Security, Trust and Privacy in the SEcure MObile Payment Service

Stamatis Karnouskos [a], Anna Hondroudaki [b], András Vilmos [c], Balázs Csik [d]

[a] Fraunhofer Institute FOKUS (www.fokus.fraunhofer.de), Kaiserin Augusta Allee 31,
D-10589, Berlin, Germany, email: Stamatis.Karnouskos@fokus.fraunhofer.de

[c] Intrasoft International (www.intrasoft-intl.com), 19,7 Km Markopoulou Ave,
GR-19002 Peania, Athens, Greece, email: Anna.Hondroudaki@intrasoft-intl.com

[b] SafePay Systems Ltd (www.safepaysys.com), Kapás u. 11-15,
H-1027, Budapest, Hungary, email: vilmos@safepaysys.com

[d] ProfiTrade 90 Ltd (www. profitrade.hu), 25. Bécsi út,
H-1023, Budapest, Hungary, email: balazs.csik@profitrade.hu

Abstract: The Secure Mobile Payment Service (SEMOPS – www.semops.com) is an innovative solution for delivering a global mobile payment service. Among other requirements common to the mobile payment services, SEMOPS has tackled the security, trust and privacy issues that mobile payment scenarios pose. Existing approaches in mobile payment procedures have done little to fully address these three requirements. Via its open design, SEMOPS addresses these areas not only at the technology level but at the business model level as well. We present here the SEMOPS related activities with respect to security, trust and privacy, as they have been implemented into this mobile payment service.

Keywords: security, trust, privacy, business model, mobile commerce, mobile payment

1 Introduction

Security and privacy are essential elements for the success of mobile commerce and its applications. They are business enablers and not just add-on features. This is due to the fact that both elements are critical in fostering users' trust towards any mobile services and applications. Security, privacy and trust have been identified as critical enablers for the success of mBusiness by many European Union funded roadmap projects such as PAMPAS (Pioneering Advanced Mobile Privacy and Security [1]) and MB-net (A Network of Excellence on mBusiness Applications & Services [2]), as well as others such as Accenture & CERIAS [3].

In a mobile payment (MP) scenario we can define these three requirements as follows:

- Security: All steps in the procedure must be secure from the technology point of view. This means that confidentiality, integrity, availability and accountability requirements must be satisfied at the technology level.
- Trust: Trust is primarily a statement of belief. Mobility introduces critical and complex trust problems that are greater than the ones that have existed before in computer networks. Trust relationships at

different levels exist in the mobile payment procedure. For MP, trust must exist on the procedures (business side) and in the technology (trusted computing base)

- Privacy: The sensitive user data must be protected. Furthermore it should not be possible for any party to get the full payment process data, e.g., by linking a specific purchase to a specific user and/or her bank account.

Existing approaches in mobile payment procedures have done little to fully address these three requirements. Most MP procedures today use SMS or IVR (interactive voice response) as a method to verify user's identity, methods that have been proven to be insecure. Furthermore, users are usually asked to provide their personal information to a third party service provider in order for them to be able to register and get the service. Therefore they are asked to place immediate trust of their money and personal data on a previously unknown party. This third party is able to have the complete set of data for any transactions users make, therefore it is able to monitor users' private lives and of course do indirect profiling. It must be kept in mind that user-perceived security (the combination of technical security and trust in the procedures of the approach) is a critical factor [6] that decides on the success or failure of a payment service and therefore it has to be done correctly from day one.

The rest of the paper is structured as follows: We make a small introduction on the service and a typical scenario describes how it functions. Then we focus how security, trust and privacy are tackled in the SEMOPS business model [4] and its architecture [5]. Finally we refer to some future technology challenges, which will have an effect on SEMOPS and generally on any mobile payment procedure.

2 SEMOPS payment service

The payment service developed within the SEMOPS project is novel in the sense that it establishes a process flow that allows cooperation between banks and mobile operators. The transaction flow, which is customer-driven, follows a simple credit push model.

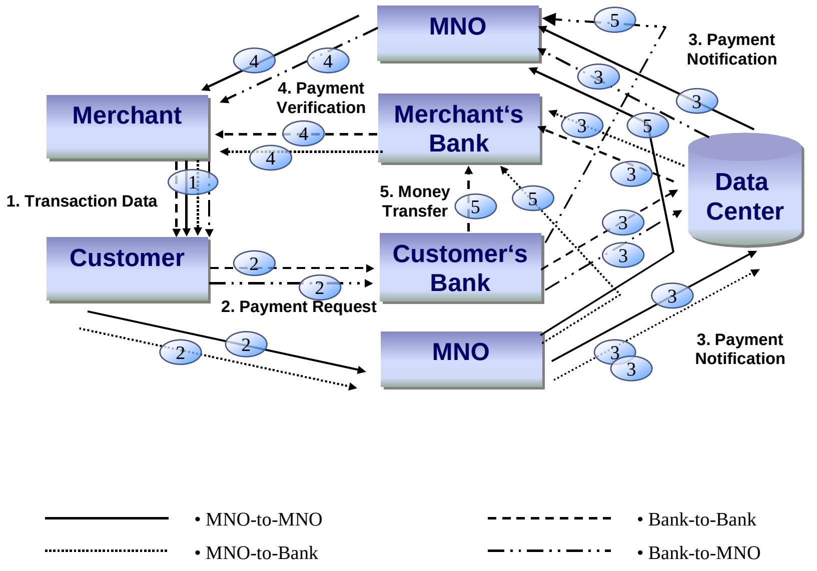

Figure 1 - High-level information and money flow

In Figure 1, one can distinguish the main players and components in a mobile payment scenario. Each user (customer or merchant) interacts with his payment processor e.g. home bank or mobile network operator

(MNO) only. The banks and MNOs can exchange messages between them via the Data Center (DC). We should mention that the legacy systems of the bank and the merchant are integrated in the SEMOPS infrastructure and are used as usual. A typical scenario assumes that:

1. The merchant (in general any realPOS/virtualPOS[1]) provides to the customer the necessary transaction details.
2. The customer receives the transaction data and subsequently initiates the payment request, authorizes it and forwards it to her payment processor (at the customer's bank or MNO).
3. The payment processor identifies the customer, verifies the legitimacy of the payment request and forwards this request to the merchant's payment processor via the DC.
4. The merchant's bank receives the payment notice, identifies the merchant and requests from him to confirm or reject the transaction.
5. Once the merchant side confirmation comes, the fund transfer is done and all parties are notified of the successful payment.

There can be different combinations, depending on whether the user (customer or merchant) uses her bank or MNO account and whether the merchant accepts the payment in his bank or MNO account. Furthermore the SEMOPS model is extensible, therefore any third service provider that can offer the customer an account (e.g., credit card or financial service provider) can also easily slip in the role of the bank.

3 Security, trust and privacy in SEMOPS system

This section focuses on the way all three requirements are tackled via novel existing technology.

3.1 Security Considerations

SEMOPS built up its security framework at the payment processor's side taking into account the following considerations:

- Banks do not allow encrypted information into the Intranet; therefore decryption must be done in the Demilitarized Zone (DMZ).
- Banks usually have their own authentication system, therefore SEMOPS must co-operate with existing infrastructures.
- SEMOPS uses heterogeneous transmission channels, including "strange" ones, like USSD; therefore secure protocols like SSL/TLS cannot be always used to encrypt the transmission channel.
- Different country regulations prohibit the usage of the same keys for encryption and signing; therefore SEMOPS must have multiple key pairs.

[1] VirtualPOS is any mobile device that can act as a POS.

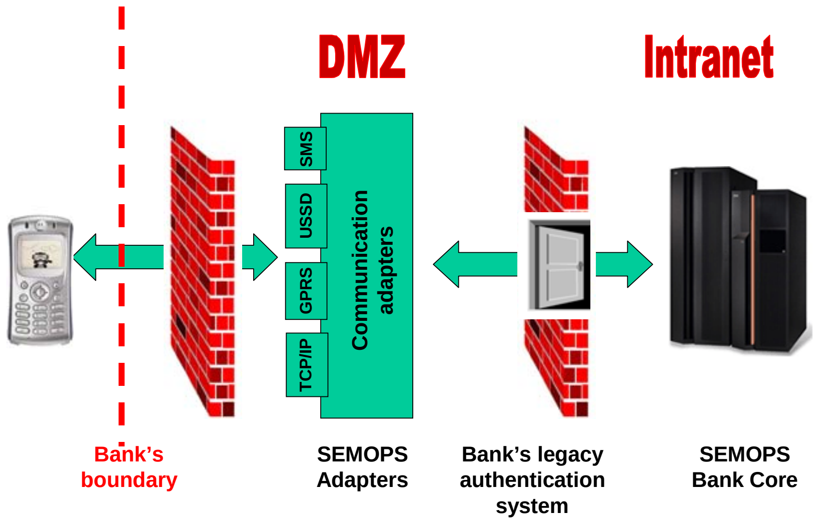

Figure 2 - Security infrastructure at the payment processor's side

Based on these limitations, SEMOPS realizes the security model depicted in Figure 2. The termination of the physical channels and the decryption of the messages take place in the DMZ. The decrypted information reaches the SEMOPS bank Module (residing on the Intranet of the bank) through the bank's standard authentication system, which is already used for applications such as home banking. Currently SEMOPS uses 1024 bit RSA encrypted XML with 3DES message keys, and also uses 1024 bit RSA digital signatures on the messages, but with a different key pair. The hardware security modules execute all the cryptographic operations in the system, resulting in the split security operations depicted in Figure 3.

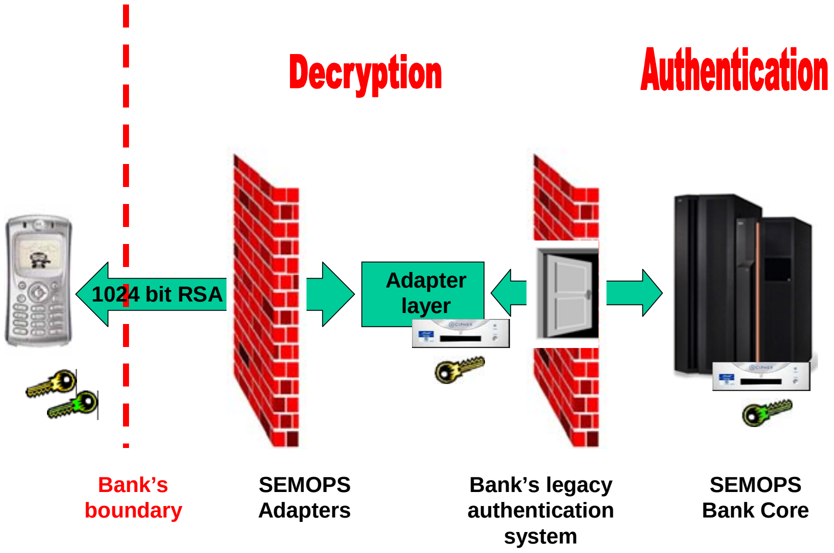

Figure 3 - Split security operations of SEMOPS

SEMOPS uses dual authentication method for identity control. Depending on the payment processor's requirement it is able to use digital signatures or encrypted pass-phrase authentication. The payment processor can decide, which authentication method to use and it provides his own public key (generated either by a trusted third party, or by the payment processor itself) to his users When the signed payment confirmation arrives the recipient is sure that the original data was not altered (data integrity), that the message could only have been signed by the holder of that private key (entity authentication). Therefore, the uniqueness of the digital signature and the underlying hash value provides an acceptable level of assurance to authenticate the sender and to verify that the sender was the originator of the signed data. Currently Secure Hash Algorithm (SHA-1) is used for all hashes in SEMOPS, including the hashes used in signatures. All references to hash algorithms are interpreted as using the SHA-1 hash algorithm defined in FIPS 180-1.

SEMOPS provides a strong end-to-end encryption for transferred data and allows the usage of different authentication techniques embedded into this encryption. This seems a viable solution, but in live environments it must be adapted to the usual practices of banks, which insist on not allowing anybody else to authenticate their users, as this task has to remain within the banks' legacy procedures.

3.2 Trust Considerations

The SEMOPS application for the mobile device is implemented in a) J2ME and b) with SIM toolkit (STK). We have taken into account the java language offered security in order to provide a trusted environment for the application to run, however also the STK implementation provides also a trusted base since it is harder to modify that part. Furthermore any updates happen via a secure connection to a trusted server or over-the-air (OTA) from the respective MNO that has control of the SIM card. Having a trusted execution environment is under heavy research internationally. SEMOPS tackles also trust at the business model, therefore an immediate need for add-on services like rating services are not needed.

3.3 Privacy Considerations

The user data that reside on the payment processor are protected with state of the art technology solutions such as encryption, limited availability, key management etc. The same is true for the data relying on the mobile phone, to which the user has access via a SEMOPS-specific authentication such as entering a password. Furthermore all SEMOPS interactions that contain user private data are exchanged over secure links with a single, user-trusted entity. The SEMOPS IDs masquerade the specific transaction, which is not traceable with only that info known. Since the business model of SEMOPS tackles also the privacy, there is not an immediate need at the moment to address it further via add-on solutions such as anonymity/ pseudonymity services etc.

4 Security, Trust and Privacy in SEMOPS business model

This section focuses on the way all three requirements are tackled in the business model of SEMOPS.

4.1 Security Considerations

Although security concerns have been addressed mainly at the technology level, the SEMOPS business model ensures some attributes of security from different perspectives. As far as confidentiality is concerned users have absolute control of the usage of transaction related data. In fact the goods and the merchant that is being paid are known only to the merchant's bank and not the payer's bank. Therefore each player alone e.g. the user's bank cannot make any user profiles with the complete transaction info. Doing so however may be required by law in some countries, and indeed can be done with the cooperation of all three entities i.e. the user payment processor, the DataCenter and the merchant payment processor.

In addition, due to the credit push model of SEMOPS, the customer is the driver of the payment process. No payment will be initiated without the customer's explicit approval. Call theft preventing built in mechanisms in mobile devices ensure that the initiator of a SEMOPS transaction is clearly identifiable. In contrast to SEMOPS, in case of credit card based transactions, in most countries, if the user claims not to have authorized a transaction by a credit card, say, the transaction has to be cancelled and the bank cannot prove that the user is not cheating (accountability). Even when the secure access of the mobile phone has been compromised, unlawful transactions have to be deposited into a bank account, which can be traced.

4.2 Trust Considerations

SEMOPS is taking advantage of existing trust relationships among end users and their long-time partners such as banks and mobile network operators. The SEMOPS business model has taken advantage of these trust relationships by developing a decentralized subscription model, where only the bank registers for the mobile payment service which afterwards is provided to all users without explicit registration to a third party service provider. Existing social trust in legacy procedures, transferred into mobile world tackles a very often mentioned weakness of mobile commerce which has been repeatedly reported by surveys, namely that the user can not trust any virtual company that he can not in the real world physically access and complain/sue. In the SEMOPS business model we have a ring of trust. The user has to trust only his payment processor and that's it. The banks that join the service have to trust each other (this is done today among banks and a legal framework regulates it). Finally each payment processor is responsible for their users. Mechanisms like real-time refunding as well as integration of existing legacy procedures in banks such as internal rating systems are hidden from the end-user, something that promotes simplicity and trust in the SEMOPS procedure as a whole.

Apart from the fact that each actor in the business model interacts only his/her trusted partners there are other ways in which the SEMOPS business model promotes trust:

- The SEMOPS business model guarantees that the merchant will be paid in real time. The merchant may not know where the money is coming from but he receives a guarantee from his own trusted payment processor that he will be paid for a certain transaction.
- The money received or spent, through SEMOPS usage, always come out of a user's bank account, or mobile operator managed account so there is not any possibility of losing money if the mobile device is lost (no device-stored money tokens).

4.3 Privacy Considerations

In most users' minds, providing data to a bank or MNO is not the same as providing data to a third-party service provider. Similarly, Internet based fiascos have proven this fear to be a legitimate one, as bankrupt providers have sold their customer-info to others for profit, or accidentally via security holes, private user data were leaked. SEMOPS takes advantage of existing social trust and integrates it in its business model.

Using SEMOPS customers do not provide any sensitive private information to the merchant or to any third party service provider. Depending on the channel they use for the initial transfer of the transaction data they may provide however their phone number if an SMS communication is chosen, but again if IrDA or Bluetooth are chosen this transaction may remain anonymous. Customers may retain their anonymity against the merchant if they wish so, therefore they can make anonymous transactions which is not the case today for most payment services. This level of privacy is comparable to that offered by real cash based transactions. As mentioned before, the whole of transaction details can only be revealed to an entity that has gathered the data from the payment processors and the DataCenter for a legitimate reason such as money laundering or crime fighting.

5 Future Directions

The Mobile Payment (MP) area is generally still in its infancy. SEMOPS is an innovative solution that can lead us to something better, namely a global mobile payment service. For this to happen, some future challenges need to be successfully tackled. SEMOPS, like almost all existing approaches focuses on 2G or 2.75G infrastructures in order to achieve the critical mass once it is commercial. However, if SEMOPS becomes commercial, that would be in a 2-5 year timeframe, where other technology trends probably govern the market.

The infrastructure itself is rapidly evolving. The début of UMTS, wireless LAN, WiMAX and other 3G and beyond technologies will provide new capabilities that will free MP from some its current limitations and allow more sophisticated approaches to be developed. 3G and beyond infrastructures provide advanced capabilities as they introduce execution environments for 3rd-party service providers, and the rise of virtual MNOs (an operator without a physical network but with the ability to switch his own traffic and to issue his own USIM/SIM cards) will have an effect on existing processes and models. Future mobile payment services, will have to take into account the new security capabilities offered by such infrastructure for security, privacy and trust management.

The device manufacturers continue to bring on the market mobile phone models that have advanced capabilities (we are heading towards smartphone domination) and host their own execution environment. It is a matter of time for cryptographic services to be integrated in the devices that will make possible secure communication on voice and data. Furthermore the privacy is at high risk, since interception of data can be done from distance and without physical access. Mobile public key infrastructure (mPKI), mobile digital signatures, encryption, and biometric authentication are expected to be widely available in the near future. Therefore SEMOPS will examine these methods in order to provide strong security and privacy whenever it is required, and always in balance with the other requirements such as usability. Furthermore Identity Management efforts are ongoing for the Internet community and several standardization consortia such as Radicchio (www.radicchio.org) and Liberty Alliance (www.projectliberty.org) work towards federated identity in virtual world. If such efforts are successful, they will have a catalytic effect on MP domain, as they will provide a homogeneous identity framework capable of bridging universally the real and virtual world. Therefore efforts towards this direction, like the newly announced (March 2004) cooperation of NAC, OMA, OSE, PayCircle, SIMalliance and WLAN Smart Card consortium with the Liberty Alliance in order to demonstrate that federated identity is among others a key enabler in mobile payments is a hint towards the trends of time.

Furthermore, SEMOPS and other existing systems use for P2P payments transmission protocols like IrDA, Bluetooth. Apart from these, promising is also the future on Instant Messaging (IM) and Near Field Communications (NFC). The IM will not only allow bridging together the Internet and mobile services and payments, but also allows P2P payments where the two or more parties are not in the same physical space. Recently NTT DATA and SEMOPS pioneered this area and demonstrated at CEBIT 2004 (www.cebit.de), that such an approach is viable and promising. NFC is a very short-range wireless technology (distances measured in centimeters) that is optimized for intuitive, easy and secure communication between various devices without user configuration. Adopting this will mean that the device can authenticate on behalf of the user, which will eliminate the need for pin numbers and passwords, and boost user friendliness. Both IM and NFC approaches will have an impact on security, trust and privacy issues on SEMOPS and generally in any mobile payment service.

Taking into account the above, SEMOPS will continue in the future to monitor all existing standardization initiatives as well as the future technology trends. The next step for SEMOPS is to work towards these domains with a focus on 3G and beyond technologies as well as advanced future scenarios. Some of these targets include:

- Focus on emerging infrastructures with a minimum 2.5G/2.75G.
- Enhance security by taking into account what 3G infrastructures offer and what the latest mobile phone generation supports.
- Use the “Identity Management” efforts in Liberty Alliance and Radicchio consortia.
- Actively participate in existing MP standardization consortia and also fora that directly deal with security, trust and privacy issues in the mobile world, and that are relevant to mobile payments.
- Explore in depth new interaction channels like Instant Messaging and NFC.
- Work towards refining the SEMOPS interfaces to be more extensible, open and closer to the standardization efforts. Then these interfaces could be openly shared in order to get feedback and process further with the evolution of SEMOPS.

6 Conclusions

This paper presented the way security, trust and privacy issues are addressed within the SEMOPS project both from the technology point of view as well as in the business model. SEMOPS aims at realizing a secure and trusted mobile payment service that also protects the user's privacy and can fully handle totally anonymous payments – something that only by cash or anonymous tokens (prepaid cards) is possible today. It is clear that security has to be present both on the business model as well as in the technology used to implement the service from day one and can not be considered as a future add-on. Trust on the procedures and usage of already existing trust links (e.g. among banks and their users) have to be taken into account in order to support a successful service launch and operation. Privacy of the users needs to be protected and user-controlled. This is important especially in the electronic world where the user may not fully anticipate the possible privacy threats as in real life.

Finally, let us mention that while comparing SEMOPS with most of the existing MP procedures, we can clearly state that it has a more advanced approach that addresses better the security, trust and privacy issues in total, than most MP procedures do today. The SEMOPS consortium has just finished an initial prototype of its service, and is working towards validating itself in real-life scenarios and testbeds with the aim to enhance, evolve and provide a commercial service in the near future.

7 References

[1] Deliverable D04: Final Roadmap (Extended Version), Pioneering Advanced Mobile Privacy and Security (PAMPAS - www.pampas-eu.org).

[2] G. Giaglis, P. Ingerfeld, S. Karnouskos, P. Lee, A. Pitsillides, N. Robinson, M. Stylianou and L. Valeri, "mBusiness Applications and Services Research Challenges", White Paper, 24th November 2003, MB-net Project (IST-2001-39164).

[3] "Roadmap to a Safer Wireless World", Security Report, Accenture and CERIAS, Oct 2002. http://www.cerias.purdue.edu/news_and_events/events/securitytrends/

[4] S. Karnouskos, A. Vilmos, P.Hoepner, A. Ramfos, N. Venetakis, "Secure Mobile Payment - Architecture and Business Model of SEMOPS", EURESCOM summit 2003, Evolution of Broadband Service, Satisfying user and market needs, 29 Sept - 1 Oct, 2003, Heidelberg, Germany.

[5] A. Vilmos and S. Karnouskos, "SEMOPS: Design of a new Payment Service", International Workshop on Mobile Commerce Technologies & Applications (MCTA 2003), In proceedings of the 14th International Conference (DEXA 2003), IEEE Computer Society Press, pages 865-869, September 1-5, 2003, Prague, Czech Republic (ISBN 0-7695-1993-8).

[6] Stefan Heng, "E-Payments: modern complement to traditional payment systems", Economics: Digital Economy and structural change, Deutsche Bank Report, May 6, 2004, No 44, Deutsche Bank Research.