

Deepnet Unified Authentication

Two-Way and Two-Factor Authentication for Web Applications

In today's online business world, plagued by phishing, pharming, keylogging, spoofing, man-in-the-middle attacks and other forms of online scams, passwords are no longer sufficient to protect businesses and their customers. Implementing a strong, multi-factor and mutual authentication solution is essential for businesses to minimise the risk of financial loss and to restore consumer confidence.

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.



Deepnet Unified Authentication Platform (Internet Edition) is a two-way and two-factor authentication solution designed specifically for web applications such as online banking, shopping and gambling etc., 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, voice-print), as the second factor. This eliminates the need to distribute new hardware, making the system cost effective, user friendly and simple to manage.

Deepnet Unified Authentication Platform is designed for simple integration with existing web applications and their customer management systems. The architecture and inter-faces are designed to minimise modification to the customers' existing IT infrastructures and application frameworks.

❁
The Safe Bank

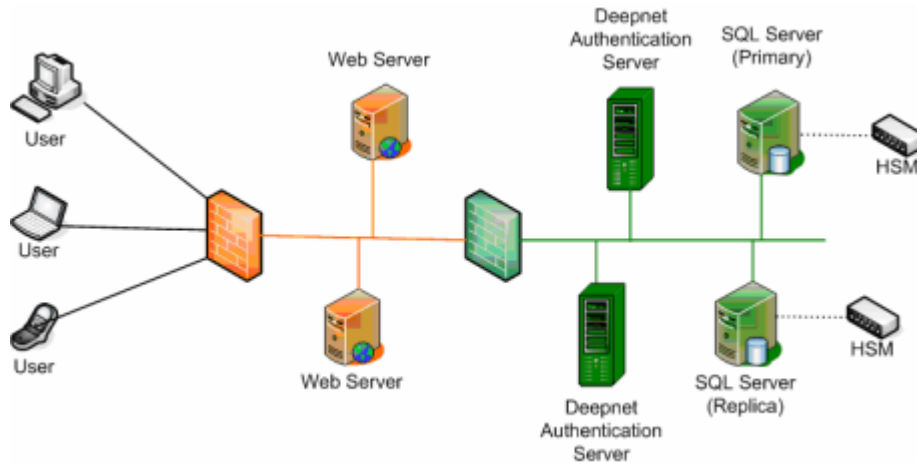
Personal Business Commercial	<div style="display: flex; justify-content: space-between;"> <div style="width: 60%;"> <h3 style="margin: 0;">Logon</h3> <p style="color: red; font-weight: bold; margin: 5px 0;">Please confirm that your site stamp and image signature are correct before you enter your password</p> <p> Password: <input style="width: 150px;" type="password"/> </p> <p style="text-align: center;"><input type="button" value="Sign In"/></p> </div> <div style="width: 35%;"> <h3 style="margin: 0;">Your site stamp</h3>  </div> </div>
<div style="display: flex; justify-content: space-between;"> Copyright (c) 2006 The Safe Bank Authentication by Deepnet Security </div>	

Key Benefits

- Two-Factor Authentication
- Two-Way Authentication
- No Hardware
- No Software
- Easy to Integrate
- Quick to Deploy
- Simple to Manage
- User Friendly
- Cost Effective

Technical Specification

The authentication platform consists of one or many Web Servers, Deepnet Authentication Servers, SQL Servers and optional Hardware Security Modules (HSM), as illustrated below.



These servers can be installed and operating on separated machines or on a single machine, depending on the scale of the customer's business applications.

Web Server

Deepnet Unified Authentication platform supports all types of popular web servers, including Microsoft Internet Information Server (IIS, ASP, ASP.NET), Java Server Pages (JSP) and Apache Web Server.

Deepnet Authentication Server

Deepnet Authentication Server is a secure, scalable, cross-platform authentication server that centrally controls access to web applications. Deepnet Authentication Server is designed to be deployable across a wide range of commonly available platforms that supports Java. Therefore, it can run on Windows, Linux, Unix, Sun OS and many mainframes.

SQL Server

Deepnet Unified Authentication platform supports a wide range of high- performance SQL database servers, including MS-SQL, Oracle and MySQL.

HSMM

For additional security, the token database can be further protected by employing hardware encryption. Deepnet Unified Authentication supports Hardware Security Module (HSM) including Eracom ProtectServer, nCipher nShield and nethSM. Installation of HSM is optional, as Deepnet Unified Authentication has an in-built Software Security Module (SSM).

Authentication Methods

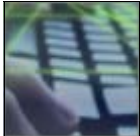
Deepnet Unified Authentication Platform supports several authentication methods including mobile phone based one-time password token, device based soft token, virtual smart card and software-only behaviour biometrics.



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.



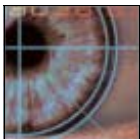
Smart ID is a virtual smart card in a software form factor, providing the same advanced security functionality as physical smart cards, but at only a fraction of the cost. Smart ID is fully compliant with PKI architecture with supports of PKCS #11 and MS-CAPI. Smart ID is available for Windows 2000/XP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



Smart 2x2 is a smart device token that requires a browser plug-in. Smart 2x2 is natively supported by Deepnet Explorer web browser, and its plug-in software is available for Internet Explorer and Firefox for Windows.



Remote 2x2 is a remote two-factor authentication solution that requires no hardware and no software installation. All the user needs is a standard web browser such as Internet Explorer, Firefox or Safari for Mac OS.



Site Stamp provides a simple yet effective way for users to sign and stamp websites that they trust. Site Stamp presents users with their own personalised images to ensure that they are communicating with the legitimate website and not a fraudster.