The Adoption of Single Sign-On and Multifactor Authentication in Organisations – A Critical Evaluation Using TOE Framework

Marise-Marie D'Costa-Alphonso
University of Southern Queensland, Melbourne, Victoria, Australia
Marise.Alphonso@gmail.com

Michael Lane
School of Information Systems, Faculty of Business, University of Southern Queensland, Toowoomba, Queensland, Australia
Michael.Lane@usq.edu.au

Abstract

The proliferation of user credentials for system access coupled with the resulting rising security threats have led to the development of single sign-on (SSO) access control and multi-factor authentication (MFA) technologies. This paper provides an overview of these authentication mechanisms, highlighting the current state in the marketplace and describing the key enabling technologies. We conducted a qualitative analysis to identify the key factors facilitating and inhibiting the adoption of SSO and MFA by organisations using the Technology-Organisation-Environment (TOE) framework. The resulting analysis indicates a range of technologies, protocols and configurations that can be employed depending on the type of authentication and level of security required. The findings suggest that a number of technology, organisation and environment factors both positively and negatively affect organisational adoption of SSO and MFA. There are a number of key benefits gained from adopting SSO and MFA such as increased corporate security and reduced organisational costs of managing access control. There are also a number of key challenges to be overcome by organisations adopting SSO and MFA. These include the ability to accommodate the complexity of multiple heterogeneous systems and to be resilient to new information security threats thereby allowing a SSO and MFA solution to deliver improved and secure access control to information systems both within and across organisations.

Keywords: Single Sign-On (SSO), Multifactor authentication (MFA), Technology-Organisation-Environment framework (TOE), Authentication technologies, Organisational adoption of SSO and MFA

Introduction

In many organisations, system users are required to remember a number of different usernames and passwords on a daily basis to access core systems. In dealing with the complexity of multiple user names and passwords organisations often have to make a compromise between user convenience and security.

Single sign-on (SSO) access control and multifactor authentication (MFA) are security mechanisms that aim to shift the balance of this compromise by making access to core business systems both more convenient for users and more secure. In this paper a critical review of these two related security authentication mechanics provides insights into the current technologies and protocols, which enable SSO and MFA. In addition the organisational and environmental aspects that influence implementation of SSO and MFA are presented. Challenges and benefits that organisations need to consider when adopting SSO and MFA are also highlighted to offer views as to whether the 'security-user convenience compromise' does indeed shift. Then we present a preliminary analysis of the key factors impacting on SSO and MFA implementations in organisations guided by the Technology-Organisation-Environment (TOE) framework. This analysis is informed by the opinions of industry practitioners working in this domain who have discussed these topics on blogs and online discussion forums. Finally we present our conclusions and implications regarding this research and provide suggestions for future work in this area.

Overview of Topic and Current State of Play

Background

Users increasingly access a myriad of systems applications on a daily basis via devices such as desktop computers, laptops, mobile phones and PDAs from a variety of locations. For each of these systems applications, users may have separate identities for authentication as shown in Figure 1. The explosion of system applications such as email, customer-relationship management and financial systems (Osterman Research Inc, 2009) coupled with multi-device access to these systems requires concrete security measures to manage data integrity, user privacy and network security. In addition, user convenience is an important consideration that security solutions should address to prevent users from having to re-authenticate themselves repeatedly (FinallySecure, 2009).

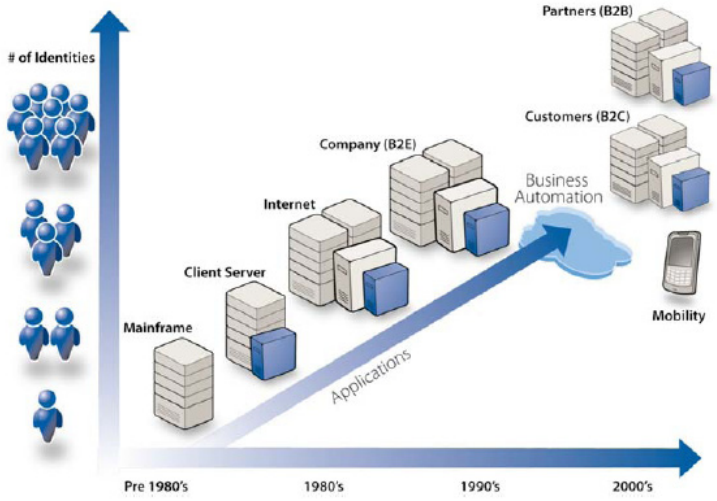


Figure 1: Multi-system, multi-device, multi-identity proliferation
(Source: Shaw, 2008, p. 1 used with permission)

Currently the average user accesses around 12 different password-protected systems daily at work (Osterman Research Inc, 2009). With so many passwords to remember users either write them down ("The value of enterprise single sign-on," 2006), use the same password to access multiple

systems (Osterman Research Inc, 2009) or make them easy to remember and hence easy to crack via dictionary attacks or social engineering techniques (Liou, 2007; Panko, 2009) – thereby decreasing system security. This factor together with others such as increased help desk costs and the need for shared workstation support are the driving forces behind adoption of single sign-on systems (Kreizman, 2008) and multi-factor authentication technologies.

Single Sign-On

Single sign-on bears the promise of addressing the issues of user convenience, reduced costs and increased security (Robbins & Hamilton, n.d; SearchSecurity.com, 2008). Single sign-on (SSO) refers to a user entering just one set of credentials for authentication and authorization and thereafter being able to access multiple applications securely and seamlessly. These applications may reside on multiple domains and the SSO system handles the user's credentials across these domains (The Open Group, 2009).

SSO did not initially work as anticipated because the technologies performed poorly, but this has now changed ("The value of enterprise single sign-on," 2006). SSO is projected to increase in popularity due to the increasing business interactions that enterprises have with employees, business partners and customers (Dubin, 2008b) via their computer networks and systems applications. Maximising user convenience for system access has the equal benefit of reducing organisational IT costs since SSO systems streamline the authentication and authorization process (Schneier, 2005a; SearchSecurity.com, 2008).

Organisations are also embracing SSO solutions as part of their Identity and Access Management (IAM) suites (Dubin, 2008b; The Strategic Counsel, 2007) - requirements in many industries in order to meet mandated compliance from regulations such as Sarbanes-Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA) in the US (Dubin, 2008b) - requiring sophisticated access control functions. These include user provisioning and user auditing, for example, the time users spend on systems, users login times and so on (Dubin, 2008b; Osterman Research Inc, 2009). In the US, 36% of healthcare organisations are currently using SSO (Tiazkun, 2009).

In Australia, organisations may employ IAM suites with SSO to comply with the National Privacy Principles contained in the Privacy Act 1988 (Australian Government Office of the Privacy Commissioner, 2009), whereby data integrity and security enforcement is assisted by these technological solutions. Multi-factor authentication used in combination with SSO addresses the needs of organisations to meet regulatory compliance in relation to access control while at the same time ensuring there is much tighter control over who can legitimately access systems applications and data at the appropriate levels.

Multi-Factor Authentication

Authentication refers to the process of proving your identity and verifying that you are who you say you are (Panko, 2009). There are a variety of authentication factors employed by information systems including passwords, biometrics, one-time password (OTP) tokens, smart cards and digital certificates (Osterman Research Inc, 2009; Panko, 2009).

These authentication mechanisms fall into three categories as shown in Figure 2. Authentication is termed 'multi-factor' if at least two out of these three categories are needed by a user to authenticate themselves in one particular instance. Using more than one factor results in the employment of 'defense in depth' - the principle that having multiple lines of defense leads to less system vulnerabilities (Panko, 2009). Examples of MFA include the use of an ATM card requiring a PIN (something you know) and the card (something you have); a OTP token, which reveals a pass-

code when a button on the device is pressed (something you have) and a password (something you know) to access a system.

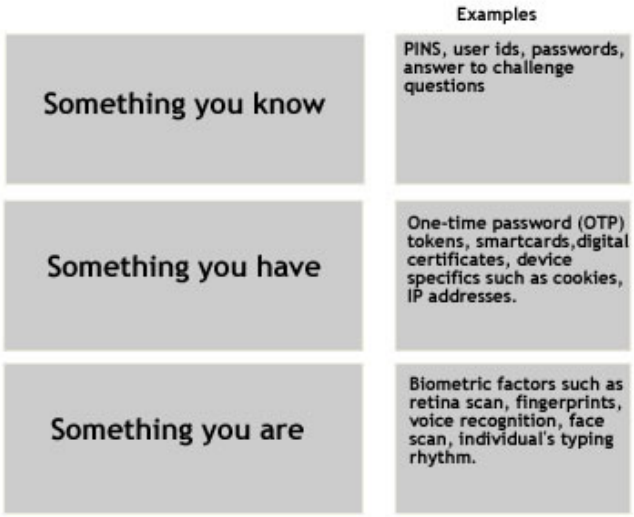


Figure 2: The types of multi-factor authentication
(*Source*: developed for this research)

One issue with SSO can be described as 'the keys to the castle or kingdom' dilemma (De Clercq, 2002; "The value of enterprise single sign-on," 2006) or the 'master key' (Shaw, 2008, p. 13) problem, whereby a compromised SSO credential may facilitate undesired behaviour in enterprise systems. This is where multi-factor authentication becomes an important complementary technology as an additional security layer in organisational SSO implementations.

Current Status of SSO and MFA in the Context of the TOE Framework

The current state of SSO is somewhat confusing with no clear standards and many vendors offering similar yet different SSO solutions and different protocols (Pandit, 2009). Major market leaders include Imprivata, Citrix and Passlogix (Kreizman, 2008; "The value of enterprise single sign-on," 2006).

In an attempt to examine and understand the various processes that influence the adoption of SSO and MFA solutions by organisations, the Technology-Organisation-Environment (TOE) framework proposed by Tornatsky and Fleischer (1990) will be used. In our analysis, a number of online sources of empirical qualitative data have been analysed and the results mapped to criteria within the three contexts of technology, organisation and environment of the TOE framework.

The TOE framework has been used by a number of studies to investigate the adoption of a variety of technological innovations within corporations such as Open Systems (Chau & Tam, 1997), EDI (Lee, 1998) and E-business (Zhu, Kraemer, & Xu, 2006). Figure 3 highlights categories within each of the three contexts of the TOE framework that can be used as a basis of analysis to determine which factors carry most weight in guiding an organisation's decision-making and approach to the adoption and implementation of technological innovations such as SSO and MFA.

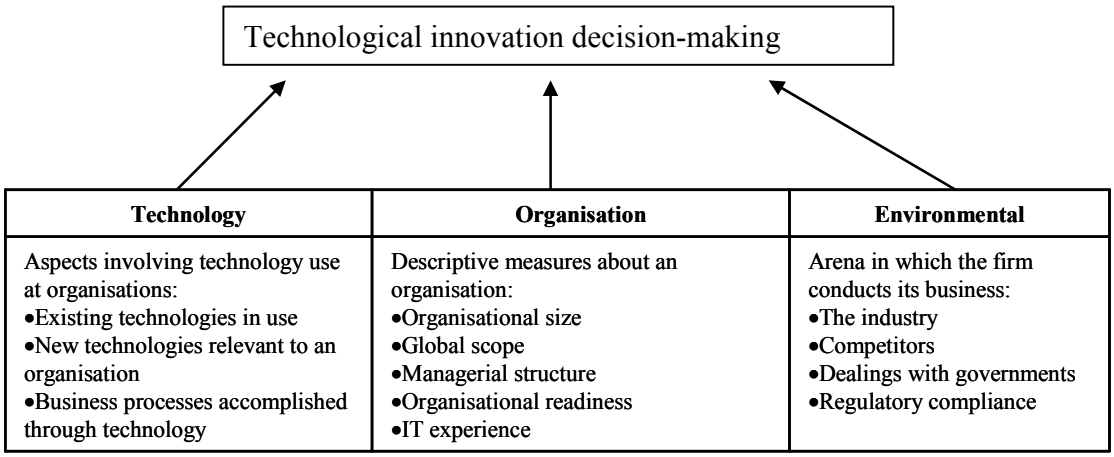


Figure 3: Some of the aspects examined by each of the TOE contexts
(*Adapted from*: Chau & Tam, 1997; Lee, 1998; Zhu et al., 2006)

Technological Context

A scalable and flexible solution

Scalability and flexibility of MFA solutions are a key consideration for organisations (Infoworld, 2009). The potential technologies - OTP, USB tokens, biometrics, digital certificates and so on that can be implemented should be evaluated by management in terms of current and future organisational requirements (Donnaruma, n.d.) and with consideration to all facets of the existing infrastructure (Infoworld, 2009; Nagel, 2009). Increasingly users may access a system through various means such as a client application, a web browser, or a cell phone or smart phone web browser; therefore implementing comprehensive security in terms of access control (Panko, 2009) is imperative for the protection of a company's network (Infoworld, 2009).

Fit with the existing ICT infrastructure

The proper implementation of technology, such as a web browser making SSL server certificate validation obvious and simple, is necessary to reduce security risks. Part of the security problem stems from underlying systems such as the computer operating system. In Microsoft Windows XP for example, users need to have administrative rights to install applications and this provides the opportunity for malware such as Trojan horses to be unknowingly installed onto the system (Schneier, 2005a). Such issues need to be addressed by implementing the best fit of MFA and SSO authentication solutions for the organisation based on existing technical infrastructure and other factors such as cost. Thorough research of available technologies is necessary for this to be successful (Nagel, 2009). Iannarelli (as cited in Schneier, 2005a) argues there is a significant drop in fraud and identity theft if authentication technology is properly implemented, specifically in relation to financial institutions. There is general consensus in the industry that no authentication schemes protect against attacks such as Man-In-The-Middle or Trojan horses (Schneier, 2005a) – however, determining the best solution for the current organisational situation is a best effort possibility. In addition, organisations that adopt MFA benefit from the trend of merging physical and logical security (Dubin, 2008a) whereby gaps in the two security domains can be closed and overall security better managed (Imprivata, 2009).

Solution complexity

Complexity and integration issues are cited as the major challenge for MFA and SSO implementations (Infoworld, 2009; Schneier, 2005a) and may change the way a company operates (Donnaruma, n.d). Factors such as the number of disparate systems that require encompassing security and methods of accessing these systems add elements of complexity and therefore require more organisational resources for support and maintenance. Allocating sufficient time and resources for an authentication implementation, including time for testing the system increases the probability of successful adoption (Nagel, 2009). Thorough project planning for a SSO/MFA organisational project, accounting for various system elements, is therefore necessary for project success.

The combination of SSO and MFA in security solutions is an important consideration in the selection of a solution (Infoworld, 2009) and leads to more robust security (Bigler & McCollum, 2004; Farnum, 2006; FinallySecure, 2009; Liou, 2007) thereby better protecting company networks. Industry experts state that even two-factor authentication is much better than password-only authentication regardless of which factors are used (Vance, 2006). Figure 4 indicates current authentication methods (based on market research survey results). MFA, as indicated by the red arrow, is used approximately 60% less than username/password authentication. Hence the adoption of MFA by organisations is still relatively low.

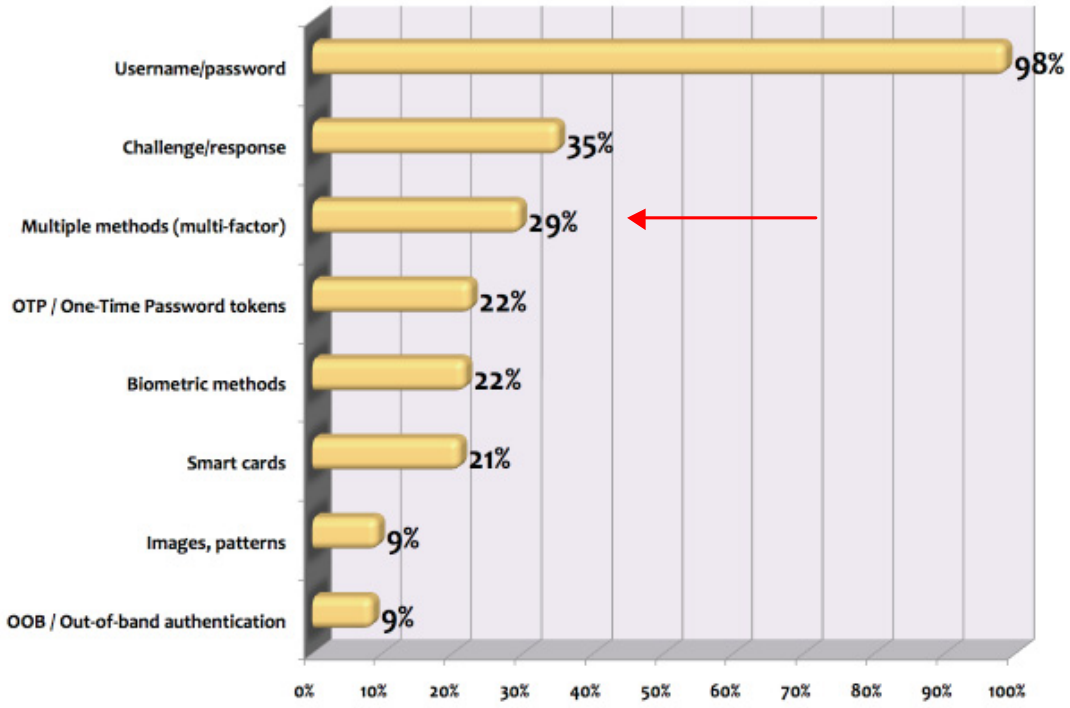


Figure 4: Authentication methods currently in use

(*Source*: Used with permission of Pistol Star and Osterman Research Inc, 2009, p. 12)

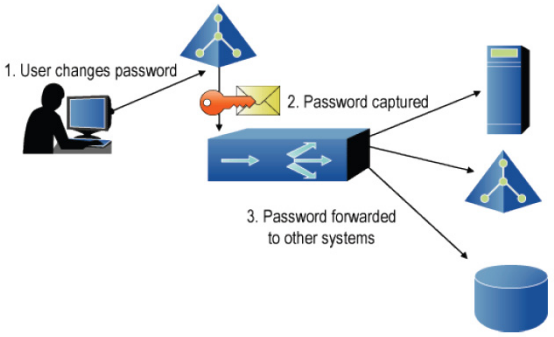
Key enabling network technologies and protocols

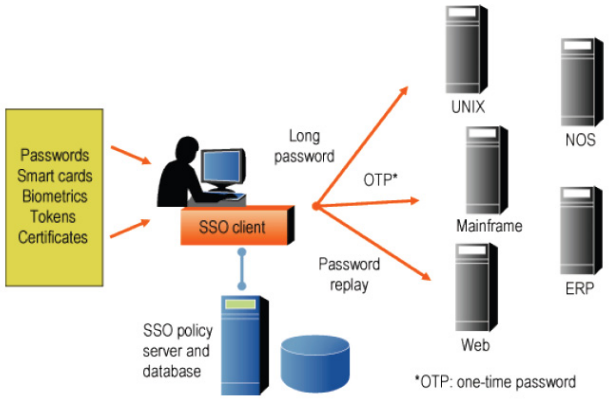
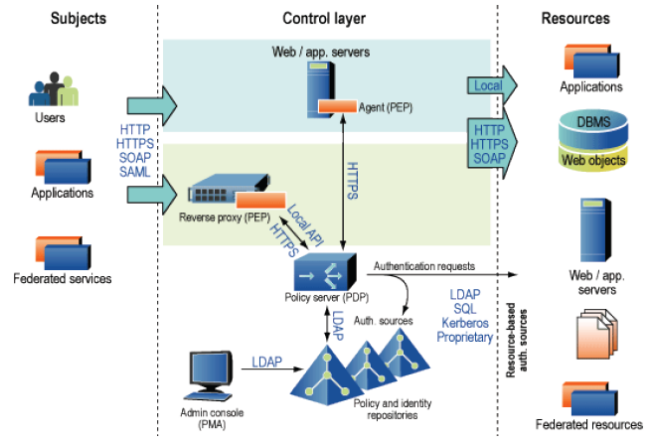
SSO implementation alternatives: There are a number of SSO technology alternatives, which may be classified as *active* (where the user is required to enter credentials whenever requested by

an application or another resource*)* or *background or passive (*where the infrastructure handles the credentials without prompting the user*)* authentication services (Liou, 2007). Alternatives also differ based on whether the SSO scope is extended to include multiple organisations and infrastructure platforms that may be using different credential authorities (De Clercq, 2002). In addition, SSO and MFA choices may be made based on various technologies and protocols. Refer to Table 1 for the various alternatives.

Table 1: Single Sign-On alternatives

(*Adapted from*: Boettcher, Daiberl, Fischer, & Liu, 2007; De Clercq, 2002; Gebel, 2008; Kelley & Poynter, 2002; Quest Software Inc, 2008; Robbins & Hamilton, n.d)

Type of Single Sign-On	Characteristics of SSO Solution	Illustration of Concept	Enabling Technologies for SSO (with MFA in some cases)
Holy Grail	• End-user has one logon to every resource without need to re-enter credentials • Credentials transparently presented to subsequent applications/systems • Efficient, secure, compliant method of Single-Sign On: Kerberos model • Authentication only provided		Kerberos protocol, RADIUS protocol, LDAP, PKI encryption
Password Synchronisation (Also known as Directory Single Sign-On)	• End-user has single password to all systems which are synchronized • Authentication requests are forwarded to central server • End-user still has to enter password for different applications as is prompted to do so		Agent XML scripts to synchronise application credentials, centralized authentication server, self-service password management, Out-of-band authentication

Enterprise Single Sign-On (ESSO)	• End-user has single login • Automated tool logs users into other systems and generates complex passwords that user does not need to know • Central point of management for multiple authentication schemes • Convenient for end-users • IT staff have to manage logins • Allow organisations to transition to using multi-factor authentication schemes		Multifactor authentication technologies, Agent XML scripts to synchronise application credentials between authentication server and client machine, Out-of-band authentication, PKI encryption
Web Single Sign-On	• Wider end-user base for an organisation – employees, customers, business partners • Limited to browser-based technology • Login only once to applications users need • Easier to manage than ESSO as authentication/authorization is managed centrally at web portal		HTTP, SAML, Cookies, Kerberos, LDAP, SOAP, OpenID, SQL

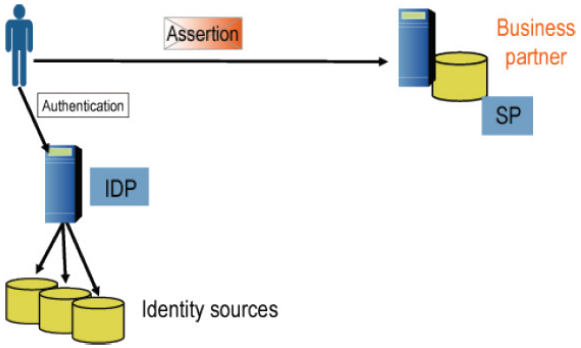
Federated Single Sign-On	• Similar to Web SSO as only allows access to web applications • Access to an organisations applications and its business partner applications is possible via identity assertions		SAML, Web Services Security (WSS), SOAP

Table 2 illustrates how these types of SSO technologies are employed across organisations for various user types. As more business is conducted across a variety of industries, Federated SSO is likely to increase in adoption due to the cross-integration capability it provides.

Table 2: Single sign-on Technologies
(Adapted from: Robbins & Hamilton, n.d, p. 3)

Types of Applications / User Types	Intranet Client/Server	Intranet Browser-based	Internet Browser-based	Extranet Browser-based
Employees	E-SSO; Directory Synchronisation; Kerberos	E-SSO; Directory Synchronisation; Kerberos, Web-SSO	E-SSO; Web-SSO	
Business Partners			Web-SSO	Federated SSO
Customers			Web-SSO	

SSO-enabling technologies and protocols

Kerberos: The Kerberos protocol is an open standard defined by the Internet Engineering Task Force (IETF) that is used on many platforms (De Clercq, 2002). It provides token-based strong authentication for client/server applications using secret-key cryptography and makes use of a server – the Key Distribution Centre - that authenticates a user's identity to other servers for a session (De Clercq, 2002; Griffeth, 2009a). The trust relationship between primary and secondary authentication domains is based on cryptographic methods that are used to validate the user token. Remote Procedure Calls (RPC) are typically used to transport authentication tickets (De Clercq, 2002). If an organisation wishes to authenticate users using SSO to multiple applications across various technologies, then Kerberos is a good choice (Griffeth, 2009a). But systems applications have to support Kerberos for this to work (Robbins & Hamilton, n.d.).

The Lightweight Directory Access Protocol (LDAP): The Lightweight Directory Access Protocol (LDAP) is used to query directory servers – servers that centralize information about an organisation such as employee names, telephone numbers and credentials (Panko, 2009) and also resources such as printers (Harris, 2007). Microsoft's version of LDAP - Active Directory – enables true SSO using Kerberos but only for Windows environments (Shaw, 2008). LDAP permits the use of directory-based SSO as one credential is used across multiple applications. Using a central LDAP server for application authentication is more practical instead of building authentication into each application (Gebel, 2008). Figure 5 illustrates where LDAP is used between a directory service and an authentication authority.

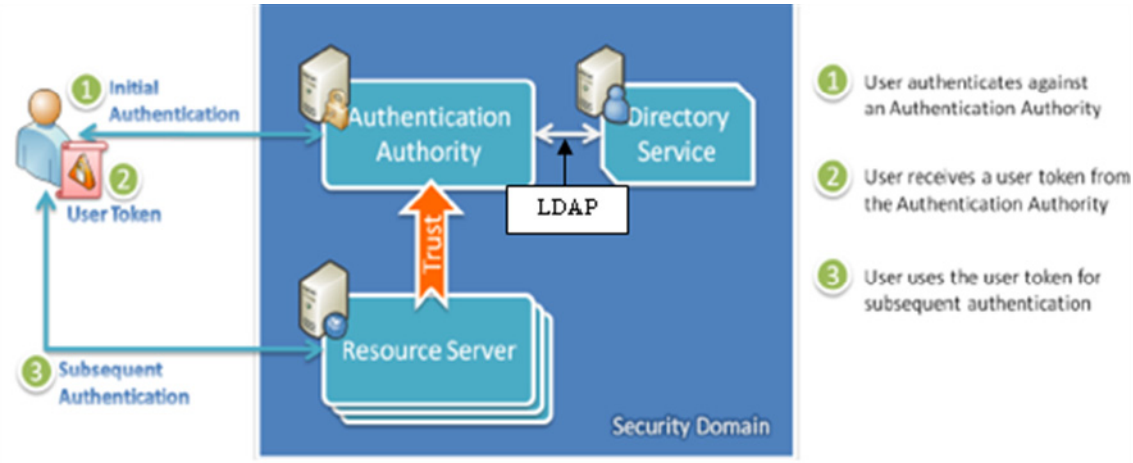


Figure 5: General security model for SSO with LDAP
(*Adapted from:* Boettcher et al., 2007, p. 2 with permission)

RADIUS protocol: The Remote Authentication Dial-In User Service (RADIUS) protocol is a connectionless client/server protocol (based on UDP) used for authentication (CISCO, 2006). RADIUS is useful for authenticating remote users who connect via a VPN, for example (Posey, 2005). When provided with user credentials, a RADIUS server – which is usually a daemon running on a Unix or Windows machine - can support various authentication mechanism such as PAP, PPP or Unix login (CISCO, 2006).

Agent Scripts: Scripts that run on a central authentication authority server can be used to synchronise a user's password across systems when security policies are revised or passwords change (Kelley & Poynter, 2002). This can be done via XML scripts and encryption using Structured Query Language (SQL) to manipulate the data in databases.

Cookies: Cookies are a token-based SSO technology for HTTP environments (De Clercq, 2002). Since the Internet is stateless some vendors use cookies - pieces of software that are downloaded onto the client machine - to authenticate sessions for certain time periods (Huntington, 2006a). After the cookie expires, the user will have to be re-authenticated.

Digital Certificates and Public Key Infrastructure (PKI): A Public Key Infrastructure (PKI) refers to a system used for storing and maintaining encryption keys (Dubin, 2006). Asymmetric public-private key encryption technology is employed as defined by the X.509 standard – which pertains to a particular certificate format (Housley, Ford, Polk, Solo, 1999).

In a PKI-based SSO environment, users first register with an authentication server (known as a Certificate Authority (CA)). The CA authenticates a user's identity based on verifying credentials against a credential database and then generating a public key certificate (based on a public key sent by the user), which is sent back to the user. This public key certificate and the user's private key - which are stored on the client machine or other means of authentication such as a smart card - are then used to generate a token, which is used to authenticate the user to additional authentication authorities. The trust relationship between primary and secondary authentication authorities is established based on a certificate issued to the secondary authority by the primary authority (De Clercq, 2002).

Security Assertion Markup Language (SAML): Security Assertion Markup Language (SAML) is a platform-independent, non-proprietary, XML-based protocol developed by Organisation for the Advancement of Structured Information Standards (OASIS) and is used for communicating user identities between parties (Boettcher et al., 2007; Organisation for the Advancement of

Structured Information Standards [OASIS], 2005). It is typically used between two or more parties who conduct business with each other (OASIS, 2005).

SAML is a key aspect of Federated SSO because it enables domains that implement different authentication mechanisms to communicate (Gebel, 2008). Federated identity refers to different parties agreeing to trust each other's identity management (Beckett, 2004). It is a dominant movement in identity management today due to cross-authentication system communication (OASIS, 2005).

Federated SSO allows a user to sign on once and be authenticated to access various systems. The federated identity management system enables a user's identity to be distributed across policy and/or application domains to which the user may require access. Different domains choose to rely on identity credentials that are held elsewhere (Paul, Yuzo & Kenji, 2005). The entities involved here are the user, the Identity Provider (IdP) and the Service Provider (SP) as shown in Figure 6. The IdP makes 'assertions' about the user's identity and attributes to the SPs. (OASIS, 2005).

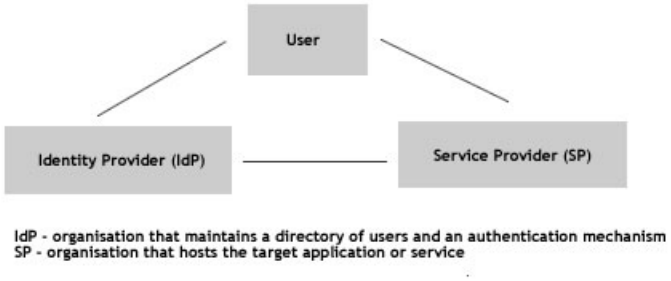


Figure 6: High-level overview of how SAML works
(*Adapted from*: Gebel, 2008, p. 12 with permission)

1. User has an account with an IdP
2. User wants to use a particular application hosted by the SP
3. IdP and SP have want to federate identities and have some sort of relationship

Other standards such as Shibboleth – for access to higher education research resources - and Liberty Alliance – for Web Services access - are based on SAML (OASIS, 2005).

Web Services Security (WSS): Web Services Security (WSS) specifies methods of encoding authentication and other security tokens – Kerberos tokens, user IDs/passwords, X.509 certificates, SAML assertions - in Simple Object Access Protocol (SOAP) message headers (Gebel, 2008). Using the WSS standards (WS-*), business entities can communicate across applications, domains and platforms.

OpenID: OpenID is a means of identifying oneself on the web. Described as an Internet driving license ("OpenID Explained," n.d.) it allows users to have one username and password for use on a variety of websites. OpenID is decentralized as users can choose where to host their identities and service providers can choose from a variety of software implementations and vendors (Becker & Norlin, 2006).

Technologies for MFA

Out-of-band authentication uses two separate network channels for communication with the user (Osterman Research Inc, 2009). For example, a computer network, which a user is trying to connect to, and a mobile phone network that the user has access to. The user may have to verify their identity via one channel before access is granted via the other.

Multi-factor authentication technologies such as One-Time Passwords (OTP), smart cards and biometrics can be used in conjunction with technology such as PKI encryption. OTP can be delivered in a variety of methods using XML/SOAP/SAML: via SMS, flash drive, key fob and can be derived based on client/server time synchronization or mathematical algorithms (Nagappan, 2009; Osterman Research Inc, 2009). Smart cards can store digital certificates and biometric information and can be contact or contactless cards (Nagappan, 2009).

Organisational Context

User acceptance

Usability is one of the most important factors in the organisational context of the TOE framework since the security of a system ultimately lies in the actions of the users. Passwords alone are no longer considered robust due to reasons such as users writing them down and sending them in emails (Schneier, 2005b). An MFA and SSO solution will be successful if both internal and external users of an organisation's systems use the technology, such as SSL certificates, in the correct manner (Schneier, 2005a). Organisations need to understand how users work and the key factors to user acceptance are convenience and improved user experience (Nagel, 2009; SearchSecurity, 2008; Witman, 2007). If users are customers, improved system usability translates to customer loyalty (Witman, 2007) and ultimately to increased business value.

The balance between usability and security can be challenging to achieve. For example, some banks have transaction validation solutions of requiring the user to enter a token for every transaction (Schneier, 2005a). This method increases security and prevents fraud, a major consideration of organisations in selecting an authentication solution (Infoworld, 2009), but could be cumbersome for customers and potentially result in a loss of customers. The adoption of a solution will affect employee productivity therefore an analysis of how people do their jobs should be conducted to prevent employee frustration. Employees will be unhappy carrying five different tokens to access five systems, for example. On the other hand, having one token for SSO to all five systems leads to the 'too many eggs in one basket' problem (Schneier, 2005b) referred to earlier in this paper whereby one compromised set of credentials gives an attacker access to multiple corporate systems.

Regardless of the technology chosen, good communication is paramount for user acceptance of an authentication solution (Nagel, 2009). In addition, training for internal users should be planned carefully accounting for the fact that the rollout of a solution may affect organisational departments in different ways (Donnaruma, n.d) and therefore testing should be done early, often and include departments outside the IT department or power-user community (Nagel, 2009).

Management support

Obtaining top management support for an MFA and SSO implementation, like in any IT project, increases successful adoption rates (Schwalbe, 2007). It is important that IT people sell the solution as a business solution that aims to provide value (Nagel 2009) by reducing the burden on current IT resources and staff (Infoworld, 2009). The requirements driver for a SSO solution should be clear whether it is usability-driven to reduce labour costs via reduced help-desk calls or security-driven to step up organisational security obfuscation (as cited in D'Costa-Alphonso, 2009).

Security professionals within the organisation or the outsourced company should perform an assessment of the current security weaknesses in relation to access control for systems applications and obtain high-level sponsorship as soon as possible. This management support will reverberate through the organisation and subsequently assist with employee buy-in (Nagel, 2009).

Organisational size and fit

The MFA methods adopted can be used in various ways, for example, taking into account: the work environment (Imprivata, 2009); to access content that has higher sensitivity (Dubin, 2008a) or content that has more risk (Huntington, 2009; Osterman Research Inc, 2009); areas that require more security, for example, certain applications, transactions (Imprivata, 2009). Other types of authentication factors while not typical include geo-location and transaction monitoring. These factors when combined with others are useful for fraud detection based on deviation from a user's normal behaviour (Huntington, 2009; Vance, 2008).

The increase in the number of remote and mobile employees at organisations affects the choice of authentication solutions (Infoworld, 2009) due to the element of secure access via blackberry devices or wireless LANS for example. It is imperative that the implementation of an MFA and SSO solution focuses on the current business needs and drivers (Donnaruma, n.d.).

Security budget

The cost versus risk battle is constant in the world of security. Organisations must assess whether the cost of protecting assets exceeds the value of the asset (Schneier, 2005b), in which case the protection is draining the budget. Security professionals must link authentication implementation projects to pressing business needs and isolate business problems that these solutions can solve (Nagel, 2009). In doing so, the cost-risk balance can be better addressed and return on investment reaped by the organisation.

Environmental Context

Regulatory compliance

A recent Forrester research report indicates that MFA adoption is on a steady rise. Even organisations that are not in heavily regulated industries need to adopt MFA because of the advantages it provides (Imprivata, 2009). Regulatory compliance, such as that required by the Federal Financial Institutions Examination Council (FFIEC) for Internet banking in the US has driven the rise of MFA (Cobb, 2009; Dubin, 2008a). Indeed, the finance industry is currently the most aggressive in adopting two-factor authentication, primarily due to financial systems having to adhere to strict guidelines with regards to information security (Schneier, 2005a), while adoption is rather slow in other sectors (Vance, 2008). A study by Aberdeen Group highlighted that organisations enjoying the best security performance had increased MFA implementations by 300% over a nine-month period (Imprivata, 2009). This finding suggests that MFA methods will continue to gain traction as means of improving overall security. SSO assists in the auditing and monitoring of user accounts thereby increasing corporate security and adherence to compliance such as the Sarbanes-Oxley Act (SOX) (SearchSecurity, 2008)

Increased regulation, such as that seen in the finance industry, could increase the employment of MFA and SSO solutions in other industries. When credit card liability was the consumer's problem, organisations did not strive to improve their security. However, due to regulation the onus is now on organisations and therefore they are continuously required to refine their security (Schneier, 2005a), although implementing SSO and MFA to support electronic commerce transactions still appears to be problematic.

Industry outlook

There is no industry-accepted standard for enforcing good password selection thereby leading to uneducated users exposing organisations to increased risks and successful system attacks by script kiddies (Schneier, 2005a). This issue of enforcing sufficient strong password selection can be addressed individually by organisations through their information security policy. With the new authentication methods, many information security standards organisations including the Organisation for the Advancement of Structured Information Standards (OASIS), the OpenID Foundation, the Liberty Alliance and the Smart Card Alliance are pushing for strong authentication standardisation because this will allow for better compliance to future industry regulations for user role-based restrictions (Beckett, 2004; Vance, 2008).

Competitive pressure

The use of robust SSO and MFA methods can give an organisation a competitive advantage over other firms in its industry (Nagel, 2009; Witman, 2007) and enhance its reputation due to the investment it has made in better protecting customer data (Witman, 2007). Customers are now more aware of security and privacy issues and addressing these issues will ensure customers remain loyal to the organisation (Schneier, 2005a). A recent survey indicates that organisations consider improving customer confidence in the areas of data security for sensitive or private information, an important factor in their selection of an authentication system (Infoworld, 2009).

Key Benefits and Challenges of SSO and MFA

Table 3 summarises the benefits associated with implementing SSO and MFA within organisations.

Table 3: Benefits associated with an SSO/MFA implementation

Benefits	Benefit explained
Increased user productivity and user satisfaction	Single sign-on reduces time users spend logging into systems therefore increasing workforce productivity (FinallySecure, 2009; Passlogix, 2009; Schneier, 2005a) – Example, in healthcare industry SSO prevents constant login and logout scenarios when workers have to switch among many different systems (Tiazkun, 2009).
Reduced IT costs	Password reset calls to IT helpdesk cost estimated $25 each (Gebel, 2008). SSO reduces number of help-desk calls (FinallySecure, 2009; Imprivata, 2009; Schneier, 2005a) by up to 95% (FinallySecure, 2009) since users have fewer passwords to remember. In addition, the costs of development (Passlogix, 2009), installation and maintenance of separate authentication systems for applications are reduced (Liou, 2007) as SSO solutions provide central management of users (De Clercq, 2002; FinallySecure, 2009; Passlogix, 2009; SearchSecurity.com, 2008). Cost of MFA systems such as fingerprint scanners is decreasing and reliability is improving, further reducing IT costs and improving efficiency (Imprivata, 2009).
Increased corporate data security	Employing SSO allows user passwords to be complex and change frequently as users do need to remember multiple passwords (Passlogix, 2009). System security is increased and reduced probability of user password interception via tactics such as social engineering (Farnum, 2006; FinallySecure, 2009; Griffeth, 2009b). Security policies can be more robustly employed and centralized in an organisation (De Clercq 2002; FinallySecure, 2009). The risk of a hacker obtaining the 'keys to the castle' reduced by using MFA with SSO and gives more assurance of a user's true identity (Griffeth, 2009b; Passlogix, 2009) - sometimes required for systems or transactions of higher risk to an organisation (Huntington, 2009; Osterman Research Inc, 2009). SSO with MFA also prevent phishing and malicious code infections because while user's password may be compromised, additional authentication factors such as tokens or biometrics cannot be obtained (Griffeth, 2009b; Uniejewski, 2005). With MFA, user's passwords for SSO can also be easier to remember because of the extra layer of security that MFA provides (Osterman Research Inc, 2009). The merger of physical and logical security also aids in MFA adoption as employees can use same devices for two purposes (Dubin, 2008a).
Adherence to regulatory compliance	Regulatory compliance such as HIPAA and Sarbanes-Oxley Act in the US and Privacy Act in Australia call for data privacy and integrity. SSO assists with logging and monitoring of user accounts via auditing and tracking user activities assisting organisations to adhere to these Acts (Osterman Research Inc, 2009; SearchSecurity.com, 2008).
Increased business customer base	The need to create a user account requiring a password deters many people from registering on retailer websites (IBM Global Services, 2002). This is lost business for owners. SSO can assist with technology such as OpenID where user need not register with a password, encouraging more registrants and business.

Table 4 provides an overview of the main challenges that organisations will have to overcome in a SSO/MFA implementation.

Table 4: Challenges associated with SSO/MFA implementation

Challenges	Challenge explained
Addressing new methods of attack	While MFA minimizes security problems related to access control (Dubin, 2008a; Schneier, 2005a) claims that MFA does not contribute to increased security: OTP tokens can be compromised by man-in-the-middle phishing attacks (Dubin, 2008a; Osterman Research Inc, 2009; Schneier, 2005a); smart cards can be hacked (Dubin 2008a) or lost/stolen (Osterman Research Inc, 2009); attackers can use Trojan horses to piggy-back user sessions after they have logged in (Schneier, 2005a). There are further claims that MFA involving out-of-band authentication is cumbersome for users (Osterman Research Inc, 2009). Security experts say although MFA can be cracked, it does add additional layers of security (Dubin, 2008a; Schneier, 2005b) more within corporate networks and less over the Internet because attackers will merely change tactics (Schneier, 2005a, 2005b).
User acceptance	Success of SSO and MFA requires user acceptance. Users may be reluctant to carry around MFA tokens or be fingerprinted (Vance, 2008). Tokens can also be easily damaged, misplaced or forgotten by users (Cobb, 2009). Privacy issues need to be addressed as ownership of personal profiles and information is an unresolved personal issue that could limit SSO and MFA adoption (IBM Global Services, 2002). User acceptance and training on the benefits of SSO with MFA is a key challenge.
Costs	Depending on SSO and MFA technology involved and size of an organisation, system costs (for install and maintenance) can be extremely high (Cobb, 2009). Some existing organisational systems such as client software may not support MFA devices and in these cases, additional hardware or software may need to be purchased, configured and installed (Bigler & McCollum, 2004). A cost-benefit analysis may be useful in determining the worth of SSO and MFA.
SSO and MFA rollout	Planning a SSO implementation bears both technical and business challenges (Robbins & Hamilton, n.d.). For example, if the SSO system fails, all users will be locked out (Huntington, 2006a). In order to overcome these challenges, enterprises should undertake an analysis of the business including elements of organisational size, business drivers, risk levels of corporate systems, user base, compliance requirements and so on (Osterman Research Inc, 2009; Robbins & Hamilton, n.d.; SearchSecurity.com, 2008). The outcome of this process will enable an organisation to implement an SSO solution that best fits its needs. Figure 7 highlights SSO areas that should be addressed.
System complexity	SSO is a process not a product (Huntington, 2006a) and successful implementation relies on finding appropriate business fit for this security process. Implementations and deployment can be complex, more so if MFA is used with SSO (Cobb, 2009). Equipment used for MFA is not without flaws – for example, fingerprint readers can give 'false rejections' meaning the real user is mistakenly not authenticated (due to for example, having a cut on their finger) (Osterman Research Inc, 2009). Incorporating legacy applications into SSO as well as systems that may be acquired via corporate mergers or acquisitions (Kreizman, 2008) also adds complexity because of integration of disparate technologies.

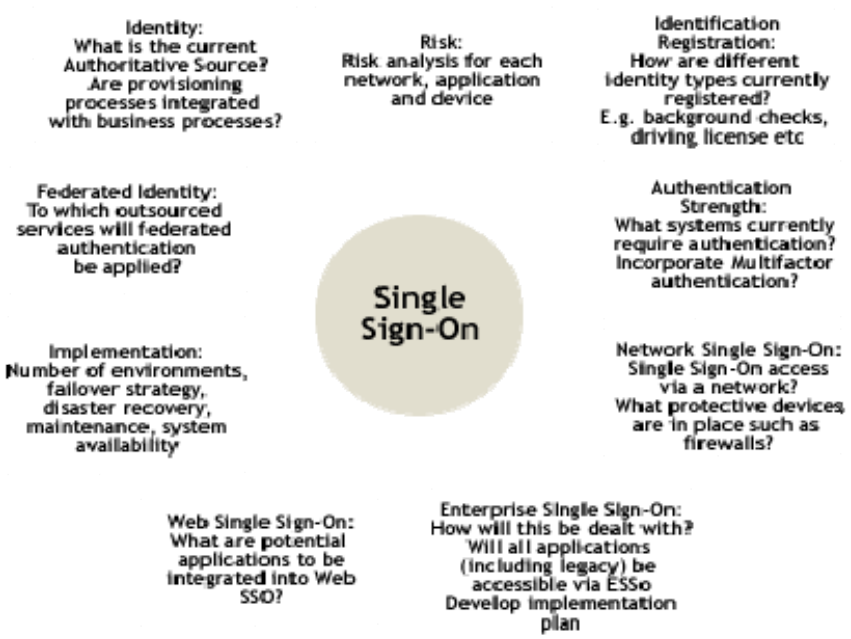


Figure 7: Aspects to address to overcome SSO challenges
(*Adapted from*: Huntington, 2006b)

Research Question and Method

The general research question that was investigated in the first phase of this study was:

What are the key factors facilitating and inhibiting the adoption of single sign-on (SSO) and multi-factor authentication (MFA) in organisations?

Our motivation and justification for conducting this exploratory study, is that while much has been written about by practitioners of SSO and MFA, this is largely anecdotal and there is little empirical research on the factors impacting on the adoption of SSO and MFA. A qualitative approach was deemed appropriate to guide the focus of the first phase of this exploratory study (Miles & Huberman, 1994; Yin, 2009). A qualitative approach allowed the researchers to explore the research question in an interpretative manner in line with the research objectives. It was necessary to capture rich domain knowledge from practitioners experienced in implementing SSO and MFA solutions in large organisations, in order to identify the key issues in relation to the general research question that reflect the reality of current practice.

A content analysis of some active online information security blogs and discussion forums where SSO and MFA was a discussion thread allowed us to analyse the views of experienced and expert practitioners in relation to the adoption of SSO and MFA in organisations. Our content analysis of these online discussions was guided by the Technology-Organisation-Environment (TOE) framework that was outlined in the literature review section of this paper. In the next phase of this study we will conduct structured interviews with informants from organisations that have adopted SSO and MFA, and industry practitioners who have expertise in the implementation of SSO and MFA in organisations and have agreed to be involved in the next phase of the study.

These online discussions of SSO and MFA were analysed using the qualitative data analysis software package NVivo 8 (QSR International, 2009). This software package allowed for the exploration of raw data and identification and coding of the common themes guided by our theoreti-

cal framework as well as the identification of relationships between themes in a rigorous manner. While there are some limitations in the approach used, it is felt that the richness of the data collected far outweighed the methodological shortcomings of such an approach.

Discussion of Key Findings of Data Analysis

The analysis of the qualitative sources of data addressed the general research question:

'*What are the key factors facilitating and inhibiting the adoption of single sign-on (SSO) and multi-factor authentication (MFA) in organisations?'*

The key findings of the data analysis are discussed below in the context of the TOE framework.

Technology issues

A SSO and MFA solution suitable for existing technical infrastructure and scales for future organisational growth

An important consideration in the implementation of SSO and MFA is the scalability and customizability of the technical solution. The choice of technology and the fit to the various systems in use is a key factor inhibiting successful implementations of MFA as evidenced in the following comment by a practitioner in response to an article by world-renowned information security expert Bruce Schneier.

> *"I would tend to agree that in the 'big picture', if technology isn't used properly or the technology isn't implemented properly, it doesn't matter how many factors of authentication one has."* (as cited in Schneier, 2005a)

Another practitioner comment highlights the importance of having a scalable SSO solution that can be altered due to changes in business processes or corporate mergers, for example.

> *"Every time the business requires a change to security policy, access control or SSO expansion, there is a potential change to your SSO environment. I would advise checking internal processes and business change projections for the next few years before embarking on the deployment. If future planning is built into the design phase, ongoing operational needs can be reduced dramatically*."(as cited in D'Costa-Alphonso, 2009)

An interesting approach to an MFA solution is the use of a mobile phone to generate and distribute one-time passwords via SMS messaging. A practitioner comment to this approach to two-factor authentication highlights that such an approach needs to ensure security of mobile phones as well:

> *"For a corporation, you would need to have a solid mobile phone program in place, where you can ensure that the phones are secured, remotely wiped if lost or stolen*"(as cited in Axworthy, n.d.)

The comment above provides an example of the comprehensive approach that organisations would need to take in employing a MFA solution in terms of addressing the risk that an employee's mobile phone could be compromised.

Man-in-the-middle attacks and Trojan horses can compromise two-factor authentication solutions (Schneier, 2005a) therefore the MFA solutions employed by an organisation would require a secure technical infrastructure. A solution offered in response to Schneier's post by a practitioner indicates the use of two technologies organisations can be used to ensure the security of their MFA technical infrastructures:

> *"Use a keystroke analytics technology to ensure that passwords are actually typed in by the person assigned the password, i.e. www.biopassword.com* ."(as cited in Schneier, 2005a)

Organisations need to clearly identify the technical infrastructure requirements that currently exist and could exist in the future based on planned or emergent organisational strategies before selecting and implementing an SSO and MFA solution successfully.

The complexity of the client workflow environment

Technology within an organisation may also include the processes that employees follow in order to get their work done. This may include workflow processes for example where data moves between different systems that have different identity access requirements. A practitioner experienced in many SSO implementations highlights this as a key technical issue in projects he has participated in:

> *"The main issue I encounter every time I do a SSO project is the complexity of the internal application workflow in the client environment. The client rarely understands the information gathering required for a SSO project. They hardly every have resources with a solid understanding of the internal application workflow let alone the databases behind it. That information is crucial to deliver success*."(as cited in D'Costa-Alphonso, 2009)

Another practitioner who has seven years experience in designing and implementing SSO solutions for public and private organisations similarly commented on the challenges of implementing SSO in complex workflow environments*:*

> *"These days rather than the technology for profiling applications being the stumbling block (used to be historically) one of the largest headaches can be the workflow of credentials within the application. Where most applications simply require a username and password and you are either presented with an access or denial to the application I am seeing a lot more complex workflows with cross application authentication, transactional authorization, re-authentication and password change screens being part of the initial login screen*."(as cited in D'Costa-Alphonso, 2009)

Integrating a number of applications with a SSO solution would require extensive analysis of the authentication method each application employs:

> *"Integration with other products is important. For example, if you need delegated credentials (user logs on to app[lication] that needs to exercise rights against say a database as that user (for audit reasons) then understanding what all the intermediate layers supports is important*."(as cited in D'Costa-Alphonso, 2009)

For web applications, the length of session timeouts may need to vary across applications and the SSO implementation team would need to get consensus from application owners to define rules such as acceptable time allocation for session timeouts at an enterprise-wide level so as to enable smooth workflow processes. This is outlined in the practitioner comment below:

> *"SSO should be a simple authentication API and authentication token sharing system, have the proper access to the auth[enticated] information and passing along a token based hash that would be valid throughout the whole usage of the system and based off on specific business rules about session expiration and timeout rules defined by your enterprise architecture team following the mutual agreements within the whole enterprise-wide level*."(as cited in D'Costa-Alphonso, 2009)

With regards to MFA, authentication within a workflow process can be problematic in terms of the increasing numbers of remote and mobile employees. A comment made by a practitioner highlights this issue:

> *"However, one problem which I see (and have also encountered) is users who change states/countries. Because their mobile phone connectivity may not be available everywhere they roam, it may directly impact their access to their own accounts*."(as cited in Axworthy, n.d.)

The above comment is an example of client workflow issues with MFA when employees try to access corporate systems via their mobile phones across a geographically dispersed organisation.

It should also be noted that these technology issues also have organizational implications when there is a negative impact on workflow processes.

Organisational issues

Management support

Obtaining management buy-in for a SSO and MFA solution – IT project - increases the chances of successful adoption. The focus of the SSO / MFA project should be communicated and conveyed by management to employees to garner their support and acceptance. Management would have to sell the benefits of a SSO/MFA project in different ways, depending on what the drivers are for its adoption in an organisation, as commented by a practitioner:

> *"For example, is your project security-driven (i.e., you really want a strong authentication technology, and SSO is the way to integrate that with your legacy applications) or convenience-driven (i.e., your users are just tired of typing so many passwords), or perhaps just cost-driven (reduce help desk call volume)."* (as cited in D'Costa-Alphonso, 2009)

Management must support the authentication initiative and perform a cost-benefit analysis in conjunction with a risk analysis for protecting assets so the cost of investing in SSO and MFA technology is justifiable. The asset will be protected – so long as the benefit of protection outweighs the cost and the risks. The comment below by a practitioner emphasizes this point:

> *"In many scenarios I have seen the cost of protecting an asset exceeding the value of the asset. This is not good security. It is simply just throwing money at a problem only to learn it will require more money later as risk changes."* (as cited in Schneier, 2005a)

Organisational readiness

Organisational readiness implies that a thorough requirements analysis is conducted by the organisation in the planning stages of an SSO/MFA project. This analysis should include the involvement of internal resources at the organisation during the project among other requirements as outlined in the practitioner comment below:

> *"The first stage in planning an SSO project is knowing your needs in regards to security, infrastructure, budget, and the expected 'user experience'. Also worth considering, even with the employment of specialists to deliver your end solution, there will be high and unavoidable internal resource requirements and this element is often not accounted for when planning an SSO implementation*."(as cited in D'Costa-Alphonso, 2009)

Another interesting perspective on organisational readiness is the key difference between organisations in the public versus commercial sectors in terms of their readiness to adopt SSO/MFA solutions as explained by this practitioner:

> *"In my experience I find that commercial organisations are able to assign resources quite quickly and focus on driving the solution through to completion and reap the true ROI benefits whereas public sector organisations have so many projects on the go at any one time that focus is sometimes lost and it takes a larger effort by the supplier to drive the customer through to completion*."(as cited in D'Costa-Alphonso, 2009)

Other aspects of organisational readiness include highlighting the key requirement that is driving the SSO project as stated by a SSO practitioner:

> *"Another real important factor is the requirement that drives the project. Is it a usability driven project (reduce labor and help desk costs linked to loss of productivity) or a security project (obfuscate passwords to users, increase password strength by randomizing password, increasing length and complexity). A skilled SSO expert would recommend different approaches depending of the requirement."* (as cited in D'Costa-Alphonso, 2009)

Understanding the key requirements driving the project is clearly important - these should be the focus of the SSO/MFA project planning phases to ensure that the organisation is ready for implementation.

User readiness and acceptance of an SSO solution is critical to ensuring overall organisational readiness as noted by a practitioner:

> *"I also find that it is the end users that determine the success of the project, if it makes their life easier then it is usually successful. If it changes or deviates away from their current work processes too much they will object to a change."* (as cited in D'Costa-Alphonso, 2009)

User readiness and acceptance is also critical for the successful adoption of an MFA solution as indicated in this comment by a practitioner with regards to using a mobile phone for MFA:

> *"Having 2 factors is better than having 1 factor. The second factor depends on your users and environment. In some cases you may need to implement more than one type to accommodate all your different users and environments. Keep in mind: you should always choose something that is simple and easy to use. It if requires training, installing, deploying etc it will be a pain for everyone every day and people won't use it."* (as cited in Axworthy, n.d.)

The following practitioner comment summarises the importance of gaining user acceptance for adoption of a SSO and MFA solution:

> *"Bottom line: understand where your users come from (physical location, logical relationship to the network, authentication mechanism, device type and form factor and where they are going (target application). Then figure out how to meet those constraints."* (as cited in D'Costa-Alphonso, 2009)

Environmental issues

Industry regulation

Clearly laws and regulations within certain industries mandate appropriate levels of security and privacy for information systems and information assets and necessitate that organisations within those industries adopt certain technologies such as SSO and MFA. The practitioner comment below emphasises this fact with regard to financial institutions:

> *"I'd agree that banks get more serious about security when there's some legal liability involved."* (as cited in Schneier, 2005a)

Social knowledge

System users – customers and employees - are becoming increasingly aware of security and privacy issues and hence organisations now have an obligation to better educate and inform customers and employees about the appropriate use of technologies that protect them in this regard as noted in the Schneier (2005a) blog:

> *"Big players have tried for years to keep the down side away from the news (to gather customers) but I think the time has come to educate people on the Do's and Don'ts in an open way. In the end, it's always on their side."* (as cited in Schneier, 2005a)

Due to increasing user awareness there is pressure on organisations to implement robust security measures to protect consumer data.

Table 5 summarises the key factors identified in this study, via our analysis of the knowledge embedded in online practitioner forums, which affect organisational adoption of SSO and MFA in the context of the TOE framework. Based on the analysis of these research sources factors are categorized as either inhibiting or facilitating the adoption of SSO and MFA solutions.

Table 5: Key factors that affect the organisational adoption of SSO and MFA

Technology	Organisational	Environmental
Suitability and scalability of the SSO/MFA solution with the existing technology infrastructure (I)	Management support (F)	Industry regulation (F)
Complexity of the workflow environment (I)	Organisational readiness (F)	Social knowledge (F)

Legend:

(F) – factor facilitating adoption of SSO and MFA

(I) – factor inhibiting adoption of SSO and MFA

Table 5 above indicates that technology factors would appear to be primary inhibitors to the adoption of SSO and MFA within organisations while organisational and environmental factors would appear to primarily facilitate adoption.

Benefits and Challenges of Implementing SSO and MFA in Organisations

Based on the analysis performed previously, we identified the key benefits for an organisation implementing SSO and MFA:

- The achievement of the primary goal that drove the project – whether it was user satisfaction, reduced costs or the increased protection of a company network.
- The adherence to industry regulation such as user activity auditing within corporate systems achieved via a SSO/MFA solution.
- Increased competitive advantage due to the ability to ensure increased security and privacy of consumer data.

Despite the possible benefits a number of challenges would need to be addressed for successful implementation of a MFA/SSO solution:

- A major challenge is looking to the future – in terms of scalability, organisational strategy and timing. The MFA/SSO solution must be adaptable to changes that may occur in the future. If the intention of an SSO/MFA implementation is user satisfaction, then it is important to understand how employees perform their jobs to gain their acceptance of the solution. This can be a difficult process involving understanding how jobs are performed in the context of multiple systems and complex workflows.
- While current security measures are being developed and implemented, hackers are developing new and improved means of breaking into systems. It is therefore a constant challenge to ensure that organisational security is robust and comprehensive.

Limitations and Future Work

The limitations of the first phase of this research include that some of the qualitative data obtained from online blogs and discussion forums was secondary and the perspectives of key stakeholders such as senior management and end users was not directly solicited. Therefore, certain assumptions may have been made by the authors in interpreting and presenting the results of the

qualitative data analysis. Future research will focus on conducting a suitable number of interviews with the key stakeholders such as senior management, IT professionals, and end users in adopting organisations and with consulting practitioners in the field of SSO and MFA. This will provide a richer set of data and allow a more robust interpretation of the key facilitating and inhibiting factors for the adoption of SSO and MFA solutions, which can be mapped more precisely onto the TOE framework.

Conclusions and Implications

The challenge for organisations to find an authentication solution that is both convenient and secure is ongoing. Single sign-on and multifactor authentication technologies have somewhat assisted with advancing the security industry towards presenting such a solution. Due to the wide choice of SSO and MFA technologies and options, a thorough analysis of security requirements should initially be conducted. This analysis should focus on aspects such as system users, the business of an organisation and types of system applications. Benefits reaped from such authentication mechanisms, such as increased system security and reduced administration costs are apparent, however for a successful implementation a number of difficult challenges – most importantly, combating smarter attacker tactics – have to be overcome.

The results of the analysis conducted for this paper indicate that technology issues are the main factors inhibiting the adoption of SSO and MFA within organisations; this is partly due to complexities of existing technical infrastructures and workflow processes. This is not to imply that organisational and environmental issues are entirely facilitating – they do influence the degree of successful adoption but are affected by factors such as management support and organisational communication, which can be successfully, controlled with robust change management processes within the organisation.

References

Australian Government Office of the Privacy Commissioner. (2009). *NPPs plain English summary*. Retrieved October 3, 2009,from http://www.privacy.gov.au/materials/types/law/view/6893

Axworthy, H. (n.d.). *Would you use one-time-only passwords if they were generated on your phone?* Retrieved November 20, 2009, from message posted to LinkedIn group, http://www.linkedin.com

Becker, P., & Norlin, E. (2006). The case for OpenID. *DigitalID World*. Retrieved October 9, 2009, from http://blogs.zdnet.com/digitalID/?p=78

Beckett, H. (2004). Who goes there? *Computer Weekly*, 62-64.

Bigler, M., & McCollum, T. (2004). Single sign-on. *Internal Auditor, 61*(6), 31-34.

Boettcher, T., Daiberl, J., Fischer, A., & Liu, L. (2007). Unleash the power of single sign-on with Microsoft and SAP. *Collaboration Technology Support Center – Microsoft – Collaboration Brief September 2007*. Retrieved October, 5, 2009, from http://download.microsoft.com/download/c/6/c/c6c42b9f-66f4-47b3-99be-8e5afa1ddc9a/SSO%20with%20MS%20and%20SAP.pdf

Chau, P. Y. K., & Tam, K. Y.(1997). Factors affecting the adoption of open systems: an exploratory study. *MIS Quarterly*, *21*(1), 1-24.

CISCO. (2006). *How does RADIUS work?* Retrieved October, 13, 2009, from http://www.cisco.com/application/pdf/paws/12433/32.pdf

Cobb, M. (2009). Why multifactor authentication hasn't taken off. *TechTarget*. Retrieved August, 6, 2009, from http://searchsecurity.techtarget.com.au/articles/34435-Why-multifactor-authentication-hasn-t-taken-off

D'Costa-Alphonso, M. (2009). *Does anyone have experience with an organisational single sign-on implementation? What are the typical issues that were encountered and had to be addressed for the imple-*

mentation to be successful? Retrieved November 28, 2009, from responses to message posted on social business networking site LinkedIn SSO Group, http://www.linkedin.com

De Clercq, J. (2002). Single sign-on architectures. *Infrastructure Security, 2437*, 40-58.

Donnaruma, D. (n.d). Multi-factor authentication. *Technology Management.* Retrieved October 2, 2009, from http://www.socialtext.net/techmgt/index.cgi?multi_factor_authentication

Dubin, J. (2006). *How PKI systems work*. Retrieved October 9, 2009, from http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1174566,00.html

Dubin, J. (2008a). *Understanding multifactor authentication features in IAM suites*. Retrieved October 2, 2009, from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1314185_mem1,00.html

Dubin, J. (2008b). *Trends in enterprise identity and access management.* Retrieved October 2, 2009, from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1319773_mem1,00.html ?ShortReg=1&mboxConv= searchSecurity_RegActivate_Submit&

Farnum, M. (2006). *The multi-factor authentication's relationship to SSO.* Retrieved October 2, 2009, from http://infosecplace.com/blog/category/multi-factor/

FinallySecure. (2009). *Already working or still authenticating again, again, and again? Smart enterprise single sign-on*. Retrieved September 24, 2009, from http://www.finallysecure.com/html/fileadmin/files/pdfs/WPs/FinallySecure_Whitepaperr_SecureSignOn_EN.pdf.

Gebel, G. (2008). Burton Group technical position on reduced sign-on. *Identity and Privacy Strategies*. Retrieved October 2, 2009, from https://wiki.doit.wisc.edu/confluence/download/attachments/10031748/Reduced+Sign-On+Technical+Position.pdf?version=1

Griffeth, D. (2009a). *Using Kerberos for single sign-on*. Retrieved October 4, 2009, from http://searchsecurity.techtarget.com.au/articles/31160-Using-Kerberos-for-single-sign-on

Griffeth, D. (2009b). *How to use single sign-on for web access control to prevent malware*. Retrieved September 26, 2009, from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1349071,00.html

Harris, S. (2007). *CISSP all-in-one exam guide*. Retrieved October 2, 2009, from http://books.google.com.au/books?id=tiKZ0ssRvsC&dq=password+synchronization+technologies&source=gbs_navlinks_s

Housley, R., Ford, W., Polk, W., & Solo, D. (1999). *Request for comments: 2549 Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. Retrieved October 9, 2009, from http://www.ietf.org/rfc/rfc2459.txt

Huntington, G. (2006a). *Single sign-on underneath the hood – What senior managers need to know*. Retrieved October 2, 2009, from http://www.authenticationworld.com/Single-Sign-On-Authentication/SingleSig nOnUnder-neathTheHood2006.pdf

Huntington, G. (2006b). *101 things to know about single sign-on.* Retrieved September 23, 2009, from http://www.authenticationworld.com/Single-Sign-On-Authentication/101ThingsToKnowAboutSingleSignOn.pdf

Huntington, G. (2009). *The business of authentication*. Retrieved October 2, 2009, from http://www.authenticationworld.com

IBM Global Services. (2002). *Single sign-on: Putting users first*. Retrieved September 25, 2009, from http://www-935.ibm.com/services/id/igs/pdf/g510-1649-00-etr-single-sign-on.pdf

Imprivata. (2009). *A more secure front door: SSO and strong authentication.* Retrieved September 29, 2009, from http://www.imprivata.com/stuff/contentmgr/files/1/594534094da355ff789b2732f0c7f1ef/misc/a_more_secure_front_door_0909.pdf

Infoworld. (2009). *The need for two-factor authentication at enterprise organizations*. Retrieved October 6, 2009, from http://www.infoworld.com/d/security-central/wp/need-two-factor-authentication-enterprise-organizations-327

Kelley, D., & Poynter, I. (2002). *Single sign-on 101: Beyond the hype*. Retrieved October 2, 2009, from http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-poynter-sso.ppt

Kreizman, G. (2008). *Magic quadrant for enterprise single sign-on*. Retrieved September 23, 2009, from http://mediaproducts.gartner.com/reprints/ca/160413.html

Lee, M. K. O. (1998), Internet-based financial EDI: Towards a theory of its organizational adoption, *Computer Networks and ISDN Systems, 30*(16), 1579-1588.

Liou, M. (2007). *Enterprise single sign-on best practice considerations*. Retrieved October 2, 2009, from http://ca.com/files/WhitePapers/enterprise_sso_best_practice_wp.pdf

Miles, M. B. & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Thousand Oaks, CA: Sage.

Nagappan, R. (2009). *Stronger/multi-factor authentication for enterprise applications*. Paper presented at the OWASP seminar. Retrieved September 27, 2009, from http://www.coresecuritypatterns.com/blogs/wp-content/uploads/2009/02/owasp-multifactorauthn-rameshnagappan.pdf

Nagel, B. (2009). Risk-based multifactor authentication implementation best practices. *IAM Insights*. Retrieved November 20, 2009, from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1368238,00.html

Organisation for the Advancement of Structured Information Standards. (2005). *SAML v. 2.0 executive overview*. Retrieved October 3, 2009, from http://www.oasis-open.org /committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf

OpenID explained. (n.d.). Retrieved October 9, 2009, from http://openidexplained.com

Osterman Research Inc. (2009). *Authentication in the enterprise: Current and changing requirements*. Retrieved September 26, 2009, from http://viewer.media.bitpipe.com/1149286151_178/1251217323_698/White-Paper_Authentication-Trends.pdf

Pandit, A. (2009). *ESSO vs web SSO - which one's right for you?*. Retrieved October 5, 2009, from http://iam.abhijitpandit.com/2009/09/06/esso-vs-web-sso--which-ones-right-for-you-.aspx?ref=rss

Panko, R. (2009). *Business data networks and telecommunications* (7th ed.). Upper Saddle River, New Jersey, USA: Pearson Education.

Passlogix. (2009). *The death of passwords*. Retrieved September 25, 2009, from http://www.passlogix.com/document_library/DeathtoPasswordsWP.pdf

Paul, M., Yuzo, K., & Kenji, T. (2005). Federated identity management for protecting users from ID theft. *Proceedings of the 2005 workshop on Digital identity management.* Fairfax, VA, USA, 77-83.

Posey, B. M. (2005). *Solutionbase: Best practices for implementing RADIUS*. Retrieved October 13, 2009, from http://articles.techrepublic.com.com/5100-22_11-5513942.html

QSR International. (2003). *NVivo*. Retrieved February 10, 2009, from http://www.qsrinternational.com/

Quest Software Inc. (2008). *Single sign-on*. [Online video]. Retrieved October 4, 2009, from http://www.youtube.com/watch?v=ITZjNRG_LOA&feature=related

Robbins, C., & Hamilton, E. (n.d.). *Successfully deploying single sign-on within an outsourced environment*. Retrieved October 2, 2009, from http://www.insight.co.uk/files/whitepapers/Single%20Sign%20on%20 (White%20paper).pdf

Schneier, B. (2005a). *The failure of two-factor authentication*. Retrieved October 2, 2009, from http://www.schneier.com/blog/archives/2005/03/the_failure_of.html

Schneier, B. (2005b). Is two-factor authentication too little, too late? Yes. *Network World, 22*(13), 32-32.

Schwalbe, K. (2007). *Information technology project management* (5th ed.). Boston, MA: Thomson Course Technology.

SearchSecurity.com. (2008). *Enterprise single sign-on: easing the authentication process*. Retrieved October 2, 2009, from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1338507_mem1,00.html?asrc=SS_CLA_299860&psrc=CLT_14

Shaw, J. (2008). *Enterprise single sign-on: The holy grail of computing*. Retrieved September 25, 2009, from http://i.zdnet.com/whitepapers/QuestSoftware_ESSO_HolyGrail.pdf

The Open Group. (2009). *Introduction to single sign-on*. Retrieved October 2, 2009, from http://www.opengroup.org/security/sso/sso_intro.htm

The Strategic Counsel. (2007). *North American enterprise IT users – Security and identity access and management outlook*. Retrieved October 2, 2009, from http://whitepapers.windowsecurity.com/whitepaper1729/

Tiazkun, S. (2009). *Sign of the times*. Retrieved October 2, 2009, from http://www.fedtechmagazine.com/article.asp?item_id=567&sv=related

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington, Massachusetts: Lexington Books.

Uniejewski, J. (2005). Is two-factor authentication too little, too late? No. *Network World, 22*(13), 32-32.

The value of enterprise single sign-on. (2006, March 8). [podcast]. Gartner Voice. Retrieved September 23, 2009, from http://www.gartner.com/it/products/podcasting/asset_145695_2575.jsp

Vance, J. (2006). Guide to Factor/factor. [cover story]. *Network World, 23*(22), 36-38.

Vance, J. (2008). Token resistance. *Network World, 25*(48), 28-32.

Witman, P. D. (2007). Banking regulatory response –The case of strong authentication. Paper presented at the *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, Colorado, August 9-12

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Los Angeles: Sage.

Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of innovation assimilation by firms in different countries: A technology diffusion perspective on e-business. *Management Science, 52*(10).

Biographies

Marise-Marie D'Costa-Alphonso has worked as a software developer and analyst for 9 years. She has experience in various industries with several programming languages developing applications for deployment on desktop, web and mobile phone environments. She has an MBA with a concentration in Information Systems from the University of Southern Queensland. Her research interests include the organisational use of information systems, the alignment of IT and business strategy, mobile and wireless computing and information security.

Dr Michael Lane is a Senior Lecturer and member of the School of Information Systems in the Faculty of Business. He has a PhD in Information Systems from the University of Southern Queensland. Michael's research is concentrated in the area of strategic management of ICT including sustainable use of ICT, the changing role of chief information officer (CIO), information security management, wireless and mobile computing.