"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 minimised, 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 minimised[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 minimise 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 minimised.

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

- The ability to seize a persona must be pre-authorised 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, organisation, computing device, code, data, or physical possession; also any self-managed collection or organisation 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.