Agency for Digital Government

IDENTITY PROOFING PRACTICE STATEMENT MITID ERHVERV

Version: 1.0

Author: Agency for Digital Government, MitID Erhverv

Published: January 2026

Erhverv

Table of contents

Change history

Version	Date	Change description
1.0	26-01-2026	Initial version

1. Introduction

This document constitutes the identification practice statement for entities registered in MitID Erhverv. It describes how registration procedures fulfil the requirements from [ETSI TS 119 461] at Baseline level and Extended Level of Identity Proving (LoIP).

In the following it is assumed that private MitIDs (MitID issued to Natural Persons) used in the identity proofing contexts have Extended LoIP.

This document is valid from 27 January 2026

1.1. Reading instructions

This document lists the practice of the identity proofing of applicants registered in MitID Erhverv.

Section **Fejl! Henvisningskilde ikke fundet.** describes how MitID Erhverv complies with general requirements from [ETSI TS 119 461]. There are 2 types of applicants in MitID Erhverv namely Legal Persons and Natural Persons representing a Legal Person. Section 5 describes how registration of Legal Persons complies with [ETSI TS 119 461] in two different identity proofing contexts and section 6 describes how registration of Natural Persons representing a Legal Person complies with [ETSI TS 119 461] in two other identity contexts.

Relevant requirements from [ETSI TS 119 461] are extracted and inserted with *blue italic text* followed by the practice in which the IPSP complies with the requirement.

1.2. Introduction to NSIS

The Danish Agency has developed the National Standard for Identity Assurance Levels (NSIS) for the purpose of creating a framework for trust between digital identities and digital ID services and NSIS serves as a reference framework and guideline for the work on user identity management in the Danish public sector.

NSIS is based on international standards and frameworks to ensure interoperability, knowledge sharing, compliance and support for the internal market, including the [eIDAS2] Regulation and the associated [Impl1502] on "Levels of Assurance" (LoA). The NSIS “substantial” LoA is comparable to eIDAS “substantial” LoA and NSIS “high” LoI is comparable to eIDAS “high” LoI. Since NSIS in its nature is not restricted to the scope of national identity schemes but can be applied to any identity scheme, the peer review process is not a supported method for ensuring compliance but instead NSIS relies on a compliance assessment from an independent NSIS auditor.

Furthermore, NSIS does have extra requirements compared to [Impl1502]. Relevant to this present practice statement NSIS regulates the binding of natural persons associated with a legal person in [NSIS] section 5.2.

Several legal entities have established NSIS compliant identity providers in the organisation in order to be able to use the internal employee identity scheme as federated identities.

An entity claiming NSIS compliance is under supervision of the same supervisory authority that supervises compliance with [eIDAS2]. The supervisory body maintains and publishes a list of compliant entities which can be downloaded from:

https://digst.dk/nsis/.

2. References

Reference	Document
[eIDAS2]	Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 and Directive (EU) 2022/2555
[ETSI EN 319 401]	ETSI EN 319 401 V3.1.1 (2024-06) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI TS 119 461]	ETSI TS 119 461 V2.1.1 (2025-02) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
[GRPS]	Den Danske Stat Practice Statement on General Security Requirements for Trust Service Providers.
[DocumentationReqEIA]	Documentation verifying the role of the management representative within the organization. https://mitid-erhverv.dk/en/get-started-with-mitid-erhverv/prepare-to-enter-into-a-connection-agreement/documentation-verifying-the-role-of-the-management-representative/.
[NSIS]	National Standard for Identiteters Sikringsniveauer (NSIS) Version 2.1 https://digst.dk/media/s0spdxxi/national-standard-for-identiteters-sikringsniveauer-nsis.pdf (in Danish) An English translation of version 2.0.1a https://digst.dk/media/ec4jdtbr/nsis-engelsk-version-201a.pdf
[Impl1502]	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

Reference	Document
	Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj/eng

3. Terms and Abbreviations

Abbreviation	Term
Applicant	Person (legal or natural) whose identity is to be proven as defined in [ETSI TS 119 461]
Baseline LoIP	Baseline LoIP as defined in [ETSI TS 119 461]
CAR	Conformity Assessment Report. In this context the CAR is an assessment of an IPSP's conformity with [ETSI TS 119 461] unless else explicitly noted
CPR	Det Centrale Personregister (Danish national civic registration system)
CPR number	Danish social security number registered in CPR
CVR	Central Virksomhedsregister (Danish national trade registration system)
CVR number	National Trade Registration number registered in CVR. A unique identification of Danish legal entities.
DIGST	Danish Agency for Digital Government
Extended LoIP	Extended LoIP as defined in [ETSI TS 119 461]
IPSP	Identity Proofing Service Provider as defined in [ETSI TS 119 461]
LoIP	Level of Identity Proving as defined in [ETSI TS 119 461]
TSP	Trust Service Provider in this document referring to MitID Erhverv as Identity Proofing Service Provider

4. General requirements for the MitID Erhverv as IPSP

4.1. Risk Management Framework and Risk Assessment

OVR-5-01: *The requirements specified in ETSI EN 319 401 [1], clause 5 shall apply.*

See below

> ***REQ-5-01:*** *The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues*
>
> See [GRPS]
>
> ***REQ-5-02:*** *The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.*
>
> See [GRPS]
>
> ***REQ-5 -03:*** *The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).*
>
> See [GRPS]
>
> ***REQ-5-04:*** *The risk assessment shall be regularly reviewed and revised.*
>
> See [GRPS]
>
> ***REQ-5-05:*** *The TSP's management shall approve the risk assessment and accept the residual risk identified.*
>
> See [GRPS]

OVR-5-02: *The IPSP's risk assessment shall be updated yearly.*

The risk assessment is updated on a yearly basis.

OVR-5-03: *The IPSP's risk assessment shall cover relevant risks related to identity proofing and at least:*

a) An assessment of the risks related to identity fraud; and

b) An assessment of the risks related to information systems security.

The risk assesses the risk related to identity fraud and information system security.

OVR-5-04: *The IPSP's risk assessment shall be updated if an identity proofing process is changed.*

Any major change including change in an identity proofing process will result in a risk assessment.

OVR-5-05: *The IPSP shall have a documented and effective procedure for threats intelligence that ensures that the IPSP's service is adapted to new threats.*

Procedures for threats intelligence are implemented, and the risk assessment are updated according to findings from the threats intelligence.

OVR-5-06: *The IPSP's risk assessment shall be updated according to findings from the threats intelligence procedure.*

See above.

[CONDITIONAL] OVR-5-07: *If the Baseline LoIP is claimed, the risk assessment shall consider at least attackers with moderate attack potential.*

The risk assessment considers threat agents with high attack potential which also applies to threat agents with moderate attack potential.

OVR-5-09: *Based on findings from the threats intelligence procedure and changes to the risk assessment, the need for training of personnel shall be assessed and training be carried out if needed.*

Training of personnel takes identified threats into account.

OVR-5-10: *The IPSP shall state in its practice statement goals for quality and security in terms of resilience to false acceptance and false rejection of applicants and perform regular testing of the performance against these goals.*

The goal for false acceptance for both legal persons and natural persons associated with legal persons is 0 cases per year.

The goal for false rejections for legal persons is maximum 10 cases per year before the legal person may complain of wrongfully rejection and have the case reviewed. The goal is measured by the number of complains.

The goal of false rejections for natural persons associated with legal persons is 0 cases per year.

These goals are measured with regards to the scope of the IPSP. E.g. if a person has wrongfully obtained another person’s MitID and uses this for identity proofing in MitID Erhverv’s use cases, this will not be counted.

4.2. Policies and practices

OVR-6.1-01: *The requirements specified in ETSI EN 319 401 [1], clause 6.1 shall apply.*

See below

REQ-6.1-01: *The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.*

The MitID Erhverv's practices are specified in this present practice statement.

REQ-6.1-02: *The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.*

This practice statement is approved by management, published and communicated to relevant parties.

In particular:

- ***REQ-6.1-03X:*** *The TSP shall have a statement of the practices and procedures used to address all the requirements of the applicable trust service policy as identified by the TSP.*

All applicable requirements are addressed in this present practice statement.

- ***REQ-6.1-04:*** *The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.*

See [GRPS]

- ***REQ-6.1-05X:*** *The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to demonstrate conformance to the trust service policy.*

This present practice statement has been made public for download.

- ***REQ-6.1-06:*** *The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.*

DIGST has a management body responsible for approving this present practice statement.

- ***REQ-6.1-07:*** *The TSP's management shall implement the practices.*

See [GRPS]

- ***REQ-6.1-08:*** *The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement.*

See [GRPS]

- ***REQ-6.1-09 [CONDITIONAL]:*** *When the TSP intends to make changes in its practice statement that might affect the acceptance of the service by the subject, subscriber or relying parties, it shall give due notice of changes to subscribers and relying parties.*

See [GRPS]

- ***REQ-6.1-10:*** *The TSP shall, following approval as in REQ-6.1-06 above, make the revised TSP's practice statement immediately available as required under REQ-6.1-05 above.*

See [GRPS]

- ***REQ-6.1-11:*** *The TSP shall state in its practices the provisions made for termination of service (see clause 7.12).*

See [GRPS]

OVR-6.1-02: *An IPSP claiming compliance with the present document shall identify in its practice statement the use cases for which compliance is claimed.*

MitID Erhverv is compliant with [ETSI TS 119 461] for the following use cases:

- 9.3 Use case for identity proofing of legal person on Extended LoIP
- 9.4 Use case for identity proofing of natural person representing legal person on Baseline LoIP and Extended LoIP

OVR-6.1-03: *Identification of use cases for which compliance is claimed shall be by reference to specific parts of clause 9 and/or Annex C of the present document*

See practice for ***OVR-6.1-02*** above.

OVR-6.2-01: *The requirements specified in ETSI EN 319 401 [1], clause 6.2 shall apply.*

See below

REQ-6.2-01: *TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.*

See [GRPS]

REQ-6.2-02: *The terms and conditions shall at least specify for each trust service policy supported by the TSP the following:*

a) the trust service policy being applied;

b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;

c) the subscriber's obligations, if any;

d) *information for parties relying on the trust service;*

e) *the period of time during which TSP's event logs are retained;*

f) *limitations of liability;*

g) *the applicable legal system;*

h) *procedures for complaints and dispute settlement;*

i) *whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;*

j) *the TSP's contact information; and*

k) *any undertaking regarding availability.*

The terms and conditions for MitID Erhverv specifies the elements listed above.

> ***REQ-6.2-03:*** *Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.*
>
> Subscribers and parties are informed of the precise terms and conditions as part of the onboarding to MitID Erhverv.
>
> ***REQ-6.2-04:*** *Terms and conditions shall be made available through a durable means of communication.*
>
> See [GRPS]
>
> ***REQ-6.2-05:*** *Terms and conditions shall be available in a readily understandable language.*
>
> See [GRPS]
>
> ***REQ-6.2-06:*** *Terms and conditions may be transmitted electronically.*
>
> See [GRPS]

OVR-6.3-01: *The requirements specified in ETSI EN 319 401 [1], clause 6.3 shall apply.*

See below

REQ-6.3-01: *The TSP shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.*

See [GRPS]

> ***REQ-6.3-02:*** *Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.*

See [GRPS]

In particular:

- ***REQ-6.3-03:*** *A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.*

See [GRPS]

- ***REQ-6.3-04:*** *The TSP shall establish procedures to notify of important changes in the provision of the trust service to the appropriate parties in accordance with business requirements and relevant laws and regulations, including changes in the provision of trust services and the intention to cease on its provision.*

See [GRPS]

- ***REQ-6.3-05X****: The TSP shall publish and communicate the information security policy to all employees who are impacted by it.*

See [GRPS]

- ***REQ-6.3-06X:*** *The TSP's information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.*

See [GRPS]

- ***REQ-6.3-07X:*** *Any changes that will impact on the level of security provided shall be approved by the management body referred to in REQ-6.1-07.*

See [GRPS]

- ***REQ-6.3-08X:*** *The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.*

See [GRPS]

- ***REQ-6.3-09X:*** *The maximum interval between two checks shall be documented in the trust service practice statement.*

See [GRPS]

4.3. Management and operation

OVR-7.1-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.1 shall apply.*

See below

> ***REQ-7.1.1-01*** *The TSP organization shall be reliable.*
>
> See [GRPS]
>
> ***REQ-7.1.1-02:*** *Trust service practices under which the TSP operates shall be non-discriminatory.*
>
> See [GRPS]
>
> ***REQ-7.1.1-03:*** *The TSP should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP's terms and conditions.*
>
> See [GRPS]
>
> ***REQ-7.1.1-04:*** *The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.*
>
> See [GRPS]
>
> ***REQ-7.1.1-05:*** *The TSP shall have the financial stability and resources required to operate in conformity with this policy.*
>
> See [GRPS]
>
> ***REQ-7.1.1-06:*** *The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.*
>
> See [GRPS]
>
> ***REQ-7.1.2-01:*** *Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets.*
>
> See [GRPS]

OVR-7.2-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.2 shall apply.*

See below

> ***REQ-7.2-01X:*** *The TSP shall ensure that all personnel and contractors apply information security in accordance with the established information security policy, topic-specific policies and procedures of the TSP.*

See [GRPS]

In particular:

- ***REQ-7.2-02:*** *The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding cybersecurity and personal data protection rules as appropriate for the offered services and the job function.*

See [GRPS]

- ***REQ-7.2-03X:*** *The TSP shall identify at least one person responsible for network and information security and reporting to top management.*

See [GRPS]

- ***REQ-7.2-04X:*** *TSP's personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.*

See [GRPS]

- ***REQ-7.2-05X****: This should include regular (at least every 12 months) updates on new threats and current security practices.*

See [GRPS]

- ***REQ-7.2-06X:*** *Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures.*

See [GRPS]

- ***REQ-7.2-07X****: Information security roles and responsibilities, as specified in the TSP's policy on the security of network and information systems, shall be documented in job descriptions or in documents available to all concerned personnel and allocated accordingly.*

See [GRPS]

- ***REQ-7.2-08X:*** *Trusted roles, on which the TSP's operation is dependent, shall be clearly identified.*

See [GRPS]

- ***REQ-7.2-09X:*** *TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.*

See [GRPS]

- ***PRO-7.2-10X:*** *Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.*

See [GRPS]

- ***REQ-7.2-11X:*** *Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.*

See [GRPS]

- ***REQ-7.2-12X:*** *Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.*

See [GRPS]

- ***REQ-7.2-13X:*** *All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.*

See [GRPS]

- ***REQ-7.2-14X:*** *Trusted roles shall include roles that involve the following responsibilities:*

  a) Security Officers: Overall responsibility for administering the implementation of the security practices.

  b) System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.

  c) System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.

  d) System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.

See [GRPS]

- ***REQ-7.2-15X:*** *TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security.*

See [GRPS]

- ***REQ-7.2-16X:*** *Trusted roles shall be accepted by the appointed person to fulfil the role.*

See [GRPS]

- ***REQ-7.2-17:*** *Personnel shall not have access to the trusted functions until the necessary checks are completed.*

See [GRPS]

- ***REQ-7.2-18X: [CONDITIONAL]*** *When personnel are working remotely, TSP shall implement cybersecurity measures to protect information accessed, processed or stored outside the TSP's premises.*

See [GRPS]

In particular:

- ***REQ-7.2-19X: [CONDITIONAL]*** *TSPs allowing remote working activities shall issue a topic-specific policy on remote working that defines the relevant cybersecurity conditions and restrictions.*

See [GRPS]

OVR-7.3-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.3 shall apply.*

See below.

REQ-7.3.1-01: *The TSP shall ensure an appropriate level of protection of its assets including information assets.*

See [GRPS]

REQ-7.3.1-02X: *The assets provided through a supply chain shall be protected as specified in clause 7.14.*

See [GRPS]

REQ-7.3.2.01X: *The TSP shall maintain an accurate inventory of assets as a prerequisite for effective technical vulnerability management and shall assign a classification consistent with the risk assessment.*

See [GRPS]

REQ-7.3.2-02X: *For asset, or group of assets, the inventory shall contain, when applicable:*

a) a unique asset ID;

b) an asset description;

c) the asset owner;

d) the asset location;

e) the asset type (e.g. software, hardware, services, facilities, HVAC systems, personnel, physical records);

f) the type of information processed or/stored in the asset and its information classification;

g) the date and version of the asset's last update or patch;

h) the classification level of the asset; and

i) the asset's end of life.

See [GRPS]

REQ-7.3.2-04X: *The TSP shall assure that the availability requirements of each asset, or group of assets, classified are aligned with the delivery and recovery objectives as described in the business and disaster recovery plan.*

See [GRPS]

REQ-7.3. 2-05X: *The TSP shall conduct periodic reviews of the classification levels of the assets.*

See [GRPS]

REQ-7.3.2-06X: *The TSP shall identify, document and implement rules for the acceptable use of and procedures for handling information and other associated assets.*

See [GRPS]

REQ-7.3.2-07: *The TSP shall implement and document procedures in case of change or termination process of, internal and external personnel, contractors or other third parties in order to include the return of all previously issued physical and electronic assets owned by or entrusted to the TSP.*

See [GRPS]

REQ-7.3.3-01X: *All storage media shall be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the TSP's classification scheme and handling requirements.*

See [GRPS]

REQ-7.3.3-02X: *Storage media used within the TSP's systems shall be securely handled to protect storage media from damage, theft, unauthorized access and obsolescence.*

See [GRPS]

REQ-7.3.3-03X: *Storage media management procedures shall protect against obsolescence and deterioration of storage media within the period of time that records are required to be retained.*

See [GRPS]

OVR-7.4-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.4 shall apply.*

See below

REQ-7.4.1-01: *The TSP's system access shall be limited to authorized individuals.*

See [GRPS]

In particular:

- ***REQ-7.4.1-02X:*** *The TSP shall administer user access of operators, administrators and other privileged accounts and system auditors applying the principle of "least privileges" when configuring access privileges. In particular:*

See [GRPS]

- ***REQ-7.4.1-03X:*** *The TSP shall provide setting up specific accounts to be used for administrative purposes like installation, configuration, management or maintenance.*

See [GRPS]

- ***REQ-7.4.1-04X:*** *Privileged accounts shall be used only if the privileges are necessary for the specific activity.*

See [GRPS]

- ***REQ-7.4.1-05X:*** *Strong identification, authentication and authorisation procedures shall be used for privileged accounts.*

See [GRPS]

- ***REQ-7.4.1-06X [CONDITIONAL]:*** *Where appropriate, the TSP shall ensure that users and devices are authenticated by multi-factor or continuous authentication mechanisms, such as secure voice, video and text, before accessing the TSP's network and ITS information systems, depending on the classification of the systems to be accessed.*

See [GRPS]

- ***REQ-7.4.1-07X:*** *The TSP shall review access rights to privileged and administrator accounts at planned intervals, and access rights shall be modified based on organisational changes. The result of the review, including the necessary changes of access rights, shall be documented.*

See [GRPS]

- ***REQ-7.4-1-08X:*** *The TSP shall ensure that access permissions are modified accordingly upon termination of employment or change of function.*

See [GRPS]

- ***REQ-7.4-1-09X:*** *Access to information and application system functions shall be restricted in accordance with the access control policy.*

See [GRPS]

- ***REQ-7.4.1-10X:*** *The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.*

See [GRPS]

- ***REQ-7.4-1-11X:*** *TSP's personnel shall be identified and authenticated before using critical applications related to the service.*

See [GRPS]

- ***REQ-7.4-1-12X:*** *TSP's personnel shall be accountable for their activities.*

See [GRPS]

- ***REQ-7.4-1-13X:*** *Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) or storage media (see clause 7.3.2) being accessible to unauthorized users.*

See [GRPS]

OVR-7.5-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.5 shall apply.*

See below

REQ-7.5-01: *Appropriate security controls shall be in place for the management of any cryptographic keys, cryptographic algorithms, and cryptographic devices throughout their lifecycle.*

See [GRPS]

OVR-7.6-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.6 shall apply.*

See below

In particular:

- ***REQ-7.6-02:*** *Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals.*

See [GRPS]

- *REQ-7.6-03: Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.*

See [GRPS]

- *REQ-7.6-04: Controls shall be implemented to avoid compromise or theft of information and information processing facilities.*

See [GRPS]

- ***REQ-7.6-05:*** *Components that are critical for the secure operation of the trust service shall be located in a physically protected security perimeter, and access control against intrusion and alarms to detect intrusion.*

See [GRPS]

OVR-7.7-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.7 shall apply.*

See below

REQ-7.7-01: *The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.*

See [GRPS]

In particular:

- ***REQ-7.7-02:*** *An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.*

See [GRPS]

- ***REQ-7.7-03:*** *Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.*

See [GRPS]

- ***REQ-7.7-04:*** *The procedures shall include documentation of the changes.*

See [GRPS]

- ***REQ-7.7-05:*** *The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.*

See [GRPS]

•REQ-7.7-06X: Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

See [GRPS]

- ***REQ-7.7-07X:*** *The TSP shall specify and apply procedures for ensuring that:*

a) security patches are applied within a reasonable time after they come available;

b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and

c) the reasons for not applying any security patches are documented.

See [GRPS]

REQ-7.7-08X: *The TSP shall establish, document, implement, monitor, and review configurations, including security configurations, of hardware, software, services and networks.*

See [GRPS]

REQ-7.7-09X: *The TSP shall monitor configurations with a comprehensive set of system management tools.*

See [GRPS]

REQ-7.7.10X: *The TSP shall review configurations on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed.*

See [GRPS]

OVR-7.8-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.8 shall apply.*

See below

REQ-7.8-01: *The TSP shall protect its network and systems from attacks.*

See [GRPS]

In particular:

- *REQ-7.8-02: The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.*

See [GRPS]

- ***REQ-7.8-03:*** *The TSP shall apply the same security controls to all systems co-located in the same zone.*

See [GRPS]

- ***REQ-7.8-04:*** *The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.*

See [GRPS]

- ***REQ-7.8-05:*** *The TSP shall explicitly forbid or deactivate not needed connections and services.*

See [GRPS]

- ***REQ-7.8-06:*** *The TSP shall review the established rule set on a regular basis.*

See [GRPS]

- ***REQ-7.8-07:*** *The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.5]).*

See [GRPS]

- ***REQ-7.8-10:*** *The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems).*

See [GRPS]

- ***REQ-7.8-11X:*** *The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.*

See [GRPS]

- *REQ-7.8-12: If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.*

See [GRPS]

- ***REQ-7.8-13:*** *The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.*

See [GRPS]

- ***REQ-7.8-14X:*** *The vulnerability scan requested by REQ-7.8-13 should be performed once per quarter.*

See [GRPS]

- ***REQ-7.8-15X:*** *The TSP shall protect its network and information systems against malicious and unauthorised software by means of malware detection and removal software, which is updated at least on a daily basis.*

See [GRPS]

- ***REQ-7.8-16X:*** *The TSP shall regularly update its malware detection and repair software*

See [GRPS]

- ***REQ-7.8-17X:*** *The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.*

See [GRPS]

- ***REQ-7.8-18X:*** *The penetration test requested by REQ-7.8-17X should be performed at least once per year.*

See [GRPS]

- ***REQ-7.8-19X:*** *The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.*

See [GRPS]

- ***REQ-7.8-20X:*** *Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.*

See [GRPS]

- ***REQ-7.8-21X:*** *Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.*

See [GRPS]

OVR-7.8-02: *The information system making the identity proofing decision shall be logically or physically separated from non-critical information systems at the IPSP.*

The information system making the identity proofing decision is a dedicated system, MitID Erhverv.

OVR-7.9-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.9 shall apply.*

See below

REQ-7.9.1-01X: *The TSP shall establish mechanisms to detect potential security incidents and to respond accordingly by implementing tools and processes to enable continuous monitoring and logging of activities on the entity's network and information systems.*

See [GRPS]

In particular:

- ***REQ-7.9.1-02X:*** *Monitoring activities should take account of the sensitivity of any information collected or analysed.*

See [GRPS]

- ***REQ-7.9.1-03X:*** *Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.*

See [GRPS]

- ***REQ-7.9.1-04X:*** *The TSP shall maintain, document and regularly review logs which shall include:*

  a) outbound and inbound network traffic;

  b) activities regarding user administration and permission management, access (including privileged access) to systems and applications;

  c) activities performed with administrator accounts;

  d) assess or changes to critical configuration files and backups;

  e) security relevant logs;

  f) use and performance of system resources;

  g) physical access to facilities, where appropriate;

  h) access and use of network equipment and devices; and

  i) environmental events, where appropriate.

See [GRPS]

- ***REQ-7.9.1-05X:*** *The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.*

See [GRPS]

- ***REQ-7.9.2-02X:*** *The TSP shall comply with reporting obligations as mandated by relevant legislative frameworks for network and information security incidents, including supervisory authorities and CSIRTs.*

See [GRPS]

- ***REQ-7.9.2-03X:*** *TSPs shall inform stakeholders about incidents according to agreed communication plans.*

See [GRPS]

- ***REQ-7.9.2-04X:*** *The TSP shall establish and maintain effective communication plans that include incident categorisation, well-defined escalation procedures, and standardised reporting protocols*

See [GRPS]

- ***REQ-7.9.2-05X:*** *The TSP shall ensure that personnel possess the necessary competencies to proficiently detect and respond to security incidents.*

See [GRPS]

- ***REQ-7.9.2-06X:*** *The TSP shall create and maintain comprehensive documentation throughout the incident detection and response process.*

See [GRPS]

- ***REQ-7.9.2-07X:*** *The TSP shall establish clear interfaces between the incident handling and business continuity management functions to ensure a coordinated and cohesive response during incidents.*

See [GRPS]

- ***REQ-7.9.2-08X:*** *The TSP shall test and review regularly and after incidents roles, responsibilities and appropriate procedures.*

See [GRPS]

- ***REQ-7.9.2-09X:*** *The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.*

See [GRPS]

- ***REQ-7.9.2-10X:*** *For any vulnerability, given the potential impact, the TSP shall [CHOICE]:*

- *create and implement a plan to mitigate the vulnerability; or*

- *document the factual basis for the TSP's determination that the vulnerability does not require remediation.*

See [GRPS]

- ***REQ-7.9.2-11X:*** *Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.*

See [GRPS]

- ***REQ-7.9.2-12X:*** *The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.*

See [GRPS]

- ***REQ-7.9.3-01X:*** *The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.*

See [GRPS]

- ***REQ-7.9.3-02X:*** *Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.*

See [GRPS]

- ***REQ-7.9.3-03X:*** *The TSP shall establish a simple procedure allowing its staff, contractors and customers to report possible network and information security incidents.*

See [GRPS]

- ***REQ-7.9.3-04X:*** *The TSP shall communicate the reporting procedure to its contractors and customers and shall train its staff to follow the reporting procedure and to address the appropriate point of contact.*

See [GRPS]

- ***REQ-7.9.4-01X:*** *The TSP shall analyse the reported events and assess their severity.*

See [GRPS]

- ***REQ-7.9.4-02X:*** *The TSP shall be capable to reassess and reclassify events based on new inputs.*

See [GRPS]

- ***REQ-7.9.5-01X:*** *The TSP shall keep itself informed about technical vulnerabilities of all information systems it uses.*

See [GRPS]

- ***REQ-7.9.5-02X:*** *The TSP shall evaluate the TSP's exposure to such vulnerabilities and take appropriate measures.*

See [GRPS]

- ***REQ-7.9.5-03X:*** *The TSP shall identify the root cause of an incident and shall conduct a post-incident review possibly resulting in measures mitigating the risk of the recurrence of similar incidents.*

See [GRPS]

- ***REQ-7.9.5-04X:*** *The TSP shall ensure that each past incident led to a post-incident review.*

See [GRPS]

OVR-7.9-02: *Reporting obligations according to ETSI EN 319 401 [1]* **REQ-7.9.2-02X** *and clause 7.9.3 shall be fulfilled as required by the identity proofing context and the obligations of the TSPs relying on the IPSP's service.*

The IPSP has procedures in place for reporting incidents to relevant parties, including supervisory bodies and relying TSPs.

OVR-7.10-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.10 shall apply.*

See below

REQ-7.10-01: *The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.*

See [GRPS]

In particular:

- ***REQ-7.10-02:*** *The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.*

See [GRPS]

- ***REQ-7.10-03:*** *Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.*

See [GRPS]

- ***REQ-7.10-04:*** *Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.*

See [GRPS]

- ***REQ-7.10-05:*** *The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.*

See [GRPS]

- ***REQ-7.10-06:*** *The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.*

See [GRPS]

- ***REQ-7.10-07:*** *Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.2).*

See [GRPS]

- ***REQ-7.10-08:*** *The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.*

See [GRPS]

OVR-7.11-01*: The requirements specified in ETSI EN 319 401 [1], clause 7.11 shall apply.*

See below

REQ-7.11.1-01*: The TSP shall define and maintain a continuity plan to enact in case of a disaster.*

See [GRPS]

REQ-7.11-1-02X: *In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.*

See [GRPS]

REQ-7.11.2-01X: *The TSP shall maintain backup copies of information and sufficient resources, including facilities, network and information systems as well as personnel in accordance with risk assessment and business continuity plan.*

See [GRPS]

REQ-7.11.2-02X: *The TSP shall define backup plans taking into account at least the following:*

a) recovery times;

b) assurance of the backup copies' completeness and accuracy (including configuration data and information stored in cloud service environment);

c) storage of backup copies at a safe location or locations, which are outside the network of the system backed up and are at sufficient distance to escape any damage from a disaster at the main site;

d) physical/environmental and logical controls for backup copies in accordance with their information classification level; and

e) processes for restoring information from backup copies (including approval processes).

See [GRPS]

REQ-7.11.2-03X: The TSP shall perform integrity check on the backup copies.

See [GRPS]

REQ-7.11.2-04X: *The TSP shall test at planed intervals the recovery of backup copies and redundancies and shall take corrective actions in case of findings. The results of these tests shall be documented.*

See [GRPS]

REQ-7.11.3.-01X: *The TSP shall establish processes for crisis management addressing at least:*

a) roles and responsibilities in crisis situations;

b) mandatory and voluntary communications between the TSP and relevant competent authorities, and

c) appropriate controls for maintaining network and information security in crisis situations.

See [GRPS]

REQ-7.11.3-02X: *The TSP shall implement a process for managing and making use of information received from National CSIRT or, where applicable, competent authorities useful for crisis management.*

See [GRPS]

REQ-7.11.3-03X: *The TSP shall test and review, at planned intervals or in the post-incident review process, its crisis management plan.*

See [GRPS]

OVR-7.11-02: *Processes for crisis management according to ETSI EN 319 401 [1],* ***REQ-7.11.3-01X*** *shall be as required by the identity proofing context and the obligations of the TSPs relying on the IPSP's service.*

Crisis management is implemented as part of the business continuity plan.

OVR-7.12-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.12, excluding* ***REQ-7.12-11****, shall apply.*

See below

REQ-7.12-01: *Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.*

See [GRPS]

In particular:

- ***REQ-7.12-02:*** *The TSP shall have an up-to-date termination plan.*

See [GRPS]

Before the TSP terminates its services at least the following procedures apply:

- ***REQ-7.12-03:*** *Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.*

See [GRPS]

- ***REQ-7.12-04:*** *Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.*

See [GRPS]

- ***REQ-7.12-05:*** *Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.*

See [GRPS]

- ***REQ-7.12-06:*** *Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information.*

See [GRPS]

- ***REQ-7.12-07:*** *Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.*

See [GRPS]

- ***REQ-7.12-08:*** *Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.*

See [GRPS]

- ***REQ-7.12-09:*** *The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.*

See [GRPS]

- ***REQ-7.12-10:*** *The TSP shall state in its practices the provisions made for termination of service. This shall include:*

a) notification of affected entities; and

b) where applicable, transferring the TSP's obligations to other parties.

See [GRPS]

OVR-7.13-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.13 shall apply.*

See below

REQ-7.13-01: *The TSP shall ensure that it operates in a legal and trustworthy manner.*

See [GRPS]

In particular:

- ***REQ-7.13-02:*** *The TSP shall provide evidence on how it meets the applicable legal requirements.*

See [GRPS]

- ***REQ-7.13-03:*** *Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.*

See [GRPS]

- ***REQ-7.13-04:*** *Applicable standards on accessibility such as ETSI EN 301 549 [**Fejl! Henvisningskilde ikke fundet.**] should be taken into account.*

See [GRPS]

- ***REQ-7.13-05:*** *Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

See [GRPS]

OVR-7.14-01: *The requirements specified in ETSI EN 319 401 [1], clause 7.14 shall apply.*

REQ-7.14.1-01X: *The TSP shall identify and implement processes and procedures to address security risks associated with the use of products and services provided by suppliers, including the ICT supply chain.*

See [GRPS]

REQ-7.14.1-02X: *The TSP shall define, document and implement processes and procedures to manage the information security risks associated with the use of supplier's products or services.*

See [GRPS]

In particular,

- ***REQ-7.14.1-03X:*** *The supply chain policy shall identify and communicate the TSP's role in the supply chain.*

See [GRPS]

- ***REQ-7.14.1-04X:*** *The supply chain policy shall define criteria for selecting and contracting suppliers or service providers. Criteria shall include:*

  a) the ability of the supplier or service provider to meet the cybersecurity specifications, risks and classification levels of the TSP's services, systems or products delivered by the supplier or service provider;

  b) the ability of the TSP to diversify sources of supply and to limit vendor lock-in; and

  c) the results of the coordinated security risk assessments of critical supply chains.

See [GRPS]

REQ-7.14.2-01X: *Processes and procedures shall be defined and implemented to manage information security risks associated with the information and communication technologies products and services supply chain.*

See [GRPS]

In particular:

- ***REQ-7.14.2-02X:*** *TSP shall define information security requirements to apply to ICT product or service acquisition.*

See [GRPS]

- ***REQ-7.14.2-03X:*** *TSP shall require that ICT services suppliers propagate the TSP's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the TSP.*

See [GRPS]

- REQ-7.14.2-04X: TSP shall require that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities.

See [GRPS]

- ***REQ-7.14.2-05X:*** *TSP shall request that ICT products suppliers provide information describing the software components used in products.*

See [GRPS]

- ***REQ-7.14.2-06X:*** *TSP shall request that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation.*

See [GRPS]

- ***REQ-7.14.2-07X:*** *TSP shall implement a monitoring process and acceptable methods for validating ICT products and services conform to stated cybersecurity requirements.*

See [GRPS]

- ***REQ-7.14.2-08X:*** *TSP shall implement a process for identifying and documenting product or service components that are critical for maintaining functionality.*

See [GRPS]

- ***REQ-7.14.2-09X: TSP*** *shall obtain assurance that critical components and their origin can be traced throughout the supply chain.*

See [GRPS]

- ***REQ-7.14.2-10X:*** *TSP shall obtain assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features.*

See [GRPS]

- ***REQ-7.14.2-11X:*** *TSP shall implement processes to ensure that components from suppliers are genuine and unaltered from their specification.*

See [GRPS]

- ***REQ-7.14.2-12X:*** *TSP shall define rules for sharing of information regarding the supply chain and any potential issues and compromises among the TSP and its suppliers.*

See [GRPS]

- REQ-7.14.2-13X: TSP shall implement specific processes for managing ICT component life cycle and availability and associated security risks.

See [GRPS]

REQ-7.14.2-14X: TSP shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

See [GRPS]

REQ-7.14.2-15X: *The TSP shall define, implement and communicate to all relevant interested parties topic-specific policies on the use of cloud services and on how the TSP intends to manage information security risks associated with them.*

See [GRPS]

REQ-7.14.3-01X [CONDITIONAL]: *When the TSP makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it shall maintain overall responsibility for conformance with the supply chain policy, its information security policy and the requirements defined in the trust service policy.*

See [GRPS]

REQ-7.14.3-02X: *The TSP shall define the outsourcers' liability and ensure that outsourcers are bound to implement any controls required by the TSP.*

See [GRPS]

In particular:

- ***REQ-7.14.3-03X:*** *These processes and procedures shall include:*

    a) those to be implemented by the TSP;

    b) those the TSP requires the supplier to implement for the commencement of use of a supplier's products or services; and

    c) those the TSP requires the supplier to implement for the termination of use of a supplier's products and services.

See [GRPS]

REQ-7.14.3-04X: *The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements to ensure that there is clear understanding between the TSP and the supplier regarding both parties' obligations to fulfil relevant information security requirements.*

See [GRPS]

REQ-7.14.3-05X [CONDITIONAL]: *When the TSP makes use of a trust service component provided by another party it shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.*

See [GRPS]

REQ-7.14.3-06 [CONDITIONAL]: *When the TSP makes use of a trust service component provided by another party it shall ensure that the security and functionality required by the trust service component meet the appropriate requirements of the applicable policy and practices.*

See [GRPS]

REQ-7.14.3-07X: *The TSP shall include in their services agreements "Service level agreements" and/or auditing mechanisms ensuring that direct suppliers and service providers, including cloud computing providers, take appropriate security measures addressing the TSP's security requirements aligned with the TSP's risk assessment.*

See [GRPS]

In particular:

- ***REQ-7.14.3-08X:*** *Compliance with TSPs security policies and requirements shall be considered in the selection process of any direct supplier or service provider as part of the procurement process.*

See [GRPS]

- ***REQ-7.14.3-09X:*** *Applicable TSPs security policies and requirements and shall be included in contracts with direct suppliers or service providers.*

See [GRPS]

REQ-7.14.3-10X: *The TSP shall review the supply chain policy and monitor, review, evaluate and manage changes in the cybersecurity practices of direct suppliers or service providers at planned intervals or after an incident related to the provision of services from direct suppliers or service providers.*

See [GRPS]

REQ-7.14.3-11X: *The TSP shall establish and maintain a register of suppliers and their agreements to track where the TSP information is managed and/or archived.*

See [GRPS]

REQ-7.14.3-12X: *The TSP shall regularly review, validate and update its registry of suppliers and their agreements to ensure that they are still valid, fit for purpose, and include the relevant information security clauses.*

See [GRPS]

4.4. Attribute and evidence validation

ISS-8.5.2-01: *Evidence of the identity proofing process shall be gathered and retained in compliance with the identity proofing context.*

Evidence is archived for 7 years.

ISS-8.5.2-02X: *The evidence of the identity proofing process shall document the authoritative and supplementary evidence used in the identity proofing process and the issuer or source of that evidence.*

MitID Erhverv ensures that the identity proofing process documents the authoritative and the supplementary evidence, as well as the issuer or source of that evidence.

ISS-8.5.2-03: *The evidence of the identity proofing process should completely document the identity proofing process.*

The evidence is logged and/or archived.

Note that evidence related to the enrollment of legal persons in MitID Erhverv is deleted after 6 month in order to be compliant with GDPR.

ISS-8.5.2-04: *Evidence of the identity proofing process shall be retained for the necessary retention time given by the identity proofing context.*

Evidence is archived for 7 years.

ISS-8.5.2-05: *The evidence of the identity proofing process shall be stored in a tamper-proof way.*

The evidence of the identity proofing process is stored in a tamper-proof way.

ISS-8.5.2-05A: The time of completion of the identity proofing process shall be part of the evidence.

The time of the completion of the identity proofing process is logged.

ISS-8.5.2-06: *The evidence of the identity proofing process shall be stored in a way that guarantees the confidentiality of the information.*

The evidence is stored in a system with permissions based on need-to-know- and least-privilege-principles.

ISS-8.5.2-07: *The evidence of the identity proofing process shall be stored in a way that ensures the possibility to search, retrieve, and re-verify the identity proofing result.*

The Application Logging Framework (ALF) ensures that the identity proofing process is retrievable, searchable, and re-verifiable.

ISS-8.5.2-08*: At the end of the retention time defined by* ***ISS 8.5.2-04****, the evidence of the identity proofing process and all personal data on the applicant shall be deleted.*

Evidence including personal data is deleted at the end of the retention time.

4.5. Use cases for identity proofing

USE-9.1-01X: *To be compliant with the present document, an identity proofing process shall conform to at least one of the use cases in clause 9 or Annex C of the present document for Baseline LoIP or Extended LoIP.*

See section 4.2 in the present document.

USE-9.1-01A: *Compliance with the claimed use cases and the claimed LoIP from the present document should be assessed by an independent, accredited conformity assessment body.*

The use cases and the claimed LoIP is assessed by an accredited conformity assessment body on a regular scheduled basis.

USE-9.1-02X: *The requirements in the following clauses of the present document shall apply to all use cases:*

- *clause 5 (operational risk assessment);*

See section 4.1

- *clause 6 (policies and practices);*

See section 4.2

- *clause 7 (identity proofing service management and operation);*

See section 4.3

- *clause 8.1 (initiation);*

See section 5.1.1, section 5.2.1, section 6.1.1 and section 6.2.1

- *clause 8.2.1 (attribute and evidence collection general requirements);*

See section 5.1.2, section 5.2.2, section 6.1.2 and section 6.2.2

- *clause 8.3.1 (attribute and evidence validation general requirements);*

See section 5.1.3, section 5.2.3, section 6.1.3 and section 6.2.3

- *clause 8.4.1 (binding to applicant general requirements); and*

See section 5.1.4, section 5.2.4, section 6.1.4 and section 6.2.4

- *clause 8.5 (issuing of proof).*

For clause 8.5.1 see section 5.1.5, section 5.2.5, section 6.1.5 and section 6.2.5.

For clause 8.5.2 see below.

***USE-9.1-03X:** Other use cases than those in the present clause 9 may be specified by combining elements from clause 8 of the present document in different ways; for such use cases, the resulting use case's proper handling of the risks identified as relevant to the Baseline or Extended LoIP shall be demonstrated.*

The proofing context described in section 6.2 Local IdP is based on a transitive use case where an ETSI TS 119 461 CAR is used as basis for registering entities in MitID Erhverv.

5. Registration of Legal Persons

In MitID Erhverv the registration process of legal persons has two registration processes both initiated by the applicant using the same registration entry point. The first registration process is denoted fast-track and is fully automated whereas the second registration process denoted slow-track involves manual validation of provided evidence.

The registration corresponds to [ETSI TS 119 461] 9.3 Use case for identity proofing of legal persons. Since the CVR number is collected for the legal person as part of the identity proofing process, this means that this identity proofing can be used for issuing qualified certificates according to the requirements in [ETSI TS 119 461] Annex C section C.2.5.

To be identified the applicant must be an organisation registered in CVR.

Target level for Legal Persons is always LoIP Extended.

5.1. Identity proofing for Legal Persons using fast-track registration

In the fast-track registration of a legal person, information on natural persons with authority to represent the legal person can be retrieved from CVR and the natural person applying for the legal person is identified via MitID to be one if the persons with authority to represent the legal person. In this case the registration can be done without manual verification of evidence by IPSP staff.

USE-9.3-02X: *The identity proofing shall use documents and attestations as authoritative evidence witnessing the purpose of the identity proofing according to the requirements in clauses 8.2.8 and 8.3.8 of the present document.*

In fast-track registration no additional documents are required.

[CONDITIONAL] USE-9.3-03X: *If the legal person is registered in a trusted register, the requirements in clauses 8.2.6 and 8.3.6 of the present document shall apply.*

See section 5.1.2 and section 5.1.3 regarding attribute and evidence collection and validation.

[CONDITIONAL] USE-9.3-03A: *If the legal person is not registered in any trusted register, the attributes that would otherwise be collected and validated from a trusted register shall be collected and validated by other means providing the same confidence as a trusted register would do.*

N/A

USE-9.3-04X: *The identity proofing may use authentication by eID means as evidence according to the requirements in clauses 8.2.4 and 8.3.4 of the present document; requirement VAL-8.2.4-02X or VAL-8.2.4-02A apply dependent on whether the desired LoIP is Baseline or Extended.*

N/A

USE-9.3-05X: *The identity proofing may use a digital signature with a certificate as evidence according to the requirements in clauses 8.2.5 and 8.3.5 of the present document; requirement VAL-8.2.5-03X or VAL-8.2.5-03A apply dependent on whether the desired LoIP is Baseline of Extended.*

N/A

USE-9.3-06: *The identity proofing may, in addition to documents and attestations and trusted register as covered by requirements USE-9.3-02X and USE-9.3-03X, use additional trusted registers and/or proof of access and/or additional documents and attestations as supplementary evidence.*

N/A

5.1.1. Initiation

***INI-8.1-01X:** The applicant shall be informed of, and shall actively accept before the identity proofing process is started, the purpose of the identity proofing and the related terms and conditions as required by the identity proofing context.*

The application process for a registration in MitID Erhverv explicitly informs and requires that the applicant confirms that an identity proofing process is started, and the applicant is presented with terms and conditions for using MitID Erhverv.

***INI-8.1-02X:** If alternative identity proofing processes are available to achieve the purpose of the identity proofing, the applicant should be allowed to select which of the alternative processes to use.*

Applicants who fulfil the requirements for the fast-track application should not be offered the slow track alternative since this is a more cumbersome way to register.

***INI-8.1-03X:** The applicant shall receive clear guidance regarding how the identity proofing process will be carried out, regarding the identity information that will be collected, regarding what data is kept and for how long, regarding the evidence that the applicant is required to present, and regarding any tool that the applicant is required to use.*

As part of the application process the applicant is presented with the requirements to apply.

The terms and conditions include MitID Erhverv retention rules.

***INI-8.1-04:** The identity proofing process, or at least one process if alternative processes are available, shall be available to persons with disabilities in accordance with the applicable legislation.*

MitID Erhverv and thereby the proofing processes are compliant with the Danish law ”Lov om tilgængelighed af offentlige organers websteder og mobilapplikationer”, which requires availability to persons with disabilities.

5.1.2. Attribute and evidence collection

***COL-8.2.1-01X:** Mandatory and optional identity attributes to collect shall be defined for each identity proofing context.*

The CVR number to which the applicant is associated is a mandatory attribute collected during the process.

***COL-8.2.1-01A:** All mandatory attributes for a specific identity proofing context shall be collected.*

The natural person applying on behalf of the applicant provides the CVR number.

***COL-8.2.1-02:** The identity attributes collected shall provide unique identification of the applicant for the identity proofing context.*

CVR is a unique identification of the applicant.

COL-8.2.1-03X: *The identity attributes collected shall be validated by use of one or more authoritative evidence and optionally one or more supplementary evidence.*

The CVR number is validated in CVR.

COL-8.2.1-04: *The evidence collected shall meet the requirements of the identity proofing context.*

In fast-track registration the natural person applying on behalf of the applicant must authenticate using MitID and the CPR number of the person must be registered in CVR to be a person authorized to represent the applicant.

COL-8.2.1-05: *The evidence shall be issued by entities trusted in the identity proofing context.*

See answer to COL-8.2.1-04 above.

COL-8.2.1-06X: *The identity proofing practice statement shall identify a list of the identity proofing use cases supported, the authoritative and optionally supplementary evidence that shall be trusted, and, as far as possible, the identity proofing contexts supported.*

The present document constitutes the identity proofing practice statement for MitID Erhverv.

COL-8.2.1-07: *The freshness of the identity attributes obtained from evidence shall be evaluated against the freshness requirements of the identity proofing context.*

The identity attributes are collected from MitID, CPR and CVR number which are all synchronized at least on a daily basis.

USE-9.3-01: *The identity proofing shall collect attributes according to the requirements in clause 8.2.2.2 of the present document.*

> ***COL-8.2.2.2-01X:*** *For each identity proofing context supported, the means used to collect identity attributes for a legal person shall be identified by the identity proofing practice statement.*
>
> Fast track registration is one of two identity proofing contexts supported. The other context (slow-track registration) is described in section 5.2.
>
> ***COL-8.2.2.2-02:*** *The attributes collected shall uniquely identify the applicant as a legal person in the identity proofing context.*
>
> The CVR collected as an attribute uniquely identifies the applicant as a legal person.
>
> ***COL-8.2.2.2-03:*** *The following attributes shall, as a minimum, be collected if the applicant is a legal person:*
>
> *a) full name of the legal person;*
>
> *b) country of registration of the legal person;*
>
> *c) unique identifier and type of identifier for the legal person (unless such identifier does not exist).*

The full name and the CVR number of the legal person are collected from CVR. Country of registration of the legal person is always Denmark.

COL-8.2.6-01X: *For each identity proofing context supported, a list of the trusted registers used to collect and/or validate attributes, and whether lookup in these registers is mandatory or optional, shall be identified by the identity proofing practice statement.*

It is mandatory to use CVR as a trusted register to collect and validate attributes for legal persons.

COL-8.2.6-01A: *Attributes collected from a trusted register shall be reliably linked to the applicant.*

Attributes collected from CVR are reliably linked to the applicant.

COL-8.2.6-02: *Only official national or nationally approved registers should be accepted as trusted registers.*

CVR is a nationally approved register.

[CONDITIONAL] COL-8.2.6-03X: *If the applicant is a legal person and is registered in an available trusted register accepted as authoritative source, this register shall be used for collection and/or validation of the attributes of the legal person.*

It is mandatory to use CVR as a trusted register to collect and validate attributes for legal persons.

5.1.3. Attribute and evidence validation

VAL-8.3.1-01X: *All necessary identity attributes shall be validated to the required reliability by an authoritative source.*

The CVR number is validated using CVR.

VAL-8.3.1-02: *Evidence of the identity proofing process shall be collected and secured supporting requirements in clause 8.5.2 of the present document.*

The evidence is secured according to clause 8.5.2 [ETSI TS 119 461]. See section **Fejl! Henvisningskilde ikke fundet.**.

VAL-8.3.1-03X: *The handling of differences in encoding of identity attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

Encoding of identity attributes are based on UTF-8.

VAL-8.3.1-04X: *The handling of differences in name attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

N/A. CVR number is unique. The name of the applicant is always derived from the authoritative source CVR.

VAL-8.3.1-05: *The identity proofing process shall verify that the evidence is of a type accepted according to the identity proofing context.*

Only MitID is accepted as evidence of the natural person applying on behalf of the applicant.

***VAL-8.3.1-06X:** The identity proofing process shall verify that the issuer of evidence is trusted according to the identity proofing context.*

MitID is considered trusted in this identity proofing context.

***[CONDITIONAL] VAL-8.3.1-07:** If the evidence has an explicit validity period, the identity proofing process shall verify that the time of the identity proofing is within this validity period.*

N/A

***VAL-8.3.1-08X:** The identity proofing process shall verify the authenticity and integrity of the evidence, i.e. that the evidence is genuine and presented in its original form.*

MitID is validated as an integrated part of the authentication process.

***VAL-8.3.1-10X:** The IPSP shall for all accepted evidence document the security features that are to be verified.*

MitID is validated as an integrated part of the authentication process.

***VAL-8.3.1-11X:** The identity proofing process shall whenever practically possible verify that the evidence is valid at the time of the identity proofing.*

MitID status is checked as an integrated part of the authentication process.

***VAL-8.3.1-12:** Validation of evidence shall be done in an environment controlled by the actor responsible for the identity proofing process.*

Validation is done in an environment controlled by IPSP.

***VAL-8.3.6-00:** Successful authentication of a trusted register and validation of authenticity and integrity of the communication with the trusted register shall imply that the statement of the trusted register on validity of identity attributes is trusted.*

All communication with CVR is done using secured connections to ensure the authenticity and integrity of the identity attributes implying that the values of the attributes are trusted.

***[CONDITIONAL] VAL-8.3.6-01:** If the communication towards the trusted register is online, the communication channel shall be secured by using an up to date version of the TLS protocol or another protocol offering a comparable level of security.*

Communication towards CVR is online and the channel is secured using an up-to-date version of the TLS protocol or another protocol offering a comparable level of security.

***[CONDITIONAL] VAL-8.3.6-02:** If the communication towards the trusted register is online, the trusted register shall be authenticated.*

CVR is authenticated using the built-in security mechanisms of the communication protocol.

***[CONDITIONAL] VAL-8.3.6-03:** If the communication towards the trusted register is message-based, all messages shall be authenticated and integrity protected*

The data in the communication towards CVR is authenticated and the integrity is secured using the built-in security mechanisms of the communication protocol.

***[CONDITIONAL] VAL-8.3.6-04:** If the communication towards the trusted register is message-based, all messages containing personal identity information shall be encrypted.*

The data in the communication towards CVR is encrypted using the built-in security mechanisms of the communication protocol.

***VAL-8.3.6-05X:** The integrity and authenticity of identity attributes obtained from the trusted register shall be validated.*

The data in the communication towards CVR is authenticated and the integrity is secured using the built-in security mechanisms of the communication protocol.

***VAL-8.3.6-06X:** The procedure to apply in case of discrepancies between the identity attributes obtained from trusted registers and information from other evidence shall be specified in the practice statement.*

N/A

5.1.4. Binding to applicant

In the fast-track registration, natural persons with the authority to represent the legal person e.g. CEO, Chairman of the board is retrieved from CVR. The applicant's representative needs to authenticate using his or her MitID (with registration on LoIP Extended) as part of the registration process for the fast track.

***BIN-8.4.1-01X:** The identity proofing process shall verify that the applicant is the legitimate holder of the authoritative evidence.*

In the fast-track registration, natural persons with the authority to represent the legal person e.g. CEO, Chairman of the board is retrieved from CVR. The applicant's representative needs to authenticate using his or her MitID (with registration on LoIP Extended) as part of the registration process for the fast track.

***BIN-8.4.1-02X:** The identity proofing process shall verify that the authoritative evidence is in the possession of the applicant.*

See answer to BIN-8.4.1-01X above.

5.1.5. Issuing of proof

Upon successful registration, the applicant appoints an organisational administrator and an identity administrator with access to MitID Erhverv using MitID as access mechanism. This appointed administrator can apply for certificates for the legal person via MitID Erhverv after a MitID authentication. The identity administrator can also appoint other natural persons associated with the legal person to authenticate on behalf of the legal person using MitID.

ISS-8.5.1-01: *The result of the identity proofing shall be delivered securely to the trust service provider, regarding the authenticity, integrity, and confidentiality of the result.*

MitID is associated with the MitID Erhverv identity and subsequently used by the applicant when identifying to the TSP via a MitID Erhverv identity broker.

ISS-8.5.1-02: *The result of the identity proofing process shall convey the LoIP achieved by the identity proofing process for the identity attributes required for the unique identification of the applicant in the identity proofing context.*

Since MitID Erhverv in this use case only manages applicants on LoIP Extended as IPSP, this is implicit.

[CONDITIONAL] ISS-8.5.1-03X: *If the identity proofing process conveys identity attributes that are not required for unique identification in the identity proofing context, and whose assurance differ from the LoIP of the overall result of the identity proofing process, an indication of the differing assurance should be conveyed in the identity proofing result.*

N/A

5.2. Identity Proofing for Legal Persons using slow-track registration

In the slow-track registration of a legal person the natural person applying on behalf of the legal person and identified with MitID cannot automatically be verified as a person authorized to represent the legal person. This can be because CVR does not contain information on who is authorized to represent the legal person or because the applying natural person is not on the list of natural persons registered to be authorized to represent the legal person. In this case the registration requires a manual verification if evidence by IPSP staff.

5.2.1. Initiation

INI-8.1-01X: *The applicant shall be informed of, and shall actively accept before the identity proofing process is started, the purpose of the identity proofing and the related terms and conditions as required by the identity proofing context.*

The application process for a registration in MitID Erhverv explicitly informs and requires that the applicant confirms that an identity proofing process is started, and the applicant is presented with terms and conditions for using MitID Erhverv.

INI-8.1-02X: *If alternative identity proofing processes are available to achieve the purpose of the identity proofing, the applicant should be allowed to select which of the alternative processes to use.*

Applicants who do not fulfil the requirements for the fast-track application shall use the slow track alternative.

***INI-8.1-03X:** The applicant shall receive clear guidance regarding how the identity proofing process will be carried out, regarding the identity information that will be collected, regarding what data is kept and for how long, regarding the evidence that the applicant is required to present, and regarding any tool that the applicant is required to use.*

As part of the application process the applicant is presented with the requirements to apply. This includes the required documentation listed for each type of organization at [DocumentationReqEIA].

The terms and conditions include MitID Erhverv retention rules.

***INI-8.1-04:** The identity proofing process, or at least one process if alternative processes are available, shall be available to persons with disabilities in accordance with the applicable legislation.*

MitID Erhverv and thereby the proofing processes are compliant with the Danish law ”Lov om tilgængelighed af offentlige organers websteder og mobilapplikationer”, which ensures availability to persons with disabilities.

5.2.2. Attribute and evidence collection

***COL-8.2.1-01X:** Mandatory and optional identity attributes to collect shall be defined for each identity proofing context.*

The CVR number to which the applicant is associated is a mandatory attribute collected during the process.

***COL-8.2.1-01A:** All mandatory attributes for a specific identity proofing context shall be collected.*

The natural person applying on behalf of the applicant provides the CVR number.

***COL-8.2.1-02:** The identity attributes collected shall provide unique identification of the applicant for the identity proofing context.*

CVR is a unique identification of the applicant.

***COL-8.2.1-03X:** The identity attributes collected shall be validated by use of one or more authoritative evidence and optionally one or more supplementary evidence.*

The CVR number is validated in CVR.

***COL-8.2.1-04:** The evidence collected shall meet the requirements of the identity proofing context.*

In slow-track registration the natural person applying on behalf of the applicant must upload a document signed by a natural person authorized to represent the applicant, additional evidence according to [DocumentationReqEIA] proving the authority and must authenticate using MitID.

***COL-8.2.1-05:** The evidence shall be issued by entities trusted in the identity proofing context.*

See answer to COL-8.2.1-04 above.

COL-8.2.1-06X: *The identity proofing practice statement shall identify a list of the identity proofing use cases supported, the authoritative and optionally supplementary evidence that shall be trusted, and, as far as possible, the identity proofing contexts supported.*

The present document constitutes the identity proofing practice statement for MitID Erhverv.

COL-8.2.1-07: *The freshness of the identity attributes obtained from evidence shall be evaluated against the freshness requirements of the identity proofing context.*

The identity attributes are collected from MitID, CPR and CVR number which are all synchronized at least on a daily basis.

USE-9.3-01: *The identity proofing shall collect attributes according to the requirements in clause 8.2.2.2 of the present document.*

> ***COL-8.2.2.2-01X:*** *For each identity proofing context supported, the means used to collect identity attributes for a legal person shall be identified by the identity proofing practice statement.*
>
> Slow-track registration is one of two identity proofing contexts supported. The other context (fast-track registration) is described in section 5.1.
>
> For the slow-track evidence of the management of the applicant must be provided. The required documentation for each type of organization is listed at [DocumentationReqEIA].
>
> ***COL-8.2.2.2-02:*** *The attributes collected shall uniquely identify the applicant as a legal person in the identity proofing context.*
>
> The CVR collected as an attribute uniquely identifies the applicant as a legal person.
>
> ***COL-8.2.2.2-03:*** *The following attributes shall, as a minimum, be collected if the applicant is a legal person:*
>
> *d) full name of the legal person;*
>
> *e) country of registration of the legal person;*
>
> *f) unique identifier and type of identifier for the legal person (unless such identifier does not exist).*
>
> The full name and the CVR number of the legal person are collected from CVR. Country of registration of the legal person is always Denmark.

COL-8.2.6-01X: *For each identity proofing context supported, a list of the trusted registers used to collect and/or validate attributes, and whether lookup in these registers is mandatory or optional, shall be identified by the identity proofing practice statement.*

It is mandatory to use CVR as a trusted register to collect and validate attributes for legal persons.

COL-8.2.6-01A: *Attributes collected from a trusted register shall be reliably linked to the applicant.*

Attributes collected from CVR are reliably linked to the applicant.

***COL-8.2.6-02:** Only official national or nationally approved registers should be accepted as trusted registers.*

CVR is a national approved register.

***[CONDITIONAL] COL-8.2.6-03X:** If the applicant is a legal person and is registered in an available trusted register accepted as authoritative source, this register shall be used for collection and/or validation of the attributes of the legal person.*

It is mandatory to use CVR as a trusted register to collect and validate attributes for legal persons.

5.2.3. Attribute and evidence validation

***VAL-8.3.1-01X:** All necessary identity attributes shall be validated to the required reliability by an authoritative source.*

The CVR number is validated using CVR.

***VAL-8.3.1-02:** Evidence of the identity proofing process shall be collected and secured supporting requirements in clause 8.5.2 of the present document.*

The evidence is secured according to clause 8.5.2 [ETSI TS 119 461]. See section **Fejl! Henvisningskilde ikke fundet.**.

***VAL-8.3.1-03X:** The handling of differences in encoding of identity attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

Encoding of identity attributes are based on UTF-8.

***VAL-8.3.1-04X:** The handling of differences in name attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

N/A. CVR number is unique. The name of the applicant is always derived from the authoritative source CVR.

Other evidence is uploaded documents which are processed manually in the verification process.

***VAL-8.3.1-05:** The identity proofing process shall verify that the evidence is of a type accepted according to the identity proofing context.*

Only MitID is accepted as evidence of the natural person applying on behalf of the applicant.

Provided evidence is manually verified to be of accepted types according to [DocumentationReqEIA].

***VAL-8.3.1-06X:** The identity proofing process shall verify that the issuer of evidence is trusted according to the identity proofing context.*

MitID is considered trusted in this identity proofing context.

Provided evidence is manually verified to be issued by a trusted source according to [DocumentationReqEIA].

***[CONDITIONAL] VAL-8.3.1-07:** If the evidence has an explicit validity period, the identity proofing process shall verify that the time of the identity proofing is within this validity period.*

If the provided evidence has an explicit validity period, it is manually verified that the identity proofing is within this validity period.

***VAL-8.3.1-08X:** The identity proofing process shall verify the authenticity and integrity of the evidence, i.e. that the evidence is genuine and presented in its original form.*

MitID is validated as integrated part of the authentication process.

The provided authenticity and integrity of the provided evidence is manually verified through visual inspection.

***VAL-8.3.1-10X:** The IPSP shall for all accepted evidence document the security features that are to be verified.*

MitID is validated as an integrated part of the authentication process.

N/A for provided documentation.

***VAL-8.3.1-11X:** The identity proofing process shall whenever practically possible verify that the evidence is valid at the time of the identity proofing.*

MitID status is checked as an integrated part of the authentication process.

It is not practically possible to verify that the provided evidence is valid at the time of the identity proofing.

***VAL-8.3.1-12:** Validation of evidence shall be done in an environment controlled by the actor responsible for the identity proofing process.*

Validation is done in an environment controlled by the IPSP.

***VAL-8.3.6-00:** Successful authentication of a trusted register and validation of authenticity and integrity of the communication with the trusted register shall imply that the statement of the trusted register on validity of identity attributes is trusted.*

All communication with CVR is done using secured connections to ensure the authenticity and integrity of the identity attributes implying that the values of the attributes are trusted.

***[CONDITIONAL] VAL-8.3.6-01:** If the communication towards the trusted register is online, the communication channel shall be secured by using an up to date version of the TLS protocol or another protocol offering a comparable level of security.*

Communication towards CVR is online and the channel is secured using an up-to-date version of the TLS protocol or another protocol offering a comparable level of security.

***[CONDITIONAL] VAL-8.3.6-02:** If the communication towards the trusted register is online, the trusted register shall be authenticated.*

CVR is authenticated using the built-in security mechanisms of the communication protocol.

***[CONDITIONAL] VAL-8.3.6-03:** If the communication towards the trusted register is message-based, all messages shall be authenticated and integrity protected*

The data in the communication towards CVR is authenticated and the integrity is secured using the built-in security mechanisms of the communication protocol.

***[CONDITIONAL] VAL-8.3.6-04:** If the communication towards the trusted register is message-based, all messages containing personal identity information shall be encrypted.*

The data in the communication towards CVR is encrypted using the built-in security mechanisms of the communication protocol.

***VAL-8.3.6-05X:** The integrity and authenticity of identity attributes obtained from the trusted register shall be validated.*

The data in the communication towards CVR is authenticated and the integrity is secured using the built-in security mechanisms of the communication protocol.

***VAL-8.3.6-06X:** The procedure to apply in case of discrepancies between the identity attributes obtained from trusted registers and information from other evidence shall be specified in the practice statement.*

N/A

5.2.4. Binding to applicant

***BIN-8.4.1-01X:** The identity proofing process shall verify that the applicant is the legitimate holder of the authoritative evidence.*

In the slow-track registration natural persons with the authority to represent the legal person e.g. CEO, Chairman of the board is retrieved from evidence provided by the applicant. This natural person must authenticate using his or her MitID (with registration on LoIP Extended) as part of the registration process for the slow-track or sign a document giving a deputy with a MitID permission to apply. In the latter case the deputy must authenticate using his or her MitID (with registration on LoIP Extended).

***BIN-8.4.1-02X:** The identity proofing process shall verify that the authoritative evidence is in the possession of the applicant.*

See answer to BIN-8.4.1-01X above.

5.2.5. Issuing of proof

Upon successful, registration the applicant appoints an organisational administrator with access to MitID Erhverv using MitID as access mechanism. This appointed administrator can apply for certificates for the legal person via MitID Erhverv after a MitID authentication and/or can appoint an identity administrator. These organisational and identity administrators can appoint other natural persons associated with the legal person to authenticate on behalf of the legal person using MitID.

***ISS-8.5.1-01:** The result of the identity proofing shall be delivered securely to the trust service provider, regarding the authenticity, integrity, and confidentiality of the result.*

MitID is associated with the MitID Erhverv identity and subsequently used by the applicant when identifying to the TSP via a MitID Erhverv identity broker.

***ISS-8.5.1-02:** The result of the identity proofing process shall convey the LoIP achieved by the identity proofing process for the identity attributes required for the unique identification of the applicant in the identity proofing context.*

Since MitID Erhverv in this use case only manages applicants on LoIP Extended as IPSP this is implicit.

***[CONDITIONAL] ISS-8.5.1-03X:** If the identity proofing process conveys identity attributes that are not required for unique identification in the identity proofing context, and whose assurance differ from the LoIP of the overall result of the identity proofing process, an indication of the differing assurance should be conveyed in the identity proofing result.*

N/A

6. Registration of Natural Persons representing LegaPerson

No natural persons can be registered as an identity in MitID Erhverv without being associated with a legal person identified in MitID Erhverv as described in section 5.

The registration corresponds to [ETSI TS 119 461] 9.4 Use case for identity proofing of natural person representing legal person. Since the CVR number is collected for the legal person as part of the identity proofing process and the natural person is identity proved on LoIP Extended, this means that this identity proofing can be used for issuing qualified certificates according to the requirements in [ETSI TS 119 461] Annex C section C.2.6.

Target level for natural persons representing legal person is always LoIP Extended if the applicant identifies using a private MitID. If the organisation is configured with Local IdP the target level depends on the compliance scheme ([NSIS] or [ETSI TS 119 461]) used for the Local IdP.

6.1. Identity proofing for Natural Persons representing Legal Person having a private MitID

In this use case the natural person is identified using a private MitID during the identity proofing process. This covers two situations: As an integrated part of the registration of the associated legal person (for the first administrator) or when a user is enrolled by an administrator of the legal person after the legal person is registered in MitID Erhverv. In both cases the natural person must authenticate using private MitID.

***[CONDITIONAL] USE-9.4-01X:** If Baseline LoIP is targeted, the identity proofing for the natural person shall be done according to at least the requirements for one of the use cases for Baseline LoIP in clause 9.2 of the present document.*

N/A

***[CONDITIONAL] USE-9.4-01A:** If Extended LoIP is targeted, the identity proofing of the natural person shall be done according to the requirements for one of the use cases for Extended LoIP in clause 9.2 of the present document.*

The identity proofing is based on a MitID belonging to the natural person on LoIP Extended compliant with [ETSI TS 119 461] clause 9.2.

***USE-9.4-03X:** Evidence validation for the legal person shall be according to the relevant clauses 8.3.2 to 8.3.8 of the present document.*

The evidence validation for the legal person is based on the identity proofing of legal persons described in section 5 compliant with [ETSI TS 119 461] clauses 8.3.2 to 8.3.8.

***[CONDITIONAL] USE-9.4-04:** If the legal person is registered in a trusted register, the requirements in clauses 8.2.6 and 8.3.6 of the present document apply.*

The legal person is registered in a trusted register CVR registration is described in section 5 compliant with [ETSI TS 119 461] clauses 8.2.6 to 8.3.6.

***[CONDITIONAL] USE-9.4-05:** If the legal person is not registered in any trusted register, or the required attributes to validate the role of the natural person concerning the legal person are not present in the register, the required attributes for the legal person, including the natural person's authorization to represent the legal person, shall be validated by other means providing the same confidence as a trusted register would do.*

The legal person is always registered in the trusted register CVR. If the required information is not present in CVR, the identity proofing will be based on the slow track registration described in section 5.2 where other means of validation providing the same confidence as a trusted register would do.

***USE-9.4-06:** The identity proofing may, in addition to trusted register as covered by requirement **USE-9.4-04**, use additional trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.*

N/A

6.1.1. Initiation

***INI-8.1-01X:** The applicant shall be informed of, and shall actively accept before the identity proofing process is started, the purpose of the identity proofing and the related terms and conditions as required by the identity proofing context.*

An appointed administrator for the legal person requests the creation of an electronic identity for a person representing the legal person. This initiates the identity proofing process with an email sent to the applicant. The email contains information, purpose and terms and conditions of the identity proofing process and a link to activate the process if accepted by the applicant.

***INI-8.1-02X:** If alternative identity proofing processes are available to achieve the purpose of the identity proofing, the applicant should be allowed to select which of the alternative processes to use.*

N/A

***INI-8.1-03X:** The applicant shall receive clear guidance regarding how the identity proofing process will be carried out, regarding the identity information that will be collected, regarding what data is kept and for how long, regarding the evidence that the applicant is required to present, and regarding any tool that the applicant is required to use.*

The applicant will receive clear guidance on the identity proofing process including what data is collected and kept and for how long, and that the user needs to use his or her MitID as identity evidence. This guidance is provided in the email described above.

***INI-8.1-04:** The identity proofing process, or at least one process if alternative processes are available, shall be available to persons with disabilities in accordance with the applicable legislation.*

MitID Erhverv and thereby the proofing processes are compliant with the Danish law ”Lov om tilgængelighed af offentlige organers websteder og mobilapplikationer”, which ensures availability to persons with disabilities.

6.1.2. Attribute and evidence collection

***COL-8.2.1-01X:** Mandatory and optional identity attributes to collect shall be defined for each identity proofing context.*

MitID UUID (unique id from MitID), name, email address and either social security number or birth date shall be collected for each identity.

The CVR number for which the applicant is associated is a mandatory attribute collected during the process.

***COL-8.2.1-01A:** All mandatory attributes for a specific identity proofing context shall be collected.*

MitID UUID, name, email address and either social security number or birth date are mandatory attributes to be collected.

For the initial natural person representing a legal person the CVR number is collected as part of the general MitID Erhverv application and subsequently the CVR number is implicitly collected, based on which legal person the applying administrator is belonging to.

***COL-8.2.1-02:** The identity attributes collected shall provide unique identification of the applicant for the identity proofing context.*

MitID UUID is a unique identification of the applicant.

COL-8.2.1-03X: *The identity attributes collected shall be validated by use of one or more authoritative evidence and optionally one or more supplementary evidence.*

MitID on LoIP Extended is used as an authoritative source to validate the identity attributes. If the social security number is collected as evidence the CPR system is used to validate the name of the applicant.

COL-8.2.1-04: *The evidence collected shall meet the requirements of the identity proofing context.*

MitID on LoIP Extended and the associated identity attributes meet the requirements of the identity proofing context.

COL-8.2.1-05: *The evidence shall be issued by entities trusted in the identity proofing context.*

MitID on LoIP Extended is trusted in this identity proofing context.

Accepted evidence of the relationship to the legal person for the applicant, when the applicant is the initial natural person representing the legal person, is issued by entities trusted in the proofing context as defined in [DocumentationReqEIA].

Evidence of the relationship to the legal person for the applicant, when the applicant is a consecutive natural person representing the legal person (after the initial MitID Erhverv application for the legal person), is implicitly trusted, based on which legal person the applying administrator is appointed by.

COL-8.2.1-06X: *The identity proofing practice statement shall identify a list of the identity proofing use cases supported, the authoritative and optionally supplementary evidence that shall be trusted, and, as far as possible, the identity proofing contexts supported.*

The present document constitutes the identity proofing practice statement for MitID Erhverv.

COL-8.2.1-07: *The freshness of the identity attributes obtained from evidence shall be evaluated against the freshness requirements of the identity proofing context.*

The identity attributes are collected from MitID, CPR number and CVR number which are all synchronized at least on a daily basis.

USE-9.4-01B: *Attribute collection shall be according to the requirements of clause 8.2.2.3 of the present document.*

See below

> ***COL-8.2.2.3-01:*** *Identity attributes for the natural person shall be collected according to the requirements in clause 8.2.2.1 of the present document.*
>
> The identity attributes for the natural person are collected as part of the identity proofing of MitID.
>
> ***COL-8.2.2.3-02:*** *Identity attributes for the legal person shall be collected according to the requirements in clause 8.2.2.2 of the present document.*
>
> The identity attributes for the legal person are collected as part of the identity proofing of the organisation cf. section 5.

***COL-8.2.2.3-03:** The role of the natural person with respect to the legal person and identification of the source of the authorization of the natural person to represent the legal person shall be collected.*

The natural person representing the legal person is only registered as "associated with" since roles and authorisations may change dynamically after the identity proofing is finalized. Authorisation is not directly in the scope of MitID Erhverv identities.

***USE-9.4-02X:** Evidence collection shall be according to the requirements in clause 8.2.9 of the present document.*

See below

***COL-8.2.9-01:** Evidence for the natural person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.*

[ETSI TS 119 461] clause 8.2.3 "Use of physical or digital identity document as evidence" does not apply in this context.

***COL-8.2.4-01X:** For each identity proofing context supported, the conditions that an eID or eID scheme is required to fulfil to be accepted for identity proofing shall be identified by the identity proofing practice statement*

MitID eID scheme is required as accepted for identity proofing.

***[CONDITIONAL] COL-8.2.4-02X:** If the Baseline LoIP is targeted, the eID shall at least conform to eIDAS LoA substantial or conform to another assurance level framework offering comparable assurance to eIDAS LoA substantial*

N/A

***[CONDITIONAL] COL-8.2.4-02A:** If the Extended LoIP is targeted, the eID shall conform to eIDAS LoA high or conform to another assurance level framework offering comparable assurance to eIDAS LoA high.*

Only MitID identities on LoIP Extended are accepted and is considered an assurance level comparable to the requirement. This shall be assessed by a CAB.

***[CONDITIONAL] COL-8.2.4-03X:** If required attributes to be collected cannot be validated by the authentication using the eID means, these attributes shall be collected from other sources and validated, including assessing that the attributes are bound to the applicant, by use of other authoritative sources in accordance with the identity proofing context.*

N/A

[ETSI TS 119 461] clause 8.2.5 "Use of existing digital signature means as evidence" does not apply in this context.

[ETSI TS 119 461] clause 8.2.6 "Use of trusted register as supplementary evidence" does not apply in this context.

[ETSI TS 119 461] clause 8.2.7 “Use of proof of access as supplementary evidence” does not apply in this context.

[ETSI TS 119 461] clause 8.2.8 “Use of documents and attestations as supplementary evidence” does not apply in this context.

COL-8.2.9-02: *Evidence for the legal person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.*

See section 5 on how evidence of the legal person’s identity is collected.

COL-8.2.9-03X: *For each identity proofing context supported, the accepted means to evidence the link between the natural person's identity and the legal person's identity shall be identified by the identity proofing practice statement.*

See practice for *COL-8.2.1-05* above.

COL-8.2.9-04X: *For each identity proofing context supported, the positions, roles, or other relationships accepted for a natural person to represent a legal person shall be identified in the identity proofing practice statement.*

Positions, roles and other relationships are not directly in the scope of a MitID Erhverv identity and is therefore not registered for the applicant.

COL-8.2.9-05X: *For each identity proofing context supported, any freshness (current) requirement applicable to any statement or document regarding the natural person's relationship to the legal person shall be identified by the identity proofing practice statement.*

See practice for *COL-8.2.1-07* above.

[CONDITIONAL] COL-8.2.9-06X: *If the legal person is listed in a trusted register, the role of the natural person concerning the legal person shall be collected from or validated against this register to the extent that the register is accessible and that the required attributes are present in the register.*

For the initial natural person representing a legal person in fast-track registration the natural person is listed in CVR with CPR number. This CPR number is collected and validated against the CPR number registered for the MitID.

For the initial natural person representing a legal person in slow-track registration the natural person is not listed in CVR and cannot be collected from or validated against this register. Alternative evidence is collected cf. section 5.

For subsequent identification of natural persons representing a legal person the CVR is not used for collection of evidence, but the relation is based on the registration by the legal person’s MitID Erhverv identity administrators’ relation.

[CONDITIONAL] COL-8.2.9-07X: *If the legal person is not listed in a trusted register, or the required attributes to collect or validate the role of the natural person concerning* *the legal person are not present in the register, the role of the natural person concerning the legal person shall be collected or validated by other means providing the same confidence as a trusted register would do.*

N/A. Only legal persons registered in CVR can be registered.

COL-8.2.9-08: *Documents and attestations from the concerned legal person may be used as evidence of a natural person's authorization to represent the legal person.*

See practice for *COL-8.2.9-06X* above.

6.1.3. Attribute and evidence validation

***VAL-8.3.1-01X:** All necessary identity attributes shall be validated to the required reliability by an authoritative source.*

The attributes related to the applicant as a natural person are validated using MitID attributes.

The CVR number is validated using CVR.

***VAL-8.3.1-02:** Evidence of the identity proofing process shall be collected and secured supporting requirements in clause 8.5.2 of the present document.*

The evidence is secured according to clause 8.5.2 [ETSI TS 119 461]. See section 4.

***VAL-8.3.1-03X:** The handling of differences in encoding of identity attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

Encoding of identity attributes are based on UTF-8.

***VAL-8.3.1-04X:** The handling of differences in name attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

N/A. The name of the applicant is always derived from the authoritative source MitID.

***VAL-8.3.1-05:** The identity proofing process shall verify that the evidence is of a type accepted according to the identity proofing context.*

Only MitID is accepted as evidence of the applicant.

***VAL-8.3.1-06X:** The identity proofing process shall verify that the issuer of evidence is trusted according to the identity proofing context.*

MitID is considered trusted in this identity proofing context.

***[CONDITIONAL] VAL-8.3.1-07:** If the evidence has an explicit validity period, the identity proofing process shall verify that the time of the identity proofing is within this validity period.*

N/A

***VAL-8.3.1-08X:** The identity proofing process shall verify the authenticity and integrity of the evidence, i.e. that the evidence is genuine and presented in its original form.*

MitID is validated as an integrated part of the authentication process.

***VAL-8.3.1-10X:** The IPSP shall for all accepted evidence document the security features that are to be verified.*

MitID is validated as an integrated part of the authentication process.

***VAL-8.3.1-11X:** The identity proofing process shall whenever practically possible verify that the evidence is valid at the time of the identity proofing.*

MitID status is checked as an integrated part of the authentication process.

VAL-8.3.1-12: *Validation of evidence shall be done in an environment controlled by the actor responsible for the identity proofing process.*

Validation is done in an environment controlled by IPSP.

USE-9.4-03X: *Evidence validation for the legal person shall be according to the relevant clauses 8.3.2 to 8.3.8 of the present document.*

Evidence validation for the legal person is based on the identity proofing of the organisation cf. section 5.1.3.

[CONDITIONAL] USE-9.4-04: *If the legal person is registered in a trusted register, the requirements in clauses 8.2.6 and 8.3.6 of the present document apply.*

The requirements in [ETSI TS 119 461] clauses 8.2.6 and 8.3.6 are applied to the identity proofing of the organisation cf. section 5.1.3.

[CONDITIONAL] USE-9.4-05: *If the legal person is not registered in any trusted register, or the required attributes to validate the role of the natural person concerning the legal person are not present in the register, the required attributes for the legal person, including the natural person's authorization to represent the legal person, shall be validated by other means providing the same confidence as a trusted register would do.*

N/A. Only legal persons registered in CVR can be registered.

USE-9.4-06: *The identity proofing may, in addition to trusted register as covered by requirement **USE-9.4-04**, use additional trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.*

N/A. Only legal persons registered in CVR can be registered.

6.1.4. Binding to applicant

BIN-8.4.1-01X: *The identity proofing process shall verify that the applicant is the legitimate holder of the authoritative evidence.*

Verification that the applicant is the legitimate holder of the authoritative evidence is done via an authentication with MitID on LoIP Extended.

BIN-8.4.1-02X: *The identity proofing process shall verify that the authoritative evidence is in the possession of the applicant.*

Verification that the applicant is in possession of the authoritative evidence is done via an authentication with MitID on LoIP Extended.

See also the answer to *COL-8.2.1-05* with regards to the binding of the natural person to the legal person.

6.1.5. Issuing of proof

***ISS-8.5.1-01:** The result of the identity proofing shall be delivered securely to the trust service provider, regarding the authenticity, integrity, and confidentiality of the result.*

MitID is associated with the MitID Erhverv identity and subsequently used by the applicant when identifying to the TSP via a MitID Erhverv identity broker.

***ISS-8.5.1-02:** The result of the identity proofing process shall convey the LoIP achieved by the identity proofing process for the identity attributes required for the unique identification of the applicant in the identity proofing context.*

Since MitID Erhverv in this use case only manages applicants on LoIP Extended as IPSP this is implicit.

***[CONDITIONAL] ISS-8.5.1-03X:** If the identity proofing process conveys identity attributes that are not required for unique identification in the identity proofing context, and whose assurance differ from the LoIP of the overall result of the identity proofing process, an indication of the differing assurance should be conveyed in the identity proofing result.*

N/A

6.2. Identity proofing for Natural Persons representing Legal Person registered via Local Identity Providers (Local IdP)

In MitID Erhverv an organization (legal person) can develop their own identity proofing framework and have the natural persons in the organization synchronized in MitID Erhverv. An organization can only use this option if the organization as a legal person is already registered in MitID Erhverv and they continuously present MitID Erhverv with either an [NSIS] conformity report where the organization processes are validated on level “Substantial” or higher (hereafter denoted “[NSIS] Substantial CAR”) or an [ETSI TS 119 461] CAR stating that natural persons in the organization are identified on LoIP Extended.

If the organization demonstrates [NSIS] substantial compliance via a [NSIS] Substantial CAR, the targeted LoIP will be Baseline. If an organization demonstrates [ETSI TS 119 461] LoIP Extended compliance via an [ETSI TS 119 461] CAR, the targeted LoIP will be Extended.

If an organization demonstrates [NSIS] compliance, but wants the applicants to be LoIP Extended (e.g. for receiving qualified certificates), they are referred to activate the applicants with the applicant’s private MitID (see section 6.1 above).

Note that the first natural person registered associated with the legal person will always be identified and authenticated using private MitID and hence this use case does not apply to this natural person.

***[CONDITIONAL] USE-9.4-01X:** If Baseline LoIP is targeted, the identity proofing for the natural person shall be done according to at least the requirements for one of the use cases for Baseline LoIP in clause 9.2 of the present document.*

This is based on the organization’s [NSIS] Substantial CAR presented to MitID Erhverv.

***[CONDITIONAL] USE-9.4-01A:** If Extended LoIP is targeted, the identity proofing of the natural person shall be done according to the requirements for one of the use cases for Extended LoIP in clause 9.2 of the present document.*

This is based on the organization's [ETSI TS 119 461] CAR presented to MitID Erhverv.

***USE-9.4-03X:** Evidence validation for the legal person shall be according to the relevant clauses 8.3.2 to 8.3.8 of the present document.*

The evidence validation for the legal person is based on the identity proofing of legal persons described in section 5 compliant with [ETSI TS 119 461] clauses 8.3.2 to 8.3.8.

***[CONDITIONAL] USE-9.4-04:** If the legal person is registered in a trusted register, the requirements in clauses 8.2.6 and 8.3.6 of the present document apply.*

The legal person is registered in a trusted register CVR registration is described in section 5 compliant with [ETSI TS 119 461] clauses 8.2.6 to 8.3.6.

***[CONDITIONAL] USE-9.4-05:** If the legal person is not registered in any trusted register, or the required attributes to validate the role of the natural person concerning the legal person are not present in the register, the required attributes for the legal person, including the natural person's authorization to represent the legal person, shall be validated by other means providing the same confidence as a trusted register would do.*

The legal person is always registered in the trusted register CVR. If the required information is not present in CVR, the identity proofing will be based on the slow track registration described in section 5.2 where other means of validation providing the same confidence as a trusted register would do.

***USE-9.4-06:** The identity proofing may, in addition to trusted register as covered by requirement **USE-9.4-04**, use additional trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.*

N/A

6.2.1. Initiation

***INI-8.1-01X:** The applicant shall be informed of, and shall actively accept before the identity proofing process is started, the purpose of the identity proofing and the related terms and conditions as required by the identity proofing context.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***INI-8.1-02X:** If alternative identity proofing processes are available to achieve the purpose of the identity proofing, the applicant should be allowed to select which of the alternative processes to use.*

N/A

***INI-8.1-03X:** The applicant shall receive clear guidance regarding how the identity proofing process will be carried out, regarding the identity information that will be collected, regarding what data is kept and for how long, regarding the evidence that the applicant is required to present, and regarding any tool that the applicant is required to use.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***INI-8.1-04:** The identity proofing process, or at least one process if alternative processes are available, shall be available to persons with disabilities in accordance with the applicable legislation.*

MitID Erhverv and thereby the proofing processes are compliant with the Danish law ”Lov om tilgængelighed af offentlige organers websteder og mobilapplikationer”, which ensures availability to persons with disabilities.

6.2.2. Attribute and evidence collection

***COL-8.2.1-01X:** Mandatory and optional identity attributes to collect shall be defined for each identity proofing context.*

The mandatory and optional identity attributes to be collected are defined in the OIOSAML profile.

The CVR number for which the applicant is associated is a mandatory attribute collected during the process.

***COL-8.2.1-01A:** All mandatory attributes for a specific identity proofing context shall be collected.*

For the initial natural person representing a legal person, the CVR number is collected as part of the general MitID Erhverv application and subsequently the CVR number is implicitly collected based on which legal person the applying administrator is belonging to.

***COL-8.2.1-02:** The identity attributes collected shall provide unique identification of the applicant for the identity proofing context.*

OIOSAML includes a mandatory unique identifier and other attributes which uniquely identifies the applicant.

***COL-8.2.1-03X:** The identity attributes collected shall be validated by use of one or more authoritative evidence and optionally one or more supplementary evidence.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***COL-8.2.1-04:** The evidence collected shall meet the requirements of the identity proofing context.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***COL-8.2.1-05:** The evidence shall be issued by entities trusted in the identity proofing context.*

Accepted evidence of the relationship to the legal person for the applicant, when the applicant is the initial natural person representing the legal person, is issued by entities trusted in the proofing context as defined in [DocumentationReqEIA].

***COL-8.2.1-06X:** The identity proofing practice statement shall identify a list of the identity proofing use cases supported, the authoritative and optionally supplementary evidence that shall be trusted, and, as far as possible, the identity proofing contexts supported.*

The present document constitutes the identity proofing practice statement for MitID Erhverv.

***COL-8.2.1-07:** The freshness of the identity attributes obtained from evidence shall be evaluated against the freshness requirements of the identity proofing context.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***USE-9.4-01B:** Attribute collection shall be according to the requirements of clause 8.2.2.3 of the present document.*

See below

> ***COL-8.2.2.3-01:** Identity attributes for the natural person shall be collected according to the requirements in clause 8.2.2.1 of the present document.*
>
> This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.
>
> ***COL-8.2.2.3-02:** Identity attributes for the legal person shall be collected according to the requirements in clause 8.2.2.2 of the present document.*
>
> The identity attributes for the legal person are collected as part of the identity proofing of the organisation cf. section 5.
>
> ***COL-8.2.2.3-03:** The role of the natural person with respect to the legal person and identification of the source of the authorization of the natural person to represent the legal person shall be collected.*
>
> The natural person representing the legal person is only registered as "associated with" since roles and authorisations may change dynamically after the identity proofing is finalized. Authorisation is not directly in the scope of MitID Erhverv identities.

***USE-9.4-02X:** Evidence collection shall be according to the requirements in clause 8.2.9 of the present document.*

See below

> ***COL-8.2.9-01:** Evidence for the natural person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.*
>
> This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***COL-8.2.9-02:** Evidence for the legal person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.*

See section 5 on how evidence of the legal person’s identity is collected.

***COL-8.2.9-03X:** For each identity proofing context supported, the accepted means to evidence the link between the natural person's identity and the legal person's identity shall be identified by the identity proofing practice statement.*

See practice for *COL-8.2.1-05* above.

***COL-8.2.9-04X:** For each identity proofing context supported, the positions, roles, or other relationships accepted for a natural person to represent a legal person shall be identified in the identity proofing practice statement.*

The natural person representing the legal person is only registered as “associated with” since roles and authorisations may change dynamically after the identity proofing is finalized. Authorisation is not directly in the scope of MitID Erhverv identities.

***COL-8.2.9-05X:** For each identity proofing context supported, any freshness (current) requirement applicable to any statement or document regarding the natural person's relationship to the legal person shall be identified by the identity proofing practice statement.*

See practice for *COL-8.2.1-07* above.

***[CONDITIONAL] COL-8.2.9-06X:** If the legal person is listed in a trusted register, the role of the natural person concerning the legal person shall be collected from or validated against this register to the extent that the register is accessible and that the required attributes are present in the register.*

For the initial natural person representing a legal person in fast-track registration the natural person is listed in CVR with CPR number. This CPR number is collected and validated against the CPR number registered for the MitID.

For the initial natural person representing a legal person in slow-track registration the natural person is not listed in CVR and cannot be collected from or validated against this register. Alternative evidence is collected cf. section 5.

For subsequent identification of natural persons representing a legal person the CVR is not used for collection of evidence, but the relation is based on the registration by the legal person’s MitID Erhverv identity administrators’ relation.

***[CONDITIONAL] COL-8.2.9-07X:** If the legal person is not listed in a trusted register, or the required attributes to collect or validate the role of the natural person concerning the legal person are not present in the register, the role of the natural person concerning the legal person shall be collected or validated by other means providing the same confidence as a trusted register would do.*

N/A. Only legal persons registered in CVR can be registered.

***COL-8.2.9-08:** Documents and attestations from the concerned legal person may be used as evidence of a natural person's authorization to represent the legal person.*

See practice for *COL-8.2.9-06X* above.

6.2.3. Attribute and evidence validation

***VAL-8.3.1-01X:** All necessary identity attributes shall be validated to the required reliability by an authoritative source.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***VAL-8.3.1-02:** Evidence of the identity proofing process shall be collected and secured supporting requirements in clause 8.5.2 of the present document.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***VAL-8.3.1-03X:** The handling of differences in encoding of identity attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***VAL-8.3.1-04X:** The handling of differences in name attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***VAL-8.3.1-05:** The identity proofing process shall verify that the evidence is of a type accepted according to the identity proofing context.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***VAL-8.3.1-06X:** The identity proofing process shall verify that the issuer of evidence is trusted according to the identity proofing context.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

***[CONDITIONAL] VAL-8.3.1-07:** If the evidence has an explicit validity period, the identity proofing process shall verify that the time of the identity proofing is within this validity period.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

VAL-8.3.1-08X: *The identity proofing process shall verify the authenticity and integrity of the evidence, i.e. that the evidence is genuine and presented in its original form.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

VAL-8.3.1-10X: *The IPSP shall for all accepted evidence document the security features that are to be verified.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

VAL-8.3.1-11X: *The identity proofing process shall whenever practically possible verify that the evidence is valid at the time of the identity proofing.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

VAL-8.3.1-12: *Validation of evidence shall be done in an environment controlled by the actor responsible for the identity proofing process.*

This is based on the organization's [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

USE-9.4-03X: *Evidence validation for the legal person shall be according to the relevant clauses 8.3.2 to 8.3.8 of the present document.*

Evidence validation for the legal person is based on the identity proofing of the organisation cf. section 5.1.3.

[CONDITIONAL] USE-9.4-04: *If the legal person is registered in a trusted register, the requirements in clauses 8.2.6 and 8.3.6 of the present document apply.*

The requirements in [ETSI TS 119 461] clauses 8.2.6 and 8.3.6 are applied to the identity proofing of the organisation cf. section 5.1.3.

[CONDITIONAL] USE-9.4-05: *If the legal person is not registered in any trusted register, or the required attributes to validate the role of the natural person concerning the legal person are not present in the register, the required attributes for the legal person, including the natural person's authorization to represent the legal person, shall be validated by other means providing the same confidence as a trusted register would do.*

N/A. Only legal persons registered in CVR can be registered.

USE-9.4-06: *The identity proofing may, in addition to trusted register as covered by requirement* ***USE-9.4-04****, use additional trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.*

N/A. Only legal persons registered in CVR can be registered.

6.2.4. Binding to applicant

BIN-8.4.1-01X: *The identity proofing process shall verify that the applicant is the legitimate holder of the authoritative evidence.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

BIN-8.4.1-02X: *The identity proofing process shall verify that the authoritative evidence is in the possession of the applicant.*

This is based on the organization’s [NSIS] Substantial CAR or [ETSI TS 119 461] CAR presented to MitID Erhverv.

6.2.5. Issuing of proof

ISS-8.5.1-01: *The result of the identity proofing shall be delivered securely to the trust service provider, regarding the authenticity, integrity, and confidentiality of the result.*

The achieved LoIP is populated securely to the trust service provider ensuring authenticity, integrity and confidentiality via a MitID Erhverv identity broker.

ISS-8.5.1-02: *The result of the identity proofing process shall convey the LoIP achieved by the identity proofing process for the identity attributes required for the unique identification of the applicant in the identity proofing context.*

The achieved LoIP and attributes required to uniquely identify the applicant is populated securely to the trust service provider via a MitID Erhverv identity broker.

[CONDITIONAL] ISS-8.5.1-03X: *If the identity proofing process conveys identity attributes that are not required for unique identification in the identity proofing context, and whose assurance differ from the LoIP of the overall result of the identity proofing process, an indication of the differing assurance should be conveyed in the identity proofing result.*

N/A