Self-Sovereign Identity and IoT

Sovrin Foundation SSI in IoT Task Force
August 2020

sovrin
identity for all

Table of Contents

Executive Summary

Recent advances in computing and networking technologies now extend the digital world far beyond the obvious screen of the personal computer or smartphone to include the most mundane of physical objects. Manifest as an Internet of Things (IoT), our automobiles, thermostats, medical devices, livestock tags, and door locks now compute and connect across global networks. With more than 27 billion connected devices actively deployed in IoT, the very environments in which we live and work are now online.[1]

By 2025, more than 75 billion connected devices will extend the internet into the physical world as both a communication and control system without precedent.[1] Changes in this digital ecosystem—intentional or not—can, for the first time, produce physical consequences across thousands of systems separated by thousands of miles, paradoxically extending both our control and our risk. This power to sense, connect, and cause change equally invites opportunity and threat.

The nexus of threat and opportunity in IoT centers on identity and authority—currently there is no universal means to distinguish a thing from all others or determine what that thing is allowed to do. This lack of identity and authority hampers the development of multi-party IoT services and ecosystems, preventing the emergence of valuable new use cases, and makes it harder to provide effective solutions to the growing threat of cyber attacks. Self-Sovereign Identity (SSI) offers a durable identity for things and deliberately communicates authority, providing an emerging method by which to capitalize on IoT business opportunities and mitigate cyber threats.

In this white paper we compliment a generative argument, developing several pressing problems within IoT, with framework technical and business arguments that support value propositions for SSI in IoT. However, this white paper is not meant to be either an exhaustive analysis of alternatives, nor a deeply technical exposition. Instead, our aim is to highlight compelling business opportunities to create and capture value, motivating rigorous collaboration between what might otherwise be disparate SSI and IoT communities.

We will use three personas — Jamie, Bob, and Bessie the Cow — in this white paper to provide a basic introduction to SSI and IoT, explore practical challenges in context, and describe how SSI in IoT can meet these challenges. We start by introducing basic IoT concepts including: Machine to Machine communication, Machine to Person communication, Digital Twin; and IoT Security, Architecture, and Network Design considerations. Within the context of Jamie, Bob, and Bessie, we then explain the challenges of securing constrained devices, identifying and authorizing devices, managing device updates, maintaining secure communications, and ensuring data privacy and integrity. Next, we describe how SSI in IoT can help solve these challenges. Finally, we illustrate the business value of SSI in IoT.

We explain that SSI in IoT can significantly increase value and reduce risk for business. SSI in IoT can increase revenue by both driving new classes of business opportunities, in application domains such

[1] The IoT Rundown For 2020: Stats, Risks, and Solutions

as telemedicine, and opening the way for new, networked business models. The unparalleled security, privacy, and standardization that SSI in IoT confers can reduce operating and maintenance costs by simplifying device interactions and allowing for greater business process automation.

SSI-enabled devices can use many cryptographic methods to validate their identity, thereby extending the benefits of cryptographic protection through to a range of constrained devices, including low-power units with basic 8-bit microcontrollers. This mitigates a growing tide of critical network vulnerabilities and attack vectors exposed in the IoT. Finally, with security and privacy by design, SSI in IoT promotes low-cost compliance with new regulation, such as General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA), including facilitating third party audit.

The investment required to implement SSI in IoT to address security issues is significantly less than the cost of doing nothing. Under current protocols, the growing multitude of connected devices will quickly become a liability for organizations of all sizes, prohibitively increasing basic operating costs and opening new cyber vulnerabilities that threaten not only business viability, but also physical safety.[2] By applying SSI to IoT, organizations can begin to mitigate these growing cyber-physical risks, and capitalize on 21st century opportunities.

[2] Internet Of Things: Counting The Cost Of Cyberattacks

Introduction

The internet of things (IoT) is a ubiquitous web of devices sampling, interacting and being integrated into our everyday lives. The IoT is sometimes obvious (as in the case of an autonomous vehicle), and sometimes invisible (integrated inside other appliances). These devices range from large scale industrial equipment (wind turbines) to connected light bulbs in your home. In 2018, the number of connected devices on the planet exceeded the number of people—and growth is forecasted to continue, exceeding 75B by 2025. In short,anything that can be accessed over the web meets the definition of an IoT device.

While these devices and systems provide a great deal of value in our daily lives, at the same time there are serious systemic security issues within the IoT sector that continue to elude resolution. These problems are hard, which is why they have not been solved in the past. If we continue to neglect them, it puts the very society we now live in at risk.

In late May 2019, the Self-Sovereign Identity (SSI) in IoT Task Force was formed under the auspices of the Sovrin Foundation Governance Framework Working Group, to research and create a paper on how SSI can address some of the current business and security challenges in IoT. The Task Force is made up of volunteers from industry and academia. While the Task Force is under the guidance of the Sovrin Foundation, the efforts to address these challenges extend beyond the realm of a single organisation. Our goal has been to keep the paper's content as broad spectrum across the technology as possible without losing value.

This paper proposes technical solutions to the questions of identity, security, privacy, and other operational and architectural challenges of the IoT sector. We represent that neither the questions we have addressed nor the answers we have provided are exhaustive; but we believe that the solutions outlined in this paper will provide good options for resolving some of these longstanding challenges.

This paper has been written for technologists, business people and policy makers (in that order). We have endeavored to make the language accessible to all, but have not allowed technical detail to suffer at the expense of a wider audience.

The paper takes the following structure:

- Section 1 provides a high-level overview of the IoT sector, including operating and hardware constraints.
- Section 2 provides an overview of the Persona's created by the task force to elucidate challenges in the machine to machine (building automation) and machine to person (wearable technology) and thing (digitally tagged) interactions.
- Section 3 provides outlines of the identity, security, operational and architectural challenges we will cover in the paper.

- Section 4 discusses proposed solutions to the challenges of section three, utilizing Decentralized Identifies (DIDs), Verifiable Credentials (VCs), and some of the emerging sector protocols.
- Section 5 addresses how DIDs and VCs create business value and identifies potential cost savings or new products or services that can be created through the integration and support of DIDs and VCs within the IoT device architecture.
- The conclusion is a summary of how we believe the IoT sector can adopt and implement these technologies and a proposal of specific areas of work for a future "SSI in IoT Working Group".

Key Terms

Key Term	Definition
Agent	An Agent is software that acts on the behalf of an Entity (person, organization, or thing) that connects to a network that performs several functions autonomously with the Digital Wallet: • sends and receives messages • encrypts and decrypts information • signs digital information on behalf of the Entity • manages information in the Digital Wallet • backup and restore information[3]
Decentralized Identifier (DID)	A **decentralized identifier** (**DID**) is a globally unique identifier that is the core component of the decentralized digital identity and decentralized public key infrastructure (DPKI) for the Internet layer. Combined with the use of distributed ledger technology (DLTs), DIDs become the central component of a globally resolvable identifier that can cryptographically verify ownership of the identifier. A **DID** is associated with exactly one DID Document. For **Self-Sovereign Identity (SSI)**, which can be defined as a lifetime portable digital identity that does not depend on any centralized authority, DIDs provide a new class of identifier that fulfills all four requirements: persistence, global resolvability, cryptographic verifiability, and decentralization.[4] [5]

[3] The Current and Future State of Digital Wallets, Darrell O'Donnell, Continuum Loop Inc.
[4] https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/did-primer.md
[5] https://www.w3.org/TR/did-core/#keep-personally-identifiable-information-pii-private

DIDcomm	DIDComm Messaging is a mechanism for people, institutions, and IoT things to interact via machine-readable messages, using features of decentralized identifiers (DIDs) as the basis of security and privacy. It works over any transport. For example: HTTP, Bluetooth, SMTP, NFC, or web sockets.[6]
Digital Twin	The digital representation, or representative, of a thing. The representation is often in the cloud, but may be held on a hub in a LAN close to a device, and in some cases even within the device itself. See Appendix Two.
Digital Wallet	Digital Wallet: A software module, and typically an associated hardware module, for securely storing and accessing Private Keys, Link Secrets, other sensitive cryptographic key material, and other Private Data used by an Entity. A Wallet is accessed by an Agent.[7]
Entity	As used in IETF RFC 3986, Uniform Resource Identifier (URI), a resource of any kind that can be uniquely and independently identified.[8]
IoT Device	Devices, mechanical and digital machines that can be provided with unique identifiers (UIDs) and the ability to sense and transfer data over a network without requiring human-to-human or human-to-computer interaction.
Verifiable Credentials (VCs)	A set of one or more claims made by an issuer. A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects.[9]

IoT Background

The Internet of Things, or IoT: three little letters that have a huge range of meaning. An IoT device can range from a smart light bulb installed in your living room, to a wind turbine in the Baltic, to an autonomous drone out of sight overhead to the heart monitor in your Apple watch.

Not all IoT devices are powerful enough to perform cryptography and public key encryption.

In the world of device control every device has at least two levels of access control. The first is the control channel. The control channel is the interface over which the device receives instructions from the device controller. This channel typically has a bi-directional control flow. The second channel is the data channel. The device transmits sensor data on the data channel. In transmitting data, the channel can be point to point or open transmission.

[6] decentralized-identity/didcomm-messaging
[7] Sovrin Glossary V3
[8] Sovrin Glossary V3
[9] Verifiable Credentials Data Model 1.0

MACHINE TO MACHINE

For the purposes of this paper, we define Machine to Machine as any configuration where there is control and/or data communication between an IoT device and another computer, smartphone, or device. This could be as simple as a temperature sensor sending temperature data to a data recorder, or as complicated as an autonomous humanoid robot operating a piece of industrial equipment (e.g a forklift in a warehouse) that could be operated either by the robot or a human.

MACHINE TO PERSON

For the purpose of this paper, we define Machine to Person as any configuration where a device is attached to, or worn by, a person. The device is measuring some aspect of the person's personal or physical environment and transmitting this data directly or indirectly to a connected device. In this paper we reference glucose level sampling, location and gait data collection from shoe-based inserts transmitted to a smartphone and then to a centralized hub. This paper does not cover all ranges of wearable devices nor the privacy issues around the collection of Personal Identifiable Information (PII).

DIGITAL TWIN

In essence, there is the real thing in the physical world, and there is its digital representation. The latter can be referred to as the former's *digital twin*. For example, a business has an accounting system, which is a set of data and computational processes. Taken together, these data and processes are a digital representation of the business, or its digital twin.

"The digital twin concept consists of three distinct parts: the physical product, the digital/virtual product, and connections between the two products." [10] The connection can be active (a smart meter) or passive (Universal Product Code [11] or affixed tag) and links the physical device with its digital representation.

SECURITY

Information security or cybersecurity requirements can be identified using the CIA Triad, a simple model outlining the three governing security principles of **Confidentiality**, **Integrity** and **Availability** (CIA). The CIA Triad is applied to Operational Technology (OT) deployments and used to consider the behaviours and interactions between system components, including IoT devices, on-site servers and computers and cloud services.

[10] Digital twin

[11] A barcode symbology used to track retail goods, managed by GS1 (GS1 | The Global Language of Business)

Confidentiality considers measures taken to guarantee that data is protected from unauthorised access, which includes unauthorised access to file storage or databases, or interception of data as it travels between devices.

Integrity ensures the accuracy of data as it moves through workflows, processes, and across systems making sure that data is not deleted or modified without authorisation.

Availability ensures that authorised users have timely and uninterrupted access to information and resources in the system.

The priority and resources given to each axis of the triad will depend on the nature of the business under consideration. In some situations confidentiality will be most important, whereas others may require significant attention to be applied to providing extremely high availability. Self-Sovereign Identity protocols employ cryptographic techniques which can assist developers in addressing each of the elements of the CIA Triad.

IoT SYSTEM ARCHITECTURE

The industry literature shows that there are many architecture models currently in production within the IoT space. In its simplest form, the architecture of an IoT system (Figure 1) can be conceptualized as a three layer model: wireless sensor network (WSN) [12], cloud servers, and business application layer. It is possible to envision each of these layers being decomposed to sub-layers, but depth and complexity should be driven by application requirements versus any dogmatic approach.

The core components of the WSN are the edge sensors and actuators and nodes. These are components that monitor, control, act, and/or collect data within the physical environment of the IoT solution. The edge is the source of the data which can be locally processed or directly distributed to the controlled devices. As the number of IoT nodes explode, there is a real concern that the amount of computing power and bandwidth needed will exceed that which is available in the cloud. The 'Fog" is created by locating compute power at edge, nearer to the edge nodes thereby eliminating the need for increased bandwidth.

The controllers, gateways or hubs that coordinate all the actions of the edge devices are typically located in cloud computing resources. As edge devices are added, removed or moved on the network, they must be able to communicate with these controllers to join or leave the networks. Given the expected growth in the IoT space, the ability to manage these processes securely and efficiently is currently an active area of research and development.

Finally, at the business application layer, the data and information from the sensors are turned into business value. This layer may in fact also be cloud based, but is integrating into API layers of the hubs or controllers. Organizational Enterprise Resource Planning (ERP) systems could be an example of the kinds of applications sitting in the business application layer.

[12] Note: WSN typically include both IoT sensing(collecting data) devices and actuators (causing actions - e.g. turn on lights, ventilation systems, unlock doors,...)

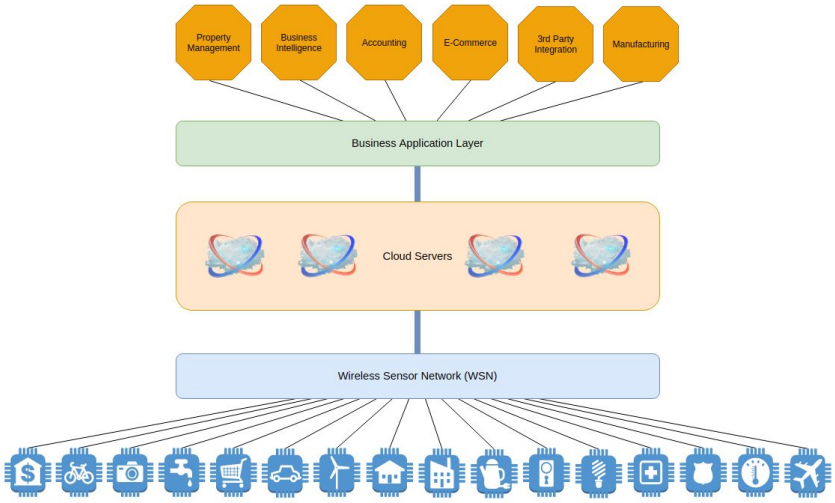

Figure 1: IoT System Architecture

IoT architecture can also be seen from a functional services layered approach as can be seen from the diagram below (Figure 2). This approach aids high level infrastructure design allowing for substitution of the services or components within each layer.

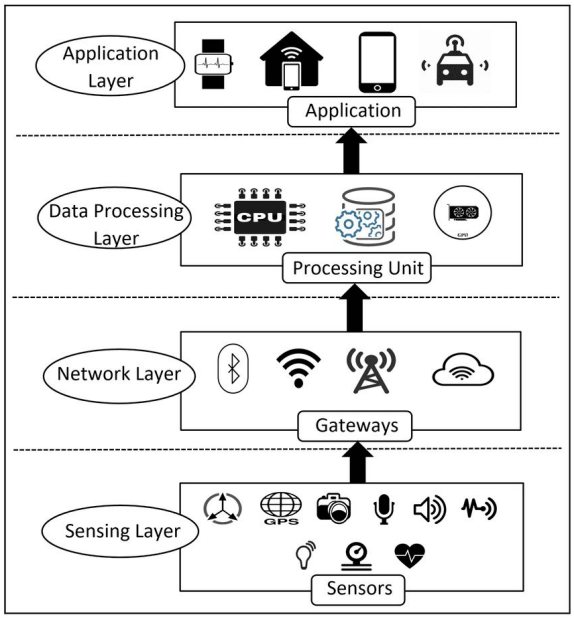

Figure 2: IoT Architecture as functional services

Both designs allow you to view different aspects of an IoT architecture, and when combined, give a full picture of IoT possibilities. [13]

NETWORK DESIGN CONSIDERATIONS

In determining the appropriate network design or IoT scheme, it is important for network designers to not only consider basic security requirements described by the CIA triad, but to also consider those requirements necessary for resilience. Given a network composed of many devices and a dynamic membership, the key network design considerations become integrity, availability, and scalability. [14]

Integrity is about being able to trust the data and its source being produced and distributed from a device. Integrity comes from the combination of identification of the specific device, authentication of the device to the network, and cryptographic assurance that the data received was sent from the device. The indisputable identification of the source of the data fulfills the non-repudiation requirement of integrity.

As devices and networks become more pervasive and increasingly provide critical systems, resilience and reliability are core requirements of IoT networks. Being able to easily, quickly, and securely add or remove devices to/from networks is essential to scalability.

Personas

In order to increase comprehension we have created a series of personas that describe environments where IoT devices are present and impact our lives in both our work and home environments. In this effort we have created three layers of classification: devices that are operating with devices (Machine to Machine), devices that are operating with direct connection to a person (Machine to Person), and the digital representation of a cow (Digital Twin).

JAMIE

Jamie is a 55-year-old male who has had Type 1 diabetes since childhood. In recent years, he has been using a glucose meter implanted under his skin. The glucose meter connects to an App on his phone to keep a record of his glucose levels. Jamie has been sharing this data with his endocrinologist.

Challenges

- Privacy
- Medical information permissioned access
- Location information permissioned access

[13] IoT Architecture Layers and Components. | Download Scientific Diagram

[14] Bubbles of Trust: A decentralized blockchain-based authentication system for IoT

Recently, doctors diagnosed Jamie with dementia. Jamie's neurologist warned him and his wife, Anne, that cognitive impairment makes it more likely that Jamie will wander off and not be able to return home. The doctor suggested that Jamie and Anne consider adding a pair of shoe inserts to Jamie's shoes. These inserts can recognize Jamie by his gait and can even track Jamie's physical location.

Anne and Jamie decided the value of being able to find Jamie in an emergency outweighed the risk of someone else tracking his location. However, this privacy and potential personal safety risk is another worry for Anne.

BOB

Whilst the staff on the trading floor intently monitor the trajectories of stock markets, exchange rates, treasuries and high yield bonds, Bob, as the Infrastructure Manager, has a far different view. Bob is responsible for all the infrastructure that exists to run the facility and keep the bank's staff, financial resources, confidential information and proprietary data safe. The facility has networks for wireless LAN, lighting, heating, area access and CCTV, among others. Bob has several teams of personnel that are responsible for ensuring all the systems within the trading floor are functioning correctly. Controlling, upgrading and adding new subsystems to any of the networks requires significant time and effort for Bob's team. In addition, since the bank that owns the facility is tightly regulated, it has legal and safety requirements that must be maintained. This compliance requirement provides a constant pressure to keep all systems secure and up to date on security patches and procedures.

Challenges

- Number of devices and networks to manage
- Access control for a large number of personnel
- Device control, upgrading and replacement
- Meeting legal and safety requirements

BESSIE THE COW

Bessie is a 14-month old Black Angus cow being raised by a rancher (keeper). The keeper (in contrast to the owner) of Bessie is required to keep records about Bessie, from birth to death. The tracking of cattle (and other farm animals) throughout their lives is a critical element in ensuring safety of the food supply chain. Every keeper of cattle is required to register every animal they have on their farm with governmental organizations [15] [16] and all movements of cattle must be recorded and reported. In Europe and the UK animals are required to have passports in which the keeper must record all the required immunization and movement history.

Challenges

- Identity
- Scalability
- Reporting requirements (movement, transfer of ownership)
- Data security and data sharing

[15] Approved Farm Management Packages
[16] Keep a holding register for cattle - GOV.UK

In 2001 the United Kingdom experienced an outbreak of foot and mouth disease. This is a highly infectious disease, for which there is no cure. By the time the outbreak was eradicated over 6 million cows and sheep had been destroyed with a cost of 8 Billion GBP to the UK. [17] Between 2018 to 2020 China lost up to 60% of their hog production (~100 million pigs) to African Swine Fever outbreak. [18] The outbreak then spread to other countries in Asia with the toll so far impacting 25% of the world's pigs. It is for these reasons that governments are very serious on the regulations around the health and movement of animals.

Herd management is critical to success in ranching. Cattle have long been branded (to identify them as members of a specific herd) and tagged (to identify them as a *particular* member of the herd). A generation ago, these records might have been maintained in a small notebook carried in the rancher's pocket, but today this information is kept either in paper based registries and passports or in herd management software. However, one thing hasn't changed: the high degree of manual interaction for input and recording of data.

Even with herd management software, keeping track of the cattle data and being able to transfer it easily when cattle are sold or moved is still a significant challenge, and it often involves stacks of paper being sent to government agencies and exchanged with new keepers/owners.

This provenance data is very important when the cow is finally slaughtered and processed or when disease outbreaks happen. Any IoT system tracking beef must include the ability to associate each individual product ID back to Bessie's identity and records.

Challenges

Despite the rapid growth of IoT across all sectors of society, many significant security gaps persist and several new vulnerabilities have emerged. The diversity of vendors and platforms and nascent regulation have exacerbated the technical difficulties in closing these gaps. In late 2017, IBM published [19] the following list of the top 10 security threats within the IoT sector:

1. Secure constrained devices
2. Authorize and authenticate devices
3. Manage device updates
4. Secure communication
5. Ensure data privacy and integrity
6. Secure web, mobile, and cloud applications
7. Ensure high availability
8. Detect vulnerabilities and incidents
9. Manage vulnerabilities

[17] https://en.wikipedia.org/wiki/2001_United_Kingdom_foot-and-mouth_outbreak
[18] As China recovers from COVID-19, African Swine Fever threatens its pig population
[19] IoT Security Issues: Top 10 Challenges – Build Smart. Build Secure

10. Predict and preempt security issues

SSI cannot address all of these threats, but it does offer viable and scalable solutions for the first five of these challenges.

SECURING CONSTRAINED DEVICES

Advances in micro-electronics, computing, batteries, and networking technologies have newly-enabled the production of IoT devices at low cost and high volume. Unique device identification, specific authentication, trusted communication, and wider device management methods depend on the performance capacity of the IoT devices in question. Some non-critical use cases, such as those where an IoT device interacts with a single private user only, could rely on low-demand methods, e.g., device identification by IP address.[20] More effective security solutions, such as cryptography-based approaches, would benefit critical applications, such as Jamie's, and especially those that require interoperability with third parties—a situation shared by Jamie, Bob, and Bessie.

Cryptography-based approaches depend on sufficient device resources. Even so, many manufacturers design IoT devices with significantly constrained MCU performance, power, nonvolatile storage, and entropy sources to minimize part cost drivers and extend the ubiquity of IoT device deployment. Vendors, enterprise network administrators, and consumers alike face a difficult admixture when confronting the demand to manage security risks in constrained IoT devices across a variety of use cases and competitive markets.

This Task Force believes that using part cost as the primary driver for determining component selection ignores secondary systemic costs of security challenges and abandons the potential new business opportunities that arise when having a high assurance digital identity connected to the device.

AUTHORIZE AND AUTHENTICATE DEVICES

A key position of this Task Force is that the correct context should be "*Identification, Authorization and Authentication.*" Since the creation of the internet, the lack of a solid secure identity model has been the root cause of many of the security issues being experienced today. Security models of Authorization and Authentication have been in existence for 10+ years, yet have not solved the underlying security issues. With a secure high assurance identity as the first step in the process, confidence is established that the device on the other end of the communication link is the device expected.

The diagram below (Figure 3) shows an identity lifecycle overlaid on the IoT life stage model described by Kevin Guerin at Waveston. [21] In this white paper we will focus on Initialisation and Use

[20] Enabling the Internet of Things
[21] A life cycle approach for IoT security

stages. We propose an IoT *security* lifecycle within which we have identified seven steps most relevant to risk management and security challenges in IoT.

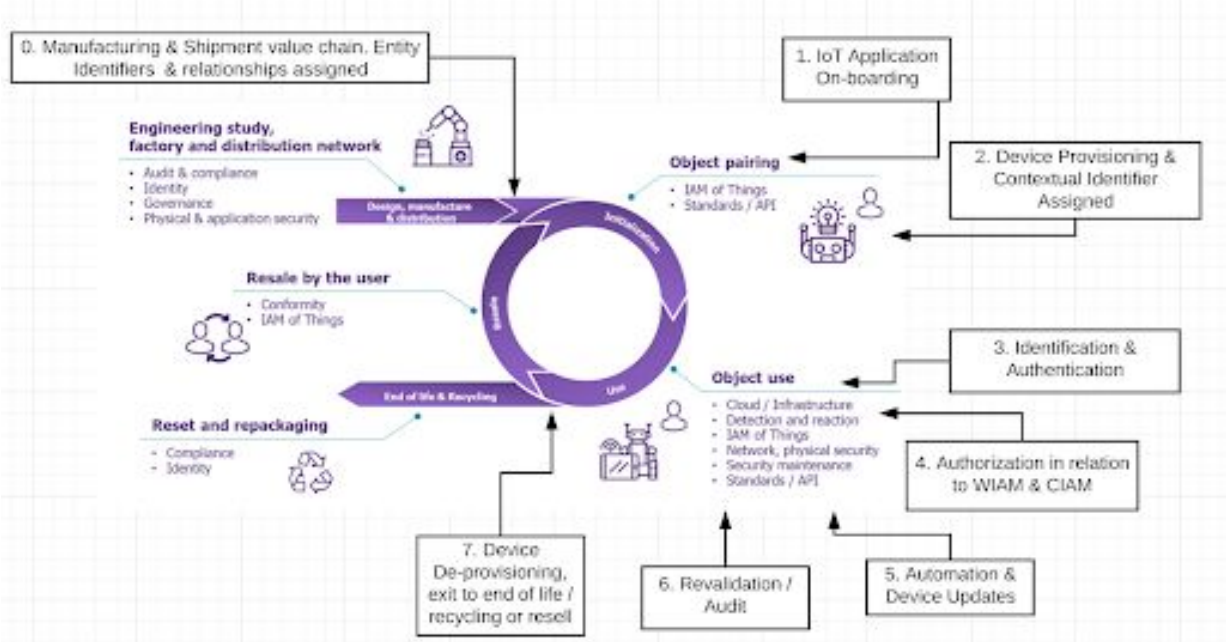

Figure 3: IoT Lifecycle Security

LIFE STAGE: INITIALISATION

1. IoT Application On-boarding.

Many IoT use cases, such as Bob's smart building, leverage a broad scope of different IoT applications. The core business benefits derive from the coordination between these IoT applications. Any new on-boarding of an IoT application will affect the identity management of both new devices and of existing applications in operation.

2. Device Provisioning and Contextual Identifier Assigned.

During manufacturing, the manufacturer will assign entity identifiers. Assignment of these identifiers is crucial to management of security and liability. Once an IoT application is deployed, a contextual identifier will be assigned, either in addition to or in relation to the original manufacturer's identifiers.

Provisioning a device for a network is the combination of identifying and authorizing that device for the IoT network. More broadly, provisioning a device involves the following steps, although not necessarily in this order:

- Configure the IoT device by controller or delegated entity.
- Deploy the IoT device in the field.
- Establish connection between the IoT device and the controller.

Depending on the specific network configuration, the controller can be local, in an edge gateway, or in the cloud.

LIFE STAGE: USE

3. Identification and Authentication.

Identification is the process of answering the questions:

"Should I enroll this new Thing/Entity?"
"Is this Thing/Entity the same Thing/Entity I am expecting it to be?"

Identification begins by determining if the IoT device to be identified is known to the host and controller. Each IoT device must have a unique identifier that allows the host and controller to differentiate the specific IoT device from other devices during initial connection. Typically, the algorithm controlling the connection creates an identifier ad hoc while connecting the IoT device to the network (e.g., private/public key, X.509 certificate). Alternatively, the device manufacturer may assign an identifier during device production (e.g., VIN, UUID, vendor id, mac address). Unique identification is essential, even for a rancher who seeks to effectively manage Bessie using IoT devices amongst a wider herd of cattle. It is with a known identity that a device is authenticated to the network it connects to.

4. Authorization in relation to WIAM and CIAM.

Authorization is the process of verifying whether or not that specific entity (organisation, person or thing), is allowed to perform specific operations after a successful identification and authentication process. These authorization policies must interwork with the Workforce Identity and Access Management (WIAM) policies, important for the permissions of Bessie the cow's rancher. Customer Identity and Access Management Policies (CIAM) will be equally important to establishing and maintaining the permissions of Anne and Jamie.

Many manufacturers and network designers use a "grant all" authorization policy for IoT devices, reasoning that an individual IoT device operates within a narrow purpose. The permissive "grant all" authorization policy allows a properly identified entity to perform all operations on the IoT device.

Sharing details of the identification mechanism (e.g. login and password) either intentionally [22], or as a result of a phishing[23] attack, can create a high risk of security breach by another entity gaining unintended access. Unintended access could create grave risks for Jamie.

Some IoT devices can provide multiple types of authorization policies. Controllers manage these different policies. Detailed policy management quickly becomes difficult with increasing scale as the number and variety of devices grows and myriad policies must be matched to specific actors using a distribution of controllers. Bob faces this difficulty because he must deal with both many people and numerous IoT devices.

5. Automation and Device Updates

Most technologies, and especially those incorporating software, can benefit from the deployment of additional features, automation of key processes, and correction of newly-discovered security problems. Enterprise network administrators, facilities managers, and device owners face new challenges when applying these updates across a growing variety and number of IoT devices. Bob must manage hundreds of devices that are not only physically spread across his building but that also connect through multiple networks. Some of these networks are dedicated, some open access. Anne wants every assurance that any security flaw in Jamie's glucose monitor can be patched quickly. However, in the race to market, some manufacturers have designed IoT devices that do not accept software updates or do so in an insecure manner.

A typical device update process requires that software be retrieved from a remote location and transferred to the IoT device (Figure 4). In most cases a centralized controller initiates the update process. The process involves accessing a remote server, downloading a firmware image, verifying the image, and then updating the device.

[22] Ferreira, A., Correia, R., Chadwick, D., Santos, H.M., Gomes, R., Reis, D. and Antunes, L., 2013. Password sharing and how to reduce it. In IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 22-42). IGI Global.
[23] Hong, J., 2012. The state of phishing attacks. Communications of the ACM, 55(1), pp.74-81.

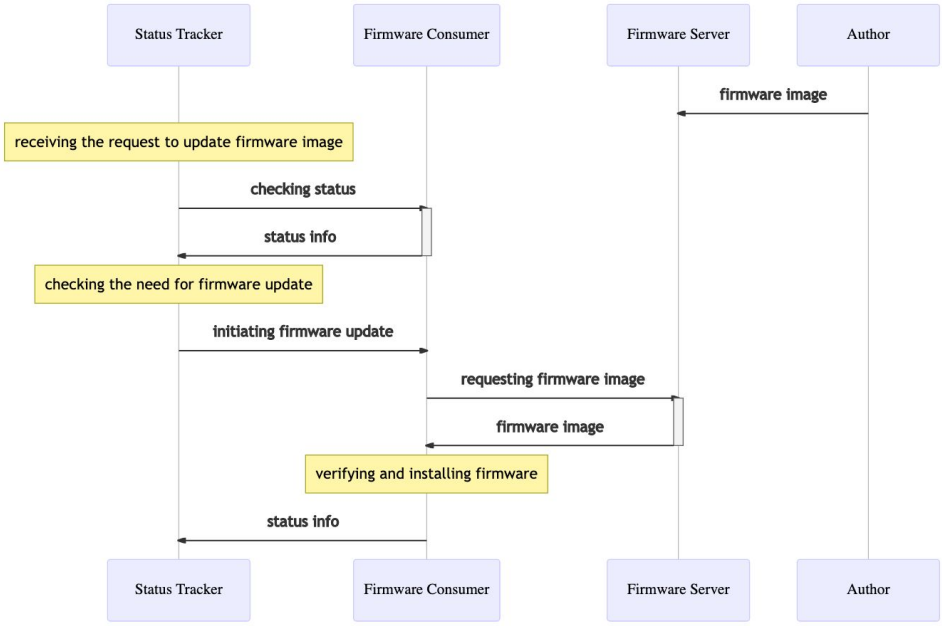

Figure 4: Secure software update process for IoT devices [24]

Definitions:
Firmware (FW) Consumers : stores and runs firmware on IoT devices
Status Tracker : check and monitors on the status of firmware inside FW Consumers
Author: produces firmware image of IoT devices and uploads it to FW-Server
FW Server : distributes firmware packages

There are multiple potential areas of vulnerabilities within this IoT device update process. Because of the wide deployment of single IoT device classes, a malicious party could leverage these vulnerabilities in a single attack vector to compromise devices at global scale.

6. Revalidation and Audit.

Revalidation is the process of confirming and authenticating device qualities or credentials, for example following a software update. Revalidation of a device might also be required if there are changes related to CIAM or WIAM for example if Bob gets a promotion, and a new facilities manager is employed.

Audit is not only an important tool for compliance which is crucial to many regulated industries, but also is increasingly used as an assurance tool within a dynamic risk management framework.

[24] ITU SG17-TD1547 Study Group 17 - Draft Recommendation ITU-X.secup-iot : liaison-2018-09-12-itu-t-sg-17-suit-ls-on-sg17-work-item-xsecup-iot-secure-software-update-procedure-for-iot-devices-attachment-1.pdf

7. Device De-provisioning, exit to end of life / recycling or resell.

Device de-provisioning is analogous with the 'Leavers' process in human IAM lifecycles, however within IoT, de-provisioning of a device that is often part of a system or network of devices has more significant security consequences than off-boarding a human for the overall service provision, and is often closely aligned with the provisioning or re-configuration of a new device to take over the function of the old one. At the point of de-provisioning, the hand-off to the next life stages of recycling or resale may include a change of contextual identifier.

SECURE COMMUNICATION

Currently, both enterprise and consumer IoT devices rely on transport layer encryption methods for secure communication (i.e., encryption of the wired or wireless path or medium). Transport layer encryption requires shared keys or certificates to authenticate the connection between devices and encrypt the path. However, application level encryption with optional path encryption is a preferred practice in many environments.

Protecting data as it travels on wireless or wired networks between IoT devices and their controller is very important. The telemetry data from Jamie's glucose meter must arrive unaltered, consistently, and to only the intended recipients. Today's secure IoT systems typically use well-established cryptographic protocols such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), to encrypt data as it travels between endpoints. These methods, familiar from the widely used https protocol, use certificates which have been pre-installed on each endpoint and rely on a public key infrastructure (PKI). Some IoT devices, particularly those aimed at consumers, come pre-installed with certificates signed by a publicly-trusted Certificate Authority. However, in the enterprise the experience is that trust levels of manufacturer self signed certificates vary widely. This results in enterprises issuing self signed certificates and adds the managing of a PKI to the list of responsibilities of the IT department. PKI Management increases in difficulty with every IoT device that is added to the network, as every device needs to have certificates generated, deployed and maintained.

ENSURE DATA PRIVACY AND INTEGRITY

As with Identification, Authentication and Authorization, this challenge needs to be expanded to "Ensure data privacy, integrity and provenance". The data supply chain needs to have the same level of ethical bar as any physical good or service. In our rapidly coming digital world, the requirement of providing a chain of custody of data will be key in establishing the principle of ethical data.

Establishing data privacy requires allowing access only to those people, software processes, applications, machines, or devices that are part of the authorization mechanism for that specific data set. In the context where an IoT device is interacting directly with an individual, explicit consent is essential to maintain compliance with current privacy regulation (i.e., concerning Personal Health

Information) as data is moved and stored through different media. However, many current IoT devices operate in a context of near zero human interaction, and instead rely on general access policies.

Consent must be granted by the subject of the data (e.g., Jamie) or their guardian (e.g., Anne). Coupling the consent directly with the data read from the IoT device is an optimum method of handling consent through a data flow. Consent could subsequently expire or be revoked, and there must be a method to then restrict access to this data. Trustworthy, dynamic consent mechanisms allow the creation of rich access policies that accommodate unforeseen emergency situations where the delegation of access to emergency services or medical professionals might be of value. Providing law enforcement and emergency medical personnel temporary access to Jamie's location data and blood sugar parameters might provide enormous benefit were he to go missing.

Not only is dedicated consent an important consideration for IoT device data flows, but maintaining the integrity of that data is also a key challenge. A variety of natural and malicious influences can corrupt raw data. Man-in-the-middle attacks are an example of a malicious influence that Bob must guard against in his IoT device data flows. Different encryption-based or fingerprinting of the data can help mitigate the risk to data privacy, confidentiality, and integrity. Even so, many current IoT devices rely on unencrypted communications, increasing these risks.

CHALLENGE SUMMARY

Jamie, Bob, and Bessie the Cow highlight the above technical challenges. We must address these challenges to both realize the value from IoT devices, and manage risks to safety, security, privacy, and profitability.

Jamie

For Jamie, who is living with dementia and diabetes, it is important that accurate readings from his glucose meter are delivered to the systems employed by his endocrinologist so that safe observations can be maintained. Any interference with these readings, and delivery of erroneous data either through accident or ill-intent, could cause distress, and even to lead to dire consequences. As Jamie's dementia worsens and he starts to wander, location information shared by his smart insoles will play a vital contribution towards recovering him safely. At these times, his family or care partners will want to share his location, and data from his smart soles with law enforcement, so that they can affect a rapid and safe recovery. Once Jamie is home again, it is important that his privacy is restored, and access to Jamie's personal data including location and blood data are brought back within its normal bounds. This level of granular control over data access is rare in current Machine to Person devices and services, constraining uptake and even feasibility of such services.

Bob

The Infrastructure Manager, Bob, must manage an increasingly-complicated array of constrained devices connected across a variety of public and private networks. Some of these devices are installed wirelessly and without connecting to power mains. Methods that require power-intensive

operations from these devices create a more difficult operational problem for Bob, where he must also then manage higher demand for battery replacement. These devices will routinely interact with third parties and must be managed throughout their lifecycle as they are installed, provisioned, updated, patched, and decommissioned. A scope of actors within the company requires varying levels of access to both individuals and families of devices. For example, the security staff will use the CCTV system, badge interrogation sensors, and connected door locks during the conduct of their duties, but they do not need to install or remove these devices. Reducing costs is a major value driver for Bob and a factor by which his performance is measured. Many of the IoT devices he installs have just enough resources for their intended purpose. Even so, the complex web of connections could create an attack vector to sensitive systems through a seemingly non-critical and unsecure component, such as the lobby fish tank thermometer or Heating Ventilation and Air Conditioning (HVAC) system service endpoint. Sensor telemetry data (e.g., room thermostat temperature) must also arrive without tamper or eavesdropping so that control systems function as intended. A robust protocol that encompasses all Bob's networked devices and allows simple, trustworthy management would help Bob realize value and minimize business risk for the company.

Bessie the Cow

Bessie the Cow's keeper must be able to easily identify Bessie and is required by law to report her birth and sirage, movements, health conditions (immunizations, illnesses, pregnancies). Recording this information is done both with paper and RFID based systems. The global food supply ecosystem has become extremely complex and the ability to securely, easily and quickly trace and identify sources of disease outbreak or tainted food products is critical to limiting the spread of disease and ensuring the safety of the food supply.

Solutions

JAMIE

Securing communications

Anne contacted her local diabetes and Alzheimer associations and discovered that she and Jamie could store all their personal information on their phones, and they could use a digital wallet (much the same as Anne uses today to pay for groceries) to establish secure communications with another digital wallet. Inside this secure connection, Anne could safely grant access to their personal data to the other party with confidence the other party was who they claimed to be. Currently, Anne doesn't know if others have access to the data from Jamie's glucose meter other than his doctor.

How can SSI help?

With the use of DIDcomm and Peer DID connections Jamie's glucose meter can connect securely to a smartphone. Peer DIDs are used to create unique secure identifiers known only to the glucose meter

and the smartphone. DIDcomm is a protocol that runs over existing industry transport protocols (BLE, NFC, HTTPS,...) providing a secure communication layer for the exchange of DIDs and Verifiable Credentials. In the DIDcomm exchange, encrypted messages pass between the two agent endpoints (smartphone & glucose meter). Each message is encrypted with the other party's public key and decrypted by the other party with their private key. As the shared keys exist only between Jamie's glucose meter and the smartphone, no one can impersonate Jamie.

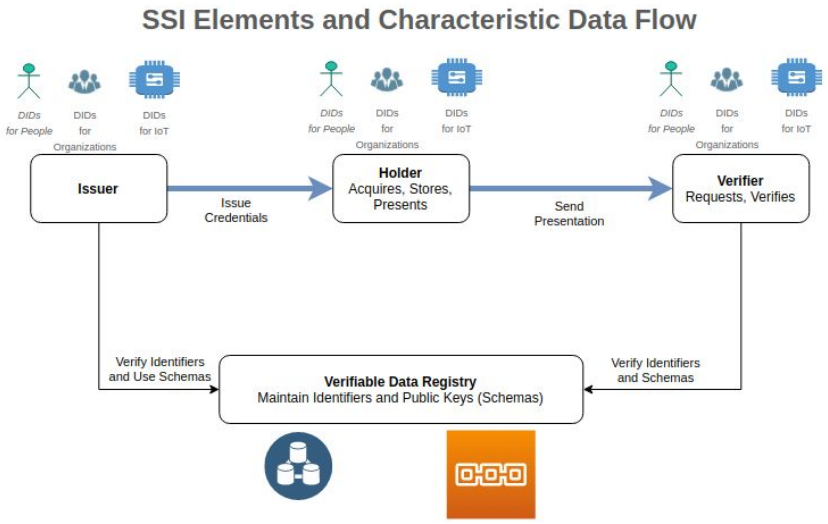

Figure 5: SSI elements and data flow

Ensuring authorized data exchange between devices

While Anne researched insulin monitor manufacturers she found one that looked promising, though she didn't know enough about the technology to be sure. IMX was the company who described how they interoperate with client pumps:

> "The first change in the relationship with clients is now they control the data produced by our insulin monitor. We work with PeaceOfMind, a trusted credential service company that issues credentials to IMX on behalf of the client. This credential gives IMX access to data from the monitor as it is stored in a special data container on the internet. Our monitor produces rich data sets, and this use of verifiable credentials for access and rich data semantics for data capture enable us to provide even better service to our clients. We can ship artificial intelligence models to the client's phone that can interpret the data and provide feedback to the client."

Curious, Anne researched PeaceOfMind further and learned that this was an organization that offered services to patients and their families who were faced with potential life threatening medical conditions, through the issuance and control of Verifiable Credentials. This sounded reassuring to Anne, and since there was only one manufacturer that offered her this kind of control and utility, she

contacted IMX directly.

The next innovation Anne explored was shoe inserts, she found only one credential-based product, the Boot.id company. Boot.id ships shoe inserts that include computer and communication devices that stream data about Jamie's biometrics, including an analysis of his gait, to Jamie's mobile phone. Like IMX, Boot.id relied on Anne (Jamie's guardian) to authorize PeaceOfMind to issue Boot.id a controllership credential. This (revokable) credential grants Boot.id access to the data from Jamie's insoles.

How can SSI help?

As above, by using DIDcomm and Peer DIDs to identify and connect ensures that only Boot.id is capable of securely exchanging data from Jamie's insoles. This process allows the data generated by the insoles to be provenanced with the insoles public key and encrypted using the Boot.id's public key ensuring only Boot.id can decrypt the data. By establishing a secure high assurance identity for the insoles in Jamie's shoes, it is possible to provide a defense in depth strategy for the devices keeping Jamie safe.

Ensuring data privacy

Being able to control Jamie's data has true value to Jamie only when Jamie can safely share that data with known entities. Another concern is which data gets shared. To protect Jamie's privacy, he needs to limit which data is visible, when, to whom and how. For example, if Jamie's age is important, Jamie's credential should have a data point for age, not date of birth. In other words, Jamie wants to maximize the value of his shared data while minimizing risk to his privacy.

How can SSI help?

VCs have been designed with the intent for sharing, delegation and revocation. The holder of the credential (or their legal guardian) can choose to grant temporary permission to another individual or organization access to the credential in its entirety or some subgroup of the claims included in the credential. For example, in Jamie's situation, Anne has been made his legal guardian, if Jamie goes missing, Anne can authorize PeaceOfMind to issue a credential to law enforcement granting access to Jamie's location data and his glucose meter readings for the duration of the search operation. The law enforcement agency would present this credential to Boot.id and IMX during the search & rescue operation. However, once Jamie is found and is safe, Anne can easily revoke the credential, fully restoring Jamie's privacy. The key here is that Jamie's guardian (Anne) has full control over granting and revoking access to Jamie's data.

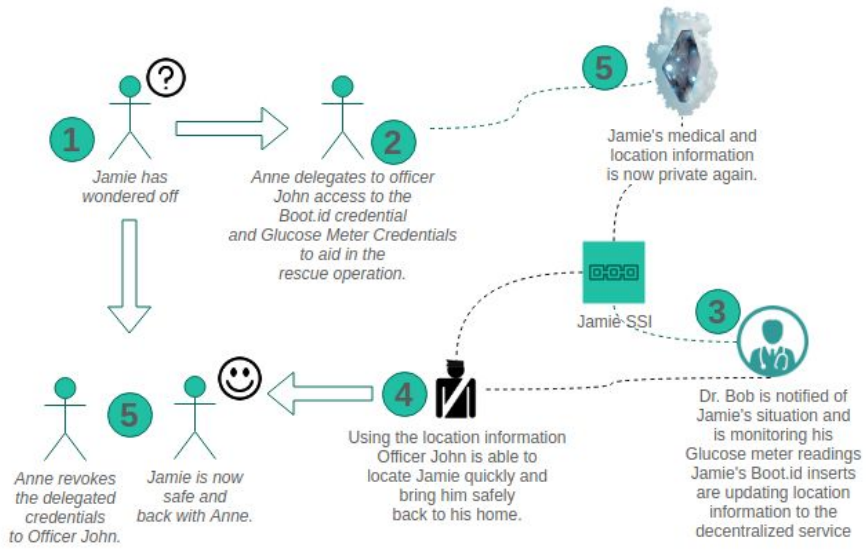

Figure 6: SSI in rescue operations

BOB

IoT in the Enterprise consists of both controller and non-controller based systems (local and cloud hosted) and covers a large spectrum from HVAC and building facilities to corporate business services including lighting, security doors, physical access points, room temperature sensors, motion sensors, booking panes and on-person things. The types of IoT devices are constantly expanding and they use different mediums and security measures depending on the business units that own and control them.

Bob has commissioned an IoT asset management platform in a bid to manage all this complexity. This is an AI enabled software/hardware package designed to manage a wide array of equipment and sensors in industrial facilities or commercial buildings including IoT devices with their own digital identities and credentials, together with data management and storage. The platform itself also has its own digital identity and credentials. A human operator oversees critical actions, business rules and decision algorithms of the system, while many IoT communications and actions are handled automatically.

The new asset management solution will help Bob and his team implement efficient and consistent device monitoring, maintenance, automation and presence, yet a number of obstacles remain.

Number of devices & networks to manage

Currently the system relies on pre-shared keys or self signed certificates and PKI to Authorise and Authenticate IoT devices. While the current methods provide a measure of security, as the number and range of devices deployed increases, the risks of a security breach also increase as a result of increased complexity and overhead of device administration. Bob is conscious that not all devices in the building have been issued with certificates, while others probably have certificates that are no longer valid.

How can SSI help?

DIDs can be both public and private. In Bob's scenario there is a value using both. If the manufacturer has a public DID that is encoded into the device, the immutability of the blockchain and the ability to correlate this DID to the manufacturer increases Bob's confidence and assurance that updates and credentials on the device are legitimate and not compromised.

When Bob connects the device into his network there will be an exchange of private DIDs (or Peer DIDs) between the controller and the device. These peer DIDs have two functions, first to ensure the identity of the devices on either side, and second to create a secure communication channel between the devices.

DIDs and VCs provide a global means to establish the identity of IoT devices, people, and organisations. This enables Bob to standardise the management of both Machine To Machine interactions (e.g. CCTV cameras uploading their footage to a server) and Machine to Person interactions (e.g. doorways controlling entering and exiting of restricted areas).

The use of DIDs and VC's in the asset management platform and wider IT ecosystem will increase security by ensuring all IoT devices are able to definitively self-identify and authenticate. Centralised management of the process of issuing DIDs and credentials improves and simplifies device management workflows, reducing errors such as out-of-date certificates.

Access control for a large number of personnel

Smooth operations on Bob's trading floor depend on people, assets and physical access points continuously and securely exchanging data. Joiners and leavers of both devices and people are a security risk and a compliance challenge that must be continually managed. The building's systems and IoT devices are attached to a range of different networks, meaning it can be hard to confirm that all a leaver's credentials have been revoked across all systems.

Physical moves are frequent within the Financial Services industry and present an additional headache for Bob. Disconnecting and reconnecting physical access points to the network during moves is a manual and time-consuming process: each access point must be individually configured, joined to controllers and certificates validated.

How can SSI help?

SSI enables fine grained access control policies to be implemented across all building systems and access points via the IoT asset management platform's control panel. Credentials can be dynamically revoked, removing the risk that access to some systems is unwittingly maintained.

> *Revocation of credentials is a critical element in ensuring integrity of the overall ecosystem. There must be a means to allow the issuer of a VC to revoke the credential without having to interact directly with the credential holder. Likewise, the entity verifying the received credential needs a means to validate the VC is still valid without checking with the Issuer. This is very important to maintain privacy and prevent correlation. This is done with the use of a Revocation Registry. (For more information on the technical details of revocation see here.)*

Public DIDs are attached to physical access points, private pairwise DIDs and Verifiable Credentials reside in a digital wallet on employees' personal devices, enabling authorized employees to satisfy a proof request and gain access to the IoT enabled service. For example, rights to access a department's document printer could be embedded in a VC[25].

Device control, upgrading and replacement

Bob is responsible for ensuring new devices are securely provisioned onto the network and that all devices are protected by certificates and running the correct version of software. It's hard to keep track of this, as updates are currently managed by different teams.

The increasing prevalence of cameras and low-power sensors on the network is a worry, as Bob knows these types of devices are hard to secure and can potentially create a backdoor onto the network.

How can SSI help?

Decentralised Identifiers can be contained within lightweight software suitable for constrained devices and provisioned onto diverse devices. Authentication by Verifiable Credentials by a traditional IAM solution can be managed through the use of SIOP DID Profile [26] *or Verifiable Credential*

[25] Lagutin, D., Kortesniemi, Y., Fotiou, N. and Siris, V.A., 2019. Enabling decentralised identifiers and verifiable credentials for constrained IoT devices using OAuth-based delegation. In Workshop on Decentralized IoT Systems and Security (DISS 2019), San Diego, CA, USA.

[26] https://identity.foundation/did-siop/#op

Authentication via OpenID Connect. [27] *Either of these mechanisms enable the use of Verifiable Credentials through the existing OIDC-core standard.*

For devices that have the minimum capability to support SSI, agents and wallets can be added to the IoT device. If the device does not meet the minimum requirements, then the use of a trusted Proxy Server as defined by the draft IETF Authentication and Authorization for Constrained Environments standard [28] *can provide the capability required.*

With SSI it is easier to add and remove both users and devices, streamlining user administration, device configuration and setup, increasing productivity of the network team.

Once added to the network, devices can be set up to generate and register their own network identity; the Service Discovery element within the DID specification creates the possibility of automated device on-boarding. DIDs can be rotated and revoked for added flexibility and security, [29] [30] *without the need to involve a third party Certificate Authority at additional cost to the bank.*

Bob is now fully in control over the process of keeping device software up to date. By assigning DIDs and VCs to software servers, Bob can confidently automate the process of issuing firmware updates, knowing his devices can only communicate with authorised parties. He can even require multiple parties to sign updates for critical devices.

Meeting legal and safety requirements

Within the financial services industry, regulatory requirements are steadily increasing. Bob will need to provide a credible audit and validation capability to show compliance with these regulations, support insurance requirements, and meet health and safety mandates. User access and device histories for the trading floor of Bob's building are distributed across a variety of databases. The distribution of these databases makes it challenging for Bob to consistently prove regulatory compliance. Persistent record-keeping requirements and frequent audit requests require Bob and his team to perform extensive ad-hoc data gathering, reduction, and sharing, a labor-intensive process.

How can SSI help?

By implementing SSI in the bank's network of connected devices, either in-house teams or third party auditors can complete compliance requirements in an easily-verifiable and tamper-resistant way.

Metadata associated with data transmitted from an SSI-enabled device can be packaged into a VC and signed by the transmitting device, attesting to the data's credibility. Because the VC is a

[27] https://github.com/bcgov/vc-authn-oidc/blob/master/docs/README.md
[28] draft-ietf-ace-oauth-authz-24 - Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)
[29] What if I lose my phone?
[30] https://dhh1128.github.io/zkpcreds/trust-paradox-rebuttal.html (see especially section 4).

cryptographically-secured data structure, the data are both identified and tamper-resistant, meeting the "non-repudiation" security requirement.

SSI strongly enables GDPR compliance. DIDs and VCs are fundamentally based on a privacy-by-design approach. For example, DIDs and VCs enable selective disclosure and data minimisation principles in the credential presentation process. This facet of the presentation process enables a stream-lined "right to be forgotten." Further, SSI reduces the amount of data shared by selectively providing only that data requested, avoiding unnecessary exposure of Personally Identifiable Information (PII).

BESSIE

Identity

Every cow in Bessie's herd must have an identifier. Today at birth every animal is tagged (whether a live birth or not) and must be reported to governmental organizations. While historically this identifier has primarily been used for disease management increasingly this identifier is the link to her digital twin. Throughout Bessie's life her digital twin will be updated with health related information, movement and sale data.

Even though Bessie's data is now stored in a Herd Management System, data collection in the field is still a manual and time consuming process.

How can SSI help?

By extending the current identity model to include Decentralized Identifiers and Verifiable Credentials integrity and security of the information being recorded is increased. By giving each animal its own DID the owner of the animal now has the ability to create a secure delegation credential for Bessie. This is of particular value when the owner of the cow is not the keeper. Additionally, the DIDs and VCs of persons who interact with Bessie (vet's, keepers, transporters) during her life can now be linked to her digital twin.

Scalability

Farming is a tough business, the ability to easily, quickly and accurately collect all the information needed to manage a herd and meet regulated reporting requirements is key in keeping a farming operation viable.

Once the cow has been sold and has departed the rancher's custody, the rancher has limited to zero visibility into the downstream custody of Bessie's products. Downstream supply chain partners receive some data, such as the Country of Origin, Farm name/address/contact information, certifications, if any, and veterinary records. These records may be in paper form or electronic.

When slaughtered and processed, a typical beef cow like Bessie can be broken into up to 400 individual meat products. One important data requirement of any IoT system tracking beef includes the ability to associate each individual product ID back to Bessie's identity and records.

How can SSI help?

By linking Verifiable Credentials (VCs) of every interaction with Bessie (vetting, movement between farms, sale) help ensure that Bessie's data — and the data from the products that are created from her — have been cryptographically secured. As mentioned above, these VCs link back to the identification of the persons (and their certifications) that have provided these services.

For example, if Bessie has been sold as an organic, hormone free cow, or as a Kosher or Halal the VCs that state this will link back to the individual and certifications that attest to these claims.

Through VCs, we can ensure that bad actors downstream within the supply chain cannot alter Bessie's records. In an insecure system, someone could alter Bessie's credentials to show her as "certified USDA Organic" and command a markup on all 400 products.

VCs can also ensure that the sensors used in Bessie's lifetime are in fact the ones assigned to her since birth.

Movement and transfer of ownership

In many instances Bessie may be managed by someone other than her owner. It could be that the owner of Bessie has leased some land to keep their herd on, or that Bessie is included in a larger herd that is owned by a consortium of investors. The keeper of the herd is managing the herd on behalf of the investor owners.

Every movement of a cow is required by law to be reported as well as the health/immunization status of the animals being transported. The keeper of the animal is required to supply the Cattle Passport for each animal with each transfer of possession (not necessarily ownership).
In a perfect world, data about Bessie — health, dietary and certifications — has been captured by the keeper on a regular basis and is stored within a herd management platform. This *origin* data would be transferred to the next custodian of Bessie: likely, the logistics company delivering Bessie to an abattoir, kicking off a digital chain of custody.

How can SSI help?

In the prevention of fraud or theft when Bessie is managed by someone other than her owner, the owner can issue a delegated Keeper Verifiable Credential, that is linked to Bessie's DID. The lack of an 'Ownership' credential would prevent the illicit sale of Bessie, protecting the owners' investment in Bessie.

In addressing the processing of movement filings, by linking Bessie's DID to a movement VC, an audit chain of where, when and whom is created. This chain of evidence can be supplied to regulating authorities.

Owners are concerned with maintaining the health of their animals, even when transporting to an abattoir. An animal that is not cared for properly (fed, watered) while in transport does not reach the final sale point in good health. This impacts the price the owner will receive for the animal. By linking the animal's DID to an IoT sensor in the truck carrying them that is recording ambient temperature as a VC the owner and purchaser now have a secured, accurate record.

Data security and data sharing

As in many supply chains, the production of food is still a heavily paper based industry. Every cow on a farm must have a passport that identifies and records all information on the animal. As a paper based process, this is wide open for error or fraud, even with handheld RFID readers and electronic herd management systems the data is recorded in proprietary systems with limited data sharing capabilities.

How can SSI help?

First by securing the sources and chains of data. By using cryptographically secure Verifiable Credentials that are linked to the various parties involved in the care and raising of beef cattle, transparency is brought into the food supply chain.

With the elimination of paper based records, and the use of interoperable, open source, Open Standards based DIDs and VCs regulators and all stakeholders of the cattle industry will gain efficiencies in their operations through the reduction of manual processes and the increased integrity and assurance of the whole supply chain.

Business Value of SSI in IoT

INCREASE REVENUES

Whole new classes of business opportunities are created when identity, privacy and data accuracy are enabled at a very low cost point. These attributes of SSI in IoT build trust and reduce security risks enabling the application of IoT in higher value use cases. For example, within the healthcare sector moving from telemedicine (Jamie takes the blood sugar monitor reading and reads it out over the phone to his doctor), to personalised or precision medicine (Jamie's blood sugar monitor automatically connects with a diabetes management service).

It also opens the way for new, networked business models in the Machine to Machine IoT space. For example the business models of vendors supplying the individual components within a smart building

can be connected, with data flowing freely between their devices. These data flows could be underpinned by smart contracts that automatically remunerate the data producer, providing an incentive for disparate vendors to participate in the ecosystem.

REDUCE COSTS

A typical Enterprise IoT network requires multiple API connections to be established and maintained in order to ensure identity, trust and interoperability across devices and vendors. Custom software development is frequently required in order to add new vendors and service providers. Changes to APIs create the need for firmware updates to all connected devices. The operational costs of maintaining such networks escalate rapidly as the size and complexity of the network grows.

Once SSI is added, devices can identify, authenticate and communicate directly with other devices and apps, including those from other vendors, reducing the costs of API and firmware maintenance. A verifiable record of each device's history is available to be queried during the authentication process, increasing trust and facilitating serverless data exchange.

SSI-enabled devices can provide businesses with access to structured, semantically-rich attestations of device data quality, overcoming several basic shortcomings of established methods used to verify digital assets through public and private key signatures.[31] Increased standardization in the sharing of these datasets and provenance will enable business processes automation with greater confidence, further reducing operating costs.

SSI can also facilitate compliance with auditing requirements - a growing burden in industries such as financial services and life sciences - by providing an immutable record of key events and interactions that is available for inspection by third parties.

REDUCE RISK

For any business, the financial impact of a data security breach is significant. Research by IBM suggests the direct costs of an enterprise data breach average $3.92m.[32] The indirect costs can be far higher: according to research released by Comparitech in November 2019, the share prices of companies disclosing a data breach fell by an average of 7.27 percent. Two years later, breached companies were found to underperform their index by -13.27 percent.[33]

SSI enhances the security of IoT networks and minimises the risk of cyber attacks by enabling businesses to standardise device provisioning and management and extend PKI across all connected devices. SSI-enabled devices can use any suitable cryptographic method to validate their identity, meaning the benefits of cryptographic protection can be extended to a wide range of devices

[31] Certifying Provenance of Scientific Datasets with Self-sovereign Identity and Verifiable Credentials
[32] 2019 Cost of Data Breach Report
[33] How data breaches affect stock market share prices

including low-power units with basic 8-bit microcontrollers.[34] Even simpler devices can be secured with SSI by combining DIDs and VCs with a delegated authorization framework such as OAuth. Incorporating DIDs and VCs in IoT also promotes GDPR compliance, as the technology features privacy by design.

BUSINESS IMPACT: JAMIE

Jamie's case is one example of a growing number of Machine to Person IoT services that help improve clinical management and keep patients safe by providing physicians and emergency services with real-time access to critical medical data.

However, privacy and security risks are a key barrier that can adversely affect patients' and clinicians' level of trust and willingness to adopt and use such services[35].

SSI provides a viable means to address these concerns. In Jamie's case, this entails using Verifiable Credentials to ensure only authorised entities can access Jamie's personal medical and location data - with the access conditional on a live emergency in the case of blue light services - and DIDcomm to assure data privacy during transit.

Jamie's use case is predicated on being able to preserve his privacy absolutely, given the sensitive nature of his medical and location data. SSI is uniquely placed to satisfy this requirement and has great potential to unlock demand for similar use cases.

The business opportunity for such services is clear: the global telemedicine market size was estimated at USD 41.4 billion in 2019 and is expected to witness a CAGR of 15.1% to 2027, with the coronavirus pandemic expected to boost demand for solutions that enable caregivers to maintain communication with their patients and to actively manage them during adverse conditions[36].

We can not put a quantitative dollar value on what IoT devices like the biometric insoles and digital identity will save public safety in the search for missing persons. They will certainly enhance the investigation and speed up locating Jamie thorough data obtained. Law enforcement will be provided a timely notification through Jamie's insoles that he fell. Through his verified credentials they will know Jamie requires assistance and obtain verified data like: name, next of kin, location, weather, and vitals. This trusted information will allow law enforcement to send the proper resources to assist Jamie with his emergency, i.e. medical care, search personnel, support resources like helicopter, canine, high angle rescue.

This data will enable law enforcement to determine the urgency of the call while being dispatched and ultimately reduce the time required to locate Jamie and return him to his family with the goal of finding him in the best possible condition in the shortest amount of time. The primary value will be reduced man hours and resource deployment. Helicopter fuel costs approx. $1,500/hour, not including flight crew wages or maintenance costs incurred by flight time for missions. Ground searcher costs

[34] Improving the Privacy of IoT with Decentralised Identifiers (DIDs)
[35] Privacy and Security Concerns in Telehealth
[36] Telemedicine Market Size, Share, Growth Report, 2020-2027

like fuel and wages are typically not calculated as they are covered by other budgets. Ancillary benefits will be SAR resources available for other calls, reduced equipment maintenance, such as helicopter hourly maintenance. IoT devices typically allow SAR resources to go directly to Jamie for the rescue vs the traditional search and rescue model which exists without the aid of locating technologies.

Ultimately law enforcement's involvement will be significantly reduced because Jamie's care partners will be able to bring him home safely the majority of the time without involving them.

BUSINESS IMPACT: BOB

To quantify the business benefits of streamlined SSI-based IoT network management let's return to the case of Bob, network manager of a regional trading floor at a well-known bank.

The network comprises around 200 IoT devices including networking kit, physical access points, meeting room panels, cameras and door locks. Provisioning & maintenance of PKI certificates tends to be manual and ad-hoc, with responsibility split across the Windows, Network, Security and Facilities teams depending on device type.

The rigour of certificate deployment is currently uneven at best. Processes to track, verify, update and revoke device certificates are inconsistent or absent, and it can be difficult to ascertain who is responsible for a given device (or whether anyone took over when they left).

These challenges are getting exponentially harder as the number of devices connected to the network grows. In response, Bob selects an SSI based solution to run alongside the existing IAM platform. Over time, IoT device management is transitioned to the new solution, resulting in the following business outcomes:

	Existing IoT Solution	New SSI based solution
Nature of device credentials	"This device is protected by a certificate issued by a trusted Certificate Authority"	"This is Device ID 12345"
Nature of data credentials	"This data was created by a device protected by a certificate issued by a trusted Certificate Authority"	"This data is signed by Device ID 12345"

Provisioning & maintenance of certificates / DIDs	Responsibility sits across multiple teams, since different device types are managed by different business units.	One person / team is now responsible for the entire IoT estate Every deployment looks the same – device type is irrelevant
Expected time requirement to deploy and manage certificates / DIDs	1.0 Full Time Employee (split 70% device administration, 30% compliance across the year)	0.7 Full Time Employee
Expectation re % of devices with correctly deployed certificates / DIDs	75% will be deployed as intended (e.g. deployed with a pre-shared key)	95%+
Expectation re % of devices with correctly maintained certificates / DIDs	5-10% of devices have no certificate 5-10% of devices have out of date / otherwise invalid certificate	95%+

Source: based on real-world deployment

The key outcomes following transition from centralised PKI to SSI based device management are enhanced IoT network security due to increased compliance with device onboarding and software updating protocols, together with a 30% reduction in time spent on device management.

BUSINESS IMPACT: BESSIE

The business impact of adding DIDs and VCs into the meat supply chain can close (or severely reduce) one source of fraud that plagued the industry ever since its creation, the proof of ownership of the animal (otherwise known as 'rustling'). Today, ownership is represented by paper records and possession of the animal. If the animal is being kept on leased land or is being managed by an intermediary of the actual owner, the ability to modify records and illegally sell the animal is not difficult and continues to exist.

With the introduction of DIDs and VCs the ownership credential is maintained by the owner and only a delegated keeper credential is issued to the individual or organization managing the animal. Closing an age old gap in the process, as the credentials are connected to the secure DID of Bessie. Without this provenance chain, sale of Bessie into the high value food chain is not possible.

Second, is the creation of a cryptographically secure data graph of all the interactions with Bessie over her lifespan. This would include the VCs of specific immunizations, linking back to the manufacturer, batch, production date,.. . the licensing credential of the Vet who cared for Bessie, the operating license credential of the transport company that moved Bessie from farm to abattoir and finally the processing of Bessie as being slaughtered in accordance with Kosher regulations with the credential of the Rabbi that observed the process.

Finally, by leveraging the interoperable, open source and open standards of the DID and VC technology, the cattle industry can eliminate many of the paper based problems that exist in all supply chains (lack of transparency, loss of paperwork, fraud). In industries where supply chains are long and complicated, use of interoperable open standards greatly reduces the processing times of paperwork at each ownership transfer point.

With Verifiable Credentials all stakeholders can easily check and verify the origin and transformation (or growth) path of the animal from conception to meat processing to delivery to shelf.

IMPLEMENTATION AND RUNNING COSTS

Throughout this paper we have used the three personas of Jamie, Bob, and Bessie to illustrate the business benefits that SSI brings into the IoT sector. However, any business case also needs to consider the costs of implementation and maintenance.

The ever-growing range of IoT devices, from cars to water and wind sensors, feature varying resource profiles (storage, power, compute, memory). When designing any IoT network the resource profile of existing and new devices needs to be factored into the overall solution. Over the past five years the availability of MCUs that are capable of supporting required cryptographic functions has both increased and the costs have come down significantly. However, they are slightly more expensive than non-cryptographically enabled devices. It is critical that the market communicate clearly to IoT device manufacturers and innovators, that cryptographic support is no longer a perk or luxury item, but a 'must have' in the effort to close the security holes within the IoT sector.

As with all IoT sectors, support of older or constrained devices in the network is very much a requirement. SSI solutions can support older devices through the use of proxy based or hybrid solutions to facilitate encryption and key management.

SSI can be integrated into existing enterprise IT infrastructure without replacing or modifying legacy applications by leveraging existing elements of the current OpenID Connect and OAuth2 standards. [37] [38] [39] For example Evernym's Verity platform enables organisations to issue DIDs to devices via a

[37] https://github.com/bcgov/vc-authn-oidc/blob/master/docs/README.md
[38] https://identity.foundation/did-siop/#op
[39] Improving the Privacy of IoT with Decentralised Identifiers (DIDs)

central console, IDRamp enables SSI to be combined with existing corporate logins, and Ockam's serverless solutions enable developers to remotely provision DIDs via a simple API call.

The costs of implementing and maintaining SSI based IoT security stem from internal software development effort and/or fees charged by SSI solution providers. Solution providers use varying cost models including fixed subscription fees, variable data transaction fees or a combination of both. Implementation costs are likely to be competitive with other standards-based solutions such as X509 certificates, since DID methods obviate the need for central certificate authorities and generally seek to minimise the amount of data that is written to the ledger.

In closing, SSI based identification and credentials provides the market a means of

1. Establishing high assurance identity of the devices participating in their networks
2. Provenancing data being supplied to the networks they are connected to
3. Allows IoT devices to identify and authenticate with high assurance the commands and updates they are receiving
4. Provides a means of delegating capabilities to other network participants while never surrendering ultimate control of the device (or thing).

Conclusion and Next Steps

Throughout the paper we used the three Personas of Jamie, Bob and Bessie to illustrate five of the top ten current security challenges in the IoT sector. SSI technologies of decentralized identifiers, verifiable credentials and the DIDcomm protocol provide novel mechanisms to close these gaps.

We have presented not only the technical opportunities, but also the areas of business value that can be unlocked when things are assigned durable identities and verifiable authorities.

SSI has potential to create value for any organisation invested in the Internet of Things.

1. It allows IoT-enabled businesses to save on operational costs and grow IoT networks faster through streamlined device lifecycle management.
2. It can dramatically reduce data liabilities and cybersecurity threats by providing a simpler and more consistent means of securing diverse IoT devices and enabling them to communicate securely.
3. SSI enables new IoT ecosystems and higher value use cases based on the value of verifiable data and enhanced trust and security that are derived from deploying SSI.

These benefits will come to the fore as IoT devices and networks continue to proliferate.

TRUST OVER IP FOUNDATION

A Self-Sovereign Identity ecosystem requires coverage of three dimensions, the technical challenges, the business opportunity and the governance of the ecosystem. This paper has covered the technical challenges and business opportunities, it has not covered the governance concerns. Governance is about the technical controls and business processes that establish and maintain the trust layer to create confidence in the operation of an ecosystem.

This is the objective of the Trust over IP Foundation, a new Foundation [40] under the Linux Foundation that is focused on defining the trust frameworks required to have high assurance digital identity in a purely digital world. The Task Force recommends the coordination and relationship with ToIP in the definition of IoT trust frameworks be included as part of a charter for a future SSI and IoT Working Group.

AREAS FOR FURTHER RESEARCH

As with any effort of this nature, the number of questions being raised at the beginning of this process has increased with greater understanding of the problem space. The task force deliberately put many of these questions to the side in order to complete the task at hand. Areas of future research for a formal SSI in IoT Working Group would be:

- Cryptography and encrypted data storage on IoT devices
- Data supply chain, creating a custody chain proving provenance of data with DIDs and VCs
- Interoperability of DID IoT agents and credential exchange
- Identity provisioning, quantifying cost savings
- Trust and governance frameworks for IoT
- How SSI measurably reduces risks around IoT
- Role of credentialing AI for IoT devices
- How SSI interacts with IoT hubs/controllers
- Interactions between SSI and IoT protocols (CoAP, MQTT, OSCORE, etc.)
- SSI, IoT and Zero Trust Networks

DOCUMENT MANAGEMENT

Authors

Richard Allain, Iain Barclay, Duwane Bryan, Bruce Conrad, Michael Corning, Todd Gehrke, Damian Glover, Nicky Hickman, Robert Mitwicki, Michele Nati, Chris Raczkowski, Tony Rose, Pierlugi Riti, William Sanitago, Mark Scott, Michael Shea, Scott Warner, Jamie Stirling, Eric Weaver, and special mention to Bessie the Cow.

[40] Trust Over IP - Defining a complete architecture for Internet-scale digital trust

With thanks to members of the Sovrin Guardianship Task Force and Sovrin Governance Framework Working Group for their time, knowledge, and expertise in bringing the paper to life.

Revision History

Date	Version	Author(s)
March 2020	0.1 (Initial working draft)	Team
June 30, 2020	0.5 (First release candidate)	
July 17, 2020	0.7 (External Review)	Steve Babbage, Nicky Hickman
July 30, 2020	0.8 (Second release candidate)	Team
August 30, 2020	1.0 (Final Release candidate)	Team

How to cite this white paper:

The Sovrin Foundation (2020), Self-Sovereign Identity and IoT (A whitepaper on the security opportunities and business potential for self-sovereign identity with the Internet of Things)

Disclaimer

PLEASE NOTE: THE INFORMATION PROVIDED BELOW IS FOR INFORMATIONAL PURPOSES ONLY AND MAY NOT BE RELIED UPON BY ANY PARTY AS LEGAL ADVICE. PARTICIPANTS IN THE SOVRIN NETWORK SHOULD CONTACT THEIR COUNSEL TO OBTAIN ADVICE WITH RESPECT TO THE POTENTIAL APPLICABILITY OF THESE, AND OTHER LAWS TO THEIR INTERACTION WITH THE SOVRIN NETWORK.

Copyright

Appendix 1 - Digital Twin

DEFINITION

In essence, there is a real thing in the physical world, and there is its digital representation. The latter can be referred to as the former's *digital twin*. For example, a business has an accounting system, which is a set of data and computational processes. Taken together, these data and processes are a digital representation of the business, or its digital twin.

Another term in common use, introduced by AWS,[41] is "device shadow" which consists of the data representing a device in the physical world. For IoT, we would prefer the term "digital twin" because *not all things are devices*. Furthermore, we are interested not just in the data, but in the processes as well.

According to Wikipedia, [42] "The digital twin concept consists of three distinct parts: the physical product, the digital/virtual product, and connections between the two products." The connection is referred to by GS1 as a "digital link" [43] and reified as a UPC code or other tag affixed to a product which connects it with its digital representation.

CAPABILITIES

The digital twin is more than data, but includes computational capabilities. The digital twin should react to events it receives from the physical device or about the physical thing, in order to update its state. It should also respond to queries from interested and authorized parties to provide information about the physical thing's current or historical state. In some cases commands may be given through the digital twin to an actual device.

Some IoT Devices are connected to the Internet, and are capable of communicating directly to their digital twin. Other things do not have communication capability, but can still be considered to be on the Internet because their digital twin is there, so it is possible to make everything "smart" [44] simply by tagging the thing with a machine readable code. Then when a person scans the tag, an event is sent to the thing's digital twin and appropriate action is taken therein.

As an example (elaborated below), Jamie has a simple, unconnected device for measuring his glucose level, in case he ever needs to do it manually. Anne has given this device a tag, so after taking a reading Jamie (or Anne) would scan the tag and enter the reading into the digital twin of a thing-on-the-internet which we might call "Jamie's glucose level".

---

[41] What is AWS IoT? - AWS IoT
[42] Digital twin
[43] Digital Link - Standards
[44] squaretag

LIFECYCLE

The digital twin of a particular item could be created as early as during product conception or production. When an item goes to a dealer or wholesaler, its digital twin would go with it. Ownership of the digital twin (as represented by a new private key) transfers along with ownership of the physical thing. When the item is sold, both the physical item and its digital twin become the property of the consumer, who now controls both. Hosting of the digital twin might still be provided by the manufacturer (or dealer) but could in principle be hosted by the current owner, probably through a service provider.

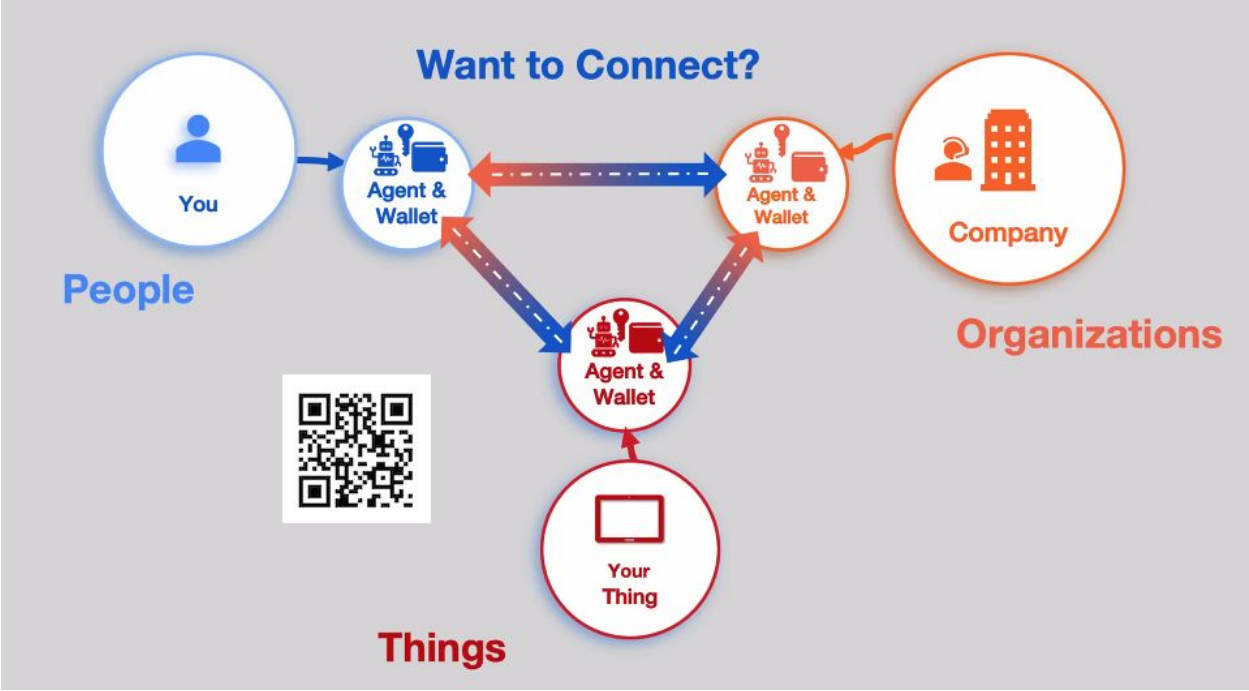

Figure 7: SSI and digital twins

In the Figure 7, from, [45] the "Agent & Wallet" bubbles are digital twins of the Company, the Thing, and the person respectively (starting at upper right and moving clockwise). The connections (the wide, two-lane arrows) are created in that same order: As the thing is being manufactured, as it becomes owned by the person, and as the owner decides to communicate with the manufacturer. The terms "Agent" and "Wallet" are in common use in the SSI ecosystem, and these act as digital twins. Narrow arrows show the "digital link" in each case.

As permitted by the owner, the manufacturer may receive notifications and/or data from the thing's digital twin. In this way the manufacturer can collect useful information about how the item is used and how it is performing. In the other direction, again under the owner's control, the manufacturer may provide recall notices or other information of interest to the owner.

[45] "The future of communication is DID Comm", Vic Cooper, IIW 30, April 2020

When an item, say a car, is sold by its original owner to another person, the digital twin could go with the car. The original owner could first, while leaving in the maintenance history, remove the trip history from the digital twin, as part of the sale process.

Eventually the item will have reached the end of its useful life and will be owned by a junkyard or be in a landfill. The digital twin may still continue to be useful, but may eventually be scrapped.

EXAMPLE

Jamie's FreeStyle Lite is a device (but *not* an IoT device) and is sometimes used to measure his glucose level (normally, his subcutaneous device is taking measurements periodically and sending them to the digital twin owned/operated/controlled by its manufacturer, IMX).

Connection with digital twin

Anne has attached an identifying tag to it. This allows for it to be connected to a digital twin (owned/controlled by Anne and Jamie) when one of them scans the tag with a smartphone.

The device itself looks like this (Figure 8) (note the attached QR Code [46] [47]):

Figure 8: Glucose Meter

[46] squaretag

[47] QR Codes and RFID chips are not the only ways to tag something which itself has no connectivity. A couple of other new things: from MIT: https://news.mit.edu/2020/cryptographic-tag-supply-chain-0220 one millimeter-sized chip that includes cryptography and from UCSD: https://ucsdnews.ucsd.edu/pressrelease/new-chip-brings-ultra-low-power-wi-fi-connectivity-to-iot-devices?_ga=2.105314950.463686660.1582114694-527546069.1579867513 a low power WiFi chip smaller than a grain of rice

When the owner scans the tag

After taking a reading, Jamie (or Anne) would scan the tag, and see a form on the smartphone with one box to fill in -- the reading number -- and the keyboard set to numeric. Upon entering the three digit number, the reading will be recorded in the digital twin (on the Internet).

When a third party scans the tag

If someone else scans the tag, perhaps because they found the device sitting on a bench at a bus stop, they would see a message like this:

Figure 9: Proposed lost item message

Anne could have set up more detailed contact information, or she could do that only when she realizes the device has been lost, perhaps even offering a reward.

Digital twin web page

The figure above shows that the device, or more accurately it's digital twin, has a public web page. But it also has a private web page, viewable by its owner.

When logged in to Manifold (an open source personal digital twin management solution [48]) on her laptop or tablet, Anne would see the digital twin (along with those of other things she owns) represented by a card looking like this:

[48] Manifold - Thing Management Platform, Picolab/Manifold: An IoT application to manage your Pico Device Shadows

Figure 10: Digital twin card

Integration possibilities

Jamie's subcutaneous monitor sends its readings through the IoT to a digital twin maintained by its manufacturer. If the manufacturer allows this functionality, Anne could provide a webhook that would update her digital twin, so that automatic and manual readings could be combined into a single data stream, owned and controlled by Anne and Jamie (note, HIPAA would have to be satisfied as well).

Connection in this way of a simple (i.e., not "smart") device to a digital twin for the purpose of keeping data it produces, has been called an "activity context" [49] (and the activity is itself a "thing" on the Internet, and therefore part of the IoT).

[49] Activity Contexts in SquareTag