Identity Assurance

The art of knowing your customers

John Erik Setsaas
2016-11-16

SIGNICAT
Disclaimer

Please note that this presentation is for information purposes only, and that Signicat has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation.

The future strategy and possible future developments by Signicat are subject to change and may be changed by Signicat at any time for any reason without notice.

This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Signicat assumes no responsibility for errors or omissions in this document.
Identity assurance background
Traditional assurance

- Physical meeting
- Bring ID papers
- Verification done by a person
User expectation

• Digital registration
• Everything can be done from home
• Using any type of device

• No human interaction
What the user meets

- Difficult to become a financial customer
- Do not understand why
  - I have to provide so much info?
  - I have to upload my passport?
  - It is so easy to sign up at web stores
    - Using social media

40% have abandoned some kind of application form for financial services in the past 12 month
What the business sees

- Time consuming
- Costly
- Complex
- Losing potential customers
- Losing money

![Graph showing decrease in revenue](image)
On-boarding challenges

- **Digital on-boarding is a complex process**
  - How to verify that the person is who he or she claims to be?
  - What about KYC (Know Your Customer) requirements?

- **Digital on-boarding is costly**
  - Often requires manual steps (both for the consumer and the organization)

- **Digital maturity of the population**

- **Trust**
  - People are reluctant to use digital identity
  - Surveillance (Ref. Snowden)

A good solution should empower the user to overcome fear of surveillance
Identity assurance must be simplified!
Identity assurance
Business motivation

$ $ $

• Risk
  – Will you get paid for your services?

• Consequence
  – Loss of money

§ § §

• Regulations
  – KYC
  – AML

• Consequence
  – Loss of money
  – Loss of reputation
KYC – Establish trust in the identity

• Collect and analyze information
• Name matching against lists of known parties
  – such as PEP (Politically Exposed Person)
• Determine risk
  – Money laundering, terrorist finance, or identity theft
• Create transactional behavior profile
• Monitor against expected behavior
  – Including behavior of customer’s peers
Reasonable assurance

- Establish a **reasonable assurance** that the user is who he or she claims to be

- **What is reasonable depends upon factors including**
  - Jurisdiction
  - Risk vs consequences
  - Resources
  - Technology state of the art
eIDAS assurance levels (EU regulation 2014/910)

Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person.

The requirements established should be technology-neutral. It should be possible to achieve the necessary security requirements through different technologies.
What can a user use to prove his or her identity?

- Proof of address
- Possession of phone
- Commerical identity
- Self portrait
- ID paper
- Physical or virtual meeting
- Derived identity
What can the bank do to verify the identity?

**Automatic checks**
- Social media attributes
  - Name, phone etc
- Social media ratings
  - Recommendations
- ID paper OCR
- Registries
  - PEP/OFAC
  - Credit rating
  - Business roles
- Web searching

**Manual checks**
- Visual check of information
  - ID paper vs photo etc
- Phone call
- Video conference
User motivation vs business risk

I want to check out your banking app

User motivation

I want to buy a house

Simple assurance

Full KYC compliance
The gradual approach example 1

The ID paper approach
John wants to sign up with the bank

The bank needs a reasonable degree of assurance

Assurance threshold 1
Limited functionality

Assurance threshold 2
Full functionality
John provides basic information

John Doe
555-1234
1970-04-05
John responds to OTP (One Time Password)

Assurance
John

Upload self-portrait with OTP

Bank

John Doe
555-1234 [verified]
1970-04-05

[verified]
Assurance

Upload passport

John

Bank

John Doe [verified]
555-1234 [verified]
1970-04-05 [verified]

[verified]
John Bank

Manual check

John Doe
555-1234 [verified]
1970-04-05
[verified]

Assurance
The gradual approach example 2

The social media approach
Log on to commercial identity

John

Bank

John Doe
555-1234
1970-04-05
John responds to OTP
(One Time Password)
John

Bank

John Doe
555-1234 [verified]
1970-04-05

Web verification

Assurance

PEP
OFAC

SIGNICAT
Summary

• Decide what reasonable assurance means for your organization

• Define several levels

• Decide which means of assurance
  – And how to combine them

• Make it simple for the end-user
End of presentation

John Erik Setsaas

John.Erik.Setsaas@signicat.com
@jsetsaas