BankID

BankID Digital Identity

BankID Digital Identity Platform – A modern life enabler

- **BankID intro**
  - the company, the product, light demo

- **BankID functionality**
  - Authentication
  - Digital transactional signature
  - Digital Onboarding
    - ID document verification (Passport and ID-card)
    - Biometrics / face recognition
  - Digital ID issuing

- **Security & Tech**
  - Way of working. How come 18 years without breaches?
  - High level security description
  - Tech overview, how does it work?
  - Development, Architecture and Operations. BankID way of working from these perspectives in order to ensure security, quality, performance and availability.
  - Risk & fraud capabilities
    - Risk-engine & Anti-fraud

- **Q&A ongoing during the seminar**

BankID - Base facts

Why BankID

BankID figures

7B+ transactions	8M end users 98,5% of SE population	6K+ integrated service providers	100% of Swedish banks	99,99% availability	79 NPS score

BankID platform

- Digital onboarding
- Electronic signing
- Fraud analytics
- Mobile ID
- Biometrics
- Identity access management
- Authentication
- Risk engine
- Privacy protection

BankID ref cases (among the 6000+)

P2P payments swish

Integrator CGI

Digital mail KIVRA

E-health KRY 1177 VÅRDGUIDEN

Governmental Skatteverket

Logistics/e-com postnord

Banking/Fintech Nordea DNB

Automotive VOLVO

BankID

Advantage BankID

Operations

- Size and scalability
- 18 years in operation / no security breach
- Vast ecosystem circum navigating BankID

Risk reduction

- Proven real time risk engine and fraud prevention tool set

Digital Onboarding

- Bank security level digital onboarding incl. biometrics, liveness control and Passport/ID card chip sensing

Security

- Bank security level for Authentication, transaction/agreement Signature, Digital Onboarding and Fraud prevention

User experience

- NPS 79 (Net Promoter Score)
- Milli second process time

The Digital Ecosystem

Get the app from
App Store or Google play

The ID Provider
grants you a digitial ID

Get access to 6000+ services
with one identity, one password

The Digital Ecosystem

BankID

User Apps
iOS / Android

Base Services
User Authentication
Electronic Signature
Onboarding ID Provider
Onboarding Service Provider
eID Issuing
eID Blocking
Reports
Support

Add-On Services
Risk Engine
Fraud Analytics
Extended eID
User Notification
Professional Services
Extended Support

Handelsbanken
Swedbank
SEB
Nordea
Danske Bank
Länsförsäkringar Bank & Försäkring
ICA banken
ÅLANDSBANKEN
Sparbanken Syd
skandia

Digital ID as a Service

BankID DevHub

CGI
scrive.
Signicat
Svensk E-IDENTITET
IDKOLLEN

Main sector

Mathem
AVANZA
skandia
benify
ICA
3
KRY
net on net
swish®

Public sector

VELLINGE KOMMUN
NACKA KOMMUN
Skatteverket
DIGG MYNDIGHETEN FÖR DIGITAL FÖRVALTNING Agency for Digital Government

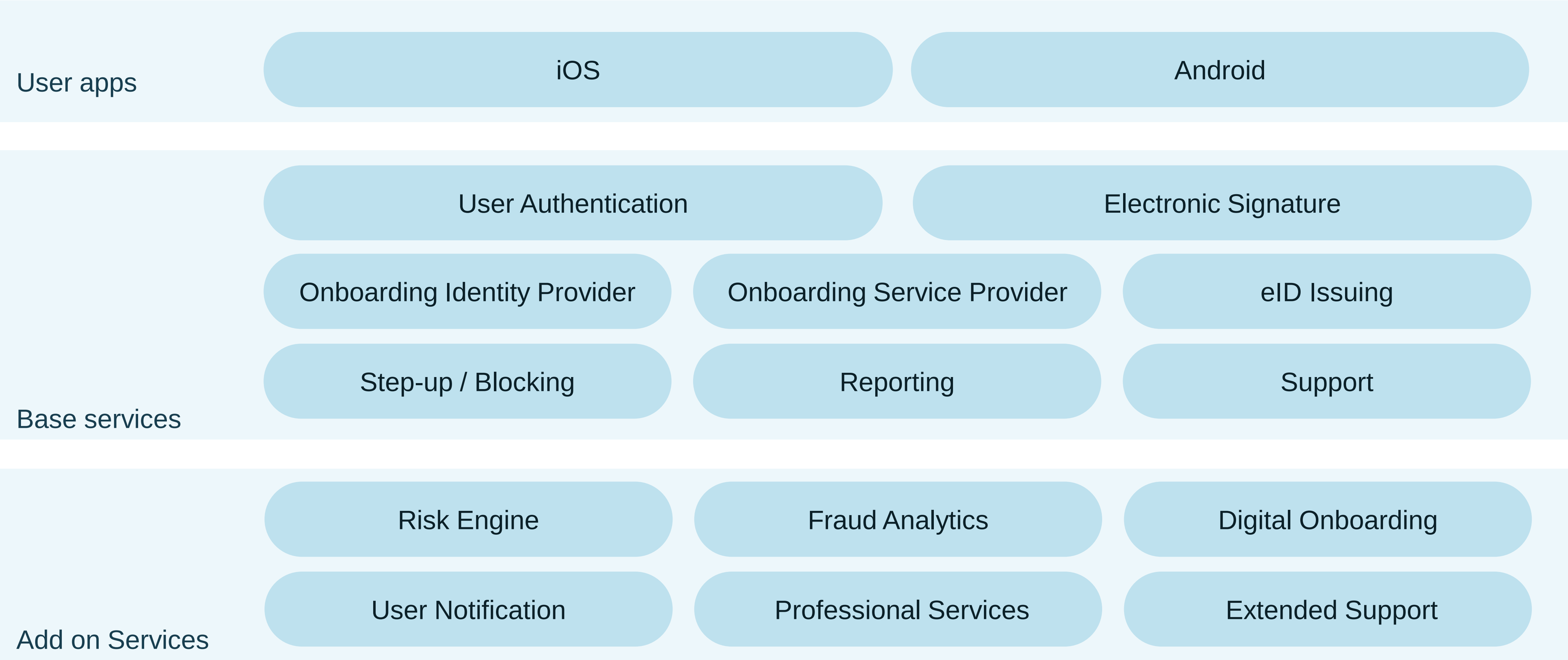
Services → Distributers → Service → Integrators/Partners → Service Provider → End users

BankID

The BankID Identity Platform

Functionality

BID Identity Platform



User apps

iOS

Android

Base services

User Authentication

Electronic Signature

Onboarding Identity Provider

Onboarding Service Provider

eID Issuing

Step-up / Blocking

Reporting

Support

Add on Services

Risk Engine

Fraud Analytics

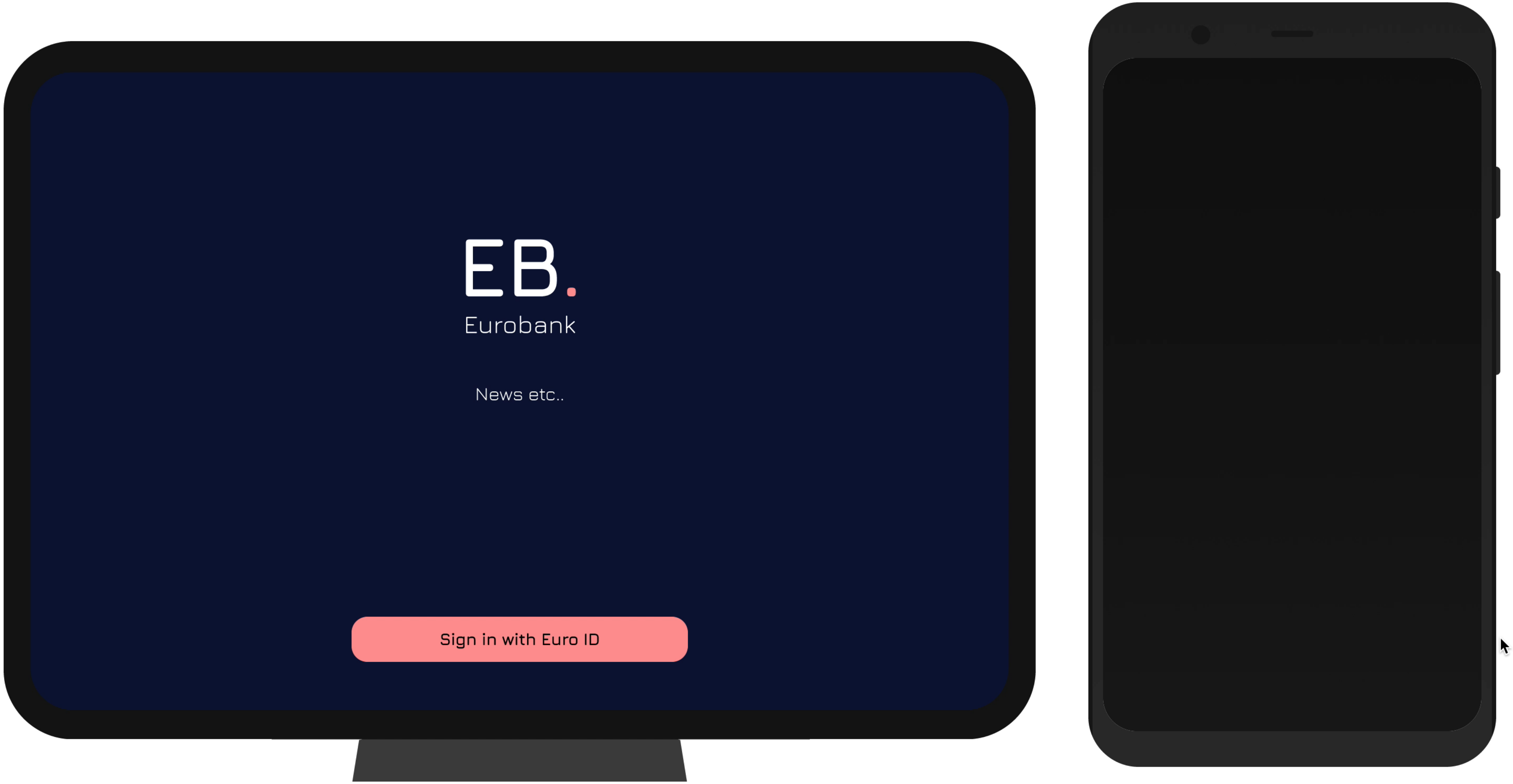
Digital Onboarding

User Notification

Professional Services

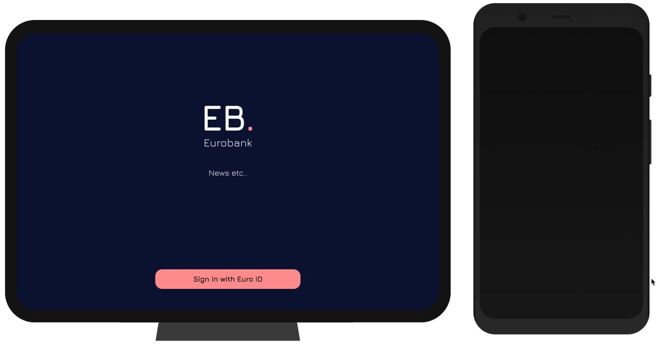
Extended Support

Customer Authentication



Functionality

Customer/User Authentication



Digital Signature

- In use case P2P Payment (Swish)

BankID Digital Onboarding (incl. ID document verification & face biometrics)

- https://drive.google.com/file/d/1kT86Xb_c8YoVgMoTL1JtNapFUicYg1ZJ/view
- https://cdn.bankid.com/video/BankID_Instruktionsfilm_en_sub.mp4

The Trust Framework and Digital Scheme for Issuers of BankID

Regulatory framework to create and maintain:

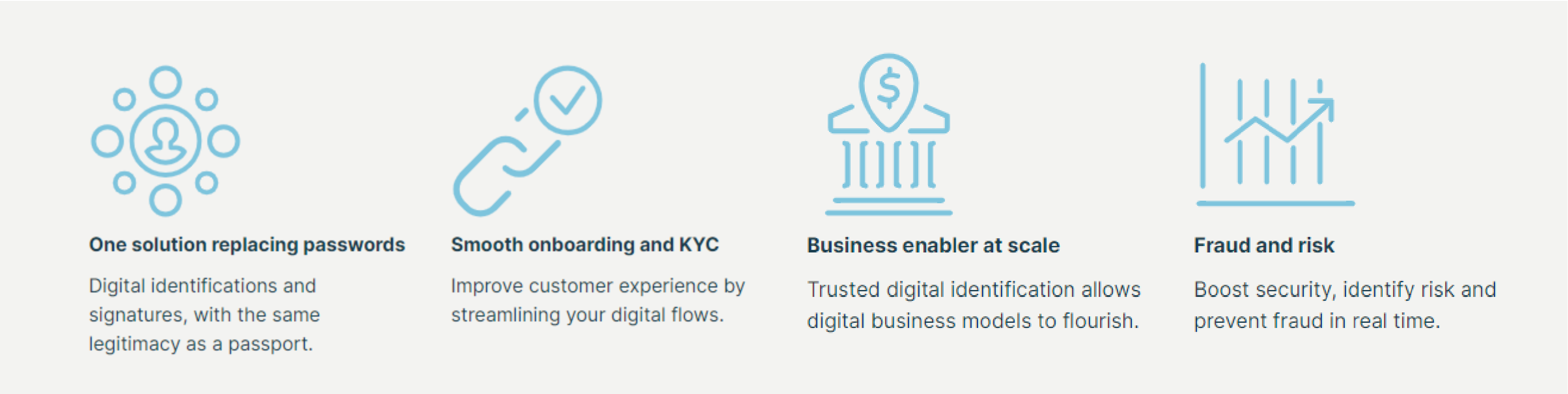
- A high level of trust to the common framework for all stakeholders (ID providers, Service providers, end users and government)
- A high level of security
- Clear responsibilities
- Governance structure

All issuers need to comply to the framework, consisting of:

- Process and procedures
- Technical requirements
- Legal requirements
- Security standards
- Internal / External Audits
- Requirements on Service Provider and End User onboarding
- Service Levels

Maintaining the framework

- One owner of maintaining, developing and follow-up on compliance
- Participation in joint forums



One solution replacing passwords

Digital identifications and signatures, with the same legitimacy as a passport.

Smooth onboarding and KYC

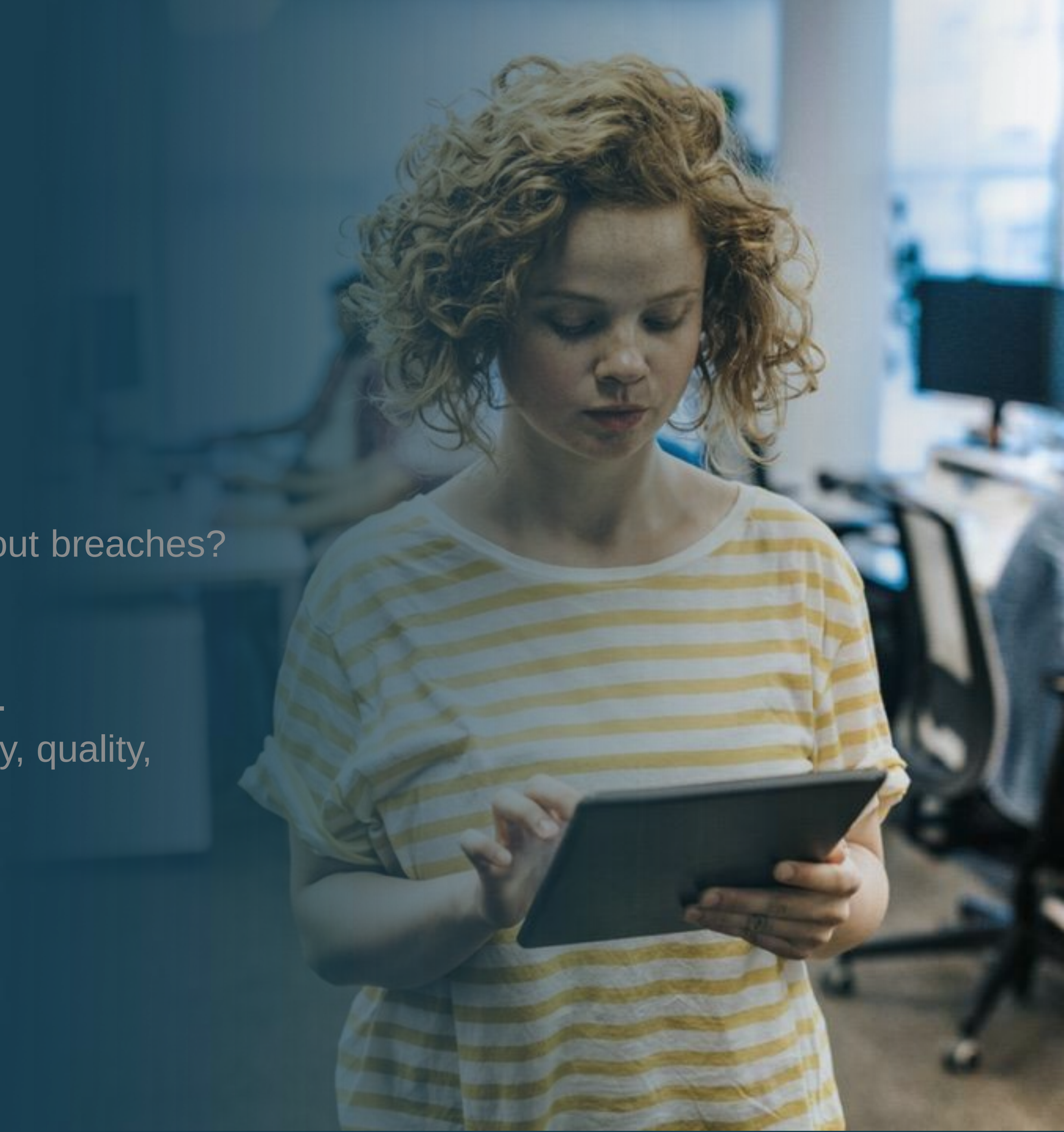
Improve customer experience by streamlining your digital flows.

Business enabler at scale

Trusted digital identification allows digital business models to flourish.

Fraud and risk

Boost security, identify risk and prevent fraud in real time.



Security & Tech

- Way of working - How come 18 years without breaches?
- High level security description
- Tech overview - how does it work?
- Development, Architecture and Operations.

  BankID way of working ensuring security, quality, performance and availability

How to create trust in a digital identity, enabling an ecosystem

Secure Customer ***Onboarding***

Strong Customer ***Authentication & Signature***

Context is key

Easy to do the right thing

Protect systems & customers data

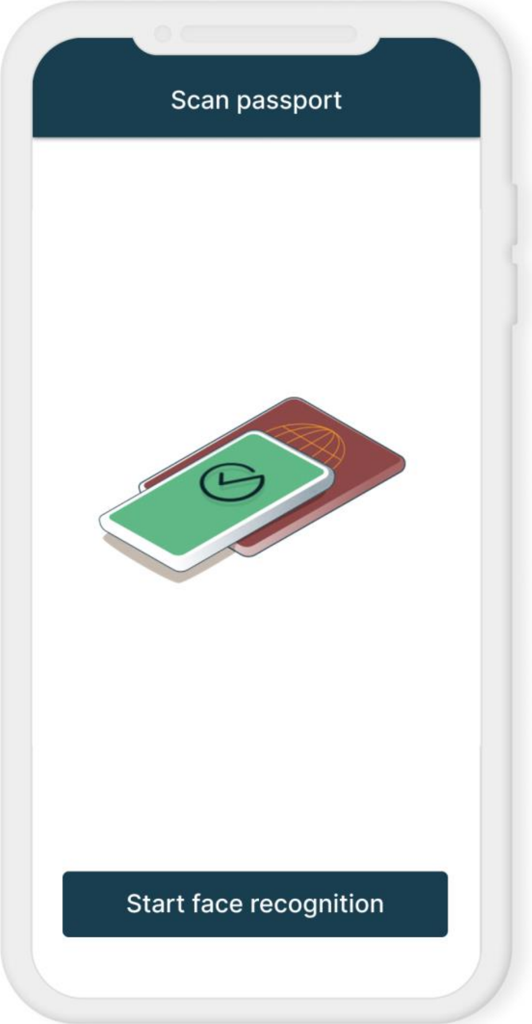
Common ***framework*** & digital scheme

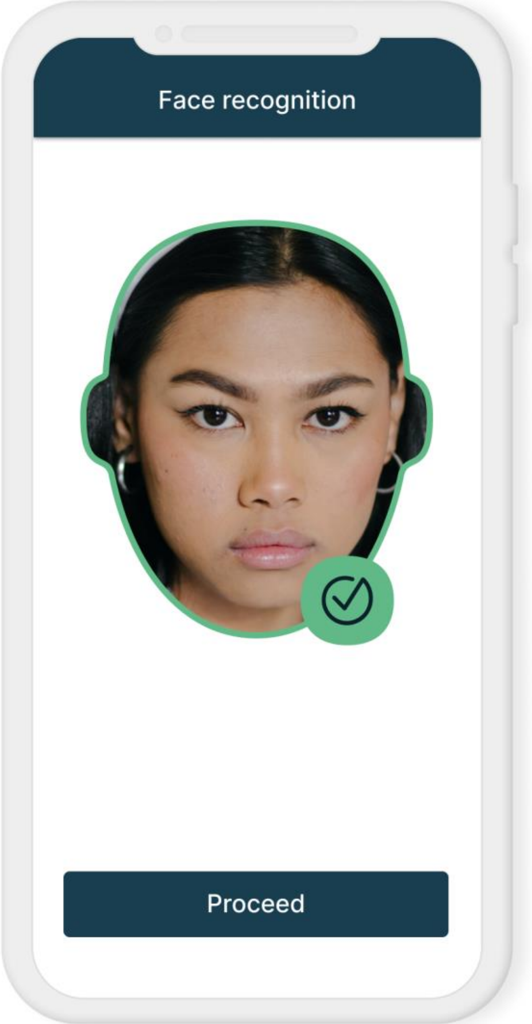
Realtime Risk Assessment

Prevent and monitor ***Fraud***

Secure Customer Onboarding

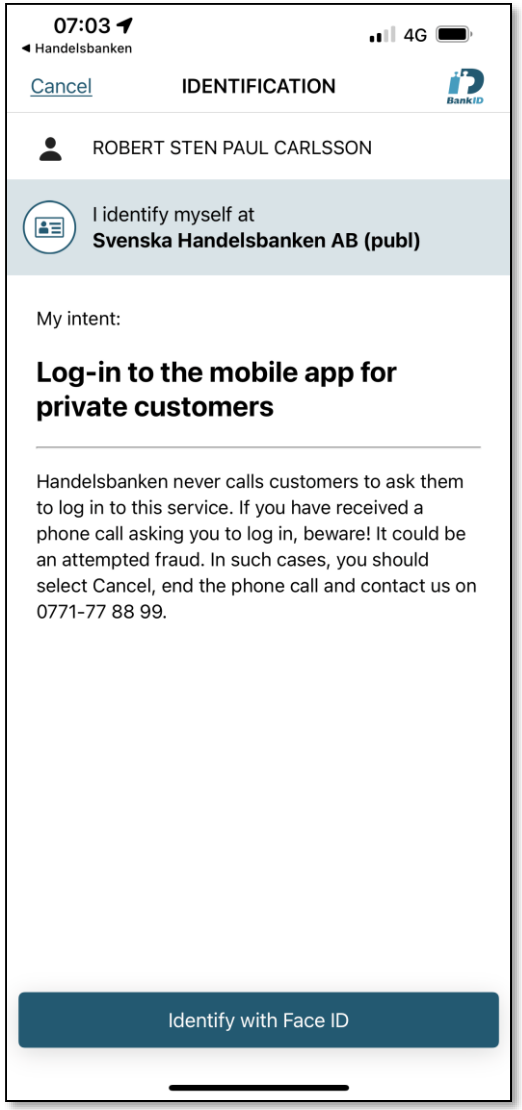
Secure Customer
Onboarding





Strong Customer Authentication

Strong Customer
Authentication & Signature



07:03
◂ Handelsbanken
4G

ROBERT STEN PAUL CARLSSON

I identify myself at
Svenska Handelsbanken AB (publ)

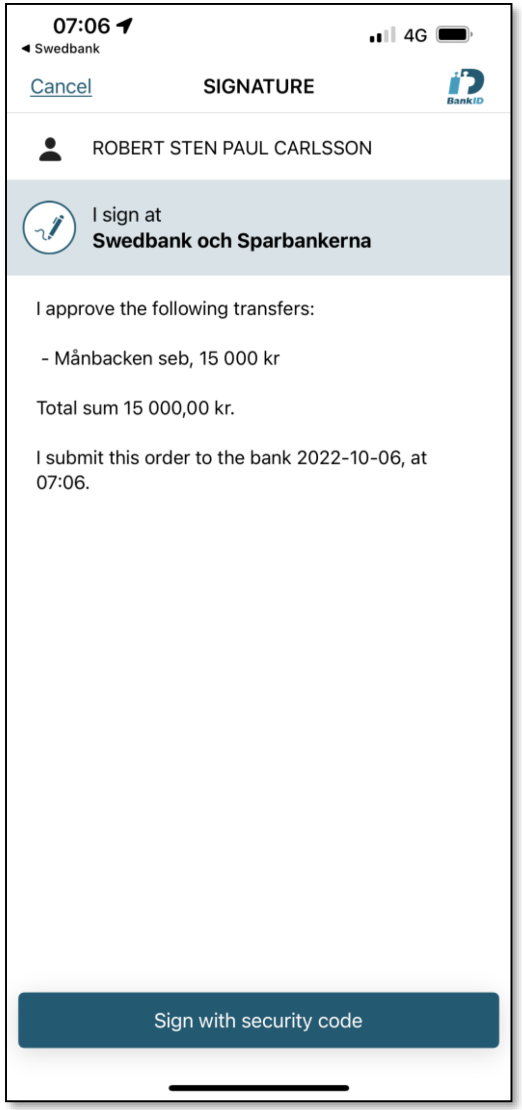
My intent:

Log-in to the mobile app for private customers

Handelsbanken never calls customers to ask them to log in to this service. If you have received a phone call asking you to log in, beware! It could be an attempted fraud. In such cases, you should select Cancel, end the phone call and contact us on 0771-77 88 99.

Context is key

Context is key



ROBERT STEN PAUL CARLSSON

I sign at
Swedbank och Sparbankerna

I approve the following transfers:

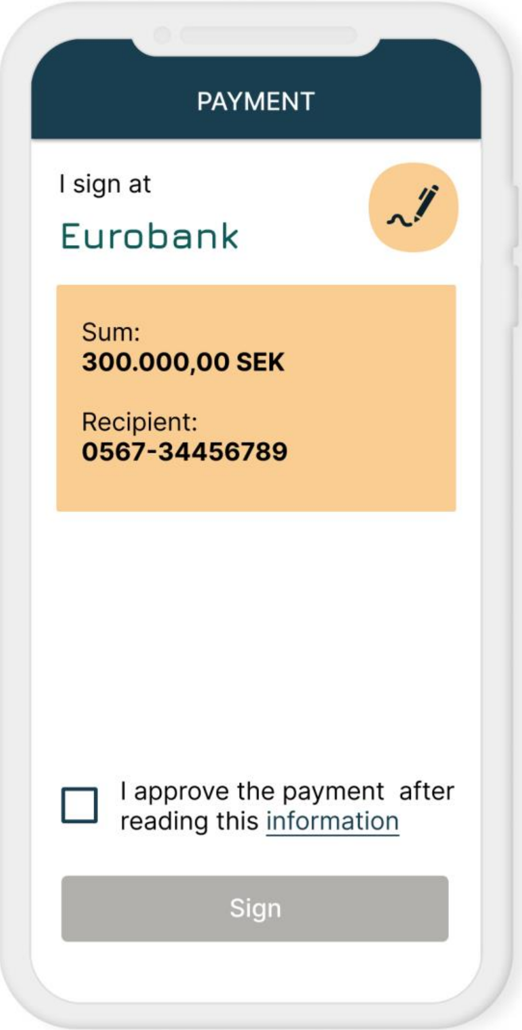
- Månbacken seb, 15 000 kr

Total sum 15 000,00 kr.

I submit this order to the bank 2022-10-06, at 07:06.

Easy to do the right thing

Easy to do the right thing



PAYMENT

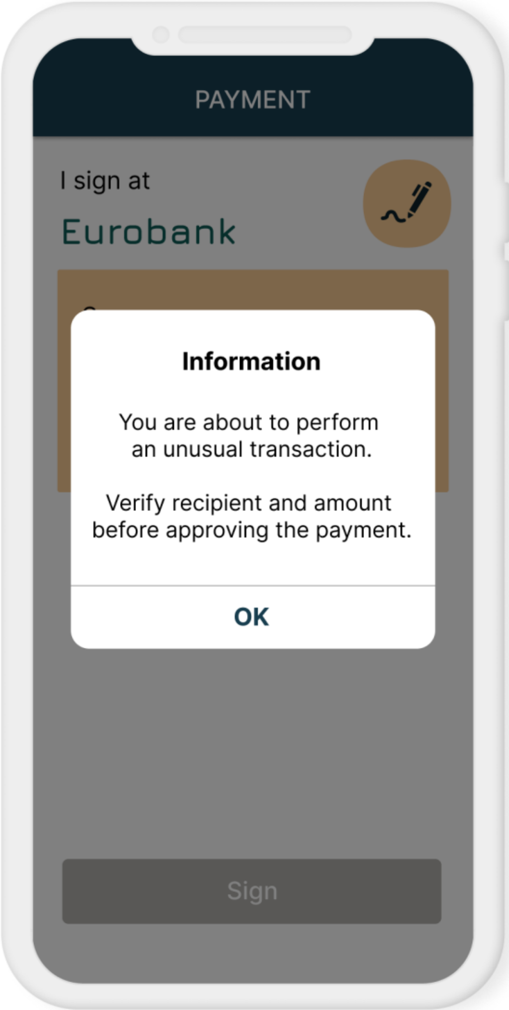
I sign at

Eurobank

Sum:
300.000,00 SEK

Recipient:
0567-34456789

□ I approve the payment after reading this information



PAYMENT

I sign at

Eurobank

Information

You are about to perform an unusual transaction.

Verify recipient and amount before approving the payment.

Technical framework and security measures – An introduction

Protect systems & customers data

- **Public Key Infrastructure** - The BankID infrastructure builds upon a traditional Public Key Infrastructure, where each participating issuer acts as a registration and certification authority (RA/CA).
- **Crypto standard** - Technical security follows international cryptographic standards NIST and best practices in regards to key lengths and algorithm lifecycle management.
- **API** - The relying parties (the service providers, SP) integrates with the infrastructure through a proprietary web service API.
- **Backend role** - Certificate validation and revocation checking itself are supported by the backend infrastructure, and the results are provided as a identity / signing certificate through the API to the relying parties (SP's).
- **Guidelines** – Recommendations and details on how the infrastructure works can be found in the BankID Relying Party Guidelines:
  - https://www.bankid.com/en/utvecklare/guider

Data Handling and Integrity

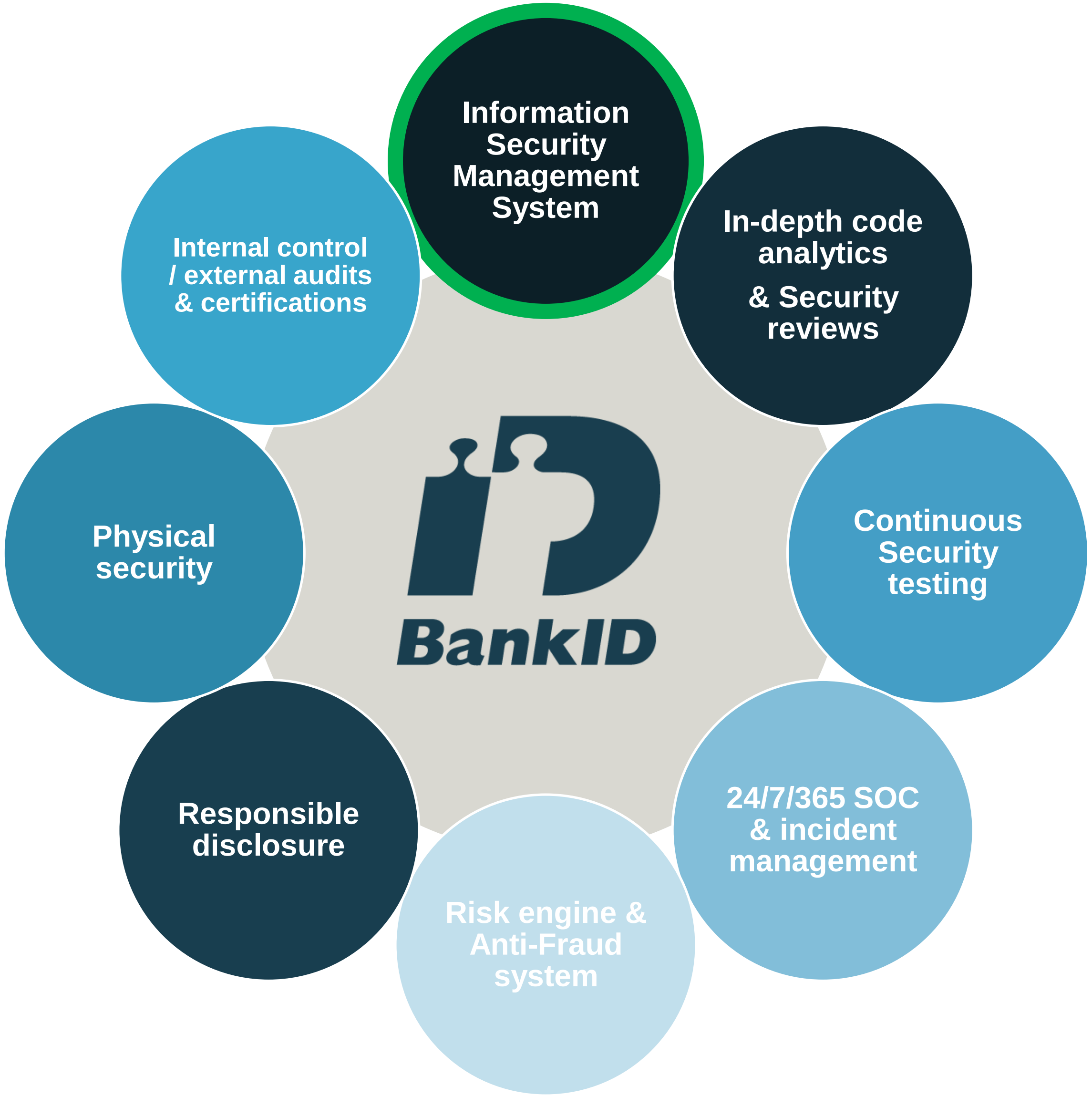
Protect systems & customers data

- **Terms & Conditions** – Define where data is stored, responsibilities, user rights & how to get info (ex. GDPR), info to user when onboarding (Terms & Conditions).
- **Data Controller / Data Processor** - Responsibilities regarding records: The issuing organization is the Personal Data Controller and BankID is the Personal Data Processor.
- **Issuing log records** - The issuing organization keeps records of the application process, delivery and revocation of the eID, as well as the applicable Terms & Conditions and other agreements entered into with the customer.
- **Tech log records** - The central infrastructure keeps log records of technical events according to the payment service directive and keeps the records for the specified retention time.
- **Records protection** – Protection of records are regulated in the BankID requirement framework to provide a strong and secure solution, mitigating relevant risks. We also follow relevant legislation, i.e. GDPR, AML and terrorism legislation.

  BankID also maintains segregation of duties between personnel working with the management of the technical system and personnel involved in the keeping of log records.
- **Records life cycle & retention** - BankID applies a 3-2-1 backup strategy and protects these through archival at different locations. Information to be destroyed are purged every month from the systems.

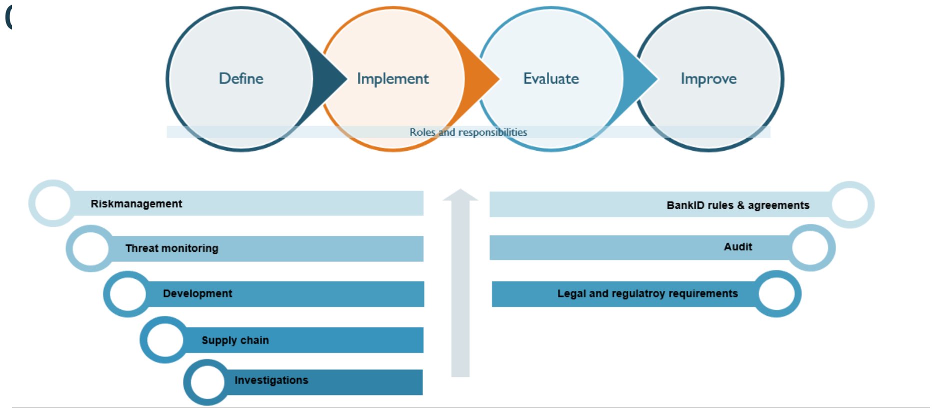
Overall security – a general decription

At BankID security is a central part of all aspects of our business trough high demands and continous improvements


Information Security Management System
In-depth code analytics & Security reviews
Continuous Security testing
24/7/365 SOC & incident management
Risk engine & Anti-Fraud system
Responsible disclosure
Physical security
Internal control / external audits & certifications
BankID

Compliance and Certifications

- **Governance** - The governance of security within BankID is coordinated by group security as the second line of defense, following the COSO-model, in cooperation with all parts of the organization.
- **ISMS** - It aims to control, facilitate and implement well-balanced security measures throughout the organization using an established information security management system (ISMS) according to the international standard ISO/IEC 27001:2013.
- **Audits** - The ISMS is continuously audited by both internal functions and by external independent auditors as per requirement over three year increments decided by the CEO and the Board of Directors.
- **Risk Management** - Risk management is an important part of any security management system and within BankID, the risk management process adheres to ISO 31000:2018 and is well established throughout the organization the infrastructure as well as operating the infrastructure.



BankID Security Overview

- **ISO certifications** - The technical infrastructure and its operation are certified in accordence to ISO9001:2008, ISO14001:2004, ISO 20000-1:2011 and ISO/IEC 27001:2013

- **eIDAS** - BankID is reviewed in eIDAS peer-review and meets the level substantial.

- **Strong customer authentication** - BankID performs audits for compliance to PSD2. Fulfilment of requirement in regards to strong customer authentication as to article 97 in directive EU 2015/2366 in accordance with the technical regulatory standard which have been delegated in regulation EU 2018/389 (RTS).

- **EU payment service directive** - Fulfilment of requirements in EU 2015/849 payment service directive article 13.1 (a), identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.

- **Government authorization** – BankID is authorized by the government accordingly to FATF. BankID is as well reviewed and approved by the Swedish Agency for Digital Government as Swedish eID level 3 ***“Kvalitetsmärket Svensk e-legitimation”*** *(https://www.digg.se/digital-identitet/e-legitimering#kvalitetsmarket_svensk_e-legitimation)*

Svensk e-legitimation

PSD2

FATF

BankID

BankID Risk and Fraud capabilities

- Intro and BankID ”Threat landscape”
- Proactive risk capabilities
- Fraud analysis

The BankID threat landscape

- **Digital** – The society in BankID home market is very digitalized compared to many others. BankID is a big part of that societal journey. Most shops and stores do not accept cash and the amount of cash is low -> “Fraud goes digital” / Digital Threat
- **Advanced** – Talented social engineering fraudsters and patterns with efficient crime-as-a-service software, modus and tools
- **National and International** - Fraud schemes including native and international fraud clusters targeting bank customers
- **Trust** – In BankID home market Sweden, citizens put great trust in society and authorites. For good and for bad when it comes to a new type of social engineering threat
- **Weak links** - BankID is a proven set of tools and processes to neutralize weak links in the threat landscape such as stolen passwords, stolen digipass, social engineering of many kinds, friendly-/credit-/first party-fraud, money muling and more

The BankID threat landscape

The BankID risk and fraud capabilities aim to target:

1

ID-theft targeting BankIDs
A BankID must be issued to the correct user

2

BankID transaction theft
A BankID transaction must not be stolen or initiated by a fraudster

3

Unauthorized / fraudulent use
A BankID must not be used as a tool of crime against a service / customer i.e. money laundering or welfare crime

The BankID Risk and Fraud capabilities ***DETECTS, ANALYZES, PROTECTS*** and ***ACTS*** in all parts of the BankID customer flow

BankID Real Time Risk assessment - Introduction

BankID has comprehensive real time risk assessment capabilities based on metadata such as:

- Customer
- Device
- Transaction / Network metadata
- Position
- Pattern / Anomaly detection

…with the purpose of discover and prevent ID-theft, fraudulent transactions and friendly-/credit-fraud – in real time

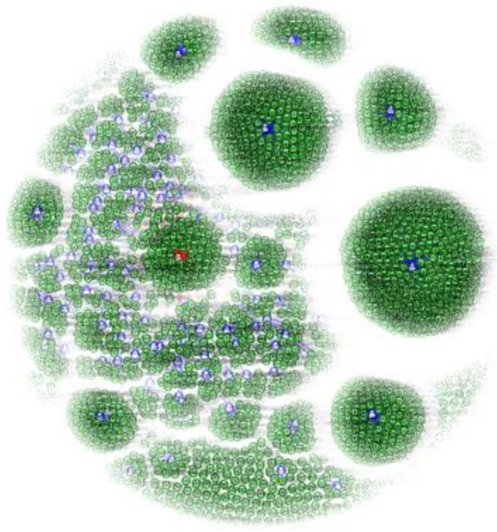
1. **Protects issuing of BankID**
   All new BankIDs are risk assessed with automatic actions or enforcements where required

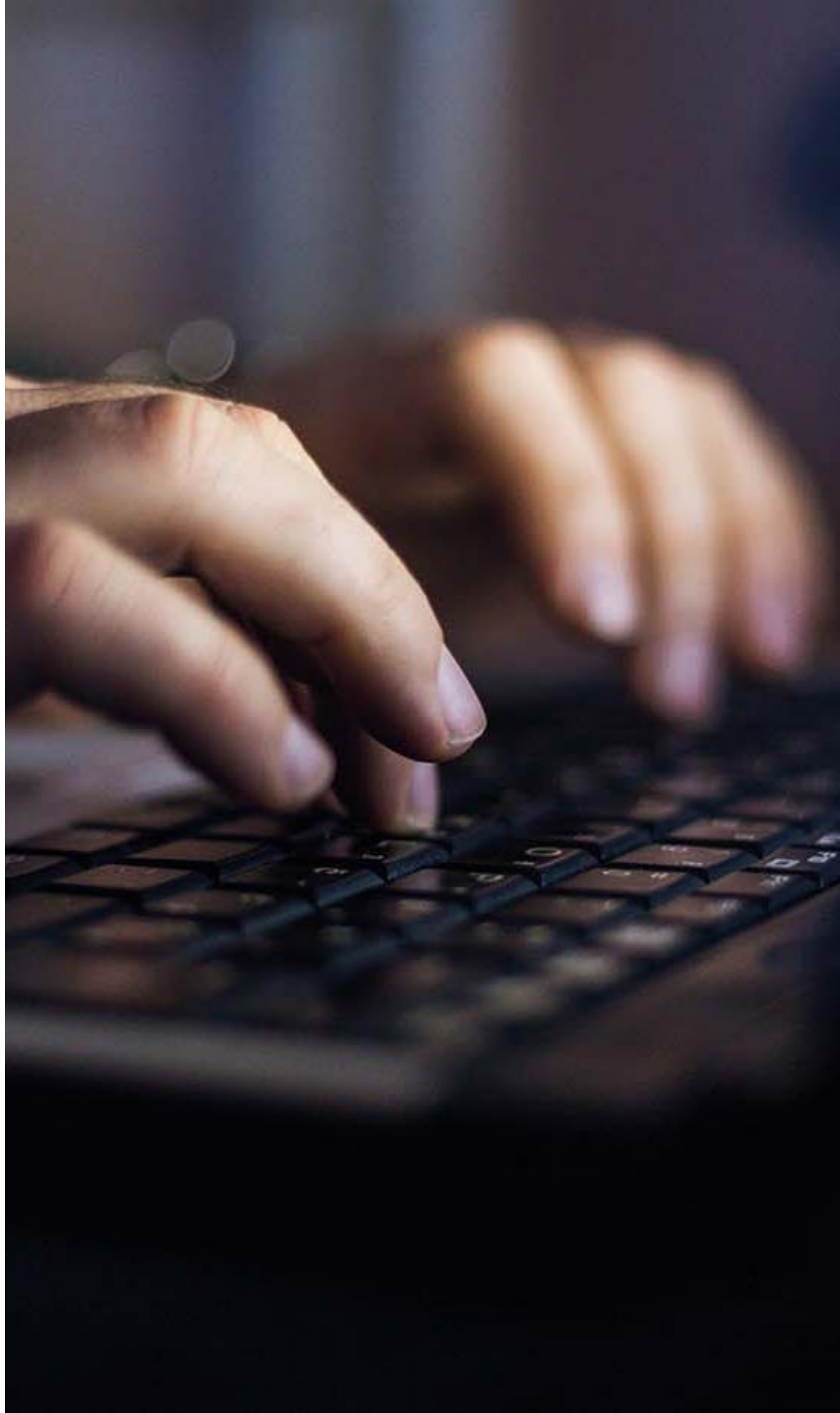
2. **Protects BankID transactions**
   All transactions are risk assessed with automatic actions or enforcements where required

3. **Risk metadata**
   Risk metadata from BankID can be fed into other tools for an even more comprehensive risk assessment including bank/service data

BankID Fraud Analysis capabilities

- Real time / Tactical / Strategical analysis tool set
- Single case analysis – when fraud is a fact
- Extraction of “BankID Usage Reports” to crime prevention authorities
- Automated and manual classification of risk data
- Alarms - fraudulent issuing or usage
- Pattern and anomaly detection capabilities





BankID Digital Identity Platform – A summary of Grnet Tech Day

- **Intro BankID**

- **BankID eID in:**
  - Issuing, Authentication, Transactional signature, Digital Onboarding (ID doc. verification, Biometrics) as well as in Risk & fraud prevention

- **BankID ”Security & Tech Way of working”**
  - Security and Tech overview (Development, Architecture and Operations)
  - Ensuring security, quality, performance and availability

- **We hope we have contributed**
  - With insights and experiences on how to scale an eID securely
  - By hopefully inspire you to act
  - By telling BankID is a white label platform, suitable even in Greece

BankID

Roland Jansson
roland.jansson@bankid.com

Robert Carlsson
robert.carlsson@bankid.com

Karin Hermansson
karin.hermansson@bankid.com

Andreas Bergqvist
andreas.bergqvist@bankid.com