Smart Insights

Digital ID and physical ID on a convergence path

In collaboration with:

TRUSTECH
PAY | IDENTIFY | CONNECT & SECURE
Incorporating CARTES SECURE CONNEXIONS

WHITE PAPER

Table of Contents

Author: Boris Loktev - bloktev@smartinsights.net

Publication date: September 2017

Published by Intelling, 9 - 13 rue Bel Air, 13006 Marseille, France
www.smartinsights.net-report@smartinsights.net

Cover page image's source: ourwindsor.ca

1. Overview

A critical problem in cyberspace is knowing with whom one is interacting. The secure transactions industry has developed methods to determine the identity of a person in digital space. Even though there are attributes associated to a person's digital identity, there might be attempts to change these attributes or even identities could be masked or dumped and new ones created. The industry has been developing many authentication systems and digital identifiers that address these issues. Solution vendors are still on an improvement path to reach global and verified identification systems, bringing solutions to privacy and security related to digital identity. So, how important is Digital Identity and what is it exactly?

Digital ID is an online identity, which is equivalent to the personal ID of a person or entity adopted in cyberspace. All the information collected online concerning a person or an organization takes part of a digital ID. The simple example is social media web sites: by updating a profile picture a user adds information to his/her digital identity. We are using web services almost on daily basis, for example, in order to make an online payment, which needs to be secure. Digital ID plays a crucial role for operations like this one. More precise and accurate the identification is, more secure is the operation. Year by year, the importance of digital identification is being one of the most discussed subjects. Because depending on the level of complexity of ID one can be more assured and will decrease the risk of a threat. However, hacker attacks are not something unusual nowadays. A digital identity is linked to a series of digital and physical identifiers, like biometrics (example: fingerprints), ID documents (example: passport), an email address, URL or domain name. Because identity theft is rampant on the web, digital identity authentication and validation measures are critical to ensuring web and network infrastructure security in the public and private sectors.

Nowadays online world is of a great importance and the process of identifying yourself in a secure way is becoming more and more crucial. There is an issue between the average users and technology experts, as users do not like the complexity, while experts are ready to cope with complex solutions to reach the desired security level. As a consequence, the identifying process must be easy and fast. That is why industry is bringing solutions for reducing the number of different IDs for one user. The goal is to reach the maximum convergence between the Digital ID and physical one. Personal details could be linked in every service used. This reduces the risk of invasion or loss of information. One ID – less information to remember.

Source: ca technologies

That is what has been happening in Estonia since 2002: every citizen in the country is being issued by the state with a smart ID card that allows having an access to numerous different services. With using only one ID an Estonian citizen can do bank operations, apply for medical services, pay public transfer fees, vote and even put comments on the local newspaper's website. All this is using one Digital and main ID. This high level of convergence could be envisioned as the goal of many states in a modern world.

All this information was mostly related to people. However, the ID of objects is becoming more essential every year. Typically, digital ID principles and methods are experiencing a convergence phase between people, entities and objects.

2. Digital Identity

2.1 Digital ID needs

A digital identity is a combination of credentials that allows managing an individual's authentication, authorization and access rights. Digital ID is being used mostly for two reasons: Authentication & Authorization.

2.1.1 Authentication

Authentication is the process of ensuring that the entity which is attempting to connect to a given service is legitimate and identified. Authentication is a key aspect of trust-based identity attribution, providing a codified assurance of the identity of one entity to another. Authentication methodologies include the presentation of a unique object such as a bank credit card, the provision of confidential information such as a password or the answer to a pre-arranged question, the confirmation of ownership of an e-mail address, and more robust but relatively costly solutions using encryption methodologies. In general, business-to-business authentication prioritizes security while user to business authentication tends towards simplicity. Physical authentication techniques such as iris scanning, fingerprinting and voiceprinting are getting more market acceptance and providing improved protection against identity theft.

ABN Amro, a Dutch bank, began offering mobile onboarding in November 2015 to ease the sign-up process for prospective customers. ABN Amro is using technology from Mitek: Mobile Verify, through which customers scan their IDs (the Netherlands issues official identification to all residents) and take pictures of their faces using their smartphones. The bank started scanning customers' IDs and customers take pictures of their faces with a smartphone. The Mitek software reads and compares the data in the QR code on the back of the customer's ID card with what is printed on the front. It also matches the photo on the ID document with the selfie. Mitek first verifies the authenticity of a document, and then evaluates the information in the document and applies it for data validation and reputation analysis. In the background, the bank performs its normal new customer identity and fraud checks.

2.1.2 Authorization

Authorization is the process of giving the access to a given service (after the successful process of authentication). Authorization depends on authentication, because authorization requires that the critical attribute (*i.e.*, the attribute that determines the authorizer's decision) must be verified. For example, authorization on a credit card allows to complete a transaction. Authorization of an employee will provide that employee with access to network resources, such as printers, files, or software.

2.2 Enrollment process

A secure Digital ID needs a secure enrolment process. Enrolment of Digital ID is a chain that ranges from the application to creation of an electronic identity. This step has a key role to play because this is the phase when the user's biographical data, such as name, date of birth and signature as well as unique biometric features, such as the facial image or fingerprints, are assigned to one particular individual. Not all services require the same level of certainty when enrolling users. A simple access to a website does not require the same level of certainty as financial transactions or access to secure services. Enrollment procedures have to be adjusted to the required level of security.

2.3 Digital ID types

2.3.1 Generated by user

This type of Digital Identity is one of the most spread nowadays: online accounts in numerous websites are created by users. The example is social media websites where you need to create a login and password using your personal e-mail or phone number. So, no additional entity is involved.

Source: arstechnica.com

2.3.2 Generated by private authority

This type of Digital ID is also very common in everyday life. Typically, a financial institution, as a private authority creates accounts and issues cards with specific identification numbers, *i.e.* creates an ID.

2.3.3 Generated by public authority

This type is even more common, because, here, we talk about governmental ID, meaning every passport or ID card issued by a government. While physical ID comes from a long history of citizen identification and traditional paper technologies, digital ID relates to computers and our current highly connected world. With governments setting up electronic ID infrastructures and private entities increasing the robustness level of their ID databases, the limit between physical ID and digital ID is increasingly blurred and systems are converging.

2.4 Authentication Factors

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user *knows*, something the user *has*, and something the user *is*. Each **authentication factor** covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.
Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified. The three factors (classes) and some of elements of each factor are:

- the **knowledge factors**: Something the user **knows** (e.g. a password, partial password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question, or pattern), security question;

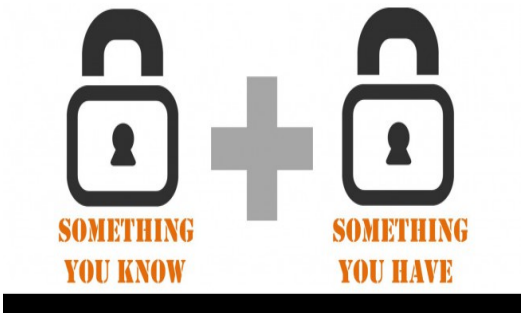
- the **ownership factors**: Something the user **has** (e.g. wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token);

- the **inherence factors**: Something the user **is** or **does** (e.g. fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier);

As it was mentioned above there are three types of authentication factors:

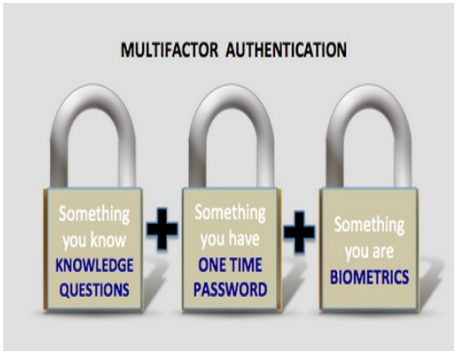
a) One Factor Authentication – “something that you know”, example is login & password created by a user and asked every time he/she wants to do some operations on concrete website.

b) Two Factor Authentication (2FA) – "something that you know" plus "something that you have", example is login & password plus a hardware device. This type of authentication is more popular because it has an additional layer of security. Another well spread and popular example is mobile 2FA. As it was said before a person needs to possess something in order to use 2-factor authentication. The major drawback of authentication performed using something that the user possesses and one other factor is that the plastic token used (the USB stick, the bank card, the key or similar) must be carried around by the user at all times. And if this is stolen or lost, or if the user simply does not have it with him or her, access is impossible. Mobile phone two-factor authentication was developed to provide an alternative method that would avoid such issues. If users want to authenticate themselves, they can use their personal access license (*i.e.* something that only the individual user knows) plus a one-time-valid, dynamic passcode consisting of digits. The code can be sent to their mobile device by SMS or via a special app. The advantage of this method is that there is no need for an additional, dedicated token, as users tend to carry their mobile devices around at all times anyway.



Source: Gemalto

c) Multi-factor authentication – "something that you know", "something that you have" and "something that you are or that you do". Typical MFA scenarios include: 1) Reading a card and entering a PIN; 2) Logging into a website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the requester's phone or email address; 3) Downloading a VPN client with a valid digital certificate and logging into the VPN before being granted access to a network; 4) Swiping a card, scanning a fingerprint and answering a security question; 5) Attaching a USB hardware token to a desktop that generates a one-time passcode and using the one-time passcode to log into a VPN client.



Source: newsbytes.ph

2.5 Digital ID tools

Source: colorado.edu

Mentioned previously, there are numerous identification tools, here are some examples: a) login & password; b) OTP (one time password usually produced by a token or generated by ATM); c) Biometrics (Example: fingerprint or iris); d) Out-of-band (second verification means – for example, a website might verify a user's identity by sending out a SMS to user's cell phone rather than enter the login & password. This tool helps to prevent man-in-the-middle attacks due to the fact that there are two different channels, which are more difficult to hack).

3. Federated ID

It is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. Identity federation offers economic advantages, as well as convenience, to enterprises and their network subscribers. For example, multiple corporations can share a single application, with resultant cost savings and consolidation of resources. In order for FIM (federated id management) to be effective, the partners must have a sense of mutual trust. Authorization messages among partners in an FIM system can be transmitted using Security Assertion Markup Language (SAML) or a similar XML standard that allows a user to log on once for affiliated but separate websites or networks.

Digital identity platforms that allow users to log onto third-party websites:

- Microsoft account – Formerly Windows Live ID
- Google
- Yahoo! – users can use their Yahoo! ID to log onto other sites, and users used to have the possibility to log onto Yahoo! with their Google or Facebook IDs.
- Twitter
- LinkedIn
- PayPal
- SecureKey
- Foursquare

3.1 Single Sign-On (SSO)

Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. Credentials for authorization are stored on a dedicated SSO policy server, which passes along the specific authentication credential it has stored for an individual user. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when the user switches applications during the same session. SSO is helpful for documenting logging and monitoring user accounts, which improves organizational security, makes user's life simpler and allows to log all accesses to a given service for legal tracking purposes.

3.2 OpenID Standard

OpenID is an open standard and decentralized authentication protocol. Promoted by the non-profit OpenID Foundation, it allows users to be authenticated by co-operating sites (known as Relying Parties or RP) using a third party service, eliminating the need for webmasters to provide their own ad hoc login systems, and allowing users to log in to multiple unrelated websites without having to have a separate identity and password for each.

Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, Yahoo!, the BBC, IBM, PayPal, and Steam, although some of those organizations also have their own authentication management.

3.3 OAuth

OAuth (Open Authorization) is an open standard for token-based authentication and authorization on the Internet.

OAuth allows an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password. OAuth acts as an intermediary on behalf of the end user, providing the service with an access token that authorizes specific account information to be shared.

3.4 FIDO, a standardized approach to federated ID

The **FIDO** ("Fast IDentity Online") **Alliance** is an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices and the problems users face creating and remembering multiple usernames and passwords.

The mission of the FIDO Alliance is to change the nature of online authentication by:

- Developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users;
- Operating industry programs to help ensure successful worldwide adoption of the specifications;
- Submitting mature technical specification(s) to recognized standards development organization(s) for formal standardization.

Some FIDO Alliance members:

- Alibaba Group
- ARM
- Bank of America
- CrucialTec
- Nok Nok Labs
- Lenovo
- Samsung
- Google
- Yubico
- Synaptics
- Intel
- Microsoft
- Oberthur Technologies
- Visa
- Qualcomm
- PayPal
- MasterCard

One of the most important specifications: Universal 2nd Factor (U2F) is an open authentication standard that strengthens and simplifies 2FA using specialized USB or NFC devices based on similar security technology found in smart cards.

During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over NFC. The user can use their FIDO U2F device across all online services that support the protocol leveraging built-in support in web browsers.

Another specification is called UAF (Universal Authentication Framework) or Passwordless UX. The passwordless FIDO experience is supported by the Universal Authentication Framework (UAF) protocol. In this experience, the user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the microphone, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user.

Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN.

What is important to mention is that all FIDO solutions are certified and standardized. The FIDO Certification program allows members and non-members to measure compliance and ensure interoperability among products and services that support FIDO specifications. Companies completing certification may display the FIDO Certified logo to demonstrate to consumers, customers and partners that they have created a highFIDO Cert interoperable FIDO implementation that is known to work with other FIDO implementations.

4. Identity 2.0 & Identity 3.0

Identity 2.0 is term for user-centric identity management on the internet, in which users have complete control over which third party authenticates them. It also implies that users have control over the data they share over the internet and can transfer and delete the data when required. The "2.0" was taken from the widely used "web 2.0" term that refers to user-oriented capabilities. This type is related to such an approach as OpenID.

Identity 3.0 is a term used to define the next generation of digital identity, which moves beyond basic Digital Identity and Identity 2.0. There is a need for a shift to identity 3.0. Technologies in encryption, privacy, biometrics and security are becoming more complex and advanced. So, the identity management of a previous version is not enough to maintain the highest level of security and functionality.

The key principles were defined in 2014 by the Global Identity Foundation, a not-for-profit organization working to define the components of a global digital identity ecosystem.

5. Digital ID for the Internet of Things (IoT)

With billions of connected objects anticipated in the upcoming years, Digital ID of objects is almost as important as Digital ID of humans. The goal is to create a standardized framework to identify individually objects in a secure and accurate manner.

Several hacks have already been undertaken targeting connected objects. As the objects considered in IoT are generally small, have low power, are always on and lack user interface, they need to be identified securely to allow building a security infrastructure.

To build the required security for the Internet of Things, thee objects are provided with unique identifiers and the ability to transmit them in a secure way (using cryptographic techniques) over the communication channels.

End-to-end security is to be taken into account when designing any connected objects system. A global IoT dedicated security scheme is to be built along with the design of the system, including semiconductor, hardware, network software and application.

Such a security system need to be built on a reliable identity system allowing to identify with certainty each object. To accomplish this, objects need to be enrolled, just as humans, one need to setup an authentication system and an identification system, mimicking the Digital ID systems developed for humans.

6. Glossary

2FA	Two-Factor Authentication
ATM	Automated Teller Machine
DNA	Deoxyribonucleic Acid
FIDO	Fast Identity Online
FIM	Federated ID Management
ID	Identity
IoT	Internet of Things
MFA	Multi-Factor Authentication
NFC	Near Field Communication
OAuth	Open Authorization
OTP	One Time Password
PIN	Personal Identification Number
RP	Relying Parties
SAML	Security Assertion Markup Language
SMS	Short Message Service
SSO	Single Sign-On
U2F	Universal Second Factor
UAF	Universal Authentication Framework
URL	Uniform Resource Locator
VPN	Virtual Private Network
XML	Extensible Markup Language

Published by:
Intelling, 9-13 rue Bel-Air, 13006 Marseille, France
www.smartinsights.net -report@smartinsights.net

Publication date: September 2017