OUTLOOK

Visions and research directions for the Wireless World

2014, No 11

Cyber Security in Future Internet

Security & Privacy by Design

White Paper

Cyber Security in Future Internet

- Security & Privacy by Design -

Editor:

Mario Hoffmann

Authors:

Ann Cavoukian, Michelle Chibba
Nigel Jefferies
Jörg Heuer

Project website address: www.wwrf.ch

Table of content

1. Introduction

Cyber security[1] in Future Internet will face new challenges and threats. Global connectivity of people, things, and services on a large scale, new access channels, massive resource sharing in clouds as well as cyber-physical convergence require innovative technical solutions and a socio-political discourse.

Addressing these challenges nations around the world have defined and updated their cyber security strategies during the last five years. Cornerstones of the cyber security strategy of the US for example are the "International Strategy for Cyberspace"[2], the "Draft Strategy for Improving Critical Infrastructure Cybersecurity"[3] as well as the "National Strategy for Trusted Identities"[4]. Finding authoritative Chinese sources that provide a detailed definition of cyber security and the challenge it poses is difficult. Anchors for further reading are available in "China Moves Forward on Cybersecurity Policy"[5] and "Chinese Views on Cybersecurity in Foreign Relations"[6]. The European Union has defined the following five strategic priorities in the Cyber Security Strategy[7]: (1) Achieving Cyber Resilience, (2) Drastically reducing cybercrime, (3) Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy, (4) Develop the industrial and technological resources for Cybersecurity, and (5) Establish a coherent international cyber space policy for the European Union and promote core EU values. The status of the implementation of the EU's Cybersecurity Strategy has been recently discussed at a high-level conference in Brussels[8]. An overview of further references worldwide can be found at the website of NATO Cooperative Cyber Defence Centre of Excellence[9].

In general, there is neither 100% security nor 100% privacy in the Future Internet. Instead, security requirements and privacy concerns of the participating parties have to be considered, analysed, and balanced – if necessary by sophisticated assessments from domain to domain, from context to context, from use case to use case. Design principles are available for around ten years supposed to enabling SW and HW

[1] Definition: "Cyber security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.", taken from http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667, Feb 2013

[2] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, May 2011

[3] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, Feb 2013

[4] http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf, Apr 2011

[5] http://thediplomat.com/2012/07/china-moves-forward-on-cybersecurity-policy/, Jul 2012

[6] http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf, Sep 2013

[7] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667, Feb 2013

[8] EU Cybersecurity Strategy - High Level Conference, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-high-level-conference, Brussels, 28th Feb 2014

[9] https://www.ccdcoe.org/328.html, updated on 10th Mar 2014

developers to take security and privacy into account from the very beginning. The two most prominent design paradigms are: Security & Privacy by Design.

In Jan 2013 Ann Cavoukian and Mark Chanliau discussed the convergence of the two paradigms Security & Privacy by Design in a white paper[10]. They stated that by adopting these paradigms good privacy and security might be embedded directly into information systems, processes and architectures, and that this might minimize the likelihood of data breaches recurring in the future. In other words: Addressing security goals – i.e. confidentiality, integrity, availability – as well as data protection goals – i.e. transparency, unlinkability, intervenability[11] – in every system design early on may save reputation, resources, and revenue. The white paper concludes that with considering these principles the impact of security vulnerabilities can be minimized, privacy can be preserved, and identity propagation across heterogeneous vendors can be ensured, especially in mobile computing, online social networks, and cloud computing.

In the following outlook of the Wireless World Research Forum particular perspectives of cyber security in Future Internet on the basis of security and privacy by design have been contributed on the basis of a panel discussion having taken place at WWRF Conference in Vancouver, Oct 2013. The outlook covers (1) recommendations from the Office of the Information and Privacy Commissioner, Ontario, Canada, by Ann Cavoukian and Michelle Chibba, (2) an analysis of the Cyber Security Landscape in Europe by Nigel Jefferies as well as (3) a concrete use case on how a mobile operator implements and integrates the wallet paradigm in his service ecosystem by Jörg Heuer.

[10] Ann Cavoukian, Marc Chanliau, “Security and Privacy by Design – A Convergence of Paradigms”, Jan 2013, http://www.ipc.on.ca/images/resources/pbd-convergenceofparadigms.pdf

[11] Thomas Probst, Marit Hansen, “Privacy Protection Goals in privacy and data protection evaluations”, https://www.datenschutzzentrum.de/guetesiegel/Privacy_Protection_Goals_in_privacy_and_data_protection_evaluations_V05_20120713.pdf

2. A Regulator's Perspective: Leading the Way with Privacy by Design

Ann Cavoukian, Michelle Chibba, Information and Privacy Commissioner of Ontario, Canada

2.1 Introduction

As threat levels rise, security professionals are increasingly being called upon to develop new ways to protect critical infrastructure components. In this drive for unattainably perfect security, we are likely to experience a loss of privacy and freedom. As Benjamin Franklin, one of the founding fathers of the United States, wisely observed, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Proposals to obtain security at any cost must be resisted. We must seek measures designed to provide both security and privacy, in an accountable and transparent manner. Whether the issue is one relating to cyber security standards[12] or innovative wireless technologies[13], we must reject the dated zero-sum, either/or, win/lose approach. By shifting to a positive-sum mindset focused on win-win solutions, we will be able to accommodate multiple legitimate interests such as advancements in wireless enabled smart electrical grids, smart homes and smart communities, thereby avoiding unnecessary trade-offs and false dichotomies.

This paper is based on the premise that the future of privacy can be ensured through the adoption of Privacy by Design (PbD)[14]. Notwithstanding that strong legislative protections are necessary to preserve our right to privacy, the capabilities of wireless technology are advancing far too fast for compliance with regulatory schemes alone, to be sufficient. Digital information, once breached, is nearly impossible to recover. Thus, it is critical that protections be built directly, not only into technologies, but into the culture of entire ecosystems – so that privacy is a core functionality, and not just a problem to be overcome after-the-fact.

2.2 The Essence of Privacy

Although the definition of informational privacy will differ among jurisdictions, the essence of privacy relates to one's ability to have control and freedom of choice about the collection, use and disclosure of information about ourselves—what we might call our personal data flows. Privacy is about having a right to "informational self-determination," a term that was first used in a German constitutional ruling concerning personal information collected during Germany's 1983 census.

[12] NIST has introduced a Cyber Security Framework, November 2013 for U.S. critical infrastructure that provides guidance to manage cyber related risk while protecting business confidentiality, individual privacy and civil liberties.

[13] See WWRF Visions for the Wireless Future Wireless World 2020 Workshops in Visions and research directions for the Wireless World, May 2013, No.8.

[14] www.privacybydesign.ca

It is significant that almost any information (e.g., a set of numbers on a RFID tag, the sequence of points that make up a biometric template), if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational. The definition of privacy, therefore, can be quite broad in scope and the challenges for privacy and data protection are equally broad.

Privacy is also contextual. Personal information provided in different contexts will vary. Identities may be used in or out of context. Identities used out of context generally do not bring desired results. For example, trying to use a coffee card to cross a border is clearly out of context. On the other hand, using a bank card at an ATM, a government-issued ID at a border, a coffee card at a coffee shop, are all clearly in context.

To clarify, privacy is not about keeping information secret or hiding it. Organizations are not prevented from collecting and using personal data, or having a meaningful interactive relationship with individuals. A number of factors must be taken into account, however, when implementing privacy practices, including legal requirements, available technologies, social norms and business processes. We want privacy provisions to be applied in a practical manner that considers all of these varied interests, benefits and risks. Critical to this is an understanding that security does not equal privacy. While information security is extremely important, the term privacy subsumes a far greater set of protections than security alone. In their custodial role, organizations that process personal data must have user-centric controls that incorporate principles such as, purpose specification, personal consent and use limitation.

We must remember that the right to privacy "protects people, not places."[15] In a 2012 case discussing the right to "public privacy" — a privacy right closely associated with our right to informational privacy — in Canada, the Ontario Court of Appeal stated that "personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society."[16] Indeed, in the information and technology era we live in, the protection of our right to informational privacy is increasingly critical to the preservation of our rights to life, liberty, and security of the person — in essence, our freedom.

2.3 Privacy in an Interconnected Wireless World

Addressing the privacy and security of mobile communications has become critical, as these devices and necessary infrastructure have reached penetration levels unlike any other major communications technology. ITU's The World in 2013: ICT Facts and Figures report predicts that there will soon be as many mobile-cellular subscriptions as

[15] In reference to the US 4th Amendment see Facts and Case Summary: Katz v. United States 389 U.S. 347 (1967).

[16] David M. Porter. Reasonable Expectations of Privacy in the Computer Age: A Brief Review of Regina v. Ward 2012 ONCA 660 and Regina v. Cole 2012 S.C.C. 53. McCarthy Tetrault. January 2013.

people inhabiting the planet, with the figure set to nudge past the seven billion mark early in 2014.

In addition to this widespread penetration, mobile devices are becoming more advanced, as they are increasingly engineered to be capable of performing most of the same types of actions as laptop or desktop computers (with the primary exception of applications that require very high processing power). Yesterday's cell phones have become today's "smart" mobile devices, thanks to broadband network access to the Internet and Web and enhanced sensor, storage and processing capabilities that enable new feature and service innovations.[17] Mobile computing devices have become ubiquitous, serving as personal travelling companions and tools for hundreds of millions of people. As such, they need to be secure, trusted and empowering. On top of the benefits for any time communication and connection, these advances are making information truly mobile – wherever they are, users can quickly find, or be provided with, information related to their immediate interest, location or problem, and can keep vast quantities of digital resources available at all times. Where the Internet can be said to have sparked an 'information revolution,' the infrastructure required for deployment and use of mobile technologies has sparked an 'access revolution.'

Of course, information passing to and from a single, powerful mobile device raises potential privacy and security issues. Any concerns that one may have had with personal computing can now be said to apply to wireless mobile communications technology – and any concerns about ISPs quickly translate to the central hub for all phone calls made, text messages sent, and data transferred: the network provider. In addition to this, a host of current and future issues are raised by the combination of significant computing power and a portable form factor. Communications to and from the device will be wireless, by and large – signal interception is thus a concern that must be addressed.[18]

Legitimate data transactions also raise privacy concerns, particularly as location data is increasingly being associated with mobile communications. Unlike laptop or other portable computers with which users generally engage on an 'as-needed' basis, mobile devices are likely to be 'always-on' (to allow for reception of incoming phone calls, text messages, etc.) – as such, tracking the location of a mobile device will often give a highly accurate impression of its owner's movements throughout the day.[19] Finally, the small, portable nature and high value of mobile devices makes them prone to loss or

[17] A. Cavoukian. Mobile Near Field Communications (NFC) "Tap 'n Go" – Keep it secure and private. November 2011. This paper examines NFC technologies and their growing deployment in mobile devices. Four consumer use cases illustrate NFC functionalities and benefits. Privacy and security risks are identified, and solutions are offered for NFC mobile device and application developers that are informed by PbD.

[18] A. Cavoukian and K. Cameron. Wi-Fi Positioning Systems: Beware of Unintended Consequences – Issues involving the unforeseen uses of pre-existing architecture. June 2011. This paper speaks to the need for innovative solutions to change the existing model of using persistent MAC addresses that remain uniquely bound to a mobile device.

[19] German Green Party member Malte Spitz published his own data collected by his cell phone carrier from August 2009 to February 2010. To illustrate just how much detail from someone's life can be mined from this stored data, ZEIT ONLINE has "augmented" Spitz's information with records that anyone can access: the politician's tweets and blog entries were added to the information on his movements. Source: www.zeit.de/datenschutz/malte-spitz-data-retention

theft – a significant issue when such devices are assigned increasingly more functionalities, and store increasingly more personal or otherwise sensitive data.[20]

The increasing ubiquity and power of mobile devices are beginning to both clarify and magnify their associated privacy concerns. However, rather than waiting for issues to arise, academics and industry professionals are looking to get out ahead of the curve, taking a proactive (rather than reactive) approach to building privacy into the industry – without losing the significant benefits associated with fully realized functionalities.[21] This is the heart of Privacy by Design – anticipating and addressing privacy issues before they become problems, in a positive-sum manner.

2.4 Privacy and Consumer Trust

We have seen a significant increase in the quantity of personal data online and its use for commercial purposes. Personal information has ipso facto become a money of exchange. To quote Meglena Kuneva, former European Commissioner for Consumer Protection: "Personal data is the new oil of the internet and the new currency of the digital world."[22]

Personal information must be managed responsibly. When it is not, accountability is undermined and confidence/trust is eroded. Consumer surveys show that a high percentage of consumers (98%) are concerned about mobile privacy and a significant percentage will not download apps they don't trust.[23] Another study found that Americans overwhelmingly consider information stored on their mobile phones to be private — at least as private as information stored on their home computers.[24]

It goes without saying, then, that a data breach has a negative impact on an organization's reputation and bottom line. Indeed, a recent survey showed that 89% of consumers avoid doing business with companies where there have been privacy concerns.[25] Moreover, the cost of a breach is no longer insignificant. "In the five years we have conducted this study, we have continued to see an increase in the cost to businesses for suffering a data breach," said Dr. Larry Ponemon, chairman and founder of The Ponemon Institute. "With a variety of threat vectors to contend with, companies must proactively implement policies and technologies that mitigate the risk of facing a costly breach." The Institute found that, in 2013, the most expensive data

[20] A. Cavoukian. Safeguarding Privacy on Mobile Devices. 2013. http://www.ipc.on.ca/images/Resources/safeguarding-privacy-on-mobile-devices.pdf

[21] See WWRF User Profiles, Personalization and Privacy in Outlook: Visions and research directions for the Wireless World, May 2009, No.3.

[22] See World Economic Forum, Personal Data: The Emergence of a New Asset Class, January 2011; World Economic Forum in collaboration with The Boston Consulting Group, Unlocking the Value of Personal Data: From Collection to Usage, February 2013.

[23] Truste. Mobile Privacy: A User's Perspective, Identifying and delivering the protection consumers want. A Harris Interactive Survey. Spring 2011.

[24] Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, Mobile Phones and Privacy, Jul. 11, 2012, available at http://ssrn.com/abstract=2103405.

[25] Truste. U.S. Consumer Privacy Confidence Index (Research Report), Harris Interactive, January 2013.

breach event cost a company nearly $31 million to resolve. The least expensive total cost of data breach for a company included in the study was $750,000.[26]

2.5 Leading the Way with Privacy by Design

In the context of our growing dependence on information and communications technologies (ICTs), the lack of transparency and accountability regarding data flows is a major factor contributing to consumer privacy concerns. The challenge we face is protecting and promoting individual privacy while at the same time allowing for the socio-economic opportunities and benefits derived from the permissioned contextual use of our personal information.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation. The Privacy by Design framework employs an approach that is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

The 7 Foundational Principles of Privacy by Design have proven to be a valuable resource for individuals and organizations around the world. In October 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. This was followed by the U.S. Federal Trade Commission's recognition of Privacy by Design in 2012 as one of its three recommended practices for protecting online privacy in its report entitled, Protecting Consumer Privacy in an Era of Rapid Change – a major validation of its significance.

More recently, Privacy by Design has been incorporated into the European Commission plans to unify data protection within the European Union with a single law – the General Data Protection Regulation. In particular, Privacy by Design is reflected in the proposed regulation by requiring data processors as well as producers of IT systems to design their offers in a data-minimizing way, with the most data protection friendly pre-settings. A strong principle of purpose limitation means that only data necessary for the provision of a service would be processed.

Privacy by Design provides a holistic method for proactively embedding privacy into information technology, business practices, and networked infrastructures.

[26] Ponemon Institute. 2013 Cost of Data Breach Study: Global Analysis. Ponemon Institutes Research Report, May 2013.

2.6 The 7 Foundational Principles

The objectives of Privacy by Design — ensuring privacy protection and gaining personal control over one's own information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles:

2.6.1 Proactive not Reactive; Preventative not Remedial

The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2.6.2 Privacy as the Default Setting

We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

2.6.3 Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

2.6.4 Full Functionality — Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.2

2.6.5 End-to-End Security — Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

2.6.6 Visibility and Transparency — Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

2.6.7 Respect for User Privacy — Keep it User-Centric

Above all, Privacy by Design requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

2.7 Conclusion

By taking a pro-active approach to privacy, organizations not only avoid the privacy harm and ensuing regulatory burden but can gain a strategic advantage. This win-win privacy strategy not only results in greater consumer trust but organizations also mitigate their exposure to lawsuits, bad publicity/brand reputation and the direct costs associated with a breach. Paying attention to privacy makes good business sense and we want to lead the way with Privacy by Design.

3. Cyber Security – A European Perspective

Nigel Jefferies, Huawei Technologies

3.1 The Cyber Security Landscape in Europe

The issues of cyber security are the same the world over, but there are distinct approaches being taken in different regions to solve them. In Europe, there is a unique environment, with a large number of independent states, most of them members of the European Union. There is a high level of technology penetration, and a sophisticated and educated consumer base.

From the European Union perspective, the key players are the main EU institutions, the Parliament representing the people of the EU, the Council representing the individual member states and the European Commission, the civil service of the EU which drives the development and implementation of regulations and directives which apply in each of the member states.

In addition, there are EU agencies such as ENISA (the European Network and Information Security Agency), and number of European standards bodies, such as ETSI and GSMA, as well as international standards bodies, such as ITU based in Geneva. Within Europe, there is a strong research base supported by EU and national collaborative research programmes such as Horizon 2020. There is a wide range of industry players, from major multinational manufacturers and vendors to network operators with global reach and a thriving start-up community in some areas. Clearly there is also influence from non-European governments, and international institutions.

The development of cyber security policy and strategy within Europe is driven by the competing and complementary demands of all these players. From the EU point of view, the priorities are the develop industry policy that will protect and enhance European industry, consumers and critical information infrastructure, and enhance trade and international relations. Member states have their own requirements on national security which must also be taken into account.

Technology developments such as the development of 5G wireless systems, the increasing use of the cloud, and the growth of machine-to-machine communications, all demand the adoption of new techniques and policies to ensure the protection of all the players mentioned above.

3.2 Industry Associations and Groupings in Europe

There are a number of important industry associations, user groups and other organizations in Europe that have an impact on, or an opinion on, cyber security issues. Not all of these are exclusively European, or even based in Europe.

For instance, Digital Europe (http://www.digitaleurope.org/) is a trade body for the ICT industry in Europe, while many of its members are US-based companies. It has a working group on security and data protection which meets monthly. ECTA, the

European Competitive Telecommunications Association, (http://www.ectaportal.com) is a body representing non-traditional telecommunications operators, promoting free markets in Europe, and has an ad hoc security group.

All the mobile network operators are represented in the London-based GSMA, which was originally established to facilitate roaming and other interactions between operators, and has a long-established Security Group and Fraud Forum. It has a global membership.

Traditional European network operators make up the membership of ETNO, which lobbies the European Commission on behalf of the industry.

On the standards front, the main organization is ETSI (European Telecommunications Standards Institute), which runs an annual Cyber Security Workshop and the well regarded SAGE (Security Algorithm Group of Experts). Together with CEN and CENELEC, they have recently produced white paper on cyber security to be presented to the European Commission.

Other initiatives in Europe include the eSRT (European Security Round Table http://www.security-round-table.eu/) which brings together EU institutions, NATO and other relevant actors to discuss security in the wider sense, and the SDA (Security and Defence Agenda, http://www.securitydefenceagenda.org) which is a neutral platform for discussing such issues, and has its own cyber security initiative. The European Privacy Association (www.europeanprivacyassociation.eu/) represents the ICT industry on privacy issues, while EOS (the European Organization for Security, www.eos-eu.com) represents the security industry. The Digital Enlightenment Forum (www.digitalenlightenment.org) is an open community of individuals and organizations that works toward sustainable digital society.

3.3 The EU Cyber Security Strategy

Last year the European Commission developed and published its Cyber Security Strategy. This strategy was driven from three separate parts of the Commission: DG Home Affairs (under Commissioner Malmström), DG Connect (Commissioner Kroes) and the European External Action Service (Baroness Ashton). They identified five strategic priorities for the EU in its cyber security strategy: to become ‘cyber-resilient’, to reduce cybercrime, to develop industrial and technological resources in Europe for cyber security and to establish a coherent international cyberspace policy for the EU that promotes core European values.

The intention was that this would be supported by a Directive on Network and Information Security that would establish national frameworks on network and information security facilitate cooperation between competent authorities in the member states and ensure the security of the networks and information systems of public administrations and market operators.

3.3.1 The NIS Platform

To complement and underpin the NIS Directive, the Commission has established the Network and Information Security (NIS) Platform. This will help implement some of the measures set out in the Directive, for instance, by simplifying incident reporting, and ensure its convergent and harmonized application across the EU. In addition to that, it is expected to provide input to the research and innovation agenda for security ICT.

To achieve this, the NIS Platform has set up three working groups. WG1 focuses on risk management, including information assurance, risk metrics and the raising of awareness. WG2 picks up the coordination of information exchange and incident coordination, including incident reporting and risk metrics for the purpose of information exchange, and ensuring that the need for information exchange does not itself add to the risk experienced. Finally, WG3 is focussed on ICT research and innovation, with the aim of developing a strategic research and innovation agenda that can be used to motivate and guide research programmes such as Horizon 2020.

3.3.2 ENISA

The European Network and Information Security Agency (ENISA) was formed in 2004, as a centre of expertise that supports the Commission and the EU member states in the area of information security. In particular, it facilitates the exchange of information between EU institutions, and the public and private sectors. As part of the Cyber Security Strategy, the mandate for ENISA has been extended until 2020.

3.3.3 The EU Cybercrime Centre

The European Cyber Security Strategy proposes the establishment of an EU Cybercrime Centre, as part of Europol, and located within its existing structures. Such a centre would focus on the cybercrime committed by organized crime groups, particularly those generating large criminal profits, such as online fraud. It would also encompass cybercrimes that cause serious harm to their victims, including online child sexual exploitation, for instance, and work against cybercrimes (including cyber attacks) that might affect critical infrastructure and information systems within the European Union. The four main functions of the EU Cybercrime Centre would be:

- To serve as a focal point for the distribution of information about European cybercrime
- To pool European cybercrime expertise to support capacity building by member states
- To become the collective voice of European cyber crime investigators across the different jurisdictions in Europe and
- To work with both the enforcement agencies and the judiciary

3.4 Cyber Security in Industry

Nowadays, many companies are establishing cyber security and security by design strategies. Typically, those strategies focus on how good practice can be built into a

company's 'DNA'[27]. Strategies provide input to the ongoing discussion around policies, procedures, norms and the challenges of cyber security, discussing the transformations that vendors, mobile operators, and Internet service providers are considering in order to meet these challenges, and calls for new international cyber security standards to be developed, agreed and implemented globally.

For such companies, and others in similar industries, 'strategy, plans, governance, processes, accountability and supporting technology must be integrated, seamless, repeatable and auditable. They must dynamically change to new challenges and new requirements.'

Figure 1[28] indicates the complexity and breadth of a process required to ensure that products can be designed, manufactured, sold and integrated into customers' systems in a way which does not threaten the security of any of the stakeholders.

In each part of the process, a company needs to ensure the right security standards, requirements and best practice. The design, build and test needs to be carried out with security in mind. Sales need to be done properly, and in a legally compliant way. The product will need to be manufactured securely with components that have not been tampered with in any way. Installation servicing and support needs to be carried out in a secure way. And the whole process needs to be auditable, following the auditors' ABC maxim: 'Assume nothing, believe no one, and check everything'.

[27] Recently, Huawei for example has published a white paper on cyber security. It was launched in October by John Suffolk, Huawei's Global Cyber Security Officer and is available online at http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-310548.htm.

[28] Kindly provided by Huawei's white paper.

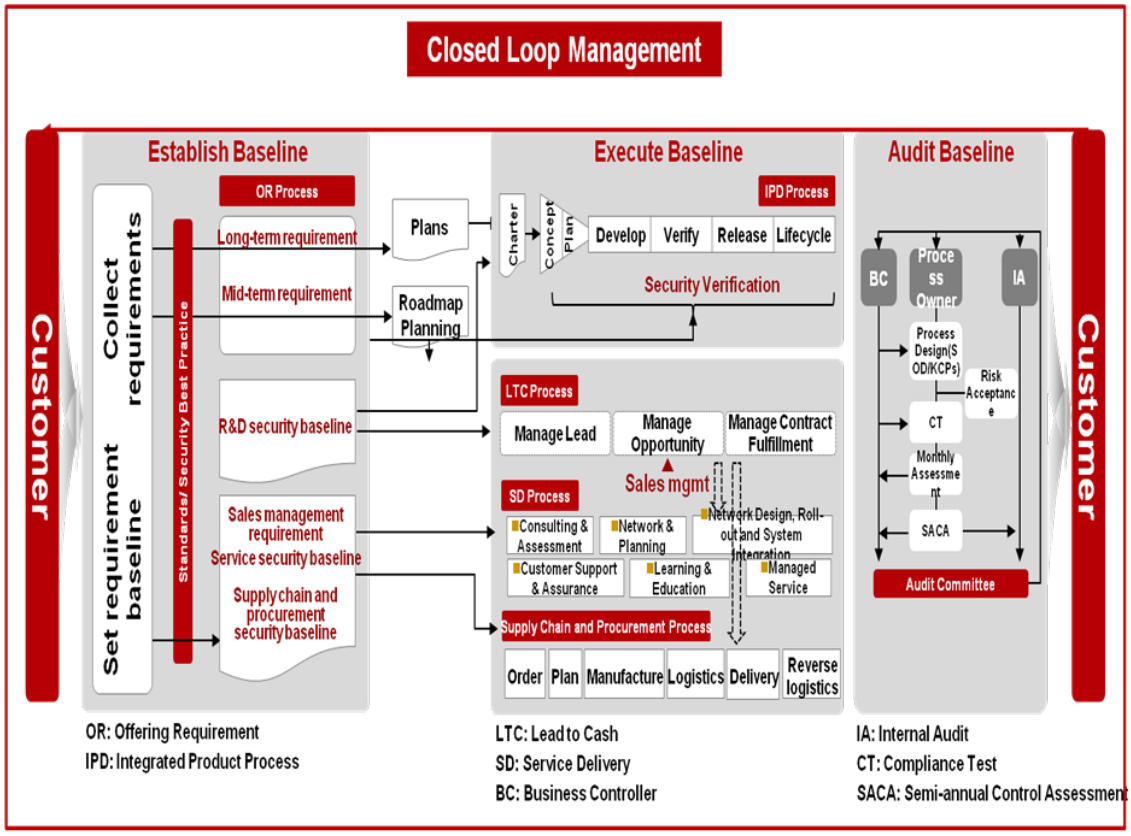

Figure 1: Closed Loop Management, Source: Huawei

4. The Wallet Paradigm – A Convergent Approach

Jörg Heuer, Telekom Innovation Laboratories, Deutsche Telekom AG

Identity management has been the focus of our team's work for many years. Shortly after they became available we started to use next generation SIM cards (UICC) to let third parties implement secure authentication for VPN access, combining it with Near Field Communication (NFC) we implemented secure ticketing for public transport and P2P proximity money transfer (pocket money function). The amalgamation of these – typical assets of mobile operators – and a wider view on identity requirements on the web and in the IT world has created a notion for wallets which is not limited to mobile phones and serves much more than payment transactions. The approach intrinsically supports users in exerting control over identity data and transactions and shows a way towards commercially viable user-centricity with a high level of security compared to existing online solutions.

4.1 What, Wallets?! Why Wallets?

The term 'wallet' has been in the press for several years now and for more than two years connected with the notion of a 'mobile wallet', replacing credit – or other payment – cards. In October 2012 Gigaom listed a set of wallets published by various players (see Figure 2; all of them with a focus on payment and little identity or online functionality.

Figure 2: Mobile Payments - Comparing the Players (Gigaom 4. Oct. 2012)

The players involved are reasonably powerful, and virtually all of the bigger mobile operators have started to introduce their own 'wallets' as well. So far none of them has even faintly succeeded in becoming a digital wallet for the future user in a generic sense. Nevertheless, the potential is huge. Many of the companies involved have access to a secure element (SE) which is an integral part of future SIM cards, but also can be found on some smartphone devices. An SE can host many smartcard applications at once, replacing dozens of plastic cards in a way that payment terminals and smart card readers, won't have to know.

This is achieved by employing near field communication (NFC) a wireless technology designed to work at extremely short distances only, giving the users confidence they can control whether an entitlement is actually being used or not. Despite a few security and control flaws the technology might have, it is recognized by the payment industry. MasterCard and VISA have introduced payment protocols and NFC functions are more and more common on plastic credit cards. Consequently an increasing amount of payment terminals is getting equipped with NFC – just as several smartphones in the higher price ranges down to the upcoming FireFoxOS phones in the mid- to low price-range come with built-in NFC transponders.

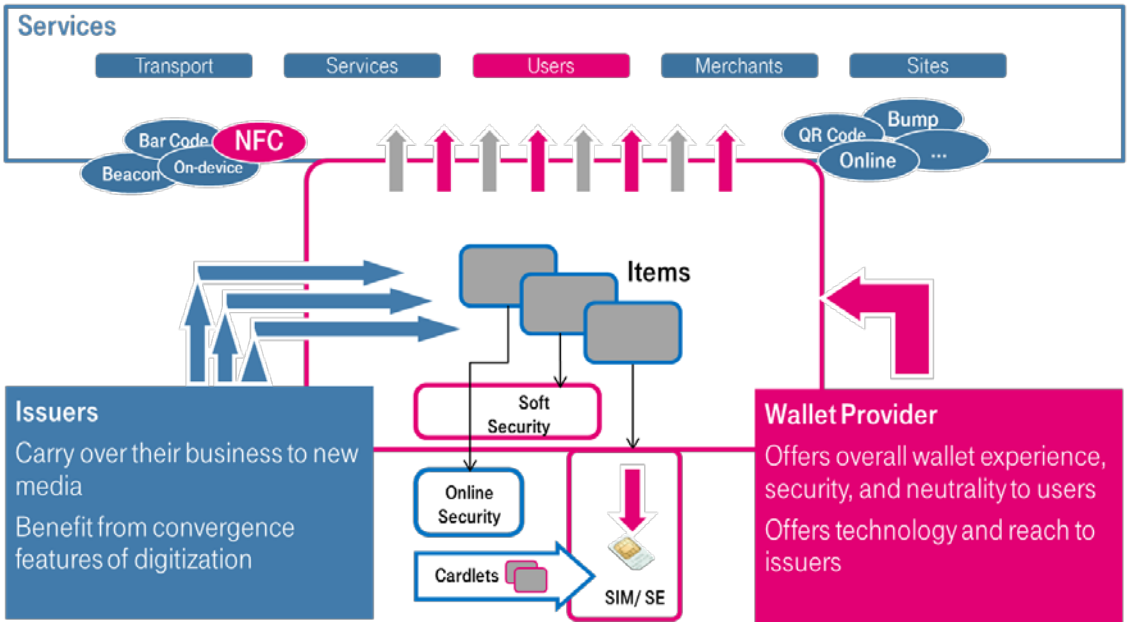

Figure 3: Simplified view on a convergent wallet platform architecture

To take the wallet idea where it helps to deliver more control for the end-user and foster a dynamic business ecosystem, the concept of a digital wallet needs to be generalized. We turn it into a neutral platform approach which doesn't focus one or two commercial use cases, but a user-centric concept around payment, entitlements and identities, collectively called 'claims'.

As can be seen in Figure 3, the generalized digital wallet concept embraces the use of SEs and NFC, but it also introduces the wallet as a 'blank canvas' which is used by service providers (specifically those that 'issue' any kind of 'tokens') to deliver their specific services. They may make use of assets like SEs, but are also able to employ regular cryptography in main memory or refer to their own security services in the cloud if online connection can be provided. The wallet provider may offer own services and use own assets too, but most important is, that the wallet – and most likely all relevant assets, like SEs, NFC transponders, etc. – are made available to any issuers/ services of the user's choice. Technology neutrality and non-discrimination will be the pillars for an approach to replacing our leather wallets entirely – and adding all the value digital wallets may deliver above their physical counterparts.

The following sub-chapters are only able to touch on some of the main aspects of such a paradigmatic approach:

- Client-centric, yet cloud-enabled
- User-centric, yet a basis for a viable commercial ecosystem
- Convergent across proximity, online and API-based transactions
- Supporting strong hardware-based authentication as well as future mechanisms (e.g. biometry)
- Technology-neutral, running on all operating systems with proper interaction capabilities, making use of system features as far as they are present

4.2 Identity, Items and User-Centricity

The approach taken here tries to project the need for some place to stow away valuables, keys and cards, as well as any kind of entitlements from and for the digital domain, which we call 'claims'. The visualization of a wallet allows to represent such rights and keys as 'cards', 'coupons', 'tickets' or similar objects, which we collectively call items. This concept aspires to create confidence in the end-user (and many of the service partners alike) that virtual items can be distributed and controlled similarly to their physical counterparts – and it creates a measure for the success of the technical designs in achieving this. However, there are benefits to the virtualization which must not be forfeit in the endeavour to create likeness with the physical world.

In many cases real world aspects can be generalized and be used in the broader scope of a digital wallet. Even today's payment cards already are multi-functional – and actually might even support different technologies: a credit card can still be used to mechanically print the card onto a form, if no reader for a magnetic strip is available. Modern cards usually have a chip embedded which directly connects to a payment terminal – and many might – as a fourth method – support NFC already.

In the example shown in Figure 4 this fact is generalized: a virtual card carries several different capabilities, which the wallet can show to the user. The use of the item might depend on a certain functionality (like hardware security being required for a proximity payment transaction) and availability of certain device features supported by the item (like NFC in this case). However, in addition, login functionality could be embedded in the item. When a website requires authentication, and accepts the issuer, the user will be able to pick the item – effectively choosing this specific identity for the given transaction. Whether the issuer uses the SE and whether the online service requires hardware security, is up to the respective parties. Mandatorily requiring hardware security and a specific communication technology, might limit the applicability of the wallet and the items in it to the very small number of devices. Within this framework it would be possible to provide a representation of the item, a visible customer number, and probably a cryptographic token for online use at all times. For secure NFC-functionality, not only an NFC-equipped device but also an SE might be supported, by the item's implementation. Nevertheless, the item could be used as a token of customer relationship by millions of customers, making them aware of the additional

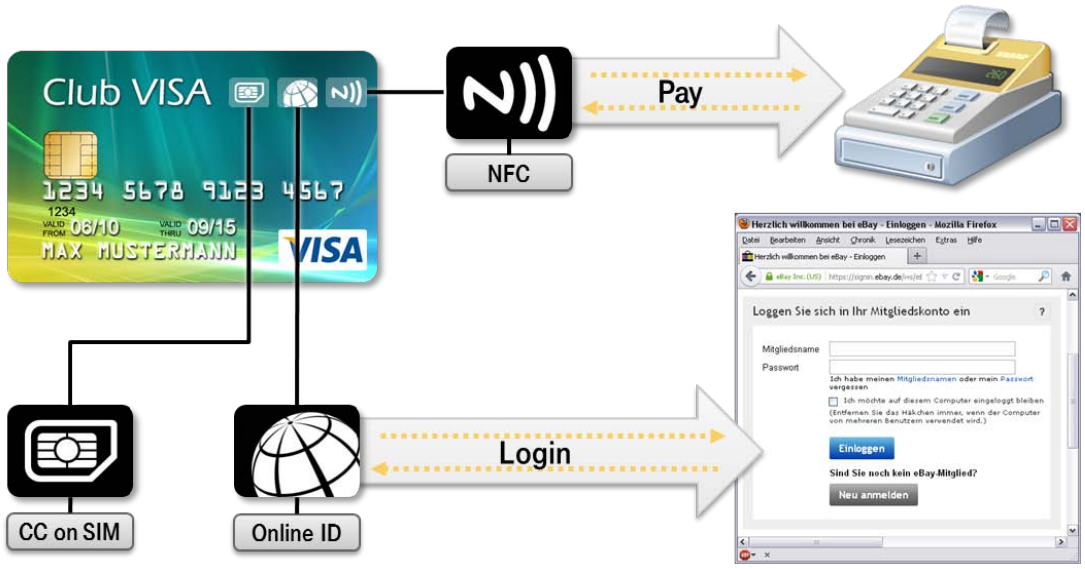

Figure 4: Schematic view on a multi-functional virtual item in a digital wallet

options available and giving those who already have the right equipment a noticeable advantage. There are many chances to reward higher security assets being made available (incentivizing users to buy phones with appropriate features, getting a new SIM), while maintaining compatibility with existing login schemas.

This concept should provide a clear path towards replacement of username/ password with cryptographic tokens being stored and associated with a wallet item. Moreover, a user might own several items usable at a specific service, providing a choice of which identity to use in a certain situation. In the usage scenario provided below, it should become clear that an online registration in the future might result in a ‘customer card’ being issued in return. For the five freemail accounts a user might own, five items will be available to choose from, when logging in. In a user-centric ‘pureplay’ scenario it is conceivable that an issuer of an identity ‘forgets’ all the other registration information (also alleviating the company of any privacy restrictions and liabilities) as it can be stored and signed (to protect from alterations) within the ‘identity card’ which will always be made available when the user logs in to the service again.

4.3 Usage Scenarios and Use Cases

An experimental version of the client software has been used throughout 2013 in a public trial with approx. 30 users at the Hamburg soccer club HSV. The primary function incorporated turnstiles equipped with NFC readers and an authentication schema developed by SkiData, one of the world’s leading vendors for building access control systems. For the wallet a set of virtualized tickets was created which could be ordered on a website after login. At the stadium the ticket could be selected, and thus, its NFC function be activated. When the phone is presented to the reader in the turnstile, the turnstile recognizes it as a valid ticket and opens.

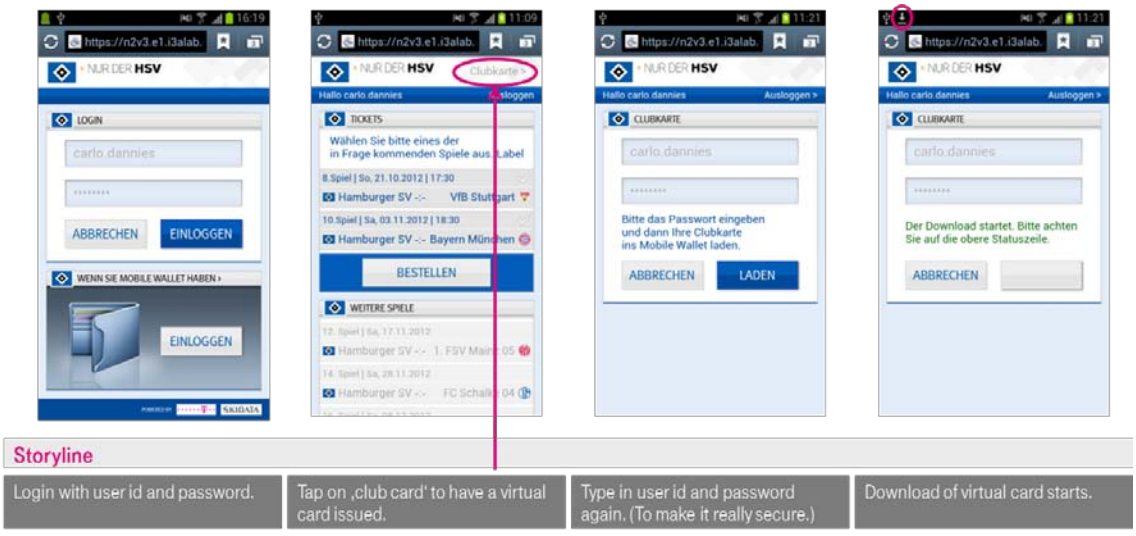

Figure 5: Flow for the acquisition of a club card via web portal

For the purpose of this document, a different functionality within the scenario will be highlighted: The issuance of a club card and its use for the ticket ordering process on the web site (Figure 5).

1. The portal's login page allows for regular login with username/ password. For the wallet scenario an option has been added to allow for the use of a wallet on the same device if present. It is conceivable that the web site could ask for the existence of a wallet or any kind of an 'identity selector' on the device so that non-wallet users wouldn't see any difference at all. (Though it might be useful to make people aware of the opportunity…)
2. Once logged in, the user might ask for a club card being issued, in case there is none on the wallet yet. This would be a typical function found in the 'account' or 'profile' section of a service and the business logics around it are entirely up to the service. It is conceivable that a fee can be asked for the issuance of a club card, especially if it requires security hardware being rented or if process costs are significant.
3. In our example additional security is applied and the user is asked to provide the password again (between login and application for the club card time might have passed and users might have changed.) Again, this is up to the issuer and might even be connected to a process involving risk analysis in the backend before a club card gets issued at all.
4. In this instance a club card is issued, using the standard upload process of the Android operating system the wallet runs on. (Denoted by the symbol in the top line of the screen under the control of the operating system and well-known to Android[29] users.)

Behind the scenes, in this particular implementation, a JSON authentication token was generated which can be passed on to the web page asking for an authentication token

[29] The model implementation was done on an Android phone. The wallet itself runs wherever HTML5 can be run, and in particular the online functions could be ported to other platforms with little effort.

in the same way as on the first screen in the figure above. Furthermore some administrative information (categories and rules) got packaged together with a URI to the graphical representation of the club card. This does not only allow for a proper display of the item in the wallet but also might help the user to categorize and manage hundreds of wallet items at once. The wallet software also makes use of this kind of meta-information to e.g. match a website's requirements with the existing tokens to reduce the choices offered to the user to the accepted items.

Certain token types (e.g. JSON and SAML), identity frameworks and protocols can be supported in the wallet itself, others can be implemented through cardlets on the secure element, improving security with hardware functionality, or make use of APIs for the management of items in trusted software modules in- or outside of the wallet.

4.4 Acceptability, Attractiveness, Marketability

Preserving an item metaphor as basic principle for user and partner interaction, several benefits can be realized:

- Reduction of complexity in user interaction around authorization tokens, certificates, etc.
- Harmonized handling of various security, authentication and identity transactions
- Compatibility of business processes for services
- Abstraction of various technical capabilities and protocols
- Creation of an ecosystem for digital claims with attractive propositions for existing players (e.g. in the payment ecosystem) but also with tremendous potential for new services and innovations

The added feeling of control (only items which have been selected in the wallet can be read via NFC) and harmonized interaction across all different kinds of items has shown best results in user tests. Not all interests of parties in the ecosystem can be addressed at once, and – at no costs – confidence of the users should be betrayed. The paradigm lends itself to a high level of transparency as all the information within an item could be displayed and transactions will be recorded in a history function. We have found several instances where suspected disadvantages compared to existing methods could be turned into true win-win situations (Figure 6):

- Coupon marketers are happy to use the wallet as a new channel, but users asked for automated use of coupons which would render coupons as marketing means effectively useless: the wallet can help to sort out applicable coupons automatically, but the general policy of always making transparent what is going to be communicated, provides proper awareness for the source of benefits being given.
- Existing applications for payment, couponing or ticketing seem like completion to a user-centric wallet. Through the introduction of an API the wallet became open to such applications. Almost all participants in the relevant market segments see the advantage of a neutral application governing, e.g. NFC

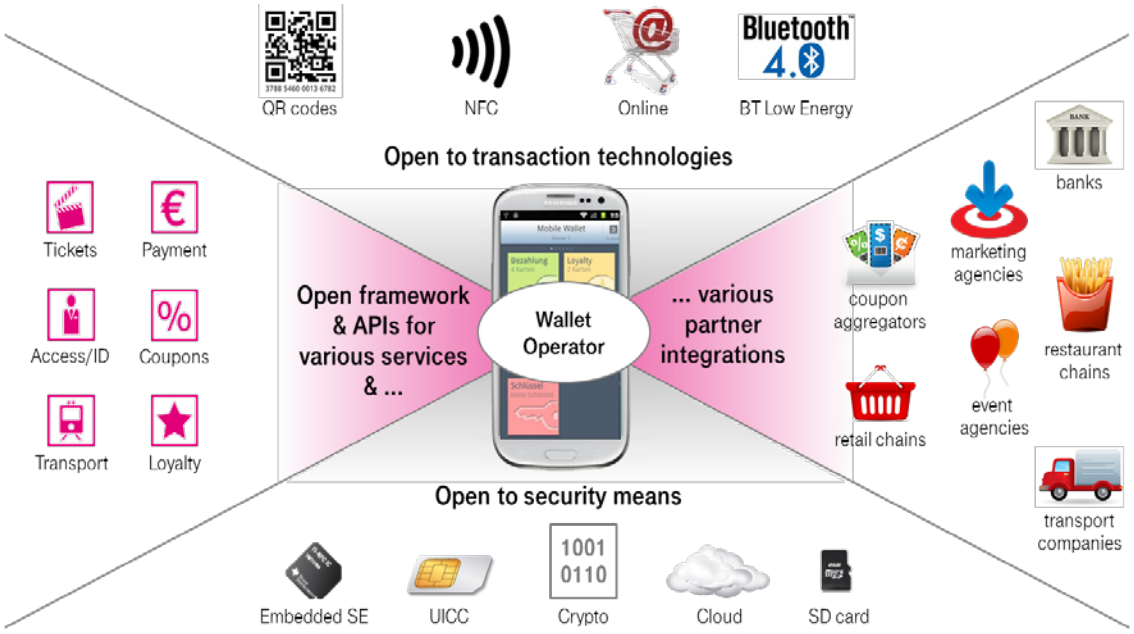

Figure 6: The digital wallet ecosystem

transactions across all different brands as limited choice (and fencing out direct competitors from a brand's marketing application is just normal) also limits acceptance on the consumer side. E.g. coupon apps can even provide additional functionality to the wallet, but now can cede coupons over to the wallet for combined NFC check-out with payment and loyalty cards at the payment terminal.

- The overall concept of the convergent wallet has been influenced by the works of Kim Cameron and the Info Card foundation. By opening up the playing field for the exact implementation, protocols and security mechanisms being used[30], token-based authentication and authorization can be packaged in an attractive and 'tangible' way. In fact, adding OAuth 2.0 to an existing loyalty card should be just as easy as creating virtual customer cards from username/ password-based identity management of today's web services.

The business ecosystem our work envisions embraces distinct roles for wallet providers and service providers. Wallet providers might want to get paid for their reach in the end, but it might also be attractive to lower entrance barriers in the beginning. Most likely to become wallet providers are those, who also own critical assets like secure elements which service providers are willing to disburse in exchange for higher security. Many transaction types can be enabled by the wallet provider which can be monetized: application for a payment or loyalty card, download of a coupon, use of keys and tokens, etc. A wallet provider who promises to keep identity information secure and increases convenience might also find that consumers are willing to pay for something which really is 'their digital wallet', and not the one of brand XYZ.

[30] CardSpace came with its own protocol and security provider concepts, based on WS*

The service providers (especially the issuers) will regard digital wallets as additional channels for their regular businesses – for the good and the bad of it: for marketing purposes a convergent wallet is a clear step forwards in 'cross-channel marketing' justifying new expenses, to event and transport ticketing, NFC and a convergent purchase process holds benefits enough to reduce operational costs in the mid-term. For payment providers and banks the benefits are not so obvious, plastic cards are not likely to be dropped for the next five to ten years, and customers might not want to pay for another (virtual) payment card. The first proximity payment services not supporting and issuing plastic cards anymore will likely be able to reduce their cost structure significantly and cause an innovation impulse in the industry. Besides such disruptive changes, fraud management for virtual cards in wallets can be improved above the plastic card level to make this digitization step attractive to the more flexible payment services.

4.5 Outlook and Conclusion

The current development of wallets throughout industries can help a user-centric identity paradigm to succeed in the market. The design presented is a commercially viable approach covering many of the privacy concerns we might find throughout different regions, cultures, industries and technical capabilities.

Work is ongoing to replicate and synchronize a user's wallets on different devices. Standardization of interfaces to web browsers could help to incorporate wallets into online processes. Current provisioning processes for secure elements, as well as business support functions for wallets are complex – and, as a consequence, often overly expensive. The wallet paradigm presented herein should allow for massive scale to bring down these costs offering appropriate security at appropriate costs. There is a need to for strong authentication and more security in the identity and e-commerce industries; alongside secure elements in SIM cards and mobile phones, PC chipsets hold potential (e.g. TPM) for wallets on PCs. Due to the technology neutrality of the approach presented, non-mobile devices could be added to the momentum of a wallet with relatively low effort.

Overall goal here is to ease the use of crypto- and hardware-based security and bring down costs, so Internet security can be increased significantly within the next years. The wallet providers will have to take a neutral position (perhaps not in the beginning, where exclusive partnerships might be needed to distribute the financial burdens of the product introduction across several parties) and will be forced to watch their use of critical data to prove trustworthiness to customers and partners. NFC technology has already introduced means to not even let the wallet provider know that the NFC function has been used for a payment transaction. Wallet providers might want to avoid liabilities on the one hand but also could provide added value to the end-user by aggregation of such data. User-centricity can be a way to solve this seeming contradiction – the user could decide to let the wallet provider use the data to implement useful functionality.

It is conceivable that a wallet provider can offer services around privacy and transparency. For example, a password safe functionality could be integrated into the wallet, representing every username password-combination as virtual card, or a guarantee for unlinkability of data communicated in transactions could be provided as a service to privacy-aware issuers. Another option might be a service for users to trace back past actions for more transparency, export them to financial management or tax calculation software.

The approach presented doesn't try to solve the issues of privacy, security, or transparency in an all-embracing solution; it won't stop identity theft or abuse of personal data either. It might, nevertheless, prove to be a tool in the hands of the user towards informational self-determination. To the industry it might be a puzzle piece to increase security in the mass market, to win and keep the confidence and trust of all the people in the digital world of the (not so far) future.

4.6 References

[1] E.-J. Steffens, A. Nennker, Zhiyun Ren, Ming Yin, L. Schneider; The SIM-based mobile wallet; 11/2009; DOI:10.1109/ICIN.2009.5357095 In proceeding of: Intelligence in Next Generation Networks, 2009. ICIN 2009.

[2] GSMA, Mobile NFC - White Paper: The Mobile Wallet; September 2012; http://www.gsma.com/mobilenfc/wp-content/uploads/2012/10/GSMA-Mobile-Wallet-White-Paper-Version-1-0.pdf

[3] Kim Cameron; The Laws of Identity; May 2005; http://msdn.microsoft.com/en-us/library/ms996456.aspx

[4] Information Card Foundation; http://informationcard.net/

5. Outlook

5.1 Research Agenda 2020 – Recommendations

Recently, at the CeBIT fair 2014 representatives from Fraunhofer[31] handed over a cyber security strategy and position paper[32] to Germany's Federal Minister of the Interior and the Federal Minister of Education and Research. Seven action items have been identified building the recommendations for the research agenda until 2020:

1. Leadership in cross-domain security technologies
   Support of research and development of cross-domain security technologies improving the security level of enterprise software, embedded systems, industry 4.0, and Internet based services.
2. Cyber Security Laboratories
   Both potential and impact of new solutions to fight cyber crime and industrial espionage have to be proven by empirical analyses and prototypes in cyber security labs.
3. Security by Design
   The development of methods, processes, and tools needs to support the complete security life cycle of products, solutions, and services.
4. Verifiability by independent 3rd Parties
   The position paper recommends testing and evaluation of security solutions at every stage of the development life cycle by independent 3rd parties.
5. Privacy by Design
   Personal data is supposed to be protected by privacy enhancing technologies and infrastructures in order to avoid unauthorised access and misuse.
6. Overview of the situation for decision makers
   Up-to-date aggregation and interpretation of vulnerabilities and incidents underpins a reliable and sustainable overview of the situation to support decision makers efficiently and effectively.
7. Usable Security
   Security methods, mechanism, and processes need to be defined in such a way that developers, administrators, security experts as well as non-technical people are able to fulfil and achieve security related goals.

The three contributions discussed in this WWRF Outlook have already pointed out some promising approaches to single agenda points from above. How to implement Privacy by Design, for example, has been described in 7 Foundational Principles by the Information and Privacy Commissioner of Ontario, Canada, in chapter 2. Two general

[31] http://www.fraunhofer.de/en.html

[32] http://www.fraunhofer.de/content/dam/zv/de/ueber-fraunhofer/wissenschaftspolitik/Fraunhofer-Strategie-%20und%20Positionspapier%20Cyber-Sicherheit%202020.pdf, Mar 2014

perspectives on cyber security are shown in chapter 3; first, the summary of the European Cyber Security Strategy gives an overview about the landscape, industry associations and groupings; second, a short overview about cyber security in industry gives some insights on how a large Internet supplier addresses cyber security in general. The so-called wallet paradigm, finally, explains in chapter 4 how to integrate security mechanisms by design in mobile apps in a user friendly way.

5.2 EU Horizon 2020

Research funded by the European Commission is divided into Framework Programmes, usually of six years each. Most current projects are being funded under the 7th Framework Programme (FP7) which, in the period 2007-2013, has spent around €300m on projects under the heading of 'Trust and Security'.

Beginning of 2014 the EU's new research framework programme "Horizon 2020" has started with the first calls[33] for proposals. From a cyber security perspective two calls are most interesting. The first one is part of the comprehensive ICT objectives in the *industrial leadership* pillar: "ICT-32-2014: Cybersecurity, Trustworthy ICT"[34]; this call contains from security-by-design for end-to-end security to activities supporting the cryptography community a broad range of research and development activities in order to identify new paradigms for the design and implementation of security, privacy, and trust. The second call related to cyber security "DIGITAL SECURITY: CYBERSECURITY, PRIVACY AND TRUST"[35] is part of the *societal changes* pillar. Major objectives range from privacy to access control as well as risk management and assurance models.

5.3 The Role of WWRF

The Wireless World Research Forum, in parallel, will continue with supporting the exchange of cyber security challenges and strategies in its Working Groups and conferences. Since 2001, the conferences have been providing a platform for pre-standardisation and global dissemination of project results. And in particular, special sessions like in Vancouver will – from time to time – raise awareness for cross-cutting challenges such as security, privacy, and trust. At all events the four Working Groups are open for addressing specific security requirements and privacy concerns according to their focuses: "WG A – User Needs & Requirements in a Wireless World", "WG B – Services, devices and service architectures", "WG C – Communication architectures and technologies", and "WG D – Radio Communication Technologies".

[33] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/index.html

[34] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/96-ict-32-2014.html, deadline Apr, 23rd, 2014

[35] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2014-1.html, deadline Aug, 28th, 2014

6. Authors

(In alphabetical order)

Michelle Chibba, Policy and Special Projects at Office of the Information and Privacy Commissioner

Biography: Michelle Chibba oversees the Policy Department and Special Projects at the Office of the Information and Privacy Commissioner of Ontario, Canada (IPC). Her department is responsible for conducting research and analysis, as well as liaising with a wide range of stakeholders to support the Commissioner's leadership role in proactively addressing privacy and access issues affecting the public. She has over two decades of professional experience, most of it in the public sector where she managed several strategic policy projects. Early in her career, Ms. Chibba worked in the private sector as well as for a non-governmental policy research organization in the U.S. One of her many accomplishments within the government was as Quality Manager for the Health Economic Development Unit, where she was instrumental in implementing a quality management system that was successfully registered to the ISO 9001 standard. For this, she received the Amethyst Award for Outstanding Public Service. She is also a recipient of an Ontario Ministry of Health and Long-Term Care ACE Award for achievement, commitment and excellence in Stakeholder/Partner Relations. Ms. Chibba received her master's degree from Georgetown University (Washington, D.C.), with a focus on ethics and international business.

Jörg Heuer, Research & Innovation Director Payment & Transactions, Innovation Policy at Deutsche Telekom Laboratories

Biography: Jörg Heuer started working for a Deutsche Telekom engineering subsidiary in 1997, defining and leading more than 30 projects for all divisions of the Deutsche Telekom group. Currently Heuer is responsible for Technology Exploration and the publishing of a periodic report on technology developments for CTO/ CMO level management and innovation departments of Deutsche Telekom group. He is the responsible senior manager for the 'Overarching AAA Programme' (Authentication, Authorization, and Accounting) of the group's innovation department.

Mario D. Hoffmann, Head of Department "Service & Application Security", Fraunhofer Institute for Applied and Integrated Security (AISEC)

Biography: Mario D. Hoffmann (43) received his diploma in computer science from Darmstadt University of Technology, Darmstadt, Germany, in 1998. His diploma thesis he completed at Nanyang Technological University, Singapore. In 1999 he joined the Fraunhofer Institute for IT Security (SIT) in Darmstadt becoming

head of department ”Secure Mobile Systems” in 2004. Since 2009 he has been responsible for the research department “Service & Application Security” at the Fraunhofer Institute for Applied and Integrated Security (AISEC) in Garching (near Munich). Mario Hoffmann has been coordinating research projects and proposals for more than ten years. His research is dedicated to multilateral secure identity management in contextual environments. Mr. Hoffmann has been chair of the Working Group "Security & Trust" of the Wireless World Research Forum (WWRF) from 2005 to 2012. Since 2009 he has been playing an active role in the Kantara Initiative – hosting the yearly conference in 2012. He has been track and workshop chair as well as member of programme committees of distinguished conferences and author and co-author of more than twenty publications.

Dr. Nigel Jefferies, Chair of WWRF and Senior Standards Manager with Huawei Technologies

Biography: Nigel Jefferies is a senior standards manager with Huawei Technologies and Chairman of the Wireless World Research Forum. He is currently a member of the Secure ICT Research and Innovation working group of the European Commission’s NIS (Network Information Security) Platform. Previously he was Head of Academic Relationships within Vodafone Group Research & Development and a Principal Mathematician at Racal Research Ltd. In the past he led the European-funded IST project SHAMAN, which studied the security of future mobile systems, and ran the Secure Applications Steering Group for Mobile VCE. Other collaborative research projects on various aspects of security for mobile communications include 3GS3 in the UK-funded LINK programme, and ASPeCT and USECA in the European ACTS programme. His research interests include cryptography, security of systems and applications of mathematics to telecommunications. He received a PhD in functional analysis from Goldsmith's College, London, and an MA in mathematics from the Queen's College, Oxford, and is a visiting professor at Kingston University. He is a Fellow of the Institute of Mathematics and its Applications and a Chartered Mathematician.

7. Imprint

Wireless World Research Forum
c/o Format A AG
Pfingstweidstrasse 102b
CH-8005 Zürich

Secretariat:
Vinod Kumar
Alcatel-Lucent France
Centre de Villarceaux
Route de Villejuste
91 620, NOZAY
France
e-Mail: vinod.kumar@alcatel-lucent.com
Phone : + 33 1 30 77 27 37
Fax : + 33 1 30 77 61 75

The WWRF is a non-profit organisation registered in Switzerland

Chairman of the Forum:
Dr. Nigel Jefferies

Editor-in-Chief: Mr Sudhir Dixit

The WWRF Outlook Visions and research directions for the Wireless World

ISSN 1662-615X is published non-periodically by the Wireless World Research Forum
http://www.wwrf.ch