CALL 4 COMMENTS FOR NIST STANDARDS-Proposals for improvement for NIST regulation and regulations

NIST is particularly interested in comments and recommendations for the following topics:

- *Capabilities and innovative approaches for remote identity proofing to achieve equivalent assurance as in-person identity proofing.*

1.The NIST Special Publication 800-paragraph 63A **Act, which is the most emphasized in the subject of the requirements for Indetity proofing,** in section **4,** describes the **following:**

Identity proofing's sole objective is to ensure the applicant is who they claim to be to a stated level of certitude. This includes presentation, validation, and verification of the minimum attributes necessary to accomplish identity proofing. There may be many different sets that suffice as the minimum, so CSPs should choose this set to balance privacy and the user's usability needs, as well as the likely attributes needed in future uses of the digital identity. For example, such attributes — to the extent they are the minimum necessary — could include:

1.Full name

2. Date of birth

3. Home Address

This document also provides requirements for CSPs collecting additional information used for purposes other than identity proofing.

The sole purpose of proof of identity is to ensure that the applicant is the one who claims to be at an established level of certainty. This includes presenting, validating, and verifying the minimum attributes required to perform identity verification. There can be many different sets that are sufficient at a minimum, so CSPs should choose this set to balance user privacy and usability needs, as well as the likely attributes required in future uses of digital identity. For example, these attributes—to the extent that they are the minimum required, might include:

1.Full name

2. Date of birth

3. Address

This document also provides requirements for CSPs that collect additional information used for purposes other than proof of identity.

The following amendment is **proposed:**

The main objective[1] of proof of identity is to ensure that the applicant is the one who claims to be at an established level of certainty, according to international standards such as: eIDAS, KYC,

[1] We consider that it is not the only one because this type of identification will also allow us to recognize whether this person is a politically exposed person or similar person, as well as other objectives of anti-

among others. This includes presenting, validating, and verifying the minimum attributes required to perform identity verification. There can be many different elements that are considered sufficient at a minimum, so CSPs[2] must review, discriminate, and choose within this set of minimum elements, so that certainty is made to balance the user's privacy and usability needs, as well as the likely attributes required in future uses of digital identity. For example, these attributes—to the extent that they are the minimum required, might include:

1.Full name

2. Date of birth

3. Address

4.Cell phone number and/or mail (some code or message may arrive)

5.Videoidentification with some sign of life such as a smile or another.

This document also provides requirements for CSPs that collect additional information used for purposes other than proof of identity.

Why is this amendment proposed?

Because as drafted the rule gives full discretion to CSPs when it really should not be so and they have to follow a number of additional security measures, so that in fact the identification both in person and remote (digital identification) can be carried out in an appropriate way and generating trust in the users in virtus of their particularities and generating on the other hand certainty for the CSPs who perform this process of verification of the identification, especially as the standard says according to future uses and other practices and standards that work very well for this type of process - even more remote identification - globally.

2.The NIST Special Publication 800-paragraph 63A Act, which is the most emphasized in the subject of the requirements for Indetity proofing, in section **4.1,** describes the **following:**

Note: The identity proofing process can be delivered by multiple service providers. It is possible, but not expected, that a single organization, process, technique, or technology will fulfill these process steps.

Note: The identity verification process can be performed by multiple service providers. It is possible, but not expected, that a single organization, process, technique, or technology will meet these process steps.

The following amendment is **proposed:**

Note: The identity verification process can be performed by multiple service providers. It is possible, but not expected, that a single organization, process, technique or technology meets

fraud recognition based on the data of the person in this "identification process", which generate greater certainty.

[2] A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP can be a separate third party or issue credentials for its own use.

these steps of the process, in any case these organizations must always submit a simple report but express the innocuousness of the in-person and non-face-to-face identification procedure, in accordance with the standards established in the regulations and other world-class standards.

Why is this amendment proposed?

It seeks to avoid the full discretion of service providers and that they meet all the requirements to be considered as qualified service providers and that at the same time through the issuance of the report referred to generate a simple document that generates greater certainty in case of any claim or misunderstanding regarding identity and its verification processes either in person , but mainly in remote identification.

3.The NIST Special Publication 800-paragraph 63A**Act, which is the most emphasized in the subject of the requirements for Identity proofing,** in **section 4.2,** describes the **following:**

1. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.

*The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled. For example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud counter-measures when anomalies are detected.*

1. No proof of identity shall be carried out to determine the suitability or right of access to the services or benefits.

Identity verification and enrollment processes WILL BE PERFORMED in accordance with an applicable written policy or *declaration of practice* that specifies the specific steps that have been taken to verify identities. The *practice statement* will include control information detailing how the CSP handles verification errors that cause an applicant to not register successfully. For example, the number of intentos allowed, test alternatives (for example, in person or if it fails remotely), or fraud countermeasures when anomalies are detected.

The following amendmentis**proposed:**

1. No proof of identity shall be carried out to determine the suitability or right of access to the services or benefits.

Identity verification and enrollment processes WILL BE PERFORMED in accordance with an applicable written policy or *declaration of practice* that specifies the specific steps that have been taken to verify identities. The *practice statement* detailed in section xxxxx,[3]which will include control information detailing how the CSP handles verification errors that cause an applicant to not register successfully. For example, the number of intentos allowed, test alternatives (for example, in person or if it fails remotely), or fraud countermeasures when anomalies are detected,suchas:

[3] It should be noted where it is or in any case design and incorporate it as an annex or through a memorandum, like others that introduce additional issues to the NIST legislation, some standard format of this declaration.

-Prior to the verification, the CSP should carry out the specific risk analysis

-The CSP will document the procedure and test its effectiveness, reviewing the results in writing.

- The CSP shall have staff who have specific training in non-in-person identification procedures by videoconference, this must be consistent with the functions performed and be accredited in accordance with the provisions of international standards related to the subject.

- The process of identification by videoconference must be recorded with record date and time.

-Users must expressly consent to the completion of the non-in-person identification procedure by videoconference and the recording and preservation of the process, before or during the identification process.

-The identification process may not be completed where (i) there are indications of falsity or manipulation of the identification document, or (ii) there are indications of non-correspondence between the holder of the document and the user being identificationd, or (iii) the conditions of the communication prevent or make it difficult to verify the authenticity and integrity of the identification document and the correspondence between the holder of the document and the customer being identification.

- CSPs must obtain and retain a photograph or snapshot of the front and back of the identification document used. The photograph or snapshot obtained shall meet the conditions of quality and sharpness, indicated in other sections of the NIST and memorandums, which allow its use in investigations or analyses and shall be preserved

- Prior to the execution of any transaction, the obligated subject shall verify that the client is not subject to national or international sanctions.

While non-face-to-face identification procedures by videoconference can be outsourced and/or outsourced, the CSPs in charge assume full solidarity responsibility with the entities that have contracted them.

It is important that CSPs appoint an expert to issue a report on the adequacy and operational effectiveness of the non-in-person identification procedure by videoconference.

Why is this amendment proposed?

We propose this improvement because we consider that the regulations as it is proposed although it facilitates and encourages remote identification in a face-to-face and synchronous way but not the asynchronous one, it is demonstrated according to international regulations that we will share with you through the following link that there are countries that have been implementing the topic of video identification synchronously but also asynchronously with great success and that this in COVID times (quoting the memorandum : **M-2 0-19 MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES,** which mentions the problem caused by access to many services due to the lack of the establishment of an appropriate and suitable digital boarding process) has facilitated access for many users to carry out formalities remotely , safe and reliable as there are digital on boarding processes and/or synchronous video identification but above all asynchronous that really facilitates the goal according to the needs of users.

The NIST Special Publication 800-paragraph 63A Act, which is the most emphasized in the subject of the requirements for Identity proofing, in section **5.1,** describes the **following:**

The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes necessary to resolve to a single individual. It provides the CSP an important starting point in the overall identity proofing process, to include the initial detection of potential fraud, but in no way represents a complete and successful identity proofing transaction.

The purpose of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes needed to resolve a single individual. It provides the PSC with an important starting point in the overall identity verification process, to include the initial detection of potential fraud, but does not in any way represent a complete and successful identity verification transaction.

The following amendment is proposed:

The purpose of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes needed to resolve a single individual. It provides the CSP with an important starting point in the overall identity verification process, to include the initial detection of potential fraud, but does not in any way represent a complete and successful identity verification transaction.

As we have mentioned in previous comments we consider that video identification should be emphasized and to add some additional checkpoints to such procedures we add that: That validation and verification of identity should be improved and strengthened in the identification processes and above all of video identification, according to the following:

-By psychological interrogation and observations made during the identification procedure, the employee must be satisfied with regard to the adequacy of the information contained in the identity document, the information provided by the person to be identified during the interview, as well as the stated intention of that person. Questions may also be asked, for example, regarding the age, date, and place of birth of the ID.

-Smile as a life proof implementation, especially for cases where video identification occurs asynchronously and in any case to speed up the syncrony.

Why is this amendment proposed?

Because we consider that **the validation and verification of identity through proof of life especially in cases of video identification** (synchronous and asynchronous)is necessary and that this element allows to guarantee the security of the non-in-person identification procedure.

3. The NIST Special Publication 800-paragraph 63A Act, which is the most emphasized in the subject of the requirements for Identity proofing, in section **9.3. there, describes** the following:

Since remote identity proofing is conducted online, follow general web usability principles. For example:

- *Design the user interface to walk users through the enrollment process.*
- *Reduce users' memory load.*
- *Make the interface consistent.*
- *Clearly label sequential steps.*
- *Make the starting point clear.*
- *Design to support multiple platforms and device sizes.*
- *Make the navigation consistent, easy to find, and easy to follow*

Because remote identity verification is done online, follow the general principles of web use. For example:

o Design the user interface to guide users through the enrollment process.

o Reduce users' memory load.

o Make the interface consistent.

o Clearly label sequential steps.

o Make the starting point clear.

o Design to support multiple platforms and device sizes.

o Make navigation consistent, easy to find and easy to follow

The following amendmentis**proposed:**

The text is fine,but can be supplemented, with the following specifications:

Because remote identity verification is done online, follow the general principles of web use. For example:

o Design the user interface to guide users through the enrollment process.

o Reduce users' memory load.

o Make the interface consistent.

o Clearly label sequential steps.

o Make the starting point clear.

o Design to support multiple platforms and device sizes.

o Make navigation consistent, easy to find and easy to follow

- Determine the list of documents that will be considered valid for the purposes of identification procedures
- Ensure at all times the quality of the procedure in terms of connectivity, image sharpness and usability of platforms or channels for these purposes.

- Implement and provide necessary information security mechanisms to the platforms to be used for identification procedures
- Ensure the proper use of user data (only for certain purposes), continuously asking the user for consent on each of the concessions that he/she makes and where the CSPs assume joint responsibility with the entities that contracted them for the identification processes in case of a mishap, indicating transparently the protocol.

Why is this amendment proposed?

Because the suggested proposals only provide greater certainty, trust and security to the processes of non-face-to-face identification, so that users have less resistance when using them and thus we save the privacy of the data generating a sense of transparency and trust as other countries have been developed in which we observe good practices such as: Spain, Germany and Austria..

RESOURCES OF INFO THAT HAVE BEEN USED & CONSULTED:

1.file:///C:/Users/andre/Dropbox/Documentación%20del%20Proyecto%20(1)/Entregables/Entregable%202%20-%20Analisis/Official%20rules%20and%20codes%20VF/USA/NIST%20Special%20Publication%20800-63-%20Digital%20Identity%20Guidelines-con%20referencias.pdf

2.file:///C:/Users/andre/Dropbox/Documentación%20del%20Proyecto%20(1)/Entregables/Entregable%202%20-%20Analisis/Official%20rules%20and%20codes%20VF/USA/NIST.SP.800-63a-%20con%20referencias%20y%20resaltado.pdf

3. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

4.file:///C:/Users/andre/Dropbox/Documentación%20del%20Proyecto%20(1)/Entregables/Entregable%202%20-%20Analisis/Official%20rules%20and%20codes%20VF/USA/NIST.SP.800-63c-con%20referencias%20y%20resaltado%20.pdf

5.file:///C:/Users/andre/Dropbox/CALL%20FOR%20COMMENTS%20DE%20ESTÁNDARES%20Y%20LEYES/NIST/M-19-17%20for%20heads%20and%20agencies.pdf

6.file:///C:/Users/andre/Dropbox/CALL%20FOR%20COMMENTS%20DE%20ESTÁNDARES%20Y%20LEYES/NIST/M-20-16%20COVID.pdf

7.file:///C:/Users/andre/Dropbox/CALL%20FOR%20COMMENTS%20DE%20ESTÁNDARES%20Y%20LEYES/NIST/M-20-19-%20Harnessing%20Technology%20to%20Support%20Mission%20Continuity.pdf

8.file:///C:/Users/andre/Dropbox/CALL%20FOR%20COMMENTS%20DE%20ESTÁNDARES%20Y%20LEYES/NIST/NIST.CSWP.01162020.pdf

9.file:///C:/Users/andre/Dropbox/CALL%20FOR%20COMMENTS%20DE%20ESTÁNDARES%20Y%20LEYES/NIST/NIST.CSWP.04162018.pdf

10.Benchmarking for IDB of worldwide regulation