

SurePresence: Location Proofs for Wearable and Kiosk Devices

Miguel Cordeiro Francisco
Instituto Superior Técnico, Universidade de Lisboa
Lisbon, Portugal
miguel.c.francisco@tecnico.ulisboa.pt

Abstract—The world is moving beyond the smartphones and the mobile computing paradigm, with more devices and network connections present in everyday life in more inconspicuous ways. Wearable devices, like smartwatches, are further connecting people to the world. New applications are possible such as activity and location tracking that allows health monitoring. More generally, wearables allow more access to services, which for many of them, the location information needs to be trusted. If the service output is valuable, the user may be tempted to bypass the application location verification. This is why many location-based applications need protection against location spoofing. One approach is to use a location certification solution, but so far they have not been integrated with ubiquitous technology. In this work, we introduce SurePresence, a system that allows people to verify their location using wearable and kiosk devices integrated into their everyday life, presenting a seamless user experience. We present a specific implementation of our system that allows a patient to verify his presence when attending a medical appointment through three novel kiosk-based location proof techniques. Our evaluation included a user study that showed that our system is feasible, providing verifiable location proofs using constrained devices in seamless ways and can be used in many other real-world use cases.

Index Terms—Internet of Things, Location Certification Systems, User Experience, Security, Privacy

I. INTRODUCTION

In recent years, we witnessed an increasing interest and usage of Internet-connected devices with the intent of providing more harmonious ways of life. These connected devices can gather sensed data, and this data can be used for more efficient processes and actuators that can be used to perform useful actions. These so-called *smart objects* can be combined and constitute the Internet of Things (IoT) [1]. They can be used for multiple purposes, which is reflected in the heterogeneity of the underlying technology that manages heating, security, and other management chores which requires different software and hardware necessities.

Wearables are a type of IoT device often used in health monitoring applications and are heavily based on data collection through sensors. Kiosks, another type of IoT device, serve as the physical frontier between the consumer and the application, and their usability is very important. Depending on the use case for such devices, the requirements may differ. Thanks to these types of devices, people are becoming even more connected to the world, beyond smartphones, exploring new interacting ways with constrained devices.

In this work, our focus is on *location-based applications* that need the trustable user location context to provide certain functionalities. Usually, these services need to know the location of the user or the collection of past tracked locations and use evidence to allow for location proofs.

A. Location Proofs

Currently, many location-based mobile applications do not verify the given user location information because they do not have the means to do it or simply because they think it is unnecessary, making them vulnerable to location spoofing attacks. Or even if they do verify, it is not in an effortless and good experience, requiring multiple and complex actions from the user. Sometimes the user has no actual reason to spoof, as it wants to receive the service. However, malicious users can abuse this trust and attempt location spoofing or even denial-of-service attacks, to obtain exclusive or specific functionalities from valuable services.

One solution to prevent location spoofing is *location certification systems* [26] [6] which are essential enablers for secure and reliable location-based services (LBS) that protect and verify information about the location of users. The functionalities of these systems can be leveraged with the usage of IoT and constrained devices, to seamlessly produce and verify location proofs. Users may lose interest in systems that are too focused on security and that ignore user experience. Leveraging the usability of location certification systems has not been a concern for the past years.

This work was done in the context of the SureThing project [21][18][8]. It allows the creation and validation of location certificates through Smartphones and IoT devices.

B. Contributions

Our contributions in this work are the following: development of SurePresence, a smartwatch, and kiosk-based location certification system for smartcards and ubiquitous devices; implementation of SurePresence in a medical use case, where a patient is able to verify his presence when attending a medical appointment; development of three novel location proof techniques based on the interactions of different devices with a kiosk; assessment of the user experience provided by the novel location proof techniques through a user study.

C. Outline

The remainder of the document is structured as follows. Section II presents related work in the fields of location certification systems and relevant use cases for location proofs, IoT technologies, including IoT devices, and an overview of usable security. Section III describes the SurePresence system, and its design aspects, and in Section IV its implementation for a medical use case, including the used platforms and the novel kiosk-based location proof techniques. Section V presents the evaluation of our solution including the novel location proof techniques through a user study. Finally, in Section VI we discuss the results obtained from our evaluation and Section VII presents the conclusion and future work.

II. RELATED WORK

We start by showing work related to existing location certification systems and use cases for location proofs, in Section II-A. Then, in Section II-B, we summarize works that have been presented in the area of IoT, specifically related to two types of devices: Wearables and Kiosk devices. Finally, in Section II-C we show previous work related to Usable Security, one of the most important concepts regarding usability in secure systems.

A. Location Certification Systems

Location certification systems provide reliable and verified information about the location context of a user. Location-sensitive applications need this information because they cannot rely only on GPS.

In 2011, Zhu and Cao [26] introduced APPLAUS, a witness system based on neighboring mobile devices, capable of providing location proofs for nearby provers, through Bluetooth communication. Ferreira and Pardal [8] present another system that not also relies on witnesses to verify the presence of the devices of other users but also on three location proof techniques, including geographic and Wi-Fi/Beacon fingerprinting. Nosouhi et al. [4] show us PASPORT, a system capable of producing and verifying location proofs without the need of fixed wireless infrastructure in that location and based on a witness model focused on the anonymization of users.

1) *Location Certification Architecture*: We can conclude the state-of-art location certification systems have converged to the generic architecture that can be seen in Figure II-A1 and includes the following entities: **Prover** - The user of the system trying to prove his presence at a location; **Verifier** - An entity that validates the location proof submitted by the prover; **Witness** - A neighboring user of the prover that provides location proof for him. Can also be a prover; **Certificate Authority** - Third-party entity responsible for authenticating the users of the system.

2) *Use of Location Proofs*: Location proofs can be used in all types of sectors. In the workplace, can be used to confirm attendance in reunions or in schools, for students to prove their attendance in classes or exams. A tourist can use location proofs to verify his presence in specific landmarks of a tourism

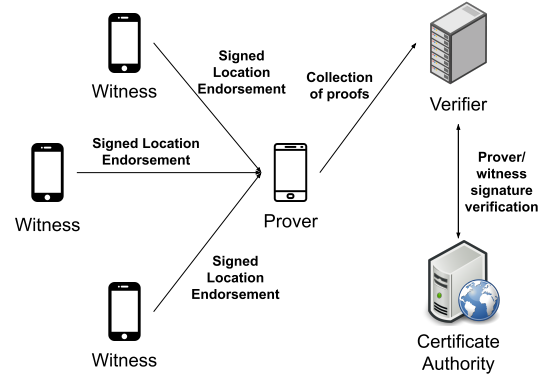


Fig. 1. Location Certification Systems Generic Architecture.

trip or shops can use location proofs to measure the loyalty of a client, by verifying how many times he visits them [22].

We will be focusing on the two fundamental cases of rastreadability: **Track** Singular Locations and **Trace** an Itinerary.

Track Singular Locations is an elementary use case related to a singular place when it is only needed to verify the presence of a person in one unique location. This represents the most simple case of location proofs: does not require verification and analysis of previous or future proofs to guarantee the integrity of this one.

Trace an Itinerary is a use case related to an itinerary as a whole proof. An itinerary represents a location chain, which is a composition of location points with a specific visiting order. Thus, the verification process of points of interest may be different depending on the location and the environment, but it still depends on the verification of previous location points, like in smart tourism.

B. IoT Technologies

Al-Fuqaha et al. [2] give us a complete summary of all related research work done in IoT. It is done as a survey covering all aspects of IoT including architecture, core elements, standards for IoT protocols, main challenges, and the following key ideas:

- 1) A five-layer architecture - Business, Application, Service Management, Object Abstraction, Objects - is the most applicable model for IoT applications, providing simplicity and abstraction.
- 2) Regarding the IoT computation building block, Android is the most complete operating system to be used in IoT environments.
- 3) There is no correct standardized protocol to be used in the different architectural layers because they depend on the scenario and functionality we want to provide.

Frustaci et al. [9] give us a summary of security issues relative to different protocols, respective vulnerabilities, and

possible attacks in all three layers of the basic IoT model: perception, transportation, and application. Denial of Service (DoS) attacks constitute the biggest threat to IoT security since they can be done in all three layers.

1) *Wearable Devices*: Wearable devices constitute the interface between IoT systems and human users. They can collect and transmit data over the internet or even interconnect with other IoT devices in the same area, like in a smart space. However, communication impacts their battery life.

Al-Sarawi et al. [3] review and study different communication protocols through different criteria including power consumption, range, network, topology, and cryptography. 6LoWPAN and BLE have matured and have become state-of-art wireless communication protocols for IoT devices. Related to power consumption, Trappe et al. [23] study the types of threats low-end Internet-connected devices face and the trade-off between the energy needed to execute the core application and needed to compute conventional cryptography.

Fitbit, a tracking wearable, is also studied to identify its

2) *Kiosk Devices*: Interactive kiosks have been developed since 1977, with the purpose to provide access to information and other services, like Internet access or ticket selling platform. Nowadays, these systems show a similar overall architecture: the kiosk device itself and a database server that collects and stores information provided by the kiosk. The kiosk is based on three components: The kiosk hardware, software, and application [14].

Single Board Computers equipped with sensors, communication actuators, and security functionalities, like Raspberry PI and Arduino Yun, can be used to realize such IoT products [2]. In [11] it is shown how a Raspberry Pi is used to make a low power consumption electronic voting kiosk booth.

C. Usable Security

Zurko et al. [27] conceived one of the early concepts of user-centered security in the 1990s. They showed several approaches on how to achieve it depending on the stage of development. User-centered security design from the early stages is the most highlighted approach in the paper, even presenting a case study. One of the five lessons learned by Balfanz et al. [5] is that both concepts must coexist in the very first stages of system design and that applying one on top of the other after the design process is a mess.

Authentication ceremonies are one of the most important and well-understood security usability challenges, specifically in secure messaging [7][24]. Users must complete a sequence of secure manual operations to verify their identity but those may introduce awkwardness to the users because they may represent policies or mechanisms that go against their values. A solution, shown by Lorri et al. [16] is to make users believe that their assets are under attack and that the security mechanisms provided by the authentication ceremony are effective against such attacks.

Fassl et al. [7] describe an entire user-centered design approach based on a four-stage process, where the last stage is a mixed-methods evaluation containing a user survey that tries

to understand the perceived security, relative to the possible threats of the system, and a User Experience Questionnaire, along with a Systems Usability Scale section. We followed a similar approach to evaluate the usability of our solution.

D. Summary

Location certification systems have come a long way, but have converged into a general architecture, including witnessing systems and digital signatures as proofs. Location proofs have multiple use cases, from medical appointments to the commercial sector. IoT technologies are diverse and heterogeneous and there is not a single standard protocol to be used every time. The five-layer IoT architecture provides a model for developing any IoT functionality. Both hardware and software IoT stack show vulnerabilities and mitigating them cost processing power and energy consumption. Authentication ceremonies are one of the most well-understood challenges in usable security, being the borderline between the emotions and values of users and secure systems. There are no location certification systems especially targeted at wearable devices focused on leveraging the user experience.

III. SUREPRESENCE

We developed SurePresence, a two-components application that allows a user to prove his location when interacting with a presence interactive kiosk through the use of location proofs. These two components are: *Client* and *Kiosk*; the first component represents the prover that makes location claims while the second represents a witness of the system that endorses the claim. In Section III-A we detail all aspects of the design of the SurePresence system and in Section IV we show the implementation of our solution in a medical office use case where a patient is able to justify his absence of work or school when attending an appointment, using location proofs.

A. Design

We now explain all aspects regarding the design and development of the SurePresence system and its location proof techniques. We discuss the assumptions, identify the requirements, and present the architecture of our system.

1) *Assumptions*: The entities utilizing SurePresence, which we call system operators, are the businesses that need location certificates to provide some service or functionality. They decide the locations where to use our solution, called points of interest, that influence the chosen location proof technique.

We assume the kiosk is a plug-and-play device [20] and is only deployed in trusted locations. These are hand-picked points of interest that do not show any harm to the kiosk, possibly protected by a bystander, and that have trustworthy resources, like a reliable power source or Wi-Fi connection.

We assume the devices where SurePresence is deployed are capable of providing a location or position of a user through GPS or GNSS. Our solution does not generate the location of a user, only proofs to ascertain its legitimacy. For now, we also assume that those services are responsible for the distribution of keypairs for their users and symmetric keys to be used in

the communications between the users and the kiosk. We also assume the previous distribution of the digital certificates of the kiosk and the server, for secure communications. We also assumed an already logged-in account in the development and evaluation of the SurePresence application.

Finally, we assume that either the kiosk or the client will have a Wi-Fi connection at some point, to submit the location certificate to the server. The best-suited technique to be used will be determined by which entity has a Wi-Fi connection.

2) *Requirements*: SurePresence should only produce location certificates for authenticated users. Even if a user does not have an account, he should be able to authenticate himself when interacting with the kiosk. The need of having an account drastically reduces the user experience of the authentication ceremony since the user is forced to register an account before interacting with the kiosk. Finally, our solution does not depend on the location, environment, or context of usage to produce location certificates. So we can summarize the functional requirements:

- **R1** - Location proofs can only be produced for authenticated users.
- **R2** - The user does not need an account when approaching a kiosk.
- **R3** - The kiosk component of SurePresence only requires a consistent power source from the deployment location to successfully endorse a claim and submit it to the verifier.

The most important non-functional requirement is *usability* in order to leverage the user experience provided by SurePresence. Other requirements are: **Portability** - SurePresence should be ready to be used in some mobile and wearable devices and should be able to create location certificates in their absence; **Adaptability** - The authentication ceremony needed to create location certificates must be familiar to users; **Interoperability** - The different operators, entities, and technologies should be able to communicate among themselves to create the location certificate; **Verifiability** - Any location certificate produced should be verified and cannot be consumed if it is not; **Extensibility** - Our system must be flexible for future modifications and extensions; **Security** - All components of our solution should resist to all types of attacks; **Privacy** - Sensitive and private information about the user should not be disclosed in the absence of a bystander.

3) *Architecture*: The architecture of the developed SurePresence application is illustrated in Figure 2 and it is based on the state-of-art location certification systems architecture shown in Figure II-A1. In SurePresence, though, witnesses cannot act as provers, since our only witness is a trusted interactive presence kiosk. Provers of our system are portrayed as SureThing users. The server acts as a verifier by receiving the location claims and endorsements and verifying their legitimacy generating location certificates. In our architecture, we do not have a Certificate Authority (CA), since both witness and verifier are trusted entities and the prover authenticates himself using an API authentication token.

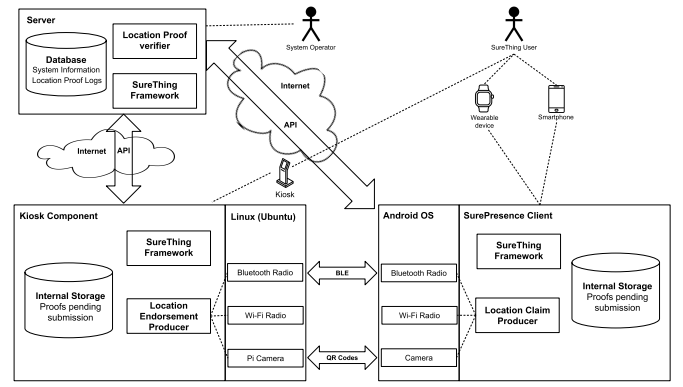


Fig. 2. SurePresence Architecture.

The client component on the bottom right side represents the prover. It is a component that runs on smartwatches and smartphones and has the responsibility of authenticating the user when interacting with the kiosk and generating signed location claims. Our witness model consists of just one entity, the kiosk component on the bottom left side. Just like in APPLAUS [26], PROPS [10], PASPORT [19] and in [4], the witness is capable of generating both claims and endorsements, depending on the location proof technique. The server, which can be seen on the top left corner of the figure, acts as the verifier and is responsible for storing verified location certificates. The API request handler will deal with all requests made by the kiosk and client API, over the Internet. The remaining elements will be explained throughout this work.

This client-server model with a single witness also represents a simpler architecture when compared, for example, with a peer-to-peer communication model.

As detailed in Figure 2, proofs pending submission can be stored locally and submitted once a Wi-Fi connection is established in both kiosk and client devices. Thus, a constant connection to the server is not necessary.

4) *Security and Privacy*: In our model, we consider the server and the kiosk as trusted entities, and the client as untrusted. Although it is unusual to consider a witness as a trusted entity, the kiosk will not have human control and will not help provers in possible collusion attacks. The user even after authentication may still be a malicious prover.

The communication between the client and the server is similar to the communication between the kiosk and the server, which is over a REST API using the HTTPS protocol. REST is an architectural style for web services, defining a set of constraints to be used in the communication with those services. One of the constraints that define a RESTful system is that it must be based on a client-server architecture, just like the SurePresence, but does not restrict the technologies communicating, providing the interoperability requirement.

HTTPS is a secure extension of HTTP with TLS in the transport layer, to provide applications with secure TCP connections. These are commonly used and widely supported by

most programming languages. We studied the possibility of using COAP, instead of HTTP, but it does not include any security features, besides showing bad packet delivery [25] since it uses UDP datagrams, which are unreliable. To provide security, DTLS would need to run on top of UDP, but it is not suitable to be used in IoT devices [13]. The communication between the client and the kiosk is over BLE.

Digital certificates provide authentication to both the kiosk and server. These certificates are bundled with the client application, on both the kiosk and user side, as part of our assumptions, previously described in Section III-A1. We ignored the client authentication since we considered the same logged-in account, as described in Section III-A1.

IV. IMPLEMENTATION

We deployed the SurePresence application in a medical office use case, where a patient, acting as prover, authenticates himself with the interactive kiosk, present in the medical office, and generates a location certificate that can be used to obtain the legitimacy of the medical appointment, in case the patient needs to obtain any legal document for the absence of work or school. This use case represents the singular *location case of traceability*, presented in Section II-A2, since attending a medical appointment does not require assessing any past locations or proofs. In Section IV-A we detail the platforms and technologies used to deploy SurePresence. In Section IV-B we describe the novel location proof techniques a prover can perform when interacting with a kiosk to generate location certificates. In Section IV-C we do a summary of the major aspects of our implementation of SurePresence.

A. Platform

We developed the client wearable application for the Android Wear OS since Android is the most complete operating system to be used in IoT environments, as we previously concluded in Section II-B. Our client application is written in Java 8 and our chosen SDK version was 26.

The SurePresence client smartphone application is targeted for Android (8.0) based smartphones. It was written in Java 8 and also uses the SDK 26.

The SurePresence kiosk application is targeted at any Ubuntu-based device. The application was mainly written in Python 3, including the Graphical User Interface, which was developed using the PyQt¹ library. The application includes a Java 8 component required to execute the official Portuguese government middleware for reading the citizen card (smart card)². To read QR codes, we use the Zbar³ library.

B. Novel Location Proof Techniques

We present the novel location proof techniques through which a user can generate a location certificate when using the SurePresence system and interacting with the kiosk. They benefit from the presence kiosk that authenticates the user

and generates location endorsements to strengthen the claims produced by the users. These techniques present different interactions with the kiosk using different devices. Those interactions are perceived by the user as authentication ceremonies since it is easier to understand the concept of authentication rather than location proof.

1) *Kiosk-Only Technique*: This technique allows a user to prove his location only by using his citizen card. We make use of the official Portuguese official citizen card middleware, as previously mentioned in Section IV-A, to read all the information we need to authenticate the prover, without damaging or modifying the smart card. This is taken care of by the smart card reader embedded in the kiosk.

The user approaches the kiosk, selects the citizen card icon, and introduces the citizen card in the reader as shown in the kiosk UI. Only public information, including the name and the citizen card ID, is read from the citizen card since private information is not necessary and would require an authentication PIN from the user. Unlike the other techniques, the prover does not create his own location claim, which is taken care of by the kiosk. Although it may seem odd that it is a witness claiming the presence of the prover, it is justified by the physical interaction with the kiosk when introducing the citizen card to the reader. The location claim requires a unique ID from the user, which in this case is the citizen card ID. The kiosk creates a signed location endorsement from that claim and sends both artifacts to the Verifier. Therefore, it requires a Wi-Fi connection. After concluding this process, the kiosk informs the user he can remove his citizen card.

2) *Kiosk-Wearable Technique*: This technique is the most IoT-ready of the three. It generates a location certificate through the interaction of a wearable device with the kiosk.

To start the authentication ceremony, the user needs to select the smartwatch icon of the kiosk main screen. Then, he opens his wearable application and selects the “Kiosk” button. After pressing it, an auxiliary thread on the wearable will initiate all the necessary Bluetooth structures to connect to the kiosk. When the wearable has everything set up, it displays its own device name, so that it can be identifiable by the user. The wearable has to send user information to the kiosk so that the user is authenticated and a location certificate can be created for him. The kiosk does not know the name or the MAC address of the wearable that is supposed to connect while the wearable application knows exactly the MAC address of the kiosk. Therefore, the kiosk has to scan for the wearable device. Otherwise, it would need to accept any BLE connection, which is extremely unsafe.

After pressing the “next” button in the kiosk UI, the kiosk scans for nearby devices. For each device found, it will update the list in its interface with the name of the device found (or the MAC address, in case the name is not defined), from which the user selects its device and confirms it.

After confirmation, the kiosk sends a connection request to the chosen wearable, which is waiting for connections. If the connecting device does not have the known MAC address of the kiosk, the connection request is rejected.

¹<https://wiki.python.org/moin/PyQt>

²<https://www.autenticacao.gov.pt/web/guest/cc-aplicacao>

³<https://github.com/Polyconseil/zbarlight>

The wearable creates a location claim with the e-mail of the logged-in user and other relevant information including its location. A file with the MAC address of the deployed kiosk and the latitude/longitude of its location is bundled with the wearable application. The wearable signs the claim, creating a signed location claim. Such artifact is read through Bluetooth Low-Energy by the kiosk that creates a location endorsement with the information provided by that claim and signs it creating a signed location endorsement, which is sent to the Verifier.

3) *Kiosk-Smartphone Technique*: This technique was originally proposed by Maia et al. [18], in the SureThing context, but never deployed.

The technique is started by selecting the smartphone icon in the kiosk UI. Then, the user needs to access the “QR Code” section on his smartphone application, which automatically generates a signed location claim, displaying it in a QR code.

The kiosk, using its camera module, scans the QR code and obtains the signed location claim. It creates a signed location endorsement encoded in a Base64 string and displays it in a new QR code, so that the user scans it with his smartphone application, through the “Scan” section. A successful scan gives audio feedback. Since a QR code does not know when it is scanned, we had to include in the kiosk UI a “done” button on the top right corner of the screen to conclude the technique.

Unlike the previous techniques, it is the prover who submits both claim and endorsement to the Verifier side, once he establishes a Wi-Fi connection. Therefore, the smartphone locally persists all generated signed location claims and scanned signed location endorsements, through an SQLite database. This database provides two tables, one for each artifact, where the key in both tables is the UUID identifying them.

This technique appears to be suited to remote locations or isolated environments where can be impossible for the kiosk to obtain a signal or to establish a Wi-Fi connection.

C. Summary

In this Section, we presented SurePresence including its design aspects, the requirements, and assumptions, as well as its architecture and a security assessment of the whole system. We then detailed the implementation of SurePresence for a medical appointment use case, including the platforms where it was developed and three novel location proof techniques based on the interaction of a presence kiosk.

V. EVALUATION

This Section presents the evaluation of the SurePresence system. We first do a requirements check on the implemented code in Section V-A. We then describe the user study performed on the SurePresence system and its location proof techniques in the context of medical appointments. Finally, we do a quantitative and qualitative evaluation of the results from the user study, analyzed and discussed in Section VI.

A. Requirements Assessment

We start by assessing the functional and then the non-functional requirements of the SurePresence system.

1) *Functional Requirements*: All three requirements, enumerated in Section III-A2, were ensured by the flexibility of the different ways of generating location certificates through the three techniques. The **R1** requirement is ensured by the fact that, without user authentication, a location certificate is never produced. If a user does not have an account logged in any of the two ubiquitous devices, he can still use his citizen card to authenticate himself using the Kiosk-Only technique.

When approaching a kiosk the user does not require an account, both logged in or simply created. Similar to the previous requirement, the citizen card ensures the **R2** requirement, as it is sufficient to authenticate the user and generate location certificates, leveraging the usability of our system. Enforcing a patient to create an account at the medical office, just to authenticate himself, would provide a poor user experience, and our system would probably be ignored at the office.

The **R3** requirement is completely ensured by the Kiosk-Smartphone technique as it locally stores the location claims and endorsements. The kiosk component only requires a reliable power source to successfully witness a prover and endorse a claim. A reliable Wi-Fi infrastructure is not required to endorse location claims and submit them to the verifier.

2) *Non-functional Requirements*: Regarding the non-functional requirements, the SureThing framework ensures most of them. Thanks to both Core Utils and Core Data libraries we ensure the **Interoperability**, **Verifiability** and **Extensibility** requirements. This framework is detailed in the full document of this article. The **Portability** requirement is ensured by the Kiosk-Only technique since it is not needed any ubiquitous device to produce both location claims and endorsements. The **Adaptability** requirement can only be assessed through the user evaluation, detailed in Section V-B. We discuss if this requirement was ensured in Section VI. Both **Security** and **Privacy** requirements were ensured for the Kiosk-Wearable technique, thanks to the implementation of an end-to-end application-layer protocol to protect messages. Such protocol is detailed in the full document of this article. Regarding the remaining techniques, since we consider the kiosk as a trusted witness, we considered it will not disclose any type of information. The Kiosk-Smartphone technique is vulnerable to location spoofing attacks since the QR codes can be exchanged between multiple users.

B. User Evaluation

We start by outlining the research questions we aim to answer with this evaluation. In Section V-B2 we do a characterization of the users recruited for the user study. In Section V-B3 we describe the relevant materials used in the user study, as well as the environment it took place. In Section V-B4 we detail the steps of the procedure that conducted the study. The information that was collected throughout the user study is described in Section V-B5. In Section V-B6 we specify the design of the study and how we analyze its resulting information. Finally, in Section V-B7 and Section V-B8 we present the results obtained from both evaluation methods.

1) *Research Questions:* We conducted a user study to help us answer the following research questions regarding our implementation:

- i Which location proof technique is the user more comfortable with?
- ii Which technique has the smallest time per action ratio?
- iii What is the effectiveness of each novel location proof technique?
- iv From the perspective of the user, which technique is less vulnerable to the presented threats?

2) *Participants:* We recruited 32 randomly selected students in the Instituto Superior Técnico Alameda Campus. Their average age was 21.28 (*std.* = 2.247), where the majority were men (56.3%) and had never used a smartwatch before (59.4%).

3) *Apparatus:* The user study took place in a room in the place, with a consistent power supply and Wi-Fi connection. The interactive kiosk was built using a Raspberry Pi 4 equipped with a 720x480p resolution touchable screen, a Pi camera, and an external USB smart card reader. A Huawei Watch 2 and a Samsung Galaxy S9 were used to simulate the respective techniques.

4) *Procedure:* The overall purpose of the study was explained to the participants before asking them to complete the authentication ceremony for each location proof technique, randomly ordered. After completing them, the participants were given a questionnaire to complete, with a user characterization section, a User Experience questionnaire, and a perceived vulnerability section on multiple model threats. The last two sections were classified using 5-point Likert-scales [15] (1 - Totally disagree/Not vulnerable; 5 - Totally agree/very vulnerable; respectively for each section). The User Experience metrics can be seen in Table V-B7b and the multiple threats were explained through storyboards, which can be seen in Figures 3, 4, and 5.

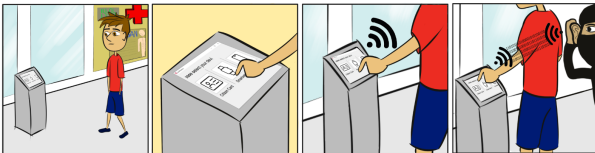


Fig. 3. Man-In-The-Middle threat storyboard.



Fig. 4. User Information Disclosure Threat Storyboard.

An interview composed of three questions was made at the end of the questionnaire, to understand the favorite and



Fig. 5. Location Spoofing Threat Storyboard.

TABLE I
AVERAGE TIME AND NUMBER OF ACTIONS RESULTS FOR ALL THREE LOCATION PROOF TECHNIQUES AUTHENTICATION CEREMONIES.

	Citizen Card		Wearable		Smartphone	
	avg.	std.	avg.	std.	avg.	std.
Nr. actions	3.06	0.354	7.47	0.842	7.19	0.738
Time (s)	12.74	3.838	25.55	10.589	48.28	19.429

the safest authentication method perceived by the user and in which other contexts could SurePresence be used.

5) *Dependent Measures:*

a) *Quantitative data:* We collected several measures regarding the authentication ceremonies of each technique: time and number of actions needed to conclude them and their success. We collected the values of the Likert scale for each User Experience metric as well as the Likert scale vulnerability values of each technique for each threat.

b) *Qualitative Data:* We collected the answers from the interview, which include data about the usefulness of the SurePresence system compared to current medical office solutions, other useful use cases, and the safest/favorite technique of the participants.

6) *Design and Analysis:* We analyzed the quantitative ordinal measures using descriptive statistics. Then, we compared them against a within-subject factor using three conditions (techniques), where the participants only had one trial for each condition, which was done using the Friedman test. For the measurements that showed no statistical differences between the different conditions, we applied post-hoc tests using Mann-Whitney tests [17] with Bonferroni correction [12].

7) *Quantitative Evaluation:* We first analyze the results of the measurements previously described in Section V-B5a where we refer to the first two points as authentication metrics, as shown in Section V-B7a and evaluate the results obtained from the User Experience section of the questionnaire in Section V-B7b. Finally, we evaluate the results obtained on the perceived vulnerability of each technique for each threat.

a) *Authentication Metrics:* The results obtained for the average number of actions and the average time required to

TABLE II
FRIEDMAN TEST STATISTICAL RESULTS OF THE AUTHENTICATION METRICS FOR ALL THREE LOCATION PROOF TECHNIQUES AUTHENTICATION CEREMONIES.

	Friedman Test		
	chi-square	df	p-value
Nr. actions	55.143	2	0
Time (s)	54.813	2	0

TABLE III
AVERAGE VALUES FOR EACH USER EXPERIENCE METRIC IN ALL THREE LOCATION PROOF TECHNIQUES.

	Citizen Card		Wearable		Smartphone	
	avg.	std.	avg.	std.	avg.	std.
Easiness	4.75	0.803	4.44	0.801	3.66	1.066
Fastness	4.75	0.803	4.47	0.879	3.78	1.070
Compreh.	4.75	0.803	4.38	0.833	3.56	1.162
Stress	1.44	1.045	1.81	1.330	2.19	1.424
Trust	4.34	1.260	4.13	0.833	3.75	1.164
Security	4.34	0.983	4.16	0.987	4.31	0.965
Privacy	3.81	1.230	4.09	1.088	4.28	0.958

TABLE IV
FRIEDMAN TEST STATISTICAL RESULTS OF THE USER EXPERIENCE METRICS FOR ALL THREE LOCATION PROOF TECHNIQUES AUTHENTICATION CEREMONIES.

	Friedman Test		
	chi-square	df	p-value
Easiness	29.718	2	0.000
Fastness	27.831	2	0.000
Compreh.	29.459	2	0.000
Stress	12.057	2	0.002
Trust	11.268	2	0.004
Security	5.148	2	0.076
Privacy	7.815	2	0.020

successfully perform each location proof technique can be seen in Table V-B7a. The Wearable and Smartphone techniques present a similar required average number of actions. We performed a within-subject factor comparison using three conditions (techniques) for both metrics.

A Friedman test revealed a significant effect of each technique on the number of actions and time needed for authentication as shown in Figure V-B7a. A post-hoc test using Mann-Whitney tests with Bonferroni correction, resulting in a significance level set at $p\text{-value} < 0.017$ ($\alpha = 0.05$, $df = 2$), showed the significant differences in the number of actions ranks between all techniques. The citizen card takes a lot fewer actions to successfully authenticate a user.

A similar post-hoc test using Mann-Whitney tests with the same Bonferroni correction showed significant differences in time ranks between all techniques. The Citizen Card technique takes a lot less time to authenticate a user.

b) *User Experience Metrics*: The obtained average results of the User Experience metrics can be seen in Table V-B7b. The Citizen Card technique presented the best results for all metrics, except for the privacy one. The Wearable technique presents more similar results to the Citizen Card technique rather than the Smartphone one, which is clearly the worse, as showcased by the not overlapping confidence intervals presented in Figure 6.

A Friedman test revealed a significant effect of each technique on all user experience metrics, except for the security one ($\chi^2 = 5.148$, $p\text{-value} = 0.076$). These results can be seen in Table V-B7b.

A post-hoc test using Mann-Whitney tests with Bonferroni correction was done for every metric, except for security. Regarding the easiness, fastness, and comprehensiveness met-

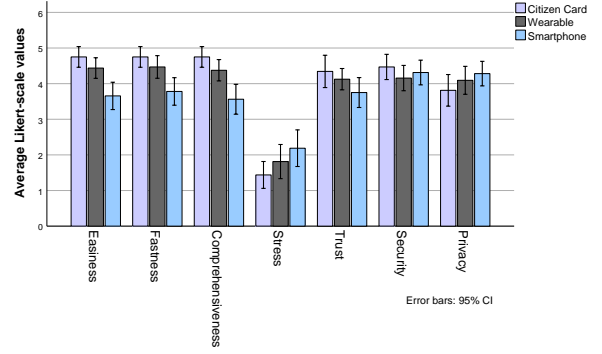


Fig. 6. User Experience Metrics plot with Confidence intervals for each location proof technique.

TABLE V
AVERAGE RESPONSES OF THE USERS PERCEPTION OF THREE THREAT MODELS ON ALL THREE LOCATION PROOF TECHNIQUES.

	Citizen Card		Wearable		Smartphone	
	avg.	std.	avg.	std.	avg.	std.
Man-In-The-Middle	2.03	1.307	2.75	1.218	2.47	1.164
Information Disclosure	3.06	1.435	2.47	1.016	2.87	1.264
Location Spoofing	2.91	1.510	3.75	0.916	3.44	1.076

rics, the test showed significant differences in their ranks between the three location proof techniques. Regarding the stress metric, the test only showed significant differences between the Smartphone and the Citizen Card ($Z = -2.827$, $p\text{-value} = 0.005$). About the trust metric, the test showed no significant differences between all techniques, since all obtained $p\text{-value} > 0.017$. Finally, the Smartphone technique ensured the most privacy, as shown in Figure 6.

c) *Threat Models*: The obtained average values perceived by the users of the vulnerability of the techniques for each threat can be seen in Table V-B7c. The Citizen Card technique is perceived as the least vulnerable technique regarding Man-In-The-Middle and Location Spoofing attacks, while the Wearable as the most vulnerable. These roles switch for the Information Disclosure threat, which is corroborated by the previously obtained values for the privacy metric.

A Friedman test revealed a significant effect of the technique on the vulnerability perception of the users on the Location Spoofing attack ($\chi^2 = 13.816$, $p\text{-value} < 0.01$), while it did not show statistical differences between techniques for the

TABLE VI
FRIEDMAN TEST STATISTICAL RESULTS OF THE THREAT MODELS ON ALL THREE LOCATION PROOF TECHNIQUES.

	Friedman Test		
	chi-square	df	p-value
Man-In-The-Middle	4.515	2	0.105
Information Disclosure	5.952	2	0.051
Location Spoofing	13.816	2	0.001

remaining attacks. These results can be also seen in Table V-B7c. The same post-hoc test showed significant vulnerability differences between the Wearable and the Citizen Card techniques ($Z = -2.922$, $p\text{-value} = 0.003$).

8) *Qualitative Evaluation*: In this section, we do a qualitative evaluation of the results obtained from the user study, specifically from the interviews.

a) *Interviews*: The Citizen Card technique was the favorite of the participants ($N = 24$): “It is the easier, faster, simpler, more convenient, safer, more efficient and more universal technique”. The same technique was also chosen as the most secure ($N = 19$), where 12 of those 19 responses were following this line of thought: “The citizen card presents less danger thanks to security inherent to the smart-chip”. Registering students in educational events were the majority of the answers of other use cases for SurePresence.

VI. DISCUSSION

We now discuss the results obtained from the SurePresence evaluation done through the user study and analyze RQ1 through RQ4 (stated in Section V-B1).

Research Question 1 The Citizen Card technique is the most straightforward technique when looking at the authentication metrics, as would be expected since the number of actions in an optimal authentication with the citizen card is inferior to the number of actions needed for the remaining techniques. Looking at the user experience metrics, the citizen card was the clear winner, where the Friedman test revealed a significant distance for the remaining techniques regarding all metrics, as well as their average values. The Citizen Card technique is the easiest, fastest, and most comprehensive technique of the three, requiring only one action different from clicking. It also presents to be the most trustworthy technique, thanks to the trust of the users in the security inherent to the smart chip. Regarding the same metric, the results between the Citizen Card and the Wearable are similar, which makes us optimistic about the usage of wearables in a hospital context. Finally, complementing this with the first question of the interviews, where the Citizen Card technique was the preferred one (24 out of the 32 participants), we conclude the kiosk-only technique is the one the user feels more comfortable with, thus answering the first research question and ensuring the **adaptability** non-functional requirement.

Research Question 2 The time needed for a user to authenticate is directly related to the number of actions he needs to perform. So, it is understandable that the Mann-Whitney tests between the Wearable and the Smartphone techniques for both authentication metrics showed different results since the actions related to scanning QR codes are much more complex than just selecting a device from a list. The time per clicks ratio, which represents the time needed to act, gives us more meaningful and fair conclusions, which can be seen in Table VI, for each location proof technique.

The Wearable and Smartphone techniques have a similar number of actions, as shown in Table V-B7a so this ratio tells us that the Smartphone technique is badly designed and using

TABLE VII
TIME PER ACTION RATIO FOR EACH LOCATION PROOF TECHNIQUE.

	Citizen Card	Wearable	Smartphone
Time per action (s)	4.16	3.42	6.71

QR codes may be too difficult for the user. Answering the second question, it is the Wearable technique that presents the smallest time per action of all three techniques. This is a promising result for the usage of IoT devices in location certification systems and is even more impressive when looking at the fact that 59.4% of the participants had never used a smartwatch before the study.

Research Question 3 The Smartphone technique had 62.5% effectiveness while the remaining techniques had 100% thus answering the third research question. It shows that people are not as acquainted with QR Codes as they think since most of these participants did not know the difference between scanning a QR code and having a QR code being scanned.

Research Question 4 The obtained results regarding the security metric show *there are no statistically significant differences between techniques* but we can make a more fine-grained analysis looking at the results of the threat models. The participants perceived the Wearable technique as the most vulnerable regarding Man-In-The-Middle attacks. The Citizen Card is the most vulnerable technique to the disclosure of private information. Regarding Location Spoofing attacks, the Wearable technique is once again perceived as the most vulnerable technique because it uses an easily shareable device from the point of view of the user. Such opinion is more divided when it comes to the Citizen Card since some users consider it as a unique and intransmissible device. Overall, the citizen card shows to be the most secure technique for the participants regarding the three possible threats, which answers the last research question.

VII. CONCLUSION

Location certification systems are crucial enablers for secure and reliable location-based services. They verify information about the location of users and prevent location spoofing attacks on applications. An attempt to make such systems usable and secure is to leverage IoT and constrained devices, allowing the generation and validation of location certificates in more seamless ways.

We presented SurePresence, a location certification system that through the interaction of multiple ubiquitous devices with a presence interactive kiosk, allows the generation of location claims and endorsements.

We implemented a prototype of SurePresence for a medical use case where a patient can issue location proofs when attending a medical appointment, verifying his presence through three novel kiosk-based location proof techniques.

We assessed the user experience and perceived security provided by the SurePresence system and its location proof techniques through a user study covering user experience

metrics and the perceived vulnerability of each technique for the illustrated threats. The Citizen Card technique was perceived as the most usable, most secure, and most ready to be used in a medical context, with a user information privacy tradeoff, while the Wearable technique presented surprising results regarding the provided user experience.

A. Achievements

We developed a location certification system capable of verifying the presence of a prover in a singular location through the interaction of multiple devices with a kiosk. We implemented SurePresence in a medical use case, where a patient, attending a medical appointment, is able to verify his presence. We evaluated the user experience provided by the novel location proof techniques as well as the perceived security of the SurePresence system.

B. Future Work

A comparative evaluation between a single witness and peer-to-peer witnesses for the same and other use-cases should be done to understand if the role of the kiosk is critical regarding the user experience it provides.

ACKNOWLEDGEMENTS

This work was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UIDB/50021/2020 (INESC-ID) and through the project with reference PTDC/CCI-COM/31440/2017 (SureThing).

REFERENCES

- [1] Architecting the Internet of Things. Springer-Verlag GmbH (2011), https://www.ebook.de/de/product/14076594/architecting_the_internet_of_things.html
- [2] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials* **17**(4), 2347–2376 (2015)
- [3] Al-Sarawi, S., Anbar, M., Alieyan, K., Alzubaidi, M.: Internet of things (iot) communication protocols: Review. In: 2017 8th International Conference on Information Technology (ICIT). pp. 685–690 (2017)
- [4] Alamleh, H., AlQahtani, A.A.S.: A cheat-proof system to validate gps location data. In: 2020 IEEE International Conference on Electro Information Technology (EIT). pp. 190–193 (2020). <https://doi.org/10.1109/EIT48999.2020.9208243>
- [5] Balfanz, D., Durfee, G., Smetters, D., Grinter, R.: In search of usable security: five lessons from the field. *IEEE Security & Privacy Magazine* **2**(5), 19–24 (sep 2004). <https://doi.org/10.1109/msp.2004.71>
- [6] Canlar, E.S., Conti, M., Crispo, B., Di Pietro, R.: Crepuscolo: A collusion resistant privacy preserving location verification system. In: 2013 International Conference on Risks and Security of Internet and Systems (CRiSIS). pp. 1–9 (2013). <https://doi.org/10.1109/CRiSIS.2013.6766357>
- [7] Fassel, M., Gröber, L.T., Krombholz, K.: Exploring User-Centered Security Design for Usable Authentication Ceremonies. Association for Computing Machinery, New York, NY, USA (2021), <https://doi.org/10.1145/3411764.3445164>
- [8] Ferreira, J., Pardo, M.L.: Witness-based location proofs for mobile devices. In: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). pp. 1–4 (2018). <https://doi.org/10.1109/NCA.2018.8548244>
- [9] Frustaci, M., Pace, P., Aloï, G., Fortino, G.: Evaluating critical security issues of the iot world: Present and future challenges. *IEEE Internet of Things Journal* **5**(4), 2483–2495 (2018)
- [10] Gamba, S., Killijian, M., Roy, M., Traoré, M.: Props: A privacy-preserving location proof system. In: 2014 IEEE 33rd International Symposium on Reliable Distributed Systems. pp. 1–10 (2014). <https://doi.org/10.1109/SRDS.2014.37>
- [11] Gurubasavanna, M.G., Ulla Shariff, S., Mamatha, R., Sathisha, N.: Multimode authentication based electronic voting kiosk using raspberry pi. In: 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)-I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on. pp. 528–535 (2018). <https://doi.org/10.1109/I-SMAC.2018.8653726>
- [12] Haynes, W.: Bonferroni correction. pp. 154–154. Springer New York (2013). https://doi.org/10.1007/978-1-4419-9863-7_1213
- [13] Karagiannis, V., Chatzimisios, P., Vázquez-Gallego, F., Alonso-Zárate, J.: A survey on application layer protocols for the internet of things (2015). <https://doi.org/10.5281/ZENODO.51613>
- [14] Kaur, H., Malhotra, S.: Use of “kiosks” as a self service tools in libraries. In: 2018 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS). pp. 269–271 (2018). <https://doi.org/10.1109/ETTLIS.2018.8485257>
- [15] Likert, R.: A technique for the measurement of attitudes. *archives of psychology* (1932)
- [16] Lorrie Faith Cranor, S.G.: Security and Usability: Designing Secure Systems That People Can Use. OREILLY MEDIA (2005), https://www.ebook.de/de/product/3593364/lorrie_faith_cranor_simson_garfinkel_security_and_usability_designing_secure_systems_that_people_can_use.html
- [17] MacFarland, T.W., Yates, J.M.: Mann–whitney u test. pp. 103–132. Springer International Publishing (2016). https://doi.org/10.1007/978-3-319-30634-6_4
- [18] Maia, G.A., Claro, R.L., Pardo, M.L.: Cross city: Wi-fi location proofs for smart tourism. In: Grieco, L.A., Boggia, G., Piro, G., Jararweh, Y., Campolo, C. (eds.) Ad-Hoc, Mobile, and Wireless Networks. pp. 241–253. Springer International Publishing, Cham (2020)
- [19] Nosouhi, M.R., Sood, K., Yu, S., Grobler, M., Zhang, J.: Passport: A secure and private location proof generation and verification framework. *IEEE Transactions on Computational Social Systems* **7**(2), 293–307 (2020). <https://doi.org/10.1109/TCSS.2019.2960534>
- [20] Sad, A.M.H., Choyon, M.M.S., Rhydwani, A.H.M., Hossain, C.A.: An interactive low-cost smart assistant system: Information kiosk as plug play device. In: 2020 27th Conference of Open Innovations Association (FRUCT). pp. 193–199 (2020). <https://doi.org/10.23919/FRUCT49677.2020.9211057>
- [21] Santos, H.F., Claro, R.L., Rocha, L.S., Pardo, M.L.: STOP: a location spoofing resistant vehicle inspection system (2020)
- [22] Saroui, S., Wolman, A.: Enabling new mobile applications with location proofs. In: Proceedings of the 10th Workshop on Mobile Computing Systems and Applications. HotMobile '09, Association for Computing Machinery, New York, NY, USA (2009). <https://doi.org/10.1145/1514411.1514414>
- [23] Trappe, W., Howard, R., Moore, R.S.: Low-energy security: Limits and opportunities in the internet of things. *IEEE Security Privacy* **13**(1), 14–21 (2015)
- [24] Vaziripour, E., Wu, J., O'Neill, M., Clinton, R., Whitehead, J., Heidbrink, S., Seamons, K., Zappala, D.: Is that you, alice? a usability study of the authentication ceremony of secure messaging applications. In: Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security. p. 29–47. SOUPS '17, USENIX Association, USA (2017)
- [25] Yassein, M.B., Shatnawi, M.Q., Al-zoubi, D.: Application layer protocols for the internet of things: A survey. In: 2016 International Conference on Engineering & MIS (ICEMIS). IEEE (sep 2016). <https://doi.org/10.1109/icemis.2016.7745303>
- [26] Zhu, Z., Cao, G.: Applaus: A privacy-preserving location proof updating system for location-based services. In: 2011 Proceedings IEEE INFOCOM. pp. 1889–1897 (2011). <https://doi.org/10.1109/INFCOM.2011.5934991>
- [27] Zurko, M.E., Simon, R.T.: User-centered security. In: Proceedings of the 1996 workshop on New security paradigms - NSPW '96. ACM Press (1996). <https://doi.org/10.1145/304851.304859>