Expanding Web Single Sign-On to Cloud and Mobile Environments
The World of Online Business is Rapidly Evolving...

In years past, customers once tiptoed cautiously into the realm of online banking, bill payment and other Internet-based business. Today, however, millions are comfortable performing a host of transactions online—and relying on the supporting organizations to maintain a secure environment.

As a result, companies are rapidly expanding the ways they provide online services to customers, employees and partners to make convenient anywhere, anytime access and any-device options the new standard. Their goal? Gain greater efficiencies, enable improved responsiveness and deliver a better user experience.

This includes delivering secure services via:

- Web browser-based applications
- Mobile applications
- Open Web services interfaces

But no matter how online services are accessed, or how many users access them, a fundamental concern remains: Organizations need to protect larger and larger volumes of sensitive data while still allowing users to easily conduct business.
The use of traditional Web single sign-on (SSO) in web access management (WAM) has been critical to controlling access to resources, while providing a seamless and secure experience for online users. It has enabled them to readily move from one web-based transaction to another, smoothly interacting with other applications or external sites along the way.

For example, the simple transaction above requires multiple security steps to confirm the customer's identity and allow the requested online banking actions to be performed. Yet, the customer only needs to log in once, using one set of credentials, to access personal account details and information from an affiliated, external financial planning website.
...and Single Sign-On (SSO) is Evolving With It (Continued)

1. First, the customer’s identity must be confirmed. Methods to do this today include asking the customer to associate an image with an account, or to confirm the answer to questions created upon customer account set-up.

2. Based on the identity confirmation, the customer is allowed or disallowed to conduct the requested transaction. Enabling this requires security features to be built into the website, related security policies maintained and audits performed of the customer’s actions after logging in.

3. Next, the security of back-end transactions must also be ensured. Connecting to the bank’s applications, perhaps at a separate financial institution, must be done in a secure fashion.

4. Lastly, the connection to the bank’s financial planning partner must be securely achieved—also with SSO. If the bank were to force the customer to log in again to the financial planner’s website, he or she might find that process onerous and leave the bank.

But as your organization moves beyond early web-based operations and introduces mobile and cloud-based initiatives, you need to extend SSO to secure these new services and related methods of access. At the same time, you must address the unique requirements of an increasingly diverse portfolio of applications, such as Microsoft® SharePoint® Server and SAP®, and the varied types of users who interact with them. As part of an ongoing process, making changes like these requires a flexible solution that will enable you to act quickly to meet new demands.

THE STEPS IN A TYPICAL ONLINE BANKING SCENARIO:

1. First, the customer’s identity must be confirmed. Methods to do this today include asking the customer to associate an image with an account, or to confirm the answer to questions created upon customer account set-up.

2. Based on the identity confirmation, the customer is allowed or disallowed to conduct the requested transaction. Enabling this requires security features to be built into the website, related security policies maintained and audits performed of the customer’s actions after logging in.

3. Next, the security of back-end transactions must also be ensured. Connecting to the bank’s applications, perhaps at a separate financial institution, must be done in a secure fashion.

4. Lastly, the connection to the bank’s financial planning partner must be securely achieved—also with SSO. If the bank were to force the customer to log in again to the financial planner’s website, he or she might find that process onerous and leave the bank.

But as your organization moves beyond early web-based operations and introduces mobile and cloud-based initiatives, you need to extend SSO to secure these new services and related methods of access. At the same time, you must address the unique requirements of an increasingly diverse portfolio of applications, such as Microsoft® SharePoint® Server and SAP®, and the varied types of users who interact with them. As part of an ongoing process, making changes like these requires a flexible solution that will enable you to act quickly to meet new demands.
Building On the Basics

While supporting an increasingly complex array of access requirements, your security—and SSO—fundamentals remain the same. You need to know who your users are, control what they can do and be able to both monitor and audit their actions based on individual entitlements.

Starting with the basics helps you build a strong security foundation. But new technology requirements are changing the SSO landscape. In particular, three key areas are having a major impact:

- Extended services
- Cloud adoption
- Mobile and the consumerization of IT

As access requirements grow and change, proactive organizations implement additional safeguards while sticking to security essentials. This helps them prevent risks ranging from malicious attacks to threats from internal users who fail to follow security policies and procedures.
Extended Services for Advanced Authentication

To stay competitive, organizations are rapidly complementing existing business models with online services that take advantage of the latest technologies. This often involves supporting multiple device types such as laptops, tablets and smartphones, as well as new mobile- and cloud-based infrastructures. And it creates a number of authentication challenges, including:

- Addressing the specific usage and access-level requirements of all end users
- Supporting situation- or risk-based authentication
- Providing convenient online access with full protection for both the user’s identity and sensitive application data
- Securing on-premise and cloud-based applications
- Protecting critical transactions from online fraud

So what can you do to minimize all these access-related risks, while simultaneously keeping your data safe and promoting online activity?

Traditional Web SSO relies on risk-appropriate authentication to protect transactions based on pre-defined rules and models. But given the complexity of user interactions in today’s IT environments, more advanced forms of authentication are required.

Solutions for extended services provide an effective response through risk-based evaluation. Using risk-based evaluation, you can apply adaptive authentication techniques to assess a user and determine an appropriate “risk score” based on a mix of access factors.

The same features that add to user convenience—support for various device and user types, along with multiple application access points—contribute to potential security risks without proper authentication and authorization mechanisms.
Extended Services for Advanced Authentication (Continued)

More advanced authentication using risk-based evaluation provides the context you need to comprehensively gauge the risk of individual users. By continually monitoring their typical application usage and access patterns, you’ll be able to quickly identify actions that fall outside of normal behavior—such as their logging in from a coffee shop instead of at home. You can then request additional credentials to confirm their access rights or take whatever steps are necessary to prevent unauthorized use. This is especially critical when users are attempting to perform high-risk actions.

A key feature of advanced authentication is the ability to profile users based on past behavior, and then flag out-of-the-ordinary actions that could present serious security risks.

- **Where is the user?**
  - Is the location inherently suspect?
  - Has the user been there before?
  - Where was the user recently?

- **What system (device) is the user utilizing?**
  - What kind of device is it?
  - Has the user utilized it before?
  - Has the device changed since it was last used?

- **What is the user trying to do?**
  - We look at more than just authentication, e.g., what is the requested action?
  - Is the action inherently risky?
  - Has the user done similar actions before?

- **Is it consistent with the user’s historical actions?**
  - Is this a normal time of day for the user?
  - Is the frequency of log-in abnormal?
  - Is the current action consistent with prior actions?
Federated SSO enables user credentials to be trusted across multiple IT systems or applications, leveraging industry standards—such as security assertion markup language (SAML) and its “identity cookie approach”—to authenticate in-bound data.

In an extended-service environment, however, people may be accessing systems using multiple authentication methods, including smart cards, biometric devices and two-factor authentication. For this reason, it makes sense to employ an authentication solution that also offers session management functionality, as it provides the ability to perform both hardware- and software-based token translation.
Enterprises that employ session management to enable advanced authentication and enhance federated SSO are better prepared to handle extended-service requirements.

Session management offers other sophisticated capabilities to enhance the security of identity access and management processes. Depending on your extended-service needs, it may also be worthwhile to implement:

- SSO zones to isolate and lock down all or part of high-security applications
- Authentication selectors to allow users to select different ways to log in
- Directory chaining to link multiple user directories, simplifying access rights management and eliminating the need for users to re-establish credentials during a session
- Levels of trust to enable step-up authentication based on an established ranking
- A centralized audit of all user log-ins, as well as related activities following log-in, for improved monitoring and compliance

Inbound

- Logon form
- Basic authorization
- X.509 certificates
- CA Advanced Authentication
- SecurID™
- CA Risk Authentication
- RSA adaptive authorization
- Smart cards
- Biometric devices

Outbound

- SAML 1.0
- WS-Fed
- SAML 2.0
- OpenID

Session Management

WebLogic
WebSphere
JBoss

SAP
SharePoint
Oracle
PeopleSoft
Siebel

IIS
Apache
IHS
HP Apache
Oracle HTTP
Oracle iPlanet
Cloud Adoption Creates New Security Considerations

Private clouds, public clouds and Software-as-a-Service (SaaS) offerings. Without the need to manage a physical infrastructure, these and other variations on the cloud can give enterprises a lower-cost, flexible way to provide services. For this reason, cloud adoption has soared, increasing the ever-growing base of internal and external users accessing online applications.

While adding another layer of access requirements, cloud-based services must still be delivered conveniently and securely. As you implement them, you need to enhance existing SSO mechanisms with stronger forms of authentication that protect your data, but don’t detract from the user experience.
Engaging Mobile Users

Driven by both employee and customer demands, mobile technologies have surged in popularity. Mobile spend continues to increase as more people use smartphones and the mobile apps market reaches new heights.

Given these trends, it’s no wonder the use of mobile technology is spreading like wildfire. Organizations like yours have found it to be a highly effective way to engage their customer base and drive top-line revenue. From improving access to products and services to enabling mobile sales teams, they’re building mobile applications to make both customer and employee transactions faster and easier to perform. But to promote user adoption, you need to deliver a consistent, secure user experience.

Whatever mobile applications and browser types companies support, they need to keep ease of use and secure access top of mind.
Meeting Mobile Requirements, Protecting Mobile Data

To give users the mobile access they desire and protect sensitive data, you need to build appropriate levels of device- and application-specific security—without inserting unnecessary steps that inconvenience customers or delay transactions. This requires a solution capable of handling:

- **Location-related requirements:** IP addresses assigned by carriers and access through virtual private networks may reflect switch-versus-actual locations. This makes it impossible to know if the user is at an expected location, and calls for validation against multiple factors to confirm the identity of the person attempting access.

- **Multiple form factors for credentials:** Because mobile devices can be easily misplaced or stolen, you may need to provide additional security measures aligned to transaction risk levels. For example, a one-time password may be used to verify valid credentials for online purchases. It may also be prudent to require a supplemental voice biometric in other situations.

- **Integration of authentication:** As you develop mobile applications, you must be able to embed authentication methods so that you can meet your access-related security requirements. Alternatively, if the mobile device allows, you can employ cookies to pass along credentials from an approved device to the application in question for the same purpose. And when mobile users interact with external applications, you’ll also want to allow them to seamlessly and securely extend their sessions to other applications.
Assessing Your Capabilities

By fully evaluating how you are providing user access today, you can pinpoint where advanced authentication and authorization methods should be applied to improve the security of web-, mobile- and cloud-based transactions.

As you do, keep in mind that employing a single, robust security solution is the ideal way to support all your user access requirements. Such an approach eliminates fragmented security practices to enable greater control over access management.

At the same time, it helps you more cost-effectively implement the enterprise-wide security required to safeguard critical data and applications.

Ultimately, it allows you to better address user expectations for convenience while providing added protection from all types of access-related security threats.

Key Advanced Authentication Capabilities

- Multiple authentication methods/credentials
- Two-factor authentication with no change to user log-in experience
- Rules and model-based risk evaluations to protect transaction
- Device identification

Key Benefits

- Improved user experience
- Reduce risk of fraud
- Increased customer adoption
- Greater administrative efficiency

With the right solution in place, you’ll be able to meet multiple IT challenges while securely expanding your online presence for strategic business benefit.
CA Security Solutions

At CA Technologies, we understand how important it is to strike the right balance between enterprise data security and convenient user access. And, we’ve developed solutions that address advanced access security requirements in Web, mobile and cloud environments.

CA Single Sign-On
CA Single Sign-On provides an essential foundation for user authentication, SSO and browser- and mobile-based authorization, as well as reporting activities. It enables you to create granular policies that can help control access to critical applications based on a flexible set of static or dynamic criteria, such as user attributes, roles, time, location or data sensitivity.

A standards-based identity federation solution, CA Federation enables users of one organization to easily and securely access data and applications of partner organizations. It can be integrated with CA Single Sign-On or deployed as a standalone solution.

CA Risk Authentication
CA Risk Authentication provides real-time protection against identity theft and online fraud using risk-based adaptive authentication. It evaluates the fraud potential of online access attempts—from enterprise Web services to consumer e-commerce transactions—and calculates the risk score based on a broad set of variables. All this is done transparently without inconveniencing legitimate, low-risk users.

CA Strong Authentication
CA Strong Authentication includes a wide range of fraud detection and multifactor authentication methods to reduce the risk of online fraud for e-commerce, Web portals and remote access.

For more information about CA security solutions, visit www.ca.com/auth-sso

CA Strong Authentication and CA Risk Authentication are visible as authentication services within the CA Single Sign-On interface.

Used for authentication
- Initial user and step-up authentication
- Applied against specific SSO Zones
- In conjunction with the authentication levels of CA Single Sign-On

Used for authorization
- Risk score is passed to CA Single Sign-On and held throughout the user’s session to be evaluated for additional access requests or transactions.
- CA Strong Authentication can be utilized to help enforce policy-based step-up authentication based on the risk score.
CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.