Enhancing Identity Assurance across all Access Scenarios Cost Effectively with IBM ISS Identity and Access Management Services – total authentication solution

I-Lung Kao
Internet Security Systems
IBM Global Technology Services Group

Executive Summary

Identity thefts and frauds have caused significant financial losses and image damages to businesses across industries. Password, as the most commonly used authentication factor, cannot alone provide appropriate identity assurance for many application access and business transactions. To reduce the chance of passwords getting guessed or stolen, many organizations have attempted to apply more complex password policies, but it has been proven to be an effectiveness-limited practice and in many situations has caused more help desk calls. Some organizations try to use password management tools to ease the user's burden due to password plurality, but these tools often aggregate the risks or the attack point. Strong authentication, based on two or more authentication factors, is the only effective way to raise the identity assurance level.

Strong authentication is needed in any high-risk access scenarios either within the business or between the business and its customers and partners, such as online/mobile financial transactions, remote corporate access, privilege user logon, and primary network logon. Many countries have specific regulations that mandate or recommend the use of strong authentication for electronic financial transactions. As the Internet and mobile phone are becoming more popular deliver channels for products or services of many businesses, use of strong authentication is deemed absolutely necessary to raise the identity assurance level in performing high-value operations or transactions.

There are however several challenges that organizations need to overcome in order to effectively adopt strong authentication as a strategic, enterprise-wide security solution. Different applications may use different authentication mechanisms, protocols, and identity databases, so implementing strong authentication on a per-application basis is costly and ineffective. A large variety of hardware or software-based authentication tokens have existed on the marketplace. The fact that most authentication token providers focus on specific scenarios with their own specialized solutions greatly complicates the decision of the business in choosing a solution that can fulfill the needs of different applications with various authentication tokens, based on assessment of risk, cost, and usability. Furthermore, to maximize the ROI in facing new or changing security challenges, organizations would like to adopt a future-proof solution that allows enabled applications to switch from one authentication method to another without major changes to the applications. Finally, implementing strong authentication in an enterprise is not a straightforward project. It needs well planning, innovation, execution, coordination, communications, and training, delivered by a team with technical excellence, proven methodologies, best practices, and global experiences.

IBM ISS Identity and Access Management Services - total authentication solution is a fully integrated, enterprise-wide, and cost-effective strong authentication solution to help organizations enhance identity assurance across various business applications and access scenarios. It delivers a highly-secure centralized authentication infrastructure that can be easily integrated with various applications or IT infrastructure components via its API or standard authentication protocols such as RADIUS or LDAP. It supports a very wide range of hardware or software or mobile phone-based authentication tokens that allow

maximum flexibility in choosing a specific authentication method for each scenario. The solution can be easily integrated with an organization's identity management, access management, fraud detection, or other security management solutions, to effectively incorporate strong authentication into the organization's overall security strategy and architecture. With industry-leading methodologies, best practices, and highly skilled professionals, IBM has successfully implemented the solution in enterprises of various sizes to help customers significantly raise the identity assurance level for critical business application access.

1 Needs to Enhance Identity Assurance beyond Password

Authentication is the first step to protect an organization's network, systems, and data from illegitimate access. Password, though still the most commonly used authentication method, has been recognized to be vulnerable to a wide variety of passive or active attacks. To reduce the chance that passwords are guessed or stolen, organizations have been trying to apply more stringent password policies such as increasing the complexity of the passwords (e.g., composing characters, password length) or mandating periodical password changes. However, stretching out the usage of password is neither security-effective nor cost-effective because it places a lot of burdens on end users, makes passwords even more exposed as users tend to write down complex passwords, and increases the volume of the help desk calls for resetting forgotten passwords.

According to a study, a typical enterprise user has 12 to 15 pairs of ID/password to manage. Password management tools such as Personal Password Wallet, Self-Service Password Reset (SSPR), Web Single Sign-On (WSSO), and Enterprise Single Sign-On (ESSO) have been used by organizations to ease the burdens of user and reduce help desk calls. The main idea of these password management tools is to centralize the storage or administration of all the passwords so the user has a single place to manage or access all the passwords. The biggest issue with this methodology is that centralizing all the passwords will also aggregate all the risks or the attack point at the same time. When a user's primary password used to manage or access all the other passwords is compromised, so are the user's accounts on all the systems and applications to which the user has access.

Many organizations have started to realize that the most effective way to raise the identity assurance level during authentication is to use two-factor authentication which is usually based on the traditional "something you know" form factor (e.g., password) plus another form factor that is either "what you have" (e.g., key, badge, smart card, token) or "what you are" (e.g., fingerprint, voice). Strong authentication based on two factors is much more effective in reducing the risk associated with password attack (identity theft of fraud) and thus the chance of losing valuable business data that may very possibly lead to financial loss or damage to the image and reputation of the business. Many countries already have specific regulations (e.g., FFIEC in US) that mandate or recommend the use of strong authentication for electronic financial transactions. Some other security related regulations (e.g., HIPAA, Sarbanes-Oxley, GLBA, and DPA) also recommend or imply enhanced authentication as part of the business's strategy to mitigate the overall security risk. Moreover, when the Internet and mobile phone are becoming more popular delivery channels for the products or services of many businesses, use of strong authentication is the most effectively way to raise the confidence levels of both the business and the end users in performing high-value transactions over these inherently insecure channels.

2 Challenges of Adopting Strong Authentication

Although organizations have recognized that strong authentication is needed to effectively enhance the identity assurance for application accesses and service transactions, there are some challenges that organizations need to overcome from both business and technical perspectives.

First, strong authentication is needed in multiple access scenarios, either within the business or between the business and its customers and partners. In general, the access scenarios where strong authentication is highly recommended to be used include:

- Online financial transactions (e.g., online business/retail banking, online shopping, eCommerce)
- Mobile based financial transactions (e.g., mobile banking)
- Remote corporate access (via VPN gateway) by employees or partners
- Privileges user (administrator) logon
- Primary network logon (e.g., initial logon to WSSO or ESSO)

The applications involved in these different access scenarios currently may use different authentication mechanisms, protocols, and identity database. However, when it is time to enable individual applications to use strong authentication, an enterprise-wide and strategic approach should be adopted. Organization should consider deploying a strong authentication solution that can address the needs of as many business applications and access scenarios as possible. This implies the solution should not be tied with any existing application's interface, protocol, or backend database. In other words, the solution should be 'application-neutral'.

Secondly, on the market there are many strong authentication products that vary considerably in their technologies and functions, and there have been various taxonomies by industry analysts to classify these authentication methods. Each authentication method has its own strength and weakness in terms of supported security level, deployment cost, and usability, which all need to be considered together to determine its most suitable scenarios. While hardware-based tokens such as OTP tokens, smart cards, USB devices are used commonly in some enterprise and consumer environments, software or mobile phone-based authentication tokens are getting more attentions and acceptance recently due to their lower cost, less on-going management overhead, and higher convenience of use. When organizations try to enable different business applications and infrastructure components to use strong authentication, they find it a very challenging task because of the confusion caused by a wide variety of different authentication methods and tokens and the fact that most authentication token providers focus on solving specific authentication issues with their own specialized solutions. Many solutions use proprietary algorithms and protocols or dedicated architectures so it is difficult to get interoperability among different authentication methods.

Thirdly, organizations always would like to maximize their technology investment. When a strong authentication method is chosen for resolving a specific identity issue today, it does not mean the method will be able to address future authentication requirements. It is a known fact that new security threats appear at an increasingly faster rate, and the techniques to exploit the security weakness in one application spread to

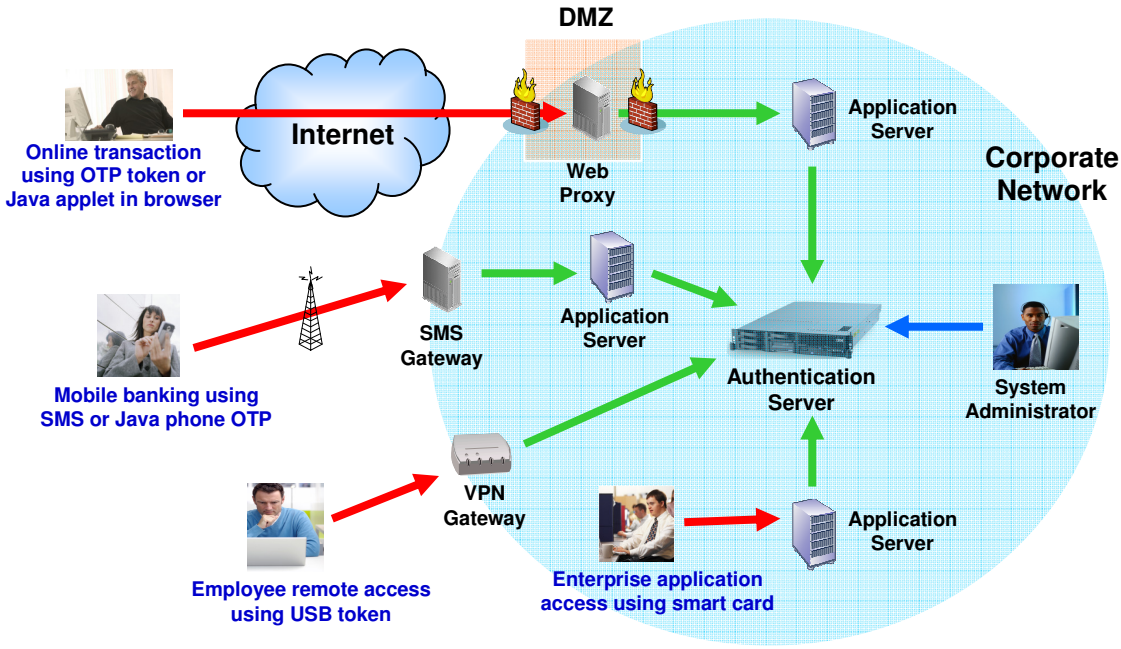
other applications quickly. It has also been a trend that government regulations to tighten up identity security expand to a broader set of business areas and transactions. Therefore, to maximize the ROI on strong authentication, organizations need to consider the future-proof characteristic of the solution, i.e., whether the solution is flexible to allow a business application to switch from an authentication method to another one (as a result of the organization's decision to get more security, less cost, or better user convenience) without any major changes to the application.

Finally, implementing a strong authentication solution in an organization is not a straightforward IT project, so the cost and complexity associated with the solution's implementation needs to be fully understood and managed. Adopting strong authentication is usually not transparent to end users so all users need to be communicated, educated, and provisioned in advance so they can be ready to use strong authentication. Related administrators, help desk personnel, or support engineers of the organization all need to be trained well to fully support strong authentication as part of their responsibilities. The strong authentication solution itself has to be highly secure, robust, available, scalable, high-performance, and easily manageable, simply because authentication, as the first step of access control, is a critical function for running any business. All the human oriented security best practices also apply to strong authentication.

3 IBM ISS Identity and Access Management Service - total authentication solution

To help organizations adopt strong authentication efficiently and effectively and overcome all the challenges and issues described above, IBM ISS Identity and Access Management Services offers the **Total Authentication Solution** (the "Solution"). The Solution is provided to help organizations enhance identity assurance across various business applications and access scenarios such as online/mobile transactions, VPN access, and enterprise application access with:

- a highly secure centralized authentication infrastructure that can be easily integrated with business applications
- support for a wide range of hardware, software, and mobile phone-based authentication methods that allows maximum flexibility in the choice of a specific authentication token based on assessment of risk, cost, and ease of use
- consulting, design and implementation services from IBM to deliver complete strong authentication solutions to organizations



With IBM ISS IAM Services - **total authentication solution,** customers are provided with an enterprise-wide, token-agnostic, cost-effective, and future-proof strong authentication solution that allows a client to

- combat identify theft and fraud strategically
- comply with regulations efficiently
- conduct secure businesses over new delivery channels cost-effectively
- maximize investment in facing changing security challenges

4 Technical Features and Capabilities

The Total Authentication Solution is designed and developed with leading-edge security technology that delivers a very rich set of capabilities to address various authentication requirements.

4.1 Authentication Server

The Authentication Server, a core component of the Solution, is to handle all authentication requests from various applications via the Client Authentication API or standard authentication protocols such as RADIUS and LDAP. Besides static passwords, the Authentication Server supports a wide variety of 2nd factor authentication tokens such as hardware tokens from popular vendors including those OATH based, software tokens such as Java Applet embedded in browsers, mobile phone tokens such as SMS based OTP, and some other token forms such as grid cards and pin mailers. The lifecycles of all the supported tokens can be managed by a web browser-based admin

module, with multi-domain support for compartment of token users and separation of duties for administrators.

The Authentication Server is delivered as a security appliance based upon IBM xSeries model 3550 or 3650 and a hardened Linux OS with built-in packet filtering firewall. It also contains a FIPS 140-2 certified HSM (Hardware Security Module) for secure key storage and all cryptographic functions.

The Authentication Server is designed to be secure, versatile, high-performance, and easy to administrate, and the specific features that exhibit these design principles are elaborated below.

4.2 Token Support

The Solution has support for a wide variety of authentication tokens (beyond password):

- **Hardware token** (to be purchased separately) -
  - VASCO: supported natively
  - RSA SecurID : supported natively
  - SafeWord: via RADIUS to SafeWord server
  - OATH HOTP (RFC 4226):
    - Feitian
    - Verisign (OEM from VASCO)
    - Entrust
    - ActiveIdentity
    - Aladdin
  - OATH Time-based OTP:
  - Mastercard CAP/CAP-E:
    - Gemalto
    - Advanced Card Systems (ACS) with Oberthur smartcards
    - Xiring
  - Smart card/USB token with pubic-key certificate

- **Software token** -
  - Windows PC token: One-time passwords generated by software tokens installed on Windows platform based on S/Key (RFC2289) and OATH (RFC4226)
  - Java Applet in browser: One-time passwords generated by a Java Applet embedded in a browser
  - Email OTP: One-time passwords sent via email

- **Mobile phone token** -
  - Java phone midlet OTP: One-time passwords generated by a Java phone Midlet (supporting J2ME MIDP 1.0, MIDP 2.0, sAppli, iMode iAppli) installed in Java-enabled phones, based on S/Key (RFC2289) and OATH (RFC4226)

- SMS OTP: One-time passwords transmitted via SMS from a messaging gateway
- Voice call-back: One-time passwords communicated to the user via phone

- **Paper token** -
  - Grid (matrix) card: One-time passwords produced based on a specific pattern on a matrix card issued to the user
  - Scratch card: Pre-defined one-time passwords (in a batch) issued to the user on a scratch card
  - Pin mailer: One-time passwords printed on paper that is mailed to the user

The design philosophy of the Solution behind the support for such a wide variety of authentication tokens is simply to be token-agnostic (i.e., we attempt to support as many tokens as possible and we do not differentiate any hardware token from others). This allows the organizations to apply strong authentication across various business applications and access scenarios and get maximum flexibility in choosing a specific token based on risk, cost, and usability.

4.3 Client Authentication API

The Client Authentication API (the "API") is a Java-based library to allow applications to connect via 2-way SSL to the Authentication Server to carry out authentication, authorization, and administration operations.

Enabled business applications can use the API to authenticate users using 1st factor, 2nd factor, or a combination of two factors, with any supported token. The API also allows applications to authorize a business transaction using specific transaction values.

The API allows organizations to integrate the Solution with their existing enterprise identity management or token provisioning services so the users and tokens can also be created and managed through those services.

The API supports functions for various server maintenance operations such as database backup and restore and audit log download. This enables the system management services of an enterprise to include the Solution in the regular backup of critical databases as well as the daily maintenance of audit logs.

Another feature of the API is its built-in support for high availability and disaster recovery that is important for any organization with uninterrupted authentication service as part of its business/IT requirements. It is described in detail below.

4.4 Standard Protocol Support

The Authentication Server has 'out-of-the-box' support for standard authentication protocols such as RADIUS and LDAP. The support for RADIUS allows the VPN gateways from major VPN vendors (e.g., CISCO, Juniper, Checkpoint, Nortel, and

Microsoft) to seamlessly work with the Solution, providing strong authentication for remote corporate access from employees or business partners. The support of LDAP allows the business systems or applications that use LDAP for authentication (e.g., Unix/Linux PAM LDAP, MS IIS LDAP plug-in, and pGINA) to integrate with the Solution efficiently, enabling more secure access to these systems and applications.

4.5 Web based Administration

All the administration functions of the Solution are performed via a web browser running on an administrator's machine. Access to the administration functions is controlled by 2-factor authentication (such as ID/password + smartcard), and all the communications between the web browser and the Authentication Server are protected by HTTPS.

The administration functions are categorized as follows:

- **Domain Management**: 31 user domains can be established and supported by one Authentication Server. Each domain functions independently with its own cryptographic keys, database and security policies. Each domain can have its own domain administrators setting up different authentication token policies for the domain. The multi-domain capability allows an enterprise to support multiple divisions or departments that may require different tokens or policies and enforces separation of duties for better administration security.
- **User Management**: All user related administration functions including user creation, suspension, revocation, and deletion. Users can also be created using batch upload from an existing user identity repository such as Active Directory.
- **Token Management**: The administration of lifecycles of various categories of tokens, including token creation, configuration, and assignment to users.
- **Security Management**: Administration of security policies and attributes, including password policy management, key management, certificate management, and authentication protocol management.
- **Server Management**: Administration of the server including server start-up/shutdown, audit log management, and secure database backup/restore.

4.6 Capacity and Performance

The Authentication Server is designed to possess large capacity with high performance to satisfy the requirements of large enterprises for strong authentication. The database imbedded in the Server can support up to 5 million users, which far exceeds the need of a typical organization even for consumer-oriented services. If more users are to be supported, multiple authentication servers can be installed and configured. The performance of the Authentication Server is summarized as follows:

- Support 100 end-to-end RSA authentications/sec
- 5,000 concurrent login sessions
- 250 OTP generations/sec
- 150 RSA decryptions/sec

4.7 High Availability and Disaster Recovery

Since authentication is a critical function for running business, the Solution has built-in support for high availability and disaster recovery. If two authentication servers are configured in a production environment, they will synchronize the databases with each other in real time. When one server is not reachable for any reason, the Client Authentication API used in the enabled application will redirect the authentication request to the other server, totally transparent to the application. For preparation of disaster recovery, another authentication server can be configured in an organization's back-up site. The back-up server can be configured to synchronize with the production servers automatically or at regular intervals. When a disaster happens to the production environment, the back-up server will pick up the authentication responsibility immediately.

4.8 Password/OTP Protection End-to-End

For the case of a password or OTP sent from a browser, the Solution provides additional security feature so the password/OTP will not be exposed in the clear to any intermediate party on the entire path from the browser to the Authentication Server. This protection is provided by embedding a Java Applet in the browser that will encrypt the password/OTP before it leaves the browser. Since the password/OTP is encrypted, sniffing attack can be effectively prevented. A random number is also used to prevent replay attacks. The web application server that provides the business services cannot access the encrypted password/OTP, so the risk of exposing password/OTP to the web server's administrator or in the server's audit log is significantly reduced. The encrypted password/OTP will not be decrypted until it reaches the Authentication Server. Furthermore, all the cryptographic functions are performed within the HSM (Hardware Security Module), so the password/OTP is never exposed outside of the HSM.

This end-to-end password/OTP protection feature allows organization to use one or two factor authentications in an insecure environment, however with the security risk significantly reduced.

4.9 Security Features to Protect the Architecture

Because an authentication solution is an important part of an organization's security infrastructure, it needs to be highly protected from security attacks from either insiders or external hackers. Many security features have been implemented to protect the accesses to, the communication with, and the database storage of the Authentication Server:

- Access to the Authentication Server
  - Smart card is needed to initialize, start and shutdown the Authentication Server and all I/O (keyboard, mouse, monitor) is disabled.
  - 2-factor authentication is required to access the Authentication Server via the Web Admin.
  - Public-key certificates are used to mutually authenticate the API application and the Authentication Server.

  - Separate of duty is enforced in domain administration. Each user domain administrator only has privileges to mange his own domain. Privileges of administrators and operators are separated.

- Communication protection
  - Communications between any API application (including the Web Admin) and the Authentication Server are all encrypted with SSL.
  - A packet filtering firewall is embedded within the Authentication Server to control inbound traffic.

- Storage protection
  - All passwords and keys in the database are encrypted with a 'master key' protected in a FIPS 140-2 level 3certified HSM.
  - The keys stored in the HSM will be erased if any physical tampering is detected.

5 Integration with other Security Products and Solutions

The Solution can be easily integrated with an organization's identity management, access management, or other security management services, as part of the organization's overall security strategy. The Solution's centralized server architecture, independence of applications and tokens, and full-functional API support makes the integration feasible in almost any customer environment.

The Solution has support for integration with major Tivoli security products such as Tivoli Access Manager for e-business (TAMeb) and Tivoli Identity Manager (TIM). The Solution can also be integrated with a fraud detection/management product so whenever an identity fraud is suspected, the authentication server can be requested to authenticate the user using another authentication factor beyond password.

5.1 Integration with Tivoli Access Manager for e-business

IBM Tivoli Access Manager for e-business (TAMeb) is to provide an enterprise-wide centralized access control infrastructure for web applications. The WebSEAL component of TAMeb is a proxy web server that performs initial authentication, access control, and single sign-on for all the web applications within an enterprise.

The Solution can be fully integrated with TAMeb to provide strong authentication for initial logon to the WebSEAL server, so a higher identity assurance can be established before the user is granted access to web applications behind the enterprise's firewall.

5.2 Integration with Tivoli Identity Manager

Tivoli Identity Manager (TIM) is to provide an enterprise-wide solution for identity lifecycle management. TIM provides full administrative functions and workflow capabilities to provision identity data from a company's human resource database to various applications such as DBMS, directory servers, and business application servers, via application specific agents or adaptors.

The Solution can be fully integrated with TIM so TIM can be used to provision user and token related data to the authentication server via an agent implemented with the Client Authentication API. This allows the Solution to be incorporated to the enterprise's identity management infrastructure.

5.3 Integration with Fraud Detection

A fraud detection product is used to assess initial logon of a transaction or in-session activities for behavioral anomalies that indicate potential fraud. Whenever a possible fraud is detected, additional actions like requiring the user to logon using strong authentication can be taken to prevent a real fraud from happening.

The Solution is ready to be integrated with a fraud detection product. The fraud detection product can be configured to collect strong authentication data from the user and pass the data on to the authentication server for authentication. Combination of strong authentication and fraud detection provides layered security for the organizations that have needs of high identity assurance.

6 Typical Deployment Scenarios

The Solution is provided to fulfill the strong authentication needs of many applications across the enterprises. It can be deployed in many scenarios where one factor authentication (i.e., password) is deemed insufficient to establish an identity for access to systems, networks, applications, or data.

Two typical scenarios that the Solution has been deployed by many organizations and the benefits rendered by the deployment of the solution are described below.

6.1 Secure Online and Mobile Banking

Many banks or financial service companies (stock brokerage, mutual fund supplier, insurance, etc.) are already using online service (via the Internet) as a major channel to provide their products and services. Mobile banking (or mobile financial service) is emerging quickly as another low-cost delivery channel, and its usage is expected to grow significantly in the next few years, simply because of the high penetration of mobile phones in many regions.

However, ID/password is still the dominating authentication method for online and mobile banking or financial services, even it has been commonly recognized that financial transactions over vulnerable channels such as the Internet need to better secured. Strong authentication is a critical step to prevent various frauds that exploit the weakness of these channels.

In general, there are some typical challenges for financial institutes to protect their online and mobile services. The Total Authentication Solution has been deployed by many banks to establish a centralized strong authentication infrastructure for both delivery channels with high security and manageability achieved at the same time. The typical business challenges and the benefits provided by the Solution are summarized in the following table:

Business challenge	Solution benefit
Only ID/password is used for online banking and mobile banking.	One-factor authentication (ID/password) is smoothly migrated to two-factor authentication with deployment of hardware token, SMS, or Java-enabled phone
Not all communication channels are protected with encryption.	Messages are encrypted end-to-end, from the browser to the authentication server.
Database used by applications for authentication is not well protected.	All authentication data including passwords and keys are hash-encrypted in a centralized database, and the encryption key is protected in HSM.
Customers have different service characteristics (e.g., corporate banking, private banking, and retail banking) and user groups that need to be segregated.	Multiple domains are created for different services and user groups and separate token/password policies are set for each domain.
User capacity and run-time performance are potentially significant issues for a large number of users (e.g., retail banking)	One authentication server supports up to 5 million users and delivers high performance for numerous concurrent logons.
More consistency is needed in managing online banking, mobile banking, or other electronic channels.	Only one web admin console is used to manage users, tokens, and policies across multiple banking delivery channels.

6.2 Remote Corporate Access

While more and more employees work from non-traditional office locations (e.g., homes, hotels, airports, customer sites) and the corporate network needs to be more accessible to business partners, it is important for an organization to ensure any remote access to its internal network, applications, and data is strictly controlled. VPN gateway is usually the primary mechanism to authenticate users using the RADIUS protocol. Some organizations allow employees to access their business email accounts from a browser,

using a web server as a proxy to access the internal email server. The web proxy server may use a standard protocol such as LDAP to authenticate users.

Most RADIUS and LDAP applications use ID/password only. However, remote access to corporate resources is a scenario that definitely needs stronger authentication, simply because password alone is too weak to establish a user's identity when the user is not within the organization's premise.

The Solution has been deployed by organizations to establish a centralized strong authentication infrastructure for VPN access, remote email access, and access to critical enterprise applications. The typical business challenges and the benefits provided by the Solution in those environments are summarized in the following table:

Business challenge	Solution benefit
Remote email access is vulnerable to phishing and sniffing attacks.	Java applet is embedded in browser as a second authentication for remote email access. Email access from office is still ID/password based for convenience.
Only ID/password is used for VPN logon	SMS or hardware token is used for all VPN logon.
It is expensive and risky to change the applications to use another authentication systems and protocols.	No application change is necessary because RADIUS and LDAP are supported "out of the box".
The IT security team spends too much time administrating security patches to OS.	No security patching is needed as the authentication server is an appliance.
It is costly to implement and maintain authentication mechanism and data for individual applications.	One single authentication infrastructure is used by multiple applications across the enterprise, in spite of specific needs of each application.
Organization plans to support new authentication methods for some applications in the near future.	The solution is future-proof and versatile so applications can switch from one authentication method to another easily.

7 Conclusion

IBM ISS Identity and Access Management Services - total authentication solution is a fully integrated, enterprise-wide, and cost-effective strong authentication solution to help organizations enhance identity assurance across various business applications and access scenarios such as online/mobile transactions, VPN access, and enterprise application access. It delivers a highly-secure centralized authentication infrastructure that can be easily integrated with various applications or IT infrastructure components via its API or standard authentication protocols such as RADIUS or LDAP. It supports a very wide range of hardware or software or mobile phone-based authentication methods that allow

maximum flexibility in choosing a specific method or a specific hardware token based on assessment of risk, cost, and usability for each scenario. The Solution can be easily integrated with an organization's identity management, access management, fraud detection, or other security management solutions, to effectively incorporate strong authentication into the organization's overall security strategy and architecture. With industry-leading methodologies, best practices, and highly skilled professionals, IBM has successfully implemented the Solution in enterprises of various sizes to help customers significantly raise the identity assurance level for critical business application access.

8 For More Information

To learn more about IBM ISS Identity and Access Management Services – total authentication solutions, contact your IBM representative or IBM Business Partner, or visit:
http://www.ibm.com/services/us/index.wss/offerfamily/gts/a1027701