



100111000011100
110110001001010
101111000111000
111001110101010
101010100111001
100011010100110

Deepnet Unified Authentication

Maximum Security at Minimum Cost

Introduction

The Need for Strong Authentication

- Password Authentication
- Two-Factor Authentication
- Two-Way Authentication
- Transaction Authentication

The Barriers to Strong Adoption

- High Cost of Ownership
- Low User-Friendliness
- Lack of Interoperability
- Lack of Flexibility
- Lack of Scalability

The Need for Unified Authentication

The Deepnet Unified Authentication

- Single Platform
- Multiple Credentials
- Multiple Solutions
- Central Management
- Cross Platforms

Conclusion

- Technical Advantages
- Business Benefits

ID FRAUD AFFECTS 25% OF BRITONS

According to the UK consumer watchdog Which?, 25% of UK adults have had their identity stolen or know someone who has been affected by identity fraud.

The survey also reveals the alarming fact that only 1 in every 3 people shred bills, or safely dispose of them and use different passwords for their accounts.

Identity theft is one of the UK's fastest growing crimes. It is estimated that ID criminals defrauded Britons out of £1.3bn last year alone.

— BBC, March 2007

Introduction

These days, not a single day passes without a new story emerging about an identity theft or a network break-in due to stolen user credentials. With the expansion of network based applications, this trend is only going to continue. Unfortunately, the dominant authentication system in use today is based on the username and password. This relatively weak system is subject to a number of flaws, including notoriously poor user password choices, password harvesting via keylogging software, phishing attacks and other forms of identify theft.

The most common solution to these authentication problems is to use a two-factor authentication system. Two-factor authentication works by requiring both something you know and something you have. The 'something you know' is typically a password or PIN, and the 'something you have' is usually a hardware token.

Two-factor authentication systems are secure because it is very difficult to obtain possession of both factors. Even if an attacker manages to learn the user's password, it is useless without also having physical possession of the user's token. Conversely, if the user happens to lose their hardware token, the finder of that token would be unable to use it unless he or she can also obtain the user's password.

Organizations that wish to deploy strong authentication have a variety of methods from which to choose. These methods range from hardware or software based one-time password (OTP) tokens to biometric, smart card and PKI systems. However, no single solution has widely displaced the traditional username and password authentication because these solutions have been either expensive to implement or difficult to use.

To address these issues, Deepnet Security has introduced a new system for strong authentication. Based on the open authentication standard promoted by the Open AuTHentication (OATH) working group, the Deepnet Unified Authentication Platform provides a common, open standards-based platform for authenticating users and devices. Using this highly scalable platform, enterprises can deploy multi-purpose credentials that support Windows Network Logon, Virtual Private Networks, Outlook Web/Mobile Access, Citrix Web Interface and Internet Applications.

The solution reduces total cost of ownership (TCO) of strong authentication by as much as 60 percent by taking advantage of an enterprise's existing infrastructure, employing cost-effective tokens and enabling self-service management of common lifecycle tasks.

THE ERA OF PASSWORDS IS OVER

Passwords just don't work anymore. As computers have gotten faster, password guessing has gotten easier. Ever more complicated passwords are required to evade password-guessing software. At the same time, there's an upper limit to how complex a password users can be expected to remember. About five years ago, these two lines crossed: It is no longer reasonable to expect users to have passwords that can't be guessed. For anything that requires reasonable security, the era of passwords is over.

— Bruce Schneier

The Need for Strong Authentication

Until fairly recently it was sufficient for most computer users to identify themselves with a simple password: they entered a username, then provided the password associated with it.

One of the weaknesses of username and password is the fact that the password is static: it does not change from one authentication attempt to the next. Administrators may insist that passwords are changed every 3 months or even every month, however that still gives an attacker a significant amount of time to steal the static password.

Another issue with passwords is that users and helpdesk administrators want them to be easy to remember but IT managers and security managers want them to be difficult to guess. These requirements tend to work against one another. It is much easier to remember words than it is a series of random characters, but it is much easier to guess a word than a series of random characters.

One final weakness of username and password as an authentication model stems from the fact that username and passwords have been around for so long which has meant that there are many effective password-cracking and stealing software widely and freely available on the Internet.

All of the above means that password protection involves management resources as well as security risks. It is estimated that the cost of managing passwords is to be from \$75 to \$150 per user, per year which does not count lost productivity due to downtime as the user waits to access an application.



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers in May 2007.

Anti-Phishing Working Group.

PHISHING EXPLOITS ON THE RISE

Phishing is a form of social engineering in which criminals pose as legitimate entities in order to obtain personal information such as credit card numbers, account passwords and social security numbers from unsuspecting consumers. Typically, phishers use fraudulent websites or the email addresses of trusted brands in order to send spam email messages that dupe recipients into providing confidential data. They then use the personal information to commit credit card fraud, identity theft and other crimes.

Unfortunately, phishing attacks continue to rise at an alarming rate. According to the Anti-Phishing Working Group, in April 2007 there were 55,643 new phishing sites detected, which stayed live for an average of 3.8 days. Financial Services continue to be the most targeted industry sector at 92.5% of phishing sites detected.

Two-Factor Authentication

In a world plagued by various forms of password-theft attacks such as keylogging spywares, phishing emails and spoofing websites, it becomes increasingly clear that the single-factor authentication system relied on the username and password does not provide sufficient protection for many businesses and their customers.

A two-factor authentication system requires at least two of the three universally recognized authentication form factors:

- 'Something you **know**', such as a password or PIN.
- 'Something you **have**', such as a smart card or hardware token.
- 'Something you **are**', such as a fingerprint or a retinal scan.

Common implementations of two-factor authentication use 'something you know' (a password) as one of the two factors, and use either 'something you have' (a physical device) or 'something you are' (a biometric such as a fingerprint) as the other factor.

A real application of two-factor authentication in everyday life is withdrawing money from an ATM. The user is required to enter their card in the ATM (something they have) and then type their PIN (something they know).

Strong, two-factor authentication helps prevent identity theft because it is very difficult for attackers to obtain possession of both factors. Strong authentication addresses the need for advanced levels of identity verification and is essential for protecting online businesses and preserving confidence in ecommerce and communication.

Top 4 reasons to embrace two-factor authentication

1. Password is not safe

Security professionals have long known that password authentication is not secure, but that concern has been mostly theoretical until now. With the rising tide of phishing, keylogging and other large-scale organized criminal attacks that exploit the weakness of passwords, the Internet must quickly move to a higher level of security.

2. Risks are Increasing

The rapid rise of phishing attacks in recent years is the evidence that hackers are now money driven. There are many ways for them to make money with stolen information with very little risk of being arrested. Defence in depth is required and two-factor authentication should be used to protect both businesses and consumers .

3. Customer Confidence

The prosperity of e-commerce and e-banking is being undermined by user insecurity and overly complex security process, as a result of attempting to combat against the fast growing phishing attacks. Implementing an effective two-factor authentication system can minimise the risk of financial loss as well as restore customer confidence.

4. Compliance & Regulation

Increasingly companies are deploying two-factor authentication because they are forced to. The credit card companies are requiring merchants and payment processors to meet the PCI Data Security requirements, which require two-factor for remote access to their networks. Banks are subject to the FFIEC guidelines which require online banks to adopt a variety of multi-factor authentication measures to secure online access to account information and transaction functionality.

FFIEC COMPLIANCE

The Federal Financial Institution Examination Council (FFIEC) guidelines require online banks to adopt a variety of multi-factor authentication measures to secure online access to account information and transaction functionality. The FFIEC issued these highly visible guidelines in response to increasingly sophisticated electronic attacks that compromise personal identity information and erode customer confidence in online banking security. If you are a financial institution, you risk regulatory non-compliance penalties and customer defections from online services if you fail to deploy solutions that meet FFIEC guidelines.

Two-Way Authentication

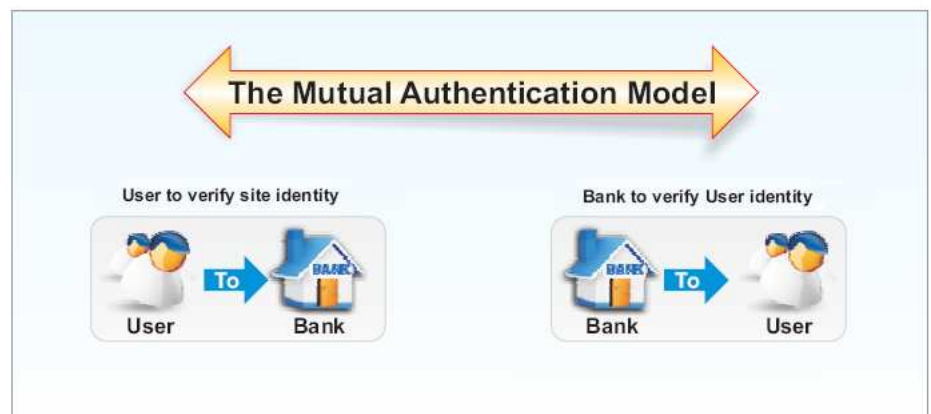
While two-factor authentication system offers much better security than the single-factor, password-based authentication, unfortunately it alone does not protect against advanced attacks. Particularly the so-called Man-In-The-Middle attacks.

A Man-In-The-Middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. In a MITM attack, the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it.

Phishing is essentially a MITM attack. The user is misdirected, for example by social engineering or DNS poisoning, to a fraudulent site. To prevent phishing consistently requires strong mutual (two-way) authentication - validating the server to the user and the user to the server.

As the FSTC wrote in its January 2005 report*, "Better institution-to-customer authentication would prevent attackers from successfully impersonating financial institutions to steal customers' account credentials; and better customer-to-institution authentication would prevent attackers from successfully impersonating customers to financial institutions in order to perpetrate fraud."

Mutual authentication is really site authentication to the user combined with user authentication to the site. Site authentication is currently provided by SSL certificate. However, the SSL certificate may prove the legitimacy of the website. It does not necessarily prove the website's authenticity. Furthermore, many users rarely check SSL certificates for validity or do not understand how to validate SSL certificates. Fraudulent websites can use self-issued SSL certificates to fool users or generate a fake SSL "padlock" and position it over the padlock location in the web browser. Recently, there have been numerous phishing attacks utilizing SSL certificate padlocks. SSL site authentication is clearly compromised. Something more secure and easier is needed.



*"Understanding and Countering the Phishing Threat". Financial Service Technology Consortium, January 2005

Transaction Authentication

Like any wars between Good and Evil, the good guys always find a way to win. Yet the bad guys always seem to be able to find a new way to terrify the world once again. As businesses implement two-factor authentication to protect user's login sessions, attacks are evolving from phishing for users' login credentials to stealth Man-In-The-Browser (MITB) attacks that intercept and modify transactions.

Man-In-The-Browser (MITB) attack is a newly discovered variant of Man-In-The-Middle (MITM) attack that waits until users log in, to strike. This type of attack defeats previous user authentication. Hackers modify data transmitted during a legitimate session, without the user knowing until it's too late. For example, users could unknowingly transfer a large sum of money directly into a hackers' account.

Gartner Research VPs Avivah Litan and Ant Allan wrote, "MITM attacks can modify customer-generated transactions or generate new transactions; phishing/pharming directs a customer to a bogus server that completes the connection to the bank's server. The man 'in the middle' might actually be in the customer's PC: Trojan software can create a hidden browser session and generate transactions on the back of a legitimate strongly authenticated session..."*

Some existing systems for authenticating online transactions, such as manual phone calls and dedicated hardware token devices, have failed to be adopted widely. This is because they are difficult to use and deploy, require dedicated single-use hardware devices or simply cost too much.

Some other systems authenticate transactions by asking users to authenticate themselves again using two-factor authentication such as one-time passwords. This type of transaction authentication does not prevent MITM attacks, as it authenticates only the user instead of the data of the transaction. The only way to defeat the MITM attacks in online transactions is to digitally sign the transaction data in a out-of-band channel.

Financial institutions currently rely on longer payment clearance windows to catch fraudulent activities. With less time to detect fraud after the fact, financial institutions will need fraud prevention measures in the form of strong user and transactions authentication to make payments faster and more secure.

* "Transaction Verification Complements Fraud Detection and Stronger Authentication". Gartner, September 2006.

The Barriers to Strong Adoption

A variety of strong authentication products, ranging from OTP tokens, PKI smart cards to biometrics etc, have been available in the market for a couple of decades. However, despite the strong need for strong authentication, there is no single solution that has been widely adopted to displace the traditional password authentication. High cost of ownership, low user-friendliness, lack of interoperability, lack of flexibility and lack of scalability have been key impediments.

High Cost of Ownership

Traditionally, strong authentication solutions rely on specialised security hardware devices such as OTP tokens, smart cards and biometrics reader and scanners. These hardware devices are not only expensive to produce they are also costly to provision, administer and support, resulting in high cost of ownership.

Hardware token cost can be classified into four categories:

- Purchase Cost
- Provision Cost
- Replacement Cost
- Renewal Cost

Purchase Cost. Conventional security tokens are single-purpose hardware devices dedicated to user authentication only. Needless to say, they are expensive to purchase.

Provision Cost. Hardware tokens must be physically dispatched to the users. There are various costs incurred in the deployment of tokens including administration, registration and delivery.

Replacement Cost. Hardware tokens can be easily lost or damaged. On average, about 10% of hardware token device are lost or damaged before they reach the end of their lifecycle.

Renewal Cost. Hardware tokens typically expire in a three to five year period.

Low User-Friendliness

Apart from the cost, one of the other major barriers to the adoption of existing hardware token-based authentication solutions is the requirement for users to carry a physical device at all times. Carrying a single-purpose hardware device is not only inconvenient but also resented by many potential users. As a result, many users leave their security tokens on their desktop or even attach tokens to laptop computers, simply defeating the purpose of two-factor authentication.

Lack of Interoperability

Different business applications require different levels of security. Some application involve highly sensitive data or high-value transactions, therefore require the top-level security. In some other applications, however, a medium-level security might just be adequate enough.

To accommodate diverse security requirements, enterprises often deploy multiple authentication systems. Unfortunately, existing authentication products are mostly built on proprietary hardware and software technologies. They do not interoperate easily with the products of other vendors. This lack of interoperability prevents deployment of cost-effective, user-friendly solutions. Enterprises have to repeat investments into separate solutions and users have to learn to use multiple products. This limitation forces enterprises to depend heavily on a single vendor that has no incentive to reduce cost or drive innovation over time.

Lack of Flexibility

Different users have different lifestyles, hence desire different forms of credentials. Employees who need building-access security and strong network-access security may favour a combination of RFID smart card and OTP token. Marketing and sales executives who travel frequently may prefer mobile phone-based OTP tokens. Consumers using online banking applications may favour the simplicity of token-less security.

Most of today's authentication products offer only one type of credential, making it impossible for enterprises to provide choices of authentication methods to their employees, business partners and customers. This lack of flexibility is another major barrier for enterprises to adopt strong authentication.

Lack of Scalability

For strong authentication to be widely adopted to secure large-size enterprise and consumer applications, it has to be highly scalable.

The majority of existing authentication solutions are stand-alone, requiring user data to be duplicated and synchronised across applications and networks. To process and maintain the large number of user accounts and user credentials, data duplication and synchronisation require tremendous computing power as well as significant labour resources. Managing multiple systems and creating the infrastructure to support high performance, high availability and rapid growth of data directories is a complex, time-consuming and costly task.

The Need for Unified Authentication

In today's world of remote workers, mobile users, business partners, customers and hackers, the infrastructure of access control is being redefined. Enterprises therefore have to provide various methods to facilitate access to their enterprise network.

You are looking for effective and efficient ways to control the access to a wide range of business application:

- Windows network logon
- Outlook Web/Mobile Access
- VPN Remote Access
- Citrix Web Interface
- Web-based applications

You want to provide flexible, user-friendly authentication methods to a wide range of audience:

- Employees in the office
- Contractors on the hot desk
- Remote workers at home
- Mobile users on the move
- Business affiliates
- Business partners

You are looking for a secure and versatile authentication platform that can protect your business and users against a wide range of attacks:

- Keylogging
- Phishing
- Pharming
- Spoofing
- Man-In-The-Middle
- Man-In-The-Browser

You want a single, all-in-one authentication platform that provides unified interfaces and management services that work across all forms of strong authentication:

- Two-factor authentication
- Two-Way authentication
- Transaction Authentication

You want one single enterprise authentication platform that offers greater control and flexibility in determining in real-time how to secure different users and their connectivity based on the risks associated with the information they are accessing and transactions they are performing. You are also looking for more cost-effective alternative to the expensive, traditional two-factor authentication tokens such as RSA SecurID tokens.

What you are looking for is a unified authentication platform.

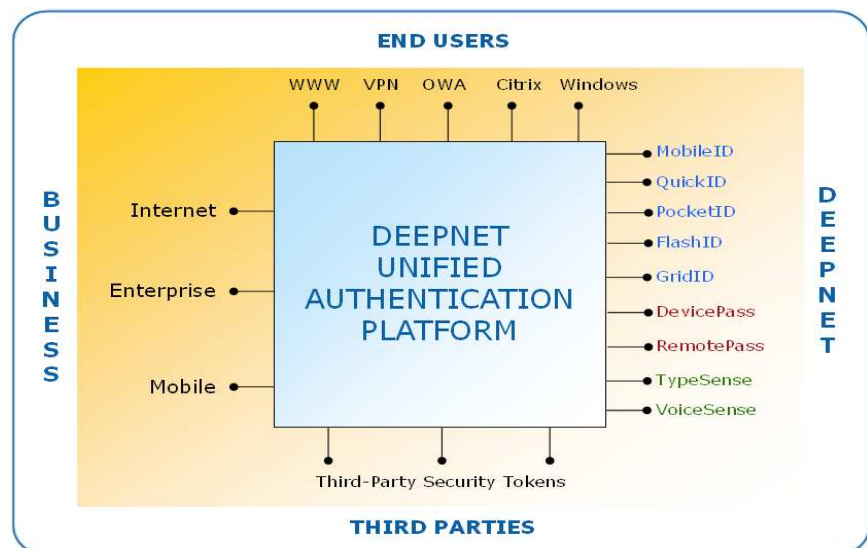
The Deepnet Unified Authentication

Deepnet Unified Authentication is the only authentication platform that meets all requirements of unified authentication. It enables you to deploy strong authentication across your diverse users, devices, applications and transactions. It enables you to apply the right level of authentication tailored to the risk associated with the connection and actions that a user is performing. It enables you to offer choices of authentication methods that match the lifestyle of modern users, encouraging widespread adoption of strong authentication.

Single Platform

Through one single platform, Deepnet Unified Authentication provides a rich set of user credentials and authentication methods including OTP tokens, smart tokens, biometrics and device and website authentication. It enables business organisations to deploy strong authentication across Enterprise network, Internet and Mobile applications. It provides many out-of-the-box enterprise and web solutions such as VPN, OWA, Citrix and Windows Logon.

Deepnet Unified Authentication is an open authentication platform based on OATH's vision of universal strong authentication. It can support any OATH compliant security token devices of third-party vendors, as well as some proprietary security tokens such as RSA SecurID and VASCO DigiPass.

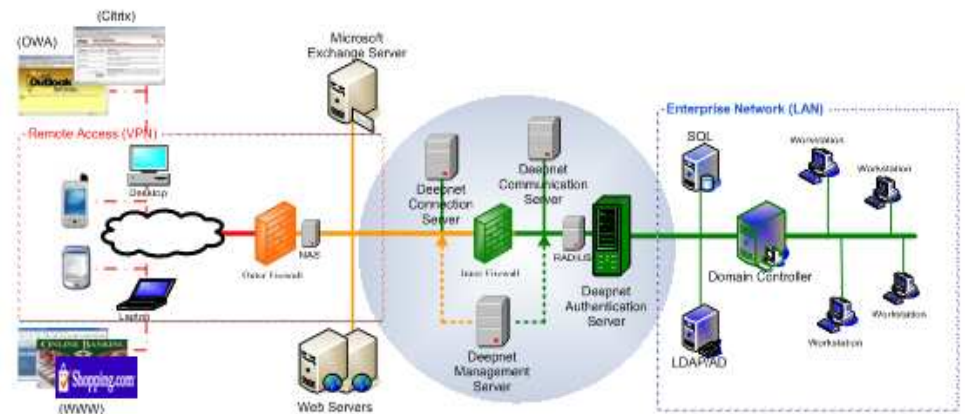


Architecture

Deepnet Unified Authentication Platform is designed for simple integration into the customers' existing IT infrastructures and application frameworks with minimum modification. Its architecture employs the 3-tier design consisting of Agents, Servers and User Directories.

The entire platform consists of the following components:

- Authentication Server
- Communication Server
- Connection Server
- Management Server
- Database Server
- Directory Server
- Hardware Security Module



Authentication Server

The Authentication Server centrally controls access to enterprise networks and web applications. It provisions and manages all user accounts and their credentials, devices and tokens.

Communication Server

The Communication Server is a gateway for the authentication server and the management server to communicate with the users via emails, SMS text messages and other communication channels.

Connection Server

The Connection Server is a gateway for the authentication server to communicate with authentication clients such as MobileID and TypeSense etc.

Management Server

The Management Server is a web-based, centralised management centre for the system administrators to manage applications, user accounts and tokens as well as system settings and audit trails etc.

Database Server

The Platform uses a SQL database as its user and token repository. It supports all popular SQL servers such as MS-SQL, Oracle and MySQL. The database can be software or hardware encrypted.

Directory Server

The Platform supports assignment of tokens to users residing in a LDAP directory, such as the Active Directory, without modification of the directory schema. User credential data is not imported from the directory, 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.

Hardware Security Module

For ultimate security, the database can be further protected by employing hardware encryption. The Platform supports Hardware Security Module (HSM) including Eracom ProtectServer, nCipher nShield and netHSM. Installation of HSM is optional, as the Platform has an built-in Software Security Module (SSM).

Multiple Credentials

Deepnet Unified Authentication Platform provides a rich set of user credentials and devices in various forms ranging from OTP tokens, PKI smart tokens, biometrics to token-less device authentications and image-based website authentication.

OTP Tokens



MobileID transforms any JAVA enabled mobile phone into an One-Time Password (OTP) token device, providing the most cost-effective OTP-based two-factor authentication solution. MobileID is an ideal replacement to the conventional one-time password hardware tokens.



QuickID turns any mobile phone into an authentication token by sending one time password via SMS text message to the mobile phone.

QuickID is the quickest and simplest way of providing a secure two-factor authentication solution.



PocketID is an OTP token in the form factor of a plastic card - the same size as a credit card. It can be easily carried in your pocket or wallet. For banking customers, it can be combined with your existing credit cards or bank cards. For enterprise customers, it can be combined with your employee identity smart cards.

PocketID provides the perfect balance between security and portability.

Deepnet Unified Authentication

Maximum Security at Minimum Cost



SafeID is a compact security device that generates one-time passwords (OTP) with a single press on a button. It enables the users to logon to secure applications safely and securely, such as VPN remote access, windows logon and online banking.

Unlike conventional security tokens that often expire in 3 to 5 years, Deepnet SafeID never expires as it is empowered by a renewable battery, offering a very high return of investment.



FlashID intelligently transforms the standard USB flash drive into a security token, which can then be used in any applications where two-factor authentication is required.

FlashID provides a more cost effective hardware token-based authentication solution than the conventional dedicated hardware token.



GridID is a simple, effective, two-factor and two-way OTP authentication method based on security grids. These security grids are typically printed on credit card-sized cards that can be easily carried in user's wallets, or they can be printed on the back of employee access badges, credit cards or ATM cards.

Unlike other grid cards that are not protected when lost or stolen, Deepnet GridID can be protected with a PIN or password.

Biometrics



TypeSense is a software-only biometric authentication based on typeprint recognition that uses keystroke dynamics to accurately identify a user by their typing rhythm and pattern.

TypeSense provides dependable, immediate and unobstructed access to online accounts at any time and any place. It is handy, reliable, low-cost, easy to implement and use.



VoiceSense is a text and language independent biometric speaker verification system that verifies the speaker's identity in real time using a simple spoken phrase. The ubiquitousness of computer microphone and mobile phone makes the voice authentication an ideal two-factor authentication solution for enterprise, online banking and telecom applications.

Deepnet Unified Authentication

Maximum Security at Minimum Cost

Device Authentication



DevicePass creates a unique “deviceprint”, a digital fingerprint of the device, using the device’s hardware characteristics including the hard disk ID, CPU serial number and network MAC address etc.

Combining the deviceprint with a user name and password, online and enterprise applications can restrict access to only trusted devices and authenticated users.



RemoteID can identify an online user by remotely fingerprinting the user’s PC device without installing any additional end-user software.

RemoteID delivers a low-cost two-factor authentication solution for mass-market web applications such as online banking and ecommerce websites.

Smart Tokens



SmartID is a 3-in-1 solution that combines virtual smart card, plug-and-play USB flash drive and TPM (Trusted Platform Module) security chip, providing the same advanced security functionality as conventional plastic smart cards. SmartID is designed to support public key infrastructure (PKI) for authentication, digital signatures and file encryption as well as securely storing Windows credentials for authentication but at the fraction of a cost of the conventional smart cards.

Website Authentication



Site Stamp provides a simple yet effective way for users to sign or stamp websites that they trust. At logon, Site Stamp presents users with their own personalised dynamic images to ensure that they are communicating with a legitimate website and not a phishing website.

Site Stamp delivers a low-cost two-way authentication solution for mass-market web applications such as online banking and ecommerce websites.

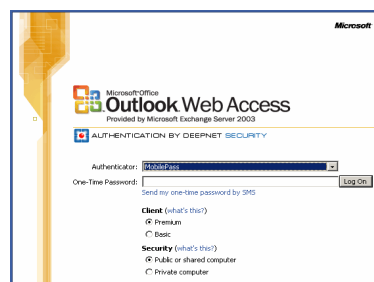
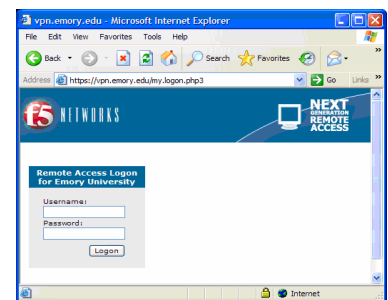
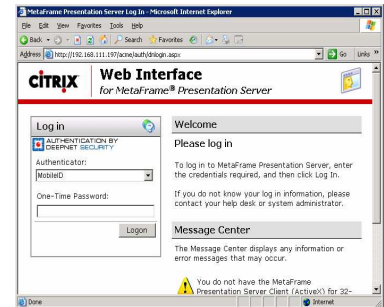
Multiple Solutions

Deepnet Unified Authentication is a truly open platform based on industry standards such as LDAP, RADIUS, X509 and PKCS. The Platform employs these standards to interoperate automatically with a number of network and business applications that require strong authentication, such as IPsec VPN and SSL VPNs that natively support both X.509 and RADIUS-based authentication.

For applications that do not natively support RADIUS or PKI, the Platform provides a set of out-of-the-box solutions including:

- Windows Logon
- Outlook Web Access (OWA)
- Outlook Mobile Access (OMA)
- Internet Information Server (IIS)
- Citrix Web Interface

Deepnet also provides a software developer kit (SDK) that allows IT developers to integrate Deepnet unified authentication into their custom application environment.

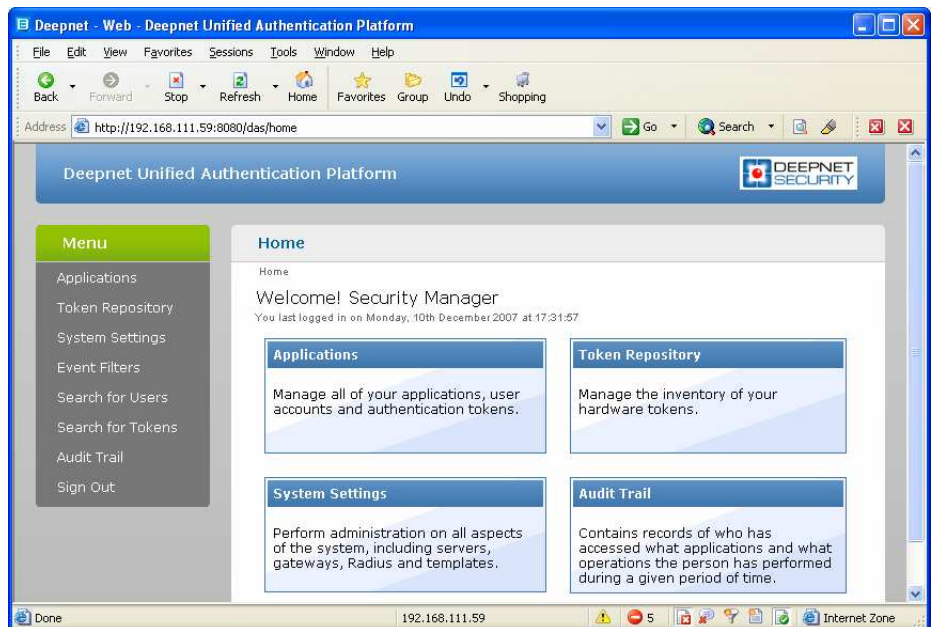


Central Management

Deepnet Unified Authentication Platform provides a web-based management console that enables the system administrators to manage applications, user accounts and tokens from any standard web browser.

The Management Console supports help desk and administration functions by providing tools for lifecycle management tasks such as token provision, activation, revocation, tracking and auditing.

The Management Console also provides an audit trail facility that records all significant events including passed and failed validations, activations, revocation etc.



Cross Platforms

Built on Java technology, Deepnet Unified Authentication Platform runs on any operating system that supports Java Virtual Machine (JVM) such as Microsoft Windows 2000/2003 servers, Linux, Unix and Sun OS.

Conclusion

Strong authentication is essential for both small and large business organizations to protect their enterprise networks, remote access and Internet services from the increasing threats of identity theft. Although there are a number of proprietary strong authentication solutions available in the market, no single solution has been widely adopted because these standalone solutions are expensive for businesses and inconvenient for users. Key contributors to this problem are: single-purpose hardware tokens, lack of interoperability and flexibility, limited integration and poor scalability.

The Deepnet Unified Authentication Platform addresses these issues by enabling enterprises to employ a single integrated platform for all their strong authentication needs to all types of users. By using the devices that users already have (mobile phones, employee ID cards and USB flash etc) and by taking advantage of an enterprise's existing infrastructure, it reduces the total cost of ownership and increases the usability of strong authentication.

Key Technical Advantages

- Open Architecture allows for new authentication methods and applications to be supported through simple upgrades.
- Three-Tier Framework allows for seamless integration into enterprise's existing infrastructure.
- Unified Platform provides security, flexibility and usability, offering the maximum protection at the minimum cost.

Key Business Benefits

Cost Effective

Deepnet Unified Authentication reduces total cost of ownership of strong authentication by as much as 60 percent by:

- providing multi-purpose hardware tokens and software tokens
- taking advantage of an enterprise's existing infrastructure
- enabling self-service management of common lifecycle tasks
- protecting all types of applications in one single platform
- reducing the cost of procurement, provision, management and maintenance

User Friendly

Deepnet Unified Authentication enables users to choose the authentication credentials that match their lifestyles and encourages widespread adoption of strong authentication.

Future Proof

Deepnet Unified Authentication provides a holistic, future-proof solution that can accommodate technology advances and evolving business requirements.

About Deepnet Security

Deepnet Security provides enterprises, financial institutions and ecommerce websites with the most flexible, two-factor and two-way authentication solutions that are user friendly and cost effective. Our key product, Deepnet Unified Authentication Platform, is a single integrated authentication platform for provisioning, managing and verifying all types of user credentials such as hardware tokens, soft-tokens, mobile tokens, smart tokens and keystroke biometrics.

For additional information please visit www.deepnetsecurity.com.

Deepnet Security Limited
Maples Business Centre
144 Liverpool Road
London N1 1LA
United Kingdom

Email: sales@deepnetsecurity.com
Tel: +44 20 7700 4282
Fax: +44 20 7697 8282