A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 1

Identity Trust Abstract Model

Disponibile anche in italiano
www.isaca.org/currentissueforums

The identity of an Internet citizen, or netizen,[1] is generally determined by asking the digital citizen to share personal data with the authentication system to obtain credentials to access data. But is it really necessary to disseminate personal data on the Internet, even on the systems visited only once? Maybe not. Investigating the concept of identity trust (i.e., the ability to establish trust for identities in the digital world) can help practitioners better understand the identification process.

Identity verification when accessing valuable resources, in particular for subjects coming from the outside of the information security management system, is essential. Identification is a key step in creating a reliable communication channel, which also includes the creation of the channel itself and the assignment of access rights to resources. Creating a secure channel and applying access rights can be consolidated processes due to the availability of mature technologies and secure protocols. However, the issue of identity verification still presents difficulties for determining a solution that is suitable to manage every possible scenario.

One possible solution is the double trustee, a method of identification that places the identified and identifier on the same level, creating a symmetrical scheme of mutual trust for their identities.

Digital Identity Recognition

The real challenge is to be able to identify a digital stranger without requiring a personal data exchange and using unnecessarily complicated mechanisms. Current identity recognition mechanisms can be grouped into two categories.

The first category can be labeled the single domain. It requires that the user to be identified is registered in an authentication system, which is part of a single digital ecosystem of shared resources. In the initial registration phase, the user must provide the system with the personal data needed to issue authentication credentials, whether they are simple, such as a password, or complex, such as a two-factor mechanism. The authentication system is a container of all identities and a collector of all access requests. It has no responsibility for establishing the veracity of the digital identity received; its only task is verifying the correctness of the identification credentials within its ecosystem. In this scenario, the validity of

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*.

credentials has more importance than the subject's identity. For example, when activating a subscription to a service, for the provider, it is more important to verify payment authorization than to verify the exact name of who paid.

The second category can be labeled the single trustee. It requires the presence of a third party, which acts as a trustee (identity provider), records the personal data of each entity and then guarantees their identity in the authentication process. Everyone must trust the identity provider and must provide it with the necessary data to properly determine identity. The identity provider is responsible for establishing the veracity of the digital identity (which corresponds to an actual entity) and verifying the correctness of the identification credentials. The use of this single trustee makes it possible to access different ecosystems of resources, not interdependent between them (the point of contact is precisely the single trustee), always with the same identity. However, the process is constrained by the need to share the same trustee, and, therefore, is not always possible. If two subscriptions are activated for two different service providers that use two different identity providers, identity must be provided to both identity providers.

It is not realistic to impose the same trustee to two entities (i.e., natural person, legal person or system) that are unknown to each other but need to interact with each other, such as for the supply of a service. By definition, the trustee must be chosen freely. Consequently, a more general mechanism is needed for any relationship between applicant and service provider without mutual knowledge *a priori*. The need to be recognized on new digital ecosystems, or access those where data are already known from new devices is constantly growing. In everyday life, services that require user recognition are innumerable, even if the guarantee of certain identity is not always an indispensable requirement. Some examples include paying for food delivery, sending a document to an organization, responding to a survey, accessing a bank online, participating in an online chat, buying a ticket to a show, booking a hotel room, confirming attendance at a conference or scheduling a medical examination.

Risk Related to Identity

Frequent use of digital identity creates risk, such as digital identity theft, which is often more serious than theft of a physical identity document because the theft is typically not discovered until adverse consequences occur. It can lead to legal or economic implications ranging from minimal to serious; therefore, it is not prudent to simply accept the risk. All activities that require identity verification have related risk, but they do not all use the same solution to mitigate that risk. For example, services that require a payment have circumvented the issue by prioritizing checking if a credit card is active rather than claiming recognition. The risk is thus transferred to the owner of the credit card. For other services, the driver for choosing the identification mechanism is the cost. This is a valid option only if the consequences have negligible impact.

> "All activities that require identity verification have related risk, but they do not all use the same solution to mitigate that risk."

Some services use identification as an excuse to require an abundance of personal data. Furthermore, the number of different methods or complicated methods lead to repeated requests for personal data on the Internet with low consideration of privacy issues and the principle of necessity. Therefore, users are expected to trust those who request the data without reassurance or transparency on how the data are being shared or used. Consent to treatment is not an authorization for the amount of data requested in the registration, it is a declaration of use according

to the purpose of the law, but it is a weak protection compared to the infinite opportunities of use.

The recording of personal data has nothing to do with the identification mechanism. Registration and identification take place at different times and are aimed at distinct tasks. The legal solution is to apply the principle of portability of digital identity (i.e., the right to avoid new repetitive recordings of personal data); however, there is not yet a practical mechanism to implement it. Furthermore, the identification of a digital identity should not be associated with physical identity except for situations of legitimate need and protection of the data subject.

A New Solution

There are pros and cons to each of the two categories of identification. The first category, the single domain, is efficient in ascertaining identity, but the complete registration of personal data must be repeated for each new authentication system, even when it is not clear how the data are used. The second category, the single trustee, has more application flexibility and technical complexity and manages to satisfy the request for identification with the right attention to personal data, provided that everyone recognizes the same trustee. Therefore, it is not applicable to all situations and is often limited to entities of a single country.

A different approach is needed. A method whereby both entities can trust each other through their own trustee, which certifies identity recognition without requiring the sending of personal data, except for data that are strictly necessary. This approach could be labeled the "double trustee".

The idea of a double trustee derives from the general principle of digital identification through a third-party guarantee of identity—that is, the mechanism must guarantee trust in the veracity of the digital identity itself while the personal data are used only in legitimate circumstances. Furthermore, the method must go both ways because trust must be mutual. This means that if a user identifies with a system, the system must also identify with the user. Before proposing a method that meets these concepts and to better understand the logic, it is helpful to consider how this mutual guarantee of identity could be achieved in a virtual world such as the Internet.

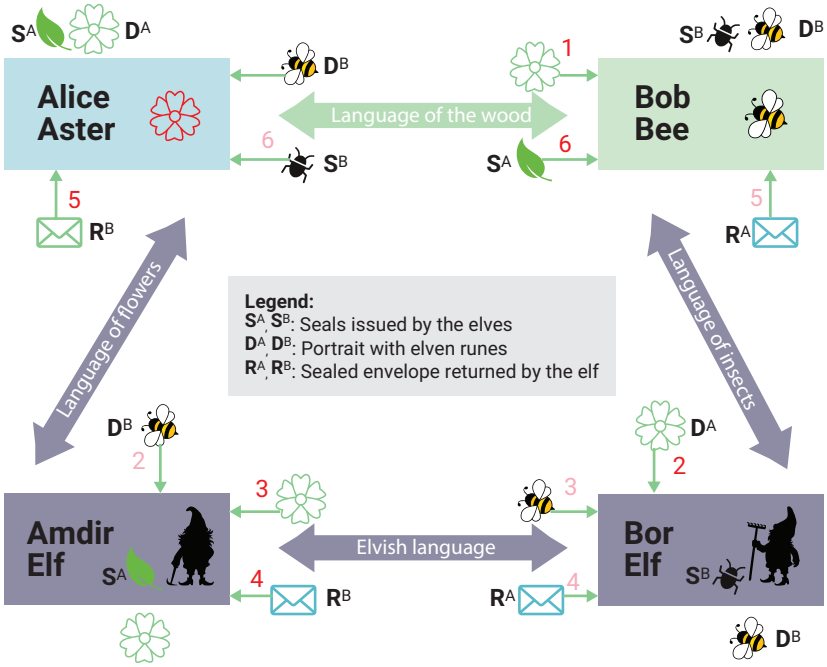
"The idea of a double trustee derives from the general principle of digital identification through a third-party guarantee of identity."

Example of the Wise Elves Forest

This fantasy-world example is based on an enchanted forest of wise elves. The animals and plants live a harmonious life in continuous interaction with each other. Relations between the different species are entrusted to the arbitration of the community of elves. Each elf is responsible for civil coexistence for a specific species and, ethically, is able to protect their interests relative to others. The elves communicate in an ancient language known only to them, called Elvish. In this example, there are two elves: the elf of the flowers Amdir (supervisor) and the elf of the insects Bor (trusted person) (**figure 1**).

Other inhabitants of the forest included in the example are Alice Aster, a flower that produces an exclusive pollen, and Bob Bee, an insect that produces a renowned honey. In this example, Alice and Bob do not know each other yet. Bob needs to buy the particular

FIGURE 1
Example of Identification Schema



pollen produced by Alice, while Alice must sell just to Bob, due to family tradition of the Aster with the Bee. To ensure that they can be certain of each other's identity, the trust guarantors, the elves, come to their aid.

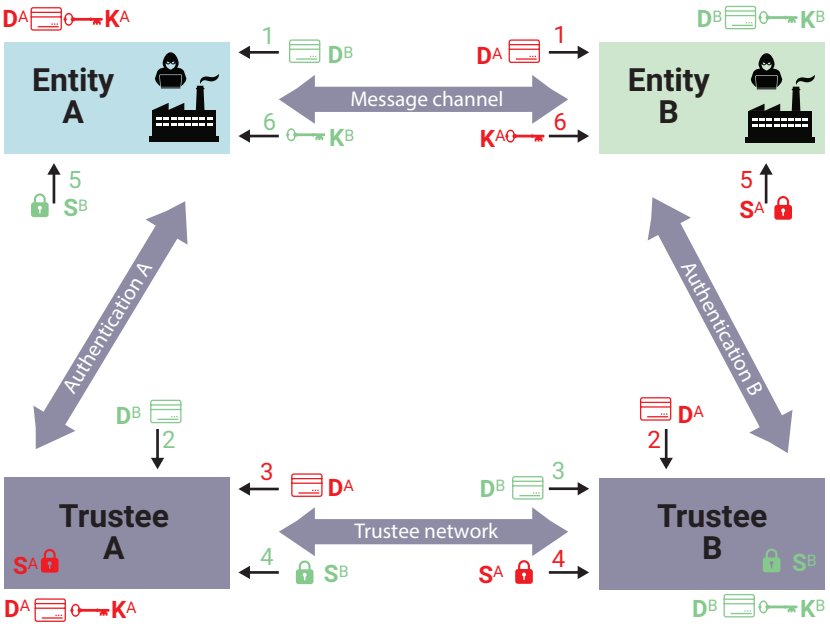
In phase 1, Alice and Bob exchange photo identification (D^A and D^B), made and signed by their trustee elves: Amdir for Alice and Bor for Bob. In the back of the portrait, in the language of the elves, there are additional details about Alice and Bob and the names of their trustee elves with their own seals. In phase 2, Alice passes the portrait of Bob to Amdir so that, in phase 3, Amdir can contact the elf quoted in the back of the portrait, Bor, to verify Bob's identity. Similarly, as a mirror image, Bob passes the portrait of Alice to Bor to contact Alice's trustee, Amdir, to verify Alice's identity. In phase 4, the trustee elves confirm, or reject, the identities with custom-sealed envelopes. Alice and Bob know the seals of their respective trustee elves because every morning the elves visit their protégés and leave an updated copy in case the seal has changed.

One elf's answer is not read by the other elf because it is passed within the sealed envelope. In phase 5, the trustee elves forward directly to Alice and Bob the sealed envelopes. If the seals are intact and correspond to the copies held, their mutual identity is confirmed. Then, in phase 6, seals are exchanged, confirming that the identification is complete and demonstrating that the information received is intact. Unfortunately, it is unknown whether Alice and Bob are who they say they are because no one is able to intercept or understand all the messages exchanged. However, Alice and Bob know the truth about the identity of the other and business can be conducted.

To understand how robust this identification scheme is, consider the example of Bad Wasp, of the insect family, who is one of Bob's competitors. Bad is fraudulently trying to buy pollen as Bob. If Bad tries to fake Bob's photo identification, he will not be authenticated by Bor Elf. If he disguises himself as Bob and tries to hijack the shipment to Bob's home, he will still be exposed because Bor sends his messages directly to Bob. The integrity of the message is verified by both Bob and Bor. Even the attempt to falsify Bor's message cannot succeed because Amdir confirms the origin, and even if there was a way to deceive Amdir, the last recipient is Bob, who would know if the seal had been illegally altered. Each message is always verified, both as the origin and integrity, and on each path, there is a different language.

FIGURE 2

Symmetrical Identification Scheme



A Symmetrical Scheme for Certified Digital Identity

The example of how Alice and Bob identified each other can also be applied to two digital entities: A and B (**figure 2**). Digital identities can represent a person, an enterprise, a system or something else. It does not matter what they represent, just that they are a reference for something that really exists. Furthermore, the names of the entities should be built as email addresses. It is similar to whether the name of a tenant (email name) is associated with the address of the residence property (email domain). The property owner is an ideal subject to guarantee the identity of its tenants. In a computer network, the domain authentication system knows all the members of the network domain.

In this scheme, the two digital entities (A and B) are connected to each other by means of a communication channel and, at the same time, are able to authenticate themselves to their trusted system. Trustees A and B are the managers of their network domain S and recognize all the entities included. The two network managers are in contact with each other on a specific overlay network, which the entities cannot access. For this example, the two

digital entities belong to different network domains and, therefore, need a reliable mechanism to verify their identity. **Figure 2** illustrates the six phases of identity verification:

1. The two entities exchange digital badges, D^A and D^B. The badge is metadata that contain information on digital identity. The data contained there include at least the username, the address (Internet Protocol [IP] and media access control [MAC]), the name of the entity's own trustee and an information integrity marker generated by its own trustee at the time of authentication.
2. Each of the two entities sends the badge received from the other entity to its own trustee.
3. The two trustees exchange the digital badges, D^A and D^B, received from their own entities and containing the digital identification data of the other entity.
4. The two trustees prepare seals, S^A and S^B, to be forwarded to the trustee of the counterpart entity. The seal is encrypted metadata that require a key, K^A and K^B, to be opened, and it contains part of the badge data received for integrity checks. The key was sent to the trustee's own entity at the time of authentication.
5. The two trustees forward the seal received from the other trustee to their own entities.
6. The two entities exchange digital keys, K^A and K^B, to open the seal arrived from the trustee. The digital key is a token used to open the entity's own trustee's messages.

"The interception of messages is prevented by the presence of four distinct communication channels that operate on different paths and carry out integrity tests."

The communication mechanism is perfectly symmetrical, based on four nodes, two entities and two trustees. Each node has a mirror that completes the same operations, which are generally simple.

The greatest time is linked to transit of the message from sender to recipient. The entity and the trustee send and receive a total of three messages each. This process is as follows:

- Each entity, during authentication with its trustee, sends the data of its location on the network and receives its own badge in addition to the decryption key of the messages sealed by its trustee. Entities exchange badges with each other and then forward them to the trustee indicated on the badge. If they receive a seal from a trustee, they forward the decryption key to the other entity. If they receive the key from an entity, they open the corresponding seal and confirm the identity or not.
- Trustees receive messages, process responses and forward them. If they receive a badge from an entity, they forward it to the trustee indicated on the badge. If they receive a badge from a trustee, they forward their own custom seal for that badge to that trustee. If they receive a seal from a trustee, they forward it to the entity indicated by the seal.

Security Considerations

Security is guaranteed by the presence of several independent paths to convey messages, which are then subject to integrity checks using information that is partly incoming and partly located in the node already. The overall security level of the identification of the two entities is equal to the security level of the single authentication between entity and trustee. This mechanism establishes recognition of the entity, which is then guaranteed to the other entity. If a step fails, identification fails. Each entity decides with the trustee which authentication method to use based on the risk analysis for that identity. A wide range of solutions is currently available to satisfy every need in terms of both cost and benefit. It can be a simple password, a confirmation Short Message Service (SMS) or a more sophisticated method.

The interception of messages is prevented by the presence of four distinct communication channels that operate on different paths and carry out integrity tests. The way to communicate between the two entities is a choice imposed by the circumstances without guarantees on the level of protection. It does not represent a vulnerability because validation messages must pass on each channel, making any initial impairment useless. Each entity authenticates with its own trustee, on a secure channel and with a

predefined protocol. The trustees communicate with each other on a dedicated network with intrusion monitoring and a specific process for admitting new nodes. All nodes are selected after a preliminary process to ensure that they meet the specific requirements of that network. If the domains of the two trustees coincide, the mechanism is simplified because everything can be managed internally by the single trustee.

The exchange of identities can introduce fake nodes or false messages; therefore, the messages must pass a series of integrity checks to look for anomalies in the forged messages, consequently blocking the identification process if necessary. This mechanism of exchanged messages and cross-checks enables the trustees to recognize if the badge has been compromised, and it allows entities to recognize if the seals are not original. Furthermore, if a false badge manages to pass identity verification by the trustee, the response is still sent to the real entity (and not to the counterfeit one) because the entity's contact information is determined by the respective trustee during authentication.

The advantage is the security obtained by using information from different sources to carry out integrity checks. The information is saved statically, in the device safe, and must be regenerated periodically. A long retention period exposes the information to a greater chance of attack than information that is retained only as long as necessary for use and then loses validity. For performance reasons, the entity's authentication credentials with its trustee may be usable for multiple consecutive identifications or as long as risk conditions permit; then they should be updated.

Conclusion

The basic mechanism of the double trustee has many advantages, but there may be more complex situations that require an expansion of this solution. For example, instead of having an entity that delivers one or more services, a service may require an interface with many interchangeable entities between them, or, instead of using digital identities totally free of personal data, it may require the management of particular categories of personal data. For the latter case, it is possible only after the consent of the data subject is achieved and it occurs in a controlled mode to ensure the protection of such data. The practical implementation of a concrete and heterogeneous situation, complete with the protection of personal data in unsafe environments, is discussed in part 2 of this series, "Identity Trust Service Implementation."[2]

Endnotes

1 Merriam-Webster Dictionary, "Netizen," *https://www.merriam-webster.com/dictionary/netizen*

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*