

Grant agreement number: 216890



Project title

Think Tank for Converging Technical and Non-Technical Consumer
Needs in ICT Trust, Security and Dependability

Instrument

Coordination & Support Action

Deliverable reference number and title

D3.3 Public Consultation Report

Start date of project: 1st January 2008

Duration: 30 months

Organisation name of lead contractor for this deliverable

Waterford Institute of Technology

Table of Contents

| | |
|---|-----------|
| 1. INTRODUCTION | 3 |
| 2. METHODOLOGY | 5 |
| 2.1. OVERVIEW | 5 |
| 2.2. THE CONSULTATION QUESTIONNAIRE..... | 6 |
| 3. ANALYSIS AND CONCLUSIONS | 8 |
| 3.1 Trust Engineering..... | 8 |
| 3.2 Architecture..... | 17 |
| 3.3 Cyber-Security | 24 |
| 3.4 Accountability..... | 30 |
| 3.5 E-identity..... | 36 |
| 3.6 Privacy | 43 |
| 3.7 Protection..... | 51 |
| 3.8 Usability | 56 |
| 3.9 Management & Governance | 61 |
| 3.10 Socio-economics..... | 65 |
| 3.11 Miscellaneous Commentary..... | 70 |
| 4. OVERALL LEVELS OF ENDORSEMENT | 73 |
| ANNEX A – QUESTIONNAIRE | 75 |
| ANNEX B – RESEARCH CHECKLIST | 83 |
| ANNEX C – WRITTEN RESPONDENTS | 95 |
| ANNEX D – PUBLIC CONSULTATION POSTER | 97 |

1. Introduction

This Deliverable sets out the results of the Consultation process undertaken in the Think-Trust Project. This wide-reaching Consultation was launched on October 7th, 2009, and intensified over a four month period from January to April 2010. It elicited the opinions of a wide range of organisations, institutions and individuals.

The findings from this Consultation, together with the conclusions of discussions from various project-related events¹, will be used to finalise Think-Trust’s Recommendations Report (final) – D3.1c.

The Consultation process was included in the project to provide the wider ICT security community with the opportunity to comment on the interim research challenges identified in the project. The approach taken to the Consultation process has been detailed in [Deliverable D3.2](#), (submitted February 2010).

Diagram 1 below sets out the process through which the Think-Trust project worked to identify a series of research challenges in the area of trustworthy ICT. Public Consultation and the securing of additional inputs from the wider security community forms an important part of this process and feeds into the development of D3.1c Research Recommendations (final) which is due for publication in June 2010.

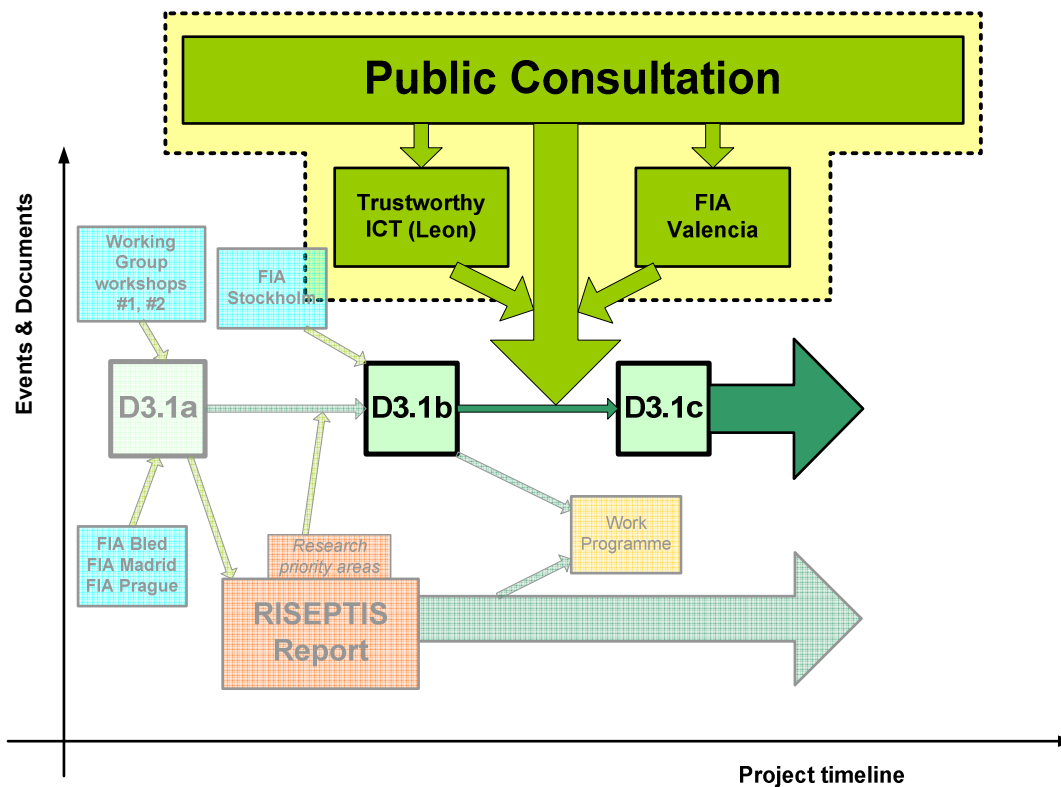


Figure 1 – External Feedback Contributions to the Project Recommendations

¹Including Trustworthy ICT (Léon, Spain), FIA Valencia.

The Consultation Process was officially launched on October 7th, at the FIA 'Trust and Identity' Caretakers' Workshop. At this event, the Think-Trust interim research recommendations were presented to a cross-section of experts from the domains of 'Networks', 'Future Content', 'Service Platforms', 'Service Infrastructure' and 'Identity & Privacy'.

This initial launch was followed up with announcement in the project's website ([click here](#)) and newsletter ([click here](#)).

Posters (see Annex D) announcing the consultation process were also displayed at the [FIA Stockholm](#) event--designed to make the wider trust and security community aware of the interim recommendations from the project and making them aware of the opportunities to input and comment. A similar poster was also displayed at the [Irish Future Internet Forum](#) event which took place on December 3rd, 2009, in Dublin, Ireland. This event was attended by a variety of researchers from academia and industry and included key notes from Conor Lenihan, TD, the Irish Minister of State for Science, Technology, Innovation & Natural Resources and Mr. Jacques Bus, Head of Unit 'Trust & Security in ICT Research'.

The process was also announced and discussed at the [Trustworthy ICT conference](#) in Léon, Spain on 10/11 February, 2010. Much of the conference proceedings were based around the recommendations contained in the RISEPTIS Report, with a number of members of the RISEPTIS advisory board and Think-Trust participating as speakers, panellists and session chairs. The interim research challenges and the Consultation were announced and discussed in [Session 2: Trustworthy Networked Service and Computing Environments](#).

Structure of the Consultation Report

This document is set out as follows:

- Chapter 2 'Methodology' details the methodology used to capture input during the consultation process. Feedback was captured through a [questionnaire](#) and [research checklist](#). Account was also taken of views expressed at FIA and related events (including Leon Trustworthy ICT conference)
- Chapter 3 'Analysis and Conclusions' analyses the feedback received and also records respondents' comments on each of the ten research areas.
- Chapter 4 'Levels of Endorsement' provides a preliminary examination of the overall ranking of the ten different research challenge areas, based on the feedback received in the consultation. A prioritisation of the research areas is made on the basis of the feedback.

The conclusions and main findings contained in this report are carried through to Deliverable D3.1C "Towards a Trustworthy Information Society: The Research Challenges".

Annexed to this report are:

- The consultation questionnaire (Annex A)
- The research checklist (Annex B)
- List of those who gave written responses (Annex C)
- Promotional poster displayed at FIA Stockholm (Annex D)

2. Methodology

2.1. Overview

The objective of the Consultation phase was to engage a wide range of opinions through a process which involved written and oral feedback together with inputs from related events. Feedback was captured through a [questionnaire](#) and [research checklist](#). In the questionnaire, which is a detailed document, respondents were asked to score the identified challenges according to a scale.

The conclusions of discussions at relevant events were also noted and are reflected in Deliverable 3.1c. The interim research challenges identified in the project formed the basis of the Consultation process. These recommendations concern the main challenges and key research priorities in the area of **Trust, Security and Dependability** and stem from the four priority areas identified in Recommendation 1 of the [RISEPTIS Report](#).

- Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
- Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
- Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
- Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management

The interim research challenges which formed the basis of the public consultation process were grouped under ten headings in [Deliverable 3.1b](#) (Interim Recommendations Report) This Deliverable in turn, was informed by the earlier [Deliverable 3.1a](#).

The ten research areas in which input was invited are:

1. ***Trust Engineering***
2. ***Architecture***
3. ***Cyber-security: Engineering and Technology***
4. ***Accountability***
5. ***E-Identity***
6. ***Privacy***
7. ***Protection***
8. ***Usability***
9. ***Management & Governance***
10. ***Socio-economics***

2.2. The Consultation Questionnaire

In the Questionnaire, respondents were asked to rank a series of challenges in each of the ten areas according to the following criteria:

| | |
|------------------|---|
| <i>A*</i> | <i>Absolutely Mandatory</i> |
| <i>A</i> | <i>Essential</i> |
| <i>B</i> | <i>Necessary</i> |
| <i>C</i> | <i>Required for new technologies / threats</i> |
| <i>D</i> | <i>Required for new attractive services</i> |
| <i>X</i> | <i>Not necessary or not urgent</i> |

In analysing the various scores returned from respondents (chapter 3), we consider the specific challenges in any one area as being endorsed if they received a majority of '*absolutely mandatory*', '*essential*' or '*necessary*' rankings. Challenges that received a significant number of '*required for new technologies/threats*' or '*required for new attractive services*' scores were considered as being more medium-term, while those challenges receiving a noticeable number of '*not necessary or not urgent*' scores, are considered as being longer-term issues.

The overall ranking of the ten research areas (in terms of prioritisation) is based on the accumulated '*absolutely mandatory*', '*essential*' and '*necessary*' scores received by each research challenge area in the survey.

The questionnaire and research checklist were distributed widely. Dissemination and announcements included the following:

- Think-Trust website
- Future Internet Assembly attendees
- Mailing list contacts of Think-Trust partners
- Projects in FP7 ICT Workprogramme 2007-2008 Objective 1.4 (Secure, dependable and trusted Infrastructure)
- ETPs
 - NEM
 - NESSI
 - eMobility
- Projects in Security Research Programme and other relevant projects
- Announcement in European Commission newsletter – Unit F5 'Trust & Security'
- Announcement in Think-Trust e-newsletter
- STORK Community of Interest

In addition to direct mailings, the questionnaire and research checklist were also available for download from the homepage of the [project website](#) and for on-line completion through [Survey Monkey](#). Two [LinkedIn](#) discussions were also started within the 'Information Security Community' and the 'Irish Future Internet Forum' groups. In both discussion groups, the project's work, its research challenges and its public consultation process were announced.

Announcements of the process were also made at:

- FIA Trust & Identity preparatory workshop, Brussels, October, 2009
- Internet Governance Forum 2009, Sharm El Shiek, November, 2009
- FIA Stockholm, November, 2009
- Irish Future Internet Forum, Dublin, December, 2009
- Think-Trust FIA meeting, Brussels, January, 2010
- Trustworthy ICT Conference, Leon, February, 2010
- CEPIS event, Budapest, March, 2010
- FIA Valencia, April, 2010
- InfoSec, London, April, 2010
- INCO-Trust workshop, New York, April, 2010

Almost 50 written responses were received from various stakeholders during the consultation process, in addition to the informal discussions and verbal feedback collected. Of those respondents who returned the consultation questionnaires—where scores were assigned to the various challenges—the vast majority completed it in full, giving up to 75 individual scores in some cases. Each respondent who filled out the research checklist inserted up to 10 comments before returning it.

3. Analysis and Conclusions

This section sets out the analysis of the feedback captured through the [questionnaire](#) and [research checklist](#). In the detailed questionnaire, respondents were asked to score the identified challenges according to the scale outlined in chapter two.

The scores received were considered in the analysis along with comments received in response to prompts such as:

- *Do you agree that these are the principal research challenges in this area?*
- *Do you think we need to add additional topics?*
- *Which topics need to be amplified or extended?*
- *Should any topics be removed, down-graded, or postponed?)*

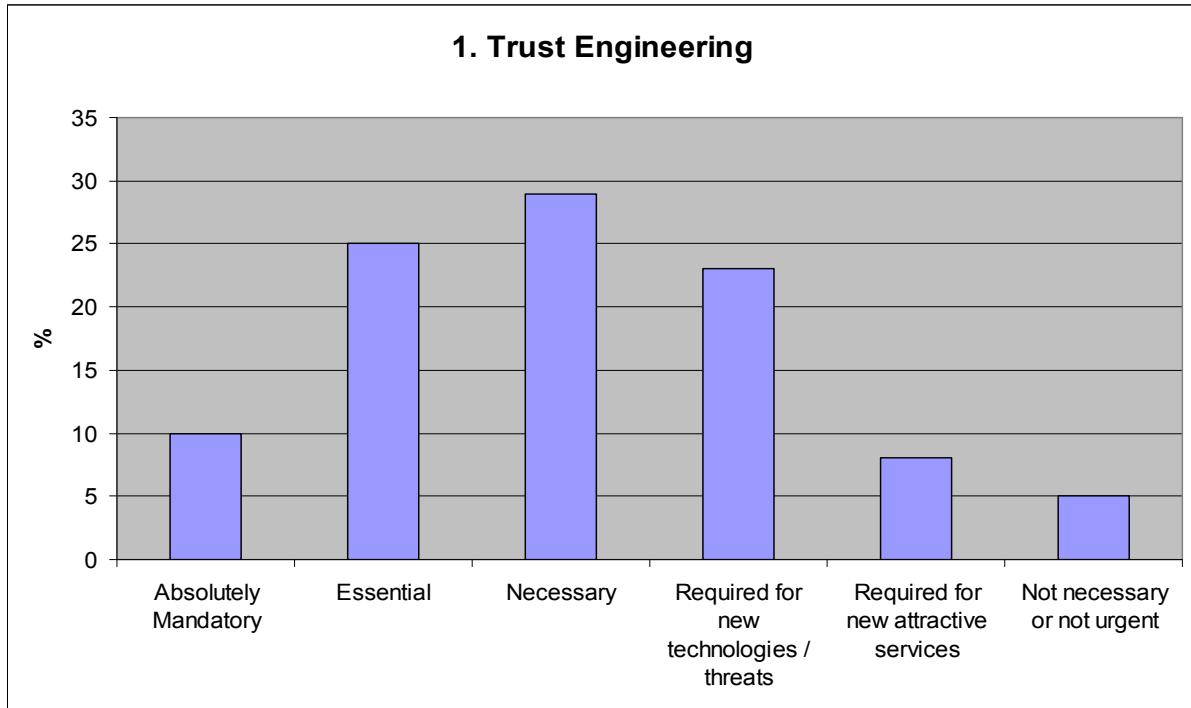
In the following pages, the feedback received is presented by means of a statistical analysis and notation of relevant commentary. In this regard, it is important to note that a significant number of responses stated simply 'Agreed', 'OK', 'These are the correct challenges in this area', etc. Such replies are not included in this document, as they merely endorse the identified research challenges. We have, therefore, focused on the more in-depth, contextual comments received – be they constructively critical or otherwise.

3.1 Trust Engineering

When the overall picture is considered, the challenges identified in D3.1b in the area of 'Trust Engineering' were endorsed by the majority of respondents. 64% of the scores registered indicated that the identified topics were either 'absolutely mandatory' (10%), 'essential' (25%) or 'necessary' (29%).

Only 5% of the scores considered any of the challenges identified to be either 'not necessary or not urgent'.

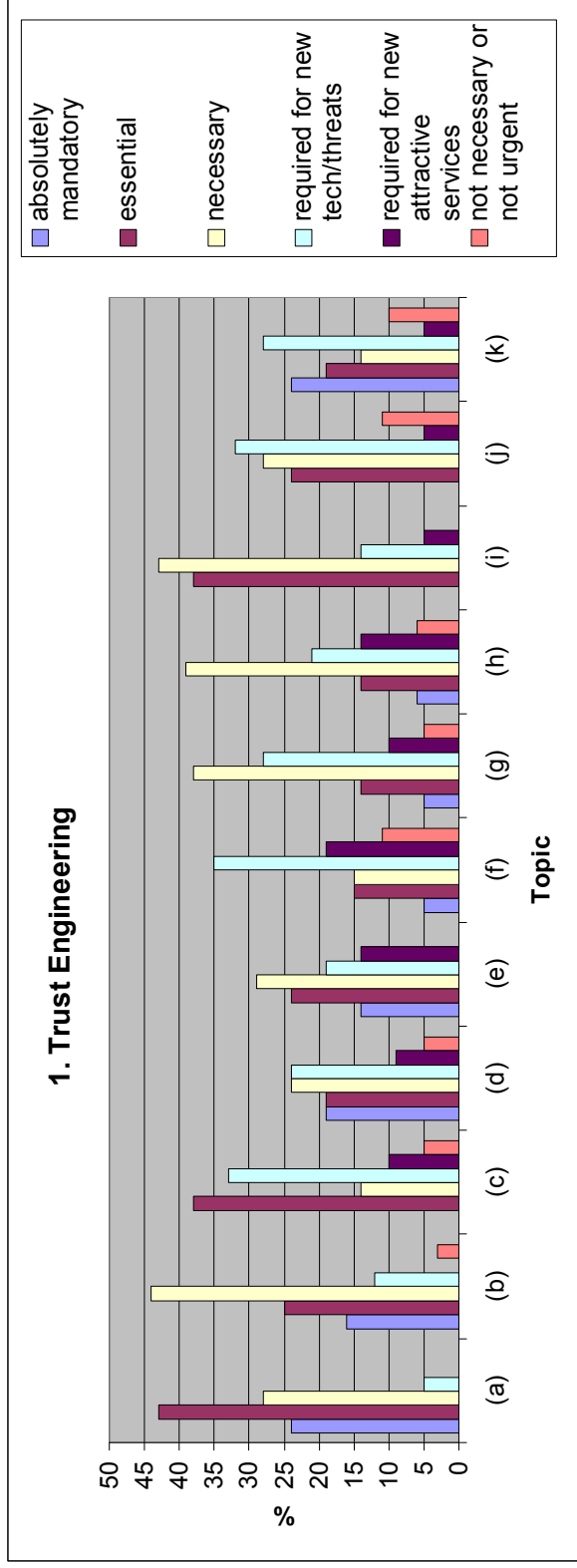
The graph overleaf shows the combined scores registered in the area of Trust Engineering



Graph 1.1 Trust Engineering – Combined Scores

Turning to the **individual challenges** within the Trust Engineering area, there are a number of interesting points emerging, as can be seen from graph 1.2 overleaf:-

- The challenge of **supporting trust relationships** received the highest level of endorsement and recognition with 95% of scores indicating that this area was either ‘absolutely mandatory’, ‘essential’ or ‘necessary’.
- 84% of respondents said that the **‘development, expression and use of trust indicators’** was either ‘absolutely mandatory, essential or necessary’. Only 2% thought it ‘not necessary or not urgent’
- It is interesting to note that challenge (f) **‘Tools to Calculate Trust’** had few ‘absolutely necessary’ scores (5%). About one third of respondents currently consider the challenge to be ‘absolutely mandatory’ essential or ‘necessary’ but over 50% thought it will be required for ‘new technology/threats’ or ‘new attractive services’.



Graph 1.2 Trust Engineering – Individual Challenges Scores

| | Topics |
|-----|--|
| (a) | Support trust relationships (establishment, management, and maintenance); |
| (b) | Development, expression and use of trust indicators; |
| (c) | Automatic computation of trust assertions, based on policy frameworks that take into account user preferences; |
| (d) | Life-cycle management, including maintenance, repair and recovery; |
| (e) | Models, methodologies, measurement of trust (see Quantification below); |
| (f) | Tools to calculate it (a combination of assisting the user and quantifying personal trust); |
| (g) | Assessment of availability / downtime / integrity / confidentiality to feed into trust models; |
| (h) | Delegation and acceptance of trust and privileges; |
| (i) | Scaling results on trust experiments from the laboratory environment to the real worlds of the Future Internet? |
| (j) | Generalisation of security predictions across different software components, programming languages, systems, environments? |
| (k) | Collection and sharing of security-related data for experimental research. |

Commentary received in this area is set out below:

Inside of trust framework we could make further subdivision into preventive measures (e.g. secure software engineering), monitoring or assurance measures (e.g. agile certification etc). One of the largest issues will be dynamicity of trust which implies monitoring and control mechanisms

=====

Yes, I think that the evaluation of trust is paramount, since security has well-known limits, both in terms of methodology and in terms of possibilities. The methodology only provides us with subjective, incomplete security measures. Besides, it is generally impossible to reasonably verify a result of a calculation; also, it is generally impossible to verify that your data has not been handed out to the unknown third parties or that no data mining has been applied to it.

In the world of semi open and open IT systems, security has clear limits. It is important to define and assess other, alternative system properties. The notion of systems and especially of open, complex systems needs to be integrated in this research agenda

=====

I see a big difference in consumer related „trust“ and business related trust - and, even more, between consumers and businesses. The major difference is the capability of enforcement of rights - that has a big impact on trust. Therefore, I would suggest to add to look also at these aspects from the two different views. Also: trust may be different in different cultures. Although this is not a technical issue, it should also be taken into account, namely, that trust may be realized / attained / managed / seen differently per cultural environment.

=====

The research challenges are OK. I would like to add:
Trust quantification and management experimentation in cloud service environments, since trust is of outmost importance in those kind of environments. Standardized, or at least widely-accepted trust indicators are needed for clouds.

=====

I think that the quantification of Trust could be more explicit. Perhaps you might find something from the master project worth referencing http://www.master-fp7.eu/index.php?option=com_docman&task=cat_view&gid=35&Itemid=60

Or specifically these slides from TAS3 project are on trust metrics <http://www.tas3.eu/project/publications/dissemination/trust-metrics-tas3-approach-eic-2009.pdf/view>

I don't think that (g) is a high priority at the moment as research into network mgt should be able to re adapted for trust models

=====

Add: Distributed Trust Models. If an entity presents credentials to a Trust authority, these credentials should be available anywhere a trust decision is required, ideally without that entity needing to present those credentials again.

=====

These areas are very inclusive. I would recommend that within the model section that maturity model concepts be used to better reflect levels of trust.

=====

Concerning trust indicators and many of the other points a trust framework should offer the ability to combine trust indicators from different sources. Mash up services and aggregator functions on the web are already quite common but the origin of information that is mashed up is not always transparent (provenance) and their aggregated trust is often independent of their origins.

=====

I fully agree with the above agenda.

Moreover, I believe that this area has a significant overlap with "Usability", as Trust is mostly a subjective estimation carried out by individuals who assess their own experience and context.

Concerning the quantification of Trust, Security and Privacy, there is much to do. I wrote an article that relates the uptake of privacy technology innovation to the availability of a decision-making procedure based on a quantification of risks and technology benefits, which can add to this area:

Fritsch, Lothar und Abie, Habtamu. (2008) A Road Map to the Management of Privacy Risks in Information Systems, in: Gesellschaft f. Informatik (GI) (Eds.): Konferenzband Sicherheit 2008, Lecture Notes in Informatics LNI 128, 2-Apr-2008, Bonn, Gesellschaft für Informatik, pp. 1-15.

Quantification in this context leads to cost and effectiveness transparency of trust properties.

=====

The issue of trust engineering is quite broad and it is difficult to say that the listed topics cover the principal research challenges. This is clear that computational trust engineering is one of the main research challenges of trust engineering. However the listed topics do not appear to us connected to a known computational trust framework and they seem a bit disorganised from this point of view.

One of the main research challenges in this area would be to build upon previous work and have a continuity of funding in people working in this field, for example, as a trust research excellence centre rather than various disconnected projects restarting almost each time from scratch. Funding network of excellence involving previous people having already worked in this field would also be one of the research challenges because it has never really be done although such communities exist. For example, the trustcomp.org community has focused on computational trust since 2004 and has now more than 250 industrial and academic members. The research challenge to come up with a coherent trust engineering framework may be the one to start with.

=====

No specific comments, only a question: does your view of trust include reputation management?

In this case, I think issues related to the reputation metrics, reputation management framework, etc. must be addressed also.

Commentary received on specific topics:

(a) Support trust relationships (establishment, management, and maintenance);

Make trust scalable

=====

User-friendly, efficient, automatic

=====

(b) Development, expression and use of trust indicators;

Reputation-based schemes

=====

Have to be meaningful

=====

Perhaps mention the development of a “Quality of Trust” factor

=====

Might in addition look at cognitive models of trust, their stability, and their correlation with specific user groups (such as the blind, or memory-impaired).

=====

(c) Automatic computation of trust assertions, based on policy frameworks that take into account user preferences;

Also take into account the context; e.g. important to know who and under what conditions the assertions are given

=====

This is achieved by user preferences in Perimeter GUI

=====

(d) Life-cycle management, including maintenance, repair and recovery;

Could be interpreted as a subset of (e) Models, methodologies, measurement of trust

=====

(e) Models, methodologies, measurement of trust (see Quantification below);

May be promoted to second/third point. Possible additional topic "anonymity and privacy vs. trust"

=====

(f) Tools to calculate it (a combination of assisting the user and quantifying personal trust);

This is achieved by the Trust Engine in Perimeter

=====

(g) Assessment of availability / downtime / integrity / confidentiality to feed into trust models;

Context in general, also situations

=====

Should mention availability, downtime, etc as examples as there are other measurements/metrics that can be used to feed into trust models e.g. other security areas, cooperation

=====

(h) Delegation and acceptance of trust and privileges;

Make things more scalable

=====

Should be an intrinsic part of the system, but it could exist without this

=====

(i) Scaling results on trust experiments from the laboratory environment to the real worlds of the Future Internet?

Validating meaning of trust with users

=====

(j) Generalisation of security predictions across different software components, programming languages, systems, environments?

Interesting, but difficult to achieve. The assumption here is that there is no trust between 2 endpoints and you try to calculate based upon network security characteristics, applications security, hardware security; i.e. everything that is in between the endpoints. Where do you stop?

=====

More integrating various security predictions to determine overall effect

=====

(k) Collection and sharing of security-related data for experimental research.

Most interesting for IDS systems

=====

Possible additional research challenge is "merging various measurements including QoS, functional, roles, and reputation-based service properties and behaviour measurements that can be used collectively in measuring and predicting trust"

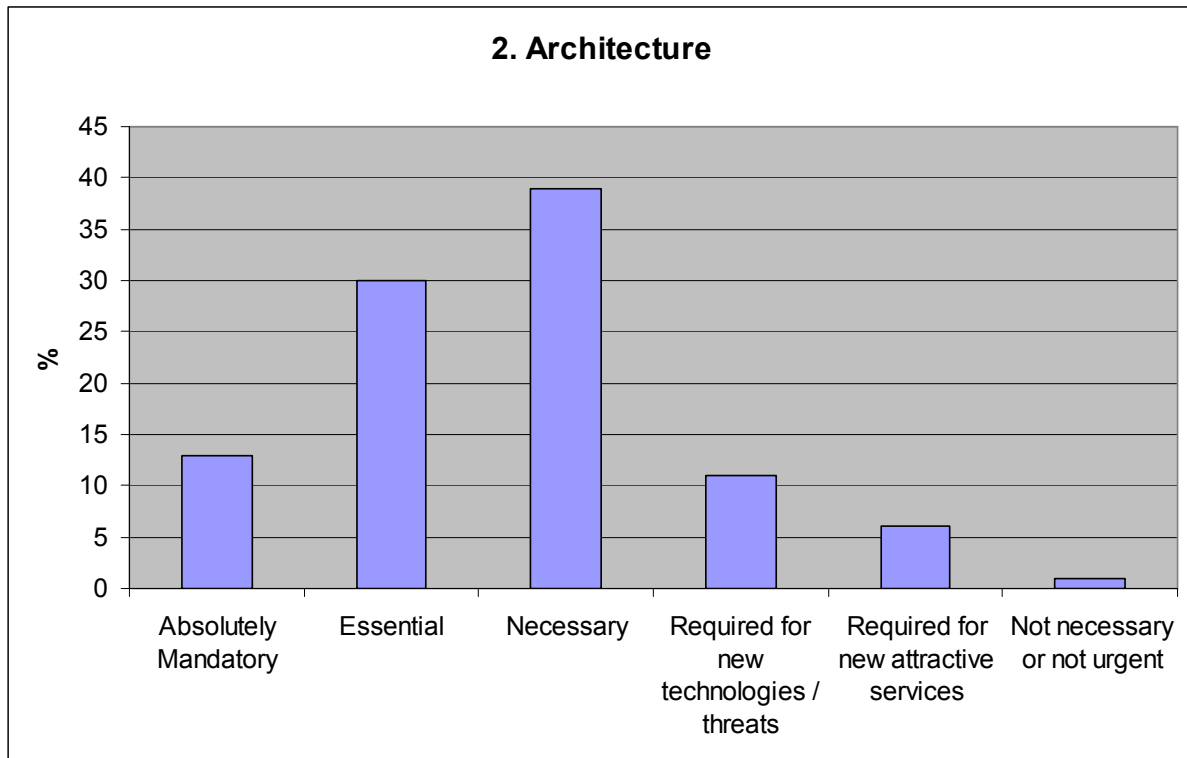
=====

3.2 Architecture

When the overall picture is considered, the challenges identified in D3.1b in the area of ‘Architecture’ were endorsed by the vast majority of respondents. Over 80% of the scores registered indicated that the identified topics were either ‘absolutely mandatory’ (12%), ‘essential’ (30%) or ‘necessary’ (39%).

1% of the scores considered any of the challenges identified to be either ‘not necessary or not urgent’.

The graph below shows the combined scores registered in the area of Architecture:

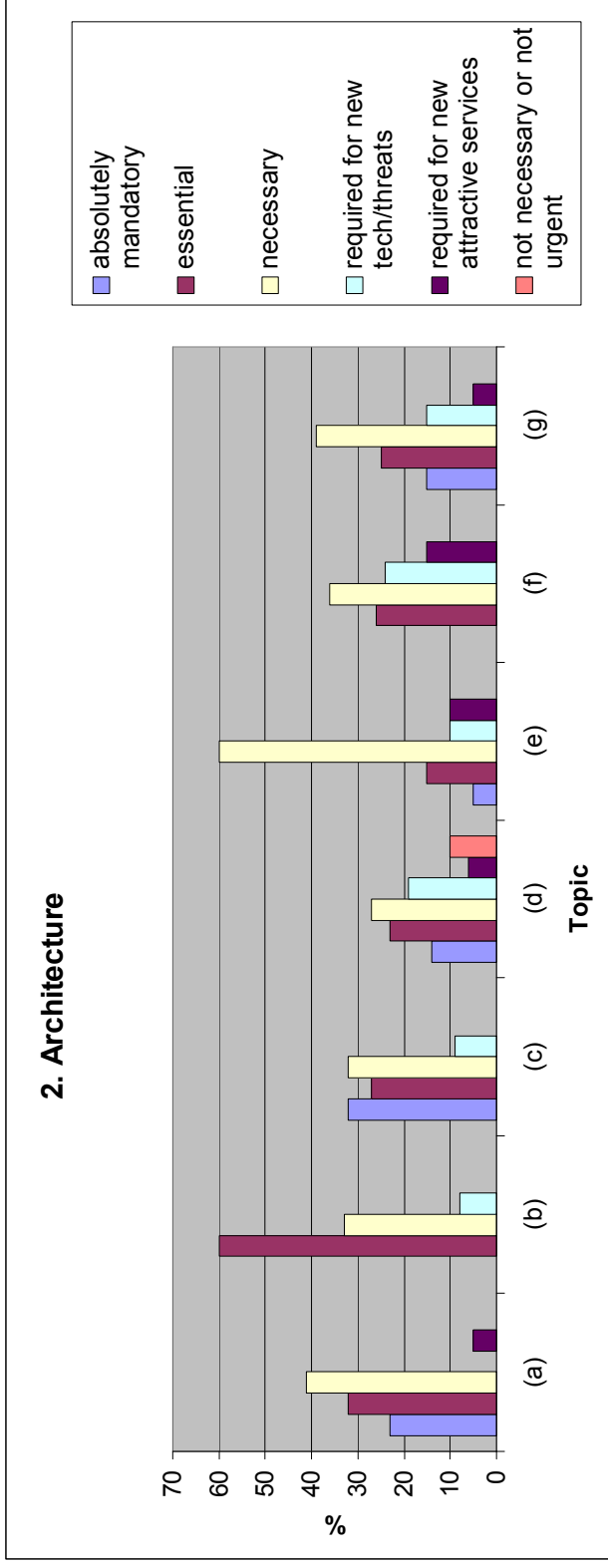


Graph 2.1 Architecture – Combined Scores

Turning to the **individual challenges** within the Architecture area, there are a number of interesting points emerging, as can be seen from graph 2.2 overleaf:-

- The challenge of **(a) ‘policy awareness and transparency’** as architecture properties received a very high level of endorsement with 95% of scores indicating that this was either ‘absolutely mandatory’, ‘essential’ or ‘necessary’. None of the respondents considered this challenge ‘not necessary or not urgent’.
- This was closely followed by challenge **(b) ‘Transparency support: monitoring; observability; logging, accessibility’**, which 92% of the scores indicated it to be either ‘essential’ or ‘necessary’, while the remaining 8% considered it as a requirement for ‘new technologies/threats’.
- In contrast, the scores for challenge **(d) ‘Meta architecture –higher-level abstractions to help structure a global information security architecture?’** are far more evenly spread: absolutely mandatory = 14%, essential = 23%, necessary = 27%, required for new technologies/threats = 19, required for new attractive services = 5%, not necessary or not

urgent = 10%. To a lesser extent, the scores for challenges **(f) 'Damage control: domains, partitioning, compartmentalisation in (e.g.) Cloud environment, including dynamic service composition/aggregation'**, and **(g) 'Architectural Standards (to support)...'** were also broadly spread with opinion appearing to be more divided.



Graph 2.2 Architecture – Individual Challenges Scores

| | Topics |
|-----|--|
| (a) | Policy awareness and transparency as architectural properties |
| (b) | Transparency support: monitoring; observability; logging, accessibility |
| (c) | Consistency of security and trust facilities and mechanisms across layers and domains |
| (d) | Meta architecture –higher-level abstractions to help structure a global information security architecture? |
| (e) | Network and service architectures – scalability and interoperability of the current architecture consider service composition/aggregation) |
| (f) | Damage control: domains, partitioning, compartmentalisation in (e.g.) Cloud environment, including dynamic service composition/aggregation |
| (g) | Architectural standards (to support): pre-conditions for interoperability; verification of conformance requirements; built-in emergency measures; establish workable definitions concept (metadata, ontologies, etc.); support for security policy management, including the ability to attach policy information to data. |

Commentary received in this area is set out below:

Control process architecture could be added.

=====

I am not sure how policy awareness can become an architectural property? Policy-awareness seems to be subject to behavioural analysis and less to a specific, chosen architecture.

Meta-architecture approach seems interesting. It would be nice to have best-practice like architectural patterns with known high-level properties and advantages, especially in the extra-functional domain (security, robustness, etc). Being capable of producing systems from known given patterns would revolutionize system design. However, to be able to do this, we might need to change the whole current system design methodology and start basing the services on other paradigms than client-server, function-to-box assignment, etc.

Assurance might be a missing keyword here: indeed either you trust a system, or you'll demand assurances (security assurance, privacy assurance, quality assurance, ...) from the system or its owner (i.e. certainty, evidence or third-party certifications that the system in question behaves as expected).

=====

It is difficult to say that the listed topics are the principal research challenges in the area of architecture because they appear to us to be either vague or too narrow without an explanation about how they are connected together and how they fit into a higher level architecture framework. The research challenge to come up with a coherent architecture framework may be the one to start with.

=====

Additional Topics:

A relevant topic is that the FI network architecture shall include resilient and dependable network access technologies which are able to assist society in emergency scenarios. In this regard, the key role of Satellite Networks shall be highlighted as satellite networks

are not subject to man made or natural disasters, provide high reliability and availability, provide service continuity and fast recovery even in low density populated areas, and also provide end-to-end control.

=====

Overall good, but I doubt that more Meta will help. On the contrary, I think we should develop a hands-on understanding. I suggest to delete (d) (or at least for formulate it more concretely) „Policy awareness“ may also be misleading in the sense of „political“ policy. I think what is meant is policy like concrete descriptions of expectations on non-functional properties for architectures. Then I would strongly agree.

=====

Addition: Building security and trust measurability increasing mechanisms into architectures.

=====

With reference to the last point “security policy management ...” one interesting point is the possibility to complete a data policy with instructions on how to “manipulate” the data in some circumstances.

For example, health records data are required by health organisations for different goals. Most of these data are not required in a complete form, for some purposes only a strict subset of exact health data are required, for other purposes only approximate data (e.g. the patient’s ZIP code instead of the exact patient’s address).

Traditional security policy only focuses on specifying the context information to be acquired to determine if the access to the resource have to be granted or denied. In the example reported above, therefore, security policies cannot help. Having the possibility to specify the “accuracy” (and how to process the basic data to obtain it) could help in handling situations like the one exemplified above

=====

“Might be worth mentioning threat and vulnerability management under damage control

Not sure if the example - compartmentalisation in, (for example), Cloud environment – is accurate?”

=====

Good list. Emphasise the links between Trust and other security services, such as authorisation and access control.

=====

Commentary received on specific challenges:

(a) Policy awareness and transparency as architectural properties;

=====

(b) Transparency support: monitoring; observability; logging, accessibility;

Perhaps mention Refactoring as well here”

=====

Might possibly mention “audit trails” rather than “logging”, as the latter refers a rather arbitrary context.”

=====

Should be high up on the agenda

=====

(c) Consistency of security and trust facilities and mechanisms across layers and domains;

Could include removal of redundant features (across all aspects, not just trust)”

=====

Add the long-term availability of facilities with its consequences (long-term archival, long-term key management, time stamping, key renewal, signature refreshment, exchange of personnel and responsibilities reflected in policies, ...)

=====

(d) Meta architecture –higher-level abstractions to help structure a global information security architecture?

=====

(e) Network and service architectures – scalability and interoperability of the current architecture consider service composition/aggregation);
=====

(f) Damage control: domains, partitioning, compartmentalisation in (e.g.) Cloud environment, including dynamic service composition/aggregation;
=====

(g) Architectural standards (to support): pre-conditions for interoperability; verification of conformance requirements; built-in emergency measures; establish workable definitions concept (metadata, ontologies, etc.); support for security policy management, including the ability to attach policy information to data.

Get these right from the start to get all of the above fall into place more easily
=====

Assuming formal rather than de-facto standards
=====

At least domain-specific standards
=====

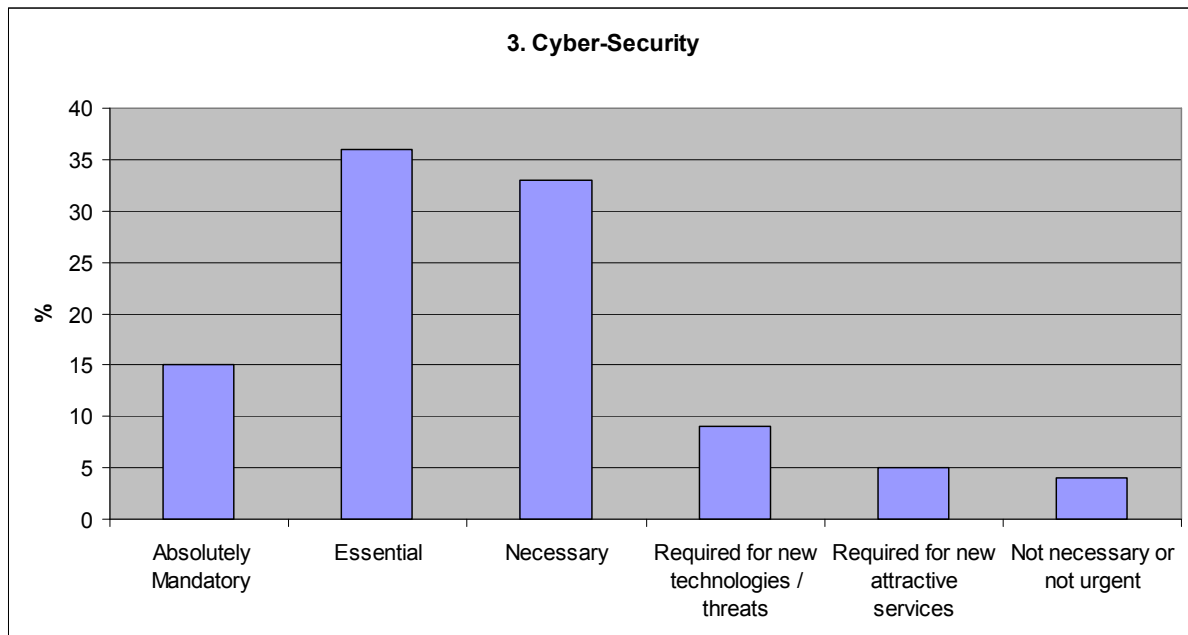
Suggest something for data storage and compliance is included
=====

3.3 Cyber-Security

When the overall picture is considered, the challenges identified in D3.1b in the area of ‘Cyber-Security’ were endorsed by the vast majority of respondents. Over 84% of the scores registered indicated that the identified topics were either ‘absolutely mandatory’ (15%), ‘essential’ (36%) or ‘necessary’ (33%).

4% of the scores considered any of the challenges identified to be either ‘not necessary or not urgent’.

The graph below shows the combined scores registered in the area of Cyber-Security:

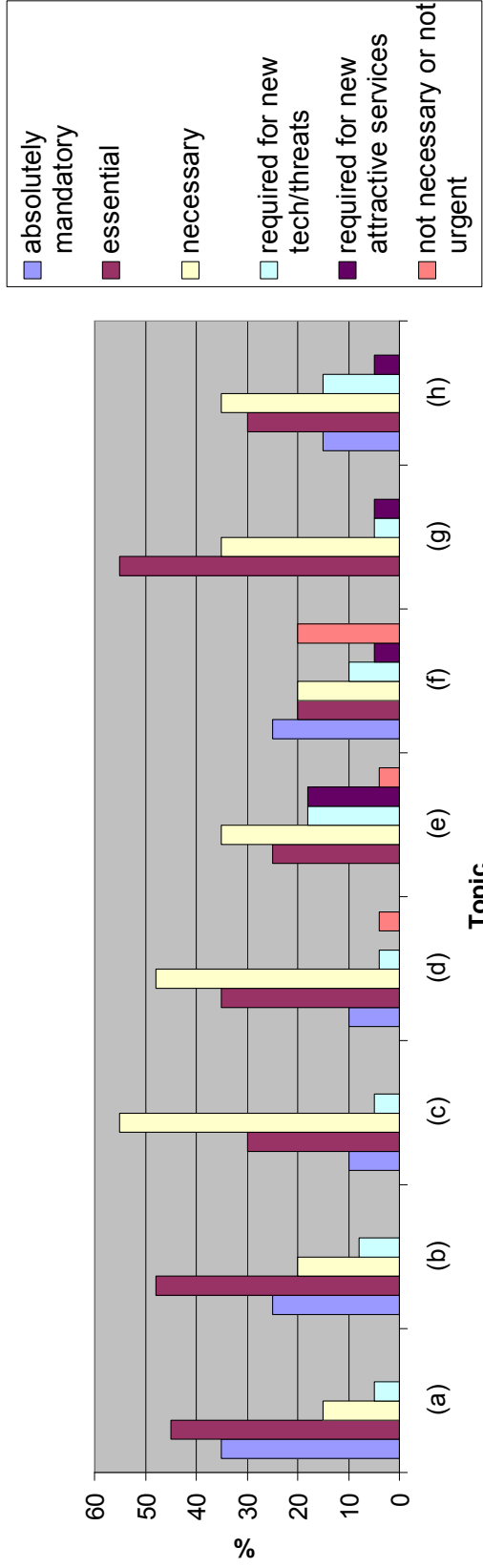


Graph 3.1 Cyber-Security – Combined Scores

Turning to the **individual challenges** within the Cyber-Security area, there are a number of interesting points emerging, as can be seen from graph 3.2 overleaf:-

- 80% of the scores registered for challenge (a) ‘**Techniques and mechanisms to provide protection, assurance and integrity**’ considered this to be either ‘absolutely mandatory’ or ‘essential’. Similar trends were noted in scores registered for challenge (b) ‘**Robustness, resilience, survivability**’.
- Topics (c) ‘**Criteria and standards to support policy governance**’, (d) ‘**Interoperability, and platform independence**’ and (e) ‘**Virtualisation to support construction of complex concepts such as high-demand, critical services on otherwise limited technologies**’ were noteworthy due to the high percentage of ‘necessary’ scores received, with a notable correlation of ‘not necessary or not urgent’ scores – 5% for (d) and (e).
- Challenges (f) ‘**Security in environments with scarce resources**’ and (h) ‘**Tools and technologies to support design and construction of future trusted environments and networks**’ attracted the broadest range of scores. Challenge (f), in particular, received a noticeably high level of ‘not necessary or not urgent’ scores: 20%.

3. Cyber-security



Graph 3.2 Cyber-Security – Individual Challenges Scores

| | Topics |
|-----|--|
| (a) | Techniques and mechanisms to provide protection, assurance and integrity; |
| (b) | Robustness, resilience, survivability; |
| (c) | Criteria and standards to support policy governance; |
| (d) | Interoperability, and platform independence; |
| (e) | Virtualisation to support construction of complex concepts such as high-demand, critical services on otherwise limited technologies; |
| (f) | Security in environments with scarce resources; |
| (g) | Support for legal policies and requirements; |
| (h) | Tools and technologies to support design and construction of future trusted environments and networks. |

Commentary received in this area is set out below:

Cross-border and cross-sector Information sharing is the most important issue.

=====

What is missing here, is the notion of alternative security models. We should extensively study the possibility to complement protection through other operational security models, like disinformation, deterrence, etc.

When talking about legal policies and requirements, we might also want to mention economic factors and especially interests and concerns.

=====

Additional Topics:

In terms of interoperability, the seamless interoperability/integration of terrestrial and satellite networks shall also be addressed. Such interoperability shall be pursued at multiple levels: service, management, subscription handling, authentication and authorization, accounting/billing and networking levels.”

=====

I would have expected „self-healing“, robust in the sense of „forgiving, flexible“, mechanisms that detect security issues and overcome them themselves without human interaction....

=====

OK. Self-adaptation and adaptive security management could be added (together with robustness, resilience and survivability)

=====

All are important; a)-d) are essential. f) might be particularly challenging - security processing tends to be seen as an overhead so is often weak in resource-limited environments such as wireless sensor networks, etc. Possibly add a reference linking Trust to

Intrusion Detection Systems - if an intrusion is suspected but not proved to be an attack - should we fully trust that agent?

=====

Two topics need to be clarified. The first assurance. Assurance for what should be clarified. You can provide assurance of system integrity, the protection of personal information, the resilience of systems. Assurance needs to be placed into a context. Policy governance is a difficult term as well. Governance is a board and executive responsibility that is discharged in part through the development of policy. Policy is a governance tool.

=====

“As this is an area that has seem many wild, uncoordinated spending campaigns by governments lately, I feel that there should be a meta layer around the “engineering” that actually harnesses the engineers into reality, and “security” spending into obligations concerning their effectiveness. I’d like to suggest
 (I) Tools and methods for managing changing requirements, and properties of cyber security systems
 (K) Tools for monitoring the effectiveness of cyber security systems”

Commentary received on specific challenges:

(a) Techniques and mechanisms to provide protection, assurance and integrity;

Particularly assurance

=====

Not very clear; protection of ..., user assurance?, integrity of what?
 Better integrity of data in communication?

=====

(b) Robustness, resilience, survivability;

Should also be extended to clarify "of what and why" Cloud security is a major research topic with several facets e.g. compliance, privacy could also be added here.

=====

Do you mean techniques and mechanisms for (b) also? What about fraud, crime challenges to safeguard EU citizens? Maybe mention social networking technologies here as significant challenge for cyber-security?

=====

(c) Criteria and standards to support policy governance;

Measureable de-facto standards

=====

Liberty Alliance IGF

=====

(d) Interoperability, and platform independence;

May be demoted to last point as it is arguably not in general as directly-related as other points

=====

(e) Virtualisation to support construction of complex concepts such as high-demand, critical services on otherwise limited technologies;

Perhaps a mention of scalability here is needed

=====

(f) Security in environments with scarce resources;

Especially field devices, and even lower levels like sensors or actors

=====

(g) Support for legal policies and requirements;

As long as they are not contradictory

=====

Across multiple legal domains, else A (rather than D)

=====

Alignment of policies across Europe

=====

(h) Tools and technologies to support design and construction of future trusted environments and networks.

If it is built into the system, then it prevents a lot of problems later
on thru retro-fitting or having to re-invent parts of the system

=====

Engineering tools supporting security set-up

=====

Software Testing and Experimental testing could be added here

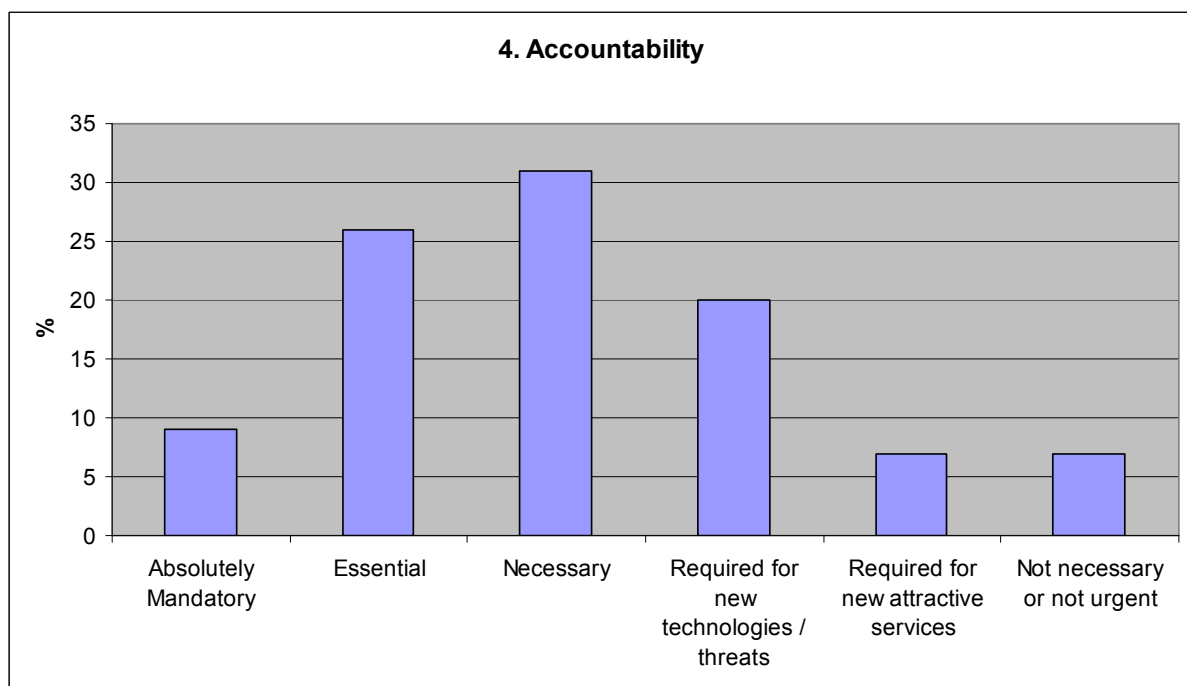
=====

3.4 Accountability

When the overall picture is considered, the challenges identified in D3.1b in the area of 'Accountability' were endorsed by the majority of respondents. Over 66% of the scores registered indicated that the identified topics were either 'absolutely mandatory' (9%), 'essential' (26%) or 'necessary' (31%). However, it is interesting to note that there are fewer 'absolutely mandatory' scores here when compared with other research areas in the questionnaire. It is also interesting that there is a comparatively higher level of scoring for 'required for new technologies/threats' (20%) and 'required for new attractive services' (7%).

A significant 6% of the scores considered any of the challenges identified to be either 'not necessary or not urgent'.

The graph below shows the combined scores registered in the area of Accountability:

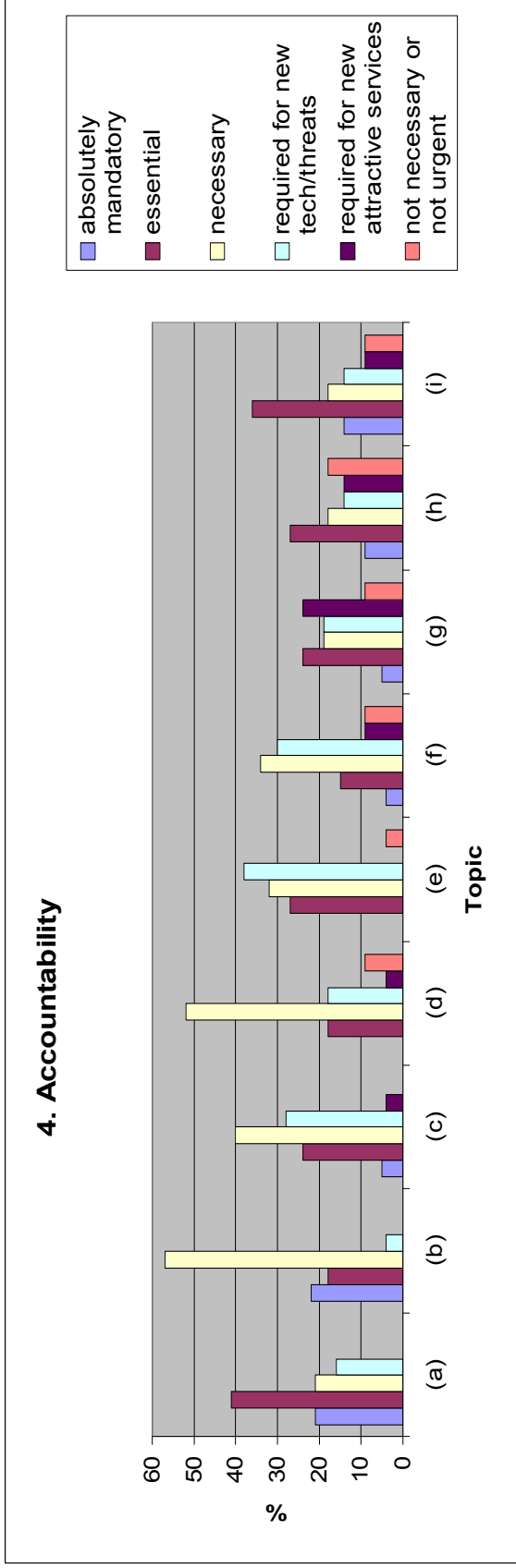


Graph 4.1 Accountability – Combined Scores

Turning to the **individual challenges** within the Accountability area, there are a number of interesting points emerging, as can be seen from graph 4.2 overleaf:-

- Challenges (g) '**Applicability to charging and payment**', (h) '**Anonymous/pseudonymous charging and payment systems**' and (i) '**Anonymisation or impersonation tools...**' attracted widely spread scoring. For example, 18% of scores for (h) indicating it is 'not necessary or not urgent'. This divergence of opinion is also somewhat reflected in the commentary received in this section.
- Challenges (a) '**Means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress**', (b) '**Interoperable, robust accountability framework: that balances privacy and traceability; that is economically feasible; that protects against non-repudiation but also against incorrect attribution**' and (c) '**Consistent interpretation of security policy agreements; appropriate standards**

for protocols and interfaces, and for tools to enable compliant usage' received very high levels of endorsement.



Graph 4.2 Accountability – Individual Challenges Scores

| | Topics |
|-----|--|
| (a) | Means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress; |
| (b) | Interoperable, robust accountability framework: that balances privacy and traceability; that is economically feasible; that protects against non-repudiation but also against incorrect attribution; |
| (c) | Consistent interpretation of security policy agreements; appropriate standards for protocols and interfaces, and for tools to enable compliant usage; |
| (d) | Traceability and accountability on global accountability-type principles; |
| (e) | Territorialisation of (trace/log) information; local domain policies and management; restricted 'sharing' only with authorised participating domains; |
| (f) | Real-time, large-scale test-beds to generate confidence; |
| (g) | Applicability to charging and payment; |
| (h) | Anonymous/pseudonymous charging and payment systems; |
| (i) | Anonymization or impersonation tools to produce untraceable, but trustworthy, valid sources/channels for eg, provision of economic, social, or health statistics. |

Commentary received in this area is set out below:

We are talking here about accountability in the sense of enabling technologies. We might also want to talk about what should not be possible regarding accountability, notably with respect to privacy.

We might want to promote a new drift to distributed systems, away from the current hype of centralized cloud-like platforms. Centralized platforms put too much power in the hands of their operators. One will not be able to effectively prohibit data mining. Anonymization has been shown to not work reliably when additional information is available from alternative sources.

=====

Again, for cloud environments:

- Responsibilities and liabilities in cloud environment
- Technical support for global (or at least EU-wide) register owner / privacy legislation

=====

Perhaps the challenges for accountability in Europe includes consensus across EU member states, agreed legal system in relation to cyber crime/activities, updated EU legislation
May also be pertinent to mention centralisation and the non-centralised approach to accountability

=====

Add a reference to federation of administrative domains. Each domain will have its own accountability, but end-to-end communication implies federation and hence management of trust relationships at a higher level.

=====

I couldn't agree more!

I imagine e-voting, whistle-blowing, and anonymous participation in the political process (observation / consuming of information and the press) as further "Other areas related to accountability". However, I recommend to focus slightly more on the data minimalization principles in data protection frameworks, e.g. regarding personal Internet media delivery with Watermarks and

policies. Normally, there should be no need to attach a personal identifier to a piece of MP3 music, if there are other ways to manage obligations.

Commentary received on specific challenges:

(a) Means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress;

Not on the internet in general. Maybe in federations or communities. If you mean user-controlled privacy, it is very important.

=====

(b) Interoperable, robust accountability framework: that balances privacy and traceability; that is economically feasible; that protects against non-repudiation but also against incorrect attribution;

=====

(c) Consistent interpretation of security policy agreements; appropriate standards for protocols and interfaces, and for tools to enable compliant usage;

How do you ensure consistent interpretations?

=====

Seems complex - is the first part targeting technology or policy in the wider sense? the remainder of the sentence refers to technology. I strongly believe in the first part being a very high priority challenge but less for technology though.

=====

(d) Traceability and accountability on global accountancy-type principles;

Already required in energy automation

=====

Who is going to do that?

=====

(e) Territorialisation of (trace/log) information; local domain policies and management; restricted 'sharing' only with authorised participating domains;

I understand it as marking data with localisation info. See geo-trust

=====

Include having flexibility to determine the domain (who is in it? And what resources it contains?)

=====

(f) Real-time, large-scale test-beds to generate confidence;

Why only test-beds?

=====

Accountability is hierarchical and non-real-time

=====

Perhaps this line is a bit to general

=====

(g) Applicability to charging and payment;

Billing is a huge area which has many of its own security issues!

=====

(h) Anonymous/pseudonymous charging and payment systems;

Hasn't that already been sorted out?

=====

Maybe look @ ONE Project"

=====

(i) Anonymization or impersonation tools to produce untraceable, but trustworthy, valid sources/channels for eg, provision of economic, social, or health statistics.

Research is increasingly indicating that anonymisation / impersonation is not effective at obscuring an individual

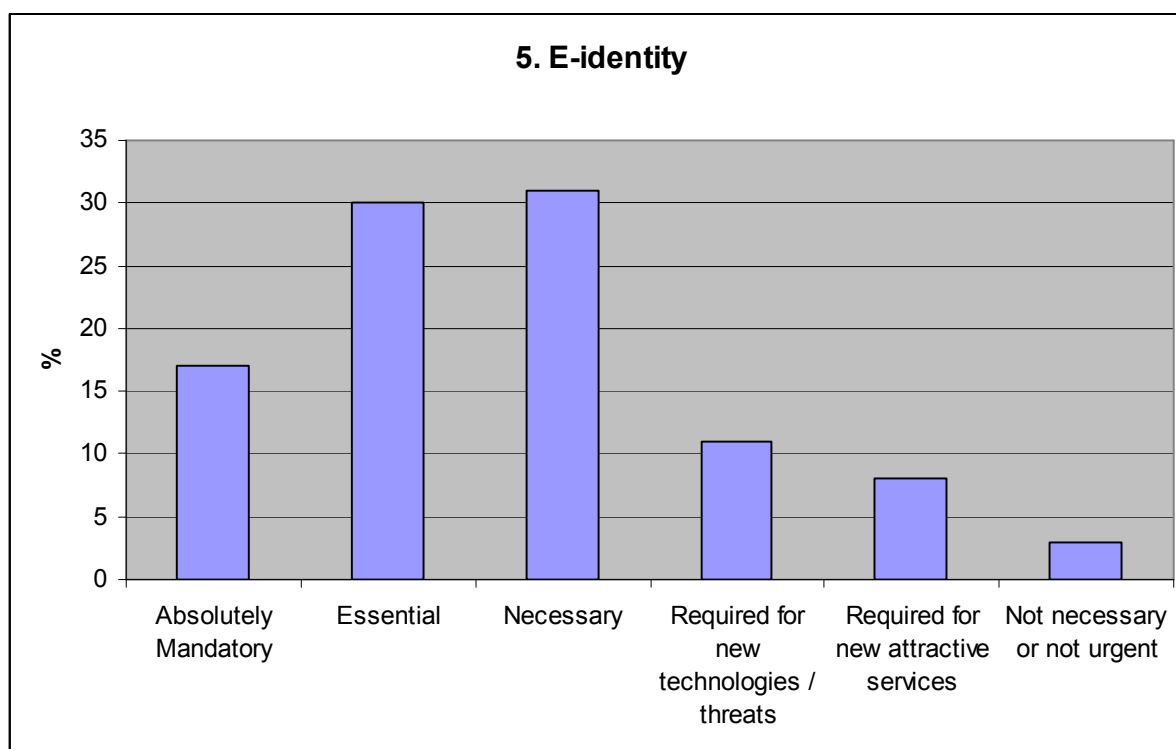
=====

3.5 E-identity

When the overall picture is considered, the challenges identified in D3.1b in the area of 'E-identity' were endorsed by the majority of respondents. 78% of the scores registered indicated that the identified topics were either 'absolutely mandatory' (17%), 'essential' (30%) or 'necessary' (31%).

However, it is noticeable that the responses are more evenly spread across each category, than in other areas of the questionnaire. In particular, there are substantial 'required for new technologies/threats' scores (11%) and 'required for new attractive services' (8%).

The graph below shows the combined scores registered in the area of e-identity:

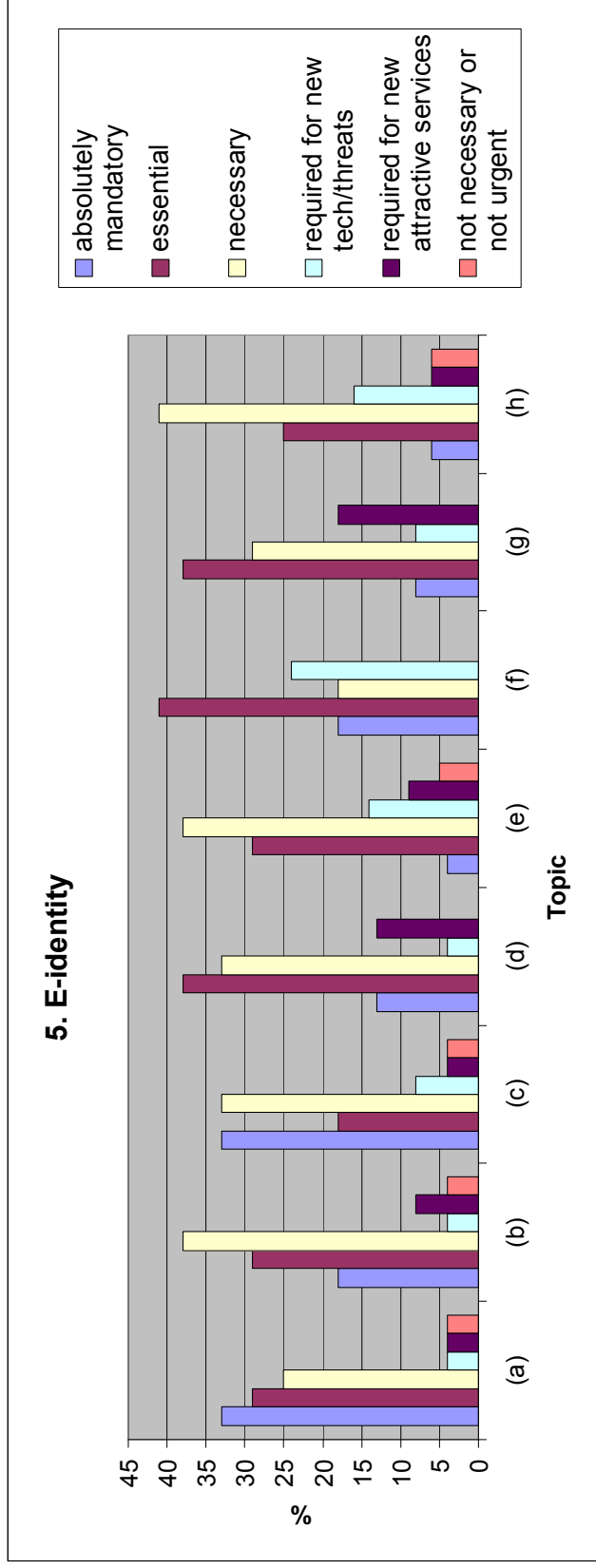


Graph 5.1 E-identity – Combined Scores

Turning to the **individual challenges** within the E-identity area, there are a number of interesting points emerging, as can be seen from graph 5.2 overleaf:-

- Challenge **(a)** '**Common EU framework for identity and authentication**' received high levels of endorsement, with 87% of responses indicating it is either 'absolutely mandatory', 'essential' or 'necessary'.
- When compared with other areas of the survey, it is interesting to note that challenges **(e)** '**Standardised linkages to related and dependent concepts (accountability, access-control, etc.)**' and **(h)** '**Communication setup and routing that are identity-data-aware only as necessary for network functions, without making the related users identifiable or traceable**' received relatively high 'not necessary or not urgent' scores, with **(e)** registering 5% and **(h)** registering 6%.
- It also interesting to note that challenge **(f)** '**Claim-based approaches using novel and existing cryptographic protocols to eventually avoid ID architectures with a centralised components that**

everyone needs to trust received a relatively high (24%) level of 'required for new technologies/threats' scores.



Graph 5.2 E-identity – Individual Challenges Scores

| | Topics |
|-----|---|
| (a) | Common EU framework for identity and authentication |
| (b) | Interoperability of/with alternative (and current) ID schemes |
| (c) | Flexibility of choice of identity and ID-protection options/choices, including partial IDs and anonymity when appropriate |
| (d) | Life-cycle management of IDs, with protection recovery from loss or failure |
| (e) | Standardised linkages to related and dependent concepts (accountability, access-control, etc.) |
| (f) | Claim-based approaches using novel and existing cryptographic protocols to eventually avoid ID architectures with a centralised components that everyone needs to trust |
| (g) | Technology to support new business models for central, decentralised, and claim-based approaches |
| (h) | Communication setup and routing that are identity-data-aware only as necessary for network functions, without making the related users identifiable or traceable |

Commentary received in this area is set out below:

A common worldwide framework for privacy-preserving easy-to-use strong identity management seems to us to be the main research challenge.

=====

Additional Topics:

See point above for seamless interoperability between terrestrial and satellite networks to be addressed at multiple levels.

=====

Agreed. Although I still don't understand what a „common EU framework“ will actually leverage. Federation and interoperability technology is available - what is this more? Governance to enforcing it? But then this is not a technology challenge...

So personally I would skip (a) and (b), and push (a) in the policy debate.

=====

Additions:

- Adaptive authentication and authorization based on authentication strength / levels of assurance of authentication mechanisms
- Quantification of identity management

=====

In the Internet of Services advanced and user controlled (or user centric) identity delegation mechanisms are required so that back end services can operate on end-user behalf therefore assuring correct use of resources, accountability, etc.

Of course identity delegation mechanisms have to comply with privacy, anonymity, etc.

=====

All important. This impinges directly upon EU citizens - so should be a source of future case studies. Phishing (misrepresentation) leading to identity theft is directly related to Trust issues

=====

This area is highly relevant for the near and distant future. I suggest to add:

(i) Inclusive Identity Management for a lifetime.

- E-inclusion of special needs groups that will have difficulties with certain ID technologies.
- Development of a multi-channel strategy where a whole portfolio of ID technologies can replace each other in case of changing capabilities of a citizen over lifetime (or the technological out-phasing of an outdated technology)
- Development of a methodology to ensure equal security, trust and privacy levels of alternative ID channels.

(h) Redundancy and lock-in prevention.

- Recently, banks in Germany were very lucky that their bank cards still carried magnetic strips, after the smartcard chip had a serious problem with the year 2010. The banks were able to reprogram the terminals to use the strip.

Without this option, a complete disruption of card payment and terminal self-service had been the consequence.

- ID systems should be developed, deployed, operated and supervised to ensure “backup” strategies and redundancies are available that don’t compromise trust and security.

Commentary received on specific challenges:

(a) Common EU framework for identity and authentication;
 STORK project is in progress

=====

Should be orientated on existing schemes, but not rely on non-trustworthy, non-EU providers (Google)

=====

I thought this a) and b) were already en route? Do not we have a go for a European eID?”

=====

This would require a whole standardisation & Certification stage

=====

(b) Interoperability of/with alternative (and current) ID schemes;

Federated ID schemes?

=====

(c) Flexibility of choice of identity and ID-protection options/choices, including partial IDs and anonymity when appropriate;

User centric identity. Beware: user should know what they are doing – acceptance and transparency key. E.g. we noticed that user didn't like the CardSpace business card metaphor and rather preferred a simple web page to monitor and consent the exchange of identity information.

=====

I am assuming within the common framework.

=====

Mandatory for acceptance - and it has to be understood that different types of transactions and interactions require different levels of trust, security, ID...

=====

Let the individual people data subjects decide

=====

(d) Life-cycle management of IDs, with protection recovery from loss or failure;

(de)provisioning of ID in federated environments in not trivial and probably unsolvable.

=====

Per session?

=====

(e) Standardised linkages to related and dependent concepts (accountability, access-control, etc.);

Don't invent anything which doesn't support an "embrace and extend" approach

=====

(f) Claim-based approaches using novel and existing cryptographic protocols to eventually avoid ID architectures with a centralised components that everyone needs to trust;

Depends on the setting. In a federation this might work. Trust can be centralised while the architecture itself is decentralised. Important to know who is regulating the system: market or government?

=====

Important to understand "claim" in a broad term to avoid a limitation to Microsoft-driven (valid!) approaches which might become sort of a "political" issue

=====

(g) Technology to support new business models for central, decentralised, and claim-based approaches;

Indeed, who is paying the identity provider for authenticating the user; who will pay for the rollout of user identities, and how much will they pay/charge?

=====

(h) Communication setup and routing that are identity-data-aware only as necessary for network functions, without making the related users identifiable or traceable

Is an issue in e.g. e-invoicing: knowing where to send the e-invoice to in a landscape that is crowded with Billing Service Providers and clouded with regulation is not trivial.

=====

Regulation, legislation in relation to e-identity - without making the related users identifiable or traceable – unless required under legislation? Maybe mention issue/challenges of multiple identities – social, personal, professional

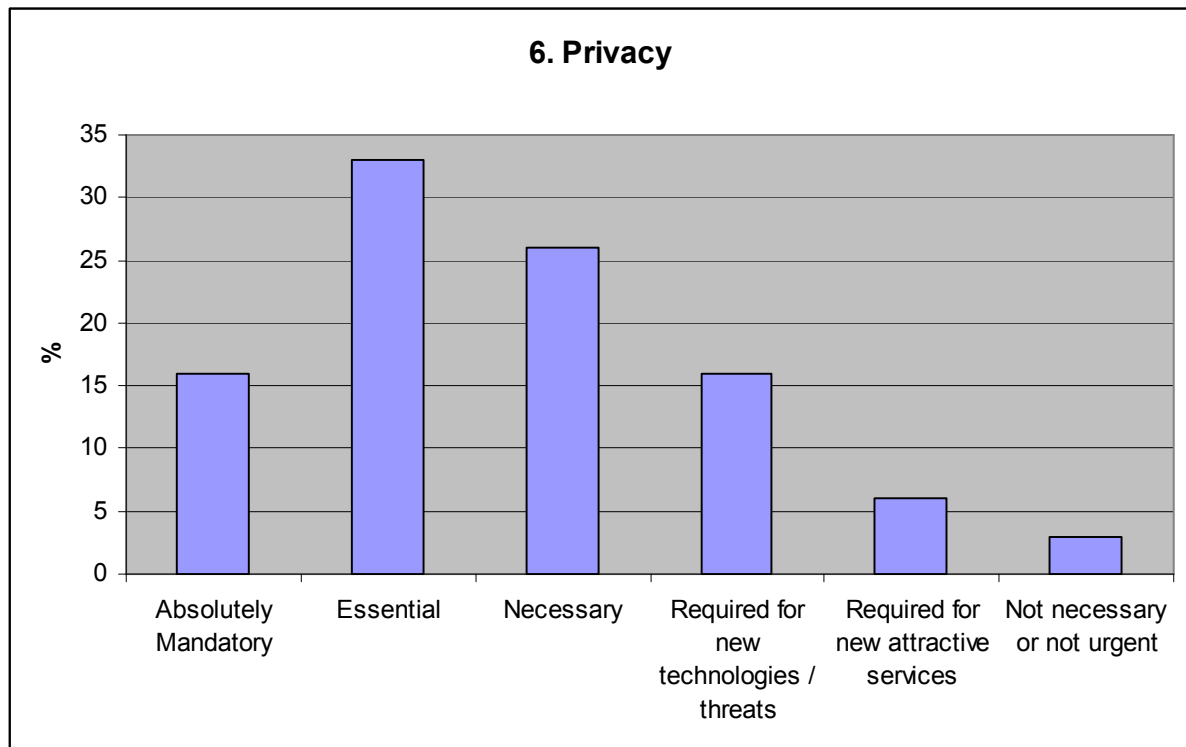
Cross check with PICOs, PRIMELIFE recommendations? Identity management in cloud computing?

=====

3.6 Privacy

When the overall picture is considered, the challenges identified in D3.1b in the area of 'Privacy' received a very strong endorsement in the survey, with one of the challenges receiving 100% scores of 'absolutely mandatory', 'essential' or 'necessary'. Overall, 75% of the scores registered indicated that the identified topics were either 'absolutely mandatory' (16%), 'essential' (33%) or 'necessary' (26%).

The graph below shows the combined scores registered in the area of privacy:

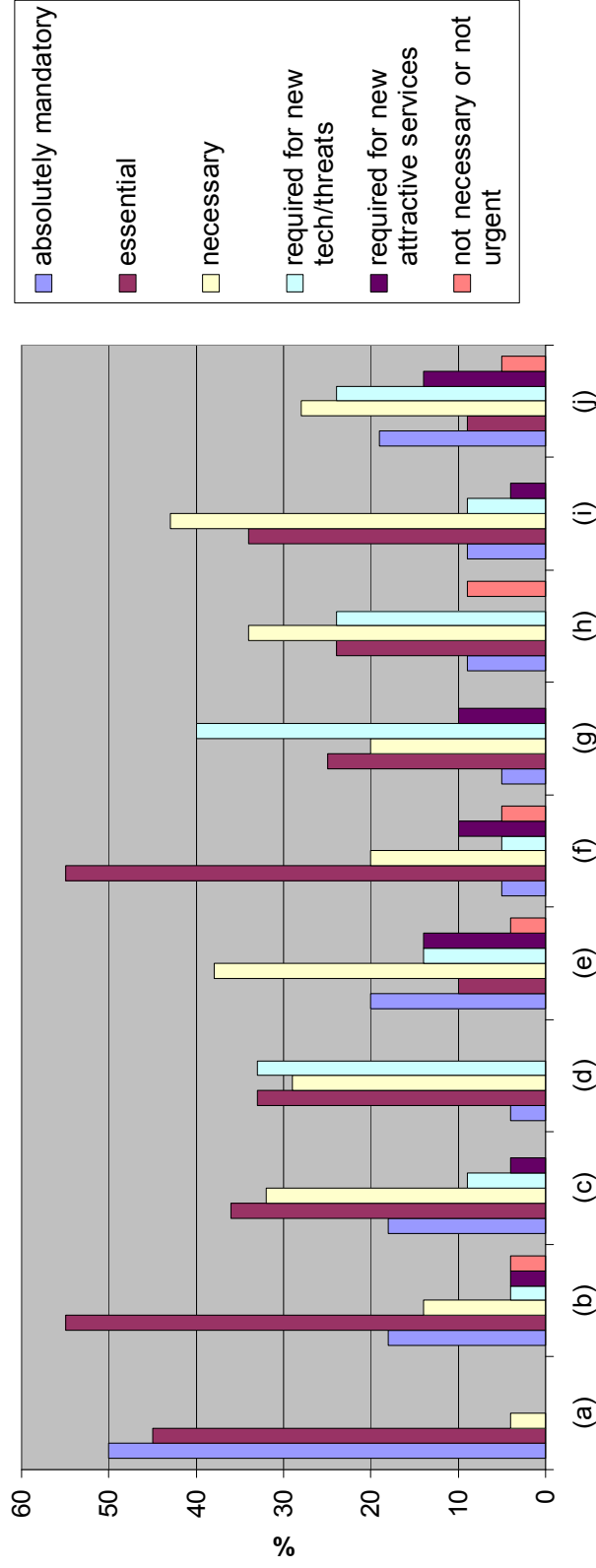


Graph 6.1 Privacy – Combined Scores

Turning to the **individual challenges** within the Privacy area, there are a number of interesting points emerging, as can be seen from graph 6.2 overleaf:-

- Challenge (a) '**Minimisation of unintended acquisition of personal and other sensitive information**' was the first challenge in the questionnaire where all respondents indicated that it was either 'absolutely mandatory', 'essential' or 'necessary', with a substantial 95% considering it to be either 'absolutely mandatory' or 'essential'.
- Challenges (b) '**Fine granularity access control to identity-related information**' and (f) '**Possibility to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates**' received very high 'essential' scores, (both 55%).
- Challenge (h) '**Use and control of identity-related information for network (e.g. routing) purposes without compromising privacy**' received a significant 9% score in the 'not necessary or not urgent' category.

6. Privacy



Graph 6.2 Privacy – Individual Challenges Scores

| Topics | |
|--------|---|
| (a) | Minimisation of unintended acquisition of personal and other sensitive information |
| (b) | Fine granularity access control to identity-related information |
| (c) | Further development of Privacy Enhancing Technologies (PETs); tools to check privacy assurance and tools to advance transparency regarding used data |
| (d) | Use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users |
| (e) | Methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, including revocation/retraction |

| | |
|-----|--|
| (f) | Possibility to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates |
| (g) | Personal/communal collector of personal garbage/litter (or timed auto-self-destruct) |
| (h) | Use and control of identity-related information for network (e.g. routing) purposes without compromising privacy (see 5(h), above) |
| (i) | Standardised techniques to assure privacy across the various internet layers, through to network level and maintaining consistent privacy across different environments |
| (j) | Tools and concepts for deleting data in the internet (“forgetting”) – see (g), above |

Commentary received in this area is set out below:

What about a fully homomorphic encryption as a way to treat/act on encrypted data? Does this have any future/real impact? This approach also has some limits (who has registered this data? Who has asked for its submission? Who can access it? Etc.) Should this be studied in details?

Data possession proofs might be an interesting topic in this area. Instead of handing out data, we might want to look into technologies providing proofs of data possession. A related but fairly well understood area are ZK proofs.

Deleting data in the Internet is suggestive. What matters is that data be lost after some specified period. This however does not imply that it needs to be deleted. It can also vanish, become incomplete/undecodable, we could lose keys to it, etc.

=====

Privacy should be taken into account in trust solutions.

=====

Reputation management sets new issues on privacy.

=====

Again, for cloud environments (same as in Accountability):

- Responsibilities and liabilities in cloud environment
- Technical support for global (or at least EU-wide) register owner / privacy legislation

=====

Forensic tools and their ability to evade privacy
Awareness/education for citizens

=====

Links between Privacy and Trust are not as strong as those between Identity and Trust. Thus this section is less important than others in respect of Trust - though still important in its own right....

=====

Since privacy is so critical and the experience of breaches somewhat common this section may need to address monitoring and response requirements

=====

This should be put in the context of identity hiding - I am quite happy that data can be generated as a cause of my action, but not related back to me.

=====

The headline of this area should be “Privacy technology”. If you actually meant “Privacy” in all its flavours, then I’d suggest to add:

1. The transformation of the OECD privacy principles (the basis of many of today’s data protection laws) from the computing paradigm of the 1970ies to the distributed world of mobile, distributed services and company mergers.
2. The inclusion of full data processor liability for privacy infringements.
3. The development of mandatory auditing and certification schemes.

In addition, I believe that the connection between “privacy” and “identity” is not included strong enough. The linking with a person, its identifiers and its identity create most of the privacy risks. Concerning electronic identities and identifiers, it is crucial to:

1. Support authority over the creation, certification and use of identities (e.g., who will be allowed to name-tag a person on Facebook by using their identifier). Authority concepts could be all from centralized PKI to self-established PGP/OpenID schemes with user side authority over identifiers.
2. Restrict function creep of identifiers (social security numbers were not meant as ID numbers, e-mail-addresses with their vulnerability for spam were not meant to be “login names” for Facebook).
3. Research ways of providing transactions and managing relationships based on short-lived data, and short-lived identifiers;
4. Support users in managing their personal crowd of identifiers and the purposes they are used for.

Concerning (j), I think that a deletion tool will be useful only after a detection tool has actually found a bit of personal information that shouldn't be there. Hence, I suggest a

* Framework for the management and detection of personal information in the internet of services and the internet of things. I imagine user-side DRM techniques to mark released data objects, registries analogue to patent and art registries used to generate evidence, and regulation of search engines and on-line archives that collect internet information (e.g. to generate personal reports, process watermarks to support privacy,) . All these mechanisms would support the detection and the containment of personal information that is "out there".

Commentary received on specific challenges:

(a) Minimisation of unintended acquisition of personal and other sensitive information;

Minimisation is not strong enough
=====

I'm not actually sure how important this is to the individual citizen
=====

Would be great
=====

An EU law already exists for this??
=====

(b) Fine granularity access control to identity-related information;

This 1st requires the definition of private or sensitive information
=====

In industry, roles are used
=====

Who is going to control or manage that?
=====

We have to fundamentally think about this – I've suggested at the MISC conference in London to think about applying approaches derived from Information Rights Management at the attribute level

which would require some fundamental changes but is most likely the only way to do it – would be definitively worth a research project to further evaluate

=====

This should be already built into the above?

Perhaps you are missing an important point on the whole privacy challenge – the Education of Users should not only be mentioned but should be high on the list (In our opinion!!)

=====

(c) Further development of Privacy Enhancing Technologies (PETs); tools to check privacy assurance and tools to advance transparency regarding used data;

Tools (and standards) that make transparent and more intuitive/understandable what data (and to who) we provide when accessing services (even simply using our browsers) are urgent to actually preserve our privacy

=====

(d) Use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users;

Related to identity (de) provisioning. Move from push to pull mechanisms.

=====

(e) Methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, including revocation/retraction;

We are working on this user-controlled privacy, but how to collect the consents is not trivial

=====

There was a study on privacy agreements (maybe by PEW) - time it would take an average American to read all agreements that he came across in his lifetime - it was a rather large number, this could relate to (e).

=====

(f) Possibility to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates;

Controlled by whom? Essential - yes. Feasible - Bruce Schneier says no. I tend to share his opinion.

=====

(g) Personal/communal collector of personal garbage/litter (or timed auto-self-destruct);

RFID scrambler

=====

(h) Use and control of identity-related information for network (e.g. routing) purposes without compromising privacy;

=====

(i) Standardised techniques to assure privacy across the various internet layers, through to network level and maintaining consistent privacy across different environments;

=====

(j) Tools and concepts for deleting data in the internet ("forgetting");

This is just impossible as there is no clear-cut boundary to the Internet

=====

Refers to "personal" data."

=====

Should be prioritised, the early internet generation and even today the concept of a personal footprint on the internet is almost non-existent, careless use is common place. Does this however stand in contrast to accountability? Maybe a topic covering the weighting and effects of the different technologies/concepts should be high on the agenda too?

Or a public education might also do the trick?"

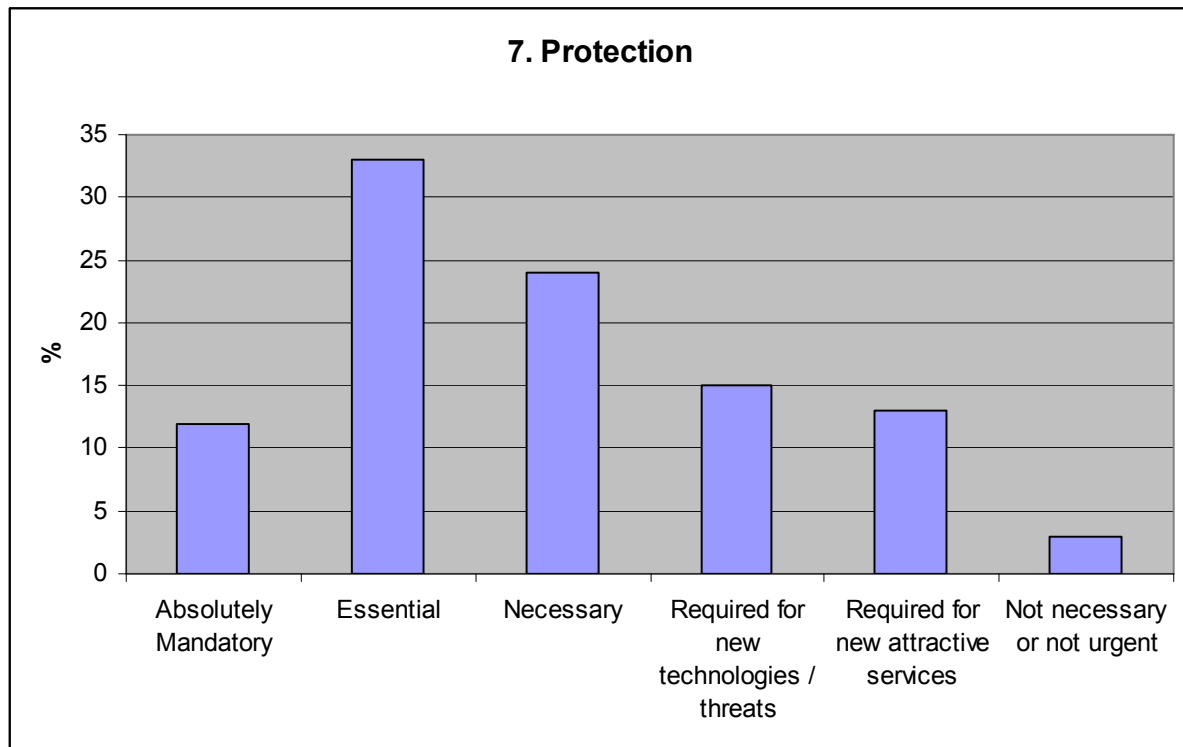
=====

3.7 Protection

When the overall picture is considered, the challenges identified in D3.1b in the area of ‘Cyber-Security’ were endorsed by the vast majority of respondents. Over 69% of the scores registered indicated that the identified topics were either ‘absolutely mandatory’ (12%), ‘essential’ (33%) or ‘necessary’ (24%).

3% of the scores considered any of the challenges identified to be either ‘not necessary or not urgent’.

The graph below shows the combined scores registered in the area of protection:

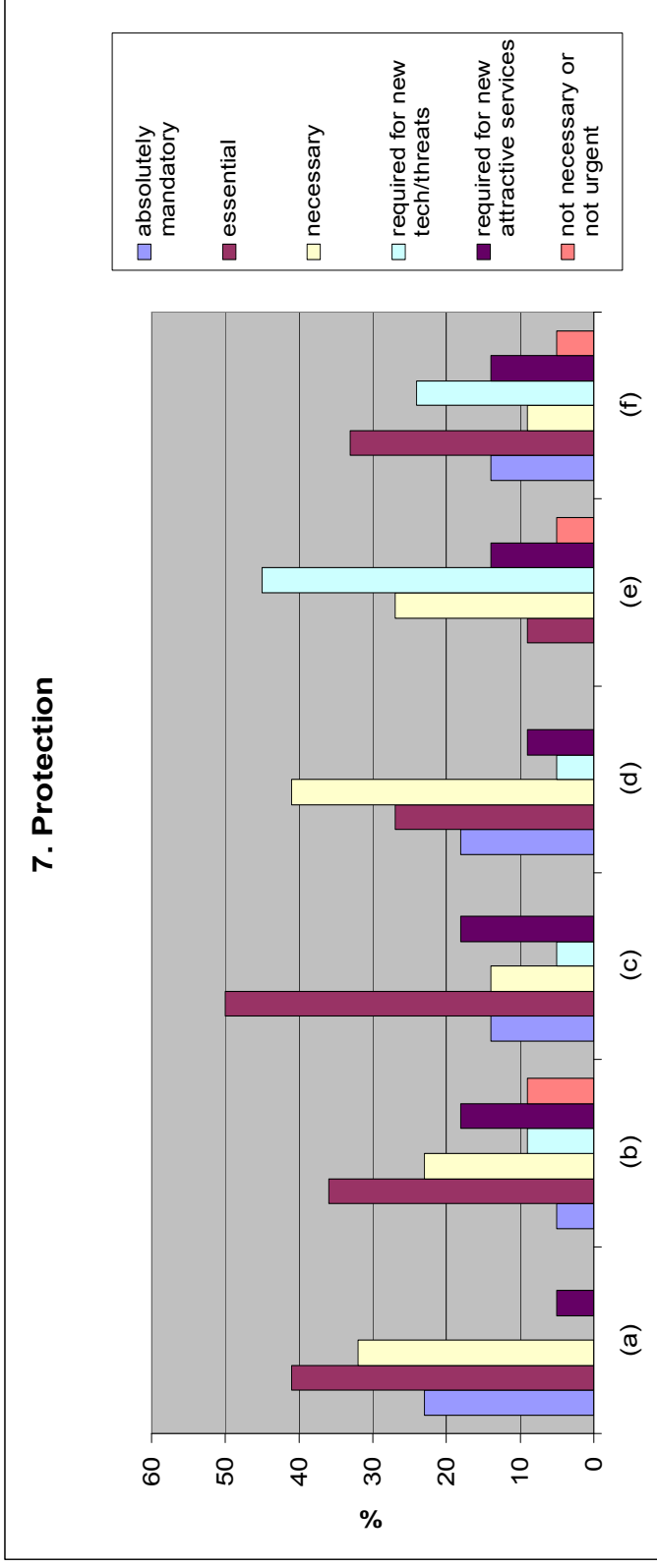


Graph 7.1 Protection – Combined Scores

Turning to the **individual challenges** within the Protection area, there are a number of interesting points emerging, as can be seen from graph 7.2 overleaf:-

- Challenge (e) **‘New cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age’** received a score of 45% in the category of ‘required for new technologies/threats’.
- Challenge (c) **‘Fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc.’** received a combined score of 64% for ‘absolutely mandatory’ (14%) and ‘essential’ (50%).

7. Protection



Graph 7.2 Protection – Individual Challenges Scores

| | Topics |
|-----|---|
| (a) | Protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications) |
| (b) | Domains, partitioning, compartmentalisation, fire-breaks –leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage |
| (c) | Fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc |
| (d) | Mutual authentication, with multiple devices (ideally, technology invariant) |
| (e) | New cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age |
| (f) | Uses of eID and its components in protecting the interests of its subject (data protection, etc.) |

Commentary received in this area is set out below:

“Privacy protection should be taken into account in trust solutions.

=====

“Additional Topics:
 Protection of society ALWAYS and ANYTIME shall also be addressed. In this regard, the key role of Satellite Networks with respect to their ubiquitous access capabilities as well as their dependability capabilities to assist society even in emergency scenarios (e.g., floods, earthquakes, fires, etc) shall also be addressed.”

=====

Agreed - though I would emphasize the „semi-trusted zones“ idea and expand on this. This has a number of consequences also related to trust management. Today’s trust management (and also to some extent as treated in 1)) is binary: there is trust or there isn’t. A more fine-grained, claim-based trust model allowing for semi-trusted zones depending on attributes, parameters alike is critical. Maybe a good idea is to move this topic into „trust management“ ???

=====

Very important - particularly in respect of mitigation of risks. Good strategies are listed above.

=====

If this area is related to privacy, then there should be mention of:

- Mechanisms that support audits
- Mechanisms that support management of obligations/policies in a long-term perspective

=====

Commentary received on specific challenges:

(a) Protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications);

Focus should be on integration. Most approaches today are either looking for data at rest, in transit or in use, but not at all stages. A project which focuses on how to do this in an integrated manner might improve the competitive position of European vendors.

=====

(b) Domains, partitioning, compartmentalisation, fire-breaks – leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage

=====

(c) Fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc;

In energy automation, access control based on roles is currently being pushed - manageable access control

=====

Multiple attributes instead of bases. I recommend using "security" instead of "protection".

=====

Has relationships with comment in the "Architecture" sections.

=====

Related to (c) quantification of access control, and its relation to authentication"

=====

(d) Mutual authentication, with multiple devices (ideally, technology invariant);

Very important and is currently quite disregarded

=====

End-users increasingly require confidence in the identity of their counterparts

=====

(e) New cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age;

Not urgent in 1-3 years

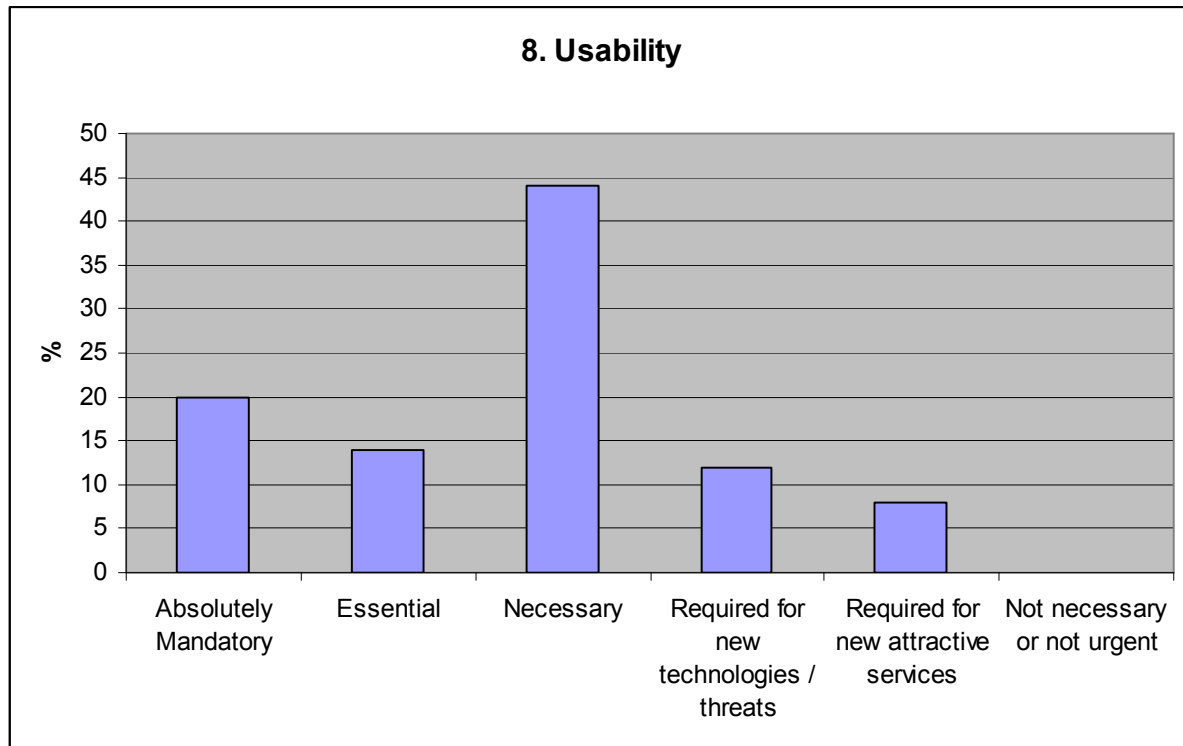
=====

(f) Uses of eID and its components in protecting the interests of its subject (data protection, etc.)
=====

3.8 Usability

Responses received in this area are noteworthy in that only 0.1% of replies considered 'usability' to be 'not necessary or not urgent'. Overall, 78% considered usability to be 'absolutely mandatory' (20%), 'essential' (14%) or 'necessary' (44%).

The graph below shows the combined scores registered in the area of usability:

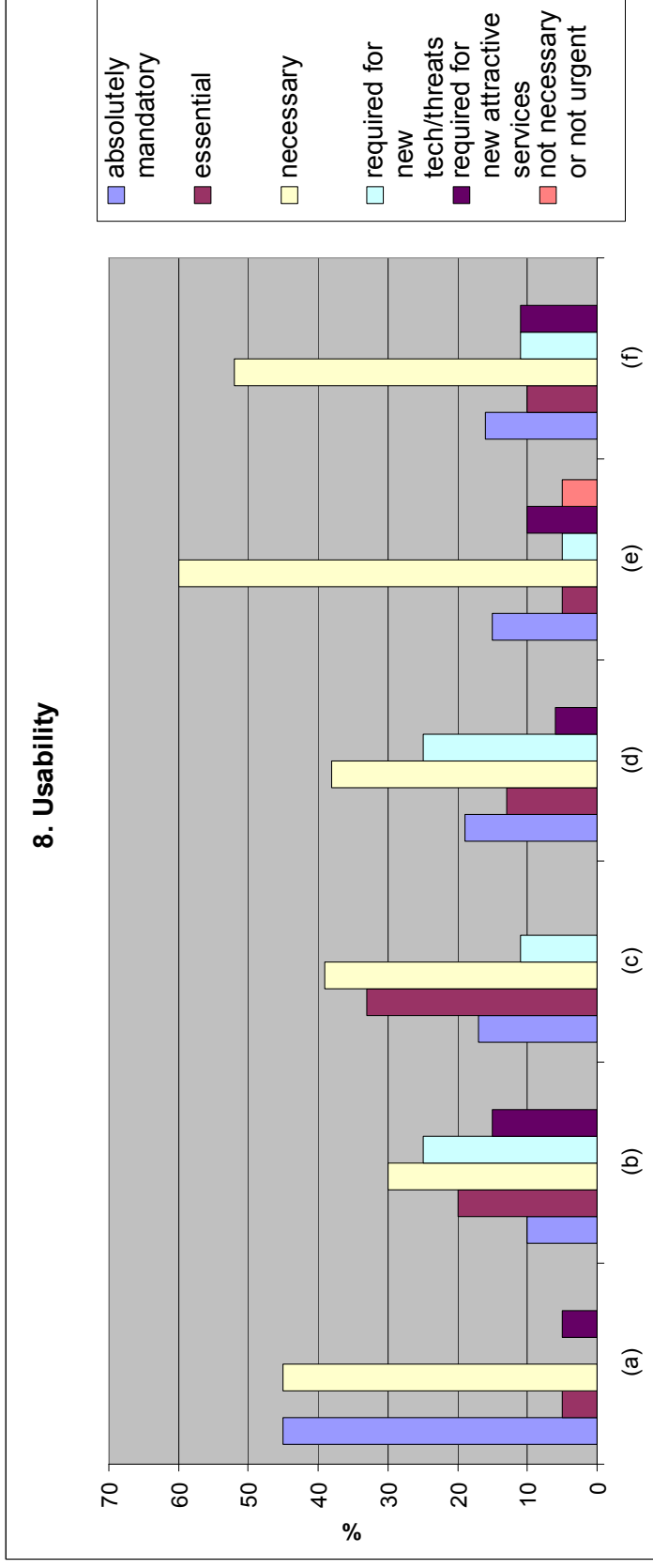


Graph 8.1 Usability – Combined Scores

Turning to the **individual challenges** within the Usability area, there are a number of interesting points emerging, as can be seen from graph 8.2 overleaf:-

- Five of the six challenges in this area registered no 'not necessary or not urgent' scores. Only **(e) 'Attention to user/system interaction: sympathetic user interfaces, but with advanced options'** received scores in this category, while challenge (a) 'Support for the individual user (user-centricity)' received a high level of 'absolutely mandatory' scores (43%).
- It is also interesting to note that each challenge has very high 'necessary' scores: **(a) 'Support for the individual user (user-centricity)'** - 44%; **(b) 'Environment can adapt to user choice as well as presenting auto-configurations based on assumptions and profiles, depending on levels of (user) trust (of environment)'** - 30%; **(c) 'What does the user want or need by way of security and trust facilities and functionality? (including non-technical, human aspects) - how is this delivered'** - 38%; **(d) 'What are the impacts and implications for the underlying mechanisms and functionality'** - 37%; **(e) 'Attention to user/system interaction: sympathetic user interfaces, but with advanced options'** - 60%; **(f) 'Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; this may include decision support, recommended options, and the capturing of user preferences (profile)'** - 53%.

8. Usability



Graph 8.2 Usability – Individual Challenges Scores

| | Topics |
|-----|---|
| (a) | Support for the individual user (user-centricity) |
| (b) | Environment can adapt to user choice as well as presenting auto-configurations based on assumptions and profiles, depending on levels of (user trust (of environment) |
| (c) | What does the user want or need by way of security and trust facilities and functionality? (including non-technical, human aspects) - how is this delivered |
| (d) | What are the impacts and implications for the underlying mechanisms and functionality |
| (e) | Attention to user/system interaction: sympathetic user interfaces, but with advanced options |
| (f) | Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; this may include decision support, recommended options, and the capturing of user preferences (profile). |

Commentary received in this area is set out below:

We might want to study usability more specifically bound to the trust, assurance, ID management and privacy instruments mentioned before. These need per se comprehensible and well-balanced user interfaces

=====

Usability of trust and security solutions is a main research challenge.

=====

The topics represent high level research challenges. Can also add topic "Tools and methodologies for user development of software and services".

Topic (e) is traditional area that is already extensively researched and developed unless it refers to specific aspect that is not yet tackled.

=====

Ok. (not 100% convincing why to put money there).

=====

Usability of security and privacy mechanisms at end-user's responsibility!

=====

All are important to ensure user buy-in.

=====

Please read "Nudge" by Thaler and Sunstein on human economic behaviour. The most interesting point is the status quo. If there are default settings they will most likely stay... comment due to the term advanced options and choices - this is not always good.

=====

In addition, research should shift focus away from "forcing" users to understand a single security or ID technology into research about a

“portfolio” or multiple channels of equivalent security techniques that offer choice to users (blind ones, dement ones, ones with no fingers, people that get older...)”

Commentary received on specific challenges:

(a) Support for the individual user (user-centricity);
 We shouldn't over-estimate the capability of an average user to act user-centric and education project should be part of this
 =====
 Give control and responsibility
 =====
 Perimeter proposes a new paradigm for user centricity. Maybe mention this area should be user driven with the living labs taken into account
 =====

(b) Environment can adapt to user choice as well as presenting auto-configurations based on assumptions and profiles, depending on levels of (user) trust (of environment);
 Needs a focus on privacy, as profiling and adaption will inevitably collect personal, medical profiles of special needs users. In addition, there might be severe abuse potential with respect to impulse shopping, price discrimination, and online fraud.
 =====

(c) What does the user want or need by way of security and trust facilities and functionality? (including non-technical, human aspects) - how is this delivered?
 In a user-friendly manner
 =====

(d) What are the impacts and implications for the underlying mechanisms and functionality?
 =====

(e) Attention to user/system interaction: sympathetic user interfaces, but with advanced options;

This is best left to vendors and the evolution of their products instead of doing it in a project

=====

Take context into account. For example, when can I bother the user with a consent question?

=====

(f) Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; this may include decision support, recommended options, and the capturing of user preferences (profile).

Learning systems

=====

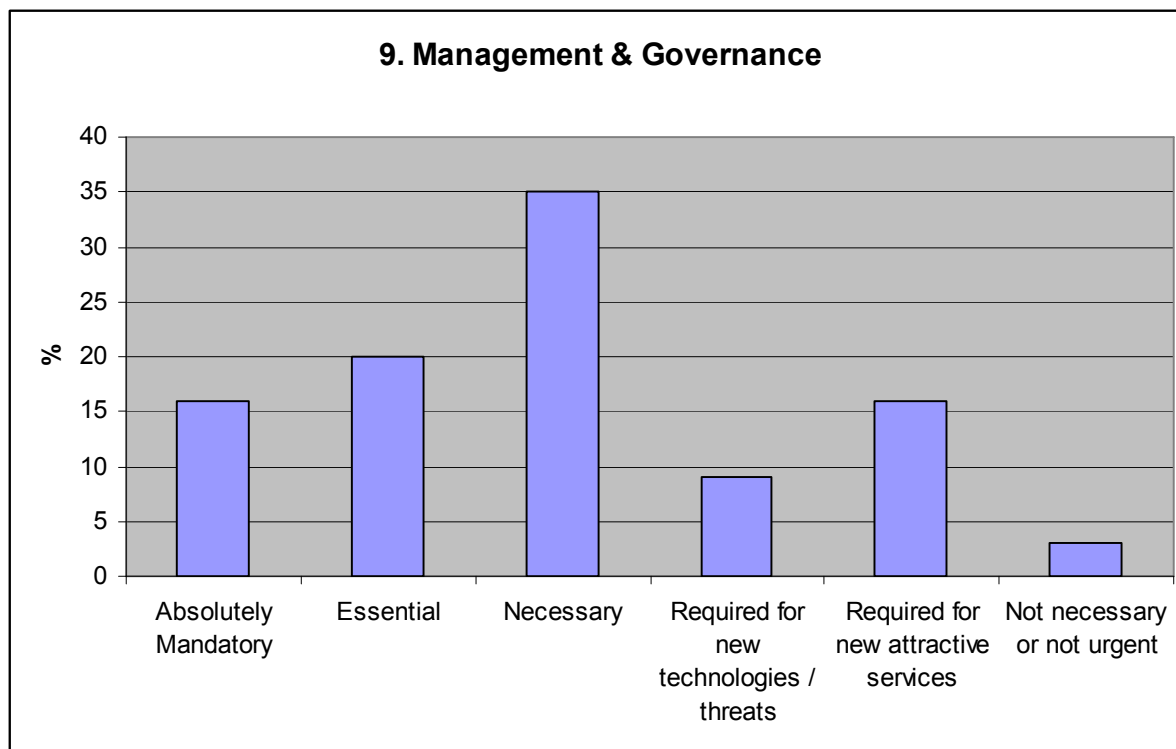
Reads a little misleading. It sounds like users are too stupid to use security "right". I believe that users don't want to spend their time managing security, but rather understand security/risk as it is presented by a system, and then adapt their behaviour. This is a very difficult topic, which is related to transactions, server- and service side policies, regulation, liability and market competition. I think that the sustainability of business processes based on tools and technologies to earn and keep user trust, quality perception, and risk balanced, might be an alternative to (f).

=====

3.9 Management & Governance

Over 70% of the scores registered indicated that the identified topics were either 'absolutely mandatory' (16%), 'essential' (20%) or 'necessary' (35%).

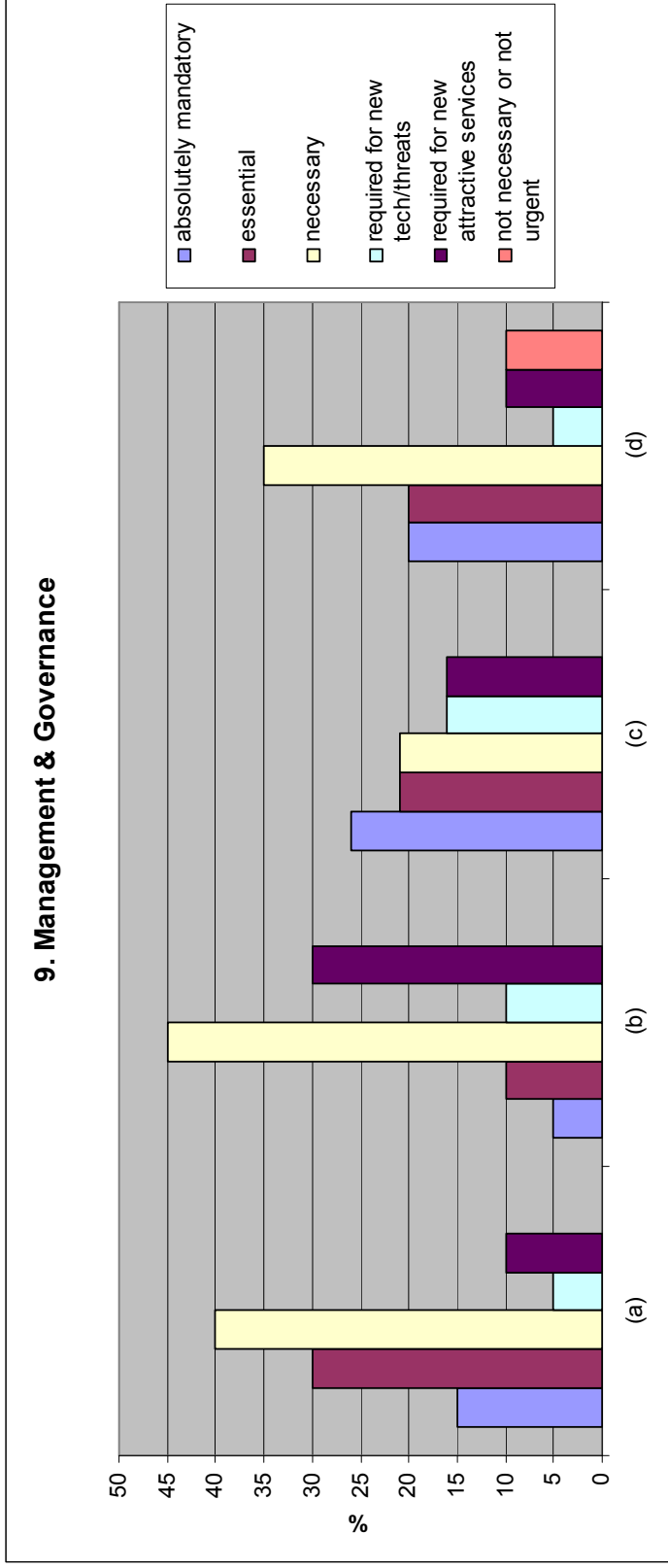
The graph below shows the combined scores registered in the area of management and governance:



Graph 9.1 Management and Governance – Combined Scores

Turning to the **individual challenges** within the Management and Governance area, there are a number of interesting points emerging, as can be seen from graph 9.2 overleaf:-

- Challenges (c) **'Technical support for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions; at a simpler level, the regulatory aspects to support the interoperability of security policies are necessary: from civil law for individuals and society, and contract law for business, to common law and the support of small claims'** and (d) **'The relationships between eIDs and Government (.gov) must be given special attention – registrations, births, marriages, deaths, etc.'** appear to have attracted evenly spread scores, with (d) in particular receiving a score of 10% for 'not necessary or not urgent'.
- Challenge (d) is also noteworthy for the fact that it is the only category to receive a 'not necessary or not urgent' score (10%).
- Challenges (a) **'Framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs'** and (b) **'Investigation of economic feasibility and possible alternatives'** have quite high 'necessary' scores, (40% and 45%, respectively).



Graph 9.2 Management and Governance – Individual Challenges Scores

| | Topics |
|-----|---|
| (a) | Framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs |
| (b) | Investigation of economic feasibility and possible alternatives |
| (c) | Technical support for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions; at a simpler level, the regulatory aspects to support the interoperability of security policies are necessary: from civil law for individuals and society, and contract law for business, to common law and the support of small claims |
| (d) | The relationships between eIDs and Government (.gov) must be given special attention – registrations, births, marriages, deaths, etc. |

Commentary received in this area is set out below:

To achieve a worldwide standard for trust solutions seems to be the main management and governance challenge.

=====

Additional Topics:
 Centralised management is also another topic of relevance. In this regard, the advantage of Satellite Networks shall be highlighted where the network management is centralized and under control of the operator and the access to the network is strictly under control of the Network Control Centre.

=====

Some overlap here with other areas – eg. I put need for legislation under e-Identity but perhaps it is all covered under this mgt and governance section?

=====

In addition, any security technology or measure shall not be deployed or implemented without being managed by a ISO27000-like risk management and mitigation facility that constantly monitors its performance, cost, and effectiveness.

=====

Commentary received on specific challenges:

(a) Framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs;

Should definitively be part of trust management.

=====

(b) Investigation of economic feasibility and possible alternatives;

This should be fundamental

=====

Clarification of return on security investment

=====

Something where we might do specific research

=====

In some cases there may be some risk V cost V benefit analysis left to the user

=====

(c) Technical support for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions; at a simpler level, the regulatory aspects to support the interoperability of security policies are necessary: from civil law for individuals and society, and contract law for business, to common law and the support of small claims;

A very complex issue

=====

Should add:

- transformation of governance of data protection to a more executive administration with jurisdiction over private-sector data collections
- introduction of privacy liability and software liability as a measure to remove market failure

=====

(d) The relationships between eIDs and Government (.gov) must be given special attention – registrations, births, marriages, deaths, etc.

Personal ID should be allowed to be de-coupled from Govt if the individual so wishes

=====

Not clear to me where this comes from - eIDs can also be provided in a market setting

=====

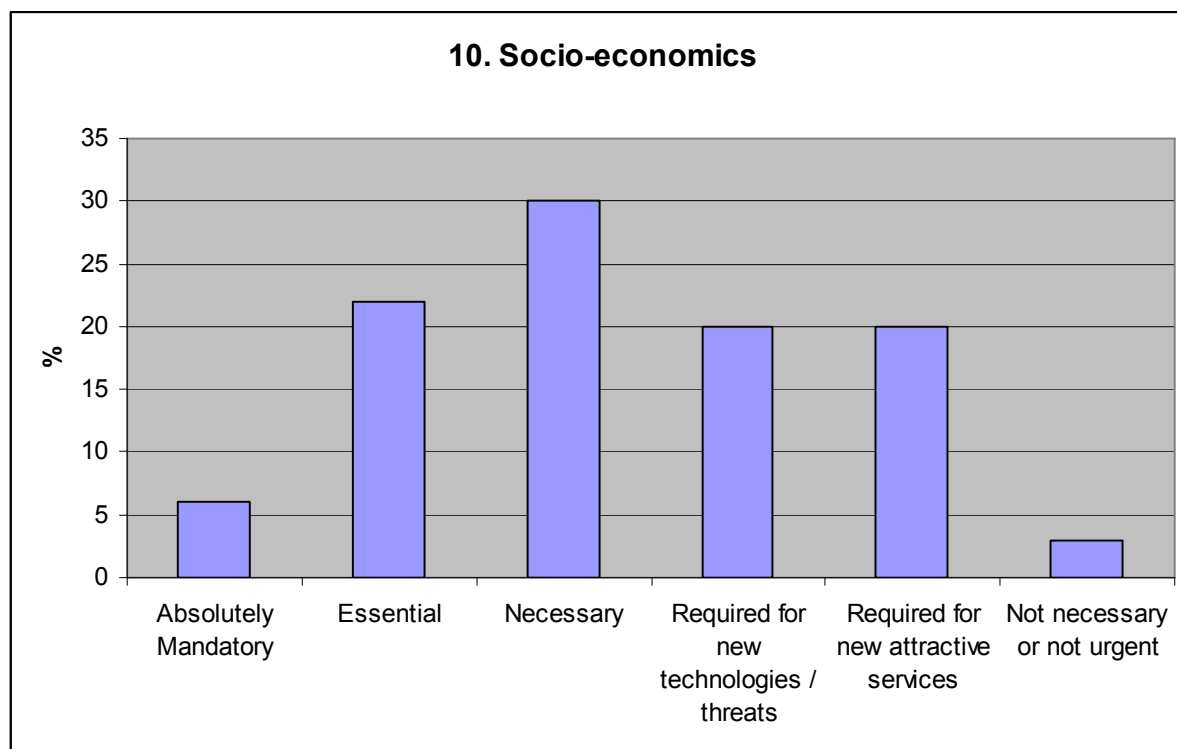
I imagine consensus and uniformity of approach is major research challenge.

=====

3.10 Socio-economics

The overall picture for socio-economics challenges identified is broadly in line with the response profile seen in other areas. Almost 60% of the scores registered indicated that the identified topics were either 'absolutely mandatory' (6%), 'essential' (22%) or 'necessary' (30%).

The graph below shows the combined scores registered in the area of socio-economics:

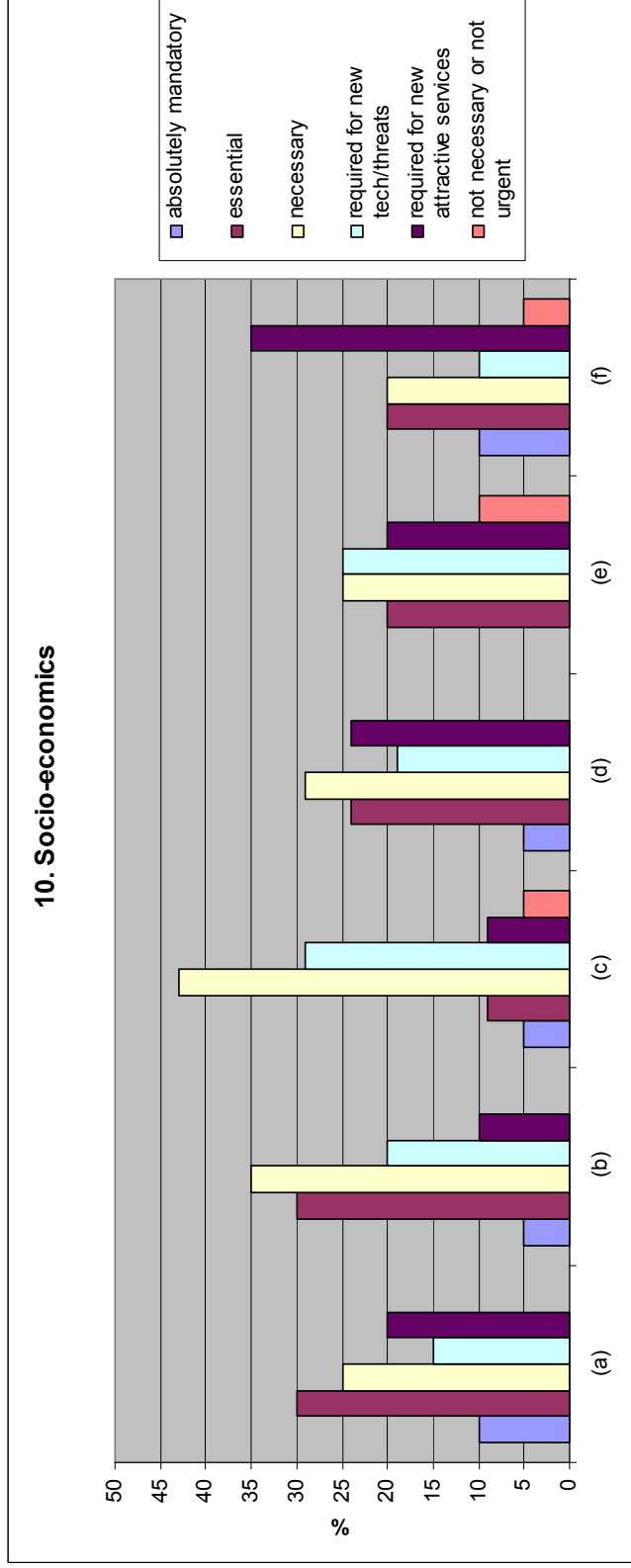


Graph 10.1 Socio-economics – Combined Scores

Turning to the **individual challenges** within the Socio-economics area, there are a number of interesting points emerging, as can be seen from graph 10.2 overleaf:-

- Challenge (b) **'Explore role of other areas of business/industry should be examined to learn how they handle security/risk-analysis, eg, can the insurance industry balance risk and cost for different categories of users? with formal certification of trustworthy products/services and the classification of users, and no-claims discounts, additional premiums for risky use, exclusions, etc'** received a combined score of 70% from respondents who considered it 'absolutely mandatory', 'essential' or 'necessary'.
- Challenge (e) **'Constant engineering vigilance about economic viability: is it more cost-effective to (generically) prevent a data breach or just address the consequent (case-by-case) damage after the event'** was considered to be 'not necessary or not urgent' by 10% of those who responded to the survey.

10. Socio-economics



Graph 10.2 Socio-economics – Individual Challenges Scores

| | Topics |
|-----|--|
| (a) | Convergence and coordination of technology with other areas and disciplines, with parallel advances in non-technological areas |
| (b) | Explore role of other areas of business/industry should be examined to learn how they handle security/risk-analysis, eg, can the insurance industry balance risk and cost for different categories of users? with formal certification of trustworthy products/services and the classification of users, and no-claims discounts; additional premiums for risky use, exclusions, etc |
| (c) | Analysis of economics and inertia in the market place – why has security and trust been undervalued? – but possibly need to approach via the cost of insecurity; and user-perception of value of trust and security versus goodies and add-ons |
| (d) | Incorporation of EU legal framework, for all jurisdictions currently covered, together with new laws and regulatory measures as necessary |
| (e) | Constant engineering vigilance about economic viability: is it more cost-effective to (generically) prevent a data breach or just address the consequent (case-by-case) damage after the event |
| (f) | Exploration of market place and related drivers for eID management (and other security and protection): to place Identifying credentials on different platforms; user-choice of ID 'home'; economic value of secondary usages. |

Commentary received in this area is set out below:

Need to integrate the notions of externalities, risk assessment and its limits, alternatives to the risk assessment based security methodologies, maybe regulatory issues where risk assessment on own assets does not yield sufficient security measures.

=====

It would be very interesting to have socio-economic research project investigating the impact in the long term of poor privacy protection compared to strong privacy protection.

=====

Additional Topics:

Provision of Future Internet services to ALL implies not only to urban areas but also to low density populated areas as well as to mobile platforms which are beyond the reach of terrestrial network means. In this regard, the key role of Satellite Networks, particularly with respect to the FI service provision to low density populated areas shall also be highlighted from the perspective of Social Inclusion.

=====

Additional topic:

Forensics: Enhance capabilities for deep dive forensics to do more detailed security analysis.

=====

Usability is an additional factor to be considered in this context (usability is one of the main reason behind point (c))

=====

Additional topic:

Research on the distribution of power, costs, risks and benefits of security technologies for the wealth, democratic participation, and self-determinance of the individual; Development of regulatory, technical and economic frameworks to balance the above distributions with respect to EU social, economic, legal and democratic policy; The implementation of a monitoring scheme for

obvious and suspected market failures in the security industry and the deployment and governance of their products upon society (e.g. why is there a flood of cheap, unencrypted surveillance cameras on the market that violate principles by the dozen? Why do we spend millions for hi-tech gadgets in airport security while there hasn't been a single terrorist attack on a large ferry boat – which is very easy to carry out by just driving a van onto the ferry).

=====

Commentary received on specific challenges:

(a) Convergence and coordination of technology with other areas and disciplines, with parallel advances in non-technological areas;

New ways of working and use of social media may require new security / trust approaches

=====

Always mandatory

=====

(b) Explore role of other areas of business/industry should be examined to learn how they handle security/risk-analysis, eg, can the insurance industry balance risk and cost for different categories of users? with formal certification of trustworthy products/services and the classification of users, and no-claims discounts, additional premiums for risky use, exclusions, etc;

Use of hyves ID for accessing "my music" portal or bank ID for "my health insurance provider" portal

=====

Perhaps mention the development of a "Quality of Trust" factor

=====

(c) Analysis of economics and inertia in the market place – why has security and trust been undervalued? – but possibly need to approach via the cost of insecurity; and user-perception of value of trust and security versus goodies and add-ons;

Not under-valued but rather ignored (cost-risk approach)

=====

Has a sweeping statement why has security and trust been undervalued? Surely its connected to risk –perhaps the risk wasn't

high and who is in a position to say it has been undervalued or valued at all? Is education of users significant

=====

(d) Incorporation of EU legal framework, for all jurisdictions currently covered, together with new laws and regulatory measures as necessary;

Only data protection or broader? If a comprehensive integration is intended - daunting task. (Across MS regions, domains, areas). Stream-lining an option?

=====

Should be upgraded

=====

(e) Constant engineering vigilance about economic viability: is it more cost-effective to (generically) prevent a data breach or just address the consequent (case-by-case) damage after the event;

i.e. "smart regulation"

=====

The social dimension is missing - consideration should be dual. Social and economic

=====

If test-beds are used correctly a level of realism can be achieved without incurring huge costs.

=====

(f) Exploration of market place and related drivers for eID management (and other security and protection): to place Identifying credentials on different platforms; user-choice of ID 'home; economic value of secondary usages.

Social and legal consequences of secondary usage

=====

3.11 Miscellaneous Commentary

In addition to the commentary received in the individual research areas, a number of “more general” comments were received – these are set out below:

Online services are increasingly being sold via mobile phones. Our mobile is a personal device which we almost always have on us – so it can also serve as a means of authentication. We therefore see a great future for mobile centric identity solutions based on the user and his or her mobile.

=====

In general, authorisation hasn’t received a lot of attention yet; the focus has always been on authenticating the user and how to do this e.g. in a federated manner. A major issue in an identity federation is related to the management of access rights to federated resources. These rights are typically specified in policies. Users and service providers will need to have a unified, conceptually centralized “view” of the policies that they have specified and a unified understanding of how the policies will play out in the underlying infrastructure. This understanding can for instance be based upon roles or attributes; the latter seems the most flexible for use in a federation. How to come to this view is not trivial and requires policy alignment and standardisation, user control, transparency, flexibility. Moreover, aspects like delegation of authority and group management issues need to be taken into account as well.

=====

Today’s identity management solutions are suitable for static information exchange by means of request-response mechanisms only. The dynamic nature of several identity-related attributes such as location or other context information requires a different means of communication than that is used for more static information. The objective is therefore to make a (federated) identity management framework that can handle dynamic profile information (i.e., through an event-driven or subscription-based exchange of context information).

=====

The transparent nature of pervasive and ubiquitous computing environments where context information is used to enhance service experience motivates the need for security functionality that will be transparent, customized, and non-intrusive. The context sensitive

adaptive security paradigm allows for adaptation of the security depending on a set of relevant information collected from the dynamic environment and the preferences and capabilities of the interacting entities, i.e. the context. As the environment evolves, the context changes and so should security in order to dynamically cope with new requirements. Security services, like authentication and access control, can and should be made less intrusive, more intelligent, and able to adapt to the rapidly changing contexts of the environment.

=====

There is wide awareness that something will need to be done about all aspects of security for the cloud ; although, as above, 'solutions' were being offered, but these obviously had very limited, closed scope or made big assumptions about the nature of the cloud environment on offer – like their cloud was entirely supplied and controlled by one supplier, and yes this could indeed be sold to small(ish) organisations as a means to get rid of the IT 'department' and cut their expenditure to precisely only what we need and when we want it ; eg, very limited functionality workstation (lap-top, say) with set of pointers to trusted resources

=====

There is a need for better usability of security functionality and facilities:

- at the operational level – for the actual users of the system;
- at the system management level – the controls on the security functions and operations;
- at the system specification level – tools to assist managers responsible for the purchase and deployment decisions.

=====

Although it is implicit in what we already have on accountability and traceability, there may not be much about the handling of the audit-trail-type information, particularly the tools to make sense of – and protect – the masses data that could be produced: searching for needles in haystacks in many cases.

=====

In my own words, we need to find ways of generating inter-operability, not total consistency which won't be achieved for some time. Hence I have advocated some sort of privacy and security risk rating process analogous to credit risk rating (Moody's; Standard &

Poors etc) where a rigorous process is supposed to lead to a trustworthy rating to be consumed by other parties (eg lenders) on a caveat emptor basis. For some further thinking on this, see the brief paper I presented at the Trust in the Information Society conference in León earlier this month online at www.iispartners.com/Publications/index.html#Yr2010.

=====

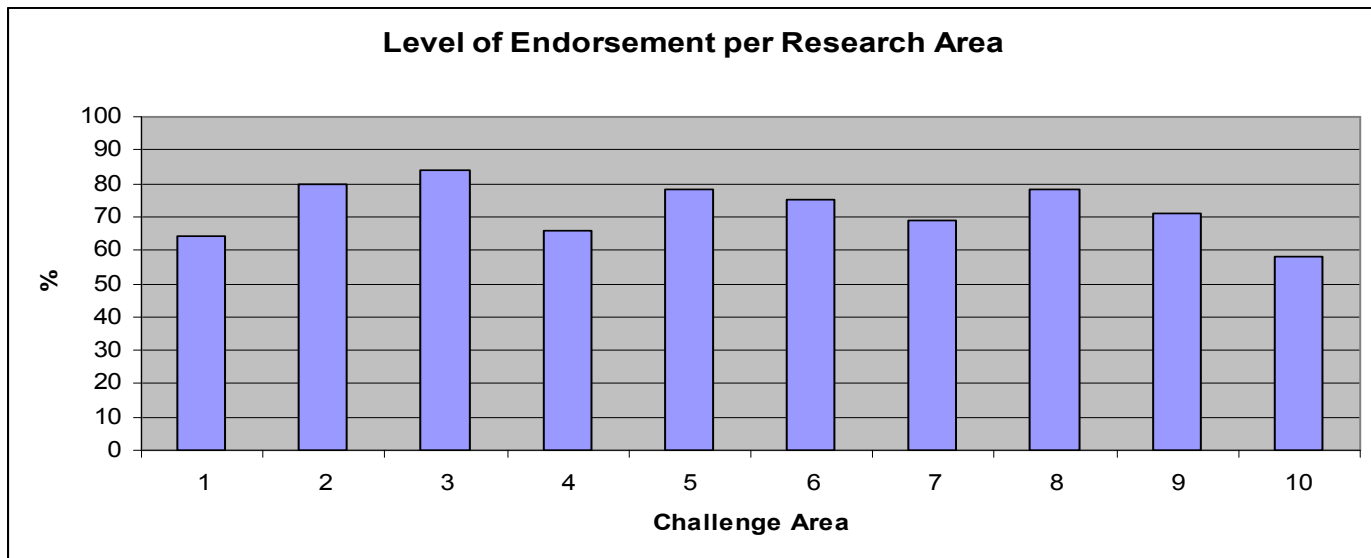
The list of topics is very good, wide scope but very relevant issues.

Topics related to security in scenarios with scarce resources should be amplified, in my opinion.

Also those related to mobility of users should be extended.

4. Overall Levels of Endorsement

The graph below sets out the combined percentages of ‘absolutely mandatory’, ‘essential’ and ‘necessary’ scores received by each research challenge area in the survey. While every area received strong endorsement indicating its relevance, a ranking based on the above, allows us to attempt a prioritisation of the 10 research areas.



Graph 4.1 Combined levels of endorsement received by each challenge area

Key to Challenge Areas:

1. *Trust Engineering*
2. *Architecture*
3. *Cyber-security: Engineering and Technology*
4. *Accountability*
5. *E-Identity*
6. *Privacy*
7. *Protection*
8. *Usability*
9. *Management & Governance*
10. *Socio-economics*

The table overleaf sets out the ranking (prioritisation) based on our analysis with the combined percentage scores per area (these percentage scores are the totals of ‘absolutely mandatory’, ‘essential’ and ‘necessary’ scores received in each area

- 1. Cyber-security – 84%**
- 2. Architecture – 80%**
- 3. E-identity – 78%**
- 4. Usability – 78%**
- 5. Privacy – 75%**
- 6. Management and Governance – 71%**
- 7. Protection – 69%**
- 8. Accountability – 66%**
- 9. Trust Engineering – 64%**
- 10. Socio-economic – 58%**

Discussion of the scores and comments received in each of the ten areas is carried through to Deliverable D3.1c, “Towards a Trustworthy Information Society: The Research Challenges” D3.1c lists the key research challenges (taking account of the prioritisation above) with a description of potential longer term vision in each challenge area which could form the basis of trustworthy hardware and software for the future internet.

Annex A – Questionnaire



Public Consultation

Recommendations Questionnaire

Introduction

The Think-Trust project has identified an interim set of research challenges that require attention in order to provide trustworthy² hardware and software for the Information Society. These research challenges stem from the four priority areas identified in Recommendation 1 of the RISEPTIS Report (<http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html>).

- Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
- Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
- Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
- Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management

We are now seeking input on these interim research challenges from the wider trust and security communities. For further details on these research challenges, please see Deliverable 3.1B (Interim Recommendations Report) on the Think-Trust website (<http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html>).

If you would like to have your opinion heard, please score the identified research challenges in this questionnaire (pp. 3 - 8)

(Completion of this questionnaire should take no more than 15 minutes)

The feedback received during this public consultation process will contribute to the final Think-Trust Recommendations Report (D3.1C), due for publication in June, 2010.

Responses by April 12th, 2010

Paper: Kieran Sullivan
TSSG
ArcLabs Research and Innovation Centre
Waterford Institute of Technology
West Campus
Carriganore
Waterford
IRELAND.

Electronic: consultation@think-trust.eu

² For the purposes of this questionnaire, trust and security covers a broad spectrum that includes the trusted use of (and trust in) communications and services; privacy and protection of personal and commercially sensitive information; and protection of services and infrastructure (cyberspace).

Questionnaire

Please assign one of the following scores to the challenges identified.

- A*** absolutely mandatory for progress from current position
- A** essential to provision of trust and security for Future Internet and the Information Society
- B** necessary to achieve broad usability and uptake
- C** required longer-term response to new technologies and potential threats
- D** required for provision of attractive and competitive services
- X** not necessary or not urgent

(optional)

| RESPONDENT NAME | ORGANISATION | E-MAIL ADDRESS |
|-----------------|--------------|----------------|
| | | |

| | Comment | Score |
|--|---------|-------|
| 1. Trust 'engineering' | | |
| Development of overall framework for trust | | |
| (a) Establishment, management and maintenance of trust relationships; | | |
| (b) Development, expression and use of trust indicators; | | |
| (c) Automatic computation of trust assertions, based on policy frameworks that take into account user preferences; | | |
| (d) Life-cycle management, including maintenance, repair and recovery; | | |
| (e) Models, methodologies, measurement of trust (see Quantification below); | | |
| (f) Tools to calculate trust (a combination of assisting the user and quantifying personal trust); | | |
| (g) Assessment of availability / downtime / integrity / confidentiality to feed into trust models; | | |
| (h) Delegation and acceptance of trust and privileges. | | |
| Quantification of trust, security and privacy | | |
| (i) Scaling results on trust experiments from the laboratory environment to the real worlds of the Future Internet; | | |
| (j) Generalisation of security predictions across different software components, programming languages, systems, environments; | | |

| | Comment | Score |
|---|---------|-------|
| (k) Collection and sharing of security-related data for experimental research; | | |
| 2. Architecture | | |
| (a) Policy awareness and transparency as architectural properties; | | |
| (b) Transparency support: monitoring; observability; logging, accessibility; | | |
| (c) Consistency of security and trust facilities and mechanisms across layers and domains; | | |
| (d) Meta architecture –higher-level abstractions to help structure a global information security architecture; | | |
| (e) Network and service architectures – scalability and interoperability of the current architecture; | | |
| (f) Damage control: domains, partitioning, compartmentalisation in, for example Cloud environments, (including dynamic service composition/aggregation); | | |
| (g) Architectural standards (to support) <ul style="list-style-type: none"> • pre-conditions for interoperability; • verification of conformance requirements; • built-in emergency measures; • workable definitions concept (metadata, ontologies, etc.); • security policy management, including the ability to attach policy information to data; | | |
| 3. Cyber-security: Engineering and Technology | | |
| (a) Techniques and mechanisms to provide protection, assurance and integrity; | | |
| (b) Robustness, resilience, survivability; | | |
| (c) Criteria and standards to support policy governance; | | |
| (d) Interoperability, and platform independence; | | |
| (e) Virtualisation to support construction of complex concepts such as high-demand, critical services on otherwise limited technologies; | | |
| (f) Security in environments with scarce resources; | | |
| (g) Support for legal policies and requirements; | | |
| (h) Tools and technologies to support design and construction of future trusted environments and networks; | | |
| 4. Accountability | | |

| | Comment | Score |
|---|---------|-------|
| (a) Means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress; | | |
| (b) Interoperable, robust accountability framework (that balances privacy and traceability; that is economically feasible; that protects against non-repudiation but also against incorrect attribution); | | |
| (c) Consistent interpretation of security policy agreements; appropriate standards for protocols and interfaces, and for tools to enable compliant usage; | | |
| (d) Traceability and accountability on global accountancy-type principles; | | |
| (e) Territorialisation of (trace/log) information; local domain policies and management; restricted 'sharing' only with authorised participating domains; | | |
| (f) Real-time, large-scale test-beds to generate confidence; | | |
| (Other areas related to Accountability) | | |
| (g) Applicability to charging and payment; | | |
| (h) Anonymous/pseudonymous charging and payment systems; | | |
| (i) Anonymization or impersonation tools to produce untraceable, but trustworthy, valid sources/channels for eg, provision of economic, social, or health statistics; | | |
| 5. E-Identity | | |
| (a) Common EU framework for identity and authentication; | | |
| (b) Interoperability of/with alternative (and current) ID schemes; | | |
| (c) Flexibility of choice of identity and ID-protection options/choices, including partial IDs and anonymity when appropriate; | | |
| (d) Life-cycle management of IDs, with protection recovery from loss or failure; | | |
| (e) Standardised linkages to related and dependent concepts (accountability, access-control, etc.); | | |
| (f) Claim-based approaches using novel and existing cryptographic protocols (to eventually avoid ID architectures with a centralised components); | | |
| (g) Technology to support new business models for (a) central, (b) decentralised, and (c) claim-based approaches; | | |
| (h) Communication setup and routing that are identity-data-aware only (as necessary for network functions, without making the related users identifiable or traceable); | | |
| 6. Privacy | | |

| | Comment | Score |
|--|---------|-------|
| (a) Minimisation of unintended gathering of personal and other sensitive information; | | |
| (b) Fine granularity access control to identity-related information; | | |
| (c) Further development of Privacy Enhancing Technologies (PETs); including tools to check privacy assurance and to advance transparency regarding used data; | | |
| (d) Use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users; | | |
| (e) Methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, (including revocation/retraction); | | |
| (f) Option to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates; | | |
| (g) Personal/communal collector of personal garbage/litter; | | |
| (h) Use and control of identity-related information for network (e.g. routing) purposes without compromising privacy; | | |
| (i) Standardised techniques to assure privacy across the various internet layers, (through to network level and maintaining consistent privacy across different environments); | | |
| (j) Tools and concepts for deleting data in the internet; | | |
| 7. Protection | | |
| Related to Privacy, above (plus confidentiality and integrity for business/administrations) | | |
| (a) Protection of data processing, storage and transmission, (including the shielding of resources and assets - information, services, devices, communications); | | |
| (b) Domains, partitioning, compartmentalisation, fire-breaks – leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage; | | |
| (c) Fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc; | | |
| (d) Mutual authentication, with technology-invariant, multiple devices; | | |
| (e) New cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age; | | |

| | Comment | Score |
|--|---------|-------|
| (f) Uses of eID and its components in protecting the interests of its subject (data protection, etc.); | | |
| 8. Usability | | |
| (a) Support for the individual user (user-centricity) | | |
| (b) Develop environments that can adapt to user choice as well as presenting auto-configurations based on assumptions and profiles; | | |
| (c) User needs (security and trust facilities and functionality) - including non-technical, human aspects; | | |
| (d) Impacts and implications for the underlying mechanisms and functionality; | | |
| (e) User/system interaction: sympathetic user interfaces, but with advanced options; | | |
| (f) Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; | | |
| 9. Management and Governance | | |
| (a) Framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs; | | |
| (b) Investigation of economic feasibility and possible alternatives; | | |
| (c) Technical support for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions – <i>regulatory aspects to support the interoperability of security policies, from:</i> <ul style="list-style-type: none"> • <i>civil law for individuals and society;</i> • <i>contract law for business; and,</i> • <i>common law for the support of small claims;</i> | | |
| (d) The relationships between eIDs and Government (.gov) – registrations, births, marriages, deaths, etc; | | |
| 10. Socio-economic | | |
| (a) Convergence and coordination of technology with other areas and disciplines, with parallel advances in non-technological areas; | | |
| (b) Role of other areas of business/industry in handling security/risk-analysis, e.g. can the insurance industry balance risk and cost for different categories of users, with formal certification of trustworthy products/services and the classification of users, no-claims discounts, additional premiums for risky use, exclusions, etc.; | | |

| | Comment | Score |
|--|---------|-------|
| (c) Analysis of economics and inertia in the market place – why has security and trust been undervalued; | | |
| (d) Incorporation of EU legal framework; | | |
| (e) Constant engineering vigilance about economic viability, (<i>is it more cost-effective to prevent a generic data breach or just address the consequent case-by-case damage after the event;</i> | | |
| (f) Exploration of market place and related drivers for eID management (and other security and protection); | | |

Overall coverage (free text)

- Are there additional topics that need to be added to the interim list above?
- What topics need to be amplified or extended?
- Should any topics be removed, down-graded, or postponed?

Annex B – Research Checklist



Public Consultation

Research Checklist

| RESPONDENT NAME | ORGANISATION | E-MAIL ADDRESS |
|-----------------|--------------|----------------|
| | | |

Introduction

The Think-Trust project has identified an interim set of research challenges that require attention in order to provide trustworthy³ hardware and software for the Information Society. These research challenges stem from the four priority areas identified in Recommendation 1 of the RISEPTIS Report (<http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html>).

- Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
- Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
- Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
- Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management

We are now seeking input and comment on these interim research challenges from the wider trust and security communities. For further details on these research challenges, please see Deliverable 3.1B (Interim Recommendations Report) on the Think-Trust website (<http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html>).

We are asking for your comments and feedback on the research challenges identified by the project

The feedback received during this public consultation process will contribute to the final Think-Trust Recommendations Report (D3.1C), due for publication in June, 2010.

Responses please by May 7th , 2010

Paper: Kieran Sullivan
TSSG
ArcLabs Research and Innovation Centre
Waterford Institute of Technology
Carriganore
Waterford
IRELAND

Electronic: consultation@think-trust.eu

³ For the purposes of this checklist, trust and security covers a broad spectrum that includes the trusted use of (and trust in) communications and services; privacy and protection of personal and commercially sensitive information; and protection of services and infrastructure (cyberspace).

The following research challenges have been identified
in the area of
Trust Engineering

Development of Trust Framework

- (a) Establishment, management and maintenance of trust relationships;
- (b) Development, expression and use of trust indicators;
- (c) Automatic computation of trust assertions, based on policy frameworks that take into account user preferences;
- (d) Life-cycle management, including maintenance, repair and recovery;
- (e) Models, methodologies, measurement of trust (see [Quantification](#) below);
- (f) Tools to calculate trust (a combination of assisting the user and quantifying personal trust);
- (g) Assessment of availability / downtime / integrity / confidentiality to feed into trust models;
- (h) Delegation and acceptance of trust and privileges;

Quantification of Trust, Security and Privacy

- (i) Scaling results on trust experiments from the laboratory environment to the real worlds of the Future Internet;
- (j) Generalisation of security predictions across different software components, programming languages, systems, environments;
- (k) Collection and sharing of security-related data for experimental research;

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
Architecture

- (a) Policy awareness and transparency as architectural properties;
- (b) Transparency support: monitoring, observability, logging, accessibility;
- (c) Consistency of security and trust facilities and mechanisms across layers and domains;
- (d) *Meta* architecture –higher-level abstractions to help structure a global information security architecture;
- (e) *Network* and *service* architectures – scalability and interoperability of the current architecture;
- (f) Damage control: domains, partitioning, compartmentalisation in, (for example), Cloud environment;
- (g) Architectural *standards* (to support):
 - pre-conditions for interoperability;
 - verification of conformance requirements;
 - built-in emergency measures;
 - workable definitions concept (metadata, ontologies, etc.);
 - security policy management, including the ability to attach policy information to data;

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified

in the area of

Cyber-security: Engineering and Technology

- (a) Techniques and mechanisms to provide protection, assurance and integrity;
- (b) Robustness, resilience, survivability;
- (c) Criteria and standards to support policy governance;
- (d) Interoperability and platform independence;
- (e) Virtualisation to support construction of complex concepts such as high-demand, critical services on otherwise limited technologies;
- (f) Security in environments with scarce resources;
- (g) Support for legal policies and requirements;
- (h) Tools and technologies to support design and construction of future trusted environments and networks;

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
Accountability

- (a) Means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress;
- (b) Interoperable, robust accountability framework (that balances privacy and traceability; that is economically feasible; that protects against non-repudiation but also against incorrect attribution);
- (c) Consistent interpretation of security policy agreements, appropriate standards for protocols and interfaces, and for tools to enable compliant usage;
- (d) Traceability and accountability on global accountancy-type principles;
- (e) Territorialisation of (trace/log) information, local domain policies and management, restricted 'sharing' only with authorised participating domains;
- (f) Real-time, large-scale test-beds to generate confidence;

(Other areas related to *Accountability*)

- (g) Applicability to charging and payment;
- (h) Anonymous/pseudonymous charging and payment systems;
- (i) Anonymisation or impersonation tools to produce untraceable, but trustworthy, valid sources/channels for eg, provision of economic, social, or health statistics;

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
E-Identity

- (a) Common EU framework for identity and authentication;
- (b) Interoperability of/with alternative (and current) ID schemes;
- (c) Flexibility of choice of identity and ID-protection options/choices, including partial IDs and anonymity when appropriate;
- (d) Life-cycle management of IDs, with protection recovery from loss or failure;
- (e) Standardised linkages to related and dependent concepts (accountability, access-control, etc.);
- (f) Claim-based approaches using novel and existing cryptographic protocols (to eventually avoid ID architectures with centralised components);
- (g) Technology to support new business models for (a) central, (b) decentralised, and (c) claim-based approaches;
- (h) Communication setup and routing that are identity-data-aware (as necessary for network functions, without making the related users identifiable or traceable);

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
Privacy

- (a) Minimisation of unintended gathering of personal and other sensitive information;
- (b) Fine granularity access control to identity-related information;
- (c) Further development of Privacy Enhancing Technologies (PETs), including tools to check privacy assurance and to advance transparency regarding used data;
- (d) Use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users;
- (e) Methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, (including revocation/retraction);
- (f) Option to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates;
- (g) Personal/communal collector of personal garbage/litter;
- (h) Use and control of identity-related information for network (e.g. routing) purposes without compromising privacy;
- (i) Standardised techniques to assure privacy across the various Internet layers (through to network level and maintaining consistent privacy across different environments);
- (j) Tools and concepts for deleting data in the internet;

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
Protection

(Related to ***Privacy*** above)

- (a) Protection of data processing, storage and transmission, (including the shielding of resources and assets - information, services, devices, communications);
- (b) Domains, partitioning, compartmentalisation, fire-breaks – leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage;
- (c) Fine granularity access control based on multiple bases for authentication and authorisation, e.g. IDs, privileges, roles, etc.;
- (d) Mutual authentication, with technology-invariant, multiple devices;
- (e) New cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age;
- (f) Uses of eID and its components in protecting the interests of its subject (data protection, etc.);

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
Usability

- (a) Support for the individual user (user-centricity);
- (b) Develop environments that can adapt to user choice as well as presenting auto-configurations based on assumptions and profiles;
- (c) User needs (security and trust facilities and functionality) - including non-technical, human aspects;
- (d) Impacts and implications for the underlying mechanisms and functionality;
- (e) User/system interaction: sympathetic user interfaces with advanced options;
- (f) Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms;

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
Management & Governance

- (a) Framework for consistent expression and interpretation of security policies, and the means to implement policies at all levels, from network layers up to business and legal needs;
- (b) Investigation of economic feasibility and possible alternatives;
- (c) Technical support for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions: - *regulatory aspects to support the interoperability of security policies, from*
- *civil law for individuals and society;*
 - *contract law for business;*
 - *common law for the support of small claims*
- (d) The relationships between eIDs and Government (.gov) – registrations, births, marriages, deaths, etc.;

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

The following research challenges have been identified
in the area of
Socio-economic

- (a) Convergence and coordination of technology with other areas and disciplines, with parallel advances in non-technological areas;
- (b) Role of other areas of business/industry in handling security/risk-analysis, *e.g. can the insurance industry balance risk and cost for different categories of users, with formal certification of trustworthy products/services and the classification of users, no-claims discounts, additional premiums for risky use, exclusions, etc;*
- (c) Analysis of economics and inertia in the market place – why has security and trust been undervalued;
- (d) Incorporation of EU legal framework;
- (e) Constant engineering vigilance about economic viability, *(is it more cost-effective to prevent a generic data breach or just address the consequent case-by-case damage after the event);*
- (f) Exploration of market place and related drivers for eID management (and other security and protection);

Comments

(e.g. Do you agree that these are the principal research challenges in this area?: Do you think we need to add additional topics?: Which topics need to be amplified or extended?: Should any topics be removed, down-graded, or postponed?)

Annex C – Written Respondents

Written responses to the Public Consultation were received from the following:-

Almgren, Magnus: magnus.almgren@chalmers.se
Angelika, Staimer: Angelika.staimer@siemens.com
Bodea, Gabriela: gabriela.bodea@tno.nl
Bramhall, Pete: pete.bramhall@hp.com
Carter, Fred: Fred.Carter@ipc.on.ca
Christos, TSELIKIS: TSELIKIS.Christos@haicorp.com
Crompton, Malcolm: mcrompton@iispartners.com
D'Antonio, Salvatore: saldanto@unina.it
Dimitrov, Kiril: kpd@iccs.bas.bg
Dionysiou, Ioanna: dionysiou.i@unic.ac.cy
Djambazova, Edita: ead@iccs.bas.bg
Falk, Rainer: rainer.falk@siemens.com
Fries, Steffen: steffen.fries@siemens.com
Gresser, Jean-Yves: jgresser@noos.fr
Herzog, Uwe: herzog@eurescom.eu
Hulsebosch, Bob: Bob.Hulsebosch@novay.nl
Koster, Paul: r.p.koster@philips.com
Kuppinger, Martin: mk@kuppingercole.com
Larduinat, Xavier: Xavier.Larduinat@gemalto.com
Lopez, Javier: jlm@lcc.uma.es
Mitchell, Chris: me@chrismitchell.net
Morrow, Susan: susan.morrow@avocosecure.com
Neumann, Heike: heike.neumann@nxp.com
Paulus, Sachar: paulus@fh-brandenburg.de
Samp, Krzysztof: krzysztof.samp@itti.com.pl
Surridge, Mike: ms@it-innovation.soton.ac.uk
Rammig, Ralf: ralf.rammig@siemens.com
Weippl, Edgar: EWeippl@sba-research.org
Butler, Bernard: bbutler@tssg.org
Dooly, Zeta: zdooly@tssg.org
Elshaafi, Hisain: helshaafi@tssg.org
Fritsch, Lothar: Lothar.Fritsch@NR.no
Gittins, Benjamin: cto@pqs.io (Parts 1 – 6)

Hale, Ronald: rhale@isaca.org

Hecker, Artur: artur.hecker@enst.fr

Liolos, Konstantinos: klio@space.gr

Pasic, Aljosa: aljosa.pasic@atosresearch.eu

Paulus, Sachar: paulus@fh-brandenburg.de

Power, Gemma: gpower@tssg.org

Prasad, Neeli: np@es.aau.dk

Presser, Mirko: mirko.presser@alexandra.dk

Rotondi, Domenico: Domenico.Rotondi@TXTGroup.Com

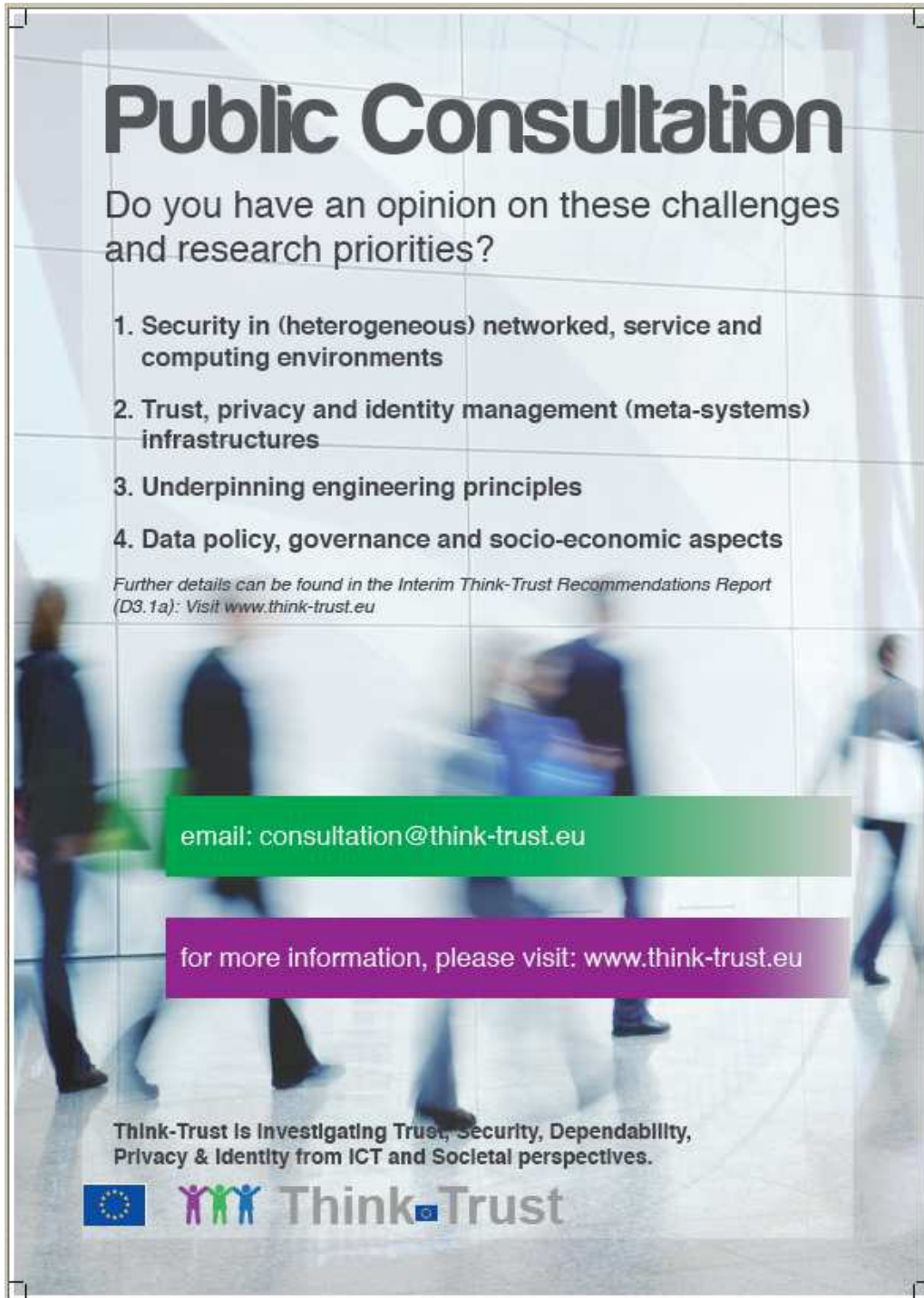
Savola, Reijo: Reijo.Savola@vtt.fi

Seigneur, Jean-Marc: seigneurj@gmail.com

Various responses via Keith Howker

In addition to the above, text and verbal feedback was also noted..

Annex D – Public Consultation Poster



Public Consultation

Do you have an opinion on these challenges and research priorities?



1. Security in (heterogeneous) networked, service and computing environments
2. Trust, privacy and identity management (meta-systems) infrastructures
3. Underpinning engineering principles
4. Data policy, governance and socio-economic aspects

Further details can be found in the Interim Think-Trust Recommendations Report (D3.1a): Visit www.think-trust.eu

email: consultation@think-trust.eu

for more information, please visit: www.think-trust.eu

Think-Trust is Investigating Trust, Security, Dependability, Privacy & Identity from ICT and Societal perspectives.

 Think-Trust