How to Digitally Verify Human Identity

The Case of Voting

Disponibile anche in italiano
www.isaca.org/currentissue

How important is individual identity in human beings, really? There are several possible answers, ranging from irrelevant to fundamental, but it depends on the context. In prehistory, there was likely no personal identity at all—only a dichotomic group identity. Subjects belonged to a utilitarian group that could comprise friends or enemies, males or females, or strong or weak, and so on. However, today personal identity is indispensable to the coexistence of people in society. All individuals have their own registered histories and identities to help them foster relationships with others or access services.

Technological evolution and new social habits have exacerbated the need to identify a person with increasing precision. In many countries, a license is required to drive a car, a passport is required to visit another country, a social security number (or equivalent) is required for a medical examination and an identity card (or equivalent) is necessary to exercise the right to vote. On the other hand, this excess of information used for identification is contrasted with the need to respect the fundamental rights and freedoms of people's privacy and, in particular, their right to protect their personal data. The difficulty lies in determining the right balance between the effectiveness of identification and people's privacy rights.

Defining Human Identity

Human identity is the set of characteristics that make an individual in society unique (when referring to a single individual, not the human species as whole). In a social context, it is a method of identifying a person compared to others. In computer terms, it is an object that has a unique code, internally to a defined space, associated with various attributes and methods of treatment. Defining identity in an abstract way is easy. But in practice, there are several different ways to choose or treat individual characteristics to identify subjects, which is more difficult. Sometimes, in addition to the information strictly necessary for the recognition of identity, further classes of information are requested, such as the address, gender, age or a photo of the person. In addition, these data over time may need to be changed, perhaps because personal characteristics have changed, or because the service has been terminated or for any other need of the interested party.

LUIGI SBRIZ | CISM, CRISC, CDPSE, ISO/IEC 27001:2013 LA, ITIL V4, NIST CSF, UNI 11697:2017 DPO

Is a lead auditor and senior consultant on risk management, cybersecurity and privacy issues. He has been the risk monitoring manager at a multinational automotive company for more than seven years. Previously he was head of information and communication operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia) and was the worldwide information security officer for more than seven years. He developed an original methodology for internal risk monitoring, merging operational risk analysis with consequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and an integrated system involving risk monitoring, maturity model and internal audit. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn at *https://www.linkedin.com/in/luigisbriz* or at *http://sbriz.tel.*

The identification method used must satisfactorily identify (i.e., authentication) a subject to consequently recognize the person's right (i.e., authorization) to complete certain actions or prohibit them. Sometimes it is not necessary to correctly identify an individual who requires a service; it is sometimes sufficient to obtain an adequate guarantee of a legitimate use of the identification method assigned for access. That is, if the credentials presented are considered authentic or the device is recognized, then the operation is authorized. For example, if the cash withdrawal from an automated teller machine (ATM) is performed by someone other than the holder of the bank account, but the person is in possession of the correct account credentials, the operation is considered lawful because the identification is made based on the physical device and password. The account holder is aware of the consequences of a lost device or disclosed password and assumes accountability for the diligent custody.

The construction of a realistic identity to be used on the Internet cannot be limited itself to a mere technological solution; it must include an abstract representation of the personal behaviors and distinctive characteristics of the individual. Furthermore, the characteristics to consider may have evolved with technology and may require periodic adjustments if they change over time. The primary reason for ensuring that an identity is constantly up to date is to counteract its falsification or misuse. Such a threat may appear in the form of a deep fake, which alters the human form in a graphic representation of the real world, making it difficult to verify the authenticity of the presented identity.

There is no single solution for managing identity recognition on a network. The proposed method will distinguish between two types of identity registration based on different complexities and characteristics.

1. Registration of a complete, secure, certified identity, to be of reference for other identities. To guarantee these properties, the certification of an authority is required, and, therefore, it will not be possible to resort to an entirely online procedure. Physical recognition is necessary to give value to the registration itself and activate the consequent certified online identity.
2. An identity that is easily used for daily activities and its application must be stress-free, fast and secure. It is used exclusively online and certified by the first type of identity.

Before explaining the network identity management scheme, it is helpful to analyze the different identity registrations used in daily life to understand how many different situations and solutions have been adopted for the same purpose: to recognize the identity of a person.

Contexts in Which Identity Is Required

In everyday situations in which it is necessary to demonstrate one's own identity, identification is mainly managed with physical documents issued by government bodies or electronic credentials issued by organizations' systems that authenticate the validity of the credentials. Some of the most common examples are illustrated in **figure 1**.

There are countless other situations in which a user profile is created and authentication credentials are issued, although each circumstance may have different requirements for identification. It is also worth noting that not all requests for personal data are regulated on a need-to-know basis. The principle of need to know is a basic concept of information security, and it requires that only necessary information is processed; collecting unnecessary information can compromise privacy.

Registrations and Personal Profiles

One concern related to the high number of identity recordings that occur on a daily basis is the repeated provision of personal data to service providers. This can become habitual to the average user and lead the user to pay less attention to the circumstances surrounding data collection. Recording personal data at a higher frequency exposes data to risk, and it also often means that there is not a clear explanation of why the data need to be provided and how they are being used. In addition, in the case of termination of a service that required personal data, data are not always promptly deleted according to the planned (contractual and legal) terms, exposing them to risk of unauthorized or illegal use (e.g., identity theft).

The countermeasure to the problem of the number of registrations and the amount of personal data entered is the use of a trustee who has custody of the personal data and has the right to operate in a controlled ecosystem made of technologies, protocols and operators of proven trust.[1, 2] The only guarantee of the real and complete identity of a person is the government entity that manages the legal identity and provides physical identity cards. This does not mean that there must be a single physical database containing all classes of personal data, such as personal, health, judicial, school and employment, only there is a single access control system for government databases.

In practice, it is like having access to a virtual database of legal data, managed by a trusted state custodian (i.e., government agency) that has the authority to regulate the registration operations of

LOOKING FOR MORE?

- Read *Identity and Access Management Audit Program. www.isaca.org/iam-audit-program*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 1

Types of Identity in Daily Life

Document or Process	Identity	Characteristics
Passport	Digital but static (renewed after a number of years)	It can be reduced to an object composed of two parts: the information related to the subject's public identity and that which can be accessed by another country. Public data are partially visible (e.g., personal information, photo), while the biometric data of the person and integrity of the physical document are accessible via digital signature.[a]
Identity card	Digital but static (renewed after a number of years)	It is a reference document depicting a person's identity, but it is made for manual use, and although it has data in a digital format (e.g., magnetic strip, reading chip, holographic), it is not structured to be used with current technologies and the evolution thereof.
Driving license	Digital but static (renewed after a number of years)	It is formed by two types of information, one of identity and the other of specific driving qualification data. The latter data are the objective of the document but only in combination with the correct identity.
Social security number (SSN)	Static, electronically readable	It is a unique code associated with an individual for tracking activities conducted by public administration or government entities. It has no identity authentication goals; it only points to a person's data. It is sometimes required on websites to reduce user duplication.
Bank credentials	Digital, dynamic, strong authentication	Now more prevalent for digital banks, these vary in relation to the evolution of security technologies but do not directly authenticate the person. Rather, they are self-referencing; they verify that the credentials themselves are really those assigned. Separately, each bank or payment circuit retains the identifying data of the person and the risk profile.
Fidelity card	Static, electronically readable	Although nominal, it does not aim to recognize a person, but rather to direct the viewer to the buyer's purchasing data. The need is to identify the purchase profile that could also be associated with a group of people, such as a family.
Smartphone	Subscriber identity module (SIM) card and device ID	The SIM card is an integrated circuit that stores the phone number (i.e., international mobile identity), even before that of the person. There is no guarantee of the identity of the user, but the authentication of the device is guaranteed by valid international regulation, similarly to the eSIM,[b] a programmable SIM card that is embedded directly into the device.
Voting procedure	Physical recognition	Generally, authentication by an identity document is required before a person may access the voting booth. This is the most secure process, but requires voters to physically access the polling station.
	Postal voting	The postal vote is based on the principle of the double envelope, an external one for the sender identification, and an internal anonymous envelope to preserve the confidentiality of the vote. The check is on the consistency of shipping data and the integrity of the envelopes used. The counting process is slow and does not provide sufficient guarantees on the free expression of the vote.
	Remote electronic voting	Remote electronic voting (via the Internet) uses the same concept as postal voting. The physical envelopes are replaced by encapsulated digital messages. The external one is digitally signed by the voter and the internal one is anonymous. It is an effective technological response to the slowness of the physical counting of votes, however, the free expression of the vote is not verified and there is the risk of computer fraud.[c, d]

Sources: a) International Civil Aviation Organization (ICAO), "Public Key Directory: Secure Cryptographic Authentication of Chip-Based Traveler Information," *https://www.icao.int/Security/FAL/PKD/Pages/default.aspx*; b) GSMA, "eSIM," *https://www.gsma.com/esim/*; c) American Association for the Advancement of Science (AAAS), "Internet or Online Voting Remains Insecure," USA, 10 March 2021, *https://www.aaas.org/epi-center/internet-online-voting*; d) e-Estonia, "i-Voting—The Future of Elections?" 6 March 2019, *https://e-estonia.com/i-voting-the-future-of-elections/*

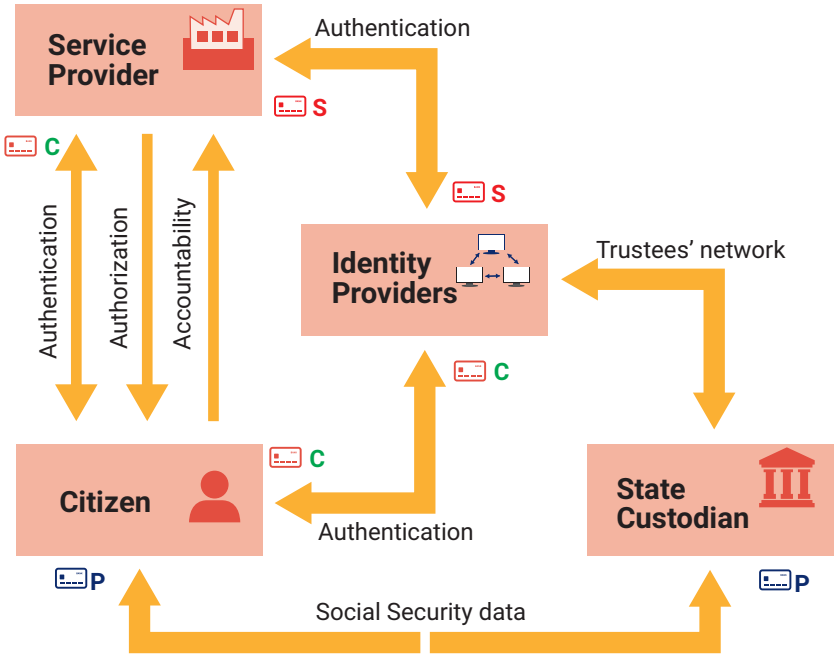
the legal digital identity of citizens to release the personal digital certificate (**figure 2**) and guarantee confirmation of legal identity to the subjects who require it for a legitimate reason.

Schema of an I-Identity Solution

Technically, to securely recognize a user on the Internet with a mechanism that guarantees reliability and practicality, it is necessary to resort to federated digital identity systems. They must be built on open authentication standards, for example OpenID Connect 1.0 (OIDC),[3] which adopts the OAuth 2.0 authorization protocol based on the exchange of tokens,[4] but there must be the possibility of adding appropriate extensions, such as the categorization of identity providers. Suppose a person (i.e., citizen) needs to create a user profile to access a new service (i.e., service provider). As an alternative to the classic

FIGURE 2

Scheme of Identity Recognition on the Internet



submission of personal data with a copy of an identity card repeated on each website accessed, it is more efficient to have an online mechanism entirely based on digital certificates issued by a certification authority (i.e., identity provider) that guarantees the integrity of the information received by a public authority (i.e., a state custodian). Each person would need a personal digital certificate (P) to manage relations with the public administration and one or more common digital certificates (C) for daily activities. The digital certificate is a mix of information about the person, the device and the trusted organization that issues it and signs it by encryption.

The personal certificate (P) is issued by a public authority (i.e., state custodian) following physical recognition by a local authority relevant to the residence of the citizen. The state custodian can be thought of as a tree structure: The top are the data and the roots are the government agencies that provide the private certificates, including the authorization of access to personal data categories based on the applicant's authorization profile. For example, for roadside control, all of a driver's personal data relating to demonstrating the ability to drive a vehicle should be available to law enforcement. In general, all the data necessary for public social and civil services would be available to the respective public control bodies. A centralized blockchain records all the identification queries for any forensic analyses, while analysis tools of network traffic verify the certificate by combining applicant, authorization class, device, type of data and data classification information to create alarms and report excesses or data processing abuses.

The common certificate (C) is then issued by its public identity trustee (i.e., identity provider) following online recognition by the public authority (i.e., state custodian). The state custodian, as guarantor of the highest-level identity, interacts with public identity providers on a special overlay network. They return a class of personal data following the authentication of the private certificate. This allows the identity provider to create the username and certificate to use in public and send it to the applicant. It is likely that this operation would require a payment.

With the public username and the common certificate, a person can create a profile with the service provider. In the registration form, the username and, as an alternative to the password, the common certificate can be used with a selection of personal data communicated automatically (e.g., name, address, birthdate, gender). The data available are restricted to those owned by the identity provider that do not exceed those present in the physical identity card. To send more data, it is necessary to define a broader mechanism, which would be regulated by an international standard created for the circumstance and involve a state custodian.

The service provider automatically sends the applicant's certificate (C) to its identity provider in addition to its own certificate (S). This validates the identity of both the applicant and the service provider. Therefore, the applicant is automatically informed of the registration of activities to demonstrate the legitimacy of the actions carried out. At this point, the service provider system grants privileges and permissions to access the data.

This identification scheme is secure because it is based on the recognition of the device (included in the certificate), the network address of the applicant (included in the authentication package), the ability to contact the certificate issuer (for integrity verification) and the robustness of cryptographic keys (encryption of the communication channel and data). The strength of the mechanism is linked to the possibility of making immediate controls for these factors with a choice of technology adequate to each of them. It is a form of defense in depth (DiD), with verification of the origin of the request (device, address), the identity of the issuer (certificate), the correctness of the recipient (consent) and the integrity of the messages (encryption). The effort is focused on the contrast of false identities.

This identification scheme can be generalized by removing the constraint of the identity provider for applicant and service provider. Both can authenticate themselves on their own identity providers and almost nothing will change except for an exchange of certificates between the two identity providers to ascertain the validity of the certificate issued by the other provider.

Schema of an I-Voting Solution

Another possible application relating to the certification of a person's identity is online secure voting. In general, electronic voting (evoting) presents various methods aimed at simplifying the expression of the vote and the rapid counting of votes through electronic and/or computer technologies. Among these are the methods that are implemented through the Internet (I-voting), with the aim of proposing a process that combines the most widespread communications medium in the world, the Internet, with the basic requirements of a public vote. The four primary requirements to vote are the right to vote, freedom of expression of the vote, the certain identity of the voter and the secrecy of the vote. The right to vote requires that there are no impediments to the vote itself. The difficulty in accessing the site and where the electoral booth is installed can make a difference in participating in the vote. Developing an application to vote via the Internet (I-voting) based on digital identity certified by a network of identity trustees requires more than just a technical effort; it must be combined with remote control procedures managed by operators.

The main components are all available, they just need to be put together. There are protocols to manage authentication and there are also artificial intelligence (AI) programs to recognize a person via webcam; however, the requirement linked to the freedom of expression of the vote still requires human judgment. The software should be open source, and remote human control should guarantee aspects related to the freedom of the vote. A voting application available to download to a smartphone could have several features (**figure 3**) to safeguard the criteria required for a safe and effective voting process.

The proposed mechanism at the device level could work as follows. The voter, through the smartphone application and using an encrypted connection, is authenticated with the personal digital certificate issued by the state custodian. The facial recognition software, drawing on the custodian's personal data, evaluates the physical identity and acts as the first filter to allow access to the virtual electoral office. This is a call center of selected people with the same criteria as a physical electoral station. Each operator can interact with more voters simultaneously and has at least one supervisor who monitors their activities. A brief set of text instructions informs the voter of the need to enable the operator to take control of the device—in particular, the room and microphone, but without being able to see the contents of the virtual voting card. If the voter agrees, control of the voter's environment, including the camera and microphone, is enforced and the vote begins.

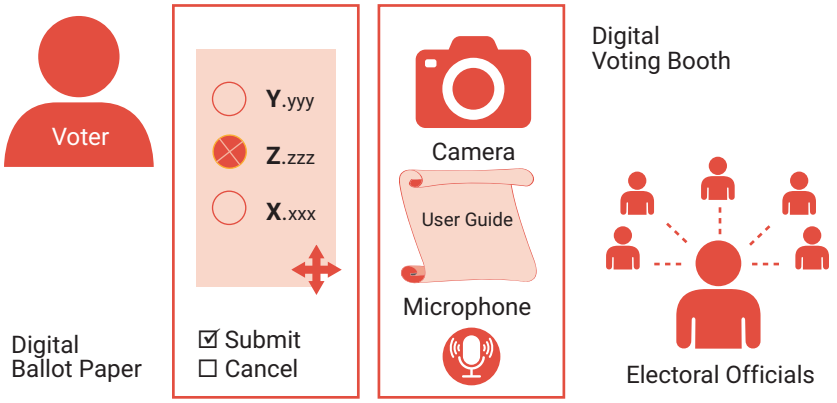
This proposed solution has many similarities to physical voting. The voter is recognized before accessing the vote, and the virtual electoral office, through the control obtained by operating the device, guarantees that the voter is free to act without the influence of others. The remote operator is always prevented from viewing the operations on the voter's screen, guaranteeing confidentiality. As a further guarantee, it would be appropriate to allow the voter to change the presentation layouts of candidates to prevent an external observer from inferring the selections of the voter by observing the voter's hand movements. The operator can block the voting operation in the event of an infringement of the electoral rules. After completing the selections and confirming the vote, the smartphone is unlocked and the voter can use it again with full freedom.

Options for the Electoral Station

Even if a smartphone application were created, an in-person voting option would still be necessary for anyone facing obstacles such as cost, lack of familiarity with the use of smartphones, or distrust in the application solution, or simply because a backup solution is necessary. To set up an electronic voting booth, desktops, laptops or tablets can be used with a version of the software that, if present,

FIGURE 3

Voting Scheme via Smartphone Application



The proposed mechanism of digital identification aims for a balance between the complexity of the necessary technological components, the process of managing identity providers and ease of use for the user.

disables the camera, microphone and keyboard, but enables the mouse (or touchscreen). Deactivation works because the control is implemented by the electoral officials, while the software module of the voting event remains unchanged. To be able to use any computer without changing its configuration, the software must be installed on a removable and bootable device, managed by authorities only to avoid tampering with a voting booth identifier certificate. The voting operation is activated by the electoral officials sending an enabling message to the voting booth (e.g., via wireless Bluetooth) composed of the identification code of the voting booth, the SSN of the voter and the certificate of the electoral official. When establishing the polling station, the devices used by the electoral personnel and the necessary digital certificates are distributed.

To facilitate anyone unable to access the polling station, a mobile voting booth can be created using a tablet or a laptop in accordance with the procedure for setting up a polling station. The dedicated electoral staff should reach and recognize the voter, enable the voting device, deliver it to the voter (or their legal trustee) and ensure the confidentiality of the vote. At the polling station, it is also useful to prepare a simulation booth of the voting operations to aid situations in which there is a lack of digital culture.

Conclusion

To effectively manage the identity of a person on the Internet, a solution must be easy to use, and it must be secure to avoid counterfeits. It cannot always be entrusted exclusively to technology because sometimes human input is required, as in the example case of I-voting. At the same time, the solution must guarantee a legitimate level of anonymity to avoid excessive use of personal data, to limit the impact of identity theft, and to be compliant with privacy regulations. For physical documents, the origin of personal information is under the protection of government agencies so that there is a referee who can enforce regulation in the event of disputes and, similarly, protect the party that provides services.

The proposed mechanism of digital identification aims for a balance between the complexity of the necessary technological components, the process of managing identity providers and ease of use for the user. The use of a government agency as a custodian of the original data related to the identity of a person is nothing new. Such a practice should not be considered a loss of individual freedoms, because it is analogous to what already exists and is the basis of the organization of social life. Technology is simply an excellent means to make this process of using a digital identity more efficient. The use of digital documents is a sustainable solution in terms of resources and practicality and is suitable for use on the Internet. For daily network activities that do not require the certainty of identity, it is possible to use simplified identities (managed by identity providers) in addition to the legal personal identity (managed by the custodian). The management of this process does not require a complex system. It only requires a network of identity trustees capable of providing flexibility to accommodate the peaks of demand, ensuring the resilience of the service and guaranteeing security.

This ecosystem of technological infrastructures, protocols and operators, guaranteeing the reliable and practical recognition of a person, allows for better security on the network, lower costs and fewer disputes. In general, the reliability and security of a digital identity system can also be a boost to create new egovernment services to include citizens in a more eco-sustainable and efficient technological environment.

Endnotes

1 Sbriz, L.; "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 1," *ISACA® Journal,* vol. 2, 2022, *https://www.isaca.org/archives*

2 Sbriz, L.; "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 2," *ISACA Journal,* vol. 2, 2022, *https://www.isaca.org/archives*

3 OpenID, Specifications, *https://openid.net/developers/specs/*

4 OAuth, OAuth 2.0, *https://oauth.net/2/*