Do Public/Private Digital Identity Schemes Need National Identity Standards Overseen by Mandatory External Assessments?

Nils Inge Brurberg

EEMA annual conference 2019

Betalingsinfrastruktur i verdensklasse !!

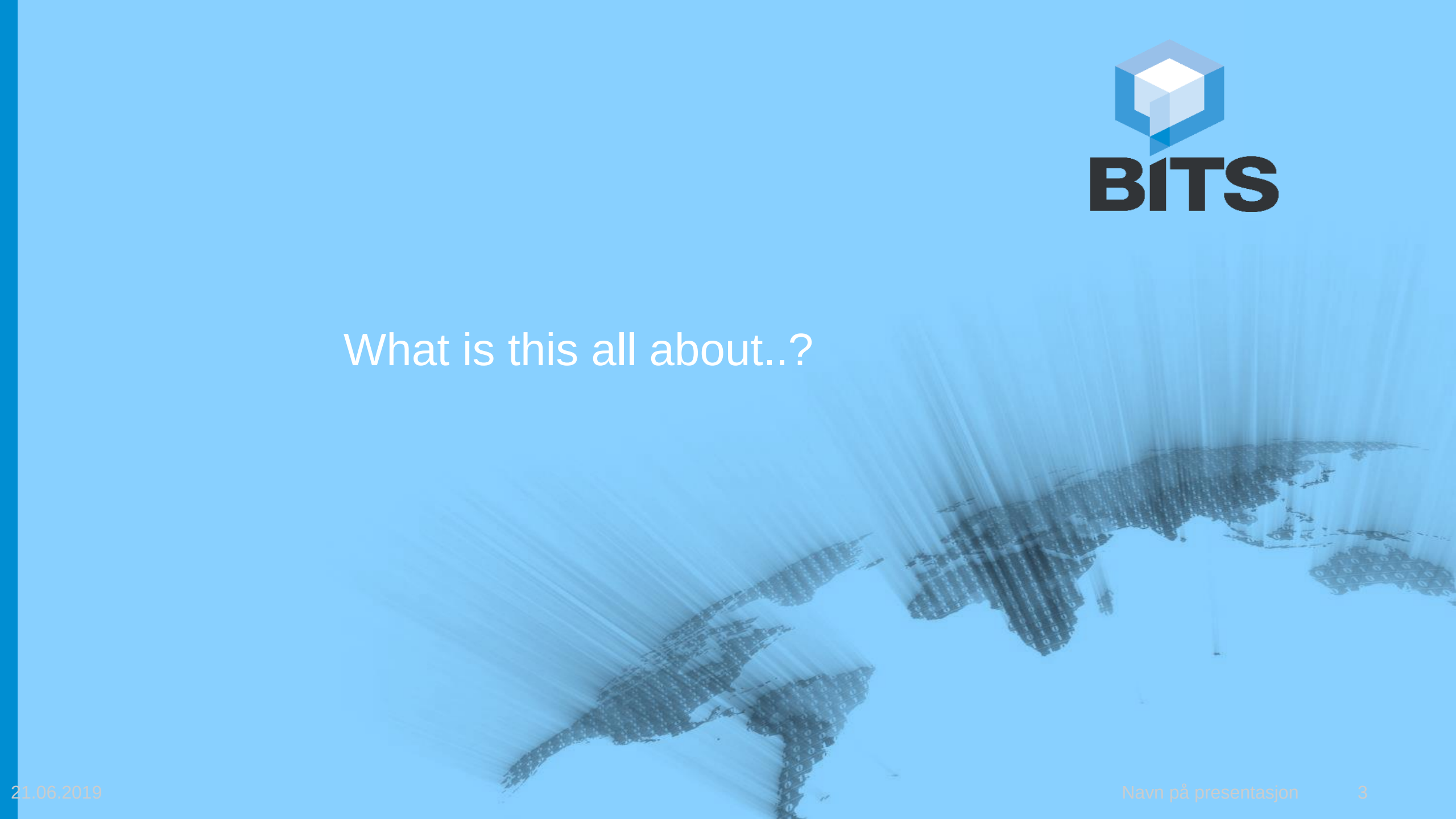
How physical do you have to be?

Nils Inge Brurberg

EEMA annual conference 2019

Betalingsinfrastruktur i verdensklasse !!

What is this all about..?



Rationale

The good story

- Banks and public sector have become more and more digital during the recent years.
- BankID identification and signature is used everywhere in digital services.

However…

- Due to legal and practical reasons, persons still need to meet in person with an approved physical identity document (i.e. passport) for first time identification and registration with an eID provider.

Drivers

Identity providers have large incentives to provide automated solutions for onboarding of new customers as well as for re-validating existing customer relationships.

- Customer expectations to modern online services
- Cost reductions
- Reduced time to enable service
- 24/7 service
- No need to travel to the identity provider’s office
- Efficient customer capture
- Efficient re-authentication of customers

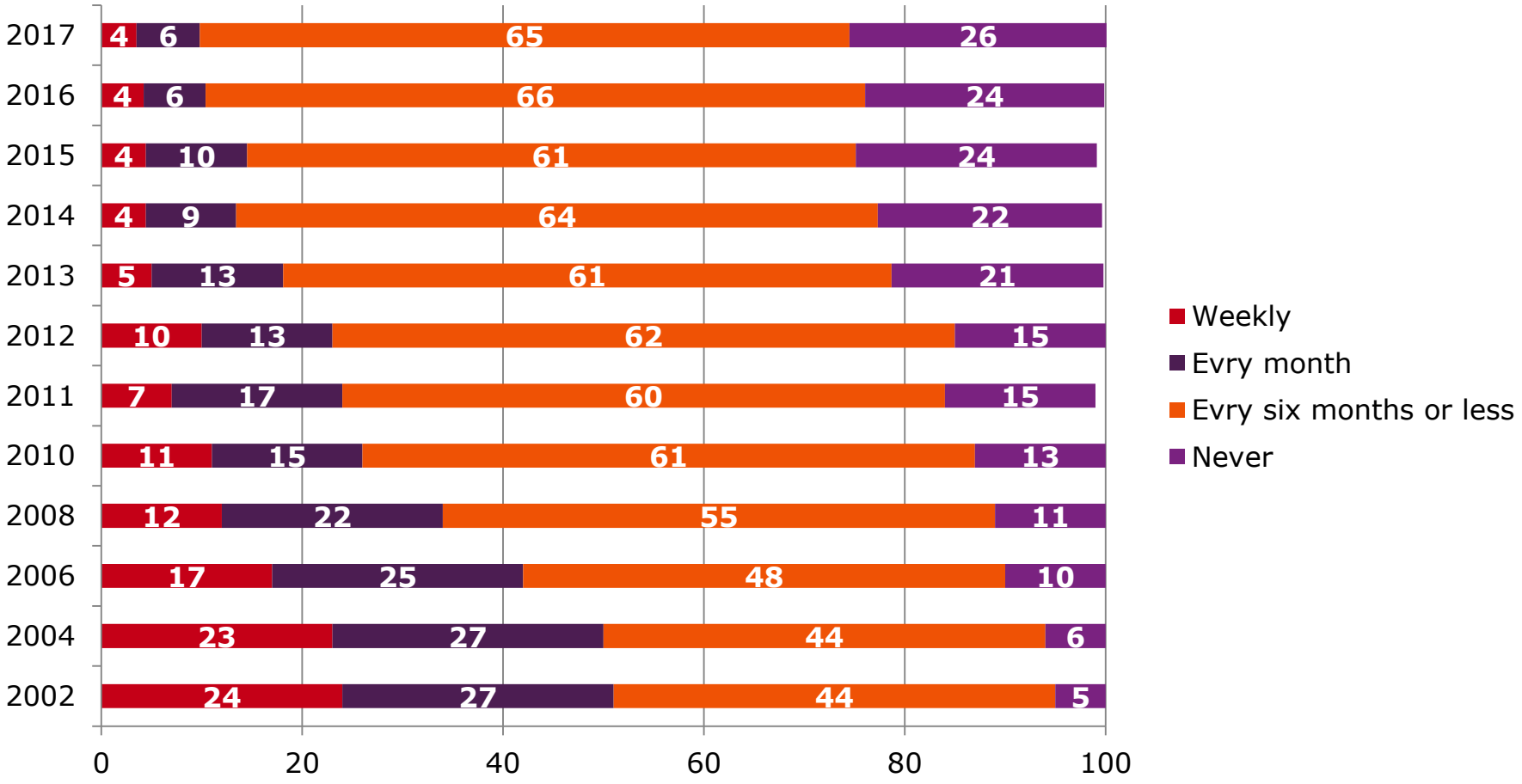
Identified obstacles…

Legal requirements

- Identification requirements for access to banking services
- Anti-money-laundering requirements
- Identification requirements related to issuing eID and eSignature certificates according to eIDAS and national legislation
- BankID is used for public sector services, hence need for ‘approval’ from agencies currently sceptical to digital-only-onboarding

The need for an alternative to physical presence

Visit to the Bank office 2002-2016



% of population agea 15 år + (frem til 2016)

Kilde: Forbruker- og finanstrender 2017

Physical identication numbers

- During a 12-month period in 2018 the number of passports scanned in the banking offices sums up to **around 700.000**
- If we assume that one passport scanning takes around 30 minutes with preparations, this activity costs the banking industry around **200 FTE's** each year.
- As the customer must also meet up in person in the bank, during banking hours it is estimated that this in addition cost the society around **400 FTE's.**
- If we can reduce the cost for banks and society by **50%** by using electronic processes it is quite easy to understand the impact of solutions based on common requirements on business and society.

Bits working group on secure digital identification of identity

About the working group

Bits initiated a working group to define a set of general requirements for solutions for digital identification of physical persons.

The goal is to create a basis for common evaluation and approval of solutions for establishing and verifying new customer relationships without the need for physical presence.

- Identify business requirements
- Identify external requirements, i.e. legal and other
- Identify available technologies
- Evaluate acceptable risk appetite and security levels
- Evaluate solutions vs business requirements

Identify and describe user stories

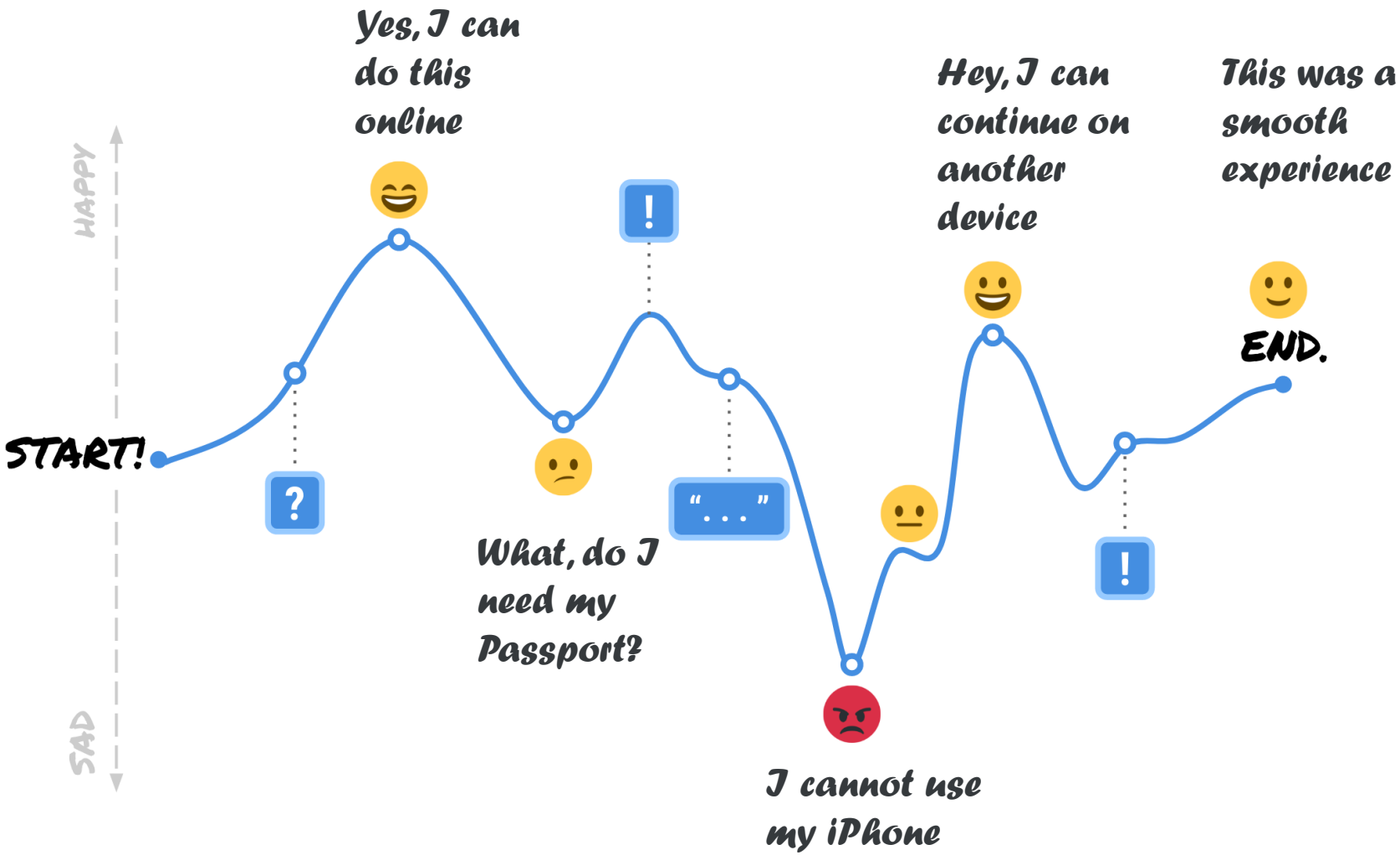
New customer relationship

Basis for issuing e-ID and e-Signature

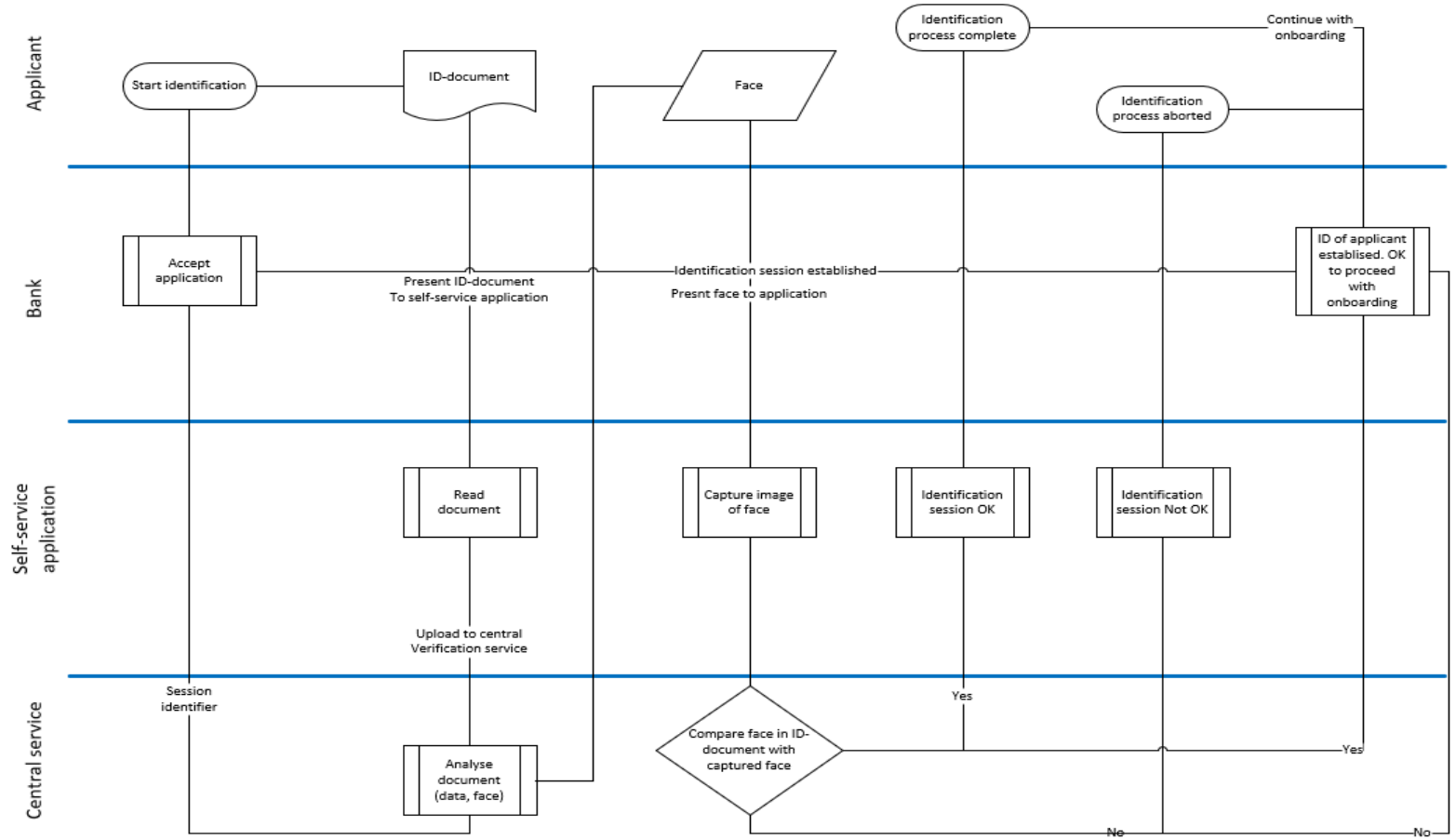
- Electronic ID enabling banks to fulfil PAD requirements (Payment Accounts Directive)
- Issuing electronic ID and electronic signature (BankID)

Verify existing customer relationships (verify identity)

USER JOURNEY



Generic user journey



User journey steps

1. Person applies for service that requires the verification of identity
2. Person is redirected to self-service application
3. Application is accepted, pending verification of identity
4. The applicant presents the ID document to the self-service application
5. The machine-readable information (eg VIZ, MRZ and RFID chip) in the ID document is read by the self-service application
6. The machine-readable information (eg VIZ, MRZ and contents of RFID Chip) in the ID-document is uploaded to the central verification service
7. The ID-document is checked by the central verification service, ie. If it is genuine and valid (authenticity check)
8. The applicant registers new biometric data with the self-service terminal
9. The biometric data is uploaded to the service provider
10. The uploaded or streamed biometric sample of the applicant is verified (compared) against the biometric data earlier uploaded from the ID-document
11. Identity is verified at certain level

Types of requirements (1)

General requirements

Client server architecture

Client captures and protects data

Server processes data

Device, Connectivity and software requirements

Client operating system

Client ID document optical capture device

Client ID document RFID capture device

Client Biometric sample optical capture device

Client application user interface

Client application security

Communication security

What is «good enough»?

Must be sufficient, but what does that imply?

= Equally good, or better than current practices

How to make the process less dependent on humans?

International competition / FinTechs challenge established boundaries

Different levels for different use-cases and needs

The challenge in the time to come

- ✓ Complex area with many requirements and stakeholders
- ✓ Technology – NFC is available on Android handsets, will become available soon on Apple Iphone – roomers say
- ✓ Need acceptance from the whole industry and public sector
  - ✓ National level
  - ✓ European level

Conclusion

- We have developed a requirement document covering security and functionality that can be used as a basis for solutions.
- Now, we need acceptance from government, other stakeholders in our home market.
- We believe that our work could be beneficial to the European community of banks, public sector agencies and other industries that require to identify employees, contractors and clients in an online setting.
- European Commission have also taken an interest in our work, DG Connect joined our workshop in February.
- Norwegian banks and public sector agencies will pilot solutions during 2019/2020. Based on the experiences we will seek approval on national level, and then on European level.

The requirements document

- Our current requirements document will be available after the conference.
  - **Secure digital verification of identity** v 0.99

- Comments and suggestions to the document can be sent to:
  - nib@bits.no

Thank you for the attention

Nils Inge Brurberg

NIB@bits.no

+47 92400125

www.bits.no