Prepared for:

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

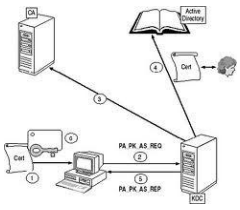
Daon Response

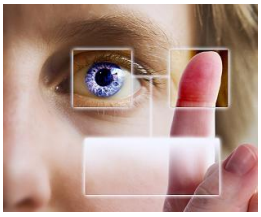
Notice of Inquiry

Models for a Governance Structure for NSTIC

22 July 2011








Submitted by:

Catherine Tilton
cathy.tilton@daon.com
703-984-4080

"Recipient of the 2008 Frost and Sullivan Best Practices Award for Product Strategy Leadership"

Submitted for:

Daon
11955 Freedom Drive
Suite 16000
Reston, VA 20190

Introduction

Daon is pleased to respond to this Notice of Inquiry regarding the NSTIC governance structure. Having been involved in identity management for over a decade, and as a potential participant within an identity provider, Daon offers its interest and the benefit of its experience. In addition, as one of the leaders of the Registered Traveler Interoperability Consortium, we offer lessons learned through this public-private partnership.

In addition, Daon actively participates (and holds leadership roles) in a number of standards development organizations (including ANSI/NIST, INCITS, ISO, and OASIS) and believes this experience can be applied to the question of governance and consensus across a range of stakeholders.

Registered Traveler Interoperability Consortium

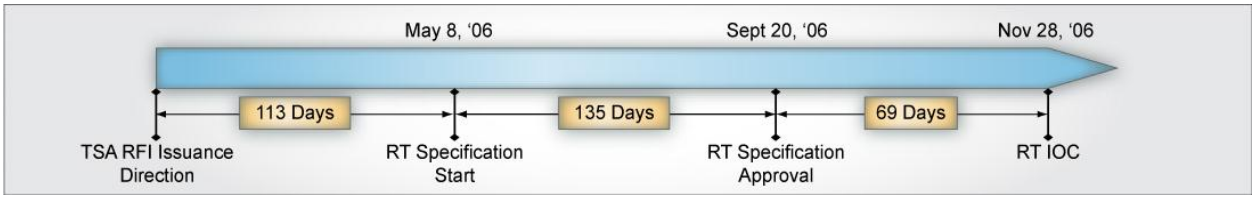
In 2005 there was a desperate need to reduce congestion in airport security lines. Airport operators, government, industry and the traveling public began calling for a "registered traveler" program that would enhance security by providing pre-screening of frequent travelers, and simultaneously produce a revenue stream for airports and service providers. Two of the key backers of the initiative were the Transportation Security Administration (TSA) and the American Association of Airport Executives (AAAE).

The Aviation and Transportation Security Act (ATSA) directed the US Transportation Security Administration (TSA) to "explore" options for expedited travel at airports where known travelers could be identified as not posing or not suspected of posing a known threat."

In mid-2005, the AAAE created the Registered Traveler Interoperability Consortium (RTIC) to define and establish the mutual and common business practices and technical standards that would complement federal standards and help push forward a national Registered Traveler program. The RTIC consists of over 60 airports, government agencies, and dozens of technology companies, system integrators, and service providers. As part of the RTIC, a service provider council was established which included a committee to draft the interoperable technical specification.

Areas of similarity between the RT and NSTIC initiatives are their security focus, use of similar technologies, and public-private partnership aspects.

Of interest is the speed at which the consortium performed its function. Below is a timeline of its activities and major milestones.



Jan. 23, 2006 RTIC reaches an agreement in principal for operation, governance, and interoperability of a US RT program. Agreement is endorsed by TSA.

May 08, 2006 RTIC adopts a model for operation, governance, and interoperability for US RT. The Model is endorsed by TSA. The RTIC begins work on the detail technical specification.

Sept. 20, 2006 The RTIC Technical Interoperability Standard is ratified by members and approved by TSA.

Nov. 28, 2006 The TSA issues an **"**Authority to Operate" for the AAAE Central Identity Management System and the US Registered Traveler program becomes operational.

Although the RTIC was successful in this regard, it was not without its lessons learned. Below are some of these that may be useful to the NSTIC effort.

- *Public-private partnership model worked*. In the case of RT, this allowed the leveraging of expertise and aggressive schedules of industry with requirements and oversight of government.

- *Consensus takes work*. However, having a broad cross-section of stakeholders who are willing to roll up their sleeves and allow for some give and take (i.e., compromise) led to the best overall specification.

- *Get the fighting over early*. Agreeing the broad principles and gaining broad alignment at the start of the process can take a lot of work but speeds the overall process.

- *Separate business requirements and technical design task forces*. Having clearly defined responsibilities within these groups helps prevent technical team members from debating/misinterpreting requirements.

- *Choose section editors and section teams carefully*. Align assignments to expertise areas.

- *War-room environment provided a focused focal point and maintained momentum*. Daily stand ups, with critical players present, resulted in fast identification and resolution of issues.

- *Active involvement of stakeholders critical to success*. Continual interaction with all stakeholders maintains program alignment

Response to Selected NOI Questions

The NOI posed a set of specific questions regarding NSTIC governance. Daon has chosen to respond to certain of these questions, as provided in the table below. Further thoughts can be on these and related topics can be found in the following section.

1.1. Given the Guiding Principles outlined in the Strategy, what should be the structure of the steering group?
First, it is important to define the larger context. All stakeholders comprise the NSTIC community of interest. Such a COI can be organized into a forum or consortium, to which each entity may obtain membership. This is the group from which the Steering Group (SG) draws to execute its functions. The SG should be composed of a set of officers + at-large members. Officers may include a chair, vice-chair, secretary/secretariat, etc. The size should be kept manageable – in the 9-15 range. Work of the SG should primarily be accomplished through working groups – a combination of standing groups and ad-hoc groups. For example, there may be working groups established for policy, architecture, interoperability standards, etc. Members of the working groups will include those from the COI membership. Chairs will be appointed by the SG. The SG should initially be appointed (by the President or his designee, e.g., Secretary of Commerce) based on a self-nomination and evaluation process, with a mixture of 2, 3, and 4 year terms. After the first term, SG positions will be filled by election (staggered 3 year terms) by the COI membership. The composition should be approximately 30% government, 50% private industry, and 20% academia/civil society. Initially, NIST should chair the SG (for a 2-3 year term), but afterwards the chair shall be elected by the SG. Further breakout of the private industry representatives can be made by sector, if desirable. See next section for more detailed recommendations that expand upon, or in some cases, provide alternatives to, the above.

1.8. What are the most important characteristics (e.g., standards and technical capabilities, rulemaking authority, representational structure, etc.) of the steering group?
The most important characteristics are vision and oversight. The SG must have a clear and committed vision as to what NSTIC and the identity ecosystem/framework will become and the management skills to drive it forward to reality.

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, as an early and significant adopter, should maintain a role in the SG for perpetuity; although that role may decrease over time (most likely to one member). Initially, the government will act as a catalyst for establishing the ecosystem and afterward will continue to ensure that the guiding principles are upheld.

It is right that government leadership come from the Department of Commerce, its role of facilitating commerce and its role in setting standards used by both government and industry. It may be useful to also have representation from one of the other government departments/agencies that are expected to be large users of the eventual NSTIC capabilities.

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 NSTIC vision of a working and thriving Identity Ecosystem is a huge undertaking. Government leadership is critical to the success of the strategy as it lends credibility as well as the early funding required for start-up. However, it is equally important that the private sector buy-in to the vision and believe that it is economically sustainable in the open market. Thus, it is important that the government be an early adopter to a) absorb the initial risk that comes with being that early adopter and b) create a market that other commercial enterprises will follow.

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

First, the government can take a strong role in ensuring that the identity eco-system is comprehensively defined, from a multi-disciplinary perspective, using solid system engineering principles.

Second, the government can facilitate the involvement of the broadest set of stakeholders.

Third, the government can institute pilot programs to prove out the concept and demonstrate that it works.

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?

As addressed in Question 1.1, the initial composition of the SG should be approximately 30% government, 50% private industry, and 20% academia/civil society, with the government representation possibly decreasing over time.

There are a number of roles in the identity ecosystem – citizens/consumers who are to be identified, relying parties/users/adopters seeking to verify identities for various purposes, and suppliers/identity providers who will offer identity verification products and services. These are represented by individuals, organizations, corporations, and institutions across many functional and vertical lines. A proactive role will be required to ensure that each has a voice and can participate in the process.

Key roles should be represented on the steering group, but that should not be the only means of participation. Each role is part of the community of interest and should have the opportunity to participate in working groups and provide input to key decisions. This may take the form of a membership vote on key specifications, such as technical architecture, interoperability specifications, or policy documents.

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

It is not practical for every stakeholder group to have a seat on the SG itself or it will become unmanageable. However, it may be useful to establish an ombudsman role such that each interested entity will have a voice. Also, key documents may be opened for public review and comment.

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?

One risk in this area is that only the very large corporations or industry sectors (i.e., the 800 pound gorillas) are represented and the voice of small businesses/sectors are drowned out. It may be useful for one seat on the SG to be held by a smaller business.

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?

Fees can act as a barrier to entry, particularly for individuals, small businesses, and non-commercial entities. If instituted, a tiered structure is desired.

Methods are desired to prevent influence being directly proportional to fees paid.

Besides fees, travel costs can be another barrier to entry, so use of electronic methods for meetings and balloting may offset this.

4.4. How should the steering group maximize the Identity Ecosystem's interoperability internationally?

Use of international, rather than national, standards should be adopted wherever possible. Liaison with these international standards development organizations (SDOs) may be useful.

In addition, with respect to steering group initiation, the NOI identifies three categories of formation – new organization, existing stakeholder organization, or use of government authorities. Although the latter two have the advantage of speed, they may also come with an existing structure, culture, and rules that bias the process. Therefore, creation of a new organization is preferred.

Further Thoughts and Recommendations

Below are provided some more detailed suggestions regarding NSTIC steering group principles, structure, and operations. Note that these suggestions imply heavy government involvement; however, we would expect this to decrease over time to eventual private leadership.

A. General Principles:

1) Must have private sector involvement/leadership but facilitated by government
2) Must be representative of key private sector partners and issues
3) Must have access to the President
4) Must have administration support for recommendations
5) Must have direct connection to appropriate standards bodies
6) Needs clear communications and collaboration strategies
7) Needs to be transparent
8) Needs to be a Committee with a subcommittee/WG structure and by-laws

9) Needs to have clear goals and timeframes with mechanisms for assessing how well they have been met
10) Congress should provide the first two years funding for NSTIC staff and operations (through Department of Commerce) in order to minimize bias and allow for quick start.

B. Steering Group:

1) Macro Steering Group needs a luminary leader, possibly from academia or a well-respected former political or industry leader. Could possibly have co-chairpersons. This person(s) is expected to be appointed for a two year term and exert strong leadership. Also need a strong Executive Director of this SG as a full-time position.

2) Representatives on the Steering Group could be from entities like (each entity can also supply one full-time staff person):

a) U.S. Chamber of Commerce
b) ACLU
c) Consumer Federation of America
d) National Governor's Association
e) Commerce Secretary/NIST Director
f) TechAmerica
g) American Bar Association
h) President's National Security Advisor
i) President's National Economic Advisor
j) National Small Business Association/Small Business Council of America
k) National Retail Federation
l) Consumer Electronics Association
m) Electronic Privacy Information Center
n) Purdue University/MIT/Carnegie Mellon University/UCLA/George Mason University/Harvard
o) American Bankers Association
p) Electronic Frontier Foundation
q) Digital Due Process Coalition
r) Consumers International/Consumers Union
s) U.S. Conference of Mayors
t) American Medical Association
u) Federal Trade Commission Director
v) UN/ISO/ANSI/OASIS
w) U.S. Chief Technology Officer/Chief Information Officer
x) The Financial Services Roundtable
y) Center for Democracy and Technology

These would be in addition to other private industry entities representative of the identity provider community.

C. Suggested Steering Group structure with potential Subcommittees* (each Subcommittee needs an external liaison to interface with other subcommittees):

1) Macro Steering Committee
2) Privacy Subcommittee
3) Standards and Interoperability Subcommittee
4) Legal/Liability/Accountability/Risk Subcommittee
5) Policy and Regulatory Subcommittee
6) Security/Compliance/Enforcement/Metrics Subcommittee
7) International and Governmental Subcommittee
8) Technology/Architecture and Innovation Subcommittee
9) Financing/Cost/Competitiveness/Small Business Subcommittee
10) Consumer Issues/Marketing Subcommittee

*Note: Subcommittees could be the formal component, with limited membership, with one or more working groups (with broader membership) reporting into it OR subcommittees and working groups could be synonymous.

C. Suggested NSTIC Staff Offices:

1) Administration/Finance/IT/HR
2) Public and Media Affairs
3) Committee Operations Support
4) Legislative Affairs
5) Member Relations and Business Affairs
6) Records Management
7) Legal

D. First Steps:

1) The President (or his designee) to designate a leader or co-chairs of the NSTIC Governance Group and appoint Government members to the Steering Group. Full SG membership should be limited to not more than 21 members. SG meets monthly for the first year.
2) Steering Group has final vote authority for issuance of all policy and regulatory directives. All policy directives must be voted affirmatively on by at least three-fourths of the SG with at least three-fourths of the members voting. Each directive can originate in any subcommittee but SG may direct appropriate lead subcommittee.
3) The President appoints initial government members of the Steering Group to two-year terms. Political orientation should not be a factor in any appointment.
4) Subcommittee members to be solicited by Federal Register Notice with final decisions for appointments by majority vote of SG. No more than 15 members on a

subcommittee. Each subcommittee member may bring one half-time staff person to help them.

5) Subcommittee chairs are initially appointed by the SG and later selected by vote of each subcommittee/WG. Terms are for two years unless removed by majority vote of SG with two or more SG members requesting a removal vote. Subcommittee members meet twice monthly for the first year.
6) Government to provide space for NSTIC staff and SG staff as part of two-year funding through Commerce.
7) Executive Director recruited and approved by NSTIC SG chair/co-chairs. Executive Director hires NSTIC office leaders.

E. NSTIC Operations:

1) All SG, subcommittee, and WG meetings open to the public and generally following the principles of the Federal Advisory and Committee Act (FACA).
2) All records, with the exception of security classified materials, should be open to the public through a website.
3) Recommendations or suggestions from the public should be welcomed at public meetings and through the website and tracked for internal accountability.
4) This is not a government organization so it is not subject to the Administrative Procedures Act or Congressional direction.
5) Members, committee/subcommittee and NSTIC staff will adhere to a code of conduct approved by the Steering Committee.
6) Parliamentary procedures will be used by the NSTIC Steering Committee and all subcommittees.
7) NSTIC may employ expert consultants if approved by a majority of the Steering Committee.
8) NSTIC should periodically self-assess its principles and operations with respect to its efficiency and effectiveness.

F. Linkage to Government Processes:

1) US Government needs to have a corresponding Principals Committee and structure to consider implementing regulations, directives and processes as well as proposed laws to follow NSTIC architecture.
2) Recommend to UN/ISO that they establish a liaison with NSTIC and consider if any of the NSTIC materials are suitable for input to or adoption as standards and to ensure NSTIC synchronization with other international efforts.
3) Ensure liaison with National Association of State CIO's and National Conference of Mayors for State and Local synchronization as appropriate.

Conclusion

Daon looks forward to receiving the report and recommendations proceeding from this NOI. We believe that the Identity Ecosystem envisioned by NSTIC will enhance the security of our G-C/B and B-C/B transactions and thereby facilitate both eGovernment and eCommerce.