Financial Services Industry

Bernhard Hämmerli

Norwegian Information Security Laboratory,
Department of Computer Science,
Gjøvik University College, Norway

`bmhaemmerli@acris.ch`, `Bernhard.Hammerli@hig.no`

Abstract. Critical infrastructure and services in financial industry are important for our society and the financial industry starts to understand the topic beyond the normal and well maintained Business Continuity Management and Disaster Recovery Plans (BCM & DRP). Today, the international backbone financial infrastructures operate pretty well, but in the infrastructure towards clients, two issues are utmost critical for the banks: Drive By Download and Phishing; both are related to stealing identity and money via e-banking. This is one of the results achieved by the EU project **Parsifal (Protection and Trust in Financial Infrastructure)** (Parsifal-Team, 2010), for compositing a research agenda for the cyber security of the financial industry.

Keywords: Critical Information Infrastructure Protection, Financial Industry, Resilience and Robustness, CIP, CIIP.

1 Overview

The financial sector is vital to the economy to keep key processes up and running. Key processes are cash for the population, providing liquidity and core processes as payments, credit, clearing, securities trade, settlement and foreign exchange. The international infrastructure is based mainly on SWIFT communications and messages, the national payment systems are very divers and many states have even more than one system. The financial sector was very early aware on information risks and provided according business continuity plans.

First we describe the financial service and market infrastructure (section 2), then about the regulation and standards (section 3) and we elude on technical risks (section 4). As in every new trans-disciplinary topic, a glossary and an ontology (how the terms relate to each other) accepted for all parties has to be developed (section 5). Some aspects of actual status and trends of the financial infrastructure are presented in section 6. The Parsifal project's findings and its recommendation (section 7) give an introduction in the pending research challenges as it is in 2010, including the view of the experts and their priority.

2 Financial Services and Market Infrastructure

2.1 Services of the Financial Sector

The Banking and Finance Sector, the backbone of the world economy, is a large and diverse sector primarily owned and operated by private entities. This Sector consists of many fine grained and a few worldwide operating financial institutions, including:

- depository financial institutions
 - banks
 - thrifts
 - credit unions
- insurers
- securities brokers/dealers
- investment companies
- certain financial utilities

Financial industry provides a broad array of products to their customers. These products:

- allow customers to deposit funds and make payments to other parties, nationally and internationally;
- provide credit and liquidity to customers;
- allow customers to invest funds for both the long and short term;
- transfer financial risks between customers (trade finance business);
- access to stock exchange; and
- currencies, equity shares, bonds, derivatives as well as loans.

The financial institutions that provide these services are all somewhat different, each within a specific part or parts of the financial services marketplace. Financial institutions operate to provide customers the financial products they want, ensure the institution's financial integrity, protect customers' assets, and guarantee the integrity of the financial system. As such, financial institutions and the financial market manage a wide variety of financial and certain non-financial risks.

2.2 Financial Market Infrastructure

Today, financial institutions deal primary with financial information and risks. The money itself (coins and bills) is less and less important, since most accounts are kept and transfers are executed on the electronic money, hence all within the cyber infrastructure. The computing systems and its inter-networking is therefore an essential infrastructure for the financial sector. The banks are mostly interlinked with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network.

SIWFT means three things for the financial institutions:

1. a secure network for transmitting messages between financial institutions;
2. a set of syntax standards and market practices for financial messages (for transmission over SWIFTNet or any other network)
3. a set of connection software and services, allowing financial institutions to transmit messages over SWIFT network.

The SWIFT messages are today transmitted with the IP protocol in a secure way (with VPN) often in dedicated high secure and high reliable networks. The most important interbank systems are depicted in (Figure1).

Specifically the main elements of such interbank system are (see Figure 1):

Details in Figure 1:

- CLS (Continuous Link Settlement) Market infrastructure for multi-currency settlement of western currencies (USD, EUR, JPY, CHF, etc.)
- CSD (Central Securities Depository) Market infrastructure for settlement of Securities
- ICSD (International Central Securities Depository) Market infrastructure for cross border settlement of securities transfers
- SIC: Swiss Interbank Clearing as an example for national clearing and formats
- T2 (TARGET2): Market infrastructure for settlement of payments (in Euro)
- T2S (TARGET2SECURITIES) Market infrastructure for settlement of payments and securities (delivery versus payment). Operations planned for 2014.

SWIFT uses own message types, developed in the last 30 years (named MT), the ISO15022-standard in the securities business and since a few years also ISO 20022 standard for financial services messaging. ISO20022 describes a metadata repository containing descriptions of messages and business processes, and a maintenance process for the repository content.

The **Electronic Banking Internet Communication Standard** (short **EBICS**) is a transmission protocol between banks and clients for orders and getting information. It's a secure channel over internet with a client-driven authentication and used in Germany and France. Switzerland and Austria are in the discussion to use also this standard for here customers. So the "E" in EBICS is changing from "Electronic" to "European".

Additionally, strong identification and authentication systems are systems every network participant has to trust and to rely on SWIFT uses (IdenTrust) Public Key Infrastructure Identities.

It is evident that banks are heavily dependent on high reliable and secure communication infrastructures; towards customers the public internet with VPN is predominant, amongst the institutions itself the internet protocol is used often on rented “private communication links”. However, those links are in shared Telco infrastructure by today. In the data processing centre message queues are used to store orders and task. The messages are structured and standardized, and as description language more and more XML is used.

In respect to financial infrastructures, the focus of the following considerations will be on the financial ICT infrastructure, and how to increase its protection in the framework of the critical information infrastructure protection (CIIP)

3 Regulation and Standards

3.1 Regulation of the Financial Sector

In addition to the actions of financial institutions, direct financial regulation applies to many, but not all, financial services providers. The regulation of the financial sector is fragmented and reaches from worldwide institutions (World Bank, Bank for International Settlements BIS) to large scale regional regulation e.g. EU, US down to single national state regulation. In general, financial regulation is complex; it manages and regulates various forms of risk and guard against prohibited practices.

3.1.1 Regulations from Bank for International Settlement

BIS (Wikipedia on Bank for International Settlements) takes care for regulation as follows:

- to make monetary policy more predictable and transparent among its 57 member central banks
- to regulate capital adequacy and make reserve requirements transparent.

Role in banking supervision: The BIS provides the Basel Committee on Banking Supervision with its twelve-member secretariat, and with it has played a central role in establishing the Basel Capital Accords of 1988 and 2004. There remain significant differences between US, EU and UN officials regarding the degree of capital adequacy and reserve controls that global banking now requires. Put extremely simply, the US as of 2006 favoured strong strict central controls in the spirit of the original 1988 accords, the EU was more inclined to a distributed system managed collectively with a committee able to approve some exceptions. The UN agencies especially ICLEI are firmly committed to fundamental risk measures: the so-called triple bottom line and were becoming critical of central banking as an institutional structure for ignoring fundamental risks in favour of technical risk management.

3.1.2 Basel II Regulations

The financial sector holds many risks which could endanger a financial institution. As in every business, the first risk priority is focused on the essential market risks, which are according Basel II regulation categorized in three prioritized main pillars (Wikipedia on Basel II):

1. The first pillar deals with maintenance of regulatory capital calculated for three major components of risk that a bank faces: **credit risk**, **operational risk**, and **market risk**. Other risks are not considered fully quantifiable at this stage.
 - The credit risk component can be calculated in three different ways of varying degree of sophistication, namely standardized approach, Foundation IRB and Advanced IRB. IRB stands for "Internal Rating-Based Approach".
 - For operational risk, there are three different approaches - basic indicator approach or BIA, standardized approach or TSA, and the internal measurement approach (an advanced form of which is the advanced measurement approach or AMA).
 - For market risk the preferred approach is VaR (value at risk).
2. The second pillar deals with the regulatory response to the first pillar, giving regulators much improved 'tools' over those available to them under Basel II. It also provides a framework for dealing with all the other risks a bank may face, such as **systemic risk**, **pension risk**, **concentration risk**, **strategic risk**, **reputational risk**, **liquidity risk** and **legal risk**, which the accord combines under the title of residual risk. It gives banks a power to review their risk management system.
3. The pillar aims to promote greater stability in the financial system by allowing market discipline to operate by requiring lenders to publicly provide details of their risk management activities, risk rating processes and risk distributions.

Market discipline supplements regulation as sharing of information facilitates assessment of the bank by others including investors, analysts, customers, other banks and rating agencies. It leads to good corporate governance. When marketplace participants have a sufficient understanding of a bank's activities and the controls it has in place to manage its exposures, they are better able to distinguish between banking organizations so that they can reward those that manage their risks prudently and penalize those that do not.

On the operational side the activities against money laundering and terrorism are an example, introduced from the government side and resulting in a deep impact for the operational business, even on a daily base.

As shown, the financial sector has many risks inside the business part of the sector, which are by far more important than the infrastructure risks but also influenced by technical risks. A clear confirmation of this fact was the financial turmoil in 2008 (Dick K. Nanto, 2009) which caused the financial institutions to focus on their core business and neglected for a period the infrastructure risks.

However, the infrastructure, mainly the ICT infrastructure and its security, remains essential for the financial services operation. This means a technical risk which influence from a basic level mostly of other risks. Therefore, the next subchapter will elaborate on ICT.

3.2 Characteristics of EU Financial Services

As a strategic goal EU regulators act for customer interests to push financial services towards an adoption of increased open market competition and the provision of harmonized services across national boundaries in all EU member states.

As stated in section 1, the financial services industry is heavily dependent on ICT technology and its providers. Therefore, competitiveness in the financial services sector depends on the cost of accessing and processing data and hence on the technological solutions that allow such data access and processing. Furthermore, market advantage means accessing better financial data (including background data) and accessing it faster. Even more advantage get the biggest banks with whole sale conditions (the larger the dealt volume is, the better are interest rates, conditions and direct access to central systems of the financial sector. In this context the evolution of data standards and data exchange rules define positions for market competitiveness. Because of the importance of these positions, rules are strongly controlled by the financial services community itself. And last but not least, only a certain parts of financial data are really sensitive. But if so, confidentiality of these data is essential for activities in the financial services sector.

3.2.1 Single European Payment Area (SEPA)

The European Commission has established the legal foundation through the Payments Services Directive (PSD) which was translated by the European Payments Council (EPC) into operation, in more than 30 European Countries. By the end of 2010 SEPA had a cross border market share of 14%, meanwhile the political will was to be predominant by at this point in time. The European Commission took measures to foster SEPA.

The EPC is committed to delivering three pan-European payment instruments:

- For credit transfers: *SCT – SEPA Credit Transfer*, operational January 2008
- For direct debits: *SDD – SEPA Direct Debit*, operational November 2009
- For cards: *SEPA Cards Framework*, operational, 2011

The Euro system however urges more efforts in the area of card payments and the urgent resolution of issues with the third type of payment instrument, SEPA Direct Debit (SDD).

The fast introduction of SEPA to user should not suppress that in the national domains still specialists and often manifold payment systems are operational. To be effective, harmonization of payment services is still an important objective such that national entities are directly applying SPEA standards as ISO 20022 (XML message transfer format), IBAN and BIC to gain full benefit in local and EU processing. SEPA is not just a business project, but is also closely linked to the political ambition to move towards a more integrated, competitive and innovative Europe and therefore today and even more in future a critical financial infrastructure.

3.2.2 Markets in Financial Instruments Directive (MiFID)

The goal of MiFID¹ (introduced Nov.1, 2007) is to protect investors, increase transparency of the financial markets and integrity of the financial service provider and provides standards for the following key aspects:

1. **Authorisation, regulation and passporting:** Firms covered by MiFID will be authorised and regulated in their "home state" (broadly, the country in which they have their registered office). Once a firm has been authorised, it will be able to use the MiFID passport to provide services to customers in other EU member states. These services will be regulated by the member state in their "home state" (whereas currently under ISD, a service is regulated by the member state in which the service takes place).
2. **Client categorisation:** MiFID requires firms to categorise clients as "eligible counterparties", professional clients or retail clients (these have increasing levels of protection). Clear procedures must be in place to categorise clients and assess their suitability for each type of investment product. That said, the appropriateness of any investment advice or suggested financial transaction must still be verified before being given.
3. **Client order handling:** MiFID has requirements relating to the information that needs to be captured when accepting client orders, ensuring that a firm is acting in a client's best interests and as to how orders from different clients may be aggregated.
4. **Pre-trade transparency:** MiFID will require that operators of continuous order-matching systems must make aggregated order information on "liquid shares" available at the five best price levels on the buy and sell side; for quote-driven markets, the best bids and offers of market makers must be made available
5. **Post-trade transparency:** MiFID will require firms to publish the price, volume and time of all trades in listed shares, even if executed outside of a regulated market, unless certain requirements are met to allow for deferred publication.
6. **Best execution:** MiFID will require that firms take all reasonable steps to obtain the best possible result in the execution of an order for a client. The best possible result is not limited to execution price but also includes cost, speed, likelihood of execution and likelihood of settlement and any other factors deemed relevant.
7. **Systematic Internaliser:** a Systematic Internaliser is a firm that executes orders from its clients against its own book or against orders from other clients. MiFID will treat Systematic Internalisers as mini-exchanges hence, for example, they will be subject to pre-trade and post-trade transparency requirements.

In infrastructure terms, MiFID compliance means best execution in respect to technical performance, e.g. order of execution, speed and overhead costs. Especially in degraded infrastructures are MiFID requirements difficult to perform.

¹ These requirements tend to be applied in future to other financial instruments.

3.3 Standards in the Finance Sector

In the financial markets in the nineties, the desire to automate the electronic execution of equity transactions and their related derivative products led to the emergence of Financial Information eXchange FIX (FIX-Group F. S.) and Financial products Markup Language FpML (FIX-Group), based on eXtended Markup Language XML, as open standards that were pushed by the major fund managers and traders such as Fidelity Investments and JPMorgan. Further standards efforts are:

1. The Expert Group on e-Invoicing triggered in 2008 a harmonization between CEFAC, NES and ISO on supply chain standards.
2. Pan European Public Procurement Online (Peppol-Team), an EU FP7 project is pushing efforts to align company identifiers and product identifiers in multiple EU countries. Collaboration between distinct players around open standards is evolving at the same time.
3. The adoption of Microsoft Advanced Message Queuing Protocol AMQP² has brought a close collaboration between Microsoft and the open source community in the further development of cloud computing
4. The collaboration between the European Payment Council EPC and GSMA – the mobile operators association - around open standards for mobile payment processing brings two industries together that previously were fighting for the same customers of these mobile payment services.

4 Technical Risks

4.1 Technical Infrastructure Overview

Analysing the technical infrastructure, we have to be aware on the dependability aspects: It is really important to now that the public internet and Telco system has to work, that the power provider must deliver electricity (of course sever have uninterruptable power supplies UPS, but not all (network)-infrastructure and certainly not the end user PC, even so laptops have battery for a few hours) in order to operate the bank owned infrastructure. In some case, where water is used for cooling, also the water supply must be available to avoid damage at the electronic components (yellow infrastructure in Figure 2).

Furthermore the operating systems, then various tiers of middleware and the applications must be up and running such that a bank can operate. The red arrow in figure 2 just shows one element in the chain of dependability considerations. In reality all chains involved into critical services must be analysed in equal way to get a profound analysis of the service availability.

With software oriented architecture SOA the application landscape changes, and will be for more distributed on different systems, internally, but partly also depending externally in case that data or service element of external services (e.g. stock prices,

² <http://www.amqp.org/>

exchange rates etc.) are used. This trend – together with the virtualization and introduction of cloud services, leads to deeper and more specialized production chains in informatics, in analogy to the one, which Taylor³ (1856-1915) has introduced in mechanical production in the late 19th century. Details are discussed in the next subchapter.

The overall complexity and robustness is obvious in Figure 2:

Fig. 2. Robustness of a single process (red: dependability chain)

³ http://en.wikipedia.org/wiki/Scientific_management

4.2 Risks of Mechanism for Distributed Processing

The following trend in IT-architecture has been observed in vast discussion and in many related literature, e.g. (Financial-Services-Club, 2009):

1. Decoupling of data storage from data processing and the further growing capacity and performance improvement of data processing.
2. Proliferation of data processing is the use of “Mashups”, a means to create composite applications to share and combine internal and external data sources by creating enterprise composite applications: with this technique, the value creation chain will be extended in respect to geographical location, number of involved components, number of involved actors.
3. Use of cloud computing, which promise to make it possible for the sharing of resources on an unprecedented scale. Additionally is to add the cost pressure towards cloud computing: economy of scale allows offering servers at a much cheaper rate in comparison to on site server production. Also, the corporate data are in cloud computing on the cloud provider’s servers: according measures must be taken to comply with confidentiality and data protection law.
4. Shared infrastructure services with this centralized security operation centres dealing with network intrusions, threats; security policy enforcement and configuration lead to dynamically managed infrastructures.
5. The delocalisation of services (e.g. storage in one country, computing in another one) is by today more an academic option; however, it would increase the number of attack points, but it might be also a chance to improve overall resilience, when applied properly.

The security challenges of the above trends apply can become both, point of attack and a step towards better structured and maintained process: additional point of attack for example with the distribution of service execution, and an opportunity to ensure processes are followed more accurately and that financial institutions comply with regulations because of detailed formulation of contractual issues and completely separation of service production and service audit.

In terms of C(I)IP very long and distributed service production chains, as well as outsourcing and the movements into clouds adds many additional components which are internetworked and might be cause to turn down the overall system. It needs more accurate risk assessment and specific evaluation of overall resilience and robustness.

In terms of business continuity, the distribution of services could be even a measure for robustness, if every service is ran at different places and a seamless switch over between the service instances is foreseen. Assuming this really works, still the network must be high reliable and must have at least a second if not a third channel for emergencies. Given this architecture, the positive effect on resilience and robustness will happen.

Finally, banking secrecy law prohibits in some countries outsourcing of banking. Encrypted data would enable in spite of privacy concerns outsourcing. Processing of encrypted data is a research field by today, but still in its infancy.

4.3 Facilitating Customer Access to Financial Data and Cash

4.3.1 Developments in Online Banking

The accessibility of financial data by customers of banking services is emerging: e.g. in US on-line banking grew in 2008 nearly 30%. And in September 2008 SWIFT launched a product that enables SMEs to connect directly to this bank-owned network for the instruction of payments and collection of bank account information. To make this happen, the bottlenecks of middleware in the secure distribution and processing must be removed, especially for very high volumes of financial information between multiple applications. Advanced Messaging Queuing Protocol AMQP, which has been implemented by Microsoft, is one solution to the challenge.

The acceptance of online banking including online banking security was researched in depth (Detecon Consulting, 2001) in four EU countries. Customer acceptance and willingness to secure end device vary through the researched countries. However, acceptance and according customer end protection are essential prerequisites.

4.3.2 Banking Moving into Mobile Space

Small devices basically split up in two technologies: GSM based systems and Internet protocol driven Systems. For both the European Payments Council (EPC) has accelerated the deployment of services that enable consumers to pay for goods and services in shops, restaurants and other locations using their mobile phones. Initially, it was about defining a contractual framework document detailing the minimum set of requirements for a so-called Trusted Service Manager to interface with banks and mobile operators. Mobile banking is mainly delivered by technologies like SMS or Unstructured Supplementary Service Data USSD (value added GSM service), Mobile Internet Browsers or downloadable applications (typically Java). In numbers, 25% of transactions will be in 2011 from mobile internet and around 10 % from native mobile telephone protocol, such as SMS or USSD.

Meanwhile in the beginning only very few mobile services were offered, today already quite sophisticated applications are available, e.g. the EPC (European Payment Council) has enabled SEPA payments across 31 countries via cell phone. Furthermore, some production chains include mobile technology as part of the native or the security process. E.g. mobile transaction number as security for home banking or Hal-Cash, which uses SMS for ATM withdrawal without plastic card: Persons in need (e.g. lost bourse) can just type in a secret code received by SMS and they receive the money signed off by a friend at any ATM in Europe (Wilcox, 2009) (Flatraaker).

4.3.3 Identity Management in Financial Services

As a key issue of electronic financial data the control over customer accesses requires a resilient identity management system IdM (e.g., reduced sign-on, provisioning and access-management) constantly progressing in accordance to the overall internet developments. IdM is one of the key critical financial infrastructures without it any reliable and secure transaction can take place. The market offers dozens of IdM technologies —including biometrics, smart cards, tokens, radio frequency

identification (RFID), public key infrastructure (PKI), and Bluetooth-based devices—in the field of credential issuance, authentication, and verification, but none of these technologies has emerged as a universal standard.

In the modern world steeling identity means at the end steeling money. Especially in the view of e-banking, secure processing of sensitive data is essential to avoid significant losses and attacks on customer information and assets. Some of the currently available digital identity methods of verifying transactions in e-banking services are:

- **Biometric ID:** This verification method linked to human trait has the major advantage of being secure against faking. However, if biometric Id is not processed on a second channel, the application can still be intercepted with the effect that the higher degree of security becomes useless.
- **Federated ID:** At present, each bank establishes its own electronic ID. The setting up of multi-part IDs would result in important saving to companies admitting such identities, as e.g. the BankID in Norway already does.
- **Mobile Transaction Authentication Numbers (mTAN):** These and similar forms identify identities on a separate channel such as special hardware devices which are already able today to discover attacks produced by “drive-by downloads” or e-mail attachments. However, the automation of the process is weak and therefore this method serves for private individuals only. Furthermore, with the next generation of mobile users, there will be no assurance, that the mobile IP connection and the mTAN are on different channels.

Again, the value and urgency of secure and cost optimized identities is absolutely critical and crucial for secure banking, without any workaround we know of by today!

In respect to financial C(I)IP the trend to mobility adds an additional component, which is significant for the society and therefore critical. Certain processes, as e.g. mobile TAN require a robust and reliable mobile infrastructure: another element added which must be up and running to complete processes. But also in the general online access, secure and cost optimized identities are a prerequisite to operate B2B and B2C. A failure of IdM would cause equal effect as a blackout of the whole infrastructure.

4.4 Technical Risks: The Sectors View

In a discussion with financial experts working in the business continuity and critical infrastructure field some challenges were depicted in an interview which demonstrate the broadness of the topic expanding the infrastructure issue by personnel and localisation issues:

1. Non predictable message volumes: The institution can handle normal everyday volumes of electronic orders. To stress test infrastructures up to 2005 one believed, that a factor 3-5 of the normal everyday volume would be sufficient. However, a few extraordinary situations in recent years let the

volume increase to factor 20. Meanwhile everyday statistics can be handled well institutions have to be prepared for an unknown increase, which might appear again, but very rarely. Options to act are – both additional and longer delays in processing the message queues - or a black out for the time of too intense processing requests.

2. Every institution can prepare itself, however, whether in the inter-institution communication, the counterparty is able to operate messages in the back office is not predictable, even so, contract are designed such they it should be able.
3. Larger institutions have back up sites and are able to transfer while operating the business from one data centre to another. Within a national state this has no legal obstacles, internationally, there are rules partly prohibiting a swap over.
4. Another major concern is operations with human interactions: First the human interactions are not scalable. Extra work force needs time to build and cannot be increased by factors within hours. Second, diseases such as bird's flu, SARS and new virus combinations may lower the operational workforce within hour to days, e.g. in two days the workforce could shrink by 80%. To counter fight such scenario, isolation of people, home working places, additional hygienic measures are foreseen, as well as reassigning displaceable work to other sites, where the disease is not active.
5. The cash process must be organized in a crises resistant way, such that without power and telco the population can provided with cash or according other payment options.
6. Liquidity processes are essential to banks and allow operating the business. Especially centralized settlement (like TARGET2, CLS) was introduced at large – after the Herstatt case in 74 (Wikipedia, 2010) - to avoid unnecessary counter party risks.

Elaborating on the challenges, there are three backup pillars which must be kept in mind:

1. IT: IT involved in critical processes must have according backup infrastructures, often direct backup sites as well as swap over to processing centres of other locations in case of worldwide institutions.
2. Personnel: Epidemics must be prepared, crises scenarios trained and shifting work or personnel to other non-epidemic sites of the world, if available.
3. Localities: is the third element in the strategy which allows lots of flexibility as shown in the first two points. Important is to realize that all three together lead in a pre-prepared optimized interaction to best results.

Furthermore, the interests in CIIP have to be elaborated:

1. Legal compliance must be kept with regulatory frameworks of the international regulators as well as national and local regulators. This is a prerequisite to get the license to run the business and to get access to the according provider (e.g. SWIFT).

2. The single institution has interest to protect itself in a way that economic prosperity of the institution is maintained: Business Continuity Management BCM and Disaster and Recovery Planning DRP are used to keep the institution alive and operational for economic purposes. Most institutions are good at this.
3. National economic supply: National states are usually not interest in a single institution, but in keeping critical sectors alive. Even single institutions are in general not in the focus of national states, very large single institution with a “Too big to fail” challenge are very much in the focus. Both, the collection of many average sized institutions and very large one, offer critical services to the citizen and companies, which could damage if not available – social life or have a long lasting negative impact as e.g. economic problems, poverty etc. The usual approach to identify challenges and actions to be taken is starting with public private partnership round tables (facilitating government experts, sector delegates and specific suppliers, delivering core infrastructures). The work is defining vulnerabilities of the sector and according risks, discussions of counter measures and incidents, such that best common effort can be taken to counter fight incidents - either in advance or if already happened – with concentrated common effort.

4.5 Incidents: The Motivation to Act

Security in general, information- and IT-security, military and CIIP follow all the line, that the primary trigger to act on improving security, resilience and/or reconstruction /crisis preparation are incidents. No incidents is often translated in a yearly budget decrease a round 10%. Unfortunately, this is not the case of the financial sector that suffered for several incidents in the last years. In the follow we report some of them to stress, further to the urgency to improve the protection of the IT components, the need to learn on past event in order to design more efficiently robust solutions.

4.5.1 Swiss Telekurs Payment System

Telekurs (today SIX group) operates on behalf of all Swiss banks the Point of Sales POS electronic payments and the network of automatic teller machines ATM for withdrawing cash. It is an essential infrastructure for all Swiss citizens. Saturday, December 23, 2000 a tape was falling into the central tape robot and blocking this device (Neumann). As a consequence, at the day of most turn over in the year – the day before Christmas – the complete system, i.e. all POS and ATM were blocked and did not allow the customers to pay!

This incident triggered to a redesign of the POS/ATM system, increasing offline capabilities and business continuity. Switzerland had – because of this incident – much earlier realized robustness in POS/ATM compared to other countries.

4.5.2 Swiss Post Finance

Slammer malware was discovered and – after billions of US \$ damage – remediated with virus control in Jan 2003. However, October 8 2003, Swiss Post Finance had a

major incident, with Slammer. In a closed server farm – not connected to the outside world, and therefore not performing all updates and protection measure – was Slammer introduced by a maintenance computer. For hours one of the very core financial systems of Switzerland was unusable.

This incident lead to completely new awareness levels, in respect to counter measure and updates.

4.5.3 Mariposa

In 2009/2010 the Defence Intelligence group³¹ discovered a botnet with one of the most extensive networks ever observed. A sinkholing conducted between December 2009 and February 2010 made it possible to detect 11 million unique IP addresses. The network was called "Mariposa" (Spanish for "butterfly") (MELANI, 2010-1), since the botnet was created using the Butterfly malware kit. The Spanish name is due to the fact that the botnet operators were Spaniards.

The main purpose of the botnet was to steal sensitive data from infected computers. This included information about accounts, names of users, passwords, and details concerning online bank accounts. Part of the infected computers also included malware to launch DDoS (distributed denial of service) attacks. Clients of the 40 largest banks worldwide as well as computers of at least half of all Fortune 1000 companies were victims of this botnet. The victims came from 190 countries.

The Butterfly malware kit was developed by a hacker named Iserdo. The 23-year-old was recently arrested in the Slovenian city of Maribor. The botnet operators were arrested in Spain the beginning of the year. The operation conducted by the Guardia Civil led to the arrest of three Spanish citizens. These were identified by the pseudonyms they used on the Internet and their ages: Netkairo, 31, Johnny Loleante, 30, and Ostiator, 25.

However, the Spanish justice authorities had to follow their own country's criminal code. According to statements by Major Cesar Lorenzana, the deputy director of the technological crimes unit of the Guardia Civil, it is not a crime in Spain to operate a botnet or to disseminate malicious code. The only possible indictment is data theft.

4.5.4 Zeus and SpyEye – Merger of Largest E-banking Trojans?

The Trojan "Zeus" is probably the most widespread e-banking malware currently in circulation. There are numerous reports, articles and activities on this topic (MEALNI, 2010-2). From early 2010, another e-banking malware called "SpyEye" made a name for itself. SpyEye integrates a function with the name "Zeus Killer Code". This function seeks to determine whether an infected computer already contains Zeus. If it does, the rival is eliminated. This effectively led to a war between the two trojans. The author of recently became famous in the underground scene when he announced in July that the author of "Zeus" had given him the code of the malware and delegated administration of its customers to him. In various subsequent messages, Harderman publically announced that version 2 of Zeus would no longer be further developed. The community would be able to count on a new malware, however, which would be developed from the merger between SpyEye and Zeus.

4.5.5 Waddell and Reed Financial Inc. Impact of Erroneous Human Input on Algorithmic Trading

May 6, 2010 around 14.45 a trader made an erroneous input for a deal and sold 75000 E-mini Futures (actual value ca. 4 billion USD) for very little money, because the decimal dot in the number was set wrong (Westbrook, 2010). Figure 3a demonstrates the impact on the E-mini future, 3b shows Dow Jones impact, 3c shows the impact on the Waddell & Reed Inc. stock and 3d demonstrates influence on other stocks, went to pennies within minutes: Accenture, shown at left, fell from above \$40 at 2:47 to \$0.01 at 2:48, but then within 90 seconds, the Dow was back up 543 points and ended up closing out down only 3.2% overall.

Fig. 3. Algorithmic trading reaction on erroneous human input

Concluding this case nothing really went wrong in infrastructure, it was just a human error. However, there have been no controls on plausibility when this deal was made. Such a control could avoid the very short break down of the market and the unjustifiable losses and win's which occurred. The danger stemmed from the fact, that – after erroneous human input - finally algorithm versus algorithm followed to trade without any human interaction.

4.5.6 Asking for Realistic Countermeasures in a Given Context

These fundamental different attacks represent some danger for the financial sector. However, all these attacks had no long lasting bottlenecks in large regions for the

broad publicity, as the criticality definition of CIP would require. Considering the criticality, we have indicator what could happen, when we do not react carefully; but as in most other sectors, the real CIP incident did not happen yet. This fact – in spite of all excitement for C(I)IP – is very important to recognize, such that the community can position itself correctly in a given context and is not over demanding measures.

4.6 Relationship between Technical Risks and Business: Alignment Countermeasure to Threats

The common power of around 80 financial ICT experts was used to generate mini cases / scenarios for which security or criticality is important. The 160 mini cases or scenarios were analysed in tow aspects: Firstly, distribution from local to global (horizontal) and secondly, fragmentation of the service creation chain (from all concentrated to fine grained fragmentation) (Susan Morrow, 2009) :

- Vertical: longer and longer value chains lead naturally to fragmentation between players, everyone contributing to separated or integrated services. At the same time there is a concentrated move which may result from several factors: It may be standardization across borders (e.g. Single European Payment Area SEPA) or single – shop local or regional trade platforms.
- Horizontal: this naturally reflects the concerns of transactions extending across borders between states, across regions or across continents.

The fascinating insights received from this analysis, was a misalignment of today's countermeasures in respect to the basic threat properties along the two axes. Even so, experts already know that the arms race of computer defence and computer attacks is very asymmetric in the favour of the attackers, this view opens aspects with a big potential to identify new countermeasures facing the arms race challenge.

Fig. 4. Positioning threats in the global IT infrastructure

Explanation of the Identified Elements

- **Business blob:** it simply illustrates that nowadays there is no firm trend regarding financial business. In all areas financiers and bankers are opportunistic risk takers, while financial markets and mathematical trading exacerbates short terms views to the level of the second!
- **Technology:** is dominated by world-wide providers, with a strong appetite to offer more than just tech services world-wide.
- **Infrastructures:** from being mostly local and fragmented they evolve. Not exactly like business. There is a trend towards regionalization or globalization but as the stakeholders describe it along two separate paths, one is along fragmented infrastructures – this may mean of different banking institutions with a global reach or of connected systems. For example from a technical infrastructure perspective CLS (Continuous Link Settlement) is one platform while it is interconnected with many other systems- the other one is towards concentrated market places or interbank systems (see e.g. the NYSE, or TARGET2).
- **Threats:** One could say that threats may arise from anywhere e.g. hackers are very opportunistic too. However stakeholders expressed their concerns somewhat differently. They see them concentrating along one axis from local/concentrated (see e.g. 9/11, identity thefts by the millions) to global/fragmented (see simultaneous flash attacks coordinated across borders, for which there is currently no adequate response).
- **Governments** are by nature local and fragmented. This is somewhat counterbalanced by mostly regulatory institution e.g. the Bank of International Settlement (BIS), the European Central Bank (ECB). Overseeing systemically important infrastructures is a joint effort in a few instances. For example, for the oversight of SWIFT the National Bank of Belgium acts as the lead overseer as SWIFT is located in Belgium. However, they are supported by G-10 central banks. The oversight focuses primarily on ensuring that SWIFT has effective controls and processes to avoid posing a risk to the financial stability and the soundness of financial infrastructures. Similar arrangements are in place for CLS. This seems to fall short of a comprehensive view/action capability.
- **Countermeasures** may be defined regionally or less often globally. They are always acted and controlled locally. This state of affairs seems in strong contradiction with the challenges posed by the threats.
- **IDM, Fraud, Theft and Apps:** however there are a few areas where solutions seem to be at hand or close to it. They are fragmented. Some complain: there are already too many possibilities. There is a call for standardization, interoperability or even uniqueness. The latter seems to be justified for concentrated infrastructures only.

4.7 CoMiFin Communication Middleware for Monitoring Financial Critical Infrastructure to Enhance Cyber Defence

CoMiFin (Communication Middleware for Monitoring Financial Critical Infrastructure) (Comifin-Team, 2008) is an EU project funded by the Seventh Framework Programme (FP7), started in September 2008 and continuing for 30 months. The research area is Critical Infrastructure Protection (CIP), focussing on the Critical Financial Infrastructure (CFI).

An increasing amount of sensitive traffic is being carried over open communication media, such as the Internet. This trend exposes services and the supporting infrastructure to massive, coordinated attacks and frauds that are not being effectively countered by any single organisation. In order to identify threats against critical infrastructures and business continuity, CoMiFin aims to facilitate information exchange and distributed event processing among a subset of participants grouped in federations. Federations are regulated by contracts and they are enabled through the Semantic Room abstraction: this abstraction facilitates the secure sharing and processing of information by providing a trusted environment for the participants to contribute and analyse data. Input data can be real time security events, historical attack data, logs, and other sources of information that concern other Semantic Room participants. Semantic Rooms can be deployed on top of an IP network allowing adaptable configurations from peer-to-peer to cloud-centric configurations, according to the needs and the requirements of the Semantic Room participants.

A key objective of CoMiFin is to prove the advantages of having a cooperative approach in the rapid detection of threats. Specifically, CoMiFin demonstrates the effectiveness of its approach by addressing the problem of protecting financial critical infrastructure. This allows groups of financial actors to take advantage of the Semantic Room abstraction for exchanging and processing information, thereby allowing them to take proactive steps in protecting their business continuity, for example, through generating fast and accurate intruder blacklists.

5 The Need for Glossaries and Ontologies

Glossaries and ontologies (SLTTGCC, 2005), (Gresser, Draft Ontology Of Financial Risks & Dependencies, 2009), (Gresser, Ontology of Financial Risks & Dependencies: Vol 2 Glossary, 2009) are very useful when scientifically approaching a new domain as it is the critical financial services. Many organizations made home grown and national language based terms which are of limited use in pan European discussions of the sector. In (Gresser, Draft Ontology Of Financial Risks & Dependencies, 2009) a comprehensive set of ontology graphs were developed: Figure 5 is intuitively understandable and describes the basic financial services and system.

To approach the CIP component of the financial services, the single graph must be expanded in mind to many corporate entities, delivering the service, in many different states, also exchanging information worldwide. Such a heavy secure and worldwide

distributed and interconnected system is provided by the Society for Worldwide Interbank Financial Telecommunication, SWIFT, for financial messaging, containing payment information in the message body. Beside of the technical challenge to design and operate such systems, there are also legal challenges concerning regulations which are different in cross-border situations.

Fig. 5. Top Level Financial Industry Ontology

And finally, CIP is about understanding of the dependencies and vulnerabilities in local, cross-border and international dimensions and converting the respective analysis in measures before, during and after the crises.

6 Financial Infrastructure: Status and Trends

6.1 Today's Status of Open and Harmonized EU Financial Market

The financial market has a rapid emergence of open infrastructures, with a widespread sharing of data. On the upside, this is perceived as a real opportunity in enabling new forms of performing financial business or to introduce new value added services. On the downside, the gradual replacement of physical boundaries with logical boundaries was regarded to be a major challenge for the financial services sector and their critical infrastructures. The reality of a situation where information is shared rapidly with third party companies such as suppliers and partners could compromise the privacy of customers and harm competitiveness by putting intellectual property and commercially sensitive information at risk. Increased openness of infrastructures is perceived to create risk for the owners of the Critical Financial Infrastructures (CFI) but also for the users of data processed by these infrastructures.

6.1.1 Markets Access of Non-banks

These regulations have indeed facilitated the ability of non-banks to offer traditional banking services. As an example of the changing landscape for financial infrastructures, VocaLink made public in 2008 that its bank shareholders are looking to sell a stake in the firm to non-bank investors.

In the investment banking arena, many experienced traders have in recent years established hedge funds that have become key trading partners of the traditional investment banks and independent technology providers have established electronic trading platforms that increasingly gain market share from the traditional exchanges.

A growing number of service providers have started to offer information processing services to the customers of banks (fund managers, companies and even consumers) that directly compete with the existing financial services. These offerings also cover increasingly the value added services that the banks were intending to include in their services portfolio (such as e-invoicing and identity management).

Non-banks are less regulated and therefore more flexible in service creation. The market share of non-banks has been increased and is also a threat to the stability of the financial market. Also, non-banks IT systems perform often better and through technological performance business advantages are attempted.

6.2 Accelerated Dematerialization of Supply Chains in the EU

The application of new web technology and its improved integration techniques began in 2008 leading to substitution of paper by electronics means. This substitution is called dematerialization of the supply chain.

SEPA and e-invoicing are expected to contribute to the Lisbon agenda by making Europe the most competitive and dynamic knowledge-based economy in the world by the end of 2010. E-invoicing does not form a part of SEPA, but is a value added services are built on top of SEPA, which relies on the clearing and settlement infrastructures.

Furthermore, 10 public administrations in Europe started in the fall of 2008 to execute on the Pan European Public Procurement Online (Peppol project www.Peppol.eu) on cross border e-procurement, e-ordering and e-invoicing which has today less than 20% of EU's GDP, but as strategic target is more than 50% coverage.

The trend to electronic processing increases the dependability on the according infrastructure and its criticality. Robustness and resilience are therefore central design criteria.

6.3 Growing Complexity, Volume and Transaction Speed

The discussion what could be different in financial IT systems from others, the resulted in the combination of complexity, volume and speed of executing financial transactions meanwhile maintaining reliability, confidentiality and integrity.

The speed of transaction processing was given a further boost by the introduction in 2008 of faster payments by the UK banking community. Previously cleared funds arrived with the beneficiary after passing through a three-day clearing cycle. But pressurized by the UK government, payees are able to receive cleared funds rapidly and payers have the certainty that their funds have been debited immediately. Similar developments in the EU by establishing the TARGET2-system offer the same near-time settlement for the Euro. Further developments in the TARGET2SECURITIES system (T2S) will allow customers to settle not only the payments in near time, also reduce the settlement time for securities. This will cause enormous efforts in changing the way how clearing works by today.

Growing Complexity in Foreign Exchange Markets.

Historically, currency trading has been a "closed" market, reserved primarily for central banks. However, with the advent of web-based trading applications and overall advances in technology, small retail traders and even individuals can now participate from their desktops directly in the forex markets on equal footing with these large institutions. Examples for electronic trading technology are electronic trading platforms such as OANDA⁴ or Swissquote⁵. These platforms use innovative computer and financial technology to provide Internet-based forex trading and currency information services to everyone and is rapidly becoming more attractive as an alternative investment opportunity.

New Complexity: Adaption to New Internet Ipv6.

Ipv6 will enable Internet to reach almost any object on the planet. This will inevitably extend the number of contact points for financial transactions by several orders of magnitude, likely not to its final reach but still very significantly. IPv6 will bring first enormous efforts for switching the infrastructure to the new protocol. Many devices

⁴ <http://www.oanda.com/>

⁵ www.swissquote.ch

must be changed because upgrades will not be available. Additionally, new opportunities for banks as well as new “transaction” operators, e.g. robots, may be generated as well as the complexity of infrastructure (number of nodes) will increase dramatically.

6.4 Conclusion on Current Situation in Financial Sector

It is important to recognize that we take a dynamic view of the situation with regard to key decisive factors while classical risk analysis tends to be more static. The fact that EVOLUTION IN ITSELF IS A RISK FACTOR is often minimized by classical approaches of risk assessment. They tend to be static and do not reflect reality to a limited degree only.

Nowadays the finance and the defence communities may not perceive risks in the same way:

- Finance top managers tend to perceive IT infrastructures, as an amplifier of financial moves see the current crisis. This has been known for some time. Is it permanent or can something dampen the effect? "Fuses" are already in place for stock markets;
- Finance people tend to prioritize the threats on their infrastructure less than other issues like (financial) risk management. Do they actually take them as something for IT specialists or do they give sufficient consideration to the consequences? The current trend is probably closer to the first option, which has proven by the financial turmoil 2008/2009.

Finance top managers are likely to act on two factors: first the consequences which may result from threat scenarios especially when compliance is not met, and second what they can actually do when such a scenario occurs. With respect to infrastructures these factors play in opposite directions: the more IT will take over services, the fewer financiers can act on infrastructure and will therefore not feel in command. This latter trend is very hard to reverse and deserves a more detailed analysis, respectively, the causality of unfortunate incidents and how business or management attitudes may trigger or facilitate these incidents and identifies lessons from it. Another issue is threat & risk assessment. Said bluntly, some of the threats might not interest bankers because their customers will bear all consequences.

7 Challenges in the Future: Results of Parsifal

Parsifal: Protection And tRuSt In Financial infrastructures (Parsifal-Team, 2010) project was launched in September 2009 and targeting the ambitious objective concerning coordination activities between the stakeholders necessary to protect CFI and information infrastructures, both today and tomorrow, and specifically those areas which span beyond a single bank or a single country. Parsifal goals are:

1. Bringing together Financial industry and R&D stakeholders from ICT Security areas;

2. Contributing to the understanding of CFI challenges in the next five years;
3. Developing longer term visions, research roadmaps, CFI scenarios and best practice guides;
4. Coordinating the relevant research work, knowledge and experiences.

The Parsifal project had 6 Partners and was running for 18 month.

7.1 Parsifal Methodology

The PARSIFAL objective is to provide input to future research programmes and further strengthen the engagement between the European Commission and the financial Services industry in terms of trust, security and dependability of these critical financial ICT infrastructures.

The main tool to achieve the project's ambitious objectives has been the setting up of an expert stakeholder group (ESG), comprising stakeholders from the industry and research communities. This group included representatives of several key actors in critical financial service industry CFI protection. Among them were high level representatives and decision makers that have the power to decide where to invest in research in the upcoming years.

To get a comprehensive and high quality input from the stakeholders, two workshops were organized. The first workshop included presentations from relevant experts to stimulate the discussion and identify the main issues in CFI protection: This set the ground for the working groups in three main streams:

1. Controlling Instant On Demand Business in CFI: Authentication, Identity Management, Resilience and Denial of Service.
2. Entitlement Management and Securing Content in the Perimeterless Financial Environment: Identity, Policy, Privacy and Audit.
3. Business Continuity and Control in an Interconnected and Interdependent Service Landscape: Cross Border and Cross Organisations.

The three stakeholder working groups used written exercises and discussion to define future scenarios and challenges in CFI protection. The final result was a set of eight recommendations for research.

The next step was to prioritize these recommendations. The second workshop was used to present the recommendations to the stakeholders and ask them about their priorities. Using an online survey (*via* web and email), a wider group of stakeholders was contacted to include their priorities and recommendations.

7.2 Parsifal Recommendation and Research Directions

In table 1 the eight recommendations are explained with reflection of the streams in which they were elaborated.

Table 1. Work streams and Recommendations

Stream 1: Instant on Demand Business	<p>1. Classification of identity attributes for on-line and mobile users of financial services should be defined and well understood by providers of these services and their customers.</p> <p>2. Trust indicators need to be developed, which allow for the various gradients of trust any entity might achieve when using specific financial services.</p> <p>3. Support platforms are needed for the management of multiple identities to allow consumers to authenticate themselves with various professional and private identity attributes.</p>
Stream 2: Entitlement Management	<p>4. Digital identities are required that are highly standardised across the financial services sector, with the introduction of mandatory IDs for all financial institutions, cross border interoperability and a “single/global” identity issuing authority.</p> <p>5. Data Security measures are required, such that a digital identity links directly with a security policy to a data object, that data is secured as encapsulated entities, and with flexible security policies that are based on individual access rights plus Digital Rights Management (DRM) for enterprise content to allow for flexible security policies and geographic boundary control.</p> <p>6. New Computing Paradigms need to be analysed, which allow for de-perimeterization of the organisation, e.g. Cloud Computing, supported by any new security focus. Predictive models need to be created to understand security risks. Cross border legal issues need to be resolved.</p>
Stream 3: Business Continuity	<p>7. Design and implementation of secure platforms and applications, which should include an alternative and secure communication system/infrastructure, to be overseen by adequate coordination response team(s) at a national and international level.</p> <p>8. Testing, design and implementation of such secure platforms, applications and infrastructures through trustworthy exercises between CIP-sectors and governments. Models for business continuity need to be extended to (1) sharing risks and (2) end-to-end communication between trade participants, as well as to (3) the volume and the complexity of specific financial markets. These models should be "crash" tested, regularly evaluated and updated.</p>

7.3 Prioritisation of the Eight Parsifal Recommendation

Experts were invited to vote on the eight recommendations. The following options were available for voting: Absolutely urgent, urgent, must be addressed, not urgent. Although the results are apart from each other, the results points clearly out, that the recommendations and priorities have found agreement in the community.

Fig. 6. Voting results of the experts on the eight recommendations

In a complex process with consideration of the stream and sense of urgency figure 6 was developed showing the timeline (starting with recommendation eight), the dependencies and interrelation of the eight recommendations. The timeline is important when considering the sequence in which recommendation are dealt with.

Fig. 7. Dependencies between the eight recommendations

7.4 Conclusions on Future Challenges in Financial ICT

The very first and important statement we have to make is the excellence the financial sector has reached. From all infrastructure failure we have experience by now are only very on a recognizable level. And even those were not really long-lasting and impacting essentially economy or society. Vice versa the business failure have tradition and occur periodically from 1929 to 2009 again and again. Obviously the infrastructure risks were easier to handle and sector handled those better than their business. However, the ICT has a very unpredictable side, and this needs attention.

From the Parsifal project stakeholder group we know what the future focus should be (table 1). We observe from the eight main challenges that there are many challenges related to identity management (1,3,4,5), two are related to business continuity management BCM and are rated as the most important one (7,8) and the last two (cloud computing risks stemming from new technologies and trust indicators enabling clients to estimate trust-level for inter-acting with banks when connected with different infrastructures (home, office, public wireless etc.).

Meanwhile the BCM and new technological risks are well known to the community, the identity and cloud challenge might be often underestimated in both, the critical meaning for the sector and the cost saving potential. Especially identities are essential for interacting in the virtual rooms. In research secure cross-border identities an identity economics are often discussed, but seldom the risks beyond the corporate relevance, such as the criticality for the sector.

Acknowledgment. Parsifal project team are indirect co-authors and kindly permitted to use the projects documents to write this chapter: Rafael Llarena & Aljosa Pasic ATOS Origin Spain, Susan Morrow & Sandy Porter Avoco Secure, Henning Arendt Arent Business Consultant, Jean-Yves Gresser and Tom Buschman Edge international BV, James Clarke and Kieran Sullivan Waterford Institute of Technology Ireland.

Furthermore, Christian Kleine UBS AG, Rolf Prantl (especially for figure 1, he was contributing) and Pius Steiner deserve my thanks for review and content enhancement.

Specific References

- Comifin-Team. Communication Middleware for Monitoring Financial Critical Infrastructure (2008) Von, <http://www.comifin.eu/abgerufen>
- Detecon Consulting. Study - The Value of Information Security to European Banking Institutions. Zürich, Detecon (2001)
- Dick K., Nanto, C. S.: The Global Financial Crisis: Analysis and Policy Implications. Abgerufen am 26. 4 2011 (October 2, 2009) von, <http://www.fas.org/sgp/crs/misc/RL34742.pdf>
- Financial-Services-Club (October 2009) Von, <http://thefinanser.co.uk/fsclub/2009/10/cloud-computing-needs-better-definition-to-succeed.html>abgerufen

- FIX-Group. (kein Datum). Abgerufen am 2011. 7 31 von Request for Participation: FIX-FpML Collaboration Working Group,
<http://www.fixprotocol.org/discuss/read/5341e8a6>
- FIX-Group, F. S. (kein Datum). FIX Protocol. Abgerufen am 2011. 7 31 von
<http://www.fixprotocol.org/what-is-fix.shtml>
- Flatraaker, D.-I.: Sepa Standards – Sepa goes mobile. EPC Newsletter (January 2009)
- Gresser, J. Y.: Draft Ontology Of Financial Risks & Dependencies. Abgerufen am 26. 4 2011 von [parsifal-project.eu](http://www.parsifal-project.eu) (2009),
[http://www.parsifal-project.eu/images/PublicDeliverables/PARSIFAL%20D2.1%20Draft%20Ontology%20of%20Financial%20Risks%20Dependencies%20Within%20and%20outside%20the%20Financial%20Sector%20V3.0%20\(Glossary\).pdf](http://www.parsifal-project.eu/images/PublicDeliverables/PARSIFAL%20D2.1%20Draft%20Ontology%20of%20Financial%20Risks%20Dependencies%20Within%20and%20outside%20the%20Financial%20Sector%20V3.0%20(Glossary).pdf)
- Gresser, J. Y.: Ontology of Financial Risks & Dependencies: Vol 2 Glossary. Abgerufen am 26. 4 2011 von [parsifal-project.eu](http://www.parsifal-project.eu) (2009),
<http://www.parsifal-project.eu/images/PublicDeliverables/parsifal%20D2.1%20draft%20ontology%20of%20financial%20risks%20and%20dependencies%20within%20and%20outside%20the%20financial%20sector.pdf>
- IdenTrust. (kein Datum). IdenTrust. Abgerufen am 31. 7 2011 von
http://www.identrust.com/pdf/IdenTrust_Privacy_WhitePaper.pdf
- MEALNI. (31. 12 2010-2). Semi-annual report 2010/2. Abgerufen am 27. 04 2011 von,
<http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=en>
- MELANI. (30. 6 2010-1). Semi-annual report 1/2010. Abgerufen am 27. 4 2011 von,
<http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=en>
- Neumann, P. G. (kein Datum). ACM Digital Library. Abgerufen am 31. 7 2011 von,
<http://portal.acm.org/citation.cfm?id=505778&dl=ACM&coll=DL&CFID=37083720&CFTOKEN=98694083>
- Parsifal-Team. Protection and Trust in Financial Infrastructures. Abgerufen am 2011. 7 31 von (2010),
<http://www.parsifal-project.eu>
- Peppol-Team. (kein Datum). eProcurement without Borders in Europe. Abgerufen am 2011. 7 31 von <http://www.peppol.eu>
- SLTTGCC. Critical Infrastructure Data Taxonomy: Common Terminology for Describing Critical Infrastructure. Abgerufen am 26. 4 2011 von US Department of Homeland Security (2005),
http://www.dhs.gov/files/publications/gc_1226595934574.shtm
- Susan Morrow, G. J.-Y.: D3.4 Mapping of Research Challenges to CFI Scenarios. Abgerufen am 29. 4 2011 (October 13, 2009) von,
http://www.parsifal-project.eu/index.php?option=com_content&view=article&id=73&Itemid=59
- Westbrook, N. M.: Bloomberg Business Week. Abgerufen am 31. 7 2011 (2010) von,
<http://www.businessweek.com/news/2010-10-01/waddell-reed-trades-said-to-help-spur-may-6-crash.html>
- Wikipedia on Bank for International Settlements. (kein Datum). Abgerufen am 26. 4 2011 von,
http://en.wikipedia.org/wiki/Bank_for_International_Settlements

Wikipedia on Basel II. (kein Datum). Abgerufen am 4 2011 von,
http://en.wikipedia.org/wiki/Basel_II
 Wikipedia, S. r. Settlement risk. Abgerufen am 6. 5 2011 (August 26, 2010) von,
http://en.wikipedia.org/wiki/Herstatt_Risk
 Wilcox, H.: Banking on the mobile - Mobile Banking, Strategies, Applications & Markets
 2008-2013. Juniper Research White Paper, Basingstoke (January 2009)

General References

- [1] European Payment Council: Towards our single payment area (February 25, 2009),
<http://www.europeanpaymentscouncil.eu/index.cfm>
- [2] COSO - Enterprise Risk Management - Integrated Framework , Executive Summary
 (September 2004),
http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf
- [3] Research and Development Committee, Financial Services Sector Coordinating Council
 for Critical Infrastructure Protection and Homeland Security (FSSCC), Research Agenda
 for the Banking and Finance Sector (September 2008)
- [4] International Telecommunication Union, Information Society Statistical Profiles, 2009 –
 Africa, http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-RPM.AF-2009-PDF-E.pdf
- [5] Committee on Payment and Settlement Systems (CPSS - Bank of International
 Settlement), The interdependencies of payment and settlement systems (June 2008)
- [6] European Central Bank (ECB), Public consultation on glossary of terms related to
 payment, clearing and settlement systems (September 30, 2008)
- [7] Federal Office for Information Security, BSI – Standard- 100-4, Business Continuity
 Management, version 1.0 (2009) <http://www.bsi.bund.de/grundschutz>
- [8] British standard Institute, Information technology — Security techniques — Information
 security management systems — Code of practice for information security management,
 BS ISO/IEC 27001:2005, BS 7799-1:2005 (July 2007)