

# Beyond DRM - Using the TPM to Enable an User-Friendly WLAN-Access

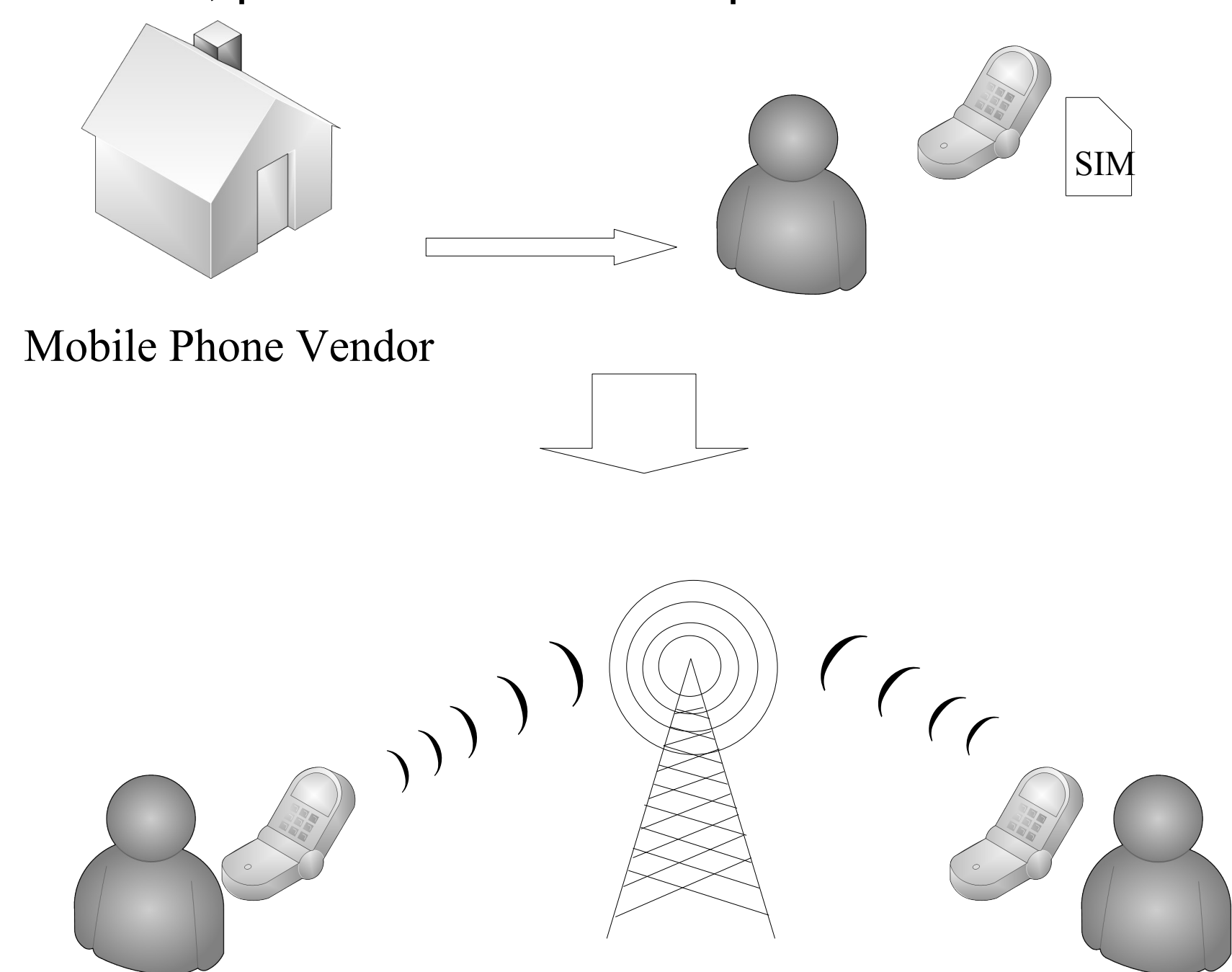
**ABSTRACT** The Trusted Platform Module (TPM) is known and hated as being useful for DRM. But there are more user-friendly application for this module, for instance the possibility to use it for user authentication in wireless networks.

## Introduction

If somebody speaks about TPMs, he usually thinks of DRM. That's why many people disable the TPM of their computer, if they have one. In the future, also mobile phones will be equipped with TPMs and that is not as bad as many people think. There are some user-friendly applications, that are only possible using TPMs. One such application is the user-friendly usage of WiFi phones as they are not very comfortable till now. You think, they are already comfortable enough? The next sections will show, that they may be improved.

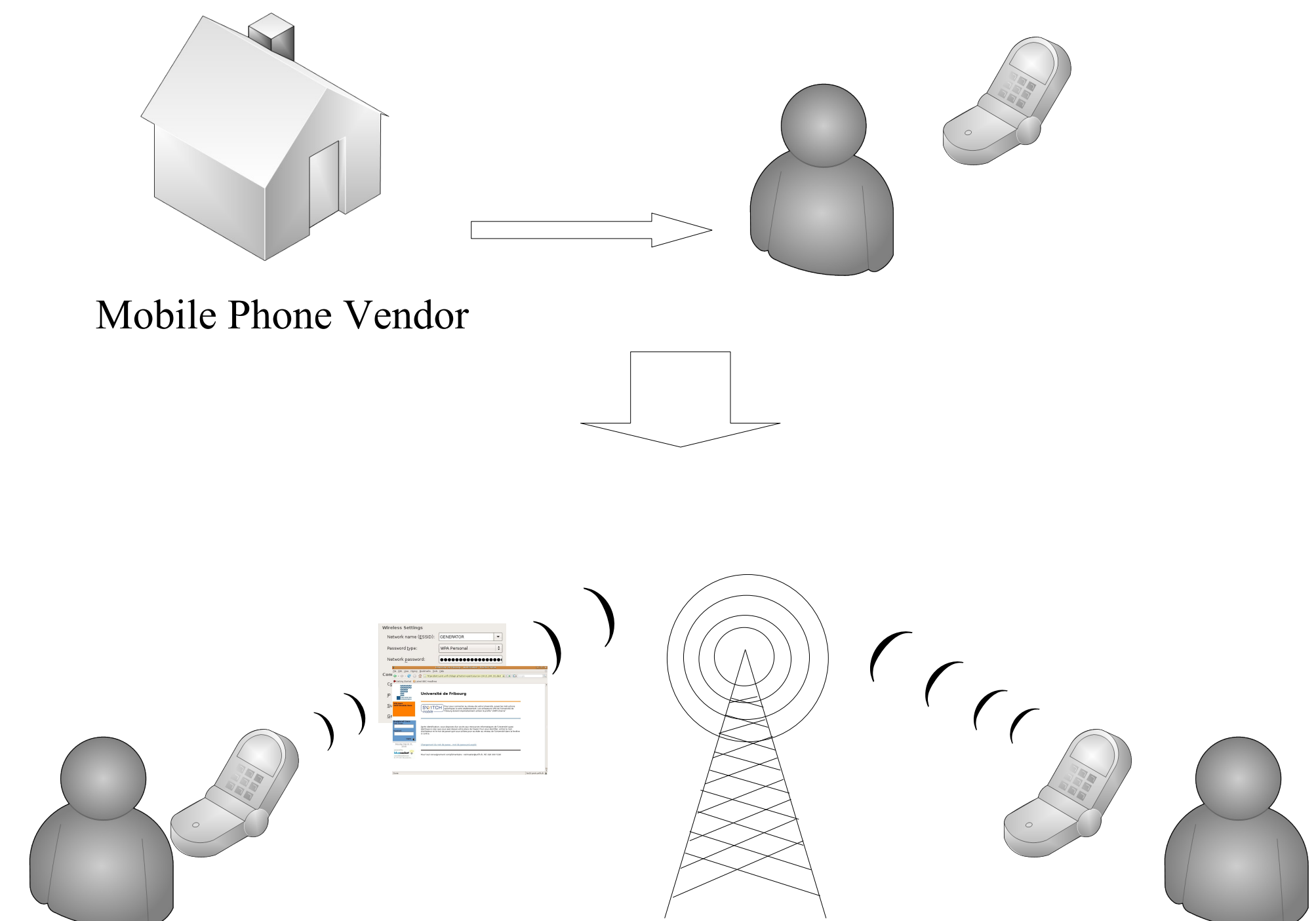
## GSM Networks

From the user's point of view, GSM networks are one of the simplest networks, that exist. After buying a mobile phone and a SIM card, it just works. There is no need for any further configuration. Things like user authentication have been specified in the GSM standard right from the beginning. There is an unique identity for each user, called Subscriber Identity Module (SIM). Using those SIM cards, the user is able to connect to every GSM network using his mobile phone without thinking about how to configure it. If the users wants to have a new GSM identity, he just has to buy a new SIM card, put it into his mobile phone and use it.



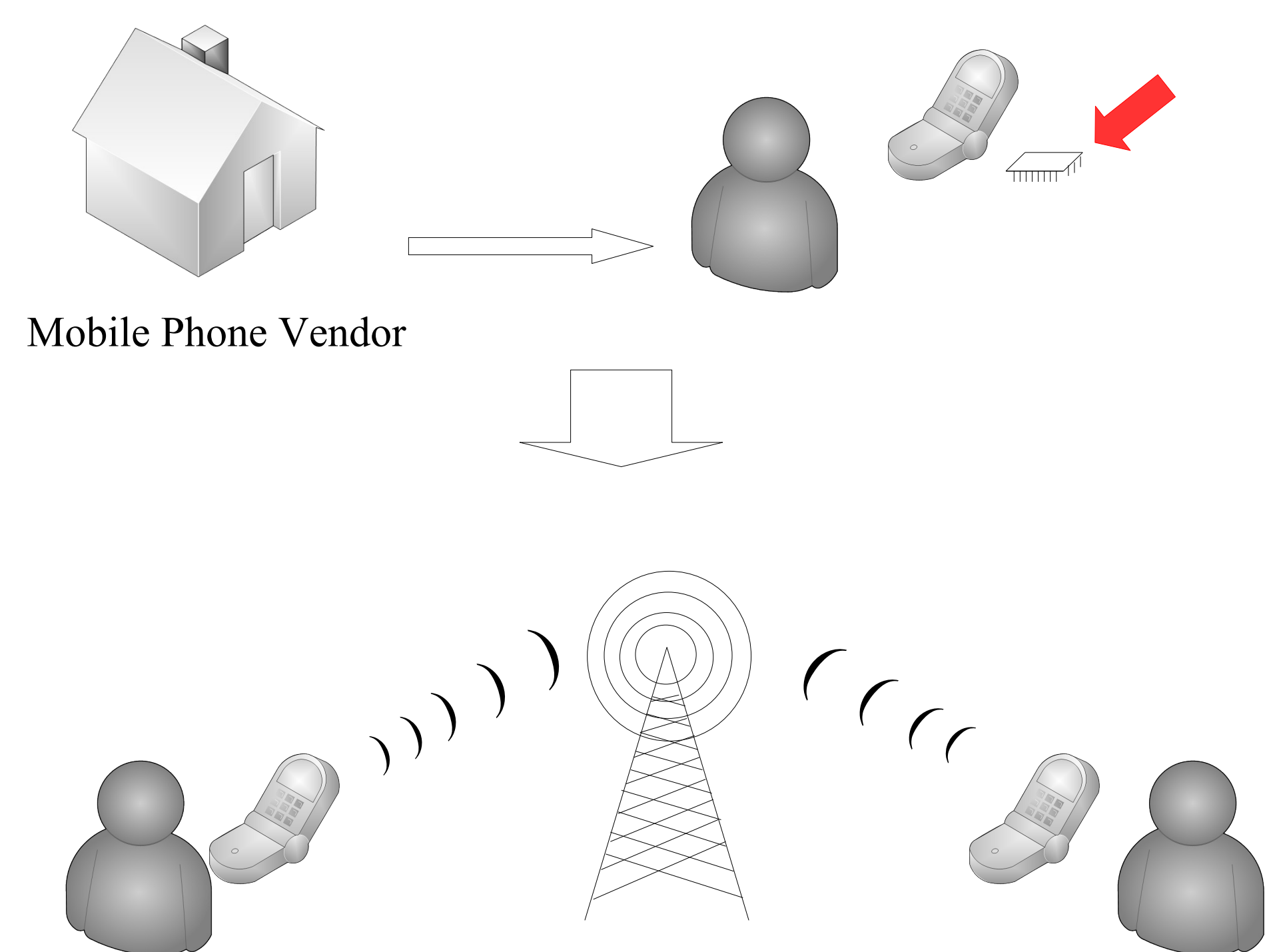
## Wireless Networks

This is completely different for 802.11 networks (WLAN). The 802.11 standard first only specified the data transmission details. That lead to the emergence of various different authentication protocols that are not compatible to each other. Beside the fact that those protocols do not scale very well, cannot be automated or are simply not secure enough, one of the biggest disadvantages from the user's point of view is that they have to be configured manually, which is usually not an easy task.



## Wireless Network with TPM Authentication

To enable GSM like comfort in 802.11 networks, we propose to use the EAP-TLS authentication protocol with an TPM extension. EAP is short for Extensible Authentication Protocol, like the name says, a very flexible authentication framework. Within this framework, it is possible to use already know authentication frameworks like simple username-password authentication or the Transport Layer Security protocol (TLS). For our purposes the EAP-TLS implementation is the best choice as it is a very scalable and secure mutual authentication protocol. TLS requires certificates, also on the client side when using mutual authentication. Everybody who has already tried to retrieve his own X.509 certificates knows, that this is rather complicated process. To ease this process, we use the Trusted Platform Module (TPM) shipped with the majority of the new PCs and notebooks. As the TPMs come with certificate infrastructure, the process of certification retrieval may be automatized like the whole authentication process. Doing so, we get an authentication protocol as comfortable as the GSM authentication.



## CONCLUSIONS

The TPM makes the difference! Using the Trusted Platform Module enables the users to access WLANs as simple as GSM networks. And just a final remark: TPMs are not really useful for DRM, that's just a rumour :-)