

Security in Hand

MobileID™

mobile, two-way and two-factor authentication

MobileID transforms mobile phones, PDAs and PCs into One-Time Password (OTP) token devices, providing enterprises, banks, online service providers and retailers with a cost-effective means to provide strong authentication protection to their customers, business partners and employees without deploying additional, dedicated hardware tokens.

One-Time Password tokens provide a secure and easy to use authentication solution, but traditional solutions require users to carry a dedicated hardware token for each application that they use. MobileID transforms an existing mobile device into a security token, eliminating the need for consumer and enterprise users to carry additional and multiple dedicated hardware tokens. In addition to two-factor authentication, MobileID also delivers two-way authentication. Traditional OTP authentication is one way only – the user authenticates their identity to the application provider. One-way authentication cannot prevent phishing or spoofing attacks whereby a fraudulent website attempts to steal users' identities by masquerading as a legitimate commercial website.

MobileID works with any JAVA enabled mobile phone, including Windows Mobile for Smartphone and PocketPC, RIM Blackberry, Symbian OS and Palm OS. A MobileID Desktop Edition is also available which supports Windows 2000/XP and Vista.

MobileID is the most cost effective way of providing a secure two-factor authentication solution.

KEY FEATURES

2x2 Authentication

Unlike other OTP token-based authentication solutions that offer only one-way authentication, MobileID delivers a strong two-way and two-factor authentication(2x2) - the user and the service can be mutually authenticated. In the authentication process, a pair of one-time passwords (OTP) is used to authenticate the user to the service as well as the service to the user.

MobileID is the only product in the market today that provides an OTP-based, two-factor and two-way authentication solution.

Challenge & Response

MobileID can also be configured as a Challenge-Response device, whereby the user is asked to enter a Challenge Code given by any service application, after which the MobileID generates a Response Code to be used to authenticate the user to that service. Challenge-Response authentication provides additional security to the simple OTP authentication.

Digital Signature

MobileID provides confirmation of transaction details by using a digital signature which provides high assurance that the submitted transaction has been authorised by the user and that the transaction has not been modified en route by impostors since the authorisation, by Man-In-The-Middle or Session Hijack attacks.



PIN Protected

MobileID token is protected by enhanced security features. In the case of the user's mobile phone having been lost or stolen, an additional PIN can be set by the user to stop the MobileID from being operated by unauthorised persons.

Multiple Tokens

MobileID is designed to allow one mobile device to be used as a token generator for any number of online services, applications or products, so that users do not need to carry different tokens for different products.

Dual Algorithms

MobileID supports both event-based and time-based one-time passwords.

OATH Compliant

MobileID is consistent with the reference architecture set forth by the initiative for Open AuTHentication (OATH) and compliant with the OATH HOTP algorithm proposed as a standard within the IETF.

KEY BENEFITS

User Friendly

Mobile phones have become an inseparable part of peoples' lives. Using the mobile phone as a secure token frees the users from carrying dedicated token device. MobileID is the ideal replacement to the conventional one-time password hardware tokens.

Cost Effective

MobileID utilises existing devices that users already have, mobile phones, eliminating the need to purchase and deploy additional new hardware tokens, or replace lost and damaged hardware tokens. MobileID is the most cost effective one-time password token in the market.

Easy to Deploy

MobileID is extremely easy to deploy—it can be deployed over the air onto the user's mobile phone with one SMS message. For enterprise applications, MobileID tokens can also be downloaded onto mobile phones via Bluetooth on the corporate network.

Multiple Solutions

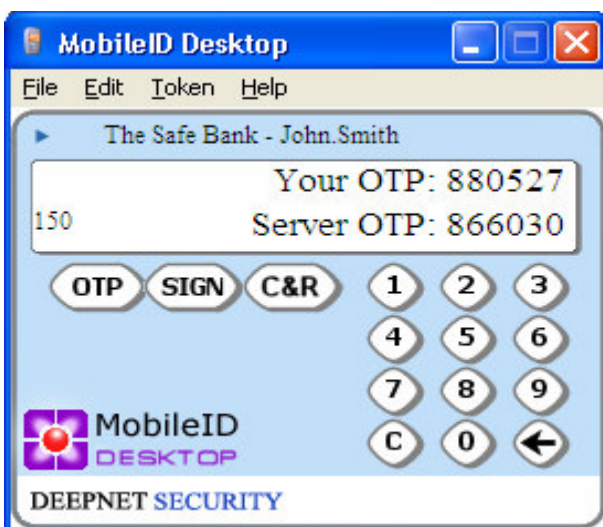
MobileID is supported by the Deepnet Unified Authentication Platform that provides token registration, provisioning, and lifecycle management functions. With Deepnet Unified Authentication Platform, MobileID can be used to provide two-factor authentication for a wide range of enterprise and web applications, including:

- Windows Network Logon
- Windows Remote Desktop
- IPSec VPN Logon
- SSL VPN Logon
- Microsoft Outlook Web Access
- Citrix Web Interface

MobileID is the ideal two-factor authentication solution for enterprise and consumer applications

"The growth of mobile computing combined with the rise in malicious attacks, especially the mounting concern over identity theft and phishing, has increased the need for strong authentication for remote access, user login, and single sign-on... OATH-compliant soft token solutions extend two-factor authentication support through devices that are in common use, such as mobile phones, PDAs, and PCs, which could help to extend this level of security to a broader audience of users."

Joe Greene, VP IT Security Research, IDC.



MobileID is available for:

- JAVA enabled phones: J2ME 1.1 or later;
- RIM Blackberry 3.6 or later
- Palm 5 or later
- Symbian 4 or later
- Windows Mobile for Pocket PC 2003/2005 or later
- Windows Mobile for Smartphone 2003 or later
- Windows Desktop: Windows 2000/XP or later