

# Mobile Signature



*Qualified electronic signatures carried out with the mobile phone*

## What it is

- Mobile phone based eID solution
- Server side qualified electronic signature using mobile phone

## Key features:

- No acquisition costs for smartcards or smartcard readers
- No software installation necessary (for middleware/ drivers etc.)
- Not specific platform/ system (Windows/ MacOS/Linux/....) required
- Increased usability due to the use of familiar technology (mobile phone)
- High security level

## Mobile signature

The citizen card is an essential component of [Austria's E-Government strategy](#) and approach. The [citizen card](#) concept offers functionality for the identification and authentication and – by using qualified electronic signatures – constitutes the foundation for legal security.

As the citizen card concept is built upon open standards, it allows all signature cards and storage mediums, which fulfil citizen card specifications and legal requirements to be used. The concept just determines certain standards in terms of functionality. There are no restrictions to the concrete, technical implementation as long as the legal requirements (such as usage of “secure signature creation devices”) are met. This fosters solutions in different technology sectors such as the mobile phone sector.

Starting in the fourth Quarter 2009 the so-called mobile signature will offer a comfortable alternative to the current smartcards. This server-based citizen card solution for qualified electronic signatures means a further important step towards usability and dissemination of modern E-Government services.

## Architecture/Technology

The mobile signature builds upon the two factor authentication approach as it is known from the smartcard concept – knowledge and possession. The sole control of the signature keys by the signatory was implemented by combining “knowledge” (the knowledge of a PIN) with “possession” (holding the mobile phone).

The server (hardware security module) safely stores the cryptographic keys. Apart from private keys and the corresponding certificates, some personal data (identity link structure) that are needed for authentication - are securely stored on the server. After registration citizens have to define a secrecy PIN which is used to decrypt and trigger the private key for electronic signature. Each time the server carries out a signature on behalf of a citizen the specific secrecy PIN has to be entered to unlock (decrypt) the private key. The signatory's PIN (a chosen password) is used as a factor to encrypt the signature keys, possession of the corresponding mobile phone gets proven by an ephemeral transaction number (TAN) sent via text message (SMS). The ephemeral TAN is valid for a couple of minutes only. This procedure ensures that the private key is under the sole control of its owner.

