

Deepnet Unified Authentication

Two-Way and Two-Factor Authentication for Windows Logon

The use of strong authentication instead of traditional static passwords to access a Windows network is a necessary critical step to protect enterprise's most critical information assets and valuable data. Unfortunately, most existing strong authentication solutions require additional hardware devices such as smart cards, USB keys or One-Time Password (OTP) hardware tokens, which are expensive to implement, deploy, manage and very inconvenient to the users.

Achieving the right balance of authentication security, without compromising the user experience or the bottom line, has always been a challenging task for businesses.



Deepnet Unified Authentication Platform for Windows Logon is a two-factor authentication solution designed specifically for Windows network, without the requirements of new hardware devices. Deepnet Unified Authentication Platform utilizes the devices users already have (computers, mobile phones, PDA etc) or the user's behavioural biometrics (typing pattern, voiceprint), as the second factor. This eliminates the need to distribute new hardware, making the system cost effective, user friendly and simple to manage.

With the built-in RADIUS component and the support for Microsoft Active Directory, Deepnet Unified Authentication Platform for Windows Logon can be easily integrated with the customers' existing IT infrastructures.



The screenshot shows the Windows XP logon screen with the following elements:

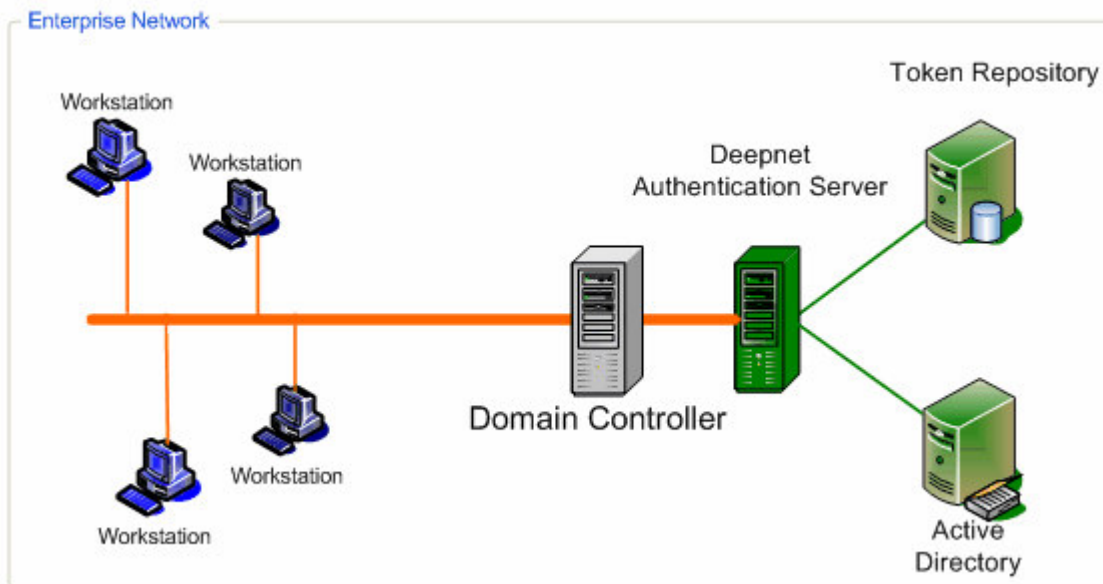
- Title Bar:** Log On to Windows
- Header:** Microsoft Windows XP Professional logo and copyright information (© 1985-2001 Microsoft Corporation).
- Authentication Section:** A box titled "Authentication by Deepnet Security" with a red and blue icon.
- Fields:**
 - User name: J.Smith
 - Authenticator: Mobile 2x2 (dropdown menu)
 - One-Time Password: 686428
 - Account Password: masked with dots
 - Log on to: ACME (dropdown menu)
- Buttons:** EN, OK, Cancel, Shut Down..., and Options <<

Key Benefits

- Provides a user-friendly and cost-effective strong authentication solution.
- Eliminates password-only related vulnerabilities.
- Manages user account centrally through the Management Console.
- Improves productivity without compromising security.
- Offers flexible choices of authentication credentials and tokens.
- Unifies authentication for all enterprise applications with a single platform.

Technical Specification

Deepnet Unified Authentication Platform for Windows Logon consists of the Windows Domain Controller, Deepnet Authentication Server, Token Repository server and Active Directory server, as illustrated below.



Deepnet Authentication Server and its Token Repository (SQL Server) can be installed and operating on separated machines or on a single machine, depending on the scale of the customer's enterprise network.

Domain Controller

Deepnet Unified Authentication (Windows Logon) supports Microsoft Windows 2003, Windows XP and Windows 2000 servers.

Deepnet Authentication Server

Deepnet Authentication Server is a secure, scalable, cross-platform authentication server that centrally controls access to enterprise networks. Deepnet Authentication Server is designed to be deployable across a wide range of commonly available platforms that supports Java. Therefore, it can run on virtually any operating systems including Windows, Linux, Unix and Sun OS.

Token Repository

Deepnet Authentication Server uses a SQL database server as its token repository. It can be connected to the customer's existing SQL server (MS-SQL 2000/2003, Oracle) or MySQL server which is included in its installation package.

Active Directory

Deepnet Authentication Server supports assignment of tokens to users residing in Active Directory without modification of the directory schema. User data is not imported from the directory into Deepnet Authentication Server. Instead, Deepnet Authentication Server queries the directory during the authentication process to validate the user's status. Changes made in the directory are automatically and immediately reflected in Deepnet Authentication Server.

Authentication Methods

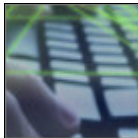
Deepnet Unified Authentication Platform supports several authentication methods including mobile phone based one-time password token, device based soft token, virtual smart card and software-only behaviour biometrics.



Mobile 2x2 is a one-time password token application. It is a small J2ME application downloadable to any Java enabled mobile phones, including Windows Mobile, RIM Blackberry, Symbian OS and Palm OS. Mobile 2x2 also supports Windows desktop. Its Desktop Edition runs on Windows 2000/XP and Windows Mobile.



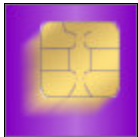
Mobile Pass is also a one-time password solution. While Mobile 2x2 generates one-time password offline, Mobile Pass delivers one-time password in real time via SMS, email or voice over the phone. Mobile Pass works with any mobile phone.



TypeSense. Based on the Keystroke Dynamics science, TypeSense accurately identifies users by their “type prints” - the unique patterns they type characters across a keyboard. TypeSense requires no hardware and no software installation.



VoiceSense is a text and language independent biometric speaker verification system that also requires no hardware and no software installation. Voice can be received from the user’s mobile phone, landline telephone or computer microphone.



Smart ID is a virtual smart card in a software form factor, providing the same advanced security functionality as physical smart cards, but at only a fraction of the cost. Smart ID is fully compliant with PKI architecture with supports of PKCS #11 and MS-CAPI. Smart ID is available for Windows 2000/XP and Windows Mobile.



Device Pass is a software-based two-factor authentication solution based on patent-pending device fingerprinting technologies. Device Pass client is available for Windows 2000/XP and Windows Mobile.