DOI: 10.5748/19CONTECSI/PSE/GOV/7034

IDENTIFICATION AND APPLICABILITY OF ADDITIONAL SECURITY FACTORS ON THE GOV.BR DIGITAL IDENTITY PLATFORM

Sandro Leite Furtado ; https://orcid.org/0000-0003-3800-1538
Universidade de Brasília

George Marsicano Corrêa ; https://orcid.org/0000-0001-9212-9124
Universidade de Brasília

IDENTIFICATION AND APPLICABILITY OF ADDITIONAL SECURITY FACTORS ON THE GOV.BR DIGITAL IDENTITY PLATFORM

ABSTRACT

The gov.br Digital Identity (ID) is the Brazilian Federal Government authentication platform used to provide access to different public services, which has several solutions and integrations up than 3,600 public services available to Brazilian citizens, such as digital certificates, banks authentication solutions and data validation in Federal Government databases. Due to its importance and criticality, gov.br ID suffers daily attacks attempts from malicious people who seek to appropriate third-party accounts to request public services of financial nature with the intention of applying blows to the Brazilian Government, harming the citizen who is the real owner and holder of the benefit. Aiming to further improve the security of gov.br ID and access to digital public services, this work carried out a systematic literature review (SLR) to identify additional security factors candidates to be implemented in the current solution. Conducting this SLR we found five additional security factors, namely: RBA, Tripwire, login rituals, OTP, and Bluetooth. From this, an analysis was carried out of each of the factors, in relation to their possibility of implementation in gov.br ID. Finally, the results of this work presents subsidies for maintaining the robustness of gov.br ID ecosystem that supports thousands of daily accesses.

Keywords: Identity Digital, Digital Authentication, Two-Factor Authentication

1 Introduction

The Brazilian Federal Government is working on the creation of a Digital Identity (ID) which has the objective to guarantee the correct identification of a citizen who, being correctly identified, will have access to public services and personal data following the dispositions of the General Data Protection Law.

The digital government secretary of the debureaucratization secretary, the management, and the digital government of the economy ministry possess as a guideline promoting technological platforms that ease the use of public services to the average citizen. The Federal Government published the Decree n° 10.332, 28th of April 2020 the Digital Government Strategy (known in Brazil by the Portuguese acronym, EGD) 2020-2022, the objects of the initiative consists in ”12.2 Make the digital identity available to citizens with the expectation of forty million emissions until 2022.

Digital government secretary is responsible for managing and promoting the use of the gov.br ID Platform and, above all, safeguarding the data of more than 120 (one hundred and twenty) million IDs. Throughout the existence of the gov.br ID Platform, several public agencies have joined and integrated their public services into the Federal Government’s authentication service, currently, the platform has more than 3,600 integrated digital public services. From the adoption of public institutions by the gov.br ID Platform as an

authentication solution, several of these services depends exclusively on gov.br ID for the identification of their user.

These IDs grant access to more than three thousand digital public services. Therefore, citizen authentication on the gov.br ID Platform is required identification and authentication process. Identification is a combination of characteristics or attributes that make a person unique to the gov.br ID while authentication is a way of validating the veracity of something or someone. For matter, Digital government secretary created three ID levels (bronze, silver, and gold) and for each of these levels, it was necessary to carry out cooperation agreements between institutes, as well as the integration of systems for the validation of biographical and biometric data in government databases.

As gov.br ID Platform is the gateway to access social security, education, tax, and fiscal public services, it suffers constant attacks attempts, for example, the use of robots to attempt to create accounts that intend to explore the carousel of questions, in this way, authentication solutions by themselves, with static passwords can often be vulnerable to attack. Therefore, additional authentication factors are used to improve this process. The additional fact of authentication can be understood as the use of more than one component to ratify the user's identity in the authentication process.

In this context, in order to improve the security access of all public services integrated into the gov.br ID Platform, this research proposes to identify additional authentication factors that could be used to improve the Platform process of authentication in order to improve the ID's protection against malicious attempts to hijack gov.br ID accounts in order to access government public services.

2 Literature Review

In this direction, the key concepts discussed throughout this work will be presented. In section 2.2, the concepts of identification and authentication are presented, bringing the characteristics and particularities of a person as ways of inferring their identification. On the part of Digital Identity, section 2.3, it is clarified the user's perspective and how he interacts in the digital world, as well as the identity life cycle, and presents the principles and levels of the gov.br Identity, in the Brazilian context. Finally, in the 2.4 section, an additional element, can guarantee greater security for the Platform.

2.1 Brazilian Identification System

Initially, the Brazilian Identification System was based on identifying criminals. Then advanced to identify Brazilian travelers outside the country and finally identify all Brazilian. In 1907, the first civil Identity Document was issued in Rio de Janeiro by the Identification and Statistics Department of the Federal District Police. The ID contained some attributes: Name, Parentage, Fingerprints, and Descriptions of Features such as scars and tattoos.

Currently, the physical IDs or Civil Registers - known as Registro Geral (RG) in Portuguese - are issued by Identification Institutes of the Civil Police of each State and the Federal

District. Each State issues an RG with a number from that respective state. However, with the advancement of technology, the RG issuance process was reformulated, and the use of inks for fingerprints was replaced by the biometric scanner. Likewise, digital signatures replaced the pen signatures and the photographs that were previously fixed on the forms are now taken during the identify appointment.

In the most recent activity for modernization, the Brazilian executive branch approved the creation of National Civil Identification (known in Brazil by the Portuguese acronym, ICN), with the objective of identifying Brazilians in their relations with society and with governmental and private bodies and entities. Furthermore, it is intended to concentrate data from the states' identification systems, allowing an exchange of information and a single number for each Brazilian in all states ICN.

2.2 Digital Identification and Authentication

An Identity refers to the combination of attributes that makes a person unique in a given context (Group, 2019). The identification process establishes/determines a person's identity by collecting and proofing relevant identity information (Group, 2019). In other words, identification is the process of certifying that a particular attribute chosen from a real-world entity proves to belong to that entity (Ford, 1998). According to the ID4D Guide (Group, 2019), identification systems can help answer some questions: "Who are you? Are you who you claim to be? Are you authorized or eligible for something?"

On the other hand, authentication is the process of checking someone or something that claims or claims to be a certain identity (Halonen, 2000). According to Ashibani, Yosef, and Mahmoud (Dressel et al., 2019), there are two types of authentication: explicit and implicit. Implicit authentication does not require user intervention, however, explicit authentication requires intervention.

According to Ford (Ford, 1998), there are five methods of authenticating a person: something the person knows, something the person owns, something the person is, where the person is at the time of authentication, and establishment of authentication by a reliable third party.

Identification and authentication systems sometimes access additional information that goes beyond the limits of the identification system itself, that is, an exchange of information between government branch bodies. This exchange of information is necessary to complement and validate the identification of a user by a certain institution. In other cases, the same identification system may provide manufacturer identification or eligibility determination.

2.3 Digital Identity

The concept of Digital Identity can be understood as a unique representation of a person involved in an online transaction (of Standards and Technology, 2017). With the increase in the adoption of IDs, especially with the use of biometrics in the validation of the

person, the demand for solutions to protect against the expansion of cybercrimes and identity theft increases (Geteloma et al., 2019). The application of the ID concept carries the challenge of verifying individuals on an open network, providing ground for opportunities for identity theft and other attacks that fraudulently claim another individual's ID (Standards and Technology, 2017).

This lifecycle is important for establishing trust between people, identity providers, and public and private entities in a variety of operations (Group, 2019). This series of stages in the identification process lifecycle is composed of four main processes: Registration, Issuance, Use, and Management.

The registration process is the initial state where a subject registers their identity for the first time. To obtain this registration the subject needs to go through an identity claim, where attributes are collected such as biographical information (e.g., name, sex, birthday, address). Then it is necessary to go through the identity proof where those data previously given are verified and have their authenticity proved. The issuance process consists of the emission of the subject's credential or authenticators (e.g., cards, certificates, PINs) and can be used as an identity. The Usage is when someone uses the identity to prove its identification, for example, to access some government services. At last, Management is the process to manage (also updating and reviewing) the subject's data and identity credentials by some previously defined process. This process is represented in Figure 1.

In Brazil, the Digital Government Secretary built the gov.br ID Platform, a digital identity solution that has been in operation since 2018. Until March 2022, the application has more than 126 (one hundred and twenty-six) million digital accounts. This platform has three authentication concepts of identity levels, namely, bronze, silver, and gold.

Each one of these levels has a defined process (Executivo, 2021) to be obtained. The Brazilian citizen can submit to obtain the gov.br identity by following it. The levels and their processes to be obtained are shown below:

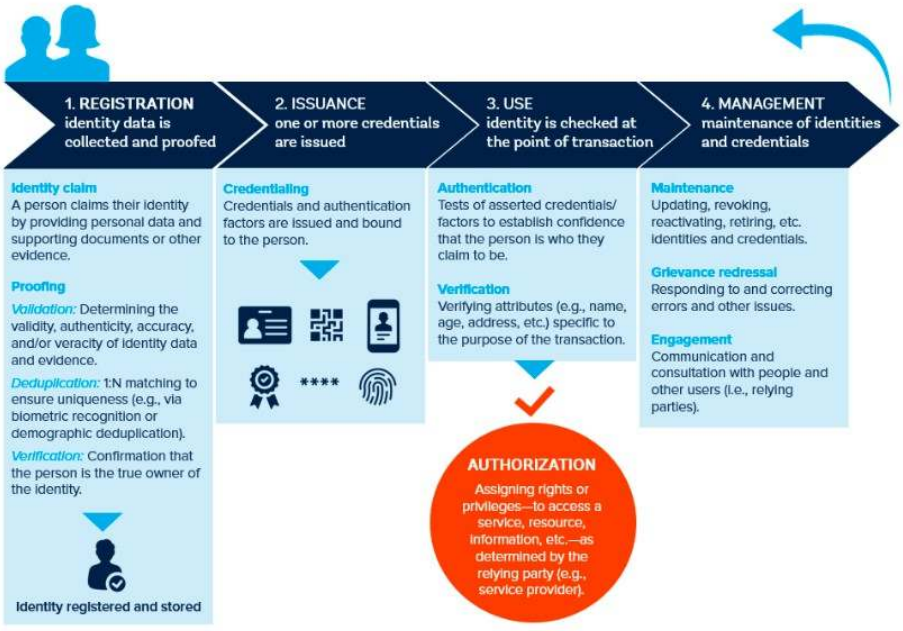

Figure 1: Identity lifecycle. Source: (Group, 2019)

ID - Bronze:

- Online Registration form to validate data at the Brazilian Internal Revenue Service;
- Online Registration form to validate data at Brazilian National Institute of Social Security (known in Brazil by the Portuguese acronym, INSS);
- Registration face-to-face at INSS agencies.

ID - Silver:

- Facial validation by the gov.br app to check the photo on the database of the National Driver's License (known in Brazil by the Portuguese acronym, CNH);
- Validation of data at the accredited bank via internet banking;
- Validation of data with username and password of government employees at the database of Federal Government Personnel Management System (known in Brazil by the Portuguese acronym, SIGEPE);
- Validation face-to-face at National Traffic agencies.

ID - Gold:

- Facial validation by the gov.br app to check the photo on the database of electoral justice;
- Validation of data with a Digital Certificate compatible with the Brazilian Public Key Infrastructure in Brazil (known in Brazil by the Portuguese acronym, ICP-Brasil).

An overview of the gov.br ID Platform is shown in Figure 2.

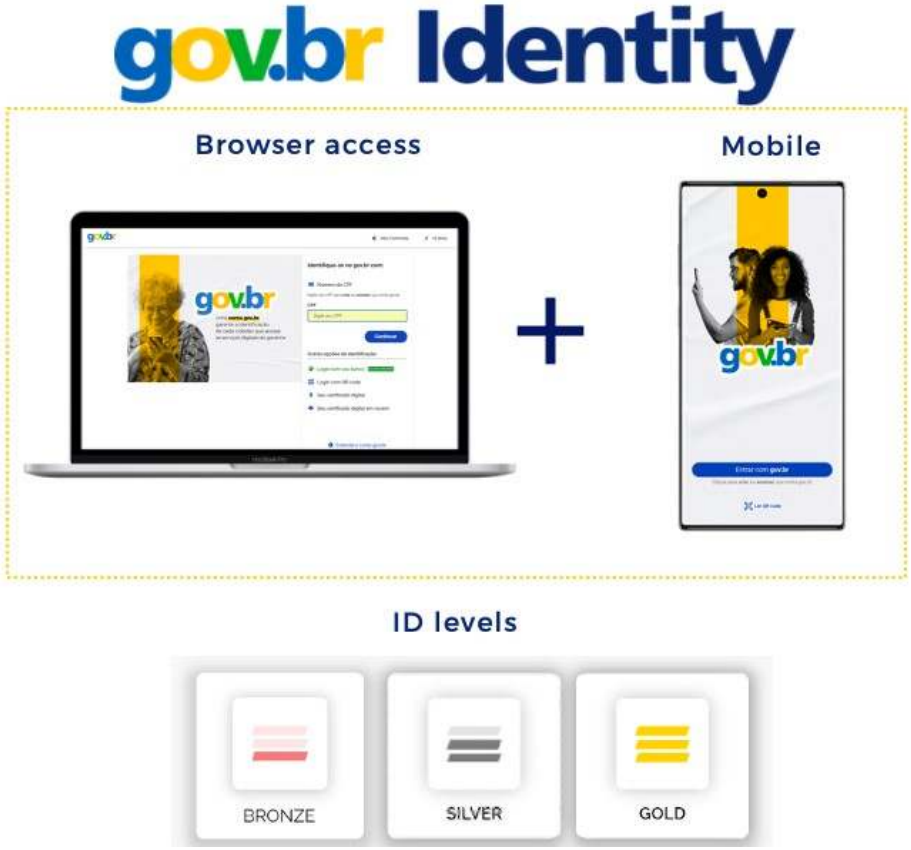

Figure 2: gov.br ID Platform

The gov.br Digital Identity allows access to several digital public services integrated with the gov.br ID Platform. Therefore Brazilian citizen does not need to go face-to-face to a public agency counter when they need something related to the State. They are health services, and student services, such as the National High School Exam (known in Brazil by the Portuguese acronym, ENEM), Unified Selection System (known in Brazil by the Portuguese acronym, SISU), University for All Program, known in Brazil by the Portuguese acronym, PROUNI), and Student Financing Fund known in Brazil by the Portuguese acronym, FIES), which also allows access and documents such as the National Driver's License (known in Brazil by the Portuguese acronym, CNH) and the Individual Taxpayer Registry (known in Brazil by the Portuguese acronym, CPF), as well as access to social security services and others.

Furthermore, considering beyond the 3.600 integrated public services, the gov.br ID Platform has other features and system integration already available such as integration with digital certificates; Partnership in authentication Process with banks platforms; data validation in government databases integration with the gov.br App; integration with portal gov.br and integration with the SMS Platform.

To exemplify in a simple way the architect view to the gov.br ID Platform we created the Figure 3 presenting the relationship between its connections.

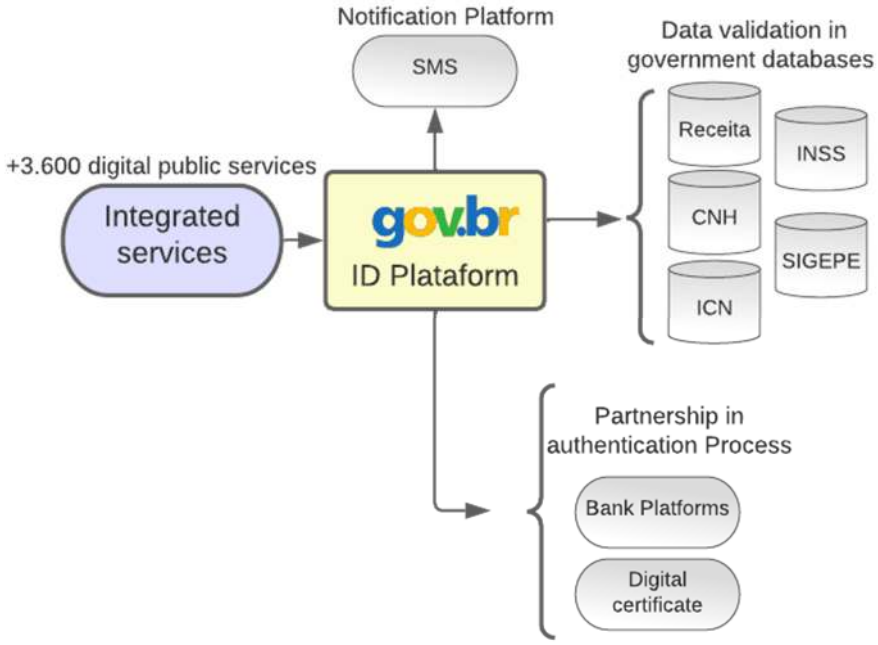

Figure 3: Integration's ID platform

2.4 Additional Authentication Factor

Systems, in general, use static authentication mechanisms, that is, based on static passwords. However, this type of mechanism is vulnerable to various types of attacks (Shirvanian and Agrawal, 2021). These vulnerabilities can be mitigated using systems with multi-factor authentication (MFA), more specifically, two-factor authentication (2FA) (Stanislav, 2015). In this way, more than one type of element can be used to guarantee authentication in addition to the static password, which could be many mechanisms, for example, biometrics, smart cards and One-Time Passwords (OTP) (Shirvanian and Agrawal, 2021).

Onetime Password (OTP) is a code generated through algorithms, without connecting the client to the server. The mobile phone will act as a token and use certain factors unique and depending on the configuration it may involve the combination of characters and symbols. It is usually implemented as a temporality additional security factor, The client may submit the password online or through a device such as an ATM machine. A program will be installed on the client's mobile phone to generate the OTP (Aloul et al., 2009).

Biometric is a behavioral trait, based on biological, anatomical, and physiological measurements that can be captured and used for recognition purposes. There are several forms of biometric geometry, such as facial recognition, digital recognition, voice recognition, signature recognition, and key or screen press patterns. According to Camp (Camp, 2004), the use of biometric technology to identify and digital authentication of individuals involves three distinct phases:

1. Sampling Phase: Capture of a person's biometric identifier, then the average measurement is used to produce the digital model of that individual;
2. Storage Phase: Encrypting of the digital model of the individual and storing it in portable tokens or database, that can be individualized or not, or remotely in a cloud (Odun-Ayo et al., 2017);
3. Recognition Phase: It is a comparison of the physical aspect you present for authentication against the digital model that has been stored. In this case, it is essential that there is a correspondence between the compared data, that is, the data obtained from the capture in phase 1 and the data obtained at the moment of phase 3.

Therefore when software has multi-factors it can be assumed that even if an attacker compromises one of the factors, the protection level is higher considering that the attacker will need to compromise the remaining factors (KOSE et al., 2020, Konoth et al., 2020). One of the benefits of adopting MFA is to provide a resilient form of user authentication and it appears to be a very cost-effective mechanism (KOSE et al., 2020). In addition to the initial authentication, the second authentication factor is used to protect other sensitive transactions, such as bank transfers (Konoth et al., 2020).

3 Methodology

This work is a Systematic Literature Review (SLR) based on the guidelines proposed by Kitchenham et al. (Kitchenham and Charters, 2007). Therefore, this paper is divided in three phases:

First of all, is exposed the **Planning**, this phase defines the work goals, the SLR protocol preparation, and the evaluation of the research protocol, which was tested when applied the search string in the chosen databases. Then, in the **Conduction** phase, the studies were identified through the application of the research strategy, defined in the planning phase, and selected according to the planning, where data is collected and synthesized. Finally, the **Report** phase, is composed of the documentation and description of results, preparation of answers to research questions, and dissemination of results.

3.1 SLR Planning

This study is inserted in the context of the developing a master's thesis. These results will be used as input for solutions decisions and implementation. First of all, the literature was manually searched for checking the existence or not of other surveys about the topic of this study. No similar study was found. Therefore, the development of the review SLR protocol was started.

The first step was to **establish the research questions**, which according to Kitchenham et al. (Kitchenham and Charters, 2007) is the most important part of any survey. This study will be guided by the following questions:

• QP.1 Which identified two factors of authentication in the literature are related to a Digital Identity?

• QP.2 Which identified multi-authentication factors in the literature are related to a Digital Identity?

To be considered two-factor authentication (2FA), a solution always requires the user to present two authentication factors from two different categories, such as a possession factor and a knowledge factor, to verify their identity. Multifactor authentication is broader than two-factor authentication. Requires the system to use two or more factors in the authentication process. Therefore, the researchers chose to perform the analysis separately, considering that for the RQ2 (MFA) the combination of factors could influence its usage and in its applicability. The academy perspective over these two approaches could provide a wider vision of the solution prospection permitting a better decision maker information to the process of selecting the additional authentication factor.

Subsequently, was define the automatic research strategy to delimit the primary studies, through the execution of research strings search. This search was preceded by a manual search of works related to the topic, which could help to establish the strings. In addition, for the composition of the string, we also used the keywords present in the research questions. From that, the string was: “Digital identity” OR “digital authentication” OR “digital identification”) AND (“two-factor authentication” OR “second factor authentication” OR “multi-factor authentication”). This string was run on Scopus, ACM Digital Library, IEEEXplore, and Science Direct databases.

The next step was established potentially parameters to select relevant works. Thus, the following **inclusion and exclusion criteria** were defined:

Inclusion Criteria (IC):

- IC.1 - The work helps to answer the research questions;
- IC.2 - The work was published after 2019;
- IC.3 - The work was written in English or Portuguese (from Brazil).

In October 2019 the Mundial Bank published a guide that describes the main concepts to implement a digital identity from its conception until its usage by users to access public digital services. This guide has its foundation in NIST and provides a beacon to several countries on their journey toward these concepts. Thus the authors consider this guide as a landmark for its research, justifying its inclusion in IC2.

Exclusion Criteria (EC):

- EC.1 - The work does not present additional security factors to a digital identity;
- EC.2 - editorials, journals, abstracts, tutorials, reports workshop, opinions, conference summaries, theses, dissertations, technical reports, books, shorts papers;

- EC.3 - works with propositions of physical security mechanisms;
- EC.4 - works not accessible;
- EC.5 - duplicates between research bases;
- EC.6 - secondary and tertiary works.

In order to **Assessment the Quality (AQ)** of the selected primary studies, three questions were used, which were answered with Yes (Y), Partially (P), or No (N). The questions are:

- AQ.1 - Were presented results of the applicability of the proposed factors?
- AQ.2 - Were there additional factor(s) and/or security tool(s) presented that can be applied to digital identity?
- AQ.3 - Were the limitations of the work(s) described?

Each of the answers has an assigned weight: (S) = 1, (P) = 0.5 and (N) = 0. From this, the score of quality of each work was calculated by the sum of the weight from each answer.

As far as **data extraction strategy** is concerned, the whole process was supported by the use of the MS Excel tool. The form used for data extraction was built to allow the registration of the following information: Title, abstract, author(s), additional factors, or techniques applied to solve the security requirements problem.

For the **analysis of the collected data**, the selected works were assigned a quality score. Those who did not reach the score as defined in the quality assessment criteria were considered unfit for this SLR, since they could have little similarity to the object of this study, mitigating damage to the results.

Finally, as a **review** from the process, checkpoints were established at the end of each executed phase. Initially, to discuss the adequacy of the protocol and later to evaluate the results obtained in each phase. After all, two researchers participated in the review. The following items were used, as proposed by Kitchenham et al. (Kitchenham and Charters, 2007):

- Search strings are properly derived from search questions;
- The data to be extracted adequately approaches the research questions;
- The data analysis processing is adequate to answer the research questions.

To evaluate the results, it was verified if they were coherent and adequate to answer the research questions guiding this survey.

4 SLR Conduction

This section presents SLR Conduction protocol going through the studies selection where the research strategy is applied, Quality Assessment, Data extraction and data analysis.

4.1 Primary Studies Selection

The primary study selection identified 09 potential works when searching into digital databases.

The result of the search string in the Scopus database was 160 works while in the ACM Library database 23 were found, IEEE Xplore the amount was 57 and finally, in ScienceDirect only 8, totaling 248 works.

The execution in the Scopus database directly complies with criteria IC.1, therefore, 160 works were found that with the application of the inclusion criteria IC.2, were reduced to 63 works, applying the IC. 3 the total of 63 were maintained.

In the ACM database, the total found after IC.1 was 23 works, applying the inclusion criteria IC.2 left 11 works, and applying IC.3 11 were kept.

While in IEEE Xplore after applying IC.1 57 works were found, applying the inclusion criteria IC.2 18 works were suitable, and applying IC.3, 18 were kept.

Finally, in the ScienceDirect database, the total found after IC.1 were 08 works, applying the inclusion criteria IC.1, 01 work remained.

Therefore, there were a total of 93 works, considering the sum of the bases that were submitted to the inclusion criteria. With the application of the exclusion criterion to consider only the works that meet the EC.1 criterion, 25 works were excluded.

Following the application of the exclusion criteria, the EC.2 criterion was applied, 11 works were excluded. With the application of the EC.3 exclusion criterion 05 works were excluded. the EC.4 exclusion criterion was applied, 16 works were excluded. And finally, 27 works were excluded with the EC.5 criterion.

There were no works identified as secondary or tertiary, according to the EC.5 criterion. The application of this research strategy and its selection criteria are illustrated in Figure 4.

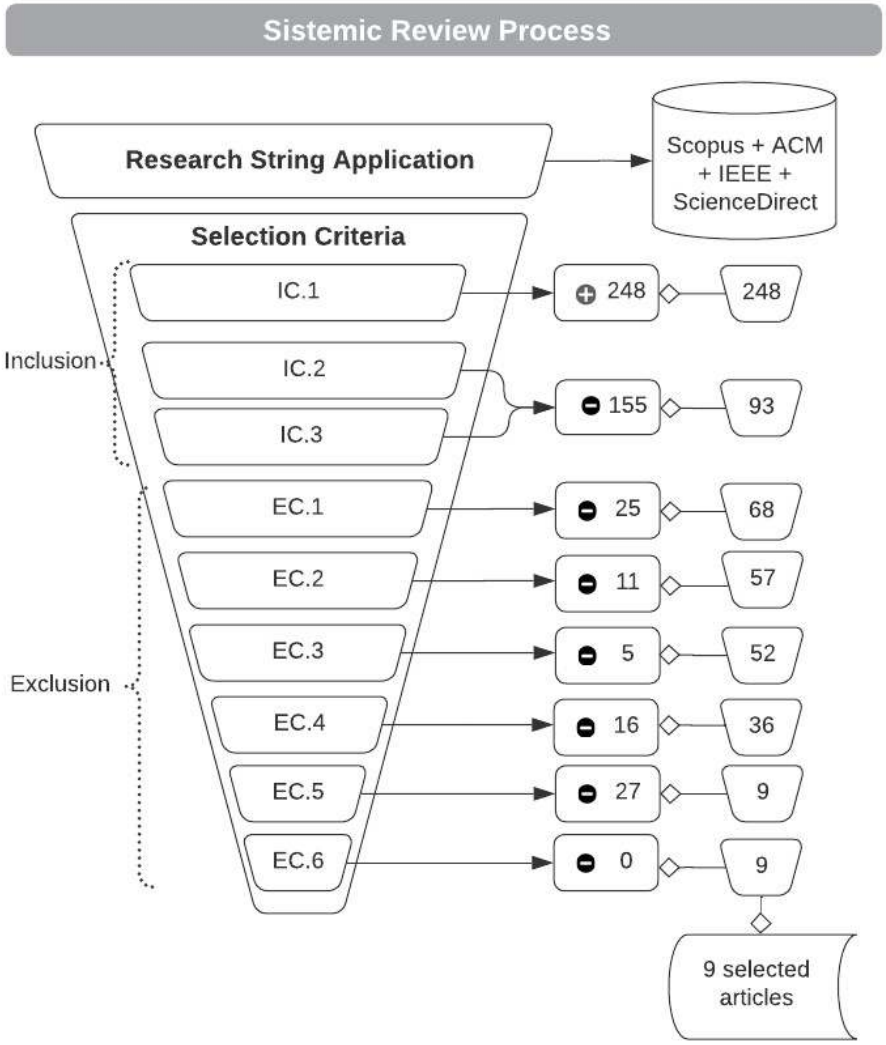

Figure 4: SLR Process.

Thus, 09 works remained for analysis and submission to the Quality Assessment process. The works are presented in Table 1 for better visualization of the findings and their information.

Table 1: Primary Study Sources

ID	Title	Authors	Ref
S1	SecuriCast: Zero-touch twofactor authentication using Web-Bluetooth	Dressel, T. and List, E. and Echtler, F.	(Dressel et al., 2019)
S2	Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication	Seta, H. and Wati, T. and Kusuma, I.C.	(Seta et al., 2019)

S3	A Proposed Unified Digital Id Framework for Access to Electronic Government Services	Geteloma, V. and Ayo, C.K. and Goddy-Wurlu, R.N.	(Geteloma et al., 2019)
S4	A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing	Kumar, S. and Jafri, S.A.A. and Nigam, N. and Gupta, N. and Gupta, G. and Singh, S.K.	(Kumar et al., 2020)
S5	Click This, Not That: Extending Web Authentication with Deception	Barron, T. and So, J. and Nikiforakis, N.	(Barron et al., 2021)
S6	Securing remote access to information systems of critical infrastructure using two-factor authentication	Bruzgiene, R. and Jurgilas, K.	(Bruzgiene and Jurgilas, 2021)
S7	TrustedID: An Identity Management System based on OpenID Connect Protocol	KOSE, Busra OZDENIZCI and BUK, Onur and MANTAR, Haci Ali and COSKUN, Vedat	(KOSE et al., 2020)
S8	More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-Based Authentication	Wiefling, Stephan and Du¨rmuth, Markus and Lo Iacono, Luigi	(Wiefling et al., 2020)
S9	2D-2FA: A New Dimension in Two-Factor Authentication	Shirvanian, Maliheh and Agrawal, Shashank	(Wiefling et al., 2020)

4.2 Quality Assessment

According to the defined quality assessment, the selected works were analyzed and scored. As part of the quality assessment process, the average rate metric demonstrated in the presented formula 1 was established so that baselines for adequacy to quality assessments (QA) were calculated. In this way, the baseline used for the cut is a higher value than the one obtained by applying the formula in which the total value of the grades is divided by the number of evaluated works.

$$s = \frac{(\sum \beta)}{\omega} \quad (1)$$

Having:

s = works average. β = value assigned to the works in QA.

ω = total number of works evaluated.

Hence, having ${}^{P}\beta = 17$ and $\omega = 9$, the calculation result is $s = 1.88$ as cut line of this quality evaluation. After all, 4 works were excluded for having a lower value than s, leaving 05 papers to be analyzed by the authors.

The result of this Quality Assessment is presented in Table 2 where the papers are listed by ID, answers for QA questions and its Score to the QA questions. The table is divided by selected and removed papers.

Table 2: Quality Assessment

	ID	QA1	Q2	QA3	Score
Selected	S8	S	S	S	3.0
	S5	S	S	S	3.0
	S9	S	P	S	2.5
	S1	P	S	S	2.5
	S2	S	S	N	2.0
Removed	S6	S	P	N	1.5
	S4	P	P	N	1.0
	S3	N	S	P	1.0
	S7	N	P	N	0.5

4.3 Data extraction

The data extracted from each study is listed below:

- Title;
- Abstract;
- The author(s);
- Additional factors or techniques applied by the work.

Table 3 presents the extracted data from the selected papers during the QA. For this matter the title has been changed by ID and the abstract has been suppressed over space issues.

Table 3: Data Extraction form

ID	Authors	Additional Factors
S1	Dressel, Thomas, Eik and Florian Echtler	OTP, Bluetooth

		(appSecuriCast)
S2	Henki, Theresia Wati, and Ilham Cahya Kusuma	OTP, Secure Hash Algorithm 1 (SHA1)
S5	Barron, Timothy, Johnny So, and Nick Nikiforakis.	Tripwire, Login Rituals
S8	Wiefling, Stephan, Markus Durmuth, and Luigi Lo Iacono	RBA
S9	Shirvanian, Maliheh, and Shashank Agrawal.	OTP

4.4 Data analysis

Finishing the conduction of this survey and based on the quality assessment, five primary works were selected, which are related to six additional security authentication factors, as shown in Table 4. The OTP (One-Time Password) is the additional factor that more appears in the primary works, appearing in three works, in two of them combined with other mechanisms.

5 SLR results

In this section, the results of the survey are presented and guided by the research questions.

5.1 QP1. Which identified two factors of authentication in the literature is related to a Digital Identity?

The work **S2** (Seta et al., 2019) proposes a solution using the OTP authentication method and the secure algorithm with *hash* algorithm 1 (SHA1). The method allows systems not only to rely on the username and password to log into the user's account but additionally to the common login process, the user must receive a token or code that is used to log into the user's account.

Table 4: Articles and Additional Factors

ID	RBA	Tripwire	*Loginrituals*	OTP	Bluetooth	SHA1
S8	x					
S5		x	x			
S9				x		
S1				x	x	
S2				x		x

The authors highlighted the fragility of using OTP with SHA1 to generate a code, that can not be the same, because this code can only be used once and within a certain time limit. Using SHA1 with different long input strings produced output with a fixed length *string* of 160 bits. The test results that 30 seconds is enough to prevent hackers from logging in and taking over the account without permission and also prove that this authentication can greatly enhance the security of the authentication process. Based on the results of the security tests performed by the authors, the authentication process using OTP and SHA1 still needs some improvement.

The work **S8** (Wiefling et al., 2020) deals with addresses Risk-Based Authentication (RBA). It is identified as a significantly different behavior from the user's routine, and additional authentication factors are requested. The authors point out that RBA has the potential to offer more usual authentication, but RBA's security perceptions and usability are not well studied in the literature. The proposal of the work is a study between groups in a controlled environment with 65 participants to evaluate two different types of RBA decisions (when there is a change of device or when there is a change of location, both types use re-authentication via email for confirmation), a type of 2FA (via email) and password-only authentication. The four methods chosen were based on the author's observations of next-generation deployments over RBA and other popular authentication methods. The results presented by the work indicated that RBA is considered more useful than the types of 2FA studied. It is also perceived as more secure than password-only authentication and is considered comparatively secure against the 2FA of the evaluated application types.

The work **S9** (Shirvanian and Agrawal, 2021), proposes a double authentication mechanism called by the authors of 2D-FDA (*Two Dimensions - Second Factor authentication*). According to the authors, 2D-2FA has three main features: First of all, after filling the username and password in a login terminal, a unique identifier is displayed for it. The user enters this identifier on their previously registered 2FA device according to the identification criteria. Afterward, a single-use PIN is calculated on the device and automatically transferred to the server, which is indicated by the authors as a differential in the 2D-FDA proposal, being the two dimensions that propose the name of the mechanism, since the PIN can have a high level of entropy, making guessing attacks inefficient. Finally, the identifier is also incorporated into the PIN calculation, which makes simultaneous attacks ineffective. It is noteworthy that usability and security studies were carried out to evaluate the applicability of 2D-2FA which demonstrates that the proposed system offers an error rate of almost 50% lower and 2/3 better efficiency with a performance of 2 to 3 times more fast compared to commonly used PIN-2FA.

5.2 QP.2 Which identified multi-authentication factors in the literature are related to a Digital Identity?

The work **S5** (Barron et al., 2021) presents two mechanisms related to a parameterization performed by the user, namely: tripwire and rituals logins. In the tripwire mechanism, the User can customize his web page or application, creating a trap that can be avoided by the legitimate owner, so if a tripwire is detected, it is assumed that is an intrusion, and actions security are triggered. it's important to highlight, that it is possible that these

traps may be triggered by the legitimate owner, occasionally, in case of forgetfulness. In the Ritual Logins mechanism, the user performs an access configuration, that is, he determines a sequence of clicks/access (a ritual) that will be performed immediately after authenticating on the platform. If the person who accesses does not execute the sequence exactly, countermeasures are adopted and the user is automatically logged out of the platform. The combination of these mechanisms generates the multiple application of factors proposed by the authors that were evaluated from a user study that evaluated the detection rate of tripwires against simulated intruders, 88% of whom clicked on at least one tripwire. The creation of custom login rituals by web users was evaluated from the perspective of practicality and memorization of these rituals over time. Of the rituals created by users, all were unique and 79% of users were able to reproduce their rituals. The authors point out that the work is not intended to replace standard authentication practices, but that their results showed that deception-based mechanisms can provide effective layers of additional security.

The work **S1** (Dressel et al., 2019) created an additional factor called: SecuriCast, this factor uses the OTP associated with the Bluetooth of the user's smartphone, through a connection established between browsers and mobile devices. The SecuriCast consists of three main components: the service provider that wants to authenticate the user, a browser, that supports WebBluetooth for the login process, and the user's smartphone with the application SecuriCast which will provide the second factor. SecuriCast has two forms: zero-touch and notify, in the first one, the user receives four keywords to verify and confirm the authentication attempt. In the second one, the user receives a six-digit code to be manually entered. The authors carried out a case study with a group of 30 volunteers among university employees and students, the analysis showed that SecuriCast zero-touch offers slightly better than GoogleAuthenticator, but performance has not reached a statistically significant level. The authors note that this slight difference could probably be related to the additional interaction currently required to configure the Bluetooth, but this connection may disappear in future versions of WebBluetooth. SecuriCast notify takes longer than the other modes, however, the authors point out that this difference is likely related to the relatively unknown process of comparing four keywords and would decrease with practice.

6 Discussions

This section discusses the results, their implications for academia and practice, as well as the limitations associated with this research.

6.1 Discussion of Results

An analysis was carried out to assess whether the additional factors presented in the selected primary works are feasible in the context of the Digital Identification System of the Brazilian Federal Government.

RBA proves to be an interesting additional factor when the system in which it is applied has a good infrastructure for behavioral analysis. That is, the system necessarily collects user location data and monitors access by controlling when devices other than the

initially linked device access. For scenarios that differ from the default user behavior, a second authentication factor is required to guarantee access authorization.

The tripwire and rituals logins bring an attractive approach to the solution, it is considered an additional factor aimed at answering the question: What does the user know? Since the trap and the initial access sequencing were defined by him. Therefore, even if the attacker obtains the login and password credentials, it would be necessary to overcome these additional factors. Assuming that the attacker has no idea of the existence of these additional factors and that they could even be reconfigured, it becomes even more complex to overcome these obstacles.

Regarding the additional OTP security factor, the combination of this factor with SHA1 did not bring significant results in the study of (Seta et al., 2019), which makes it impracticable to use in the improvement processes of the gov.br ID Platform. The use of the combination of OTP + Bluetooth brings significant challenges to the authentication process with good results demonstrated by the authors both in the use of the zero-touch model and the notify model. Consequently, that can be considered for use on the gov.br ID Platform.

The additional factors proposed, according to this work, mostly refer to a way to implement an MFA, either using OTP or combined with other factors.

The gov.br ID already implements the OTP additional authentication factor to offer citizens the option of receiving a code through the gov.br ID application, this procedure can be done on the gov.br ID online Platform. Once the second factor is enabled, any login attempt, whether on the web or via the app, will need to inform the code generated via OTP. The code is informed by the citizen and gov.br ID performs the validation, allowing or not the completion of the authentication process. But this factor can be improved by using the propositions found in this SLR. In addition, the RBA shows potential to be applied to gov.br ID, and it is necessary to verify that the aspects of the solution do not violate any clause of the LGPD, considering that for its operation it is necessary to collect georeferencing data, and to link and device control.

In addition, the use of biometrics in the process of creating or retrieving the gov.br Digital Identity (ID) was identified. Facial biometrics is used in the gov.br application through the onboarding process, at this time a comparison is made between the photo collected by the application with the National Civil Identity (ICN) database, when the user has a registration in the ICN, which assigns it the Gold ID or in the National Driver's License Registry (Renach) database, which assigns it the Silver ID category, respectively.

The factors identified in the literature, gov.br ID already implements the additional OTP authentication factor as described above. The factors RBA, Tripwire, Login Ritual OTP+Bluetooth and OTP+SHA1 are the factors that were identified as the ones that differ from those currently implemented in the gov.br ID Platform.

Considering that the implementation of multi-factors in the gov.br ID Platform can bring additional steps during the authentication process, this evolution must also be evaluated from the usability aspect, since the citizen's experience must be considered (Hassan and Galal-Edeen, 2017). Usability is one of the ways to add value to the user experience of a (Anitha and Prabhu, 2012) product.

Wiefling et al. (Wiefling et al., 2020) and Hirvanian and Agrawal (Shirvanian and Agrawal, 2021) also evaluated the application of the additional authentication factor from a usability perspective, demonstrating that this combination can bring benefits to the user. In the context of the gov.br ID Platform, the benefits can also be observed considering that the gov.br ID is the main form of access to meet various public policies for citizens in the digital world.

It should be noted that the first author of this work works at the Digital Government Secretary (known in Brazil by the Portuguese acronym, SGD), specifically, at the General Coordination of Digital Identity Platforms, this *background* makes it possible to carry out a more in-depth analysis of the data.

6.2 Implications for Academy

From an academic point of view, the contributions of executing this SLR are the investigation of the scenario of using additional authentication factors in the scope of digital identity. Such investigation identified a small number of works (five papers) related to the theme, contributing to the survey of these works and identification of these additional factors. This identification will allow other authors to explore these additional factors and their applicability in other authenticators and their access credentials (IDs), once applied, their data will be able to contribute to the comparison with other additional factors implemented, in order to have the additional factor that closer to success.

6.3 Practical Implications

As a practical implication we understand that the identification of the second factors is the main contribution considering that this work brought the factors registered and described in a succinct way to facilitate the industry usage and by this research itself. Furthermore, it is expected that the study case implementation of the factors will be a great practical contribution allowing others to analyze the results obtained from this research. As this article is part of a master's project, we still have the implications somehow still in the field of hypotheses, which limits us to present only the implications identified through the execution of the current phases of the project. We also believe that the registration of the protocol of this research will bring benefits in terms of the industry, allowing a practical and reproducible approach. Finally, we hope that the findings contributed to the improvement of the ID gov.br platform.

6.4 Review Limitations

The most common limitations in a systematic review are coverage, possible biases introduced in the selection process, and inaccuracies during data extraction and quality assessment. These are also the main possible limitations of this review.

To minimize these issues, we strongly relied on the guidelines reported by Kitchenham et al. (Kitchenham and Charters, 2007), regarding the construction of SLR

protocols. It should be noted that the protocol of this research was constantly reviewed by more than one researcher. Including your search string, inclusion and exclusion criteria, etc. Conflicts regarding the need for adjustments were agreed upon in meetings held between the researchers involved in this study.

Regarding coverage, automatic searches were performed in Scopus, ACM Digital Library, IEEEXplore, and ScienceDirect databases. Such a limitation may have contributed to the identification of a reduced amount of work, which may provide only a partial view of the possible answers to the research questions. Although, the researchers, from this SLR, have a perception that the amount of published works on double authentication and multi-authentication related to Digital Identity is still small.

As for the extraction and analysis of data, checkpoints were carried out among the researchers in order to minimize inconsistencies and misalignments regarding the understanding and procedures to be used. However, it was noticed that the lack of involvement of a third researcher may have contributed to the generation of problems in the interpretation of the identified data.

Finally, not perform a manual search after the automatic search, in order to complement the results obtained by the automatic search. Despite the researchers involved in the research understanding that the results would not be changed due to the scarcity of studies found because the research topic is still quite new.

7 Final Considerations and Future Work

Security in the context of gov.br ID is extremely important, considering the high volume of transactions and amounts of daily access to the platform. In this sense, conducting this SLR contributed to the identification of six different possible additional security factors that can be used in authentication/identification contexts from the primary studies evaluated in this protocol. These factors are used in combinations between themselves likely in the literature. Analyzing the combination of additional factors, OTP+SHA1, it was identified that they did not bring significant results in their application, making them difficult to use in the context of gov.br ID application.

In future works, the use of these five factors: Tripwire, login rituals, OTP, and OTP + Bluetooth will be evaluated, as well as the survey of which additional factors are already in use or in the process of being implemented, the choice of additional factors with the potential to be implemented in the gov.br ID Platform. In addition, the implementation of the chosen factor(s) and finally the evaluation of the results will be discussed and presented.

REFERENCES

Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 641–644.

Anitha, P., & Prabhu, B. (2012). Integrating requirements engineering and user experience design in product life cycle management. *2012 First International Workshop on Usability and Accessibility Focused Requirements Engineering (UsARE)*, 12–17.

Barron, T., So, J., & Nikiforakis, N. Click This, Not That: Extending Web Authentication with Deception. In: In *Asia ccs 2021 - proceedings of the 2021 acm asia conference on computer and communications security*. New York, NY, USA: Association for Computing Machinery, 2021, 462– 474.

Bruzgiene, R., & Jurgilas, K. (2021). Securing remote access to information systems of critical infrastructure using two-factor authentication. *Electronics (Switzerland)*, *10*(15).

Dressel, T., List, E., & Echtler, F. (2019). Securicast: Zero-touch two-factor authentication using webbluetooth. *Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems*. https://doi.org/10.1145/3319499.3328225

Executivo, P. (2021). Landing page gov.br [Access at: 2020-10-25]. https://www.gov.br/governodigital/pt-br/conta-gov-br

Ford, M. (1998). Identity authentication and 'e-commerce'. *Journal of Information, Law and Technology*, *1998*.

Geteloma, V., Ayo, C. K., & Goddy-Wurlu, R. N. (2019). A proposed unified digital id framework for access to electronic government services. *Journal of Physics: Conference Series*, *1378*(4), 042039. https://doi.org/10.1088/1742-6596/1378/4/042039

Group, W. B. (2019). Id4d practitioner's guide [Access at: 2021-10-25]. https://id4d.worldbank.org/guide

Halonen, T. (2000). Authentication and authorization in mobile environment. *Tik-110.501 Seminar on Network Security*.

Hassan, H. M., & Galal-Edeen, G. H. (2017). From usability to user experience. *2017 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, 216–222.

Kitchenham, B. A., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (tech. rep. EBSE 2007-001). Keele University and Durham University Joint Report.

Konoth, R. K., Fischer, B., Fokkink, W., Athanasopoulos, E., Razavi, K., & Bos, H. (2020). Securepay: Strengthening two-factor authentication for arbitrary transactions. *2020 IEEE European Symposium on Security and Privacy (EuroS P)*, 569–586.

KOSE, B. O., BUK, O., MANTAR, H. A., & COSKUN, V. (2020). TrustedID: An Identity Management System based on OpenID Connect Protocol. *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 1–6.

Kumar, S., Jafri, S. A. A., Nigam, N., Gupta, N., Gupta, G., & Singh, S. K. (2020). A new user identity based authentication, using security and distributed for cloud computing. *IOP Conference Series: Materials Science and Engineering*, *748*(1), 012026.

of Standards, N. I., & Technology. (2017). *Digital identity guidelines: Nist sp 63b*. CreateSpace Independent Publishing Platform.

Seta, H., Wati, T., & Kusuma, I. C. Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication. In: In *Proceedings - 1st international conference on informatics, multimedia, cyber and information system, icimcis 2019*. Jakarta, Indonesia: IEEE Computer Society Press, 2019, 115–120.

Shirvanian, M., & Agrawal, S. (2021). 2d-2fa: A new dimension in two-factor authentication. *Annual Computer Security Applications Conference*, 482–496. https://doi.org/10.1145/3485832.3485910

Stanislav, M. (2015). *Two-factor authentication* (Vol. 4). IT Governance Ltd.

Wiefling, S., Du¨rmuth, M., & Lo Iacono, L. (2020). More than just good passwords? a study on usability and security perceptions of risk-based authentication. *Annual Computer Security Applications Conference*, 203– 218. https://doi.org/10.1145/3427228.3427243