UDC: 004.77.056.523
Professional paper

VERIFICATION OF ELECTRONIC IDENTITY IN FEDERATED SYSTEMS USING MULTI-FACTOR AUTHENTICATION

Vjollca SHEMSHI[1], Florim IDRIZI[1], Hirijete IDRIZI[1], Nexhibe SEJFULI RAMADANI[1]

[1]*Faculty of Natural Sciences and Mathematics, University of Tetova, Ilinden n.n., 1200 Tetovo, Republic of North Macedonia*
**Corresponding author e-mail: vjollca.ismaili@unite.edu.mk*

Abstract

Electronic authentication (e-authentication) is a process to provide electronic identity trust to users who register electronically in an information system. Verifying the identity of students and the veracity of their work is very important for academic institutions because only in this way can academic misconduct be reduced and on the other hand ensure the quality of education.

In recent years there has been increasing research into technological innovations that combat fraud and copying. Currently, password-based credentials are one of the most widely used authentication mechanisms, despite their weaknesses.

Today digitalization is pervasive in all parts of modern society. One of the main ways to keep this process safe is the verification process. This process begins with the evolution of authentication systems ranging from One Factor Authentication (SFA), and Two-Factor Authentication (2FA) to Multi-Factor Authentication (MFA).

All these systems have their advantages and disadvantages which negate the lawful use of the user. It can often happen that passwords are forgotten, the wrong placement of the code on the smart cards can be done or biometrics can become temporarily unavailable, such as loss of fingerprint quality. Moreover, biometrics is not safe if used as a single authentication factor as it can be copied (an attacker can take a copy of a fingerprint and build a copy).

The purpose of the document is to analyze the level of electronic identity security and electronic identity verification for users who wish to have certain resources using many authentication factors as well as the credentials given to users after successful verification of their identity by a party providing the credentials service.

Keywords: electronic identity, security of electronic identity, two factor of authentication, multi factors of authentication

1 Introduction

Determining identity indicates whether a subject is who they claim to be. Electronic identity verification determines that an entity attempts to access an electronic service that has under its control one or more valid credentials which relate to that entity's electronic identity [1].

Usually, the identity of an individual is verified using one or more factors, as the most common factor used is a personal identification number or PIN, then we have a password, we also have other factors that we know or possess only from an authorized user [6].

Authentication with an authentication factor (SFA) requires a user to verify his/her identity using only one authentication factor, such as: a PIN, an answer to a security question, or a fingerprint.

Authentication with two or more authentication factors in addition to the basic factors requires more methods to verify the identity of an individual. So, in addition to the PIN code that a user must possess, he must also provide an identification card (ID card) or use biometric techniques that will verify the identification of the user such as: facial features, iris pattern, fingerprints, etc. [6].

Verification mechanisms are categorized as follows: [2]

1. Something we know (for example, a password or a PIN).
2. Something we have (for example, a cell phone or a sign).

3. Something we are (for example, a fingerprint or other biometric data).

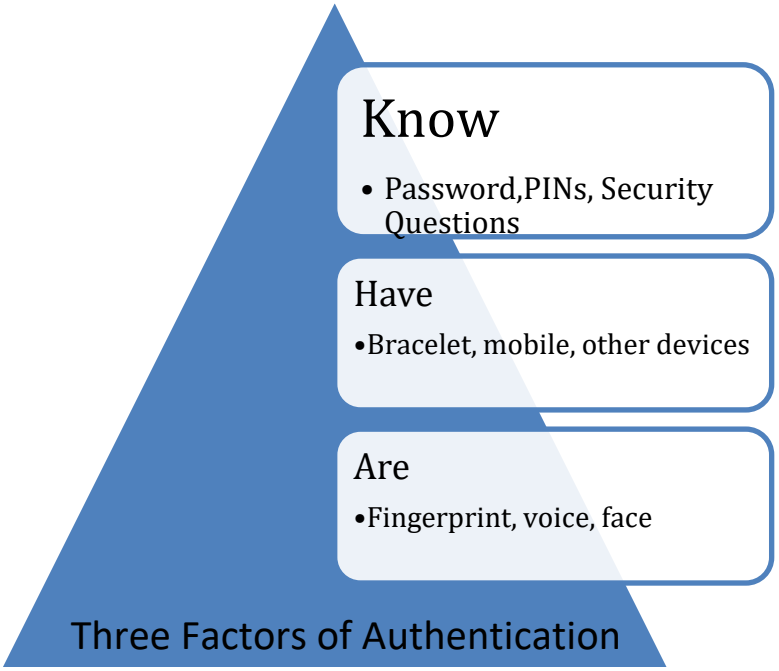

Figure 17: Three factors of Authentication

In addition to using three-factor authentication, a high level of security also can be achieved by using some authentication factors that are more difficult to find or falsify, and by implementing stricter mechanisms to protect their secrecy. Stricter mechanisms (e.g., more complex passwords) and better protection against malicious actions (e.g., password encryption with a strong algorithm) provide a higher level of trust in user authentication [6].

Multi-factor authentication (MFA) is a method that requires user authentication to be done by providing two or more authentication factors to gain access to such a resource, MFA is a fundamental component of user access management and a strong identity policy (MFA). In addition to the basic authentication requirements such as just a username and password, the MFA requires more additional factors to verify the data which reduces the likelihood of a potential cyber-attack.

2 Fundamentals and Related Work

Electronic authentication usually consists of three main stages. The first phase is the registration of users, and in the second phase, we have the verification of the identity of the user and the issuance or destruction of credentials.

For example, if a user wants to access certain services specified by the Service Provider the user must first register with the Registration Authority, which may be the SP itself or maybe a third group providing credential services for Service Provider.

Based on the service that the SP provides, RA may need to verify that the identity is a true one and that the user is the person entitled to use that identity (i.e., verify the user's identity proof). Once the user is successfully registered, a credential can be issued to him. The credential can be something the user knows (e.g., a PIN or password), or something the user has (e.g., an intelligent card).

The user must prove his identity to the verifier, demonstrating that he possesses a valid credential. When the credential reaches the expiration time, it must be renewed so that the user has further access to the SP, otherwise it is destroyed [5].

3 The purpose of the research

The three main types, we will consider, to perform electronic user identification using the two authentication factors are:

- **One-Time Password (OTP) Deployment:** Randomly generated, uniquely and specifically for each user entry [3]. OTP authentication offers many advantages over static passwords. Unlike static passwords or traditional passwords, where a user has it very easy, it is enough to enter the password only once and I will use it whenever I want to access his account.
  While a user gains access to his account using an OTP, he can only log in once and then the code becomes invalid, which cannot be reset by attackers. OTPs are usually generated by algorithms that use randomness. This makes it harder for attackers to think about how to use them. OTPs may only be valid for short periods, require the user to have knowledge of a previous OTP, or provide the user with a challenge (e.g., "please enter the third and sixth numbers"). All those measures reduce attacks in an environment where password-only authentication is considered. In the following figure, we have presented the path that the person who wants to identify in a federated system must go through. Based on the idea presented in the following figure, we propose that this system offers electronic identity security for all users registered in the system.

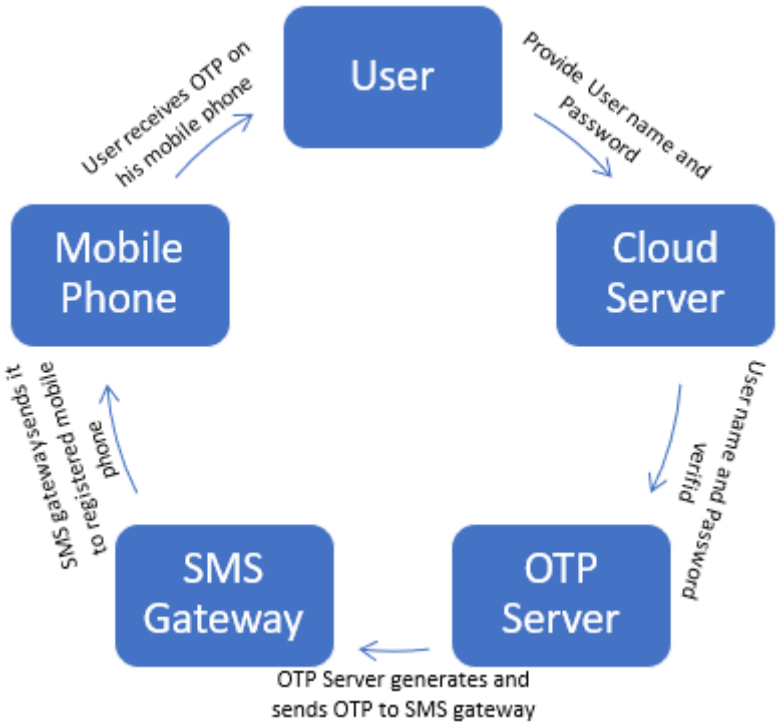

Figure 18: OTP process with two factors of authentication

- **Biometric Authentication:** Biometric Authentication offers an excellent combination of security. Biometrics is an automated method of identifying a person based on a biological characteristic [4]. Many biometric applications require the user to place their finger on a scanner to obtain

biometric traces. Biometric verification is usually very convenient and easy for users and provides very effective protection against attempts and opportunities for illegal entry [3]. If we want to use multi-factor authentication, to identify electronic identity then we must use Biometric Authentication. In a federated system to identify the electronic identity of a user, we propose that in addition to the OTP process, biometric authentication should also be considered based on the model presented below, as only in this way do we have full security of the data.

.

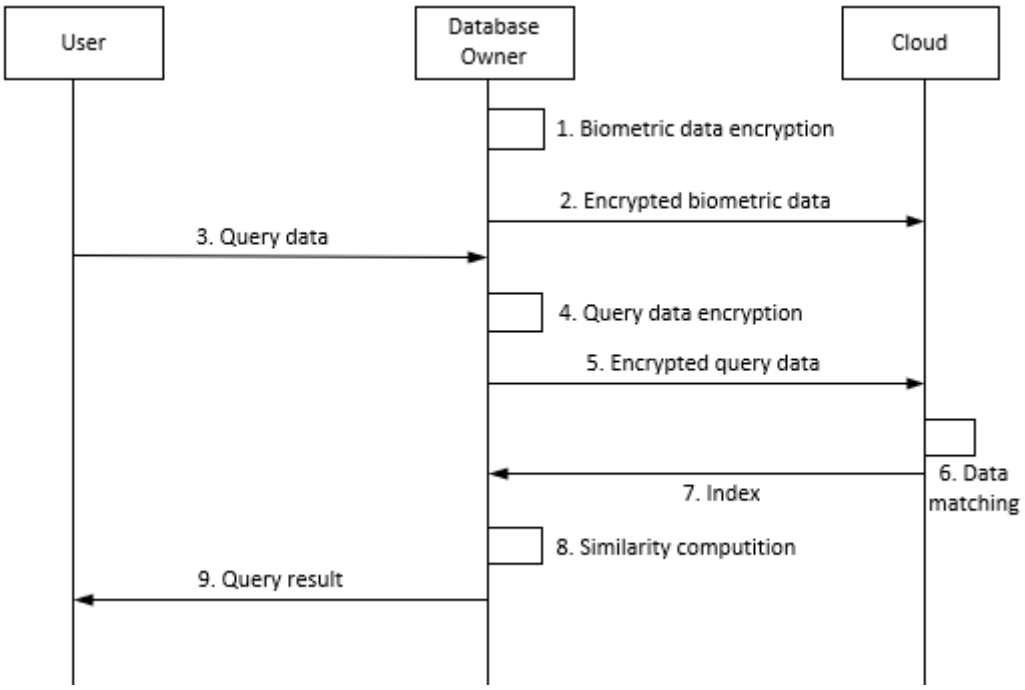

Figure 19:Biometric Authentication model

- The main goal to reach a secure solution should be to maximize the protection of the user identity while minimizing the user concern. The ability to intelligently enforce security policy enables the protective potential for a two-factor solution to be fully realized, also adapts any access mode to minimize user concerns [3,4].

Conclusion

For electronic systems, it is very important to regenerate user identities and cryptographic protection of the authentication process in the system development process. The level of trust of different credentials should also be determined using the level of Assurance (LoA) which verifies that access to resources is given only to users whose identities have been verified [7]. This reflects the level of trust in a process that uses authentication to determine the identity of a user who has been given credentials and the level of trust that the user uses in credentials.

It is a fact that happens in electronic systems, that users at some point may lose or forget their account passwords such as a PIN or some other verifying information. These systems need to have the ability to securely retrieve verification information by utilizing credentials without adversely affecting the integrity of the verification systems. Electronic identity management is a very important security issue to having access to various electronic services, as organizations must securely exchange personal information while maintaining the integrity and confidentiality of user data. However, work still needs to be done with

building a complex architecture that will support the identification of each type of educational unit to store the eID on their original server in a secure manner.

References

[1]. Hassan, Shahid, Nordin Simbak, and H. Yussof. "Structured Vetting Procedure Of Examination Questions In Medical Education In Faculty Of Medicine At Universiti Sultan Zainal Abidin Malaysia." *J. Public Health Med* 16 (2016): 29-37.

[2]. Dasgupta, Dipankar, Arunava Roy, and Abhijit Nag. "Multi-factor authentication." *Advances in User Authentication*. Springer, Cham, 2017. 185-233.

[3]. Liu, Wenzheng, Xiaofeng Wang, and Wei Peng. "Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things." *IEEE Access* 8 (2019): 8754-8767.

[4]. Kalunga, Joseph, and Simon Tembo. "Development of fingerprint biometrics verification and vetting management system." *Am. J. Bioinforma. Res* 6.3 (2016): 99-112.

[5]. Yao, Li. *A structured approach to electronic authentication assurance level derivation*. The University of Manchester (United Kingdom), 2010.

[6]. Blue, Juanita, Eoghan Furey, and Joan Condell. "A novel approach for secure identity authentication in legacy database systems." *2017 28th Irish Signals and Systems Conference (ISSC)*. IEEE, 2017.

[7]. John Elliott, Margaret Ford, Dave Birch – Consult Hyperion "Menaging multiple electronic identity" - ENISA staff involved in the project: Demosthenes Ikonomou, Rodica Tirte / European Network and Information Security Agency Technical Competence Department