# Two-step verification as a safety measure for learners and teachers: an attempt to implement it in a real environment

Angélica González Arrieta, Daniel López Sánchez, Ángel Luis Sánchez Lázaro, María Belén Pérez Lancho, José Rafael García-Bermejo-Giner, Juan Andrés Hernández Simón and Pastora Isabel Vega Cruz angelica@usal.es, lope@usal.es, alsl@usal.es, lancho@usal.es, coti@usal.es, jahsimon@usal.es, pvega@usal.es

> Departamento de Informática y Automática Universidad de Salamanca Salamanca, Spain

Abstract- IT-based mechanisms are nowadays widespread and indeed essential, both in the first steps of learning and in university. In the latter case, a large amount of information is provided by teachers to learners, plus grades are uploaded which should only be seen by those they belong to. Further, email is used throughout, and Cloud-based repositories are used by all concerned. Secure access is an obvious requirement, and this is the goal pursued in the University of Salamanca. Two-step authentication can be done in several ways, be it in software, in hardware or by means of a mixture of both. This paper describes the various types of two-factor authentication in use today, as well as the experience of the authors when such a system was deployed in the University of Salamanca.

### Keywords: Universal SecondFactorAuthentication (U2F), Fast IDentify Online (FIDO) keys, on-line service

## 1. THE PROBLEM IN CONTEXT

Authentication techniques can be split into two groups: UAF or Universal Authentication Factors and U2F or Universal Twofactor Authentication. The first makes use of just one of the usual authentication factors: biometric data, physical devices (dongles) and passwords. The second one makes use of not just one but two of these methods. Indeed, passwords can be guessed, hardware keys may be stolen, and even biometric data can be simulated. Clearly, a combination of two of the previous factors provides better security because two obstacles are harder to circumvent than just one (Megouache, 2020).

A second authentication factor, hence, enhances security in comparison to single-factor systems (Ding Wang, 2020). For instance, a popular system in banking is the use of a plastic card engraved with an array of numbers. Each cell holds a couple of numbers, which the user must provide upon request when a financial operation is to be carried out. A second example is the use of a mobile phone to which some secret code is sent; the user must enter that code to confirm the operation. This is done by means of an app that can be installed in any smartphone. In this way, a dynamic authentication key is generated, which acts as a further authentication level and makes electronic fraud correspondingly harder.

European directive PSD2 (Payment Services Directive) (EUR-Lex, 2015) has been instituted to reinforce safety when buying or selling through Internet. This bill was passed on 2015, and it was adopted in Spain on January 1st, 2021. This type of security should really be in place in many other sectors which, like Teaching, make widespread use of a simpler mechanism like user/password combinations.

Both the online and the contact teaching/learning process make use of on-line services. To use them, both teachers and learners must authenticate. That is, teachers and learners use email, cloud storage, various platforms that hold information used in remote and contact learning, virtual libraries, and indeed servers that hold student grades. Obviously, all these services require knowing the precise identity of the user.

This paper describes current authentication methods in the University of Salamanca. There exists an authentication portal shared by students and teachers; through the portal, users can access their email (see Fig. 1) and a contents platform, Moodle (see Fig. 2).

SAL	VN B&
Id USAL @usal.es	UTILICE OTROS MÉTODOS DE AUTENTICACI
Contraseña	The Create its Meansh and Create its Meansh

Figure 1 User authentication portal for email access in the University of Salamanca.



Figure 2 User authentication portal for Moodle access (Studium.usal.es) in the University of Salamanca.

Two alternative methods can be used for authentication, a seen on previous figure.

CEUR-WS.org/Vol-3129/paper108.pdf

Besides, U. of Salamanca offers the community an app called Latch: this is a mobile app that makes it possible to use a second authentication factor, by means of a temporal PIN that can be compulsory or optional. (*Figure 3*).

SICPD 🖗 Quienes se	rnos + Servicios +	Guiles y ayudas + Noticias + Avisos +	Q, Bérgerda
Coerties y access a los servidos     Interdidad CÁL     enábras visanias y actuales te p     Latic correjo de agendida     - Corre parar a cancel la age     Corre allibra Latif ne modo C	Parel / Contan y accord Latch: cerrojo	a las servidos o de seguridad	
Como solicar Latón en modo PN     Como suar Latón paso a paso     Camo suar Latón paso a paso     Camo suar sustenizario	Disponible para (8)*** (8)***	utation (S) Team	
Conception of the concept	Descripción	Latch o cerrejo es una app para móviles que la chece un regundo fac temporal cono función de seguridad opcionel u obligatoria. Por tento, con esta aplicación artedimos un <b>nivel adicional de prote</b> c algabas.	ctor de autenticación basado en un PIN z <b>olón</b> en el acceso a tus servicios
<ul> <li>Infraentructuric redei y alternas</li> <li>Administraction electrónica</li> <li>Apreyra e la docersola</li> <li>Gerdice universitatia: aplicacianes de</li> <li>Te interesa</li> </ul>		Latch le protegerá en el caso de que te heyan robado tu contraseña. Latch le protegerá en el caso de que ta latch: "Si alguien conociese ni cost aplicaciones cuando estrin bloqueadas, sucederán dos cosas, primero Información, ni accederán a mis recursos, etc.) y angundo te llegará un los motidido oportansis.	tranefa y tratane de entrar en tus no tendrío acceso (no verio mi a alerta al redvil, para que puedas tomar

# Figure 3 Safety Latch.

This app adds an additional level of safety when accessing digital services. Latch protects those users whose password has been guessed or found out. That is: if a user's password is stolen, Latch will keep intruders from entering. Any attempt to use the password without the cooperation of Latch will keep the intruder from using any apps. This means there is no access to personal data or resources, and further an alert is sent to the phone so that measures can be taken.

Our study of the situation serves more than one purpose. First, it is an attempt to make users conscious of the need to use safer authentication methods, because a user/password combination is not secure enough. A second goal is to find out the actual degree of usage of Latch in the community. Finally, we consider the use of safety keys as a second authentication factor; is a second authentication factor viable in the context of access to services in Salamanca's University?

### 2. Description

As stated, the teaching/learning process involves many online services that store a lot information, both personal information of teachers and other types of information that belongs to students. The usual combination of username and password is no longer enough; many attacks have taken place lately and as a result the user/password of millions of persons has become public. This is especially damaging when, as is the case of students and teachers, many services share the same authentication.

Of course, actually logging on your own computer is a first barrier; one must log on before authenticating in some server. Indeed, operating systems offer possibly more than one way to authenticate for logon. Windows offers several options as seen in (Figure 4). Besides the usual user/password combination, one can make use of face recognition, fingerprint validation, and a safety device or key.



Figure 4 Windows session start-up options.

A *safety key* es is a hardware device (see Figure 5) that may be used in stead of a user/pwd combination in order to start a session in a web server. The device is used together with a digital footprint or PIN, so that even if the device were stolen one cannot stat a session without the PIN or digital footprint created previously.



Figure 5 Safety Key FIDO.

Two-step authentication is made easy by physical safety keys. One no longer must check a mobile device or email; just by inserting the key in a port the computer will authenticate the user. In a way, keys act like portable ID documents that, as USB devices, can be connected to a computer.

Safety keys are standard hardware devices that work through U2F. Instead of receiving a code, one connects the key to the computer to log in.

Keys look much like normal USB flash sticks. Internally, they have a chip with firmware that verifies both the account and the URL one wants to access. This avoids phishing and thus makes it impossible to supplant the user.

There exist several types of safety keys, depending on the connection methods they offer. Briefly, available key types are as follows:

- USB, with a type A or C connector. They are inserted in a compatible USB port in the device one wants to log on into.
- USB/NFC, which besides the USB connection offer NFC to perform verification just by placing the device near the NFC reader in our computer.
- USB/NFC/Bluetooth, which adds Bluetooth. In this way, even if the computer does not have an NFC antenna, on can use the key through the widely available Bluetooth connection.

Safety key operation is, well, secure. FIDO keys generate a couple of cryptographic keys when used. The private key is kept in hardware in the user's device. The online service checks that key by means of a mathematical operation; but the private key can only be unlocked when the user consents from the local device. Consent can be given by means of a fingerprint, o by entering a PIN. This method is described in many presentations one can find in Internet (FIDO, slideshare, 2021).

The FIDO Alliance is an open industrial whose goal is to help reduce dependence on passwords. It promotes the development of standards of authentication and certification, as well as the use of these standards and the compliance of devices with those standards (FIDO, Autenticación más simple y sólida, 2009). Many important business concerns are part of FIDO, like Microsoft, Google, Samsung, Apple, PayPal, Visa, American Express, Lenovo, Intel, Yahoo and Nok Nok, among others. Thus the usage of FIDO keys can be taken for granted as part of their products.

Various important companies like Google (Ayuda de cuenta Google, 2021) and Facebook (Servicio de ayuda Facebook,

2021) offer web support to activate safety keys. Others, like Dropbox (Dropbox, 2021) provide information pertaining to the way to enable two-step authentication.

Configuration of safety keys is simple. One must look for an option called "Add Safety Key" in the safety options of the various services. This option normally offers more than one way to enhance security: physical USB keys, or the chance to user a mobile phone as a safety key. This option is relatively new; users must confirm their identity from the phone when they try to access a server or service.

Google explains how to use two-step authentication in order protect accounts from hacking, even if the password has been stolen. Additionally, one can find the configuration procedure for safety keys embedded in a mobile phone to do a secure session start-up from devices based on Chrome OS, iOS, macOS and Windows (Google, Usar la llave de seguridad integrada de tu teléfono, 2021).

The access method for a Google account is described in this paper because the University of Salamanca has externalized its email by means of Gmail. Google provides personal or Workspace accounts, and each type can make use of different procedures to authenticate (Google, Seguridad, 2021). Workspace accounts require an administrator to authorize twostep verification, since those are institutional accounts.

The study of physical FIDO keys has required both software and hardware resources:

**USB FIDO keys with NFC and JavaCard**. These safety cards (FIDO U2F Security Key) can be used in machines based on Windows<sup>TM</sup>, Mac OS<sup>TM</sup> and mobile Android<sup>TM</sup> devices. These type of FIDO keys has been selected because JavaCard makes it possible to safely run small Java apps (applets) in the key. **Server software to control FIDO keys**. This is the

activation software for FIDO keys. Indeed, a demo version has been used (Cloudentify, 2021); should the software be deployed for various web services in the university of Salamanca, it would be necessary to implement the proper software.

We have been unable to find any Spanish universities that make use of FIDO keys as the second factor in two-step authentication. The authors contacted the proper authorities in the University of Salamanca to make USAL a pioneer in the deployment of a FIDO system. Our goal is to use FIDO keys for logging on to the on-line Moodle campus, and for authentication into the intranet of the academic administration system.

#### 3. Results

This study has implied 63 students form the Grado en Informática (Computer Science) of the Science Faculty and 54 staff members of said Faculty. The procedure was carried out just before the onset of COVID. This is a review of the authentication methods of the users when they access the digital services of the University for Salamanca. In particular, a second factor of authentication called Latch was offered to the members of the community involved in the study.

Students make use of their user/pwd combination in most cases (See Table 1).

Table 1 Authentication methods preferred by students.

	Authentication methods				
		ID with	Digital		
		card	Certificate		
	usr/pwd	reader	FNMT	Other	
0 Never	0,0%	81,0%	85,7%	87,3%	
1 Almost never	1,6%	7,9%	3,2%	0,0%	
2 Some times	3,2%	1,6%	0,0%	1,6%	
3 Almost always	14,3%	1,6%	1,6%	0,0%	
4 Always	81,0%	0,0%	0,0%	1,6%	
No answer	0,0%	7,9%	9,5%	9,5%	

Very few students have installed Latch (Figure 6 (a)) and most of them use it rarely (Figure 6 (b); Error! No se encuentra el origen de la referencia.).



(b) Usage.

Staff members use the user/pwd combination in most cases for access to online services in the University of Salamanca. Some of them use a certificate emitted by the FNMT, an a few use ther DNIe (electronic ID in use in Spain), see Table 2. Professors have normally attended courses taught by the University of Salamanca; further, a digital certificate is required for other external activities like accreditation or research recognition.

Table 2 Authentication method used by start methoers	ntication method used by staff	members
--	--------------------------------	---------

	Authentication methods			
	usr/pwd	ID with card reader	Digital Certificate FNMT	Other
0 Never	0,0%	63,0%	53,7%	63,0%
1 Almost never	0,0%	3,7%	7,4%	0,0%
2 Some times	1,9%	3,7%	9,3%	0,0%
3 Almost always	9,3%	0,0%	1,9%	0,0%
4 Always	87,0%	0,0%	1,9%	0,0%
No answer	1,9%	29,6%	25,9%	37,0%

One can see that less than one fourth of the staff members who answered the poll have installed Latch (see Figure 7(a)). Of these, only one half use it (see Figure 7 (b)). This percentage is only slightly higher than that of students and it is possibly due to fearing illegal access to grades.



Figure 7 (a) Staff members who have Latch installed. (b) App usage.

Students were also asked about the need to increase safety in university online services. A relatively high number (58,7%) agreed about this need. The first poll was posed to staff members, degree and master students, and non-faculty staff. Participation was 75.9%, 11.1%, 7.4% and respectively 5.6%. One can see a smaller need for increased security that could be attributed to the fact that some of them make use of Latch (see Table 3).

Table 3	3 N	leed	to	increase	safety	level	ls.

	Staff members	Students
Yes	46,3%	39,7%
No	50,0%	58,7%
No answer	3,7%	1,6%

Results show that a second authentication factor is hardly used, although it is indeed available. This may be due to lack of knowledge about Latch, or perhaps because using a mobile phone for authentication could be cumbersome. Hence, other alternatives for second factor of authentication are being offered to the community (indeed safer alternatives).

The various authors have tested different authentication methods. Each of them met different problems. Keys have been found to be only officially compatible with Google Chrome. Firefox requires a plugin; work seems to be in progress to make it natively compatible. One further obstacle is that to access Google Drive for key activation one must make use of a smartphone. In this case, since USAL provides VoIP, each teacher has an assigned phone number, but students would have to use their own devices.

All participants in this review registered their safety keys USB/NFC/Bluetooth in the test web (Cloudentify, 2021) and web access by means of the key was achieved with no problems.

## 4. CONCLUSIONS

- Most users do not know the existence of a second authentication factor offered by USAL; in fact, they do now know that Latch is available. Of the few who know about Latch, most do not have it installed and those do, do not use it.
- Two-factor authentication is necessary to access the virtual campus, and to use other services that deal with grades and with private data. Nowadays this can be done by means of a digital certificate, by a usr/pwd combination may also be used.
- Handling of FIDO keys is simple, as tested in several services.
- A second authentication factor in the form of a hardware device increases safety when compared to other authentication methods.
- Safety in online teaching/learning processes requires further study. One must consider the viability of making FIDO key usage compulsory for access.
- The investment needed to increase safety is modest. To be precise, a FIDO key should be provided to all involved, plus a web application must be developed in order to control service access by means of the keys.

Possibly, an increase of safety in authentication will have a positive influence on teaching. Nowadays, most of the teaching in USAL is carried out in contact hours. The difficulty of online teaching is related to student authentication, even more so when evaluation is done online. One doubts about giving more weight to continuous evaluation because online exams or tasks uploaded to a platform offer no proof about their authorship. In that sense, a better knowledge about just who is online is positive; with further help concerning authorship, one might indeed increase the offer of virtual, partly presential or fully online learning. For instance, two-factor verification with FIDO keys would increase the safety of exams sent through email between teachers. Further, exams kept in the cloud would be safe even when usr/pwd combinations are stolen since the key would be required for access. The list is long, and one can think of many other instances in which two-step verification would be most useful.

### ACKNOWLEDGMENTS

We would like to thank USAL for the various times in which help has been offered as grants for innovation projects, particularly for the grants awarded to our proposals "Análisis y propuesta de diferentes métodos de autenticación para el acceso a las plataformas de formación on-line y al servicio de calificación de actas. (Project code: ID2016/0106)" and "Llaves FIDO (Fast IDentify Online) como segundo factor de autenticación en la gestión on-line de los procesos de enseñanza y aprendizaje (Project code: ID2017/030)" which have made this project possible.

Our thanks are due too to the student of the "Grado en informática" of the University of Salamanca and to those staff members of the Science Faculty who cooperated with us in various ways.

#### Reference

- Ayuda de cuenta Google. (2021). Found in Utilizar una llave de seguridad para la verificación en dos pasos: https://support.google.com/accounts/answer/6103523?co =GENIE.Platform%3DAndroid&hl=es
- Cloudentify. (2021). Prueba usao la clave de seguridad FIDO U2F. Obtenido de https://u2f.cloudentify.com/u2fdemo/
- Ding Wang, X. Z. (January de 2020). Understanding security failures of multi-factor authentication schemes for multiserver environments. Found in https://id.elsevier.com/ as/hx96h/resume/as/authorization.ping?client\_id=SDFEv3&state=retryCounter%3D0%26csrfToken%3Dff70cb4 1-4a18-4532-8a60e3bc32b95420%26idpPolicy%3Durn%253Acom%253A

elsevier%253Aidp%253Apolicy%3Durn%253Acom%253A elsevier%253Aidp%253Apolicy%253Aproduct%253Ai nst\_assoc%26returnUrl%3D%2

- Dropbox. (2021). Cómo habilitar la verificación en dos pasos. Found in https://www.dropbox.com/ es\_ES/ help/security/ enable-two-step-verification#2falsecuritykeys
- EUR-Lex, A. t. (25 de noviembre de 2015). Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015. Found in https://eur-lex.europa.eu/ legal-content/ES/TXT/?uri=celex%3A32015L2366
- FIDO, A. (2009). *Autenticación más simple y sólida*. Found in https://fidoalliance.org/
- FIDO, A. (2021). *slideshare*. Found in Alianza FIDO: https://www.slideshare.net/FIDOAlliance/presentations
- Google. (2021). Seguridad. Found in https://myaccount.google.com/security
- Google. (2021). Usar la llave de seguridad integrada de tu teléfono. Found in https://support.google.com/ accounts/answer/9289445?co=GENIE.Platform%3DAnd roid&oco=0

- Megouache, L. Z. (2020). *Hum. Cent. Comput. Inf. Sci. 10, 15* (2020). Obtenido de Ensuring user authentication and data integrity in multi-cloud environment: https://link.springer.com/ article/10.1186%2Fs13673-020-00224-y
- Facebook Help Service. (2021). ¿Qué es una clave de seguridad y cómo funciona? Found in https://es-la.facebook.com/ help/401566786855239