Single Sign-on (SSO) to Cloud based Services and Legacy Applications
“Hitting the IAM wall”

Marcus Lasance

Phillipsite 5, 3001 Leuven, Belgium
Verizon Business
marcus.lasance@verizonbusiness.com

Abstract

With the advent of the de-perimeterized organization and increased scepticism around ‘Cloud Security’
is SSO still a viable worthwhile goal for organisations?

Single Sign-On (SSO) projects are a special case of Identity and Access Management (IAM) projects. They
are usually undertaken with the aim of increasing the user friendliness of Corporate IT systems’ user log-on
processes. This should result in abolishing the use of multiple username and password combinations the
user has to remember and change at different intervals. The SSO aim should be achieved without jeopard­
izing information security in any way. Increasing user convenience in such a manner will increase user
satisfaction with the IT department along with general productivity levels.

Cost control related to IT help desks resetting forgotten passwords should follow.

SSO can also help organizations address information security compliance requirements, through the central
logging (and audit facilities) of all access attempts and authorization decisions granted in relation to the
organization’s restricted information resources. Sometimes compliance objectives are in fact the major busi­
ness driver for SSO.

In the consumer space customer loyalty and retention rates are often cited as an important commercial
driver for SSO projects.

With the advent of the de-perimeterized organization’ and increased scepticism around ‘Cloud Security’ is
SSO still a viable worthwhile goal for organisations?

This paper takes a closer look at special security issues arising when an organization attempts to create an
Enterprise Single Sign-On (ESSO) solution that includes both legacy applications hosted within traditional
organizational firewalls and a new breed of ‘Cloud Based’ solutions that are following the Software as Service
(SaaS) model and therefore can be hosted with any number of Service Providers (SP) ‘in the cloud’.

1 Examining the role of IAM as SSO enabler

When thinking about SSO and Information Security two conventional wisdoms often come to
mind. The first is the concept of avoiding dependence on ‘the weakest link’ in your organizations
defences. The second is the concept of not wanting to put all your eggs in one basket.

1 http://www.opengroup.org/jericho/deperim.htm

N. Pohlmann et al.(eds.), ISSE 2010 Securing Electronic Business Processes,
DOI 10.1007/978-3-8348-9788-6_5,
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011
For the weakest link in protecting information assets read 'Username and Password' which, like no other authentication method, is highly vulnerable to social engineering attacks, malware key loggers and yellow 'post-it' notes left by lazy PC users for office cleaners to read.

In a homogenous single organization from an IT perspective the weakest link argument against SSO can be quickly countered by giving, as part of the project, all users a much stronger form of authentication. This usually means replacing 'Username and Password' with two factor authentication.

In other words, the bar is raised for everyone, without exception. This in itself can of course be a costly exercise, wiping out any potential cost savings of an SSO project.

Another question is: “Will all the business partners in a given federation be able to set the bar for information protection at the same high level?”

The question is not just related to the available budget in other parts of the federation, e.g. to purchase authentication tokens, but also a question of compatibility of security policies and audit capabilities between partners.

In the UK a ‘fly on the wall’ TV documentary recorded the unauthorized access of client financial records by call center employees from a marketing agency contracted by a well know high street bank. The call centre had a high staff turnover and was in fact ‘recycling’ a number of not individually assigned network access tokens to access client accounts. This is of course not the kind of federated SSO we want, as any audit log would prove absolutely nothing except that the bank was not really in control!

The ‘putting all your eggs in one basket’ paradigm could be used to make a case against SSO, with the argument that if one individual computer system’s security was to be breached at least the integrity of most other systems could be presumed still to be intact.

This is a very weak argument. How many users use the same username password combination for many of the corporate applications they access? For the simple reason they cannot begin to remember them all and writing them down is prohibited? The added protection provided by multiple sign-on(s) may be just an illusion!

2 No SSO without solid Identity Management!

As the example in the frame above illustrated, once SSO is enabled with a strong authentication form factor (RSA SecureID Token, PKI smartcard or OTP) it becomes of paramount importance to manage the users’ entire life cycle with the organization. An ex-employee logging in with a token that was not decommissioned is still a security breach. This means, not only are we aiming to provide the right levels of access from day one with the organization and making the new employee immediately productive; we also need to ensure that access is removed the very instant an employee leaves the company, sometimes well before! The same applies to partner employees.
Based on our investigations, a number of data breaches still originate from within the company, sometimes from disgruntled employees, sometimes unwittingly by current employees, who get tricked into downloading malware applets that log key strokes from passwords.

Role Based Access Control (RBAC) is an important mitigating factor of such risks. RBAC helps prevent the occurrence of 'role creep.' This is the often occurring situation, whereby during the course of their career within an organization employees tend to accumulate more and more access rights. This happens when access right for new roles are added to a user profile, but seldom removed when no longer needed.

The ability to introduce strict segregation of duties is a second benefit that should come from an RBAC project forming an integral part of any SSO or wider IAM project. Examples include purchasing managers not being able to approve their own purchase orders.

Looking more to IT roles, the person performing database back-ups does not require access to that database content as a user. So while he is allowed to make copies for safe keeping, he may not log into it and access sensitive data. In the context of IT, roles are also important in helping enterprises prevent default admin passwords on shipped devices to remain unchanged when such devices are deployed, as this class of credentials is especially prone to attack from malware. This area of IAM is often referred to as 'Privileged Account Management' and specialized vendor solutions exist that can be obtained from Verizon Business.

3 What makes Access Control ‘in the Cloud’ special?

The introduction of this paper already highlighted the fact that incompatible security policies between cloud partners can be an issue.

So can privacy issues. Will access to all event logs be given, when these are shared with other cloud customers and might reveal sensitive information about those other parties?

In this paper we limit ourselves to addressing technical issues like different communication protocols and encryption standards used.

A common term for these types of standards and the problems they try to solve is Federation.

Before we explain the concepts and standards around Federation it is useful to examine the situation organizations face when Federation is not required, because they have not truly begun the process of de-perimeterization. This state is sometimes called the ‘moat and castle’ model of the organization.

3.1 Conventional SSO Solutions

Until not very long ago, the bulk of SSO solutions on the market were designed to provide single sign-on to applications that on the whole reside within one and the same security domain.

SSO marketing terms like ‘simple to install’ and ‘agent-less’ are tell tale signs, that all such Web Access Control (WA) solutions do is examine the URL of the incoming browser request, look up

2 Verizon Business 2009 Data Breach Investigations Report
in a directory if a security policy is attached to it and execute the policy in the form of a simple 'grant' or 'deny' access decision.

A slightly more sophisticated form of access control uses session 'cookies' that are passed to agents that need to be installed on each web server of the organization, but does not require any client side software to be installed. Client side software plug-ins, often required to 'SSO enable' legacy applications, are usually a big turn-off for the IT department. This is due to the extra overhead this causes in desktop management, meaning locking down all work PCs to an approved specification and the right level of security patches like installed anti-virus software.

3.2 Access to non web based legacy applications

Of course not every business critical legacy application is necessarily web enabled. Because of the IT department’s resistance to installing client-side software, to overcome this problem Citrix like terminal server solutions are dominating this end of the market. The user is in effect looking at a virtual desktop running on a server, which can be properly locked down and secured by the IT department, where a laptop might not.

3.3 Legacy Applications need user provisioning

Web Access Gateways providing SSO can be regarded as applications that escort users to the front door of an application. If it is a simple web page they want to look at, the user can see its contents, perhaps fill in a form, but not much more.

Most web-enabled corporate applications like ERM/CRM systems require further information to authenticate a user in a particular role. Some users have read-write access rights, but to only their own department’s stored information. Others, like auditors, may search all departments but have read-only access. Legacy applications usually have information about all authorized users stored in specific user tables within an underlying Relational Data Base System (RDBMS). Users and their authorized roles do not appear out of nowhere. Traditionally they were created by a super-user, often someone in the IT helpdesk department. This is not good practice. It would be better to use an automated provisioning system in combination with a workflow tool and RBAC and put that responsibility back with the business where it belongs.

To allow the application to make its own authentication decisions, the Web Access solution can carry the necessary information attributes - like a unique username - in its HTML header. This header is formed when the Web Access gateway, which acts as a proxy for the real web server, redirects the user to their intended web application.

Note: Web Access Gateways generally do not create or delete users on target systems. This function is usually reserved for ‘super users’ in the business or administrative functions in the IT department. If user creation is automated, this is a function of provisioning systems and not generally considered to be part of an SSO project, but of a wider IAM project.
4 SSO to Web applications ‘in the cloud’ using federation

In our definition of cloud computing we will generally be talking about ‘Private Clouds’, that means outsourced IT applications where we have a business relation with the outsourcing provider and at a VPN like trusted connection to the Service Provider (SP). In the loosely coupled world of a Service Oriented Architecture (SOA) the problems we have seen connecting to trusted private clouds are only exacerbated.

A common factor between cloud applications is that they are generally well protected behind someone else’s firewall. If the services were not provided by a reputable SP we would not want to do business with them in the first place! Thankfully some trust frameworks are emerging, so that we can start to form an objective opinion about the security policies and reputation of most public SPs.

Where we have some control over our own firewalls, we must assume that opening the necessary ports on other organization’s firewalls - to allow automated user provisioning and deletions - will be severely restricted if not impossible.

As an IT industry this problem has long been acknowledged and standardized protocols have been created that allow the federation of Identities and access control policies. The relevant standards are:

- SAML
- XACML
- Liberty Alliance
- ADFS / WS-Security
- Information Cards/OpenID

It is important to remember that while the above industry initiatives provide a secure and standardized way to exchange user and role information, none of the above standards are designed to create a new user with the right access rights ‘on the fly’ at the target cloud system.

If we take the case of federation using the Security Assertion Mark-up Language (SAML), both the Service Provider (SP) and the Relying Party (RP) must install a Federation Server that supports the same version of SAML, which also has proven to be interoperable ‘out of the box’ in one of the leading Security Events’ sand pits or interop demos.

Even after a new user has successfully been authenticated at the RP-end through a process of certificate exchange, the business partners will have to agree which other attributes can and need to be exchanged in the signed SAML header or subsequent back channel attribute requests over SSL. The privacy and other issues that need to be resolved before a successful federation can be set up must not be underestimated and can result in significant costs in the form of Professional Services (PS) charges.

When setting up a web of federated identity processes, each system or entity must establish trusted links with every other entity, creating a web of VPN connections. However, this complexity increases management overhead and limits the flexibility to leverage different specifications as
new relationships are formed and dropped and cloud applications are added and removed from a portfolio of approved services.

Verizon Business PS has considerable experience in the setting up, testing and implementing of Federation Agreements between Business Partners.

By using Identity Managed Services – Web Access (IMS-WA), a completely outsourced IAM solution from Verizon, organizations can utilize the Verizon IdP as a single trusted link that all systems can leverage, much like a hub with spokes. Once a user is authenticated, the user can log in to any other federation-enabled service, including cloud applications like Salesforce.com and ADP.

5 SSO to Web applications ‘in the cloud’ using a User Centric Identity Management Framework (UCIF)

Verizon like many other global service providers has come to the realisation that for truly global web 2.0 types of clouds even the hub and spoke model of federation eventually will not offer a scalable or economical solution. This is often referred to as ‘hitting the IAM wall’.

Verizon has joined forces with other global service providers to create the Open Identity Exchange (OIX). Along with the increasing acceptance of Information Cards and OpenID at social networking sites and services that are truly cloud based like GoogleDocs, comes the acceptance that, for some applications at least, there comes a limit to what can be achieved with a web of federation agreements and VPN tunnelling the cloud until it looks more like a bowl of spaghetti.

What is needed and what is emerging is a global identity meta system, where users are taking more and more responsibility for managing their own Identity affairs, including requesting access to the cloud applications they need to do their job. In doing this they will need to be backed up by a special kind of trust provider, also called an Identity Provider (IdP).

The ultimate aim should be that relying parties can stop hoarding silos of sensitive information about users, not essential for their core business processes. They now leave this for IdPs to worry about.

Protecting sensitive information is an expensive business for organizations and increasing regulation and audit requirements only adds to the burden.

From a macro economic and business perspective it makes sense to outsource this burden to a specialized IdP that can help enterprises collect and maintain the information which may be required for a full set of ‘in house’ identity and credentialing services, such as:

- Initial registration and verification of base identity data like name and address including the checking of government credentials like passports and e-Id cards
- Checking utilities (gas, water and electricity) provided to the individual’s main place of residence
- Checking credit worthiness with credit agencies
- Checking where people geographically are and detecting anomalies in converging networks to help detect and prevent fraud.
• Checking professional qualifications with educational institutions and professional bodies to check an identity is licensed to practice in a restricted profession.
• Giving the user the ultimate control over what attributes of their identity are shared with Relying Parties.

Users that require access to cloud-based services just present the SP with an Information Card containing signed claims and all the trusted attributes necessary to create a new account ‘on the fly’ or ‘Just in Time’. Such claims could include role claims signed by an employer, professional claims like a license to practice signed by the professional body the user belongs to.

Identity Providers will also increasingly play a role in generating the audit logs for forensic investigations when things go wrong. For this purpose special audited Information Cards can be used. These can be compared with the event and access logs of the relying party in the cloud to extract relevant forensic data, while safeguarding the privacy of other cloud users.

The most successful SaaS providers in the cloud already are set up to consume Information Cards and OpenId as an alternative to SAML. All they need is a valid set of signed claims to give the user what they need and a commercial agreement (if not a ‘free’ service) about who will pay the bill!

The principle of ‘minimum disclosure’ means this could be as little as a verified claim the user is an adult, or a that a doctor is licensed to practice in a certain country.

![User Centric Cloud model](image-url)
6 Conclusion

The complex account management and provisioning actions, necessary to achieve Single Sign-On (SSO) to an organisation's IT resources, were difficult enough to accomplish before the advent of "Cloud Computing". Easy availability of "Software as a Service" means today entire departments are starting to use cloud computing resources, often without due consideration of cloud security concerns.

The access rights to privileged accounts, necessary to achieve Identity and Access Management by IT administrators, can often not be granted by cloud service providers who have to organise multi tenancy in their systems without jeopardizing security and privacy for their co-hosted customers.

The answer lies in the application of standards for user- and account provisioning, but also the realisation that in future identity must be seen as the central organizing principle for simplifying sign-on(s) in an increasingly complex digital world taking shape in the cloud.

Many experts believe privacy concerns can only be addressed by putting individuals back in charge of their own identities. This can mean 'just in time' provisioning and deprovisioning of accounts the user may have 'in the cloud' on the basis of proven identity claims supplied by trusted Identity Providers.

In the emerging global identity meta system, IdPs like Verizon Business will play a vital role in releasing the massive potential benefits for users and relying parties be they commercial organisations or governments.

By participating in the launch of OIX and the imminent issuance of different levels of assurance identities that can be used at an increasing number of Government and Social Networking sites, Verizon Business proves that also in this area of identity management for the cloud we intend to play a leading role.