WHITE PAPER ENTERPRISE SINGLE SIGN ON

tools4ever

TABLE OF CONTENTS

Introduction 3

Password complexity 3

Advantages of Single Sign On 4

Why Single Sign On? 5

SSO support 5

Enterprise SSO and Authentication Management 6

Authentication Management 6

SSO-software Vendors 7

Architecture 8

ARCHITECTURE - Automated login 8

E-SSOM Client 9

E-SSOM Service 9

Login Configuration Management 10

ARCHITECTURE - AUTHENTICATION MANAGEMENT 11

Additional checks 11

ARCHITECTURE - Fast User Switching- SHARING A WORKSTATION 13

ARCHITECTURE - Follow Me 14

ARCHITECTURE - Failover/Load balancing 14

ARCHITECTURE - Identity Management Integration 15

Reporting 15

Appendix I: Authentication equipment 16

Introduction

Medium to large organisations operate complex networks comprising of a variety of applications running on multiple systems. Users need to have access to various applications for things such as e-mail, the helpdesk, document management, customer data and operational & financial processes. In order to comply with increasingly strict security requirements, end-users have to enter separate username and password combinations for each application. This can easily involve entering credentials for 12 different applications or more [Source: SINGLE SIGN ON SURVEY REPORT, July 2011]. This produces a number of issues:

- The manual entry of credentials is time-consuming and far from user-friendly.
- Users manage their usernames and passwords with unsafe techniques, e.g. sticky notes, pieces of paper, very simple passwords, etc.
- The helpdesk frequently fields calls from users who have forgotten their passwords, resulting in elevated support costs.

Password complexity

For system administration and information security, various (counter) measures are taken to keep the network safe, such as using complex passwords, setting a maximum validity period for passwords and instructing users not to write down their passwords. These measures produce increasing frustration amongst users, and more often than not, a deluge of password reset calls to helpdesk.

These issues gave rise to the development of Enterprise Single Sign On (SSO) solutions. Once a SSO solution has been set –up, users only have to log into each application once, after which the SSO solution will automatically remember each set of credentials used for each application.

The single login can be further simplified and secured by expanding SSO with authentication management. Then the login credentials are no longer based on a username and password, but are replaced by a combination of a smartcard and PIN code. Users will then be able to log in by presenting their smart card to a card reader connected to their PC and entering a PIN code. This means they no longer have to remember any (complex) passwords, yet still have direct access to all authorised applications across the network. The result is secure access (based on two-factor authentication) as well as optimum user convenience.

This whitepaper outlines the possible benefits that Enterprise SSO and authentication management (smart card-based login) can offer organisations.

ADVANTAGES OF SINGLE SIGN ON

Single Sign On offers organisations various important benefits. The main advantages include:

- *Enhanced user convenience and productivity*
  End users get quick and easy access to all the required resources, yielding greater productivity.

- *Mitigation of security risks*
  End users no longer have to jot down usernames and passwords on a slip of paper and keep it near their machine.

- *Greater security of the corporate network*
  SSO prevents users from gaining/having unauthorised access to the corporate network. They will only have access to applications for which they have right of entry.

- *The helpdesk is burdened with less password reset calls*
  End users are less likely to forget their passwords as they only have to remember one. This results in reducing password-related helpdesk calls.

- *Improved service levels*
  Since the helpdesk receives fewer password-related calls, their time can be focused on more critical issues, thus improving service levels.

- *Compliance (HIPAA, SOX, etc.)*
  SSO offers various compliance options:

  - Authentication management makes it possible to introduce strong authentication (two-factor authentication) without compromising user convenience.

  - In a single SSO action, access to the entire network for an end user can be revoked rather than for each individual application.

  - SSO provides reporting on the date and time users' accounts have been accessed.

  - SSO offers the ability to perform various additional checks before users are logged in. An example is to give business-critical applications an additional security layer that verifies whether the correct end user is attempting to access the system. A smart card or PIN code can be used for this.

Why Single Sign On?

Why should organisations implement an SSO solution? There are two main reasons, namely user convenience (1) and enhanced information security (2).

For end users, user convenience is an important priority. In this situation, the demand for an SSO implementation comes from within the organisation (rather than from IT or security). This involves the demand to simplify the login process and to reduce the number of login actions, which can be triggered by business efficiency objectives (budgetary concerns) or other common reasons, such as:

Making applications available to all employees rather than to just a small group. For instance, all employees may have to register their work activities in the ERP system. Another scenario is the distribution of salary slips electronically rather than by post.

The introduction of a company-wide system to which everybody must log in.

Information security enhancement is often driven by changes in legislation and regulations (HIPAA, SOX, etc). A common change is the introduction of strong authentication. Technically this is simple to implement with password complexity, but this often results in a strong decline in user convenience as they have grown accustomed to their limited character passwords.

Lack of user convenience produces various negative side effects. Users will scribble their passwords on slips of paper, will share credentials, will phone the helpdesk to have their passwords reset, etc.

One way to increase user convenience along with implementing strong authentication, is to combine an SSO solution with authentication management. The latter will allow end users to log on to Active Directory quickly and conveniently using an authentication token such as a smart card. The SSO software will ensure that users are automatically logged in when they launch an application. This means users will no longer have to authenticate themselves afterwards by logging in to applications, which instead will be handled automatically by the SSO software.

SSO support

The implementation of a third-party SSO is not required by definition if all the applications in the network, or at least the commonly used applications, provide native support for SSO, e.g. through integrated LDAP authentication based on Active Directory. Unfortunately integrated SSO is not always supported. In other scenarios, an additional application management effort is required because the relations between application accounts and Active Directory accounts have to be tracked. Integrated SSO is often supported by current applications, but generally not by legacy or Cloud/SaaS applications.

ENTERPRISE SSO AND AUTHENTICATION MANAGEMENT

There are many different types of Single Sign On. This white paper focuses on **Enterprise** SSO. Enterprise SSO (E-SSO) is based on the idea that all target systems (applications, systems and platforms) across the organisation (LAN) as well as outside the organisation (SaaS/cloud) can be controlled through an automated login procedure — regardless of whether the target system supports an authentication pool such as integrated authentication, Kerberos, NTLM, SAML or LDAP authentication.

To operate properly, E-SSO does not have to be integrated with one of the authentication protocols mentioned above. E-SSO solutions can recognise login screens, automatically enter credentials and click the login button.

E-SSO ensures an automatic login to all applications and systems for which the end user has been assigned access permissions. The advantage of this concept is that E-SSO can be deployed quickly in any network and supports 100% of the application and system landscape. This means E-SSO is not dependent on a software vendor's native support for a default authentication protocol.

AUTHENTICATION MANAGEMENT

As soon as the application landscape has been secured on the basis of a single username and password, many organisations will want to enhance the security of the single access verification. A key reason for introducing strong authentication is the need to comply with stricter legislation and regulations. The introduction of a complex password is usually not sufficient and often causes end user resistance. A better alternative is to implement two-factor authentication based on a smart card (something you own) and a PIN code (something you know). Implementing two-factor authentication requires the creation of a link between a smart card and a username/password in Active Directory. This type of functionality is referred to as authentication management. Authentication management provides this link, and also handles the registration of smart cards, integration with the login screens (XP, Vista, Cisco, Juniper, Windows 7 etc.) and the control of the card reader hardware. [1]

[1] This white paper refers to a 'card reader'. However, authentication is not limited by definition to reading smart cards. E-SSOM supports a host of authentication tokens. Appendix I includes a complete overview of supported devices. All references in this document to ´card reader ´ are thus understood to mean any of the authentication tokens listed in Appendix I.

SSO-software Vendors

There are various SSO solutions vendors. With its Enterprise Single Sign On Manager (E-SSOM) suite, Tools4ever offers a company-wide SSO solution with innovative features such as two-factor authentication, fast user switching and follow-me. These features will be discussed in the next chapter.

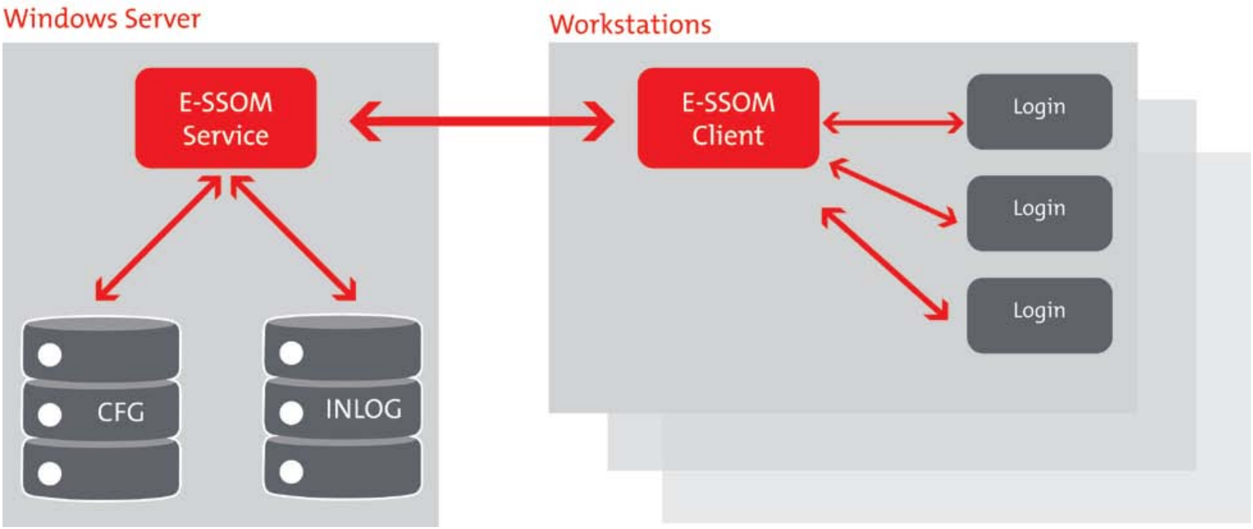
ARCHITECTURE

This chapter provides an overview of the main architectural components of E-SSOM. The following components are described in further detail:

1. Automated login (traditional SSO)
2. Authentication management (card-based login)
3. Fast user switching (the ability to log in to a network or log off, quickly)
4. Follow me (the ability to launch a Citrix session quickly)
5. Failover/load balancing (ensuring speed and reliability)
6. Integration of identity management (integration with user account and password management)

ARCHITECTURE - AUTOMATED LOGIN

Below is a schematic overview of the E-SSOM architecture for the automatic handling of login screens.



E-SSOM Client

The E-SSOM Client is installed on every workstation in the network. This service monitors for the display of login dialogues. This is an event-driven rather than polling-based mechanism. In other words, the E-SSOM Client will only be activated if there is a relevant event, e.g. a user logging in or out of an application. E-SSOM offers a broad range of methods for detecting the correct event and dialogue. In fact this is E-SSOM's most important feature, as it enables the detection of all applications in the network. E-SSOM supports virtually any imaginable application, including DOS, TelNet, Oracle, SAP, Mainframe, Java, browser (SaaS/cloud) and traditional client/server software. Therefore the E-SSOM Client ensures that end users are automatically logged in to their applications in the right way and with the correct credentials. The information required for this is provided by the E-SSOM Service.

E-SSOM Service

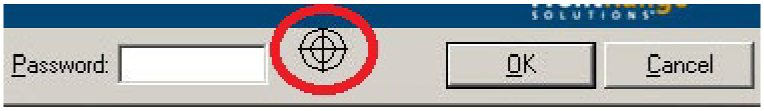
Every E-SSOM Client communicates with the central E-SSOM Service. The E-SSOM Service stores all the login configurations and login data needed to log in automatically to the applications launched on the workstations in a SQL Server database.

1. ***Login configurations***
   The login configurations indicate the appearance of login dialogues (e.g. the locations of the username and password fields and the location and shape of the login button). Subsequently, various login dialogues are available for each application. Examples of login dialogues are 'normal login', 'password modification', 'password expiration' and 'wrongly entered password'. E-SSOM contains a default library of configurations allowing it to handle the most common applications and dialogues. If the particulars of an application deviate from the information contained in this library, E-SSOM can leverage a set of features allowing it to handle these differences.

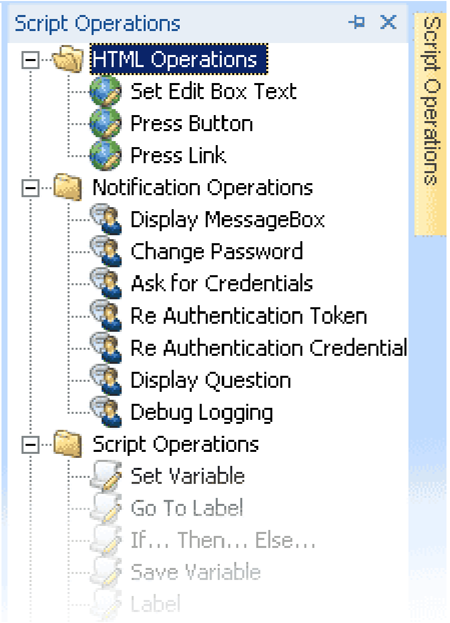
2. ***Login data***
   The first time a user launches an application, E-SSOM will not have a username and password available for that application. When end users enter their credentials, E-SSOM will store this in its database, which is strictly encoded using the DPAPI security mechanism. The next time the user launches the application, E-SSOM will know what the dialogue looks like based on the login configuration, and the combination of the username and password will be available. This allows E-SSOM to log the user on automatically without them needing to enter credentials.

Login Configuration Management

In essence, E-SSOM offers two options for the management of login configurations. The first and most common method is to use a wizard. Through the use of a visual interface, E-SSOM administrators can add applications. For instance, the screenshot below shows how the location of the password field is indicated with an icon in the shape of a cross-hair.

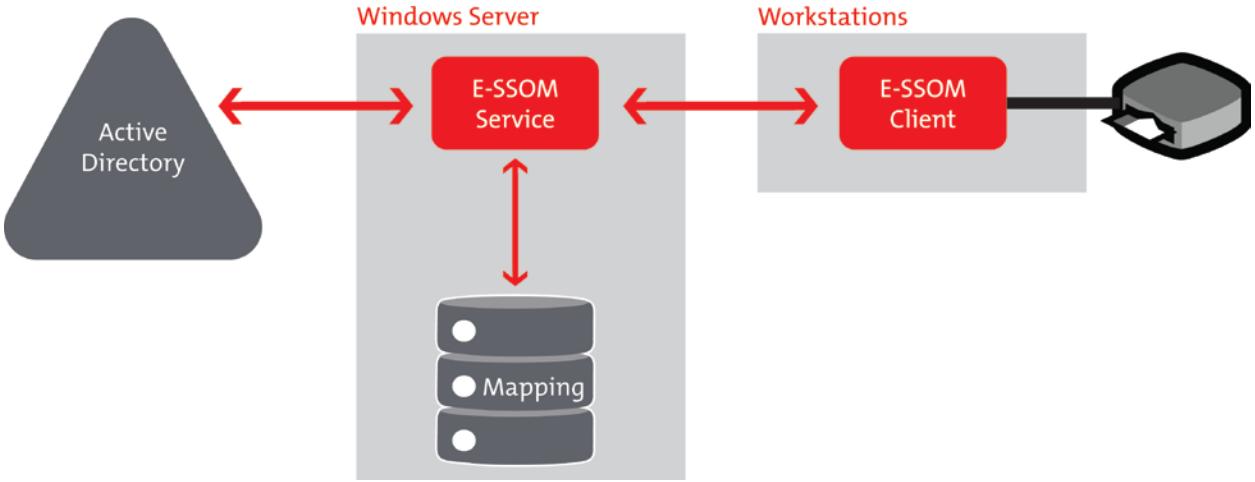


The second method presents the E-SSOM administrator with a state-of-the-art interface where any required feature can be created using a visual scripting language. The screenshot below shows an example of available actions. Features that can be created with this method include re-authentication of users when they launch a particular application, displaying a notification of scheduled maintenance during the login procedure, the creation of a link between a physical access system and computer access and the implementation of password changes after users have logged on.



ARCHITECTURE - AUTHENTICATION MANAGEMENT

Below is a schematic diagram of the E-SSOM architecture showing the integration cycle from the card reader to a user account in Active Directory.



The E-SSOM Client that has been installed on the workstation is integrated directly with the card reader's driver software. It can send queries to the card reader such as 'Is the card placed in the reader?', 'Is the card near the reader?'', 'What is the card's RFID?''. E-SSOM can also respond to any event generated by the card reader, e.g. when the card is held near the reader.

The E-SSOM Client communicates with the central E-SSOM Service through an encrypted connection. The E-SSOM Service manages the relation between the card ID (RFID) and the user credentials in Active Directory. Through this relation (mapping), the E-SSOM Client can obtain the credentials of users who want to log onto the network using their smart card. To enable a direct login, the E-SSOM Client requires integration with the GINA (XP) or Credential Provider in Vista/Windows 7. Based on the user credentials obtained from the central E-SSOM service, E-SSOM can log the user in directly. Depending on the specific configuration, the E-SSOM Client will provide the end user with access. Specific settings may include 'PIN code correct', 'permitted workstation' and 'during office hours'.

ADDITIONAL CHECKS

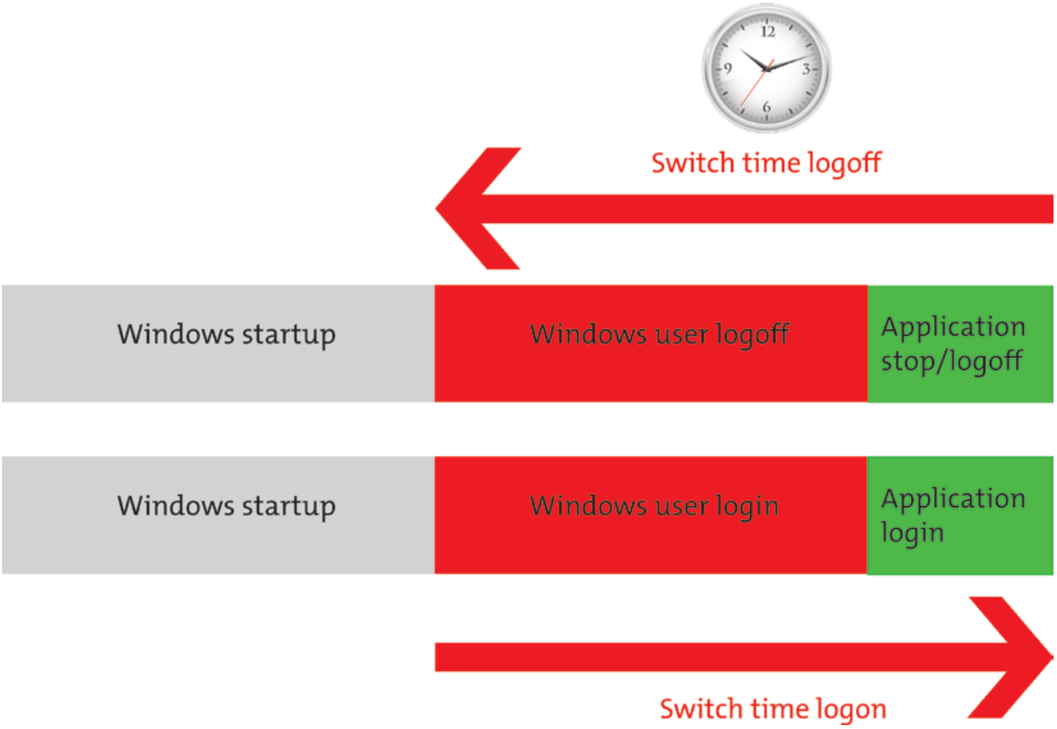
To enhance information security, it is possible to apply checks after a user has logged in on the network. For instance, it is possible to require users to place their smart cards in the card reader before a particular application is launched. For this purpose the E-SSOM Client will query the card reader (e.g. 'Is the card placed in the reader?').

Additional authentication management options include:

- *Auto Application Start*
  When end users have verified their identity using their smart card and PIN code, the system will automatically launch a set of applications and log them in, so that they can start working immediately.
- *Auto Application Close*
  When a workstation has been locked by a user, other users will typically only be able to log in after restarting the workstation. E-SSOM offers the ability to unlock workstations without the need of a restart. It will fully stop the applications of the locked user and perform a fast user switch or follow me to the new user.
- *Self Service registration*
  When a user holds an unknown card against the reader, E-SSOM will ask which username/password has to be linked. It is not required to centrally link and issue cards in advance. The end user himself will be able to perform the registration process resulting in a considerable reduction of the workload on the central smart cards issuing point.
- *PIN code memory*
  After users have entered a PIN code, E-SSOM will remember it for a predefined period. This means users do not have to enter the PIN code each time they use their smart card to log in.
- *Behavioural authentication*
  E-SSOM enables users to exactly define how smart cards must be handled. For instance, they can indicate that the card should remain in the reader (contactless reader) during the period the employee is logged in. Another option is only to require this during login or alternatively to require the card to be presented to the reader for a couple of seconds. As long as the reader supports these options, they can be set in E-SSOM.
- *Multiple authentication tokens*
  E-SSOM supports the use of multiple smart cards per user account. End users can link various different cards (access badges, canteen passes, payment cards etc.), as well as different types of IDs (cards, biometrics, texting etc.) to the same user account. As long as the hardware reader is able to recognise the card, end users will be able to create the link with the user account through a self-service registration process.
- *Multiple user accounts*
  Besides the use of multiple smart cards, E-SSOM supports the use of multiple user accounts per card. When end users use their smart card to log in, E-SSOM will ask them which user account must be activated. Available options will be a one PIN code to cover all accounts or a PIN code for each selected user account.

ARCHITECTURE - FAST USER SWITCHING- SHARING A WORKSTATION

After Windows has started up, users will normally spend several minutes logging in and out of applications. During the login on a Windows domain, the user's credentials are verified, the user profile is loaded, network settings including shares are created, printer settings are set and so on. In a typical office environment, these start-up times are cumbersome yet acceptable. However, in non-standard environments (e.g. in the process industry and healthcare sector) where workstations are shared by users, this represents an unacceptable amount of time. Below is a schematic overview of the wait times experienced when a user logs out and another user logs in.



The active user’s entire environment must be stopped, including the Windows logout. Furthermore other complicating factors may apply –for example, the active user’s account may be locked. The only person able to unlock the workstation is the active user. If he or she is absent, other users will have no other option but to shut down and restart the workstation. This leads to even longer wait times. Added to which, the active user’s current activities are not saved and/or applications are not properly closed.

After the lengthy Windows login process, the applications for the new users will finally be launched. The start-up times for complex client/server applications can be substantial.

Fast User Switching drastically reduces the time required to log out one user and log in the next. This occurs in E-SSOM (E) within the space of a second. FUS also supports unlocking the active user account and offers the possibility of closing the active user's current activities properly.

Using a smart card as an authentication token can simplify and accelerate this process even more. When a user presents a smart card to the reader, E-SSOM will detect this. The user will automatically be switched and logged in and the right applications will be launched, without any need for the user's intervention.

ARCHITECTURE - FOLLOW ME

The Follow Me feature offers an alternative to Fast User Switching, and only works in combination with Citrix or Terminal Services. The user will start by logging in to the network and launching the required applications (E-SSOM will take care of the automatic login). If users switch workplaces, they will have the option to 'take along' the logged-in session to another workplace. They will have direct access to the desktop they launched earlier, along with the applications they opened previously. As with Fast User Switching, it is possible to link the switching of users to a smart card, allowing users to authenticate themselves using a card and optionally a PIN code. Most Follow Me features (95%) are provided by Citrix or Terminal Services. Primarily, E-SSOM sets up the link between the user and the open session directly from the GINA or Credential Provider, which means the end user does not have to reconnect to the open session. This is done automatically during the Windows login. E-SSOM also ensures that workstations that have been locked by another user are correctly unlocked.

ARCHITECTURE - FAILOVER/LOAD BALANCING

Once a SSO solution has been implemented, end users will become increasingly dependent on it. Over time, they will have completely forgotten the passwords for the various applications, passwords may have also been automatically modified by E-SSOM (e.g. where a password has expired). This is why the availability and proper operation of the SSO solution is absolutely business-critical. E-SSOM ensures that end users are always able to use the software. It uses various different mechanisms for this purpose:

1. *Replication*
   E-SSOM stores all variable configuration data (login configurations and data) in a Microsoft SQL Server database. MS SQL Server offers various default techniques ensuring high availability and optimum performance. These include data replication between databases and the installation of a SQL Server on a cluster server. It is possible to configure an unlimited number of E-SSOM Services across the network. There are no technical limitations or licence restrictions. The E-SSOM licence is based on the actual number of end users, and poses no limitations on the number of servers used for purposes such as load balancing, failover, testing and development, etc.

2. *Offline support*
   E-SSOM offers a feature that ensures it will continue to operate even if a network failure were to occur. To provide this offline support, E-SSOM saves a copy of the information available in the central E-SSOM Service on the end user's workstation. This enables users to continue work as normal, even if they are no longer connected with the section of the network where the E-SSOM Service is located. The locally stored data is encrypted and only contains information required for the active user.

3. *Open standards*
   E-SSOM only uses open standards and is implemented in a Windows environment. E-SSOM is not an appliance or black box. It operates in conjunction with all the default Microsoft updates. It can also be managed by a Microsoft administrator, and supports all types of virtualisation etc. In other words, E-SSOM provides seamless integration with Active Directory. No installation of DLL files, restarts of domain controllers or scheme extension are required.

ARCHITECTURE - IDENTITY MANAGEMENT INTEGRATION

The implementation of Single Sign On (SSO) in organisations often forms part of an Identity Management (Idm) implementation program. The objective will be to implement all Idm components holistically to prevent a fragmented (incompatible) Idm strategy.

Tools4ever offers an end-to-end Idm solution catering for any organisational requirements. As a market leader in Identity & Access Management, they have vast experience in implementations spanning an 11 year history. Tools4ever uses a well-balanced implementation approach. All its solutions offer seamless integration through the use of open standards.

With regard to SSO, E-SSOM can be implemented as a standalone solution or can be integrated with user identity management solutions from other vendors (e.g. Microsoft FIM) through using SPML 1.0/2.0. It can also be integrated directly with Tools4Ever's UMRA solution. As a result, when new user accounts are created, they are also created directly in E-SSOM, which eliminates the enrolment process (the need for the end user to remember credentials for each application), and makes it even easier for end users to start using SSO.

REPORTING

With the changes in legislation and regulations (HIPAA, SOX, NEN7510, HKZ etc.), reporting requirements are becoming stricter by the day. Organisations have to constantly be aware of who has had access to a particular system, including the date and time of access. Reports must be available centrally to the security officer and distributed on a periodic basis. Since E-SSOM provides an additional level of security between end users and the applications in the network, the solution can maintain a precise audit trail, providing a detailed overview with each report.

APPENDIX I: AUTHENTICATION EQUIPMENT

- UziPas
- Digent FD/FM 1000 fingerprint sensor
- BioLink U-Match fingerprint sensor
- Iridian with Panasonic Iris camera
- OmniKey CardMan 5121/5125 RFID/smartcard reader
- (MIFARE/HID Aladdin eToken Pro/SC
- Aktiv USB ruToken
- GSM phone/SIM card (IrDA, Bluetooth)
- Dallas iButton (USB/COM/LPT readers)
- Any USB flash drive
- Any other BioAPI 2.0 or 1.1 compliant hardware
- Biometrics sensors supported through Bio-Key BSP
- Atmel AT77UR200 (500 dpi)
- Authentec AF-S2, AES4000, 1601/1610, AES2501/2510 swip
- Crossmatch Verifier 300 (500 dpi)
- Digital Persona U.are.U 4000b (508 dpi)
- Biometrika HiScan & FX2000 (500 dpi)
- Fingertech BIOCA-120 (400 dpi)
- Fujitsu MBF200 (500 dpi)
- Futronic FS-80, FS-88, FB-80 & FB-88 (500 dpi)
- GreenBit DactyScan 26 (500 dpi)
- Identix DFR-200, BTO-500, DFR-2100, DFR-2080 (500 dpi)
- Lumidig Venus (500 dpi)
- SecuGen Hamster III, III+, IV (508 dpi)
- Tacoma Technology Inc, STM01A1 (500 dpi)
- Testech BIO-I (500 dpi)
- UPEK TCS1 & TCS2 (Touch Chip) TCS3 (Touch Strip) (508 dpi)
- Validity Sensors Inc, VFS130, VFS201, VFS301 (500 dpi)

Tools4ever

14 Miller Court
Tewkesbury
Gloucestershire, GL20 8DN
Tel. 0845 017 1499
Fax. 01684 438 789