July 21st, 2011

National Institute of Standards and Technology
c/o Annie Sokol
100 Bureau Drive
Mailstop 8930
Gaithersburg, MD 20899

Dear Sir / Madam,

The Jericho Forum® is a independent group of Chief Information Security Officers from leading corporations and other senior security professionals working together in a vendor neutral / vendor free environment to define the way forward to common Information Security problems facing us globally, based on the premise that corporations and users are becoming de-perimeterized (that is the notion that most corporate boundaries are becoming irrelevant as the need to collaborate takes precedence). This leads to the need for a de-perimeterized Identity Ecosystem, "Identity without Borders".

The Jericho Forum sees the problems of identity as key to solutions in this area and for the last year has spent its effort in defining the principles by which such a global identity ecosystem should operate. This we published in May 2011.

For practical purposes the Jericho Forum is run on a day-to-day basis as a forum of the Open Group (who will make their own submissions) but operates with a high degree of independence, based on the Jericho Forum heritage, through an elected board.

The Jericho Forum is very supportive of the NSTIC effort, and we are writing to provide input on behalf of the Board of the Jericho Forum to the NSTIC NOI.

The Jericho Forum "Identity Commandments" are provided in Appendix A of this response.

1. 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?

Jericho Forum Response:

The Steering Group should be comprised of people charged to provide both expert guidance, but also their independence from the many competing voices. Their remit should be to govern the provision of an open, globally implementable solution that will equally protect the rights of individuals and resource owners.

The Steering Group, however comprised, will need a very clear mandate, with clear objectives and goals (success criteria) defined, if is to navigate it way through the competing commercial and governmental, and social pressures to which it will be subjected.

We feel that the Structure of the Steering Group will need to change / evolve during the phases of the project; please see our response to 1.4 for a fuller explanation.

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?

No Jericho Forum response offered

1.3. Are there functions of the Steering Group listed in this Notice that should not be part of the Steering Group's activities? Please explain why they are not essential components of Identity Ecosystem Governance.

No Jericho Forum response offered

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?

Jericho Forum Response:

Based on the work on the "Identity Commandments" that the Jericho Forum has already published, here is what we believe are the key challenges (and missing pieces not listed in this notice) to being able to implement a fully workable identity ecosystem in line with the NSTIC vision, and our comments of what we think the Steering Group will need to do to deliver solution in these areas.
To explain our thinking we have illustrated each item, where necessary, with an explanation of the problem that needs solving / addressing;

1. *Identity encompasses not just people*
   In line with the ISO standard we believe that a viable ecosystem that can be properly leveraged to make risked based decision encompasses not just identity about people, but also organizations, devices, code and agents. Our work to date suggests that solving this for people (but mindful of the other types on entities) is 90% of the problem.
   ***We believe the Steering Group will need to sponsor and have access to an expert reference body to provide advice on how the identity ecosystem must work for all entities**.*

2. *Key solutions required*
   From the work already done by the Jericho Forum, we believe that there a number of key challenges that need to be solved for a viable ecosystem to evolve and be trusted, these are;

   2.1 Requirement for a switch in mindset from Enterprise Centric Identity and Access Management to a more inclusive and effectively protected User and Resource Centric frame, which supports a balance of User and Resource Owner Primacy. Without this mind-shift a solution on the scale that NSTIC envisages will not scale to three hundred million Americans, let alone globally.
   We believe the Steering Group will need to provide education to prospective solution providers to achieve this essential mind-shift in thinking prior to the proposal of solutions.

   2.2 A method of immutably binding the entity (typically a person) to their core identifier (probably their master private key).
   The Steering Group will need to set the parameters/requirements/goals for this device and we would envisage a competition, along the lines of the DARPA challenges, to develop prototypes.

   2.3 The definition of the cryptography required to mix the core identifier from the person (or entity) with identifiers from (say) the Inland Revenue Service to create new crypto that is recursive.
   We believe that all the fundamental cryptography exists, but the challenge here is a standard implementation that is recursive.
   The Steering Group will need to develop a requirements specification (with input from cryptography experts) and then we would envisage there would be an open, global competition, as was held for AES.

   2.4 The method by which a person would "claim" attributes about themselves, linking their core identifier to information held by 3rd parties (such as a Health Provider, Government Agency, e-Commerce provider or Credit Card Company).
   The Steering Group will need to sponsor work to identify standard methods for claiming identity attributes; this will form a core part of the identity ecosystem reference model.

3. *Goals for a viable identity eco-system*
   Whereas the initial NSTIC documentation provides the high level aspiration for the identity ecosystem there needs to be lower level goals or measure of success.
   The Steering Group will need to set and manage these goals, including;
   - *The principles by which any identity ecosystem would operate – we would commend the work already done the Jericho Forum in this area.*
   - *A series of goals or measures of success for actual design of the identity eco-system.*
   - *What a identity ecosystem reference model will need to look like, and how it will be managed (this in turn will help define/influence how the Steering Group will need to evolve into steady state)*
   - *How the pilot(s) will be managed / governed and a definition of the success criteria for those pilots*
   - *Goals for the governance of the identity ecosystem post implementation.*

4. *Finance and budgets*

   Specific budget expenditure capability enabling the Steering Group to fund the sub-projects and pilots, where required, to reach a steady state in the optimal time frame.
   The Steering Group will need to evaluate requests for funds, as well as provide budgets and monitor spending against those budgets.
   This will require the effective development of an economic and social environment which in turn would allow the growth of a successful business model that would fund the identity ecosystem

5. *Liaison, legal and international – stakeholder management*

   The Steering Group will need to work with the international standard and other bodies to enshrine the solutions into legislation, standards and defacto-standards.
   For example; work done by the Jericho Forum has identified the fact that (we do not believe) that a person has a right to a unique identity under the UN Declaration of Human Rights, this is probably critical if NSTIC is to meet its international aspirations.

6. *Evolution – freedom to manage its own destiny*

   Freedom to evolve into whatever type of (private) legal entity best meets the needs of the identity ecosystem and will achieve both the perception and actual independence desired.
   The Steering Group will need to reference and take advice from other similar bodies that have successfully made this transition.

7. *Patents and Reference Models*

   For the eventual identity ecosystem to be globally adopted, the solutions and reference model must be unencumbered from patents, licensing or any other restrictions.

   The Steering Group will need to ensure that anything proposed is unencumbered from any such limitation and must ensure that at the demise (or evolution) of the Steering Group that the IP behind the identity ecosystem is adequately held in trust for the community.

1.5. To what extent does the Steering Group need to support different sectors differently?

Jericho Forum Response:

It is critical that all sectors are able to provide input to the Steering Group and we acknowledge that the representative bodies for each sector will differ.

However, we believe that an identity eco-system, implemented correctly, will meet all these diverse needs and so the Steering Group should limit the support to ensuring that this is the case, rather than trying to tailor any identity ecosystem to working with any legacy solutions currently implemented by any one sector.

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?

Jericho Forum Response:

See our response to 1.5 above

Where conflict with rules or laws occur and the Steering Group feels such this compromises the goals of NSTIC then there may be their need to revise existing legislation or regulations, (US and possibly international) and it is here Government can assist.

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?

Jericho Forum Response:

See the response to 1.5 and 1.6

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

Jericho Forum Response:

See the response to 1.4, 1.5 and 1.6

Above all, the Steering Group must demonstrate consensus-driven governance and communication.

The Steering Group must be composed of individuals with established expertise and experience in relevant fields, ideally with cross-industry knowledge. The size of the Steering Group should enable flexibility and cross communications by global experts in an environment that is consensus, and not lobby, driven.

The work of the Steering Group should be completely open and transparent to the public. It must be balanced so that the agendas of any one sector do not dominate the legitimate interests and participation of any others. In particular there must be no perception that money (big lobby interests) buys votes or outcomes.

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?

Jericho Forum Response:

The government should be one representative with no greater or lesser vote/influence than any other participant

The Jericho Forum is aware of other (foreign) Government Initiatives in identity that insisted on the incorporation of closed code with the subsequent suspicion of "back-doors" leading to credibility failure and subsequent rejection by the public.

We would fully support the NSTIC aims of a public run identity service and the "light-touch" government involvement together with the stated aspiration for the Government role as a "philanthropic benefactor" providing seed-money.

2. Steering Group Initiation

There are many means by which the Steering Group could be formed, and such structures generally fall into three broad categories:

a) A new organization, organically formed by interested stakeholders.

b) An existing stakeholder organization that establishes the Steering Group as part of its activities.

c) Use of government authorities, such as the Federal Advisory Committee Act (FACA), to charge a new or existing advisory panel with formulating recommendations for the initial policy and technical framework for the Identity Ecosystem, allowing for a transition to a private sector body after establishing a sustainable Identity Ecosystem, or through the legislative process..

Questions:

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?

Jericho Forum Response:

We feel that option c) would be counter to the stated aim of NSTIC (and section 4 of this document) of fostering an identity ecosystem that can be adopted globally.

Both options a) and b) have merit, but the feeling is that a small Steering Group convened under "option a" which has the ability to utilize (or outsource) the services (say for sub-committees) of established groups ("option b") would provide the best option.

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?

Jericho Forum Response:

Provided the Steering Group's charter is set-up correctly we believe that it increases the likelihood of success.

*Government leadership can kick start this initiative so long as the Steering Group has appropriate representation and is open to input from **all** legitimate interested parties, see previous Stakeholder input).*
The implication of "Private Sector" leads to a concern that Individuals and Charities might not be effectively represented in favor of a primarily commercially driven steering group.

Further, this should include international representation to ensure that strategies developed encompass all the relevant cultural and regional needs.
The US Government should see itself as a philanthropic benefactor, neither leading nor directing, and during this initial phase should steadfastly resist any government from taking such a role.

The end-goal of the Steering Group must be to transition to a permanent structure, independent of government, which will manage and evolve the standards and IP behind the identity eco-system.

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

Jericho Forum Response:

First, *by providing the necessary seed capital, to be used by the Steering Group (with appropriate oversight).*

Second, *but the leveraging the expertise of external groups, especially those with an open heritage, such as the Jericho Forum, the Open Group, the Kantara Initiative, either for input to the Steering Group, or for out-sourcing sections of work to.*

Third, *by the use of open competition, allowing input from all interested parties, and importantly (where cryptography is concerned) the critical inspection of proposed solutions.*

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?

Jericho Forum Response:

During the establishment of the Steering Group, efforts by individual stakeholders or groups of stakeholders to dominate or control the group will have to be resisted. The use of transparent, representative and democratic processes is the best way to manage the risk.

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.

Jericho Forum Response:

The Jericho Forum was originally founded as an independent body and ran for about a year in that mode. Our eventual home of the Open Group was borne out of finding a body with similar aims and ethos that could provide a suitable home for the group. Experience shows that a period of "courtship" followed by a reasonably long "engagement" meant that both parties entered the final "marriage" arrangement with eyes fully open.

3. Representation of Stakeholders in the Steering Group

Questions:

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?

Jericho Forum Response:

Our experience in producing Jericho Forum output is that the actual work and decision are made by a handful of people, taking input and ideas from a larger group.

Thus a small Steering Group (under 10 people) with appropriate structures that allows input from the wider community would seem optimum.

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

Jericho Forum Response:

By input to one of the nominated sub-groups or sub-organizations or direct to the Steering Group, we would envisage that each of the key stages of development be open to input from all interest parties to formulate the goals and objectives (design principles) for each area.

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?

Jericho Forum Response:

Identify the different Stakeholders and ensure that there is an appropriate representation of these stakeholders. Based on recent work at the EURIM Identity Governance working group there are number of ways to classify Stakeholders;

By their Identity Role

- ***Principal(s)/(Requesting Party)*** *The entity that wants access to another entity (organizations, devices, services or individuals). (Goal: Reliable and often Secure Access)*
- ***Relying Party(s)*** *- (Resource Owner) The Entity that uses Attributes to make the access decision.*
- ***Identity Service Provider(s)*** *- The various service providers involved*
- ***Trusted Attribute Provider(s)*** *- The entities that have control over key attributes associated with other entities, and can verify claims related to these attributes.*
- ***Government****(s) - In their role of providing an regulatory environments that foster good practice and meet other national needs*

By their Type

- *Individuals, Commercial Enterprises, Charitable Enterprises, Governments*

All the Steering Group members (and other sub-group members) should be appointed for their balance, objectivity and expertise, and effective representation of the identified stakeholders.

Additionally all appointments should be made with the condition that if they are paid by a vendor, or have any vested interests, that those interests are declared and they recuse themselves from any vote where a perception of bias could be perceived.

All votes and decisions should be open and published.

The Steering Group should aim for consensus, and not "simple majority" voting.

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?

Jericho Forum Response:

No, not in the initial stages, to ensure there is no perception of paying for influence.

One of the goals for the Steering Group should be to work out an acceptable funding structure to enable the steady state organization to be self sufficient.

3.5. Other than fees, are there other means to maintain a governance body in the long term? If possible, please give examples of existing structures and their positive and negative attributes.

Jericho Forum Response:

See our response to 3.4 above.

3.6. Should all members have the same voting rights on all issues, or should voting rights be adjusted to favor those most impacted by a decision?

Jericho Forum Response:

Yes, but in reverse of what this question implies; any vested interest should be declared and the representative should recuse themselves from any vote.

See our response to 3.3 above for a fuller response.

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?

Jericho Forum Response:

There should be broad representation TO the Steering Group, but not necessarily broad representation WITHIN the Steering Group itself. See our responses to 3.1, 3.2 and 3.3.

4. International

Given the global nature of online commerce, the Identity Ecosystem cannot be isolated from internationally available online services and their identity solutions. Without compromising the Guiding Principles of the Strategy, the public and private sectors will strive to enable international interoperability. In order for the United States to benefit from other nations' best practices and achieve international interoperability, the U.S. public and private sectors must be active participants in international technical and policy fora.
No single entity, including the Federal government, can effectively participate in every international standards effort. The private sector is already involved in many international standards initiatives; ultimately, then, the international integration of the Identity Ecosystem will depend in great part upon private sector leadership.

4.1. How should the structure of the Steering Group address international perspectives, standards, policies, best practices, etc?

Jericho Forum Response:

The remit of the Steering Group should be the development of an Identity Ecosystem that can be adopted internationally (i.e. it would be a US-initiated strategy with international participation and contribution leading to a system that can be implemented internationally).

To this end, the remit, governance and composition of the Steering Group must commit to its eventual deliverables (be they standards, operating rules, MoU's, processes, etc.) being fully open with the standards and reference model held in trust for the community by an independent body (either a new body or a suitable existing body).

An example is the Open Group holding reference model for UNIX POSIX.

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

Jericho Forum Response:

Our belief is that standards and policy development organizations, trade organizations and foreign governments have vested interests in their current standards, solutions and the status-quo, none of which to-date have delivered a strong, trusted, global Identity Ecosystem.

Thus the current direction of listening to and taking submissions from all interested parties is the correct approach, however the resultant Identity Ecosystem will need to be new and radically different in approach (though we believe all the fundamental technology exists) from anything implemented today.

4.3. On what international entities should the Steering Group focus its attention and activities?

Jericho Forum Response:

Other key international groups are those involved in privacy, accepting that the concept of privacy, particularity for the individual citizen, is far more mature outside of the US.

This should probably involve embracing a fundamental design goal of "user centric identity" and the principle of the individual citizen being in control of their identity (please refer to the Jericho Forum "Identity Commandments" in Appendix A below), as increased control of identity for individuals (an NSTIC objective) reduces the sharing and exposure of data, and in this way fundamentally provides increased privacy protection.

Although, once personal information is shared, the need for privacy transcends national borders and privacy protections will need to be considered in this global context.

4.4. How should the Steering Group maximize the Identity Ecosystem's interoperability internationally?

Jericho Forum Response:

International interoperability should be a design goal for the Identity Ecosystem. If it can operate as a source of strong identities, trusted internationally, this will benefit governments, global businesses and global e-commerce.

We believe that the Steering Group should, as a priority, set a series of design goals that can be seen as being beneficial by the US government, other sovereign governments, global businesses, citizens and other interested parties.

We foresee some common goals that would gain international support, these being that:

- *(a) Global Governments can consume and trust a strong identity not issued by them;*
- *(b) Businesses will be able to consume and trust a strong identity not issued by them;*
- *(c) The standard for the Identity Ecosystem must be cable of being replicated in any country, meaning it is vendor and country neutral, and fully open;*
- *(d) All crypto used by the Identity Ecosystem must be fully open and royalty-free with publication of all cryptographic algorithms and code to ensure there is no suggestion of a back-door.*

We commend the example of the open competition for AES and a great example of openness fostering the adoption of a new strong crypto standard that rapidly achieved global acceptance and use.

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

Jericho Forum Response:

We foresee times when the fulfillment of the NSTIC goals may furthered by the funding of experts with specific knowledge and perspectives pertinent to NSTIC, to enable them to participate in the deliberations of the Steering Group or other activities of sub-groups, irrespective of location, country or willingness of the organization that may employ them to pay.

Ultimately this is about getting the right people, for the right role!

Thank you for considering our input to this important initiative. If you have questions regarding the Jericho Forum input to the NSTIC NOI our contact details are below.

Yours sincerely,

On behalf of the Jericho Forum Board

Paul Simmonds	Adrian Seccombe	Ian Dobson
Jericho Forum Board	Jericho Forum Board	Director, Jericho Forum
+44 1753 202 898	+44 1483 562471	+44 191 236 4102
paul@simmonds.org.uk	adrian@e-trust.org.uk	i.dobson@opengroup.org

Attached: Appendix A – Jericho Forum "Identity Commandments" – May 2011
https://www.opengroup.org/jericho/Jericho%20Forum%20Identity%20Commandments%20v1.0.pdf

"Identity" Commandments

The Jericho Forum® Identity, Entitlement & Access Management (IdEA) Commandments define the principles that must be observed when planning an identity eco-system.

Whilst building on "good practice", these commandments specifically address those areas that will allow "identity" processes to operate on a global, de-perimeterised scale; this necessitates open and interoperable standards and a commitment to implement such standards by both identity providers and identity consumers[1].

The IdEA commandments serve as a benchmark by which Identity, Entitlement and Access Management concepts, solutions, standards and systems can be assessed and measured. They are supported by a Jericho Forum IdEA Glossary and other related documents. They also build on the higher level Jericho Forum Commandments, in particular Commandments 2, 8, 9 and 10.

Identity and Core Identity

1. All core identities must be protected to ensure their secrecy and integrity

Core identifiers[2] must never need to be disclosed and are uniquely and verifiably connected with the related Entity.

Core identifiers must have a verifiable level of confidence.

Core identifiers must only be connected to a persona via a one-way linkage (one-way trust).

An Entity has Primacy over all the identities and activities of its personae.

Entities must never be compelled to reveal a persona, or that two (or more) persona are linked to the same core identity[5].

2. Identifiers must be able to be trusted

Identifiers must be appropriately unique and related to the entity's core identifier to enable a definable level of [system] trust of the entity to exist.

The identifier for a persona (even if serial pseudo-anonymous[3]) can be used to develop reputational trust of that persona; for example for credit transactions.

The identifier for a persona when linked to other attributes or other persona can develop contextual trust; for example linkage to government issued attributes / identifiers.

3. The authoritative source of identity will be the unique identifier[4] or credentials offered by the persona representing that entity

Entities have primacy over all linkages of their personas with their public identifiers.

The strength of the identity offered will define the level of trust that can be placed in the related persona, especially when a verified identifier or verifiable credentials are offered.

Multiple Identities (Persona)

4. An Entity can have multiple, separate Persona (Identities) and related unique identifiers[5]

A Principal or resource owner may choose when to create a Persona (Identity) and related Unique Identifier, and which attributes are connected to that persona.

---

1 Jericho Commandment #4 and #8 apply to ensuring open, secure and interoperable standards
2 A core identifier may refer to a physical, biological or digital entity
3 Serial pseudo-anonymity: guarantees the same entity in multiple interactions without being able to identify the actual entity
4 A 3rd party (e.g. organisation) may choose to create a shadow or internal identifier for an entity for internal purposes
5 We consider this as something that should be enshrined in privacy law; and/or in UN Declaration of Human Rights

Persona (including serial pseudo-anonymous persona) must inherit strong and verifiable sameness from the core identifier without compromising or exposing the core identifier.

Personas must be identifiable as unique, in the context of their usage and interaction.

An individual persona may use several distinct unique identifiers.

5. Persona must, in specific use cases, be able to be seen as the same

It must be possible for an entity to substitute one persona for their currently-interacting persona, without disrupting the trustworthiness of its relationships.

Multiple interactions with some third-parties may require that the interacting persona is consistent over time, and an entity cannot interact multiple times using separate persona. For example; in voting where an entity may only have one vote.

Persona (Identity) Attributes

6. The attribute owner is responsible for the protection and appropriate disclosure of the attribute[6]

The exposure of attributes must be minimized, as over-exposure allows the potential aggregation of attributes to link individual persona or to derive the core identity.

Attribute owners should only maintain attributes for which they are the authoritative source and/or that are directly relevant and necessary.

Attribute owners must ensure that attributes are accurate, relevant, timely, and complete and must delete attributes that are no longer directly relevant and necessary.

Attributes must be protected against loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

7. Connecting attributes to persona must be simple and verifiable

A persona is a collection of an entity's attributes and may be provided from different attribute providers (including certified or self-asserted attributes).

Entities must be able to link to attributes related to them, with one or more of their persona, from the authoritative source that holds the attribute (via a claiming process).

Attribute providers have a duty of care to the entities whose information they hold. In particular, they must assist entities who want to challenge and/or change and/or remove information held about them.

8. The source of the attribute should be as close to the authoritative source as possible

The originating source of a personas attribute is responsible for the accuracy [7] and maintenance of that attribute.

The principal or resource owner is responsible for the validity of any attribute it presents.

The receiving party should authenticate the persona's attributes and their relationships by reference to the attribute provider (authoritative source) of the attribute.

The receiving party should validate the persona's attributes with a relevant attribute provider and their trust relationships with that provider.

The receiving party is ultimately responsible for deciding upon the acceptable level of risk associated with the level of validation[8] of a particular attribute.

Certifiable attributes from a trusted source, must include the reference to their origin which can be used to validate the attribute(s).

[6] Much of this principle reflects the NSTIC "fair information practice principles" (fipps)

[7] EU Data Protection Principles # 4

[8] The strength of validation (and hence trust) may range from weak for a self asserted attribute to strong in the case of an authoritative source

Entitlement management and resource access

9. A resource owner must define Entitlement (Resource Access Rules)

Resource access rules should be simple[9] and minimal, thus ensuring attribute requests are minimized[10], and avoiding the over exposure of attributes from different persona[11].

Where resources have multiple owners each owner should be able to set their subset of rights.

10. Access decisions must be relevant, valid and bi-directional

Access must be granted based on rules evaluated using current (valid) attributes.

Attributes that have a temporal component may affect access and entitlement rules.

Requests for attributes should, wherever possible, use attribute derivation to minimize the exposure of attributes. For example: Are you 18?[12] Rather than request the Date of Birth.

If logging access decisions, the attributes together with the logic used at the time of the decision, and the outcome, should be recorded.

Entitlement rules may drive a (bi-directional) negotiation as part of a transaction set-up process, which results in access with reduced functionality.

Usage and Delegation

11. Users of an entity's attributes are accountable for protecting the attributes

Identity service users are responsible for balancing the need for privacy and transparency.

The retention (and/or caching) of attributes must be minimized.

12. Principals can delegate authority to another to act on behalf of a persona

The principal must be able to delegate only a sub-set of the persona being delegated.

The receiving Principal must be able to negotiate or decline such delegation.

The acceptability of delegation must be defined when defining entitlement.

The Principal must be able to revoke any delegation, and the revocation of the persona by the principal should automatically revoke any delegation of that persona.

In delegating authority, this should never allow the impersonation of the Principal.

13. Authorized Principals may acquire access to (seize) another entity's persona

The ability to seize a persona must be pre-authorized by the entity[13].

Seizure must be of individual persona and never indirectly through seizure of the core identity.

Seizure must have appropriate safeguards, and be reserved for cases when the entity is unable to give their consent; for example when they are unconscious, non-compos mentis, or dead.

Any seizure of another's persona must be logged and where possible should alert the affected entity prior to the instigation of the seizure.

14. A persona may represent, or be represented by, more than one entity

The entities in a collective body[14] have primacy over its persona, and thus its membership, activities, and disclosures.

The member of a collective body, operating with the persona of the collective body, can be identified, and trusted, by other entities. This applies even if the membership of the collective body is secret.

A persona representing multiple entities should be clearly identifiable as a collective persona.

---

9 Jericho Forum Commandment #2

10 EU Data Protection Principles # 3

11 Risk: Over exposure allows the potential aggregation of identities to derive the core identity

12 The correct way is to query "were you born before [today's date – 18 years]"

13 This accepts that, for example, non-preauthorisation of a healthcare record may result in the death of the entity

14 A collective body consists of a collection of entities (e.g. corporation, family, help desk) that operates with a single (collective) persona

Conclusion

The shift from Enterprise and Application or System Centric *Identity and Access Management* to User and Resource Centric **Identity, Entitlement and Access Management** holds the triple promises of Lower Cost, Higher Security/Trust and Increased Flexibility. These benefits will have a major positive impact on the way the world will innovate and trade. The new frame must however be managed with the context created by these Commandments to gain these benefits.

There is also a major infrastructure investment required to create the next generation "Identity" Management approach. This investment in turn requires a shift in the business model and the enthusiastic uptake of the services that will encourage a cultural shift that will value Transparency as much as it does Privacy. Open access to the reputation of entities will go a long way to raising the e-Trust barrier.

Definition of Terms Used / Glossary

Attribute An observable property of an entity.

Core Identity A unique physical, biological or digital entity, which has exclusive use of the associated core identifier and understands the linkage to any associated persona.

Core Identifier Immutable and secret means which uniquely identifies an entity.

Credential Immutable combination of Verified Identifier and Verified Attributes.

Entity Any person, organization, computing device, code, data, or physical possession; also any self-managed collection or organization of entities.

Entitlement A usage right for a resource owned by some other entity.

Identity Synonymous with persona.

Identifier An attribute of a persona which identifies it, with sufficient uniqueness and immutability, that its trustworthiness can be assessed in a known context.

Persona A user-centric term. An entity uses a persona to represent an aspect of itself (such as, parent or employee and client or a server) through a collection of attributes, in any interactive situation.

Primacy The state of being first (the most important), where you are in control of your identity.

Principal Entity whose identity can be authenticated (standards: X.1252, ISO 29115).

Resource A service which its owner can provide to another persona.

Trust An entity's confident reliance on the outcome of an interaction.

Verified Attribute An Attribute that has been assigned to an entity by a trusted third party.

Verified Identifier An Identifier that has been linked to an entity by a trusted third party.

These definitions are clarified and expanded in the Jericho Forum Identity Glossary.