A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 2

Identity Trust Service Implementation

Disponibile anche in italiano
www.isaca.org/currentissueforums

Identifying a physical person on a network using their digital name (username) is a task made possible by the authentication system. The system first recognizes the validity of digital identity and then associates the personal information it received during the subject's registration. In many other situations, only the validity of digital identity is sufficient to activate a service; for example, a free subscription to a newsletter via email. Unfortunately, additional and unnecessary personal data are often required to obtain a service and adequate data protection measures are not offered. Those who require data assume to have the right to do so, justified by the lack of alternative identification methods, and those who deliver data do not have the time or ability to verify the effectiveness of any guarantees offered, including legal ones. Further, there is no guarantee of the effectiveness of the control on the recorded data; for example, sometimes a photocopy of an identification (ID) card is enough to activate a new digital identity. But what if the photocopy is stolen?

This approach must be rebalanced with symmetrical recognition between the two parts that must be identified. The proposed method assigns equal rights to each party and requires mutual recognition based

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

Has been the risk monitoring manager at a multinational automotive company for more than seven years. Previously, he was responsible for 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 an operational risk analysis with a 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://it.linkedin.com/in/luigisbriz* or at *http://sbriz.tel.*

on the guarantee that identity has been established by two trustees; because there is one trustee for each party, this method is called the double trustee.

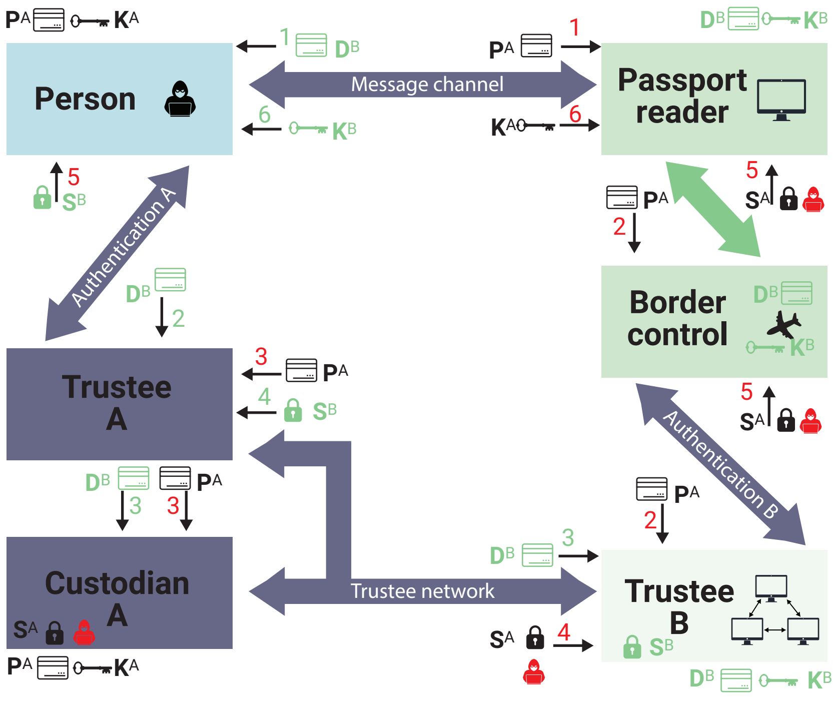
Implementation of a means of managing digital identity based on the concept of identity trust, as discussed in part 1 of this series, “Identity Trust Abstract Model,”[1] is best described by using a complex situation from real life as an example. Passport control is an excellent example because it encompasses several challenging issues, including organizing the network of trustees on two levels, managing multiple points of authentication for complex entities and considering the international enterprises managing the network of trustees.

Passport Control Example

The airport represents a typical complex entity in the sense that it delivers an identification service for innumerable recognition stations, coordinated by a command center of operations. Each station must have the ability to completely fulfill all identification formalities in compliance with strict rules. All passports are equipped with microchips that contain the person’s information and is used to automate the process (i.e., making some information available to automatic control readers). Other information can be requested from the airport authorities to those of the passport emission country.

FIGURE 1

Symmetrical Identification Scheme With Physical Identity



The passport verification process represented in **figure 1** can be used as an example to understand symmetrical identification schemes with physical identity. Furthermore, the need-to-know principle (i.e., a user is only allowed to access a resource when they have the right level of security and operational need), typical of personal data protection, will be continuously applied, both to minimize the risk of improper use of data and to allow a more efficient process (no redundancy).

Physical identity is guarded by a trustee called custodian. The custodian has the legal authority to carry out the physical identification of the owner of the digital identity and protect the related personal data. Therefore, in the trustee network there are two types of nodes: the custodian of the physical identity, who manages personal data, and the trustee of the digital identity, who manages the authentication of the username that circulates on the network. Each entity can request more than one digital identity, either from the same trustee or from different ones.

At the airport, the national border control authority is responsible for performing passport control through various physical passport reading stations that are either automated or manned by personnel. For more effective management, this authority role must be identified as a single entity by the trustee. Therefore, a single electronic identity card is issued to the authority in the airport and is managed by a central system that acts as a hub for all passport readers located in the airport. All passport control stations in the airport share the same credentials present in the central system, except for the necessary distinctions related to the physical address on the network and the device identification. The badge has selectors to indicate whether the sender is an entity or a device (consequently, some predefined optional fields have the coordinates of the hub system, as only the latter can interact with the trustee).

The person should be equipped with a smartphone for access to the trustee. Otherwise, the passport microchip can be used, but the level of security will be lower because the mechanism is not symmetrical. The identification process between the person (P^A badge) and the passport reader (D^B badge) begins with a QR[2] code at the passport control station, or with similar contactless technologies. The QR code is a simple URL associated with the passport reader that can be scanned to view the information form and request consent to send personal data (this step activates the exchange of badges). The six stages of identification are as follows:

1. The person uses a smartphone to exchange digital badges (P^A and D^B) with the passport reader. The person updates the badge with authentication on their trustee. Among the data communicated to the trustee, there is a flag requesting that the person's physical identity be sent to the passport reader. The passport reader has a copy of the airport badge (digital identity) that has been provided by the border control hub system, which received the badge from Trustee B. A predetermined aging policy regulates how often the badges of all active readers need to be updated.
2. The person's smartphone and the passport reader send the badge received from the counterparty to the trustee. The D^B badge goes to Trustee A (and automatically includes the list of categories of personal data to be communicated), and the P^A badge goes to Trustee B, forwarded by the control authority's hub system.
3. The two trustees exchange the digital badges (P^A and D^B) received from their own entities. As soon as Trustee A receives the P^A badge confirming that the D^B badge is authentic, it forwards the two badges to Custodian A. The P^A badge is used for the integrity test, and the D^B badge is used to access the data of Trustee B and its applicant. The custodian may also refuse to send personal information if the custodian believes the recipient does not offer sufficient safeguards.
4. Trustee B prepares the S^B seal and forwards it to Trustee A. Custodian A prepares the S^A seal and forwards it to Trustee B. All the seals are of a standard size, even though they may not include all personal information required. This keeps the information more secure because there is no apparent difference between personal and digital identity seals. It is more difficult for a malicious observer of network traffic to identify personal data when standard-size seals are used. However, when data exceed the standard size, these missing data are accessible to the recipient via a link and a cryptographic key (specific to the passport reader), appropriately inserted into the seal.

> "The goal is not to make it impossible to access the data but to delay the usability of the information until the identification is accepted or rejected."

5. Trustees forward the seals to entities without taking any further action. In the case of the S_A seal, the receiving entity is the hub system of the border control authority, which forwards it to the correct passport reader.
6. As soon as the seals arrive, the person's smartphone and the passport reader exchange the digital keys K^A and K^B to open the seals. The passport reader retrieves any additional personal data if there is not enough space in the seal for the complete message.

The process seems complex, but, in reality, only a few operations need to be carried out, and they are computationally simple. It may seem easier to simply read the microchip in the passport, but the information it contains is not verifiable in a short time, and it cannot effectively manage updates. The personal data badge contains the indicators for the categories of personal data to be sent. These categories, intended as blocks of data, must be codified according to an open standard to produce easily interpretable messages, such as via the Multipurpose Internet Mail Extensions (MIME) protocol.[3] This is a simple method used to encapsulate different contents and associate them with an address that includes the name of the data subject, a separator sign and the domain name of the identity provider. The data categories to be sent are selected in the submission consent form. Examples of categories include personal data, health data (e.g., vaccinations, blood group, allergies) and passport information (e.g., number, photo, emergency contacts, active visas). The default is to send only the real name, and each block of additional data requires consent.

Implementation Considerations

Each data subject may have multiple digital identities; therefore, the device used in the identification process must include a digital identity safe to

> "To counteract interception, badge, seal and key messages must have a standard fixed length, regardless of the amount of information they contain, and they must be encrypted."

contain them. During the authentication phase with the trustee, this safe should be updated with the current identification data on the device network and the identity recognition data required by the authentication process. The communication channel should always be encrypted, and even though this is not an absolute security measure, it should be implemented to strengthen the protection against unauthorized attempts to listen in on data traffic. The goal is not to make it impossible to access the data but to delay the usability of the information until the identification is accepted or rejected. Each new authentication invalidates the previous information by updating the recognition credentials.

Digital identity should be represented by a username created in the form of an email address. An example is "avatar_name@trustee.home," with "avatar_name" the name chosen to identify the entity in cyberspace, "trustee" the name of the domain associated with the trustee and "home" the International Organization for Standardization (ISO) standard ISO 3166-1 *Codes for the Representation of Names of Countries and Their Subdivisions—Part 1: Country Code* alpha-2 code[4] of the registered office of the trustee's country. The digital identity protects the personal data of the actual entity, but the trustee cannot be only virtual. To ensure that the data of entities are fully protected, trustees must be public entities with legal constraints.

The recognition process starts with the identification form, issued by one of the two parties, but instead of the password field, there is a selection of possible identification methods. Examples include a password, a trusted digital identity or a strong authentication mechanism. The same identity can be used with multiple identification mechanisms, configured *a priori* and chosen on the basis of the accepted risk level. The general steps to verify digital identity are as follows:

1. The username (name of the e-identity) is entered.
2. The type of identification is selected (with or without sending personal data).
3. The credentials are updated with the trustee or those in the safe.
4. The device automatically sends the badge, waits, and sends the badge of the other entity, waits for the seal, opens it and sends the key to the other entity.
5. If the seal opens, the identity is confirmed; otherwise, the process is interrupted.

The functional model of the identity provider can be based on existing frameworks, such as the Security Assertion Markup Language (SAML),[5] which allows the creation of a federated single sign-on (SSO) system. The communication mechanism between different identity providers must be added; therefore, the name of the chosen identity provider must be added to the name of the data subject.

How to Address Abnormal Situations

In any node there can be a nonacceptance of the message circulating due to misalignment of information or integrity problems. The process stops in the first node where any abnormal situation occurs and the lifetime of the cycle is exceeded. In each node, the continuation of identification is cancelled without releasing any message. The failure to send negative feedback following an anomaly stops the dissemination of indicators that the credentials may be being used by malicious subjects. Cancellation for whatever reason requires the restart of the verification cycle with the issuance of new credentials.

To counteract interception, badge, seal and key messages must have a standard fixed length, regardless of the amount of information they contain, and they must be encrypted. The strength of the encryption is less important than its efficiency. The encryption should last only as long as necessary to complete the identification cycle. Any restart will take place with new credentials.

Issuance of a New Digital Identity

The custodian is the legal manager of personal data, appointed by a governmental authority of the country where the person requesting a digital identity maintains a legal residence. This activity involves the recognition of the real person and a first device, which is the master. The custodian proceeds with the person's recognition either through the physical presence of that person or the online presentation of official identity documents. Additional devices can be added for confirmation via the first device. The master can be replaced by one of the other devices through a simple automated online procedure. Periodically, personal identification data, such as passport photos, must be updated according to a schedule established by the governmental authority, or more frequent updates may be required by the custodian in the event of high risk or accident.

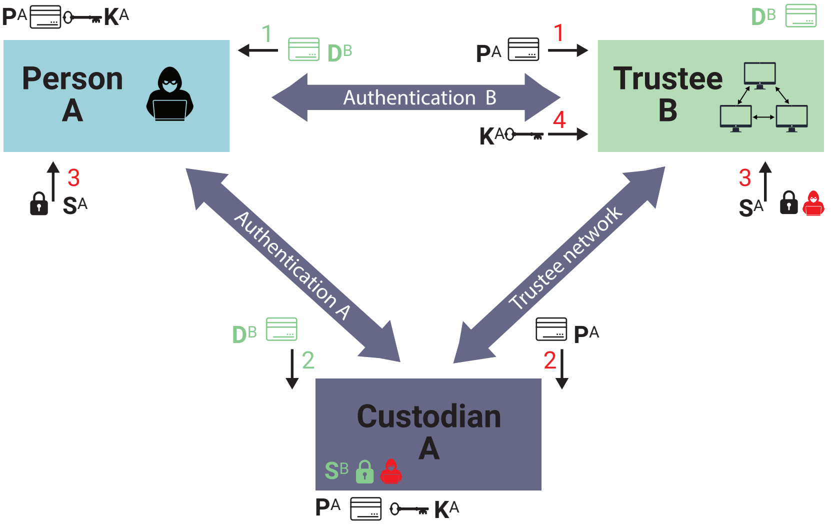
The preparatory phase of any eidentity request is the registration of personal data with the custodian, which issues a digital P^A badge that can later be registered with any trustee. The P^A badge is identified by a username in the format "hex_string@custodian.home," where "hex_string" is a fixed-length sequence of random hexadecimal characters defined by the custodian. It does not contain any reference to either the person or the date of issue and can be revised on request to the custodian. A prefix-type format linked to a control code is suggested, which can be easily constructed from "MOD 13 prefix" (or some other module[6]) to intercept a possible entry error.

Once the personal badge (which contains no personal data but consists of a digital identity guaranteed by the custodian) has been received, one or more digital identities can be requested. The creation of a new eidentity takes place in four phases, as **figure 2** illustrates.

1. Person A sends Trustee B the digital badge P^A issued by Custodian A and receives the badge D^B. The P^A badge contains a flag that defines this message exchange as a registration with a trustee. The proposed username contains the domain of the trustee.
2. Person A and Trustee B, respectively, send the D^B and P^A badges to Custodian A. The D^B badge contains an information field with the new username chosen by Person A.
3. Custodian A prepares the S^A seal with the registration data of the natural person, as defined by the standard.

FIGURE 2

Creation of a New Digital Identity



4. Person A and Trustee B receive the seal, and upon receipt, Person A sends key K^A to Trustee B to open the seal.

Digital identities are managed by trustees, so it is reasonable to expect to incur an annual subscription cost, similar to the cost of acquiring a domain name on the Internet. This management system avoids excesses both in the number of identities owned and in the frequency of identity renaming. A decommissioned identity must remain archived to allow traceability of the owner for a sufficient period to ensure that there can be no fraud related to identity exchange. Blockchain managed by trustees guarantees a temporal log of registrations, cancellations and identification operations that may be needed in the event of forensic activity. The trustees can be the same entities that manage the sites' domain names or the managers of public mail servers, but they must be subject to specific security certification to protect the entities that register their identities. Therefore, an international supervisory authority for trustees is essential.

> "The use of double trustees addresses the mutual recognition of two entities without the prior registration of personal data on each new authentication system."

Conclusion

The use of double trustees addresses the mutual recognition of two entities without the prior registration of personal data on each new authentication system, thus maintaining anonymity. In addition, it helps authorities combat fraud resulting from identity theft, as absolute anonymity is not possible when entering into contractual agreements. Contractual relationships necessitate the informed sharing of personal data. Therefore, digital identity does not represent the actual name of a physical entity, but it provides a means for local authorities to trace the trustee and, from this, the custodian. Only the authorities of the custodian's country of residence or one of its entities have the right to access all personal data.

For this mechanism to be effective, it is essential to establish a single international authority with the power to regulate the work of trustees, the format of messages, the management of the trustee network and the governance of controls. This authority must preserve the quality of the service and enforce an ethical code to protect the identified subjects. Trustees must carry out their duties with the utmost transparency. Their primary responsibility is to ensure the authenticity of messages; no further processing of personal data, other than that required to identify the entity, can be allowed, and user profiling must be expressly prohibited. Furthermore, systematic control of the trustee's activities by external certification bodies is useful to maintain the overall climate of trust in the operations carried out. In addition, custodians should be subject to periodic privacy audits of the data processed by legally competent authorities.

The problem of excessive use of personal data has been addressed by demonstrating ownership with the use of a specific username at a given time. This method promotes anonymity, as it excludes the other party from accessing personal data without consent and assigns the criteria for tracing the real data to a guarantor of digital identity, with the sole intent of preventing any form of abuse. In effect, this is a controlled loss of anonymity. People's actual identities cannot be used without their knowledge, but, at the same time, they are not completely anonymous because the legitimate authority can trace them. On the Internet, freedom is sacred, but it is always balanced by responsibility for one's actions.

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] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 18004:2015 *Information Technology—Automatic Identification and Data Capture Techniques—QR Code Bar Code Symbology Specificatio*n, Switzerland, 2015, *https://www.iso.org/standard/62021.html*

[3] Techopedia, "Multipurpose Internet Mail Extensions (MIME)," 1 February 2017, *https://www.techopedia.com/definition/1693/multipurpose-internet-mail-extensions-mime*

[4] International Organization for Standardization (ISO), ISO 3166-1:2020 *Codes for the Representation of Names of Countries and Their Subdivisions—Part 1: Country Code*, Switzerland, 2020, *https://www.iso.org/standard/72482.html*

[5] OASIS Open, OASIS Security Services (SAML) TC, *https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security*

[6] Gauss, C.; A. A. Clarke; *Disquisitiones Arithmeticae, English Edition*, Yale University Press, USA and UK, 2009