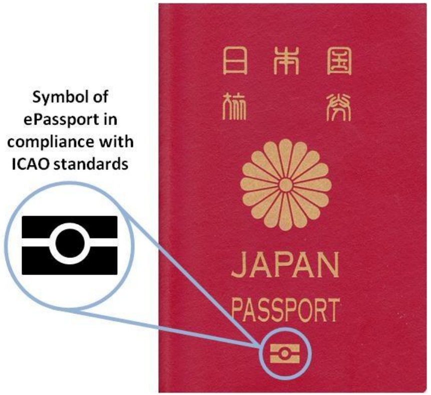
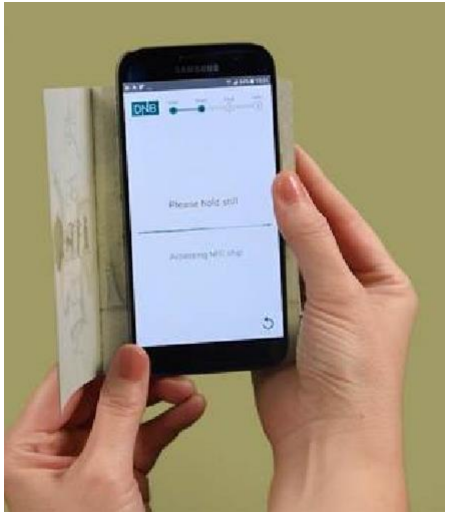
Workshop on digital onboarding solutions
Brussels - 28th September 2018

Jannicke Birkevold
www.idmee.com

A little bit of context

- Norway has the world's best digital infrastructure, according to the World Economic Forum's "Networked readiness index".
  - 96% of Norwegians use the internet, and 90% bank online. Only 6% of payments are made in cash.
- The banks in Norway collaborate on a common eID that is used by both the private and public sectors – Bank ID
- The concept of BankID requires the banks to have mutual trust in the work that the other banks do when onboarding customers and issue a BankID
- BankID is reviewed for approval on eIDAS level high these days
- DNB is the largest bank in Norway
- DNB is the owner of IDmee (DNB ID Solutions AS)
- IDmee is implemented in DNB, but also sold to third parties


Symbol of ePassport in compliance with ICAO standards



IDmee

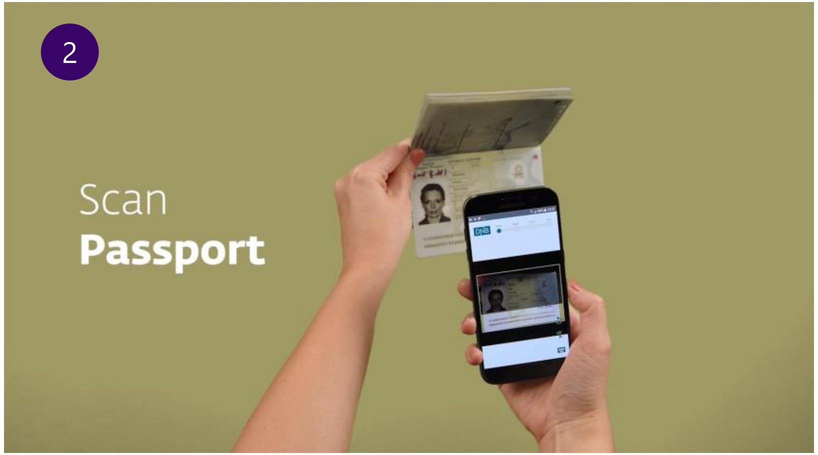
- Scans and reads the passport with an NFC enabled mobile phone.*
- Checks that the person carrying out the process is the rightful owner of the passport.
- Ensures that the information is transmitted in a secure manner.

*Android

Demo or Video

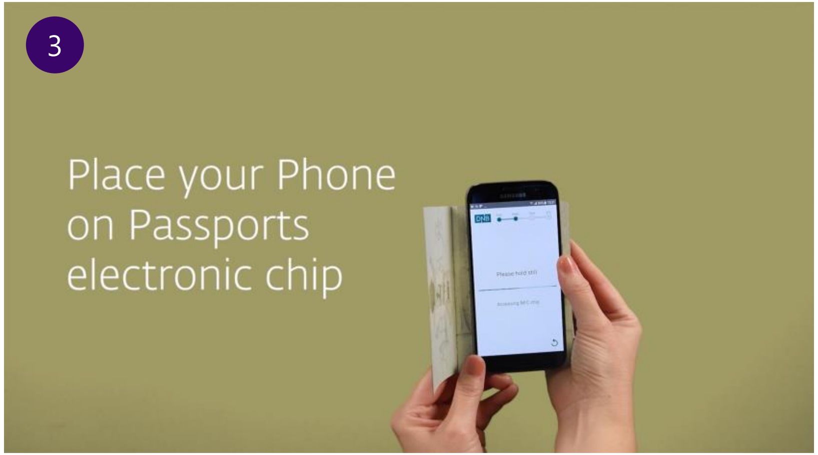
1

Find your **Passport** and **Phone**



2

Scan
Passport



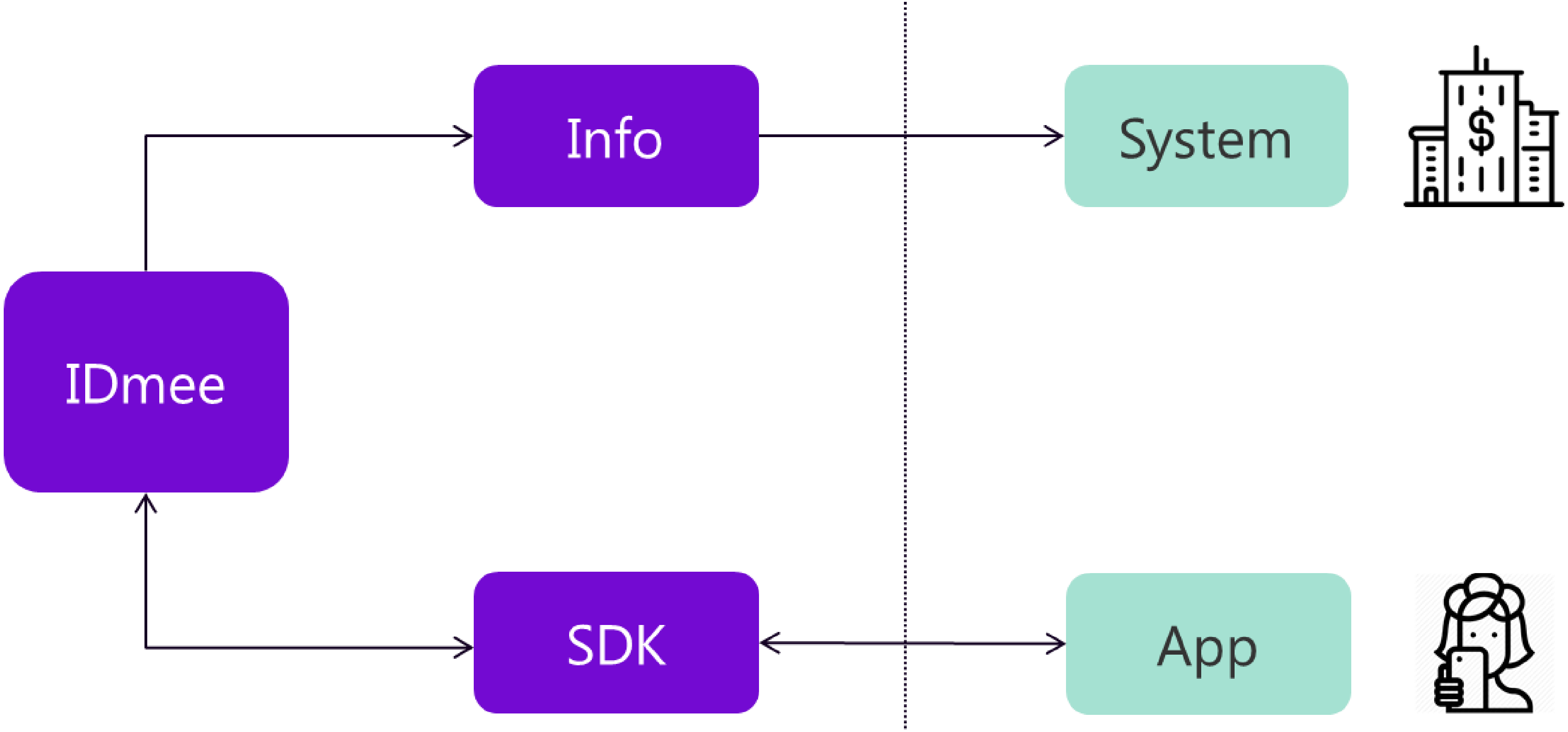
3

Place your Phone
on Passports
electronic chip

4

Use your camera for facial recognation

IDmee

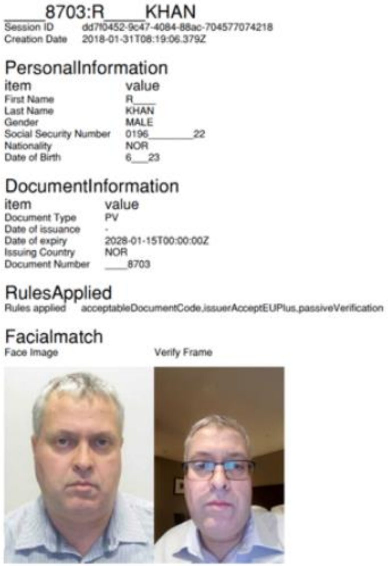


PDF file + JSON file

The solution provides a signed PDF file containing:

- Information read in a secure manner from the passport. This information is read electronically (NFC) and the information was signed by the authority issuing the passport. The solution will check both the signatures and ensure that the certificate used to sign does indeed come from the authority in question.
- An image electronically read from the passport. Again this is signed information and subject to the same validations as the other information read.
- An image captured during the face recognition to serve as illustratively proof of this process.
- An image captured of the front page of the passport. This can be used if visual inspection is required.

- Please notice that for illustration the personal information has been obfuscated.



____8703:R____KHAN

Session ID dd710452-9c47-4084-88ac-704577074218
Creation Date 2018-01-31T08:19:06.379Z

PersonalInformation

item	value
First Name	R____
Last Name	KHAN
Gender	MALE
Social Security Number	0196________22
Nationality	NOR
Date of Birth	6___23

DocumentInformation

item	value
Document Type	PV
Date of issuance	-
Date of expiry	2028-01-15T00:00:00Z
Issuing Country	NOR
Document Number	____8703

RulesApplied

Rules applied acceptableDocumentCode,issuerAcceptEUPlus,passiveVerification

Facialmatch

Face Image Verify Frame

Takeaways from implementing IDmee

- IDmee – digital onboarding for eIDAS level high
- IDmee is considered AML/KYC compliant
- It is a ongoing process to recognize IDmee as a digital onboarding solution for BankID in Norway

- ID papers used to issue an eID
- ID papers owner + person = True
- Documenting the process
- Transfer of data

ID papers used in digital onboarding

ID papers used as underlying documentation of ID when issuing an eID on level high:

- Must have an RFID chip containing biometric information (photo and fingerprints), as well as other personal information that is also physically recorded in the personal page of the passport
- The contents of the chip must be signed using strong cryptography and a non-revoked certificate issued by the authorities of the country in question that has been reported to ICAO and is possible to verify
- As part of the validation of the document's authenticity, the RFID chip in the document must be read by appropriate equipment and checked

- Identity documents without an RFID chip can not be used for digital onboarding

Validate ID owner + person = True

- We must validate that the ID owner and the person who carry out the digital identification is the same

- It is a key requirement that the photo in the RFID chip be compared to the physical appearance of the person carry out the digital identification. There should be a reasonable degree of consistency between the appearance of the person who presents the credential document and the image
- The verification carried out must be sufficiently secure to ensure that it is the correct person who performs the verification process and that the process is not manipulated
- For digital identification, it is important that the solution has a high degree of resistance to attack and fraud (masks, makeup, persons similar to the subject, video manipulation using avatars etc).
- The solution must be able to detect attack and fraud even in an environment that is considered compromised (rooting, jailbreak or equivalent).

Documentation of process

- The information read from the RFID chip must be documented
- Security items, how they were checked, and the result of the check must be documented
- It must be documented that the “ID owner + person = True” process has been completed
- All information must be sent to the issuer of the eID who is responsible to store this

Photographs

- Photographs submitted during digital onboarding may be used as a basis for comparison at a later date if and when this is needed.
- Photographs should include the following elements.
  - Picture taken from the pass RFID piece
  - Image of the person who completed the process and was used for face recognition
  - Picture of the document's cover page.

Transfer of data

- The transfer the data must be encrypted / privacy protected from solution to eID issuer.
- This means transport level encryption, but where content integrity has to be secured end to end by signing or equivalent technical solutions.

Other input

- Apple
- AML regulations vs eIDAS

Quick easy and personal - Without compromising security
www.idmee.com