MOBILE FINANCIAL INFORMATION SERVICES, SECURITY, AND CERTIFICATION

Jan Muntermann, Heiko Roßnagel, Kai Rannenberg
Chair of Mobile Commerce and Multilateral Security
Johann Wolfgang Goethe-University Frankfurt
Graefstrasse 78

Tel. +49-69-798-25307
Fax +49-69-798-25306

D-60054 Frankfurt / Main, Germany
www.whatismobile.de

Abstract: *Non-institutional investors are normally unable to react quickly to market events, which can have significant impact on their portfolio value. Especially when a critical market event occurs much depends on processing the information efficiently and in time. Mobile information services may then improve the information supply for these investors. In this contribution we will determine which financial information services are suitable for mobile use and show what kind of improvements the use of this technology will provide. We take a look at the potential benefits of mobile financial information pull and push services and also determine the security requirements of such services comparing them with what current technology has to offer. It shows that none of the technologies used today is able to provide the support for all the stated security requirements and that at least three areas would profit from certification.*

Keywords: Mobile Commerce, E-Finance, Mobile Brokerage, Security Requirements

E. Nardelli et al. (eds.), *Certification and Security in Inter-Organizational E-Service*
© International Federation for Information Processing 2005

1. INTRODUCTION

The dynamic stock market developments of the last years showed that staying up to date with regard to financial information is of paramount importance. Otherwise investing in stock markets loses its attractiveness [FoRe03]. Therefore an automated supply of personalized and decision relevant information, independent from time and the location of the investor is needed. While demand-oriented web-based information services such as observation and alerting systems have improved the information supply for investors [LooCha02], these traditional client/server systems can not provide time and location independent services. Therefore these infrastructures are not appropriate for an automated delivery of time critical financial information. In particular for non-institutional investors, who are unable to track all relevant market events, mobile financial information services can help reducing reaction time and moving these investors on a level playing field with the institutional investors. Mobile information services allow real-time information delivery and can heavily cut reaction time to market events, e.g. bad market news published as company announcement. The growing availability of powerful mobile devices and new wireless data services (e.g. GPRS) is enhancing the availability and affordability of mobile financial information services. Since the transferred information is the basis for initiating and blocking high-volume monetary transactions (or at least for influencing them), a high level of security is needed, e.g. to prevent attackers from spying, suppressing, or manipulating information. The goal of this paper is to show which type of financial information services are suitable for mobile usage and how these services might be implemented. We then focus on how to secure these services adequately and on how they are secured currently. Section 2 provides an overview on financial information services and their usage in mobile environments. Section 3 discusses the security requirements of these services as well as the level of security provided by market-available technologies. Section 4 concludes our findings and gives an outlook on future work and the need for certification.

2. MOBILIZED FINANCIAL INFORMATION SERVICES

2.1 Financial Aspects

By allocating securities, investors diversify their portfolio and choose the most appropriate ratio of risky and less-risky assets [ElmKi03]. This allocation aims at an efficient ratio of potential returns versus risks taken. Therefore investors require powerful real-time information services. This need increases if the portfolios contain various risky and volatile assets.

Today so called "pull" and "push" *information services* are available, which require different information system infrastructures. Using pull services investors can request relevant market information to prepare decisions. Furthermore push services which are triggered by market events can deliver information in real-time. Based on the received information it might be advisable to reallocate portfolio positions quickly. This reallocation is done by selling and buying (new) assets and is supported by so-called *transaction services*. The availability of new, web-based I&C-systems in the area of information and transaction services has empowered non-institutional investors during the recent years. Even though, most of these systems cannot provide location independence for users needing information in optimal time.

Non-institutional investors are usually not able to analyze all portfolio relevant market information continuously, as they have more things to do than to watch monitors with stock quotes the whole day. They also are not professionally trained in quickly deciding which information is relevant to their investment decisions. Mobile information services enable location independence while personalized services help to filter the information flow.

2.2 Portfolio Observation

Portfolio observation services can be realized by monitoring market events and continuously analyzing the portfolio status based on criteria defined by the investor. The investor determines events to be monitored by e.g. defining static and dynamic price limits and also determines the preferred communication channel. For this configuration conventional web-based systems can be used, while the delivery of the notifications needs push services such as e-mail, Short Message Service or Multimedia Message Service.

However, portfolio observation comprises more than monitoring price limits. General market information that might be relevant for the portfolio development needs to be identified, selected, and delivered. Examples are personalized notifications in case of changing portfolio ratios (such as the stock quotes), financial metrics (e.g. changes in credit ratings), or market information (such as company announcements). All this might have major impact on the short-term development of shares, especially if published financial parameters do not comply with market expectations. This effect can be measured by comparing the price movement during the event period (e.g. the respective trading day) with the movement during another observation period (e.g. the trading days before) in which no critical market event occurred [MuMa04].

2.2.1 Added Value from Mobile Support

In general mobile portfolio observation enables faster reactions, especially through reduced delays for thę delivery of information and through the delivery of personalized market information. The monitoring is usually realized by processes on backend-systems (application and database servers) at the online broker or the bank. The investor is informed via push services if a monitored event occurs.

In particular, the mobile enhancement in terms of information delivery makes portfolio observation a mission-critical and helpful asset. Relevant information can be the above-mentioned company announcements, in which companies publish e.g. quarterly financial data or news from their management board. This information may well cause abnormal price changes, especially if new information differs from market expectations [Graha62]. On the other hand for periodically calculated portfolio figures, that are usually calculated once a day, mobile push services are not required because the information content of these figures is of longer lifetime. In this case conventional web services are appropriate.

2.2.2 Technical Realization of Mobile Information Services

A well-known GSM Phase 1 Service offering push functionality is the Short Message Service (SMS). This service has been a market success in the last years, representing remarkable revenue for the companies providing the system infrastructure. However, one weakness of the SMS is that it does not guarantee delivery time. Version 2.0 of the Wireless Application Protocol (WAP) [WF01] defines a push service framework, which specifies protocols to transfer messages and documents to mobile devices within classic client/server environments. Although this framework was released in July 2001 appropriate push services are not yet available. The availability of mobile devices supporting WAP 2.0 did not change much of this situation. The WAP Forum has been substituted by the Open Mobile Alliance (OMA) in 2002, which already has released an extension of the previous push framework [OMA02]. This extension is able to process incoming e-mails through the so-called e-mail notification (EMN). This technology requires new mobile devices with EMN support and an installed conventional e-mail client which enables the device to download e-mails from conventional mail servers.

2.3 Portfolio Analysis

Besides providing share prices and calculating portfolio metrics the portfolio analysis assists investors to improve their investment decisions. Furthermore, it supports investors to identify positive and negative correlations of asset returns and risk measured in price variances. Portfolio analysis provides different types of information, which have different maturity. Some information doesn't change very often (e.g. assets of a balance sheet); some can only be calculated periodically due to high calculation complexity [Daco01]. Usually pull services are used for portfolio analysis, i.e. when the shareholder requires information about portfolio positions, after the portfolio monitoring service informed about a relevant market event.

2.3.1 Added Value from Mobile Support

Web-based portfolio analysis services are available for several years and have enormously improved the information supply for investors. To support long-term (strategic) investment decisions, web-based information services are appropriate. However the focus of mobile financial information services is to support investors' in urgent (intraday) investment decisions. Already the introduction of these web-based systems has reduced the possible decision horizon enormously. The timelines of sensitive investment decisions depend on risk attributes and on the availability of portfolio analysis systems [BoMe00]. When short-term information is needed (due to highly volatile asset classes) conventional web-based systems can not guarantee an adequate service. A basic analysis is the supply of current price information and the performance of the portfolio positions. If a situation demands a short-term shifting of portfolio positions, a calculation of optimal buying and selling volumes might help achieving a portfolio composition with an efficient ratio of risk and expected return. As such calculations require historic quote series [Shar66], it is sensible to do calculations on the application servers. Moreover new market forecasts or quarterly business figures may require a spontaneous research about a certain company. In this case the investor has to get a quick review of the most important financial statistics.

2.3.2 Technical Realization of Mobile Portfolio Analysis

In the mobile setting a wide range of services and system infrastructures can be used to realize a reasonable portfolio management. When much information is required an implementation via pull services is advisable, and this leads to the usage of WAP. WAP has been developed for GSM data services with their low data rates. The aim was to develop a protocol family, which allows to access documents on the internet. These documents have comparatively simple designs to keep the data volumes low. Although WAP could not meet expectations in terms of market penetration, it is useful for mobile portfolio analysis, as the lack of multimedia support is negligible.

3. SECURITY REQUIREMENTS OF MOBILE FINANCIAL INFORMATION SERVICES

3.1 General Security Requirements and Mobile Financial Information Services

Four general criteria [Rann00] can help to structure the security requirements on the mobile usage of suitable financial information services:

1. ***Confidentiality***: Confidentiality is the protection from unauthorized disclosure of information to third parties. Those could be employees of the financial service provider, the mobile service provider or anyone else. Within the scope of mobile financial services this includes for example the protection of the user from exposing his financial situation or trading strategy to others.
2. ***Availability***: Availability is the protection from unauthorized withholding of information or services, i.e. information services. It can be very damaging for an investor to get time-critical information delayed or not at all. Since financial information services could have a direct influence on possibly following transactions, the lack of availability of a service can cause a damage for the investor, e.g. if he fails to sell his declining stocks.
3. ***Integrity***: Integrity protects the user from unauthorized manipulation of data or systems. It ensures the user that the data he receives hasn't been altered while being sent to him or while being on his device. False, modified or insufficient information might lead to wrong decisions and to financial losses. Since unauthorized manipulations can't be prevented in non-trusted environments, the integrity of the used data must be protected by all means necessary and breaches have to be detected and documented.
4. ***Accountability***: Accountability defines the fact that actions or documents can be associated with the originator, who could be a person or company, so that they cannot deny transactions they made at a later date. After complaints from customers about misleading information or unauthorized transactions resulting in financial losses, one wants to be able to trace back the originator of the information or who has altered the transaction?

3.2 A Short Security Analysis of Mobile Financial Information Services

3.2.1 Portfolio Observation

In the area of portfolio observation individual messages on new events will be delivered by means of push technology. The level of security depends initially on the relevance of the portfolio respectively on the delivered message but also on the relevance the delivered message may have for the portfolio. For example, a limit message must have a high level of confidentiality as any information delivered to the investor would allow direct assessments of the investments in his portfolio. The information gained could be used directly against the investor by e.g. estimating discrepancies in his financial position and making those public. It could also be used indirectly as basis for an attack on the integrity of selected information e.g. modifying the information or forging it.

Ad hoc disclosures need less confidentiality than limit messages as not all ad-hoc messages the investor receives relate to titles in his portfolio. However, it could still be possible to some extent to draw conclusions on the content and titles contained in the portfolio. When general information and trends do not allow conclusions about the portfolio content or the investment strategy this information does not need to be treated in confidentially.

Missing availability of services in the push scenarios may result in serious consequences e.g. considerable financial losses if limit messages are delayed intentionally or by accident.

Preserving integrity is the prime objective for portfolio observation services, since they depend on the correctness of information. Accountability and the knowledge of the source of information are important, if decisions have to be made in short time and no second or third sources can be used.

3.2.2 Portfolio Analysis

If closely related to a specific portfolio, portfolio analysis does disclose quite a lot about the content as well as the trading strategy of the owner. Hence the confidentiality level depends on the requirements of the owner. The requirements related to integrity and accountability of a portfolio analysis increase with the importance of the decisions as a result of that portfolio analysis. The requirements on the integrity do increase the lesser the possibilities are (e.g. due to time constraints) to call for further analysis for comparison purposes. The availability requirements of portfolio analysis services depend on the actual need of the investor making decisions and how time critical these are.

3.3 Suitability of Used and Available Technology in Regards to Security

3.3.1 Short Message Service (SMS)

The Short Message Service (SMS) is an attractive option for financial service information providers. Here the data of the service information provider will be transmitted to the SMS service centre (usually a mobile communication provider). From there, it will be forwarded by (cable) data links and eventually delivered to the mobile device over the air. During this process the data is transmitted as plain text except during the wireless transmittal. Consequently the security target of confidentiality is not achieved without introduction of security measures at the user level [FuFri01].

Also a manipulation of data during the transfer over the various communication paths cannot be prevented or traced back by the investor. Moreover an effective identification of the originator of the message is not possible as the mobile phone number indicated on the SMS message can be easily manipulated in the SMS-centre. Offers about how to send SMS under any sender number can be found on the internet [Eton03].

A possible solution to this problem is the use of a suitable 'signature process' [Ran03] which is able to protect the integrity and accountability on application level. To enable this the mobile device needs specific software for the verification of signatures. This however is a major challenge due to the many different types of mobile devices. Similar problems occur if full confidentiality is required, e.g. via encryption on the application level from the initial source to the final recipient. Full availability of SMS-messages does not exist. There is no guarantee that messages will be delivered at all or that they will be delivered in time, since SMS messages are being delivered based on the load of the network (store-and-forward service) [Schi03, GSM01].

3.3.2 WAP

WAP 1.x uses WTLS, a security protocol based on SSL, to improve the confidentiality and reliability of data during transmittal [Schi03]. The WTLS protocol supports primarily the security objectives of accountability, confidentiality and integrity. However, a problem exists if the WAP-server is not installed in the protected area of the financial information service provider and is connected directly to the infrastructure of the mobile communication provider. In that case end-to-end security will get lost at the place where the WAP-Gateway does decrypt the data. [FuFri01]. WAP 2.0 uses TLS to secure the communication and ensures real end-to-end security. However, only a few devices support TLS [cf. 2.2].

3.3.3 Web-based solutions

Especially the integration of PDAs and mobile phones offers new perspectives for mobile financial service providers. New mobile devices have web browsers able to encrypt the data transmitted by means of SSL. This enables a real "end-to-end" security during the transmission. The integrity and authenticity of the data can be achieved by means of digital signatures, provided suitable programs are available on the user platform (device) [Ran03]. With web-based solutions all security requirements can be fulfilled provided that the service providers as well as the mobile device do support the relevant protection technology.

4. CONCLUSION AND FUTURE WORK

The mobile financial information services introduced provide advantages for investors as well as for service providers: The timely and location independent delivery of time critical market information improves the level of information of investors, which may result in improved investment decisions. From the view of providers of mobile financial information services the upgraded service quality and service personalisation may improve customer relations. The security requirements for mobile financial information services are rising with the specialization and personalization of the required information and also with a reduction of the time between the receipt of information and need for decisions. Current applications do not or not yet comply with the security requirements. They still need to be enhanced by encryption and signature procedures as well as by redundancy concepts at the user level. In at least three areas certification would be useful:

1. Does the mobile device display the content correctly? This would be a certification towards the investor using the Common Criteria [ISO1999] and being paid by the device manufacturer or communication provider.
2. Does the SIM produce correct signatures? This would be a certification towards the investor and broker using the Common Criteria [ISO1999] being paid by the SIM manufacturer or communication provider.

3. Does the SIM represent a liable investor? This would be a certification towards the broker, using e.g. a signature certificate according to the EU directive. Payment for this would have to come from the investor or the communication provider – the latter to encourage mobile brokerage and the related traffic.

5. REFERENCES

[BoMe00] Bodie, Z.; Merton. R. C.: Finance, Upper Saddle River, New Jersey, 2000.

[Daco01] Dacorogna, M.; Gençay, R.; Müller, U.; Olsen, R.; Pictet, O.: An Introduction to High-Frequency Finance, San Diego, Califonia, 2001.

[Dorn01] Dornan, A.: The Essential Guide to Wireless Communications Applications – From Cellular Systems to WAP and M-Commerce, Upper Saddle River 2001.

[ElmKi03] Elmiger, G.; Kim, S.S.: RiskGrade Your Investments, Hoboken, New Jersey 2003.

[Eton03] e-tones.co.uk: „Anonymous SMS", www.e-tones.co.uk/index.php?cpid=31, [2003-06-14].

[EU_esig1999] European Union: DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.

[FoRe03] Forrester Research: Eurpean Online Finance's Quit Boom, Cambridge, 2003.

[FuFri01] Fuchß, T.; Fritsch, L.: Endgeräte für den M-Commerce: Defizite und Aussichten, in KES 1, Ingelheim 2001, 6-8.

[Graha62] Graham, B.; Dodd, D. L.; Cottle, S.: Security Analysis – Principles and Technique, 4th Ed., New York 1962.

[GSM01] GSM Association: Identification of Quality of Service aspects of popular Services (GSM and 3G), Version 3.0.0, www.gsmworld.com/documents/ireg/ir41.pdf, 2001, [2003-06-08].

[GSM03] GSM Association: MMS - What is MMS?, www.gsmworld.com/technology/mms/whatis_mms.shtml, 2003 [2003-05-28].

[ISO1999] Evaluation Criteria for IT Security, Parts 1-3; International Standard 15408; 1999

[LooCha02] Looney, C. A.; Chatterjee, D.: Web-Enabled Transformation of the Brokerage Industrie. In: Communications of the ACM, 45 (3), 2002.

[MuMa04] Muntermann, J.: Notifying Investors in Time - A Mobile Information System Approach, Proceedings of the 10th Americas Conference on Information Systems (AMCIS'2004); New York, August 2004

[OMA02] Open Mobile Alliance: E-Mail Notification Version 1.0. www.openmobilealliance.org/ omacopyrightNEW.asp?doc=OMA-EMN-v1_0-20021031-C.zip, 2002, [2003-07-10].

[Ran03] Ranke, J.; Fritsch, L.; Rossnagel, H.: M-Signaturen aus rechtlicher Sicht. Datenschutz und Datensicherheit 27 , Wiesbaden 2003, 95-100.

[Rann00] Rannenberg, K.: Multilateral Security – A concept and examples for balanced security. Proc. 9th ACM New Security Paradigms WS 2000, Cork, Ireland, 151-162.

[Schi03] Schiller, J.: Mobile Communications,2nd Edition, London 2003.

[Shar66] Sharpe, W. F.: Mutual Fund Performance. Journal of Business, 1966, 39 (1),119-138.

[StraAna03] Strategy Analytics: Global Cellular Data Forecasts (2003 - 2008), 2003.

[WapFo01] WAP Forum: WAP Push Architectural Overview, Version 03-Jul-2001. www1.wapforum.org/tech/documents/WAP-250-PushArchOverview-20010703-a.pdf, 2001, [2003-02-12].