Generalization of Secure Wearable Authentication through Self-Sovereign Identity and IoT Parallels

Jordan C. Hazelip
California State University, San Bernardino
Dr. Joon Son*
California State University, San Bernardino
Vijay Bhuse
Grand Valley State University

Abstract
This article delves into the inherent limitations of secure wearable devices while highlighting the potential of Self-Sovereign Identity (SSI) as a forward-thinking authentication solution. It offers a critical analysis of the restrictions tied to wearable devices, including their size, computational capacity, battery life, and battery drain caused by the computational demands of additional authentication protocols. Conversely, SSI pioneers a decentralized, user-centric paradigm in authentication, equipping users with complete control over their personal identity data. This groundbreaking approach can be seamlessly incorporated into secure wearable devices, thereby engendering an intuitive authentication platform that boasts user control, privacy, portability, and interoperability. In order to bring to life the practical implications of SSI, the article presents a tangible scenario showcasing its successful integration with wearable device authentication. For future inquiries, it advocates the focus be on creating a viable SSI model for effortless wearable authentication, studying the energy consumption patterns of SSI, and investigating alternate trust networks that could find application in this context.

Keywords: SSI, Self-Sovereign Identity, cybersecurity, Internet of Things (IoT), authentication, wearable devices.
JEL Classification: O30

Corresponding author: json@csusb.edu
Declaration of interest: none
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

1. Introduction

The process of authentication requires the identification of an entity and its identity (Mare et al., 2018). This process actively associates principles to principles for authorization to occur. Authentication can be achieved through several factors: Something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). These factors are vulnerable on their own but are fundamentally strong when put in pairs (e.g., something you are and something you have). Pairing two factors together increases the likelihood of reducing potential vulnerabilities associated with authenticating resources. It has then been recommended that this two-factor authentication (2FA) be utilized to strengthen the resistance to known authentication vulnerabilities (Huang & Guo, 2021).

The utilization of touch-based authentication (something you have) is prevalent within many organizations. An informal research venture conducted by students participating in the Information Security Research and Education (INSuRE) program at California State University, San Bernardino sought to develop a generalized authentication scenario and custom cryptographic protocol (Luna et al., 2021). This project was presented to eighty individuals from different agencies and universities. This development was created to identify issues within identifying employees. The advancement of cybersecurity threats and vulnerabilities has made it increasingly difficult to identify an identity employee. This project was to address the implementation of seamless wearable authentication by a user to decrease potential vulnerabilities in authentication. The project dubbed "SWAG: Secure Wearable Authentication Gear" was proposed by Dr. Joshua Guttman (2021). Dr. Guttman had a direct oversight of the project and guided the research in the direction he saw fit to their idea. The problem posed for this project was to identify a means of employee identification and validation through custom cryptographic protocols. This was directly influenced by the increase in difficulty associated to cybersecurity threats and system vulnerabilities. The researchers completed a generalized scenario with the inclusion of alternative authentication paths for those with disabilities (Luna et al., 2021). This scenario development framed the requirements for the custom cryptographic protocol. The researchers then developed the goal of identifying a secure means of message flow between the following four devices: Wearable device, turnstile, database, and workstation. This message flow was later visualized by utilization of the Cryptographic Protocol Shapes Analyzer (CPSA) provided by Dr. Guttman. This collaboration led to the refinement of message flow and interactions by the researchers.

The SWAG project attempted to answer if there was a possibility of creating a custom cryptographic protocol, if even a generalized form, to minimize vulnerability and attack vectors. This is theoretically possible but not without extreme taxation on the need to create a protocol ground-up. The purpose of this research is to approach the prior SWAG topics from a perspective of generalization and how it could be applied to an organization. The researchers found that a real-world context should be adhered to. That context would lead to a development of security measures that would be focused on reducing vulnerabilities. This culminating project will expand on this idea of seamless wearable authentication and aim to answer the following questions:

> Q1: What are the limitations of a wearable device actively participating in a cryptographic exchange?

Q2: How can the relationship between Self-Sovereign Identity (SSI) and Internet of Things (IoT) influence the future of secure wearable authentication?

We will present the literature review and hypothesis in the next section. This is followed by the limitations of a wearable device and how they relate to IoT devices, SSI and its relationship to IoT device and how it can influence the future of secure wearable devices, and the conclusion.

2. Literature Review

The literature discussed is purely to fill potential knowledge gaps for the discussions and arguments seen in later sections. This will directly influence the commentary and contributions associated to the research questions posed in the previous section.

2.1 Internet of Things

The deployment of Internet of Things (IoT) has become prevalent over the course of the last few years. This is due in part to the ease of deployment and monitoring abilities IoT can provide. IoT devices are unfortunately susceptible to many vulnerabilities that question the effectivity of said devices on a secure network. Establishing trust among participating devices has been a fundamental and practical issue (Sathyadevan et al., 2019). This can be especially said of machine-to-machine communications, which is often seen of IoT devices (Fedrecheski et al., 2020). The same can be applied to the implementation of a custom cryptographic protocol in a seamless wearable authentication scenario. Both situations have established physical and computational constraints: Storage, Random Access Memory (RAM), and battery. These limitations outline the capabilities such a device could perform, each with caveats of increased battery constraints, RAM buffer overflow, etc. An informal security analysis of IoT networks revealed that traits such as confidentiality, integrity, timeliness, resistance to attacks, and scalability of messages are needed to circumvent vulnerabilities and create trust. Battery voltage and the lightweight authentication scheme were additional factors evaluated within the security analysis. The security analysis found the battery voltage dropping in several scenarios involving a router and IoT device communicating while utilizing the lightweight authentication scheme (Sathyadevan et al., 2019). This statistical information helps to understand the balance of security and capability.

2.2 Single Sign On

Single Sign On (SSO) is an alternative authentication structure that utilizes a trust network to authenticate a user via one means of credentials. This was created to reduce the authentication times of users, with the inherent ability to decrease compromised passwords. A proposed scheme of SSO utilizes biometrics to authenticate a user (Liu et al., 2012). The goal of this scheme is to log user samples into a system to combine biometric authentication with SSO. This two-factor authentication (2FA) increases the level of security with this additional requirement. SSO requires implementation of system architecture that supports the unified approach to authentication. This requires there to be a singular database where identity authentication can be performed. An independent database would ensure the "independence of each function on the platform, but also improves the security of the whole unified identity authentication platform" (Huang & Guo, 2021, p. 70). SSO reinforces the need to have a common trust network to enable the shared-identity approach to authentication.

2.3 Cryptographic Protocol Development

Developing custom cryptographic protocols becomes difficult from this point onwards due to the security implementations that would be necessary to include to ensure the safe transit of information. The inclusion of digital signatures and cryptographic values gives an individual conducting a threat analysis a method of attestation, formally known as an attestation protocol. This process conveys hardware state, program code, and associated keys, giving focus on the information needed for security goals within this custom protocol (Guttman & Ramsdell, 2019). Thus, to evaluate the validity of a custom cryptographic protocol, CPSA was developed to delineate clarity on how a message flows through the protocol. CPSA outlines roles, message flows, and protocol skeletons to provide visual representations of a given cryptographic analysis. A form of cryptographic authentication protocol can take place through this method. This cryptographic authentication protocol can be distinct from any given method, system, or schema due to the unique nature of custom protocols. This protocol is "a set of rules, processes, or machines," that are "generically [referred] to as principals" (Abadi & Needham, 1994, p. 123). These principles can be perceived as critical when discussing and developing such a cryptographic protocol for delineation of message flow. This ensures stable communication and prevention of malicious activities by external threat actors.

2.4 Wearable Authentication

Custom cryptographic protocols can be utilized in scenarios such as seamless wearable authentication. Integrating wearable and proximity-based authentication to a given space allows for the additional layer of convenience and security to users. A method of authentication dubbed Zero-Effort Bilateral Recurring Authentication (ZEBRA) set out to solve this issue (Mare et al., 2018). This involved a user wearing a device on their wrist to track movements via accelerometer, gyroscope, and radio that communicated movements to a computer or workstation. The computer or workstation is to then interpret the movements of the user through correlation analysis: If the user moves and is near computer, stay unlocked; if user is moving but is not near computer, lock. ZEBRA was soon superseded by Seamless Authentication using Wristbands (SAW). This development utilized a token-based authentication within the wristband. The job of the wristband is to communicate the proximity of a user to a computer or workstation to not lock the user session (Mare et al., 2018).

2.5 Self-Sovereign Identity

Self-Sovereign Identity (SSI) refers to a digital identity that is fully controlled and managed by the individual or organization to which it refers. It is decentralized and does not rely on any centralized authority to validate or mange the identities. In contract, a Certificate Authority (CA) is a trusted entity Users can store their identity data on local devices and provide the required information to those who need it for validation purposes" (Bokkem et al., 2019, p.1). Platforms that utilize this type of authentication aim to implement a "decentralized system…to store and confirm user identity data". This type of information sharing can utilize smart contacts for transactions (i.e., verifying your identity to access an organization). With the inclusion of SSI in this information transaction, information is easily provable, portable, and accessible. Blockchain is a perfect foundation for SSI to build upon but is not necessarily the only way to implement SSI. Non-Blockchain variants exist, most notably I Reveal My Attributes (IRMA). This variant works

with users to "receive digitally signed attributes from trusted issuers like the government. This means that claims made are provable" (p.5). This zero-knowledge proof idea gives issuers of digital signatures control of what can be seen and modified since issuance. These digital signatures also can issue expiration dates and like attributes to be collected at each authentication interval. These attributes have the inherent goal of being as portable as possible. Without this, there will be no sense in being as data protective as IRMA aims to be. Either forms of SSI authentication, blockchain or non-blockchain, are valid solutions to an implementation of SSI as a solution to create a non-centralized authentication authority.

3. Wearable Device Limitations

3.1 Shapes and Sizes

Wearable devices are inherently limited due to their shape and sizes (Mares et al., 2018). Consumers of wearable devices, such as an Apple iWatch, Samsung Gear, and Fitbit, understand these limitations in multiple forms: How long the battery will last on one charge, how far away you can go from your phone before the device disconnects, and even how water resistant the device may be. Most of this information is common knowledge as it is inscribed onto the devices in the form of advertisements or manuals given to consumers. This sets an expectation on how these devices are capable of functioning, so a user does not go outside those parameters. These wearable devices function as an extension to a cell phone or a fitness tracker, continually sending information to and from the cellphone.

This understanding of consumer-grade wearable devices provides the framework needed to understand what a device may and may not be capable of doing. Sathyadevan et al. (2019) explored the possibility of end-node IoT sensors that are battery powered, conducting a light-weight Protean Authentication Scheme to transmit sensor data to router-nodes securely. Sathyadevan et al. (2019) developed a Protean Authentication Scheme in their research. This utilized "XOR operations and also the Advanced Encryption Standard (AES) at the gateway side whereas the edge nodes would only perform AES encryption. Keys exchanged can either be stored in a secure EEPROM or in a memory protected location which is not susceptible to cloning attack or memory dumps" (p.92,424). This pushed towards mitigating concerns of "not bringing about a noticeable increase in battery consumption" (p.92,429). The limitation of battery power provides the context for what can and cannot be computed by such a device. Sathyadevan et al. (2019) proposed that different sleep cycles could prove effective in increasing or decreasing the battery life of an IoT device. Sathyadevan et al. (2019) concluded that: To test the authentication scheme, the [re]MOTEs were set up as routers as well as edge nodes. When a MOTE acts as a router it will never go to sleep and will constantly radiate sensor values; when configured as edge nodes, it wakes up once every 320 ms and waits for five seconds looking out for any requests coming from the coordinator node. The coordinator node sends out a series of requests once in four minutes requesting sensed parameters. MOTEs will then transmit the sensed values to the coordinator and go back to sleep. (p.92,430)

Therefore, IoT devices require three main things to function: Connection, encryption, and power. These core functions are also the same as secure wearable devices. These operational requirements call back to the need for secure communications, where Sathyadevan et al. (2019) established the need to "depend on the encryption…for secure communications" (p.92,434). This common need for security and encryption is the basis for the parallels seen between IoT and secure wearable devices. This commonality is fluid in nature with the inclusion of secure cryptographic

communication between external devices. While light-weight protean authentication schemes can be utilized, the fluidness of cryptography allows for other modes of cryptographic computations to take place. Single Sign On (SSO) is an alternative form of authentication that utilizes token-based authentication and uses organization-defined encryption algorithms. This process was created to reduce the authentication time needed by users and to implement a simple authentication architecture within an organization. Huang & Guo (2021), from the article Single Sign-on Technology for Educational Administration Information Service Platform found SSO to be "more secure than the traditional login mode" (p.71). Having a single commonality of authentication and encryption within both IoT and secure wearable devices furthers the idea of both being fluid and interchangeable.

Sathyadevan et al. (2019) conducted an experiment with and without their proposed authentication scheme to compare battery levels after usage. Their results showed that there was an average power drop of 0.137504843 watts without authentication and 0.135946529 watts with authentication. These numbers emphasize the additional computational energy needed when utilizing authentication on battery-operated devices, no matter how little. The researchers experimented with their authentication scheme to confirm its efficiency. This showed no real difference in terms of battery drainage overall but showed the impact authentication schemes can have on IoT devices (p.92,434).

3.2 Security Analysis

An informal security analysis was then conducted to reinforce the need for authentication, despite the increase in electrical consumption (Sathyadevan et al., 2019). The researchers proposed that the Protean Authentication Scheme they developed can resist the following attacks: Replay and Known Key, Impersonation, Device Cloning, Eavesdropping, and Man in the Middle. The researchers believe that their proposed mechanism does "not require storing any static key value on the device. Instead, the keys are dynamically changing and shared securely to prevent message replay and device clone attacks" (p.92,434). This mechanism assumes this resistance would be a beneficial outcome in the implementation of such an authentication scheme.

3.3 Limitations

These limitations slowly become a process of balancing what is and is not needed for saving of space and/or battery power. The research conducted by Sathyadevan et al. (2019) provides us a view of how the increase in computational load increases battery consumption. We can surmise that with the increase in computational processing, the battery capacity should be increased. This is then limited by the amount of space allowed by the design of an IoT or wearable device. Bringing these limitations into the scope of secure wearable authentication, a device no bigger than a typical wristwatch would be our size limit to conform to. Mares et al. (2018) sought to establish that a "user's wristband (e.g., fitness tracker, smartwatch) acts as the user's authentication token" (p.2). This wristband is intended to communicate securely to a target desktop computer with little interaction of the user. The researchers assumed that the wristband would include an "accelerometer and gyroscope sensors and a radio (e.g., Bluetooth) to communicate to the target desktop" (p.7) to achieve this form of authentication. This form is also discussed by Sathyadevan et al. (2019) in how there is an inherent need for balance in computational energy and available battery capacity.

There are additional limitations surround the usage of radios. Mares et al. (2018, p.23) found "that Bluetooth, which is the most ubiquitous wireless protocol for personal area networks, was not designed for complex network topologies. As a result, pairing multiple desktops with a single wristband, or more generally, multiple devices with multiple wristbands, can be challenging." The researchers found that this can be remedied with the utilization of Advanced and Adaptive Network Technology (ANT+) or Texas Instruments SimpleLink to "support this many-to-many connectivity in high-density environments" (p.23). This authentication process did appear to be effective by the researchers' own claim. They stated that "SAW proved to be quick, authenticating participants within 2 s; effortless, and several participants liked the natural tap authentication interaction; usable, with a low false-negative rate of 2.5%; and secure, with a low false-positive rate of 1.8% even in the most advantageous conditions for an adversary" (p.27). The conclusion of the article reinforces the original goals of the researchers, with security constraints requiring wearable devices to be resilient to physical observation, accidental logins, and mimic attacks, with the addition of explicit intent to log in. These requirements are limitations due to the impact it has on other internal wearable device systems, such as the battery and additional power draw over time to complete authentication.

The process of connecting is limited by the availability of current technology, seeing ANT+, Texas Instruments SimpleLink, Wi-Fi, or Bluetooth all being contenders in the IoT and secure wearable device use case. The scope is further limited by the capabilities of the communication platforms. Mares et al. (2018), found that Bluetooth simply "was not designed for complex network topologies" (p.23). This limitation in Bluetooth is quickly circumvented with evidence supporting Bluetooth Low-Energy (BLE) communication. The researchers established that "Bluetooth Low Energy, however, does not require pairing, and indeed, supports some broadcast operations" (p.23). This communication platform is then reinforced by Sathyadevan et al. (2019) in the mention of having BLE included on their protocol adaptors. "The hatboard consists of the ZigBee adaptor interface and interfaces for other protocol adapters like 6LoWPAN, BLE, WiFi etc." (p.92,429). This interesting commonality between articles can then be applied to the mode of communication both IoT and secure wearable devices can potentially utilize for their communication processes.

With both IoT and secure wearable devices relying on battery-power, there is only a limited amount of electricity available that could be utilized towards an authentication process or network communication. The explicit amount of power that an authentication process draws again reiterates the need to be cautious of what processes are completed on a device. Sathyadevan et al. (2019) concluded that an overall goal of "verify[ing] the efficiency of [the] scheme" (p.92,434) is necessary to continually confirm what the computational load is at. This is to lessen or prevent preemptive drain on the battery power made available to the device. Utilizing SSO as a form of authentication would have a direct effect on the battery power. However, it is unknown how little or great this power draw can be without proper testing of this authentication scheme. The utilization of radios as a form of communication are also lumped into this battery issue. For instance, utilizing a BLE module can have other intricate forms of computation and battery consumption associated to it. While BLE has "low-energy" in the name, there could be a potential increase in overall battery consumption with this communication platform that would otherwise deter the want to use this format.

3.4 Drawing Parallels

These parallels create the needed context to understand how IoT can influence the future implementations and limitations of secure wearable authentication. The requirements seen within communication, authentication, and battery capacities emphasize the need for continual scaling of security and stability within this platform. These requirements directly influence the capabilities of what secure wearable authentication can achieve. Another aspect of the authentication process is the requirement to be connected to a certificate authority. If there was an instance where there was limited connectivity to a given authority, it would be impossible to authenticate an identity. Self-sovereign identity would resolve this issue and is investigated in the next section on how applicable it could be to secure wearable device authentication.

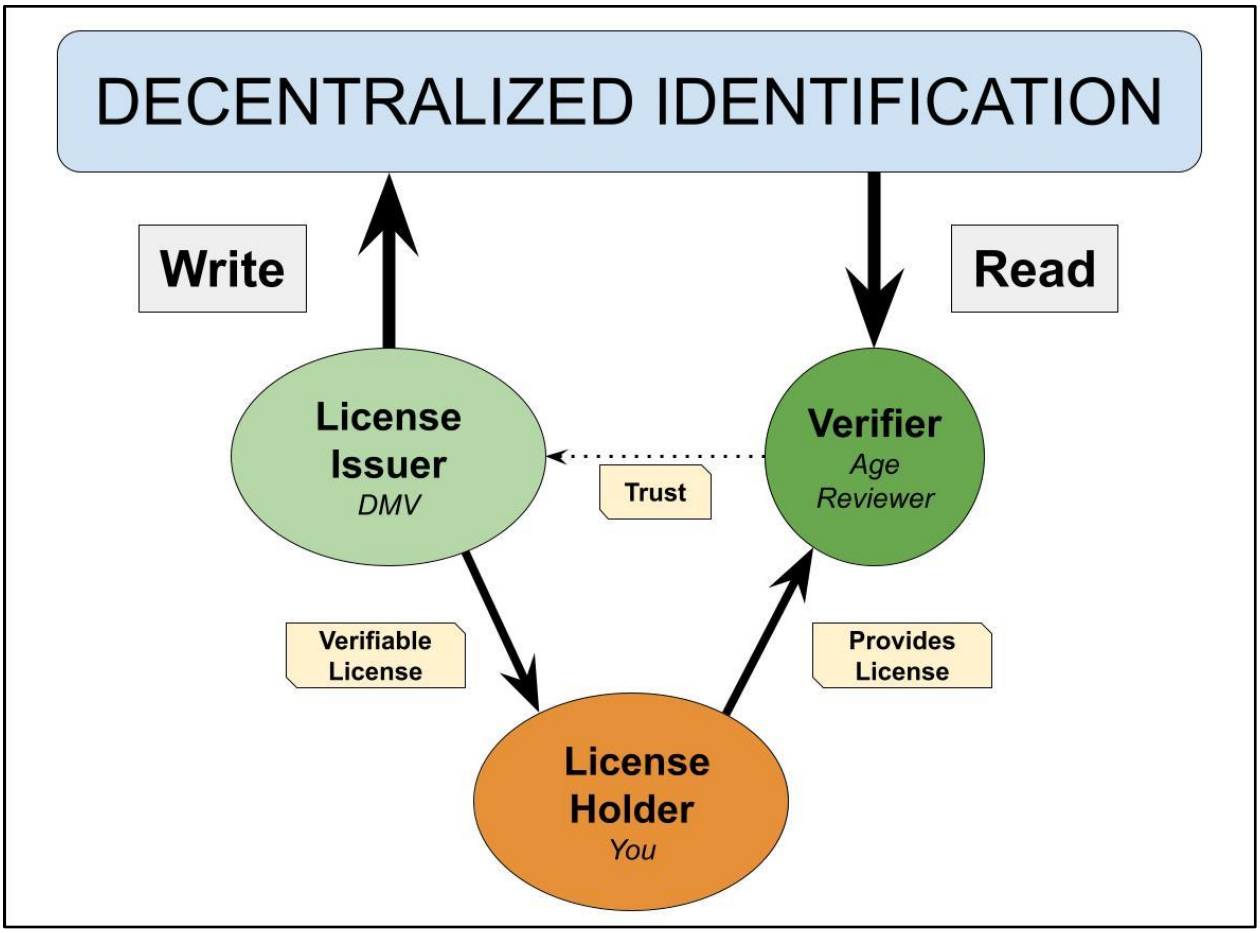
4. Secure Wearable Authentication through SSI

4.1 Understanding SSI

Authentication to web services is achieved through a centralized authentication server utilizing SSO. This can be seen through using Google's SSO to produce a login for a third-party website, reducing the number of duplicate usernames and passwords available on the internet. This format of SSO is useful in that it allows for ease of use for a user, only utilizing a single credential for authentication. The caveat to this is having no controllable limit to what the third-party website may have access to viewing when linking said accounts. We can theoretically trust Google with this process due to their secured digital identity policies (Bokkem et al., 2019), but we have no control of what we can limit in sharing. Users can refuse offering information, such as last name or phone number, to Google. This would give Google leverage in refusing to provide SSO services as a response.

Self-Sovereign Identity (SSI) is a Decentralized Identification (DID) concept that removes the limits on what you as a user can show or hide (Fedrecheski et al., 2020; Gebresilassie et al., 2020; Mühle et al., 2018; Van Bokkem et al., 2019). This enables unambiguous trust in the entity signing said identification. An example of this can be seen through a driver's license issued by the DMV. We as a population understand that these licenses are legitimate forms of identification and are 100% trustworthy. This example can be further applied to when we utilize our driver's license to verify age. The main caveat to this is that we must show all the information on the license to whomever is verifying our age. We do not need to show our home address, height, weight, etc., but instead just our date of birth and the DMV signature verifying our information is legitimate. We can achieve this through the utilization of SSI. This would increase the amount of privacy for a user and instead obscure the information not needed to verify our age.

Figure 1
Decentralized Identification Model



This decentralized authentication concept can be applied to secure wearable devices as a form of identification. Bokkem et al. (2019) identified a user-centric authentication strategy used to store and confirm a user's identity. "EverID facilitates verification of users by multiple third parties and allows the secure transfer of value between members of the network. This means that the claims made by users are provable" (p.4). This authentication type requires the utilization of a blockchain. These types of solution implementations typically involve a great deal of effort in creation for an organization and would not be a recommended path when utilizing secure wearable authentication. Non-blockchain alternatives are available and function similarly to the previous DMV driver's license example. I Reveal My Attributes (IRMA) is a platform that "implements the Idemix attribute-based credential scheme" (p.5). This platform continues to verify that all claims are indeed provable and can be trusted just as the blockchain variants previously mentioned. IRMA allows users to have "control over their digital identity. IRMA meets the (minimalization) property by using zero-knowledge proofs. Using the issuer's digital signature over the attributes the verifier can verify that the attributes were given to the user in the past, and that they have not been modified since" (p.5). IRMA is considered extremely portable, Bokkem et al. (2019) mentioning "users can bring their phones wherever they want" (p.5) to authenticate when required.

This extreme amount of portability gives secure wearable authentication an opportunity to be utilized in conjunction with SSI to create a seamless authentication platform. The utilization of these platforms can yield a format of authentication conducive to ease of access previously sought

after within Mares et al. (2018). Bokkem et al. (2019) defines IRMA as not being persistent in availability in various locations. This means "that losing your phone means losing your identity. All the attributes need to be collected again" (p.5). This non-persistent decision highlights how data-protective IRMA is and how it can be a potential benefit for sensitive environments. If a user were to lose or misplace their secure wearable authentication device, they are forced to report it as they would be unable to access an organization. This pushes a user to be responsible in protecting their device and not acting carelessly.

SSI can be applied in the scope of seamless authentication but should also be approached in the scope of interoperability with established domains within an organization. Many organizations utilize a central authentication authority or domain to confirm the identity of users. We must define constraints to capture what implementations may be useful in this combination of DID and central identification structures. Bokkem et al. (2019) defines interoperability as being widely available and not limited to certain niches. This constraint pushes for an SSI solution that would otherwise be plug and play into a given domain. IRMA is considered interoperable with a running trial with a third party. The authors provide no further information on this, but instead shows that it is indeed possible to utilize both systems.

IoT devices have been the recent target of SSI as a preferred solution for developing trust. Gebresilassie et al. (2020) identified IoT as having potential in utilizing SSI. The researchers outline SSI, in a non-blockchain environment, as allowing "IoT devices [to] prove themselves to anyone, organization, services or other things and they have the power to decide on which portion of their identity information to share" (p.4). IoT devices are becoming vital parts of our connected society in "performing autonomous decisions" (p.4) in multiple environments: Industrial, homes, offices, and hospitals. SSI is described as a preferred solution for IoT devices due to their resource constraints. IoT devices utilizing SSI "have full ownership and control over their identities via a portable, interoperable, persistent, secure, and scalable system" (p.6).

Bringing SSI to IoT addresses privacy concerns when personal data sharing is involved. Having Personally Identifiable Information (PII) within data causes many users to be hesitant in involving themselves with such a device for fear of data leaks. Fedrecheski et al. (2020) stated that "the future [of] IoT will require users to be the root of trust of their devices, leading to an owner-centric IoT" (p.5). The benefit of this is having inherent control over what is revealed or transmitted. This privacy-preserving model helps to keep personal information protected. Any communication by an IoT device is expected to "mutually authenticate, derive short-lived symmetric keys, send encrypted messages, and enforce non-repudiation" (p.5). The authors outlined several challenges relating to this process, with device constraints being the forefront of this issue. IoT devices have electrical and computational limitations that are identical to what has been discussed in 'Chapter Three: Wearable Device Limitations.' The authors expressed concerns regarding the computational overhead required when adopting an "asymmetric cryptography and coping with communication overhear of transmitting metadata, such as DID Documents and Verifiable Credentials" (p.5).

The articles written by Gebresilassie et al. (2020) and Fedrecheski et al. (2020) outline the issues and constraints that are inherent to IoT devices. These same constraints can be applied directly to secure wearable authentication devices as they follow the same criteria (i.e., battery consumption, computational overhead, etc.). The goal of trusting a device and having full credibility to an identity obtained by a wearable device is benefited by the utilization of SSI. Gebresilassie et al. (2020) outlines that a "trust score algorithm in this work will adapt the concept

of the web of trust as applicable to IoT devices" (p.5). Secure wearable devices are easily applied to this web of trust due to the ability to adapt the web of trust. Gebresilassie et al. (2020) continues to outline "other parameters like minimum security requirements, reputation and compliances will be a part of the trust score algorithm. With this trust algorithm, a device is examined if it satisfies all the requirements before it can be granted or denied access to the IoT networks and services" (p.5) The same can be said when applying this concept to secure wearable devices.

4.2 SSI Scenario Development

Secure wearable devices and SSI require a scenario to be developed to properly convey how applicable the process can be to organizations. A fictitious scenario can be drawn in this context to allow for proper articulation on how National Security Agency (NSA) credentials can be used as a form of authentication to a Navy installation. This example scenario requires three main entities: Holder (wallet), Issuer (NSA), and Verifier (Navy). Each entity is required to write their own DID document to the Distributed ledger / Network. Step 0 begins the process to confirm the validity of the entities to allow for a trust relationship to be created later. For ease in understanding the figures and their subprocesses within the steps, parts will be labeled within the figures and mentioned with their step number and sub-step number (ex., Step 1 plus Sub-step 2 will show as Step 1.2).

Figure 2

Step 0 – Preliminary Registering of DID Documents

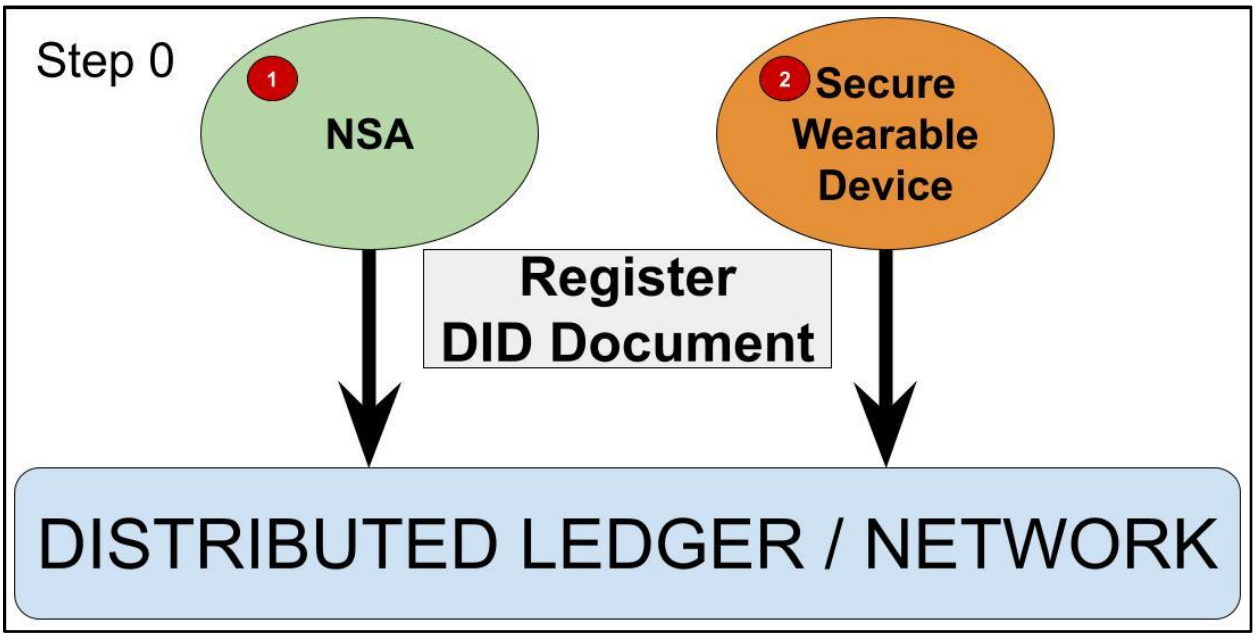


Figure 2 outlines the preliminary steps required for an Issuer and Holder. This process requires the NSA (Step 0.1) and the Secure Wearable Device (Step 0.2) to register their DID documents to the Distributed Ledger / Network. Research into the possible standards for writing DID documents returned with no results. It was then concluded that there are no current standards

available for writing DID documents. A potential format can be seen through utilization of JSON. Registering the NSA through a DID document could appear as seen in figure 3.

Figure 3
NSA DID Document Registration

```
{ "@ context": "https://www.examplensadomain.org/n/did/v1"
  "id": "did: sov: NNNN"
  "public key":  {
    "id: did: sov: NNNN # keys-1",
    "publickeyPem":
    "MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgG4TBxcbyBEKmnBK1a
    sc1vYV+3XcQMbbJxeiRw/+EueMhdhzHbhor3YkFculsdqOE5KkgXZ1Y
    eSmHh5C7CqR6K0zVRKEMO1Z5m1t/anP58xUsP3P5U0SzXIkoUPkamPv
    8F0aijJBPc98CEeP8qqmuNe3Zd8qvjhS456Qgrul9JmxAgMBAAE="
  }
  "Authentication":{
    "did: sov: NNNN # keys-1"
  }
}
```

The "id" seen within the NSA DID document is represented with "NNNN." This is a unique identifier for the NSA in our example. The "public key" section has two aspects to it: the first having an "id: did:" to identify the NSA as a DID document and the second being "publickkeyPem" to show the public key used by the NSA to verify claims. The "authentication" section is used to reference authentication types seen later in a verifiable credential. This same format can be utilized in registering a secure wearable device and is visualized in Figure 4.

Figure 4
Device DID Document Registration

```
{ "@ context": "https://www.exampledevicedomain.org/wd/did/1234"
  "id": "did: sov: 1234"
  "public key":  {
    "id: did: sov: 1234 # keys-1",
    "publickeyPem":
    "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDP0yn+X8sHzFrMbqKiPKC
    LdX55eVJJOadHK8sCai1tiBiiD9vVyhhVATm1lL6fm6aa6z7jVRb8nmUVkiC
    zXIcgNnzssNSLhWMG+R3Jat5OHwe96E3z4a5deyqhMw5oBDLNG3hKECKHYcw
    55K5qy13cdR2Fw4ekzw4JVrcRcElQAwIDAQAB"
  }
  "Authentication":{
    "did: sov: 1234 # keys-1"
  }
}
```

The same flow of information seen in Figure 3 is mimicked for the secure wearable device DID document in Figure 4. The "id" for our wearable device is seen as a unique identifier of "1234" for this example. The goal of these DID documents is to give reference to the information utilized downstream. Any questions regarding a given authentication would route back to these registrations. The registering of these DID documents completes step 0. Step 1 then begins by initiating a credential issuance to a holder. This process creates Verifiable Credentials (VC) that are issued to a holder to confirm their identity. This process is visualized in Figure 5.

Figure 5
Step 1 – Request and Issuance of Verifiable Credentials

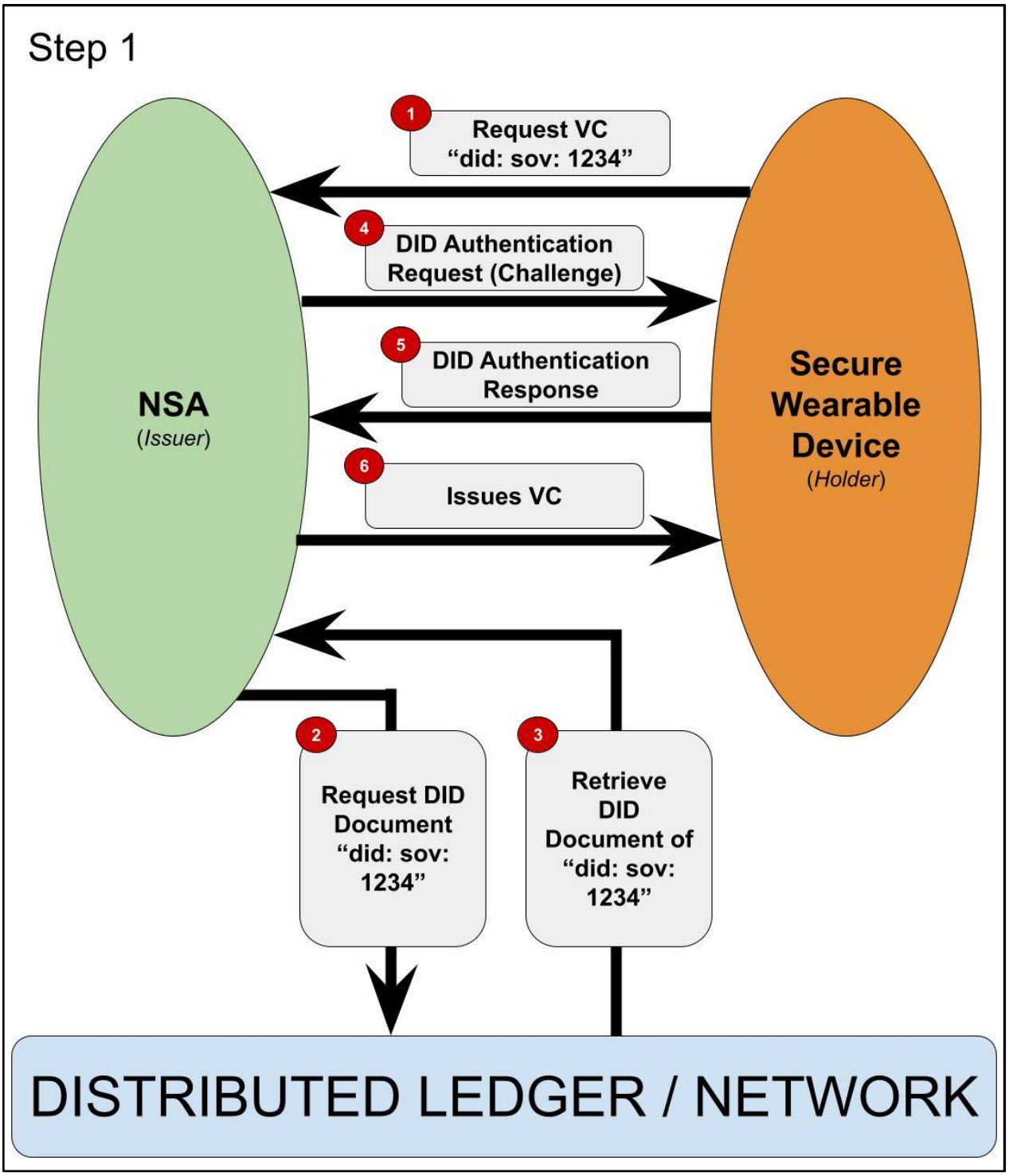


Figure 5 shows the secure wearable device requesting a VC from NSA (Step 1.1). This request contains the Distributed Ledger / Network information needed to request and retrieve information regarding the secure wearable device. The NSA is then able to request the DID document from the Distributed Ledger / Network with the included DID information received from

the secure wearable device (Step 1.2). The NSA can retrieve the information (Step 1.3) and issue a DID authentication request or challenge (Step 1.4) to the secure wearable device. A DID authentication response is then issued as the secure wearable device confirms its identity (Step 1.5) and the NSA can issue the VC (Step 1.6). The VC issued to the secure wearable device will follow the same format as previously seen with DID documents but with additional information. This is visualized in Figure 6.

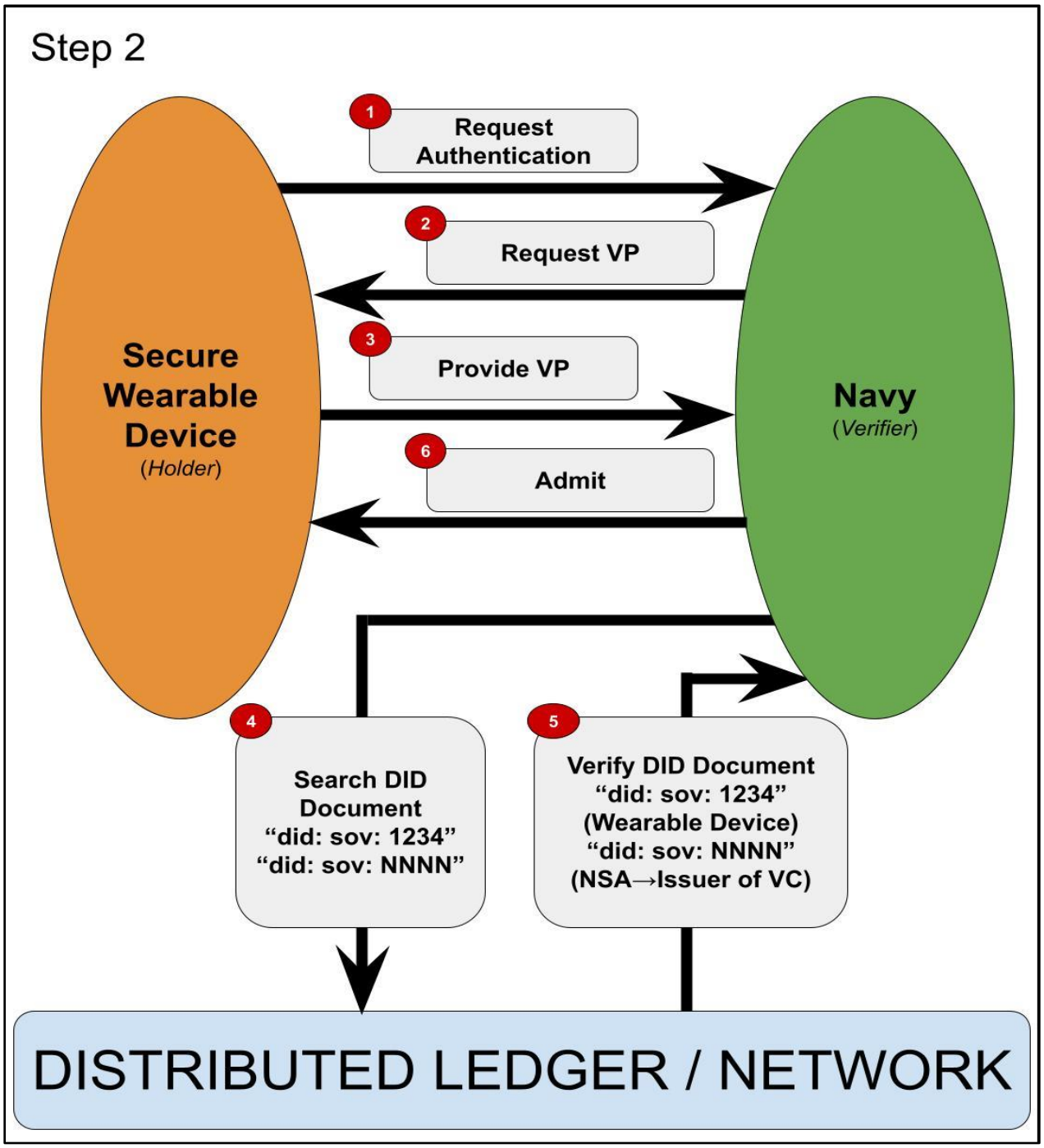
Figure 6
Issued Verifiable Credentials from NSA to WD

```
{ "@ context": "https://www.examplevc.org/vc/did/1234",
  "id": "https://www.exampledevicedomain.gov/wd/did/1234",
  "issuer": "did: sov: NNNN",
  "issuancedate": "2022-04-01",
  "expdate": "2023-03-31"
  "credential subject": {
    "id": "did: sov: 1234",
    "deviceinfo":  {
      "devicename": "XYZ-1234",
      "manufacturer": "XYZ",
      "powerconsumption": 0.04,
      "securitydomain": "NSA",
      "securityclearance": "topsecret",
      "department": "{nuclear, chemical}"
    }
  }
  "proof": {
    "type": "RSAsignature2018",
    "proofpurpose": "assertationmethod",
    "created": "2022-04-01",
    "creator": "NSA",
    "verificationmodel": "did: sov: NNNN # Keys-1"
  }
}
```

The VC has three main structures to it: context, credential subject, and proofs. These sections provide the credential information and arguments needed to authenticate later in this example. This document includes information previously written to the Distributed Ledger / Network. The "context" section of this VC provides the information related to the trust relationships and the given credentials. "id" points directly to the secure wearable devices' credentials that can be found within the NSA database of trusted devices. The "issuer" shows that the NSA issued the identity and was seen previously when registering the NSA into the Distributed Ledger / Network. The "issuancedate" and "expdate" are used to show when the credential was issued and expires. The "credential subject" section of the VC expands the secure wearable device and the identity involved. Common details such as "devicename," "manufacturer," and "powerconsumption" are used to establish the credentials and identity seen within the Distributed Ledger / Network. Information regarding the "security-domain," "security-clearance," and "department" are used to constrain the identity to only what may be allowed. These are modifiable by an organization on a per-identity basis. The last section of "proof" gives clarity on what "type" of authentication signatures are used and what "proofpurpose" is available to the identity. The "verificationmodel" is utilized in connecting the original DID document register seen within the Distributed Ledger / Network to confirm validity of the VC.

Step 2 initiates the Verifiable Presentation (VP) process. This allows for the holder of an issued identity to present their VC to a verifier. The continuation of this example has the secure wearable device holder present their issued identity from the NSA to the Navy instillation to obtain access. The understanding between the NSA and Navy is that their security clearances are equal and will have the same compartmentalization for information. Step 2 is visualized in Figure 7.

Figure 7
Step 2 – Verifiable Presentation



This process begins with the secure wearable device requesting access to the Navy (Step 2.1) seen in Figure 7. The Navy will request a VP in return (Step 2.2). The information requested

by the Navy can be a variety of things: name, organization information, age, passwords, etc. These would all be things that could otherwise be agreed upon beforehand between the NSA and Navy when issuing identities. The secure wearable device can then compose the needed information and provide that to the Navy as a document (Step 2.3). This document would mimic the same format seen prior in DID documents and is visualized in Figure 8.

Figure 8
Verifiable Presentation from WD to Navy

```
{ "@ context": "https://www.examplevc.org/vc/did/1234"
  "id": "did: sov: 1234",
  "type": "VerifiablePresentation",
  "verifiablecredential": {
    "id": "https://www.exampledevicedomain.gov/wd/did/1234",
    [...],
    "credential subject:" {
      "id": "did: sov: 1234",
      "deviceinfo":  {
        [...],
        "securitydomain": "NSA",
        "securityclearance": "topsecret",
        "department": "{nuclear, checmical}"
      }
    }
    "proof": {
      [...],
      "creator": "NSA",
      "verificationmodel": "did: sov: NNNN # Keys-1"
    }
  }
  "proof": {
    "type": "RSAsignature2018",
    "proofpurpose": "authentication",
    "created": "2022-04-01",
    "creator": "1234",
    "verificationmodel": "did: sov: 1234 # Keys-1",
  }
}
```

The VP document will only present the information asked of it. This example has the Navy asking only for the “securitydomain,” “security-clearance,” and “department,” all with the associated proofs required of these credentials. Refer to Figure 6 for the full VC. The Navy is then able to take the VP and query the Distributed Ledger / Network (Step 2.4) with the requested information. The headers of “id” and “verifiablecredential” direct the query to the locations where the registered DID documents are. The Navy can retrieve the documents (Step 2.5) from the Distributed Ledger / Network. The Navy is then able to verify the identity of the wearable device by asking the following questions:

1. Is the VC signed by NSA?
2. Is the VP prepared and signed by WD?
3. What is the identity of Holder who prepared and submitted the VP?

The Navy can confirm the validity of number 1 since it has the NSA public key from the DID document retrieved from the Distributed Ledger / Network. Numbers 2 and 3 can follow the same route of confirmation as number 1 as it has the WD public key. It is at this point that the Navy can create a trust relationship with the secure wearable device after confirming questions 1, 2 and 3. This creates a triangle of trust, establishing a basis to which the Navy can then admit the secure wearable device to their network (Step 2.6).

5. Conclusion

Secure wearable devices are limited by side, computational capacity, and battery storage. The reasoning of why these limitations exist was approached within Section 3: Wearable Device Limitations. The usage of SSI demonstrates that distributed authentication (with no central authority), computational load could be reduced. SSI could allow for an identity holder to have full ownership and control over their identity data. This would no longer have an identity holder rely on third parties to store or manage their identity data. Additionally, SSI could allow for identity holders to selectively disclose only the required or necessary information in each interaction or transaction, referred to as "minimal disclosure". This article contributes to the lack of scenario development in Section Four: Secure Wearable Authentication Through SSI and IoT that could be utilized in the structuring of a multi-level secure environment through benefits demonstrated by employing SSI within wearable devices. Future research could include statistical analysis of battery consumption in direct correlation to logical computations when employing SSI versus centralized authentication schemes like Certificate Authorities (CA). Blockchain and non-blockchain variants exist and are available to anyone utilizing SSI as a form of authentication and developer of trust.

Future research into this topic should explore the possibility of developing a working model of SSI as a form of seamless wearable authentication to an organization. It is recommended that the working model follows a generalized approach to allow for ease in scaling and implementation into participating organizations. Other avenues of this research could reach into other trust networks being developed and how they could be applied to this scenario.

References

Abadi, & Needham, R. (1994). Prudent engineering practice for cryptographic protocols. Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy, 122–136. https://doi.org/10.1109/RISP.1994.296587

Di Liu, Zhi-Jiang Zhang, & Ni Zhang. (2012). A Biometrics-Based SSO Authentication Scheme in Telematics. 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 191–194. https://doi.org/10.1109/CyberC.2012.39

Fedrecheski, Rabaey, J. M., Costa, L. C. P., Calcina Ccori, P. C., Pereira, W. T., & Zuffo, M. K. (2020). Self-Sovereign Identity for IoT environments: A Perspective. 2020 Global Internet of Things Summit (GIoTS), 1–6. https://doi.org/10.1109/GIOTS49054.2020.9119664 Gebresilassie, Rafferty, J., Morrow, P., Chen, L., Abu-Tair, M., & Cui, Z. (2020). Distributed, Secure, Self-Sovereign Identity for IoT Devices. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 1–6. https://doi.org/10.1109/WF-IoT48130.2020.9221144

Gebresilassie, S. K., Rafferty, J., Morrow, P., Chen, L., Abu-Tair, M., & Cui, Z. (2020). Distributed, secure, self-sovereign identity for iot devices. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 1–6. https://pure.ulster.ac.uk/ws/files/78499255/Distributed_Secure_Self_Sovereign_Identity_for_IoT_Devices.pdf

Guttman, J. D., & Ramsdell, J. D. (2019, September). Understanding attestation: Analyzing protocols that use quotes. In International Workshop on Security and Trust Management (pp. 89-106). Springer, Cham.

Huang, & Guo, F. (2021). Research on Single Sign-on Technology for Educational Administration Information Service Platform. 2021 3rd International Conference on Computer Communication and the Internet (ICCCI), 69–72. https://doi.org/10.1109/ICCCI51764.2021.9486813

Luna, A., Huot, J. T., Hazelip, J., Zabala, M., Bywater, Q., & Maysey, T. (2021, May). SWAG: Secure Wearable Authentication Gear. Information Security Research and Education (INSuRE) Program [Unpublished Report].

Mare, Rawassizadeh, R., Peterson, R., & Kotz, D. (2018). SAW: Wristband-based Authentication for Desktop Computers. Proceedings of ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(3), 1–29. https://doi.org/10.1145/3264935

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80–86. https://arxiv.org/pdf/1807.06346

Sathyadevan, Achuthan, K., Doss, R., & Pan, L. (2019). Protean Authentication Scheme - A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments. IEEE Access, 7, 92419–92435. https://doi.org/10.1109/ACCESS.2019.2927818

Van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology. arXiv preprint arXiv:1904.12816. https://doi.org/10.48550/arXiv.1904.12816