Nets DanID A/S
Lautrupbjerg 10
DK – 2750 Ballerup

Nets.eu

CVR 30808460

Nets DanID

CPS - Certification Practice Statement

Version 2.4

1 Document Details

Document details	
Document identification	Version 2.4
Document owner	CA Management
Document type	Mandatory
Update schedule	On-going – minimum yearly
Next planned update	On-going

2 Contents

3 Introduction

3.1 Overview

This document describes the practices that Nets DanID A/S as a certification authority (CA) employs in issuing, managing, revoking, renewing certificates.

The document is meant to establish the level of trust that both certificate holder, and certificate receiver may put in the reliability of the certificate and the solution behind. To do this, the document covers all relevant systems, processes, controls and procedures related to CA operations within Nets DanID and any third party, taking part in the CA and its operations.

The CA operations described in this Certification Practice Statement (CPS), covers CA management of the following Certificate Policies (CPs):

- Certifikatpolitik for OCES[1]-personcertifikater, version 4 (also denoted POCES)
- Certifikatpolitik for OCES[1]-medarbejdercertifikater, version 5 (also denoted MOCES)
- Certifikatpolitik for OCES[1]-virksomhedscertifikater, version 4 (also denoted VOCES)
- Certifikatpolitik for OCES[1]-funktionscertifikater, version 2 (also denoted FOCES)

3.2 Document Name and Identification

The document name and metadata:

Name:	Nets DanID Certification Practice Statement
Version:	2.4

Location:
http://www.nets.eu/dk-da/Service/kundeservice/NemID-til-private/Documents/CPS_2.4.pdf
and:
www.trust2408.com/repository/

3.3 PKI Participants

The PKI (Public Key Infrastructure) participants are:

Certification authorities
Nets DanID is the main Certification Authority under this CPS.

Nets DanID A/S
Lautrupbjerg 10
DK – 2750 Ballerup
www.nets-danid.dk
CVR 30808460

Nets DanID A/S is a fully owned subsidiary of Nets A/S.

Nets DanID A/S operates as a certification authority under the registered company names of Trust2408 A/S and Nets eSecurity A/S.

[1] OCES - Offentlige Certifikater til Elektronisk Service

The operation in Nets DanID, Aarhus uses 2 different trustworthy time sources: GPS and Frankfurt Standard Frequency Radio Station (DCF77). The operation in Nets DanID, Ballerup uses Public NTP in Germany: Physikalisch Technische Bundesanstalt, Germany "Telephone Time Service" (49) - 5 31 51 20 38.

Subscribers
Subscribers to certificates within this CPS are limited to the following groups:

- Danish citizens
- Legal Danish residents
- Users of Danish internet banking systems which can obtain a OCES certificate
- Employees of Danish registered companies and public institutions
- Danish registered companies and public institutions

3.4 Certificate Usage

3.4.1 Appropriate certificate uses

The following table illustrates how the certificates issued by the CA, may or may not be used:

Certificate usage	OCES personcertifikater	OCES medarbejder-certifikater	OCES virksomheds-certifikater	OCES functions-certifikater
Signing of messages	+	+	+[*]	+
Authentication of author / sender	+	+	+[*]	+
Protection and verification of integrity	+	+	+[*]	+
Encryption of data	+	+	+	+
Entering into a legally binding agreement	+	+	+[*]	
Maximum validity period	4 years	4 years	4 years	4 years

3.4.2 Prohibited certificate uses

Certificate issuing:

User-certificates under this CPS may not be used to sign other certificates. Note that this does not include certificates issued to CA’s controlled by Nets DanID.

Qualified certificates:

OCES certificates may **not** be used as a qualified certificate as defined in Annex II of the European Committee Directive 1999/93/EC.

3.5 CPS Administration

This CPS is administered by the Compliance Manager in Nets DanID. The CPS will be updated if changes to the Certificate Policies or our on-going risk assessments stipulate the need and is approved by CAM.

The Compliance Manager can be contacted via mail at info@danid.dk.

[*] Only allowed when the certificate is **not** bound to a person.

3.6 Definitions and Acronyms

CP - Certificate Policy

A Certificate Policy is a set of rules that specify requirements for the issuance and use of the certificates in one or more specific contexts in which there are common security requirements.

The supervisory authority develops and manages the certificate policies for POCES, MOCES, VOCES and FOCES.

CA - Certification Authority.

A Certification Authority is a physical or legal person/identity who is authorized to generate, issue and manage certificates. Nets DanID represents the CA.

CPS - Certification Practice Statement

A Certification Practice Statement is a detailed set of rules governing the CA’s operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA. The CPS represents Nets DanID’s principles and procedures used when generating, issuing and managing certificates.

In terms of the controls that an organisation observes, the method it uses to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used.

The CPS describes the processes and controls on how Nets DanID as a CA will comply with the Certificate Policies. The CPS also describes Nets DanID’s practices in governance and control of the processes for issuing, managing, revoking, renewing certificates. Processes and controls has been defined to provide reasonable assurance that the control objectives in the Certificate Policies will be achieved and undesired events will be prevented or detected and corrected.

The CP states *what* is to be adhered to, while the CPS states *how* it is adhered to.

RA - Registry Authority

The Registry Authority is a legal entity who is responsible for identification and authentication of a (future) certificate holder. Banks and municipalities represent the RA function.

4 CA governance

4.1 CA structure

The CA is structured and organised with focus on the CA operation, activities and processes. The personnel have adequate training, qualification and experience within the CA operation and processes. This includes the design and implementation of the organisational setup, roles and adequate segregation of CA duties.

The CPS and its CA processes (appendix A) focus on the design and implementation of administrative and management procedures to support the CA operation and activities.

Outsourcing of IT services are used in various degree. The CA processes (appendix A) takes into account the governance and control of a subcontractor which the CA enters into an outsourcing agreement with. A CA cannot outsource the responsibility to a third part.

4.2 Values and principles

Nets DanID is governing IT, RA processes and customer services with offset in the **COBIT** (version 4.1) framework. The organisation is following a corporate defined IT Security Policy, based upon the ISO 27001 (version ISO/IEC 27001:2013) ISO 27002 (version ISO/IEC 27002:2013) standard, and is running it's IT operations in accordance with ITIL (version 3) practices.

Nets DanID has chosen good and best practices that best support our role as CA.

COBIT

Nets DanID consider COBIT (Control OBjectives for Information and related Technology) as good practices for governance and control of IT. COBIT provides a common understanding of good IT management objectives and is the generally accepted internal control framework for IT.

The framework provides a reference process model and common language to view and manage IT activities. It provides a generic process model that represents all the processes normally found in IT functions, providing a common reference model. It acts as an integrator of more detailed international IT standards and best practices such as ISO 27002 and ITIL.

To govern IT effectively, it is important to understand the tasks and risks within IT that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor. Within the COBIT framework, these domains are called:

- Plan and Organise (PO). Provides direction to solution delivery (AI) and service delivery (DS).
- Acquire and Implement (AI). Provides the solutions and passes them to be turned into services.
- Deliver and Support (DS). Receives the solutions and makes them usable for end users.
- Monitor and Evaluate (ME). Monitors all processes to ensure that the direction provided is followed.

Nets DanID has utilised COBIT as a framework and foundation in the design of the processes and controls to ensure completeness and end-to-end view of the processes and controls. Requirements from the Certificate Policies and applicable standards and best practices have been incorporated in the relevant processes and controls. Additional key control objectives from COBIT have been incorporated as appropriate.

ISO 27002

ISO 27002 is an information security standard and provides best practices on information security management. The Nets Group IT Security Policy is based upon the ISO 27002 security standard. As a fully owned subsidiary to Nets, Nets DanID adopted Nets' IT Security Policy. Additional information security procedures have been applied in Nets DanID where the on-going risk assessments have stipulated the need.

ITIL

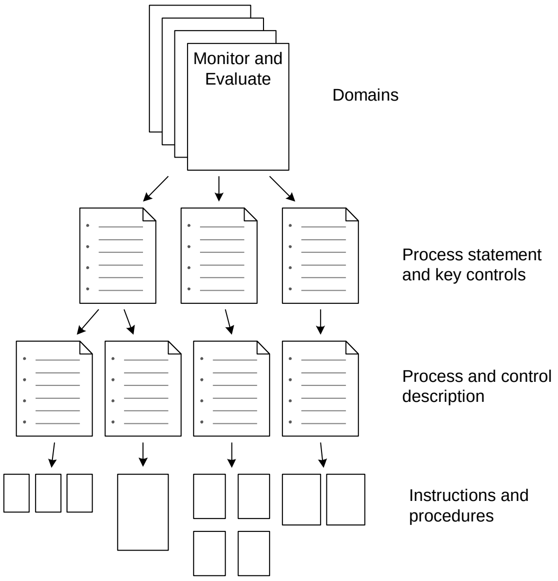
ITIL (Information Technology Infrastructure Library) provides best practices on IT service management. ITIL is process oriented and scalable to the IT organisation. Relevant ITIL practices have been incorporated into the process and control descriptions, instructions and procedures.

4.3 Governance domains

The CPS processes are structured according to the COBIT domains:

- Plan and Organise (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluate (ME)

This governance model is reflected in the CPS document hierarchy as shown in the model to the right.


Monitor and Evaluate
Domains
Process statement and key controls
Process and control description
Instructions and procedures

Domains

High level governance structure. This structure covers all processes that support our role as CA.

Process statement and key controls

Purpose and intention of the process and the associated key controls for the process.

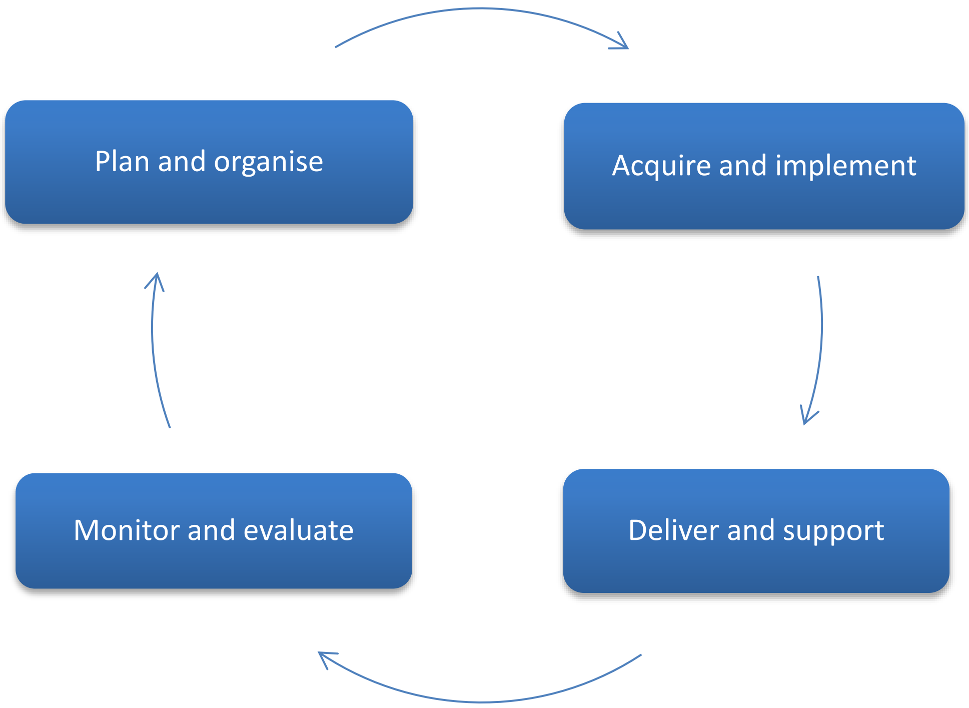
Process and control description

Detailed description of the operational compliance to the applicable process and controls.

Instructions and procedures

Detailed description of the operational procedures and guidelines, e.g. configuration, rules and parameters.

Procedures are detailed step-by-step tasks that must be performed to achieve the specific controls.



Four domains, 29 processes

4.3.1 Plan and Organise

Plan and Organise (PO) is the groundwork for managing, organising and controlling IT and all CA operation security. The domain covers all management planning within IT and other CA disciplines having security aspects.

Planning and organising is about looking ahead, preparing for what comes next and creating the structures to support work in the three other domains. The domain provides direction to solution delivery (AI) and service delivery (DS).

Planning for the future must take off from the present, the lay of the land so to speak, thus this domain relies upon crucial and valuable knowledge received from the Monitor and Evaluate (ME) domain; an iterative process. Besides the input from the ME domain, this domain also covers any analytic work required to make proper planning and governance.

It is within this domain, that quality is aligned with business needs, thus the domain also covers the overall governance of all CA processes.

The overall management of CA operation security are performed from a risk based approach. In this way, the effectiveness of assessing risks is the key to managing and balancing the right level of security and control in all CA operations and processes.

CA processes within the domain:

1. CPS management
2. CA termination management
3. Insurance management
4. Identification and authorisation management
5. Manage human resources
6. Assess and manage risks

4.3.2 Acquire and Implement

Acquire and Implement (AI) lays the groundwork for how new IT solutions, processes, vendors and sourcing partners are acquired, approved and implemented.

The domain covers both new acquisitions as well as changes to existing ones, whether these are developed, bought, taken over or otherwise acquired. The domain provides the solutions and passes them to be turned into services (DS).

All changes and new implementations must be approved at the appropriate level in the organisation. Approval must be based on a successful quality review including (risk) assessment of the required security controls.

The concept of the domain addresses three distinct actions, namely: acquiring, approving and implementing. These actions or duties are always segregated to personnel in different jobs, functions and departments within the CA.

CA processes within the domain:

1. Acquire and maintain application software and infrastructure
2. Enable operation and use
3. Procure IT resources
4. Change management
5. Release management

4.3.3 Deliver and Support

Deliver and Support (DS) defines how the daily operation, service and support are done. This is basically all day to day CA activities related to running the systems and supporting the customers. The domain receives the solutions and makes them usable for the customers.

The main objective within the domain is to deliver reliable and secure operations and customer services.

DS is the key factor in ensuring confidentiality, integrity, availability and authenticity, why these are an important part of most processes within.

CA processes within the domain:

1. Define and manage service levels
2. Manage third-party services
3. Performance and capacity management
4. Continuity planning
5. Ensure systems and infrastructural security
6. Access control

7. Security incident management
8. Customer service management
9. Problem & incident management
10. Configuration management
11. Data management
12. Physical security and management
13. Operation management
14. System termination management
15. Cryptographic key management

4.3.4 Monitor and Evaluate

Monitor and Evaluate (ME) is about awareness and defines how and what to monitor and measure. The domain is focusing on detecting problems in regards to an effective, reliable and secure operation and support.

This includes both automatic and manual controls, and covers detection, analysis, assessment and reporting.

ME is managements eyes and ears, and is in that respect a crucial part throughout CA management. In this way it also functions as the foundation for the first domain PO. The domain monitors all processes to ensure that the direction provided is followed.

The domain is in no way limited to only monitoring the running systems and services, but is also covering internal and external processes; quality of the controls associated with processes, services and systems; regulatory compliance and internal and external audit.

CA processes within the domain:

1. Internal control management
2. Compliance management
3. Audit management

4.4 Process statements and key controls

Appendix A defines Nets DanID’s processes and key controls supporting the role as a CA.

To summarise the definitions:

Process statements – why do it
Key controls – what to do
Process documents – how to do it

Process statements describe the overall purpose and intention of each process. The process statements have been designed using the COBIT framework as a foundation. This is to follow good practices along with completeness and end-to-end view of all CA processes.

Key controls define the most important security measures implemented in each process. As a total they represent the control environment for Nets DanID in the role of CA. The key controls are designed to meet the external requirements (e.g. CP and DS-484) and conform to chosen standards and internal requirements within Nets DanID.

The process statements are also referring to which standards and requirements each key control comply with. These are identified as the following sources:

Source	Description
CP	Requirements from Certificate Policies
DS-484	Reference or requirements aroused from CP
COBIT	Additional control objectives from COBIT
CA	Additional requirements raised by CA Management

Process documents

For each process statement there is at least one matching process document containing detailed description of the operational process and its associated controls. This includes detailed operational procedures, guidelines and instructions.

These processes, procedures, guidelines and instructions are incorporating existing Nets processes where possible.

The specific process documents are listed in the process statement together with any associated configuration, network design, security setup, rules, documentation, agreements and parameters.

5 Organisation and responsibilities

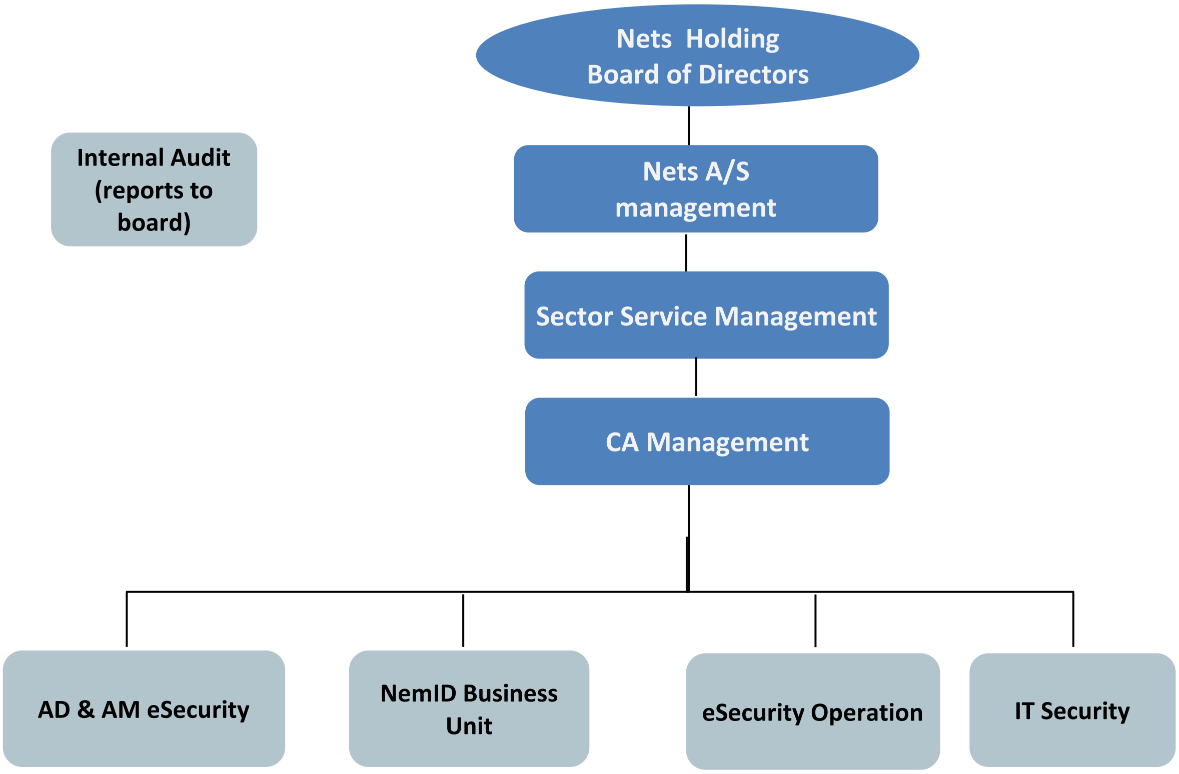
5.1 CA Management

CA Management is responsible for the management and leadership of Nets DanID and is responsible and accountable for ensuring the compliance to the Certificate Policies.

CA Management is responsible for the strategies and policies related to Nets DanID as CA.

Strategic coordination with External Audit is performed through the CA Management.

The CA organisation and its interaction with Nets is shown in the diagram below:



5.2 Security

The security responsibilities of the CA are handled as follows: IT Security covers operational security, i.e. handling of security incidents and managing internal security control. CPS compliance, risk management and governance is managed by the Business Unit.

The Compliance Manager is responsible for the administration of the CPS and validation of compliance to the Certificate Policies.

Coordination with External Audit is performed through the System Audit Manager.

5.3 Approval of CPS documents

The following responsibilities and duties are mandatory in connection with the approval of CPS process documents:

Who	What
Process owner (Operation)	• Implementation and communication of process documents after CA Assurance approval. • Quality assurance of prepared/changed process documents prior to review and approval by CA Assurance. • Owner of process documents.
Process Manager	• Development, preparation and maintenance of process documents on the basis of the process statements and key controls. • Implementation, running and maintenance of processes as

Who	What
	described in the process documents after CA Assurance approval.
Compliance Manager	• Review and recommendation to CA Management about final approval of process documents according to process statements and key controls. • Development, preparation, maintenance and approval process statements and key controls. • Assessing requests for CPR control exceptions and presenting them to CA Management for approval.

Owner, author and approver of CPS documents are as follows:

Level	Document type	Owner and author	Approver
Strategic	CA strategies and policies	CA Management	Board of Directors
Tactical	• CPS and related documents • Process statements • Key controls • Security standards and guidelines	Compliance Manager	CA Management
Conceptual	Process and control description	Process Owner/ Process Manager	CA Management
Operational	Instructions and procedures	Process Manager	Process Owner

6 Other Business and Legal Matters

6.1 Privacy statement

Our privacy principles are:

- That certificate holder own their personal data;
- That certificate holder has the right to delete their data (with respect to Danish law);
- That personal information is never shared with third parties without the certificate holders informed consent;
- That certificate holder will be given prior notice on issues affecting their information;
- That CA will comply to The Danish Act on Processing of Personal Data and other applicable statutory regulation;
- That CA will take adequate and reasonable steps to assure that information collected is accurate and secure from unauthorized access and use.

All personal data is considered both private and confidential, and is treated as such. Due to the nature of certificates, the privacy and confidentiality of any personal information contained with the certificate depend on how and where the certificates will be used by the certificate holder.

CA will protect the privacy and confidentiality as far as possible, but for any personal information contained within the certificate, the certificate holder will be responsible for handling this information with care.

Certificate holder of Personal certificates (POCES) choose full anonymity to thirds parties by leaving name, address information and e-mail out of the certificate.

CA and RA will ensure that confidential and/or private information is protected from compromise and shall not use confidential and/or private information beyond what is required for operation of the CA.

The CA is managed and operated on the basis of best practices and are subject to external audit and internal security compliance review.

The solution is built upon the principle of sole control by the certificate holder.

Nets DanID’s Privacy Policy is published on:

http://www.nets.eu/about-nets/terms-and-conditions/nets-danid-privatlivspolitik

Privacy conditions in connection with NemID are published on:
https://www.nemid.nu/dk-da/om_nemid/regler/

7 Appendix A – CA processes

1. Plan and Organise (PO)

1.1 CPS management

Process statement

The Certification Practice Statement (CPS) is a key component in establishing the degree of assurance or trust that can be placed in certificates issued by CA. The CPS and CA report are mandatory documents in issuing and operation of certificates. Other statutory and mandatory sub-documents are required to support the total publication and reporting to the supervisory authority. This requires the implementation of effective change, quality and approval procedures for the CPS, CA report and supporting documents.

Key controls

ID	Control	CP	DS-484	COBIT	CA
1.1.1	Change and quality management of CPS and CPS documents	6.1 7.1			
1.1.2	Yearly review of CPS				X
1.1.3	Yearly preparation of CA report	5.4 5.5			
1.1.4	Ensure CA report documents which requirements regarding enhanced security measures as stated in DS-484 have been implemented as a fact.	7.4.1			
1.1.5	Integration of CA organisation chart into CPS	7.4.1			
1.1.6	Integration of educational documentation into CPS	7.1 7.5			
1.1.7	Integration of Liability (insurance) coverage in the CA reporting and CPS	6.4			
1.1.9	Yearly overall evaluation of CA financial stability/-strength	7.1 7.5			
1.1.10	Dispensation to CPS compliance can only be given by prior approval by CA managements.				X
1.1.11	Major changes to NemID must be approved by CA Management				X
1.1.12	Accountability and responsibility of all CPS processes must be approved by CAM				X

1.2 CA termination management

Process statement

In case of termination of CA services, CA must ensure the continuous operational service of CRL and request of revoke. CA must also ensure that archived logs, applications, backup and data are available at least 6 years after the expiry of the last certificate was issued.

Key controls

ID	Control	CP	DS-484	COBIT	CA
1.2.1	Information to national supervisory authority and hosted customers.	7.4.9			
1.2.2	Stop of CA services.	7.4.9			
1.2.3	Information to stakeholders, certificate holders and hosted customers.	7.4.9			
1.2.4	Continuous operation and maintenance of revocation and revocation lists.	7.4.9			
1.2.5	Storage (safekeeping) of assets.	7.4.9			
1.2.6	Transfer and migration to other CA.	7.4.9			X
1.2.7	Storage (safekeeping) of old logs, application, backup and data.	7.4.9			

1.3 Insurance management

Process statement

Liability insurance coverage and policy is a mandatory document in issuing and operation of certificates. Yearly review procedures are required to support the requirement and adequate liability insurance coverage.

Key controls

ID	Control	CP	DS-484	COBIT	CA
1.3.1	Yearly evaluation of liability insurance policy of minimum coverage of 10 mill. kr.	6.4			
1.3.2	Verify periodically that CA does not limit its liability in relation to private citizens	6.4			

1.4 Identification and authorisation management

Process statement

The need to maintain the confidentiality and integrity of information and protect IT assets requires an identification and authorisation management process. This process includes establishing and maintaining procedures for identification, verification, documentation, acceptance, authorisation and handling of user identities. Reverse procedures must be applied for revocation of user identities. Also, the process addresses effective education of RA and subcontractors.

Key controls

ID	Control	CP	DS-484	COBIT	CA
1.4.1	User acceptance of Terms and Conditions including documentation	7.3.1 7.3.4 6.2			
1.4.2	Delivery of information material from ?? 3.8 "Educate and train users"	6.3 6.2			
1.4.3	Verification, logging and recording identity of applicant	7.3.1 6.1			
1.4.4	Review the Terms & Conditions concerning identification requirements	7.3.1			
1.4.5	Regular review of procedure for issuing certificates	7.3.5 7.3.3			
1.4.6	Integration of RA and subcontractors agreements into CPS	7.1			
1.4.7	Monitoring reaction times when issuing certificates	7.3.1			
1.4.8	Regular review of procedure for revoking certificates	7.3.6			
1.4.9	Verify adherence to rules regarding certificate revocation	7.3.6			
1.4.10	Tracking the recording of users acceptance of Terms & Conditions	7.4.11			X
1.4.11	Accurate and thorough recording of applicants data	7.3.1			
1.4.12	Prior to inclusion of an e-mail address in an end user certificate, the e-mail address must be verified. As a part of the verification an e-mail with unpredictable data must be sent to the e-mail account and the end user must prove knowledge of the data before the certificate is issued.				X
1.4.13	Ensuring communication/information to the certificate holder about the user obligations, including requirements to safe user behaviour.	6.2 6.3			

1.4.14	Identify needs for education and training for RA and subcontractors.			DS7.1	
1.4.15	Execute and document education and training for RA and subcontractors.	7.5		DS7.2	

1.5 Manage human resources

Process statement

A competent workforce is acquired and maintained for the creation and delivery of (IT) services. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.

Key controls

ID	Control	CP	MRTD	DS-484	COBIT	CA
1.5.1	Check of criminal record at time of employment and on-going verification of its validity	7.4.3		8.1		
1.5.2	Verify identity of new employees			8.1		
1.5.3	Production and maintenance of SAP master data and organizational diagram in CPS	7.4.1		6.1		
1.5.4	Registration and updating of the employees qualification level. Line managers are responsible to secure qualifications throughout performance evaluation	7.5		8.2.2		
1.5.5	The line manager is responsible for ensuring the sufficient education and training of the employees	7.5		8.2.2		
1.5.6	Clean-up at end of employment			8.3	PO7.8	
1.5.7	On-going follow-up on employee satisfaction levels					X
1.5.8	Appropriate disciplinary sanctions shall be applied to personnel violating CA and IS policies or procedures		5.3			
1.5.9	Development of training plans is a line manager responsibility.	7.4.7				

1.6 Assess and manage risks

Process statement

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of internal risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is made clear to the stakeholders, to enable stakeholders to align internal risks to an acceptable level of tolerance.

Key controls

ID	Control	CP	DS-484	COBIT	CA
1.6.1	Security Risk Assessment		4.1		
1.6.2	Security Risk Handling		4.2		
1.6.3	Establishing Risk Assessment Methodology (including identification, assessment and response)			PO9	
1.6.4	Establishing approval of Risk Assessment Methodology			PO9	
1.6.5	Verification of Risk Assessment Methodology compliance			PO9	
1.6.6	Assess political risks, including whether CA appears trustworthy	7.5	4.1		
1.6.7	Monitor medias				X
1.6.8	Dialogue with Management		4.2		X

2. Acquire and Implement (AI)

2.1 Acquire and maintain application software and infrastructure (IT)

Process statement

Applications are made available in line with requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This also includes the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is on-going technological support for business applications. This also requires the compliance to statutory requirements and best practices.

Key controls

ID	Control	CP	DS-484	COBIT	CA
2.1.1	Secure requirements from ISO/IEC 15408 about the products sufficient protection profile is observed	7.4.7			
2.1.2	Secure a management approved plan for build in security in the systems and infrastructure, before any development and purchase.	7.4.7			
2.1.3	Create and approve design requirements when development of systems and infrastructure (Focus on CIA (Confidentiality, Integrity & Availability) and multilayer).		12	AI2.2 AI3.2	
2.1.4	Secure key handling and storage herby is done according to the requirements in CP.	7.2.8			
2.1.5	Approval of security in special designed systems and solutions.	7.4.7	12.5.1		
2.1.6	Cryptographic modules must fulfil the requirements in FIPS 140-2 level 3, CWA 14167-3 or higher. (FIPS - Federal Information Processing Standards).	7.2.1 7.2.2			
2.1.7	Verify that strong encryption between the sites is applied – end-to-end.			DS5.11	X
2.1.8	Document the security justifications for the chosen design - what is the rationale for the design – critical security decisions.				X
2.1.9	Changes to authentication and signing protocols must be approved by AMT before changes can be made in code				X
2.1.10	Development and execution of implementation plans	7.4.7			

2.2 Enable operation and use

Process statement

Knowledge and information about systems is made available. This requires the publication and/or notification of mandatory documents, lists or information.

Key controls

ID	Control	CP	DS-484	COBIT	CA
2.2.1	Publication and communication of terms and conditions.	4.2			
2.2.2	Communication of requirements, terms, period of validity, rights of use and instructions to the users.	5.3 6.2 6.3 7.2.3 7.3.1 7.3.4 7.4.10			
2.2.3	Publication of the CPS.	7.1			
2.2.4	Publication of the public Nets DanID key from the root certificate.	7.2.3			
2.2.5	Notification of the certificate holders before certificate expiry.	7.3.2			
2.2.6	Notification of the certificate holders of locking of certificate.	7.3.6			
2.2.7	Knowledge transfer to operations, RA, sourcing partners and support.			AI4.4	
2.2.8	Distribution of CP and communications of any amendments/changes to RA.	6.1			
2.2.9	Time to process order, renewal and blocking.	7.3.1 7.3.6 6.1 7.1			
2.2.10	Timely notification and publication.	7.3.2 7.3.6			

2.3 Procure IT resources

Process statement

IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup and demands of contractual arrangements, and the acquisition itself. This also requires that security and audit conditions are incorporated into the contracts.

Key controls

ID	Control	CP	DS-484	COBIT	CA
2.3.1	Ensure that when contracting with suppliers a security and/or legal evaluation and approval is performed. All NemID agreements must be evaluated according to Nets legal checklist.			AI5.2	
2.3.2	Procurement maintains a list of subcontractors agreements.	7.1			
2.3.3	Ensure the supplier's obligation to comply with our security requirements, policies and CPS. Procurement ensures security and risk requirement are integrated in contracts according to Nets legal checklist.			AI5.4	X
2.3.4	Ensures that the conditions about the right to perform audit and security review are incorporated into the agreements according to Nets legal checklist.	5.6			X
2.3.5	Ensure formal and signed agreements with all subcontractors.	7.5			
2.3.6	Ownership of the relation to the individual supplier.			DS2.2	

2.4 Change management (IT)

Process statement

All and any changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed, documented and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment. The change management process must be linked up to the quality management process to ensure integrity in the production environment.

Key controls

ID	Control	CP	DS-484	COBIT	CA
2.4.1	Draft and maintain Change Management procedures concerning any type of change, patch or release.	7.4.7	10.1.2		
2.4.2	Ensuring adherence to Change Management procedures. Only authorized changes are introduced to the live environment.	7.4.7	12.5.1 10.1.2		
2.4.3	Ensuring application scanning and test (including security test) before releasing new versions to the live environment.	7.4.7			
2.4.4	Ensuring review of source code by independent third party.	7.4.7			
2.4.5	Ensuring procedures concerning emergency changes, patches and releases.			AI6.3	
2.4.6	Ensuring that all changes, releases and patches are recorded in the Service Change Management system.			AI6.4	
2.4.7	Perform impact analysis and prioritisation of all changes, patches and releases.			AI6.2	

2.5 Release and deploy management (IT)

Process statement

New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout, ownerships and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes. This also requires that security requirements and conditions are built-in in the design phase.

Key controls

ID	Control	CP	DS-484	COBIT	CA
2.5.1	Initial – Year 0 – controls: 1. Formal agreement with the supervisory authority. 2. Ensure that the CA root keys are not compromised. 3. Ensure that the cryptographic modules for certificate and information signing are not compromised during installation. 4. Ensure that the generation of CA's root keys and other private keys are done under dual control and monitored by two persons with trusted functions within CA. 5. Successful and approved KSC (Key Signing Ceremony) and documentation hereof. 6. Execution of IS audit and receiving of audit statement (RS 3411 type A). 7. Submission of CA report and audit statement to the supervisory authority. 8. Receivable of statement of compliance ("overensstemmelseserklæring") from the supervisory authority.	5.4 5.5 5.6 7.2.1 7.2.2 7.2.7			
2.5.2	Check the security environment concerning applications (refer to ISO/IEC 15408) - e.g. FIM status, hardening, IDS, file permissions, IP-filters.	7.4.7			
2.5.3	Establish training plans.	7.5			
2.5.4	Define data quality and privacy requirements. Define internal controls (approval) of data quality and privacy in the test environment.			AI7.4	
2.5.5	Establish a test plan addressing CIA (Confidentiality, Integrity & Availability) and design requirements.	7.4.7			
2.5.6	Ensuring a secure testing environment separated from the production environment.	7.4.7			
2.5.7	Establish an implementation plan, deployment included.	7.4.7			
2.5.8	Assess the solution or change regarding potential requirement for external accreditation.	5.6 6.1		AI7.7	
2.5.9	Ensure system ownership.				X
2.5.10	Obtain approval of the solution or change.			AI7.8	

ID	Control	CP	DS-484	COBIT	CA
2.5.11	Ensure data ownership.			DS11.6	
2.5.12	Ensure product ownership.				X
2.5.13	Ensure that any backdoors (Maintenance hooks) are removed during development or change.				X
2.5.14	Only one trusted build server must be used. The trusted build certificate must be exchanged with KMT using the standard CPS procedures. The build server must be approved by KMT, SSO and Compliance Manager.				X
2.5.15	Secure a management approved plan for building security into the systems and infrastructure, before any (critical) feature and maintenance release.	7.4.7			X
2.5.16	For security reasons all exchange of source code, documentation and other confidential material shall be coordinated and approved by SSO and Compliance Manager.				X

3. Delivery and Support (DS)

3.1 Define and manage service levels

Process statement

Effective communication between (IT) management and (business) customers regarding services required is enabled by a documented definition of an agreement on (IT) services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between (IT) services and the related (business) requirements.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.1.1	Measurement and reporting of Service Level fulfilment.			DS1.5	
3.1.2	Maintenance of SLAs (Service Level Agreements) and OLAs (Operational Level Agreements).			DS1.2 DS1.3 DS1.4 DS1.6	
3.1.3	Development of SLAs and OLAs			DS1.3 DS1.4	
3.1.4	Service Level Management			DS1.1	

3.2 Manage third-party services

Process statement

The need to assure that services provided by third parties (suppliers, vendors and partners) meet requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party IT agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the risk associated with non-performing suppliers.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.2.1	Define, maintain and follow up on security KPI's (Key Performance Indicators).			DS2.4	
3.2.2	Risk management of the supplier, including follow up on risks from the risk management by the supplier.			DS2.3	X
3.2.3	Monitoring and management of performance for suppliers, including control and follow-up on the suppliers compliance with the security related requirements.			DS2.4	
3.2.4	Distribution of CP and communications of any amendments/changes to sourcing partners	6.1			
3.2.5	Define, maintain and follow up on security KPI's.			DS2.4	
3.2.6	Ownership of the relation to the individual supplier.			DS2.2	
3.2.7	Risk management of the supplier, including follow up on risks from the risk management by the supplier.			DS2.3	
3.2.8	Monitoring and management of performance for the subcontractors.	7.3.1		DS2.4	

3.3 Performance and capacity management (IT)

Process statement

The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.3.1	Performance and capacity monitoring in general (logon, usage, ordering, revocation, revocation lists, notification.	7.3.1 7.3.2 7.3.6		DS3.5	
3.3.2	Performance and capacity planning.			DS3.2 DS3.3 DS3.4	

3.4 Continuity planning

Process statement

The need for providing continuous business services requires developing, maintaining and testing business continuity plans. An effective continuous service process minimises the probability and impact of a major (IT) service interruption on key business functions and processes.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.4.1	Maintenance and test of business continuity plans.		14	DS4.4 DS4.5	
3.4.2	Development of business continuity plans.		14	DS4.2	X
3.4.3	Development and maintenance of Business Impact Analysis.			DS4.1	
3.4.4	Verification of procedures for handling of revocation lists in case of disaster.	7.4.8			
3.4.5	Notification of critical events.	7.4.8			
3.4.6	Information to supervisory authority of irregularities in logging and yearly reporting.	7.4.11			
3.4.7	Development of IT disaster recovery plans.			DS4.2	X
3.4.8	Maintenance and test of IT disaster recovery plans.			DS4.4 DS4.5	
3.4.9	Development and maintenance of IT disaster procedures.	7.4.4		DS4.8	
3.4.10	Verification and test of disaster recovery procedures.	7.4.8		DS4.8	
3.4.11	Identification and management of SPOF (Single Point of Failure) hereunder critical services.				X
3.4.12	Reporting of test results of the IT disaster recovery plans.				X

3.5 Ensure systems and infrastructural security

Process statement

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents. This also requires the compliance to statutory requirements and best practices.

Key controls

ID	Control	CP	DS-484	COBIT	Nets security standard	CA
3.5.1	Regular execution of security tests on systems and infrastructure, at least on an annual basis.			DS5.5		X
3.5.2	Documentation and material regarding security to be classified as confidential.	7.4.11		DS5.7		
3.5.3	Ongoing maintenance and update of the anti-virus software on servers and clients.		12.6	DS5.9		
3.5.4	Ensure that network and telecommunication in Nets operate as expected to enable different security levels in different network zones and to uphold the confidentiality, integrity and availability of the network.		10.6	DS5.10	13.1.1	
3.5.5	Verify that cryptographic modules adhere to requirements as stated in FIPS 140-2 level 3, CWA 14167-3 or higher.	7.2.1 7.2.2				
3.5.6	Verify that strong encryption between the sites is applied – end-to-end.			DS5.11		X
3.5.7	Provide input to CA report documents which requirements regarding enhanced security measures as stated in DS-484 have been implemented as a fact.	7.4.1				
3.5.8	Patch management	7.4.5	12.6			
3.5.9	Verify that separation between zones is intact (logically and physically).					X

3.6 Access Control

Process statement

Access management is the process of granting authenticated and authorised users the right to access IT Assets and information systems, while preventing access to non-authorised users. Access must follow principle of least privilege and only be granted on a need-to-know basis when it is a prerequisite to perform the individual's job function.

Key controls

ID	Control	CP	DS-484	COBIT	Nets security standard	CA
3.6.1	Basic and enhanced requirements in DS-484 are to be adhered to, concerning access to systems, data and network.	7.4.6	11		9.1.1	
3.6.2	Maintain functional separation between highrisk IT-functions, e.g. Development and Operations.		10.1.3 10.1.4	DS5.4		
3.6.3	Functional separation is to be reflected in access rights.		10.1.3	DS5.4		
3.6.4	Yearly review and approval of access rights by the Product Owner/Manager.			DS5.4		
3.6.5	Regular (biannual) review of privileged users access rights, including access rights for Hardware Security Modules and investigate corrective action in case of violations.	7.2.5 7.2.7 7.2.8				X
3.6.6	CA and subcontractors must at all time maintain a list of personnel that have logical and physical access to central IT premises.		DS12.3			

3.7 Security Incident Management

Process statement

Security incident management is the process of handling security incidents. A security incident is a single or a series of unwanted or unexpected security events that have compromised security (confidentiality, integrity or availability). The objective is to identify and resolve security incidents quickly and effectively, minimise their business impact and reduce the risk of similar incidents occurring.

ID	Control	CP	DS-484	COBIT	Nets security standard	CA
3.7.1	Security Logging, monitoring	7.4.11	10.10	DS5.5	18.1.3	
3.7.2	Handling of security incidents	7.4.11			16.1.1	

3.8 Customer service management

Process statement

Timely and effective response to user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.8.1	Protection against Social Engineering - prevent, detect and correct.			DS5.9	
3.8.2	Ensure confidentiality, integrity and authenticity of the transmission and recording of sensitive/personal information.			DS5.11	X
3.8.3	Service desk - requests from customers and certificate holder.	7.5		DS8.1	
3.8.4	Detection and traceability of customer inquiries.			DS8.2	
3.8.5	Follow up on pending user/customer matters according to SLA.			DS8.4	
3.8.6	Identity checks for identification of users/customers.	7.3.1			

3.9 Problem & incidents management

Process statement

Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process maximises system availability, improves service levels, reduces costs and improves customer convenience and satisfaction.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.9.1	Information to supervisory authority.	5.6 7.4.11			
3.9.2	Information to certificate holder.	7.4.8			
3.9.3	Escalation and handover procedures.			DS8.3	
3.9.4	Upon suspicion of insider involvement, the investigation of such is transferred to the related legal department.				X
3.9.5	Identification, classification of incidents, problems, events and security breaches.		13	DS10.1	
3.9.6	Problem/incident handling, solution and tracking.			DS10.2	
3.9.7	Problem/incident closure and follow up.			DS10.3	
3.9.8	Production of Incident Reports and/or Root Cause Analysis (RCA) relating to critical breakdowns.			DS10.2	X
3.9.9	Test of incident response plans.	7.4.8			

3.10 Configuration management (IT)

Process statement

Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues more quickly.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.10.1	Basic and enhanced controls from DS-484 are to be adhered to concerning identification and classification of IT assets.	7.4.2	7		
3.10.2	Handling of cryptographic modules is according to the regulations within CP section 7.4.	7.2.7			
3.10.3	Initiate and maintain a repository containing IT assets and the configuration addressing Development and Operation.			DS9.1	
3.10.4	Maintain, verify, document licenses, especially licenses regarding OCES CA certificates.		15.1.2	DS9.3	
3.10.5	Review the integrity in the configuration.			DS9.3	
3.10.6	Establishing configuration baselines concerning specific systems.			DS9.1	
3.10.7	Controlling that systems are configured according to baseline.			DS9.1	

3.11 Data management

Process statement

Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of data. This also requires the classification and protection of data.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.11.1	Definition of backup intervals, scope and number of generations.	7.4.11			
3.11.2	Definition and maintenance of procedures for data backup and data restore.			DS11.5	
3.11.3	Access Management (controls are to be adhered to DS-484).	7.4.6	7.1.2		
3.11.4	Categorisation and protection of data according to guidelines for data classification.	7.4.2	7.2	DS11.6	
3.11.5	Deletion of privacy data when requested by citizen (The Act on Processing of Personal Data, §35)				X
3.11.6	Verify and document adherence to all requirements in CP section 7.4.11.	7.4.11			
3.11.7	Document and maintain measures according to (Bekendtgørelse 2000-06-15 nr. 528 §3, stk. 2, "Krigsbortskaffelsesbestemmelsen").				X
3.11.8	Backups must be handled and stored according to standards in DS-484, CP 7.4.11 and The Act on Processing of Personal Data.	7.4.11	10.5		X
3.11.9	Data located elsewhere must fulfil the same security requirements as the main system, including data in operation as well as data which is backed up.	7.4.4			
3.11.10	Backup copies of the CA's private keys, must be stored in cryptographic modules (FIPS 140-2 level 3).	7.2.2			
3.11.11	Verify and test data restoration.			DS11.5	
3.11.12	Verify backup performance.			DS11.5	

3.12 Physical security and management

Process statement

Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel. This also requires the compliance to statutory requirements and best practices.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.12.1	Preparation and maintenance of overview over CA site(s) and premises.	7.4.4			
3.12.2	All in scope premises used for CA functions must be classified as special security area according to DS-484 section 9.	7.4.4	9		
3.12.3	All in scope premises must have an outer security protection equivalent to DS-471 - or better.	7.4.4			
3.12.4	Security guard must be available 24 hours a day.	7.4.4			
3.12.5	Access to and stay in the central CA IT premises must be video monitored and logged.	7.4.4 7.4.11			
3.12.6	Physical security and controls must be adequate to support the CA activities and tasks.	7.5			
3.12.7	Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, vandalism, power outages, chemicals or terror.			DS12.2	X

3.13 Operation management (IT)

Process statement

Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operation management helps maintain data integrity and reduces delays. The process also requires the production of relevant documentation, guidance and manuals for users and administrators, and provides training to ensure the proper use and operation of applications and infrastructure.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.13.1	Basic and enhanced requirements in DS-484 section 10 must be complied with in relation to management of the operation of IT systems and networks.	7.4.5	10		
3.13.2	Production and maintenance of procedures for the management and monitoring of the operation of IT systems and networks.	7.5			
3.13.3	Production and maintenance of procedures for the planning and execution of jobs.			DS13.2	
3.13.4	Development and maintenance of operation manuals including operation documentation.			DS13.1	

3.14 System termination management (IT)

Process statement

Controls must be in place to ensure that confidential and/or secret data are protected against exposure in connection with system termination. All equipment with storage media containing confidential and/or secret data or applications must be physically destroyed through a controlled process.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.14.1	Destruction of confidential and private material		9.2.6		
3.14.2	Destruction of keys in HSM (Hardware Security Module) modules and destruction of HSM modules.		9.2.6		
3.14.3	Destruction of disc, CD-ROM's etc.		9.2.6		
3.14.4	Formatting of mobile medias.		9.2.6		

3.15 Cryptographic key management

Process statement

Key management determines that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys and certificates to ensure the protection of keys against modification and unauthorised disclosure.

Successful key management is critical to the security of a cryptosystem. In practice it is the most difficult aspect of cryptography because it involves system policy, user training, organisational and departmental interactions, and coordination between all of these elements. This also requires the compliance to statutory requirements and best practices. It is a key process in establishing the degree of assurance or trust that can be placed on certificates issued by CA.

Management and operation of cryptographic modules must be performed with participation of at least two people, each with its own trusted and segregated function within CA. This dual access and user's sole control are vital concepts within key management.

Key controls

ID	Control	CP	DS-484	COBIT	CA
3.15.1	Ensure generation and transport of private keys.	7.2.1			
3.15.2	Establishment of procedures for handling of cryptographic modules and follow-up on yearly basis.	7.2.7			
3.15.3	Maintenance of FIPS certification of HSM.	7.2.1			
3.15.4	Ensure the quality, integrity and protection of the root key.	7.2.1 7.2.2			
3.15.5	Handling and storage of keys according to the requirements in CP section 7.2.8.	7.2.8			
3.15.6	Verify compliance to ETSI SR 002 176 v 1.1.1.	7.2			
3.15.7	Verify compliance to newest version of DS-844 (Specification for qualified certificates)	7.3.3			
3.15.8	Verify that generation, storage, backup and transport of private keys are done under dual control by two persons with trusted functions.	7.2.1 7.2.2			
3.15.9	All handling of cryptographic modules are performed under dual control by two persons with trusted functions.	7.2.7			
3.15.10	Verify that citizens/private keys cannot be exported from the cryptographic modules.			DS5.8	X
3.15.11	Verify and control keys for code signing.				X
3.15.12	CA's private keys must have a fix validity period.	7.2.6			
3.15.13	CA must ensure that within the expiration of the private keys a new CA key pair is generated.	7.2.6			

ID	Control	CP	DS-484	COBIT	CA
3.15.14	Verify that management and handling of citizens/private keys on the Central Signature Server (CSS) are done according to the directions/requirements.				X

4. Monitor and Evaluate (ME)

4.1 Internal control management

Process statement

Establishing an effective internal control programme requires a well-defined monitoring process. This process includes monitoring and reporting of control exceptions, results of self-assessments, self-control and thirdparty reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations. It is also a key process in establishing the degree of assurance or trust that can be placed on certificates issued by CA.

Key controls

ID	Control	CP	DS-484	COBIT	CA
4.1.1	Completing and following up on internal/external security test performed by independent 3rd party (incl. Penetration test, scans, code reviews).			ME2.5	
4.1.2	Setting up and maintaining control awareness programs.			ME2.4	
4.1.3	Setting up and maintaining self-assessment programs - self monitoring.			ME2.4	
4.1.4	Remediation upon critical violations and deviations on internal controls, including preventive actions.			ME2.7	
4.1.5	Verify independent internal security compliance function.	7.4.1			
4.1.6	Vulnerability assessment of log procedure.	5.6			
4.1.7	Verify use of trustworthy time source and description of which type is applied.	6.1 7.1			
4.1.8	Control of that recognized systems and products are being used which are protected against changes.	7.4.7			

4.2 Compliance management

Process statement

Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response and obtaining assurance that the requirements have been complied.

Key controls

ID	Control	CP	DS-484	COBIT	CA
4.2.1	Verification of compliance to 'The Act on Processing of Personal Data' and other requirements in POCES CP section 7.4.10.	7.4.10			
4.2.2	Ensure that the identity documents determined/issued by the supervisory authority are known and available to applicable parties. The documents are published on www.digitalsignatur.dk.	7.3.1			
4.2.3	Verification that the OCES certificates are in compliance to the specifications listed in POCES CP section 7.3.3	7.3.3		ME3.3	
4.2.4	Ensure that CA report, audit protocol, CPS, supporting documents and liability (insurance) coverage are prepared and reported to the supervisory authority.	5.5		ME3.4	
4.2.5	Preparation and reporting of the quarterly Risk Assessment Report to the supervisory authority.				X
4.2.6	Verification of compliance to CP's, WebTrust and DS 484guidelines/standards.			ME3.1	
4.2.7	Verification of overall compliance between CPS and external requirements.			ME3.2	
4.2.8	Verification of overall compliance to IT Security Policy and CPS.		15.2	ME3.3 DS5.1	
4.2.9	Verification of compliance to applicable statutory requirements or regulation.		15.1		
4.2.10	Ensure that RA's and subcontractors are kept up-to-date and informed about current standards, policies and guidelines.				X

4.3 Audit Management

Process statement

Establishing an effective governance and assurance programme requires a well-defined internal and external monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments, self-control and third-party reviews. A key benefit is to provide assurance regarding effective and efficient operations and compliance with applicable laws, regulations and contractual requirements. It is also a key process in establishing the degree of assurance or trust that can be placed on certificates issued by CA.

Key controls

ID	Control	CP	DS-484	COBIT	CA
4.3.1	Yearly preparation of CA Management statement.	5.5			
4.3.2	Ensure planning and execution of the OCES audit including reporting to the supervisory authority.	5.6		ME4.7	
4.3.3	Planning and execution of the Netbank audit.			ME4.7	
4.3.4	Planning and execution of the WebTrust audit/certification.			ME4.7	
4.3.5	Evaluation of the need for additional audit statements from other subcontractor.			ME4.7	
4.3.6	Ensures that the right to audit, audit statements and security requirements are incorporated into the outsourcing agreements.	5.6			
4.3.7	Self-monitoring and control of subcontractor's compliance to security requirements, CPS and CP.	7.4.3 7.4.4 7.5 6.1 7.1 7.6		ME2.6	
4.3.8	Self-monitoring and control of RA's compliance to security requirements, CPS and CP.	6.1 7.1 7.4.3 7.4.10 7.4.11			

Page intentionally left blank