Identity Federation:
Citizen Consent and the Internet of Things

Author: Guy Huntington, President, Huntington Ventures Ltd.
Date: October 2017

Table of Contents

Executive Summary

With nanotechnology, devices are shrinking down to an almost molecular level and have the ability to communicate wirelessly via the Internet. These devices are beginning to proliferate in almost all aspects of our lives be it medical, transportation, government, clothing, appliances, and so on.

Since device owners have to access many different systems to manage their authorization consents, it becomes unwieldy. This paper addresses the simple question of "How do I manage all my consents across a wide variety of different devices, suppliers, and their systems in one place?"

The paper lays out Internet of Things Consent Principles, explaining each one in greater detail:

- End user consent must be required to use the device except those cases where it is mandated by laws and regulations.
- The chain of custody for consent must exist at all levels, i.e. from vendor through to final user or users based on risk and laws/regulations.
- The device, the system that controls it, and/or the identity management system the device is a part of must be able to use "User Managed Access" and also "OpenID Connect" protocols.
- Any individual, government, or enterprise offering a centralized user consent service must be mandated by laws and regulations.
- Any consent management service must adhere to regulatory security best practices including identity and credential assurance, data storage and transmission as well as archival processes.
- Based on risk, the identity assurance and the credential assurance must be applied to obtain and/or transfer consent between the user and various enterprises and/or other Internet of Things devices.
- Secure, delegated access of consent should be part of the device's consent management system.
- The user of a centralized consent management service should have the ability to transfer this service to other enterprises offering this service in a secure manner.
- When a user leaves a centralized consent management service, the service must securely store the data for a predetermined amount of time according to the timeframes set forth by laws and regulations.

The paper then identifies areas where governments need to be involved with identity and credential assurance as well as laws and regulations pertaining to consent management.

User Managed Access (UMA) is discussed from a privacy and security perspective. Users want to ensure their centrally managed consent service is secure. They won't want unauthorized access and/or someone masquerading as them, learning about, and/or changing their consents.

The paper then concludes by noting that identity federation is the heart of creating an interdependent world. **The user should be securely in control of how this technology is deployed and used.**

Introduction

With the development of nanotechnology and wireless communication, the size of wireless computer chips is becoming almost molecular in level. Nanotechnology is being implemented in everything including automotive components, medical devices, buildings and process controls, appliances, and will even eventually be implemented in clothing.

While most of the industry's focus is on producing new ways of interacting with devices, not a lot of attention is focused on user consent. Why is this important? Come with me on a journey… 5 years into the future.

You will likely be interacting daily with 20-100 or more different devices such as your fridge. Your fridge is now smart. It actually knows what is inside it, how much has been consumed, what groceries you are running low on, and the ages of the food.

You are a busy person who does not have time to shop. So, you give authorization consent to a company like Amazon or Walmart so the fridge information is automatically sent to them with predefined ordering information. You come home and find the food you need to replenish your fridge on your doorstep, which was automatically drop shipped by Amazon or Walmart using a drone. Perhaps your fridge was automatically restocked for you (https://www.foodbeast.com/news/walmart-delivery-service-home-access).

Now let's say that while you shop at Amazon or Walmart, there are some specialty stores you also like to shop at. You give your consent to the fridge to send the specialty retailers information on only the products they supply. When the product level gets low, the fridge automatically sends out information to them and the specialty retailer ships it to you. As your food preferences, budgets, and retailers change, or when you sell your fridge, you change your consent.

This is just your fridge. Imagine the complex world of consent management when you have 20-100 different Internet of Things!

Since the device owners have to access many different systems to manage their consents, it becomes unwieldly. This paper addresses the simple question of "How do I manage all my consents across a wide variety of different devices, suppliers, and their systems in one place?"

First, some underlying principles of consent management are required. These principles will provide a legislative, vendor, and user framework to operate within.

Internet of Things Consent Principles

- End user consent must be required to use the device except in those cases where consent is mandated by laws and regulations.
- The chain of custody for consent must exist at all levels, i.e. from vendor through to final user or users based on risk and laws/regulations.
- The device, the system that controls it, and/or the identity management system the device is part of, must be able to use "User Managed Access" and also "OpenID Connect" protocols.
- Any individual, government, or enterprise offering a centralized user consent service must be mandated by laws and regulations.
- Any consent management service must adhere to regulatory security best practices including identity and credential assurance, data storage and transmission as well as archival processes.
- Based on risk, the identity assurance and the credential assurance must be applied to obtain and/or transfer consent between the user and various enterprises and/or other Internet of Things devices.
- Secure, delegated access of consent should be part of the device's consent management system.
- The user of a centralized consent management service should have the ability to transfer this service to other enterprises offering this service in a secure manner.
- When a user leaves a centralized consent management service, the service must securely store the data for a predetermined amount of time according to the timeframes set forth by laws and regulations.

End user consent must be required to use the device except those cases mandated by laws and regulations

Consent to use and/or receive data or a service from a device should be required based on any applicable laws/regulations and/or risk. For example, a T-shirt you own that has a smart chip within it, will likely be low and require little or no consent, e.g. sending information to your washing machine. A driverless car owner may grant access to a driver of her vehicle. This is a higher risk and may or may not fall under certain legal laws and regulations about consent being obtained.

The chain of custody for consent must exist at all levels, i.e. from vendor through to final user or users, based on risk and laws/regulations

Chain of custody for consent, i.e. a historical record of who was granted authorizations, must exist for a device dependent upon risk and any laws or regulations applicable. Let's take two devices as examples: a fridge and the pacemaker.

The fridge consent chain of custody is not high risk. Therefore, the history of consents given for the fridge might not be held that long nor is required by law. Pacemakers are high risk with sensitive information. Therefore, the chain of custody of all consents given for this device, from the manufacturer onwards, needs to be kept for a specific period set forth by laws and regulations.

The device, the system that controls it, and/or the identity management system the device is part of must be able to use "User Managed Access" and also "OpenID Connect" protocols

"User Managed Access" (UMA) (https://kantarainitiative.org/confluence/display/uma/Home) is a vendor agnostic protocol designed to allow a user to centralize their authorization consents based on OAuth 2.0 (https://oauth.net/2/). It allows for one place for a user to go to view, change, or grant their authorizations for devices in different locations, networks, and enterprises.

Devices should also be compatible with OpenID Connect (OIDC) (http://openid.net/connect/), which is a protocol built on top of OAuth to provide identity and credential assurance. As other principles state, based on risk, the consent obtained will use higher levels of identity and credential assurance where required.

All devices and/or their control systems and/or identity management systems that control the device must be compliant with these protocols.

Any individual, government, enterprise or individual offering a centralized user consent management service must be mandated by laws and regulations

The potentially sensitive content of a user's consent means that any government, enterprise, or third party offering a centralized user consent management service must be in compliance with laws and regulations pertaining to the service.

Any consent management service must adhere to regulatory security best practices including Identity and credential assurance, data storage and transmission as well as archival processes.

Governments should have laws and regulations pertaining to consent management. This should include specifications for different identity and credential assurance levels, the way the consent data is stored, accessed, transmitted, and archived.

Based on risk, identity and credential assurance must be applied to validate the identity before applying consent

How the user provides their consent should be based upon risk. For low risk consent, low identity and credential assurances levels will be used. However, as the risk rises, higher identity and credential assurance levels should be required. Let's use the fridge and pacemaker as examples.

The fridge is a low risk device, thus requiring low levels of identity and credential assurance to ensure that you, the owner, are who you claim to be, when assigning consent. A username and password might be sufficient with no identity verification required.

A pacemaker is a high-risk device. Any changes to the authorization consent for the information this device produces should require high levels of identity and credential assurance. Identity verification from a government identity verification service and also a biometric plus a password might be required to authenticate in order to apply or change consent.

Secure, delegated access of consent should be part of the device's consent management system

A user should have the ability to delegate some or all their consent to another. Let's use the fridge as an example.

You, the fridge owner, are the principal consent manager. You choose to give your partner the same abilities to manage consent. However, you decide to restrict consent abilities to your children, only allowing them to manage a small portion of the food consent within the fridge.

The user of a centralized consent management service should have the ability to transfer this service to other enterprises offering this service in a secure manner

If a user wants to switch suppliers of their central consent management service, it should be done in compliance with laws and regulations in a secure manner. Let's use the example of a user deciding to switch from Acme Inc. as the centralized consent management service to a bank offering the same service.

Laws and regulations need to be in place prescribing standards by which the user notifies Acme Inc. of their intent to terminate the agreement and the transfer to the bank. The history of the authorization consents, the time limit that Acme Inc. retains the information, and how the information should be transferred, should be mandated by laws and regulations.

When a user leaves a centralized consent management service, the service must securely store the data for a predetermined amount of time according to the timeframes set forth by laws and regulations

Laws and regulations should apply to how long a centralized consent management services retains their records after a user leaves the service.

Governments and Consent

From the above principles, it becomes apparent that governments need to be involved in creating a citizen consent system in the following areas:

- Identity assurance
- Credential assurance
- Laws and regulations pertaining to consent management

Identity and Credential Assurance

What is identity and credential assurance?

- Identity assurance is a rating scale of risk versus identity verification processes used
- Credential assurance is a rating scale of risk versus the type of authentication used

For low risk usage, whatever the vendor and user agree to will likely be sufficient. However, as the risk rises, higher levels of both identity and credential assurance are required.

Governments are usually involved in determining identity assurance levels. Higher levels of identity assurance usually require biometrics. The same applies to credential assurance. The following paper illustrates how the old ways of doing this are no longer effective: Identity Federation: Biometrics and Governments (https://www.slideshare.net/ghuntington/identity-federation-biometrics-and-governments-sept-2017-80192336).

Governments need to lay the foundational pieces for protecting a citizen's biometrics. They also need to create a high-level identity verification assurance service upon which other levels of government and third parties use to verify and authenticate an identity.

Laws and Regulations

Governments should conduct a gap analysis illustrating where changes need to be made pertaining to citizen authorization consent. There are also cross-border authorization rights to consider.

In Europe in 2018 the General Data Protection Regulation (GDPR) regulations come into effect. In this presentation by Eve Maler, Chair of the Consumer Identity World, Work Group she lays out how UMA will assist enterprise in meeting their compliance: https://kantarainitiative.org/confluence/download/attachments/17760302/CIWUSA%20Kantara%20workshop%20GDPR%20UMA%202017-09-11.pdf?api=v2. This is just the first of many similar requirements as governments all over the world create new identity protection laws.

User Managed Access - Privacy and Security

The protocol for User Managed Access (UMA) is dependent upon OAuth 2.0 for authorization. It has been designed to work with OpenID Connect for authentication. What does this really mean?

In the Federation Protocols section of Enterprise Identity Federation: Mitigating Risks and Liabilities (https://www.slideshare.net/ghuntington/identity-federation-mitigating-risks-and-liabilities-79942481), it describes the following:

Imagine that you are constructing a strong structure using blocks. At the bottom of the structure you use six large blocks. This is the foundational piece. However, there are many different ways to assemble each of the foundational blocks, i.e. each of the large blocks is composed of smaller blocks that can be assembled differently to make the larger foundational one.

On top of the large foundational blocks, you then assemble five mid-tier blocks. Like the foundational ones supporting them, they too have different ways for each of them to be configured, i.e. each mid-tier block is made up of smaller blocks.

- The foundational blocks are JSON components and WebFinger
- Mid-tier blocks are the OAuth components

Depending upon how the blocks are configured, then the protocol that uses them, i.e. UMA, may or may not be secure. This paper by Jim Manico[1] illustrates some of the OAuth token countermeasures that need to be addressed:
https://handouts.secappdev.org/handouts/2017/Jim%20Manico/04a.%20OAUTH%20Security%20Introduction%20MODULE%202-9-2017.pdf

Regulators, vendors, identity system providers, and users need to realize that the security and privacy of their Internet of Things centralized consent is dependent on how UMA and OAuth are configured. Any enterprise embarking on a deployment of UMA centralized consent service must first consider both the legal and security implications to mitigate risk and potential liabilities.

From an end user's perspective, they will want to ensure that their centrally managed consent service is secure. They won't want unauthorized access and/or someone masquerading as them, learning about and/or changing their consents.

[1] https://manicode.com/

Summary

The noted NY Times Columnist, Thomas Friedman, in a recent column stated[2]:

> *"We're going through a change in the "climate" of globalization — going from an interconnected world to an interdependent one, from a world of walls where you build your wealth by hoarding the most resources to a world of webs where you build your wealth by having the most connections to the flow of ideas, networks, innovators and entrepreneurs. In this interdependent world, connectivity leads to prosperity and isolation leads to poverty. We got rich by being "America Connected" not "America First.*
>
> *Finally, we're going through a change in the "climate" of technology and work. We're moving into a world where computers and algorithms can* analyze *(reveal previously hidden patterns);* optimize *(tell a plane which altitude to fly each mile to get the best fuel efficiency);* prophesize *(tell you when your elevator will break or what your customer is likely to buy);* customize *(tailor any product or service for you alone); and* digitize *and* automatize *more and more products and services. Any company that doesn't deploy all six elements will struggle, and this is changing every job and industry."*

Identity federation is at the heart of this change. It is the "interdependent glue" allowing an enterprise, application, service, or a smart thing to trust one or more other entities and/or things. This occurs immediately, allowing secure authorized access from anywhere on the globe.

Identities needs to control their privacy as well as their authorizations in a centralized fashion. This is achieved by establishing laws and regulations pertaining to authorization consent and adopting User Managed Access with OpenID Connect.

A sweeping change is now upon us. **The user should be securely in control of how this technology is deployed and used**.

[2] https://www.nytimes.com/2017/09/27/opinion/globalization-trump-american-progress.html?rref=collection%2Fcolumn%2Fthomas-l-friedman&action=click&contentCollection=opinion&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection

About the Author

Guy Huntington is a veteran identity architect, program and project manager who's lead as well as rescued many large identity projects with many of them involving identity federation. His past clients include Boeing, Capital One, Kaiser Permanente, WestJet, Government of Alberta's Digital Citizen Identity and Authentication Program and Alberta Blue Cross. As one of his past clients said "He is a great find, because he is able to do high quality strategic work, but is also well-versed in project management and technical details, so he can traverse easily from wide to deep. With Guy, you get skills that would typically be encompassed in a small team of people."