Isbank Protects Mobile Online Banking with One-Time Passwords

Turkish Bank Provides Customers with SecOVID Tokens

Worms/Germany, January 04, 2006. Isbank now offers secure mobile online banking with the German vendor Kobil Systems’ one-time password solution SecOVID. Since September, the bank has been providing many of its customers with SecOVID tokens, allowing them to generate passwords for registration together with their PIN. This so-called two-factor-authentication (possession of the token and knowledge of the PIN) protects against phishing or similar password spying. User identification with one time passwords is part of Kobil’s Future Banking range of offer to protect online banking. In a pilot operation phase, Isbank is currently using another Kobil Future Banking solution, the PKI-based authentication with smart cards.

Founded in 1924, Isbank is the first central bank in Turkey and, with about 850 branch offices, one of the largest banks in the country. To enable secure online banking for their customers, the bank offers the one-time password system SecOVID for access protection. The bank has already provided 40,000 customers with the SecOVID tokens, which are available for a one-time fee. With these mobile end devices, customers can generate one-time passwords to log on to the bank server. Such passwords, which are only valid once, are much more secure than static passwords, which can easily be spied and then used abusively. For the future, access with soft tokens over mobile phones or PDAs is also planned.

Protection with one-time passwords consists of two main components: On the user side an authentication device, a PIN, for example a token, a Smart Card and a card terminal, a PDA or a handy is needed. The second component is the server which consists of a software and an administration tool for user administration. The user receives a numerical code from his authentication device, which was calculated on the basis of a 3DES-algorithm. This code is only valid once. Should anyone try to use the one-time password a second time, access is denied. This means, an attacker can’t use a sniffed or spied password. When the user enters his one-time password into the user interface, it is encrypted and then forwarded to the server via the network device (for example VPN or web server). The server checks the password and if it is correct, the user can access the network. Token and Smart Card are using an algorithm and values, that are synchronised with the one-time password server, to allow the server to verify the password. The server takes on the verification of the one-time passwords (authentication), the administration of the user rights (authorisation) and the logging of the access trials (accounting).

About Isbank:
The Isbank was founded in 1924 shortly after the Turkish Republic came into existence. It is the first central bank and one of the most reliable banks in Turkey. The bank globally counts among the largest corporations. In 2004, the company had a total of 29 billion Dollars in assets. Since its foundation, the Isbank is listed on the Stock Exchange and is being dealt at the Istanbul as well as London Stock Exchange. The bank has more than 850 branch offices all over Turkey as well as abroad.

http://www.isbank.com.tr

About KOBIL Systems:
Founded in 1986, Kobil Systems GmbH is a provider of high-security base technology in the environment of smart cards, one-time passwords (OTP) and certificates. Kobil’s objective to provide security without limitations, simply, anywhere and at anytime, has been achieved through years of research and development. The company offers its customers not only patented base technology, but also the required comprehensive professional expertise to facilitate, in co-operation with its technology partners, the easy-to-use and at the same time totally secure use of digital identity.