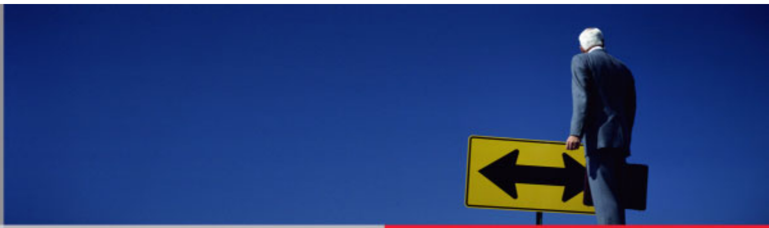
IBM

BIO-key Biometric Service Provider for IBM Security Access Manager for Enterprise Single Sign-On



Redguides

for Business Leaders

Myles Tillotson
Sean Dyon

- Make your systems and data more secure with finger-based biometric authentication
- Help your workforce become more productive by eliminating passwords entirely
- Optimize your investment in IBM Security Access Manager for Enterprise Single Sign-On

Redbooks

Executive overview

A critical challenge that virtually every organization faces is protecting internal and customer data and making access to the systems and applications that hold that data as convenient as possible. Striking the necessary balance of security and convenience starts with authenticating users accurately and quickly. But passwords, the traditional method of authentication, can be stolen or *borrowed*, and they do not always adequately protect information from unauthorized use or view. Even a single sign-on (SSO) password, which must be typed every time the user accesses a different system, does not make access any more convenient or users any more productive.

BIO-key Biometric Service Provider from BIO-key International, Inc. can help organizations meet this challenge. It provides a finger-based, biometric-enabled sign-on to IBM® Security Access Manager for Enterprise Single Sign-On. By using BIO-key Biometric Service Provider, the user places a finger on a reader. The fingerprint is then accurately and instantly identified and authenticated to enterprise applications and data that are protected by IBM Security Access Manager for Enterprise Single Sign-On. The identification and authentication occur without the user entering a user ID or password.

This more secure, more convenient form of identification is an intuitive, uncomplicated, and easy-to-install alternative to using a password that is too easily forgotten or compromised.

Business value: BIO-key Biometric Service Provider can mitigate risks, strengthen security, and improve productivity, in addition to reducing operating costs.

This secure SSO alternative can provide the following benefits:

- More secure systems and applications. No password to be stolen or shared.
- Superior user convenience. No keyboard entry of password and user ID.
- Improved user productivity. No downtime from forgotten passwords.
- Lower operating costs. Reduced help desk calls.

Other strong authentication methods, such as smart cards and RFID, that are supported by IBM Security Access Manager for Enterprise Single Sign-On still require the use of a password. The credential must be accessible and produced whenever and wherever second factor authentication is required, which can be less convenient for users than a password alone.

BIO-key Biometric Service Provider is appropriate for organizations of any size and in any industry. For example, in healthcare, BIO-key finger image capture and matching technology are already integrated with electronic health records (EHR) solutions from Allscripts and Epic serving hospitals and other healthcare providers. BIO-key finger biometrics technology is also integrated into McKesson's AcuDose-Rx system for controlled access to medications. In this case, the technology authenticates the identity of users who are accessing more than 8,000 medication cabinets nationwide.

This IBM Redguide™ publication highlights the BIO-key Biometric Service Provider solution, including details about business need and business value. This guide provides two real-world examples that show how finger-based SSO addresses common business requirements. It also presents a high-level overview of the solution architecture and how it is integrated with IBM Security Access Manager for Enterprise Single Sign-On version 8.2.

Business imperative: Balancing security and convenience

A challenge that almost every organization faces is balancing the need to protect sensitive data and granting access to the systems and applications that hold the data as convenient as possible for users. In many organizations, data security and convenient system access are mission-critical, but in potential conflict. For example, in healthcare, physicians demand instant access to electronic patient records to deliver care effectively and efficiently. Meanwhile, the Health Insurance Portability and Accountability Act (HIPAA)[1] and other rules mandate protection of that information from unauthorized users with significant penalties for violation.

Striking the necessary balance of security and convenience starts with authenticating users accurately and quickly. The traditional authentication method uses a nonsecure user ID and a password. But from a data security and user convenience perspective, passwords do not meet the challenge well.

Data security

In terms of protecting sensitive data, it is widely recognized that passwords are inadequate when used as the single and only authentication method. If passwords are easy to remember, they are easy to break. To make passwords more secure, or *strong*, they must be longer, more complicated, and less predictable, unfortunately making them more difficult to remember. As a result, users are more likely to leave password notes where they can be easily found and potentially misused. With an increasingly mobile workforce that works outside physically-secure corporate facilities, the potential for identity theft is greater than ever before.

Beyond passwords: "Companies that spend time and money creating password security strategies are largely wasting their time, because one in three employees is writing down passwords regardless of password policies. ... It's like leaving the key under the mat or in the flower box. Companies looking to ensure security should look beyond passwords to other authentication strategies."

David O'Connell, senior analyst at Nucleus Research, from "One in Three Employees Compromise Corporate Security through Lax Password Practices," at:

http://nucleusresearch.com/news/press-releases/one-in-three-employees-compromise-corporate-security-through-lax-password-practices/

[1] Under US federal regulations (45 C.F.R. § 164.312(a)) implementing HIPAA, "a covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI)." For more information, see the Health Information Privacy page at: http://www.hhs.gov/ocr/privacy/index.html

If a password is *borrowed* by another authorized user, even one with the same access privileges, it compromises the ability of the organization to accurately track critical activity such as financial transactions or drug dispensing, by an individual employee.

A password-only based SSO environment is as vulnerable to security breach as any other system that relies on passwords alone. In fact, the use of a single password for access to multiple systems and applications potentially makes the environment even less secure than it was when each system and application required a discrete password. IBM Security Access Manager for Enterprise Single Sign-On includes usage audit features to identify and quarantine any inappropriate access. Also a password-only approach does not prevent an individual from repudiating responsibility for inappropriate access or use by claiming that the user's password and user ID were stolen.

User convenience

By reducing the number of passwords and user IDs that are required for an individual user, an SSO solution, such as IBM Security Access Manager for Enterprise Single Sign-On, helps an organization address user convenience. In addition to increased user satisfaction with not having to remember and enter multiple passwords, with a single password, a user is less likely to forget a password and be locked out of an application, resulting in higher productivity.

However, in a typical organization where a user accesses multiple applications and data sources, repetitive entry of the password and user ID is still inconvenient. In some settings, such as hospitals and retail business, a user can also access multiple devices and multiple types of devices (such as a workstation, kiosk, and tablet) in multiple locations. Requiring the typed entry of a user ID and password at every location and application, even if it is the same user name and password, affects productivity and user satisfaction.

A good solution

The standard response to the security side of this challenge promoted by SSO solution providers is *strong authentication* through the use of a second method of identification, in addition to a password. In some application areas, such as electronic prescriptions and access to certain government systems, the use of a second authentication method might be required by law. This requirement is often called *two-factor authentication*. Two-factor authentication refers to the use of methods that address two of the three basic information sources that can identify a person:

- Something you know, such as a password
- Something you are, such as a biometric
- Something you have, such as a smart card or RFID card

IBM Security Access Manager for Enterprise Single Sign-On supports smart cards and RFID cards for two-factor authentication.

Strong authentication methods differ with respect to cost and accuracy. However, when employed as a second factor with a password, none of them address making access to systems and data more convenient. Two-factor authentication does not eliminate keystrokes or save time for busy users. Some level of help desk support for the SSO password must still be retained, further limiting productivity savings.

The bar is being raised higher. Users are driven by their experience with smartphones, tablets, and other personal devices. Increasingly the are expecting, if not demanding, that the business systems they use have the same graphical, touchscreen interfaces that rely as little as possible on keyboard-based text entry. The sign-on process is no exception.

The best solution

BIO-key Biometric Service Provider for IBM Security Access Manager for Enterprise Single Sign-On, packaged with the standard release of version 8.2 of IBM Security Access Manager for Enterprise Single Sign-On, meets the challenge. It eliminates the need for users to have or enter a password, except where required by law or policy. With this integrated solution enabled, as shown in Figure 1, the user is positively identified and authenticated at sign-on and any point where reauthentication is required by Windows or an application.

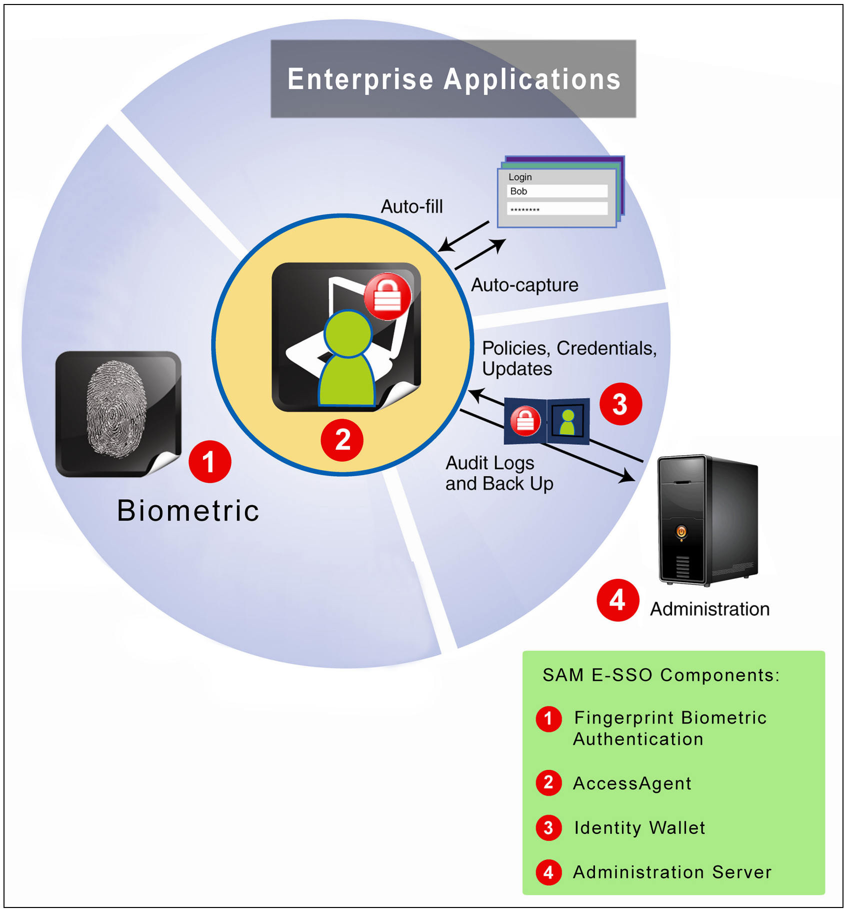


Figure 1 Fingerprint biometric authentication

The process normally takes less time than entry and authentication of a user ID and password alone. It takes less time than typical two-factor authentication that requires a user ID, password, and a smart card or other credential. In a typical work environment, where a user accesses multiple applications in a workday, these time savings can really add up. With quick and easy sign-on, the organization might even implement stronger session time-out limits. Such limits can provide further security protection from inappropriate use or view (in a retail store location or a patient-accessible area of a health facility, for example), without measurably impacting user convenience.

With BIO-key Biometric Service Provider, the user can also lock the workstation or other computer by placing their registered finger on the fingerprint reader (if configured by the administrator). This method replaces usage of Ctrl+Alt+Del and five mouse clicks that might be needed otherwise. Just placing the finger on the reader again can unlock the device.

Business value of BIO-key Biometric Service Provider

The secure finger biometric-based solution that BIO-key Biometric Service Provider offers can enhance the inherent business value of IBM Security Access Manager for Enterprise Single Sign-On in the following ways:

- More accurate user identification for more secure systems
- Enhanced user convenience for increased productivity
- Lower operating costs through reduced help desk and other support
- Reduced initial investment by avoiding second factor authentication

Accuracy

Accurate identification is essential for user authentication under an SSO solution. In terms of business value, providing access to an unauthorized person risks exposure of corporate and customer information. Alternatively, failure to provide access to an authorized user results in downtime and lost productivity.

Finger-based biometrics is generally recognized as the most cost-effective method of accurate identification for authentication purposes. Unlike passwords and *strong* authentication methods, such as smart cards, fingerprints cannot be shared or stolen. The *user* that is authenticated is always the right *person*, assuming that the user was correctly identified at enrollment.

Through an initial enrollment process, the employee's finger is scanned and digitized. Typically a primary finger is designated, and a second finger is scanned for alternate use. The data extracted from the finger scan is converted into a mathematical model, which is used to build a *registration template* that represents the features, or minutiae, of the fingerprint.

Then, when that user signs on to a system or application that is enabled by IBM Security Access Manager for Enterprise Single Sign-On, the finger is scanned and digitized again, and a *reference template* created. That template is then compared with the enrollment database to identify a positive match for user authentication.

Finger-based biometric authentication for IBM Security Access Manager for Enterprise Single Sign-On can be used on any private, shared, or roaming desktop. In addition to sign-on, it can quickly lock and unlock the desktop and switch between users, which is especially important in a shared workstation environment.

Convenience

In terms of business value, more convenient access to organizational systems and data can mean higher productivity and user satisfaction. With BIO-key Biometric Service Provider, finger scanning is straightforward. The enrollment process, which is managed through a series of IBM Security Access Manager for Enterprise Single Sign-On AccessAgent windows, usually takes less than 5 minutes. Images are captured for one finger from each hand of a user, so that an alternate is available if a user's primary finger or hand is bandaged or otherwise compromised at any subsequent sign-on.

Then when a user attempts to sign on, an AccessAgent dialog box prompts the user to place the appropriate finger on the finger reader that is attached to or embedded in the workstation or other device. As soon as BIO-key Biometric Service Provider obtains a usable finger image, it automatically starts the identification process. The match can be completed in a few seconds or less. The user does not have to remember or enter a password. And, unlike a smart-card or other token-based approach, BIO-key Biometric Service Provider does not require the user to carry or fumble with another credential or device.

This high level of convenience and speed is magnified in settings, such as hospitals, where users might physically move among different locations and access the electronic health record (EHR) system and other applications from different devices. These devices might be shared among multiple users, making faster sign-on more critical to convenience and productivity. Convenience is one of the key reasons why a large U.S. metropolitan medical center incorporated BIO-key finger biometrics into its EHR to prescribe controlled substances and to access medical records.

The HIPAA-compliant BIO-key Biometric Service Provider solution can also protect patient privacy by securing a transaction, without requiring a password or other credential that can be easily forgotten, lost, or stolen.

Operational savings

The business value of BIO-key Biometric Service Provider can also be measured in lower operational costs compared to other authentication solutions. In addition to increased user productivity from easier and faster sign-on, BIO-key Biometric Service Provider can help you gain more savings in the following areas:

- Users no longer must update or memorize passwords, make calls to the help desk for password support or reset, nor experience downtime to wait for resolution. Therefore, users and support staff can be more productive.
- Unlike other strong authentication methods, such as smart cards, purchase and distribution of credentials are not necessary. And BIO-key Biometric Service Provider eliminates the ongoing administrative cost (and hassle) of replacing damaged, lost, or stolen credentials.
- One finger reader per machine is less expensive than providing a separate smart card or other token to every user.
- Unlike other biometrics technologies, such as facial and iris recognition, no expensive equipment is required for image capture.

Deployment flexibility

Flexible deployment options can add to the potential cost savings. BIO-key Biometric Service Provider can serve an organization of almost any size or number of locations. It can be deployed concurrently with the initial IBM Security Access Manager for Enterprise Single Sign-On implementation or installed in an existing environment that is enabled for IBM Security Access Manager for Enterprise Single Sign-On.

Although it supports organization-wide use, BIO-key Biometric Service Provider can be deployed to specific users or specific workstations (or other devices) only. In a healthcare setting, for example, finger-based sign-on can be limited to physicians who use workstations in patient-accessible areas. These configurations are made by the administrator by using the IBM Security Access Manager for Enterprise Single Sign-On Machine and User Policy templates.

BIO-key Biometric Service Provider can also be used as part of a true two-factor authentication process for a specific application (or applications) only. For example, this approach can be used to ensure compliance with regulations that require two-factor authentication to prescribe controlled substances through an e-Prescription system. After entry of an SSO password and user ID, the physician user is also prompted for a fingerprint.

With the scripting utility of IBM Security Access Manager for Enterprise Single Sign-On, building this *step-up authentication* is straight forward.

Readers can be attached to a USB port on Windows desktops or notebooks, mostly eliminating any installation time or cost. In addition to inexpensive readers for normal business use, specialized readers are available for specific deployment needs. Such readers can accommodate high volume settings (for example, kiosks), harsh environments (for example, hot or cold weather or dampness), and usage with latex gloves.

Enrollment can be either supervised or user-managed (self-enrollment), as determined by the organization. In addition, training on the process of capturing the finger image correctly can be easily and cost-effectively done online or by using a DVD.

About BIO-key Biometric Service Provider

BIO-key Biometric Service Provider is a set of software services that are integrated with the IBM Security Access Manager for Enterprise Single Sign-On user authentication process and the client and server software components that manage that process. These services are built with the BIO-key Biometric Service Provider software development kit (SDK). BIO-key Biometric Service Provider supports the Biometric Service Provider application programming interface (API) standard version 1.1 as defined by the BioAPI Consortium.[2]

Components

BIO-key Biometric Service Provider comprises two primary services: *image capture* and *image matching*. When installed and configured, these services can be called only by IBM Security Access Manager for Enterprise Single Sign-On.

Image capture service

The BIO-key Biometric Service Provider image capture service manages the process of collecting the finger image from the user. This service uses the IBM Security Access Manager for Enterprise Single Sign-On Authentication Device Manager to digitize the image, extract the key features, and create a mathematical model or template. When installed and enabled, this service is embedded in the AccessAgent client.

BIO-key's patented image-processing technology uses more than 40 levels of image enhancement, ridge, minutia, and vector data to extract useful data from the raw fingerprint to create a highly discriminate template. This process mostly eliminates the possibility of a *false acceptance* or *false rejection* response. False acceptance means that an individual is incorrectly identified and authenticated as a user. False rejection means that a valid user is incorrectly rejected because a match could not be made.

BIO-key Biometric Service Provider currently supports more than 55 fingerprint readers from most major manufacturers. It also supports most embedded readers that are shipped with notebooks and other workstations. For a current list of supported devices, contact BIO-key at one of the telephone numbers listed in “For more information” on page 14.

[2] The BioAPI Consortium, of which BIO-key is a member, was formed to establish an industry standard API to interface with today's most common biometric technologies. For more information about the BioAPI Consortium, see the BioAPI Consortium page at: http://www.bioapi.org

Image matching service

The image-matching service of BIO-key Biometric Service Provider manages the process of comparing BIO-key's highly discriminate templates. It uses the patented BIO-key algorithm that compares over 1500 points of data when received from the image capture service to identify a matching fingerprint, if one exists. In a typical installation, the image-matching service of the BIO-key Biometric Service Provider is embedded in the IBM IMS™ Server and AccessAgent on the client workstation.

Other differentiating factors

In addition to the underlying finger image-processing technology that is used for capture and matching, two other factors differentiate BIO-key Biometric Service Provider: *fingerprint reader independence* and *security*.

Fingerprint reader independence

Biometric algorithms are most frequently bound to specific hardware of a specific manufacturer, limiting its ability to work with other devices and systems. Unlike most all other finger biometric software solutions in the market, BIO-key Biometric Service Provider enables enrollment, identification, and verification. These processes are performed by any of more than 50 finger scanners or readers that are produced by over 30 fingerprint reader manufacturers from around the world.

This unmatched level of support for various readers on the market can have the following impact:

- Plug-and-play flexibility to add or change readers from various current and future suppliers as applications grow and change, eliminating the need for separate SDKs for individual readers. The same single user interface, regardless of device or manufacturer, makes any change transparent to users.
- One-time enrollment for users who then authenticate on any of the supported devices. Users can enroll on one type of reader and then identify on another type of reader at a different location.
- No need for reenrollment when readers are upgraded or changed.

Many popular notebooks, tablet PCs, and workstation keyboards are now shipped with integrated fingerprint readers. These readers can be used to establish a user's identity. Also organizations can immediately use fingerprint readers on their existing notebooks, tablets, and keyboards, further reducing implementation and operational costs.

Security

In addition to adding biometric security to systems and applications enabled by IBM Security Access Manager for Enterprise Single Sign-On, BIO-key Biometric Service Provider adds *security to the biometric* at every capture, transmission, and use point. Because the data from the digitized image capture is stored as a mathematical template, the user's actual fingerprint image is not kept on any computer or in any database. Templates can be disabled, marked inactive, or removed from the system. This flexibility gives the system administrators control in all situations.

Data communications security is provided through elliptic curve public key infrastructure (PKI)-style encryption and RSA enveloping encryption, both containing four key-length variations. In addition to strong session management, the server uses a predefined and secret public key to encrypt the initial message, which contains only command and session data.

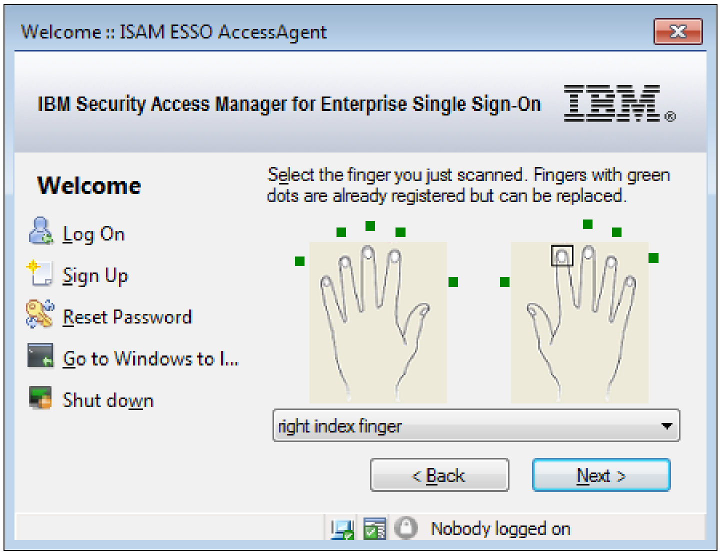
Process flow

The image capture and image-matching services of BIO-key Biometric Service Provider are started in the process flow at initial enrollment and subsequent sign-on.

User enrollment

The image capture service of BIO-key Biometric Service Provider manages the process of capturing the finger image at initial enrollment, or whenever the user enrolls another fingerprint, and creating the registration template. To associate the registration template created at enrollment with the correct user, IBM Security Access Manager for Enterprise Single Sign-On uses the user account that was created during user registration. This user account might optionally be associated with an Active Directory repository or other Lightweight Directory Access Protocol (LDAP)-based repository.

The windows for registering the user's fingerprint and associating it with the user's name and password are already built into AccessAgent. From the main Welcome window, the user scans the finger to be registered. The AccessAgent then prompts for the user's IBM Security Access Manager for Enterprise Single Sign-On user name. After the user enters their name, AccessAgent verifies that the fingerprint is not already registered and prompts the user for the IBM Security Access Manager for Enterprise Single Sign-On password. When authenticated, the user selects the appropriate finger (such as the right index finger) from an image of two hands, as shown in Figure 2.



Select the finger you just scanned. Fingers with green dots are already registered but can be replaced.

right index finger

Figure 2 Finger image capture

The number of fingers that can be captured is one finger up to ten fingers. A registration template of at least one finger from each hand is created so that a second fingerprint is available for match if the primary finger is bandaged or otherwise unusable for matching.

Quality control is built into the enrollment workflow to ensure that data is collected. The image capture service of BIO-key Biometric Service Provider is preconfigured to scan the enrollee's finger three times and to select the best capture for the registration template. AccessAgent prompts the user to scan the same finger a fourth time to verify the correctness of the captured registration template. If any of the scanned images are invalid, AccessAgent provides the appropriate error message (for example, "finger scanned too much to the right") and prompts for resubmission.

During enrollment, the workstation or other device must be connected to the network and to the IMS Server so that the registration template can be transmitted and stored with other templates of approved users in the IMS Server database. As a configuration option, this registration template can also be *cached* in the user's AccessAgent Wallet on the workstation. Caching the registration template has two purposes:

- It enables login without keyboard entry of the user name.
- It can be used for faster user access to the desktop or in other special circumstances.

Consider that a user's privileges might be revoked because, for example, the user is no longer employed by the company or is no longer granted access to the system resources. Subsequent to initial enrollment, if the user's privileges are revoked, their registration templates are removed from the IMS Server database when the user is deleted. Typically this practice is done by the administrator or the Help Desk. If the user re-enrolls on another workstation (creating another template), the template is replaced in the IMS Server database. Revoked and replaced registration templates are removed from the cached Wallet on the workstation whenever that user is connected to the IMS Server for authentication.

Sign-on

Finger-biometric based authentication can be used wherever the SSO password might be used, including Windows logon, desktop applications, and access to network applications and data. After successfully logging in to AccessAgent by using an enrolled fingerprint, the user can log on to Windows. IBM Security Access Manager for Enterprise Single Sign-On provides a custom GINA (for Windows XP) and Credential Provider (for Windows 7). With the GINA or Credential Provider option enabled in AccessAgent, the user logs on to that service first with a fingerprint. AccessAgent then completes an auto-logon into Windows.

On the Windows desktop, the authenticated user can access desktop applications. IBM Security Access Manager for Enterprise Single Sign-On provides automated sign-in to network applications and databases, as permitted by the user's profile.

IBM Security Access Manager for Enterprise Single Sign-On includes a set of configurable policies. The administrator can set them to determine when and where the registration templates that are cached in the user's AccessAgent Wallet (if implemented) and that are stored in the IMS Server database are used for matching.

In a typical organization where fingerprints are re-enrolled or templates are revoked only occasionally, IBM Security Access Manager for Enterprise Single Sign-On provides an authentication mode for access to applications and data, even when the network is slow. Two machine-level policy options can be configured to allow for immediate login to the Windows desktop:

- The *Fast Logon* policy operates much in the same way as an offline login process. When this policy is enabled (which it is by default), IBM Security Access Manager for Enterprise Single Sign-On first uses the locally cached registration template, if available, for authentication.
- After AccessAgent connects to the desktop, a second machine-level policy option, *Background Authentication*, triggers a background check against the registration template on the IMS Server to detect revocation or re-enrollment update of the template.

With this validation deferred to a transparent background service, the user accesses the desktop more quickly and the organization is assured that the correct person is logged in. If registration templates are not cached locally, this Fast Logon option is not available.

IBM Security Access Manager for Enterprise Single Sign-On also provides authentication configuration options for operational settings in which there is frequent revocation or re-enrollment. For example, users have access to multiple machines and might re-enroll from any of those machines. Authentication configuration options are also available for less common settings where there is no re-enrollment or revocation activity.

Figure 3 illustrates a typical process flow for finger biometric-enabled authentication at sign-on through IBM Security Access Manager for Enterprise Single Sign-On (shown as ISAM E-SSO in Figure 3).

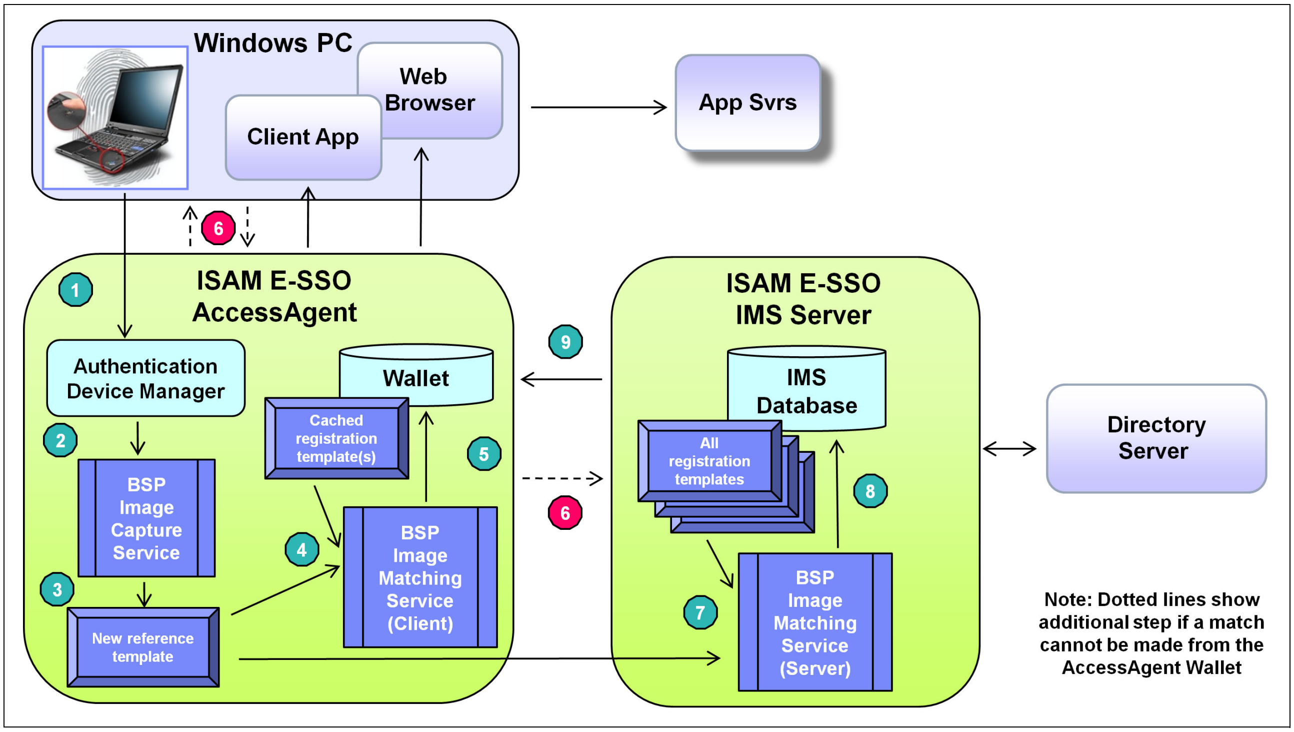

Windows PC
Web Browser
Client App
App Svrs
6
ISAM E-SSO AccessAgent
1
Authentication Device Manager
Wallet
Cached registration template(s)
2
BSP Image Capture Service
5
4
BSP Image Matching Service (Client)
3
New reference template
9
6
ISAM E-SSO IMS Server
IMS Database
All registration templates
8
7
BSP Image Matching Service (Server)
Directory Server
Note: Dotted lines show additional step if a match cannot be made from the AccessAgent Wallet

Figure 3 Typical finger biometric process flow

In this example, the organization cached the registration template that is captured by the image capture service of BIO-key Biometric Service Provider in the user's AccessAgent Wallet on the workstation. The organization stores it on the IMS Server database. With only occasional re-enrollment or revocation of fingerprints, the administrator enabled Fast Logon with Background Authentication against the image-matching service of BIO-key Biometric Service Provider.

The authentication process entails the following actions:

1. The user initiates the authentication process by placing a designated finger on the reader that is attached to or embedded in the workstation.
2. The scanned image is sent to the image capture service of BIO-key Biometric Service Provider.
3. The image capture service of BIO-key Biometric Service Provider creates a reference template.
4. The image-matching service of BIO-key Biometric Service Provider in AccessAgent compares the reference template against the registration templates that are cached in the AccessAgent Wallet.
5. A positive match result is reported to the Wallet where it is associated with the user's profile. With *Fast Logon* enabled, the user has immediate access to the desktop.
6. If no match is made to any cached template, AccessAgent prompts the user for a user name and transmits the user name with the reference template to the IMS Server for

authentication. The no-match situation usually occurs when users are not at their personal workstation or are at one that is normally shared. If the IMS Server is unavailable, the user cannot be authenticated.

7. The reference template is matched with the registration template that is associated with the user name provided by the Directory Server and stored in the IMS database by the server-level image-matching service of Biometric Service Provider. With *Fast Logon* and *Background Authentication* enabled, this step is deferred until the user logs on to the desktop.
8. A positive match result is reported to the IMS database where it is associated with the user profile.
9. Authentication is reported by the IMS Server to AccessAgent on the workstation that then provides access to appropriate network applications and databases in accordance with the user profile.

Software installation and configuration

BIO-key Biometric Service Provider is an optional enterprise authentication service in the standard release of IBM Security Access Manager for Enterprise Single Sign-On version 8.2. All required software, including reader drivers, is shipped with IBM Security Access Manager for Enterprise Single Sign-On. BIO-key Biometric Service Provider can be installed and configured by a system administrator or through integration services that are available through the IBM Global Services Group, IBM Security resellers, or directly from BIO-key.

Case studies

BIO-key's core fingerprint-based solutions are successfully used in a range of commercial, healthcare, and public sector organizations. This section provides two examples that demonstrate the use of BIO-key finger biometrics for sign-on.

Real-world testimonials: To learn more about BIO-key's real-world success, see the BIO-key testimonials page at:

http://www.bio-key.com/about/testimonials.html

Case study: Healthcare

The first case study presents a 300-member physician practice affiliated with a major metropolitan hospital.

Challenge

Doctors and staff were becoming increasingly frustrated with having to remember and periodically reset their passwords for access to their EHR system.

Solution

The EHR solution provider turned to BIO-key for a more convenient and secure alternative to the password system for their physicians and staff to use to access patient records. The solution provider now offers the BIO-key's fingerprint ID software as a more secure, convenient option to passwords as part of its standard Enterprise EHR Solution.

Now doctors place a finger on a reader to establish their identity when they sign in to the EHR software. They can sign physicians notes, prescribe controlled substances, and gain access to patient data that is protected through the Enterprise EHR.

The BIO-key software reads the fingerprint and matches it against a database of authorized users' fingerprints. Only when the match is successful, the clinician can then gain access to the EHR. The entire process takes less time than it takes to type in a password and is far more secure.

Benefit

The HIPAA-compliant BIO-key solution enhances the security of the EHRs, delivers superior accuracy, and works with every major fingerprint reader. Fingerprint identification guarantees that each patient's private medical information remains private.

Although passwords can be stolen or inappropriately shared, a doctor's fingerprint cannot. For physicians, the constant reset of passwords is an inconvenience. Using a finger to access information is considerably more convenient and allows doctors to focus on patient care. It is more secure than using passwords and ensures that only authorized staff access patient records.

Case study: Retail

The second case study examines a national cellular carrier's retail store division.

Challenge

To free in-store sales staff from stationary point-of-sale (POS) terminals, a national cellular carrier implemented a mobile POS platform based around small but powerful tablet PCs. With this platform, in-store staff was able to conduct transactions that range from answering account questions to processing accessory purchases, anywhere in the store. Because these devices operate wirelessly, federal regulations and the company security policy required protected access to these devices and the back-end retail systems with strong authentication at a user level, not at a device level. In addition, the mobile devices are shared among retail staff. Therefore, authentication is performed frequently. Traditional strong authentication methods, such as One Time Password devices, proved too cumbersome to use with the mobile form factor and stylus entry.

Solution

By using the fingerprint biometric platform from BIO-key, the company's retail staff can authenticate to the network and their POS applications with just a swipe of a finger on the tablet's built-in scanner. Any sales representative from any store can pick up any tablet, swipe their finger, and be immediately authenticated.

Benefit

Employees strongly prefer the BIO-key authentication method to passwords or token-based approaches, because it makes the login process easier, with nothing to carry, remember, or lose. At the same time, the company is assured that only authorized staff can initiate certain functions, such as approving overrides, because the biometric credential cannot be shared or stolen.

Summary

BIO-key Biometric Service Provider delivers a better way to identify and authenticate. No longer do users have to remember a password or carry an ID card. With fingerprint biometric identification, when accessing systems and enterprise applications protected by IBM Security Access Manager for Enterprise Single Sign-On, a user must place a finger on a reader for accurate identification.

This proven solution for SSO offers the following advantages:

- Makes the systems and data of an organization more secure
- Helps the workforce become even more productive, in addition to reducing support costs
- Optimizes the investment of an organization in IBM Security Access Manager for Enterprise Single Sign-On

With BIO-key Biometric Service Provider, an organization does not have to compromise on security or user convenience because it gets the best of both. The use of finger biometrics can eliminate the security threat of stolen or borrowed passwords and strong authentication credentials, ensuring that the user authenticated is the person authorized. The elimination of keyboard entry of a password can make sign-on more convenient and can make busy users more productive. By eliminating calls to the Help Desk because of a forgotten password, BIO-key Biometric Service Provider can reduce support costs.

By using BIO-key Biometric Service Provider, an organization can realize the highest value from its investment in an SSO solution. Because it is already integrated and packaged with the standard release of IBM Security Access Manager for Enterprise Single Sign-On, BIO-key Biometric Service Provider can be deployed with any existing or planned implementation. Support is available directly from IBM. With fingerprint reader independence and multivendor reader support, an organization can use existing embedded readers and add readers from different vendors in the future, without requiring system redesign or user re-enrollment.

For more information

For more information about BIO-key Biometric Service Provider and IBM Security Access Manager for Enterprise Single Sign-On, call BIO-key International at (866) 846 2594 (North America) or +1 732 359 1110 (international). In addition, see the following references:

- The BIO-key website

  http://www.bio-key.com
- IBM Security Access Manager for Enterprise Single Sign-On

  http://www.ibm.com/software/tivoli/products/access-mgr-esso/
- *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350

The team who wrote this guide

This Redguide publication was produced by BIO-key International in collaboration with the IBM International Technical Support Organization (ITSO).

Myles Tillotson is a product marketing consultant with BIO-key. He has written extensively on the application of enterprise software solutions for business and government, including case studies, customer requirements definition, system use cases, and user training guides. Before joining BIO-key, Myles worked for Unisys Corporation and the United States Federal

Government, where he began as a Presidential Management Intern. He holds a Master of Business Administration degree from the Fox School of Business, Temple University (Philadelphia, PA).

Sean Dyon is a senior BIO-key software engineer, with more than 10 years of software development, implementation, and product management experience. He developed finger biometric-based authentication solutions for users in healthcare, other industries, and with BIO-key partners. Sean provides ongoing support to IBM for the integration of BIO-key Biometric Service Provider with IBM Security Access Manager for Enterprise Single Sign-On. Sean studied Computer Information Technology at Indian River State College (Fort Pierce, FL).

Many thanks to the following people for their contributions to this project:

Mira LaCous, Vice President, Technology and Development
Dennis Wilcox, Director of Sales
BIO-key

Axel Buecker, ITSO Project Manager
Vivek Shankar, Software Engineer at the Singapore Software Lab
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

`http://www.ibm.com/redbooks/residencies.html`

Stay connected to IBM Redbooks

Find us on Facebook:

`http://www.facebook.com/IBMRedbooks`

Follow us on Twitter:

`http://twitter.com/ibmredbooks`

Look for us on LinkedIn:

`http://www.linkedin.com/groups?home=&gid=2130806`

Explore new IBM Redbooks® publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

`https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm`

Stay current on recent Redbooks publications with RSS Feeds:

`http://www.redbooks.ibm.com/rss.html`

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4892-00, was created or updated on July 18, 2012.

Trademarks