Which authentication method to choose. A legal perspective on user-device authentication in IoT ecosystems

ABSTRACT: The IoT has raised a set of challenges due to the enormous amount of data processed and the complex implementation of mechanisms to guarantee these data are exclusively accessed by authorized users. In these ecosystems some devices represent a first "access door" to data obtained from other devices or stored in the Cloud, therefore there is a particular need to implement strong authentication mechanisms that limit unauthorized accesses to thereof. The aim of this paper is to offer a legal perspective on the forces tensioning in the most common authentication methods implemented in this type of devices, account taken of the particularities of an IoT ecosystem. Due to the topic object of discussion, it is necessary to lay the technological ground in order to perform a subsequent legal analysis. The conclusions attempt to answer the question of which authentication method could be the best choice as well as offering some lines for further research and development in the area.

Keywords: Digital Identity, IoT, Authentication, GDPR, Security.

1 INTRODUCTION

We are living in a world where millions of "objects can sense, communicate and share information, all interconnected over public or private Internet Protocol networks. These interconnected objects have data regularly collected, analyzed and used to initiate action, providing wealth of intelligence for planning, management and decision-making" [[1]] (p.6123). We are referring to the world of the Internet of Things (hereafter, IoT). There is not a precise definition of the IoT. Authors such as Dr. Gilad L. Rosner and Erin Kenneally, J.D state that it can refer to a variety of objects which acquire a variable degree of networked intelligence and have "the ability to sense, amass and analyze data and communicate through networks" [[2]] (pp.13-14). Most of the objects that integrate the IoT are familiar objects (e.g., vehicles, smartphones, home appliances, toys, cameras, medical instruments…) improved with the ability to store, process and share information, "thus becoming new actors in the informational word" [[2]] (p.14) and designing spaces where real, digital and the virtual merge to create smart environment [[3]] (p.8).

Beyond its beneficial effects, the IoT is also raising a set of challenges. More specifically, interconnected devices cross and disrupt boundaries of different nature (physical, datatype or regulatory boundaries) [[2]] (p.19) due to the fact that most of the objects above-mentioned are being invited to our houses or "private environments". Consequently, notions such as "home" [[2]] and its privacy implications (e.g., Article 7 of the Charter of Fundamental Rights of the European Union) [[4]] (p.10) are being challenged. In other words, this invitation to our "private environment" allows the access to certain data or private information and, in the worst cases, could even affect the ability of the user to perceive and control who is observing or disturbing in his/her private territory [[5]]. Furthermore, the possibilities of some of these devices go beyond physical boundaries and get access to the body and emotional life. Indeed, the commercial market is offering a wide range of devices to monitor people's activities, environments, and even physical bodies and emotions [[5]].

With these references we wanted to express the potential possibilities of privacy intromissions and the magnitude of the data processing in an IoT ecosystem. In exchange, mechanisms to control intromissions and privacy violations are needed. One of the possibilities to avoid disproportionate intromissions and therefore, privacy violations, consists in reinforcing user control and management strategies. These can refer to measures of diverse types such as data pre-collection or post-collection strategies or privacy by design. However, the innovative approach of this paper is to provide an in-depth study on the role of identity management (hereafter, IdM) in the IoT as a mechanism to limit unauthorized access to the device. The study of this aspect is becoming of acute emergency considering that some devices within an IoT ecosystem represent in many cases a first "access door" to a large number of private data due to the interconnection of multiple devices and therefore multiple data sources, relying on a single authentication process or authentication means.

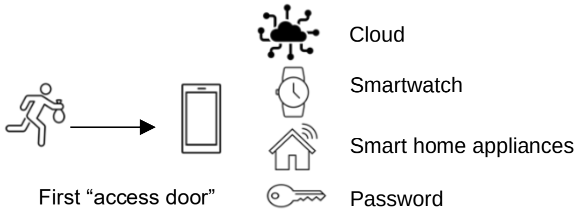

Fig. 1. Example of the smartphone as a first "access door" to private information in an IoT ecosystem

More specifically, potential negative effects and consequences of the IoT are coherently increasing with the fast development and spread thereof. In other words, nowadays the IoT is posing scenarios where all private information (or the means of access to private information) concerning an individual is regrouped into a set of devices interconnected between themselves. In return, a privacy breach might have catastrophic impact for end users. Consequently, in the current stage of the IoT (and its foreseeable evolution) we will need more safe mechanisms assuring that only authorized users can access the device, that is to say, strong authentication methods. However, these methods usually require the use of biometrics or other personal data that confirm identity of the user accessing the device, which at the same time raises other issues. The aim of this paper is to study from a legal perspective the tensions between the need of safe and convenient authentication methods in the IoT. For that purpose, we propose the study of a set of concepts as well as a comparative view between authentication methods.

2 DIGITAL IDENTITY

2.1 Concept and types

The point of departure in the study of identity is the concept of entity. An identity describes an entity within a specific scope, therefore it can be defined as "a set of all characteristics that have been attributed to an entity within a scope" [[7]] (p.5). The International Telecommunication Union also defines the concept of identity as a "representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context" [[8]] (p.4). Building on this definition, we can state that a digital identity is the digital representation of an entity detailed enough to make the individual distinguishable within a digital context [[8]]. Coherently with this definition, a reference to the concept of entity must be made. "An entity is a real-world thing" [[9]] (p.4), which includes, and at the same time distinguishes between natural or legal persons and objects. All of these can be considered entities, and therefore have an identity. However, the content thereof will vary depending on the entity to which it is applied.

This paper focuses on the identity of natural persons in user-sensor authentication. Referring the concept of digital identity to a natural person, it can be defined as "the unique representation of an individual in an online transaction" [[10]] (p.4). The concept of digital identity referred to natural persons must be designed and constrained by the particularities raised by the fact that it refers to human beings. In this sense, it must take into account that some data should not be used as they can be a source of discrimination as well as some of them are particularly sensitive (e.g., biometrics, unique identifiers…) [[11]].

To function, these identities must exist within a technical framework, that is to say, they must be managed. Following the definition given by Dr. Gilad L. Rosner [[12]] (p.98), "Identity management is an operational and technical framework that defines and administers the lifecycle, use and security of digital identities. Authentication and the management of credentials are key focuses of IdM systems. They are transactional and operated by organizations". In other words, identity management is concerned with the lifecycle of digital identities.

2.2 Identities lifecycle and "strong identities"

Identity lifecycle covers from the creation to the deletion of the digital identity (or the deregistration of the user) [[13]] [[11]]. The cycle starts with the identity proofing and enrollment of the user and concludes with the verification. However, concerning the scope of the paper, access to devices, this verification does not really take place in the majority of cases (e.g., a scenario of corporative use of devices could be different) since the key issue is to assure the person accessing the device in a later moment is the same who has set the authentication method.

Once the digital identity has been created and validated (i.e., the user has been identified), this phase finishes with the enrollment of the user and the issuance of an authenticator such as a password, token, PIN or biometric recognition. Consequently, the user is now able to perform his authentication. Authentication consists in the recognition of an identity previously issued and at the same time it can rely on different types of authentication factors and processes. These factors and processes are of interest for the purpose of this paper.

The authentication factors can be separated in three basic categories: a) Knowledge factors or "something you know" (e.g., PIN, passwords, answer questions); b) Ownership factors or "something you have" (e.g., one-time passwords, Personal Identity Verification card); c) Inherence factors- "something you are"- e.g., fingerprint, face, voice. Another category of factor could refer to location data, "somewhere you are" via IP address or behavior data, "something you do" as it was the case of Windows 8 picture password feature, although behavioral data may be considered as an inherence factor also.

On the other hand, authentication processes can be classified into two basic categories: a) Single-factor authentication - uses only one authenticator; b) Multifactor authentication -uses two or more independent authenticators from at least two different authentication factor categories.

Finally, the authorization refers to the last stage (excluding deletion or deregistration of the user). Once the individual has been verified as previously identified user, now, we process to the verification of corresponding rights and fulfillment of requests.

Depending on how phases are performed, and the parties involved, we would be in presence of different types of identities or identity management systems. The study of the types of identity management is out of the scope of this paper. With regard to the types of identities, we make appeal to the concept of strong identities understood as those identities that reach a high level of assurance during the whole identity lifecycle, that is to say, it exists a strong ID proofing during the process of binding identities, as well as in a later stage, and it operates by means of strong and safe mechanisms for identity management.

In order to illustrate this term that we propose along the paper, it is of interest to take into account the following European Union regulations, the eIDAS Regulation and the PSD2 Directive, as they state relevant legal requirements for the understanding and the definition of the concept of strong identities. These regulations have in common that both aim to achieve a substantial or even high level of assurance in authentication so that the natural person is who he claims to be, thus he/she has the right to perform the corresponding operation. The basis for these “strong identities” are the goods protected, i.e., in the scope of the eIDAS Regulation, the access to cross-border public services by citizens, and, in the scope of the PSD2 Directive, the protection of natural person’s economic goods and the well-functioning of the market. In other words, we can extract from these regulations that the legal requirements in the authentication processes vary regarding the good protected.

When a user is accessing an interconnected device such as the case of smartphones, he/she will probably gain access to not only the device but also to other accessible sources in the Cloud, uploaded content from synchronized devices or even the password manager, usually protected with the same access code of the device. As an example, for the nature of the data processed it is interesting the latest incorporation of smartwatches, aiming to offer health information to the individual as if it were a medical device and sharing this data with other devices (i.e., the smartphone). However, health data are considered as sensitive data by the General Data Protection Regulation (hereafter, the GDPR) [[14]], thus the means to access this data should assure the person accessing them is the authorized natural person, that is, a strong authentication process should be used. The issue is that the authentication process when accessing this sensitive data relies on the authentication process implemented by the device, normally a smartphone, where the synchronized content can be visualized by the user. Therefore, some devices, such as the case of the smartphone in an IoT ecosystem, represent an “access door” to other data, and the protection of these devices poses a challenge since they require an appropriate level of assurance, while at the time convenience in the access must also be maintained.

The cited regulations establish the following legal requirements in order to assure security in the authentication process, or as we have noted before, that the user performing the operation is who he/she claims to be. In the eIDAS Regulation security levels are detailed in the Annex of the Commission Implementing Regulation (EU) 2015/1502 of the 8th of September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means. Pursuing this legal text, to achieve at least the substantial level of assurance (LoAs) during authentication phase a dynamic authentication method is required [[15]] (pp.8, 9), which for its definition contained in the Article 1 (3) [[15]] (p.11) refers to a multifactor authentication process.

The EU Revised Directive on Payment Services (PSD2) within the European Economic Area introduces the concept of Strong Consumer Authentication (hereafter, SCA) envisaged by the Article 4 (30) of this text [[16]] (p.59), which has been developed in the Commission Delegated Regulation (EU) 2018/389 of 27 November 2017. The SCA requirement ensures that electronic payments are performed with multi-factor authentication to increase their security. The factors are independent in that the breach of one does not compromise the reliability of the others.

From these regulations we can conclude that multifactor authentication is generally required in environments where identity attributes need to be trustworthy shared between different parties, under the control of the natural person. This requirement can make sense in the scope of application of the cited legal instruments; however, its implementation would be more complex in IoT scenarios. On the one hand, because it would lack of convenience. On the other hand, because in many cases the interconnected device is itself, as it is the case of the smartphone, the support of the multifactor authentication process (e.g., the code we receive in the smartphone).

3 STRONG AUTHENTICATORS

At this point we have discussed that the devices operating in an IoT ecosystem require strong authentication mechanisms, especially concerning those interconnected devices that represent an “access door” to other devices or sources of data. Nevertheless, in such scenario a multifactor authentication process could raise problems in terms of convenience due to the fact, among other considerations regarding the concrete case, that these are usually devices that we access many times per day.

This section contains some reflections about the main advantages and drawbacks in the implementation of biometrics as authenticator, as well as the explanation of an innovative authentication method, the Expanded Password System (hereafter, the EPS). For the development of this section, we will refer to the reflections pointed out by the professional in the area Hitoshi Kokumai collected from a set of articles, posts and discussions.

In order to add security, it seems logical to recall the categories of authentication factors. Among these factors, we can claim that “inherence factors” offer a higher level of assurance since impersonation of the user is more complex. The most traditional “inherence” factor is biometrics; however, some reflections must be made account taken of the particularities of the scenario studied in the paper.

3.1 Biometrics, a double-edged sword

Biometric authentication refers to the automatic identification or identity verification of living individuals using physiological and behavioral characteristics [[17]]. Biometric identification is developed through different techniques, among which we can cite the most commonly used, fingerprints or face recognition (specially concerning everyday interconnected objects), but also others such as the recognition of the iris, the hand geometry or the retina [[18]]. The study of biometric identification technologies is out of the scope of this paper, but we consider pertinent to highlight some of its common features. Firstly, biometric authentication requires the use of characteristics that uniquely represent an individual. This introduces an important advantage in terms of security, as it hampers impersonation of the user but, at the same time it poses an important risk. Once biometric data are compromised, they will be compromised forever. This aspect of biometrics makes evident the need of stronger security measures when this type of authentication method is chosen, which at the same time requires robust security systems or designs. In other words, economic investment.

From a legal point of view the processing of biometric data of natural persons is included in the category of sensitive data. Therefore, since the data processing implies a high risk, pursuing Recital 84 of the GDPR [[14]] the obligation to conduct a Data Protection Impact Assessment (hereafter, DPIA) will apply. In the DPIA the proportionality of this authentication choice should be studied, as well as the specific technical measures adopted. It should be noted, however, that we are discussing the use of biometric data for authentication purposes (before the device), and not for their comparison and identification by third parties. This aspect has been recently analyzed with regard to facial recognition for identity verification and control in online exams [[19]], due to the Report 0036/2020 of the Spanish Data Protection Agency that, based on the interpretation of the GDPR and the White Paper on Artificial Intelligence of the European Commission, concluded that this case should not be considered as the processing of sensitive data. In fact, in authentication before devices it could be discussed whether the data processing exists. Nevertheless, although this interpretation can exempt from specific legal obligations, particularly concerning the legal basis of the processing, it does not change the nature of the data processed and the risks attached in case of resulting compromised.

With these reasonings, we do not intend to disqualify biometrics, but to make aware of their implications. If properly implemented, biometrics probably support the most accurate identification means in terms of assuring the user is who he/she claims to be, and it results logical for a scenario where a multifactor authentication cannot be envisaged. However, the “probabilistic” nature of biometrics makes necessary a fallback measure to cover cases of false rejection [[20]]. Indeed, contrary to the case of “deterministic” authenticators (e.g., text password, PIN or token), the user must be provided with a fallback measure to avoid situations of permanent denied access. The most common fallback measure for biometrics is the text password or the PIN, hence the user will be required to provide one of these in case of being denied access.

It must be noted that the fallback measure will apply in case of false rejection, as well as in the case of an unauthorized user. The consequence is that due to the “probabilistic” nature of biometrics and therefore their necessary implementation with a fallback measure, the real security of biometrics is reduced to the fallback measure. Exceptionally, the fallback measure could be a human manager who takes care of these false rejections. Nevertheless, this possibility would be just foreseeable for reduced scopes (e.g., to identify the employees in a company), and definitely it would not make sense to access devices that we usually have at home.

Despite the controvert conclusions about whether personal data are or not process, since we are talking about data that are in principle stored in the device, it is still of interest the principle of data minimization contained in Article 5 of the GDPR. Pursuing this principle, the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This implies considering risks and benefits attached to the data processing or, in other words, an evaluation of the proportionality [[21]]. From the proportionality perspective, it is necessary to evaluate if the aim pursued can be achieved by other means which imply a lower risk. In this sense, there might exist tensions between the agility, the security or the privacy (i.e., biometrics in authentication can be more agile, but for the nature of these data it can imply a higher privacy risk). The Spanish Data Protection Agency provided some guidelines in order to evaluate the proportionality requirements [[22]] and in the case of biometric authentication to the scenario discussed it will not fulfill the suitability and the necessity criteria (at least from a privacy perspective, that is to said, omitting convenience aspects), as the same or even higher security (since we would not consider possibilities of false acceptance) [[23]] is achieved with just a PIN or a text password.

The conclusion is that biometrics are not an ideal factor to be deployed in "multi-layer" method [[24]] in IoT scenarios, and their current implementation in "multi-entrance" method lowers the security as the possibilities of unauthorized access increase [[23]]. Nevertheless, we are aware of the advantages in terms of convenience of biometrics (e.g., fingerprints or facial recognition) as it enhances user experience, something, that is particularly relevant when we are talking about devices that we access many times per day.

However, after the reflections expressed concerning the real implementation of biometric authenticators, it might be suggested to consider different possibilities (i.e., implement stronger fallback measures) or even to come back to prior methods (e.g., the PIN or text password). Another possibility would be to explore alternative methods. In this sense, the following method represents an alternative in authentication that aims to maintain convenience for the users at the same time it avoids the use of biometric data.

3.2 The Expanded Password System

The EPS consists in an authentication method that introduces the possibility of converting text passwords into images. The authentication process would take place by selecting a set of images that only the user is able to select correctly since these images are associated with his/her autobiographical or episode memories. The functioning of the method is the following [[25]] [[26]]. The user will be able to take or select a set of pictures from his device (e.g., a smartphone). The pictures could be a picture of his last travel, furniture, objects… (ideally something that does not make the individual easily identifiable). During the authentication, the user will be presented these images among other random images and he will have to select them correctly. The identification of the pictures will be easy insofar as they are associated to his/her personal memories. Consequently, the combination of these "personal" images will be not only easy to remember but hard to forget [**Error! Reference source not found.**]. Nevertheless, it should be noted that this combination of images will be exclusively presented to the user, since software will translate these images into text passwords, that will be the ones finally stored. This would allow the user to create extreme long text passwords without the burden of remembering them.

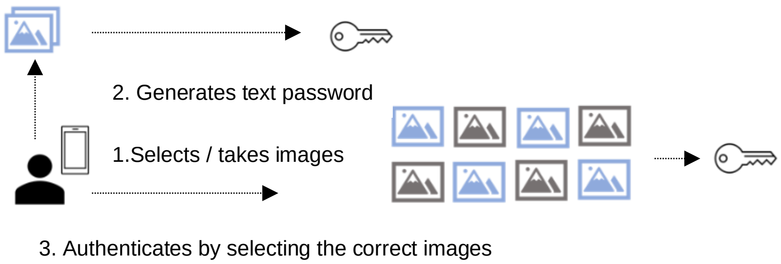
2. Generates text password
1.Selects / takes images
3. Authenticates by selecting the correct images

Fig. 2. Simplified schema of the Expanded Password System

As other authentication methods, the EPS could be implemented in different ways, hence, specific scenarios must be studied. Likewise, some considerations should be made, such as the possibilities of the user in selecting images. However, our study presumes at least an adequate selection of images (i.e., that do not make the individual directly identifiable). This approach represents an important innovation as it is a hybrid authentication factor. On the one hand, the method proposed remains in the field of knowledge factors, as long as the final output is a text password. However, conversely to the case of passwords based on pictures, this password would be intrinsically linked to the person's memories, that is to say, "something he/she is".

While not being formally considered as an inherent authentication factor, this method could replace or be implemented conjointly with biometrics for authentication in some devices as it would avoid the problem of remembering passwords or to rely on a weak PIN. Indeed, the main advantage is that the EPS will simplify the task of remembering passwords in a context where the excessive number of accounts or devices and passwords, and their corresponding correlation is becoming an unmanageable burden for the user and resulting in undesirable practices, such as the need of written down all passwords or using the same password repeated times. Likewise, the particular features of this authentication method can offer a different approach with regard to the forces tensioning. Indeed, the possibility offered by the EPS of converting text passwords into images would enhance user's convenience at the time it would offer a privacy-preserving solution since biometric data would not need to be used.

To conclude, the EPS could achieve a higher level of security reducing the scope of impersonation as the recognition of the images would be intrinsically linked to our own person and memories. Indeed, it is still possible that people in our very close or familiar environment are able to select the images correctly, but at the same time this will strongly rely on the images chosen by the user (e.g., the user could choose an image of his favorite number, letter or day of the month). Nevertheless, we must also be aware of the limitations of this method, especially in the case of diseases related to the loss or confusion of memory or personal experiences. Ultimately, a further study of this method should be considered.

4 CONCLUSIONS

The IoT is in constant evolution and development, and it is requiring technology and regulations to adapt to it. The aim of this paper was to offer a set of reflections with regard to the evolution of IdM concerning the IoT focusing on a concrete aspect, the authentication of the user before the device. The main concern raised throughout of this paper is the growing scope of the interconnected devices and their increasing functionalities. In other words, the amount and types of data processed is increasing at a breakneck speed and some devices are beginning to represent an "access door" to a large source of data, some of them considered by the GDPR as sensitive data. The clearest example of a device that represents this "access door" is the smartphone. However, we did not want to limit the reflections to this specific device as the "manager role" that the smartphone holds nowadays could be easily assumed by other devices.

From a practical point of view, we are facing a scenario where most of our private life is accessible through a single or a reduced number of devices, which raises the question of whether the access to this/these device/s is enough protected. As we have pointed out during this paper by making reference to the eIDAS Regulation and the PSD2 Directive, authentication requirements vary depending on the good protected, so, should we reinforce authentication methods for accessing smart devices? Certainly, the evolution of authentication methods implemented in interconnected devices seems to confirm that, however, some inconsistencies are also appreciated. The case of biometric authentication cited in this paper is a great example, especially considering the current global situation where most people need to wear face masks. In some devices it is enough that your face is not recognized twice to be asked your PIN or text password (e.g., easy to see by the person placed behind you in a queue). Consequently, the real security of the device is one of these methods.

This makes evident that the main improvement of biometrics for authentication, as they are implemented nowadays in a substantial number of devices, is the convenience of their use. However, does this convenience justify the use of such sensitive data? The answer is that it depends. In scenarios where strong security measures are adopted and alternative strong fallback measures are foreseeable, it might be adequate. Nevertheless, it is perfectly reasonable that devices which we are constantly using have convenient authentication methods. Consequently, the alternative proposed by the EPS might be of interest for certain scenarios (e.g., a device we use a few times per day) or as a fallback measure in biometric authentication.

In conclusion, it might be necessary to maintain biometric authentication properly implemented (i.e., where the fallback measure does not lower security) in those scenarios where a very high level of security is required, and the safeguards implemented to protect biometric data are strong enough. However, for other scenarios it might be desirable to consider alternative authentication methods that do not imply such a high risk as if biometric data are compromised. This is a topic that will foreseeably evolve and change a lot in the coming years. At the current state, it is necessary at least to reevaluate the implementation of biometrics and determine whether they are proportional with the benefit offered in the scenario discussed in the paper. Likewise, in relation to this scope, other convenient and secure methods must be explored and will hopefully appear in a near future.

ACKNOWLEDGMENTS

[*To complete after*]

REFERENCES

[1] Keyur K Patel, Sunil M Patel. 2016. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application &amp; Future Challenges*. IJESC 6*(5), 6123–6131.

[2] Gilad Rosner & Erin Kenneally J.D. 2018. Clearly opaque: Privacy risks of the internet of things. *The Internet of Things Privacy Forum May 2018* [Report] Retrieved the 5th of Mayl 2021 from: https://www.iotprivacyforum.org/clearlyopaque/

[3] Peter Friess & Ovidiu Vermessan. *2013.* Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. *River publishers' series in communications*, Aalborg, Denmark.

[4] Charter of Fundamental Rights of the European Union. Official Journal of the European Communities. C 364/1 (18th December 2000). Available online: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[5] Bastian Könings & Florian Schaub. 2011. Territorial Privacy in Ubiquitous Computing. In Eighth International Conference on Wireless On-Demand Network Systems and Services. New York 2011 IEEE Könings, 105-108.

[6] R.W. Picard. 1195. Affective Computing. M.I.T (Report No. 321) *Media. Laboratory Perceptual Computing Section Technical*. [Report] Retrieved the 5th of May from: https://affect.media.mit.edu/pdfs/95.picard.pdf

[7] Gergely Alpár, Jaap-Henk Hoepman & Johanneke Siljee. 2011. The Identity Crisis. Security, Privacy and Usability Issues in Identity Management. *ArXiv Business, Computer Science, Mathematics* 1-15. identity-crisis-body.tex 1355 2011-01-02 14:00:45Z jhh

[8] International Telecommunication Union (ITU) Digital Identity Roadmap Guide (2018) [Guide] Available online: https://www.itu.int/pub/D-STR-DIGITAL.01-2018

[9] Roger Clarke. 2010. A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation. Roger Clarke's website [Website] Retrived the 6th of May 2021 from: http://www.rogerclarke.com/ID/IdModel-1002.html

[10] Paul A. Grassi Michael E. Garcia James L. Fenton. 2017. Digital Identity Guidelines (NIST Special Publication 800-63-3). *National Institute of Standards and Technology Special Publication*. https://doi.org/10.6028/NIST.SP.800-63-3

[11] Guy De Felcourt. 2021. L'identité numérique aujourd'hui, Cours d'enseignement supérieur Société e identité numérique, presented at Université de La Rochelle [Course material].

[12] Gilad Rosner. 2014. Identity Management Policy and Unlinkability: A comparative case study of the US and Germany. Doctoral thesis presented at University of Nottingham [Doctoral thesis].

[13] FATF. 2020. Description of a Basic Digital Identity System and Its Participants. FATF, Paris [Appendix]. Available online: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Appendice%20A.pdf

[14] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol.L119 (4th May 2016) Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[15] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Official Journal of the European Union, Vol. 235/7 (9 September 2015) Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

[16] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Official Journal of the European Union, Vol. 337/35 (23rd December 2015). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

[17] James. L. Wayman (2001) Fundamentals of Biometric Authentication Technologies. International. *Journal of Image and Graphics* 01(01), 93–113.

[18] Debnath Bhattacharyya, Rahul Ranjan,Farkhod Alisherov & Choi Minkyu. 2009. Biometric Authentication: A Review. *International Journal of Service, Science and Technology* 2(3), 13–28 (2009). Retrieved the 7th of May 2021 from: https://www.researchgate.net/publication/46189709_Biometric_Authentication_A_Review

[19] Ricard Martínez Martínez. 2020. Facial Recognition identity verification and control of Online Exams. *Education and law review* No. 22

[20] Hitoshi Kokumai. 2021. Negative Security Effect of Biometrics Deployed in Cyberspace. Hitoshi Kokumai LinkedIn profile last accessed 2021/2/1.

[21] Paul Voigt & Axel von dem Bussche. 2017. The EU General Data Protection Regulation (GDPR). Springer, Cham, Germany.

[22] Spanish Data Protection Agency. Guía práctica para las evaluaciones de Impacto en la protección de los datos sujetas al RGPD. V.2018. [Guide] Available online: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

[23] Hitoshi Kokumai. 2021. Quantitative Examination of Multiple Authenticator Deployment. Hitoshi Kokumai LinkedIn profile last accessed 2021/2/1.

[24] Hitoshi Kokumai. 2016. Misuse of Biometrics Technologies. Payments Journal, May 18. Last accessed 2021/01/20 Retrieved the 7th of May 2021 from: https://www.paymentsjournal.com/misuse-of-biometrics-technologies/

[25] Hitoshi Kokumai. 2019. Passwords Made of Unforgettable Images. Payments Journal 30th September. Last accessed 2021/01/26. Retrieved the 7th of May 2021 from: https://www.paymentsjournal.com/passwords-made-of-unforgettable-images/

[26] Hitoshi Kokumai. 2018. Identity Assurance by Our Own Volition and Memory Part 1. Payments Journal 1st August. Last accessed 2021/01/26. Retrieved the 7th of May 2021 from: https://www.paymentsjournal.com/identity-assurance-by-our-own-volition-and-memory-part-1

[27] Hitoshi Kokumai. 2020. ‘Easy-to-Remember’ is one thing ‘Hard-to-Forget’ is another. Payments Journal 28th April (2020). Last accessed 2021/01/26. Retrieved the 7th of May 2021 from: https://www.paymentsjournal.com/easy-to-remember-is-one-thing-hard-to-forget-is-another