The Design Principles of Relationship Management

Version: 1.0

Date: 25 February 2015

Editor: Ian Glazer and Joni Brennan

Contributors:

The full list of contributors can be referenced here:
https://kantarainitiative.org/confluence/display/irm/Participant+roster

Status: This document is a **Kantara Initiative Final Report**, created by the IRM WG (see section 3.9 and 4 of the Kantara Initiative Operating Procedures)

Abstract:

This report discusses the Design Principles of Relationships and in the context of Identity Relationship Management. The Design Principles of Relationships have been generated as a result of industry discussions inspired by the Pillars of Identity Relationship Management.

Notice:

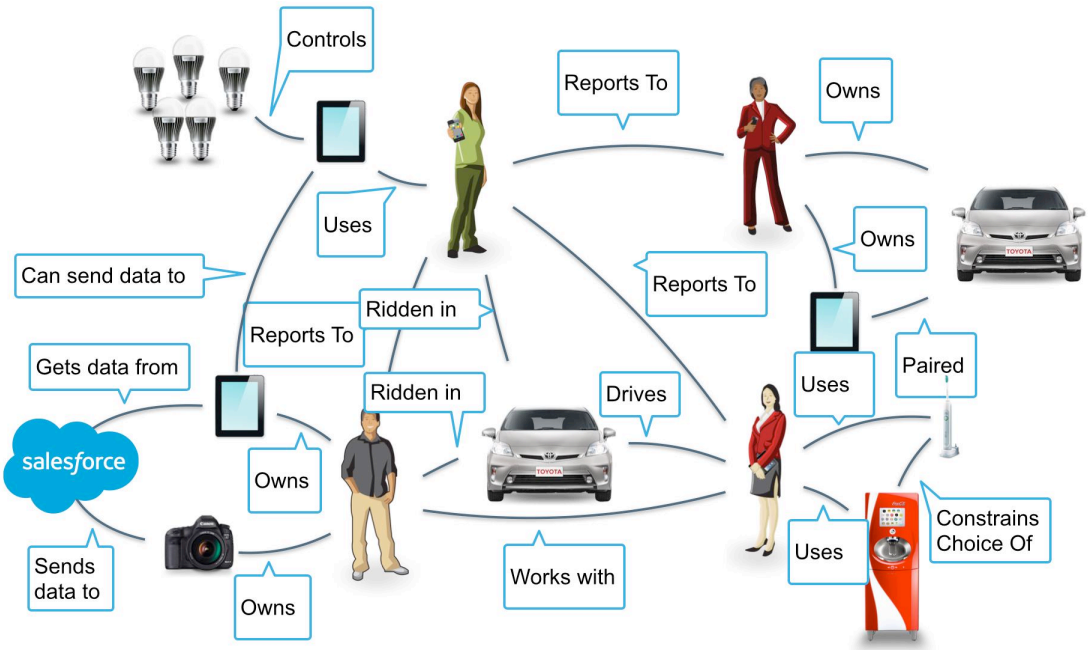
Contents

1 THE CHALLENGE JUST AHEAD

The identity and access management industry and its professionals are used to dealing with reasonable numbers of people with reasonable numbers of attributes. A classic example is employees in an enterprise setting. The enterprise has at least one authoritative source for employee identity and those identities have a few dozen attributes. Using that information, IAM systems and professionals can then begin to grant access, segregate duties, and manage user lifecycles. We have experience in handling these types of scenarios as they grow and evolve. Currently, the identity industry is primarily optimized for these scenarios.

In the near future, however, the industries current optimizations will not be sufficient. Our world is becoming one dominated by an unreasonably large amount of "things." From smartphones to connected-device laden homes to industrial sensors, the number of actors and the connections between them in the world of identity is growing at a geometric rate. Unfortunately, that growth has not been mirrored by innovation in the identity industry. The current policies, technologies and processes that govern identity management, cannot handle this changing landscape.

Finally, as things and human identities start to bind to each other, we end up with an unreasonably large number of relationships among an unreasonably large numbers of people and things, each with sets of attributes.



A world like the one depicted in the previous illustration is neither fantastic nor futuristic. It is the near future of our world. This Working Group posits that the identity industry's prior knowledge, techniques, and tools are necessary but not sufficient to solve for the problems that this near future poses. We believe that additional thought and approach is required; we offer *identity relationship management* as an additional approach to the identity industry.

1.1 Purpose and Audience

The principles in this document specify the meaning and function of relationships as a component of digital identity services. They outline what relationships need to represent and how they need to behave to maintain the integrity, coherence and utility of identity services at Internet scale. The initial goal of the document is to serve as a conversational substrate to capture evolving concepts around Identity and Access Management (IAM). The ideal goal for the document is to inform design principles for consideration and adoption and in doing so leverage Kantara Initiative process and programs broadly applicable to any innovative IAM approaches.

This document is presented as a report to the Kantara Initiative for consideration in its discussion group, work group and program efforts.

The document is also intended as a public resource for:

A. "Traditional" identity professionals curious as to how IAM could work at Internet scale, in an inter-federated world, while serving the needs of people, "things," groups, and organizations.
B. Designers, engineers and authors developing new systems, protocols and standards.
C. IT and business professionals planning and operating services within organizations and on the open market.

1.2 Why Develop "Design Principles?"

This report introduces design principles and questions meant to provoke thought and research regarding the future of Identity and Access Management in the context of the Pillars of Identity Relationship Management. In some sense referring to what follows as a set of design principles captures the aspirational notion of this Working Group; we are in search of basic principles, characteristics, and natures of relationships - things that are true and consistent.

This Working Group has formed not as an indulgence to our philosophical nature but to help the identity industry and its professionals to:

- Validate project scope
- Inform design
- Test existing solutions
- Identify gaps in existing architectures and deployment models
- Establish design patterns for IRM solutions
- Estimate complexity of implementing and/or migrating to an IRM solution
- Propose migration roadmaps

2 THE DESIGN PRINCIPLES OF RELATIONSHIPS

What follows is a point in time glimpse at Relationships and their characteristics. It is the full intent of the Identity Relationship Management Working Group to continue to refine and evolve the notion of Relationships and the associated characteristics. The Design Principles are meant to hearkening back to Cameron's Laws of Identity[1]. These Design Principles are not presented on stone tablets, eternally fixed, but on still wet clay tablets yet to be baked.

Although the following design principles describe a relationship as a connection between an individual actor and another individual actor (e.g. one person in a relationship with a single thing), the Identity Relationship Management Working Group is and will continue to be as inclusive as possible to all use cases. In this context, although the examples describe relationships between individual actors, the design principles must be able to describe and inform scenarios involving groups of actors in relationships with other groups of actors.

Similarly, although the following design principles tend to discuss person-to-person interactions and relationships, these design principles of relationships must be just as applicable to "things." Regardless of whether the Reader is considering a system of carbon- or silicon-based life forms (or more likely a mixture of both), these design principles need to be useful and relevant. That being said, it is likely that some of these design principles will have different implications depending if the relationship in question is person-to-person, thing-to-thing, or person-to-thing. The Working Group leaves the study of those nuances for later work.

Finally, this presentation of the design principles is not meant as an evaluation tool for conformance to the notion of Identity Relationship Management. The design principles are a set of design choices, not a prescriptive list of mandatory items. At this stage, it is more important for the Reader (and the identity management industry) to consider, challenge, improve, and hopefully adopt the design principles of relationships than it is to prematurely define and enforce conformance.

2.1 Scalable

Relationships must be scalable. More specifically, the model for relationships and management of relationships must be scalable. Where identity and access management has been comfortable dealing with millions of objects each with dozens of attributes, the number of relationships traditional IAM has had to manage has been fairly low. First with mobile computing and now the Internet of Things, the number of relationships IAM systems and professionals will need to

design for and manage will increase at a geometric rate. A ten million object directory will look quaint in a world of billions of "things" involved in trillions of relationships.

The notion of scalability in the world of Identity Relationship Management must cover four things:

- Actors
- Attributes
- Relationships
- Administration

The first three (actors, attributes, and relationships) are what the identity industry has grown to do well - accommodate more: more roles, more people, more systems. However the geometric increase in the number of actors and associated relationships will put a burden on existing administrative tools and techniques that the identity industry heretofore has never had to deal with. A world of relationships will require new thinking on the user experience, methods, and analogies presented to people to aid their attempt to manage their increasing complex world.

2.2 Actionable

Relationships must be actionable. We want relationships that are able to do something of value and, more specifically, relationships that can carry authorization data. However, relationships are not required to carry authorization data. The key is that they have the ability to do so.

In a traditional IAM scenario, we pass actionable information to the back-end for a classic request-response authorization model. But in an IRM (and IoT) world we must design for situations in which there is little to no connectivity to a back-end authority or that a back-end authority simply does not exist.

2.3 Immutable

Relationships can be immutable. Immutable relationships do not change. Immutable relationships may provide the ground layer for assurance in the grand scheme of Identity Access Management. Immutable relationships provide important contextual information. Immutable relationship examples might look like:

- This thing was made by Apple.
- This thing was built by Tesla.

It is crucial to observe that only some relationships are immutable. Immutable relationships are found in supply chain and industrial settings. However outside of settings such as those, most relationships are not, cannot, and should not be

immutable. “The future is unwritten,” as Joe Strummer said, and IRM and these design principles must not prevent the growth and transformation of relationships over time.

2.4 Contextual

Relationships can be contextual. More accurately stated, some relationships can be “triggered” by changes in context. Changes to conditions external to the relationship can have bearing on both how the actors in the relationship behave as well as what an external party can observe about the relationship.

Consider this example scenario: Before traveling abroad, I contract with a mobile network operator (MNO) to get a SIM card that will allow my phone to work at my destination. Until the SIM card via my phone connects with and pings a cell tower the relationship is inactive. The MNO doesn’t bill me for my usage because there’s been none. Once my phone with the SIM in it activates the relationship (by connecting to a cell tower at my destination) then the relationship between me and MNO springs into action and I begin to be billed for my usage.

2.5 Transferable

Relationships can be transferred. A transferable relationship is one in which one party in the relationships can be substituted for another. That substitution can be done on a temporary basis or permanently.

2.5.1 Temporary

A relationship and certain related attributes are temporarily transferred from one actor, entity, or device to another. These scenarios should be familiar for people working with delegation use cases.

Example: I am a client of an organization. I might want to delegate my abilities to some one else. I may seek a lawyer to draw up a Power of Attorney agreement to delegate a specified authority from one actor to another. Alternatively I can choose to remove or revoke that delegation and the transfer of authority for the relationship goes away.

2.5.2 Permanent

A relationship and certain related attributes are permanently transferred from one actor, entity, or device to another.

Example: I own a set of jet engines. I want to sell them to a client. I permanently transfer the ownership to someone else. In the real world, I would hand over the

title. In the digital world, stakeholders may seek a strong cryptographically protected flow to prove the relationship transference and context.

2.6 Provable

Relationships must be provable. In order to demonstrate to an external party that a collection of things and people are connected, there needs to be some mechanism to prove the existence of a relationship or set of relationships. The ability to prove the existence and nature of relationships improves trust between parties, provides auditability and traceability, and potentially reduces asymmetries of power.

2.6.1 Single-party Asserted

A single-party relationship is asserted by a single-party. For example, I may claim to work for Joni. In the single-party asserted scenario only one of the parties in the relationship makes such a claim. In that sense, a single-party asserted relationship feels a bit like a self-issued SSL certificate.

2.6.2 Multi-party Asserted

Multiple-parties assert that the relationship exists. For example, I claim that I work for Joni and she claims that I work for her. In the multi-party asserted scenarios all participants make associated claims that back each other's up. If I claimed to work for Joni and she says that I don't, then in the eyes of an external observer, I may or may not work for Joni. One could imagine a resolution process much like PDP-chaining in XACML version 3.0.

2.6.3 Third-party

Third-parties assert that the relationship exists. For example, human resources claims that I work for Joni. In this case, the external observer treats the statement from human resources as authoritative. Human resources is acting, to some extent, like an identity proofing service for the relationship - a relationship proofing service.

Social networks can act as relationship proofing services and the same is true of law enforcement databases that track known associates. An area worth exploring is "what are the IoT equivalents?" Will home automation companies become the "Facebook" of our things?

2.7 Acknowlegeable

Relationships can be acknowledged. Participants can acknowledge that they have relationships to other actors. In this regard, the acknowledgeable characteristic of relationships feels very similar to single-party asserted relationships. A question worth asking is, “Must all parties in a relationship acknowledge they are in a relationship?” In a situation where only one party knows of the existence of the relationship, then there is an asymmetry of power. The party that knows about the relationship can exert some form of control over the other party. For example, credit bureaus acknowledge their relationship to me but do I acknowledge my relationship with them? Similarly, I acknowledge that I have a relationship with Twitter, but do I acknowledge my followers? Do my followers acknowledge a relationship with me?

It is interesting to note that rewriting the first sentence of the previous paragraph to read, “relationships must be acknowledged by other actors” leads to a discussion of Vendor Relationship Management scenarios and techniques. It also leads to questions of personal sovereignty and data ecosystems.

2.8 Revocable

Relationships must be revocable. Identity and access management professionals understand revocation in terms of credential management. However, the common practices around data generated by relationships are less commonly understood. This concept of revocability is also related to developing legal approaches such as the Right to be Forgotten. This is the combination of asymmetry and the ability or lack of ability for a data subject to remove personally identifiable data.

Consider that I mistakenly destroy my phone. It was paired to my rental car. What happens to the data the phone passed the car’s entertainment system? Should the next driver be able to see the calls I made?

Another example from the Internet of Things: I install a smart thermometer in my home. It learns about my family’s preferred temperature and over time has saved us money by more efficiently managing the heating and cooling of the house. When we sell the house should the information be available to the new owner? Would I need to give the new owner my account information to the smart thermometer’s web site?

Other questions that require further consideration include:

- Can either party revoke a relationship?

- If I sever a relationship should any party who was part of the relationship still have access and use of what was shared in the course of the relationship?
- Does this imply the idea of cascading deletes?

2.9 Constrainable

Relationships must be constrainable. All behaviors and allowable actions associated with a relationship must be able to be constrained based on the desires, preferences, and even business models of the parties involved. In some cases, the constraints applied to a relationship looks like consent. For example, a person may allow her device to report its location with her explicit consent. In other cases, the constraints behave like Digital Rights Management (DRM) rather than consent. For example, a device may only function if the owner still has a valid license. It is important to note that although the Working Group believes that relationships should be constrainable, it does not yet have an answer for the question, "What happens when each party attempts to constrain a relationship in conflicting ways?"

3 CONCLUSION

This report has discussed the initial development of Design Principles of Relationships. The Design Principles of Relationships have been generated as a result of industry discussions inspired by the Pillars of Identity Relationship Management. The report has visualized some early problem spaces for consideration with regard to the relationships of people, things, and entities as well as the potential effects of the summation of data generation..

This report represents an entry in to high-level strategic, policy, and technology review and research around the implications of relationships and their design principles, types and axioms. This report is not conclusive but rather it is an attempt to provide a substrate for further industry development.

The report asks for industry to comment and test the Design Principles of Relationships with regard to the following considerations:

- Internet of Things
  - Industrial settings (factories, planes, etc)
  - Citizen (smart homes, sensors in public)
- Familial Relationships
  - Insurance
  - Healthcare
  - Finance
- National Identity Programs

This report asks industry to engage in conversation regarding the evolution of identity, and its intersection with Internet of Things (IoT) along the crucial triad of security, privacy, and usability.

Further discussion and research regarding the topics discussed in this report are developing within the Kantara Initiative Identity Relationship Management Work Group. Future items the Work Group is considering investigating include:

- Guides that describe Identity Relationship Management within the context of different industries and different stakeholders
- Analysis of types of common relationships such a guardianship, citizenship, and ownership and the implications to the design principles
- Formalization of the design principles of relationships, an evaluation tool to determine if a system conforms to the law of relationships
- Notation system to concisely describe relationships
- Metadata language for informing participants as to the constraints and allowable actions associated with a relationship

Please join the work group to share your value and contribution to the initiative.

4 REFERENCES

1. Pillars of Identity Relationship Management
    a. https://kantarainitiative.org/irmpillars/
2. Laws of Identity
    a. http://msdn.microsoft.com/en-us/library/ms996456.aspx
3. Right to be Forgotten
    a. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
4. Kantara Initiative Identity Relationship Management Work Group
    a. https://kantarainitiative.org/groups/irm/
5. NIST Privacy Engineering
    a. http://csrc.nist.gov/projects/privacy_engineering/index.html
6. OMB 04-04
    a. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
7. Laws of Relationships (A Work In Progress) Presentation
    a. https://www.youtube.com/watch?v=25Pk0TKf2Cc

5 REVISION HISTORY

v1 - Editing sprint closed October 21 2014

v2 – Editing sprint closed December 12 2014

v3 – Editing sprint closed January 11 2014

v4 – Editing sprint closed January 21 2015