

How to Turn a GSM SIM into a Web Server

EURESCOM P1005 Project Internal Result

Roger.Kehr@Telekom.de, Joachim.Posegga@Telekom.de

February 2000

Overview

Mobile networks like GSM or UMTS provide a security infrastructure that builds upon subscriber-individual secret keys. The key is stored in a smart card (a so-called SIM) that lives in the mobile phone. These SIMs are in fact small, but quite complex computers that come with an operating system, a file system, and even a built-in Java platform.

The WebSIM-approach turns such a SIM (and therefore also the mobile phone "around it") into a Web server. It can be transparently accessed from the Internet, processes HTTP request and works as a personal Web server for a person.

There are various applications for this technology, like authentication in Internet, online payments etc. Since the mobile phone comes with a keyboard and a display, we can also use it as a secure I/O channel: If the user of such a phone orders a product from a Web site, then this site can simply submit a HTTP request like

```
http://websim.dtrd.de/+123456789/menu=(Confirm,Cancel)
```

and prompt the user for a confirmation of the order on his/her mobile phone.

Brief Technical Description

The WebSIM is a GSM SIM with a built-in Web-Server. This integrates SIMs in the Internet and allows for transparent access of the SIM via HTTP/CGI Scripts from Internet hosts.

As a result, GSM operators can market their GSM security infrastructure in the Internet and provide SIM-services to the Internet: The WebSIM speaks the lingua franca of the Internet, HTTP, and it becomes a trivial exercise for Internet developers to include WebSIM-based services in their applications.

Services of the WebSIM that are accessible from Internet hosts can be classical security services (authentication, encryption), or GSM 11.14 commands, which provide a simple I/O interface to the user of the mobile phone. HTTP requests from a Web application to 11.14 services of a WebSIM allow e.g. for establishing a secure I/O channel to an Internet user via its WebSIM phone.

It should be noted that the WebSIM itself is not an application per se: instead it provides a horizontal technology layer, where applications can be built. The contribution

is that this technology layer is designed in the most convenient way for Internet developers and offers a radically simple interface to GSM/SIM services.

Example Usage

Assume an Internet customer ordered an item through an online Web shop. If the Web shop knows the mobile phone number of the customer, say +123456789, it can simply integrate a HTTP-request like

```
http://websim.dtrd.de/+123456789/st/si=(Confirm%20Order,Cancel,Call%20Helpline)
```

into the Web application and confirm the transaction through the GSM network. (Note: "%20" is the HTTP-encoding for a Space character; " st/si" stands for: SIM Toolkit/Select Item, cf. GSM 11.14)

This HTTP-request to the WebSIM prompts the user with a menu on its mobile phone, as shown in Figure 1. The vendor's trust in the transaction can thus be enhanced by the security of the GSM system. This security is today superior to what the Internet can offer, since a trusted channel from customers to vendors is still missing in the Internet.

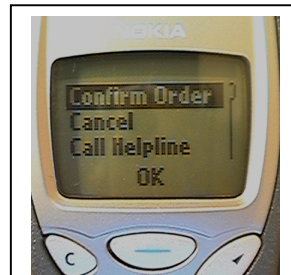


Figure 1: Screenshot

Implementation of the Prototype

The WebSIM is currently implemented on a Java SIM from Schlumberger (32K Simera); the Web Server in the SIM itself is implemented as a Toolkit-Applet of about 8K, several 11.14 commands for I/O are accessible via CGI-Scripts. The approach works with any GSM phase II+ mobile phone.

The connection between the Internet and the WebSIM is handled by a proxy host that tunnels HTTP-requests over SMS to the Web server applet in the SIM. Figure 2 shows the overall architecture: A HTTP-request arriving from the Internet for a particular WebSIM (determined by its phone number) is packed into an SMS to the SIM, where the request is unpacked and processed. The response is sent back as an SMS to the proxy, where a normal HTTP-response is send back to the originator in the Internet.

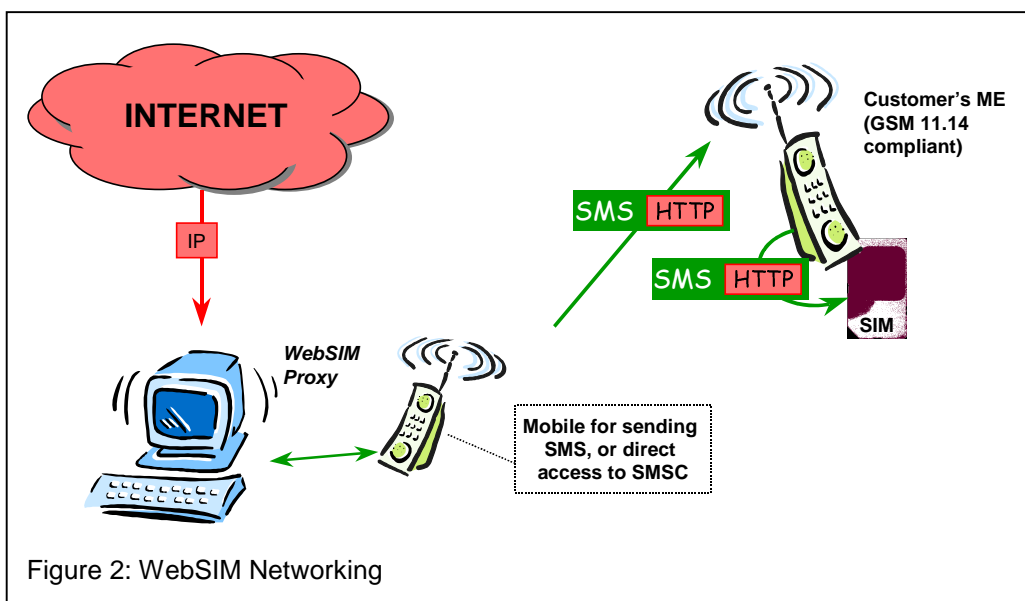


Figure 2: WebSIM Networking