Statement of Interest and Requirements for W3C Workshop on Identity in the Browser 24/25th May 2011, Mountain View (USA)

Presented by Dan Schutzer, CTO The Financial Services Roundtable/BITS

Cyber criminals are constantly challenging the strength and viability of on-line identification and authentication techniques employed by financial institutions. To counter this escalating threat most financial institutions employ layered defenses (such as out-of-band alerts and confirmations, anomalous behavioral monitoring detection) as well as multi-factor authentication in some cases, to augment ID and password, but judging by the continued success of cyber criminals in finding increasingly innovative solutions to defeat our defenses, it appears time to consider a stronger approach to authentication.

A number of events are coming together to create the needed impetus for change in our approach to authentication. These include:

1. Increasing sophistication and success of malware and cyber fraud (mentioned above)

2. Government drive for an Identity eco-system (this includes the National Strategy for Trusted Identity in Cyberspace (NSTIC), review of FFIEC Authentication guidance, possible publication of mobile security guidance, healthcare push for stronger federated identity, drive for wider deployment of the Personal Identity Verification (PIV) tokens, etc.

3. Growth of social networks, which is increasing the desire for greater user control over their sensitive data, and the need for secure and private sharing of information and other digital objects amongst trusted "friends."

4. Emergence of the cloud, which is making users more amenable to moving systems and applications outside the enterprise, and paying for these services on a usage basis. The changing economics and growing acceptance of the cloud is increasing the market for cloud-based identification services and amplifying the need for stronger authentication and access controls.

5. Emergence of new devices (e.g. iPads, smart phones) that are making possible the embedding of stronger authentication technology with greater ease of use.

6. Growth of apps stores that both allow users to select and install new identity applications, in the same way that they add an e-book, music or game app, and which increase the need for strong mutual authentication to ensure one is downloading a trusted app.

7. Emergence (and acceptance by software manufacturers) of new industry standards that enable stronger mutual authentication (e.g., Extended Validation TLS) coupled with more meaningful, usable identity indicators in web browsers (e.g., W3C WSC-UI). In the US banking vertical there is also the recent X9.117 online authentication standard and related FFIEC guidance.

It will take more than just strong customer authentication to overcome the growing sophistication of the threat. For example, a One Time Password token (OTP) is susceptible to a man-in-the-browser attack and out-of-band verifications are increasingly becoming the target of attack by fraudsters.

To combat the increasingly sophisticated threats, a systems approach that includes stronger mutual authentication of both the customer and the application service, as well as authentication

of the originator, intended recipient(s), and the content of any transaction, along with the application of layered security controls, as well as continuous monitoring of the relationship is required. But if we introduce this stronger authentication systems approach would the users come?

Users are increasingly having difficulty coping with the growing number of ID and passwords they have to remember and manage, but it beats the alternatives that have been presented to date. No matter how inconvenient the ritual of entering an ID and password onto a web page is, it is a ritual we have grown used to and adapted to. To get people to move to an alternative it must be significantly easier to use and offer some immediate benefits. It also helps if it is perceived to have a ***cool factor***.

For reasons of both economics and usability, it would be ideal if next generation identity credentials can be used across multiple delivery channels; i.e. not just online or on mobile devices, but also on face-to-face or phone/IVRU interactions. There is evidence that at least for the near future (next 2-3 years) there will be a growing diversity of devices and wireless networks. Besides smart phones, people are carrying kindles and iPads with them. There is also a growing number of networked game boxes (e.g., Wii, Xbox), and TV boxes (e.g., Apple TV and Google TV). And many who use laptops and PC's are not getting rid of them, just adding many of these other networked devices to their arsenal. These devices can connect to landlines, mobile and WiFi networks. So, any identity credential, whether embedded in a smart phone or stand-alone, would have to work seamlessly with a number of devices and networks.

As the smart phone grows in functions, applications and popularity, it will become a greater target for fraudsters and increasingly vulnerable to malware attacks. So there is a case to be made for an identity credential being implemented in either a dedicated hardware device or a protected software object, whose functionality is restricted to performing just a few key identity and authentication operations very securely to minimize its attack surface and able to work with the growing diversity of devices.

Online authentication serves a number of purposes. From a service provider's perspective, among other things, it is needed to:

1. Verify the identity, authorizations, entitlements and privileges for the entity you are currently transacting with

2. Relate the current transaction to past transactions enabling the current transaction to be conducted in context of past interactions

3. Determine what degree of trust you can attach to the current interaction. What information you can share in confidence.

From an end user perspective, mutual authentication serves an additional purpose of ensuring the service provider is in fact the entity (e.g., bank) it claims to be, and perhaps assess its reputation.

The level of assurance an application needs from the identity proofing process is not necessarily the same as the level of assurance needed from the authentication process. The former is concerned with how much information the online service provider needs to know about the user and with what certainty, while the latter deals with how sure the online service provider is that they are transacting with the same person as the last transaction, and is the person entitled and

authorized. In a federated environment (e.g., SAML SSO) the service provider performing transactions may not be the identity provider that originally carried out the user authentication.

Thus, the strength (degree of certainty) of the authentication required should be treated as a separate issue from the attributes associated with the authentication, or the confidence (strength of the identity proofing assurance process) regarding these attributes. A risk based approach is required. Applications that require very little attribute information about the customer, nor strong assurance that this attribute information is correct, may still require strong authentication of the customer. For example, many social network applications may have very little need to strongly verify the attribute information provided by its customers, but still have the need to be very sure that the person granted authorization to use and update a person's personal web pages is actually the person that page belongs to. Otherwise, the impersonator could misrepresent statements or positions, misdirect various alerts and offers, or manipulate personal information, causing embarrassment and/or damage to the actual page owner, and could result in aggregate statistics and incorrect analysis of trends, likes/dislikes, as well as impact the trust we have in various "friends." This is especially the case where the identity credential used for authentication is shared with other higher risk applications, where a compromise of the lower risk identity credential could be used to gain access to the higher risk application.

It is important to keep these two functions (identity proofing and online authentication) distinct and their needs in mind. Different online interactions require different amounts of personal information, at different levels of trust and certainty regarding the information provided. Although many applications and services require very little knowledge of one's personal attributes, other applications, such as financial and health care applications, require a far greater knowledge of one's personal attributes and have a need to verify these attributes with greater assurance.

One of the tenets of the NSTIC is the idea of credential sharing, where a user can authenticate oneself to a number of different online service providers using a single identity credential. The need to satisfy the various privacy, security and liability concerns makes this identity credential sharing more difficult. Using the same identity credential to authenticate oneself across a number of online service providers increases the value for a criminal to hijack or counterfeit the credential as it can be used to be authenticated into more online systems. Further, it simplifies the task of hijacking or counterfeiting the credential by allowing the criminal to attack the least secure, most vulnerable site. Thus it makes the case stronger for moving to a stronger authentication than ID and password.

If the wrong person is authenticated there is the issue of how the liability gets shared between the authenticating service and the relying party. One way to enhance customer privacy and to minimize the authentication service's liability is for the service to issue an identity credential to a customer based only on the information the authentication service needs to know to issue a credential, not everything the relying party might know about the individual. In this case, the authentication service only vouches for authenticating that the credential is being used by the individual they issued the credential to. The responsibility for identity proofing the user and the linking the credential to the identity attributes by which the user is known to the relying party remains the responsibility of the relying party. Another way to achieve this same result is for the issuer of the credential, the authentication service, to provide the relying party the tools to use the credential to directly authenticate the user themselves.

There needs to be an enforcement mechanism so the authenticated user, can be assured that the only use made of any revealed attributes by the various parties in the identity management supply

chain is for performing the required service, for the use advertised, not for any other purpose, and that this information will not be shared with any other non-authorized parties. This enforcement mechanism, if properly implemented, can also help to resolve and allocate liability in case of disputes

Taking all this into account one can conclude that a stronger cyber identity solution needs to achieve the following:

1. Provide secure and reliable identification and mutual authentication of all parties (e.g. user to identity credential; and of the identity credential to the online service) that is privacy-enhancing

2. Enable non-repudiation of transactions and information exchanges undertaken by authorized participants; e.g. authentication of a transaction with respect to verification of the sender, the receiver and the content of the transaction (e.g., digital signing)

3. Create a secure trusted path between identity credential, display, input device and web service

4. Make it easy to evolve and adapt to future fraudster attack innovations

5. Be perceived as compelling to users providing them greater convenience, security, privacy and other benefits (even be perceived as “cool” and easier to use without adding inconvenience or onerous delays).

6. Be open standards-based, easily interfaced to applications and certifiable. For example, adopt RESTful and/or service oriented architectural (SOA) principles that enables independent deployment of components, scalability of component interactions and generality of interfaces

7. Ensure that the identity credentials that are interoperable with respect to the issuance/enrollment and authentication protocols, where its strength is linked to standard known assurance levels.

8. Work with a diversity of devices, interoperate across web services permitting user-controlled exchange of information, and ensure the ability to securely transition strong relationships across sites and access points.

9. Be easy to interface to, optimally requiring no change, offering some combination of lower costs to operate, lower liabilities, the potential for attracting new customers, new forms of revenue, and demonstrated user demand.

10. Be capable of supporting continuous improvement

11. Enable continuous monitoring of the relationship and be risk-based such that one can escalate the challenge when there is an indication of possible hijacking or other anomalous behavior

12. Enable the user to significantly reduce the number of usernames he/she is forced to use

13. Support decoupling (independence) of the identity proofing process from the authentication process

14. Include the necessary policies, rules and operation bodies to provide a stronger “trust” anchor in the U.S. and internationally, and which provides a clear delineation of the accountability and liability associated with the issuance and verification of an identity credential

15. Provide the ability to display identity signals to the user that are both usable and spoof resistant

16. Support credentials that work on offline channels as well

17. Finally, it would be helpful to build this new authentication technology on top of existing infrastructure that already has achieved widespread market acceptance and critical mass; the web browser being one of these