



## Teleca Wireless Security Server™

*This WPKI solution enables secure identification and authentication using a mobile handset. The technology facilitates both web and mobile access without new devices. The SIM-Card in the users' existing handsets will be used, as well as the future ones. Teleca has, together with a number of banks and operators, proven this concept in the Scandinavian market.*

### Goal

Today's information society continues to develop in tact with the maturation of information technologies. Several of the most interesting applications to date are based on Internet and mobile technology. These applications are already used for many sorts of communication, i.e., transactions, information, the provision of public services, and so on.

Continued development of these services and development of new ones require confidence in the services themselves as well as their underlying security. We need feel secure that the information is correct, that the right person has access to it and that others are prevented from accessing it. The tools we use are electronic identification and signatures. As our way of living becomes more and more mobile, we need a solution that combines mobility and security.

### The TWISS Approach

The Teleca Wireless Security Server (TWISS) is a hard key PKI-solution based on existing infrastructure (mobile phones, SIM-cards, mobile Internet access) open and widely accepted standards from OMA (Open Mobile Alliance) on WAP, WIM, etc. Our value proposition contains both professional services and software. We support you with the following professional services:

### Services

- The business framework of the mobile identification services
- Specification of functional and technical interfaces
- Systems integration and development
- End-to-end test and validation of the identification service

### Software

The functionality of the TWISS software includes:

- Generating and converting content (wml and wmlscript pages) for the terminal (security channel) to consume
- Handling and binding a session with a mobile terminal (security channel) to a session within the information channel (PC, digitalTV, etc). This binding ensures that it's the same person interacts trough both sessions
- Communicating with certificate issuers to request the certificate pointed to by the URL form of certificate info that may be present in signatures. This includes the ability to authenticate itself securely during such transactions if required
- Communicating with certificate issuers to request revocation information

*Teleca is an international IT services company focused on R&D that develops and integrates advanced software and information technology solutions. With in-depth expertise in the latest technology and profound industrial knowledge, Teleca helps technology- and software-intensive customers worldwide to strengthen their market position and shorten their time to market. The company has more than 3000 employees with operations in 15 countries in Asia, Europe and USA. Teleca is quoted on the Attract40 list of Stockholmsbörsen (Stockholm stock exchange).*

### Technical data

TWISS is completely built in Java and can be run on J2EE standard application servers like BEA, Websphere, Tomcat etc...

TWISS supports the following platforms

- Windows
- AIX
- Sun Solaris
- HP-UX

The architecture makes it fully compliant with the OMA WPKI 1.0 and the guidelines from Liberty Alliance.

Teleca Wireless Security Server includes:

- Server software
- Java package for integration in existing server
- Integration toolkit including components for - Java, Microsoft COM objects, C#, VB, .Net, and Web Services
- Well documented API
- Reference manual
- User's guide

### Contact

Contact your local salesperson or see <http://www.teleca.com/> and look up the contact persons in the operators section.

