Agency for Digital
Government

Version 1.0

General Requirements Practice Statement for the Agency for Digital Government

February 2026

Table of Contents

Change Log

Version	Date	Change description
1.0	09/02/2026	Initial version

1 Introduction

1.1 Overview

The Agency for Digital Government (DIGST) has established a qualified trust service provider, Den Danske Stat, which provides qualified and non-qualified trust services that meets the requirements described in the eIDAS regulation.

Den Danske Stat provides a series of qualified trust services and acts as Certification Authority, Time-stamp Authority and management of a remote qualified signature creation device. It also provides a non-qualified Validation service, and acts as the Validation Authority for this service.

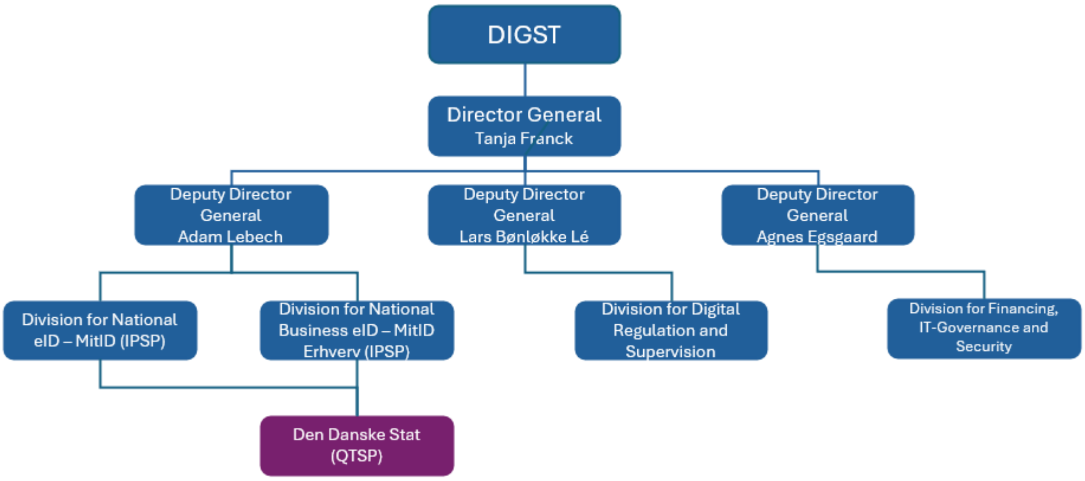
The Agency for Digital Government also operates two Identity Proofing Services:

- MitID for natural persons, and
- MitID Erhverv for legal person and natural persons associated with legal persons.

These services, MitID and MitID Erhverv are considered as trust service component and are used by the Certification Authority. For this reason, they must also comply with the requirements set out in this document.

This document constitutes the General Requirements Practice Statement (GRPS) that the Agency for Digital Government adheres to, both as a qualified trust service provider (QTSP) and as an Identity Proofing Service Provider (IPSP). It details how organizational procedures and policies fulfil the requirements from ETSI EN 319 401 v3.1.1.

Below is an organizational overview in regard to DIGST, the Qualified Trust Service Provider and the Identity Proofing Service Providers.


DIGST
Director General
Tanja Franck
Deputy Director General
Adam Lebech
Deputy Director General
Lars Bønløkke Lé
Deputy Director General
Agnes Egsgaard
Division for National eID – MitID (IPSP)
Division for National Business eID – MitID Erhverv (IPSP)
Division for Digital Regulation and Supervision
Division for Financing, IT-Governance and Security
Den Danske Stat (QTSP)

The Division for National eID manages the eID and identity proofing service MitID.

The Division for National Business eID manages the Business eID and identity proofing service MitID Erhverv.

Den Danske Stat [DDS] is a management unit within DIGST, that manages the QTSP Den Danske Stat Trust Services. This unit comprises of management personnel from both the Division for National eID [IDK] and the Division for National Business eID [KMDS].

The Division for Financing, IT-Governance and Security manages DIGST' information security management system.

The Division for Digital Regulation and Supervision hosts the national supervisory body for eIDAS in Denmark.

1.2 Reading instructions

This document lists the general requirements from [ETSI EN 319 401] and the practices that DIGST apply to ensure fulfilment of any relevant requirement either as a Trust Service Provider or as an Identity Proofing Service Provider.

Requirements from [ETSI EN 319 401] are marked in a *blue italics text*. They are immediately followed by a high-level description of the relevant practices specific to that requirement.

Requirements inherited from other ETSI standards are also marked in *blue italics text* and has a reference to the standard that it is inherited from.

Practices are not specifically marked and are written in normal black text.

1.2.1 Division specific practices

DIGST operates multiple services that must comply with the requirements of [ETSI EN 319 401], and these services may be managed by different divisions or entities within DIGST. Because each division may have varying practices or an organizational composition that necessitate specific documentation, supplementary material may be produced to fully demonstrate compliance with the requirements described in this practice statement. Any such additional documentation will be made available to a conformity assessment body or supervisory body when necessary.

Service specific practices described in this document will be marked using the responsible division or entity's abbreviation in square brackets and placed in a separate paragraph immediately following the corresponding requirement. A complete list of division abbreviations is provided in *Section 3: Definitions.*

Example:

> ***REQ-7.12-11:*** *The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.*
>
> Den Danske Stat, MitID, and MitID Erhverv have not established, nor intend to establish agreements or contracts with other parties to transfer the obligations of the TSP or IPSP in case of any service cessation.
>
> [DDS] In case of termination of the services of Den Danske Stat, availability of CRL and revocation of certificates are ensured in compliance with the existing contract.

1.2.2 Amended requirements

Some requirements may be amended or added by Commission Implementing Regulations (CIR). These requirements will be marked by a square bracket that refers to the relevant implementing regulation. If multiple implementing regulations amends or introduces a requirement, and the changes are identical, only one of the implementing regulations will be mentioned.

Example:

> ***REQ-7.8-14X:*** *The vulnerability scan requested by* ***REQ-7.8-13*** *shall be performed once per quarter.* [CIR 2025/1942]

2 References

Reference	Document
[CIR 2025/1942]	Commision Implementing Regulation https://eur-lex.europa.eu/eli/reg_impl/2025/1942/oj/eng
[CP]	Den Danske Stat's Certificate Policy https://certifikat.gov.dk/politikker-for-tillidstjenester/
[eIDAS]	Regulation (EU) No. 910/2014 as amended by Regulation (EU) 2024/1183 https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
[ETSI EN 319 102-1]	ETSI EN 319 102-1 v1.4.1 (2024-06), Electronic Signatures and Infrastructures (ESI) Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. https://www.etsi.org/standards
[ETSI TS 119 102-2]	ETSI TS 119 102-2 v1.4.1 (2023-06), Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report. https://www.etsi.org/standards
[ETSI TS 119 441]	ETSI TS 119 441 v1.3.1 (2025-10), Electronic Signatures and Trust Infrastructures (ESI); Policy requirements for TSP providing signature validation services. https://www.etsi.org/standards
[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. https://www.etsi.org/standards
[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. https://www.etsi.org/standards
[ETSI EN 319 421]	ETSI EN 319 421 v1.3.1 (2025-07), Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. https://www.etsi.org/standards
[ETSI EN 319 422]	ETSI EN 319 422 v1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles. https://www.etsi.org/standards
[NIS2]	Directive (EU) 2022/2555. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

3 Definitions

Abbreviation	Term
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DDS	Den Danske Stat is a Trust Service Provider. An entity within DIGST, established to manage the trust services that the agency provides.
DIGST	The Agency for Digital Government and relevant subcontractors
eID	Electronic identification scheme as defined in [eIDAS2]
GRPS	General Requirements Practice Statement (present document)
IDK	Division for National eIDs, proprietor of MitID.
IPSP	Identity Proofing Service Provider as defined in ETSI TS 119 461, MitID; MitID Erhverv
ISMS	Information Security Management System as defined in ISO/IEC 27001
KMDS	Division for Business eIDs and User Management Services, Proprietor of MitID Erhverv.
KØIS	Division for Financing, IT-Governance & Security, division within DIGST. Internal service division, whose primary focus is to support and maintain the organisation.
MitID	Notified eID Scheme and Identity Proofing Service.
MitID Erhverv	MitID for Business, Identity Proofing Service and non-notified eID scheme for Natural persons associated with Legal persons
Relying party	Relying party as defined in [eIDAS2]
Subject	Subject as defined in [eIDAS2]
Subscriber	Subscriber as defined in [eIDAS2]
Trust service	As defined in [eIDAS2]
TSA	Time Stamp Authority
TSP	Trust Service Provider
VA	Validation Authority

4 Additional Context

4.1 Policy specification

For all trust services issuing certificates, requirements are laid out in the Certificate Policy as defined by the Danish Supervisory Body and published on https://certifikat.gov.dk/politikker-for-tillidstjenester/. The policy covers issuance of qualified and non-qualified certificates.

For all other trust services and trust service components relevant requirements from the eIDAS2 regulation, including the corresponding Commission Implementing Regulations [CIR] and the designated standards constitute the policies for all trust services not issuing certificates.

4.2 PKI-participants

The PKI Participants of Den Danske Stat are the entities which makes use of services, or provides services which allow Den Danske Stat to provide certification services.

The PKI Participants are identified as the following:

- **Certificate Authorities:** acting as (Qualified) Trust Service Providers issuing certificates
- **Registration Authorities** performing identity proofing and registration functions (eID Services, MitID and MitID Erhverv and Connection Service)
- **Subscribers:** to whom certificates are issued
- **Signers (i.e. Signatories under eIDAS):** a natural person creating electronic signatures or seals
- **Relying Parties:** relying on certificates and other trust services
- **Other Supporting Participants:** involved in the provision or operation of trust services
- **Certificate Revocation Service:** responsible for certificate status management, including processing of revocation requests
- **Certificate Status Validation Service:** includes CRL and OCSP
- **Repository Services:** providing access to certificates, status information, and related trust data
- **Time-stamp services:** providing Qualified Electronic Time Stamps
- **Management of remote QSCDs:** The entity responsible for operating and maintaining remote Qualified Signature Creation Devices.

4.2.1 Trust Services issuing Certificates

The Den Danske Stat issues certificates in two key hierarchies for Qualified and OCES Certificates. The top level in each key hierarchy is always a self-signed root certificate. Each root certificate issues subordinate CA certificates to issue subject certificates.

Besides issuing subject certificate, the CA system also provides OCSP and time-stamp service certificates as described below.

- Qualified Root
  - Qualified intermediate
    - Qualified person
    - Qualified employee
    - Qualified organization
  - Qualified OCSP Responder for subject certificates
- Qualified Time Stamp certificates
- Qualified OCSP Responder for CA certificates
- OCES Root
  - OCES intermediate
  - OCES person
    - OCES employee
    - OCES organization
  - OCES OCSP Responder for subject certificates
- OCES OCSP Responder for CA certificates

The Den Danske Stat has been assessed for conformity under the regulation [eIDAS] and to meet the requirements in the relevant certificate policies by an accredited conformity assessment body. The conformity assessment report created by the conformity assessment body has been reviewed by the Danish supervisory body and the status granted to operate its services has been issued.

5 Risk Assessment

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.*

DIGST applies a risk-based approach to information security, and methods are based on ISO27005. The relevant division within DIGST performs and documents a service-specific risk assessment to identify, analyse and evaluate both business, technical, and other relevant risks for each service they provide.

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.*

As part of the service-specific risk assessments, a risk treatment plan is comprised to ensure mitigating activities are selected and implemented where needed.

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).*

Where risk treatment measures are selected, their implementation follows the change management procedures for the relevant division, where necessary security and operational requirements and procedures are identified before implementing the treatment measure.

REQ-5-04: *The risk assessment shall be regularly reviewed and revised.*

Risk assessments within DIGST are reviewed and updated at least annually.

REQ-5-05: *The TSP's management shall approve the risk assessment and accept the residual risk identified.*

The management of DIGST approves the risk assessment and the risk treatment plan and accepts the residual risks identified.

6 Policies and practices

6.1 Trust Service Practice Statement

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

The present document describes the general and organizational practices of DIGST and addresses the requirements from ETSI EN 319 401. For each trust or identity proofing service which is provided, a specific practice statement is comprised, addressing the requirements from relevant standards and policies for each trust service.

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.*

DIGST’ management is responsible for, and approve organizational policies, and ensures that the organization implements these.

The management of Den Danske Stat is responsible for, and approve practice statements for trust services, including the General Requirements Practice Statement [GRPS], and ensure correct implementation and communication to relevant employees and partners.

The management of the relevant divisions are responsible for, and approve practice statements for the identity proofing services, MitID and MitID Erhverv, and ensure correct implementation and communication to relevant employees and partners.

All practice statements may be split into a public and a private edition, with the public edition being published on relevant websites.

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.*

The [GRPS] together with the corresponding practice statement for each trust service, including IPSP services, describes the practices and procedures used to address all relevant requirements for each trust service that DIGST provides.

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.*

All practice statements include relevant obligations of all external organizations supporting the trust and identity proofing services and reference the applicable policies and practices that apply.

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.*

Public practice statements and other relevant documentation are published on the official websites and are available to subscribers and relying parties at all times. Additional non-confidential documentation necessary to demonstrate conformance to the applicable trust service policy can be made available on request.

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.*

The management of the Division for eID approves the IPSP practice statement relevant to the MitID service.

The management of the Division for Business eIDs and User Management Services approves the IPSP practice statement relevant to the MitID Erhverv service.

Den Danske Stat has an established management body, with overall responsibility for the TSP. The management body comprises of managers from both the Division for eID and the Division for Business eIDs and User Management Services and they approve the General Requirements practice statement and practice statements for the individual trust services.

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

The management of the relevant divisions for MitID and MitID Erhverv is responsible for implementing and maintaining the practices described in the IPSP practice statements. The management assigns resources and defines responsibilities to ensure compliance with these practises.

The management of Den Danske Stat ensures that the practices described in the following practice statements are implemented correctly:

- General Requirements Practice Statement for the Agency for Digital Government
- Den Danske Stat Certification Practice Statement
- Den Danske Stat Time-stamping Practice Statement
- Den Danske Stat rQSCD Practice Statement
- Den Danske Stat Validation Practice Statement

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

All practice statements are reviewed on a regular basis and at least annually.

The management of Den Danske Stat is responsible for maintaining, and approving practice statements for trust services, and ensures correct implementation.

The management of the relevant divisions are responsible for maintaining, and approving practice statements for the IPSPs, MitID and MitID Erhverv, and to ensure correct implementation.

REQ-6.1-09X [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.*

When the Den Danske Stat, MitID or MitID Erhverv intends to make changes in their practices that might affect the acceptance by subjects, subscribers or relying parties, the changes are assessed and approved by management and announced before they take effect.

Subscribers and relying parties are given due notice of such changes through publication of the updated practice statement on the official website and, via direct communication channels such as email or newsletters where appropriate.

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.*

Den Danske Stat, MitID and MitID Erhverv will publish practice statements on relevant websites immediately after approval.

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

The provisions for termination of service are described in detail for each of the services provided by trust or identity proofing service providers. These plans, as described in clause 7.12, set out the provisions for orderly termination of the services, including notifications, continued availability of information, retention of data and logs, and the secure destruction or withdrawal from use of relevant private keys.

6.2 Terms and conditions

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

DIGST will make the terms and conditions regarding the individual services available to all subscribers and relying parties.

The terms and conditions for the trust services are made available to all subscribers and relying parties. They are published on the official service websites and presented within the relevant applications, so that subscribers and relying parties can review them prior to using the services.

***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 each trust or identity proofing service are defined and maintained to support the applicable service policies. For each service, the terms and conditions specify, as a minimum, the scope and intended use of the service, the obligations of subscribers and relying parties, any limitations of use, applicable liability provisions, data protection and privacy information, applicable law and jurisdiction, and the procedures for complaints and dispute resolution. The terms and conditions are reviewed and updated as needed and are made available to subscribers and relying parties in accordance with clause 6.2-01.

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 relying parties are informed of the terms and conditions of the trust or identity proofing services before entering into a contractual agreement. The applicable terms and conditions are available on the official service websites prior to registration.

Subscribers must explicitly accept these terms and conditions before finalizing the onboarding for the services.

Relying parties entering into a contractual relationship must review and explicitly accept the terms and conditions before integrating to the trust or identity proofing services.

REQ-6.2-04: *Terms and conditions shall be made available through a durable means of communication.*

DIGST ensures that the terms and conditions are available on the official service websites. The terms and conditions can be viewed or downloaded as PDF-files.

REQ-6.2-05: *Terms and conditions shall be available in a readily understandable language.*

DIGST formulate terms and conditions in a clear and readily understandable language.

[IDK] For the MitID service, the terms and conditions are provided in Danish, English and kalaallisut (Greenlandic language) to ensure that subscribers can understand their rights and obligations before using the services.

[KMDS] For the MitID Erhverv service, the terms and conditions are provided in Danish.

[DDS] For Trust Services, the terms and conditions are provided in Danish and in English.

REQ-6.2-06: *Terms and conditions may be transmitted electronically.*

DIGST publishes terms and conditions at the services' official websites, and they are also transmitted electronically to subscribers and relying parties when necessary.

6.3 Information Security Policy

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.*

DIGST has a designated information security policy, including topic specific policies and guidelines that applies to all divisions and services. It is approved by management and sets out the organization's approach to managing information security.

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.*

DIGST ensures that changes to the information security policy are communicated to relevant third parties where applicable.

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.*

DIGST’s information security policy is documented, implemented, and maintained as part of DIGST’ ISMS. The policy defines security objectives and control requirements and is supported by operating procedures for the TSP’s or the IPSP’s facilities, systems, and information assets providing the services. The policies and procedures cover among other things risk management, incident management, supplier security and business continuity, and are reviewed and updated regularly to ensure they remain effective

REQ-6.3-04X: *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.*

Procedures are established to ensure notification of relevant parties, including but not limited to employees, subcontractors, authorities, and customers of significance or important changes in the provisions of the trust services, including identity proofing services.

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

DIGST’s information security policy is approved by management and published on the DIGST intranet where it is accessible to all employees. The policy is communicated to all personnel who are impacted by it as part of onboarding and through internal communications, ensuring that they are aware of their responsibilities.

Subcontractors’ information security policies are valid for subcontractors’ employees and communicated to all employees in equivalent ways. The subcontractor’s compliance with this is regularly reviewed and audited by independent third-party auditors.

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.*

DIGST’s information security policy is reviewed regularly, at least annually, or when significant changes occur. This ensures that the policy remains suitable, adequate and effective in relation to the identified risks and the operation of the trust and identity proofing services.

Regarding review of asset inventories see the description under REQ-7.3.2.01X.

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.*

The management of Den Danske Stat approves any changes that will impact the security of Trust Services.

The management of the relevant division approves any changes that will impact the security of the IPSPs.

This ensures that any changes are evaluated, authorised and documented in accordance with the governance and information security requirements.

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

Configurations in all systems related to Trust and identity proofing services are regularly checked for changes that violate security policies as described under REQ-7.7-08X.

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

The state and configuration of systems are regularly assessed for changes which could violate the security policies. The maximum interval between checks/assessments is one year.

7 TSP management and operation

7.1 Internal organization

7.1.1 Organization reliability

REQ-7.1.1-01: *The TSP organization shall be reliable.*

DIGST is a government agency and is registered as a legal person in the Danish company register, CVR with business registration number 34051178. DIGST operates on behalf of the Danish government, and through Den Danske Stat Trust Services, and the relevant divisions managing the IPSPs, MitID and MitID Erhverv, as a reliable trust and identity proofing service provider, ensuring service integrity, transparency, and compliance with applicable standards through structured governance and management system designed to ensure reliable provision of the trust services.

REQ-7.1.1-02: *Trust service practices under which the TSP operates shall be non-discriminatory.*

The practices of the trust services, including the identity proofing services are non-discriminatory and accessible to all eligible users within its operational scope. All services are provided on the basis of objective criteria and are not unnecessary influenced by applicants' identity beyond what is required to meet legal and security requirements. The services comply with the national act on accessibility requirements for products and services no. 801 from 07/06/2022, and compliance is audited by a supervisory body as specified in the law.

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.*

Den Danske Stat Trust Services, MitID and MitID Erhverv make their services accessible to applicants through service providers whose activities fall within the declared scope for each service and where applicants accept the terms and conditions before finalizing the onboarding or workflow.

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.*

DIGST is a government agency that operates both Den Danske Stat Trust Services, and the IPSPs MitID and MitID Erhverv. The State of Denmark is self-ensured, and this applies to DIGST as a government agency as stated in Circular 9783 of 9 December 2005. DIGST maintains sufficient financial resources and liability coverage to cover operational risks. This is supported by the Danish Ministry of Finance.

REQ-7.1.1-05: *The TSP shall have the financial stability and resources required to operate in conformity with this policy.*

DIGST is a government agency that operates both Den Danske Stat, MitID and MitID Erhverv. As a government agency, DIGST is supported by the Danish Ministry of Finance, and *financial stability is ensured and resources required to operate in conformity with this policy* are allocated through the annual Finance Act of the Danish State.

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.*

In compliance with the Public Administration Act and other relevant legislation DIGST has established policies and procedures for the resolution of formal complaints regarding the trust and identity proofing services from user and other relying parties.

Disputes regarding the trust and identity proofing services are processed according to each specific case.

7.1.2 Segregation of duties

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.*

DIGST ensures that conflicting duties and areas of responsibility are segregated. Segregation of duties is implemented through job descriptions, role-based access and technical controls. Roles related to development, operation and security administration are separated so the same person cannot both perform and control a critical activity at the same time. Four eyes principle or dual control is applied on changes that affect TSP’s critical assets.

Segregation of duties is verified through periodic recertification of access rights, and independent reviews.

7.2 Human Resources

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.*

DIGST ensures that all personnel and contractors follow the information security policy and related procedures. For internal employees, the ISMS is distributed and readily available on the intranet at all times. For contractors and their personnel, they are required to follow the contractors' internal ISMS and procedures, which are audited regularly by an independent third party.

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.*

DIGST employ qualified and trained staff and subcontractors with relevant expertise in cyber security and personal data protection. As part of the hiring process, the employees' experience and qualifications are validated by their direct manager and the hiring team.

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

Den Danske Stat Trust Services [DDS], the Division for National eID [IDK], and the Division for Business eIDs and User Management Services [KMDS] each have designated personnel that are responsible for network and information security who reports to the Agency's management. The personnel are all members of the CA-Management.

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.*

DIGST ensures that the personnel meet the requirement of expert knowledge through formal training, credentials, or experience. During the hiring process, employees are interviewed in multiple sessions, and they are required to produce a resume that details their experiences and qualifications, including formal training and credentials. Additionally, the candidates are required to provide references that can confirm the candidates' experience and qualifications.

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

All DIGST employees and contractors, are subject to awareness-training as part of the onboarding process. Additionally, employees are regularly updated on new threats and security practices through awareness campaigns managed by the Division for Financing, IT-Government and Security.

For subcontractor personnel, the subcontractor is contractually obligated to include security awareness training for relevant personnel, and the subcontractor is audited regularly, at least annually, by an independent third-party to confirm compliance.

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

DIGST' management have authority to administer appropriate disciplinary sanctions to Agency personnel who violates the agency's policies and procedures. HR evaluates the violation and the disciplinary sanction in accordance with applicable employment regulation.

The disciplinary sanctions may include a written warning, dismissal, summary dismissal or criminal pursuit, etc.

For subcontractor personnel, it is required that the subcontractor must retain a log of any policy violations and their consequences.

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

The following trusted roles, including roles at subcontractors, are currently identified and approved by the management of Den Danske Stat, including MitID and MitID Erhverv:

- Management
- Product owners
- Architects
- Compliance & Security Officers
- Revocation staff
- Operational staff
- Administrative staff
- System auditors

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

See REQ-7.2-07X

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.*

Job descriptions are defined for all personnel involved in the provisioning and management of the trust and identity proofing services, both temporary and permanent. Job descriptions are defined from the perspective of the roles to be fulfilled, considering segregation of duties and the least privilege principles, so that no single role is granted more access than is required to perform its assigned tasks.

For each role, the sensitivity of the position is determined based on the duties performed and the level of access to systems and information related to the trust or identity proofing services.

This sensitivity is defined by the duties performed and may result in additional requirements for background screening measures applied.

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

Job descriptions are defined in a way that clearly differentiates between general organisational functions and functions that are specific to the provision and management of the trust or identity proofing services.

For roles with TSP- or IPSP-specific responsibilities, the job descriptions explicitly describe the trust-service-related duties and the required skills, qualifications and experience in e.g. PKI, cryptography or other areas, in addition to general competency requirements for the position.

***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.*

All personnel at Den Danske Stat, MitID and MitID Erhverv are instructed to carry out administrative and management activities in accordance with the applicable information security management procedures. Operational procedures for the trust- or identity proofing services are documented, communicated to relevant personnel and aligned with the ISMS, and compliance with these procedures is monitored through management oversight, reviews and audits.

***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.*

DIGST ensures that managerial personnel responsible for the provision and management of the trust and identity proofing services possess appropriate competence. This includes experience or formal training related to the specific services provided, familiarity with the security procedures applicable to personnel with security responsibilities, and sufficient knowledge of information security and risk assessment to perform their management duties effectively.

***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.*

DIGST ensures through screening and employment contracts, that personnel in trusted roles are free from conflicts of interest that could affect impartiality.

Potential conflicts of interest are identified and assessed during recruitment, and personnel is required to disclose any situations that may give rise to a conflict of interest on an ongoing basis. Where a conflict is identified, appropriate measures are taken, such as reallocation of duties or exclusion from specific activities, to maintain the impartiality of the operations.

For personnel in trusted roles, background screening is performed to verify that their history does not contradict the trusted nature of their tasks. The background check includes:

- identity verification based on a passport or government-issued photo ID
- verification of documented references, education and professional experience
- criminal record check within the limits allowed by national legislation

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 REQ-7.2-07X

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

Personnel for trusted roles are formally by senior management. This is documented separately in addition to the hiring process.

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

DIGST ensures that trusted roles are accepted by the appointed individual before the person enters into the role. This is documented separately in addition the hiring process.

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

DIGST does not grant access to trusted functions until all required checks are completed. For roles that require a security clearance, a stand-in procedure is in place to:

- Confirm that the employee has been visually identified and that the identity has been verified based on a government-issued photo ID

- Confirm that the employee’s criminal record does not contain conflicting elements that could influence the trustworthiness of the employee

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.*

DIGST require personnel and subcontractors to use a VPN-connection to access TSP- and IPSP-networks, when working remote or using a wireless connection outside of DIGST’ premises. The VPN access must be protected with multifactor authentication.

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

DIGST Information Security Policy includes a policy on remote working, that defines relevant cybersecurity conditions and restrictions.

7.3 Asset management

7.3.1 General requirements

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

DIGST has established general policies and guidelines for management and protection of information assets.

End-user IT-assets such as personal computers and mobile phones are supplied though The Agency for Governmental IT Services (SIT). The responsibility for the protection of these assets is therefore placed at SIT.

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

Where trust and identity proofing service components are operated by external suppliers, DIGST ensures through contractual regulation and periodic assurance activities that the suppliers maintain an accurate, classified inventory of assets controlled by the supplier. Additionally, see section 7.14.

7.3.2 Assets inventory and classification

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.*

An accurate and up-to-date inventory of assets that support the provision of the trust and identity proofing services are maintained. The inventory includes relevant hardware such as servers, firewalls and network components. Each asset is assigned an owner and a classification consistent with the results of the organisation's risk assessment and information classification scheme. The classification levels are based on the need for protection in regard of confidentiality, integrity, authenticity and availability and they are reviewed regularly aligned with updated risk assessments.

The asset inventory is used as a primary input to technical vulnerability management, including the identification, prioritisation and remediation of vulnerabilities affecting systems within the scope of the trust services.

End-user computing IT assets such as administrative workstations that are used by DIGST to support the provision and management of trust and identity proofing services, are operated by The Agency for Governmental IT services (SIT). SIT maintains an accurate and up-to-date inventory of each such asset with an assigned owner and a classification consistent with the organisation's risk assessment and information classification scheme and use this as basis for technical vulnerability management.

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 REQ-7.3.2.01X.

REQ-7.3.2-03X: *The TSP shall assign a classification level to each asset, or group of assets, based on requirements for protecting confidentiality, integrity, authenticity and availability, and in accordance with its risk assessment and business value.*

See REQ-7.3.2.01X.

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 REQ-7.3.2.01X.

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

See REQ-7.3.2.01X.

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.*

DIGST has established general policies for acceptable use and handling of information and assets used in connection with information handling. These rules are set out in the ISMS and cover topics such as asset ownership, registration and classification. The rules apply to all personnel and relevant external parties with access to trust-service assets, which are communicated as part of onboarding and regular security awareness activities and are supported by technical controls and monitoring to help ensure compliance.

DIGST ensure through contractual regulation and supervision that suppliers used in connection with trust and identity proofing services have implemented formal policies for acceptable use and handling of information and related assets.

REQ-7.3.2-07X: *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.*

DIGST has established an HR procedure to ensure employees return all delivered end-user computing IT assets upon termination of employment. The procedure covers all employees including internal and external personnel and contractors.

DIGST ensure through contractual regulation and supervision that suppliers used in connection with trust and identity proofing services have formal procedures to ensure employees return of all delivered end-user computing IT assets upon termination of employment.

7.3.3 Storage media handling

***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.*

All management of storage media related to trust and identity proofing services is carried out by external suppliers. DIGST has ensured through contractual regulation and supervision that the suppliers used in connection with trust and identity proofing services have implemented formal procedures for storage media to ensure:

- Life cycle management of storage media from acquisition to exposal
- Protection of storage media from damage, theft and unauthorized access, obsolescence and deterioration

***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 REQ-7.3.3.01X.

***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 REQ-7.3.3.01X.

7.4 Access control

REQ-7.4-01: *The TSP's system access shall be limited to authorized individuals.*

Security policies have been established to document principles for system access, and access to systems related to trust and identity proofing services is restricted to authorised personnel only. User Identities and access rights are managed through documented access control procedures and supported by dedicated tools. Access is only granted to authorized persons based on defined roles and “least privilege” principles.

REQ-7.4-02X: *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.*

Procedures have been established and are being used to manage the privileged access to systems related to trust services and ensure that the principle of "least privileges" is applied when configuring access privileges. Least privileges principle is applied in the approval process, where privileged access must be approved by both leader and system owner, or through Role Based Access Control with careful design of administrative roles with specific tasks and associated access right. This ensures the required level of privilege is assessed, and that access is granted only in cases where a work-related need exists.

REQ-7.4-03X: *The TSP shall provide setting up specific accounts to be used for administrative purposes like installation, configuration, management or maintenance.*

Security policies demand that specific accounts are used for administrative purposes like installation, configuration, management or maintenance. Administrative accounts are only used for their dedicated purpose and procedures have been implemented to ensure that traceability is established so that any privileged access can be traced to an individual.

REQ-7.4-04X: *Privileged accounts shall be used only if the privileges are necessary for the specific activity.*

Privileged accounts are strictly used for when the privileges are necessary for the activity. Routine user activities are carried out using standard user permissions, while administrative tasks require activation of dedicated privileged accounts or elevated roles. The use of privileged access is controlled and monitored in accordance with the access policy.

REQ-7.4-05X: *Strong identification, authentication and authorisation procedures shall be used for privileged accounts.*

Strong identification, authentication and authorisation procedures are used for privileged accounts that access systems related to trust and IPSP services by:

- Performing identity verification of all personnel based on government-issued photo ID verification during the hiring process prior to being granted access to trust and IPSP services
- Enforcing strong multi-factor authentication mechanisms for administrative access to privileged accounts supporting the trust services
- Granting authorisation based on predefined, role-specific authorisation profiles that are aligned with job responsibilities and follow the principles of least privilege
- Linking user access rights to verified identities that are reviewed and adjusted throughout the employment lifecycle

REQ-7.4-06X [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.*

Users are authenticated with multi-factor authentication mechanisms before accessing systems related to trust and identity proofing services. The multi-factor authentication method is based on ID cards, user accounts and corresponding personal passcodes.

REQ-7.4-07X: *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.*

Procedures are in place to ensure that access rights for privileged accounts used for access to systems related to trust and identity proofing services are reviewed at planned intervals. The regular reviews of privileged accounts is conducted at monthly intervals, and the review results and changes are documented. Non-privileged accounts are reviewed once every quarter.

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

Procedures are in place to ensure that access permissions are removed upon termination of employment, and that permissions are modified upon change of functions.

Access permissions are controlled by formal processes to ensure that access is granted based on formal approval, and that the access permissions are removed when no longer required including termination of employment or change of function.

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

Access to information and application system functions is restricted in accordance with the access control policy. Role-based access controls are applied in accordance with the principle of least privilege to ensure that users are granted only the access rights necessary for their job functions. Access rights are approved, implemented, and reviewed in line with documented procedures.

REQ-7.4-10X: *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.*

The TSP’s systems provide computer security controls to enforce the separation of trusted roles identified in these practices. Security administration roles are segregated from operational roles through role-based access controls. The use of system utility programs is restricted to authorized personnel and is subject to approval and monitoring in accordance with documented procedures.

Segregation of duties is enforced through system-level security controls, including for example technical separation of functions across test, pre-production, and production environments, ensuring that access to one environment does not permit access to another. Access to privileged accounts used for administrative functions is restricted to authorized personnel and protected by multi-factor authentication.

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

All personnel are uniquely identified and authenticated before accessing critical applications related to the trust and identity proofing services. Access is granted via individual user accounts managed with the identity and access management system and protected by strong authentication in accordance with the access control policy. Shared or technical accounts are only accessed through mechanisms that ensure each action can be traced to an identified individual.

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

Personnel are accountable for their activities related to the trust and identity proofing services. Access to critical systems and applications is performed using individual user accounts, and relevant actions are logged to enable traceability to a specific person. Responsibilities and expected behaviour are defined in documented policies and procedures, and breaches of these obligations will be assessed by the security organisation and may lead to disciplinary actions in accordance with applicable HR and legal requirements.

REQ-7.4-13X: *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.*

Sensitive data are protected against disclosure through re-used storage objects or media. Storage media and logical storage objects (such as files, virtual disks or database spaces) containing sensitive information are securely erased, cryptographically wiped or physically destroyed before being re-used or released to other users, systems or environments. These activities are carried out in accordance with documented procedures and the asset and media handling requirements defined in clause 7.3

7.5 Cryptographic controls

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

Appropriate security controls are in place for the management of all cryptographic keys, cryptographic algorithms, and cryptographic devices throughout their lifecycle.

Key and device management is governed by documented policies and procedures covering the full life cycle including generation, activation, distribution, use, backup, restore, expiry and archive. The procedures include the use of dual controls for handling and accessing the cryptographic modules, segmentation of networks and components, established high-security zones, real-time monitoring of traffic, logging all activities on all cryptographic modules and security surveillance.

Private keys are generated and stored inside certified cryptographic modules and marked as no export.

[DDS] For root keys and the signing service, the cryptographic modules used are certified following Common Criteria (ISO 15408) for assurance level EAL4+ using the protection profile [CEN EN 419 221-5]. For other cryptographic modules, they are certified to meet the requirements in [FIPS 140-2] level 3.

Cryptographic algorithms and key lengths are defined in an approved cryptographic policy. All key management operations are logged to ensure traceability and integrity of the trust services, and backup copies of key material are automatically encrypted. In the event of suspected key compromise, documented incident procedures are followed, including revocation and re-keying as appropriate.

7.6 Physical and environmental security

***REQ-7.6-01:** The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security.*

The physical access procedures to protect the critical components of the trust and identity proofing services have been established and are available in internal documents. The procedures include controlled access points, security surveillance, high security zones only accessible by trusted personnel and dual access controls.

***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.*

Physical access is provided with “least privileges” principles and with additional restrictions on physical access to critical systems used for the provisioning of the trust and identity proofing services. Access to high security zones is managed by Identity Management (IDM) system and logged by the access control systems.

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

All sensitive components and physical operations of trust and identity proofing services are located within physically secure data centre facilities. The data centres have redundant power sources, supported by an uninterruptible power supply (UPS) and maintains backup power supplies for up to 72 hours.

The data centres have established central climate control systems that meet the requirements of the equipment installed, and this ensures a stable temperature throughout the data centre. Additionally, the components are mounted with fans that ensure appropriate cooling of the individual components.

Appropriate measures have been taken to prevent exposure of the equipment and cables to water. Cabling is installed under raised access floor or under the ceiling in cable baskets and various detectors in the floor, ceilings, cable baskets, etc., have been installed to detect water, fire and other unwanted substances.

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

Information is encrypted at all times, both at rest and while in transit. Additionally, access to components which process, and store information is restricted to authenticated and trusted personnel only. Access requires scanning and ID card and entering a personal PIN number. The activities that personnel perform on components are monitored and logged at all times. For components in secure rooms dual access controls are applied.

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

All components that are critical for the secure operation of the trust and identity proofing services, are located within a physically secure facility that applies multiple layers of security to safeguard the components and restrict access, including perimeter controls and monitored secure rooms.

7.6.1 Inherited requirements from service specific standards

The following requirements regarding physical security controls are inherited from service specific standards and only apply to the trust service provider, Den Danske Stat:

OVR-6.4.2-02: The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data. [ETSI EN 319 411-1]

Certificate generation and revocation management operations are carried out within physical barriers established by using data centres' secure facilities and high security zones for housing the certificate issuing and certificate revocation services.

OVR-6.4.2-03: Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. [ETSI EN 319 411-1]

Access to restricted areas is logged and audited and escorted access for non-authorized personnel is mandatory.

OVR-6.4.2-04: Every entry and exit shall be logged. [ETSI EN 319 411-1]

Access to restricted areas is logged and audited and escorted access for non-authorized personnel is mandatory.

OVR-6.4.2-05: Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services. [ETSI EN 319 411-1]

Physical barriers are established by using data centres' secure facilities and high security zones for housing the certificate issuing and certificate revocation services.

OVR-6.4.2-06: Any parts of the premises shared with other organizations shall be outside the perimeter of the certificate generation and revocation management services. [ETSI EN 319 411-1]

The services for certificate generation and revocation are placed in the same dedicated security zone.

OVR-6.4.2-07: Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. [ETSI EN 319 411-1]

All data centres have suitable and redundant power supplies and climate control systems for the requirements of the equipment installed in them. The infrastructure is protected against power failures or any other electricity supply anomaly. Appropriate measures have been taken to prevent exposure of the equipment and cables to water. The data centres have the suitable means (detectors and automatic fire suppression systems) to protect their content against fire. Cabling is installed under a false floor or under the ceiling in cable baskets and the appropriate means (detectors in the floor and ceilings) have been installed to protect them against fire.

OVR-6.4.2-08: The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery. [ETSI EN 319 411-1]

All data centres have suitable and redundant power supplies and air-conditioning for the requirements of the equipment installed in them. The infrastructure is protected against power failures or any other electricity supply anomaly. Appropriate measures have been taken to prevent exposure of the equipment and cables to water. The data centres have the suitable means (detectors and automatic fire suppression systems) to protect their content against fire. Cabling is installed under a false floor or under the ceiling in cable baskets and the appropriate means (detectors in the floor and ceilings) have been installed to protect them against fire. The data centres are furthermore protected with physical access control, and the high security zones are protected with dual access control.

OVR-6.4.2-09: Controls shall be implemented to protect against equipment, information, media and software relating to the TSP's services being taken off-site without authorization. [ETSI EN 319 411-1]

Physical security of the PKI System is used to mitigate risk of environmental or human physical threats to an acceptable level supporting the overall security and contingency requirements, including preventing PKI System equipment, information, media and software relating to the services being taken off-site without authorization.

OVR-6.4.2-10: Other functions relating to TSP's operations may be supported within the same secured area provided that the access is limited to authorized personnel. [ETSI EN 319 411-1]

Access to secure areas is limited to authorized personnel only.

OVR-7.8-02: Access controls shall be applied to the secure cryptographic device to meet the requirements of security of security cryptographic devices as identified in clause 7.6. [ETSI EN 319 421]

All trust services and their components are located and operated from the same secure zones and apply the same access controls across all trust services. This includes physical barriers through multiple security zones within the facilities and caged cabinets dedicated for the trust services.

For access to the trust services, dual access controls are applied and only accessible by trusted personnel. Non-authorized personnel may only enter the secure rooms, while being accompanied by authorized personnel.

OVR-7.8-03: The time-stamping management facilities shall be operated in an environment which physically and logically protects the services from compromise through unauthorized access to systems or data [ETSI EN 319 421]

See OVR-7.8-02.

OVR-7.8-04: Every entry to the physically secure area shall be subject to independent oversight. [ETSI EN 319 421]

Access to secure rooms is logged and may be subject to review during audits or upon request by DIGST.

OVR-7.8-05: Non-authorized person shall be accompanied by an authorized person whilst in the secure area. [ETSI EN 319 421]

See OVR-7.8-02.

OVR-7.8-06: Every entry and exit to/from the physically secure area shall be logged. [ETSI EN 319 421]

See OVR-7.8-04.

OVR-7.8-07: Physical protection shall be achieved through the creation of clearly identified security perimeters (i.e. physical barriers) around the time-stamping management. [ETSI EN 319 421]

See OVR-7.8-02.

OVR-7.8-08: Any parts of the premises shared with other organizations shall be outside this perimeter. [ETSI EN 319 421]

See OVR-7.8-02.

OVR-7.8-09: Physical and environmental security controls shall protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. [ETSI EN 319 421]

See OVR-6.4.2-08.

OVR-7.8-10: The TSA's physical and environmental security policy for systems concerned with time-stamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure to supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery. [ETSI EN 319 421]

See OVR-6.4.2-08.

OVR-7.8-11: Controls shall protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization. [ETSI EN 319 421]

See OVR-6.4.2-09.

OVR-7.8-12: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel. [ETSI EN 319 421]

See OVR-6.4.2-10.

OVR-7.9.2-01: Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. [ETSI EN 319 421]

Capacity is actively monitored and estimates of future capacity requirements are performed and reported each quarter. Estimates may be based on historic data, any information on future enrolled or disenrolled service providers or other relevant data.

7.7 Operation security

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.

All systems and components used for trust and identity proofing services are carefully assessed and selected from reputable vendors. The systems are protected against modification through the maintenance of secure configurations, and documented change and patch management procedures. The systems are protected against unauthorized modification through access control, authentication mechanisms, logging, and integrity monitoring.

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.

Analyses of security requirements are conducted during the design and specification phase for all development of systems in connection with trust and identity proofing services. The aim of this is to ensure that appropriate security controls are incorporated into the system design to achieve security by design.

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.

Formal change management procedures are established for all systems in connection with trust and identity proofing services.

Significant or critical changes, i.e. releases of new versions of software and applications, modifications, configuration changes of critical components and emergency changes, are only processed after formal approval by change advisory boards.

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

All changes processed through the formal change manage procedures are documented and stored in appropriate systems. This includes release notes for each release and formalized go-no-go meetings before any release of new changes.

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

All systems in connection with trust and identity proofing services are protected against malware and unauthorized software through a combination of endpoint protection solutions, centralised security systems and directory-based policies and other relevant techniques.

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

Descriptions of privileges and responsibilities for the trusted and administrative roles that carry out tasks which can impact the provision of trust and identity proofing services are documented as part of operational procedures, including the job descriptions

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.

Patch management procedures are established and implemented. The procedures include defined time frames for applying security patches in accordance with defined criteria for criticality, threat exposure and risk levels. As part of the procedures assessment of possible downsides to implementing patches in the sense of introduction of new vulnerabilities and impact on operations are carried out.

As part of the procedures, plans for mitigation of vulnerabilities that cannot be patched immediately are processed and approved by management, this includes analysis and reasons for not applying patches.

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

All implemented configurations to hardware and systems related to trust and identity proofing services are documented in the system documentation. Configurations are monitored and reviewed by use of configuration management tools, centralized log monitoring, continuous vulnerability scans and regularly pen-test.

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

All configurations are monitored and updated using a configuration management database.

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 REQ-7.7-08X

7.8 Network security

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

The networks of the trust and identity proofing services are protected from attacks, through scalable DDoS protection systems in multiple layers and apply both antivirus and anti-malware detection and protection software for all networks.

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.*

The networks are segmented and protected based on a risk-based approach considering both functional, logical, and physical relationships between segmented networks or zones. Between segmented networks and zones a managed firewall is applied, allowing only authorized communications to pass through.

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

All systems within a segmented zone are protected using the same security controls.

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

Firewalls are configured to prevent all protocols and accesses not required for the operation. This includes enforced encrypted traffic and protocols, zone restrictions, restrictions on network-to-network access, authentication and authorization requirements and restriction of remote access.

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

All systems are continuously hardened. This includes the deactivation of not needed processes and connections.

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

Rulesets and security controls on network devices such as firewalls are reviewed on a regular basis.

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]).*

Critical systems and components like Root CA-systems are located in separate secure zones that apply dual access controls.

REQ-7.8-08: *The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.*

The trust and identity proofing services each have dedicated networks for their individual operations. These networks are logically separated from other networks and supported by administrative networks.

REQ-7.8-09X: *The TSP shall logically separate administration systems and networks from other information systems and networks.*

See REQ-7.8-08.

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).*

The production environments and systems are separated from development-, testing- and staging environments.

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.*

The trust and identity proofing services have established trusted channels between distinct trustworthy systems. Encrypted communication channels are based on standard protocols and algorithms such as TLS.

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.*

The datacentres hosting the trust and identity proofing services all have redundant external network connections, this includes agreements with multiple internet service providers (ISP).

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.*

The trust and identity proofing services perform and document a vulnerability scan of IP addresses, at least once per quarter. The scans are documented and archived. Vulnerability scans are performed with tools from a reliable and proficient third-party.

REQ-7.8-14X: *The vulnerability scan requested by* ***REQ-7.8-13*** *shall be performed once per quarter.* [CIR 2025/1942]

See REQ-7.8-13

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.*

The trust and identity proofing services have installed advanced malware detection and removal tools from recognized third-party service providers, the tools analyse data in real-time and are updated daily.

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

See REQ-7.8-15X

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.*

Penetration tests are performed regularly, this includes when setting up the systems, after infrastructure or application modifications or upgrades that are deemed significant, and at least annually.

REQ-7.8-18X: *The penetration test requested by* ***REQ-7.8-17X*** *shall be performed at least once per year. [CIR 2025/1942]*

See REQ-7.8.17X

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.*

Penetration tests are performed using tools from a reliable and proficient third-party, which produces a reliable test report.

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.*

Firewalls protect the internal network domains from unauthorized access, including access by subscribers and third parties. The firewalls are configured to prevent all protocols and access that are not required for the operation. This includes enforced encrypted traffic and protocols, zone restrictions, restrictions on network-to-network access, authentication and authorisation requirements and restriction of remote accesses.

REQ-7.8-21X: *Firewalls shall also be configured to prevent all protocols and accesses not required for the operation of the TSP.* [CIR 2025/1942]

See REQ-7.8-20X

7.9 Vulnerabilities and Incident management

7.9.1 Monitoring and logging

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.*

Several mechanisms to detect security incidents are established as part of the infrastructure of systems related to trust and identity proofing services. This includes centralized log monitoring, intrusion detection and prevention systems and vulnerability and configuration monitoring.

The detection activities are monitored and responded to by 24/7 staffed security operation centres (SOC)

Logging of critical events is automated for systems and infrastructure in a centralized SIEM-system. Logs include security logging, error and operational performance logging and user and access logging. Stored logs include all relevant information mentioned in REQ-7.9.1-04X below.

Changes are documented and logged by use of change management procedures and supporting documentation and approval system.

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

Access to sensitive information in logs is restricted through limited user access based on roles and responsibilities and based on "least privilege" principles.

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 REQ-7.9.1-01X

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 REQ-7.9.1-01X

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 REQ-7.9.1-01X

7.9.2 Incident response

***REQ-7.9.2-01X:** The TSP shall establish incident response procedures including containment, eradication and recovery.*

The applicable and appropriate incident and/or compromise reporting and handling procedures are established and implemented.

***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.*

Reporting to supervisor authorities and CSIRT's are integrated as part the incident management processes.

Significant Incidents according to the NIS2 EU-legislation are reported to Styrelsen for Samfundssikkerhed.

Personal data security breaches are reported to the Danish Data Protection Agency.

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

Stakeholders are informed about incidents though mailing lists and optional through the website Digitaliser.dk

***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.*

Communication plans for incidents are established as an integrated part of the incident management processes. Incident categories and standard escalation procedures are included in the plans. Reporting of incidents follow standardised formats and procedures.

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

Personnel working with security incident response is recruited by competence and given the necessary professional training.

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

All phases from detection to handling of incidents are documented via the incident- and problem management procedures. This documentation includes minutes of incident-meetings, problem reports and public updates via official websites like digitliser.dk.

***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.*

Documented interfaces between incident handling and business continuity management are established. This includes clear roles, escalation criteria, communication channels, and integrated procedures to ensure a coordinated and cohesive response during incidents.

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

The roles, responsibilities, and relevant procedures for incident management are regularly tested and reviewed. Additional reviews are also conducted following incidents with the purpose of improving the incident management processes.

***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.*

Newly discovered vulnerabilities classified as critical are addressed with no undue delay as part of operation security procedures as described in section 7.7 above.

***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.*

For each identified vulnerability, a mitigation plan based on the potential impact is implemented. When determined that remediation for a vulnerability is not required justification for the decision is documented.

***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.*

Incident management procedures are applied in a way that ensure timely detection, handling and reporting of security incidents and relevant malfunctions, and to ensure fast and sufficient reporting to all relevant parties. This is done to minimize the damage and impact of security incidents and to contain incidents as effective as possible.

***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.*

Trusted roles with responsibility for incident detection, alert handling and reporting are defined and described as part of the incidents management processes.

This personnel follows up on alerts of potentially critical security events and ensure that all relevant incidents are reported in accordance with the documented procedures and escalation paths.

7.9.3 Reporting

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.*

The procedures are described in internal security breach procedures cf. REQ-7.9.2-02X. These procedures include notification of relevant parties including the Danish data protection agency (GDPR), Styrelsen for Samfundssikkehed (the NIS2-supervisory body for DIGST' systems), and the Danish eIDAS supervisory body.

[IDK] [KMDS] The NIS2 requirement of notification within 24 hours does not apply to MitID and MitID Erhverv as IPSPs. Procedures for notification of Significant Incidents in connection with MitID and MitID Erhverv therefore follows the requirement of notification within 72 hours.

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.*

Notification of natural or legal persons is handled as part of internal procedures for reporting of personal data breaches and performed in case of breach of security or loss of integrity that is likely to affect such person. These procedures ensure that notification of the breach of security or loss of integrity is performed as soon as possible and without undue delay

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.*

As part of incident management process, simple and clear procedures have been established that enable staff, contractors, and customers to report potential network and information security incidents through defined reporting channels.

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.*

Reporting procedures for network and information security incidents are communicated to contractors and customers. Instructions on staff training and point of contact for incident reporting is also communicated to contractors and customers.

7.9.4 Event assessment and classification

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

Reported incidents/event are analysed and assessed as part of the established incident management processes, including assessment of event severity

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

Reclassification of incidents/events based on new inputs are handled as part of the established incident management processes.

7.9.5 Post-incident reviews

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

Technical vulnerabilities in information systems used in connection with trust and identity proofing services are discovered through regular vulnerability scans and penetration tests. In addition, information about known vulnerabilities is received from vendors, cooperating partners and public sources.

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

The trust and identity proofing services exposure to identified vulnerabilities is evaluated as part of the documented vulnerability assessments and patch management processes. The processes also include identification and implementation of appropriate measures to mitigate the vulnerability.

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.*

Root cause identification and analysis is performed as part of the applicable problem management procedures. All handled significant incidents are evaluated with focus on possible risk mitigation measures, including mitigating activities required to prevent recurrence.

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

Post-incident reviews are conducted on all incidents as part of incident management procedures.

7.10 Collection of evidence

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.*

[DDS] All relevant information concerning data issued and received in relation to the trust services is recorded and retained in an audit log. The audit log is maintained for at least 7 years after expiry of the issued certificates.

[KMDS] All relevant information concerning data issued and received in relation to the MitID Erhverv IPSP is recorded and retained in an audit log. The audit logs are maintained for different periods depending on the type of operation and requirements related to privacy legislation. The retention periods are documented in the contract between DIGST and the subcontractor maintaining the logs.

[IDK] All relevant information concerning data issued and received in relation to the MitID IPSP is recorded and retained in an audit log. The audit logs are maintained for different periods depending on the type of operation. The retention periods are documented in the contract between DIGST and the subcontractor maintaining the logs.

Any data including records and relevant parts of audit logs will be made available for the purpose of legal proceedings if a legal basis exists e.g. warrant from a Danish court.

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

Logs and other archived records are managed with a centralized log management service and archived on separate log servers. The servers are protected with various security layers protecting the data from manipulation and unauthorized access, applying “least privilege” and “segregation of duties” principles in order to safeguard the data. Archived records are subject to the same confidentiality and integrity requirements as operational records.

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

Records concerning the operation of the trust services are completely and confidentially archived in accordance with the disclosed business practices, including this practice statement and related policies. All records required to reconstruct service events and provide evidence of the operation of the trust and identity proofing services are included in the archives.

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.*

Any data including records and relevant parts of audit logs will be made available for the purpose of legal proceedings if a legal basis exists e.g. warrant from a Danish court.

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

All logs include the time for the individual events and relevant components including network devices and operational servers are connected to NTP servers, thereby ensuring a unified and trustworthy time source for logs.

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.*

Controls are in place to ensure that the time used for audit log timestamps are synchronized with UTC continually and at least daily. The systems are connected to an NTP device that receives the time from external time source via satellite.

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 REQ-7.10-01

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.*

Appropriate protection against modification and deletion of the audit logs is implemented, and retention policies apply. Log information is stored on dedicated servers, and access to data is restricted to employees with a work-related need. Events are logged in a secure manner, that ensures that the events cannot be easily deleted or destroyed.

7.11 Business continuity management

7.11.1 General

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

A Business continuity plan is maintained to ensure the continuity of services. The Business Continuity Plan has been approved by DIGST management and is activated in case of an operational disaster. Recovery plans are maintained and tested regularly

***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.*

Contingency plans are activated in case of disaster, including compromising of one of the PKI Systems' private signature keys or other trust or identity proofing credentials. Disaster recovery plans and backup/restore facilities ensure that operations may be restored within the recovery time objectives defined in the Business Continuity Plans.

The underlying cause of the disaster is analysed and addressed following the steps in the incident and problem management processes with appropriate remediation measures as necessary.

7.11.2 Back up

***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.*

Backup facilities including the necessary IT infrastructure and personnel are established to ensure that backup copies of information are stored to the extend necessary continuity and disaster recovery plans.

***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).

Backup plans and procedures are prepared and approved in accordance with the specified demands for restore of systems and information. All relevant aspects including recovery time requirements, physical, technical and environmental protection of backup copies and restore processes are considered and are included in the plans.

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

Integrity checks are performed as part of backup procedures cf. REQ-7.11.2-01X.

REQ-7.11.2-04X: *The TSP shall test at planned 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.*

Recovery tests of backup copies and redundancies are performed as part of regularly planned preparedness tests. Test results are documented in preparedness test reports.

7.11.3 Crisis management

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.

Crisis management is defined and handled as an integrated part of the established business continuity plans

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.*

The National CSIRT under Styrelsen for Samfundssikkerhed, publishes both national and sector specific threat assessments annually, which are incorporated into the service specific risk assessments performed by DIGST.

Other information received from the National CSIRT, such as alerts on known vulnerabilities are distributed to key personnel at DIGST, who then ensures that an assessment of such vulnerabilities is performed.

Where applicable, information from other competent authorities that are relevant for crisis management is received and reviewed by relevant personnel. Such information may be used as input to the design and periodic review of the organisation’s major incident and crisis management processes. Where applicable, such information may also be used to support the handling of major incidents and crises.

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.*

Crisis management is tested and reviewed as part of the regularly test and reviews of the business continuity plans. Evaluation of crisis management is also done following an incident where contingency plans have been activated.

7.12 TSP termination and termination plans

***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.*

Separate termination plans have been established for trust and identity proofing services. All termination plans are designed to minimize the impact on subscribers and relying parties from cessation of trust services, including appropriate retention of relevant data and logs, so that this information remains available and trustworthy for the defined retention periods in accordance with legal, regulatory and contractual requirements.

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

Termination plans for the qualified trust services are maintained and reviewed at least every second year.

***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.*

The termination plan specifies the stated practice on communication to be performed.

Before a Trust Service is terminated the following will be informed:

- Subscribers of the trust service will be informed
  Subscribers will be informed at least 3 months before the service stops issuing, reissuing or renewal of certificates or stops validating signatures and seals or stops issuing timestamps. Information to subscribers of CA services will furthermore take place 6 months before initiating activities which affect already issued certificates e.g. revocation and stopping OCSP-service.
- Other contractual parties will be informed.
  Information to other contractual partners will take place at least 6 months before the service stops issuing, reissuing or renewal of certificates or stops validating signatures and seals or stops issuing timestamps.
- Relevant public authorities incl. the eIDAS supervisory body shall be identified and informed.
  Relevant public authorities will be identified and informed at least 6 months before services are stopped.
- Information about the planned termination shall be published
  At least 6 months prior to termination of trust service activities relying parties are informed via https://www.ca1.gov.dk and a press release or newsletter will be published.

Before an IPSP service is terminated the following will be informed:

- Subscribers of the IPSP service will be informed.
  Subscribers will be informed at least 6 months before the IPSP stops its services.
- Other contractual parties will be informed.
  Information to other contractual partners will take place at least 6 months before the service stops.

- Relevant public authorities incl. the eIDAS supervisory body shall be identified and informed. Relevant public authorities will be identified and informed at least 6 months before services are stopped.
- Information about the planned termination will be published The publication of the plan to terminate the service will be done via appropriate means of mass communication e.g. newsletter and/or press release.

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 REQ-7.12-03

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.*

The termination plans detail that all subcontractors' authorization to act on behalf of the TSP or IPSP must be terminated when the services are terminated.

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.*

Being a public authority under the state of Denmark, in case DIGST decides to terminate its trust and identity proofing service activities (or parts of it) none of the activities can or will be transferred to any other party.

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.*

The termination plans detail the terms for destroying private keys and their backup copies. Data to be deleted, including private keys and key backups, are destroyed or made inaccessible in a manner which prevents recovery. This includes TSA private keys and backups of TSA private keys, as well as any private key used solely for the purpose of providing the IPSP service. Before the TSP or IPSPs terminates its services, such private keys are destroyed or withdrawn from use in a way that ensures that they cannot be retrieved.

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 REQ-7.12-06

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.*

The TSP is operated by DIGST as a public authority under the state of Denmark, DIGST is not subject to private-sector bankruptcy or insolvency procedures. Liabilities arising from the provision of the trust services are backed by the State budget, and DIGST is effectively self-insured in accordance with applicable national legislation.

Termination and continuity plans are maintained ensuring that, in the event of a decision to discontinue a service, the obligations towards subscribers and relying parties are honoured, and services are terminated in an orderly manner according to plan.

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.*

a) See REQ 7.12-03
b) See REQ 7.12-06

REQ-7.12-11: *The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.*

There are no agreements, and there is no intension to establish agreements or contracts with other parties to transfer the obligations of the TSP or IPSP in case of any service cessation. As documented in termination plans, VA certificates and TSA certificates will be available on https://www.ca1.gov.dk or transferred to another public authority for publication in a reasonable time after the service is stopped.

7.13 Compliance

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

DIGST takes all the necessary steps to ensure that trust and identity proofing services operate in a legal and trustworthy manner. This is done by closely following development of new legislation in the area and implementing new legal requirements.

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

Compliance with legal requirements is implemented through documented policies, procedures, contracts and technical controls, and is supported by regular internal reviews and independent audits and conformity assessments. Relevant records and reports are retained and can be provided as evidence to supervisory authorities and auditors.

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.*

The trust and identity proofing services and the end-user products used to access those services including web portals and user interfaces, are designed and maintained with the aim of being accessible to persons with disabilities, where feasible.

The services comply with the national act on accessibility requirements for products and services no. 801 from 07/06/2022, and compliance is audited by a supervisory body as specified in the law. Accessibility reports for trust services and identity proofing services are updated yearly and made public via relevant websites.

REQ-7.13-04: *Applicable standards on accessibility such as ETSI EN 301 549 [i.6] should be taken into account.*

In the design, procurement and operation of end-user products and interfaces related to the trust and identity proofing services, relevant accessibility legislation, such as the national act on accessibility requirements for products and services no. 801 from 07/06/2022 is taken into account. The act is partially based on the ETSI EN 301 549 standard.

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.*

Appropriate and necessary technical and organizational measures have been implemented to protect personal data against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage.

These measures include strong access controls following “least-privilege” principles, strong authentication, encryption of data in transit and at rest, secure backup and recovery procedures, logging and monitoring of access to personal data, and secure disposal at the end of the retention period. Processing of personal data is carried out in accordance with GDPR and the Danish Data Protection Act.

7.14 Supply chain

7.14.1 Supply chain policy

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.*

Risk management is performed in accordance with ISO 27005, and supplier management risks have been identified and documented. Processes and procedures have been implemented to address security risks related to products and services from suppliers, including the ICT supply chain, for example through contractual security requirements and ongoing oversight. Supplier compliance with these requirements is regularly monitored and documented.

Additionally, the direct suppliers are required to perform a risk assessment in accordance with ISO27005 or similar frameworks for domains that fall within their scope of operations according to their contract with DIGST.

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.*

Risk management is performed in alignment with ISO 27005, which includes the identification and documentation of supplier-related risks. Processes and procedures have been defined, documented and implemented to manage the operational and information security risks arising from products and services provided by suppliers, including the ICT supply chain, for example through periodic assessments of supplier related risks, contractual security requirements and ongoing oversight. Supplier compliance with these requirements is regularly audited and documented.

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

As part of DIGST' ISMS a central supply chain policy is applied for all ICT systems, which also covers the trust and identity proofing services. For these services, DIGST acts as the service provider and system owner with overall responsibility, while external suppliers and their sub-suppliers deliver infrastructure and operational services under contract. The supply chain policy specifies that suppliers must document their use of sub-suppliers, and that supplier compliance with contractual security requirements is regularly evaluated and monitored.

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.*

The supply chain policy is documented in the DIGST ISMS and requires an assessment of the supplier's security practices, as well as the quality of the products or services delivered. In addition, it specifies that the selection criteria for selecting a supplier must include the supplier's ability to diversify sources and limit vendor lock-in.

The policy defines criteria for selecting and contracting suppliers, including:

- The supplier's established cyber security practices and secure development procedures
- The supplier's ability to meet the security requirements specified in the tender material for the procurement of new IT systems and the re-tendering of existing IT systems, including risk levels, and classification requirements
- The supplier's overall quality and resilience
- The supplier's ability to reduce dependency risks, including the diversification of supply chains to limit vendor lock-in

7.14.2 Supply chain procedures and processes

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.*

Risk management is performed in accordance with ISO 27005, and supplier management risks have been identified and documented. Processes and procedures have been implemented to address security risks related to products and services from suppliers, including the ICT supply chain, for example through contractual security requirements and ongoing oversight. Supplier compliance with these requirements is regularly monitored and documented.

Additionally, the direct suppliers are required to perform a risk assessment in accordance with ISO27005 or similar frameworks for domains that fall within their scope of operations according to their contract with DIGST.

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

Information security requirements have been defined for ICT product and service acquisitions. The security requirements are documented in the DIGST ISMS directions for supply chain management and include security requirements to be included in contracts including elements such as reporting of security incidents, change management and requirements for sub suppliers.

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.*

Supplier contracts for ICT services include requirements that suppliers must propagate information security requirements to any sub-suppliers involved in delivering the service. Contracts with sub-suppliers are required to define responsibilities for information security and to incorporate, as a minimum, the same security requirements that apply to the primary supplier.

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.*

For ICT products used to support and operate the trust and identity proofing services, supplier contracts require that the information security requirements are propagated to any other suppliers or entities involved in providing components for those products. The primary supplier is contractually obligated to ensure that its own suppliers and sub-suppliers comply with these information security requirements.

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

ICT product suppliers are requested to provide information describing the software components used in their products as part of supplier documentation. Solution descriptions include the overall components and explain the security architecture with details of how this is achieved.

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.*

ICT product suppliers are requested to provide information describing the software components used in their products as part of supplier documentation. Solution descriptions include the overall components and explain the security architecture with details of how this is achieved.

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.*

Monitoring processes and methods have been established to validate that that ICT products and services conform to stated cybersecurity requirements. This is performed through management oversight, monthly reporting on services' status and operations, and regular independent auditor's assurance reports.

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

Product and service components that are critical for maintaining functionality are identified and documented as part of the asset and configuration management process. Critical components are recorded in the asset inventory and managed accordingly. Any further details on asset identification and documentation are described under asset management (REQ-7.3.2-01X).

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

Critical components are procured only from approved suppliers and verified for authenticity and integrity upon receipt. I.e. through the validation of signatures, checksums, serial numbers, and physical inspection for tampering, etc. Software is obtained only from official sources and validated before use.

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

Assurance that delivered ICT products function as expected without unexpected or unwanted features. The components are inspected, validating that seals or packaging are not broken, security assessments, validation against specifications, performance testing prior to deployment and ultimately acceptance testing.

To maintain integrity ICT products are monitored for anomalous behaviour and applied with security patches and updates from trusted sources throughout the product lifecycle.

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

See REQ-7.14.2-11X

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.*

Direct suppliers are contractually obligated to inform DIGST without undue delay of any and all instances where potential issues or compromising events may arise. This includes events from the supplier's own subcontractors.

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

Management of component life cycles, availability and associated risks of ICT components is executed as an integrated part of asset management as described in section 7.3 above.

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

Direct suppliers are obligated to produce audit reports at least annually or when DIGST requests an audit. Audits must be conducted by an external third-party auditor. This includes monitoring and reviews of the supplier's information security practices and service delivery.

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.*

[DSS] [KMDS] Cloud services are not used in the provisioning or management of the trust or identity proofing services. Accordingly, this requirement is currently not applicable. Should it be decided to make use of cloud services in the future, a topic-specific cloud security policy will be defined, implemented and communicated to all relevant interested parties before any such services are onboarded, including how information security risks related to cloud use will be managed.

[IDK] A Cloud hosted service is used within a limited and specific scope in the provisioning of the identity proofing service MitID. Prior to implementation of the service thorough and detailed assessments and evaluations of security and data protection aspects has been carried out to ensure compliance with security policies and applicable legislation.

7.14.3 Responsibility, third parties agreements and SLA

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.*

The trust and identity proofing service providers always retains the overall responsibility for conformance with relevant requirements throughout the supply chain. This is ensured through detailed contractual agreements with direct suppliers.

The agreements allow for DIGST to review and audit any and all documentation required to conform with relevant requirements, including the option for auditors to inspect relevant documentation from the suppliers' subcontractors.

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.*

Liability of outsourcers is defined in the supplier contracts, including responsibility for security incidents, non-compliance and breach of agreed service levels. Contracts for outsourced services explicitly require outsourcers to implement and maintain the technical and organisational controls specified by the contract, including requirements on access control, logging, incident reporting, change management and management of sub-suppliers. DIGST reserves the right to obtain assurance for example through independent auditor's reports, and to require corrective actions if the agreed controls are not implemented or are found to be ineffective.

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.

Processes and procedures governing the use of suppliers' products and services are defined and implemented as part of the supplier management and specific supplier requirements are stated in the contracts and related procedures. These requirements specify

a) the activities to be performed by the TSP itself, including supplier selection and assessment, contract approval and ongoing oversight
b) the controls that suppliers must implement and demonstrate before their products or services are taken into use, such as fulfilling agreed information security requirements
c) the controls suppliers must implement at termination, including secure return or deletion of data, withdrawal of access, secure decommissioning of components and reasonable support for transition or migration

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.*

DIGST's agreements with direct suppliers clearly specifies that if the direct supplier is provisioning any subcontracting, outsourcing or other third-party arrangements, the direct supplier must include responsibilities in regard to information security in their contractual agreements with subcontractors. This also includes that the relevant requirements from the contract between DIGST and the direct supplier must also be carried on to the subcontractor.

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.*

DIGST's trust service provider Den Danske Stat does not make use of any trust service components provided by parties other than DIGST.

REQ-7.14.3-06X [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 REQ-7.14.3-05X

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.

Service agreements with direct suppliers and service providers, including cloud service providers, include service level commitments and auditing mechanisms to ensure that suppliers implement appropriate security measures addressing the contractual security requirements. Supplier security requirements and assurance activities are aligned with the risk assessment and are documented in contracts and supporting supplier management procedures.

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.

As public sector entity a strict ruleset for procurement applies and includes an evaluation of potential suppliers' compliance. Compliance with the security policies and security requirements is considered as part of the procurement and supplier selection process for direct suppliers and service providers following policy and guidelines specified in the ISMS. Relevant security requirements are identified for the procurement and are evaluated during supplier selection in accordance with the Supplier Management/Procurement procedures.

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

Applicable security policies and requirements are included in contracts with direct suppliers and service providers through contractual security clauses for new agreements and material contract changes. Where legacy contracts pre-date the current ISMS and do not fully reflect current security requirements, the contractual alignment is addressed through contract governance and applicable change management procedures.

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.

The trust and identity proofing services are governed by a central ISMS which includes a central supply chain policy. These are reviewed and updated regularly and at least annually.

For changes in the cybersecurity practices of direct suppliers, the direct suppliers are required to inform DIGST about changes in their cybersecurity practices, allowing DIGST to review and evaluate any changes in cybersecurity practices. The cybersecurity practices at direct suppliers are audited upon request by DIGST, and at least annually.

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.

DIGST maintains a register of suppliers and their agreements. The register records where information in relation to trust and identity proofing services are processed, managed and/or archived by suppliers, including relevant service descriptions and data handling locations where applicable.

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.

A register of direct suppliers and their agreements relevant to the provisioning of services is maintained. The register and associated agreements are reviewed and updated when there are changes in suppliers or agreements to confirm they remain valid and fit for purpose.

Direct suppliers are also required to maintain a register of subcontractors used in relation to the trust and identity proofing services. This register lists the supplier, contact person, and the scope of their operations.

Agency for Digital
Government