

## **FP7 Thematic Consultation Workshop**

### **Application Research in Information and Communication Technologies for Trust and Confidence**

Brussels, 24 January 2006

**Title** Expert Workshop on “ICT for Trust and Confidence”

**Status** Final

**Date** 16<sup>th</sup> May 2006

**Rapporteur** Tony Gore

**Distribution** Public

#### Document History

<b>Date</b>	<b>Version</b>	<b>Notes</b>	<b>Who</b>
24 <sup>th</sup> Jan 2006	0v0	Tony Gore workshop report	TG
7 <sup>th</sup> Feb 2006	0v1	Restructuring and highlighting	RS/GS
20 <sup>th</sup> Feb 2006	0v2	Tidying up of report	TG
20 <sup>th</sup> Mar 2006	0v3	Bullet point structure and reshuffling	GS
16 <sup>th</sup> May 2006	1v0	Final version	GS/TG

## Contents

<b>FP7 THEMATIC CONSULTATION WORKSHOP</b> .....	<b>1</b>
<b>APPLICATION RESEARCH IN INFORMATION AND COMMUNICATION TECHNOLOGIES FOR TRUST AND CONFIDENCE</b> .....	<b>1</b>
BRUSSELS, 24 JANUARY 2006 .....	1
DOCUMENT HISTORY .....	1
CONTENTS .....	II
<b>I. INTRODUCTION</b> .....	<b>1</b>
<b>II. DISCUSSION OF POTENTIAL FUTURE RESEARCH ISSUES</b> .....	<b>2</b>
1. MODELS FOR “SECURITY” AND “TRUST” .....	2
2. IDENTITY MANAGEMENT AND PRIVACY ENHANCING TECHNOLOGIES.....	4
3. SECURE HANDLING OF DIGITAL ASSETS.....	6
4. PROTECTION AGAINST CYBER THREATS .....	7
5. RISK MANAGEMENT AND ECONOMICAL ASPECTS .....	7
6. CERTIFICATION, BENCHMARKING AND RELATED TOPICS.....	8
7. OTHER CONSIDERATIONS .....	9
<b>III. OVERALL CONCLUSIONS AND RECOMMENDATIONS</b> .....	<b>11</b>
<b>IV. ANNEX 1 : AGENDA</b> .....	<b>13</b>
<b>V. ANNEX 2 : LIST OF PARTICIPANTS</b> .....	<b>14</b>
<b>VI. ANNEX 3 : CONSULTATION PROCESS</b> .....	<b>15</b>
<b>VII. ANNEX 4 : GLOSSARY AND DEFINITIONS</b> .....	<b>16</b>

# I. Introduction

This workshop was one of a series of workshops to assist the European Commission in detailing the directions of research in the FP7 Applications Research Area “ICT for Trust and Confidence”.

Security is moving from closed systems into a more open area, with closed systems and open systems and many combinations in between. Ubiquitous computing will lead to an increase in the number of devices to be secured by several orders of magnitude. The challenge is to use this for good, and protect the systems from failure and abuse. There will be no single point of control, and systems will be so large and complex that no-one will have a complete picture. Most systems will be dynamic as the people and objects move around.

With decreasing transparency of the underlying technology, trust becomes the ultimate success factor, combining security and dependability considerations. If something goes wrong, no one will ask for the particular reason but simply lose the trust in the technology in question and eventually drop it completely. As an example, one might think on exploited buffer overflows in Windows OS. Is this a security gap or simply insufficiently designed code?

**Therefore, security methodologies will need to support the move from integrated systems to interoperable systems and have to find its position within a global dependability framework.**

This report reflects the result of a brainstorming session with invited experts from the field. It first summarises the various issues which are supposed to play an important role in the future, followed by a set of recommendations derived from the discussion.

## II. Discussion of potential future research issues

The discussion was structured to cover the issues:

- Models of Security and Trust
- Identity Management and Privacy Enhancing Technology (incl. Biometrics)
- Secure Handling of Digital Assets
- Protection against cyber threats
- Risk Management and economic aspects
- Certification, benchmarking and related topics

It appeared, however, that most of the discussion addressed the first two items, indicating that solutions for the other areas can be expected only by taking a more holistic point of view.

### 1. *Models for “Security” and “Trust”*

- **A conceptual analysis of trust is needed.** According to the nature of the term “trust”, this analysis should be multidisciplinary – IT specialists, social science and psychologists, lawyers and philosophers. The “trajectory” that will be taken in the subsequent development of systems will depend very much on the definition of trust used. Identity plays a role in human lives. Privacy also needs to be defined, and in a way that can be measured and enforced. Privacy is currently a “fuzzy” concept and means different things to different people. Data Protection (as mainly used in the European context) has better possibilities to be mapped to quantifiable and measurable criteria.

Work is also needed on the psychology of awareness and usability of trust for which usability experts and psychologists need to be involved.

- **Proper studies need to be undertaken on use – surveys are not enough.** Generally, there is a big difference between what people say and what people actually do.

People are willing to give up privacy if they get something in return. This needs to be recognised and respected, and on the other hand awareness about the potential threats has to be improved.

Scenarios developed by industry are considered naïve and “middle class”. Social studies have to “piggy back” on technology i.e. be linked to the technology development to be direct and useful. A way has to be found to make it “cool” to protect privacy, and target teenagers who have the least understanding of the need to

protect privacy. Youngsters are confident in some areas of technology usage, but adults see privacy as more of an issue.

- There are questions to be answered on the **contractual side**, such as who is the contractual partner to a particular customer. Currently, the security market is not working properly – the risk is allocated to the weakest partner i.e. the user. A fair balance has to be created between all parties to a transaction. Typically, consumers choose on price and speed, and only then on other considerations. Security needs to be given a higher value in the view of the consumer.
- **There is a digital divide on the ability to respond to threats.** Experienced users do not have real problems with viruses, spam or phishing. But still the majority of successful attacks exploit the lack of experience of others.
- **A holistic view to security and dependability is needed.** Security is needed in three places – at the end, from end to end, and at stages in between. Security, once established, must be sustained despite evolving threats and changing patterns of usage. This could be extended to “sustainable trust”.

Integration is needed between security and trust e.g. trust based ranking, trust based access control.

- **What are the metrics of trust and privacy?** Reputation management is needed where strong security mechanisms are not feasible. Reputation based systems may reduce the need for secure mechanisms e.g. the way trust is built up on Ebay.

In data protection, how does a user enforce policies and specify protection when the data is not in the user’s scope? How is trust measured, expressed, combined etc? There was much debate around 2004 on trusted computing. In submitting data to a server, how do you know if you can trust it? Even if it is sealed, how can you know that you can trust data submitted to it.

- **“Value sensitive” designs** are needed that bridge the gap between (values, norms, laws, ideals) and (code, architectures, specifications, infrastructures). The question is how to express and implement this? **Language, methodology and tools** are required, along with the ability to specify, justify, evaluate, certify, and audit the systems.

There is a vision for risk-based security and privacy. This starts with negotiable SLAs (Service Level Agreements). Above this is a fault diagnosis based on these assurances, where reference data is collected so that cost/risk tradeoffs become quantifiable. This will gradually extend from static systems to dynamic systems as policies are developed that specify risk and trust, so that systems can adapt themselves to the risk and trust requirements.

- One useful feature is to have “**virtual identities**” – there are many applications where secure transactions can take place without knowing who you are. These are equivalent to using cash, rather than credit cards.
- It was suggested that projects should be encouraged or compelled to use **IPv6**, as this has more security features. Others argue that IPv6 is already “old Internet”.

## 2. **Identity Management and Privacy Enhancing Technologies**

- **The biggest problem is getting identity “end to end”** and this is a good use case for composability. SLAs supporting negotiable security, which is possible, and privacy, which is difficult are needed. Organisations interested in this are service providers and application providers.

- The market so far has failed to offer privacy. Should there be a public infrastructure that offers privacy, where the user can decide where their data is going to go? Should protection of data be a consumer right, in the same way that legislation protects consumers, or should it be left to the marketplace? Should there be choice and competition in security?

The citizen may really want the **right to autonomy**. There is a need to develop privacy enhancing technologies to support data protection legislation. There is a European Framework providing data protection, but no effective monitoring and policing of it.

There is a clear trend in security – rights need to be assigned to the user, not the machine, because of mobility.

- What happens when there is “**loss of privacy**”? What is the relationship with the person who has suffered the damage?

So far, privacy has been only about direct user transactions. This is going to change as we move to the next level of distributed systems and services where personal data may be held in lots of places e.g. in a networked heart monitor of a person in a gym. The users may not want their health insurance company to be able to monitor it.

- What does privacy mean in terms of pervasive ubiquitous environments? What are the privacy implications of location based services? Technologists need to be engaged with legal discussions at an early stage.

There may be businesses that cannot work because of privacy constraints. Wrong choices in technologies and laws could limit future economic growth, so careful thought needs to be given to the business implications of the way privacy is defined, implemented and protected. Some research has been done where people put a price on privacy, and this could be extended to guide the choices and ensure a balance between the individual, businesses and governments. Privacy also relates to human dignity, and this is in the EU Constitution and is non-negotiable.

**A structure is needed where dialogues can take place between lawyers and the technologists.**

- People work in many communities and need to emulate the real world. This requires deterrents and accountability, communities and partitioning. Privacy and anonymity can work with **accountability**. Security is expensive for business and difficult for users. There is an issue with the “have-nots” in terms of security and trust i.e. it should be available to all, not just those who are capable and able to pay.
- **Anonymous infrastructure has been identified as a potential key underpinning element for some services.** Should the provision of some of this infrastructure be publicly funded? Only a relatively modest amount of sustainable funding may be needed for this.

Virtual presences can avoid some of the need to protect data – this is a positive power, and is different from privacy. There are several reasons to have an infrastructure for handling anonymity – many transactions do not need to identify the partners in the transaction, just as in the real world, you can buy a book for cash, on-line the bookseller does not need to know who you are, just that the electronic funds transfer will be honoured.

As the amount of desktop processing increases, individuals are exposing more information, and an anonymous infrastructure is protection against this. Traffic analysis will give new threats to privacy, and this can be countered by routing over an anonymous infrastructure where appropriate.

- **RFID**, one aspect of ubiquitous computing, needs more work in the area of hardware privacy solutions.
- There is the need to separate biometric and identity database i.e. a weak link to enhance privacy. Biometrics are increasingly being introduced as a technical solution to authentication and authorisation, but the technologies are imperfect and the social consequences have not been thoroughly considered. Biometric machines are currently being physically attacked in France. It is clear that citizens are not seeing the advantages, only the disadvantages.

**Anonymous biometrics is a very important topic for privacy** e.g. to generate a deterministic key from a fuzzy function (finger).

- There are privacy issues relating to trust negotiation – a lot of information may be revealed during the negotiation.

**In the applications layer, ID schemes, such as secure soft IDs, micropayments and e-Delivery can lead the way.**

In most trust systems, there is a database somewhere. Databases are untrustworthy and quickly get “polluted”. Database trustworthiness needs to be researched and new solutions developed.

### **3. Secure handling of digital assets**

- There is a looming **economic conflict** over on-line **DRM** (Digital Rights Management).

**DRM needs to be developed into a single standard**, or become interoperable. Middleware that translates rights from one DRM system to another could be developed. Practical and widely available schemes for micropayments are also needed. This could lead to new trading applications. One example might be to download a photograph a private (non-professional) user has made available on a web site and incorporate it into a calendar or brochure. During the printing process, the number of copies is counted and a payment automatically transferred from the user to the copyright owner.

Digital assets require the development of robust and secure watermarking, asset processing in the encrypted domain and a variety of other services.

- **Trust establishment and Trustworthy Computing in pervasive, open environments without central control is a central challenge.**

DRM and similar aspects need to have interoperable standards – currently we have private incompatible standards. There are legal issues related to this, especially related to competition. We need multilateral security – we need to research and implement solutions to secure all participants e.g. DRM must also protect the rights of the users, as well as those of the authors.

- IT security is increasingly being used for **anti-competitive practices** and control of downstream markets. There are competition concerns – where should the law step in? Should we have open or controlled architectures?

#### 4. ***Protection against cyber threats***

- There is a developing “**malware economy**”. An anonymous infrastructure may reduce the opportunities for some cyber threats – it is harder to attack things that cannot be identified, but at the same time it may create new threats.
- Methods need to be developed for **evaluating changes to systems** that occur over time, and their impact on security, and how we control access to resources based on time and situational data (context).

#### 5. ***Risk management and economical aspects***

- **Business oriented security** can be defined as IT security plus quantifiable risk. This means that security and privacy must be monitored and managed at the business level, as well as at the technological level.

Security needs to be more than database tables etc. Languages and policies are needed to provide enforcement, but linked to the business process, which can specify some of these. Integrating the security issues into the business processes, and how to translate these (automatically) to the implementations is a challenge.

- **Risk management needs to be incorporated to provide quantitative reasoning.**

The responsibility for security properties and/or services may depend on the result of a risk analysis. Understanding of risk, and how to deal with risk, is not widespread and methods for improving this are required. Applications need to have a risk management aspect to them and measures of dependability.

The user should be able to understand the decision they make. Real threats exist from data mining, and the secondary use of data poses a great threat. The user will want to control use of data – both primary use and secondary<sup>1</sup> use. A useful technique to investigate and develop would be the ability to “corrupt” data to prevent data aggregation (in a similar way to the “dither” signal that the US has applied in the past to non-military GPS signals to make them less accurate).

- There are the economic aspects of security – a risk analysis needs input. A means of gathering data on security related events, especially where there is a high level of

---

<sup>1</sup> Secondary use of data – assume anonymous data set 1 only identifies users by postal code and age; when combined with a known second data set e.g. data with names, addresses and birthdates, it may be possible to take a unique postal code and the resulting data sets are sufficiently small that the ages and birthdates can be correlated, thus identifying every user in the anonymous set of data

damage, to establish probabilities of these. One problem is that we need this information, but enterprises are not willing to reveal it, because of the loss of reputation and trust. A solution would be to develop an **anonymous database reporting structure**. This needs to be truly anonymous and untraceable, then companies would be willing to provide the information. It is also a core technology for many privacy respecting applications.

- In studies on users' attitudes on risk it is necessary to determine if **risk compensation is a factor in trust and security** – studies show that if you reduce the risk, people will factor that into their behaviour e.g. with ABS on cars improving stopping distances, people are driving closer together.
- **Standardisation of ICT provides a realistic chance to collect risk data**, across applications and systems, across administrative domains. This enables improved risk models and calculation (providing objective, verifiable measures of security and privacy).
- The business trend towards **virtual organisations** will continue. Small businesses and consultants are frequently parts of these virtual organisations, and usually have lower capabilities in trust and security. It will be necessary to secure virtual organisations – secure dynamic service groups. This requires adaptive policy management and complex transactions.
- There needs to be an intelligible **liability framework**. When there is a problem and a liability occurs, who pays – industry or the citizen? Systems have to be robust in the face of corruption.

## **6. Certification, benchmarking and related topics**

- **Benchmarking intrusion detection** is currently difficult as there is a lack of good benchmarks for this area. Benchmarking is generally good for algorithms and products, but not necessarily for less precise systems.
- In biometrics, measurements are clear, but in general the assessment of security is not so good. There are no means of measuring resistance to fake attempts in biometrics. A test protocol is needed. Biometric benchmarking has all been done in the US; **there should be some benchmarking in Europe to take into account cultural factors**.

- **In the area of certification, it would be good to have techniques for formal verification.** Many consider it a grand challenge to make formal methods economically feasible. It can be done at the protocol level, but it is not always used by developers. It can be proved that a specification has been fulfilled, but it is much harder to prove that nothing (i.e. a security error) happens. The challenge is to bring it into daily industrial practices.

It needs to be easy to check security and privacy properties. Current state of the art allows a web service specification to be automatically checked.

- **Certification is needed** – for example, the development of biometrics has been hampered by a lack of levels of certification. For security in complex systems of systems, cost-effective evaluation and certification of systems consisting of components and/or services from different vendors are needed. Models of security and information to promote interoperability between systems are also required.

An international certification authority is required – none currently exists. Enterprises do not have sufficient knowledge of security – this can be addressed by training. Security is seen as a cost, but should be seen as an opportunity. The legal regulation lags behind the technology.

## 7. *Other considerations*

- Applications need to be more “**target driven**” i.e. solve problems than “idea driven” (which creates problems). Enterprise applications have two characteristics – a service orientation, open ASPs, application landscapes allowing third party and legacy applications; and are model driven – common model of business processes and workflow.

- For application level security, something has to be done about the **usability**, especially for the average person, and we need to increase the awareness of the end user and the security administrator. We are not there yet with the SMEs, private users, and government employees. More has to be done to protect business assets, but driven by people’s needs.

Application security is not all new technology – some layers exist and can be exploited. However, applications usually do not have all they need for this – it is a compositional problem. This can be seen when looking at services – they all have different properties, and it is a challenge to combine them.

- **Public e-services and e-government** provide one of the richest scenarios possible for trust and security. However, all aspects of security have to be considered as they are on a very large scale and affect a large number of people, and this range of people

have a wide range of expectations, understanding and competences. As a result, the services must adapt themselves to the users, not the users having to adapt to the services.

- **Mobile and dynamic coalitions** are a way forward. Entities may leave and join, just like virtual organisations. The entities interact, but this is based on trust.
- Strengths and added value can be achieved by combining mechanisms. **Designing for open systems** will make this possible, allowing weaker mechanisms to be combined and for proper fallback mechanisms on failure. Collection of forensic data will allow failures to be analysed and solutions found to continually improve security.

### III. Overall Conclusions and Recommendations

- **There is a strong requirement for an anonymous, secure, network infrastructure.** It is a key component upon which many different applications can be built. It is not clear if there should be one publicly supported infrastructure or several ones that eventually compete in the marketplace. It is likely that several would be developed, possibly with different features. Provided they are well specified and designed, interoperability should not be a problem; gateways will be able to bridge different networks. The normal concern with interfaces is with data being lost across them; with anonymity, loss of identifying data is actually a benefit.

There is a range of possible “identities”<sup>2</sup>. For some applications, real identity is essential, for others, anonymity i.e. lack of identity. However, there are applications for which “virtual identities” are useful – there is not a requirement to identify you, but there is a need to trust your identity. In some applications, the virtual identity needs to remain constant. An example of this is anonymous biometrics, where the source data is fuzzy e.g. a finger, but the identity extracted from it has to be repeatable and remain constant. To illustrate this – in voting in elections, there is a need to ensure that a person only votes once. A voting database may consist of the biometric data of those entitled to vote, but without any information that links the biometric and personal data. Thus, if the biometric data is presented a second time, the vote is invalid (and the person can be arrested, and using his/her finger as the key in the police database, identified).

Another application that requires an anonymous infrastructure is the data collection of actual breaches and threats. In order to gain as much data as possible about the true state of threats and attacks, successful and unsuccessful, we are faced with the dilemma that making this information available is not practical unless done anonymously. Revealing the data provides feedback to the attackers that may allow them to get better at it, and making it public in any way can cause an irrational loss of confidence in an organisation that could be its downfall. Just as the human body mobilises its resources to fight viruses and diseases through the nervous system reporting, so we can envisage an anonymous data collection and analysis system being used to counter threats more rapidly.

- Applications handling **identity management in the public sector** are needed. For some, the real identity needs to be known e.g. if applying for social security benefits, but in other cases, it may be a question of knowing if the person is entitled to something e.g. in drawing social security benefits.

---

<sup>2</sup> Identity in this context means “the state of having unique identifying characteristics”

- Research is needed into the **security aspects of databases** – current designs are untrustworthy and quickly get polluted and compromised.

These create challenges for applications – the tradeoffs between privacy, identity and the societal requirements that these privileges do not apply if used for anti-social purposes. There is a need for the lawyers, human rights champions, sociologists, psychologists, ethicists and technologists to engage in debate and conduct research and trials (not surveys) to get the balances between these right for society in the digital age and compatible with the EU Constitution.

- The development of **reputation based systems** can complement identity based systems. Combination with the “virtual identities” can lead to some interesting and new applications.
- **SLAs** (Service Level Agreements) need to be evolved to take into account security and privacy. Just as IP traffic has developed QoS (Quality of Service) we need to develop additional control parameters, such as SoS (Security of Service), RoS (Reliability of Service) etc.
- **Benchmarking and certification** need to be developed that can give useful comparisons of security and trust approaches and implementations.
- Applications are needed that can demonstrate **strong security through combinations of weak mechanisms**, and that these will scale to large, partially open, and mobile environments.

## **IV. Annex 1 : Agenda**

***09.30– 10.00 Registration and coffee***

**10.00 – 10.20 Opening**

Chair: J. Bus, European Commission

**10.20 – 12.30 Definition of potential future research issues Part I - Brainstorming**

Short presentation by each participant

**12.30 – 13.30 Lunch**

**13.30 – 15.30 Definition of potential future research issues Part II – Discussion and Structuring of the Brainstorming Outcome**

**15.30 – 16.30 Conclusions and next steps**

Chair: J. Bus, European Commission

***16.30 Closure***

## V. Annex 2 : List of Participants

Fred Eisner	ABM
Robert Temple	BT
Sergio Ruiz	Consejo Superior de Camaras
Fabio Martinelli	Consiglio Nazionale delle Ricerche
Urs Gattiker	CyTRAP Labs
Márton Csapodi	E-Group
Michael Waidner	IBM Research Zürich
Nahid Shahmehri	Linköpings Universitet
Casper Bowden	Microsoft
Pierre Chastel	SAGEM
Volkmar Lotz	SAP Research
Gulio Guliani	Selex
Peter Davies	Thales ESecurity
Pierangela Samarati	Universita di Milano
Jeroen van Hoven	University of Delft
Hannes Federrath	University of Regensburg
Stefan Bechtold	University of Tübingen
Pieter Hartel	University of Twente
Jim Clarke	Waterford Institute of Technology
Tony Gore	Rapporteur (Aspen Enterprises)
Jacques Bus	European Commission
Richard Sonnenschein	European Commission
Günter Schumacher	European Commission
Antonis Galetsas	European Commission
Laurent Cabirol	European Commission

## **VI. Annex 3 : Consultation Process**

A first workshop was held on 22 June 2005.

A workshop on “From Grids towards Service-Oriented Knowledge Utilities” was held on the 27-29 September 2005, with follow up meeting on 18 November 2005.

A workshop on “Security and dependability of Software and Services Infrastructures” Brussels 8 December 2005.

This workshop –on the Applications Research ICT for Trust and Confidence Brussels 24 January 2006.

A high level seminar “Trust in the Net” Vienna, 9 February 2006.

## VII. Annex 4 : Glossary and Definitions

With a multidisciplinary approach, and contributions from many areas, there is always the possibility for misinterpretations. Thus, the common understanding of terms used by the majority of people at the workshop is included here for the benefit of others.

Trust	“Accepted dependence”
Security	Confidentiality, absence of unauthorised disclosure of information. Includes integrity and availability, accountability, authenticity and non-repudiation <sup>3</sup> .  Security is protection against deliberate attacks.
Dependability	The trustworthiness of a system that allows reliance to be justifiably placed on the service it delivers.  Dependability is protection against unforeseen failures..
Resilience	Embraces both dependability and survivability, to autonomously and gracefully tackle, adapt, respond, recover, self-heal, reconfigure to accommodate and tolerate upsets, disruptions, failures and attacks.
RFID	Radio Frequency Identification Device – types of devices that can provide identification
Malware	Malicious software designed to infiltrate or damage a computer system without the owner’s consent. Malware is a generic term, including computer viruses, Trojans, worms, spyware and some adware.
DRM	Digital Rights Management – software and/or hardware that restricts access to those who own, or have purchased or rented, rights to access material such as audio and video.
GPS	Global Positioning by Satellite – a system that uses signals from satellites to pinpoint location accurately.

---

<sup>3</sup> This definition is understood by politicians, and so is the definition widely used, even if it is not the best definition.