How to secure services in the future? : Ubiquitous computing and Jini

Autor(en): **Wedmer, Edwin / Krone, Oliver**

Objekttyp: **Article**

Zeitschrift: **Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology**

Band (Jahr): **78 (2000)**

Heft 10

PDF erstellt am: **01.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-876486

Exploration Programmes:
Corporate Technology Explores Future Telecommunications

Ubiquitous Computing and Jini:

How to Secure Services in the Future?

In the future, billions of intelligent (small) devices like mobile phones, PDAs, networked cameras, home or office appliances etc. will be connected to the net and provide a rich set of new services. Users will be mobile and access these services using heterogeneous devices at different locations, and in changing environments. How can security problems be solved in this new computing world? A first step is to introduce public key cryptography on the SIM cards in mobile phones or some other personal item (e.g. iButton, smart card) carried by the user. A second step is to design and develop a platform for authentication and authorisation for impromptu client server applications.

The programme "Cards and Security" explores new security concepts and technologies with a special focus on security for mobile phones and terminals. In addition, the programme closely follows the evolution of threats to telecom services and provides advices on how to protect services and infrastructure.
With its Exploration Programmes, Corporate Technology explores next generation telecommunication technologies and new services with the goal to actively support innovative business development.

Our vision of the next step of the networked information society is that billions of small, intelligent devices will jointly provide services and access services on the net. This vision is commonly referred to as "Ubiquitous Computing" (fig.1). In order to build flexible applications for this world of services, new kinds of software platforms like Jini will allow impromptu combinations of clients and servers upon demand.
Telecom service providers will take advantage of this development by aggregating services on service portals, thus offering highly personalised service access. From an infrastructure point of view telcos will provide the access and security technology (including billing infrastructure) for both mobile and fixed terminals in order to facilitate service access anywhere, anytime.
However, to make the business work it is crucial to provide security in this future world. How? Many questions have to be answered. This article deals just with a few of them. Shall public key cryptography be introduced and how? Which security features are missing in software platforms like Jini? What should be added in the future? How can we offer a simple way for users to authenticate and authorise to a myriad of services asking for it?

EDWIN WIEDMER
AND OLIVER KRONE, BERNE

Mobile phones and handhold terminals will access billions of services and devices distributed anywhere over the net. How can we assure security? How are users and servers authenticated? How does access control work?

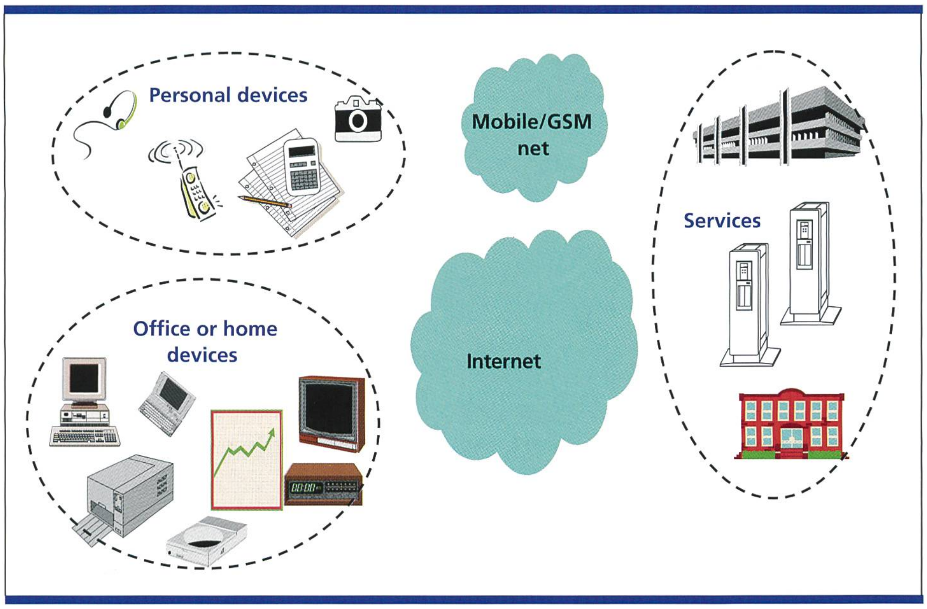


Fig. 1. Today, networked mobiles, PDAs, WEB-cameras, printer servers etc. are predecessors of ubiquitous computing. We expect them to be supplemented by many kinds of other networked personal, office or home appliances. In future, billions of small and connected computers will be in almost all devices and will access and provide services over various networks.

This article takes an operator's perspective of the future networked world. It proposes that mobile operators develop and provide a platform for security and payment of these new services. As an example we present user authentication with public keys (PKCS11) for WEB applications. We then introduce the Java/Jini software technologies, which allow spontaneous interactions of clients and servers, and discuss missing security features.
Finally, we present a security architecture for services developed and deployed using the Jini technology. The architecture provides mechanisms for authentication and authorisation which are not present in the off-the-shelf Jini distribution, hence offering to the user a single secure logon to any combination of services.
The article presents work done at Swisscom Corporate Technology (CT) in collaboration with academic institutes like EPFL, ETHZ, ICSI in Berkeley [1, 2] and with several European operators as part of an EURESCOM project called "Jini&Friends at work towards secured service access" [3, 4, 5]. CT explores and demonstrates usage and adaptation of security technology for mobile devices in an environment of spontaneous networking and service provisioning.

Use mobile Phones to make WEB more secure: WebSIM

A key for mobile telecom business is the SIM card which is used in many hundred millions of mobile phones for identifying the mobile subscriber [6]. The SIM is in fact a small computer. It can interact via display and keypad with the mobile user and communicate world wide via SMS/GSM. It can be programmed and contain cryptographic modules. It can therefore become a suitable platform for security and payment, not only for mobile telephony but also for other types of services.
With WebSIM [5] this is already possible. WebSIM is a small personal WEB server built in the SIM card that receives and answers HTTP requests via SMS (fig. 2). With WebSIM it is possible to make the WEB more secure. Any WEB application can ask the user to authenticate himself or to confirm a purchase with his personal mobile phone. The user simply enters the telephone number of his personal phone on the WEB page and the WEB application interacts via SMS with the mobile phone, executing a challenge response authentication for example.

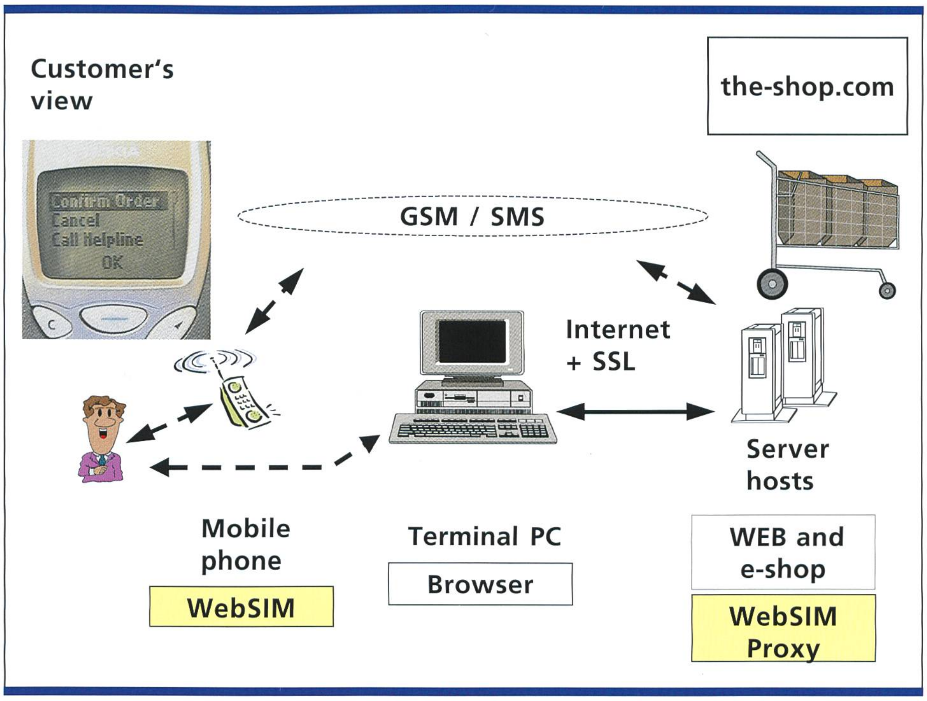


Fig. 2. The mobile phone can be used to make WEB applications more secure. An approach is to put a small WEB server (WebSIM) on the SIM card in the mobile phone and a WebSIM proxy on some server host. Any WEB application can then request for authentication of a user or for a confirmation of a purchase. After getting the phone number of the user it just asks the WebSIM proxy to send a corresponding SMS message to the WebSIM.

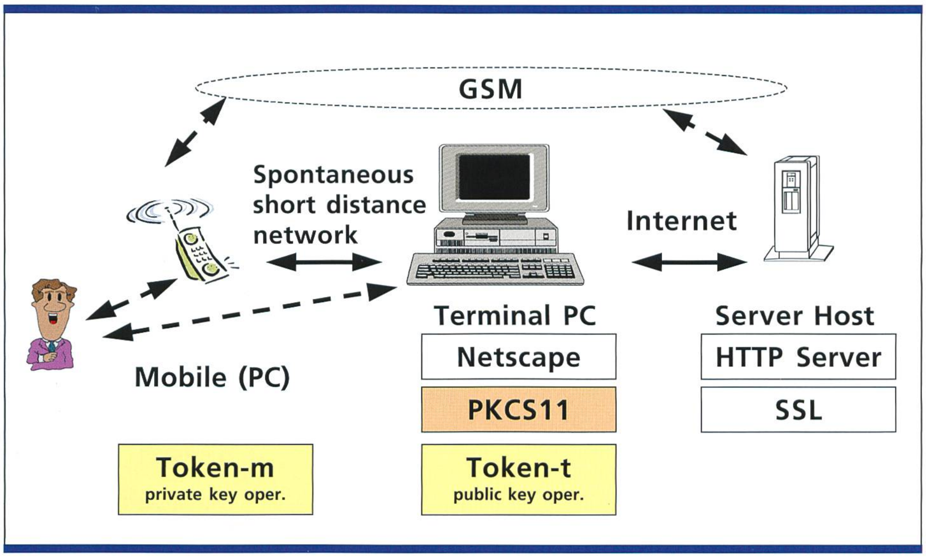


Fig. 3. In future, SIM public key cryptography and short distance networks (e.g. Bluetooth) will allow making authentication more secure and more rapid. The figure shows an approach to use the mobile phone as a token for public key cryptography together with the Netscape browser and PKCS11.

Authentication over ad-hoc short Distance Networks

An alternative to communication via SMS/GSM is to use short distance links like infrared or short distance networks like wireless LANs or Bluetooth. Together with EPFL we developed and tested special protocols for securing spontaneous short distance connections between a mobile device and a WEB browser terminal, and experimented with these protocols using public key cryptography.

In the approach shown in figure 3 we changed the PKCS11 library used by the Netscape browser. We split it into two modules, one on the terminal side and one on the mobile side. In a first step we used a mobile PC storing the users' private key in its memory. The mobile PC was communicating over a wireless LAN. The next step is going to be a mobile phone storing the private key on the SIM card and communicating over Infrared or later Bluetooth [1].

Software Technology: Java/Jini and others

With users moving worldwide and having to adapt to many different environments, computers, devices, services etc. we need a flexible software technology to cope with this complexity. There should be no need of recompilation of code, of tricky installation of device drivers, libraries, or programmes, and of rebooting machines in order to be able to use a specific service.

Java and Jini software technology is being developed by SUN [7] with the aim to make computing in future networks more flexible. Figure 4 shows – as an example – how a mobile user running a Java Virtual Machine (JVM) and Jini on his mobile PC can easily find a local print service. This is achieved by downloading the Java code needed on his mobile PC to access the service (called a print proxy) which allows the user to seamlessly use this service without the need of device driver configuration.

Besides the pioneering Java/Jini technology, alternative approaches like E-Speak from HP and UPnP from Microsoft have been developed for ubiquitous computing.

Securing Lookup, Access and use of Services: Missing Features

Obviously the user's need for flexibility and mobility contradicts requirements for secure service access. SUN has chosen a very open approach for the Jini infrastructure, however various security features are missing (fig. 5).

On the other hand, the Java programming platform has been designed with security in mind. Java offers flexible settings of execution permissions on JVM, a package for Java Authentication and Authorisation Service (JAAS), Java Cryptography Extension (JCE) and much more. SUN and various other developers look now at security issues for Jini and for mobile, spontaneous accesses in general.

Abbreviations

EURES-COM	European Institute for Research and Strategic Studies in Telecommunications
ICSI	International Computer Science Institute, Berkeley
JAAS	a Java package used to authenticate and to control access
Java	object oriented programming language developed by SUN suited for the WEB
JCE	Java Cryptography Extension
Jini	expands Java enabling impromptu networking
PKCS11	standard for token and smart card-based implementations of public key cryptography
PKI	Public Key Infrastructure, for handling public key certificates
RMI	Remote Method Invocation, enables remote communication between Java objects
SIM	Subscriber-Identity-Module, a small card inserted in mobile phones
SSL	Secure Socket Layer, for transmitting data securely over the WEB

An Authentication and Authorisation Architecture

Within the collaboration with the ICSI [2], a proposal has been made for adding secure authentication and authorisation to a Java/Jini environment (fig. 6). The goals are:

- that every service can authenticate and authorise requests by clients from anywhere on the network;
- that every client can make sure it is running only signed code from a trusted source;
- that different login policies can be defined for different users and services;
- that the client can do a single sign-on without the need to authenticate for each service he is going to use.

The prototype uses standard Java technology including JAAS for access authorisation, JCE 1.2.1 for cryptography and JavaCard 2.0 on a personal Java ring [7, 8].

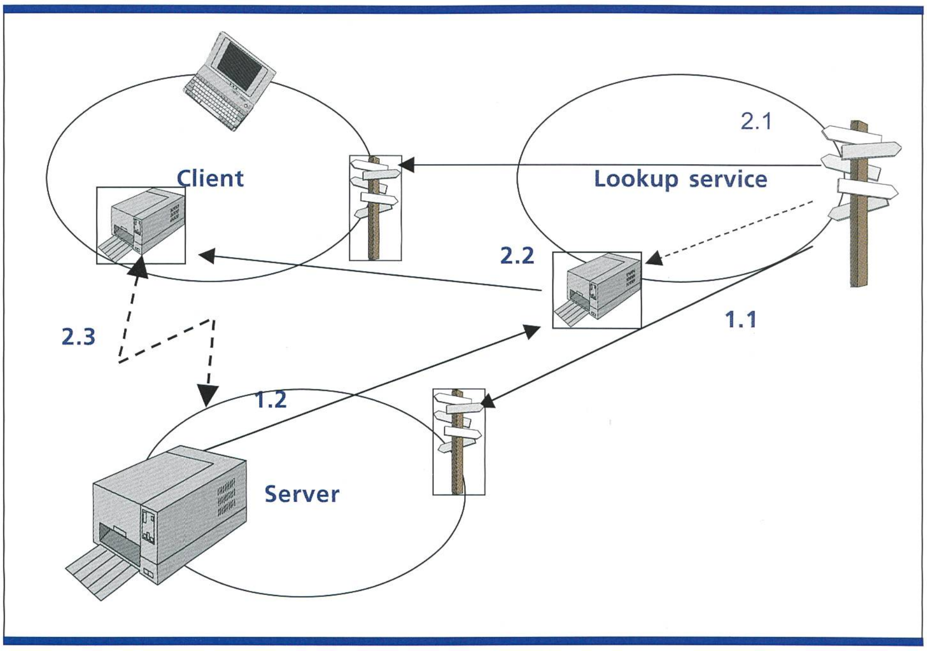
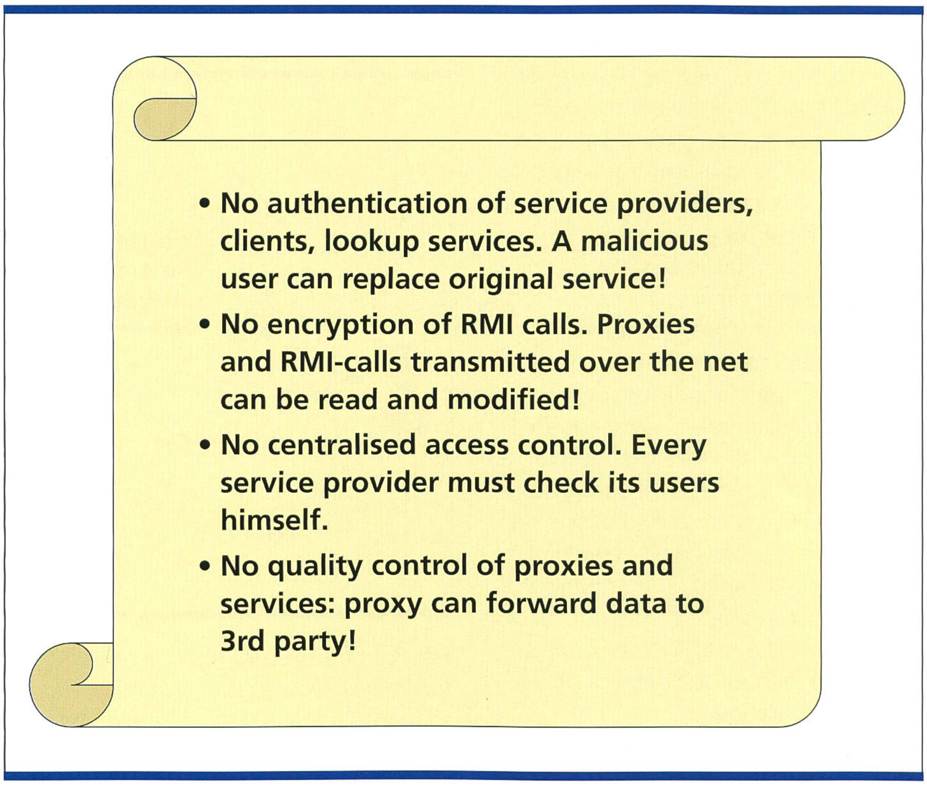


Fig. 4. Jini plus Java software platform provides a convenient way for dynamic service discovery and use. The figure shows how this works for a client on a mobile PC looking for a local printer. First, a print service must discover a lookup service (1.1) and register its proxy (1.2). Then a client on a mobile PC finds the lookup service (2.1), searches on it, downloads the print service proxy (2.2) and finally calls the print methods via the proxy and RMI (2.3).



- **No authentication of service providers, clients, lookup services. A malicious user can replace original service!**
- **No encryption of RMI calls. Proxies and RMI-calls transmitted over the net can be read and modified!**
- **No centralised access control. Every service provider must check its users himself.**
- **No quality control of proxies and services: proxy can forward data to 3rd party!**

Fig. 5. Security holes in current Jini software technology.

Conclusions

Secure service provision for mobile devices will become a big challenge for service providers in the next future. Mobile operators have a large deployed platform for identifying subscribers and charging their services. We argue that this base is very promising for securing access in a future world of ubiquitous computing and networking. 7

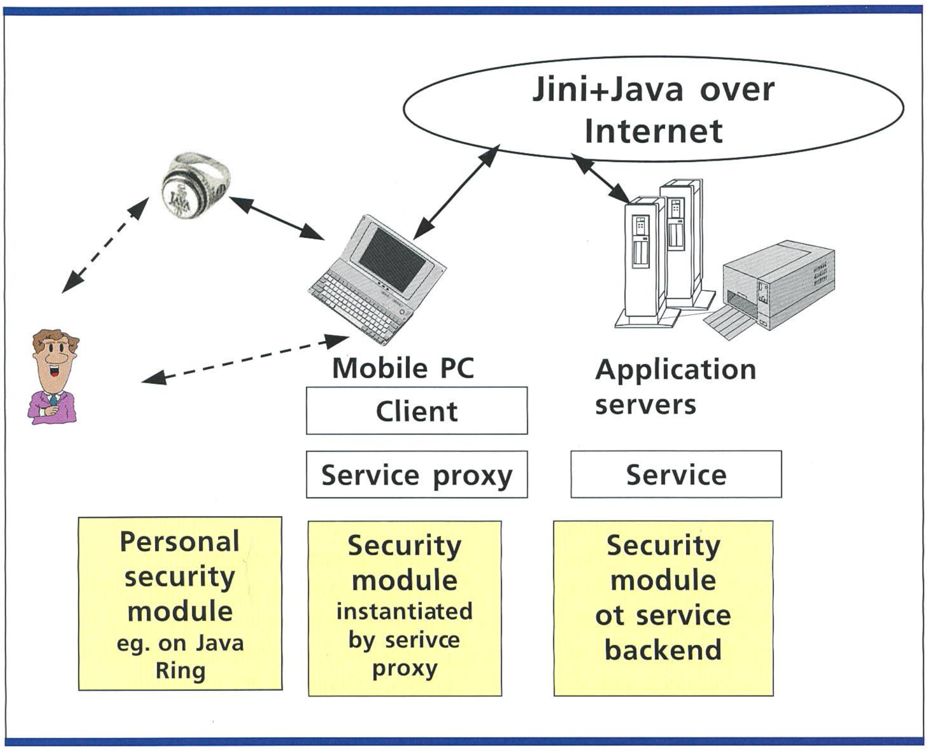

Jini+Java over Internet
Mobile PC
Client
Service proxy
Application servers
Service
Personal security module eg. on Java Ring
Security module instantiated by serivce proxy
Security module ot service backend

Fig. 6. A proposal for a platform for authentication and access control for Jini services from a mobile PC. Users look up services (e.g. information or print service) and call service methods as usual (fig. 4). However, when a service is called, the service backend on the application server checks access with an authentication service. The latter looks up the user info and security policies. Depending on the policy (and whether the user has already logged on) the service proxy may start a security module on the mobile PC to authenticate use (e.g. with a Java Ring by iButton).

References

[1] Felix Baessler, Levente Buttyan, Pascal Etienne, Frédéric Pythoud, Peter Keller, Michael Rohs, Edwin Wiedmer, Markus Wyss, "Exploration projects CASTING and Jini & Friends", Swisscom AG, Corporate Technology, Bern

[2] Oliver Krone, Thomas Schoch, "An Authentication and Authorization Architecture for Jini Services", ICSI Berkeley & Swisscom AG, Bern, August 2000

[3] EURESCOM & ICSI, "Workshop on Ubiquitous Computing", ICSI Berkeley, 31st Aug. 2000, http://www.icsi.berkeley.edu/~krone/ws.html

[4] EURESCOM, "Jini & Friends @ Work: Towards secured service access", www.eurescom.de/~public-webspace/P1000-series/P1005

[5] EURESCOM, "WebSIM", http://www.eurescom.de/websim

[6] Schlumberger, "Smart Cards & Terminals", www.1.slb.com/smartcards"

[7] SUN, "The source for Java Technology", www.javasoft.com

[8] Dallas Semiconductor, "Java-powered Ring", www.ibutton.com/store/index.html#jring

Edwin Wiedmer *did his PhD in computer science (ETH Zürich 1976), joined the telecommunication industry (Ascom) for several years and is working since 1995 as senior engineer at Swisscom Corporate Technology. He is leading projects exploring new technologies in security and mobility and offering consulting to Swisscom business units. Current exploration focus is on spontaneous and secure access to networked services and mobile devices within short distances.*

Oliver Krone *received a Diploma in Computer Science and Electrical Engineering from the Technical University of Munich, Germany and a doctoral degree (Ph.D.) from the University of Fribourg, Switzerland. After graduating from Munich, he worked as a research fellow at IBM's European Networking Center in Heidelberg, Germany where he participated in the development of a multimedia communication system. In 1998 he joined Swisscom Corporate Technology, where he designs and develops Internet-based services.*

Zusammenfassung

In Zukunft werden nicht nur Millionen, sondern Milliarden von Rechnern und Geräten vernetzt sein. SW-Programme für Anwendungen werden spontan übertragen und genutzt werden. Die Benutzer sind mobil und werden weltweit an jedem Ort via verschiedene Netze spontanen Zugang haben. Wie ist in einer solchen Welt ein sicherer Zugang zu Diensten und deren Bezahlung denkbar? Dieser Artikel zeigt auf, wie die Mobilkommunikationsanbieter eine Plattform dafür entwickeln können. Ein wichtiges Element ist die Nutzung von «Token» oder Karten mit Modulen für «Public Key Cryptography» zusammen mit überall einsetzbaren, mobilen Endgeräten, also ohne fixe Kartenleser. Der nächste wichtige Schritt ist die Bereitstellung einer Plattform für Authentifikation und Zugangskontrolle der mobilen Benutzer. Damit wird jeder Teilnehmer seine Kombination von Diensten mit einem einzigen Logon nutzen können.