W3C NSTIC Governance NOI Response

Introduction

The W3C (The World Wide Web Consortium) has been following the National Strategy for Trusted Identities in Cyberspace (NSTIC) as identity and trust are vital to the evolution for the Web. The W3C is a membership consortium founded and directed by Tim Berners-Lee focusing on facilitating the creation of royalty-free standards such as HTML and XML by the consortium members.

There are three primary concerns of the W3C regarding NSTIC.

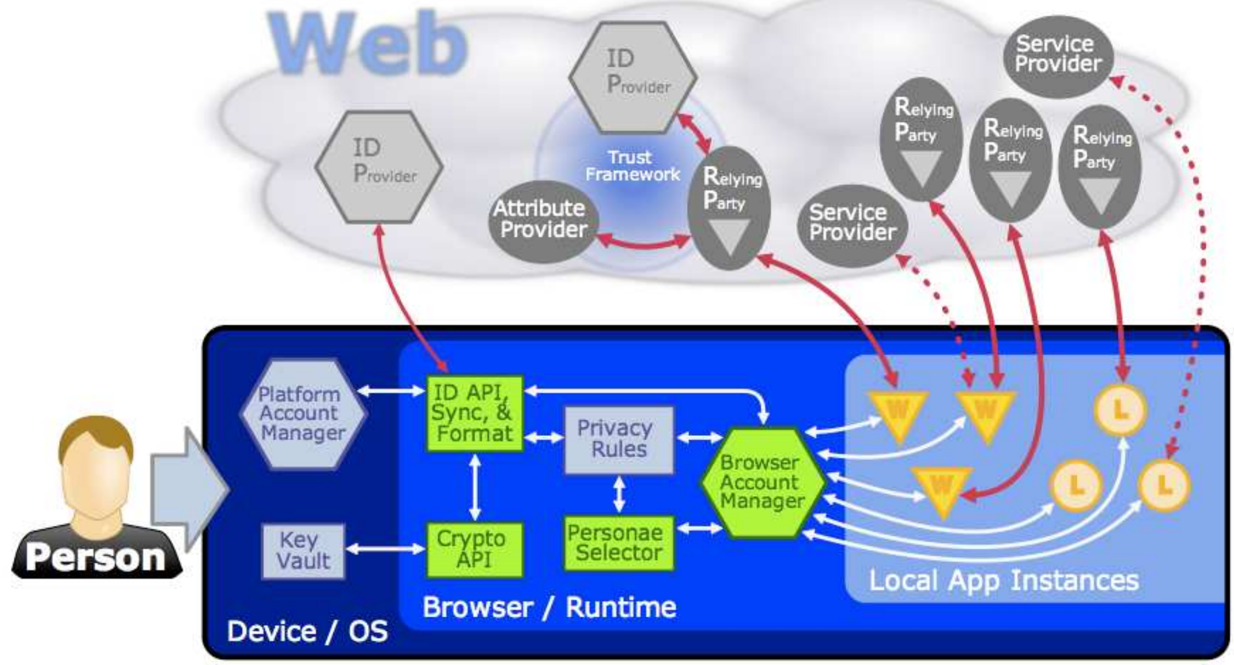
- *User-centric technical framework*: A user-centric framework based on standards in the browser and other client devices should increase simultaneously the security, privacy, and fluidity of transactions involving personal data on the Web. In this response, the W3C outlines a plan for such a user-centric architecture of identity standards that includes browsers and other client devices.
- *Royalty-Free*: All standards required or endorsed by NSTIC should be royalty free and available to the general public to implement.
- *Transparent and Accountable Process*: The steering group should have a multi-stakeholder, industry-led, open, transparent and accountable process that guarantees the creation of a fair and open market for innovation in the identity space.
- *Global Harmonization of Standards*: The W3C considers it of prime importance that standards have a global reach and focus on internationalization. This is primarily dealt with in Section 4 of the NOI.

User-Centric Technical Framework

Many identity management schemes have been proposed in the past, but have failed because of inadequate attention to the end user. NSTIC wisely identified user-centricity as a theme, but did not adequately follow through by highlighting the necessary architectural components to be truly user-centric. NSTIC's approach can be improved by more directly addressing user-centricity. We suggest to explicitly add the connection to the "person on the street", who interacts with their online identity using a number of devices on the Web, rather than only focusing on interactions between identity providers and relying parties as governed by certified trust framework in "the cloud" (i.e. on servers). The current approach seems to consider it implicit that the user has successfully authenticated and authorized the transaction in a secure and privacy-respecting manner. However, currently this is not the case for the majority of interactions with the Web. It is precisely the connection between the user and the identity provider that is the missing link underlying the identity ecosystem, and without considerable standardization on the client device the higher-level standardization around trust frameworks is unlikely to reach its full potential.

The connection between the user and the identity provider is a necessary connection to secure. Further, it is an ideal junction to enforce privacy policies. The user connects and interacts with the identity eco-system primarily through their Web-facing browsers and other applications on a large range of devices. Therefore, focus on the creation of standards for user-centric identity in the browser and other client devices (including the larger platform) should be a priority of NSTIC and work should be done to make sure such standards harmonize both with new and existing standards around server-side digital identity and trust frameworks.

The user-centric approach is illustrated in the figure below:



In detail, the flow begins with the user, who is a **Person** interacting with their local device, such as their personal computer or smartphone that runs on a platform such as an operating system. The device acts as their portal to the cloud, which the user typically interacts with via the **Web**. The user typically authenticates their identity using some combination of their platform's account manager, with a browser account manager, and/or with an identity provider in the cloud. All account managers are given by *hexagons*. At this point in the login process the user may choose different identities via a component of their account manager, the **personae selector.**

The user's connection with service providers (given by *grey circles*) on the Web is mediated by the platform's Web browser or device run-time, which is given as a *blue box*. Connections that present **security issues** are given in *red* with *whole red lines* representing **user-based authentication** (such as login via user-name passwords or using asymmetric secrets) with possible personal data transfer and *dotted red lines* representing personal data transfer (for example, to a geolocation provider, weather service, RSS feed, or other 2-way data source). Notice that the security issues (attack surfaces) are primarily between the Web and the browser/runtime. The browser/runtime is relatively secure (the *black border* behind the client-side), and the risks are outside that environment.

These service providers on the Web interact with the user via their browser/runtime, where the mobile code is communicated from the Web into the browser/device runtime either as **web pages** (*yellow triangles with a W*, where web-page is broadly construed to include any combination of HTML and Javascript applications running in a web browser) or as **local applications** (*yellow circles with an L*, such as mobile smartphone apps). These application interact via components of the account manager (*squares*) such as an **Identity API and formats** that let them interact with the account manager. Note that the browser can support non-phishable credentials such as asymmetric secrets via the access of the account manager to a **key vault** in the platform and use of a local **Crypto API** to secure connections using the keys stored safely in the key vault. The flow of personal data can be regulated by *privacy policies* specified as part of the transaction by the user or their identity provider. As given by the diagram, these account managers can communicate with each other, so that the account in a platform may be transferred both to and from various different platforms, device/browsers, and cloud-based identity providers using **Identity Sync**.

Cloud services are distinct from local identity managers, but are an equally important part of the larger picture. Cloud-based identity providers (IDPs) also benefit from a local account manager, which can act as a more secure proxy between the IDP and the site using the aforementioned Crypto API and Identity API. This secures the connection between identity providers and **relying parties** (services that consume identity information but do not host it) who have their server-to-server interactions validated by a **trust framework**, as given by the *blue connections between identity providers and relying parties*. One could imagine the local client also being certified as "trusted" although this is still open for exploration. New standards work by W3C, as explored in the "Identity in the Browser" workshop, is marked in *green*.

An important technique in the fight against phishing attacks, is the means for the browser to authenticate the website. Mutual authentication provides a means for the website to authenticate the user, and for the user to be assured that the site is same as the one for which the account was originally created with. Public key certificates have failed to live up to their initial promise for **authenticating websites**, and it is now time to find effective solutions to this challenge.

The current trend for using email addresses as identifiers is convenient for users and websites alike, but weakens privacy through the use of the same identity across many sites, facilitating linkability. A similar concern applies to the direct use of identities based upon public key cryptography. Websites and other relying parties require strong assurances regarding a particular identity, but don't need a globally linkable identity. Such assurances can be provided using strong identities where the issuing party has robust processes for verifying attributes of the identified party (the user), e.g. full name, address, date of birth and so forth. Cryptographic techniques (zero knowledge proofs) can be used to prove the possession of particular attributes to the relying party, but without disclosing a globally linkable identity. The successful deployment of **privacy friendly strong authentication** is dependent on the establishment of trusted identity providers with thorough and robust processes for issuing credentials.

Until now approaches to federated identity have ignored the browser, primarily because it was viewed as too difficult to change. However, the two key areas of **secure authentication** and **a downstream ecosystem of identity-using applications** crucially require lightweight standards around the browser and other device clients. For example, the local device is absolutely crucial to provide better authentication than the currently standard username-password symmetric secrets, and otherwise the trust frameworks will be vulnerable to the same security flaws as any other server. In fact, security within federated identity systems can be even worse, as the server-side identity provider can centralize identity credentials across many relying parties. While getting rid of user-name and passwords and replacing them with true non-phishable credentials is mentioned in the NSTIC strategy, it is de-facto impossible without standardized client interaction. Also, currently NSTIC does not specify that service providers may include a large number of web and local applications that need a uniform API to access data from the identity provider.

As demonstrated by the W3C "Identity in the Browser" workshop in Mountain View in May, there is now considerable interest by browser vendors in technology around standardizing identity in client devices, browsers, and the platform. So while the W3C does not create standards around trust frameworks and certification, the W3C is committed and uniquely positioned to be the forum for user-facing browsers and devices, and so the W3C should be part of the steering group.

Royalty-Free Standards

As the only way to demonstrably maintain interoperability is via standards, standards bodies should be involved in the governance of NSTIC.

In order to foster innovation and development, Identity technology for the Web and the Internet should be compatible with many different business models and methods of development. This includes the ability to develop relevant software according to the open source model. The standards underpinning the Identity Ecosystem should therefore be developed according to an open and transparent process; should be available to the public free of charge; and should be implementable on a royalty-free basis.

We consider this as important as other underlying principles of NSTIC such as the conformance to the fair information practice principles.

Accountable Industry-Led Process

The W3C believes the steering group should consist of multiple standards bodies and follow an open, transparent and archived process with a clear founding charter and process document. We have seen the advantages of such a process in W3C's own history. Industry groups are well-suited to address the complex technical issues involved in online identity. Transparency of both communication and process provides a neutral and accessible venue for participation from industry, government, academia and the public.

Global Harmonization of Standards

The W3C considers it of prime importance that standards have a global reach and focus on internationalization. This is primarily dealt with in Section 4 of the NOI.

Structure of the Steering Group

- *1.1. Given the Guiding Principles outlined in the Strategy, what should be the structure of the steering group? What structures can support the technical, policy, legal, and operational aspects of the Identity Ecosystem without stifling innovation?*

As digital identity is a crucial part of Web architecture involving many diverse state-holders ranging from the private sector to the federal government. The steering group should be a multi-stakeholder body of peers with a transparent process as well as a public accountability mechanism to the general public and larger private sector. Standards bodies, particularly those already involved in issues of identity and security on the Web, can serve as both a useful model for and an essential components of a steering group.

- *1.2. Are there broad, multi-sector examples of governance structures that match the scale of the steering group? If so, what makes them successful or unsuccessful? What challenges do they face?*

One of the best examples of a broad, multi-sector example of governance that involves the private sector is the Internet ecosystem. This ecosystem includes technical standards bodies, such as the IETF and W3C. These bodies have successfully created the standards such as TCP/IP and HTML that now are crucial to the success of the Internet and Web. They have well-developed governance models that fulfill the criteria of accountability and transparency, in developing standards that cater to a globally shared technical infrastructure.

The largest challenge for NSTIC is identifying the correct stake-holders and making sure they are brought to the table at the beginning, as well as devising a transparent and accountable - as well as often legally binding in terms of contracts - process.

- *1.4 Are there functions that the steering group must have that are not listed in this notice? How do your suggested governance structures allow for inclusion of these additional functions?*

While the steering group should have the power primarily to promote global harmonization of open standards across industry, create clear and legally binding contracts, and certify trust frameworks, the steering group should not become yet another standards body, but should instead using existing standards processes that already exist in the private sector. The steering group should also make sure that any standards used comply with Fair Information Practice Principles (FIPPs) and relevant US regulation, as well as be capable of technically and legally implementing the principles and goals of NSTIC.

- *1.5. To what extent does the steering group need to support different sectors differently?*

The steering group will mainly have to deal with a number of domains with differing requirements around identity, privacy, and security, and these differences will likely be crucial as regards legal contracts around identity. These domains should be identified early as possible and ideally relevant expertise engaged with by the steering group when it is initiated.

- *1.6. How can the steering group effectively set its own policies for all Identity Ecosystem participants without risking conflict with rules set in regulated industries? To what extent can the government mitigate risks associated with this complexity?*

The steering group's policies should be created in consultation with regulated industries and aim at all times to promote a fair and open market as well as widespread use across industries. This requires identifying regulated industries as stakeholders as early as possible in the process of forming the steering group.

- *1.7. To what extent can each of the Guiding Principles of the Strategy–interoperability, security, privacy and ease of use—be supported without risking 'pull through' regulation from regulated participants in the Identity Ecosystem?*

The steering group should actively promote harmonization with regulated industries before creating its contracts (such as contracts for liability), have the ability to amend these contracts based on new information or specialize such contracts for regulated industries, and have a strong representation from legal bodies from the onset of its formation.

- *1.8. What are the most important characteristics (e.g., standards and technical capabilities, rulemaking authority, representational structure, etc.) of the steering group?*

The group should consist of standards bodies from a diverse background, including but not limited to standards focused on the user-facing client device (such as browser or smartphones), standards on privacy policies and rules, standards on certification and Cloud-based identity. In fact, the primary task of the steering group should be to harmonize these standards and to ensure the various standards bodies work together to accomplish the goals of NSTIC while maintaining principles such as royalty-free standards and respecting the privacy of users.

- *1.9. How should the government be involved in the steering group at steady state? What are the advantages and disadvantages of different levels of government involvement?*

The government is an important stakeholder as it represents for the interest of the public and can be a strong voice to maintain the integrity of NSTIC's goals and vision, in particular implementation of fair information practice principles by certification authorities and royalty-free standards by standards bodies. However, the government or any part thereof should be a stakeholder and not be in a position of administrator or executor, as this may prevent the steering group from being industry-led and may stifle innovation. What is necessary is for industry to rise to the occasion to provide the general public with a secure and trustworthy Web.

2. Steering Group Initiation

- *2.1. How does the functioning of the steering group relate to the method by which it was initiated? Does the scope of authority depend on the method? What examples are there from each of the broad categories above or from other methods? What are the advantages or disadvantages of different methods?*

The government should help establish the steering group by enabling a new body organically formed from the private sector to take on the functions required by NSTIC. In its initiation phase, the government should ensure that a new organically formed body has a clear and transparent process, transparently and publicly available records of meetings and decisions, conformance to principles such as royalty-free licensing on open standards, and adequate funding to begin. A multi-phased process that first lets an initial steering group identify key missing stakeholders before creating any rules or new standards would be ideal. There are no clearly defined existing private sector bodies that would easily become the steering group without forming an alliance with existing standards organizations and other private-sector entities.

- *2.2. While the steering group will ultimately be private sector-led regardless of how it is established, to what extent does government leadership of the group’s initial phase increase or decrease the likelihood of the Strategy’s success?*

The government is one of the primary stakeholders and thus may want to be part of the steering group in initiation phase. However, the steering group must be designed by the private sector and exist to enable private sector innovation. Furthermore, not being directly administered by the government allows the private sector-led steering group to more easily internationalize its activities and deal with other governments.

- *2.3. How can the government be most effective in accelerating the development and ultimate success of the Identity Ecosystem?*

The government can be most effective by encouraging the identity ecosystem to form in the private sector. The ultimate role of the government, should it chose to participate as a stakeholder, will be to make sure that the goals of NSTIC are met with respect to increased cybersecurity as well as respect and enforcement of the privacy of users. Given that there are many aspects of privacy, identity, and security that are not well-understood, funding research pilots is also useful. Another key role of the government may be as an identity provider and relying party itself.

- *2.4. Do certain methods of establishing the steering group create greater risks to the Guiding Principles? What measures can best mitigate those risks? What role can the government play to help to ensure the Guiding Principles are upheld?*

The government should engage as a stakeholder in the steering group in order to mitigate the risk that the steering group creates market asymmetries or fails to uphold principles around an accountable and transparent process, royalty free standards, and privacy. However, the government can not administrate the steering group and the steering group can not advise the federal government, as these activities are already covered by FICAM.

- *2.5. What types of arrangements would allow for both an initial government role and, if initially led by the government, a transition to private sector leadership in the steering group? If possible, please give examples of such arrangements and their positive and negative attributes.*

The exact form of the initial government role should probably be in ensuring the composition of the steering group is inline with the goals of NSTIC by helping identity and select stake-holders, and then joining as a stakeholder, as well as identity provider and relying party in the infrastructure. Initial funding of the start-up phase of the steering group also will likely be necessary. However, in the long-term it would be ideal for the government role to be reduced to a stakeholder in a larger process no different than any other stakeholder.

3. Representation of Stakeholders in the Steering Group

- *3.1. What should the make-up of the steering group look like? What is the best way to engage organizations playing each role in the Identity Ecosystem, including individuals?*

The steering group should be a peer-based organization composed primarily of standards bodies, certification authorities, civil society, and private sector companies with no single executive organization or individual. An open processes, public comment, accountability enables individuals to participate in NSTIC in a principled manner so that all voices can be heard. Appropriate relationships with organizations in the Internet Ecosystem and civil society should be established as well.

- *3.2. How should interested entities that do not directly participate in the Identity Ecosystem receive representation in the steering group?*

There should be a clear application process with rights and responsibilities. Also, a clear and accountable process that allows for public participation and feedback is essential.

- *3.3. What does balanced representation mean and how can it be achieved? What steps can be taken guard against disproportionate influence over policy formulation?*

The steering group should ideally be self-regulating, but in the initial stages it should identify relevant stake-holders. Existing organizations with large and diverse memberships should be highly considered. As a stakeholder, in the early stages of formation the federal government should voice its opinion to help achieve balanced representation. This means that given a user-centric technical implementation plan as presented earlier, all relevant standards bodies should be included to maintain focus on the goals of NSTIC. Organizations from civil society that advocate for privacy and end-user rights should be part of the stake-holders.

- *3.4. Should there be a fee for representatives in the steering group? Are there appropriate tiered systems for fees that will prevent 'pricing out' organizations, including individuals?*

The steering group should create a sustainable funding model. Yet as with any new effort, there will be a need for funding to start-up. However, there should be no fees for individual participation in the process, as this would discourage participation of those with less financial resources. Therefore, a clear and accountable process that takes into account participation individual participation and organizations unable to pay for a fee should be created. For example, while the W3C is a membership organization with a tiered system of fees, the W3C does this through accountability to any comment from the public on its mailing lists and is opening a "community" process that does not require any fees.

- *3.7. How can appropriately broad representation within the steering group be ensured? To what extent and in what ways must the Federal government, as well as State, local, tribal, territorial, and foreign governments be involved at the outset?*

Broad representation, particularly in the formative stages of the steering group, can not be guaranteed, but the initial stakeholders, which should include the United States federal government, the carefully identify stakeholders group to ensure broad representation. In this way, any form of government, including foreign governments, can be considered stakeholders like any other organization. The main process for guaranteeing involvement of all interested parties in a clear and documented process with explicit accountability and publicly available records. This can take the form of long-standing archives.

4. International

- *4.1. How should the structure of the steering group address international perspectives, standards, policies, best practices, etc?*

The initial steering group should include global standards bodies, civil society, and private-sector companies with global reach in order to maximize the likelihood of achieving international success. The W3C would be be qualified for such a the steering group.

- *4.2. How should the steering group coordinate with other international entities (e.g., standards and policy development organizations, trade organizations, foreign governments)?*

The standards created to enable NSTIC should involve international entities from the onset, both involved in the creation and review of these standards. These standards should also have a clear path from community-driven informal specifications created by members of the general public to international standards for royalty-free implementation across national bodies. Also, the steering group should have a clear liaising process with other international bodies. Proactively creating liaison with appropriate bodies should be strategically chosen by the steering group in consultation with the government and the steering group's members should commit the resources to maintaining these liaisons.

- *4.3. On what international entities should the steering group focus its attention and activities?*

Having a clear and accountable process that is international in scope (for example, by allowing comments from outside the United States) is one method to help guide attention. Additionally, the steering group should leverage and interact with ongoing efforts by globally relevant standards development organizations.

- *4.4. How should the steering group maximize the Identity Ecosystem’s interoperability internationally?*

The main focus should be on encouraging global-level coordination on the choice of standards. NSTIC should endorse globally-recognized, royalty-free standards, and should facilitate input into the relevant standards processes. Such input could, for example, concern the ability to extend, adopt and profile existing standards dependent on specific regulatory and legal environments. Aligning with standards organizations and existing work is essential, as is back-porting technical requirements into internationally developed standards.

- *4.5. What is the Federal government’s role in promoting international cooperation within the Identity Ecosystem?*

By joining as a stake-holder and making sure the initial steering group respects a transparent and accountable process that can expand to include new international entities, the Federal Government can help the private sector create a privacy-respecting, user-centric, and secure World Wide Web based on royalty-free open standards that are globally relevant.

Response authored by Harry Halpin with comments from Nick Doty, Jeff Jaffe, David Raggett, and Thomas Roessler.