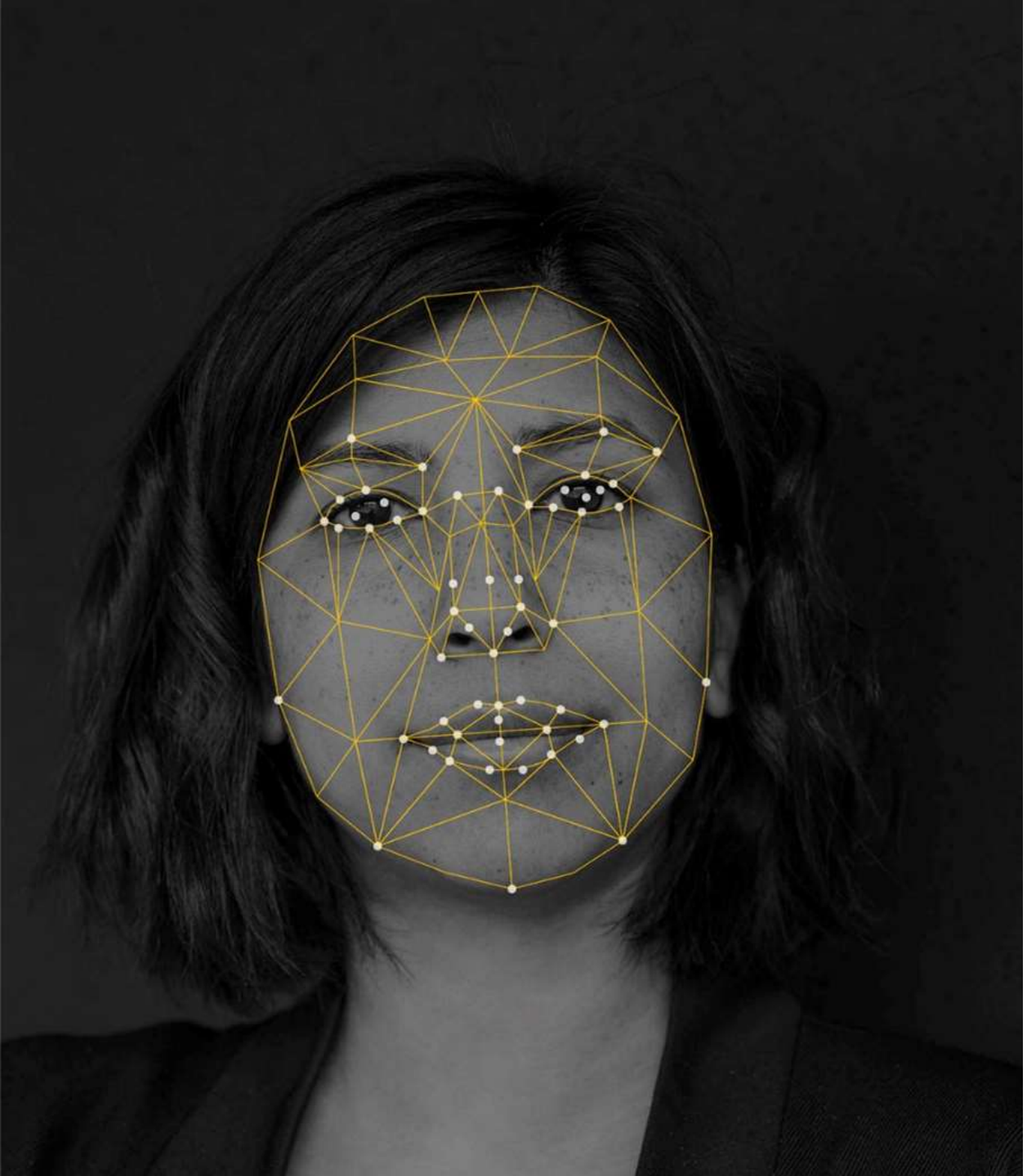


mobai

From **Secure Identity Verification**

to **Privacy-preserving Authentication**

for a **Better User-experience**

Erik Guoqiang Li
Director of R&D, Mobai AS, Norway
Email: erik@mobai.bio
Phone: +47 979 27 047

Agenda:

- A verdict of eID fraud case in the Supreme Court of Norway, 2020
- Apply face recognition based identity verification to prevent such fraud
- Apply Privacy-preserving authentication to improve user-experience
- Demo if time allows

- **A verdict of eID fraud case in the Supreme Court of Norway, 2020;**

https://www.dn.no/jus/hoyesterett/bankid-svindel/marte-eidsand-kjorven/full-seier-til-bankid-offer-i-hoyesterett-blir-kvitt-millionsgjeld/2-1-889906

Historisk BankID-dom i Høyesterett – full seier til offeret

En mann fra Sørlandet som ble et offer for BankID-svindel, og som deretter tapte i både tingretten og lagmannsretten, ble nylig frifunnet av en enstemmig Høyesterett. Høyesterett mener banken burde gjort mer for å forsikre seg om at låntaker virkelig var den han utga seg for å være. Banken bygget utelukkende på at låntakers BankID var benyttet, uten å foreta ytterligere kontroll av om avtalen faktisk ble inngått av ham.

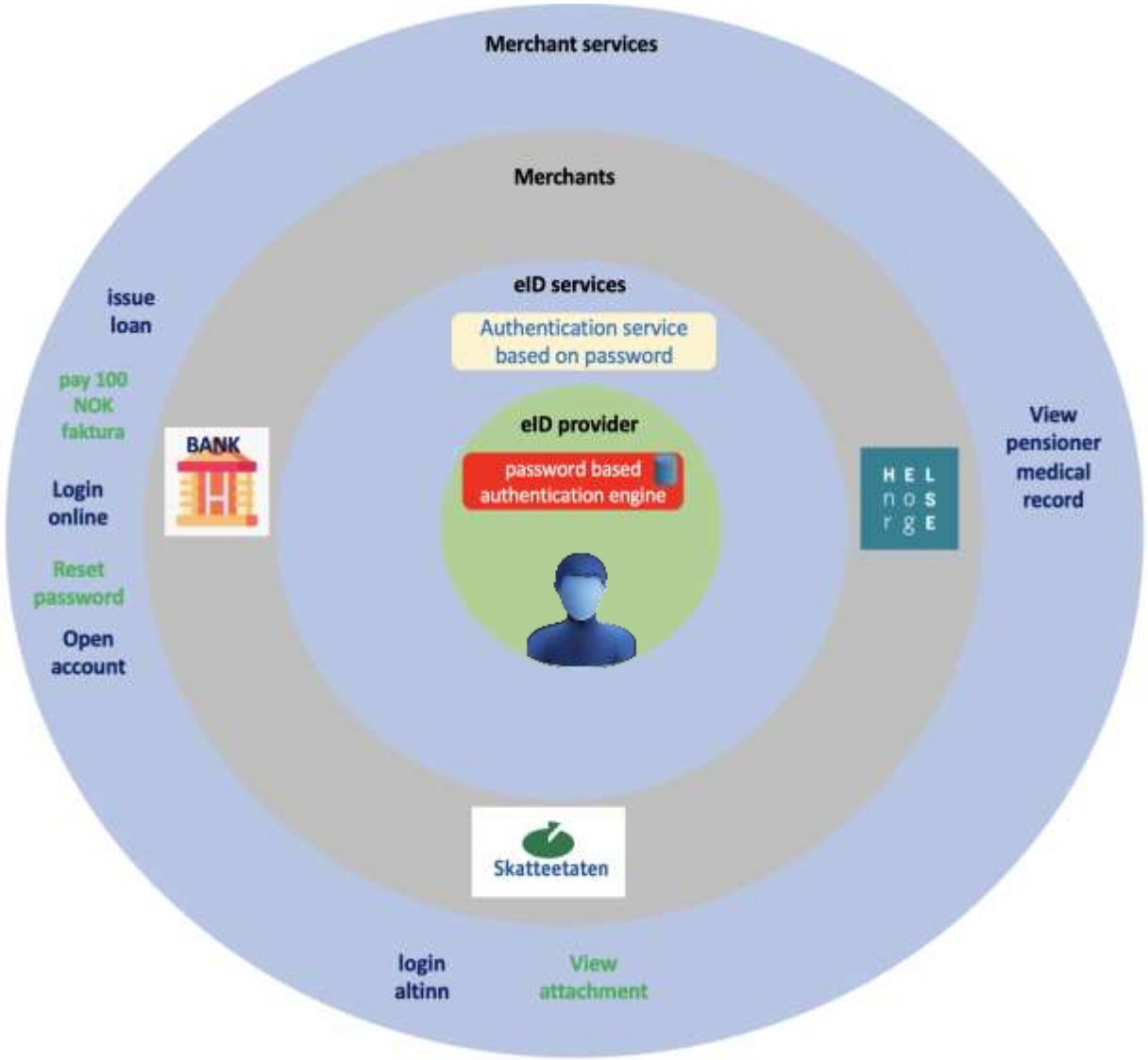
https://eurojurishaugesund.no/historisk-bankid-dom-i-hoyesterett-full-seier-til-offeret/

- *The Supreme Court believes that the bank should have done more to ensure that the borrower was really who he claimed to be.*

- *The Supreme Court states that the burden of proof will be on the party making the compensation claim. According to this, it is the bank that must provide evidence that there are circumstances that lead to liability in this type of case.*

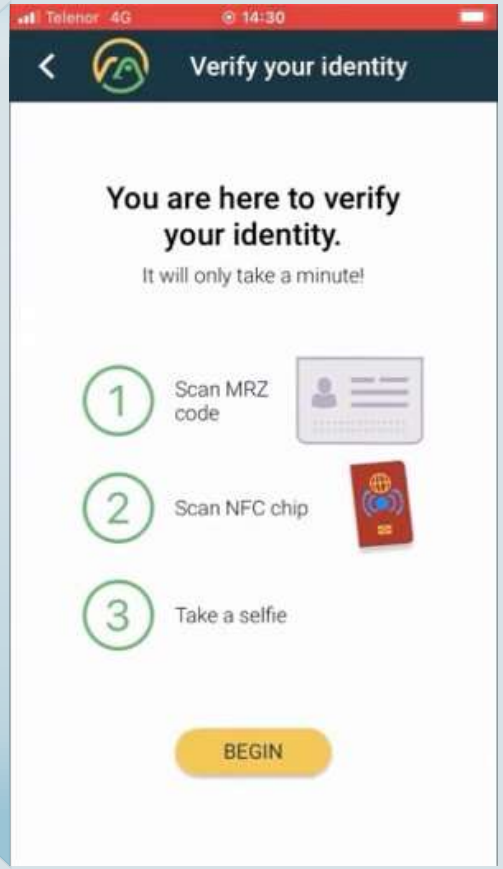
- *source: https://eurojurishaugesund.no/historisk-bankid-dom-i-hoyesterett-full-seier-til-offeret/*

❖ Apply face recognition based Identity Verification to prevent such fraud



Remote Identity Verification based on face recognition

At home



Driven by

Mobai services

Mobai Face Verification Docker Container

Certified by NIST National Institute of Standards and Technology U.S. Department of Commerce

Fraud detection modules

Mobai Face Liveness detection Docker Container

Certified by Biometrics Swiss Center for Biometrics

Mobai Deepfake detection Docker Container

Mobai Morphing detection Docker Container

Photo credit: https://www.amazon.de/Nautica-CH200-Schnellladeger%C3%A4t-Kompatibel-Navy/dp/B09PVN77Z1

European Standard to support eIDAS regulation

photo credit: https://www.identt.com/eidas-regulation-trust-services/

mobai

Shall Have: **Face verification 1:1 algorithm Face Presentation Attack Detection (PAD).**

Should Have: **Image manipulation detection (e.g, deep fake attack).**

May Have: **Face morphing attack detection.**

BITS requirement for face verification algorithm in Norway:

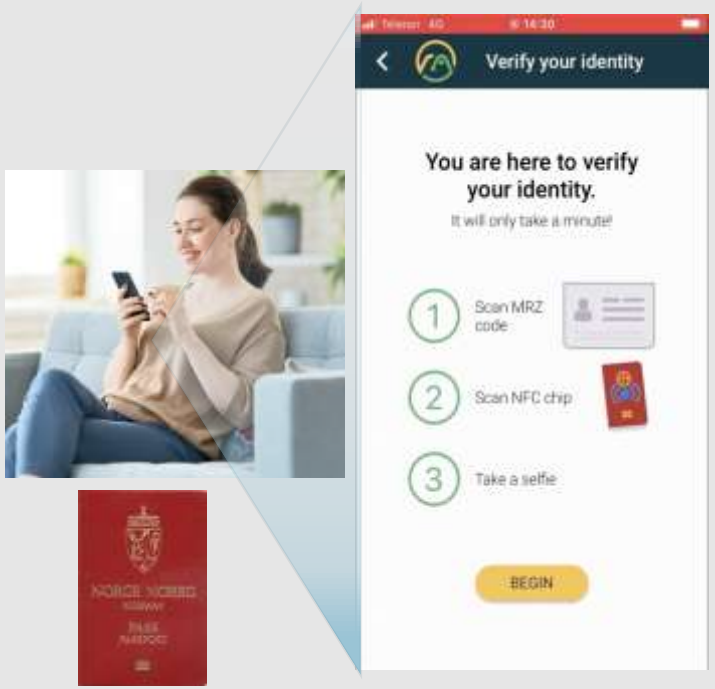
- Recommended to be evaluated by **NIST Face recognition vendor test (FRVT) with the following requirements:**
- 12.1.2:
  - FNMR rate of **less than 0,02 for FMR at 1e-05** according to the NIST Face Recognition Vendor Test (FRVT) for Visa photographs.
  - FNMR rate of **less than 0,02 for FMR at 1e-05** according to the NIST Face Recognition Vendor Test (FRVT) for Mugshot photographs.

Mobai face verificaiton algorithm meets these requirements with much better results,

Mobai PAD solution has been tested by Swiss Center for Biometrics Research and Testing which is a FIDO Accredited Biometric Laboratory, result: BPCER=0%@APCERT0%

Remote Identity Verification based on face recognition

At home



Driven by

Mobai services

Mobai Face Verification Docker Container
Certified by NIST National Institute of Standards and Technology U.S. Department of Commerce

Fraud detection modules

Mobai Face Liveness detection Docker Container
Certified by Biometrics Swiss Center for Biometrics

Mobai Deepfake detection Docker Container

Mobai Morphing detection Docker Container

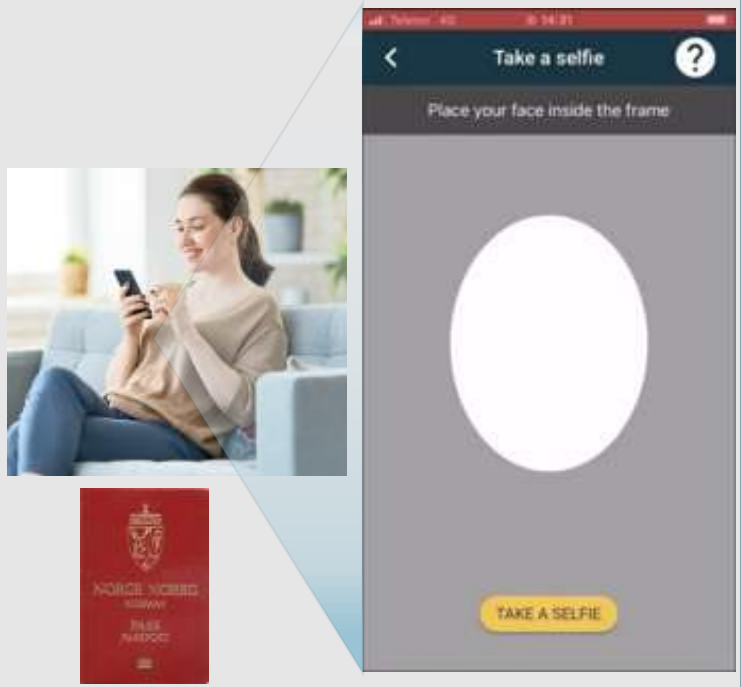
Passport photo

Photo credit: https://www.amazon.de/Nautica-CH200-Schnellladeger%C3%A4t-Kompatibel-Navy/dp/B09PVN77Z1

Remote Identity Verification based on face recognition

After storing the reference, time for ID verification can be reduced from more than 30 seconds to less than 3 seconds.

At home



Driven by

Mobai services

- Mobai Face Verification Docker Container
  Certified by NIST National Institute of Standards and Technology U.S. Department of Commerce
- **Fraud detection modules**
  - Mobai Face Liveness detection Docker Container
    Certified by Biometrics Swiss Center for Biometrics
  - Mobai Deepfake detection Docker Container
  - Mobai Morphing detection Docker Container

Passport photo

Photo credit: https://www.amazon.de/Nautica-CH200-Schnellladeger%C3%A4t-Kompatibel-Navy/dp/B09PVN77Z1

Remote Identity Verification based on face recognition

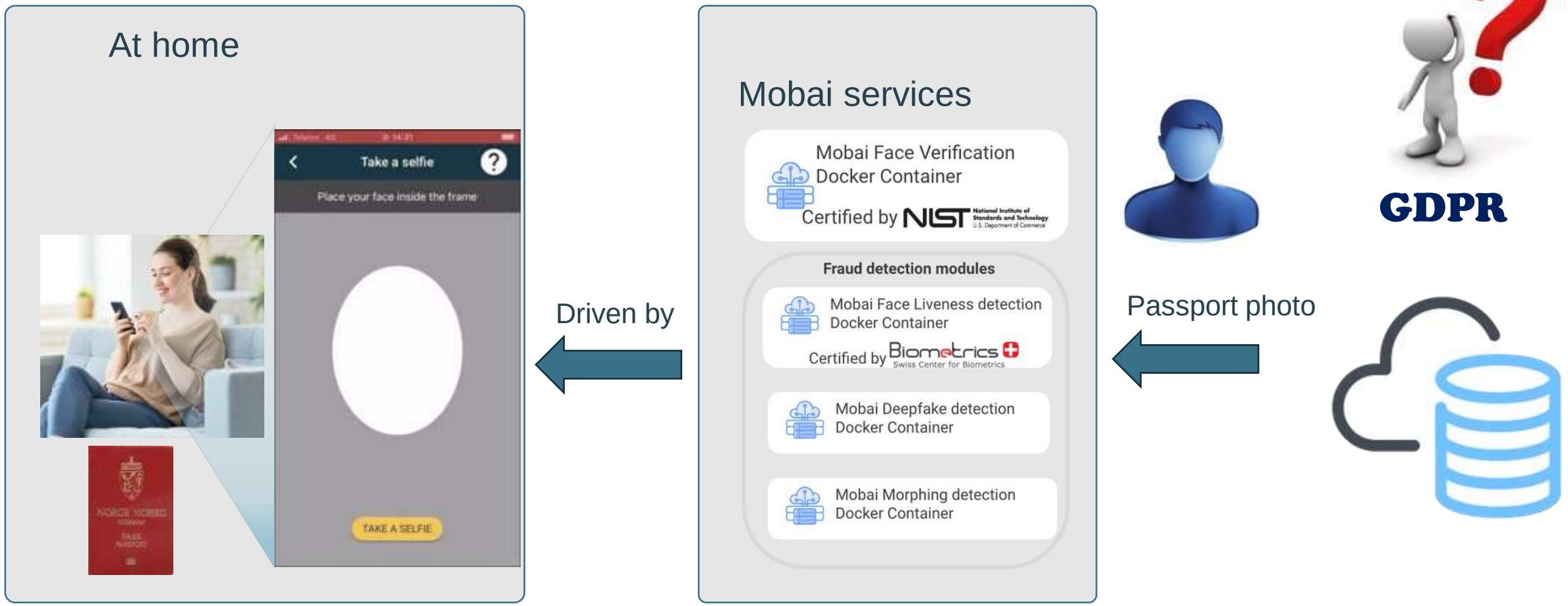


Photo credit: https://www.amazon.de/Nautica-CH200-Schnellladeger%C3%A4t-Kompatibel-Navy/dp/B09PVN77Z1

Security and privacy threats

- when storing biometric reference data

Defined by ISO/IEC24745:2022 Information security, cybersecurity and privacy protection

	Threats	Countermeasures
Storage	Database compromise — Unauthorized disclosure of BR/IR — Unauthorized replacement of BR/IR — Unauthorized modification of BR/IR — Unauthorized deletion of BR/IR — Distributed denial of service attack	— Revocable and renewable biometric references — Data separation — Database access control — Sign BR/RBR/IR — Encrypt BR/RBR/IR — Appropriate contingency planning and recovery procedures

7.1 Biometric information privacy threats

Since biometric data are PII, ISO/IEC 29100, which is a general privacy framework addressing system specific issues at a high level, should be applied. It is a general framework that addresses organizational, technical, procedural and regulatory aspects of privacy for IT systems which process and store personal identifiable information. The use of biometric data involves several threats to privacy which shall be addressed:

— Biometric references can be used to link subjects across different applications in the same database or across different databases. Privacy is related to the unlinkability of the stored BR.

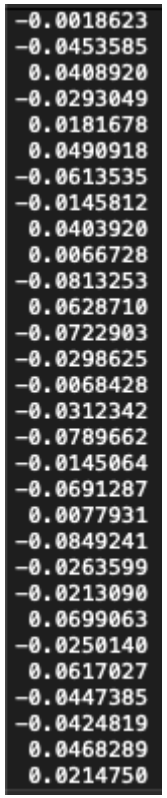
❖ Privacy-preserving authentication to improve user-experience

mobai

Fully Homomorphic Encryption → Quantum Safe Encryption

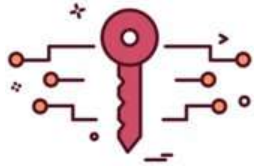
Face plaintext template

Passbilde



Secured by
Fully Homomorphic
Encryption

Encrypted with a key



Protected template

```
5e63871acdf4441e5552cd9b32ac679e60f662a6
9528e7ac13abad23ff45b01031e6cd07deb91197
3fe822732bde252508529b3975f7349a8571fb55
```

Store the protected templates for providing authentication service.

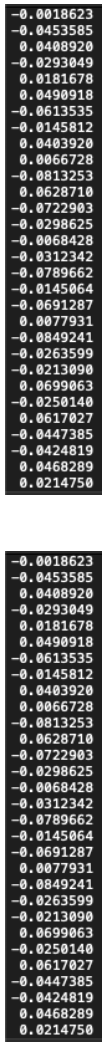
❖ Privacy-preserving authentication to improve user-experience

mobai

Face plaintext template

Passbilde

Selfie



FHE

Secured by Fully Homomorphic Encryption

Encrypted with a key

FHE

Secured by Fully Homomorphic Encryption

Encrypted with a key

This part can be deployed in a cloud environment

Protected template

5e63871acdf4441e5552cd9b32ac679e60f662a6
9528e7ac13abad23ff45b01031e6cd07deb91197
3fe822732bde252508529b3975f7349a8571fb55

Compare under encrypted domain

7c33a162fd6ecdfc8b2da78dd5e671fc54e81a77
2ba0e5c2bce24e84c42cad0f3f947ddc1f329c2c
881ac9dd5bbd3a7b97982b8ab988d9758cd7d3

Encrypted Score

3640100d8e718f00420a25afc03314476526f9e3
b26291f133d0875932a5ef56dfb9de406b46a666

Similarity Score

96.8%

Decrypt with a private key

- **Recognition Accuracy evaluation**

Selfie alike images

	Mated comparison	Non-mated comparison
Without BTP	FNMR=0/1969=0%	FMR=0/1,937,496=0%
With BTP	FNMR=0/1969=0%	FMR=0/1,937,496=0%

Threshold is decided when FMR=0.000001

Low quality/partial face images

	Mated comparison	Non-mated comparison
Without BTP	FNMR=85/1969=4.3%	FMR=0/1,937,496=0%
With BTP	FNMR=91/1969=4.6%	FMR=0/1,937,496=0%

Conclusion: no performance deterioration

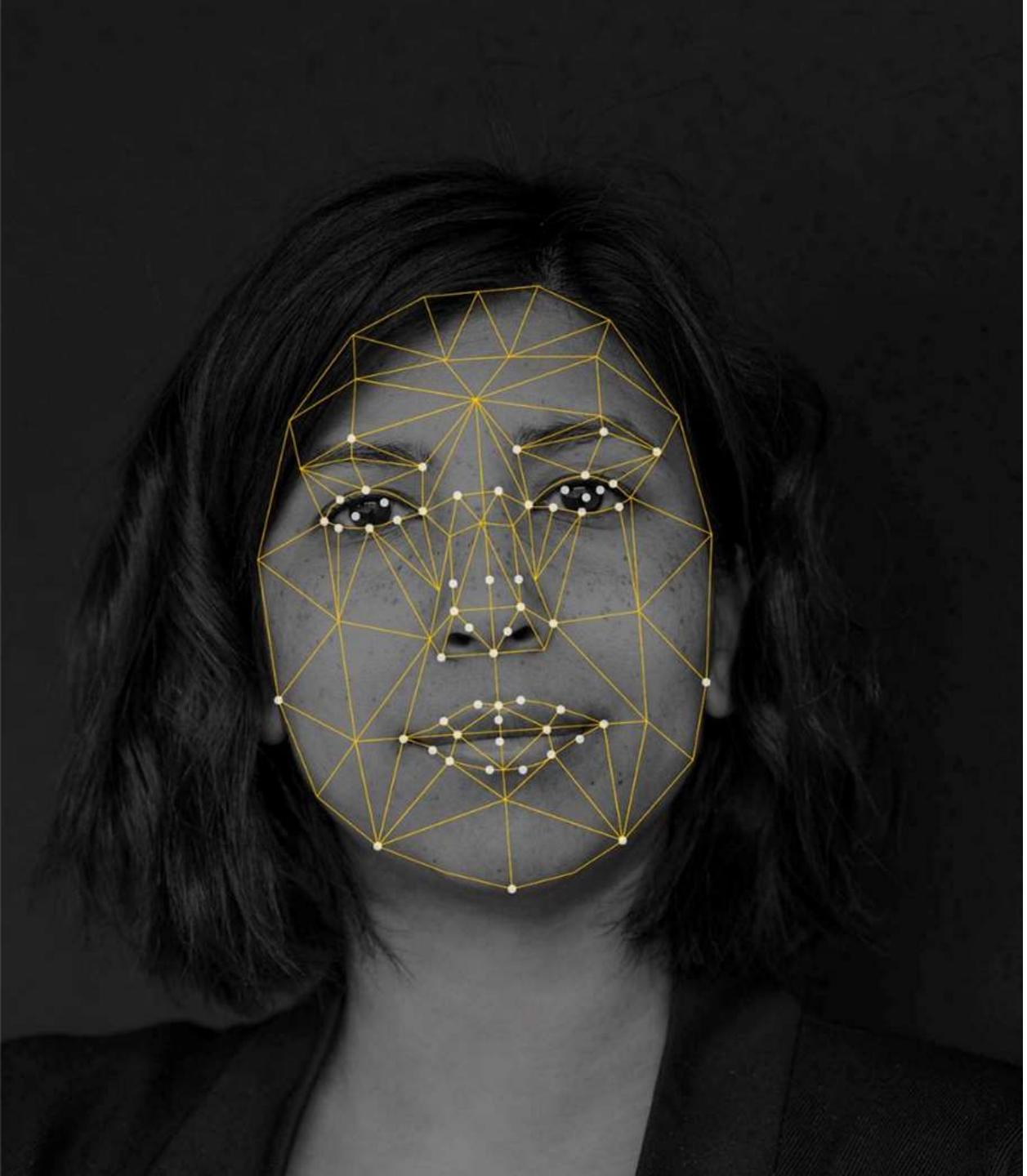
Conclusion: the performance deterioration is negligible.

Image source: NIST Color FERET dataset.

Efficiency Evaluation

	Generate templates from two images	Compare two templates	Encrypt two templates	Compare two encrypted template	Decrypt a similarity score
Average time	256 ms (based on NIST FRVT report)	1386 ns (based on NIST FRVT report)	13 ms	34 ms	2 ms
			Tested on a laptop with Intel Core i7-8650U CPU @1.9GHz		
Average time	Without template protection: ≈256 ms		With template protection: 256 + 49 = 305 ms		

Conclusion: the computation load is NOT an issue after applying homomorphic encryption.



Thank you!
Any question?

Erik Guoqiang Li
Director of R&D, Mobai AS, Norway
Email: erik@mobai.bio
Phone: +47 979 27 047