Biometrics in banking in practice

Peter Gullberg, VP Strategy, Digital Banking
2017-09-27

gemalto
security to be free

Gemalto - leader in biometric security

Government
Passport and ID Issuing




Government
Border control




Enterprise
Access control solutions

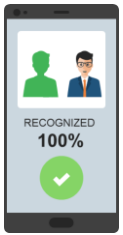

FINGERPRINT
SCANNERS

Bank
KYC / Document Verification




Bank
Remote onboarding





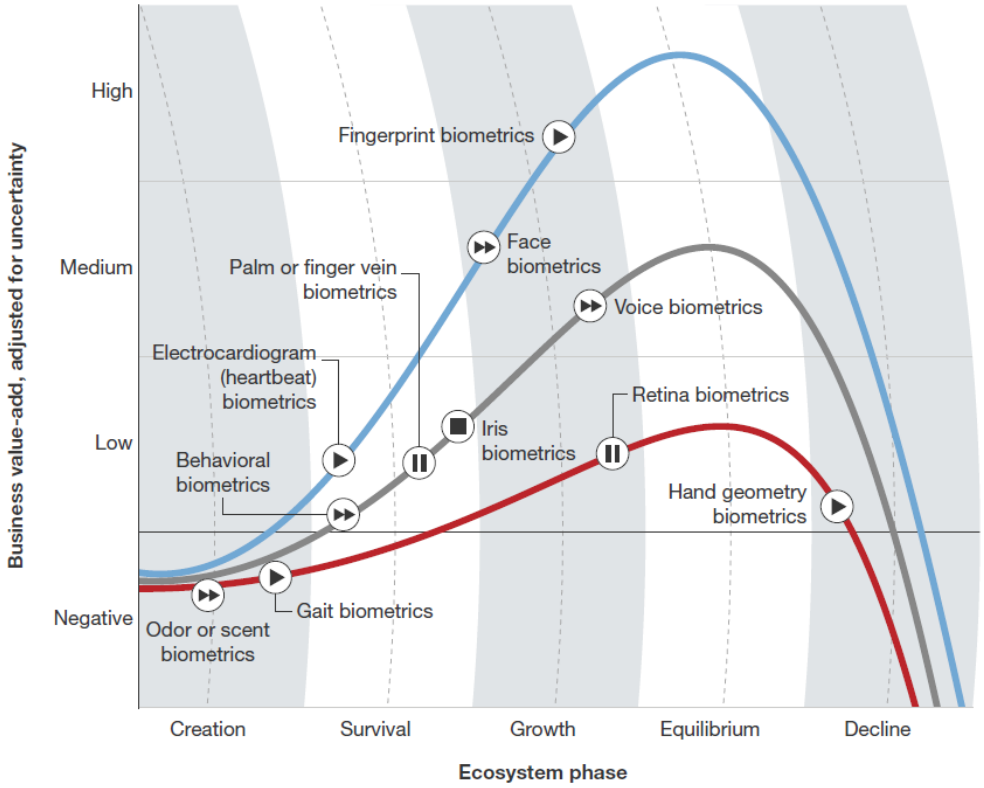
Bank
Authentication / Payment



gemalto

Current state of Biometrics and trends

Biometric Authentication - TechRadar



TechRadar™: Biometric Authentication, Q1 2017

Trajectory:

- Significant success
- Moderate success
- Minimal success

Time to reach next phase:

- < 1 year
- 1 to 3 years
- 3 to 5 years
- 5 to 10 years
- > 10 years

gemalto

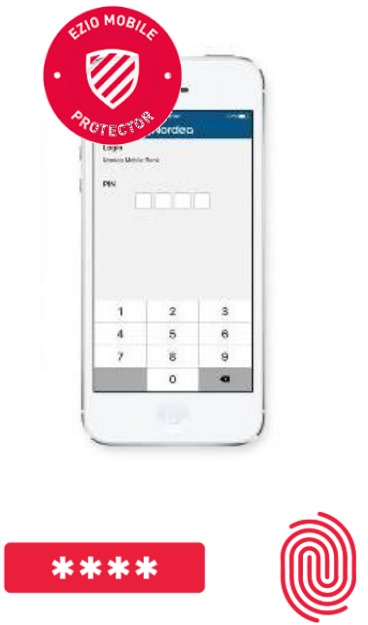
Insights on how to successfully deploy biometrics

Customer cases of Biometrics deployment

gemalto

Nordea Bank - Authentication

- Mobile Banking
  - Authentication & Signatures
  - Out-of-band Signatures
- Strong Customer Authentication using FingerPrint or PIN
- Deployed in Finland and Baltics. Other countries in progress
- Using Gemalto Ezio



Identity Verification in branch (KYC)

Rabobank

The need: Strengthen identity verification procedures in-branch to:

- Reduce identity fraud at subscription time
- Comply with AML regulations
- Automate and digitalize customer onboarding processes

Gemalto selected after an 18-month pilot
1000 workstations deployed

John goes to a branch to open a new account in Rabobank.

He is advised by a sales person. Together, they select the right product for him.

The vendor scans his Identity document using a dedicated scanner.

In a few seconds, John's ID is verified, and his information is automatically input in the CRM!

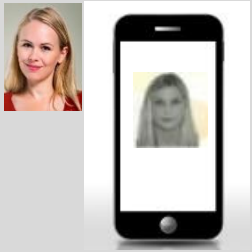
Identity Verification in a large bank in France (Remote KYC)

The need: Mainly through its personal loan activities, the bank is experiencing a **high level of identity fraud** with a limited time to make a sale.

- Strengthening their identity verification processes is a must: ID fraud represents a **significant** credit line **loss** as well as **a legal and image risk**.
- **The main use case is in-branch** verification, **but online verification will also be implemented!**

Alice wants to use the services of Bank A. She goes to a branch, is advised by a vendor, and selects the service.

Using his tablet, the vendor takes a picture of Alice's ID card.



Then the vendor verifies that Alice is the right person (no facial recognition).

Alice's identity is validated in less than a minute, and she can start using the service.

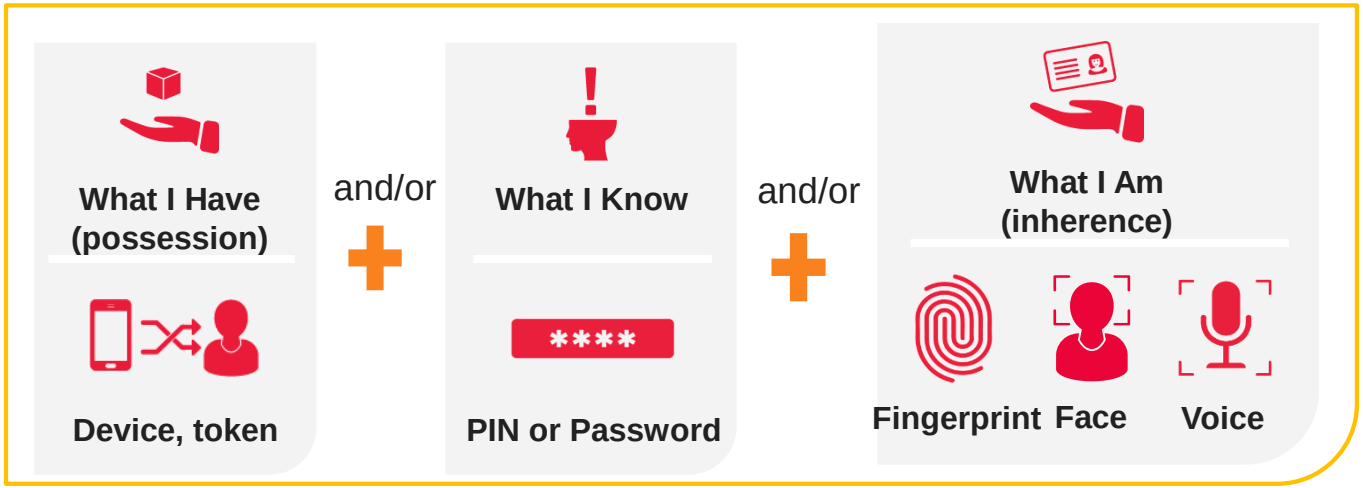
PSD2 and Biometrics

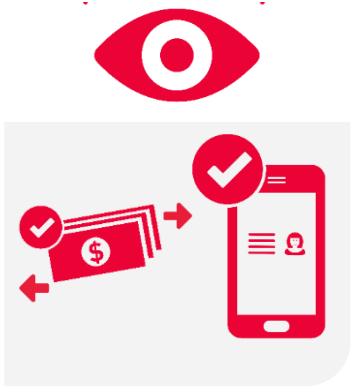
Reduce risk and increase convenience

gemalto

About Strong Customer Authentication and Dynamic Linking

PSD2, Art.97





Dynamic link of transaction to amount and payee (for payments and money transfers)

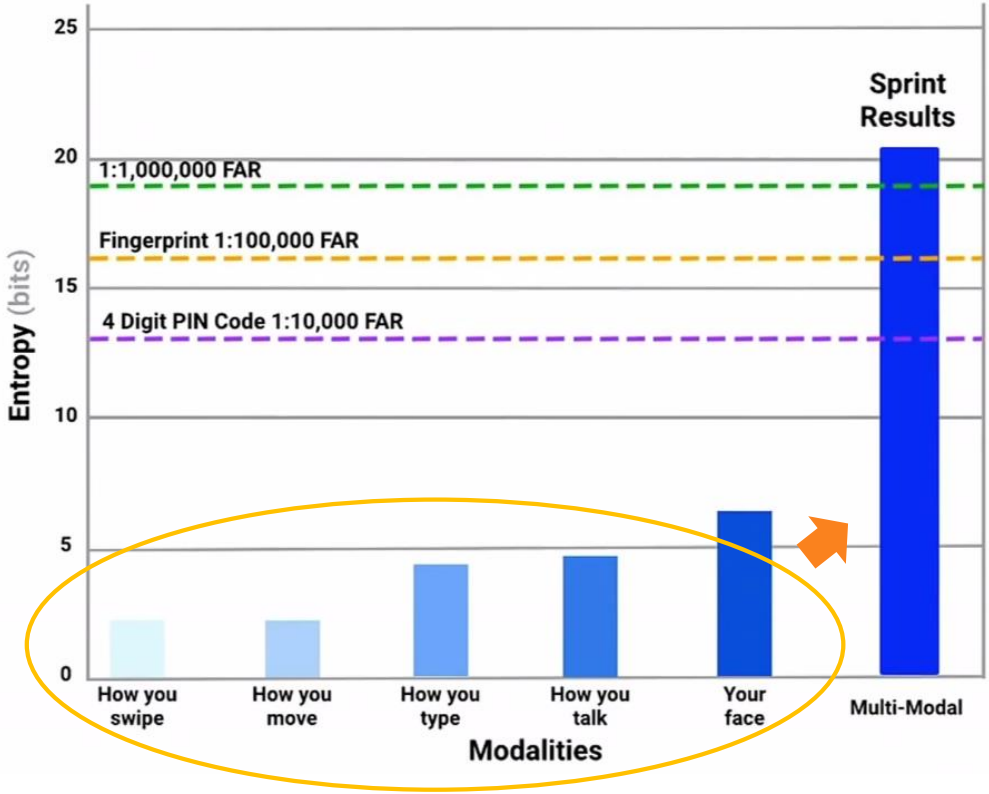
Independence: compromise of one factor shall not lead to the compromise of any other

RTS: Article 4 - "**the authentication based on two or more elements categorized as knowledge, possession and inherence** shall result in the generation of an authentication code."

gemalto

Multimodal security

- *Multimodal security - "Applying more than one security control or countermeasure"*
- By combining several biometric and other factors we achieve a security that is significantly higher than each individual factor

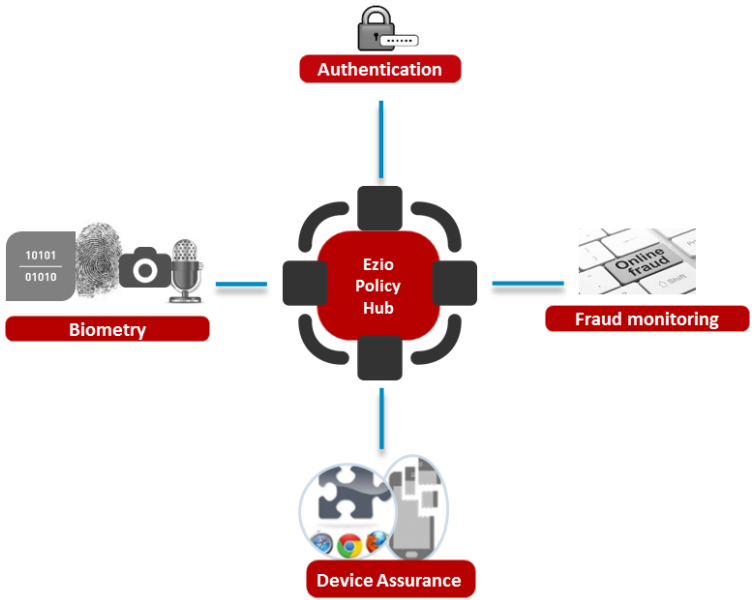


Google - Project abacus
(Sprint result is a the combined entropy of the modalities)

gemalto

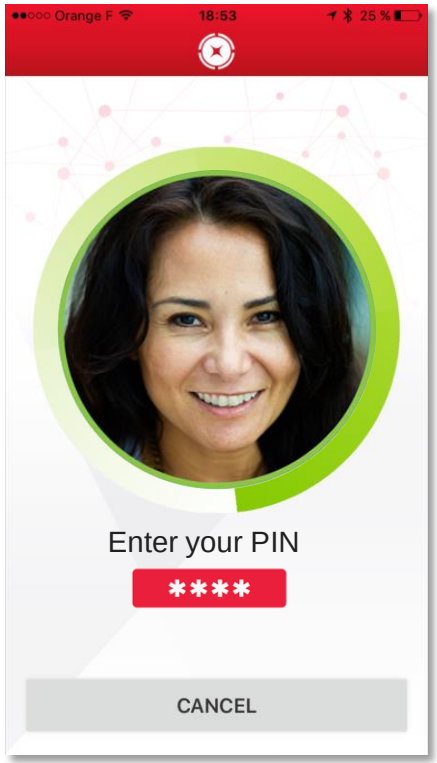
Multimodal security hub

- Aggregate all **user assurance** modalities, including **authentication**, **device assurance**, and **Fraud Monitoring**
- Allows bank to balance usability and security based on risk and context
- Reduce friction by using multimodal decision policy



gemalto

Example of multimodal authentication



What I Have (possession)

What I Know

What I Am (inherence)

Device, token

PIN

Behavior

Face

gemalto

KYC / Document and Identity Verification

WHO IS HE?

1. Document Verification
2. Biometric Authentication
3. Risk Assessment
4. Identity Verification report
5. Auto form filling CRM integration

JOHN SMITH

Mobile Device Activation

WHO IS HE?

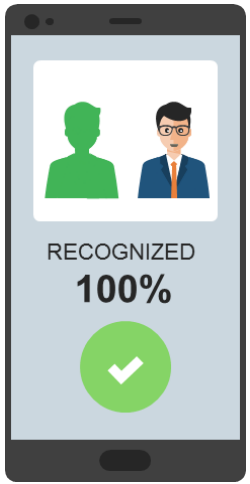
1 Document Verification

2 Biometric Authentication

3 Risk Assessment

4 Identity Verification report

5 Auto form filling CRM integration

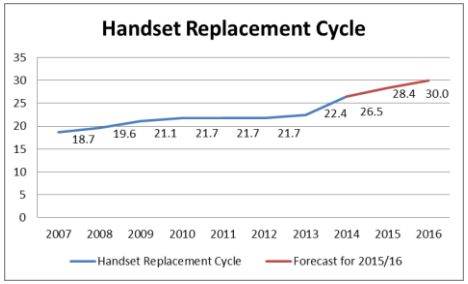


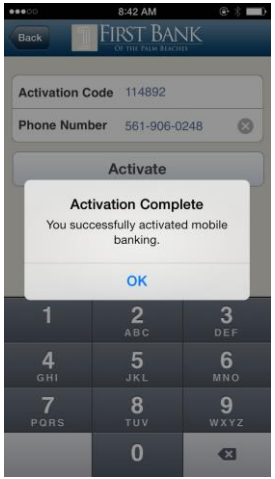
JOHN SMITH

gemalto

Mobile Device Activation

- Handset replacement cycle is around 18-24 month
- Each time a customer gets a new handset, he need to activate the device for use for banking services
- Example:
  - **A bank with 1 million customers**
  - **Customer buys in average a new device every 2 years**
  - **>40K Mobile Device Activation per month**
- Takeaway: It needs to be convenient

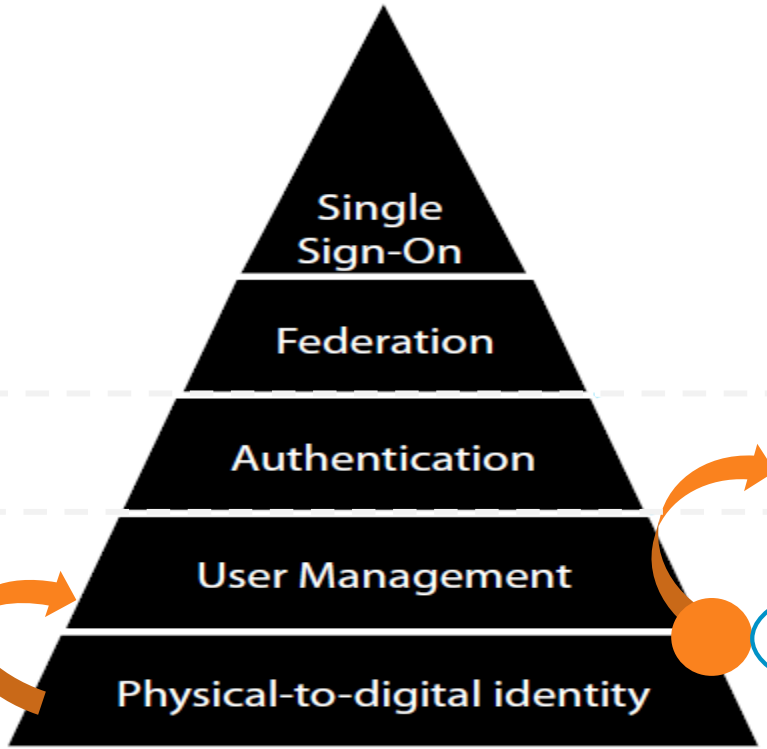




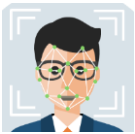
Biometric in the IAM pyramid

Identity Document Revalidation

KYC/ CDD

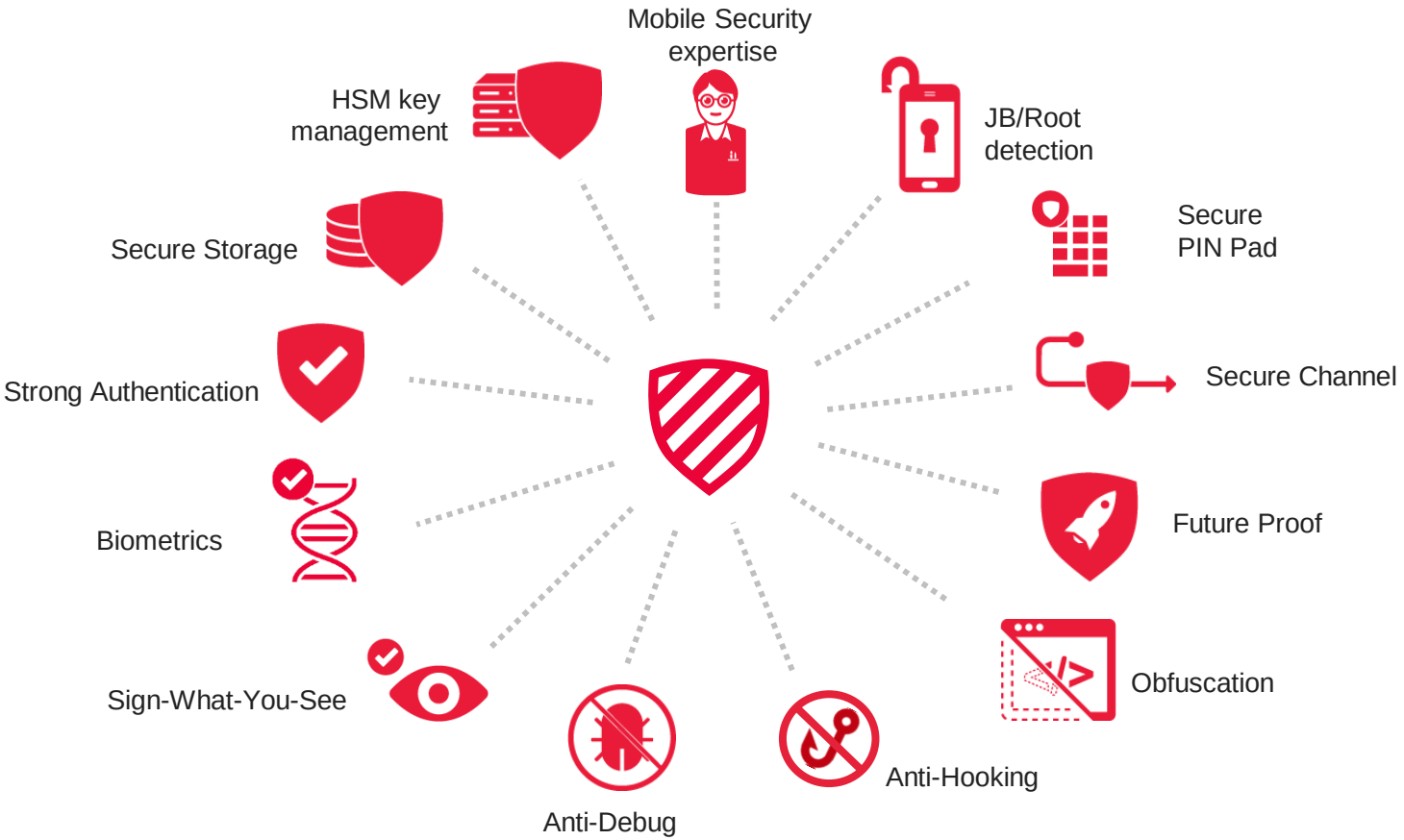


Mobile Onboarding



gemalto

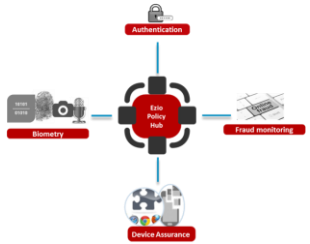
A layered approach for PSD2 Compliance



gemalto

Conclusion and suggestions

- Biometric is about convenience, let user chose, and keep fall back options
- Balance usability and risk by combining multimodal biometrics with security to reduce friction and fraud
- Make sure it's easy to onboard customers and their devices
- Make sure you partner with a solution provider that can help you with all these aspects. Gemalto is here for you



Thank you

Thanks

gemalto
security to be free