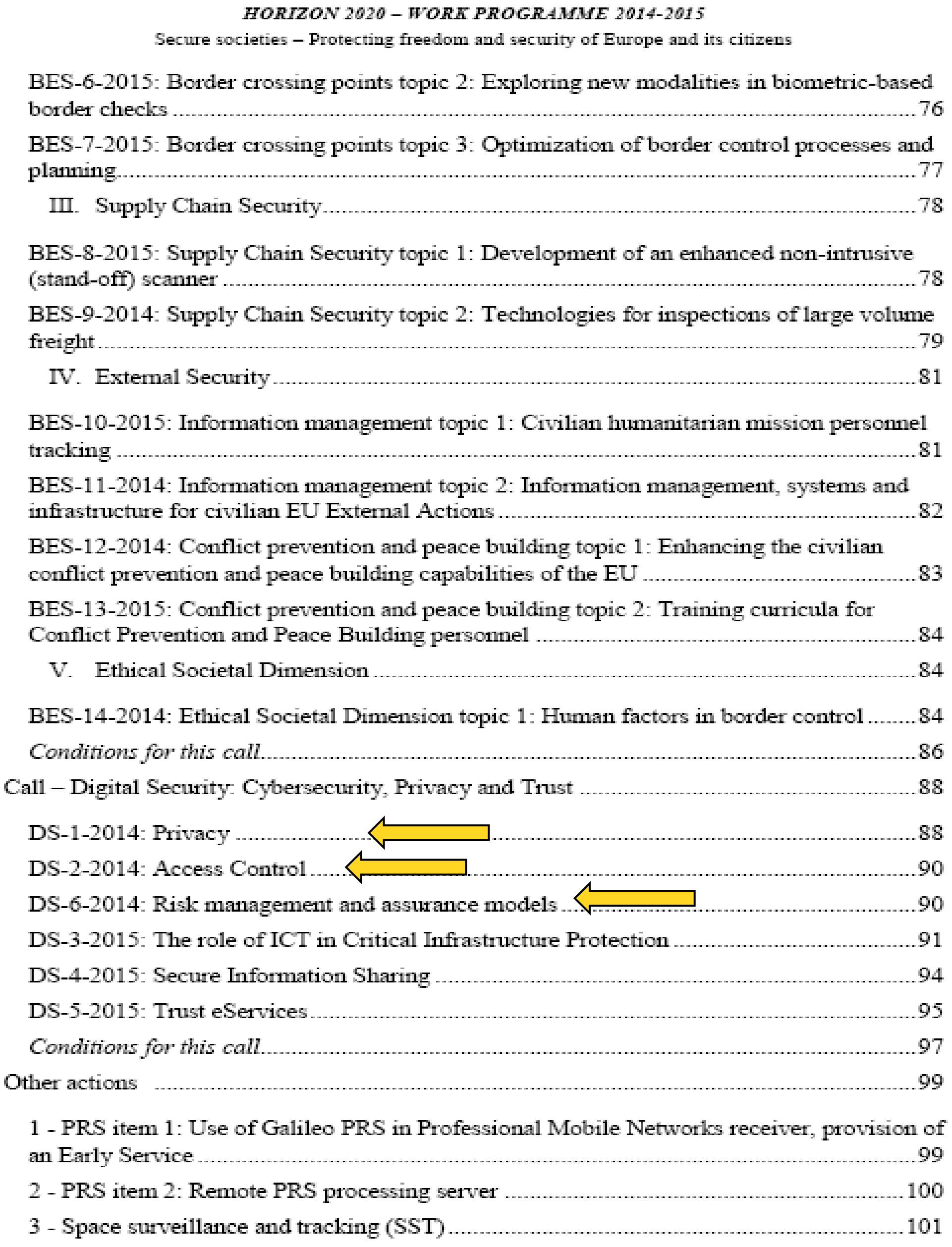
Mainstreaming embedded

Baseline

HORIZON 2020

European Commission

SC7: Protecting freedom and security of Europe and its citizens – Digital Security: Cybersecurity, Privacy & Trust



HORIZON 2020 – WORK PROGRAMME 2014-2015

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.

Focus on demonstrating the viability and maturity of state-of-the-art security, privacy and trust solutions

Three topics (H2020-DS-2014-1)

- *Privacy*
- *Access Control*
- *Risk Management & assurance models*

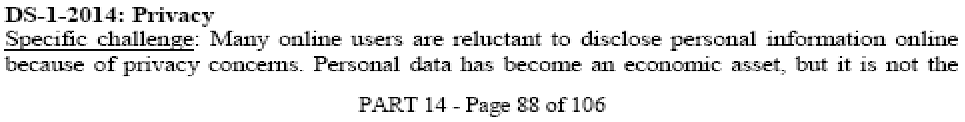
Two targets: End-users & Impact

DS 1 – 2014: Privacy (embedded)

*A practical, **user friendly** and **economically** viable implementation of relevant **legal obligations** related to personal data processing and/or prior consent.*

*Increased user **trust**, resulting in a higher uptake of online services.*

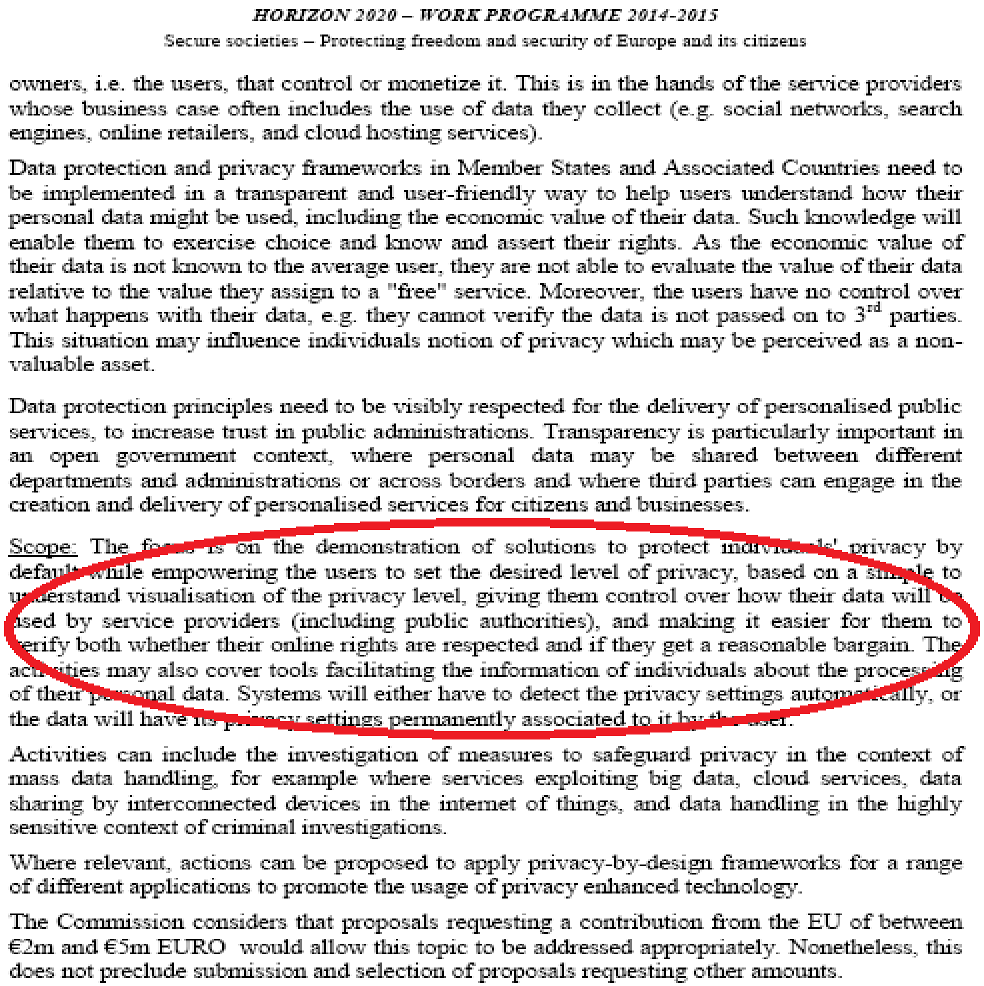
***Positive business cases** for online privacy.*



DS-1-2014: Privacy

Specific challenge: Many online users are reluctant to disclose personal information online because of privacy concerns. Personal data has become an economic asset, but it is not the

PART 14 - Page 88 of 106



HORIZON 2020 – WORK PROGRAMME 2014-2015

Secure societies – Protecting freedom and security of Europe and its citizens

owners, i.e. the users, that control or monetize it. This is in the hands of the service providers whose business case often includes the use of data they collect (e.g. social networks, search engines, online retailers, and cloud hosting services).

Data protection and privacy frameworks in Member States and Associated Countries need to be implemented in a transparent and user-friendly way to help users understand how their personal data might be used, including the economic value of their data. Such knowledge will enable them to exercise choice and know and assert their rights. As the economic value of their data is not known to the average user, they are not able to evaluate the value of their data relative to the value they assign to a "free" service. Moreover, the users have no control over what happens with their data, e.g. they cannot verify the data is not passed on to 3rd parties. This situation may influence individuals notion of privacy which may be perceived as a non-valuable asset.

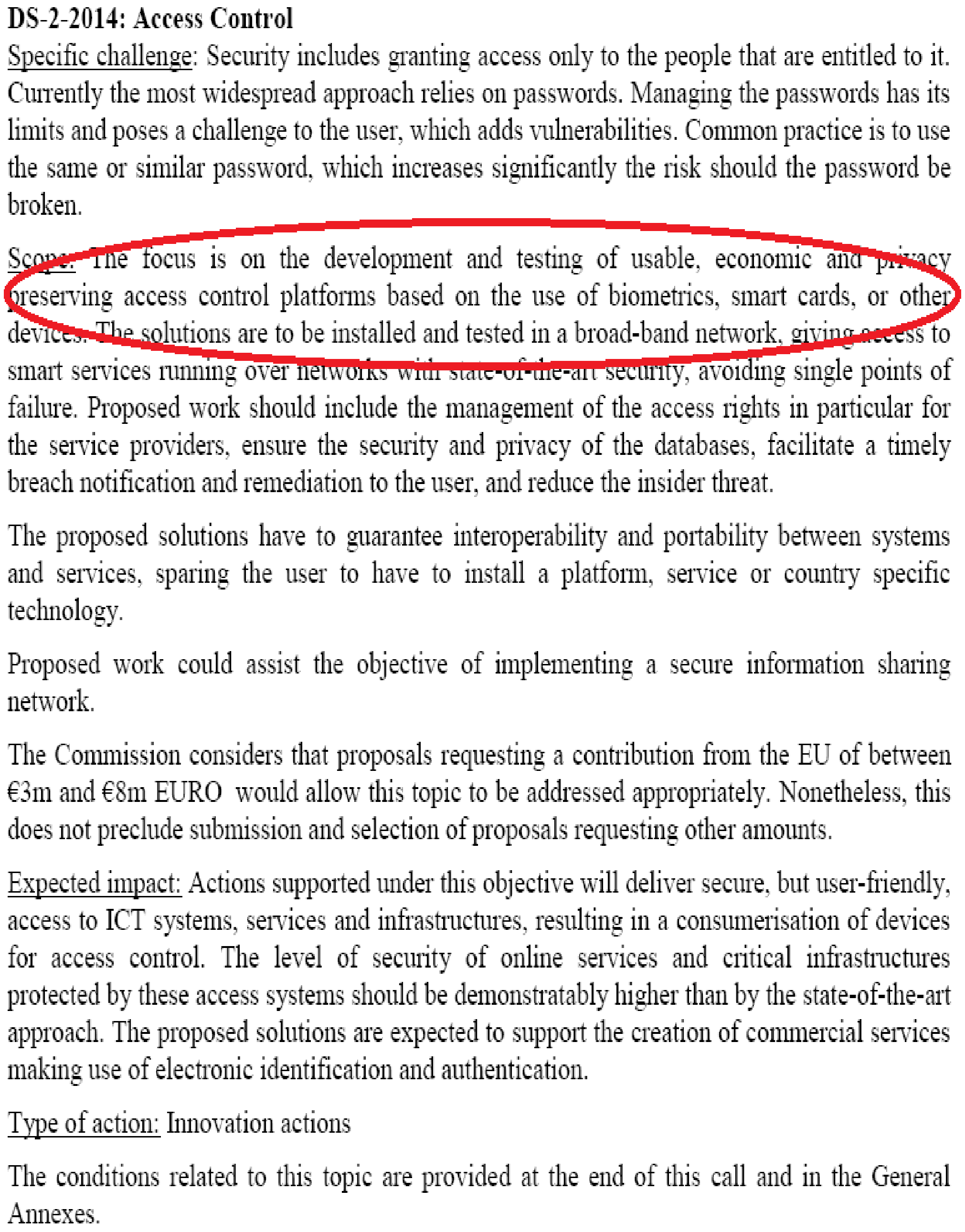
Data protection principles need to be visibly respected for the delivery of personalised public services, to increase trust in public administrations. Transparency is particularly important in an open government context, where personal data may be shared between different departments and administrations or across borders and where third parties can engage in the creation and delivery of personalised services for citizens and businesses.

Scope: The focus is on the demonstration of solutions to protect individuals' privacy by default while empowering the users to set the desired level of privacy, based on a simple to understand visualisation of the privacy level, giving them control over how their data will be used by service providers (including public authorities), and making it easier for them to verify both whether their online rights are respected and if they get a reasonable bargain. The activities may also cover tools facilitating the information of individuals about the processing of their personal data. Systems will either have to detect the privacy settings automatically, or the data will have its privacy settings permanently associated to it by the user.

Activities can include the investigation of measures to safeguard privacy in the context of mass data handling, for example where services exploiting big data, cloud services, data sharing by interconnected devices in the internet of things, and data handling in the highly sensitive context of criminal investigations.

Where relevant, actions can be proposed to apply privacy-by-design frameworks for a range of different applications to promote the usage of privacy enhanced technology.

The Commission considers that proposals requesting a contribution from the EU of between €2m and €5m EURO would allow this topic to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.



DS-2-2014: Access Control

Specific challenge: Security includes granting access only to the people that are entitled to it. Currently the most widespread approach relies on passwords. Managing the passwords has its limits and poses a challenge to the user, which adds vulnerabilities. Common practice is to use the same or similar password, which increases significantly the risk should the password be broken.

Scope: The focus is on the development and testing of usable, economic and privacy preserving access control platforms based on the use of biometrics, smart cards, or other devices. The solutions are to be installed and tested in a broad-band network, giving access to smart services running over networks with state-of-the-art security, avoiding single points of failure. Proposed work should include the management of the access rights in particular for the service providers, ensure the security and privacy of the databases, facilitate a timely breach notification and remediation to the user, and reduce the insider threat.

The proposed solutions have to guarantee interoperability and portability between systems and services, sparing the user to have to install a platform, service or country specific technology.

Proposed work could assist the objective of implementing a secure information sharing network.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €8m EURO would allow this topic to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

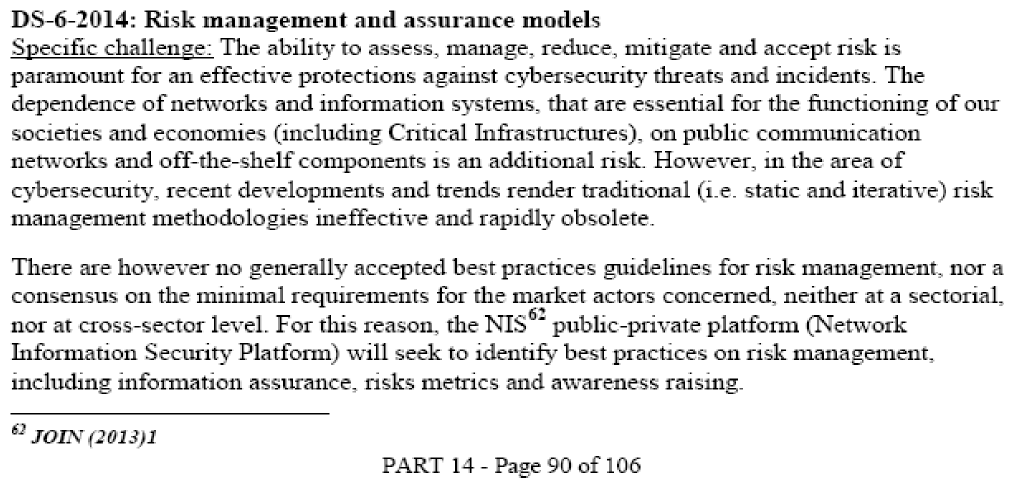
Expected impact: Actions supported under this objective will deliver secure, but user-friendly, access to ICT systems, services and infrastructures, resulting in a consumerisation of devices for access control. The level of security of online services and critical infrastructures protected by these access systems should be demonstratably higher than by the state-of-the-art approach. The proposed solutions are expected to support the creation of commercial services making use of electronic identification and authentication.

Type of action: Innovation actions

The conditions related to this topic are provided at the end of this call and in the General Annexes.

DS 2 – 2014: Access Control (embedded)

*Development and testing of **usable**, economic and privacy preserving access control platforms based on the use of **biometrics**, smart cards, or other devices.*



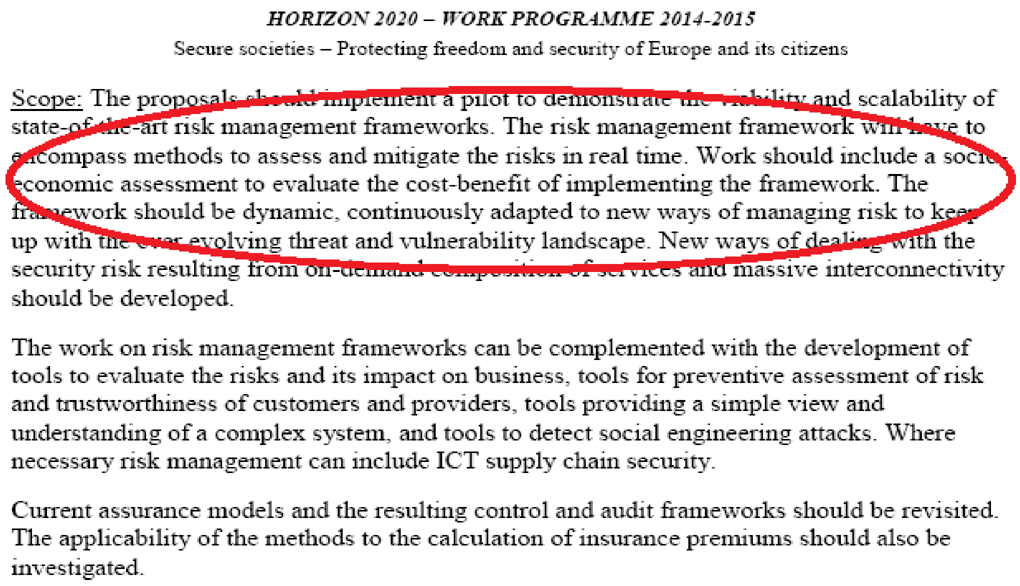
DS-6-2014: Risk management and assurance models

Specific challenge: The ability to assess, manage, reduce, mitigate and accept risk is paramount for an effective protections against cybersecurity threats and incidents. The dependence of networks and information systems, that are essential for the functioning of our societies and economies (including Critical Infrastructures), on public communication networks and off-the-shelf components is an additional risk. However, in the area of cybersecurity, recent developments and trends render traditional (i.e. static and iterative) risk management methodologies ineffective and rapidly obsolete.

There are however no generally accepted best practices guidelines for risk management, nor a consensus on the minimal requirements for the market actors concerned, neither at a sectorial, nor at cross-sector level. For this reason, the NIS[62] public-private platform (Network Information Security Platform) will seek to identify best practices on risk management, including information assurance, risks metrics and awareness raising.

[62] *JOIN (2013)1*

PART 14 - Page 90 of 106



HORIZON 2020 – WORK PROGRAMME 2014-2015

Secure societies – Protecting freedom and security of Europe and its citizens

Scope: The proposals should implement a pilot to demonstrate the viability and scalability of state-of-the-art risk management frameworks. The risk management framework will have to encompass methods to assess and mitigate the risks in real time. Work should include a socio-economic assessment to evaluate the cost-benefit of implementing the framework. The framework should be dynamic, continuously adapted to new ways of managing risk to keep up with the ever evolving threat and vulnerability landscape. New ways of dealing with the security risk resulting from on-demand composition of services and massive interconnectivity should be developed.

The work on risk management frameworks can be complemented with the development of tools to evaluate the risks and its impact on business, tools for preventive assessment of risk and trustworthiness of customers and providers, tools providing a simple view and understanding of a complex system, and tools to detect social engineering attacks. Where necessary risk management can include ICT supply chain security.

Current assurance models and the resulting control and audit frameworks should be revisited. The applicability of the methods to the calculation of insurance premiums should also be investigated.

DS 6- 2014: Risk Management and Assurance Models (embedded)

facilitate the implementation of existing and emerging requirements obligations on risk management.

Risk :

- *Perception*
- *Impact (societal, economic, legal)*
- *Tolerance (cultural, behavioral)*

Aristotelis.Tzafalias@ec.europa.eu

@EU_TrustSec

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2014-1.html

Questions?