

Mobile PKI Trial

for Vodafone UK



Short description

The wireless PKI technology is seen to be a crucial foundation for secure mobile commerce applications. Therefore customers like Vodafone UK wanted to use this trial installation as a first step to prove the efficiency and the unique security level of mobile signatures in real life. Radiocommunications Agency (RA), an Executive Agency of the Department of Trade and Industry (DTI) were Vodafone's partner in this trial in order to test the potential effects and advantages of electronic signatures for the UK Government.

The DTI trial participants (selected DTI employees) filled out their travel expense sheets on a secure Internet page, regardless of whether they were in the office or somewhere else. The form was electronically forwarded to the user and signed with the PKI functionality on the SIM card. The responsible manager then countersigned the submitted expense form. Provided with these two signatures, the form was then handled according to the standard procedures.

Operator benefits

- Generating new revenue stream with SMS traffic
- Offering registration and authentication services to 3rd parties such as banks or application providers
- Mobile PKI is fundamental for the offering of secure mobile applications
- Ease of service integration into existing workflow

G&D's scope of services and products

- Mobile PKI application on STARSIM® cards
- Design and implementation of PKI components and processes
- Consulting regarding security concept
- Data management architecture including subscriber registration process
- Key generation and management
- Acting as a non-commercial Certification Authority (CA) within this trail
- Integration of existing infrastructure with PKI processes and technology

Used technology

- STARSIM® browser with digital signature plug-ins
- SmartTrust Gateway DP5 plus signing and verification server

Detailed description

The DTI employee logs onto a secure, SmartTrust-developed web site imitating the DTI travel expense claim form. The predefined claimant's details, such as bank account and personal data, are already available with the logon so that the employee only has to fill out the variable part of the electronic form. At the end, travel expenses are automatically calculated.

After completion of the form, a message digest is calculated and sent to a predefined telephone number in order to request the digital signature. Using the STARSIM® browser card with integrated PKI functionality, the claimant can digitally sign the form with his signing PIN. This digital signature is validated in the Lightweight Directory Access Protocol (LDAP) server. If the validation is correct, a message is shown on the web site that the form has been signed successfully.

This way of performing a digital signature provides a strong user authentication including the non-repudiation of the form. The integrity of the data and the privacy fulfil the highest security level.

Network structure for mobile PKI trial for Vodafone UK

