

Mobile Government and Mobile Network Operators - Is Cooperation Possible?

Ulrich Dietz

Schlesierstrasse 18, 81669

Munich, Germany

E-mail: Ulrich.Dietz@gmxpro.de

Abstract: *The following paper outlines the technical infrastructure Mobile Network Operators are setting up for mCommerce, mEntertainment and mBusiness and summarizes possible synergies these infrastructures add to Mobile Government. Also in focus are business considerations, limiting factors and cooperative implementations of mGovernment as a public-private-partnership.*

Keywords: eGovernment, eGov, Mobile Government, mGov, Mobile Network Operator, MNO, UMTS, Security, Location-Based Services, Authentication, Public-Private-Partnership, Cooperation

1. Introduction

Governments around the world are putting huge efforts into making traditional governmental services available on the Internet. These efforts are subsumed under the phrase eGovernment (eGov). Examples are Germany's BundOnline2005 initiative (<http://www.bundonline2005.de>) or the corresponding British initiative under the umbrella of the e-Government Unit (<http://www.cabinetoffice.gov.uk/e-government>). According to (Rihaczek, 2005) authorities started the first eGovernment wave as early as 1970 with the notion that 'data should travel, not citizens' by providing single points of contact.

These governmental efforts go along with changes in the internal processes, since the reengineered processes and the huge investments in new IT infrastructure will also have the effect of transforming and modernizing the very heart of governmental affairs. One example here might be the tax authorities remote access to tax relevant internal documentation stored digitally signed in a database under control of an enterprise. This will limit extended onsite tax audits, speeds up the audits, therefore allowing more audits with the same manpower, and is seen as a way to improve fiscal fairness and neutrality of treatment.

Traditionally these efforts are intended to result in eGov services that are to be consumed on powerful desktop PCs / laptops equipped with large displays, mice and keyboards and the necessary set of software (browser, Java environment, PDF reader, ...). With the number of mobile subscribers outnumbering the number of Internet users substantially (according to the GSM Association the number of GSM subscribers reached 1.2bn globally by the end of 2004 (<http://www.gsmworld.com>) whereas the number of Internet users is given with 820 million as of February 2005 (INTERNET USAGE STATISTICS, 2005)) and along with the improved capabilities and the different usage patterns (mobile vs. fixed, personal vs. all purpose devices,...), there is clearly an incentive for authorities to also deploy adapted eGov services so that they are available as mGovernment (mGov) services.

The difficulties experienced by the Mobile Network Operators (MNOs), the mobile content providers, and other mCommerce companies over the last five or so years in implementing mCommerce, mEntertainment and mBusiness services indicate that it isn't enough to simply mobilize existing services. Instead, successful service mobilization has to take into account the situation users are in when using mobile devices and the expectations users have of these mobile services. It is also necessary to educate the users to take up usage of

such services by promoting and advertising these new possibilities. Also, quite important and sometimes underestimated or even neglected, are the technological challenges that have to be overcome. This is also true for mGov services - they aren't simply mobilized eGov services, even if some can be handled this way. In the end there are more transport and presentation means available than the mostly referred SMS.

Governments and MNOs, on one hand, share the same interests – to spread the use and acceptance of new mobile services. On the other hand, they differ in some general points. Firstly, MNOs will concentrate on a subset of the available mobile channels and secondly, they generally subsidize mobile devices and so have influence on standards and formats. Governments, in contrast, pursue an 'all channel' and 'all citizen' approach and rely on the devices that users already have in their possession.

Even as mGov does not look as an ideal MNO mobile service to support (due to the fact that these services are used less often on average compared to mobile data services and mobile portals), it might be an interesting ad-on that fosters the adoption of mobile services and turns the handset into a trusted device. This common interest might be the centerpiece of a cooperative implementation approach with the cornerstones outlined in the next chapters. Therefore, this paper evaluates the requirements for a successful mGov deployment over mobile networks and gives advice to both governments and MNOs on how to be most useful for citizens and customers in the field of mGov.

Section 2 gives an overview on the mGov situation from both the government's and the MNO's point of view. Section 3 outlines the possible fields of cooperation and section 4 delineates the economical aspects. Limiting factors are addressed in section 5 and the conclusions are drawn in section 6.

2. Situation in Mobile Government

mGovernment is often described as part of eGovernment that itself is part of a larger effort called Government. This seems true and straight forward because all that can be done mobile can also be done electronically and finally can be done the old fashioned way over-the-counter whereas not all of what can be done the old fashioned way can be done electronically and nor be done mobile. This takes both regulatory restrictions (for instance, an applicant has to be present personally when enrolling for a digital ID or if a notary is involved in the procedure) and technical restrictions (due to a limited screen size, inefficient processing power or other constraints) into account.

mGovernment is, according to (Lallana, 2004), defined as a subset of eGovernment that itself is the use of Information and Communication Technologies (ICT) to improve the activities of public sector organizations. Lallana further references that in case of mGovernment, those ICTs are limited to mobile and/or wireless technologies like cellular/mobile phones, laptops and PDAs (Personal Digital Assistants) connected to wireless local area networks (WLANs) and that mGovernment can help make public information and government services available "anytime, anywhere" to citizens and officials.

From this perspective, neither eGov nor mGov changes the way government works, only the way, citizens are able to use these service changes. In this sense, eGov adds flexibility to traditional government by making them remotely accessible anytime. mGov itself adds full location independence to that and opens government to be used anywhere.

2.1 The Governments Situation

Governments around the world are working to e-enable their services. Germany started at the EXPO 2000 in Hannover with its BundOnline2005 initiative. The aim was to have all possible federal services e-enabled by 2005. It is expected that all of the 376 services identified in 2000 will be e-enabled at the end of 2005.

All the services will be made available via the Bund Online portal (<http://www.bund.de>) that will act as the general focal point for eGovernment services. More interesting is the fact that the over 100 ministries, federal authorities and governmental service providers involved, developed a set of architectures, protocols and standards for the use in eGovernment. Two of the main components are SAGA (Standards and Architectures for eGovernment Applications) (<http://www.kbst.bund.de/saga>), a collection of assessments and recommendations on IT standards, protocols and formats and OSCI (Online Services Computer Interface) (<http://www.osci.de>), a set of profiled message formats, protocols and mechanisms to securely and confidently exchange standardized eGov messages over insecure channels. It should be stressed that a set of standards and supporting documentation has also been produced and that down the line from the federal authorities via state authorities down to the district authorities, all authorities are working together to reduce extra work and assure interoperability.

Great Britain's government developed its e-Government Interoperability Framework (e-GIF) under the lead of the e-Government Unit that holds responsibly, amongst others, for IT strategy and policy, development of common IT components and delivering citizen-centered online services (e-Government Unit, 2005).

Nearly all European countries are working on their own eGovernment projects and infrastructure with a clear national focus. This is widely seen as a first step and the European Union has set up with eEurope 2005 (<http://www.eeurope2005.org>) an umbrella initiative with the core objective 'to connect everyone and everything online - governments, schools, hospitals and businesses so that Europe becomes a better and more efficient place to live and do business'. It is clear that eEurope 2005 is more a political initiative and acts in the first place as a platform to exchange ideas and technologies. But with IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens), it runs its own program to harmonize and integrate national initiatives and drives standardization gained on a national level. Since even the national initiatives encounter difficulties, the European harmonization is a more challenging task and will deliver its results later than the national initiatives.

mGov is mentioned, in one way or the other, in some the existing projects, standards and initiatives - but only as a possibility. Nothing is said about its setup nor is it defined in any way. Even if the standards, initiatives, and projects are bearer and technology agnostic, there is hardly any reference to mGov, mobile devices and the role MNOs can play in such a setup.

Government can be grouped into a few categories. The most common category is called Government-to-Citizen (G2C) and comprises of all processes citizen will have contact to authorities. The next category is called Government-to-Business (G2B) and subsumes all processes in which authorities are in contact with businesses of any size. The last category, called Government-to-Government (G2G), is the category in which authorities are connected to each other. This can be done even on the various levels e.g. municipal or local authorities that are in contact to and doing government with federal state authorities.

The services can be grouped along the rising complexity into three different categories: Information, communication and transaction. The information services are the easiest to realize and make templates and general information available on a portal. Communication services allow interaction with the authorities, but without the ability to finalize processes for instance with an electronic signature. This is only possible in services called transactional that close an informational or communicational session with an accepted online surrogate for a handwritten signature.

The list of e-enabled German services (Fortschrittsanzeiger, 2005) is dominated by information retrieval services, as these services are the easiest to implement. It is expected that more than 70% of the German e-enabled services fall in the information retrieval services category. On the other hand only a few

transactional services have been realized so far because of the need of electronic signatures, which are costly if only used a few time a year. The influence the various upcoming eID and ePassport initiatives will have, haven't been assessed in this paper.

2.2 The Mobile Network Operators Situation

A considerable number of Mobile Network Operators (MNOs) run GSM/GPRS and UMTS networks used to deliver voice and data services. They spent approximately €200 billion in UMTS licenses in Europe (and of that, approximately €100 billion alone in Germany) and will have to invest nearly half the amount of money in infrastructure and service development to make mobile data services (mEntertainment, mCommerce and mBusiness) happen. MNOs started their data service offerings effectively with GPRS (General Packet Radio Service) and have since put considerable effort in setting up an environment to offer high bandwidth data services, able to deliver their services economically and efficiently to their customers. Mobile networks reach – depending on MNO and serviced area – a coverage up to 95% in geographical terms and up to 99% of the population and offer packet switched connections with a download speed up to 56 kbits (GPRS) and 384 kbits (UMTS). Together with the basic packet switched connections, a set of MNO value added services have been set up. These functionalities are possibly suitable for mGov, if exposed as services or via APIs. The suitability for mGov in business terms will be discussed in detail as a non-exhaustive list.

Network security

GSM/GPRS and UMTS networks come with a considerable level of security. GSM was standardized to deliver a Public Switched Telephone Network (PSTN) equivalent level of security (Boman, et al., 2002) and is regarded as robust not only because changes to the security algorithms have been made recently by replacing the security algorithm A5/2, (for what a successful attack is available), with the reasonably secure A5/1. GPRS does use different algorithms (GEA1, GEA2 and GEA3), no attacks are known for yet.

UMTS was designed with an evolved security model in mind. First of all, the authentication is done mutually (handset and network authenticate themselves to each other preventing the so called 'man-in-the-middle attacks') and the encrypted connection is delivered, compared to GSM, deeper into the network. Furthermore, the security algorithms (f1 to f5 and f8, f9) chosen by ETSI's (European Telecommunication Standards Institute) SAGE (Security Algorithms Group of Experts), are based on publicly available algorithms and have been, in contrast to the GSM mechanisms, openly discussed and reviewed. They are expected to be robust enough to withstand highly sophisticated attacks. Unfortunately, the level of security in every system is, due to advances in academia and other influences, constantly under pressure. The mobile industry is keeping up confidence in GSM/GPRS by updating algorithms that are under pressure and by adopting new design methods for UMTS security algorithms.

UMTS was designed as an evolutionary process with constant new releases. The latest release is Release 6, which will be fully standardized in 2005. Work on Release 7 has already been taken up.

USIM security

As briefly outlined above, the UMTS security is based on special algorithms that are distributed within the system. The centerpiece of a MNOs security concept is a tamper-proof, removable processor card called the USIM (Universal Subscriber Identity Module) that mutually authenticates customers to the network and reverse. The cards used for GSM/GPRS are called SIMs. The USIM holds all necessary keys and personal information and can be swapped, as a handset independent device, from one handset to another. The USIM can also be a secure storage for general information – for instance, the Java standard JSR 177 'Security and Trust Services API for J2ME' makes the USIM accessible from a Java J2ME enabled handset and turns the USIM into a storage device for sensitive information.

Additionally, the USIM can be equipped with USAT (USIM Application Toolkit), an application environment able to execute USIM based services and to display additional menus providing an easy to use interface to these services. These services can be uploaded via OTA (Over The Air) form an OTA server in the network. It is possible to make USAT-services available to selected customers only or to all customers dependent on contracts and requirements.

Identity Management Services

With the USIM MNOs do have a highly secure identity token out in the customers' hands / handsets and are willing to extend that to authenticate their customers to third party services. Therefore, a group of MNOs joined the Liberty Alliance, which standardizes identity management functionalities bridging mobile and Internet and so turning the mobile devices into a trusted, mobile passport-like devices.

IP Multimedia Subsystem

The IP Multimedia Subsystem (IMS) is an integral part of a UMTS network and represents a control channel on top of the plain packet switched connectivity to initiate, terminate and modify multimedia sessions (Boman, et al., 2002). IMS is 3GPP's (3rd Generation Partnership Project) adoption of IETF's (Internet Engineering Task Force) Session Initialization Protocol (SIP), that serves as the foundation for Internet telephony (VoIP, Voice over IP). IMS is, despite it often called so, not a service, nor is IMS intended to transport services. IMS simply enables the efficient setup and release of (voice or packet switched) connections. Access to IMS is granted with help of the ISIM, short and (unfortunately) misleading for 'IP Multimedia Services Identity Module'. The ISIM is a SIM-like application residing on the USIM and authenticates the IMS enabled handset towards the IMS enabled network.

Location-Based Services

Location-Based Services (LBS) connect the situation users are in with the location they are at and allow the delivery of tailored information such as routing and guidance to points of interest. MNOs have developed a set of network based LBS mechanisms that haven't found their way into commercialization yet. With the European Commission's E112 legislation, MNOs will be required to deliver the exact position of a customer calling an emergency number. ERTICO, a Brussels based public/private partnership for the implementation of Intelligent Transport Systems and Services (ITS) (<http://www.ertico.com>), recently completed the Emily project (<http://www.emilypgm.com>), defining a hybrid LBS system using both GPS and mobile network generated location information to enhance the reliability and accuracy both in urban and rural areas leading to a accuracy of circa 25m. Such a system might be of interest since it fulfils all necessary requirements. Only the 'costs per location event' and the related business case haven't been finalized on the MNOs' side.

Presence

Presence is a community-building tool that relays levels of activity and availability (e.g. 'on a call', 'in a meeting – do not interrupt' or even '...desperately awaiting a call...') to show up in a buddy list.

Java

Java is seen as the ideal handset application platform on which to roll out services and applications. Nearly every handset sold today is J2ME compliant and supports downloadable Java applications called Midlets. A reason for this trend is the level of security and interoperability that comes with Java. These Midlets can be audited and signed by a trusted third party. Unsigned and presumably insecure Midlets can be prevented from being executed. This increases the overall security because only approved applications can be executed. Another reason is that MNOs, as well as the application and content providers, do have influence on the development of Java via Sun's Java Community Process (JCP). This process encourages submission and development of new functionalities so that Java appears as being standardized is an open process.

Push-to-Talk over Cellular

Push-to-Talk over Cellular (PoC) is a Citizen Band like one-way functionality that lets customers set up groups that can all be reached simultaneously by pressing the talk-button on the handset. The voice is transported as data (GPRS or UMTS). Everybody in the group is able to address any one in the group by pushing the button. The service will give users worldwide accessibility once roaming and interoperability challenges have been tackled.

Instant Messaging

Instant Messaging (IM) is a technology to exchange (short) messages instantly in a chat-like communication. This can be done peer to peer or in a larger community. Voice chat can be done via PoC.

Handsets that support the above outlined features and services are already in the customer's hands. With a generation of handsets exchanged on average every 18 months, the mobile industry is able to push the newest handsets into the market at a high speed to enable the adoption of mGov services.

2.3 Mobile Industry Standardization Fora

The mobile industry has set up or is engaged in many different fora to standardize technological features, interoperability or even business models. This paragraph lists the most influential fora:

3GPP

The Third Generation Partnership Program (3GPP) (<http://www.3gpp.org>) is the European forum to standardize the technical foundation of 3G/UMTS. 3GPP standardizes air interface, security features (authentication, encryption, USIM, etc) and core network. The only services standardized by 3GPP are voice and SMS/MMS, all other services are standardized within the OMA.

Open Mobile Alliance

The Open Mobile Alliance (OMA) (<http://www.openmobilealliance.org>) brings together mobile operators, device and network suppliers, IT industry and content providers (in total over 360 partners) to standardize service enablers on the application layer and technologies able to span the mobile and IT world. For instance, OMA standardizes Digital Rights Management (DRM) mechanisms, PoC, billing and mCommerce aspects, presence, location services, messaging and many more. The WAP Forum, as well as the Location Interoperability Forum, were integrated into OMA just a few years ago.

Open Mobile Terminal Platform

The Open Mobile Terminal Platform (OMTP) (<http://www.omtp.org>), established in June 2004 by eight major MNOs, standardizes a common platform for mobile devices that allows differentiation on the application layer (for instance, the different portal offerings and all what is standardized by OMA) based on a common platform comprising of radio interface, base-band and application processors, memory management and so on.

Liberty Alliance

The Liberty Alliance (<http://www.projectliberty.org>) is a cross industry standardization body (150+ members) standardizing federated identity services for the authentication in online scenarios. The Liberty Alliance framework will enable MNOs to act as Identity Providers (IdPs). That offers their customers an easy to use Single Sign On and Identity management service to authenticate themselves securely to various mobile and online sites. A second field of activity is the area of Mobile Web Services and the necessary service discovery mechanisms.

Mobile Payment Forum

The Mobile Payment Forum (<http://www.mobilepaymentforum.org>) is a cross industry standardization body working on an interoperable mCommerce payment framework. It should be stressed, that after some years of competition between different standardization fora and industries in the field of mobile payments, the players came finally together to conclude the work within a single and widely accepted standard.

Simpay

Simpay (<http://www.simpay.com>) is a MNO driven initiative (six members) to turn the mPayment standards, as developed by the Mobile Payment Forum, to an interoperable and MNO grade mobile payment system. The effort is not limited to technical developments; Simpay will also be established as a strong and recognizable brand. First Simpay mobile payment services will be available in Q4/2005.

3. Possible Fields of Cooperation

As outlined above, authorities and MNOs have put a lot of effort into their respective fields and technologies. Authorities are working hard to get eGov up and running and MNOs are investing heavily to make their platforms and networks ready for mEntertainment, mCommerce and mBusiness. The MNOs are able to reach a huge proportion of the European and even the western population with these services. This will be achieved with handsets, which are well equipped with all necessary technologies to consume these services in a pleasurable way and the necessary and supportive core network (network, application servers and third party interfaces). Governments do have the same goal with traditional government, eGov or even mGov, that is, they have to reach and be helpful for all citizens, regardless of the MNO the citizens do have a contract with or the handset type the citizens have in use.

3.1 Cooperative Approach for the Setup of mGovernment Services

It is absolutely possible that authorities will roll out mGov services without any MNO support. It might be possible that the authorities, in the long run, will successfully implement a mGov framework. But this way forward bears also its challenges. A much better way forward is to build upon an already rolled out and proven infrastructure and so setting up mGov services reusing technological capabilities and services MNOs have already in place. These services and capabilities have been discussed in section 2.2.

Such a cooperative approach would ease and shorten the development and deployment for mGov services and would make the services available immediately on for nearly all of a MNOs customers. This could also circumvent the chicken-and-egg problem that normally delays the build up of a critical mass of users, would give customers an incentive to take up mobile services and would give MNOs a reason to strengthen their service platforms and value added MNO services.

There are already a few examples for such promising public-private-partnerships. Especially in the field of security services, cooperation and coordination does make sense. But to achieve the right balance is quite a challenge. The situation of the US initiative to implement E911, a location enhanced emergency call, is a good example. Compared with the European approach, the US legislation set in place was too strict and the deadline was too tight. That resulted in delays, drove the implementation costs over budget and resulted in MNOs setting up infrastructure they couldn't reuse for commercial offerings (DeZoysa, 2002). The EU issued a similar legislation within the eSafety activities (eSafety, 2005), called E112 (EU Commission Recommendation 2003/558/EC, 2003), to be implemented in 2003, but reduced the requirements subsequently to reflect the lessons learned and to meet the MNOs needs. It is expected that the E112 service will be operational soon.

Beside the mentioned security services, Location-Based Services and signed Java applications might also be of high interest for mGov. Location-Based Services may provide the location information used in electronic

processes or to access to information only when in a given area. Java could be an ideal way to spread handset resident and often used mGov applications that require more than a simple browser.

3.2 Incentives for Governments

Authorities willing to make mGov available will presumably profit from cooperating with MNOs in various ways. Most notable is, that authorities will get an immediate access to a large and already educated consumer base. They will also get access to the value added MNO services, which will add necessary functionality from the beginning on to mGov service offerings. This reuse of infrastructure and value added MNO services could, in the long run, reduce the development and operational costs significantly. This holds true for all mGov service types, G2C, G2B, and G2G.

3.3 Incentives for MNOs

The first incentive for a MNO is clearly airtime or volume. MNOs generally bill their customers on the basis of time or the data volume exchanged. Therefore it is beneficial for them to support any service that turns the handset into a personalized and often used device.

MNOs should regard and handle mGov services as (privileged) third party services. The mGov services can be seen as similar to banking services that require nearly the same level of security. In some way this restricts MNOs, but keeps the responsibility clear.

MNOs are in the process of establishing additional and more flexible billing mechanisms for instance based on IMS. Service billing is one of the new mechanisms and enables MNOs to bill services regardless the time used or amount of data exchanged. This can also be the billing rationale for the exposed value added MNO services like payment, ID management services, authentication and authorization, location, presence. In addition, MNOs offer content-related services like packaging, content aggregation or application signature. Even the access to some functionality of the security device SIM card or the short-listing of mGov service on their mobile portal could be made possible as a paid service.

Soft factors are, beside the fiscal issues, also of importance. Marketing and sponsoring opportunities, social responsibility and social and cultural awareness play a huge role for every large business. Given mGov isn't too attractive on its own, this can lead to active support by a MNO that in return will exploit the involvement for marketing and public relation campaigns.

4. Economical Aspects

Economical and business aspects play an important role for both, governments and MNOs - but with a different outline. Whereas authorities will have to spend the taxpayer's money efficiently to get as much as possible in return, MNOs have to be profitable and are willing to invest large sums into new business fields they hope to be profitable in return. That means that authorities and MNOs pursue conflicting goals. Authorities set their services up in a long lasting and stable fashion whereas MNOs are making trends and markets actively by investing in (sometimes short-lived) technology and marketing and so follow trends. mGov services fall effectively not in the category of short-lived services and should be offered in a stable and long lasting fashion. It is assumed that citizens will demand them stable - compared to mEntertainment, mCommerce or mBusiness services, that allow more changes reflecting actual trends.

Governments have to set up services in a economical way as they don't pursue economical profit. Their main interest is to develop and deploy mGov services that are available to everybody and this as cheap as possible. Within the next years, authorities will have to offer mGov services - the one or other way.

5. Limiting Factors

The economical basis of mGov services seems fragile. Cooperation on mGov services cannot ignore one essential fact - that the services will be offered under full governmental control and responsibility. It is not expected that authorities will share responsibilities here with the MNOs. This is especially true for communicational and transactional services that normally require sensitive personal data to be submitted.

Without being the originator of such services, MNOs can only be supportive in the areas of development and deployment, can offer hosting and outsourcing services, can offer their value added services as building blocks and can take the mGov requirements to evolve the networks, services and standards. This might be of limited appeal to the MNOs, because MNOs tend to concentrate on more profitable services and offerings.

Another limiting factor might be, that MNOs fear to be drawn into regulation afterwards, if they start cooperating with the authorities without a clear share of responsibilities and legislations. Also a limiting factor might be the tendency of the MNOs to reduce the subsidies for handsets. The effect will probably be, that the current exchange rate of 18 month slows down and delays mGov service adoption.

6. Conclusions

As outlined in this paper, mGov will take government procedures to the next level. The technologies and mechanisms have been described in detail. With the concept of cooperation, or a more formal public-private-partnership, a sensible way forward has been sketched for government authorities and MNOs, allowing them to perform and profit as much as possible in a highly interesting field.

Authorities will have to rely on proven, up to date and already deployed technology to reach a fast service adoption from the very first minute on. MNOs do have just that technology in place or are about to deploy that. This is exactly where cooperation might help to make mGov become reality.

Unfortunately, under the given circumstances, mGov does not seem to be a too lucrative field for MNOs to be active on their own, however the supplementary effects like increased traffic or possible value added service offerings shouldn't be ignored as a potential business. It should be in focus for further research to find ways to resolve that visible chicken-and-egg problem.

Business considerations should be assessed further on the basis of a more complete understanding of the drivers on both the governments and the MNOs side. As this is a first step into the assessment of a possible cooperation in the field of mobile government services, some areas have been left out for further research. MNOs are currently planning to set up WLAN (WirelessLAN) and WiMAX (Worldwide Interoperability for Microwave Access) networks in hotspots. 3GPP is in the process of standardizing WLAN and WiMAX as additional 3G bearers. The influence this will have on mGov has to be assessed independently. And secondly, several projects are ran throughout Europe to develop electronic Identity cards (eID) mostly to be embedded into updated national passports and ID cards. They will presumably be equipped with electronic signatures. If, and if so, how these cards can be used in mGov scenarios should be assessed when the directions are clear and the standards are out.

References

Boman, et al., 2002, UMTS security, Retrieved April 17th, 2005, from http://www.c7.com/ss7/whitepapers/cellular/umts_security.pdf.

DeZoysa, Sanjima, 2002, Regulatory clouds gather over LBS: The European commission and operators are

- on a collision course over Location Based Services, Retrieved April 17th, 2005, from http://www.findarticles.com/p/articles/mi_m0IUL/is_2_36/ai_83261161/print.
- e-Government Unit, 2005, Retrieved April 17th, 2005, from <http://www.cabinetoffice.gov.uk/e-government>.
- eSafety, Retrieved April 17th, 2005, from http://europa.eu.int/information_society/activities/esafety/text_en.htm.
- EU Commission Recommendation 2003/558/EC, 2003, Retrieved April 17th, 2005, from http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_189/l_18920030729en00490051.pdf.
- Fortschrittsanzeiger der Initiative BundOnline, 2005, Retrieved April 17th, 2005, from http://www.bund.de/nn_804/Content/BundOnline-2005/Fortschrittsanzeiger/Dienstleistungen-im-Ueberblick/Dienstleistungen-im-Ueberblick-knoten.html_nnn=true.
- INTERNET USAGE STATISTICS - THE BIG PICTURE, 2005, Retrieved April 17th, 2005, from <http://internetworldstats.com/stats.htm>.
- Lallana, Emmanuel C., 2004, eGovernment for Development mGovernment Definitions and Models Page, Retrieved April 17th, 2005, from <http://www.egov4dev.org/mgovdefn.htm>.
- Rihaczek, Karl, 2005, eGovernment -déjà-vu, *Datenschutz und Datensicherheit*, February 2005, page 57.