REPORT on

Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years:

"Protection of Massively Distributed Critical Financial Services" and "Trust in New Value Added Business Chains"

Workshop held in
Frankfurt, Germany
24-25 September 2007

Workshop organised and hosted by
European Commission INFSO, JRC and European Finance Forum

Authors:
Bernhard Hämmerli, JRC European Commission, HSLU and Acris GmbH
James Clarke, Waterford Institute of Technology, Ireland
Henning Arendt, European Finance Forum and @bc®
# Table of contents

Executive Summary....................................................................................................................... 3

1. Session Presentations .................................................................................................................. 4

   1.1 Session 1: Trust in new value-added Business chains ................................................................. 4
      1.1.1 Session Purpose and Goals...................................................................................................... 4
      1.1.2 Session Results ...................................................................................................................... 4
      1.1.3 Discussions of the Work Stream ............................................................................................ 6

   1.2 Session 2: Protection of Massively Distributed critical Financial Services .................................. 9
      1.2.1 Session Purpose and Goals.................................................................................................... 9
      1.2.2 Session Results ..................................................................................................................... 9

   1.3 Session 3: Protection of the Critical Base Infrastructure ............................................................ 12
      1.3.1 Session Purpose and Goals.................................................................................................... 12
      1.3.2 Session Results ..................................................................................................................... 12

2. Panel Session: Workshop conclusions on identifying Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years.............................................................................. 14

   2.1 Panel Session Purpose and Goals............................................................................................... 14
      2.1.1 Overview on subjects raised at the Workshop......................................................................... 14
      2.1.2 Questions raised from the overview statements ...................................................................... 15
      2.1.3 Conclusions on RTD areas that need further work to ensure protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years .............................................................................. 17

3. Final Conclusions ....................................................................................................................... 19

Appendix A – The Organising and Steering Committee Members of the Frankfurt workshop............ 21
Appendix B – Final Agenda ............................................................................................................ 22
Appendix C – Workshop Participant List........................................................................................ 25
Appendix D – Presentations ............................................................................................................ 26
Executive Summary

The rapid growth and deployment of Information and Communication Technologies (ICTs) that we are experiencing today is having profound impact on the financial service industry. On the one hand, the ICT infrastructures over which critical financial services are being delivered are becoming ever more interconnected, open and ubiquitous, but at the same time, ever more fragile and vulnerable to failure and cyber-attacks. On the other hand, over the coming years, it is expected that in the financial sector, the level of self-service will become significantly higher than today, with ubiquitous and mobile banking becoming strong market drivers. Industrialisation, business process outsourcing and number of intervening actors in the service value creation chain will further increase, changing the way financial services will be composed and delivered, while continuing to guarantee their very high-level of trustworthiness. This, in turn, would require: defining trustworthiness and new levels of trust in the ever increasing supply chain, and improving reliability of highly distributed infrastructures while dealing at the same time with severe constraints over business continuity management. Security and privacy in both the clients and the client advisors behaviour will be a key success factor for banking and, more broadly, for the financial industry.

In view of the above, in early 2007, an Organization committee was convened in order to prepare a workshop event on Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years. The workshop was finally held on 24-25 Sept 2007 in Frankfurt, Germany, and attracted nearly 40 attendees from major EU and global financial industry players and key members from the ICT Trust, Security and Dependability (TSD) and Critical information infrastructure protection (CIIP) research communities (academia and industry). The workshop served as an excellent platform for a structured strategic dialogue between these Stakeholders. The focus was on:

- How the situation in the European financial sector will evolve over the next 5 years in the two main themes of the workshop: protection of massively distributed critical financial infrastructures; and, trust in new added value business chains;

- Developing joint scenarios and consequent strategic plans and research directions on how future trustworthy financial services could be constructed and delivered over critical ICT-based service infrastructures and how these latter could be protected from any kind of cyber-threat.

The workshop addressed issues that span beyond a single financial institution or national market. It specifically addressed global, cross border and multi-member state issues and correlations, which may impact or destabilize critical ICT-based financial infrastructures of the European economy.

The workshop outcomes were twofold:

1. Bringing together the relevant stakeholders types (Financial industry, ICT TSD and CIIP researchers) to engage in dialogue and stimulate collaborative research actions in view of the EU's FP7 call for R&D proposals in the area of critical infrastructure protection, including the protection of ICT-based critical financial infrastructures;

2. Provide input to future strategic research directions that the European Commission will support in its next work programme for ICT security Research, for the period 2009-2010.

In the workshop, a number of themes were identified as areas for further mutual research and development between the financial industry and researchers in ICT TSD and CIIP, which are described within this report.
1. Session Presentations

1.1 Session 1: Trust in new value-added Business chains

Chair: Tom Buschmann (TWIST Process Innovations Ltd., UK)

Rapporteur: James Clarke (Waterford Institute of Technology, Ireland)

### Session Participants:

<table>
<thead>
<tr>
<th>Session 1 Part 1.</th>
<th>Session 1 Part 2.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buschmann, Tom</td>
<td>Buschmann, Tom</td>
</tr>
<tr>
<td>Clarke, James</td>
<td>Clarke, James</td>
</tr>
<tr>
<td>Canavillas, Jose Maria</td>
<td>Canavillas, Jose Maria</td>
</tr>
<tr>
<td>Oppenchaim, Serge</td>
<td>Oppenchaim, Serge</td>
</tr>
<tr>
<td>Everling, Oliver</td>
<td>Everling, Oliver</td>
</tr>
<tr>
<td>Adar, Eyal</td>
<td>Adar, Eyal</td>
</tr>
<tr>
<td>Dikkers, Hessel</td>
<td>Sepkes, Eric</td>
</tr>
<tr>
<td>Arendt, Henning</td>
<td>Dürig, Markus</td>
</tr>
<tr>
<td>Svennson, Ulf</td>
<td>Chavarri, Daniel</td>
</tr>
<tr>
<td>Aiguilar, Jordi</td>
<td>Canavillas, Jose Maria</td>
</tr>
</tbody>
</table>

1.1.1 Session Purpose and Goals

The purpose and goals of the session were twofold:

Part 1: Elaborate a number of scenarios or requirements for a Trust Framework in new value-added business chains for the next five years;

Part 2: Based upon the scenarios and requirements in Part 1, discuss and elaborate the current and future research and technological challenges to achieve the Trust framework in new value added business chains.

1.1.2 Session Results

The participants of the first session discussed the focus criteria and centre of gravity of the session theme called “Trust in new value-added Business chains”. They agreed that it was characterised by:

1. Dealing with communities both within and outside EU;
2. Dealing with huge volumes of data, operations, transactions and users;
3. Solutions that are capable of being offered and utilised by multiple entities (e.g. service providers) and not monopolistic in nature;
4. Access to markets and provision of choices. Universal access e.g. equity markets;
5. Need of modelling the execution chain and perform relative risks assessment;
6. Collaboration to aggressively prevent and, if necessary, remedy attacks on the integrity and reliability of the correlated electronic communications;

7. Need of enhancing the end user capabilities for making them as strong a link in the chain as others;

8. Need of End user control and awareness of the operational trust model;

9. Making best possible use of technology capabilities all throughout the value-added chain (banks, other financial institutions and service providers).

These nine focus points were discussed by the participants in more detail, which resulted in the following requirements being elicited by the participants:

1. Predictable and reliable communications between any market participant in a B2B context whilst:
   a. enabling participants to receive information from any source;
   b. enabling participants to provide information to any other party.

2. Easy access to financial services and innovative solutions, within national boundaries as well as cross border

   Clients can now technically trade or purchase stocks across border. Today, however, this is constrained by legal issues. In today and even more in future, it should be possible for new innovative service providers to have ready access (or easily plug-in to) other incumbent providers infrastructures and/or services transparently (e.g. without changing electronic identity) and for end-users to obtain any automated services inside and outside their country with ease. This would dramatically increase the potential for new entrants, especially innovative SMEs, to enter the fast growing markets.

3. Easy access to credit across borders.

4. Easy ability of companies to establish themselves anywhere in Europe.

5. A situation where new innovative and integrated solutions are possible and delivered without these solutions becoming “information-based-monopolies”.
   a. In a world characterised by lack of trust and uncertainties, people rush to safe havens. Market barriers for entry are, therefore, tremendous and monopolies are easily created as a result (almost by default). In an ideal scenario, it would be assured that monopolies do not emerge naturally and that competition within a market economy flourishes.

6. Necessary study and interaction is needed to enable reliable integration of worldwide financial service offerings (i.e. including China and the Islamic region), which means:
   a. A common trust framework irrespective of economic principles or other cultural differences;
   b. The ability to handle potentially exponential growth of information whilst not undermining the trust framework. For instance, ratings of organisations and of processes could be provided to facilitate predictability;
   c. A commonly accepted trust framework based on mutually agreed standards;
   d. Easy integration of new financial service offerings (i.e. Islamic finance, micro credit). This means a common trust framework that enables easy integration that does not affect the quality of the trust framework.
7. A model of collaboration where banks and other interested parties operate at an EU level to prevent and block attacks from “cyber crime”.
   a. This requires a pro-active combination of regulation and technology with stakeholder’s involvement in order to guarantee success.

8. Allowing Users to have more control over their own data.
   a. Readily available information on which data is being used, by whom, for what, …;
   b. Users control over the functionality that is on the interfaces they use (mobile phones, PDA’s, web-based tools etc).

9. A standards-based secure “vault” for each individual user of IT solutions, with the standard defined at EU or global level.

10. Widely adopted technology standards for identity management and authentication, with the standards defined at EU or global level.

11. A trust model that:
   a. clearly defines (1) what it aims to do, (2) which processes it covers and (3) who is authorised to control / authorise what.
   b. can be used to rapidly roll out innovative services throughout their value chain;
   c. is not based on heavy regulation and is not complex, but still meets its purpose;
   d. enables technologies such as SOA to be deployed by banks;
   e. enables users, businesses or service providers to define and publish their requirements such that third party service providers can have the capability to implement rapidly what is required;
   f. minimises the negative impacts of interdependence and inter-connection between users and the chain of their service providers.
   g. enables an easy creation, deployment and control of “value-added chains”, where:
      i. service providers can easily be “plugged in” and support, for instance, banks in parts of their business processes.
      ii. In order to allow this to happen, the necessary data is not just stored with one or two service providers but with the users themselves.
   h. enables the use of the mobile device for trustworthy financial transactions;
   i. can be based on mobile terminals that:
      i. can be in one instance a host, in another a terminal and in others, a communications bridge.
      ii. enable the users to securely use their mobile device anywhere at any time or be timely warned whenever this is not the case.

1.1.3 Discussions of the Work Stream

After brainstorming on the detailed scenarios, the group decided to first categorise the scenarios into a number of high level research topics upon which the key challenges and issues could be brainstormed. These high level topics included the following:
• Addressing the Quantification/Scale issues – Information overload, dynamicity and complexity of systems. Can we look at it from another perspective and use the large amounts of available data in order to quantify/adjudge the risks or levels of crime increase/decrease. (points 1 to 4 above)
• Widening and different areas of players/counterparts e.g. foreign/non foreign, banks/service providers, Technologists and User Aspects – more access, control of their data (covered across most points);
• Consideration of the Global Dimension (points 4,7,8).
• Definition and design of trust elements (models, authority, metrics to enable measurement and rating of CIP layers of protection, etc.) – (point 11 above).

In the second session, the participants brainstormed and discussed the major immediate and future challenges that need to be tackled in order to realise a Trust framework in new value-added business chains. These challenges are highlighted below:

1. **Trust, especially in the financial systems infrastructure**, is a global challenge: Identifying institutions that build up trust – whom we can trust and who earns trust. Empirical question of who builds up trust? Trust Authority Model: Trusted Authority needs definition of liability and then you can use it in a constructive way. Is it banks, is it government, is it safe?

2. **Trusted collaborations** Collaboration with third parties and dealing with communities both within and outside EU (new players that change the rules bring the need to adapt to these rules and do business with them; and, need to be collaborative between countries, and not limited to EU only). Furthermore, banks should evolve to be the partners of the business.

3. **Optimised / New business processes** Secure and Critical cores of businesses need larger distribution. There is also a factor of High volume and speed. Quantities are changing qualities – millions/billions using it so critical mass is creating changes. Need to think how to get high performance at low cost; how to unify the natural processes with the banking processes (both from technical and organisational way); how to catalyse creation processes by getting people together that don’t ordinarily work together; how to break economic monopolies by identifying new potential users, new applications; how to mix and combine banking businesses; how to develop a model for business impact.

4. **Business Ratings and Regulation** Clear observation of Ratings and Ranking industries build up. Need to think about new areas of observation and regulation (both soft regulation and Gentleman’s agreement). Need for structuring of information for selection and rating structures. Credit ratings parameters need to be researched and built – semantic, grid systems to simulate the ratings that are being provided. The need for processes and means for quicker response times in emergency cases.

5. **Empowering the end-users** End user capabilities and giving more power to end users: What are the expectations of the customers? Does it include the ability for them to refuse the technical ways we can suggest? Also, establishing “User friendliness” of our TSD solutions. End user should be part of the model descriptions from the start.

6. **Two-side authentication** (of users and clients at the same time) and **Anonymity aspects** (who will manage this? EU, Trusted Third Party Association?)

7. **Security of Systems** Banks communication systems need to be studied. There is need to protect the extranet with firewalls while dealing with huge volumes. There is a need to create or increase confidence in internet based systems in general. As we increase speed and magnitude and things get more complex, we need to redefine the risk criteria. Therefore, we need new modelling techniques for risk to deal with quantification in this new environment. There is also a need for more reliability on software models and for investigating the use and impact of Open source software in the banking sector. Regarding using the mobile terminal for data vaulting, the large challenge is not only to standardise the vault data, but also today's mobiles are not broadly equipped with the necessary features to support this concept of mobile data vaults.
8. **Interdependencies** There is need to understand the interdependencies between the multi-point, multi-distribution environment. Electricity could serve as example for ensuring and rating the CIP layers of protection.

9. **Cyber crime** is developing on the basis of mobility and speed. There is a need for further research on modelling of attacks, on phishing (identification and avoidance and stamping out of phishing), and on developing a concept of a minimal tolerance to attacks and faults.
1.2 Session 2: Protection of Massively Distributed critical Financial Services

Chair: Sandy Porter (Avoco Secure, UK)

Rapporteur: Tobias Christen, (Zürich Financial Services, Switzerland)

Session Participants:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Porter, Sandy</td>
<td>Porter, Sandy</td>
</tr>
<tr>
<td>Christen, Tobias</td>
<td>Christen, Tobias</td>
</tr>
<tr>
<td>Riguidel, Michel</td>
<td>Riguidel, Michel</td>
</tr>
<tr>
<td>Malek, Miroslaw</td>
<td>Malek, Miroslaw</td>
</tr>
<tr>
<td>Olivero, Sergio</td>
<td>Olivero, Sergio</td>
</tr>
<tr>
<td>Bus, Jacques</td>
<td>Bus, Jacques</td>
</tr>
<tr>
<td>Kotrotsios, George</td>
<td>Dikkers, Hessel</td>
</tr>
<tr>
<td>Pujol, Fernando</td>
<td>Arendt, Henning</td>
</tr>
<tr>
<td>Schreiber-Handschu, Frank</td>
<td>Svennson, Ulf</td>
</tr>
<tr>
<td>Vilanova, Marc</td>
<td>Aigular, Jordi</td>
</tr>
</tbody>
</table>

1.2.1 Session Purpose and Goals

The purpose and goals of the session were to examine the research challenges involved in:

- Trusted sharing of confidential information in massively distributed financial infrastructures.

Other goals pursued by the participants included the following:

- Identity federation in the supply chain based on trust levels that each participant needs to reach through certification.
- During disaster modes, which are characterised with transient organisational phases, there are increased risks and significantly less time to deal with them. Throughout these phases, often the additional risks and lower levels of trust are neither controlled nor internally communicated.
- Society needs to profit from convergence, for example tracking and localisation of goods
- Self healing systems, systems designed for flexibility. Individual nodes should have more intelligence. Self-conscious nodes.
- Accepted polymorphic identities: for each identity representation, some attributes are mandatory others are discretionary.

1.2.2 Session Results

The observations were confirmed, which were mentioned on day 1 in several presentations, namely

- Socio economic trends drive towards
  - Online accessible real-time services
Further industrialization and commoditization of financial service supply chain
- Privacy protection for customers
  - Exposure to online organized crime requires new approach to security modelling into business logic (misuse cases)
  - Catastrophic events transiently change risk appetite, meaning that trust (to devices and individuals) increases during recovery phase without trustworthiness having changed
The group then discussed the impact of these observations on the financial infrastructure. It was argued that the industry looks for federation of identities in market places (single sign on) as well as for supply chain integration (trust delegation). In B2B scenarios, some participants proposed that a European Agency would offer such a federation service.
The individual citizen, however, would like to prevent that relationships between her single (trans)actions can be established and prefers several separate identities, and more explicit choices of what can be done with her information. In the consumer world, we might look at more and more free services (paid by advertisement) with virtually no privacy and as an alternative paid service with guaranteed privacy. The request towards the legislation is to force service providers to offer greatest flexibility how each information item is handled.
Exposures to risks around online organized crime as well as catastrophic events require tested and reliable modes of information sharing between international enterprises, which imply that state driven crisis management frameworks can not stop at the national boundaries either.
Increasing distribution and connectivity in the infrastructure will ask for systems that are designed for reliability and contain the intelligence to cope with extra-ordinary situations. This creates new challenges in terms of distributed intelligence and interoperability. Last but not least resilient and cost-effective management of multi-owned infrastructures poses new challenges as we see a move from exception management to performance management that detects service degradations.
Prevention of identity theft was the foremost discussion topic that all participants have seen as a key challenge. Clear standards on how identity information needs to be protected and when strong authentication is required would help. It is essential that the risk is not transferred to the consumer when careless service providers go for the cheapest option.
Rather than promoting (state sponsored) single identity representations, we should allow for polymorphic identities and correspondingly bring more convenience into handling multiple identities. Another interesting opportunity could then be to increase the trust level by combining 2-3 identities that are semi-trusted to reach a higher trust level.
The group discussed that like in other science domains (e.g. pharmaceutical), it would be desirable to nurture a venture capitalist funded environment where IT driven financial services innovation are created and financial service providers are increasingly investing into IT enabled European innovation potential.
During crisis management, the normal "powers reserved" are enhanced to guarantee fast recovery and response. A number of examples were discussed to illustrate this point. One example would be "procurement of replacement equipment": normally, a procurement process takes weeks or even months; in a disaster recovery situation it may only take hours. Another example is a change management and configuration management process. Basically they both are geared to sustain an organization's IT landscape in the mid and long term. In a disaster recovery situation, however, the short term survival rules over fixed procedures. In a well organized environment the corresponding "emergency processes" are predefined (not necessarily widely communicated though).
New dimensions of scalability were discussed in several contexts and it was argued that for true scalability it must be possible to design systems without a single dispatching or single back-end system.
1.3 Session 3: Protection of the Critical Base Infrastructure

Chair: Michael Samson (Netherlands Bankers' Association, The Netherlands)
Rapporteur: Rafael Navajo (GMV, Spain)

Session Participants:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Samson, Michael</td>
<td>Samson, Michael</td>
</tr>
<tr>
<td>Navajo, Rafael</td>
<td>Navajo, Rafael</td>
</tr>
<tr>
<td>Hans-Peter, Königs</td>
<td>Hans-Peter, Königs</td>
</tr>
<tr>
<td>Masera, Marcelo</td>
<td>Masera, Marcelo</td>
</tr>
<tr>
<td>Bendisch, Uwe</td>
<td>Bendisch, Uwe</td>
</tr>
<tr>
<td>Sepkes, Eric</td>
<td>Kotrotsios, George</td>
</tr>
<tr>
<td>Dürig, Markus</td>
<td>Pujol, Fernando</td>
</tr>
<tr>
<td>Chavarri, Daniel</td>
<td>Schreiber-Handschug, Frank</td>
</tr>
<tr>
<td>Skordas, Thomas</td>
<td>Vilanova, Marc</td>
</tr>
<tr>
<td></td>
<td>Grauer, Thomas</td>
</tr>
</tbody>
</table>

1.3.1 Session Purpose and Goals

The purpose and goals of the session were to discuss the challenges associated with the following topics:

- End-user protection in a highly distributed environment (mobility);
- Secure communication channels (current and future Internet);
- In a catastrophic disaster, recovery critical infrastructure methods;
- Regulatory issues, collaboration environment.

1.3.2 Session Results

During the session, multiple issues arose related with the security of critical Infrastructure.

The group was organized in 2 parts; during the first one, the group tried to identify the different scenarios where the Protection of a Critical Infrastructure could be required. In the second part, the group discussed the challenges associated with these scenarios and related RTD topics.

SCENARIOS

In the first part of the session, the group identified the following scenarios summarized below:

**End-user protection in a highly distributed environment (mobility):** Mobility is becoming one of the main differentiators within the financial services, providing the end user to access to the financial services anytime, anywhere. This situation creates also some security deficiencies, related mainly with user terminals, privacy, malware detection and reaction, etc.
Secure communication channels (Internet), this was one of the most controversial scenarios, taking into account that the secure communication channel is in principle part of the supposed Internet security infrastructure and protocols topic. It was noted by some group members that it could not be part of this R&D initiative.

In a catastrophic disaster, critical infrastructure recovery methods: One of the main concerns is related with the critical single points of failure, what could happen in case one of the main European infrastructure nodes would be down, how could the rest of the infrastructure recover from such a situation.

Regulatory issues, collaboration environments. Define a collaborative framework, managed and controlled by automatic processes that keep up-to-date every individual European entity (banks, government, police, etc.) with the possible threats environment.

DISCUSSIONS

Once the possible scenarios were defined, during the second part of the session, the team identified the main challenges associated within those scenarios.

One of the main goals are the personal data protection (privacy), the way to define an identity and authentication management that guarantees the security within the user access taking into account the mobile environment.

In addition to the protection of personal data and to having strong authentication methods, the quality of service and service availability are also important challenges to be discussed and analyzed within the scenarios defined above.

One of the main concerns of financial entities is related with the real time proactive and trusted data sharing environment, the possibility to define a federation system where the financial entities could share threats, risks and some other important information in order to apply the pertinent protection measurements.

In order to go ahead with the previous topic, one important goal is the standardization, within the different interfaces, but also the interface standardization between communication entities.

Risk assessment and risk modelling were also some important topics discussed during the session, identifying possible risk and quantifying the impact based on those risks. For this topic, one important research area is the attack simulation and the possibility to identify cascading effects.

Other important topics discussed during the session included the following:

- European regulatory and laws enforcements
- Resiliency, redundancy, reliability of highly distributed financial environments
- Advanced behaviour detection, prevention and reaction mechanisms (i.e. heuristic analysis)
- Robust segmentation (of services and applications)
- Managing the organization of business aspects following merging of companies
2. Panel Session: Workshop conclusions on identifying Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years

Chair: Mr. Oliver Everling, Rating Evidence GmbH, Germany
Rapporteur: James Clarke, Waterford Institute of Technology, Ireland

Panel Participants:

<table>
<thead>
<tr>
<th>Name</th>
<th>Position/Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hessel Dikkers, ABM Amro, CIO</td>
<td>Michel Riguidel, ENST Paris, Professor Head of Dept. of Comp. Science and Networks</td>
</tr>
<tr>
<td>Sandy Porter, Avoco Secure, Founder and Director</td>
<td></td>
</tr>
</tbody>
</table>

2.1 Panel Session Purpose and Goals

The purpose and goals of the final panel session were to comprehensively review the workshop conclusions from the panellists’ perspectives and to open up the discussions within the plenary session to decide the best way forward.

2.1.1 Overview on subjects raised at the Workshop

- Hessel Dikkers, CIO NL of ABM Amro,
  It is clear that we are all focussing on a number of important problems that need to be solved. They have a wide and broad scope, including, for example, hacking, Business Continuity Management, scalability, numerous barriers in countries both on national and international levels, etc.
  We are struggling with the issues and challenges with a growing sense of urgency since we are seeing more and more attacks occurring. There are a number of areas that we need to collectively work on including: EU level collaboration, International collaboration, regulatory frameworks, and finding a political common ground in order to face these important topics. Facing these non-technical areas could even be considered more important than the technology and innovation areas.

- Marcelo Masera, JRC, European Commission, leader of actions on CIP
  It was evident from the discussions in the two days Workshop that considering the financial systems as Critical Infrastructure is highly complex and with many different facets. There are many actors/stakeholders involved and many levels of discussions – national, International, business, consumers, etc. Some solutions are well understood and underway, but there are many problems still not fully understood that need further research and exploration. In next 5-10 years, we need to understand these problems and develop necessary and robust solutions.

- Sandy Porter, Avoco Secure, Founder and Director
  It was interesting to see the balance of comments between the Academia and financial industrial stakeholders. The difficult issue is to deliver for all stakeholders involved what they need to solve the problems quickly in some cases starting from scratch and work their way up to final solutions. Is there something from the Framework Programme calls to enable this kind of fruitful activity? The EU has
clear key advantages and there are some potential advantages for all stakeholders that can provide short and long term gains by participating. The level and enthusiasm of the participants seem to indicate these efforts could reach fruition. Bringing the two groups together to work on short and long term goals is a very important objective.

Michel Riguidel, ENST Paris, Professor Head of Dept. of Comp. Science and Networks

The presentations over the last two days demonstrated the innovation nature of the participants, exhibiting points of views that were diverse when compared to the usual EU meeting presentations. The Industrial stakeholders and Academia need to work closely together to get a more common view and approach to addressing these huge challenges as discussed at the Workshop. Over the last days, we have been talking about multi-discipline and multi-faceted areas including technology, markets, consumer’s issues and innovation. We need to further work starting with collaborative R&D on various topics including Trust models, security, and business models amongst others even though these can be considered as moving targets.

Lutz Raettig, Vorsitzender des Aufsichtsrates / chair of the board of Morgan Stanley Bank AG and the Frankfurt Stock Exchange Council

With regard to IT systems, 30 years ago, there was only Human Resources (HR) and IT departments. Within the HR department, everyone understands everything but the IT person in charge was generally the only one that understood the IT systems. This has not changed very much in scope but in concepts and complexity. The two most important resources are still HR and IT but the IT infrastructure now delivers secure services, databases and communications channels, which requires many more people to understand the inner workings of the systems in place.

It has become abundantly clear that Business continuity management is fundamentally relevant (due to attacks, network overloads, etc).

Another interesting challenge from the IT systems perspective is the decision of what to keep in-house and what to outsource. The issues are that decisions need to be made about how much know-how you want to put in the domain of someone else external to your organisation.

Another fundamental change is people and/or organisations that were not talking to each other before (ie. Competitors) are now talking regularly in relevant forums such as the European Finance Forum. This can only be considered a positive development as many of these issues and challenges can and should be addressed in a mutually beneficial collaborative and, hence, more efficient way.

Management outsourcing is another new facet we are seeing in the Industry. The commonality amongst the constituents is that all banks have to make money. If they all start to follow the same standardized ways of in-sourcing and outsourcing, for example, which data is allowable to be given away, this would be an interesting and complex challenge. There is a need to balance between security and complexity.

Another major challenge is the role of the regulator. We all have limited capacity to run IT systems so the regulator will have a dominant role to play.

2.1.2 Questions raised from the overview statements

Q. What is the role and importance of the CIO of a banking organisation?

Hessel Dikkers, ABM Amro, CIO

The CIO role is an important one dealing with not only IT systems, but with Business continuity and Agility, and IT in-sourcing, out-sourcing and off-shoring. For Agility, the industry needs to have the
regulators involved. However, this is a conundrum as this will both help the industry yet make difficult certain other items e.g. new business models must be put through mandatory (e.g. Basel II) processes.

**Q. What other agencies/areas would be considered vulnerable?**

- Marcelo Masera, JRC, European Commission, leader of actions on CIP

Criminals and organised crime are a key issue/threat in terms of vulnerabilities. Terrorism and related activities cannot be ignored. We would be making an error to just look at present and past activities and not consider potential future malicious elements that need to be addressed. We need to make efforts to relate all these aspects in order to address Business continuity management and CIP. It should be recognised that the Governments and the regulators don’t want to interfere with the private sector but the problems are very complex and need to be dealt with at all proper levels. The structure of the models of society and flows that have been used in the past are no longer efficient any more. We need new means for handling security and Finance Industry CIP.

**Q. How vulnerable do you see the EU financial system to political actions by other states or countries e.g. US in 2002 turned off data on Iranian banks for rating data.**

- Lutz Raettig, Vorsitzender des Aufsichtsrates / chair of the board of Morgan Stanley Bank AG and the Frankfurt Stock Exchange Council

The vulnerability is in clearing and settlements agencies where scale is the name of the game. In the EU, we are concentrating on establishing more flows for clearance, but this is running a fine line. In the U.S. banks, their approach has been to have one clearing agency, which may be quite vulnerable. Within the EU, it takes a different approach and due to competitive rationale, the feeling is that we need as many as possible. However, for cost, practicality and technical reasons, you cannot have as many. In addition, there are significant globalisation issues, which restrict how many clearance agencies you can feasibly have.

**Q. In Germany, there is an initiative to orchestrate the exchange of ideas and developments for Infrastructure protection of financial and other areas. Should there be someone taking this role in EU?**

- Marcelo Masera, JRC, European Commission, leader of actions on CIP

In the European Commission, as already mentioned by Jacques Bus, there is a programme under debate regarding an EU approach but it is recognised that this will not be a quick process and this is a very new and revolutionary approach being debated. Therefore, it is encouraged that the private industry does not wait for this programme so they should act right away in a collaborative way instead.

- Lutz Raettig, Vorsitzender des Aufsichtsrates / chair of the board of Morgan Stanley Bank AG and the Frankfurt Stock Exchange Council

While this kind of EU wide programme would be welcomed, in addition to this programme coming into play, it is also recognized that politicians should be in a position to set the guidelines and industry in collaboration with academia should work on the details.

**Q. There are significant costs associated with regulatory compliance issues while at the same time there are ever decreasing IT budgets. How do you balance these two issues?**
Banks have no other choice but to comply with regulations. Therefore, it is mandatory that there is investment in these areas that will consequently raise IT costs. However, there are other areas where the IT costs are or may be going down. So, there will potentially be a small balance of the overall IT costs.

Sandy Porter, Avoco Secure, Founder and Director

In the wider perspective, it is very good to see a CIO and CEO in the panel who both recognise the real benefit of the IT security budget. “Does security pay?” is the big question. It is a real conundrum in that it very much matters when a real attack occurs and, unfortunately, we will find some companies using the “head in the sand” approach out there.

Q. From an entrepreneurial perspective, to what extent are IT costs on a level playing field between the smaller companies and the larger players, and to what extent are regulatory requirements on a level playing field with SMEs and larger companies?

Hessel Dikkers, ABM Amro, CIO

IT costs are compared related to revenues are benchmarked regularly. From the resource perspective, there are vast differences. If interested in effective risk management, there are many differences in approaches between the various Institutions. They each have to make their own judgement calls.

Q. Governments have a tendency to throw money at problems, but companies take a different approach. In this Workshop, there was a refreshing tendency to share the common requirements and come up with mutual solutions with a potential for a lower collective cost. How can we turn what was accomplished at the Workshop in order to maximise the leverage potential and provide innovative and cost effective solutions with current participants and/or potentially other participants who were not attending this event?

Marcelo Masera, JRC, European Commission, leader of actions on CIP

One year ago, there was a similar meeting with the Power industry and, initially, they were sceptical about the chance of progress but they have continued working together, and a new meeting is planned for November 2007.

Lutz Raettig, Vorsitzender des Aufsichtsrates / chair of the board of Morgan Stanley Bank AG and the Frankfurt Stock Exchange Council

We are creating an interdisciplinary approach to the finance industry approach to CIP, marketing from mathematical perspective, behavioural, technical, social and economical point of view. It took a long time to discover that although there is a competition factor, we definitely need to leverage the commonality between the institutions to everyone’s benefit.

2.1.3 Conclusions on RTD areas that need further work to ensure protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years

Hessel Dikkers, ABM Amro, CIO
A framework should be arranged at the EU level where trade will be [better] between the EU countries. The areas of most interest over the last two days are:

1. The ratings mindset, where there could be a trust rating amongst companies that are trading with each other and the related technologies;
2. Identity management and the associated technologies;
3. Securing the customer device and identification, prevention and stopping of the attacks.

- Marcelo Masera, JRC, European Commission, leader of actions on CIP

There will be significant added value if the workshop leads to a further setting up and continuity within the stakeholders in this community (Industry, Governments, Academia, etc.). Once set up, we can start to plan various activities e.g. Annual workshops, projects, seminars, newsletters, etc.

- Sandy Porter, Avoco Secure, Founder and Director

EU has the potential to create a standard across borders with respect to identity and security. We should try to capitalise on this and bring in the required stakeholders to address and deliver within the EU.

- Michel Riguidel, ENST Paris, Professor Head of Dept. of Comp. Science and Networks

Security, dependability and trust are words that are very cultural based from country to country. Identity, etc. are fundamental concepts and within the EU, we have the opportunity to federate and orchestrate our key strong points and values and put these into our security models. This could facilitate the research, development and implementation of trust infrastructures throughout the EU, and the world. In order to keep our human values, the various stakeholders need to work together: Industry, Government, and Academic. We should not reinvent the wheel but to look at the problems and not just use solutions that you find in classical textbooks but to look ahead at other innovative solutions. We need to think differently and within the next few months, to build an open consortium to exchange expertise between nations and sectors to solve immediate problems and also work on long term solutions. It is important for Europe to be at the top for these new technologies.

- Lutz Raettig, Vorsitzender des Aufsichtsrates / chair of the board of Morgan Stanley Bank AG and chair of the Frankfurt Stock Exchange Council

Security is a common problem amongst the financial industry members. Therefore, we need to work together in a common and unified way to save on resources. The increasing interplay between institutions and clients, and the shift from personal bank visits to internet banking causes a lot of challenges that need to be addressed. The industry is quite interdependent with respect to risk processes because the risks are similar in each institution and incidents of one community member radiate to others in the same market place. Redistributing identified risks within the financial community is a key issue to progress in security and dependability issues. The risk dimension is perceived as very important and we need to understand risk nature in deeper detail and better. Furthermore, means for risk communication and classification should serve to distinguish between singular risks and multiple risks.

Identification of risks that can be turned into a systemic risk is essential for progressing in the direction of risk effort minimization.

In summary, there is a resounding call for joint efforts and actions on all sides – political, industry and academic collaboration is very crucial here for success.
3. Final Conclusions

The workshop held on 24-25 Sept. 2007 brought together the stakeholders in the Financial Industry and the European RTD community members from ICT Trust, Security and Dependability and Critical Information Infrastructure Protection. The event made it abundantly clear that a significant amount of R&D must take place in a coordinated fashion in order to protect massively distributed Critical Financial Services and provide trust in new Value Added Business Chains.

The outcomes of this workshop included the following:

- In each of the scenarios, new technologies and associated risks were identified;
- Exposure to online organized crime requires new approaches to be addressed;
- Secure communication channels are required (current and future Internet);
- Regulatory issues in collaboration environments need to be addressed;
- Significant joint efforts of academia, stakeholders and regulators are needed.

Within the intensive working group sessions of the workshop, a number of scenarios, requirements and research topics were elaborated, discussed and considered in three dedicated Theme-based sessions. These were found to be beneficial and necessary for continued mutual collaboration between the stakeholders. The main outcomes of each session are as follows:

**Session/Theme 1: Trust in new value-added Business chains**

- **Trust and trusted collaborations**, especially in the financial systems infrastructure, is a global challenge:
  - Optimised / New business processes, which are secure and critical in larger, faster and more complex environments and its distribution.
  - Business Ratings and Regulation require clear observation of Ratings and Ranking industries and new areas of observation and regulation;
  - Empowering the end-users with enhanced capabilities and giving more power to End users. Examination of the expectations, roles and awareness of the customers is required from the start;
  - Two-side authentication (of users and clients at the same time) and Anonymity aspects (who will manage this? EU, Trusted Third Party Association?)
  - Security of Systems including internet-based, mobile-based, Banks communication and other financial infrastructure systems need to be studied;
  - Interdependencies between the multi-point, multi-distribution environment. Electricity could serve as example for ensuring and rating the CIP layers of protection.
  - Cyber crime is developing on the basis of mobility and speed. There is a need for further research on modelling of attacks, on phishing (identification and avoidance and stamping out of phishing), and on developing a concept of a minimal tolerance to attacks and faults.

**Session/Theme 2: Protection of Massively Distributed critical Financial Services**

- Socio economic trends drive towards:
  - Online accessible real-time services;
  - Further industrialization and commoditization of financial service supply chains;
  - Privacy protection for customers;
- Exposure to online organized crime requires new approach to security modelling into business logic (misuse cases);
- Catastrophic events are characterised by transient organisational phases with increased levels of risk and significantly less time to deal with them. Throughout these phases, often the additional risks and lower levels of trust are neither controlled nor internally communicated;
- Block attackers: Deception, counterattacks, international collaboration;
Internationally coordinated law enforcement;
Protection and competitive advantage through investing with small innovative companies;
3 corrective actions: Protect the brand; Collaboration; and, Inform Public;
Collaboration in both reactive as well as pro-active areas;
Identity management:
  o Need for Polymorphic identities: We are citizen, consumer, employee, patient, bank customer, etc;
  o We need to improve the fundamentals of identity;
  o Combine 2-3 identities that are semi-trusted to reach a higher trust level;
  o European agency as the federator for ID mgmt systems in B2B scenarios;
  o Passports are voluntary…. ID cards are mandatory;
  o Liability for B2B transactions is bound to strong identification;
  o Some identity attributes are core/mandatory others are discretionary;
  o Under the new upcoming telecom law, victims need to be informed about possible data breaches.

Session/Theme 3: Protection of the Critical Base Infrastructure
• Personal Data (privacy) protection, improvements in identity management and authentication methods, considering a mobile environment (anytime – anywhere);
• Quality of Service + Availability;
• Real Time Proactive and Trusted data sharing environment between financial and non financial entities (federation of trusted relations);
• Interfaces standardisation, risk assessment, risk modelling;
• Attack simulation facilities (cascading effects);
• European regulatory and laws enforcements;
• Resiliency, redundancy, reliability of highly distributed financial environment;
• Advanced behaviour detection, prevention and reaction mechanisms (heuristic analysis);
• Composition of trust;
• Robust and secure segmentation (of services and applications);
• Managing the organization of business aspects following merging of companies.

Throughout the workshop, a number of realistic cooperation mechanisms were presented by the European Commission. These could benefit the bringing together of the financial industry stakeholders with the communities of SDT and CIP researchers and help build up stronger and fruitful collaborations in the future. The organisers intend to follow up on these activities.
Appendix A – The Organising and Steering Committee Members of the Frankfurt workshop

Steering and Organizing Committee
Henning Arendt, Chair of European Finance Forum and @bc®
Bernhard Hämmerli, JRC European Commission, HSLU and Acris GmbH
Thomas Kohler, UBS
Thomas Skordas, European Commission, Information Society and Media, DG INFSO, Unit "Security"

Chairs Group during the meeting:
  Tom Buschman, TWIST
  Sandy Porter, Avoco Secure
  Michael Samson, Netherlands Bankers’ Association

Rapporteurs Group during the meeting:
  James Clarke, Waterford Institute of Technology (Group 1 and Panel)
  Tobias Christen, ZFS (Group 2)
  Rafael Navajo, GMV (Group 3)

Main author of this report
  James Clarke, Waterford Institute of Technology
Appendix B – Final Agenda

Time: Monday, September 24, 2007, 14:00h, to Tuesday, September 25, 2007, 16:00h
Venue: Bloomberg, Neue Mainzer Strasse 75, 63011 Frankfurt am Main

Programme September 24, 2007

14:00 Introduction
Barbara Wisch, Bloomberg
Henning Arendt, Chair of European Finance Forum
Bernhard Hämmerli, JRC European Commission, HTA and Acris GmbH

14:05 Welcome and the CIO’s view, Hessel Dikkers, CIO ABN AMRO


14:45 – 16:15 Session 1: The viewpoints of the Financial Stakeholders
14:45 New ICT Based Business Value Chains and Associated Security Challenges
Bernhard Hämmerli for Thomas Kohler, UBS
15:00 Instant Payment and its Impact on User Expectation and Infrastructure Design
Eric Sepkes, Citi
15:15 Future of Risk-based Security Architecture Design
Tobias Christen, Zurich Financial Services
15:30 European Financial Risk in Respect to the Global Financial Systems
Sandy Porter for Gary Greenwald, Citi
15:45 Turning Protective Clubs of Banks into Open Centres for Innovation
Tom Buschman, TWIST
16:00 High Impact and Low Likely Correlated Incident, e.g. Business and Infrastructure
Michael Samson, Netherlands Bankers’ Association, Advisor Information Technology
16:15 Vision for Future Security in ICT Based e-Payment and e-Settlement
Hans-Peter Königs, former CSO of Telekurs
16:30 Break

16:45 – 18:15 Session 2: The viewpoints of ICT Industry and Researchers
16:45 Enabling Identity - the key to maintaining privacy, control and security of information
Sandy Porter, Avoco Secure
17:00 Trust and Trustworthiness in Service Infrastructures and Technologies for Improving Trust levels, Jose Maria Cavanillas, Atos Research & Innovation
17:15 Future Security/Trust Issues for Financial Systems & Services  
Neeraj Suri, TU Darmstadt
17:30 Technology Evolution and New Security Challenges  
Michel Riguidel, ENST Paris
17:45 The Evolution of On-Line Fraud. New Challenges  
Daniel Chavarri, S21Sec Labs
18:00 Break
18:15 – 18:45 Discussion
18:15 First discussion and preparation of Day 2 around "Trust in new value-added Business chains, "Protection of Massively Distributed critical Financial Services", and “Protection of the Critical Base Infrastructure”
18:45 Discussion setup, structure and goals of day 2
18:50 Closing Remarks Day 1: Henning Arendt / Bernhard Hämmerli
19:30 Dinner at Klaane Sachsehäuser,  
Neuer Wall 11, 60594 Frankfurt; Phone: 069/615983; ca. 30 min. walking distance.

Programme, September 25, 2007

8:30 Keynote Master Plan CIP Germany: Actions in the Finance Sector and the (Inter-) Relation to other Sectors  
Markus Dürig, Federal Ministry of the Interior, Germany
9:00 4 short Presentations of Visions
9:00 The IT-GRCM key Challenges: Bridging the Babel Languages Gap (Governance Risk and Compliance Management)  
Eyal Adar, White Cyber Knight ltd.
9:10 Future scenario and associated risks: Hedge Funds  
Ulf Svennson, CQS
9:20 How Critical is the Rating Industry for a Sustained European Finance System?  
Oliver Everling, Rating Evidence GmbH
9:30 Modelling of Interdependencies  
Uwe Bendisch, Fraunhofer SIT
The German Savings Banks Approach  
Frank Schreiber-Handschug, Deutscher Sparkassen und Giroverband
9:50 Introduction for Scenarios and Future Challenges  
Bernhard Hämmerli, European Commission Joint Research Centre
10:00-10:20 Break
10:20-11:50  Discussion in Break out Groups on Scenarios
The basic aim will be to predict possible future infrastructure and processes and their associated risks.

- **Group 1**: Trust in New Value-added Business Chains  
  Chair: Tom Buschman, TWIST; Rapporteur: James Clarke, Waterford
- **Group 2**: Protection of Massively Distributed Critical Financial Services  
  Chair: Sandy Porter, Avoco Secure; Rapporteur: Tobias Christen, ZFS
- **Group 3**: Protection of the Critical Base Infrastructure  
  Chair: Michael Samson, Netherlands Bankers' Association; Rapporteur: Rafael Navajo, GMV

11:50-13:00 Break

13:00-14:30 Discussion in Break out Groups on Present and Future Challenges

- **Group 1**: Trust in new value-added Business chains,  
  Chair: Tom Buschman, TWIST; Rapporteur: James Clarke, Waterford Institute of Technology
- **Group 2**: Protection of Massively Distributed critical Financial Services  
  Chair: Sandy Porter, Avoco Secure; Rapporteur: Tobias Christen, ZFS
- **Group 3**: Protection of the Critical Base Infrastructure  
  Chair: Michael Samson, Netherlands Bankers' Association; Rapporteur Rafael Navajo, GMV

14:30-14:45 Break

14:45-15:45 Panel, Conclusions, Future Actions
Moderator: Oliver Everling, Rating Evidence  
Rapporteur: James Clarke, Waterford Institute of Technology

Hessel Dikkers, ABN Amro  
Marcelo Masera, JRC, European Commission  
Sandy Porter, Avoco Secure  
Lutz Raettig, Morgan Stanley Bank AG  
Michel Riguidel, ENST Paris  
Ulf Svennson, CQS  

Moderator: Oliver Everling, Rating Evidence GmbH

15:45 Next Steps — The Executive View
Lutz Raettig, Vorsitzender des Aufsichtsrates / chair of the board of Morgan Stanley Bank AG and the Frankfurt Stock Exchange Council

16:00 Plan your departure from the venue
## Appendix C – Workshop Participant List

<table>
<thead>
<tr>
<th>Name</th>
<th>First</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adar</td>
<td>Eyal</td>
<td>ITCON LTD.</td>
</tr>
<tr>
<td>Aiguilar</td>
<td>Jordi</td>
<td>La Caixa</td>
</tr>
<tr>
<td>Arendt</td>
<td>Henning</td>
<td>European Finance Forum</td>
</tr>
<tr>
<td>Bendisch</td>
<td>Uwe</td>
<td>Fraunhofer SIT</td>
</tr>
<tr>
<td>Bus</td>
<td>Jacques</td>
<td>European Commission, INFSO</td>
</tr>
<tr>
<td>Buschmann</td>
<td>Tom</td>
<td>TWIST Process Innovations Ltd.</td>
</tr>
<tr>
<td>Canavillas</td>
<td>Jose Maria</td>
<td>Atos Research</td>
</tr>
<tr>
<td>Chavarri</td>
<td>Daniel</td>
<td>S21sec Labs</td>
</tr>
<tr>
<td>Christen</td>
<td>Tobias</td>
<td>Zürich Financial Services</td>
</tr>
<tr>
<td>Clarke</td>
<td>James</td>
<td>Waterford Institute of Technology, TSSG</td>
</tr>
<tr>
<td>Dikkers</td>
<td>Hessel</td>
<td>ABN AMRO</td>
</tr>
<tr>
<td>Dürig</td>
<td>Markus</td>
<td>Bundesministerium des Innern</td>
</tr>
<tr>
<td>Everling</td>
<td>Oliver</td>
<td>Rating Evidence</td>
</tr>
<tr>
<td>Hämmerli</td>
<td>Bernhard</td>
<td>European Commission, JRC</td>
</tr>
<tr>
<td>Königs</td>
<td>Hans-Peter</td>
<td>former Telekurs CEO</td>
</tr>
<tr>
<td>Kotrotsios</td>
<td>George</td>
<td>CSEM</td>
</tr>
<tr>
<td>Malek</td>
<td>Miroslaw</td>
<td>Humboldt Universität Berlin</td>
</tr>
<tr>
<td>Masera</td>
<td>Marcelo</td>
<td>European Commission, JRC</td>
</tr>
<tr>
<td>Navajo</td>
<td>Rafael</td>
<td>GMV</td>
</tr>
<tr>
<td>Olivero</td>
<td>Sergio</td>
<td>Siti</td>
</tr>
<tr>
<td>Oppenchaim</td>
<td>Serge</td>
<td>Crédit Agricole S.A.</td>
</tr>
<tr>
<td>Paulus</td>
<td>Sachar</td>
<td>SAP AG</td>
</tr>
<tr>
<td>Porter</td>
<td>Sandy</td>
<td>Avosecure</td>
</tr>
<tr>
<td>Pujol</td>
<td>Fernando</td>
<td>Telvent</td>
</tr>
<tr>
<td>Raettig</td>
<td>Lutz</td>
<td>Morgan Stanley</td>
</tr>
<tr>
<td>Riguidel</td>
<td>Michel</td>
<td>ENST Paris</td>
</tr>
<tr>
<td>Samson</td>
<td>Michael</td>
<td>Netherlands Bankers' Association</td>
</tr>
<tr>
<td>Schreiber-Handschug</td>
<td>Frank</td>
<td>Deutscher Sparkassen und Giroverband</td>
</tr>
<tr>
<td>Sepkes</td>
<td>Eric</td>
<td>Citi</td>
</tr>
<tr>
<td>Skordas</td>
<td>Thomas</td>
<td>European Commission, INFSO</td>
</tr>
<tr>
<td>Suri</td>
<td>Neeraj</td>
<td>TU Darmstadt</td>
</tr>
<tr>
<td>Svennson</td>
<td>Ulf</td>
<td>CQS</td>
</tr>
<tr>
<td>Tomagnini</td>
<td>Orio</td>
<td>Intesa San Paolo</td>
</tr>
</tbody>
</table>
Appendix D – Presentations

Copies of the presentations are available at

http://www.effev.de/CIPF

The files are password protected and accessible for the attendees only