The WebSIM: Smartcard goes Internet

Joachim Posegga

Joachim.Posegga@Telekom.de

31.01.00 09:02

DRAFT – DO NOT DISTRIBUTE

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 compete with 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 build upon. 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 `+420603181373`, it can simply integrate a HTTP-request like

`http://www.websim.com/+420603181373/menu=(Confirm%20Order,Cancel,Call%20Helpline)`

into the Web application and confirm the transaction through the GSM network.

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.
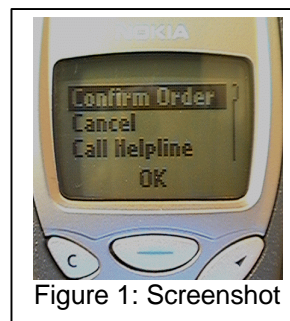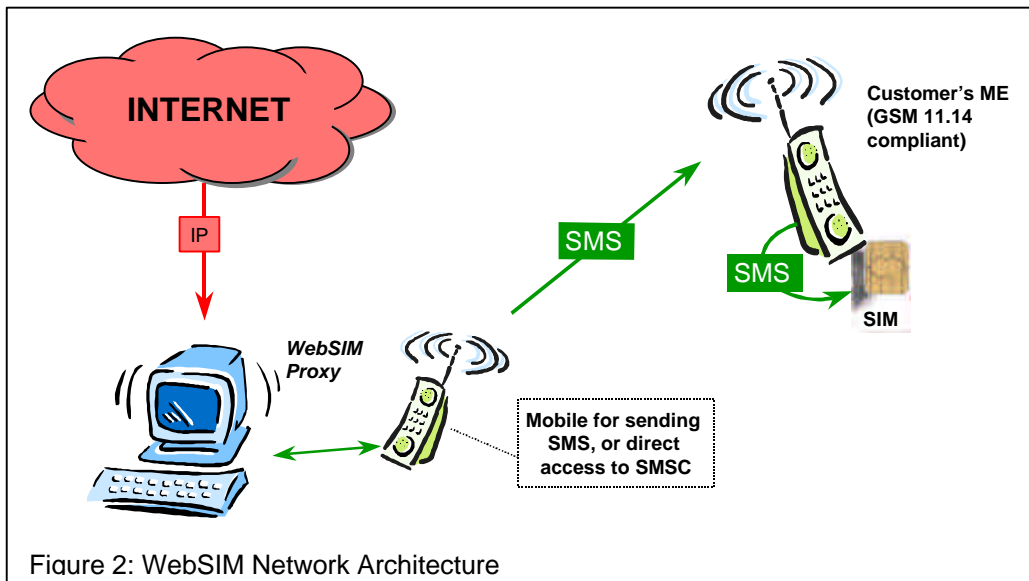

Figure 1: Screenshot

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 6K, several 11.14 commands for I/O are provided as CGI-Scripts.

Figure 2: WebSIM Network Architecture

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 a SM to the SIM, where the request is unpacked and processed. The response is sent back as a SM to the proxy, where a normal HTTP-response is send back to the originator in the Internet.