**Editorial Process Notes:**

|  |
| --- |
| **Copyright Kantara Initiative 2014****IPR: Creative Commons Share-Alike Attribution** * **This document is open for comments.**
* **To be an editor please notify the WG Lead Editor - Ian Glazer**
* **To contribute substantially to the document you must join the IRM WG.**
 |



**The Laws of Relationship Management**

**Version: 0.1**

**Date:** 2014-10-21

**Editor:** Ian Glazer and Joni Brennan

**Status:** This document is a **Kantara Initiative Draft Report**, and has not yet been approved by the Identity Relationship Management WG or Leadership Council.

**IPR**: Creative Commons Attribution-Share Alike 3.0 Unported License.

**Contributors:**

The full list of contributors can be referenced here: <INSERT IRM WG Voting Roster>

**Abstract:**

This report discusses the development of Laws of Relationships. The Laws of Relationships have been generated as a result of industry discussions inspired by the Pillars of Identity Relationship Management.

**Notice:**

This work is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported License.

**You are free:**

* **to Share** -- to copy, distribute and transmit the work
* **to Remix** -- to adapt the work.

**Under the Following Conditions:**

* **Attribution** --- You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
* **Share Alike** --- If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

**With the understanding that:**

* **Waiver:** Any of the above conditions can be waived if you get permission from the copyright holder.
* **Public Domain**: Where the work or any of its elements is in the public domain under applicable law, that status is in no way affected by the license.
* **Other Rights**: In no way are any of the following rights affected by the license:
	+ Your fair dealing or fair use rights, or other applicable copyright exceptions and limitations;
	+ The author's moral rights;
	+ Rights other persons may have either in the work itself or in how the work is used, such as publicity or privacy rights.

**Notice**: For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this document.

Copyright © 2014 Kantara Initiative

[Introduction](#h.2s8eyo1)

[Problem Space](#h.dbgdec84gmg1)

[Why Develop Laws?](#h.7le5g0c2f4q0)

[The Laws of Relationships](#h.5m4cv8mwwxlp)

[Scalable](#h.w9pha9pq0fn5)

[Actionable](#h.p441kp3iuws3)

[Immutable](#h.wfbdg11rthyi)

[Contextual](#h.ujvpif1vy1sp)

[Active](#h.mayudue025iy)

[Inactive](#h.nwwmwzgrb8x)

[Transferable](#h.vohk5sxd6w3l)

[Temporary](#h.8un5k6o0qdox)

[Permanent](#h.v9ck5k87kc0j)

[Provable](#h.rpub3ph5clj4)

[Single-party Asserted](#h.zfc2wdifgxii)

[Multi-party Asserted](#h.8g11sq99ucvw)

[Third-party](#h.i1ffu4rzibcz)

[Acknowledgeable](#h.nzg47vb93nqy)

[Revocable](#h.6n4k01yym1id)

[Constrainable](#h.7yi7qqu0smh4)

[Conclusion](#h.ekl4a87v2u16)

[References](#h.uxwss9k5wqim)

[Revision History](#h.ieif106nx2uc)

# Introduction

This report discusses the development of Laws of Relationships. The Laws of Relationships have been generated as a result of industry discussions inspired by the Pillars of Identity Relationship Management.

**1.1 Purpose**

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 the evolving concepts around Identity and Access Management (IAM). The ideal goal for the document is to inform design principles for consideration and adoption applying to Kantara Initiative developments and broadly applicable to any innovative IAM approaches.

**1.2 Audience**

The document is a reference for:

1. “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.
2. Designers, engineers and authors developing new systems, protocols and standards.
3. IT and business professionals planning and operating services within organisations and on the open market.

1.2 Meeting the new challenges of digital identity

Digital identity services exist so that relationships can be mediated and managed by information systems. Digital identity is at once the welcome mat and the pass-key at the door to every online relationship.

When identity was limited to isolated systems, and later to single organisations, those relationships were simple and relatively stable. Identity services focused on assuring the security of transactions.

Relationships, however, are a function of networks. As services and devices are added to a network and as networks are connected to each other, relationships propagate exponentially. The complexity of mediating relationships has grown in lock step with the expansion of networks.

At global scales existing design strategies reach the limits of their usefulness. Relationships are too complex and varied to be represented by attributes, credentials and permissions. The identity domain can no longer be predicated solely on the security boundaries of organisational networks. Systems that were designed to represent people in organisations will not easily represent vast numbers of small devices, or the fluid, open relationships of the Internet. It is no longer sufficient to represent relationships implicitly or as an assumed precursor to the function of access management.

The value of the network is the value of the relationships it makes possible. To secure the benefits of a networked world it is time to turn our attention to the development of principles, information and technologies designed explicitly for the safe and effective representation of those relationships.

## **Problem Space**

We, as an industry, are used to dealing with reasonable numbers of people with reasonable numbers of attributes. We have experience in handling these types of scenarios as they grow and evolve. This specific scenario might appropriately describe the current state of enterprise identity and access management.

Now we move into a world of an unreasonably large amount of “things” with a small number of attributes. This scenario does not exactly map to the processes, technologies, and policies in place today with regard to identity and access management.

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

As an industry and with regard to this final scenario of binding, interoperability, and practices, we may not have the experience and tools necessary to fully understand and address the problem space.

##  **Why Develop Laws?**

The laws this document introduces design principles and questions to shape future conclusions. We want these laws to provoke thought, and research on, the evolution of identity and access management as related to the Pillars of Identity Relationship Management.

The development of laws helps us to:

* inform design
* test existing solutions
* identify gaps

# The Laws of Relationships

## Scalable

**Relationships must be scalable.** There are many innovations approaching that are working with the management of scalability. If we only focus on scalability in terms of actors, attributes and relationships, many organizations will find themselves in a very poor position to administer the relationships. If we, as an industry, will deal with billions of things, then we will need to focus not only on more things (in all forms: actors, attributes, relationships, etc) but also scaling administration too.

## Actionable

**Relationships must be actionable.** We want relationships to be able to do something of value and, more specifically, relationships must be able to 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 state we would pass actionable information to the back-end for a classic response-request authorization model. We must understand what will happen when we don't have access to or even have the back-end type of information.

## Immutable

**Relationships can be immutable.** Immutable relationships cannot be changed. Immutable relationships may provide the ground layer for providing some type of assurance in the grand scheme of Identity Access Management compliance. Immutable relationships give important contextual information. Immutable relationships examples might look like:

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

## Contextual

**Relationships can be contextual.** Describing the nuances of contextual types of relationships presents challenges. This type of relationship needs discussion and input to have a more broad understanding of the concepts. Early contextual types may be active or inactive.

### Active

A relationship is active when conditions are met and, identified conditions make up the relationship context. In an active relationship it is context that toggles a relationship in to a state of usability.

Consider this example scenario: I travel to a foreign land. I’ve contracted with a SIM card provider to use a SIM card. I don’t own the SIM card. I put the SIM card in to the phone that I do own. Until the SIM card actually connects with and pings a cell tower the relationship is inactive and then becomes active.

### Inactive

If no parties are using the relationship it is inert. Nothing really happens. There may be a connection but the relationship is not active yet.

## Transferable

**Relationships can be transferable.** A transferable type of relationship is one that can move from one subject to another. The two types include temporary and permanent.

### Temporary

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

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.

### 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.

## Provable

**Relationships must be provable.** Provability of a relationships may eventually relate to concepts of Identity Assurance such as the “Levels of Assurance” OMB 04-04. Typically these types of relationships come in three types. There must be a mechanism to prove that a relationship exists.

### Single-party Asserted

A single-party relationship is asserted by a single-party.

Example: I work for Foo.
X relates to Y because X says so.

### Multi-party Asserted

Multiple-parties assert that the relationship exists.

Example: I work for Foo. Foo says that she works for me.
X relates to Y because X and Y say so.

### Third-party

Third-parties assert that the relationship exists.

Example: HR says that Mary works for Foo.
X relates to Y because Z says so.

## Acknowledgeable

**Relationships must be acknowledgeable.** Specifically, all parties must be able to acknowledge that they have a relationship. Acknowledgement also has some nuances regarding who recognizes which relationships. This subject would benefit from further review.

Example: I acknowledge that I have a relationship with Twitter. But do I acknowledge my followers? Credit bureaus acknowledge their relationship with me, but do I acknowledge my relationship with them?

Question: Is this actually a law or is it more focused toward Vendor Relationship Management, Personal Data Ecosystem, or other areas of privacy study and development?

## 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.

Example: I mistakenly destroy my phone and the ownership relationship is now gone. What happens to the other associated relationships?

Questions:

* 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 delete?

## Constrainable

**Relationships must be constrainable**. All relationships must be able to be managed including the introduction of constraints upon how parties in a relationship can behave. Consent is likely a key component of this constraining for manageability. However some of these types of constraints might look more like Digital Rights Management (DRM) rather than consent.

Examples: My device can report my location. My light bulb can share data with the power company. This coffee maker can only use these kinds of pods. You can only use a car to drive if you have a driver’s license.

# Conclusion

This report has discussed the initial development of Laws of Relationships. The Laws 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 potential implications of the summation of data generation effects.

This report represents an entry in to high-level strategic, policy, and technology review and research around the implications of relationships and their laws, 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 Relationship Laws, Types, and Axioms with regard to the following considerations:

* + IoT is a natural case
		- Industrial settings (factories, planes, etc)
		- Citizen (smart homes, sensors in public)
	+ Familial Relationships
		- Insurance
		- Healthcare
		- Finance
	+ Complex authorization models
	+ Regulatory influence

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

Further discussion and research regarding the topics discussed in this report are developing within the Katnara Initiative Identity Relationship Management Work Group. Please join the work group to share your value and contribution to the initiative.

# References

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

# Revision History

v1 - Editing sprint closed October 21 2014