CertiPath
www.certipath.com

July 22, 2011

TO: NSTIC Program Office
National Institute of Standards and Technology
U.S. Department of Commerce

SUBJECT: Response to Notice of Inquiry [Docket No. 110524296-1289-02]: *Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace*

CertiPath, a federation partner to the Federal Bridge Certification Authority and a provider of high assurance trust to the Aerospace Defense industry is pleased to submit the following response to the Notice of Inquiry concerning the National Strategy for Trusted Identities in Cyberspace.

CertiPath supports the notion of a multi-sector Steering Group to lead in the establishment of a national identity ecosystem. We recognize that the National Strategy for Trusted Identities in Cyberspace (NSTIC) provides a vision of what could be if we are all willing to work together to achieve it. Toward this end, the Federal community should view the national strategy as its own relying party policy, thereby creating an early critical mass that will attract identity and other service providers wishing to respond to the needs of the Federal relying parties. This will provide the critical mass that in turn attracts relying parties from other sectors, increasing the market for the identity industry and growing the ecosystem.

1. Structure of the Steering Group

It must be made clear that the identity ecosystem is led by this Steering Group. To that end, it is important that the Steering Group include representation from the major stakeholder communities. It is equally important that the members of the Steering Group represent the community, not an individual company's interests. The group should be established as a committee of peers. In lieu of electing a Chair and Vice Chair, a secretariat should be established to facilitate meetings, set dates and venues, capture minutes and action items, and moderate the meetings. The Steering Group should work on a consensus basis – while it may not be possible to eliminate a voting process completely, they should, whenever possible, negotiate differences of opinion into consensus positions. There must be a concerted effort on the part of the Steering Group not to give preferential treatment to any one stakeholder group. This can be achieved through the standard joint venture practice of each Steering Group member signing a code of conduct and ethics statement that commits them to putting the good of the NSTIC above their own organization's personal interest. This code of conduct and ethics statement would include an acknowledgment from the individual Steering Group member's parent organization that this will be the case so that individual Steering Group members cannot be called into question for making a decision that may not have been optimal for the parent organization.

The identity issues of the different sectors may have unique aspects, but the key to the success of the ecosystem is finding the common ground, and then ensuring that the ecosystem is flexible enough to accommodate the differences. Regulated industries bring their own challenge to the ecosystem, but through their representation on the Steering Group, any special considerations associated with their regulatory environment can be recognized and accounted for, in the same manner other unique aspects associated with a particular sector are addressed. The stakeholders involved in the regulated industries are best positioned to understand how the identity ecosystem can be designed to accommodate their needs.

The Steering Group may want to establish workgroups comprised of subject matter experts in different areas that will research and address particular issues raised by the Steering Group. There is probably a need for standing workgroups to address the Privacy, Legal, and Technical aspects of the Ecosystem, with the possibility of additional short-lived ad hoc groups that will be formed to address particular issues that do not fall into one of these categories and then disbanded once the issue is resolved. The working groups should be open to all interested parties and. once established by the Steering Group through nomination of a core team and provided with an objective, independently self-governing internally (setting meeting dates, times, assignments etc).

Ultimately, the functioning of the Steering Group, the secretariat and the working groups will be established through the adoption of a Charter for the group. The development and adoption of the Charter must be the first order of business once the Steering Group is formed.

The most important characteristics of the Steering Group are transparency, accountability, and the collaborative process. There should be no back-room meetings or secret deal-making behind the scenes; the individual Steering Group members must be committed to the collaborative process and accountable to the constituencies they represent – concepts that are accounted for in the Charter.

The example that may come closest to the structure needed for the Steering Group is the UK's TScheme, a self-governing group that "is the independent, industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it approves Trust Services."[1] TScheme provides a seat at the table for the UK Government as a stakeholder, but the government does not enjoy any special privilege within the group. As stakeholders, government and industry agree to support TScheme by requiring its certification for trust services within their organizations and in the federated environment. This is an important consideration for the organizations that participate in the NSTIC Steering Group. There must be agreement that the consensus decisions of the Steering Group concerning the identity ecosystem will be adopted and supported by the participating organizations, including the government.

A key aspect of the Steering Group's activities will be establishing a communications plan for carrying the message of the identity ecosystem to the Nation. Education and understanding are key components in the success of this trust infrastructure and they must extend beyond the identity, privacy, technical, and advocacy communities to the individual user sitting in front of a computer at home, at school, at work, in the public library or at the Internet cafe.

[1] http://www.tscheme.org/about/index.html

It is important that the Federal government provide support, both leadership and financial, to the establishment of the Steering Group. It could be expected that the Federal government will be asked to provide funding for operating expenses associated with the Steering Group's secretariat. However, once the Steering Group has been established, the government is simply another stakeholder group with the same responsibilities as the other participating organizations. It is conceivable that the Steering Group may recognize two 'flavors' of government stakeholders – federal and state/local/tribal – and provide seats on the Steering Group for both. It is conceivable that the National Governors Association or the National Association of State CIOs would provide Steering Group participation in addition to a Federal government participant.

2. Steering Group Initiation

It must be clear that the identity ecosystem is led by the Steering Group. To that end, the Steering Group is the final authority for the identity ecosystem's policies and operating rules, following a deliberative process which includes working group recommendations and public comment, where appropriate. To ensure its continuation, the Steering Group must foster the peer relationship of its members from the beginning. To determine Steering Group membership, the stakeholder communities must be identified and each one encouraged to nominate an individual for a position on the Steering Group. To aid the group in the nomination process, a set of recommended criteria for a Steering Group member may be provided. It is important that the identification of stakeholder groups is fair and wide-sweeping, but participation by any particularly group must be at that group's volition – encouraged, but not mandatory, and it is equally important that the represented group determine its representative – there must be no handpicked members selected at the government's discretion (except the government Steering Group member, of course).

It will fall to the Federal government to finalize the initial list of stakeholder groups based on this and other input from industry, extend the invitation to participate, and provide financial support to the fledgling group. While it is unlikely that the Steering Group will come together without this Federal government leadership, it is important that once the Steering Group membership is identified, the secretariat is established, and the first meeting has been held, the government steps back and lets the Steering Group lead. By creating a peer group supported by a secretariat, there is no need for the Federal government to take a leadership role in the Steering Group itself. Instead it can exert its influence on a par with the other members of the Steering Group.

The primary role of the Steering Group during the first few years will be establishing the criteria and certification processes for participation in the identity ecosystem. This may be in the form of technical policies and specifications, operating rules, and determining what infrastructure pieces are required to support the on-going viability of the ecosystem. This early work may take the form of an enterprise architecture that details the path to implementation complete with an end state vision and intermediate goals to show progress. Equally important to the activities that will establish the operational environment of the identity ecosystem is establishing a self-supporting financial model to cover the logistics for the ecosystem and the Steering Group. While some form of seed funding is inevitable to establish the Steering Group, it is important that it become self-supporting as soon as possible. For this reason, it can be expected that there will be a

lot of working group activity during the first year of the Steering Group's existence, but that this will taper off as decisions are made and the ecosystem begins to coalesce.

3. Representation of Stakeholders in the Steering Group

The Steering Group must remain a manageable size. Twenty to twenty-five participants are probably its limit for effectiveness. The larger population of interested organizations and individuals could then participate through the working group process. The Steering Group should be comprised of stakeholder organization representatives as previously mentioned. Among those to be considered:

- Citizen advocacy groups like the American Association for Retired Persons (AARP),
- Privacy advocacy groups like the American Civil Liberties Union (ACLU), Center for Democracy and Technology (CDT), On-Line Privacy Forum, Electronic Privacy Information Center (EPIC)
- Standards Groups like the Organization for the Advancement of Structured Information Standards (OASIS), Internet Engineering Task Force (IETF), International Organization for Standardization (ISO), American National Standards Institute (ANSI)
- Identity Industry Groups like the Transglobal Secure Collaboration Program (TSCP), Smart Card Alliance (SCA), Open Identity Exchange (OIX), Kantara,
- Banking and Financial Industry groups like the American Bankers Association, EuroCard, Mastercard, and Visa (EMVCo), BITS Financial Services Roundtable, National Automated Clearing House Association (NACHA)
- Health Care Industry groups like the Healthcare Information and Management Systems Society (HiMSS)
- Legal Industry groups like the American Bar Association
- Academia like Internet 2.
- Business advocacy groups like the Chamber of Commerce
- News media groups like the Associated Press
- Government organizations such as the National Association of State Chief Information Officers (NASCIO)

The NSTIC Program Office may want to start by determining the groups that have participated in the process to date and supplementing that list of organizations to ensure the wider community is reached. To further the success of the Steering Group and the Identity Ecosystem that it governs, the Federal government, as well as the state, municipal and tribal governments, must lead by example in asserting their trust in the identity ecosystem to the exclusion of solution providers that choose not to participate in the identity ecosystem, and by delivering their internal relying parties (application providers) and identity providers as early adopters of the ecosystem.

There should never be a fee or dues for participation on the Steering Group. It must be recognized that the organizations who provide representation to the Steering Group are giving of their time and expertise to support the NSTIC, and this willingness to serve must not carry an additional financial burden. This is true also for the representation to the working groups. There must be no pay-to-play, but it is up to the represented organizations to ensure that the representatives they nominate represents the organization's interests not their own or those of an individual company. Federal funding to support the establishment of the Steering Group and early meetings will

overcome the need to charge fees to the Steering Group members. Once established, the Steering Group must develop a financial model for sustaining the Steering Group moving forward. This is probably best achieved through some sort of revenue sharing arrangement related to ecosystem participation by identity providers, certifiers and relying parties who will require certification, trustmarking etc.

4. International

This is the National Strategy for Trusted Identities in Cyberspace. As such, it is important to understand that it has been branded as a United States undertaking. Therefore, any overtures for international participation must be carefully communicated. Do not be mistaken, the international community is watching and waiting to see what develops. Asking for information on the initiatives of some of these countries is an excellent way to foster their participation. TScheme and the Stork initiative in Europe as well as PLAID in Australia are worth understanding more about as the Steering Group begins its work. However, in the early going the Steering Group itself will be the richest source of international perspective because many of these groups are multinational in scope and they will bring this knowledge to the table as a natural part of their contribution to the solution. As the group starts to see results and the identity ecosystem begins to form, the interest of the international community will become more overt and they will approach the Steering Group. In the meantime, taking every opportunity to participate in international forums to discuss and promote the ecosystem and invite debate is an excellent way to promote openness.

The technology related to the identity ecosystem will generally not be problematic when it comes to interoperability and federated trust across international boundaries. It will be the privacy protections the ecosystem embraces. This must be a key consideration when the identity ecosystem's policies and operating procedures are being established.

On July 13, CertiPath participated in an ad hoc meeting of NSTIC stakeholders to discuss the Notice of Inquiry and engage in an exchange of ideas in preparation for developing our response. In addition to informing the debate and our response above, the group developed ten guidelines for the government's consider in the establishment of the NSTIC Steering Group. We support these guidelines and list them here:

1. Government is a stakeholder, not the administrator of the Steering Group

- No government to have oversight power in steady-state
- Could be own stakeholder group (i.e. federal, state, tribal, local, foreign etc.)
- Could be involved in more general stakeholder groups as both a Relying Party and an IdP

NOI Sections: 1.9; 2.5; 3.7

2. Government provides seed money

- Will need both monetary and in-kind support to get Steering Group off the ground in initial stages
- Included in that is the funding of pilots
- Government will also need to deliver customers

NOI Sections: 2.2; 2.3

3. Peer relationship among members

- Use a secretariat to facilitate and moderate rather than a Chair/Vice Chair
- Steering Group working groups should be liaisons with existing SDOs/Industry Working Groups
- Must avoid choke points

NOI Sections: 1.1; 3.1

4. Steering Committee processes will be transparent, deliberative, and open

- Think in terms of GOALS not MILESTONES
- Ensure targets, but limit liability to have to justify them

NOI Sections: 1.3; 1.8

5. Smart Grid is a sector specific, yet useful model of phased development (Stage 1: Design, Stage 2: Rules, Stage 3: Execution)

- Organizational model as discussion starter: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/SGIP/SGIPStructure.png
- Development of Steering Committee must come in phases, and prepare to be flexible
- Must prioritize designation of stakeholder groups
- No "NIST Oversight" in steady-state (see also Point of Consensus 1)

NOI Sections: 1.1; 1.2; 2.1; 2.2; 2.3; 2.4

6. Conscious effort to involve privacy/consumer/end-user constituencies

- Ensure that all stakeholders have voice on Steering Committee, including smaller or newer contributors to the online identity space
- Steering committee must initiate education/communication platform for end-users
- Leverage organizations that are already engaging broad populations of people (e.g. NGOs like AARP, Trade Groups, SDOs)

NOI Sections: 1.1; 3.1; 3.2; 3.3

7. Steering Committee creates a sustainable funding model, without pay-to-play relationship

- Government to provide seed money, but up to Steering Committee to determine funding structure moving forward
- Representation not contingent on fee
- Must not muscle-out stakeholders with less financial resources
- Funding source could be excise revolving fund from trustmark fees
  NOI Sections: 1.4; 3.4; 3.5

8. Sensitivity to requirements for international collaboration

- Diplomacy
- Open, collaborative approach
- Definition of stakeholders must take international community into account
- International community should be informed by
  NOI Sections: 3.7; 4.1; 4.2; 4.5

9. Minimize adverse legal impacts caused by government involvement (e.g. FACA)

- If the Steering Committee is perceived as advising the government on policy, then Federal Advisory Committee Act (FACA) will be triggered.
- FACA is painful: red tape, oversight, etc.
- *If private sector leads as by design, (and government becomes a stakeholder participant) then FACA can be avoided.
  NOI Sections: 1.1, 1.9, 2.2, 2.3, 2.4

10. Don't break anything that's working today

- Focus should be on building up from existing infrastructure, standards
- Identifying weaknesses and action plans to address them
- Helping the visibility of trusted identity
  NOI SECTIONS: 1.6 2.1, 4.4