Mobile Security for Internet Applications*

Roger Kehr[1] · Joachim Posegga[2]
Roland Schmitz[1] · Peter Windirsch[1]

[1]T-Nova GmbH, Deutsche Telekom AG
{Roger.Kehr, Roland.Schmitz, Peter.Windirsch}@Telekom.de

[2]SAP AG, Corporate Research, Joachim.Posegga@SAP.com

Abstract

The WebSIM is a technology for interfacing GSM SIMs with the Internet, by implementing a Web server inside a SIM. This paper discusses how this technology can be used for securing services over the Internet and describes several concrete application scenarios.

1 Introduction

The notion of convergence of IT and telecommunications has been around for some 10 years, but very little had happened on the technical side in the last decade. Eventually, there is now a clearly observable trend towards the merging of the Internet and mobile networks like GSM or UMTS: in particular the Japanese i-mode system [2] and subsequently the Wireless Application Protocol (WAP) [4] are major milestones towards making Internet services accessible from mobile telephone networks.

The goals underlying these developments are focused around delivering Internet services over wireless networks to mobile devices. The notion of mobile commerce arose from this as a primary application: analogously to "standard" e-commerce over the "classical" Internet, wireless devices are used for electronic transactions in mobile commerce. Overall, the underlying philosophy is to provide services of the Internet to mobile customers. Notably, this follows a one-way road: rather than merging the two worlds of the Internet and mobile networks, the Internet is "simply" expanded to mobile devices.

This paper describes an approach that investigates the opposite direction: we demonstrate how to deliver services of GSM (and its successor, UMTS)[1] networks towards the Internet:

*The research described in this paper was partly funded by EURESCOM GmbH, Project P1005. All opinions expressed in this paper are solely those of the authors and do not necessarily reflect the views of their respective employers or EURESCOM GmbH.

[1] In the sequel of this paper we will not explicitly refer to UMTS; however, our approach can easily be

GSM networks have one advantage that is still missing in the Internet: there is a usable and well-established security infrastructure. Each GSM subscriber holds a so-called SIM [7], which is a smart card (security module) used for authenticating a subscriber against the network. These SIMs hold ciphering keys and they can perform cryptographic computations; today mostly symmetric cryptography is used, but public key solutions are now becoming available as well.

Today there are roughly 350 Mio. of these GSM SIMs used in mobile phones. Being able to integrate this security infrastructure into Internet applications is a major step towards practically securing the transactions carried out over Internet and can be summarised as "Mobile Security for Internet Applications". We demonstrated with the WebSIM [5] one way to achieve this: by implementing a stripped-down Web server in a GSM SIM and connecting it to the Internet, an HTTP interface to services on a SIM is provided to the Internet. These services can be smart card based authentication, secure interaction with the card holder, etc.

Put in another way the idea underlying the WebSIM is: *350 Mio GSM subscribers carry powerful smart cards around in wireless card readers (i.e., mobile phones); why not use these cards to secure Internet transactions?*

The rest of this paper is organised as follows: Section 2 briefly reviews the technical approach of the WebSIM and forms the basis to understand the applications that are discussed in the paper: Section 3 discusses the application of the WebSIM for authentication in the Internet. In Section 4 we demonstrate an approach that allows to involve the GSM SIM application toolkit into Internet applications, providing a secure communication channel to a card holder; a set of services centred around location information is sketched in Section 5, followed by a brief discussion of end-to-end security issues in Section 6. Finally, we draw conclusions from our research and provide an outlook to future work in Section 8.

2 A Brief Review of the WebSIM

The WebSIM (see [5] for a detailed description) is, put simply, a GSM SIM that contains a stripped down Web server that is accessible from the Internet. HTTP is used as an "application launching protocol" for accessing services provided by the SIM from the Internet. In a similar way, CGI scripting technology is used in the Web for running programs on Web servers.

The WebSIM is based upon the following technological building blocks:

- A GSM phone works as a wireless smart card reader that holds a smart card (SIM).
- SIM toolkit technology [6, 10, 11] allows to run applications (applets) inside the SIM, which can communicate peer-to-peer over various GSM protocols like SMS.
- A SIM toolkit applet running inside a SIM can, in principle, implement any protocol we wish to use for talking to the SIM.

forwarded from GSM to UMTS since the relevant technological underpinnings remain, essentially, the same.

Thus, we can implement a SIM toolkit applet that works as a Web server, which means: the applet interprets a subset of the HTTP protocol and provides services that can be accessed over HTTP.

What remains is to connect the SIM to the Internet; there are several possibilities here, one is to modify a GPRS phone which has an IP address to tunnel HTTP requests sent to it over ISO 7816 to the SIM. We choose a more “conventional” solution that has the advantage of being compatible with the majority of mobile phones on the market.

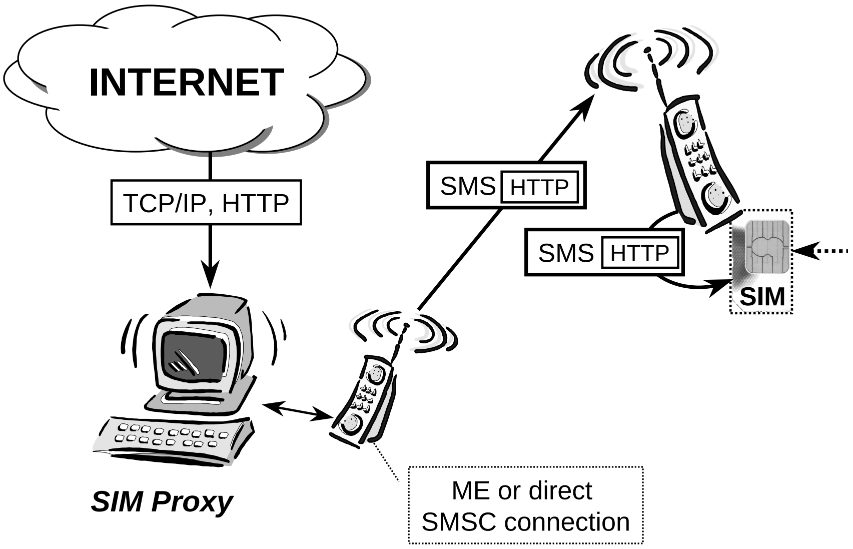


Figure 1: WebSIM Network Architecture

Figure 1 illustrates the principle: a proxy host for the SIM is hooked up to the Internet, which can send and receive SMS. HTTP requests arriving at the proxy for the SIM are tunnelled over SMS to the SIM: GSM 03.40 allows to send short messages directly to an application in the SIM (using SMS PP data download, see [8]), in our case the applications implementing the Web server. Thus, the function of the proxy is, essentially, to bridge the gap between the Internet and GSM.

The Web server application in the SIM will then parse the HTTP request that was received, perform the requested actions, like running a cryptographic algorithm and / or communicating with the user over the GSM 11.14 protocol. The result of the request is returned as an HTTP response over SMS to the proxy, which in turn sends it back to the originating address in the Internet.

HTTP is a comparably simple protocol, but since the interface to services of a smart card is also comparably simple, it is a well-suited candidate: it is easy to use, easily integrated in Internet applications, and widely known. Note, that a Web server in a SIM is not expected to host large amounts of information or HTML documents, but to provide a convenient interface to services of the SIM: These services can then be accessed via the standard protocol of the Web, HTTP. We use a stripped-down version of the HTTP protocols, which just covers the absolutely necessary part and only allow for one connection at a time.

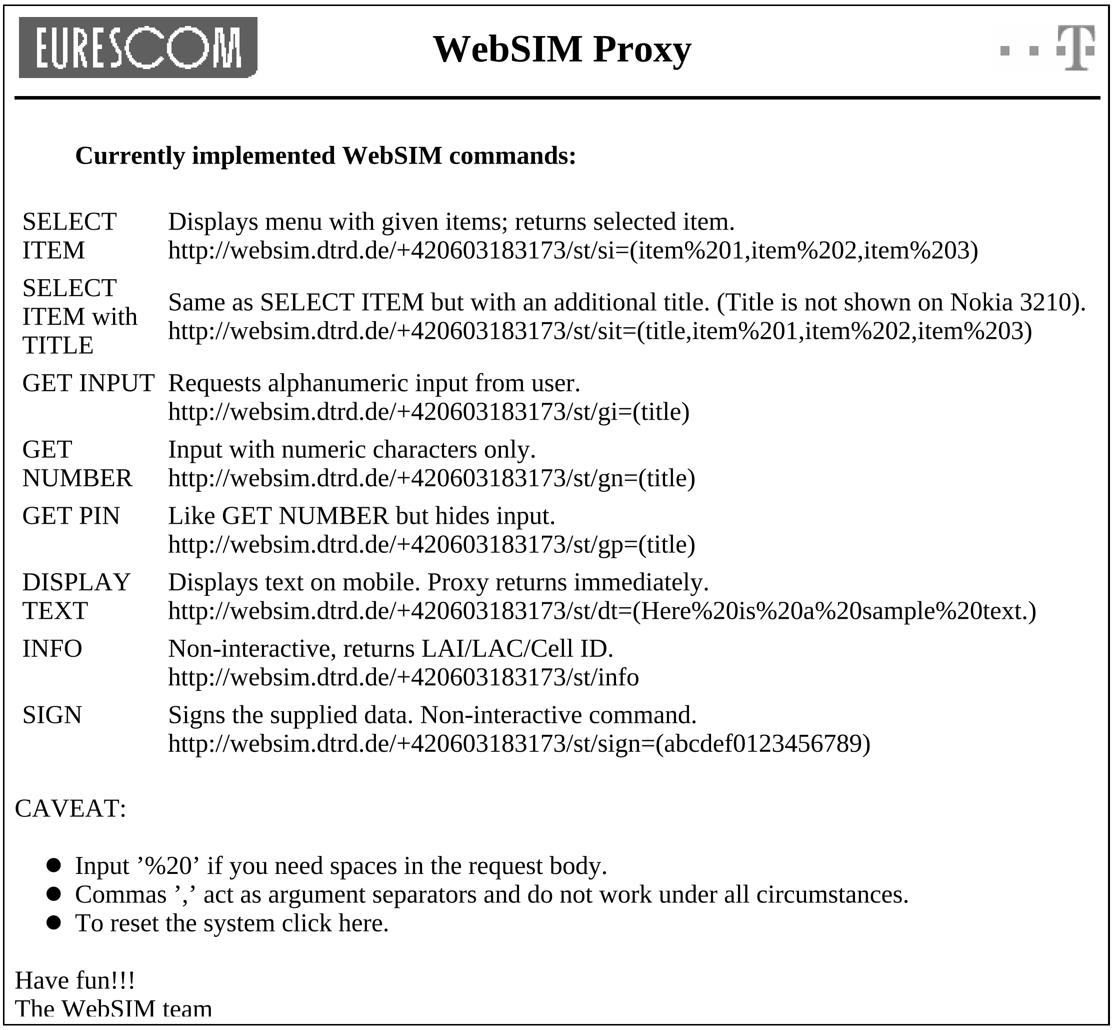
In summary, the SIM becomes a Web server on the Internet, where the proxy handles the

TCP/IP layers, and the SIM sees HTTP over SMS. As a result, the SIM is transparently accessible from Internet hosts and services of SIMs (authentication, micro payments, or whatever can be done with a smart card) can be accessed over HTTP/CGI scripts from Internet hosts.

The WebSIM was implemented in early 2000 within the EURESCOM Project P1005 [1]. The implementation is based on a Schlumberger Simera SIM [3], the application inside the SIM requires less than 10 KByte of the 32K EEPROM. On the proxy-side we use a Linux laptop running Apache, HTTP tunnelling is implemented by a couple of Perl scripts.

A small number of WebSIMs are currently used in a small field trial within the EURESCOM project; the experience so far is very promising, the system is reasonably reliable, and the execution of a HTTP request over SMS takes usually less than 10 seconds.

Figure 2 is a screen shot from the WebSIM proxy home page, which lists the currently available interfaces to SIM services.



EURESCOM

WebSIM Proxy

Currently implemented WebSIM commands:

SELECT ITEM	Displays menu with given items; returns selected item. http://websim.dtrd.de/+420603183173/st/si=(item%201,item%202,item%203)
SELECT ITEM with TITLE	Same as SELECT ITEM but with an additional title. (Title is not shown on Nokia 3210). http://websim.dtrd.de/+420603183173/st/sit=(title,item%201,item%202,item%203)
GET INPUT	Requests alphanumeric input from user. http://websim.dtrd.de/+420603183173/st/gi=(title)
GET NUMBER	Input with numeric characters only. http://websim.dtrd.de/+420603183173/st/gn=(title)
GET PIN	Like GET NUMBER but hides input. http://websim.dtrd.de/+420603183173/st/gp=(title)
DISPLAY TEXT	Displays text on mobile. Proxy returns immediately. http://websim.dtrd.de/+420603183173/st/dt=(Here%20is%20a%20sample%20text.)
INFO	Non-interactive, returns LAI/LAC/Cell ID. http://websim.dtrd.de/+420603183173/st/info
SIGN	Signs the supplied data. Non-interactive command. http://websim.dtrd.de/+420603183173/st/sign=(abcdef0123456789)

CAVEAT:

- Input '%20' if you need spaces in the request body.
- Commas ',' act as argument separators and do not work under all circumstances.
- To reset the system click here.

Have fun!!!
The WebSIM team

Figure 2: WebSIM Proxy Home page

3 WebSIM-based Authentication in the Internet

Internet service or application providers such as online book stores, Web shops, or banks need secure identification of customers. Online orders are usually placed via Web forms or call centers and authentication takes place in various forms, e.g. using password-based authentication schemes.

3.1 GSM-based Authentication

Involving the WebSIM into authenticating Internet users allows for more elegant solutions that can take advantage of secure cryptographic keys (like the subscriber's individual key Ki as illustrated in Figure 3):

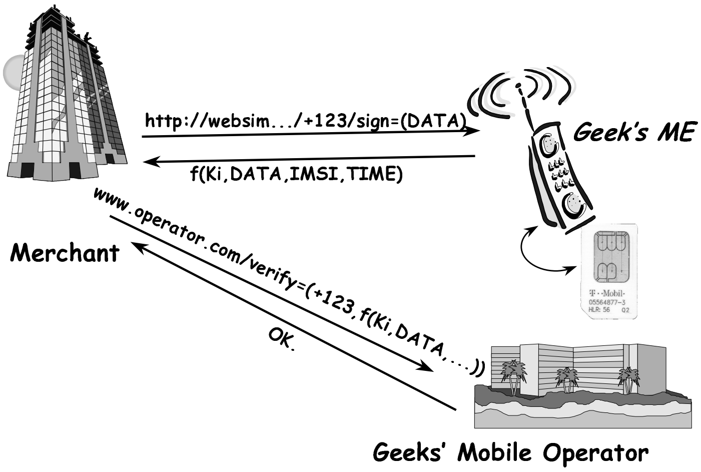

http://websim.../+123/sign=(DATA)
f(Ki,DATA,IMSI,TIME)
Geek's ME
www.operator.com/verify=(+123,f(Ki,DATA,...))
Merchant
OK.
T··Mobil·
Geeks' Mobile Operator

Figure 3: WebSIM Authentication

1. A server-side application within the WebSIM is launched through the proxy and a random challenge is passed to it as an argument.
2. The WebSIM server-side application asks the subscriber over the SIM AT protocol [6] to authorise the computation of a response f(Ki, RAND), which is returned to the originator of the request.
3. The ISP passes RAND and f(Ki, RAND) to the card issuer (resp. the party that knows Ki and f) who can verify the result.

This is a classical challenge/response authentication which can be applied to many other scenarios (home banking, access control, etc.) analogously, or can be easily adapted to provide, for instance, a session key for other purposes. For security reasons, the scenario can also be based upon other cryptographic algorithms (like 3DES or RSA) and keys other than Ki, which may be derived from Ki.

The scenario can also be easily extended to sign transactions (like online payments): note, in particular, that the incoming SMS that carries the HTTP-request contains a (reasonably) trustworthy time stamp originating from the Short Message Center that was involved. Furthermore, subscriber-individual IDs like the IMSI (International Mobile Subscriber Identity) are available in the SIM.

3.2 Provision of One-Time Passwords

One-time passwords for login procedures or TANs for bank transactions can be easily queried over WebSIM requests; we consider online shopping as an example:

- A user subscribes to a service on the Internet and tells her mobile phone number.
- The user compiles a shopping list in Internet shop and orders by submitting the shopping list.
- The Internet shop's Web server displays a one-time password to the customer. Simultaneously, the Web server issues a WebSIM request to the customer's SIM asking to enter the one time password on the mobile phone.
- The WebSIM issues an appropriate GSM 11.14 command to the mobile phone, prompting the user for the one-time password. The user enters the one-time password, which is sent back to the Web server, possibly over an encrypted communication channel.
- The Web server of the shop checks whether the entered one-time password is correct, and if so, it acknowledges the purchase.

The advantage is that an authentic channel (GSM) is used to verify the identity of the customer. Another, reversed variant of this might be as follows:

- After submitting the shopping list, the Web server generates an input form where the user has to enter a one-time password; the server sends the one-time password to the WebSIM, which is displayed on the mobile phone.
- The user enters the one-time password which is displayed by the WebSIM dialog on her mobile into the Web form. The Web server checks the one-time password and accepts submission.

Note, that similar one-time password schemes can be implemented by sending a password over a text SMS to a mobile phone user; the difference to a WebSIM-based approach one has control over the concrete form of interaction with the user, whilst a text SMS is just a (non-interactive) messaging service.

4 Using WebSIMs as I/O Channels

Interesting applications are possible if the WebSIM implements CGI scripts that provide an interface to SIM application toolkit (AT); briefly, SIM AT is a standardised protocol [6] between the mobile phone and the SIM that allows applications inside the SIM to control the behaviour of the phone: the SIM can directly interact with the user by displaying text, querying for input, setting up menus, etc.

The HTTP interface to GSM 11.14 we provide allows for following scenarios:

4.1 Secure User Interaction

A person holding a mobile phone with a WebSIM is standing in front of an ATM, and calls a telephone number displayed on the ATM. The ATM system knows the Web address of the WebSIM (from CLIP signalling [9]) it can run several subsequent CGI Scripts in the

WebSIM to authenticate the transaction, choose the amount of cash to be issued, etc. Essentially the GSM phone has become the human interface to the ATM and one can imagine ATMs that do not have complex and expensive human interface hardware but are just a telephone number sign and a cash-dispensing slot.

Analogously, one can implement online payments, access control, ticket vending, etc. See Figure 4 for example screen shots of mobile phone displays, where the SIM toolkit command “Setup Menu” is used to select from choices. Note that cryptographic means to secure the result of the user interaction (the input, or the user’s choice) are easily available inside the SIM.

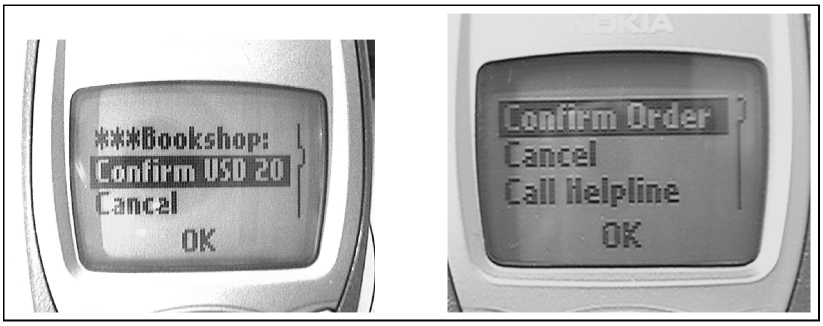


Figure 4: WebSIM Screen Shots

4.2 Internet Auction Client

In contrast to WAP which is currently a pull-based technology for Internet content there are various applications urging for a more “push”-based style of communication. As an example consider on-line Internet auctions in which a WAP user would participate by regularly checking for newly placed bids for an object of interest. This would not only be annoying for potential users but also slow and expensive.

Using the WebSIM one can implement a push-based client that behaves as follows:

- After registration for a certain item in an auction, a user delegates auction interaction to the WebSIM by providing the mobile phone number to the auction company.
- Each time a higher bid is placed – other invocation schemes can be thought of – the auction sends a request to the WebSIM that informs the mobile user about the currently active highest bid and asks for entering a new, higher bid.
- The user can then decide to decline or to increase and enter the new bid which is then sent back to the auction house that places the bid.

This turns the WebSIM into a full-fledged, mobile, push-based communication module allowing for user interaction which is not supported by, e.g. the Wireless Application Protocol (WAP).

5 Where are you? Obtaining Location Information

A mobile user’s location is a sensitive piece of information. An attacker must not be able to track a user’s location, even if he does not (yet) know which specific user he is tracing.

On the other hand, the mobile network constantly needs location information about a mobile user, in order to route incoming calls to her. Location information is provided to the network by means of "Location Updates" regularly performed by the mobile using a pseudonym, the so-called TMSI (Temporary Mobile Subscriber Identity) in order to preserve the user's privacy.

But not only network operators can make use of the user's location information: Location-based services are a hot topic in todays mobile commerce scenarios. The general assumption is that for a significant amount of mobile services location can aid in better service provisioning. Some examples:

- **Mobile tourist guide.** Get information about the mobile user's current location, its history, and other valuable information for tourists.
- **Near-by services.** Check out near-by restaurants, shops, restrooms, ATMs, public transportation facilities, etc.
- **Where am I? I'm lost!** Check for maps showing the mobile user's current location and other useful information for localisation.

Usually, these services are associated with the upcoming high-bandwidth mobile phone standard UMTS, where it is anticipated that the information is sent directly to the mobile and displayed on it. But even within GSM, the WebSIM provides a way for location-based service providers to securely get the sensitive location data directly from their customers in form of an HTTP-response packed into an SMS (cf. Section 2), without having to go via the mobile operator (actually, unless the mobile operator is not providing the service itself, the operator does not need to know which location-based services are used by its customers). To this end, we have implemented a WebSIM script that uses the SIM AT command PROVIDE LOCAL INFORMATION to query the phone for its current position within an operator's network, e.g. mobile country code, network code, local area information, and cell ID. This information may be translated by the service provider into more conventional formats such as longitude / latitude coordinates, or even into hyperlinks under which maps can downloaded indicating the position in different degrees of precision.

Currently, we are running a prototype called the *Mobile Homepage* of a mobile user [12]. This homepage can be accessed after successful Web-based authentication to restrict access to localisation information to an authorised group of people only. Furthermore this mobile homepage can show context-dependent information of a mobile user, e.g. whether she is currently in a meeting. This kind of information can be configured by a SIM AT application in the WebSIM. It allows people that have been granted access to the mobile homepage, e.g. to infer that "I'm currently in a meeting and I'm likely to be reachable in about two hours later."

6 WebSIM-based End-to-End Security

At the moment we are experimenting with putting additional security applications based on symmetric encryption, e.g. 3DES on the WebSIM. Since the WebSIM proxy can route encrypted application data transparently through to the Internet service provider, this yields a secure channel from the WebSIM to the Internet service provider, with whom the WebSIM shares a symmetric key.

This is clearly an advantage over, e.g. WAP Wireless Transport Layer Security (WTLS) [4], where the WAP gateway, lying in between the mobile terminal and an Internet service provider has to decrypt the WTLS traffic first, before it passes the data on to the Internet service provider. As a result of this drawback, many companies wanting to communicate with their mobile employees over WTLS have to put their own WAP gateways inside their company's Intranet.

However, even with the WebSIM being equipped with additional security applications, there is no real end-to-end security yet, because the network service provider still has control over the keys it is putting on the SIMs. As long as the current trust model in mobile communications, where the user has to trust the network service provider issuing the user's SIM card, is not changed, it seems doubtful that one can achieve real end-to-end security without having to introduce additional trusted third parties.

7 Related Work

We are aware of two approaches that provide a related underlying base technology that our work suggests: Jim Rees and Peter Honeyman [13] were the first to describe a Java-based smart card that handles IP packets and provides an interface through a Web server built into the card. Furthermore, Pascal Urien [14] recently proposed another approach, where the Internet connectivity as well as the Web server functionality of a smart card is handled by the card terminal. Both approaches differ from our work in that they address "classical" smart cards, whereas we primarily aim at GSM SIMs.

8 Conclusion

We described several applications based on the WebSIM technology, where services offered by a GSM-SIM are interfaced with the Internet by implementing a Web server inside the SIM. The main contribution here is to interface the GSM security infrastructure with the Internet, such that Internet applications that require security can take advantage of GSM smart cards. For this approach, we have coined the term "mobile security". Technically speaking, we provide an HTTP-interface of the SIM to the Internet, the TCP/IP part of the Internet protocol suite is handled by a proxy host in the Internet.

The main advantages of our approach is that

- it allows to reuse the existing smart cards (SIMs) in GSM mobile phones for providing security to Internet applications,
- it is easy to be integrated into Internet applications, since it just requires to embed HTTP-requests,
- it avoids the usual trouble with low-level smartcard-based protocols (T=0, etc.) or the integration of card readers into applications,
- it is completely based on standards and does not involve any proprietary protocols.

References

[1] EURESCOM P1005. http://www.eurescom.de/~public-webspace/P1000-series/P1005/.

[2] i-Mode. http://www.nttdocomo.com/imode/.

[3] Schlumberger, Inc.: Cyberflex Simera™, Technical Information. http://www.cyberflex.com/Products/MobileCom/simera/simera.html.

[4] WAP Forum. Wireless Application Protocol, Technical Specifications. http://www.wapforum.org/what/technical.htm, 2000.

[5] Scott Guthery, Roger Kehr, and Joachim Posegga. How to Turn a GSM SIM into a Web Server. In Josep Domigo-Ferrer, David Chan, and Anthony Watson, editors, *Proceedings of Fourth IFIP TC8/WG8.8 Smart Card Research and Advanced Application Conference CARDIS'2000, Bristol, UK*, pages 209–222. Kluwer Academic Publisher, September 20–22, 2000.

[6] European Telecommunications Standards Institute. *Digital cellular telecommunications system (Phase 2+): Specification of the SIM application toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface.* Sophia Antipolis, France, 1998.

[7] European Telecommunications Standards Institute. *Digital cellular telecommunications system (Phase 2+): Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface.* Sophia Antipolis, France, 1998.

[8] European Telecommunications Standards Institute. *Digital cellular telecommunications system (Phase 2+): Technical Reaslisation of the Short Message Service; Point-to-Point (PP); Service description; Stage 2.* Sophia Antipolis, France, 1998.

[9] European Telecommunications Standards Institute. *Integrated Services Digital Network (ISDN); Calling Line Identification Presentation (CLIP) supplementary service. Service description.* Sophia Antipolis, France, 1998.

[10] European Telecommunications Standards Institute. *Digital cellular telecommunications system (Phase 2+, Release 98): Subscriber Identity Module Application Programming Interface (SIM API); Service description; Stage 2.* Sophia Antipolis, France, 2000.

[11] European Telecommunications Standards Institute. *Digital cellular telecommunications system (Phase 2+): Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card; Stage 2.* Sophia Antipolis, France, 2000.

[12] Roger Kehr and Andreas Zeidler. Look Ma', My Homepage is Mobile! *Journal of Personal Technologies, Springer-Verlag, London*, 4(4):217–220, 2000.

[13] Jim Rees and Peter Honeyman. Webcard: A Java Card web server. In *Proceedings of CARDIS 2000*, Bristol, UK, September 2000.

[14] Pascal Urien. Internet card, a smart card as a true Internet node. *Computer Communications, Elsevier Science*, 23(17):1655–1666, 2000.