Analysis of Open Environment Sign-in Schemes-Privacy Enhanced & Trustworthy Approach

Zubair Ahmad Khattak, Jamalul-Lail Ab Manan*, Suziah Sulaiman
Department of Computer Information Science,
Universiti Teknologi PETRONAS, Tronoh, Malaysia
*Advanced Information Security Cluster, MIMOS Berhad,
Technology Park Malaysia, Kuala Lumpur, Malaysia
(Email: zubair_g00953@utp.edu.my, jamalul.lail@mimos.my, suziah@petronas.com.my)

***Abstract*—The third party based authentication possess users privacy concerns in an open environment such as links and traces user identities across various services. The cryptographic schemes for selective discloser of user information cannot adopt in practices, the common digital signature scheme public key have similar problem. In addition, trustworthy online computing formation is an important advance in security research that aims to use trusted computing remote attestation to overcome trust creation issues. In this paper, we propose a privacy enhanced and trustworthy authentication scheme, with underlying sign-in protocol solution for an open environment that guarantees users' privacy using blind signature scheme to be anonymous and unlinkable during sign-in to the third party service 'Identification Service Provider' (ISP). In our proposed approach, the relying party platforms should verify the integrity of ISP at user platform before redirecting the user to the Identity Service Provider (IdSP), and user system must verify the integrity of relying party platform before delivering a user identifier. Our solution is based on blind digital signature scheme to achieve our first goal, i.e. user anonymity and unlinkability at ISP. The Trusted Computing Group (TCG) hardware root-of-trust establishes trust between interacting platforms within Open Environment to achieve our second goal, i.e. measuring integrity of relying party platforms.**

***Index Terms*—Privacy, Single-sign-on, Platform attestation, Trust, Open environment, credential system**

I. INTRODUCTION

Today's Internet is a primary source for end users to login with owned credential to access many web sites. This approach is highly inconvenient and insecure, as demonstrated by the recent survey results that appeared in [1] which show that 40% of respondents are reusing the same password for multiple accounts. It is apparent that if an intruder were to have illegal access to one protected account, then it is quite possible to reuse that same password for other machines and applications. Therefore, to overcome the web login issues such as phishing attacks, password fatigue, multiple re-entering of passwords, as well as helping in reducing IT costs, computing designers are motivated to create web single sign-on (SSO) schemes. The entities involved in SSO model are identity service provider (IdSP) that have single login for all users, relying parties (RP) that are located random sites and delegates the login to identity provider. It is the role of an identity provider to authenticate and attest user identity before asserting to RP.

Some single sign-on proposals, such as Shibboleth, Windows Live ID, Facebook Connect, rely on centralized model where identity information are stored centrally and only attributes are sent to Service Providers (SPs) or Relying Parties (RPs). Others single sign-on systems, such as Liberty Alliance, WS-Federation, and OpenID, allows the identity information to be distributed and federated in such a way that the authentication process is done at any identity provider within the circle of trust (only in Liberty Alliance) [2]. However, in OpenID trust relationship like CoT is missing [3] and move trust from application level to social level [4], and hence in order to trust another person, a user must verify the person really who he claims to be [3]. Each approach is used for specific purpose such as, Shibboleth which targets academic resource sharing, whereas Liberty Alliance and WS-Federation focus on business interactions [2]. While others large email providers such as Google, Yahoo, AOL, Microsoft all adopt OpenID approach [5] [6] [7] [8] [9].

While in web single sign-on systems like OpenID, Liberty Alliance, Card Space, and Windows Live ID have the advantage of a more efficient login, they also create some serious risk to user privacy. The nucleus of the problem in both centralized and federated login is that all users that log-in to relying party web site must also flow through the identity provider. Hence, Identity Service Provider (IdSP) can easily gather user information such as linking of various websites that the user visits, track user's activities such as his/her buying habits and transaction history without the permission of the user. The data leakage reports presented in [10] [11], showed that lost of personal data in open network can bring

Zubair Ahmad Khattak is a PhD Student, Department of Computer and Information Science at Universiti Teknologi PETRONAS, Tronoh, Perak, Malaysia.
Jamalul-Lail Ab Manan is a Principal Researcher at Advanced Information Security Cluster at MIMOS Berhad, Technology Park Malaysia, Kuala Lumpur, Malaysia.
Suziah Sulaiman is a Lecturer at Department of Computer and Information Science at Universiti Teknologi PETRONAS, Tronoh, Perak, Malaysia.
(E-mail:zubair_g00953@utp.edu.my, jamalul.lail@mimos.my, suziah@petronas.com.my)
(work in progress)

doi:10.4304/jait.2.2.109-121

disaster to whom it belongs, and whoever holds the data (IdSP). The main privacy concerns mentioned in [12] are personal information collection without user awareness, personal information are being shared between businesses without user consent, using of personal information for purposes other than those stated, and failure to access, change or delete personal information after use. The survey conducted by Pew Internet & American Life Project in 2000 found that 54% of Internet users think that web site tracking of users is destructive to user privacy [13].

In web-based single sign-on, there is no way for a user to disclose his/her certain properties selectively that includes age, gender, date of birth, etc to the relying parties or service providers. Therefore, to provide a desired level of anonymity, users need to establish different identifier, called anonyms. For this purpose, computing designers have developed a number of anonymous credential systems or cryptographic schemes [14] [15] [16] [17] that support unlinkability. However, they are not yet fully adopted in practice [18].

In distributed true SSO schemes [19], without third party or minimize the control of third party, users and SPs have to trust the Authentication Service (AS) that controls, and provides the authentication service to the end users. Nearly all other schemes like Liberty Alliance, Microsoft Passport, and OpenID rely on external trusted party that provide and control Authentication Service (AS) or Identity Service Provider (IdSP). These third-party-based authentication schemes raise a number of user privacy and trust concerns presented in our previous work [20] [21] [22]. Therefore, to build a true SSO scheme without or that minimize the control of trusted third party would limit the user and SP required to have in it [23]. The TCG-conformant platform [24] addressed it using the integrity challenge/response message exchange that the SPs verify the AS's integrity and assess it trustworthiness [23]. In this approach, the owner (IT administrator/ user) of Trusted Platform activates and generates Trusted Platform Module (TPM) identities that resemble to SSO identities for each user of Trusted Platform. These SSO identities are then used for authentication purposes.

In most of open environment schemes, user privacy is a big issue, such as Kerberos, Liberty Alliance, Windows Live ID, and OpenID. The identity provider that manages and controls user identities can know who is connecting, and accessing different services. We present the details of such issues in our previous work [22]. As stated in our paper, the most serious problem is user anonymity, and unlinkability at Authentication Service Provider (ASP), and the lack of platform trust between user, identity provider/ authentication service, and service providers.

In this paper, our contribution is designing of a privacy enhanced and trustworthy sign-in scheme, and underlying sign-in protocol between participating entities for instance a user system, and a relying party system. Our scheme is appropriate for an open environment where user privacy protection & trust establishment between interacting platforms is high in demand. The objective of the underlying protocol to achieve following goals

- **User anonymity, and unlinkability at ISP (ISP)** - We use blind signatures [26] scheme that can be a part of blind signature service adopted from [18] to generate an access token. The access token consist of a user selected anonymous name & a secret value. This access token can use ISP that may be a continuous third party running service without forcing the user to reveal his/her identity. In our work we adopt the most popular OpenID flow in our protocol, as compared to the scheme described in [23] based on Liberty Alliance like flow.
- **Measuring integrity of relying party platforms** - we make use of TCG- attestation mechanism, between user platform and relying party platform both embed TPM [25]. The attestation mechanism must make sure that both systems maintain correct software and platform integrity measurement according to the TCG-conformant specification. The relying party, in our design, must first verify the integrity of an ISP and browser at the user platform before redirecting the user to the ISP for authentication assertion. Similarly, the user platform must first verify the integrity of a relying party platform requester of the user identification integrity before sending the user identifier to the RP. The Corroboration Service (CS) entity plays a role of a challenger and user platform & RP platform as target platforms. The CS will assess the integrity of both user and RP platforms. The TPM at user platform & RP platform will protect the respective software's integrity measurement from software-based attacks.

The remainder of the paper is organized as follows. In Section 2 we present a motivating scenario along with a brief problem description. In Section 3 we present our privacy enhanced and trustworthy sign-in model, a scenario, its assumptions, and related properties. In Section 4, we present a four-stage protocol one for generating user access token and another for attestation. Section 5 presents a related work and comparison of our proposed scheme with other related schemes. Finally, Section 6 concludes the paper.

II. A Motivating Scenario and Problem Description

A. Motivating Scenario

Our main motivation example is medical one. Consider a real world healthcare system that have multiple components such as doctors (hospitals) that diagnose and treat patients, pharmacy who provide doctors prescribed medicines, laboratories that conduct X-ray, HIV test, etc. We assume that to access all these services each patient present his/her Social Security Number (SSN) or Identification Card (IC) to the stamp issuing authority and get in return a slip containing an approval stamp. The

patient can present this slip to any service without showing his SSN or IC again. Here each service provider will first verify the issuing authority stamp, and if successful it will provide the respective healthcare service.

However, in open environment (Internet) users may want to have access to any of the geographically dispersed healthcare services. The user authentication (identification) to online resources would normally be based on a traditional username & password to access multiple services via single sign-on. In the single sign-on system (SSO), a user relies on identity service provider (IdSP) of his domain for instance Healthcare Department A for authentication & ISP assert the authentication result if successful to the SP. In order to protect user privacy, the ISP must perform user authentication without collecting any of the user personal information. In SSO Service Provider (SP) must trust ISP that it will assert a correct user identity. This makes it trivial for an ISP to know the user (patient) history, such as all the services he/ she logs into. The presence of honest (retentive) or dishonest ISP & SP may reveal or impersonate patient confidential data and hence raise security and privacy breach. One can see in this example that the existing healthcare system has a major weakness that allows the disclosure of user information that may be extremely private in nature to a third party or attacker. Another scenario of security and privacy breach such as banking can also be possible.

To eliminate these weaknesses three goals must be met: a) anonymity of the user (patient) at IdSP, b) unlinkability between user and his/her data (if an attacker obtains an access logs from IdSP), and c) trust establishment between these three parties such as user, identity provider, and service provider. These weaknesses pose major concerns regarding user data privacy in some scenarios such as banking, healthcare, and defense.

B. Problem Description

Today's digitally connected world especially in open environment privacy protection and user Personal Identifying Information (PII) is becoming more important then ever before [45]. Nearly in all SSO schemes, the ISP knows all users by their identifiers. These identifiers can hold various forms such as e-mail address, names, and random number etc. The user privacy concerns can rises if authentication service/identity provider has full access or hold user sensitive information such as all anonym, SP-association, and colluding SPs that may correlate distinct identities of the same user without his/ her consent. For example of such issue raised is the OpenID IdSP that is adopted by mail services providers such as yahoo, Google etc. to authenticate users. In this particular case, after authentication, they redirect back to the relying party. These providers can trace what the users have been accessing, and so no anonymity is guaranteed. In addition, external attacker can also illegally obtain access logs from IdSP.

In SSO schemes both user and SP or RP trust the AS/IdSP. In both honest and dishonest cases AS/IdSP can impersonate any registered users at every SP. This limitation exists in most of SSO schemes and it will be discussed later in this section. In this scenario described above, users and SPs or RPs have to trust the AS/IdSP.

The taxonomy of SSO given in [19] identified four main SSO categories:

- local pseudo SSO
- proxy-based pseudo SSO
- local true SSO
- Proxy-based true SSO

For more details about other SSO taxonomy, interested readers can refer to [19]. In true SSO user authenticates to Authentication Service (AS) once. In true SSO, all other SSO schemes had a limitation, have the advantage that user does not trust an entity that is under external control [19]. The trust relationship in [23] is unidirectional that the SP can only verify the client, embedded with TPM, platform and software's integrity via integrity challenge/ response. The client is lacking to assess SPs platform integrity. The local true SSO scheme which is based on trusted platform as given in [23] can illegally compromise the user privacy as the AS has access to the user sensitive information such as all anonyms, SP-associations, and login times, etc. In addition, there is a lack of mutual trust between client and SP, and system complexity is very high. Therefore, it is unimportant for an AS or IdSP to know all the web site a user logs into and hence, leads to privacy compromise being left unchecked.

The existing SSO schemes are mostly either open environment or closed environment. Some examples of open environment schemes are Kerberos, Liberty Alliance, OpenID, and Windows Live ID [22]. In open environment, privacy protection is becoming more important [45]. For instance, SSO identities contains Personal Identifying Information (PII), which correlates distinct identities of same user by colluding SPs without the user consent, this can aggregate respective user information in a single profile. Therefore a mechanism must be adopt that should guarantee user identity privacy of the SSO identity anonym; which means that the identity does not contain any PII. The user privacy issue in above open environment SSO schemes can be affected as explained below.

- In Liberty Alliance [30] [31] unlinkability of user identifiers can be affected in various ways such as identity service providers (IdSP) may know all user identifiers, SPs may collude with ISP to link user anonym, and profiling (individual SPs may maintain user information for instance telephone numbers, shopping habits, credit card numbers). In [32] [33], it was demonstrated that a man-in-the-middle attack against the Liberty-enabled client and proxy profile; whereby a dishonest service provider could interpose itself between a principal (user) and an honest service provider.
- The Kerberos [28] [29] protocol compromise may affect user privacy such as user accounts linking to user network address and identifier, replay attacks is still possible (the users tickets can be copied or captured via sniffing and

replayed later), and it is also ineffective against password guessing attacks (such as poor password).

- The user privacy at OpenID IdSP can be at risk because the identity provider performs user authentication task on the request of relying party. Therefore, identity provider can still trace all user activities such as which services has been accessed. This identity provider can be either honest or dishonest. In the case of honest, the provider can be compromised and logs can be leaked to an attacker [18]. The OpenID is also vulnerable to pushing attacks, such as mentioned in [36]. In OpenID, man-in-the-middle [37], the connection negotiated over Diffie-Hellman (DH) [38] is subjected to interception attacks. The main reason is that in Diffie-Hellman (DH) association session, the user of ephemeral-ephemeral Diffie-Hellman (DH) without built-in authentication is non-conformant with the referenced RFC 2631 [39]. Therefore, it introduces a serious risk of Identity Provider (IdP) Masquerade [40]. Also in OpenID system, the Relying Parties (RP) does not provide any checking mechanism for nonce's and is not protect against reply attacks.
- In [43], Windows Live ID phishing attack was identified, the quote "The phishing attacks last week on Hotmail were actually compromising Microsoft Live ID accounts. These credentials give a user access to multiple services including Hotmail, Messenger, Xbox Live, Office Online and Skydrive, and Bing". Another attack, in which Microsoft identification Service was partly down for one hour that appeared in [44] affected user accounts privacy using mobile-phone Web browser. This attack affected Microsoft Windows Live ID systems, in which limited numbers of customers were able to access other user accounts.

All existing SSO schemes rely on third party that provides & controls AS [22] that can affects user privacy-as described above. In our design, this is achieved with trusted ISP that interacts with Blind Token Generating Service (BTGS). The BTGS generates user access tokens. The ISP asserts user identifier to RP. The trustworthiness between user & RP platforms is achieved via TCG remote attestation mechanism [47]. The attestation mechanism enables both parties to assess each other's trustworthiness before any further interaction can commence.

In next section, we provide a detail overview of our proposed privacy enhanced & trustworthy sign-in scheme for open environment.

III. Proposed Model, Scenario, Assumptions and Properties

In this section, we present actors that play different roles in our scheme as shown in Fig. 1, which have their own pertinent goals. We will describe the attack model (attack scenario), the related assumptions and information flow in our proposed scheme.

In our model, ISP may have no interest to link a particular user's identity during sign–in to the relying party. We assume a continuous running service, ISP belongs to a third party that limits the amount of trust that the user and RPs are required to have in it [23], running on the user platform as a service. Further, we also assume that user possess a credential (username, password) with BTGS. On verification with BTGS, if access token is valid, the ISP will return an identifier to the relying party. Our approach adopts informal security properties proposed in [18] such as One-wayness, consistency, and unlinkability.

The trust between user system and relying party is established through TCG-attestation mechanism. Attestation is a mechanism in which platform (client) that needs to be verified to provide its integrity report to remote verifier (server). This mechanism can counter software-based attacks such as man-in-the-middle, and replay attacks and many more.

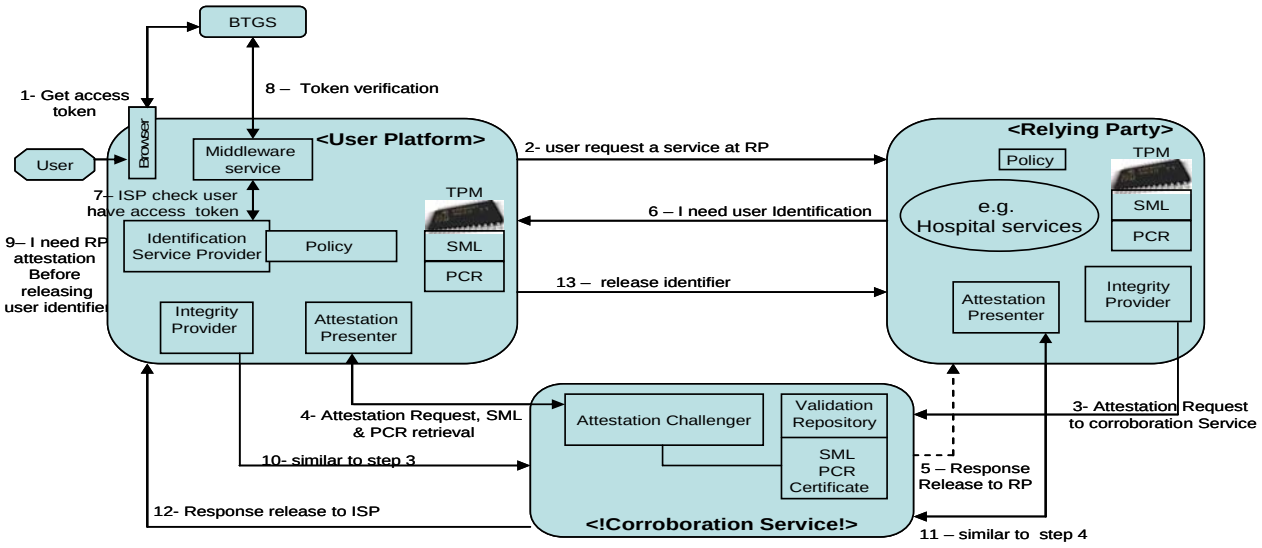

Figure 1. Privacy enhanced and trustworthy sign-in system design for open environment

The main entities involved in our model include user, blind token generating service, ISP, CS, RP, & IM components see Fig. 1 above.

A. User

The user (u) has an account with the token service. In our model, this token may be a persistent identity such as an e-mail address. We assume that during setup phase the user logs on to the token service using a common authentication approach, for instance, username and password via a browser. In our proposal, both platforms (user system and relying party) must be embedded with a TPM, which is used by the system to assure the validity of the integrity measurement for each executable that is loaded into the OS runtime. Therefore, with this mechanism, remote parties will be assured of the authenticity of the integrity measurement from the time of system booting.

B. Blind Token Generating Service

Blind token generator is a service that generates blind access tokens using blind signature service. These tokens are exchanged with ISP during token verification from BGTS. The ISP next computes one-way collision resistant function 'F' on its value and return as a part of identifier to RP, for instance $Token = (pseudo, F(T))$.

C. Identification Service Provider

The ISP relies on blind signed tokens and it authenticates the users without forcing them to reveal their identity. This is to ensure that when the user sends a request to the relying party, the Relying Party (RP) does not have any knowledge about the user identity. Therefore, RP must first verify the trustworthiness of user platform, and if the integrity measurement result is successful then only the RP will be able to send a request for user identification.

The ISP at user system contacts blind token generating service via middleware service in which ISP checks weather the user has an access token which is signed by blind signer. We assume the ISP verifies the signature on the access token privately by sending it to the blind token generating service. The ISP gets yes or no response from blind token service via middleware. It is important for ISP to send the user identifier to the RP; it must first assess the integrity of the RP. If attestation is successful, the ISP at client forwards the user identifier to the RP.

D. Corroboration Service

The corroboration service is a special entity that performs attestation on behalf of the user system and RP. The corroboration service may either be a part of a user system and RP or as an independent entity.

E. Relying Party

Relying party is an entity that may provides different services (hospital, banking) to the users. It receives user identifiers from ISP at user platform. However, it is important that before redirecting user to the ISP for user identification, the RP must first verify the user platform integrity.

F. Attestation Components

The user system and relying party contains number of attestation components such as integrity provider, attestation policy formation, attestation presentation, SML attester, and PCR attester. The CS consists of attestation challenger, SML validation, PCR validation, Certificate Validation.

The integrity provider in both user system and relying party interacts with corroboration service to request user system or relying party platform attestation. The attestation challenger at CS asks from attestation presenter at user platform or RP platform, and obtains their stored SML and Platform Configuration Register (PCR) values from user system or relying party. After getting those values are then compared with stored values at CS database. The certification validation performs TPM signature verification to ensure genuine TPM signature exist on received quote from the user system or relying party.

The policy at user system can use ISP. According to the policy, ISP first must verify the integrity of relying party platform before forwarding the user identifier on successful attestation results.

G. Attack Model

In our proposed protocol in next section IV, we assume that there is no physical attack on the embedded TPM at the user (client) and RP (server) systems. Therefore, we consider only the software-based attacks such as man-in-the-middle, replay attack, and sensitive information collection (user anonymous name linking). The attacker could be a third party ($Adversary$), intruder, honest or dishonest ISP.

H. Scenario

Let us suppose a patient (P) goes to a healthcare services provider (HSP). In this case, P plays the role of user (u), and we also have the service provider (SP).

If u visits the healthcare services provider first time for physical examination by medical staff, he must register within the healthcare system and it is then stored in the system database. Then u goes to the healthcare centre for the first time he needs medical care. He shows his passport/ Identification Card (IC) and the healthcare registration authority, on successful registration issues a typical credential such as username and password. In all the other cases u authenticates and communicates with his doctor via the healthcare application on a web browser, transmits and receives data in real time, or to fix appointments. However, in this paper our focus on user safe authentication to the healthcare system.

All communications between the u system (client) and RP (service) are performed via the internet browser. Beyond the browser, both the user system (uS) and RP (service) are out of each other controls. Consequently, the uS and RP platform, integrity can be affected, and communication channel can become vulnerable to adversary attacks in open environment.

I. Assumptions

Our proposal is based on the following assumptions:

- The third party services, such as BTGS and Identification services (IS) are fully trusted by the user. Particularly, it allows users to be anonymous at Identification Service (IS) and it cannot link user anonymous names to any kind of user data, so no user information is revealed. The integrity of browser and ISP is protected with trusted computing integrity measurement process. The Integrity measurement, [48], is like a chain process whereby a first component needs to measure second component before it can be trusted and the second component then measures a third component until the last component, after which the platform can be considered trusted.
- Each user platform (client) and RP (server) equipped with a TPM, after successful and compliant integrity measurement process are trusted platforms [49]. TPM serves as a root of trust for authenticating a host's software's configuration and provides protection to data by never releasing a root-key outside its boundaries. Moreover, a set of PCRs facilitate to measure the characteristics and properties of the platform environment such as system configuration, integrity, and executing states. Therefore, we assume both user and RP platforms holds correct configuration of its applications and platform states.
- We assume that the TPM works correctly and its operation is not manipulated using physical attacks, for instance, removing it from the user (client) or RP platforms.
- The user identity is unlinkable; we assume that the tokens are privately verified with BTGS without revealing user identity. Further, when user has a token and wants to access a service the derived identifier must not be delivered to RP before successful platform attestation of the RP. If attacker were to impersonate user and tries to access the token, it will be useless because the attacker cannot have access to the applications unless the attacker can present to RP the integrity measurement values stored in the user PCRs, which is not possible.

J. Information flow in Proposed Model

- In step 1, the user visit blind signature signer and sign-in using existing account. Next, the user selects an anonymous name that he/she wants to use on RP and a secret value (sv). The user first blind the token $\mathbb{B}(\top)$ using blind function ($\mathbb{B}$) and sent it to signer ($\leq$) for signing, without the signer knowing its content. Lastly, user unblinds the token $\leq(\top)$ using unblind function ($\mathbb{B}^{-1}$) containing user anonymous name and $\leq\vee$.
- In step 2, user sends a service request to RP.
- The RP requires user identifier, for this RP to trust ISP. However, before redirecting the user to ISP, the SP requires integrity measurement of ISP at user platform (step-3). The component-INYI at RP sends attestation request to $\subset\leq$. The above request includes target platform information, and attestation type (binary-based attestation). We assume that $\subset\leq$ implements Integrity Measurement Architecture (IMA) [55] but it can be replaced by any kind of remote attestation techniques in future.
- In step- 4, the attestation challenger at CS sends an attestation request to the attestation presenter at client platform. This request includes a nonce. The attestation presenter uses Stored Measurement Log (SML) and PCR will retrieve stored measurement log & PCR quote from the TPM. These retrieved values are sent back to the attestation challenger at CS (step- 4). Here the hashes received from SML are validated against known good hashes in validation repository. The value of PCR quote is checked against the PCR value computed from hashes in SML. This will assures the particular TPM which signed this PCR quote and that the quote is reliable (vouches) for the authenticity of the SML. The nonces in quoted values assured because replay attacks are not possible. Next, certification validation will verify the signature to make sure that a genuine TPM hardware had signed the quote. If all verifications are successful, the attestation challenger generates a response whether attestation of the target (client) is successful or failed.
- In step-5, if all checks are successful the attestation challenger at CS generates a response whether attestation of the target (client) is successful or failed and sends it to RP.
- In step-6, in case of successful attestation response, the RP will send a request for user identifier.
- In step-7 and 8 ISP on user platform, check whether user has access token and verify it from BTGS that it signed it or not. The response is send back to ISP whether it is yes/ no.
- The policy attestation, specify on client side that the attestation of the RP must performed before releasing the user identifier (step-9).
- In step-10, the component-INYI at client will request CS for measuring RP integrity. The step (11) follows the same sequence and procedure to measure RP integrity as in step (4).
- In step-12, the attestation response is forwarded to user system. Based on attestation result in step-13, the user identifier will either release or not to the RP.

K. Properties of Proposed scheme

- Our proposed scheme protects user privacy via anonymous name and secret value bundled in

access token (T = (anonym, s.v)). The ISP (third party service) cannot know who holds the access token, and cannot link to the real user identity. To recognize whether the user has access token, the ISP privately or publically can verify the signature from BTGS. Therefore, this will achieve our first goal of having user anonymity and unlinkability at ISP. In our architecture authentication is performed using software tokens created via BTGS. Other forms of authentication such as smartcard, mobile phone, and OTPs can also be used.

- Our proposed scheme can verify the trustworthiness' of user system & relying party via attestation mechanism. This attestation actually confirms, firstly, the authenticity of the user system, which runs ISP service to the relying party, and then redirecting it to ISP to request for user authentication. Secondly, the authenticity of the relying party platform to the user system, before releasing the user identifier through corroboration service. The attestation mechanism can be affective against attacks such as man-in-the-middle, pharming, replay, fake software. Through attestation mechanism, we achieve our second goal that both platforms integrity is in safe state.
- Our proposed scheme can support user mobility in a setting where every user system and relying party is trusted (attested and verified).
- In our scheme, the user and RP must trust the corroboration service; that it will verify the trustworthiness of the user system or relying party platform & software integrity.
- Our approach is also suited for open environment such as Internet where user privacy is more important to be protected compared to closed environment. Some of open environment schemes we be discussed in Section II and V.
- Our approach can adopt any attestation mechanism such as binary-attestation or property based attestation.
- The usability or ease of use of the proposed scheme is simple, such that the user does not need to carry any hardware token such as smart card or to remember many passwords. The user need only remember his/her account access information (email and password). If user successfully gets an access token from BGTS then the user does not need to enter account information again for other services. The user system hardware and software integrity is protected against attacks, every time user request a service the attestation mechanism will automatically be performed first without any user intervention.

IV. PROTOCOL

Our proposed protocol is based on four-step process that establish a user anonym, identifier, and trusted interaction between an ISP (part of user system) and a Relying Party (RP). The three important aspects of our protocol is the user anonymity and unlinkability at ISP, & trust establishment between user system & RP that enable both parties to assess each other's trustworthiness before requesting or sending user identification. (See Fig. 2 for details)

A. Setup Phase

In this step user signs in to blind signer using an existing account. The blind signer can be online or offline. After successful sign-in user will select a anonymous name and secret value. The user uses the anonymous name on the relying party. Next, the user will prepare a token $\{T = \{anonym, secret\ value\}\}$ and bundled it together with an access token. The user first blinds the token $B(T)$ and it will help to prevent the signer from being able to link user with his/her anonym. This access token will sign by blind signer. The blind signer will use 'blind signature scheme [26]' to sign $B(T)$ but with the assurance that the signer will not know its content. The result '$S(B(T))$'is returned to the user. The user will than use unblind function 'B^{-1}' to unblind the signed token '$B^{-1}(S(B(T))) = S(T)$'. The resulting '$S(T)$' that contains user selected anonymous name and a secret value.

B. Relying Party Identification and Attestation Request

To access service (S) at the Relying Party (RP), the user (U) will send a request to RP. Before redirecting the user to ISP for identification, the RP first checks for the integrity of user system.

The integrity provider at relying party sends an attestation request to corroboration service which includes target platform (user system) information, and attestation type (binary attestation). On receiving the request, the attestation challenger at CS sends an attestation request, which includes a nonce, to the attestation presenter at the UP. The attestation presenter uses SML, and PCR to retrieve Stored Measurement Log (SML) and PCR quote from the TPM. The retrieved SML, and PCR quote then are sent back to the attestation challenger at CS. At corroboration service, hashes of the received SML are validated against the good hashes in repository; quote value of PCR is checked against PCR value computed from hashes in SML, and nonce checking. This later check will give assurance that the PCR quote has been signed.

The validation of the certification guarantees that it has been signed by the genuine TPM and the TPM signature to guarantees the quote has been genuinely signed using its private key.

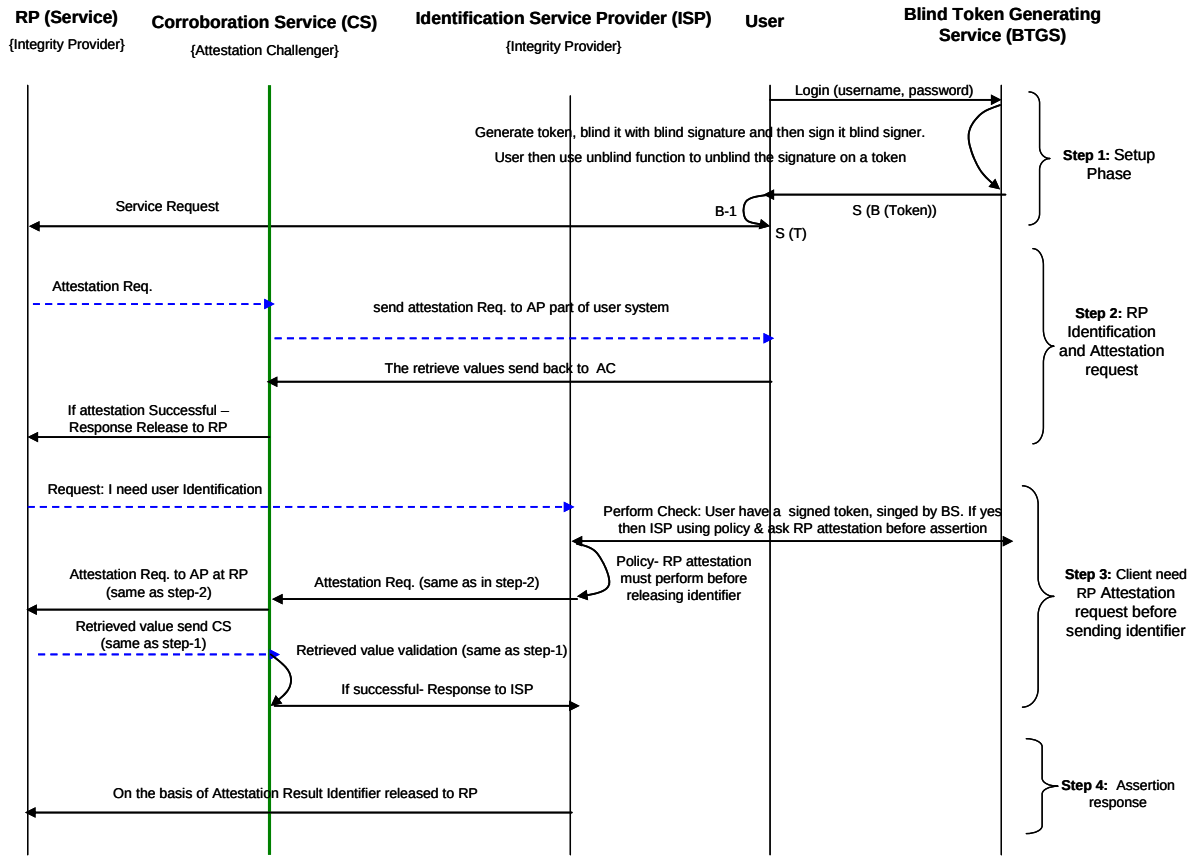

Figure 2. Underlying sing-in protocol between user, ISP and relying party

If all above checks are successful, the attestation challenger at CS produces a successful or failed response for the attestation of target platform (user system). The respective response is then released to the RP based on attestation result.

C. Client Attestation Request

The attestation challenger at CS generates response whether it is successful or fails. This response is then released to the RP, based on the attestation results the RP will then requests the ISP at client for user identification. The ISP communicates with BTGS via middleware residing at the user platform. The ISP checks whether the user has access token that has been signed by the blind signer and checks whether it is signed or not. The attestation policy at client must specify that the RP attestation must be performed before sending the user identifier.

The integrity provider part of user system sends a request (attestation) to validate service. The attestation request includes target platform (RP) information, and attestation type (binary attestation). On receiving the request, the attestation challenger at CS sends an attestation request, which includes a nonce, to the attestation presenter at the RP. The attestation presenter uses SML, and PCR to retrieve Stored Measurement Log (SML) and PCR quote from the TPM. These retrieved SML, and PCR quote are then sent back to the attestation challenger at CS. At corroboration service, hashes of received SML are validated against the good hashes in repository, quote value of PCR are checked against PCR value computed from hashes in SML, nonce & checking. The later check gives assurance that particular PCR quote has been signed. The certification validation confirm TPM signature to guarantee that the quote has been genuinely signed.

If all above checks are successful, the attestation challenger produces a response containing attestation of target platform (RP) whether it is successful or fail. This response is then released to ISP at user system. Based on this attestation response the user identifier is either released or stopped.

D. Assertion Response

The assertion response is a response based on attestation result obtained in step-3 (see Fig. 2). The ISP will compute one- way collision-resistant function (F) on sv such as $(anonym, F(T))$ and return that as part of identifier. The attacker cannot manipulate the value of $F(T)$ to obtain T. If attestation result is successful then the user identifier is released to RP.

V. Related Work

In this section, we explore most popular open environment SSO schemes initiative, credential systems and Trusted Computing (TC).

In corporate world, there are several emerging standards for open environment and the one that are most known is Liberty Alliance (LA) [30] [31] based on SAML which provides open standards for SSO. The Liberty-enabled group which is a part of circle of trust, a

federation of SPs and identity providers having business relationships. In LA the identity provider creates, maintains and manages user identity information and sends this information to the SPs.

Kerberos [28] [29] is trusted third party authentication system based on Needham and Schroeder [58] model. Kerberos works as a Network Authentication Service (NAS) which consists of a set of users, Kerberos Server (KS) that is a combination of an Authentication Server (AS) and Ticket Granting Server (TGS) and Service Providers (SPs).

Shibboleth [59] is an initiative from universities that are member of Internet2. The main goal of such initiative is for the development and deployment of new middleware technologies that facilitates inter institutional collaboration and access to digital contents. Shibboleth is build on federation concept of user attributes. When user at institute A want to access a resource at institute B, Shibboleth enables seamless access when it sends user attributes to the remote destination instead of the user having to log into institute B. The institute B can check whether the attributes of user A satisfy it policies.

OpenID [34] [35] is a URL-based identity management implementation. To login to a site that supports OpenID, the user enters his/her OpenID URI and redirects him/ her to identity provider. The identity provider authenticates the user via authentication system in placed such as passwords, smartcard, biometric and after successful assertion; the user returns back to the relying party and allow the user to use the site under claimed identifier.

Windows Live ID [41] is a single sign-on service that is developed by Microsoft to allow the end users to logon into many Microsoft websites services, using a single username and password, such as Hotmail, MSNBS, MSN, Xbox 360 xbox Live, .Net Messenger Service, Zune or MSN subscriptions and many more. Readers could refer to [42] for reference, on how the user authentication is performed in Windows Live ID.

Every subject, typically human user, in real world has some kind of credentials to use on Internet. The system that enables users to prove the possession of attributes to interested parties such as verifiers to verify whether or not user possesses attributes of interests is called credential system. A typical credential system is the infrastructure and set of procedures by which the players are interacting.

The one well known conventional digital credential system is Public Key Infrastructure (PKI) [50]. In PKI scheme, credentials are public key certificates that binds user attributes (name, public key, issue date, and expire date, etc. The two parties involved are credential issuer, certificate issuer (CA), and credential verifiers, relying parties. In PKI, user privacy can be compromised because the issuers (CA) and verifiers (RP) can identify any user using system-wide identifier. Therefore, in this way the issuer and verifier combines their knowledge about the behavior of the user and can construct individual transaction histories for all users by the correlation of issuing and showing of credentials using these identifiers.

To overcome the above issues, anonymous credentials or anonymous name systems were proposed, both of terms used interchangeably such as [16] [17] prefer the previous and others prefer the later [53] [46]. In some application for instance electronic cash, healthcare and airline ticketing systems the user privacy is important and desirable to prevent issuers and verifiers being able to associate user identifiers such as user name. Therefore, anonymous credential system avoids the disclosure of user identifier to the issuer and verifier. In addition, the credential systems that support anonymous name unlinkability is known as anonymous name systems.

One of the first anonymous credential systems was proposed by Chen in 1995 [53] that offer levels of efficiency required by practical applications. His scheme still suffers from that a third party involvement in user's registration phases. The user in Chen scheme obtains several signatures from the issuing organization. The purpose of obtaining several signatures to be able to use a credential several times, while at the same time maintaining unlinkability of the credentials. This may have several practical implications on the resource.

Damgard [61] proposed another scheme based on general complexity theoretic primitives such as one-way & zero-knowledge proofs. Therefore, this scheme would not be practically applicable. Similarly the scheme 'general credential system' proposed by Lysyanskaya, Rivest, Sahai, and Wolf [46] captures many desirable properties. However, their scheme also unable to make use in practice because based on a one-way function & general zero-knowledge proofs.

Brand's [62] proposed certificate-based system in which users can selectively disclose the attributes of their credentials. The main practical problem with this scheme that, all issuers have to agree on a universal set of security relevant parameters, which in practice may not be easy to get. However, in both Brand's and Chin's schemes if users intend to show credentials multiples of times without the danger of being linked to each other, users must obtain multiple copies of a credentials.

In addition to the above other anonymous credential systems [14] [15] [16] [17] [51] [52] [54] found in literature have not yet adopted in daily practice [18].

Diffie and Hellman [63] proposed a scheme that is composed of a private signing function (Pvt-SF) known only to the signer and public verifying predicate (Pub-VP) that is known to the verifier to verify signature on a message (M) for instance $Pub\text{-}VP\ (M, Pvt\text{-}SF\ (M)) = True/\ False$. The drawback of the scheme is that it makes it impossible to generate a signature (SF) on message (M) without the knowledge of signing function SF.

To solve the above problem Chaum [26] proposed a scheme known as blind signature system. His proposed scheme can be implementable in practice as shown by Dey and Weis [18]. The blind signature scheme [26] enhance the traditional scheme such as one given in [63] with blinded function (BF) and unblinded function (BF^{-1}). In this scheme only a user who is getting a message which is signed knows the blinded and unblinded

functions. The signer cannot know the content of the blinded message during signing process.

Trusted Computing Group (TCG) [56] introduced Trusted Computing (TC) is a special computing model that brings trust in computer platforms. This trust achieved actually through a hardware chip called TPM [57], and can perform a number of functionalities. The most important of them is that it can securely store information that will provide root-of-trust. The TPM has a number of shielded locations that are used to store platform configuration known as Platform Configuration Registers (PCRs). These PCR can store cryptographic hashes of the software which is loaded to be executed. The PCRs can only control by a mechanism called *PCR-extend* to add-in new hashes. Currently it support only SHA-1 algorithm for computing the hashes. The most prominent feature of SHA-1 is 'irreversibility' that once a hash has been stored on PCR it cannot be removed or altered by any software loaded after PCR-extend function execution. The hashes in PCR are then used to report platform configuration to the challenging party to establish a trust.

The above process known as remote attestation that enables a remote party 'Corroboration Service (CS)' to confirm the integrity of a remote platform via "trust coins" which is submitted by the TPM on the target platform.

The one of most mature techniques is Integrity Measurement Architecture (IMA) [55]. The workflow of IMA is as follows. When the kernel loads an executable it is the IMA that computes binary hash of the executable and stores this hash into a Stored Measurement Log (SML). Next IMA will use the *PCR-extended* function to aggregate the hashes of each executable loaded into a single PCR value. The IMA will use PCR {no.10} to store aggregate of all the measurement taken. For instance, if IMA measure j number of executable such as m[1], m[j2], m[j3],….,m[j] then the PCR {no.10} will contain the following aggregate SHA1 ...SHA1{SHA1{SHA1(0||m[1])||m[2]}||m[3]}...||m[j].

The TPM can only be manipulated in two ways as specified in [57]: firstly, when the system is rebooted it resets all PCR values and secondly by performing the *PCR-extend* operation. Therefore, in case where if a malicious attack successfully changes the SML but it will not be able to change the PCR values provided that the TPM complies with TCG specification.

The privacy enhanced federated login scheme presented in [18], is based on a third party (IdP), that achieve user authentication with anonymity and unlinkability. In this scheme the user privacy is still at risk, trusting its identity providers, if the identity provider gets malicious. As a result, it will raise large concerns such as the providers impersonating them to the relying parties [18]. The author proposed PseudoID is based on three main properties such as one-wayness, consistent, and unlinkable login. The one-wayness means when users possess their identities and others cannot use those identities to impersonate them at relying party for instance, username and password.

On other hand consistency means users have identities with a feature 'long-lasting' that enables them to sign-in to the relying party with the same identity several number of times for instance user have a driving license or passport through whole life. The unlinkability makes sure if an attacker obtain access logs from identity provider so attacker will be unable to guess which one is the real user logging in. Therefore practically it is essential for an unlinkable system to have the features of one-wayness and consistent

The scheme proposed by Pashalidis [23], local true SSO scheme, can compromise user privacy as Authentication Service (AS) can have access to the user sensitive information such as all anonyms, SP-associations, and login times, etc. In addition there is also a lack of mutual trust among client, and SP. The SP can verify the AS, running on user platform, integrity by integrity challenge/response. However, user platform is lacks integrity verification process of SP platform and if compromised by a malicious attacker, the user platform will be unable to detect and takes necessary measure.

The Trusted Federated Identity Management System described in [60] combines the strength of FIMS, catering for user privacy and scalability, and remote attestation to measure the client platform integrity. In this design, the IdP plays the role of challenger and client only releases its platform configuration information to its domain IdP. The entity that has a strong trust with his own IdP. The SP relies on IdP to provide the correct user identification and platform integrity information. The client platform is equipped with a TPM which protects integrity measurements of the platform and its application. SP depends on IdP to provide the correct user identifier and integrity measurement.

Table I. give below presents comparison between privacy enabled scheme [18], Trusted Computing (TC) based attestation schemes [23] [60], and our privacy enhance and Trustworthy scheme according to some fundamental criteria.

Three specific criteria dealing with privacy concern addressed in our work are anonymity, unlinkability, and third party presence. The other two criteria dealing with trustworthiness' are attestation and Trusted Platform Module. The underlying sign-in protocol in our proposed scheme supports two-factor user identification see Fig. 2 for detail. During the execution of this protocol user first must have to obtain access token (anonym, secret value) from BTGS. In second step user platform integrity verified by the CS if successful then forward attestation result to the RP platform. Based on the attestation result the RP requests ISP for user identifier.

Further RP integrity will verified via CS if successful then forward attestation result to ISP running as a continuous service on a user platform. Therefore on based of the attestation result the user identifier is either release or terminate. If either platform fails to provide correct integrity measurement the process terminate and user identifier will not released. In addition Trusted Computing (TC) measurement and reporting allows a challenger (Corroboration service) that no malicious

software executing on a target platform for instance user system and relying party in our scheme.

The comparison between some related schemes given in Table I that shows our proposed design fulfills both the user privacy and platform trustworthiness criteria. Other schemes such as those in [23] [60] [18] are lacking in some of the selected fundamental criteria.

In Pashalidis & Mitchell [23] scheme the authentication service that is responsible for user authentication & then forwards the respective user authentication to the SP. The AS in their scheme can link all user anonyms, SP association and log-in times. From privacy perspective, this is not acceptable especially when operating in an open environment. Another disadvantage of this scheme is that the user platform cannot measure the integrity of SP platform. Therefore, SP platform is lacking the ability to assure user that no malicious software is executing on SP platform or will behave as in expected manner. The scheme presented in [60], the IdP cannot provide its platform integrity report to the user platform or SP platform, and SP lacks the ability to prove its platform integrity to IdP. Therefore, in case of dishonest IdP and SP user privacy can be in danger. The question is whether their proposed scheme will be able to protect users privacy related issues mentioned in [64]. The scheme given in [18] did not embed any hardware based security device or chip such as TPM in any of the platform (user platform, IdP, and SP). Therefore, the scheme is completely missed the Trusted Computing (TC) integrity measurement and reporting. Therefore, malicious software execution in this scheme cannot be detected. The Trusted Computing (TC) attestation mechanism implementation can enhance the trustworthy communication between IdP and SP.

TABLE I.
COMPARISON OF PRIVACY PRESERVING & TRUSTWORTHY SCHEMES

Criteria	Pashalidis & Mitchell, 2003[23]	Tanveer, Nauman, Amin, Alam 2010[60]	Arkajit, & Stephen, 2010[18]	Proposed scheme & Protocol
Anonymity (pseudo)	X (AIKs)	X	√ (Blind signature)	√
Unlinkability	X	X	√ (Blind token)	√
Attestation	√ (Client with TPM)	√ (Client with TPM)	X (TPM missing)	√ (Client & RP(Server) with TPM)
Third Party presence	√ (LA, a running process AS)	√ (Shibboleth)	√ (OpenID)	√ (OpenID, a running process ISP)
TPM	√ (User platform only)	√ (User platform only)	X	√ (Client & RP(Server) with TPM)

VI. CONCLUSION

In this paper we present a model for enhancing user privacy (anonymity and unlinkability) at ISPs by using blind signature scheme, and trustworthiness between user and relying party (service) platforms through trusted computing mechanism remote attestation. In this proposal we claim that the ISPs would not able to derive user identity because it fully enforces blind signed token mechanism.

We provide detailed analysis of present SSO schemes and their limitations. The analysis shows that most of current open environment scheme are vulnerable to different kind of attacks such as man-in-the-middle attack, reply attack, IdP or AS gathering user information, and IdP & SP colluding. The comparison of selected work with our proposed scheme shows that most of third party based SSO schemes are having difficulties in achieving privacy and trustworthiness according to our selected fundamental criteria.

A two factor authenticating mechanism is proposed for authenticating users to service (hospital, bank). First user Integrity that is a basic security element incorporated in our model by the introduction of remote attestation of the target platforms. Our approach provides flexibility and can incorporate any new attestation techniques. The work presented in this paper open new research directions as mentioned in Section V.

REFERENCES

[1] S. M. Furnell., P. S. Dowland., H.M. Illingworth and P.L. Reynolds., "Authentication and Supervision: A Survey of User Attitudes, Computer & Security," Elsevier, vol. 19, pp. 529-539, 2000.

[2] U. Fargoso-Rodriguez., M. Laurent-Maknavicius and J. Incera-Dieguez., "Federated identity architectures," Work in progress session, Annual Computer Security Application Conference, 2006.

[3] K. Helenius., "OpenID and identity management in consumer services on the Internet," Seminar on Internetworking, 2009

[4] F. Culloch., "OpenID and SAML", Technical Report, Terena EuroCAMP StockHOLM, www.terena.org/activities/eurocamp/may08/slides/20080508-culloch-openID.pdf, 2008

[5] E.Sachs,Google Code Blog: Google moves towards single sign-on with OpenID,http://google-code-updates.blogspot.com/2008/10/google-moves-towards-single-sign-on.html, 2008.

[6] K. Mackey, Windows Live ID become an OpenID provider, http://arstechnica.com/microsoft/news/2008/10/windows-live-to-become-an-open-id-provider.ars, 2008.

[7] Yahoo! Announces Support for OpenID; Users Able to Access Multiple Internet Sites with Their Yahoo! ID, http://yhoo.client.shareholder.com/ReleaseDetail.cfm?releaseid=287698, 2008

[8] R. Turoczy, Microsoft Windows Live Supports OpenID, http://www.readwriteweb.com/archives/microsoft_windows_live_openid.php, 2008.

[9] G. Fietcher, OpenID 2.0 Provider support live @AOL http://practicalid.blogspot.com/2010/03/openid-20-provider-support-live-aol.html, 2010.

[10] J. Vijayan, "Wells fargo discloses another data breach," Computer World, 2006. http://www.computerworld.com/s/article/9002944/Wells_Fargodisclo _nother_data_breach

[11] R. Lemos, “Reported data leaks reach high in 2007,” Security Focus, 2007. http://www.securityfocus.com/brief/652
[12] M.Alsaleh., C. Adams., "Enhancing consumer privacy in the liberty alliance identity federation and web services frameworks," In Proceedings of the 6th Workshop on Privacy Enhancing Technologies (PET 2006), Cambridge, United Kingdom, 2006
[13] S. Fox et al., "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," The Pew Internet & American Life, 2000.
[14] J. Camenisch., T. GroB., "Efficient attributes for anonymous credentials," In Proceeding of 15th ACM conference on computer and communication security, 2008.
[15] J. Camenisch., S. Hohenberger., and A. Lysyanskaya., “Compact e-cash,” In Proceedings of EUROCRYPT 2005, LNCS 3494, Springer-Verlag, pp. 302–321,2005.
[16] J. Camenisch., and A. Lysyanskaya., “An efficient system for non-transferable anonymous credentials with optional anonymity revocation,” EUROCRYPT 2001, LNCS 2045, pp. 93-118, Springer, 2001
[17] J. Camenisch., and A. Lysyanskaya., “Signature schemes and anonymous credentials from bilinear maps,” In Proceedings of Crypto, LNCS, Vol. 3152, pp. 56-72, 2004
[18] A. Dey., and S. Weis., “PseudoID: Enhancing Privacy in Federated Login,” In Hot Topics in Privacy Enhancing Technologies, 2010, http://research.google.com/pubs/archive/36553.pdf.
[19] A. Pashalidis., and C. Mitchell., “A taxonomy of single sign-on systems”, In Proceeding of Information Security and Privacy, 8th Australasian Conference, ACISP 2003, LNCS 2727,249-264, 2003.
[20] Z. A. Khattak., S. Sulaiman., J. A. Manan,"A study on threat model for federated identities in federated identity management system," In Proceeding of information technology international symposium (ITSim), vol.2, pp. 618-623, 2010.
[21] Z, A. Khattak., J. A. Manan., Suziah, S., “User requirement model for federated identities threats,” In Proceeding of 3rd international conference on Advanced computer theory and engineering, vol.6, pp. 317-321, 2010.
[22] Z. A. Khattak., J. A. Manan., S. Sulaiman., “Trusted Computing based open environment user authentication model,” In Proceeding of 3rd international conference on Advanced computer theory and engineering, vol.6, pp. 487-491, 2010.
[23] A. Pashalidis., C.J.Mitchell., “Single sign on using trusted platform,” In Proceedings of Information Security, 6th International Conference, ISC2003, Bristol, UK, 2003, Volume2851 of Lecture Notes in computer Science, Springer-Verlag, pp54-6, 2003.
[24] Trusted Computing Group, vol.2, 2005. http://www.trustedcomputinggroup.org/files/resource_files/59C26ECB-1D09-3519-AD469EA7AFBD2E91/Best_Practices_Principles_Document_V2_0.pdf
[25] S. Bajikar., “Trusted platform module based security on notebook PCs—white paper,” Technical Report, Mobile Platforms Group Intel Corporation, 2002.
[26] D. Chaum., “Blind Signatures for Untraceable Payments,” In Proceeding of Crypto '82. pp. 199-203, 1982
[27] M. F. Grubb., and R. Carter., “Single sign-on and the system administrator,” In Proceedings of the 12th Systems Administration conference, usenix, 1998
[28] J. G. Steiner., B. C. Neuman., J. I. Schiller., “Kerberos: An authentication service for open network systems,” In Proceeding of winter Usenix conference, pp. 191–201, 1988.
[29] C. Neuman., T. Ts’o., “Kerberos: An authentication service for computer networks,” IEEE Communication, vol. 32, no. 9, pp. 33-38, 1994. http://gost.isi.edu/publications/kerberos-neuman-tso.html
[30] Liberty Alliance, Introduction to the liberty alliance identity architecture, revision 1.0, 2003. http://xml.coverpages.org/LibertyAllianceArchitecture200303.pdf
[31] A. F. Dwiputera., I. S. Ruppa., “Single sign-on architecture in public networks (Liberty Alliance),” INFOTECH seminar on advanced communication Services (ACS), 2005.
[32] B. Pfitzmann., “Privacy in enterprise identity federation-Policies for Liberty 2 Single Sign-on,” Elsevier information security technical report, vol. 9, no. 1, 2004 pp. 45-58
[33] B. Pfitzmann., and M. Waidner., “Analysis of liberty single sign-on with enabled clients,” IEEE Internet Computing, 2003, pp. 38-44
[34] P. Siriwardena, "Understanding OpenID”, 2008. http://www.slideshare.net/prabathsiriwardena/understanding-openid
[35] D. Balfanz, “Users vs identity provider in OpenID”, 2009 http://hueniverse.com/2009/07/users-vs-identity-providers-in-openid/
[36] C. Messina, “OpenID_Phishing_Brainstorm”, 2009. http://wiki.openid.net/w/page/12995216/OpenID_Phishing_Brainstorm
[37] M. Eriksson., “An example of a man-in-the-middle attack against server authenticated SSL-sessions,” In international conference on applied cryptography and network security, 2003.
[38] E. Tsyrklevich., V. Tsyrklevich., "Single sign-on for the Internet: a security story," BalckHat USA , 2007.
[39] E. Rescorla., “Diffie-Hellman key agreement method”, RFC 2631, Internet Engineering Task Force, 1999
[40] K. B. Anderson., E. Durbin., and M. A. Salinger., "Identity theft", Journal of Economic Perspectives, 22(2), pp. 171-192, 2008.
[41] M. Corporation. Introduction to Windows Live ID, 2008. http://msdn.microsoft.com/enus/library/bb288408.aspx
[42] R. Kanth., Automatic user creation/ login in commerce server starter site, 2008.http://microsoftblog.co.in/commerceserver/category/commerce-server-2007/page/14/
[43] Complete Source, Microsoft Live ID Phishing Illustrates the Dangers of Federated Identity, 2009. http://www.completesource.co.uk/2009/10/microsoft-live-id-phishing-illustrates-the-dangers-of-federated-identity/
[44] D. Bass, Microsoft examining if web users saw others accounts, 2010. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=affIdPDIbclA&pos=7
[45] J. Reagle., and L. F. Cranor., “The platform for Privacy Preferences,” Communications of the ACM, vol. 42, no.2, pp. 48-55, 1997
[46] A. Lysyanskaya., R. Rivest., A. Sahai., and S. Wolf., “Anonymous name systems,” In selected areas in cryptography, New York: Springer Verlag, 2000, pp. 184–199.
[47] G. Coker., J. Guttman., P. Loscocco., J. Sheehy., B. Sniffen., "Attestation: Evidence and trust", 10th International conference on information and communications Security, 2008.

[48] R. Sailer., X. Zhang., T. Jaeger., and L. van Doorn., "Design and implementation of a TCG-based integrity measurement architecture", In 13th USENIX security symposium, pp. 223-238, 2004
[49] The Trusted platform module, 2006 http://www.chillingeffects.org/weather.cgi?WeatherID=534
[50] W. Ford., M. S. Baum., "Secure electronic commerce: Building the infrastructure for digital signatures and encryption", Prentice Hall, Englewood Cliffs, New Jersey, 1997.
[51] G. Persiano., and Ivan Visconti., "An efficient and usable multi-show non-transferable anonymous credential system", In Proceedings of the 8th international financial cryptography conference, Lecture Notes in Computer Science, vol. 3110, pp. 196-211, Springer-Verlag.
[52] E. Verheul., "Self-blindable credential certificates from the weil pairing", Advances in cryptology Asia crypt, pp. 533–551, 2001.
[53] L. Chen., "Access with anonyms", Lecture Notes in Computer Science, vol. 1029, pp. 232-243, 1995.
[54] A. Lysyanskaya., "Signature schemes and applications to cryptographic protocol design" PhD thesis-2002.
[55] R. Sailer., X. Zhang., T. Jaeger., L. V. Doorn., "Design and implementation of a TCG-based Integrity Measurement Architecture", In Proceeding of the 13th conference on Usenix Security Symposium, 2004.
[56] Trusted Computing Group (TCG) http://www.trustedcomputinggroup.org
[57] Trusted Computing Group (TCG) Specification Architecture Overview v1.2, Technical Report, Trusted Computing Group, 2004
[58] R. M. Needham., M. D. Schroeder., "Using encryption for authentication in large networks of computers," Communication of ACM vol. 28, no. 11, pp. 993-999, 1978
[59] Internet2, Shibboleth. www.http://shibblоeth.internet2.edu
[60] T. A. Tanveer., M. Nauman., M. Amin., M. Alam., "Scalable, privacy-preserving remote attestation and through federated identity management frameworks," In Proceeding of ICISA, 2010, pp. 1-8
[61] I. B. Damgard., "Payment systems and credential mechanisms with provable security against abuse by individuals," Advances in Cryptography, pp.328-335, 1988.
[62] S. A. Brands., "Rethinking public key infrastructures and digital certificates: Building in privacy," MIT press, Massachusetts, 2000. http://books.google.com.my/books?id=U8VUaUiYohIC&lpg=PR15&ots=_WtVOHqPCw&dq=Rethinking%20Public%20Key%20Infrastructures%20and%20Digital%20Certificates%3B%20Building%20in%20Privacy%20.%20PhD%20thesis&pg=PP1#v=onepage&q&f=false
[63] W. Diffie., M. E. Hellman., "New directions in cryptography," IEEE Transaction Information. Theory, vol.22, pp. 644-654, 1976. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.9720
[64] S. McLeish "A security audit of shibboleth" 2007. http://hdl.handle.net/1988/2844

Zubair Ahmad Khattak received Bachelor and Master-Degree in Computer Science from University of Peshawar, Khyber-Pakhtoonkhwa, Pakistan, and Master- Degree in Information Technology from International Islamic University, Kuala Lumpur, Malaysia and currently is PhD student at the Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Perak, Malaysia. He is currently attached with MIMOS Berhad under student attachment program. His current research interests include privacy, trustworthy system, single sign-on, federated identity management through credential systems, and trusted computing techniques.

Jamalul-Lail Ab Manan completed his Bachelor of Engineering (BEng) in Electrical Engineering from Sheffield University, UK and Master Degree (MSc) in Microprocessor Engineering from University of Bradford, UK. In 1994 he completed his Doctoral Degree (PhD) from University of Strathclyde, Glasgow, UK. He is currently attached to MIMOS Berhad, Malaysia as a Principal Researcher in Advanced Information Security Cluster. His current interests include System Security, Identity Management & Privacy, Trusted Computing and Encryption.

Suziah Sulaiman completed her Bachelor of Science from Dalhousie University, UK and Master of Science in Business Information System, University of East London, UK and Master of Philosophy from South Bank University, UK. She completed PhD from University College London, UK. She is currently attached to Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Malaysia. Her current interests include Human Computer Interaction, User Haptics Experience, and Usability Evaluation.