\NSTIC\IDESG\IdentificationrequirementsV9.doc

NSTIC: Healthcare Identity Ecosystem Steering Group

Identification Requirements

Version 9.2~~1~~.2~~1~~, 7/23~~2~~/15

Initially shared 5/13/15

Introduction (no comments shared 6/11/15)

This document represents a restatement of identifier and identification system requirements for discussion by the Identity Ecosystem Steering Group (IDESG) which is a component of the National Strategy for Trusted Identities in Cyberspace (NSTIC).

> *"The Identity Ecosystem envisioned in the NSTIC is an online environment that will enable people to validate their identities securely, but with minimized disclosure of personal information when they are conducting transactions."*

This document separates identity requirements into those that apply specifically to the identifier and those that pertain to the automation system that supports and manages those identifiers.

Preamble **(New Comments inserted from the prior version of the preamble in April 2015)**

in an increasingly electronic environment, accurate identification is essential. Domains as diverse as government, finance, retail and healthcare all have critical dependencies upon accurate determination of individuals and systems in order to ensure proper operation and avoid doing harm. Despite this common need, no uniform, consistent and reliable mechanisms to establish, represent and verify identity have reached consensus acceptance. There does appear to be wide agreement, however, that a properly implemented identifier system would represent a major step toward achieving the objectives of an identity ecosystem. The goal of this document is to establish the requirements which any proposed solution to this deficiency must meet.

Privacy and confidentiality issues must first and foremost respect and address the individual patient preferences in any consensus statement that lists requirements for identifiers in an identity management system.

Comment [BH1]: From Tom Sullivan, accepted

-

Relying parties will determine (subject to relevant state and federal law) the Level of Assurance and what strength of authentication will be either sufficient or necessary for the different types and content of online transactions that are envisioned according to applicable regulations and internal policies. Examples of different content may include psychiatric data, genetic information, sexually transmitted diseases, etc. (sensitive content), as opposed to a request for an appointment change, some educational material or a very generic query.

Comment [BH2]: (subject to legal requirements)???

Comment [T3]: I inserted the phrase "subject to relevant state and federal law" after the word "determine" based on comments from Barry and others during g the call. Tom

Comment [BH4]: From tom Sullivan, accepted

Scope **(no comments shared 6/11/15)**

This set of requirements is intended to apply to any solution or set of solutions that are proposed as a general method to address identity requirements in cyberspace. Requirements are listed both for identifiers and for the systems that support those identifiers. Note that the focus here is on identification. Related activities such as authentication, while critical to the proper functioning of an identity ecosystem, are outside the scope of this document. [Readers: Because the following lists are complex and sometimes long I have decided to alphabetize them based on the first word. The order of the requirements is not in any way meant to indicate relative importance or any other organization.BH]

During the initial discussion there was a request for key terms with supporting definitions. The source: the "Common Criteria", Part 2, Version 2.1, Published August 1999, (Dr Tom again thanked Judy Fincher for her input and assistance on the definitions).

Key Terms and Definitions for discussion: NEW (6/11/15)

Unlinkability: Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together. Unlinkability differs from pseudonymity that, although in pseudonymity the user is also not known, relations between different actions can be provided. The following comment was shared: the use of different identifiers with different system engagements does not enable linkability nor does the use of the same identifier with the same system. However, if the identifier is used with multiple systems you can have linkability

Anonymity: Anonymity ensures that a subject may use a resource or service without disclosing its user identity. This ensures that the identity of a user is protected from disclosure

Pseudonymity: Pseudonymity ensures that a user may use a resource or service without disclosing its identity, but can still be accountable for that use. The user can be accountable by directly being related to a reference (alias) held by the TSF, or by providing an alias that will be used for processing purposes, such as an account number.

TSF – Total Security Function PP – Protection Profile ST- Security Target

For greater definitions and explanations in detail, see the minutes of our 6/11/15 call

Desirable Properties **(has been reviewed with input reflected on a line item basis)**

This is a list of desirable properties that should be kept in mind when evaluating various possible implementations of an identifier system.

1. Cost effective – Expenses relating to the identification system must be kept to a minimum.
2. Efficiency – Definitions, operations and functions must be as efficient as possible to yield a maximally effective identity ecosystem.
3. Integration – Integration of the identification system into existing IT systems must be as easy as possible.
4. Personal empowerment – The individual must be empowered to the greatest extent possible to make decisions concerning their own identity.
5. Privacy enhancing – The identification system must improve the ability of each individual to manage the privacy of their own information.
6. Simple – The identity system must be structured to maximize simplicity in both definitions and operations.
7. Trusted – All participants must be able to trust that the identity system will function properly.
8. Unlinkability – A user of various independent sessions cannot be linked to determine it is the same individual.

Comment [BH5]: 1.BH: Jim K: should take into consideration ONC 's near term requirements i.e. FHIR, HL7, FIDO alliance that now includes NIST; "Ken Kingenstein – (not on call) who represents Internet 2.0, a NIST grantee, openly commented that " FIDO is not yet mature but has potential" ref: Mark C; the goal is access device flexibility

Comment [BH6]: Edits by BH

Comment [BH7]: **Judy Fincher –the term is defined in Common Criteria BH = Judy Fincher, the user of various sessions cannot be linked; is this required in healthcare? Is this an identifier property? Or a problem with in a system – two sites are not able to link but they both know the person - there is an internal linking but not an external linking --- the authentication identity is OK but linking to the patients identity is not; patient can present at both locations with an unlinkable identity .**

Identifier Requirements

1. Abstract – Nothing in the identifier should reflect a dependence on specific properties of the associated individual or object.
2. Anonymization – Identifiers can be used for both identifiable and **non-identifiable purposes BH - omitted anonymous. Blinding is a method**
3. Capacity/scalability – The identifier must be capable of covering the associated item population for an indefinite number of years
4. Compact – The identifier should be as terse as possible. (Allis is a Pseudonym)
5. Counterfeit resistance – A thief cannot arbitrarily create valid identifiers….being modified). BH – do aliases relate to this? **Resilience is a related term that means the identity can be recovered and re-established even after theft or compromise.**
6. Deployable – The identifier must be of a form that can be deployed across a variety of media including bar codes, smart chips, printed forms and magnetic strips.
7. Domain specificity – **The identifier must indicate the nature of the item it identifies – person, device, report, concept, etc. [Does this contradict requirement #1???] new-inserted by BH *Mark is on a device MDISS.org and can lend input***
8. Flexible – The identifier can support both manual and automated processing.
9. Globally unique – Each identifier must be guaranteed unique when it is issued.
10. Language independent – Nothing in the identifier should represent a dependence on a specific language.
11. Privacy – **The identifier should indicate the basic privacy constraints concerning the associated information. BH??**
12. Standards-based – The use of a standard enables maximum adoption by avoiding competitive issues that arise if a proprietary solution is established.
13. Unambiguous – The printed representation of the identifier should not contain unclear entities such as the ability to confuse the letter o with the digit 0.

Comment [BH8]: We should discuss the bolded highlighted items at the next meeting

14. Uniform syntax – Each identifier should conform to the same syntax specifications.
15. Universal – The identifier should be applicable to both persons and nonhuman objects….to be change subjects objects environments **BH- Robin – Ann, others have objects, "subject and objects", Ann RR. Non-person, device reports, sensor data need to be defined** ***Robin also comments that we will need to identity the interface factor*** Verifiable – The recipient and all users of an identifier can verify that it is valid.

Identifier System Requirements

1. 100% accurate – Proper use of the system should enable 100 % accurate identification for 100% of the participants.
2. Anonymous use – An identifier should be able to be used to represent an anonymous (pseudonymous?) individual. **BH TES** to discuss?**
3. Authentication capable – It must be possible to augment the identification system with a variety of authentication techniques such as biometrics and knowledge based authentication.
4. Break the glass – It should be possible to override anonymous operation of an identifier for specified situations (such as medical emergencies or law enforcement) and to restore anonymity when that situation has been resolved.
5. Compatible with existing IT – To the extent possible the identifier system should build on existing IT capabilities rather than forcing them to be replaced.
6. Continuous availability – The identification system should be available on a 24 * 7 basis.
7. Cost effective – The identifier system should be designed to be as inexpensive as possible while providing the maximum value feasible.
8. Efficiency – All identifier operations should function efficiently despite the complex distributed environment where the identifiers are used.
9. Error tolerant – In any complex system mistakes will happen. Replacement of an identifier to correct an error situation should be rapid, easy, and supported across the network.
10. Decentralized operation – The identification system must be sufficiently distributed to ensure that it is not susceptible to single-point-of-failure incidents.
11. Data location – The identifier system should track the 'locations' where each identifier has been used.
12. Future proof – To the extent possible the identification system must be able to adapt gracefully to new functions and new requirements that were not foreseen at the time the system was created.
13. Language independent – The identification system should be deployable across all languages
14. Incremental – To the extent possible the identifier system should be additive to existing IT systems rather than replacing them.
15. "Lifetime" validity – With the exception of dealing with error situations, it should not be necessary for an identifier to be invalidated.

16. Minimal personal information – The operation of the identification system must be designed to keep to a minimum the amount of personal information required for correct operation.
17. Multiple identifiers – There may be circumstances which justify the issuance of multiple identifiers to an individual.
18. Multiple privacy paradigms – The identification system should be able to provide concurrent support for a variety of different privacy paradigms.
19. Network-based operation – Identifiers will be used across an arbitrary variety of distributed locations. Identifier activities (creation, tracking, management, etc.) must function properly in this distributed environment.
20. Non-repudiation – Significant identification actions must be recorded in a manner that cannot be refuted.
21. Permanent – The identification system should intentionally avoid capabilities that might lead to the reuse of identifiers. Once assigned, an identifier remains with its associated object "for life".
22. Person empowering – The identification system should maximize individual choice rather than imposing top-down restrictions.
23. Privacy enhancing – Use of the identifier system for humans must be under the control of the involved individual and should enhance rather than degrade that person's privacy.
24. Progressive deployment – The identifier system must be able to deliver value even when only part of the target population has received identifiers. It should not be necessary for the identifier to be fully deployed throughout a population in order to gain benefit from the system.
25. Readily deployable – The technologies used in the identification system should be readily available, inexpensive, easily understood and reliable.
26. Real-time operation – New identifiers can be issued whenever needed and in a matter of seconds.
27. Replacement – If an identifier is terminated it must be easy to install a replacement identifier.
28. Security – Use of the identification system should enable improved security and should not entail any activities that diminish security. Techniques such as encryption must be used to offer the maximum security possible.
29. Simplicity – The identifier system and its operation should be as easy as possible to understand and to use.
30. Termination – There must be an invalidation mechanism which permits any identifier to be rapidly and permanently deactivated.
31. Time-stamping – The identification system must keep track of the date and time when significant identification events occur.
32. Unique – No identifier is ever reused. The system must provide a "functionally unlimited" [1] number of identifiers to ensure that reuse is not required.
33. Universal – Any person or object with a valid need should be able to receive an identifier.

34. Usable – The identifier must be readily processed in both manual and automated systems.
35. Voluntary and mandatory deployment – When used for humans, identifiers should be deployable in both voluntary (each individual decides whether to receive an identifier) and mandatory (each individual is issued an identifier) methods.

Other Requirements

This is a set of other requirements gleaned from previous material that I believe need further discussion before we decide whether to include them in the document.**[BH]**

1. Patient safety despite data fragmentation using clinical decision support. **[BH - Too healthcare specific?]**
2. Support all sectors – The system should support all sectors of the U.S. market.
3. **……..?**

Additional Comments

- "Known to the practice" (healthcare) – Proper use of an identifier means it is stored in the local organization's EMPI system. When a person presents an ID that is present in the local EMPI then that person is by definition "known to the practice." If the ID is not present in the EMPI then that person is not known to the practice.
- Patient safety (healthcare) – Privacy in healthcare may be achieved through the use of multiple identifiers by an individual to segment their medical information. For such individuals patient safety must be enabled through the use of clinical decision support which has visibility to all of the identifiers being used by that individual.
- Maximize local operation – A properly implemented identity system will enable most operations to be accomplished through interactions at the local level. Only rarely will centralized identity services need to be accessed.
- Anonymous patient matching – Patients may choose to be anonymous in order to keep some of their sensitive associated information private. Alternatively, organizations may choose to anonymize data for reporting purposes such as public health, research, education and the like.