Report
Secure digital verification of identity

Version: Final report draft v 0.99

18 June 2019

TLP: GREEN

Bits AS			
Post address: Postboks 2644 0205 OSLO	Visiting address: Hansteensgt 2 OSLO	Phone: +47 23 28 45 10 E-mail: post@bits.no	Org.nr.: NO 916 960 190

1 Table of contents

Innhold

2 Document Information

2.1 Document history

Version	Status	Date	Editor
0.1	Document established	18.10.2018	Brynjel Johnsen
0.2	Updated after workshop 01.11.2018	08.11.2018	Brynjel Johnsen
0.3	Updated after workshop 22.11.2018	14.12.2018	Brynjel Johnsen
0.4	Updated after workshop 20.12.2018		
0.5	Updated and restructured	08.01.2019	Andreas Havsberg
0.51	Prepared for workgroup meeting on 22.01.2019	15.01.2019	Brynjel Johnsen
0.6	Updated after workshop 22.01.2019	25.01.2019	Brynjel Johnsen
0.61	Minor changes, introduction to legal requirements, moved chapters to increase readability	28.01.2019	Brynjel Johnsen
0.7	Updated with references to documents 13-17 below	06.02.2019	Brynjel Johnsen
0.71	Prepared for comments from stakeholders	04.03.2019	Andreas Havsberg Brynjel Johnsen
0.9	Adjusted with comments from stakeholders	26.03.2019	Brynjel Johnsen
0.99	Prepared for approval	27.03.2019	Brynjel Johnsen

2.2 Change Log (post version 1.0)

Version	Changes from previous version

2.3 Reference Documents

Forkortelse	Dokument
[1] FNO-BKORT	FNO – Regler om utstedelse av legitimasjonsbevis (Bankkort med bilde)
[2] PCI-CARD-PHYS	PCI Card Production Physical Security Requirements v1p1, March 2015
[3] PCI-CARD-LOGI	PCI Card Production Logical Security Requirements v1p1, March 2015
[4] BAX PRNT-SPEC	Bits Bankkort – Printing specification BAX - v1.2
[5] Visa PRNT-SPEC	Bits Bankkort – Printing specification Visa - v1.2
[6] MC PRNT-SPEC	Bits Bankkort – Printing specification MasterCard - v1.2

Forkortelse	Dokument
[7] ICAO-9303	ICAO – Machine Readable Travel Documents - Part 3 – Volume 1 (9303)
[8] ISO/IEC 19794-5	ISO/IEC – 19794-5:2011 - Information technology – Biometric data interchange formats – Part 5: Face image data
[9] ISO 7810:2003	Identification cards -- Physical characteristics
[10] KTRL-NUM	BSK - Bankkort - Kodeliste - Bankkortleverandører v1.4
[11] CRD-MSTR	Bits - Printed master card for quality check
[12] eID-ONB	Study on eID and digital onboarding: mapping and analysis of existing onboarding bank practices across the EU https://ec.europa.eu/futurium/en/system/files/ged/study_on_eid_digital_onboarding_final_report.pdf
[13]	*Draft Guidance for the application of the levels of assurance which support the eIDAS Regulation* https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents
[14]	ISO/IEC 30107-1 Information technology — Biometric presentation attack detection — Part 1: Framework
[15]	ISO/IEC 30107-2 Information technology — Biometric presentation attack detection — Part 2: Data formats
[16]	ISO/IEC 30107-3 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting
[17]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[18]	COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication
[19]	SO/IEC 19794-5:2011(en) Information technology — Biometric data interchange formats — Part 5: Face image data
[20]	Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons version 1.0.4 Bundesamt für Sicherheit in der Informationstechnik.
[21]	https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing
[22]	https://publications.europa.eu/en/publication-detail/-/publication/8da08249-49cd-11e8-be1d-01aa75ed71a1/language-en

2.4 Definitions

Term	Definition
ePassport (eMRP or Electronically-enabled MRP)	A machine-readable passport (MRP) containing a Contactless Integrated Circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder, and a security object to protect the data with PKI cryptographic technology, and which conforms to the specifications of Doc 9303, Part 1.
Fingerprint(s)	One (or more) visual representation(s) of the surface structure of the holder's fingertip(s).
FAR	False acceptance rate[1] The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.
FRR	False recognition rate[1] The false recognition rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false recognitions divided by the number of identification attempts.
FMR	False Match Rate Proportion of impostor attempts that are falsely declared to match a template of another object.
FNMR	False Non-Match Rate Proportion of genuine attempts that are falsely declared not to match a template of the same object.
FTA	Failure-to-Acquire Rate Proportion of the attempts for which the system fails to produce a sample of sufficient quality.
ERR	Equal Error Rate The point where the proportion of False Matches is the same as False Non-Matches (FNMR = FMR).
Machine Assisted Document Verification	A process using a device to assist in the verification of the authenticity of the document in respect to data and/or security.
Machine Readable Official Travel Document (MRtd)	A document, usually in the form of a card approximating to ID-1 or ID-2 size that conforms to the specifications of Doc 9303, Part 3, and may be used to cross international borders by agreement between the States involved.
Machine readable passport (MRP)	A passport conforming with the specifications contained in Doc 9303, Part 1, Volume 1.
Machine readable travel document (MRTD)	Official document, conforming with the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel (e.g. passport, visa, MRtd) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine.

[1] Roughly the same as FMR and FNMR respectively, but the definition distinguishes between attempts and transactions. A transaction may consist of a sequence of attempts and depending on the system's configuration the outcome of individual attempts affects the transaction different. FAR and FRR also takes the Failure-to-Acquire Rate into consideration. In case a transaction consists of exactly one attempt, FAR and FRR are calculated like this: FAR = FMR * (1 - FTA), FRR = FTA + FNMR * (1 - FTA)

Term	Definition
Machine-verifiable biometric feature	unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine.
Applicant	Person who is in the process of verifying the identity.
Subject	Person (identified entity) who has acquired or is in the process of verifying the identity. ("sluttbruker")
Person	This term refers basically to a natural persons
BAC	Basic access control (BAC) is a mechanism specified to ensure only authorized parties can wirelessly read personal information from passports with an RFID chip. It uses data such as the passport number, date of birth and expiration date to negotiate a session key. This key can then be used to encrypt the communication between the passports chip and a reading device. This mechanism is intended to ensure that the owner of a passport can decide who can read the electronic contents of the passport.
SAC	Supplemental Access Control (SAC) is a set of security features defined by ICAO for protecting data contained in electronic travel documents (e.g. electronic passports). SAC specifies the Password Authenticated Connection Establishment (PACE) protocol, which supplements and improves ICAO's Basic Access Control (BAC)
Deepfake	Deepfake, a portmanteau of "deep learning" and "fake" is an artificial intelligence-based human image synthesis technique. It is used to combine and superimpose existing images and videos onto source images or videos using a machine learning technique called a "generative adversarial network". The combination of the existing and source videos results in a fake video that shows a person or persons performing an action at an event that never occurred in reality.

2.5 Abbreviations

Abbreviations	Text
M	Mandatory (Must, Shall)
CM	Conditional -> Mandatory (If a condition is met, the requirements is mandatory)
R	Recommended (Should)
CR	Conditional -> Recommended (If a condition is met, the requirements is recommended)
O	Optional (May)

2.6 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

This document contains requirements which can be referenced by other specifications.

3 Background

During the last years private and public services deployed a wide range of self-service solutions for their customers. In Norway, the use of BankID for identification and signature purposes has enabled the banks to offer almost all services from their digital environments. BankID and other eIDs are used extensively in both private and public services in addition to online banking.

However, due to legal and practical reasons, subjects still need to meet in person with a physical identification paper (ie. passport) for first-time identification and registration with an eID provider. This is perceived as a cumbersome process both by the service providers and their customers, particularly in a country with large geographical distances. The process is expensive as the services are provided to all customers, either in their provider's offices or by purchasing an expensive service from the Norwegian Postal service. In either case the process is inefficient and may take up to a week to finalise.

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 these requirements on business and society.

As this requirement process is driven by the banking sector, the main focus of this report is on verification of identity for onboarding of customers in banks. However, in order for the requirements to succeed they need to bed widely accepted in society, and more specifically by public sector entities. Hence this also opens up for other non-banking applications for solutions based on the requirements. This is further reflected in section 5.5 where different profiles for usage scenarios are defined.

4 Drivers for solutions

Identity providers have large incentives to provide automated solutions for onboarding of new customers as well as for re-validating existing customer relationships. Today, the applicant would have to meet at an office or a certified agent, and provide proof of identity, ie. ID-document. The identity provider will need to read or scan the identity document, validate the document, and perform an identity check by comparing the picture in the identity document with the face of the applicant physically present in the office. Our assumption is that this process could be automated, thus reducing the need for applicants to meet up in person at the office.

The automated solutions need to fulfil legal, technical and security requirements enabling identity providers to provide the identity validation services where the customer is. The service can be provided by self-service kiosks, Personal computers, mobile phone/tablet apps or similar devices and software.

- 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

5 Legal and other prerequisite requirements

Overview of applicable laws and regulations with requirements that are relevant for digital verification of identity. This overview must provide information on which areas of requirements that are affected by the requirement.

5.1 Legal requirements

The following section provides an overview of the legal requirements in the following areas:

- 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

The user journey and the requirements identified in this document are sought aligned with the legal requirements as referred to in the following sections. The Norwegian AML law (Hvitvaskingsloven) and the associated provisions (Hvitvaskingsforskriften) have both a direct impact on the requirements. The relevant chapters are included in this section.

The 'Hvitvaskingsloven' sets out requirements that the information about a person's identity must be verified by physical presence with valid ID-document. If physical presence is not feasible, further documentation or further measures must be taken. The rationale behind developing these requirements is to create a baseline where a solution based on the requirements will fulfil the bank's obligations for 'further measures'.

In 'Hvitvaskingsforskriften' the definition of a valid ID-document is an original document issued by a government agency containing name, national ID-number (or equivalent), and photo of the subject. For Norwegian citizens this implies a passport. For other nationalities a government issued national ID-card may be enough if the document fulfils the general requirements.

For banks, one of the goals of the verification process is to offer the potential customer banking services, and if the customer fulfils the requirements, a BankID electronic ID and signature. For this, the bank will also have to make sure that the verification process fulfils the eIDAS-requirements and the BankID Rules (Regler om BankID). Whereas the eIDAS regulation refers to the identification of the subject may be carried out "*using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence*", the BankID rules specifically refers to that the customer must verify identity with a passport.

For a bank to onboard a new customer with no prior relationship and be able to issue a BankID to the subject, the bank must be presented with a valid passport, identify the subject holding the passport as the person the passport is issued to. In an electronic setting the bank must further enhance the probability that there is a real person, and not an electronically generated image of the person, by using different techniques to verify real person presence. Our intention is that these techniques will serve as what is referred to as "further measures" in 'Hvitvaskingsforskriften'.

Finally, the procedure must be subject to endorsement or approval as referred to in article 24 in eIDAS; "*…by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.*"

All the requirements are written with this in mind. There is no guarantee that a solution based on these requirements will be endorsed or approved by a national competent authority, but by designing a solution based on the requirements, this will increase the probability for such recognition.

5.2 AML Legal requirements

Local Law on anti-money laundering and terror financing

Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven) §12
https://lovdata.no/dokument/NL/lov/2018-06-01-23/

Field Code Changed

Norwegian original text	English translation
(1) Når kunden er en fysisk person, skal følgende opplysninger innhentes om kunden:	(1) When the customer is a physical person, the following information shall be collected about the customer:
a) Navn	d) Name
b) fødselsnummer, D-nummer eller, dersom kunden ikke har slikt nummer, annen entydig identitetskode. For personer som ikke har norsk fødselsnummer eller D-nummer, skal	e) National Identification number, D-number or, if the customer is not assigned a such identity number, another unique identity code. For

det innhentes fødselsdato, fødested, kjønn og statsborgerskap, herunder om personen har flere statsborgerskap. c) Adresse De samme opplysningene skal innhentes om den som handler på vegne av kunden, i tillegg til opplysninger om at vedkommende kan handle på vegne av kunden. De samme opplysningene skal innhentes om den som er gitt disposisjonsrett over en konto eller et depot. (2) Opplysninger om kundens identitet bekreftes ved personlig fremmøte ved gyldig legitimasjon. Dersom bekreftelse av identiteten skal skje uten personlig fremmøte, skal det fremlegges ytterligere dokumentasjon eller gjennomføres ytterligere tiltak. Opplysninger om identiteten til personer som handler på vegne av kunden eller er gitt disposisjonsrett over en konto eller et depot, bekreftes ved gyldig legitimasjon. Retten til å handle på vegne av kunden bekreftes ved skriftlig dokumentasjon.	persons persons not assigned a Norwegian identity number or D-number, additional information about date-of-birth, birthplace, gender and nationality, and of the person has several nationalities. f) Address The same information shall be collected for any person acting om behalf of the customer, in addition to information that the person is acting on behalf of the customer. This information shall also be collected about any one who has been granted rights of disposal for an account or depot. (2) Information about the customer's identity shall be verified by physical presence with a valid identity document. If the verification of the identity is made without physical presence, additional documentation or measures are required. Information about the identity of persons acting on behalf of the customer or persons granted rights of disposal for an account or depot, shall be verified with a valid identity document. The rights to act on behalf of the customer shall be verified by written documentation.

Local provisions on anti-money-laundering and terror financing

Hvitvaskingsforskriften - https://www.regjeringen.no/no/dokumenter/forskrift-om-tiltak-mot-hvitvasking-og-terrorfinansiering-hvitvaskingsforskriften/id2611046/

Field Code Changed

Norwegian original text	**English translation**
4-1 Etablering av kundeforhold	**4-1 Establishing a customer relationship**
(1) Kundeforhold skal anses etablert når kunden kan bruke den rapporteringspliktiges tjenester, for eksempel ved opprettelse av konto eller utstedelse av betalingskort.	(1) The customer relationship is regarded established when the customer can use the reporting subject's services, for example for establishing a bank account or issuing of payment cards.
4-3 Gyldig legitimasjon for fysiske personer	**4-3 Valid proof of identity for physical persons**
(1) Gyldig legitimasjon for fysiske personer ved personlig fremmøte er original av dokumenter som	(1) Valid proof of identity for physical persons when physically present is original documents that;
a) er utstedt av offentlig myndighet eller av annet organ som har betryggende kontrollrutiner for dokumentutstedelse, og dokumentene har et tilfredsstillende sikkerhetsnivå,	d) are issued by a public authority or other entity who has reassuring control routines for document issuance, and provided that the documents have a satisfactory level of security,
b) inneholder fullt navn, navnetrekk, fotografi, og	e) contains full name, signature, photography, and
c) fødselsnummer eller D-nummer.	f) Norwegian national identity number or D-number
(2) For person som ikke har norsk fødselsnummer eller D-nummer, skal legitimasjonsdokument, i tillegg til kravene som følger av første ledd, inneholde fødselsdato, fødested, kjønn og statsborgerskap.	(2) A person that are not assigned a Norwegian national identity number or D-number, the identity document

(3) Krav om navnetrekk gjelder ikke for pass. (4) Elektronisk signatur er gyldig legitimasjon for fysisk person når identiteten ikke skal bekreftes ved personlig fremmøte. Elektronisk signatur må tilfredsstille kravene i forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 3 og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift.	must also, in addition to the requirements in (1) above, contain date of birth, birth place, gender and nationality. (3) The requirement for signature does not apply for passports (4) Electronic signature is regarded as valid proof of identity for a physical person when the identity is not verified by physical presence. The electronic signature must satisfy the requirements as laid out in the provision 21. November 2005, no 1296 on voluntary self-declaration schemes for certificate issuers § 3 and that is listed in the public register according to § 11, first paragraph in the aforementioned provisions.

5.3 European legislation

Most EU-regulation apply also in Norway. Either directly or incorporated in Norwegian Law.

5.3.1 eIDAS Regulation

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

This regulation is relevant for trust service providers issuing qualified certificates. This has applicability for banks when issuing BankID to their customers but may also be relevant for other scenarios as the requirements are generally known and accepted across EU, defining different baseline levels of assurance for identification of physical persons.

Article 24 specifically details the requirements issuing qualified certificates for digital signature. The article specifies the alternatives 'physical presence', 'the use of electronic identification' and what is referred to as 'other identification methods'.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

Article 24;

1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

   The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

   a) by the physical presence of the natural person or of an authorised representative of the legal person; or
   b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or
   c) (by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
   d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

Whereas the implementing acts for eIDAS are not clear on the requirement for physical presence, the requirements for qualified trust service providers – issuers of qualified certificates for electronic signature – are written with the assumption that the person must be physically present, ref article 24.

However, article 24 also refers to other alternatives, where 24 1 (d) is particularly relevant. According to this section, the verification of identity may be ensured: "…*by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body*."

The identification method must be recognized at a national level, guarantee a reliability at the same level as physical presence, and be accepted by a national competent authority (conformity assessment body), i.e. for Norway this will be Nkom.

eIDAS article 24 has been subject to much debate, specifically whether the article provides an opening for issuers to use alternative solutions to physical presence, e.g. HQ video sessions. Nkom has referred to feedback from ETSI; "*The proof of equivalence needs to consider the impersonation risks inherent to remote applications. In particular, an uninterrupted chain of subsequent remote registration can increase such risks, because the person can never be actually seen for years, and/or because the traceability with the initial face to face is weakened*".

Article 24 1 (b) is also relevant as it refers to the verification of physical presence with an existing e-ID; "*remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'*;"

The article provides an opening for accepting electronic means of identification, if earlier physical presence can be assured or verified.

5.3.2 eIDAS Implementing acts

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

This implementing act sets out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [17].

In the below tables we have identified the relevant requirements in (EU) 2015/1502 and how they are addressed by the requirements in this document.

In several of the requirements, the notion 'authoritative source' is used. According to 2015/1502 an "*'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity*".

In the draft '*Guidance for the application of the levels of assurance which support the eIDAS Regulation' [13]*, the following examples are given for authoritative sources:

Examples of authoritative sources can include:

- National Population registers for information on person's identity data (e.g. link name to national identity number etc, verify they are not deceased)
- Government registers which have associated governing processes to ensure reliable and correct data such as passport registers, driving license databases, tax registers, social security registers
- Business registers for information on legal person's identity and binding to natural persons
- Official identity documents such as passports and identity cards
- Assertions made by an authority about a person like official documents

For the purposes of the requirements provided in this document we have relied on '*official identity documents such as passports and identity cards*'.

In the tables below we have mapped the requirements as outlined in (EU) 2015/1502 with the requirements in this document. This comparison is made to demonstrate how the relevant EU-requirements are fulfilled in this document.

Application and registration

LOA	Relevant requirement in (EU) 2015/1502	Addressed in requirements in this document
Low	1.Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.	1. The process of verification of identity is a sub-process that may result in the issuance of an eID/eSignature or other means of identification. Thus, the terms and conditions for the whole process must be handled by the calling application. The bridge between this requirement

	2.Ensure the applicant is aware of recommended security precautions related to the electronic identification means. 3. Collect the relevant identity data required for identity proofing and verification.	and the verification process is found in section 7.5 Application User Interface. 2. Same as for requirement 1. The bridge between this requirement and the verification process is found in section 7.5 Application User Interface. 3. This requirement is covered by the collection of data from the ID-document performed by the self-service-application. The requirements are found in sections 10.1 for capture of ID-document and 10.4 for reading the ID-document data.
Substantial	Same as above	Same as above.
High	Same as above	Same as above, but with reference to requirement 3, the reading of data will be based on RFID-chip as found in section 10.2.

Identity proofing and verification (natural persons)

LOA	Relevant requirement	Addressed in requirements
Low	1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2. **The evidence can be assumed to be genuine**, or to exist according to an authoritative source and the evidence appears to be valid. 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.	1. Replaced by requirement 1 Substantial and High. 2. Replaced by requirement 1, paragraph 2 for Substantial. 3. Replaced by requirement 1, paragraph 3 for Substantial, and 1 (a) for High.
Substantial	1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and **the evidence is checked to determine that it is genuine**; or, according to an authoritative source, it is known to exist and relates to a real person and **steps have been taken to minimise the risk that the person's identity is not the claimed identity**, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;	1. This paragraph is made up of three parts. Section 10.4.7 ensures that the information about the claimed identity is available. Section 10.4.1 and 10.4.2 ensures that the evidence (ID-document fulfils a set of requirements) Section 10.1 ensures that the evidence (ID-document) is in possession by the person using the self-service application. This paragraph is covered by the ID document validation requirements as described in section 10.4 This paragraph is handled by sections 11 and 12.1. For LoA Substantial the comparison of the visual picture found in the evidence (ID-document) is compared with the picture as taken by the camera in the self-service application. This

		is described in requirement 12.1.1 through **Error! Reference source not found.**. Risk-reducing measures for checking lost, stolen, suspended or revoked evidence is required if such a service is available, see requirement **Error! Reference source not found.**.
High	1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met: (a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;	For LoA High possession is further verified by using the MRZ to gain access to the RFID-chip in the ID-document and to access the biometric data, for this purpose only the high-resolution photograph is available. Recognition of biometric evidence must always be policy-based but is also enhanced by requirement 10.4.1. The check of validity is performed according to the requirements 10.4.11, 10.4.12 and 10.4.13. This is ensured by comparing the high-resolution picture found in the RFID-chip with the biometric samples taken by the camera in the self-service application. The requirements are found in 12.1.6 through 12.1.7.

A study from the European Commission on digital onboarding sums up the general requirements for these Levels of assurance like this [12]:

eIDAS LoA	Description
Low	Low provides a limited degree of confidence in the claimed or asserted identity of a person, and can be for instance characterised by assuming the following: • **Possession** of an evidence recognised by a Member State, • The evidence is genuine, • **Existence** of the identity claimed.
Substantial	Substantial provides a substantial degree of confidence in the claimed or asserted identity of a person, and can be for instance characterised by the level Low plus the **verification** of the following: • **Possession** of an evidence recognised by a Member State and check of the attributes representing the claimed identity, • Check if the evidence is genuine
High	High provides a higher degree of confidence in the claimed or asserted identity of a person, and can be for instance characterised by the level Substantial plus at least one of the following: • **Possession** of a photo or biometric identification evidence recognised by a Member State and the claimed identity is checked through a comparison with one or more physical characteristics. • Checked by procedures employed by a public or private entity in the same Member state that provide an equivalent level, • The electronic identification means is issued on the basis of a notified electronic identification means with a High LoA.

As evident from the above tables, the requirements in this document for proof-of-possession of an ID document increase as we go from LoA low to LoA high. Whereas for LoA Low and Substantial, there is a requirement that the applicant presents the ID-document for visual inspection, a higher degree of proof-of-possession is required for LoA high. This is achieved by requiring the user to not only present the ID-document for visual inspection, but also by requiring successful reading of the RFID-chip in the ID-document. This is generally accepted as resulting in a higher degree of confidence that the applicant is actually possessing the ID-document than if the applicant is only able to provide a visual representation of the document.

5.4 Scope of requirements

This section describes various areas of prerequisites which are the basis for the final requirements. The areas can be viewed as building blocks for use-cases. Each use-case will select the areas required through legal or other needs for that use-case. The requirements from each area can be assembled to achieve the complete set of requirements needed for each specific use-case. Additional Use-case specific requirements can also be added to the requirements from the prerequisite areas.

Areas can also build upon other areas. For instance, eIDAS level of assurance "High" can be an extension of requirements of eIDAS level of assurance "Substantial".

The described areas are primarily aimed at the needs of financial institutions but can easily be extended to cover areas relevant to other industries and sectors.

5.4.1 Financial sector requirements

- KYC - Know your customer: Based on legal requirements.
- AML: Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF): Based on legal requirements.
- PSD2: Payment Service Directive 2 (PSD2) and PSD2 RTS on SCA & CSC
- PAD: Payment Account Directive (PAD) and Finansavtaleloven § 14 (kontraheringsplikten)
- BankID: BankID Rules

5.4.2 Public sector requirements

- eIDAS-Low: eIDAS, assurance level Low: Based on EU legislation
- eIDAS-Substantial: eIDAS, assurance level Substantial: Based on eIDAS Low with additions stated in ETSI
- eIDAS-High: eIDAS, assurance level High: Based on eIDAS Substantial
- NO-Low: Norwegian assurance level Low ("Lavt"): Based on eIDAS Low with national additions.
- NO-Substantial: Norwegian assurance level Substantial ("betydelig")
- NO-High: Norwegian assurance level High ("høyt")

5.5 Profiles

This section defines possible use-cases and which prerequisite areas they require. The use-cases will be referred to throughout this document.

5.5.1 Financial sector profiles

Name	Description	Requirement equivalent
Bank-BankID	New customer with all banking services, including issuing BankID	KYC, AML, PAD, PSD2, BankID, NO-High
Bank-all	New customer with all banking services, excluding issuing BankID	KYC, AML, PAD, PSD2
Bank-limited	New customer with access to payment accounts with basic features ("grunnleggende banktjenester"), excluding issuing BankID	KYC, AML, PAD, PSD2

5.5.2 Public sector profiles

Name	Description	Requirement equivalent
Pub-subst	Services of substantial (betydelig) need for assurance, such as tax returns, etc.	• Norwegian issued eID: Requires NO-Substantial • EU-issued certificates: Requires eIDAS-Substantial
Pub-high	Services of high need of assurance, such as medical and health services.	• Norwegian issued eID: Requires NO-High • EU-issued certificates: Requires eIDAS-Substantial

5.5.3 Private sector profiles

Name	Description	Requirement equivalent
Priv-norm	New customer with service requiring AML, such as buying a house, auditors, accountants, power of attorney	AML
Priv-legal	New customer other legal requirements, such as identifying persons on a construction site	eIDAS-low

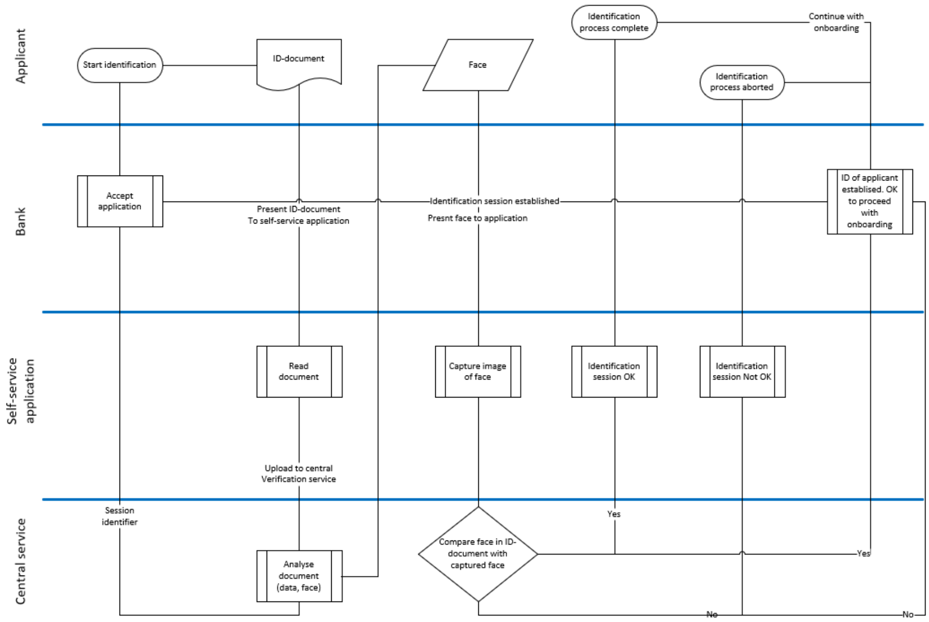
This section can be expanded further with more use-cases if needed.

	KYC	AML	PSD2	PAD	BankID	eIDAS	NO
Bank-BankID	Yes	Yes	Yes	Yes	Yes	-	High
Bank-all	Yes	Yes	Yes	Yes	-	-	-
Bank-limited	(Yes)*	Yes*	Yes	Yes	-	-	-
Pub-subst **Services of substantial (betydelig) LoA (NO certs)**	-	-	-	-	-	-	Substantial
Pub-subst **Services of substantial (betydelig) LoA (EU certs)**	-	-	-	-	-	Substantial	-
Pub-high **Services of high LoA (NO certs)**	-	-	-	-	-	-	High
Pub-high **Services of high LoA (EU certs)**	-	-	-	-	-	High	-
Priv-norm	-	Yes	-	-	-	-	-
Priv-legal	-	-	-	-	-	Low	-

* Requires additional customer measures

6 Customer journeys and use cases

Digital onboarding via secure digital verification of identity is one of the last remaining areas for digitalisation of online services. The crucial part of the digital identification process is to verify the physical identity of a person against a valid and genuine ID document and match this information with the application for identity services. The general process may be summed up by these steps:


Applicant
Bank
Self-service application
Central service
Start identification
ID-document
Face
Identification process complete
Continue with onboarding
Identification process aborted
Accept application
Present ID-document To self-service application
Identification session established
Presnt face to application
ID of applicant establised. OK to proceed with onboarding
Read document
Capture image of face
Identification session OK
Identification session Not OK
Upload to central Verification service
Session identifier
Yes
Analyse document (data, face)
Compare face in ID-document with captured face
Yes
No
No

In the following sections, the steps that the user will have to go through are presented. For each step in the process the assets, threats and consequences if the threat materialize are presented. The threats form the basis for the derivation of the requirements as presented in later sections of this document.

6.1 Person applies for service that requires the verification of identity

This initial step is a pre-step is common for all user journeys as it involves an intention of that person to on-board for a service. Normally the step involves opening an app or accessing the onboarding service in a web-service, onboarding kiosk etc connected to a central verification service. It is essential that the collection of data is performed by the self-service application, whereas the analysis of data is performed by a central processing unit, i.e. the central verification service.

As the only biometric data available to the central verification service in the ID-document is the photographic image of the ID-document holder, the capability requirements for the self-service terminal will be limited to the capture of photographic data (static or moving image) of the applicant. The requirements for the capture capability of images must be parallel to the image requirements for the digital representation of the ID-document picture.

To further enhance the probability of the real person holding the identity of the ID-document capture of live video images may also be applied.

6.2 Person is redirected to self-service application

The self-service application may be installed on a standalone terminal intended for this verification of identity purposes only, on a personal computer, or a multi-purpose mobile device (i.e. mobile phone, tablet etc). In the case for multi-purpose mobile devices the self-service application may be in the form of a standalone application, or an SDK integrated in the calling application providing a seamless user experience. In the cases where the self-service application is provided as standalone application the user will have to switch between the calling application and the self-service application. This may be done technically by application-switching, or manually by using a method enabling the user and the applications to maintain the technical and user-session.

Asset	Threat	Possible consequence
Onboarding service access	Attack on service trigger	Session takeover Information harvesting Subject is tricked into verifying identity for wrong purpose
Identification session	Session collapse	Identification session not with same entity as person expects. Identification session established with hostile party. Identity data leakage. Subject is tricked into verifying identity for wrong purpose
Device integrity	Application running on insecure device Identification process interrupted and continued later (asynchronous) Device security altered over time	Data leakage Session takeover Subject is tricked into verifying identity for wrong purpose
Application integrity	Old (possibly vulnerable) version of application software is running Application code is modified before installation Application code is modified after installation Application process is hijacked at run-time (including trojans) Application memory data is altered during runtime.	Data leakage Session takeover Subject is tricked into verifying identity for wrong purpose

6.3 Application is accepted, pending verification of identity

At this stage the identification session is established and forms the basis for the following steps.

Asset	Threat	Possible consequence
Integrity of status of the onboarding application	Attack on central verification service to change status	Status of application is changed. False acceptance of application.
Availability of identification service	DOS-attack on service or other related services	Service unavailable Fallback to other service Fallback to less secure service

6.4 The applicant presents the ID document to the self-service application

This step requires the applicant to present the ID-document to the self-service application as described in section 6.2. For all usecases the self-service application must be able to capture pictures of the ID-document, and usecases requiring eIDAS equivalent 'high' application must in addition have access to an RFID-reader capable of reading the RFID-chip using NFC technology. The requirements are based on a client-server based architecture, a stable internet connection is always a requirement.

The presentation of the ID document is made by the user, following instructions from the self-service application.

Asset	Threat	Possible consequence
ID-document general readability	Manual attack on device	Not able to read or capture data from the travel document.
Access to capture hardware	Manual attack on device Faulty device	Not able to read or capture data from the travel document.

6.5 The machine-readable information (eg VIZ, MRZ and RFID chip) in the ID document is read by the self-service application.

To be able to read the ID document, the ID-document must have a readable Visual Inspection Zone (VIZ) and a Machine-Readable Zone (MRZ) as defined in [7] ICAO-9303.

Successful reading of, and reasonable inspection of the optical security elements in the VIZ and the MRZ will result in basis for all profiles. For access to reading the RFID-chip, successful reading and inspection of the MRZ is always a prerequisite.

As outlined in section 5.3.2 the self-service application must proceed to reading the RFID-chip if the profile requires the equivalent of eIDAS 'high'. The RFID chip is read using the BAC (Basic Access Control) protocol for accessing the encrypted data. The readable information in this chip contains the subject's name, issuer data, and a high-resolution picture of the subject. The information in the chip is integrity protected with PKI keys issued by the national competent authority. The BAC protocol will be replaced by the more secure SAC (Supplemental Access Control) protocol in the coming years. EU started rolling out SAC in 2014. The procedure for accessing the RFID-chip will not be changed when introducing SAC.

If no RFID-chip is detected, the self-service application is faced with two options:

1) Continue with identification for another use-case if policy allows
2) Abort the identification session

The RFID-chip also contains other non-readable biometric information, protected by stricter access control mechanisms. These elements are only available authorised government verification purposes, and hence not useful for the other organisations for identification purposes.

Asset	Threat	Possible consequence
Readability of Visual Inspection Zone	Camera or picture quality too low Camera not able to capture security features Not all elements captured by camera Image file is changed, alteration of picture	Blurred picture Data is changed Security elements not captured
Readability of Machine-readable Zone	Image file is changed, alteration of OCR characters	Data is changed

Asset	Threat	Possible consequence
Readability of RFID chip	ID-document does not have onboard RFID-chip. RFID chip is unreadable.	Not able to read RFID-info. Identification will have to be based on VIZ, MRZ only.

6.6 The machine-readable information (eg VIZ, MRZ and contents of RFID Chip) in the ID-document is uploaded to the central verification service

The capture device and self-service application must be able to securely transfer the data read from the ID-document to the central verification service using an open network, i.e. internet.

Asset	Threat	Possible consequence
General integrity protection	Data is manipulated in transit	Integrity of data and session lost.
Integrity of VIZ	Image data is manipulated in transit by attacker	Depending on the data that is manipulated, but wrong identity may be the result.
Integrity of MRZ, if available	Image data is manipulated in transit by attacker	Depending on the data that is manipulated, but wrong identity may be the result.
Integrity of RFID data	RFID-data is manipulated in transit by attacker	Will be discovered by central verification service when verifying digital signature.

6.7 The ID-document is checked by the central verification service, ie. If it is genuine and valid (authenticity check)

Verification of VIZ and MRZ must be performed by the central verification service according to best-practice analysis of the visual information. The visual zone in the ID-document contains several security elements, but only a subset of these elements is possible to capture and verify with a general camera on a multi-purpose device. The verification must be based on image-analysis of the elements in the ID-document and OCR-elements. The minimum requirements for verification must be established to define a baseline for identification.

Identification requiring the equivalent of eIDAS ‘low’ and ‘substantial’

Asset	Threat	Possible consequence
Availability of data from VIZ	VIZ data not available (partly or completely)	Not able to populate required identity attributes
Availability of data from MRZ	MRZ data not available (partly or completely)	Not able to populate required identity attributes Not able to compare data between VIZ and MRZ Not able to create basis for reading RFID-chip for High.
The ID-document	The ID-document does not fulfil the requirements, i.e. sanity check of expected elements	ID-document cannot be used for identity verification
Image of VIZ	General quality issues Camera issues Deliberate quality deterioration	ID-document cannot be used for identity verification

Asset	Threat	Possible consequence
Picture of ID document holder in VIZ	Photo substitution	Not able to create biometric template Wrong person identified.
Data in VIZ	Image of text in VIZ not readable	Incorrect data about ID-document holder. Indication of forgery.
Integrity of data in MRZ	Deliberate change in characters	Wrong personal data Indication of forgery
Integrity of data in MRZ	Deliberate change in characters	Indication of forgery Not able to read RFID
Consistency of data across VIZ and MRZ	Data fields manipulated	Indication of forgery Wrong identity established
ID-document visible security elements	Manipulated security elements Falsified security elements Missing security elements	Indication of forgery
ID-document specifications	ID-document not according to specifications for ID-documents issued at the time of issuance	Indication of forgery
Possession of ID-document	ID-document lost or stolen	ID-document misused by other person ID-document holder not identified
Validity of ID-document	ID-document not valid	Expired ID-document used for verification of identity

Identification requiring the equivalent of eIDAS 'high'

The verification of the data read from RFID-chip relies mainly on the availability of the data and the validation of the cryptographic elements of the data, i.e. the digital signature. If the digital signature is made with the key belonging to the public key of the expected certificate, and all data is available in the RFID-chip this will be the baseline for identification as the authenticity of the document and the attributes can be technically verified.

Asset	Threat	Possible consequence
Data in MRZ	Unreadable or changed data in MRZ	Not able to negotiate session key for reading the RFID-chip using the Basic Access Control protocol or Supplemental Access Control protocol.
Availability of data from RFID-chip	Attributes not available RFID reading session	Not able to populate required identity attributes Integrity protected personal data not available High-res picture not available

Asset	Threat	Possible consequence
Integrity of data from RFID-chip	Data deliberately changed	Issuer verification not possible. Signature broken Integrity not verifiable Fallback to LOA Substantial should not be possible if RFID-data has been manipulated.
Consistency of data across VIZ/MRZ and RFID-chip	Data from VIZ/MRZ and RFID-chip not identical	Indication that ID-document is manipulated. Suspicious identification flagged for follow-up by calling application.

As evident from the above table, even if the intention was to identify the person for a given use-case, it might be possible to establish an identity for another use-case if RFID-data is not available depending on the reason why the RFID-data was not approved for ID-purposes.

6.8 The applicant registers new biometric data with the self-service terminal

The verification process takes the new sample of an eMRTD holder and compares it to a template derived from the image as found in the ID-document of that holder to determine whether the holder is presenting in the same identity.

The types of biometrics are:

- facial recognition – MANDATORY. MUST comply to [ISO/IEC 19794-5];
- fingerprint recognition – OPTIONAL. If used, MUST comply to [ISO/IEC 19794-4];
- iris recognition – OPTIONAL. If used, MUST comply to [ISO/IEC 19794-6].

Biometrics terms

The following terms are used in biometric identification:

- “verify” means to perform a one-to-one match between proffered biometric data obtained from the eMRTD holder now and a biometric template created when the holder enrolled in the system;
- “identify” means to perform a one-to-many search between proffered biometric data and a collection of templates representing all of the subjects who have enrolled in the system.

Biometrics can be used in the identification function to improve the quality of the background checking performed as part of the ID-document, visa or other travel document application process, and they can be used to establish a positive match between the travel document and the person who presents it. [7]

The presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion intended to interfere with system policy is referred to as a presentation attack [16].

In ISO/IEC 30107-1:2016 the threats are described as ‘presentation attack instruments’ (PAI). These PAI’s fall in either of the two categories; Artificial or Human. These are further broken down into the following sub-categories (the relevant presentation attacks in **bold**) [14]:

Artificial	Complete	Gummy finger, **video of face**
	Partial	Glue on finger, **sunglasses, artificial/patterned contact lens, non-permanent make up**
Human	Lifeless	**Cadaver part**, severed finger/hand
	Altered	**Mutilation**, surgical switching of fingerprints between hands and/or toes
	Non-conformant	**Facial expression/extreme**, tip or side of finger

	Coerced	**Unconscious, under duress**
	Conformant	**Zero effort impostor attempt**

Table as found in [14] page 4.

These types of attacks are addressed in the requirement section of this document. ISO/IEC 30107 (all parts) [14], [15] and [16] addresses techniques for the automated detection of presentation attacks. These techniques are called presentation attack detection (PAD) mechanisms. An overview of these are found in the requirements section.

Asset	Threat	Possible consequence
Static Image Series of static images Video	Technical image quality is deliberately made low Optical image is manipulated in device Image not according to specifications (light, contrast etc).	Image of wrong person is captured.
Presence detection in image (presentation attack detection)	Artefacts in image No liveness in images, video Subject altered Non-conformance Coercion Obscuration [14]	Not able to perform presence detection. Wrongful presence detection
Presence detection with Interaction	Interaction with challenge-response not possible with subject	Not able to verify presence detection
Integrity of Presence detection	Interaction streamed from somewhere else. Interaction played back from earlier captured video.	Presence wrongfully accepted.

6.9 The biometric data is uploaded to the service provider.

Before the photographic data captured in step 9 is uploaded to the central verification service, the data need to be integrity protected. The process of uploading the data must be protected by industry standard secure networking technologies to ensure data protection.

Asset	Threat	Possible consequence
Integrity of data in self-service application	Trojan manipulating data	Manipulated data uploaded
Integrity of data during transport	Man-in-the middle	Manipulated data uploaded
Integrity of data at the service provider	Trojan, hacking, internal threats	Manipulated data input in to verification process.

6.10 The uploaded or streamed biometric sample of the applicant is verified (compared) against the biometric data earlier uploaded from the ID-document

The process of verification of the biometric data involves comparing the captured image with the image read and uploaded from the ID-document, either the VIZ-picture or RFID-extracted image from the onboard chip.

The comparison process involves creating a template from both sources of images and comparing these. "*The template creation process preserves the distinct and repeatable biometric features from the captured biometric image and generally uses a proprietary software algorithm to extract a template from the stored image. This defines that image in a way that it can subsequently be compared with another sample image captured at the time identity confirmation is required and a comparative score determined.*" "*The verification process takes the new sample of an eMRTD holder and compares it to a template derived from the stored image of that holder to determine whether the holder is presenting in the same identity*" [7] (ICAO 9303_p9 page 5).

To further enhance the probability that the real person trying to register the identity is the same person holding the identity of the ID-document, an analysis of a series of images during interaction with the subject must be applied.

The result of the comparison process must result in an identity and a confidence score.

Identification with human based face comparison

Asset	Threat	Possible consequence
Subjective person face recognition	Human factor when comparing images from the authoritative source and the captured image.	False acceptance of wrong person False acceptance of person wearing mask or other obfuscation
Subjective presence detection	Human factor in challenge response interaction with subject Ability to detect: Artefacts in image No liveness in images, video Subject altered Non-conformance Coercion Obscuration [14]	False acceptance of synthetic person in moving image False acceptance of synthetic person in static image

Identification with machine-based face comparison

Asset	Threat	Possible consequence
Ability to create comparable templates	Specific attack based on knowledge of template algorithm	Pictures of different persons are validated by the algorithm as being the same person.
Objective comparison of templates	Low objective quality of comparison algorithm	High false positive identification High false negative identification

Asset	Threat	Possible consequence
Objective presence detection	Low objective quality of algorithm to verify presence of real person in the captured images Ability to detect: Artefacts in image No liveness in images, video Subject altered Non-conformance Coercion Obscuration [14]	Not real person accepted Real person not accepted

6.11 Identity is verified at certain level

Depending on the combination of the desired identity verification profile and the achieved profile, the central service should be able to calculate an identity confidence score. Based on this, the achieved confidence level should be used to decide on whether to apply customer measures or not.

Use-case	Confidence level 1	Confidence level 2	Confidence level 3
Bank-BankID Pub-high	Onboarding can be completed. Ordinary customer measures to be applied	Onboarding can be completed. Moderate customer measures to be applied	Onboarding cannot be completed, without measures to increase probability of identity. Depending on measures, confidence may be improved to level 2
Bank-all Bank-limited Pub-subst	Onboarding can be completed. Moderate customer measures to be applied	Onboarding can be completed. Extended customer measures to be applied	Onboarding cannot be completed. Further measures need to be taken to improve level of confidence.
Priv-norm Priv-legal	Onboarding can be completed Measures may be taken to increase assurance level to Substantial.	N/A	N/A

Security asset	Threat	Possible consequence
The achieved confidence level	Attack on the confidence level calculation algorithm	Confidence level too high False acceptance

7 Client Device, connectivity and software requirements

The requirement type defines the minimum Level of Assurance (LoA) the requirement applies to. For each of the requirements it is indicated which level of Assurance the requirement applies to.

7.1 Client Operating system

#	Requirement basis / Threat	Requirement	Profile
7.1.1	Running self-service application on insecure device	All processing and analysis of data shall be performed in the central verification service. I.e. the self-service application shall only handle capture and protection of raw data.	All
7.1.2	Running self-service application on insecure device	The self-service application shall be able to detect if the device is rooted and report this securely to the central verification service.	All
7.1.3	Running self-service application on insecure device	The self-service application shall be able to collect other runtime and environmental data and report this securely to the central verification service.	Bank-BankID Bank-all Pub-high
7.1.4	Running self-service application on insecure device	The self-service application shall abort based on instruction from central verification service.	All
7.1.5	Running self-service application on insecure device	The self-service application should disallow read/write access to itself from other applications.	All

7.2 Client ID document optical capture device

The unit needs to be able to read the ID document in some form. This section lists the requirements for a camera as such a capture device.

#	Requirement basis / Threat	Requirement	Profile
7.2.1	Camera or picture quality too low	Resolution and colour depth of picture: The camera on the self-service device must be able to capture images with a minimum of 4 megapixels.	All

<table>
<tr><th>#</th><th>Requirement basis / Threat</th><th>Requirement</th><th>Profile</th></tr>
<tr><td>7.2.2</td><td>Camera or picture quality too low
Camera not able to capture security features</td><td>Captured images shall be in full colour (not black-and-white).</td><td>All</td></tr>
<tr><td>7.2.3</td><td>Camera not able to capture security features</td><td>Capture of infrared ink</td><td>Bank-BankID
Bank-all
Pub-high

Conditional on availability for dedicated terminals</td></tr>
<tr><td>7.2.4</td><td>Camera not able to capture security features</td><td>Capture of ultraviolet ink
UV Blue and red shall be captured.
<table>
<tr><th>Criteria</th><th>UV-color</th></tr>
<tr><td>Color</td><td>Yes</td></tr>
<tr><td>Density</td><td>Yes</td></tr>
<tr><td>Stains (absence of)</td><td>Yes</td></tr>
<tr><td>Negative stains (absence of)</td><td>Yes</td></tr>
<tr><td>Even edge</td><td>Yes</td></tr>
<tr><td>Optical blur (absence of)</td><td>Yes</td></tr>
<tr><td>UV 390 nm (color adjustment preferred)</td><td>Yes</td></tr>
<tr><td>In register</td><td>Yes</td></tr>
<tr><td><b>Total</b></td><td><b>Yes</b></td></tr>
</table>
Each colour shall be evaluated according to a scale from 1-6, where 6 is perfect result. Two scores of ‘5’ or one score of ‘4’ is acceptable.</td><td>Bank-BankID
Bank-all
Pub-high

Conditional on availability for dedicated terminals</td></tr>
</table>

7.3 Client ID document RFID capture device

This section lists requirements for the RFID reader to capture information from the ID document.

#	Requirement basis / Threat	Requirement	Use-case
7.3.1	Not able to read NFC-chip	Onboard RFID reader must be able to read RFID chips with NFC-technology operating at the 13.56 Mhz frequency.	Bank-BankID Bank-all Pub-high

7.4 Client Biometric sample optical capture device

The unit used must have a device to capture the user's features in some way to compare with the ID document presented. In addition to a camera, this might be fingerprint reader, voice, etc. These are currently not further defined in this document but could be added at a later date.

#	Requirement basis / Threat	Requirement	Profile
7.4.1	Camera or picture quality too low	Pixel resolution and colour depth: The camera on the self-service device must be able to capture images with a resolution of 4 Megapixels. Captured images shall be in full colour (not black-and-white). For reference: the minimum viable file size is regarded to be around 12-20 kB for JPEG and 6-10 kB for JPEG2000.	All
7.4.2	Camera or picture quality too low	Resolution and colour depth of video: The camera on the self-service device must be able to capture moving images at 720p with 30 frames per second.	Bank-limited Pub-subst

7.5 Client Application user interface

#	Requirement basis / Threat	Requirement	Profile
7.5.1	Attack on service trigger Session Collapse Application running on insecure device	The subject shall be made aware of which data is collected and captured during the identity verification.	All
7.5.2	Attack on service trigger Session Collapse Application running on insecure device	The subject shall be made aware of where the data that is collected and captured during the identity verification is analysed and archived. This also includes the archive period.	All
7.5.3	Attack on service trigger Session Collapse Application running on insecure device	Subject must be made aware of and understand the consequences of ID-verification process.	All

7.6 Client Application security

#	Requirement basis / Threat	Requirement	Profile
7.6.1	Old (discontinued) version of the self-service application is running	The Central Verification Service must verify which version of the self-service application that is running.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

#	Requirement basis / Threat	Requirement	Profile
7.6.2	Old (discontinued) version of the self-service application is running	The Central Verification Service must maintain a list of currently allowed versions of the self-service-application.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
7.6.3	Old (discontinued) version of the self-service application is running	The self-service application must be able to terminate the session based on instruction from the Central verification service.	All
7.6.4	Self-service application code is modified before installation	Self-service application code shall be obfuscated	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
7.6.5	Self-service application code is modified after installation	Self-service application must perform self-integrity check.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
7.6.6	Self-service application process is hijacked at run-time (including trojans)	There should be protected against process injection in self-service application.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
7.6.7	Self-service application memory data is altered	The self-service application must have high resilience against trojan attacks changing data in memory.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
7.6.8	Identification process interrupted and continued later (asynchronous)	The self-service application should be able to detect if a verification session is started on one device and continued on another device.	Bank-BankID Bank-all Pub-high
7.6.9	Cryptographic key management	The self-service application should follow best practices for how cryptographic keys are managed and how the lifecycle of these keys are enforced.	All
7.6.10	Application integrity	The self-service application should not write sensitive data outside the application container or the system credential storage facilities.	All

7.7 Communication security

The self-service application must be able to communicate in a secure manner with the central verification service of the service.

The central verification service must have reliable communications with other registry servers.

#	Requirement basis / Threat	Requirement	Profile
7.7.1	Preservation of data confidentiality and integrity	Communication between the self-service application and the central verification service shall implement TLS and TLS certificate pinning	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
7.7.2	Preservation of data confidentiality and integrity	Communication between the central verification service and other registry services (such as the National Person Register) shall be secured with TLS or equivalent.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst Conditional subject to availability
7.7.3	Preservation of data confidentiality and integrity	The central verification service shall not transmit payload data to the self-service application if the self-service application cannot be correctly identified.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
7.7.4	Preservation of data confidentiality and integrity	The self-service application shall not transmit payload data to the central verification service if the central verification service cannot be correctly identified.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

8 Central verification service requirements

8.1 Server Service requirements

#	Requirement basis / Threat	Requirement	Profile
8.1.1	Attack on central service	The session and relevant session data in the central verification service must be protected from manipulation.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.1.2	Attack on central service	Only authorised and trained personnel shall have access to the server and its applications.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.1.3	Attack on central verification service to change status	The session and relevant session data in the central verification service need to be protected.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

#	Requirement basis / Threat	Requirement	Profile
8.1.4	DOS-attack on central verification service or other related services	The central verification service should be protected against Distributed Denial-of-service (DDOS) attacks, network attacks and other attempts to render the service unavailable.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.1.5	Session timeout	Sessions are invalidated at the central verification service after a predefined period of inactivity.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

8.2 Server Audit log

An audit log must exist to ensure post diagnosis can be performed to ensure re-validation if a question of correctness arises, or to investigate errors and fraudulent actions.

#	Requirement basis / Threat	Requirement	Profile
8.2.1	Compliance	The central verification service shall forward captured ID document information from Self-service application, including images to the calling institution	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.2.2	Compliance	The central verification service shall forward all static biometric information from self-service application to the calling institution, subject to legal requirements.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.2.3	Compliance	Log which verification checks are completed. If a check fails, the reason for the failure shall be identifiable in the logs.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.2.4	Compliance	Result from verification requests to other services (such as National Person Registry) shall be logged.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.2.5	Compliance	The session identifier shall be included in all log entries	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.2.6	Compliance	A timestamp shall be included in all log entries with date and time	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
8.2.7	Protection of audit log	All audit logs shall be protected for confidentiality and integrity purposes.	Bank-BankID Bank-all Pub-high

9 Session requirements

9.1 Establishing session

#	Requirement basis Threat	Requirement	Profile
9.1.1	Attack on service trigger	A technical session identifier must be established from the calling application (i.e. banking application). The session identifier shall be used to bind the user session to the technical session by all parties. The technical session identifier must be communicated to the central verification service in a secure manner.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
9.1.2	Attack on service trigger	A visual session identifier must be created by the calling application. The visual session identifier must be displayed to the applicant by the calling application (i.e. banking application), before the applicant is redirected to the identity verification application. The visual session identifier must be communicated to the central verification service in a secure manner. The visual session identifier must be presented to the applicant by the calling application and by the identification application.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
9.1.3	Session collapse	All parties must deploy strict session control. The session identifier must be present in all data communication between the parties during the identification process.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

10 Requirements for ID document capture

The ID document is captured in two ways, either visually (picture) or by reading the RFID chip in the ID document. In practice, a combination of several methods may be used as illustrated below:.

- Visual capture of VIZ only
- Visual capture og MRZ and machine-reading of RFID-chip
- Visual capture of VIZ and MRZ, and machine reading of RFID-chip

The combination of the methods used depend on the technical capability of the device used and the applicable profile for the verification of identity. See requirements below for the different profiles.

10.1 Visual capture

#	Requirement basis Threat	Requirement	Profile
10.1.1	Manual attack on device	The self-service application must have direct access to the camera on the device.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst Priv-norm Priv-legal

Consumer devices currently do not support capture of information written with infrared or ultraviolet ink using standard cameras. However, self-service kiosks can have such equipment.

Reading and verification of such information is not covered in this requirement document yet. However, it is an approach which might assist in verifying an identity for ID documents without a RFID chip or where the chip has been damaged.

#	Requirement basis Threat	Requirement	Profile
10.1.2	Camera not able to capture the image of the identity document	The multi-purpose self-service device must be able to capture an image of the ID-document. The image must of a quality that enables further analysis of the picture of the subject and OCR interpretation.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst Priv-norm Priv-legal
10.1.3	Camera not able to capture security features	The multi-purpose self-service device must be able to capture the following security features: Lamination Dynamic content of Holographic images	Bank-all Bank-limited Pub-subst Applies to multi-purpose devices
10.1.4	Camera not able to capture security features	The dedicated self-service terminal must be able to capture the following security features: Lamination Dynamic content of holographic images Infrared or ultraviolet ink features Microprint content	Bank-all Bank-limited Pub-subst Conditional on availability: for dedicated terminals only
10.1.5	Camera not able to capture security features	The self-service device must be able to capture moving images or a series of still images.	Bank-limited Pub-subst
10.1.6	Not all elements captured by camera	The self-service device must be able to capture images of the ID-document from different angles based on challenge response with the subject.	Bank-limited Pub-subst

#	Requirement basis Threat	Requirement	Profile
10.1.7	Image file is changed, alteration of picture	The self-service device must protect the captured files in device or in transit.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
10.1.8	Interaction	The self-service application must enable interaction with challenge-response between the central verification service and the person presenting the ID-document.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

10.2 RFID capture

Currently, only available for dedicated terminals, Android based mobile devices and specific personal computer models.

#	Requirement basis Threat	Requirement	Profile
10.2.1	Manual attack on device	The self-service application must have access to the NFC-reader on the device.	Bank-BankID Pub-high
10.2.2	ID-document does not have onboard RFID-chip. RFID chip is unreadable	The self-service application must be able to detect if RFID-chip is present.	Bank-BankID Pub-high
10.2.3	RFID reading session	The self-service application must be able to use the data from the MRZ to negotiate a session key with the RFID-chip using the Basic Access Control (BAC) protocol or the Supplemental Access Control (SAC).	Bank-BankID Pub-high
10.2.4	RFID reading session	The self-service application must be able to read the encrypted contents of the RFID-chip using the session key established using the BAC or SAC protocol.	Bank-BankID Pub-high
10.2.5	RFID reading session	The self-service application must logically bind the read contents of the RFID-chip to the technical session identifier.	Bank-BankID Pub-high

10.3 Logical ID-document capture

This section applies to 'logical documents' implemented in digital media only. Such an electronic identification means consists of personal identification data attributes stored within a secured enclave implemented in digital media (e.g. an app on a mobile device). These electronic identification means have no physical representation and are only electronically readable (i.e. digital only). They may rely on technology which is not yet commonplace for eID means in the public sector today, such as mobile applications. It can be assumed such means might increasingly be used. [22]

#	Requirement basis Threat	Requirement	Profile
10.3.1	Manual attack on device	The self-service application must have access to an interface to read the contents of the logical ID-document.	All
10.3.2	Logical document reading session	The self-service application must logically bind the read contents of the logical ID-document to the technical session identifier.	All

10.4 ID document validation

Profiles where RFID-chip is not required

#	Requirement basis Threat	Requirement	Profile
10.4.1	ID-document not according to specifications for ID-documents issued at the time of issuance	The central verification service should have access to a database with specifications of all european ID-documents issued for the maximum lifetime of any issued ID-document plus five years.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst Conditional on availability of database
10.4.2	The ID-document does not fulfil the requirements	The central verification service should compare the image of VIZ and MRZ for existence of expected elements at the time of issuance of the ID-document, ref 10.4.1. This includes, but is not limited to: - Check of image of ID-document to detect integrity of lamination. - Checks of image of ID-document to verify the existence of the embedded hologram. - Checks of image of ID-document to verify existence of other holographic elements. - Checks of image of ID-document to verify existence of embedded image and text-elements.	Bank-limited Pub-subst
10.4.3	Image of VIZ General quality issues Camera Issues Deliberate quality deterioration	The central verification service shall analyse the images for any artefacts either introduced by optical/technical disturbances or deliberate quality deterioration. The analysis shall be based on the checks performed in section 10.4.2.	Bank-limited Pub-subst

#	Requirement basis Threat	Requirement	Profile
10.4.4	Image of VIZ General quality issues Camera Issues Deliberate quality deterioration	The central verification service shall inspect the VIZ for signs of deliberate quality deterioration or manipulation. - Check of image of ID-document to detect integrity of lamination. - Checks of image of ID-document to verify the existence of the embedded hologram. - Checks of image of ID-document to verify existence of other holographic elements. - Checks of image of ID-document to verify existence of embedded image and text-elements.	Bank-limited Pub-subst
10.4.5	Picture of ID-document holder in VIZ Photo substitution	The central verification service shall analyse the embedded picture of the ID-document holder in the VIZ for signs of photo substitution.	Bank-limited Pub-subst
10.4.6	Image of text in VIZ	The central verification service shall analyse the text fields in the VIZ for signs of manipulation and character substitution.	Bank-limited Pub-subst
10.4.7	Image of text in VIZ not readable	The central verification service shall be able to read and interpret the data from the image using Optical Character Recognition (OCR). The following data shall be extracted from the image: - The ID-document number - The name of the ID-document holder - The name of the issuer - The date of birth of the ID-document holder - The national identification number (if available)	Bank-limited Pub-subst
10.4.8	Image of MRZ General quality issues Camera Issues Deliberate quality deterioration	The central verification service shall inspect the MRZ for signs of deliberate quality deterioration or manipulation. - Check of image of ID-document to detect integrity of lamination. - Checks of image of ID-document to verify the existence of the embedded hologram. - Checks of image of ID-document to verify existence of other holographic elements. - Checks of image of ID-document to verify existence of embedded image and text-elements.	Bank-limited Pub-subst
10.4.9	Data in MRZ Deliberate change in characters	The central verification service shall analyse the text fields in the MRZ for signs of manipulation and character substitution	Bank-limited Pub-subst
10.4.10	Integrity of data from both VIZ and MRZ	The central verification service shall compare the content from both VIZ and MRZ. - The central verification service shall abort the identification session if the datasets from VIZ and MRZ are not identical.	Bank-limited Pub-subst

Profiles where RFID-chip is required

Successful reading of the RFID-chip depends on reading of the MRZ. Hence, successful completion of LOA Substantial is a requirement before proceeding to LOA High verification of identity.

#	Requirement basis Threat	Requirement	Profile
10.4.11	RFID chip Attributes not available	The central verification service shall implement controls to check if all expected data is available from the RFID-chip. The central verification shall fallback to a lower Level of Assurance if all expected attributes are not available.	Bank-BankID Pub-high
10.4.12	Integrity of data from RFID-chip	The central verification service shall check the integrity of the data from the RFID chip. This includes, but is not limited to: - Checks that the signature is made with the correct signing-certificate - Checks that the signing certificate has not expired. - Checks of the integrity and validity of the signature (signature validation) - Verify that the certificate has not been revoked - Validate certificate chain to trusted root	Bank-BankID Pub-high
10.4.13	Data from MRZ and RFID-chip not identical	The central verification service shall compare all data from the MRZ with the data read from the RFID-chip.	Bank-BankID Pub-high
10.4.14	Check if ID-document is revoked	The central verification service should check with the issuing authority of the ID document if the document is still valid or has been revoked (lost, stolen, etc.) if such a service is available. (Such as TOVE in Norway)	Bank-BankID Pub-high Conditional on access to database

11 Requirements for subject biometric capture

11.1 Visual capture

In this section the term challenge response is used when describing the requirements for interaction between the applicant and the self-service application. The term must be understood in a broader context; "... challenge is a purposeful activity that has an expected response when in the presence of the targeted condition". The response may be voluntary or involuntary, and the challenge may be evident or non-evident to the applicant.

Applies if no RFID-data is present in chip if RFID data is not required.

#	Requirement basis Threat	Requirement	Profile
11.1.1	Static high-resolution still image Technical picture quality is deliberately made low Optical picture is manipulated in device Picture not according to specifications	The self-service application must be able to take several static images based on challenge-response [14] from the application to the applicant. The front facing static image must be according to ISO/IEC 19794-5:2011 [19] and comparable to the image embedded in VIZ in the ID-document.	Bank-limited Pub-subst
11.1.2	Moving Image (Video) Video not according to specifications	The moving image must be captured in a comparable environment as the image embedded in VIZ in the ID-document. The moving image should be according to ISO/IEC 19794-5:2011 [19].	Bank-limited Pub-subst
11.1.3	Interaction	The self-service application must enable challenge-response [14] based interaction between the central verification service and the applicant.	Bank-limited Pub-subst
11.1.4	Image integrity Image or moving image file is changed in the application. Image or moving image not from device camera	The self-service application should protect the image files from changes in memory and in transit.	Bank-limited Pub-subst optional if applicable to risk management
11.1.5	Image integrity Image or moving image file is changed in the application. Image or moving image not from device camera	The self-service application should add the technical session identifier to the metadata of the static and moving image.	Bank-limited Pub-subst optional if applicable to risk management

Applies if RFID-data is present in chip and is verified by the central verification service.

#	Requirement basis Threat	Requirement	Profile
11.1.6	Static high-resolution image front facing Technical picture quality is deliberately made low Optical picture is manipulated in device Picture not according to specifications	The self-service application must be able to take several static images based on challenge-response [14] based instructions from the application to the applicant. The front facing static image must be according to ISO/IEC 19794-5:2011 [19] and comparable to the image as extracted from the RFID-chip in the ID-document.	Bank-BankID Pub-high
11.1.7	Moving image (series of high-resolution images) Series of images not according to specifications.	The series of images image must be according to ISO/IEC 19794-5:2011 [19] and captured in a comparable environment as the image embedded in VIZ in the ID-document.	Bank-BankID Pub-high
11.1.8	Image integrity Image or moving image file is changed in the application. Image or moving image not from device camera	The self-service application may protect the image files from changes in memory and in transit.	Bank-BankID Pub-high conditional if applicable to risk management

#	Requirement basis Threat	Requirement	Profile
11.1.9	Image integrity Image or moving image file is changed in the application. Image or moving image not from device camera	The self-service application should add the technical session identifier to the metadata of the static and moving image.	Bank-BankID Pub-high conditional if applicable to risk management
11.1.10	Interaction	The self-service application must enable challenge-response [14] based interaction between the central verification service and the applicant subject.	Bank-BankID Pub-high

12 Requirements for verification of identity

This final section describes requirements for how the overall verification of identity based on the verified captured information shall be confirmed.

12.1 Comparison of ID document and biometric data

Ref: "The uploaded biometric data of the applicant is verified against the biometric data earlier uploaded from the ID-document. "

Metrics for testing of face comparison algorithms are widely recognised as being FAR/FMR and FNMR/FMR. As these metrics may differ according to the datasets they are being tested with, we have decided to include a reference to the NIST Face recognition vendor test (FRVT) [21] where all algorithms are being tested subject to the same extensive datasets. We have decided to make references to the most relevant dataset tests, including those for VISA, Mugshot and selfie images.

Profiles Bank-limited, Bank-all, Pub-subst, Priv-norm, Priv-legal

For LOA high the simple biometric comparison is made with an algorithm comparing the image from VIZ in the ID-document with the captured biometric samples. Based on a real time risk analysis a two-way audio/video session may be required.

#	Requirement basis Threat	Requirement	Profile
12.1.1	Simple objective face recognition algorithm	The simple objective face recognition algorithm recognition must deploy at least one face recognition technique/algorithms.	Bank-limited Bank-all Pub-subst Priv-norm Priv-legal

#	Requirement basis Threat	Requirement	Profile
12.1.2	Low objective quality of comparison algorithm	The captured picture must be recognized as the same person as in ID-document by a face recognition algorithm with: 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. FNMR rate of less than 0,1 for FMR at 1e-05 according to the NIST Face Recognition Vendor Test (FRVT) for Selfie photographs. [21]	Bank-limited Bank-all Pub-subst Priv-norm Priv-legal Bank-BankID Pub-high
12.1.3	Low objective quality mechanisms to verify real person in images	Based on risk analysis score from the comparison algorithm a subjective face recognition and liveness test may be required.	Bank-limited Bank-all Pub-subst Priv-norm Priv-legal
12.1.4	Subjective face recognition Human factor in direct dialogue with applicant.	The qualified operator must demonstrate ability to distinguish between different faces according to best practice in human face recognition. Training of qualified operators to detect attempts on fraud based on: 1) Face detection 2) Voice interaction 3) Psychological effects	Bank-limited Bank-all Pub-subst Priv-norm Priv-legal

Profile Bank-BankID, Pub-high

#	Requirement basis Threat	Requirement	Profile
12.1.5	Advanced objective face recognition algorithm	The advanced objective face recognition algorithm must deploy several different techniques for face recognition.	Bank-BankID Pub-high
12.1.6	Specific attack based on knowledge of algorithms	The template creation algorithm for face recognition must combine several different techniques to create comparable templates.	Bank-BankID Pub-high

For all Profiles

The following requirement applies to the confidence level calculation.

#	Requirement basis Threat	Requirement	Profile
12.1.7	Attack on the confidence level calculation algorithm	The confidence level calculation algorithm must have demonstrated a success rate of at least 99% using scientific and field tests. The results must be statistically significant.	all

12.2 Presentation attack detection

The requirements for presentation attack detection (PAD) as described in this section only applies to the same scope as the ISO/IEC 30107, i.e. the data capture process as illustrated in the below figure:

ISO/IEC 30107 focuses on biometric-based attacks on the data capture subsystem by biometric capture subjects attempting to subvert the intended operation of the system. Countermeasures against other attack vectors as illustrated in the figure is included in section 7 Device, Connectivity and software requirements, and section 8 Central Verification service requirements.

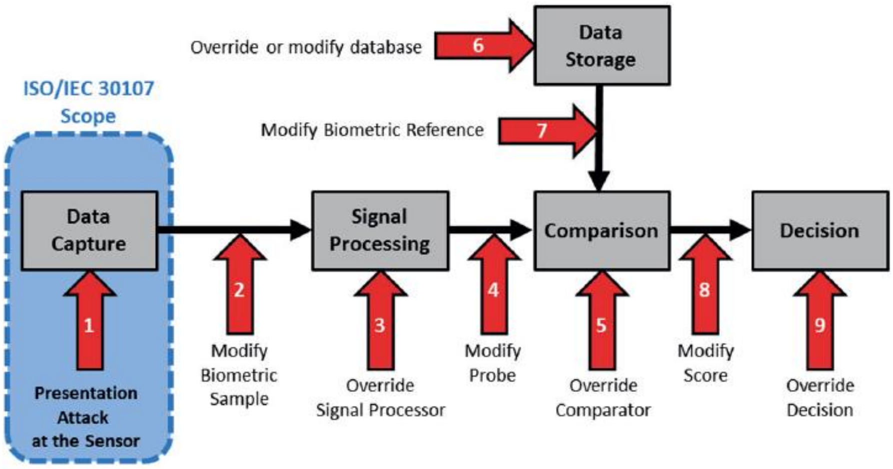


Figure 1 in [14]

#	Requirement basis Threat	Requirement	Profile
12.2.1	Subjective real person control Human factor in direct dialogue	The qualified operator must be able to detect presentation attacks based on biometric impostors. The qualified operator must be able to verify that: 1) The applicant is following the objective rules for images. 2) The applicant can follow given instructions in the challenge-response based interaction. 3) The applicant must show proof of human behaviour in the challenge-response based-dialogue. During the challenge-response interaction, the operator must identify signs of: 1) Artefacts 2) Liveness 3) Alteration 4) Non-conformance 5) Coercion 6) Obscuration [14]. Either manually or with assistance from software designed to identify the relevant signs.	Bank-limited Pub-subst Priv-norm Priv-legal

Commented [BJ1]: KOM HIT

#	Requirement basis Threat	Requirement	Profile
12.2.2	Low objective quality mechanisms to verify real person in images Subject of static image No human face presented Human wearing mask presented Deepfake	The Presentation Attack Detection (PAD) system must be able to detect presentation attacks based on biometric impostors. The PAD system must be able to verify that: 1) The applicant is following the objective rules for images. 2) The applicant can follow given instructions in the challenge-response based interaction. 3) The applicant must show proof of human behaviour in the challenge-response based-dialogue. During the challenge-response interaction, the central verification service must identify signs of: 1) Artefacts 2) Liveness 3) Alteration 4) Non-conformance 5) Coercion 6) Obscuration [14].	Bank-BankID Bank-all Pub-high

#	Requirement basis Threat	Requirement	Profile
12.2.3	Low objective quality mechanisms to verify real person in images	The PAD system must be evaluated and tested according to ISO/IEC 30107-3 [16]. The following metrics must be measured using the methodology described in article 13.2.2 in [16]: 1) Attack Presentation Classification error rate (APCER) The proportion of attack presentations using the same PAI (presentation attack instrument) species incorrectly classified as bona fide presentations in a specific scenario. 2) Bona fide presentation classification error rate (BPCER) The proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario.	Bank-BankID Bank-all Pub-high
12.2.4	Low objective quality mechanisms to verify real person in images	The PAD system should be evaluated and tested according to ISO/IEC 30107-3 [16]. The following metrics must be measured using the methodology described in article 13.2.2 in [16]: 1) Attack Presentation non-response rate (APNRR) The proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem 2) Bona fide presentation non-response rate (BPNRR) The proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem 3) Attack presentation acquisition rate (APAR) The proportion of attack presentations using the same PAI species from which the data capture subsystem acquires a biometric sample of sufficient quality	Bank-BankID Bank-all Pub-high

12.3 Other operational requirements

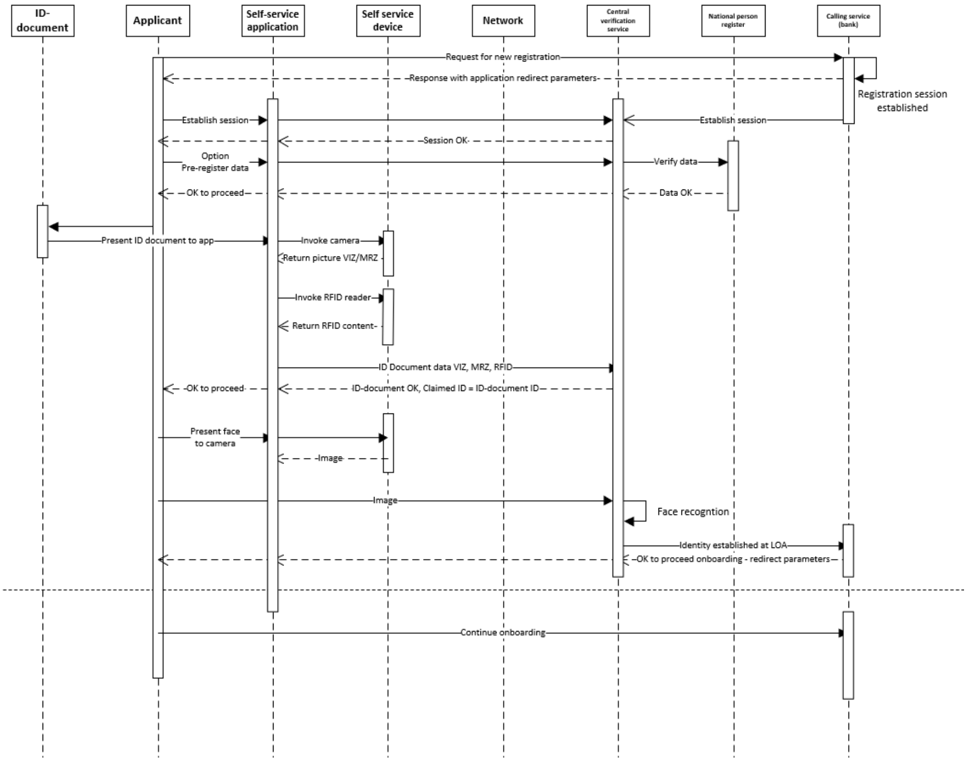
#	Requirement basis Threat	Requirement	Profile
12.3.1	Data is manipulated or removed in transit	The self-service application shall return an error-code to the central verification service if the central verification service cannot be specifically identified.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

#	Requirement basis Threat	Requirement	Profile
12.3.2	Assurance level	The verification service must provide the use-case for the identification	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
12.3.3	Confidence score	The verification service must provide the confidence score for the use-case	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst Priv-norm Priv-legal
12.3.4	Error codes	Defined error codes for any deviation from expected result must be defined for the solution.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
12.3.5	Compliance	The solution shall report attempted or suspected misuse	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
12.3.6	Compliance	The solution shall collect and make available statistics	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
12.3.7	Error handling	The central verification service must deploy failsafe fallback procedures if a problem occurs. This includes: • Return to calling application • Fall-back to less secure service	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

13 The onboarding process flows

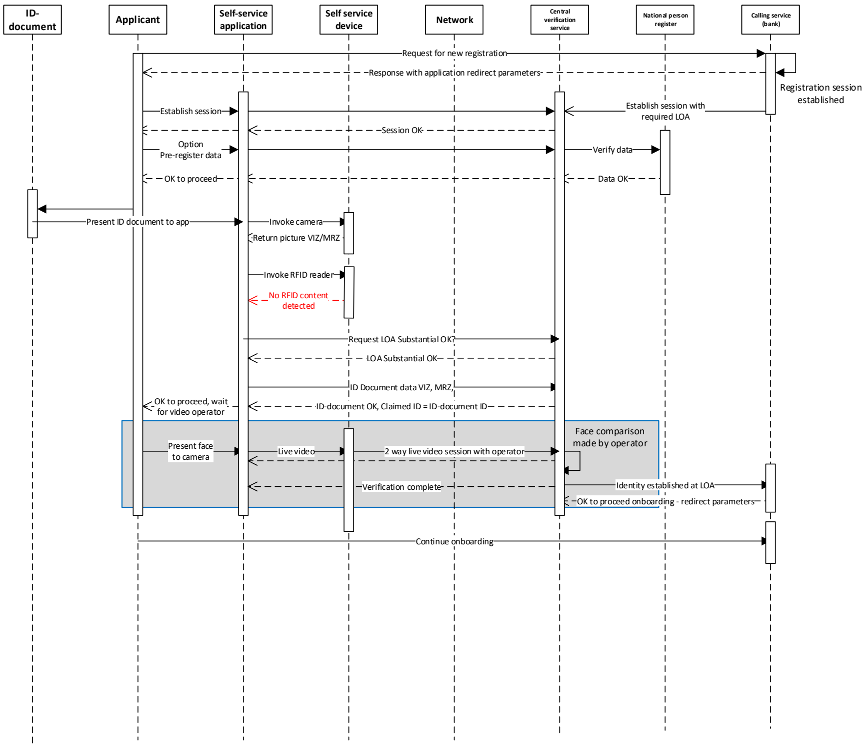
13.1 Generic ‘happy’ flow

The below sequence diagram illustrates the generic identification verification process without any exceptions.



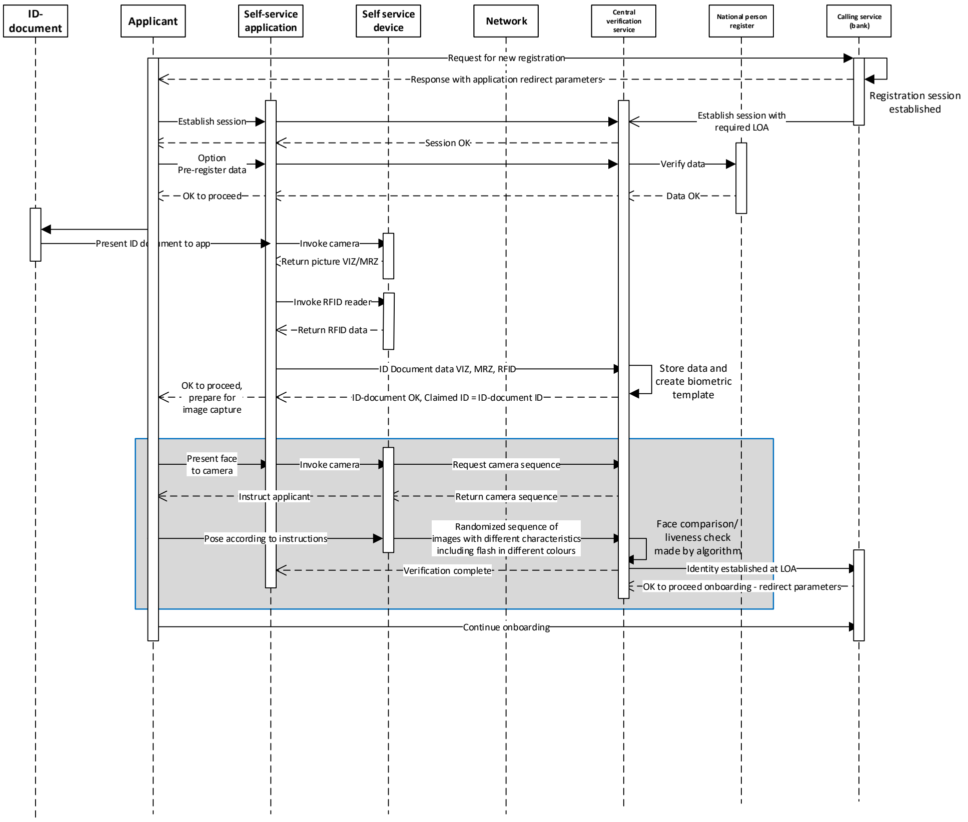
13.2 Sequence flow equivalent to eIDAS substantial or low

This diagram illustrates the flow for LOA Substantial, where this is a result of missing RFID data.


ID-document
Applicant
Self-service application
Self service device
Network
Central verification service
National person register
Calling service (bank)
Request for new registration
Response with application redirect parameters
Registration session established
Establish session
Establish session with required LOA
Session OK
Option
Pre-register data
Verify data
OK to proceed
Data OK
Present ID document to app
Invoke camera
Return picture VIZ/MRZ
Invoke RFID reader
No RFID content detected
Request LOA Substantial OK?
LOA Substantial OK
ID Document data VIZ, MRZ,
OK to proceed, wait for video operator
ID-document OK, Claimed ID = ID-document ID
Face comparison made by operator
Present face to camera
Live video
2 way live video session with operator
Identity established at LOA
Verification complete
OK to proceed onboarding - redirect parameters
Continue onboarding

13.3 Sequence flow equivalent to eIDAS high

This diagram illustrates the flow for LOA High.


ID-document
Applicant
Self-service application
Self service device
Network
Central verification service
National person register
Calling service (bank)
Request for new registration
Response with application redirect parameters
Registration session established
Establish session
Establish session with required LOA
Session OK
Option Pre-register data
Verify data
OK to proceed
Data OK
Present ID document to app
Invoke camera
Return picture VIZ/MRZ
Invoke RFID reader
Return RFID data
ID Document data VIZ, MRZ, RFID
Store data and create biometric template
OK to proceed, prepare for image capture
ID-document OK, Claimed ID = ID-document ID
Present face to camera
Invoke camera
Request camera sequence
Instruct applicant
Return camera sequence
Pose according to instructions
Randomized sequence of images with different characteristics including flash in different colours
Face comparison/ liveness check made by algorithm
Verification complete
Identity established at LOA
OK to proceed onboarding - redirect parameters
Continue onboarding

14 Appendix 1: Good Practices

In this section we have included several optional steps. These steps do not increase the probability of verifying the identity but may enhance the user experience and hence the probability of successful onboarding process.

14.1 Optional: Person registers claimed identity data in self-service application provided by service provider.

During the initial phase of the verification process, the person may be asked to register his/her claimed identity in the application.

The basis for the claimed identity may come as a result of a prior interaction with the service provider, or as an integrated part of the onboarding process. The information about a claimed identity is useful in the process but is not a requirement as the identity anyhow will be provided as a result of the verification process of the identity document. Therefore, the claimed identity is to be regarded as an optional input to the process of online onboarding.

Basis for requirements

Asset	Threat	Possible consequence	Use-case
Integrity of national identity number	Attack changing the entered national identity number	Input to verification process is changed. Not critical as it will be discovered at later stage.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

Requirements

#	Requirement basis Threat	Requirement	Use-case
14.1.1	Attack changing the entered national identity number	The national identity number as entered by the applicant must be integrity protected.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

14.2 Conditional: The service provider verifies claimed identity of applicant against the national person register

Condition: The person has provided a Norwegian national ID-number or D-number.

To verify the existence of an identity the bank can query the Norwegian person register with the claimed national identity number or D-number. This applies to Norwegian citizens and persons with permanent residence in Norway.

For foreign persons who are not listed in the national register, this option is not viable and other measures to increase the probability of the existence of the identity must be made, ref step 11 below.

Basis for requirements

Asset	Threat	Possible consequence
Access to national register	Re-routing of query to false register, returning false data	False positive, i.e. non-existing person will have status as existing False negative, i.e. existing person will have status as non-existing Other name than real name is returned
Acceptance of identity	Attack on central service	False status for identity in central service.

Requirements

#	Requirement basis Threat	Requirement	Use-case
14.2.1	Re-routing of query to false register, returning false data	The central verification service must authenticate the national register.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
14.2.2	Attack on central service	Status of identity must be protected	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

14.3 Conditional: The claimed identity of the applicant as registered in earlier is compared with the identity from the ID-document.

This conditional step depends on that a claimed identity was established earlier. If no claimed identity was established, the identity as captured from the machine-reading of the ID-document will form the claimed identity and step 3 will have to be performed as part of this step instead.

Basis for requirements

Asset	Threat	Possible consequence
Availability of data	Data deliberately removed	Less probability of establishing a 100% match
Integrity of data in central service	Any of the datasets have been changed to match the other dataset	False positive match

The information elements that can be compared are personal identification number and full name. However, the complete list of attributes available from the ID-document should be collected and used for establishing the identity of the applicant. For natural persons these attributes include:

Requirement	Attribute
Mandatory	Name*# Address*# Date of Birth*#[1] Unique identifier*[2]

Requirement	Attribute
Additional KYC	Nationality# Place of birth# Gender#
Optional KYC	Name at Birth e-mail occupation

* Required for residents for access to banking in Norway according to Hvitvaskingsloven § 12

# Required for non-residents for access to banking in Norway according to Hvitvaskingsloven § 12

[1] and [2] are available in the Norwegian identity number field. For persons with D-number and foreign ID-documents this must be read from the DOB field in the ID-document

Requirements

#	Requirement basis Threat	Requirement	Use-case
14.3.1	Data deliberately removed	The central verification unit must compare the claimed identity registered in step 1, with the identity as verified from the ID-document in step 8.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
14.3.2	Any of the datasets have been changed to match the other dataset	If the two datasets are not identical the central verification service shall return control to the calling application to restart the identification process.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

15 Verification of identity

Basis for requirements

Asset	Threat	Possible consequence
Real person presence	No human face presented Human wearing mask presented Deepfake	False acceptance of other person or entity than ID-document holder

Requirements

#	Requirement basis Threat	Requirement	Use-case
15.1.1	No human face presented Human wearing mask presented Deepfake	- The applicant must be requested by the application to move the face in different angles to detect liveness. The sequence of the requested angles must be random from session to session. - The self-service application must be able to project different light conditions on the person's face during the static and moving image session.	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst

15.2 Measures to increase the probability of the existence of identity to increase the confidence level.

Depending on the combination of desired assurance level and the actual confidence level of the identity, measures can be taken to increase the confidence level, and ultimately also the assurance level of an identity.

These measures normally involve positive verification of data with other data sources, negative verification – i.e. check with blacklists of stolen ID-documents etc.

The measures shall be based on the reasons why the confidence level is lower than expected.

Basis for requirements

Asset	Threat	Possible consequence
Data from other electronic sources (other available register)	Electronic source not available Electronic sources may not be updated with most recent data.	Not able to increase confidence, manual process needs to be invoked
Negative data from other sources (blacklists)	Electronic sources may not be updated with most recent data	Not able to increase confidence, manual process needs to be invoked
Additional documentation provided by applicant.	Document not available False documentation provided	Not able to increase confidence, manual process needs to be invoked

Requirements

#	Requirement basis Threat	Requirement	Use-case
15.2.1	Electronic source not available	TBD	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
15.2.2	Electronic sources may not be updated with most recent data	TBD	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst
15.2.3	Document not available False documentation provided	TBD	Bank-BankID Bank-all Pub-high Bank-limited Pub-subst