

---

# IBM Tivoli Access Manager and Sun OpenSSO

## - Combining the best of both worlds -

---

In this fast evolving world where businesses need to make applications available online, business leaders ask themselves questions about how to secure both the applications and the transactions. That is where the demand for **Web Application Management (WAM)-platforms** is raised from.

While multiple WAM-players are competing each other on the today's market another competition is raging in all its dimensions, those of the **strong security authentication solutions** (token, biometric, certificate ...).

**Authentication** is the process of mapping a physical user to an electronic identity. Besides the authentication process is used to verify if one is really the user (s)he is claiming to be. Up until recently, this was done by using username and password. Because of the increasing CPU-power in modern machines, breaking today's well-considered passwords becomes easier each day.

**Strong authentication**, introduced to increase protection of sensitive information, is based on three pillars:

- *Something you "know"*: A passphrase or code that only the user knows.
- *Something you "have"*: A physical device you own (token).
- *Something you "are"*: A biometric property uniquely identifying the authenticating person (fingerprint, iris, finger vein pattern,...)

To put the above in practice, a wide range of proven technology can be used.

Once a business has chosen the security solution that is compliant with the business needs, a final obstacle must be bypassed: "Is the selected strong authentication solution **supported by the WAM-platform** in place?".

This whitepaper explains how to extend the few out-of-the-box authentication mechanisms provided by **IBM Tivoli Access Manager for e-business**<sup>1</sup> with the numerous ones that are available by default when using **SUN's free OpenSSO**<sup>2</sup>-solution.

---

## IBM Tivoli Access Manager for e-business (IBM TAMEb)

---

As a leading authentication and authorization platform **TAMEb** provides a platform to centrally manage authentication and authorization to web-enabled applications. Next to providing security at user level, TAMEb also works closely with IBM

---

<sup>1</sup> <http://www-01.ibm.com/software/tivoli/products/access-mgr-e-bus/>

<sup>2</sup> <https://opensso.dev.java.net/>

Rational Appscan to address issues which may expose application vulnerabilities.

TAMeb supports a number of authentication mechanisms **out-of-the-box**:

1. Username/password
2. RSA SecurID
3. Client Side X509-certificate<sup>3</sup>
4. HTTP-header based authentication

For other authentication mechanisms, IBM has created the **Cross-Domain Authentication Service (CDAS)** which allows replacing the default authentication mechanism with a custom one. CDAS is pretty powerful but needs a considerable amount of development. No additional information can be requested from the user during authentication. Even more important: because the TAMeb-reverse proxy (WebSEAL) does not pass all the data contained in a HTTP-request to the CDAS (such as POST-data or additional HTTP-headers), some useful information can be missing to perform the authentication.

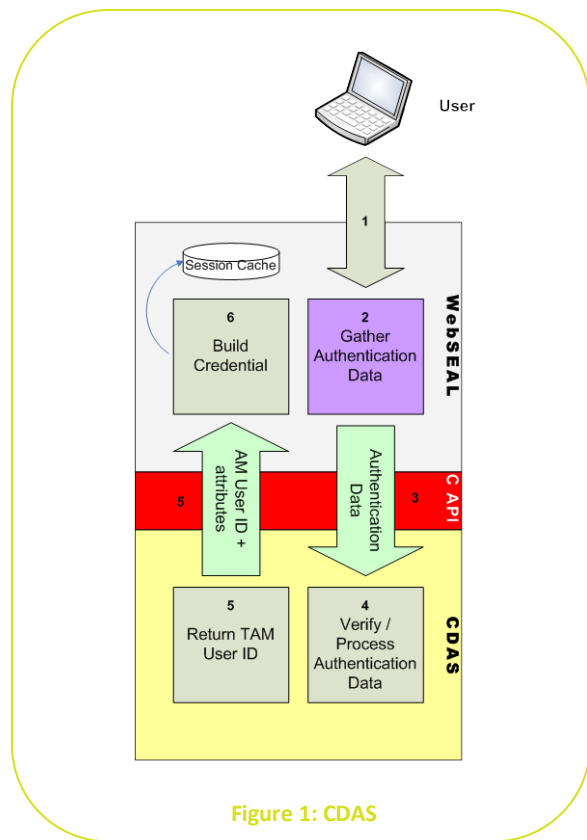


Figure 1: CDAS

Figure 1 shows the working principle of the CDAS:

1. A user tries to access a protected resource,
2. WebSEAL gathers the authentication data from the user,
3. WebSEAL passes the gathered data to the custom CDAS-library via an API-call,
4. the CDAS verifies the incoming data against an external resource,
5. the CDAS returns a user identity,
6. WebSEAL builds an internal credential for that user,
7. the user is granted or denied access based on the security policy.

IBM has introduced a new feature with the release of TAMeb 6.0<sup>4</sup>, called **External Authentication Interface (EAI)**.

Using EAI, the authentication process can be made much more flexible. Another significant advantage is that development of the authentication procedure is not longer bound to the C-language.

Figure 2 shows how EAI is implemented:

1. A user tries to access a protected resource and is redirected to the EAI-application,
2. the EAI-application gathers the necessary authentication data over HTTP,
3. after verifying the users authentication data,
4. the EAI-application returns a user identity,
5. WebSEAL builds an internal credential for that user,
6. the user is granted or denied access based on the security policy.

<sup>3</sup> Client certificate authentication cannot be done via EAI, IBM provides the "User Mapping Client Certificate CDAS" that allows to map a certificate to any TAM-user by using XSL mapping rules. The CDAS is included in the TAM-license.

<sup>4</sup> also TAMeb 5.1 FP9

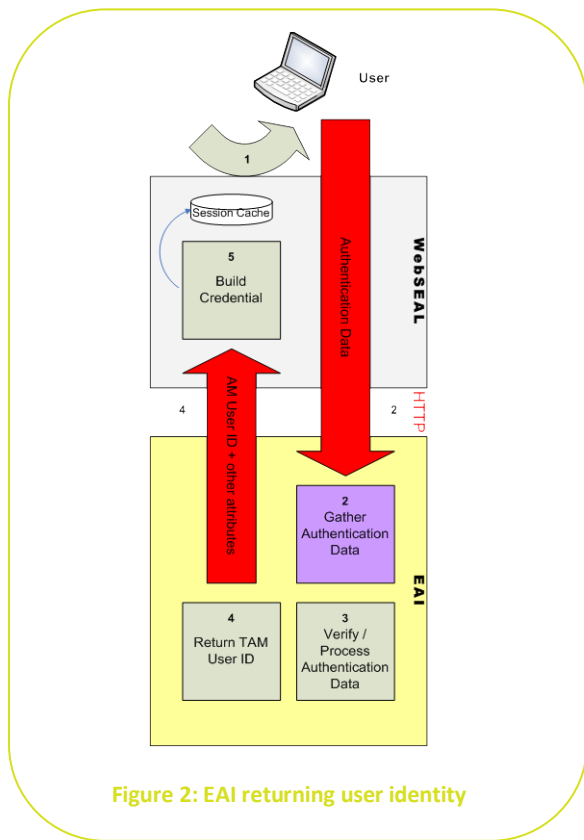


Figure 2: EAI returning user identity

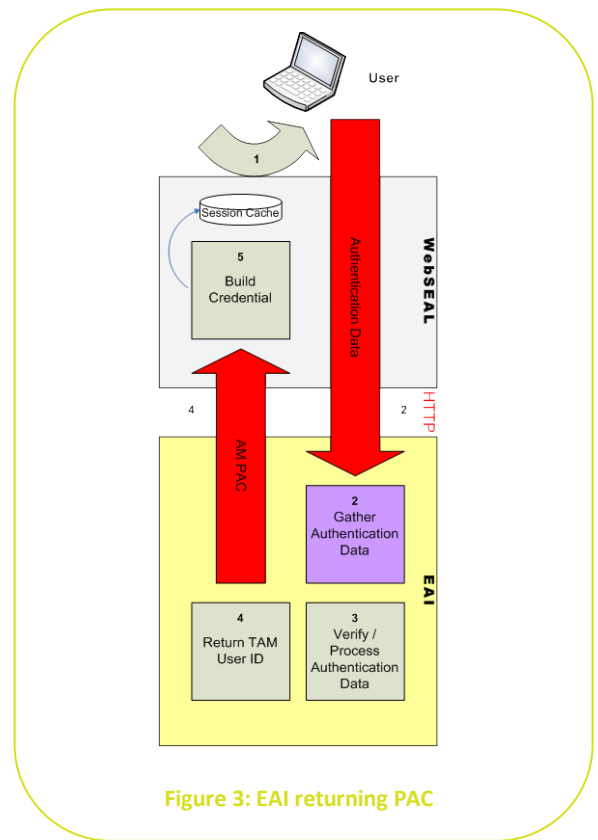


Figure 3: EAI returning PAC

WebSEAL is not longer responsible for gathering the logon information from the user. This directly indicates that the authentication process becomes more flexible than the CDAS because:

- EAI has complete access to the HTTP-request (POST-data or additional HTTP-headers),
- EAI has the possibility to interact with the user during the authentication phase, which makes it possible to implement whatever authentication strategy,
- development of the EAI-solution is no longer limited to the C-language.

Instead of sending a user identity to WebSEAL, a Privileged Attribute Certificate (PAC, another representation of the internal credential) can be sent as well, which avoids WebSEAL to make LDAP-calls to create the internal credential (see figure 3).

## Sun OpenSSO Enterprise (formerly Sun Access Manager)

Sun also plays a very important role in Web Access Management (WAM) as a **free open-source** platform, made available through the OpenSSO-project.

OpenSSO is delivered out-of-the-box with numerous strong authentication mechanisms:

- *SecurID*: Uses RSA ACE/Server software and RSA SecurID authenticators to verify identities.
- *Digipass*: A security product from VASCO providing strong user authentication via small security tokens.

- *Active Directory*: Uses an Active Directory operation to associate a user identifier and password with a particular Active Directory entry.
- *RADIUS*: Uses an external Remote Authentication Dial-In User Service (RADIUS) server to verify identities.
- *SAML*: Receives and validates SAML assertions on a target server by using either a web artifact or a POST response.
- *Windows Desktop SSO*: Allows a user who has already authenticated with a key distribution center to be authenticated by OpenSSO Enterprise without having to provide the login information again.
- *Certificate*: Enables a user to log in through a personal digital certificate (PDC).
- *OpenID*: Provides a complete OpenID Authentication 1.1 protocol compliant identity provider implementation, complete with full support for OpenID Simple Registration Extension 1.0.
- *RSA Access Manager*: allows to integrate with RSA Access Manager (formerly known as ClearTrust).
- *BiObex Authentication Management Suite*: Enables a biometrics authentication and single-signon for Access Manager secured applications.
- *Hitachi Finger Vein Biometric*: Identifies finger vein patterns that exist inside the human body, eliminating tampering while increasing reliability and security.
- *JDBC*: Enables authentication through any Structured Query Language (SQL) databases that provide JDBC-enabled drivers.
- *HTTP Basic*: Enables authentication to occur with no data encryption.
- *LDAP*: Enables authentication using LDAP bind, a directory server operation which associates a user identifier and password with a particular LDAP entry.
- *Information Card Relying Party*: allowing end users to authenticate via Windows CardSpace or other identity selectors such as DigitalMe or xmlldap.
- *Membership*: Enables user to self-register a user entry.
- *MSISDN*: The Mobile Station Integrated Services Digital Network (MSISDN) authentication module enables authentication using a mobile subscriber ISDN associated with a device such as a cellular telephone.
- *SafeWord*: Uses Secure Computing's SafeWord PremierAccess™ server software and SafeWord tokens to verify identities.
- *UNIX*: Solaris and Linux modules use a user's UNIX identification and password to verify identities.
- *Windows NT*: Uses a Microsoft Windows NTLM server to verify identities.
- *Verisign Identity Protection*: Helps consumers to log-in conveniently and securely to use your online services. Two-factor authentication, self-learning fraud detection, and a powerful validation infrastructure helps provide a secure end-to-end solution.
- *Yubikey*: Plugs into any USB slot. With a simple touch on the YubiKey, it sends the user's identity and a unique pass code every time it is used.
- *ActivIdentity 4TRESS*: Support a wide range of authentication methods, one time password tokens or smart cards, static passwords or Q&A.
- *Swekey*: The Swekey is a small USB-key that secures access to any swekey enabled web site.
- *Anonymous*: Enables a user to log in without specifying credentials.

These different authentication mechanisms can easily be chained resulting in a well-defined authentication flow, where the flow being followed depends upon the role of the authenticating user: e.g. administrator or regular user.

---

## Combining the best of both worlds

---

IBM's **TAMeb** has a **proven technology** when it comes to secure web-based backend applications. The standalone reversed proxy (WebSEAL) shields the web-enabled applications from the outside world, provides single sign-on capabilities, ease of management, integrates easily with web-enabled backend applications.

Sun's **OpenSSO** provides a **free** open-source WAM-solution which provides numerous existing authentication modules, making it the ideal partner to cooperate with IBM's TAMeb.

Meanwhile, some may ask themselves why not put this into practice? Well, IS4U did!

Figure 4 illustrates the replacement of the abstract EAI component (see figure 3) by SUN OpenSSO.

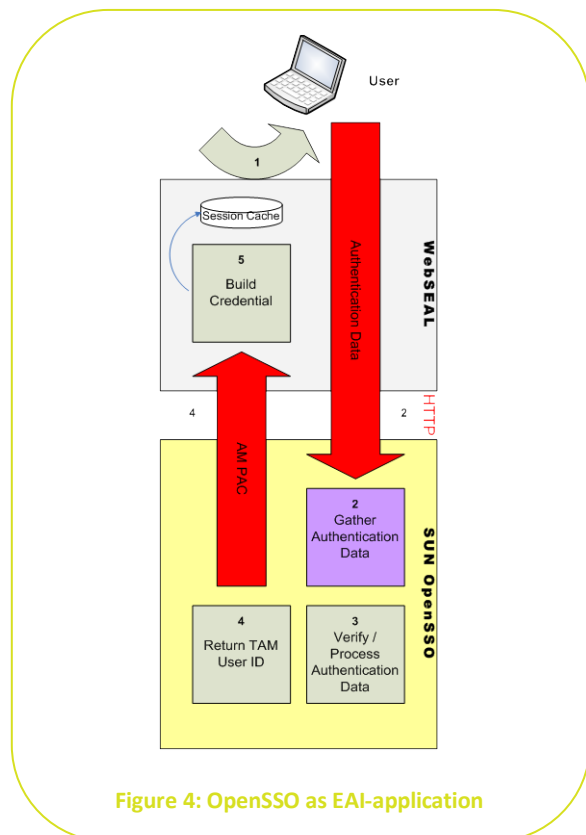


Figure 4: OpenSSO as EAI-application

---

As a multi-vendor company, IS4U does house IBM TAM and SUN OpenSSO experts that were all involved in several large projects.

---

## At a glance ...

---

IBM TAMeb does provide a **state-of-the-art secure reverse proxy** which does **easily integrates** with existing vendor or in-house developed web-enabled applications, provides several SSO-mechanisms, is available on almost every OS, ...

OpenSSO **extends** the few default authentication mechanisms of TAMeb by providing numerous authentication modules out-of-the-box.

OpenSSO does **easily integrate** with TAMeb via the newly introduced EAI-interface which makes it possible to apply an authentication strategy that fits your business security strategy.

OpenSSO is brought to the market as a **free open-source** product via the OpenSSO-project.

OpenSSO is available as a **WAR-file**, which allows running the application in a J2EE-enabled environment, e.g. IBM WebSphere. The latter solution makes it possible to run OpenSSO in a **scalable, high-available** clustered WebSphere environment.

IS4U has both the **TAM and OpenSSO-experience** to consult a business from project initiation to go-life.



**Business Park King Square  
Veldkant 33a  
B-2550 Kontich**

**Phone: +32 (0)3 451 36 60  
Fax: +32 (0)3 451 36 69  
Email: [info@is4u.be](mailto:info@is4u.be)  
<http://www.is4u.be>**

