Discrete Hardware Apparatus and Method for Mobile Application and Communication Security

Paschalis Papagrigoriou[1], Anargyros Plemenos[1], and Ioannis G. Askoxylakis[2]

[1] EMPELOR GmbH, Zug, Switzerland
{papagrigoriou,plemenos}@empelor.com
http://www.empelor.com, http://www.secocard.com
[2] Institute of Computer Science, Foundation for Research and Technology - Hellas, Heraklion, Greece
asko@ics.forth.gr

Abstract. With the dramatic shift of internet use away from desktop and laptop PCs toward smartphones and tablets, protection thresholds for application, device and communication security have significantly lowered. Most attempts on reversing this situation by means of converting standard mobile devices into tamper-proof equipment have proven to leave ample space for vulnerability of mobile processes and communication content. The only high efficacy method of sheltering against spying and fraud is seen in a new approach where a dedicated piece of discrete hardware is tasked with all security related operations while the standard cell phone or tablet remains unchanged, providing only its connectivity capabilities. The increasing cost caused by e.g. fraud in the area of mobile banking provides the background to economically justify this effort, which can in parallel support many other areas of mobile security.

Keywords: Mobile, internet, security, espionage, fraud, hardware.

1 Challenges for Mobile Application and Communication Security

Smartphones and tablet computers are on a very large scale in use for mobile internet access. Global user groups consist of consumers as well as enterprise and public sector employees. The ongoing use progression has been ignited and still is driven by aggressive offerings of internet and mobile network service providers, by declining cost of mobile communication due to increased competition, by people's growing desire for improved flexibility, competitive advantages and location independence, as well as by omnipresent promotions which are individually tailored to the consumers as a result of advanced monitoring mechanisms of their communication behaviors and patterns.

Media scientist Mark Andrejevic says "We are communicating in a context that uses us as advertising platforms for each other"[1]. Andrejevic characterizes this situation as a formal subordination of social behavior to commercial requirements.

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 102–112, 2014.
© Springer International Publishing Switzerland 2014

Mobile IT infrastructure users with their craving for increased mobility and dynamic use of resources for the purposes of accelerating communication, optimizing cost and gaining competitive advantages, seem to be willing to sacrifice their privacy. Especially younger people show an increasing tendency to "publish" their lives towards larger internet communities, thus making their personal information easily accessible for anyone. It may not be surprising at all that this promptness to publicly display personal information including photo material in social networks is thankfully welcomed by public authorities in their pursuit of alleged traffic offenders as a both legal and very cost-effective identification method.

It appears by far more worrying how simply and easily one can get access not only to publicly available information, but also to non-public information and communication. Such possibilities are offered by a tremendously high number of malicious "apps" for smartphones[2]. Recent studies[3] show how dangerous smartphone apps have become. The widespread use of so-called IMSI-catcher equipment, available by online order[4], is definitely to be considered a criminal act[5]. The associated potential risk may have a wide variety of forms and manifestations for the user of mobile communication or services provided via the mobile internet such as mobile commerce, mobile banking and mobile payment, starting from privacy intrusion, spying on intellectual property and business secrets, to classic identity theft for fraudulent purposes.

In the wake of revelations of state agency spying on consumers, business people and politicians from other nations, we can rest assured that even if criminals may lack the excessive resources which have been allocated to state spying agencies, we need to be aware that both groups of privacy intruders, those with a legal background and those without, are out there doing their jobs. Since data and voice communication have been mobilized through fast miniaturization and mobilization of devices, rapid expansion of mobile networks and growing availability of all types of services over these networks, data privacy can be compromised in ways not only available to criminal forces, but also to legal or semi-legal entities and forces[6]. All this considered, risk awareness is still at a rather low level with enterprises and consumers.

2 Conventional Approach and Failure

For the purpose of establishing the obviously missing security for the public sector, for enterprises and consumers, many contributions have been made, with mostly discouraging results: None of the mainstream service providers currently offer appropriate mechanisms, procedures or devices which could ensure sufficient security for those who need to be secured[7].

Technically, information technology has a long history of creating and offering protection. Unfortunately, this is mainly true for the immobile IT the pre-cellphone world consisting of PCs, server farms, and closed circuit networks.

Existing security means which are mainly used by enterprises and in the public sector, include defense mechanisms such as firewalls, VPN tunnels, end-to-end

encryption, two-factor authentication, strong passwords, and certificate-based logon[8]. Practically all of these protection mechanisms developed for the pre-mobile IT world can be overcome.

Privacy intrusion is possible for state-empowered forces as well as for ethical hackers. Consequently, we can rest assured that any defense can as well be overcome by terrorists, enemy states, competitors, criminals, and whoever is willing to spend enough time and energy to "hack" into privacy protection systems of the sort as it is in use today[9].

Mobile IT specialists such as providers of device management software have a tendency of creating the illusion that there is no risk in using arbitrary private end user devices in the context of confidential business processes ("BYOD"). The same can be said about providers of antivirus solutions and about device manufacturers who want to make bank customers believe that their online transactions will be executed exactly as shown on their device and a user can trust what she sees with regard to the recipient and the amount being transferred.

According to a recent study published by PwC, "Information Security Breaches Survey 2013", 50% of large (meaning enterprise level) organizations have implemented mobile device management (MDM) solutions in an effort to mitigate risks connected with BYOD or with the overall use of mobile communication devices to access enterprise resources like email, hosted applications, and file servers. These software-only protection tools give enterprises the security of "having done something". Any security breach committed by someone more malign than an ignorant employee cannot be prevented by these systems. The logic behind this mismatch is quite simple: the axiomatic paradigm "Software cannot be protected by software" prevails more than ever in the mobile sphere [5].

When it comes to hardware security, the incumbent approach of "device hardening" is basically in contradiction with the device producers' philosophy, and therefore becoming increasingly inappropriate. The shorter life cycles of consumer devices combined with the tendency of allowing use of privately owned consumer devices in a business or public administration environment represent a serious obstacle for establishing sufficient security mechanisms for all possible usage scenarios.

Public sector employees in Germany and other countries have been equipped with special versions of cellphones and smartphones to enable use of classified material on their mobile device. These devices, heaviest price tags, were ordered by the domestic IT security industry, and some of the vendors even delivered a job well done. Phones featuring virtualized operating systems and interfaces as well as customized boot ROMs requiring consent from the device manufacturer to avoid copyright infringement, can successfully prevent tapping or other forms of intrusion yet at a high cost. Besides the hefty investment for the procurement itself, the unfortunate users were gifted with devices at least three generations older than those of their peers without a phone authorized for confidential information because of the lengthy evaluation and authorization processes. In addition to this reputation affecting side effect, the "trusted" phones provide a lot less battery life and show painfully limited overall computational power.

3 A New Solution Concept

A different approach on fighting existing threats to data and communication security is the exclusive use of dedicated hardware for all security functions. There are several reasons why this approach was found more likely to achieve all safety objectives.

The solution for providing increased and sufficient mobile application and communication security in all environments where this is a fundamental requirement is the introduction of a separate security device. This device will be used in parallel with a smartphone or tablet, where the latter will provide connectivity, and the former adds the necessary security mechanisms to all activities related to the use of mobile devices.

It was found that minimum requirements for such security devices include:

- Affordability, i.e. a purchasing price within a reasonable proportion ratio to the cost of the standard mobile device it will accompany for protective purposes. Possible fraud damage prevention numbers should be left out of the equation. A recent study by PwC found that in the UK, 18% of IT spend was allocated to security in areas where security is a high priority. In other areas, the percentage spent on IT security was only 10% of the IT budget [10].
- Ease of use, i.e. an extra device which a majority of potential users will view as a discomfort should be as small and lightweight as possible to achieve maximum acceptance.
- Compatibility with widespread standardized interfaces; in the sense of fast and easy proliferation, the security device needs to provide the ability to interact with the largest possible variety of end-user devices via standard interfaces and thus maintain the greatest independency from device manufacturers and proprietary communication methods and protocols.
- Versatility in security applications; as a minimum, high-security online banking should be supported by providing a secure means of data display and input.
- For more security applications such as supporting a more secure use of credit cards and other payment types, existing processes must remain intact. A new POS device needs to be deployable without requiring changes to remainder of the existing infrastructure. This applies to the use of state of the art POS related back-end infrastructure and includes other security areas such as time and attendance control, physical access control, closed group payment systems, and the overall use of corporate and civic ID cards.
- Ideally, the device should be able to provide a wide range of security mechanisms such as storing and handling PKI-certificates for secure email, secure access to a company VPN, as well as secure voice communication with encrypted VoIP including gateways to fixed-line networks.
- It should be considered to add the function of creating a protected data area inside the smartphone or tablet, which must not be accessible without the security device in place and the authentication of the authorized user properly checked.

The challenge lies in combining the appropriate technology with the required functionality, at the same time exhibiting comfortable usability for the potential users.

3.1 Framework Architecture and State of Development

Basic Secocard Functionality. Secocard [11], developed by [12], in the first place acts as a card reader when a smartcard (ICC) is inserted into the device. The smartcard will actively trigger the ICC in-service register (ISR), which in turn notifies the ICC task about the presence of the card. The ICC task sets the card status to "PRESENT" and forwards the status to the application management task. The application management task checks the card type by means of the ICC task which returns the ATR of the ICC to the application management task which then will select the standard compliant application, i.e. it will run EMVCo Terminal or Secoder-2, etc.. The actually selected application will be communicated to the display and keypad tasks, prompting the user for confirmation.

An incoming command APDU is processed under the leadership of the application task in collaboration with the display and keypad tasks, the communication tasks, and the ICC task or NFC task[13], respectively. The framework provides a generic way of processing an incoming command APDU, and of finally sending the appropriate response APDU back to the command APDU sender.

Secocard can also act as a smartcard or ICC (acc. ISO 14443) after being switched into card emulation mode, an operating mode of the NFC framework. This mode is generally used for contactless payment and ticketing applications. An NFC enabled module is capable of storing different contactless smartcard applications in one device.

State of the Art Systems. The present state of smartcard or ICC terminal architecture mostly POS (point of sale) or card reader terminals - calls for connecting an external terminal device via USB or Bluetooth with a host system, generally a desktop or notebook PC or a smartphone or tablet computing device, using T=0, T=1 or a proprietary communication protocol[14].

This architecture is characterized by the fact that relevant data need to be signed and/or decrypted by secret information stored on the smartcard or ICC, whereas after decryption or access granted through a verified digital signature by the rightful card owner, mostly by entering the correct Personal Identification Number (PIN) on the terminal, the same data will be handled shown on a screen, altered by a keyboard inside a system environment which is not trustworthy, namely a PC or smartphone which can be subject to the presence of Trojan horse software and many other forms of malice attacks.

3.2 Secocard Architecture

Security-relevant hardware is presented as a hardware abstraction layer which can be accessed by an internet access or connectivity device via middleware.

Thus, the Secocard architecture makes use of specific hardware components, such as an embedded secure element, a capacitive touch screen, audio support, as well as all relevant communication mechanisms required to connect to a large range of mobile devices currently on the market. The types of communication links to mobile devices or to cards and card readers include NFC, Bluetooth, Smart Bluetooth or Bluetooth Low Energy, and USB. The Secocard firmware provides a framework for an open set of security applications by offering basic functionality for application management, internet access via the internet connectivity of mobile devices, and accessing smartcards, using the relevant protocols.

Not present in the Secocard architecture is a radio module for direct access to a cellular network. The same is true for WLAN . These protocols have proven insufficient for reliable intrusion protection. Higher layer protocols, though, are implemented in the Secocard framework architecture to ensure its capability to establish, maintain and use a secured IP communication with e.g. a banks back-end data center or a secure email service.

Secocard architecture, unlike standard smartphones, PCs and tablet computational devices, does not comprise an operating system capable of running an arbitrary number of applications. As a result, it cannot be made subject to intrusion or any form of exploitation. The software consists of single tasks with task interactions implemented by means of message queues and semaphores. Tasks may also be triggered by interrupts via the corresponding interrupt service routine (ISR).

The Bluetooth pairing is a service that manages the discovery process and the Bluetooth-enabled device pairing process. It provides an interface to control the discovery and pairing process, and to manage the set of paired Bluetooth-enabled devices. It also maintains a database of Bluetooth profile information for each of the paired devices.

Figure 1 gives an overview on the Secocard architecture.

Related Work. Similar approaches of using dedicated hardware are not completely new to mobile IT security. Rohde & Schwarz SIT have introduced TopSec Mobile in 2009 to support voice encryption over GSM networks in an external hardware device which at that time communicated with standard GSM phones over the speaker jack, a connection which was later replaced by Bluetooth, and VoIP support was added. While the beauty of this setting voice is transported by the standard phone and over the mobile network only in encrypted mode was evenly invulnerable to all known tapping and intrusion methods, it lacked hugely in versatility. The device was so dedicated to its only application that even something undemanding as SMS encryption could not be integrated in a form that earned user acceptance. Similarly User Centric Temper-Resistant Device[15] enables a user control security and privacy[16] preserving device that can provide a secure and trusted execution and storage platform.

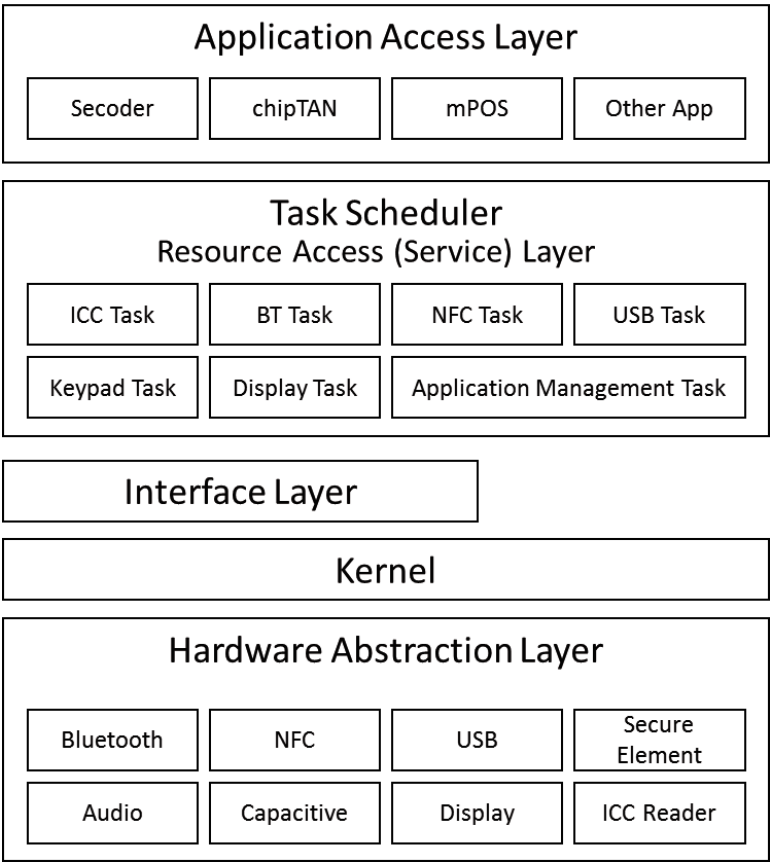

Fig. 1. Secocard architecture overview

3.3 Use Case: Online Banking

Online banking in Germany is a widespread form of handling a bank account through a web-based portal provided by a bank or a group of associated banks. It is used on a regular basis by almost 50% of all bank customers[17]. Generally, secure access to the web portal is being provided by requiring the entry of a pre-registered user name and a password. Once logged on successfully, for the transaction of wiring money or transferring funds to another account, different banks offer different varieties and methods to be used.

In almost all cases of online banking, a 6 digit transaction number (TAN) which is basically a one-time password is generated either in advance by the bank and given to the customer in printed form, where during the transaction dialog the customer is informed which exact position of the numbered TAN list must be used for the current transaction, or it is generated by a TAN generator device the bank hands out to their customers for a small fee. The TAN generator

device needs to read a certificate safely stored on the bank customer's money card, and is given the transfer information either by manual input or by reading a "flicker code" from the users PC screen.

Other methods in wider use comprise Mobile TAN (mTAN). mTANs are used by banks in Austria, Bulgaria, Czech Republic, Germany, Hungary, the Netherlands, Poland, Russia, South Africa, Spain, Switzerland and some in New Zealand, Australia and Ukraine. When the user initiates a transaction, a TAN is generated by the bank and sent to the user's mobile phone by SMS. The SMS may also include transaction data, allowing the user to verify that the transaction has not been modified in transmission to the bank.

The security level of this scheme depends on the security of the mobile phone system. It has become common in a variety of countries to attack the bank customer by obtaining a replacement SIM card for their phone either by cloning if the card data can be accessed or by ordering a replacement or multi-card from the mobile network operator if the victim's user name and password can be obtained by keylogging or phishing. As long as the victim has yet to detect that text messages are directed to anther card - as a basic function of the GSM standard, SMS will only be transferred to one card per subscriber - the attacker can transfer/extract the victim's funds from their accounts.[Wikipedia]

The mTAN online banking procedure in its vulnerability can entirely be replaced with "girocard" payment using the chipTAN standard as defined by the German credit industry. When using Secocard, keylogging and use of Trojan horses is successfully prevented, while phishing victimization unfortunately escapes technology based security solutions and instead requires the user to apply common sense.

Figure 2 provides an overview on how well-designed security standards allow safe mobile and online banking, and figure 3 presents how they were implemented on Secocard.

4 Discussion

The idea behind Secocard as a secure means of supporting protected online banking transactions and mobile payment services is that the same device with its secure architecture can also shield the dialog between bank and customer from eavesdropping and tapping. There is no need to exchange the small and lightweight device which is not really bigger than a few credit cards stacked on one another in case the bank customer subscribes to a new bank service or decides to change the way she wants to operate her account from her desk or any other place through remotely using the mobile internet - as long as the service is protected by a protocol and application which has been standardized according to the requirements of e.g. the German credit industry, and as such has been implemented beforehand. Even if an extra piece of hardware may be resented by many potential smartphone and tablet users, this may boost acceptance as the device is definitely compatible with all the smartphones, tablets and PCs. So as a result of the combinational logic, users will not have to worry whether or

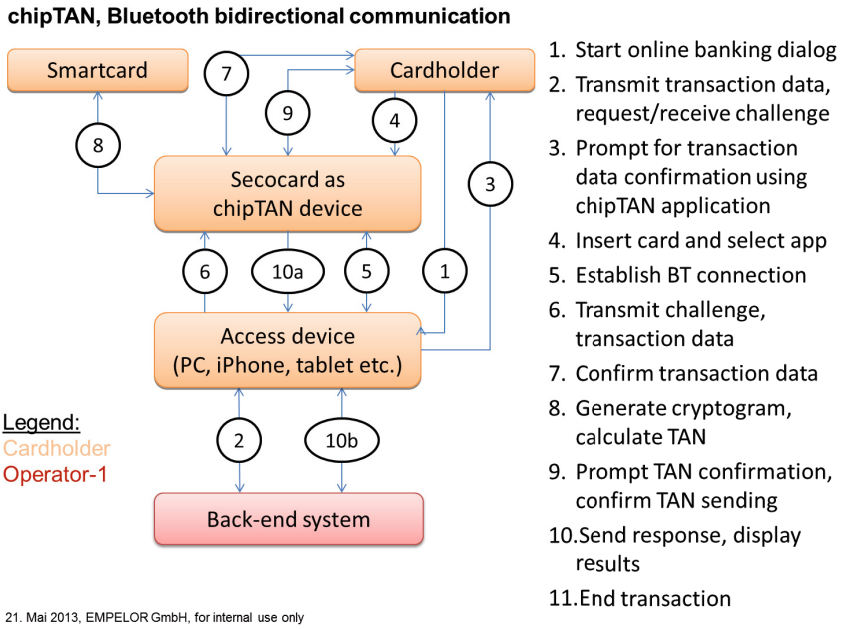

Fig. 2. Online banking process using chipTAN application on Secocard

not the next service a bank may promote could be something that will become corrupted within a few months or weeks following its introduction, as it has been the case with earlier banking applications designed to support mobile device use for online banking.

5 Conclusion and Outlook on More Supported Use Cases

Cost is definitely an issue when selecting the ideal equipment for retail card reading and transaction performing. Credit card schemes and banks are well advised to add more value to POS equipment for less cost. Secocard enables credit card schemes and acquirers to provide their merchants with full protection of a dedicated POS hardware solution which works well with their fancy smartphones and tablets. Also, the merchant can exchange the cell phone practically every day at random the POS device will remain the same and will not only run protected mobile payment and card acceptance services, but also online banking transactions and, if needed, it can also shield the dialog between the shop and a bank or a business partner, even a shop client, effectively from eavesdropping and tapping.

Reasonable manufacturing costs combined with a broad and growing selection of beneficial security functions from secure online banking and secure mobile POS to voice and email protection will contribute to making this development

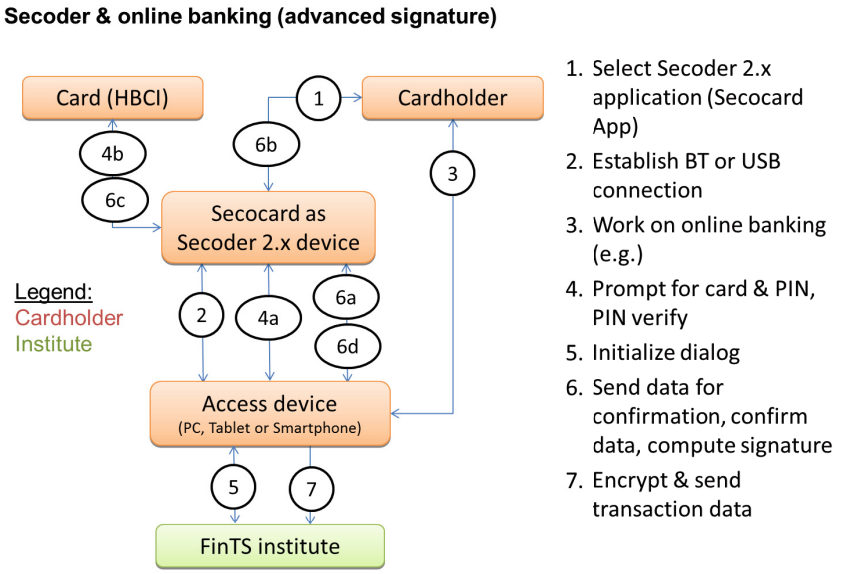

Fig. 3. Online banking process using Secoder application on Secocard

a real asset to wider user groups searching for higher levels of application and communication security. The robust architecture will show its resistance against all forms and powers of intrusion in official tests upon request by public sector customers.

In a dialog with the German public sector, support for the new electronic ID card is currently discussed as this could significantly contribute to an overall mobile data and voice privacy protection for the population.

References

1. Andrejevic, M.: Facebook als neue Produktionsweise. In: Leistert, O., Rohle, T. (eds.) Generation Facebook: Uber das leben im social net, pp. 31–49 (2011)
2. Zhou, Y., Wang, Z., Zhou, W., Jiang, X.: Hey, you, get off of my market: Detecting malicious apps in official and alternative android markets. In: Proceedings of the 19th Annual Network and Distributed System Security Symposium, pp. 5–8 (2012)
3. Suarez-Tangil, G., Tapiador, J.E., Peris-Lopez, P., Ribagorda, A.: Evolution, Detection and Analysis of Malware for Smart Devices. IEEE Communications Surveys & Tutorials, 1–27 (2013)
4. Frick, J., Rainer, B.: Method for identifying a mobile phone user or for eavesdropping on outgoing calls. Patent: EP1051053

5. Texas Criminal Lawyer Blog. Devices that Track Cell Phone Signals Violate Fourth Amendment, Say Privacy Advocates (2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf
6. Andriotis, P., Oikonomou, G., Tryfonas, T.: Forensic Analysis of Wireless Networking Evidence of Android Smartphones. In: Proc. IEEE International Workshop on Information Forensics and Security (WIFS 2012), Tenerife, Spain, pp. 109–114. IEEE (December 2012)
7. Internet Service Providers. Guiding Principles on Cyber Security. Guidance for Internet Service Providers and Government (December 2013)
8. Andriotis, P., Tryfonas, T., Oikonomou, G., Yildiz, C.: A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: Proc. 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2013), pp. 1–6. ACM Press (2013)
9. Petroulakis, N.E., Tragos, E.Z., Fragkiadakis, A.G., Spanoudakis, G.: A lightweight framework for secure life-logging in smart environments. Information Security Technical Report 17(3), 58–70 (2013); Security and Privacy for Digital Ecosystems
10. Department for Business Innovation and Skills. Information Security Breaches Survey (2013)
11. Secocard. The security Platform, http://www.secocard.ch
12. EMPELOR GmbH, http://www.empelor.ch
13. Akram, R.N., Markantonakis, K., Mayes, K.: Coopetitive Architecture to Support a Dynamic and Scalable NFC based Mobile Services Architecture. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 214–227. Springer, Heidelberg (2012)
14. Akram, R.N., Markantonakis, K.: Smart Cards: State-of-the-Art to Future Directions. In: IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 2013) (December 2013)
15. Akram, R.N., Markantonakis, K., Mayes, K.: User Centric Security Model for Tamper-Resistant Devices. In: 8th IEEE International Conference on e-Business Engineering (ICEBE 2011). IEEE Computer Society (October 2011)
16. Petroulakis, N.E., Askoxylakis, I.G., Traganitis, A., Spanoudakis, G.: A privacy-level model of user-centric cyber-physical systems. In: Marinos, L., Askoxylakis, I. (eds.) HAS 2013. LNCS, vol. 8030, pp. 338–347. Springer, Heidelberg (2013)
17. E-Banking Snapshot 39. Deutsche Bank Research (2012)
18. Courtois, N.T.: Computer Security at the Low, Hardware/Process/Memory Level. University College London (2009)
19. Leibholz, S.W., Frankel, C.T.L.: Tracking Inappropriate Data Exfiltration: Dealing with the Ubiquitous Insider Threat via Zero-Knowledge Proof (2013)