Touchless Authentication for Health Professionals: Analyzing the Risks and Proposing Alternatives to Dirty Interfaces

1st Chiarelli Araújo Vale
Official Medical Board
Federal University of Santa Catarina
Florianópolis, Brazil
chiarelli.vale@ufsc.br

2nd Frederico Schardong
Federal University of Santa Catarina
Federal Institute of Rio Grande do Sul
Rolante, Brazil
frederico.schardong@rolante.ifrs.edu.br

3rd Maurício Barros
Department of Informatic and Statistics
Federal University of Santa Catarina
Florianópolis, Brazil
mauricio.v.barros@gmail.com

4th Ricardo Custódio
Department of Informatic and Statistics
Federal University of Santa Catarina
Florianópolis, Brazil
ricardo.custodio@ufsc.br

2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS) | 978-1-6654-6770-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/CBMS55023.2022.00088

***Abstract*—One of the most significant challenges for electronic services is ensuring that the person using a service is who they claim to be with an adequate level of trust. The user identity is confirmed through authentication. However, depending on the authentication method used, this process may not provide the expected security and is often bureaucratic. The authentication of healthcare professionals imposes additional challenges. For instance, they should not be exposed to touching peripherals nor remove their masks. This article presents: (i) a risk assessment of fraudulent authentication of health professionals; (ii) a proposal of authentication assurance levels for health professionals; (iii) a discussion of touchless authentication factors for health professionals; and (iv) an empirical evaluation of the proposals.**

***Index Terms*—authentication; health; touchless; level of assurance; identity and access management.**

I. Introduction

An individual's identity can be defined as a collection of personal information that characterizes and distinguishes her in society. This information may include the person's name, height, and hair color, among other things. Other characteristics that can be used to characterize someone's identity include their date and place of birth, as well as their parents' names [1].

The digital world and its legal aspects have become increasingly important as the Internet has become a routine part of people's work and play. One of the most critical challenges for the functioning of digital societies is ensuring, with an adequate level of trust, that the individual or entity that uses a virtual service is who they say they are [2–4].

Identity and Access Management (IAM) is a collection of processes that manage all stages of user access within an organization. Among these steps are identification, authentication, and authorization [5]. This research focuses on authentication. Identification is the process of supplying data that enables the unique description of a particular entity. Authentication is the process of confirming that an identified entity is who they claim to be. Typically, this requires producing evidence that only the legitimate entity could provide. Authorization is the process of granting permission to access specific resources and data.

A white coat and a stethoscope around the neck are frequently enough for the medical doctor to be recognized by society and allowed to act in emergencies where life is in danger and other situations. Nonetheless, such professionals have their own documentation for this purpose, which is rarely presented in any situation. Ideally, health specialists should concentrate solely on their medical duties and be authenticated to electronic systems as quickly and efficiently as they are in the real world. These professionals should not be concerned or hindered by IAM technologies. Still, the professional must be authenticated, and authorized in order to engage in health-related activities.

This article proposes secure, user-friendly authentication methods for medical professionals. We conduct a risk analysis of fraudulent authentication in the medical field to determine the Level of Assurance (LoA) required for the authentication of health professionals. In addition, we revise the National Institute of Standards and Technology (NIST) recommendations for authenticators [6] to include the functional and non-functional requirements of healthcare professionals. We conclude with an empirical evaluation of an easy-to-use two-factor authentication that does not require touching potentially contaminated surfaces and provides an appropriate LoA.

The remainder of this article is organized as follows. Section II provides the necessary background to follow this work. Our proposal for touchless authentication of health professionals is detailed in Section III. Following that, Section IV presents our empirical validation of the proposed framework, and Sections V and VI present related work and our final remarks, respectively.

2372-9198/22/$31.00 ©2022 IEEE
DOI 10.1109/CBMS55023.2022.00088

II. Background

A. Identity and Access Management

IAM systems are concerned with the creation, administration, and use of: (i) identifiers, which are data used to identify a person, such as full name, email, and phone number; (ii) credentials, which are data that provide evidence of identity ownership, such as password, digital certificate, tokens, and biometrics; and (iii) attributes, which are data that describe characteristics of the identity owner. For instance, the role of the health professional in the organization, hospital, or clinic; privileges and rights; medical specialty, among other things.

Identification, authentication, authorization, and auditing are the operations that use identifiers, credentials, and attributes [7]. First, an entity identifies itself to the system using an identifier. Second, by validating access credentials, the system determines whether or not the identity is genuine. Third, the system grants the authenticated user access to specific resources. Finally, everything identity-related an entity does is recorded in the system and can be used as evidence by the parties involved.

B. Authentication

The authentication mechanisms adopted by electronic identity systems dictate how the systems that use it, known as service providers (SP) or relying parties (RP), will be utilized in the daily lives of users.

The various methods of authenticating the user's digital identity are divided into three categories [8]: (i) *the user's knowledge* of a predetermined secret, which is typically represented by a password; (ii) *something the user possesses*, such as a magnetic badge or smartcard; and (iii) *something the user is*, in this strategy, the system compares the user's biometric characteristics with pre-registered values.

Authentication schemes can be categorized according to the number of factors used in the authentication process as follows [1, 9]: (i) *single-factor authentication (SFA)*, where authentication is performed with one factor; (ii) *two-factor authentication (2FA)*, where authentication is conducted with two distinct factors. Using biometrics in conjunction with a password, for instance, provides greater security than using a single or multiple passwords; and (iii) *multi-factor authentication (MFA)*: authentication is based on multiple factors.

Considering the vulnerabilities of each authentication method, authentication schemes employing fewer factors are more susceptible to attack. When an authentication system employs a smart card and password, it is vulnerable to password guessing attacks if the smart card is lost or stolen. This issue can be mitigated by incorporating a third authentication factor. However, applying additional authentication factors complicates the authentication process [10].

C. Level of Assurance

An identity's level of assurance is the degree of certainty that an identity is uniquely related to its owner [11]. In other words, the degree of confidence that it is only controlled and used by the person to whom the identity refers. The LoA is determined by the strength of the proof of identity process as well as the credentials and authentication mechanisms used. The LoA for proof of identity is determined by the method of identification (in person or remotely), the attributes collected, and the degree of certainty of those attributes. The LoA for authentication is determined by the type of credentials used, the number of authentication factors employed, and the transaction's cryptographic strength. Our research focuses on the different types of credentials and authentication factors.

Higher LoA reduces the risk of a fraudulent identity while increasing the cost and inconvenience for identity holders. As a result, it is critical to consider the different requirements for different usage scenarios in terms of the LoA.

To increase trust in online trading systems between European countries, the European Union established the Electronic Identification, Authentication, and Trust Services (eIDAS) [12]. Focusing on countries' digital development, it is a framework for standardizing identification, authentication, and electronic signatures. In eIDAS, the LoA classification is divided into three categories. *Low* - requires at least SFA, *substantial* - requires 2FA, in which both factors can be of the same category, and *high* - requires at least two distinct categories of authentication factors and protection against duplication and tampering, *e.g.*, embedding key material in tamper-resistant hardware token + PIN.

Furthermore, NIST published guidelines that detail recommendations on potential authenticators and their characteristics based on their counterparts of eIDAS' LoA, namely Authentication Assurance Levels (AAL). Table I summarizes the requirements for each AAL, including the types of authenticators permitted, the frequency of reauthentication, and the authentication intent for each assurance level.

Alternatives to the NIST-recommended authentication guidance for AALs can be determined based on purpose, risk tolerance, existing business processes, special considerations for specific populations, and data availability that provides similar mitigations as described [13]. Our proposal for AALs for health professionals is an alternative to NIST's guidelines and is detailed in the following section.

III. AAL and LoA of Health Professionals

The NIST guidelines provide a foundation for what authenticators to use in the three levels of assurance, establishing recommendations based on security requirements. However, the presented authentication methods are not tailored to the specific needs of health professionals: methods that protect the hygiene of professionals by preventing them from touching surfaces. We present our contributions in this section.

A. Risk Analysis

To determine the minimum LoA for the authentication of healthcare professionals, potential risks must be assessed, and mitigation measures must be identified. Risk assessments determine how much risk identity proofing and authentication processes should mitigate [13]. Authentication mistakes with severe consequences necessitate higher levels of assurance.

TABLE I
AUTHENTICATOR TYPES, FREQUENCY OF REAUTHENTICATION, AND AUTHENTICATION INTENT FOR EACH ASSURANCE LEVEL [6]

Requirement	AAL1	AAL2	AAL3

Permitted authenticator types	- Memorized Secret;
	- Look-up Secret;
	- Out-of-Band;
	- SF OTP Device;
	- MF OTP Device;
	- SF Crypto Software;
	- SF Crypto Device;
	- MF Crypto Software;
	- MF Crypto Device
		- MF OTP Device;
		- MF Crypto Software;
		- MF Crypto Device; or
		- Memorized Secret plus:
		  - Look-up Secret;
		  - Out-of-Band;
		  - SF OTP Device;
		  - SF Crypto Software;
		  - SF Crypto Device
			- MF Crypto Device;
			- SF Crypto Device and Memorized Secret;
			- SF OTP Device and MF Crypto Device or Software;
			- SF OTP Device and SF Crypto Software and Memorized Secret

Reauthentication frequency	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Auth intent	Not required	Recommended	Required

However, a LoA higher than necessary can cause user discomfort and additional costs.

To determine which LoA is appropriate for the authentication of healthcare professionals, we use Grassi *et al.*'s [13] model for risk analysis. It suggests three impact levels, namely *low*, *mild*, and *high* for six categories: (C1) inconvenience, distress or damage to standing or reputation; (C2) financial loss or agency liability; (C3) harm to agency programs or public interests; (C4) unauthorized release of sensitive information; (C5) personal safety; and (C6) civil or criminal violations.

We investigate fraudulent authentication in systems for social security doctors who have access to patients' health data and create reports for paid leave and retirement. We chose a non-assistance medical area where the consequences for the patient's health are lower than in assistance areas.

C1 is *high* because, in the worst-case scenario, it will cause serious long-term inconvenience and distress, as well as damage to either party's position or reputation. In relation to C2, it is *high* because, in the worst-case scenario, it will result in a significant financial loss for any party or a substantial liability for the health care provider. C3 is considered *mild* because, at worst, it will have a negative impact on organizational operations, assets, or the public interest. The C4 is *high* because, in the worst-case scenario, disclosing personal, confidential personal, or commercially confidential information to unauthorized parties results in a significant loss of confidentiality. The C5 is *low* because, at worst, it can cause minor injuries that do not necessitate medical attention. There will always be a possibility of harming personal safety with the unauthorized release of confidential information, even if the damage is psychological. Finally, C6 is *mild* in terms of the possibility of civil or criminal violations that may be subject to enforcement efforts.

Based on this analysis, we argue that the LoA *substantial* is the bare minimum acceptable for social security medical doctors, and generalize this result to the entire health care industry. Professionals work with human lives and fraudulent authentication in computerized systems can cause patients discomfort, financial losses, or even death. We must achieve comparable outcomes by performing this risk analysis by considering other medical specialties and other categories of health professionals.

A minimum assurance level greater than substantial would necessitate a more complicated, costly, and sometimes longer authentication procedure. In addition, the higher the level of assurance, the greater the likelihood of a false negative, that is, the refusal to authenticate the correct professional. This can be disastrous in emergency sectors. Depending on the situation, it may be suggested to maintain the substantial as the minimum LoA and to increment the authorization process for each environment or professional category in order to access a particular data or tools to perform certain procedure.

B. Authentication factors

The absence of surface contact is a prerequisite for the non-contamination of both the health care provider and surfaces in general. Consequently, touchless authentication is a functional requirement for authentication factors, while practicality and security are non-functional requirements. Below are detailed requirements and suggestions for each of the three authentication categories.

Authenticators of the *what you know* category can be transmitted touch-free via voice, which can compromise security because others in the same environment can eavesdrop. Techniques of anonymization are a potential solution to this issue. It is possible to use challenge-response techniques, in which the answer to the challenge can be given as a number after the question, and possible answers displayed on the computer screen. For instance, the challenge "In what city were you born? 1. New York; 2. London; 3. Beijing". In this example, the response that others would hear is a number without any context. This authenticator can be used as a second or third factor of authentication after identification was performed with another factor.

Regarding the *what you have* authenticators, the object must be in close proximity to the user without needing to be touched in order to be inserted or brought close to a piece of equipment. These requirements are met by technologies like Radio-Frequency Identification (RFID) [14] and Bluetooth [15]. As RFID employs low-power radio signals, there is no need for physical contact between the tag and

TABLE II
TYPES OF AUTHENTICATORS, REAUTHENTICATION FREQUENCY, AUTHENTICATION INTENT, AND RISK FOR HEALTHCARE PROFESSIONALS.

Requirement	AAL2	AAL3
Touchless authenticators types	- Biometric AND (RFID OR Bluetooth OR Secret) - Secret AND (RFID OR Bluetooth)	- 2 Biometrics AND (RFID OR Bluetooth OR Secret) - Biometric AND Secret AND (RFID OR Bluetooth) - Biometric AND Bluetooth AND RFID
Reauthentication frequency	6 hours or 15 minutes inactivity	4 hours or 5 minutes inactivity
Authentication intent	Recommended	Required
Fraud Risk	Low	Minimal

the reader, eliminating the need for physical contact. The tag may be affixed to a badge, necklace, or bracelet, or it may be sewn onto the healthcare professional's clothing. Bluetooth is commonly integrated into smartphones, smartwatches, and other personal devices. When coupled with security elements found in mobile devices, it can be used in challenge-response protocols with a high degree of certainty.

The category *what you are* directly correlates to biometrics. Alternatives such as retinal, iris, voice, and manual gestures must be utilized when face masks are worn by health care professionals. Importantly, authenticators based on *what you are* and *what you have* can be used unintentionally if they are in the same environment as the reader. Consequently, biometric authenticators should, whenever possible, check for liveliness and intent during authentication and reauthentication.

Other types of information, such as location data, may be used to determine the likelihood of a fraudulent authentication but are not considered authentication factors. We recommend that such information be indicative and not restrictive when it comes to authentication. We suggest notifying the healthcare professional, for instance, that authentication was performed successfully on physically distant machines within a short time interval. Nonetheless, authentication cannot be a barrier to accessing patient data, for example, given that emergency situations frequently involve life-threatening situations.

Lastly, suppose the touchless credential defined for authentication in the computer system is unavailable, for instance, in the presence of an extensive bandage or deformity resulting from a postoperative state. In that case, it is critical that another form of secure authentication, even if with touch, be guaranteed as an option.

C. Reauthentication

Work in health care facilities is dynamic, with several professionals moving in the same environment, including professionals from other fields such as cleaning and maintenance, as well as work shifts where professionals change but patients and therapeutic approaches remain consistent. Reauthentication of health professionals is required in this context. Our reauthentication proposals take into account various situations in the work routines of different healthcare professionals, such as outpatient consultation, patient evolution in the hospital, care in an emergency care unit, and telemedicine.

The minimum level of authentication in any computerized healthcare system is AAL2, *i.e.*, LoA substantial. We recommend reauthentication every 6 hours because that is the maximum period of continuous work indicated before a brief rest of the professional on duty, and every 15 minutes of inactivity because that is the estimated time for a physical examination in a different location. Reauthentication must use all authentication factors.

For AAL3, *i.e.*, LoA high, reauthentication must occur every four hours of activity or five minutes of inactivity. At this level of assurance, authenticator combinations for authentication and reauthentication must include at least three authenticators from two different types of authentication factors, one of which must be biometrics. For reauthentication, biometrics must be accompanied by signs of liveliness and intent.

Face biometrics, for example, can facilitate easier reauthentication in the presentation of liveliness and intentionality while retaining the prerogative of no-touch. Questions such as "Do you want to keep authenticated on this system?" with the option of responding with a head movement demonstrate a simple solution for reauthentication.

Table II summarizes our proposal for the authentication of healthcare professionals, including examples of touchless authenticators, the frequency of reauthentication, and the corresponding risk level for each level of assurance. *Nota bene*: Combinations of RFID and Bluetooth in AAL2 must be analyzed according to the requirements of each case, as it is not possible to conduct proof of intent and liveliness.

D. Cryptographic Protocols

According to NIST recommendations on digital identity and authentication, authentication with AAL2 and AAL3 demonstrates that the user has control over their authenticators [6]. Authentication must be performed using secure authentication protocols and approved cryptographic methods.

In our proposal for authentication without touch, we indicate Bluetooth because it is a wireless transport protocol with provision for the use of encryption of data [15]. However, RFID, which is also a transport protocol, does not offer encryption [14]. Thus, the use of RFID must be enhanced with cryptographic mechanisms. The other authentication factors must also meet this cryptographic requirement.

IV. EMPIRICAL EXPERIMENTATION

A. Prototype Implementation

We implemented a healthcare professional electronic identity prototype that supports touchless authentication. RedHat's

TABLE III
SUMMARY OF PROPOSED CHANGES FOR PHYSICIAN AUTHENTICATION IN THE SANTA CATARINA REGIONAL MEDICAL COUNCIL SYSTEM.

Characteristic	Current	Proposal
LoA	Low	Substantial
Touch	Touch	Touchless
Fraud risk	Hight	Low
Reauthentication	Inadequate frequency	Appropriate frequency

Keycloak identity provider [16], a free and open-source system, was used to create the prototype.

As described in Section III-B, the minimum level of assurance required for the authentication of healthcare professionals is LoA substantial. We modified Keycloak in this manner to support two distinct touchless authentication factors, namely facial biometrics and the presence of a Bluetooth device. An administrator adds users into our Keycloak installation, which supports both user login and password authentication and the aforementioned touchless authentication.

B. Experimental Evaluation

To evaluate our identity provider that supports authentication methods with the level of assurance that we propose, we adapted a medical service provider, namely the Santa Catarina Regional Medical Council in Brazil [17][1], to support our identity provider. Registered doctors can issue medical certificates of incapacity for work, request exams, prescribe most medications, and make medical reports, with only the user's email and password required for authentication.

Fig. 1a depicts the authentication interface of the original system, which requests users' email and password. Fig. 1b shows the system integrated with our identity provider that enables proper healthcare professional authentication: authentication occurs securely and without touch, simply by placing the user in front of the computer. The authenticators employed were facial recognition and the presence of a known Bluetooth device belonging to the user, in this case a smartwatch. Lastly, Fig. 1c displays the identity provider's error message if the user is not wearing her smartwatch.

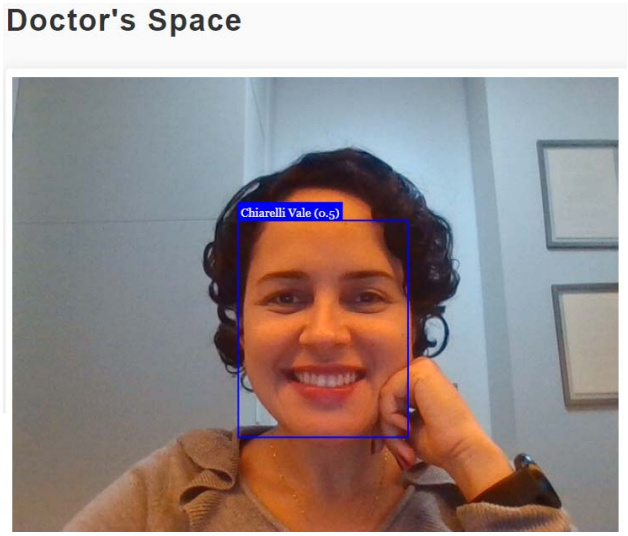
Unlike the current solution, which uses AAL1 (or LoA low) by requiring only one factor, our approach employs our multi-factor touchless authentication proposal. As a result, the risk of authentication fraud in our identity provider is reduced. Table III summarizes the differences between the form of authentication currently used and in the prototype developed.

V. RELATED WORK

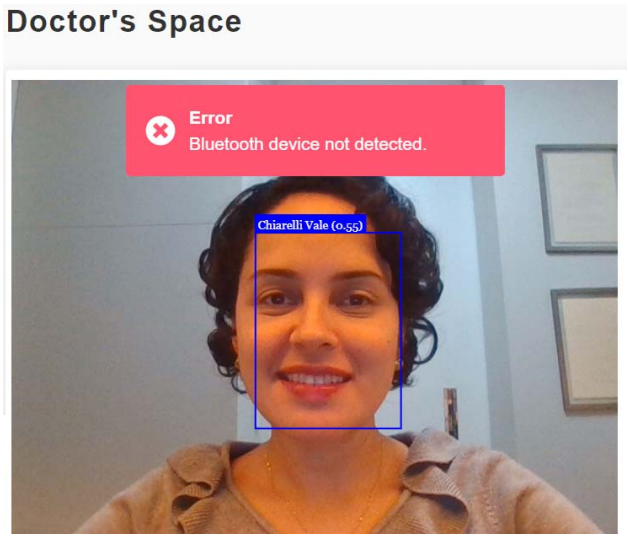
The authors of [18] proposed an online authentication and authorization scheme for e-health systems based on electronic health insurance cards and the patient's and physician's fingerprints. As discussed in this paper, biometric authentication through touch poses health risks to healthcare professionals.

[1]The interface is originally in Portuguese and was translated to English by the authors.

(a) Identification and authentication via email and password at the Santa Catarina Regional Medical Council.



(b) Using the modified Keycloak identity provider. Face recognition and presence of Bluetooth device are used for identification and authentication.



(c) An authentication error in the modified Keycloak identity provider: missing second authentication factor.

Fig. 1. Empirical evaluation of touchless authentication with AAL2.

Fang *et al.* [19] proposed an authentication scheme using physiological and behavioral characteristics through hand gestures, touch speed and pressure. The authentication mechanism requests a specific gesture, requiring the user to close four fingers and perform a certain swipe operation. Biometric factors include distance from finger touch points, while behavioral features such as speed and pressure also contain user-specific information. Thus, safety items such as liveliness and intentionality are well covered. However, health professionals touch potentially contaminated surfaces.

Guillen *et al.* [20] introduced real-time face biometric authentication for physicians and patients. Facial authentication has the advantage of being a more user-friendly method that does not require specialized data acquisition equipment. The researchers created a database of collected photos in order to train the facial authentication algorithm with different rotations, distances, expressions, and accessories. They thought about wearing glasses, hats, and scarves. In addition, images with four different facial expressions were captured. Participants were asked to show three different types of expressions in addition to neutral: smiling, screaming, and closing their eyes and opening their mouths. When contacting health services, they believed that friendly users could smile. If the patient is in a lot of pain, the second type of expression may occur. The final expression was created to take into account emergency demands during the night, when they may be tired.

There are research employing iris [21], voice [22] and facial expressions [20] to demonstrate touchless biometric authentication techniques. Although related works mention the combination of two authentication factors, none consider the broader context of e-health authentication and derive general recommendations for the area.

VI. Final Remarks

Systems with authentication based on an adequate level of assurance make it difficult for fraud to occur in the authentication of health professionals, thereby preventing negative consequences ranging from medical confidentiality breaches to risks to the patient's physical integrity. Depending on the setting and the role of the healthcare professional, the damage may be even more significant and irreversible. In healthcare, authentication with an adequate level of assurance is essential.

Using the NIST guidelines for digital authentication as a point of reference, analyzing risk and impact categories, and based on the assessment of harm and potential impacts, we determined that AAL2 (or LoA substantial) is the bare minimum to be used by health professionals.

References

[1] E. Bertino and K. Takahashi, *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

[2] T. El Maliki and J.-M. Seigneur, "A survey of user-centric identity management technologies," in *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, IEEE, Valencia, Spain: IEEE Computer Society, 2007, pp. 12–17. DOI: 10.1109/SECUREWARE.2007.4385303.

[3] F. Schardong and R. Custódio, "Self-sovereign identity: A systematic review, mapping and taxonomy," 2021. DOI: 10.48550/arXiv.2108.08338.

[4] M. d. V. Barros, F. Schardong, and R. F. Custódio, "Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass," 2022. DOI: 10.48550/arXiv.2202.09207.

[5] ISO Central Secretary, "IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts," ISOnternational Organization for Standardization, Geneva, CH, Standard, Mar. 2019, Accessed on 13 May 2022. [Online]. Available: https://www.iso.org/standard/77582.html.

[6] P. A. Grassi *et al.*, "Digital identity guidelines: Authentication and lifecycle management," Tech. Rep., 2020, p. 79. DOI: 10.6028/NIST.SP.800-63b.

[7] T. Miyata *et al.*, "A survey on identity management protocols and standards," *IEICE TRANSACTIONS on Information and Systems*, vol. 89, no. 1, pp. 112–123, 2006. DOI: 10.1093/ietisy/e89-d.1.112.

[8] V. Conti, C. Militello, and S. Vitabile, "Biometric authentication overview: A fingerprint recognition sensor description," *Int J Biosen Bioelectron*, vol. 2, no. 1, pp. 26–31, 2017.

[9] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[10] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in telecare medicine information systems," *Journal of Network and Computer Applications*, vol. 87, pp. 1–19, 2017, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2017.03.003.

[11] World Bank, *Practitioner's guide: Levels of assurance (loas)*, Accessed on 20/04/2021, Washington, DC, USA, 2019. [Online]. Available: https://id4d.worldbank.org/guide/levels-assurance-loas.

[12] European Parliament, Council of the European Union, *Regulation (eu) 910/2014*, accessed on 13 May 2022, European Parliament, Jul. 23, 2014. [Online]. Available: http://data.europa.eu/eli/reg/2014/910.

[13] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines," Tech. Rep., 2020, p. 75. DOI: https://doi.org/10.6028/NIST.SP.800-63-3.

[14] F. Thornton and C. Lanthem, *RFID security*. Elsevier, 2006, ISBN: 9780080489650.

[15] T. Panse and V. Kapoor, "A review on security mechanism of bluetooth communication," *International Journal of Computer Science and Information Technologies*, vol. 3, no. 2, pp. 3419–3422, 2012.

[16] Red Hat, *Keycloak*, Accessed on 13 May 2022, Raleigh, NC, USA, 2014. [Online]. Available: https://www.keycloak.org/.

[17] CRM SC, *Espaço do médico*, Accessed on 13 May 2022, 2022. [Online]. Available: https://api.crmsc.org.br/crvirtual-espacomedico/#/login.

[18] C.-L. Chen, M.-S. Lu, and Z.-M. Guo, "A non-repudiated and traceable authorization system based on electronic health insurance cards," *Journal of medical systems*, vol. 36, no. 4, pp. 2359–2370, 2012.

[19] L. Fang, C. Yin, L. Zhou, Y. Li, C. Su, and J. Xia, "A physiological and behavioral feature authentication scheme for medical cloud based on fuzzy-rough core vector machine," *Information Sciences*, vol. 507, pp. 143–160, 2020, ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2019.08.020.

[20] F. D. Guillén-GáMez, I. García-Magariño, J. Bravo-Agapito, R. Lacuesta, and J. Lloret, "A proposal to improve the authentication process in m-health environments," *IEEE Access*, vol. 5, pp. 22 530–22 544, 2017. DOI: 10.1109/ACCESS.2017.2752176.

[21] D. Mahto and D. K. Yadav, "Cloud-based secure telemedicine information system using crypto-biometric techniques.," *EAI Endorsed Trans. Pervasive Health Technol.*, vol. 5, no. 20, 2020.

[22] S. Krawczyk and A. K. Jain, "Securing electronic medical records using biometric authentication," in *International Conference on Audio- and Video-Based Biometric Person Authentication*, Berlin: Springer, 2005, pp. 1110–1119. DOI: https://doi.org/10.1007/11527923_115.