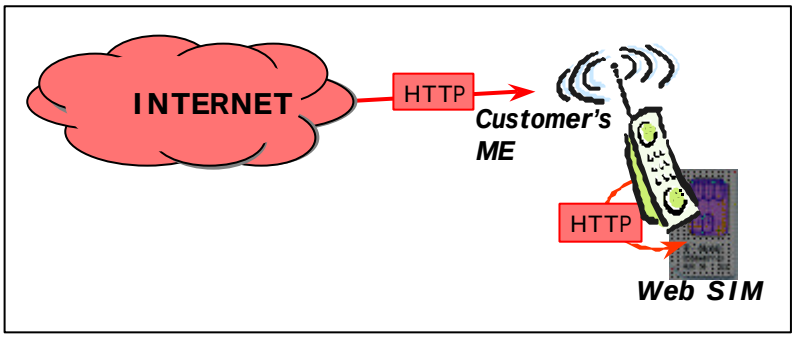
GSM SIMs as Web Servers*

Scott Guthery, Mobile-Mind, sguthery@rcn.com
Roger Kehr, Deutsche Telekom Research[1], Roger.Kehr@Telekom.de
Joachim Posegga, Deutsche Telekom Research[1], Joachim.Posegga@Telekom.de
Harald Vogt, ETH Zurich, Harald.Vogt@inf.ethz.ch

GSM SIMs are operator-trusted security servers in GSM, performing computations on behalf of a GSM subscriber. This paper outlines a prototype that integrates the GSM security infrastructure into the Internet: The idea is to extend a GSM SIM to a security server for a GSM subscriber in the Internet. Such a *WebSIM*, like any other server in the Internet, speaks TCP/IP and is transparently accessible from Internet hosts via HTTP. Specific services offered by SIMs, e.g. authentication, can be accessed from the Internet using CGI scripts.

Technically, this is achieved by implementing a small, stripped-down Web server inside the GSM SIM and making the SIMs interface accessible from the Internet (cf. Figure on the right). In this way, communicating with a SIM in a mobile phone, e.g. for authenticating a customer browsing a Web site, becomes as easy as communicating with any Web server running in the Internet.



Seen from the GSM perspective, the idea behind the WebSIM is to make the interface of today's GSM SIMs (ETSI GSM 11.11) partially available to the Internet.

Technical Outline of the Approach

Running a Web server in a SIM is less of a problem than one might think, in fact such servers for ordinary smartcards were foreshadowed in [Rees & Honeyman, 1999]. A Web server in a SIM is not expected to host large amounts of information or HTML documents, but to provides a convenient interface to services of the SIM: These services, most of which will probably be security-related, can then be accessed via the standard protocol of the Web, HTTP.

A stripped-down version of these protocols, which just cover the absolutely necessary part and only allow for one connection at a time, can be easily implemented with a Web server application of less than 10 K inside the SIM. In particular, we can very elegantly implement this functionality as an Applet on top of a SIM Toolkit platform [GSM 02.19

* An extended version of this paper is available from http://www.scdk.com/websim.pdf.
[1] The opinions expressed in this paper are those of the authors; they do not necessarily reflect the views of Deutsche Telekom AG.

and 03.19] and then use the Toolkit's interpreter for server-side scripting. This also allows for interacting with the user of the SIM's mobile phone, since SIM Toolkit provides an appropriate API for I/O from within the SIM.

HTTP messages [RFC 1945] to the SIM are be tunnelled through the data field of an appropriate ISO 7816-3 frame (payload type 2) or carried in a TTCP/IP datagram [RFC 1379, RFC 1644] within the data field (payload type 1). The current version of the WebSIM supports the HTTP/1.0 methods GET, HEAD, POST, and supports URLs [RFC 2396] of the form:

http://<userinfo>@<host>:<channel>/<path>?<query>

for accessing SIM services via CGI.

Internet connectivity of the SIM can be established in two principal ways:

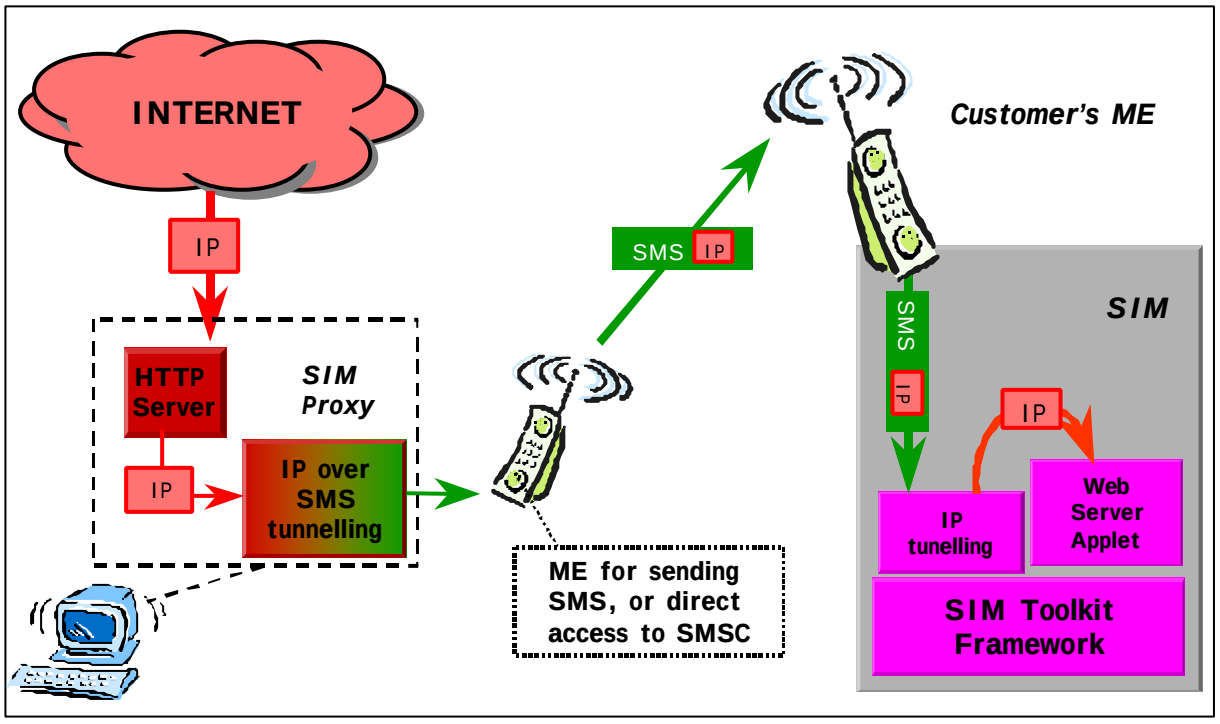
a) An MS that is connected to the Internet works as the SIM's Internet gateway, i.e: it forms a router that passes IP packets for the SIM by embedding it into APDUs, and the reverse.

b) A proxy host for the SIM in the Internet uses existing communication channels to the SIM, e.g. by tunneling IP packets through SMS to the SIM.

Alternative a) requires adaptation of mobile terminals and new standards, and is therefore not feasible in the short term. An alternative approach is b), which tunnels IP packets over SMS; this can easily be implemented today's GSM networks since it does not require any changes in the functions of MSs or the GSM network:

We set up a proxy for the SIM on the Web and have this proxy tunnel IP packets through SMS to the SIM (cf. Figure below). SMS messages arrive directly in the SIM and can be processed as required, e.g. by having Toolkit Applets register for such SMs. The procedure for proxy-based IP-communication with the SIM over SMS is as follows:

1. *An Internet host sends an HTTP request to the SIM's proxy.*



2. *The proxy embeds the request in a specially tagged SMS and sends it to the SIM.*
3. *The SIM passes the incoming SMS-encapsulated IP packet to a tunneling applet inside the SIM, that has registered to handle such tagged SMS.*
4. *The tunnelling applet extracts the IP packet and passes it to the Web server.*
5. *The Web server processes the HTTP request and formulates the response.*
6. *The HTTP response is embedded in SMS again and sent back to the proxy.*
7. *The proxy extracts IP packets from SMS message and sends it back to the originating host over the Internet.*

As a result, the SIM can be transparently accessible from any Internet host: for example, an URL request such as

http://www.operator.com/+491710000000/Identity?challenge=2A49C01

can initiate the identity application running in the WebSIM of the named GSM phone. After processing the request, which might consist of running other SIM-internal applications or commands, the result is sent back to the originating Internet host. Thus, integrating SIM-based security into Internet applications is as easy as talking to any Web server on the Internet.

Conclusion

The main contribution of the WebSIM is to provide the function of SIMs in Internet-compliant protocols anyone can use. This means, that on one hand the barrier for Smartcard applications today, which is the lack of integration of Smartcards into the IT and Internet world and the complex interaction with cards using APDUs, is overcome by providing a simple, standard protocol, i.e. HTTP, for accessing SIM services. On the other hand, we can integrate several millions of smartcards into the Internet, providing a trust infrastructure that is badly needed for electronic commerce applications.

References

[GSM 02.19] *Digital cellular telecommunications system (Phase 2+, Release 98): Subscriber Identity Module Application Programming Interface (SIM API); Service description; Stage 2*. ETSI, Sophia Antipolis, France, 1999.

[GSM 03.19] *Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™ ; Stage 2*. ETSI, Sophia Antipolis, France, 1999

[GSM 11.11] European digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.11). ETSI, Sophia Antipolis, France, 1998.

[GSM 11.14] *European Digital cellular telecommunications system (Phase 2+): Specification of the SIM application toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface (GSM 11.14).* ETSI, Sophia Antipolis, France, 1998.

[ISO 7816] ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols

[Rees & Honeyman, 1999]. Jim Rees and Peter Honeyman: *Webcard: a Java Card web server*. CITI Technical Report 99-3, Center for Information Technology Integration, University of Michigan. October 1999.