White Paper

A Comparison of Automated Sign-On Options for the Mainframe

opentext™

Mainframe Security Needs to Catch Up

The mighty mainframe is not a computing dinosaur. This powerful, high-volume machine still runs much of the corporate world's most mission-critical applications. In other words, it's not going away anytime soon. The problem is that many mainframe applications, some written decades ago, are hard-coded to handle weak case-insensitive passwords with just eight characters. That was fine back in the day, but not anymore.

Today's increasingly sophisticated security threats require something substantially stronger and easier to manage. Solutions do exist for moving beyond outdated password limitations, but how do you know which one is best for you? This paper investigates each major option and provides helpful selection guidelines.

The Problem with Mainframe Passwords

A mainframe probably just approved your recent ATM withdrawal or processed your last insurance claim. But capable as they are, mainframes have some quirks that make them odd-man-out in the modern enterprise. One of those quirks is the mainframe application password. Here's why it's problematic:

- **Misalignment with modern security needs**

  Once upon a time, networks and hackers didn't factor into our everyday lives. It's a different story now, which is why most devices and applications require a password for access. But passwords alone aren't enough. Their effectiveness depends on password standards and password management.

  Best practices veto sticky-note reminders on monitors, for instance, and prescribe ten-to-twelve character passwords with at least one capital letter and one special character. From a management perspective, a single password for access to all network resources, including mainframe applications, is simplest. But no one wants to dumb down enterprise-wide passwords to eight characters.

- **Password-management headaches**

  Most people have a tough time remembering all of their passwords. Each time they forget, the password must be reset by a systems administrator—a mundane, labor-intensive task that diverts attention away from more meaningful IT projects.

  According to the Gartner Group, 20 to 50 percent of all help desk calls are for password resets. And Forrester Research states that the average help desk labor cost for a single password reset is about $70*. Statistics may vary, but the fact remains: Password management is a waste of time and money.

*www.mandylionlabs.com/PRCCalc/PRCCalc.htm

- **An extra, outmoded step for users**
  When users log on to their computers, they typically gain access to all authorized enterprise resources—except for the mainframe. To access their mainframe application, they're forced to sign on again. And then again, for every mainframe application they access. In our era of instant access to network resources, this extra step is a relic from the past.

From security risks to IT management headaches and usability, logging on to the mainframe using an eight-character password is a practice in need of an update. But how do you choose from the available options?

Which Solution Is Right for You?

A handful of possible solutions is available for reinforcing security, getting IT departments out of the password-management business, and improving usability. These solutions—including highlights, considerations, and selection guidelines—are described below.

Enterprise Single Sign-On (ESSO)

ESSO is technology that eliminates the need for users to enter their credentials each time they access a network resource (including mainframe applications). Users authenticate just once using the enterprise's standard authentication method. From that point forward, the ESSO solution automatically signs on the user each time he or she accesses a network resource.

HOW IT WORKS

The ESSO credential store securely saves the logon information—usernames and passwords—for all users and all resources across the enterprise. Each time the user accesses a resource that requires the user to log on, the ESSO desktop agent intercepts the logon prompts, fetches the user's credentials for that resource from the credential store, and passes the credentials to the application. This process is transparent to the user and the application.

ESSO integration with mainframes works the same way. The ESSO desktop agent interacts with the mainframe application via the terminal emulator's HLLAPI interface. When the mainframe presents a sign-on screen, the agent populates it with the user's credentials, which are retrieved from the credential store.

HIGHLIGHTS

- **Requires no changes to the mainframe application**
  The mainframe application has no knowledge that an ESSO solution is behind the user sign-on process. After prompting the user for ID and password, the mainframe receives the credentials from the client. The application then checks those credentials with the mainframe's security access framework to authenticate the user—just as it always does.
- **Leverages existing enterprise authentication methods**
  No single authentication method is mandated for mainframe sign-on. ESSO leverages the enterprise's standard authentication method to identify the user and then retrieves the mainframe credentials for that user from the credential store. Even though the ESSO solution uses the eight-character mainframe application password to sign on the user, the user could have originally authenticated to the ESSO solution using username/password, a digital certificate, or a one-time-use token.
- **Includes mainframe applications at no extra cost**
  Depending on how your ESSO solution is licensed, adding mainframe sign-on may be included at no extra charge. Integration and maintenance costs still apply, but most ESSO solutions are licensed on a per-user basis regardless of the applications connected to the ESSO solution.

CONSIDERATIONS

- **Uses static passwords**
  Even though users don't manually enter their static password, it is still being used to sign on to the mainframe application. Therefore, mainframe security remains dependent upon users safeguarding their passwords, and IT departments are still on the hook for mainframe password management.
- **Is implemented as an enterprise-wide infrastructure solution**
  ESSO is almost never implemented just for mainframe access, but rather for access to all enterprise resources. Consequently, ESSO projects are typically large, costly, and span multiple years because they cut across many IT infrastructure types. Mainframe access often comes at the end, if at all, of a long ESSO deployment.
- **Requires integration of the desktop agent and the terminal emulator**
  ESSO complicates your mainframe access infrastructure. Because the ESSO desktop agent must be integrated with the terminal emulator via HLLAPI, there is more host-access related software on the desktop to manage. For example, every time you upgrade your terminal emulator, you have to ensure that the integration between the emulator and the ESSO desktop agent continues to work as expected. Depending on the emulator upgrade, the integration may need to be tweaked or recoded altogether.

IS ESSO RIGHT FOR YOU?

Has your organization already deployed an ESSO solution? Does your ESSO solution support mainframe applications? Does your corporate security policy allow static, eight-character passwords for mainframe authentication? If so, ESSO may be a viable option for automating the mainframe sign-on process.

Express Logon Feature (ELF)

ELF, also referred to as Certificate Express Logon, is an IBM solution that allows users with an X.509 certificate to automatically sign on to a mainframe application.

HOW IT WORKS

The terminal emulation client establishes an SSL/TLS connection with the Telnet server to establish the mainframe session. The emulation client then executes the logon macro, which inserts placeholders into the user ID and password fields. The Telnet server requests the user's mainframe user ID—based on the client certificate that was provided during the SSL/TLS handshake—and a time-limited, single-use PassTicket from RACF. The Telnet server then inserts the mainframe user ID and PassTicket into the placeholders from the logon macro and automatically signs on the user to the mainframe application.

HIGHLIGHTS

- **Eliminates password management**
  Because ELF employs PassTickets to sign users on to a single mainframe account, the burden of static password management is eliminated for that account. In other words, no more help desk calls for forgotten passwords.
- **Supports a two-tier architecture**
  ELF's two-tier design means that you can add automated mainframe sign-on into your environment without additional middleware.
- **Allows identity mapping in RACF**
  There's no need to implement a separate data store or LDAP directory to manage mappings between users' enterprise identities and mainframe user IDs. The user's digital certificate can be added to the user's account information directly in RACF.

ESSO: The Takeway

If your organization already has an ESSO solution, then start with that. But if you need to move away from static passwords altogether, look for a solution that uses time-limited, single-use PassTickets.

ELF: The Takeway

ELF provides a high level of security with PassTickets and is supported in the leading terminal emulation clients. But if your users don't employ X.509 certificates for authentication, or if they have more than one mainframe user ID, then you'll need a more flexible solution.

CONSIDERATIONS

- **Requires an X.509 certificate for user authentication**
  While the two-factor authentication method using digital certificates is highly secure, it is expensive to implement and manage. Today, most organizations employ username/password authentication, which isn't compatible with ELF.
- **Supports just one mainframe user ID per user**
  Because a user's certificate can only be mapped to a single mainframe ID in RACF, ELF's automated sign-on capabilities work only for users with one mainframe user ID. In other words, ELF cannot support the following two types of users:
  1. Users with access to multiple mainframe applications. In this scenario, ELF works only if the user ID is the same for all mainframe applications, which may not be possible in every environment.
  2. Users with multiple IDs for a given mainframe application. This scenario occurs when a user is granted different levels of privilege depending on the task at hand.
- **Requires that certificates be remapped every time they are updated**
  RACF's mapping between the user's certificate and mainframe ID is tied to the certificate itself, not to the user's identity. Each time the client certificate is updated—typically every two to three years for security reasons—the user's mainframe ID has to be remapped to the new certificate in RACF.

IS ELF RIGHT FOR YOU?

If your users have just one mainframe user ID and if digital certificates are part of your security infrastructure, then ELF may work for you. Otherwise, look for a more flexible solution.

Automated Sign-On for Mainframe Add-On

OpenText™ Host Access Management and Security Server (MSS) Automated Sign-On for Mainframe Add-On software works with OpenText™ terminal emulation software to automatically sign on users to IBM 3270 applications. In addition to eliminating static passwords, Automated Sign-On for Mainframe works with a variety of authentication methods to provide stronger mainframe application security without recoding.

HOW IT WORKS

When a user launches a mainframe session, the emulator's logon macro requests the user's mainframe credentials from Automated Sign-On for Mainframe. Automated Sign-On for Mainframe employs the user's enterprise identity to get the mainframe user ID. Then, working with the IBM z/OS Digital Certificate Access Server (DCAS), Automated Sign-On for Mainframe obtains a time-limited, single-use RACF PassTicket for the target application. It returns the mainframe user ID and the PassTicket to the terminal emulator's logon macro, which sends the credentials to the mainframe to sign on the user to the application.

HIGHLIGHTS

- **Eliminates password management**
  Automated Sign-On for Mainframe enables the use of PassTickets (instead of static passwords) to sign on to mainframe applications. As a result, mainframe passwords are no longer needed, and IT staff can stop resetting those that are lost or forgotten.
- **Supports a variety of authentication methods**
  Automated Sign-On for Mainframe works seamlessly with existing Identity and Access Management (IAM) systems—from directory-based username/password credentials to digital certificates (although digital certificate are not required).
- **Supports multiple mainframe user IDs**
  Automated Sign-On for Mainframe can map multiple mainframe user IDs to a single user, so users with several mainframe accounts can use automated sign-on for all of them.

CONSIDERATIONS

- **Employs a three-tier architecture**
  Automated Sign-On for Mainframe is deployed on a middle-tier server—running between the terminal emulation client on the workstation and the application on the mainframe—to retrieve the PassTicket from the z/OS DCAS service.
- **Is based on mapping of the mainframe identity to the enterprise identity**
  Once a user has been authenticated, the IAM system provides the user's enterprise identity to Automated Sign-On. In order for Automated Sign-On to function, IT must provision the Automated Sign-On system with a mapping of the user's enterprise identity to the user's mainframe identity.
- **Uses DCAS service**
  The IBM Digital Certificate Access Service (DCAS) must be enabled on the mainframe. DCAS is a component of the z/OS Communications Server (the z/OS TCP/IP networking stack). It is included with z/OS, but is not installed by default.

About PassTickets

PassTickets are dynamically generated by RACF each time users attempt to sign on to mainframe applications. Unlike static passwords, PassTickets offer replay protection because they can be used only once. PassTickets are also time-limited, meaning that they expire after a defined period of time (10 minutes by default), even if they have never been used.

Automated Sign-On for Mainframe: The Takeway

Like ELF, Automated Sign-On for Mainframe provides a high level of security with PassTickets. The difference lies in its flexibility. Automated Sign-On for Mainframe supports a variety of authentication methods and allows you to map multiple mainframe user IDs to a single user.

Is Automated Sign-On for Mainframe Right for You?

Are you being asked to strengthen the security of your mission-critical mainframe applications? Do you want to get out of the mainframe-password management business? Do you need the flexibility to support non-certificate-based authentication methods and multiple mainframe IDs for a single user? Automated Sign-On for Mainframe offers a safe, effective way to strengthen mainframe security without recoding the mainframe application.

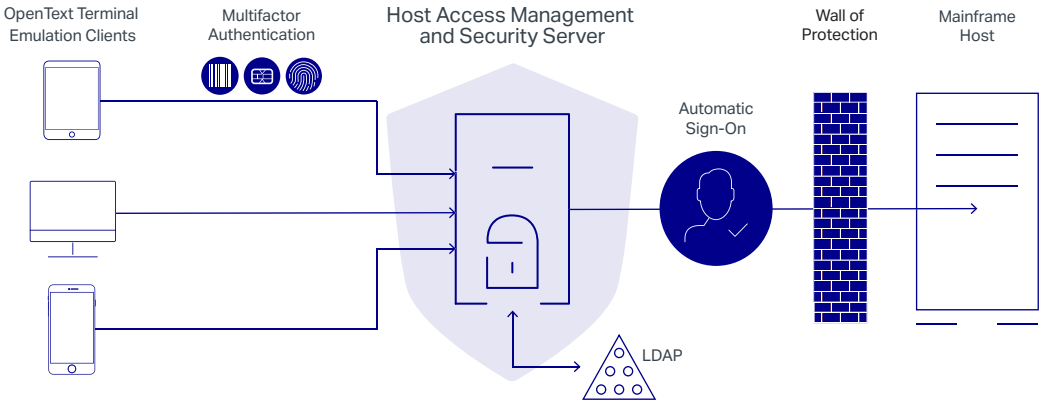

Figure 1. Users no longer need to take the additional step of entering a password to log on to their host applications after authenticating to Host Access Management and Security Server (MSS). MSS Automated Sign-On for Mainframe Add-On handles that for them.

Invite Mainframe to the Party

The mainframe isn't going the way of the dinosaur, so don't treat it that way. There are ways to move it into your modern security framework and leave the outmoded eight-character password requirement behind. Once you understand the way these solutions work, you'll be able to select the best option for your enterprise.

Learn more at
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™