What is an identity? What makes you — you?

- How do you identify yourself? What does make you unique?
- First of all, my identity is my name and my last name. I have it written down everywhere, including the passport and the front side of the banking card.
- Yes, but when you buy something in a shop, and pay with a bank card, does anyone asks for your name to make sure it’s YOUR card?
- Hmm, no.
- Then, your identity in a shop is your PIN number, correct? In this case only 4 digits make you — you. So, what is an Identity?

We identify ourselves in different situations with different utilities. We play roles. In a shop our Identity is just a PIN number, at work it is an occupation and on social networks or blogs we may have a weird nickname and still keep being yourself. In the meantime, all your friends would know that this concrete social network fake name belongs to you, and in the social network space you are YOU. You may have lots of identities. And if you don’t like your identity for some reason — whether it’s subverted in some way, or it’s insecure, or it’s inappropriate, you just delete it (close the bank account or delete the social network account) and get another one.

What is your identity?

**Individual preferences**
- Favourite brands
- Taste in music
- Interests

**Acquired attributes**
- Address
- Medical record
- Purchase history

**Inherent characteristics**
- Date of birth
- Gender
- Nationality

What do you like?

What did you do?

Where do you come from?

Digital Identity
Digitally available information about an individual

(Boston Consulting Group, 2015)
Actually, Identity is a fluid, unstable substance, which is difficult to tie to a specific “core” profile. Even if the Identity is securely bent to a birth certificate, passport, national ID card or any other ID document, the forgers are aware of the thin and weak spots and ingeniously abuse the person’s Identity integrity. Obvious fact: the electronic documents carrying a radio frequency identification (RFID) chip are able to provide higher security and decrease risks of forgery and identity fraud, rather than the conventional paper-based documents.

Today an MRTD (Machine Readable Travel Document), issued by a Government, is the one and only tool to verify the identity of a document holder. No matter what kind of a document you use – passport, ID card, driver license or residence permit — your Identity is directly linked with the data stored inside the document chip. It is very straightforward – every time you present the document when crossing a border or logging into the e-Government web space, your identity will be authenticated through online comparison of your data and primary credentials provided onsite.

Document Security

Your identity documents are extremely valuable on the black market so make sure to safeguard and place them in a fireproof lockbox until the next time you need it.

When do you need to prove your Identity?

- Open bank accounts and make everyday payment transactions
- Travel and cross borders
- Apply for visa or residence permit
- Access governmental services on e-Government web-portals
- Vote remotely and participate in the State initiatives
- Pay taxes, fines and carry out legal procurements
- Apply for and receive donations, grants, scholarships, pensions, subsidies, etc.
- Access your corporate/enterprise environment remotely
- Access educational environments remotely
- Access specific territories, buildings, properties, etc.
- Prove your legal age to take an action
- Prove custody of a child to take actions on their behalf
- Secure deals with real estate, property, vehicle
- Prove your identity to obtain notary-certified documents
- Be target of police actions or identity checks
e-Government and digital society

Today many forward-looking countries are continuously investing in digital technologies to drive country’s development and bridge the gap between the public sector and modern society. There are several countries across the world (e.g. the United Kingdom, Ireland, Latvia and Ukraine) that show a strong correlation between digital government and GDP growth.

The raising global usage of e-Government portals logically prompt us to use digital identities. To access a web-based service you won’t need a plastic card or a hard-copy booklet of your document. You would want to quickly link your real personal identity to the valid document, and authorize yourself immediately in the e-Government environment.

Types of e-Government systems

- Population registry
- Civil and criminal biometric databases
- Document issuing system and registry
- Border control system
- Healthcare system
- Public transport system
- Social security system (subsidy distribution and management)
- Education (including remote education)
- Employment system
- Real estate and vehicle registry
- Company register
- Driver registry

BENEFITS of digital government

- Security
- Efficiency
- Transparency
- Reduced administrative costs
- Economic growth
- Attractive investment landscape

e-Government: Benefits for Governments

- Improve service delivery and social welfare of citizens
- Establish a centralized point of communications for government agencies and departments
- Provide greater access and transparency of public records
- Increase efficiency and reduce time, staff and financial resources required to process paperwork

e-Government: Benefits for Citizens

- Have faster and easier access to information about public services
- Access information on a self-serve basis 24-hours-per-day seven-days-a-week
- Save money and time by using e-government services
- Experience improvements in service quality and turn-around time

“Oh my god, did you know that you can do your tax return online? I will never waster paper on this thing.”

- John Johnson, Chief Engineer

“I won’t wait in line for two hours to get my new passport because I scheduled an appointment online to get a new one.”

- Sally Smith, Primary School Teacher

TOP 3 e-Government services you use your digital IDs for:

- Apply for/Renew Licenses, Registrations, Permits
- Pay taxes
- Pay fines and tickets
How can you prove your Digital Identity?

There are many ways to prove the authenticity of your Identity. When you apply for a new electronic document, your personal data (including names, birth data, high-resolution photo, signature, fingerprints/iris samples, etc.) are recorded into a single personal profile (personal record). This data is securely encoded and stored in a Government-based citizen registry, as well as recorded into the electronic chip inside your new document. This data is protected by sophisticated software technologies, extremely difficult to forge or damage.

There are several utilities to prove your identity
- Wireless Mobile Authentication + PIN
- Face Recognition
- Fingerprint scanner, iris scanner
- Electronic signature + PIN

Evidence of Identity

The foundation, or the basis to issue a new ID document is the birth certificate, given to a person and verifying his or her existence. Birth certificates are commonly issued on paper, and can't guarantee the real and unique holder's identity. What is more, there are plenty of cases when birth certificates (breeder documents) are easily counterfeited.

What else can prove your Identity? Your social background, for example, also called as “social footprint”. If you graduated from Oxford and your ID was used there, or you have a long running banking credit score, and you also used your ID there, why do these things need to be disregarded or kept off-the-record? These exact life facts make you — you, and this proves the Evidence of Identity, along with birth certificates and other profile data.

The “Evidence of Identity” is the crucial requirement to fight against Identity fraud. This is why it’s essential to provide secure and trustworthy environment for enrolment, personalization and issuance of a secure e-ID document, to avoid corruption and document abuse.
Evidence of Identity: Role of ICAO

The ICAO Guide 9303 for Assessing Security of Handling and Issuance of Travel Documents Contracting States shall establish controls to safeguard against the theft of their blank travel documents and the misappropriation of newly issued travel documents.

Contracting States shall establish appropriate controls over the entire travel document application, adjudication and issuance processes to ensure a high level of integrity and security.

Eventually, the issued booklet or card itself (no matter if it’s an e-Passport or an e-ID card) does not prove Identity as it is. But at least it securely "seals" your ID to your personal record, where your data has been stored. Thanks to biometrics, it now became possible to dramatically decrease fraud probability, as well as to avoid the illegal document usage by imposters and look-a-likes. Many countries around the globe have introduced e-passports storing biometric information to prevent illegal entry and facilitate legitimate travel.

And thanks to the software technology, the verifying authority can link the citizen to his identity via the secure document that stores digitally signed and encrypted information.

5 Problematic Situations and Concerns

1. You wouldn’t want to carry your Document with you all the time.
Your original document can be occasionally damaged, lost or stolen. You would prefer to have a “derived” and easy-to-use technology in your smartphone to verify yourself in everyday situations, and yet you would want this technology be secure and reliable. And it’s not the future, the “derived credentials” are successfully used in many countries.

2. Your Identity can be used by someone else.
Your personal data (including photo, signature, biometrics, etc.) can be forged by some intruders and illegally used against your will. The identity of a dead person can be used to take advantage of their financial privileges and preferences. This is why you would want your ID document guarantee the highest-level protection possible. And this is the exact reason why we talk about Strong Identity.

3. You are feared that government is spying on you or worried about privacy of your personal data.
Both document verification and identity authentication are realized in the environment of public and private keys (PKI — Public Key Infrastructure). These key certificates are issued by Government-controlled trusted certificate authorities, and provide the utmost data protection level of your document. This is why all ID operations and transactions addressing e-Government and bank services are secure, given the fact the ID document is secure.

4. If something changes in your appearance, signature, or social status, you would like to be sure your ID still gets recognized.
Sometimes a person gets older, grows a beard or makes a new hair-cut. The innovative document verification technology permits processing an instant face matching procedure, if you use your smartphone. If you are logged into a remote bank service, and you need to authenticate yourself quickly, you can take a selfie on your smartphone. The application will compare your picture with the photo of the ID document with the highest accuracy, even you’re wearing a beard.

5. The Identity paradox
If you are a Government top-level executive, a bank stakeholder, a State police officer, or an employee supervisor, you would want to know who everybody else is, but you wouldn’t want anybody to know who you are. You would want full disclosure from citizens, customers and subordinates to control them, but you wouldn’t want full disclosure from yourself. This happens between regular people as well — a regular parent would want to know as much as possible about their kid’s Internet friends, but wouldn’t want their kid’s profile be detailed and open for anyone. What do you think about it?
**Privacy by design**

- Data processing in line with a codex
- Highest degree of protection
- Different use cases

---

**Derived credentials**

Derived credentials is a "light-version" alternative to your primary credentials. It’s like you’ve taken your personal record saved on the electronic document chip, encrypted it and saved again on your smartphone. So once you have verified your document in the e-Government space, you will not need to carry your passport booklet or e-ID card with you in your wallet. You are free to authenticate yourself in a user-friendly mode in a couple of seconds via your gadget.

**Requirements, terms and regulations for derived credentials**

- Derived credentials can’t exist without primary credentials.
- The usage of derived credentials is strictly voluntary.
- The aim of using derived credentials is citizens’ convenience.
- The technology has to be available on any platform, device, OS.
- The technology does not have to provide the primary document’s level of security, as soon as the primary document must be always accessible and valid.

One should accept, the user convenience boosts the technology usage and propels the business value of each participant. The Identity issuing authority is able to provide a small benefit to the public, thus improving the convenience, and boosting the use and issuance of primary credentials to build an effective e-Government society.
Identity Fraud and Identity Theft

Identity fraud is a crime where one person uses another person's personal data.
- Material fraud (physical & electronically)
- Imposters – is someone who knowingly misrepresents him or herself by using someone else’s identity or travel document
- Fraudulently obtained documents (intellectual fraud, with or without internal help)

There are three basic reason for a person to steal someone’s identity
- Hide the real identity of a person
- Make a financial profit from fraudulent activities
- Avoid financial liability such as outstanding debts and tax avoidance

Weakest links in identity fraud

Document security
False identity
Issuing procedures

Criminals switching from Document fraud to Identity Fraud is a major threat for document security

- Breeder documents – birth certificates
- Poor issuing procedures
- Linking of databases Births & Deaths
- Poor exchange of information

MRTD — a machine readable travel document with an embedded chip that stores ICAO specification compliant biometric information (e.g. fingerprints, image and signature).

Imposters — a person who pretends to be someone else in order to deceive others, especially for fraudulent gain.

Evidence of Identity — identification of an individual based on examination of identity documents bearing an image of the individual’s face and signature.

Social footprint — biographical identity that builds up over time and links to the person’s identity e.g. education/qualifications, employment history, interactions with public authorities, private organizations and banks.

Primary credentials or Root ID — acceptable primary proof of identity in a form of original or certified documents with full name and date of birth.

Derived credentials — alternative credentials that are derived from individual’s primary credentials and saved on a mobile device.
Mobile Authentication

Using a basic username and password has never been an option for high-risk public and private platforms. If the world keeps up with social and technology trends, by 2020, globally there will be 6.1 smartphone users who will likely want to authenticate their identities via smartphones (TechCrunch, 2016).

Mobile Authentication is an on-the-go solution to verify user identity and grant authorization to carry out electronic transactions. Mobile authentication solutions is a more convenient and efficient alternative to traditional processes. The layered approach of mobile authentication ensures greater security for sensitive data and transactions, protecting from any misuse of data or unauthorized access.

This system can be a means for secure authentication, when verifying and validating the genuine owner of the identity who wants to carry out electronic transactions. The mobile authentication process is carried out via smartphones, using biometric technologies. This explains why more and more smartphone manufacturers choose to embed biometric technologies on their devices.

International Regulations

Mobile Authentication is compliant with such international regulations as PSD2, eIDAS and GDPR.

PSD2 - directive on payment services across Europe.

eIDAS - interoperable framework for electronic identification and trust services for electronic transactions in the European internal market.

GDPR – regulation for individual data protection within the EU.

What makes a strong identity — strong

The use of biometrics – something you are – creates a more reliable link between the identity document and the holder. There are different types of biometrics that can help to create a strong identity, including face, fingerprints dynamic signature.

One should not forget that biometric authentication provides secure access to external e-Government portals based on such biometric modalities as face and fingerprints.

Biometric modalities

- Face
- Fingerprint
- dynamic signature
- Iris
- hand palm
- voice recognition
- veins

(X-Infotech, 2016)
Why we need 2-step authentication

What does happen when someone gets hold of your personal information? Moreover, how can you make sure the citizen logging in on the e-Government portal with a username and password really is the real person associated with this identity?

Two-factor authentication is a method that uses a combination of two different components to authorize citizens to access applications or services. Two factor authentication provides an additional level of security to secure an account and authenticate beyond usernames and passwords. It may involve a smartphone as part of the authentication process to provide a secondary confirmation and reduce elevated risks.

Levels of assurance

When two-factor authentication is implemented accordingly, it makes it very hard for evil-minded people to steal someone’s credentials. This kind of authentication requires the user to confirm their identity based on a combination of two different elements.

Elements of two-factor authentication

If one of the previous scenarios is stolen, then cyber-criminals or any other unauthorized access won’t be able to authenticate and access e-Government services.

How it works

Mobile authentication service: links between smartphone, PC, e-Government system and the authentication server.