

National Standard for Identity Assurance Levels (NSIS) Version 2.1

Released (English version): 03.06.2026

1	INTRODUCTION	4
1.1	CHANGE LOG	4
1.2	PREFACE	4
1.3	INTRODUCTION	4
1.4	PURPOSE AND SCOPE	5
1.5	EXAMPLES OF ID SERVICES AND ASSURANCE LEVELS	6
1.6	TERMINOLOGY	8
1.7	REQUIREMENT FULFILMENT	14
2	LIFE CYCLE OF ELECTRONIC MEANS	15
2.1	CHAIN OF TRUST FOR DIGITAL IDENTITIES	16
3	REQUIREMENTS FOR ELECTRONIC IDENTIFICATION MEANS	17
3.1	REGISTRATION PROCESS	17
3.1.1	Application	17
3.1.2	Identity Proofing and Verification (Natural Persons)	18
3.1.3	Identity Proofing (Legal Entities)	20
3.2	ISSUING AND HANDLING OF ELECTRONIC IDENTIFICATION MEANS	21
3.2.1	The Strength of Electronic Identification Means	21
3.2.2	Delivery and Activation	23
3.2.3	Suspending, Revocation, and Reactivation	24
3.2.4	Renewal and Replacement	25
3.3	USE AND AUTHENTICATION	25
3.3.1	Authentication Mechanisms	25
4	ORGANISATIONAL AND CROSS-CUTTING REQUIREMENTS	27
4.1.1	General Requirements	27
4.1.2	Obligation to Provide Information	28
4.1.3	Information Security Management	29
4.1.4	Logging	29
4.1.5	Facilities and Staff	30
4.1.6	Technical Controls	31
4.1.7	Notification and Audit	31
5	ELECTRONIC IDENTIFICATION MEANS ASSOCIATED TO LEGAL ENTITIES	35
5.1	ISSUING OF ELECTRONIC IDENTIFICATION MEANS	35
5.2	BINDING (ASSOCIATION) BETWEEN NATURAL PERSONS AND LEGAL ENTITIES	36
6	REQUIREMENTS FOR IDENTITY BROKERS	37
7	GOVERNANCE	39
7.1	OWNERSHIP AND MAINTENANCE OF THE STANDARD	39

7.2	TERMINATION AND FOLLOW-UP	39
7.3	LIABILITY AND INSURANCE	39
7.4	COST.....	40
7.5	SHARING SECURITY INCIDENTS.....	40
8	REFERENCES	41

1 Introduction

1.1 Change log

Date	Version	Changes
03-06-2026	2.1	English version published (courtesy translation).

1.2 Preface

This document describes the “National Standard for Identity Assurance Levels (NSIS)”, the purpose of which is to create a framework for trust in digital identities and digital ID services. The standard has been prepared and is administered by the Danish Agency for Digital Government and serves as a reference framework and guideline for the work on user identity management in the Danish public sector.

NSIS is based on international standards and frameworks in order to ensure interoperability, knowledge-sharing, compliance and support for the internal market, including the [eIDAS] Regulation, the associated Implementing Regulation 2015/1502 on "Levels of Assurance" [LOA]), user management reference architecture [REF-ARK] and [ISO 29115].

In addition to this document with normative requirements, there is also a separate guide to the National Standard for Identity Assurance Levels. This guide elaborates the requirements through explanations and examples, as well as audit instructions (see Chapter 4 for more details; otherwise, the Audit Guide for NSIS (only available in Danish) can be referred to).

Note that the present English version of NSIS is a courtesy translation, which might not be 100% accurate. In case of doubt, the Danish version of the standard should be regarded as the authoritative source.

It is strongly advised that the instructions to NSIS are read together with the standard since the instructions add to the context of understanding the requirements of the standard.

On the website of the Danish Agency for Digital Government (www.digst.dk/NSIS) one can find all relevant material, Frequently Asked Questions (FAQ) and view the ‘NSIS trusted list’. Moreover, news related to the standard as well as related material will be published in the newsletter for MitID, MitID Erhverv, and NemLog-in (www.digst.dk/NSIS).

1.3 Introduction

The standard defines requirements for the strength of an authentication process, the underlying Identity assurance process and the Electronic Identification Means used, expressed as a single 'Assurance Level'. This can also be expressed as the degree of trust a service provider may have in an authenticated Identity. Below, the

terms 'Assurance Level' and 'LoA' are used below as an expression of the same property.

The standard contains a number of requirements for ID services at three different levels of assurance referred to as 'Low', 'Substantial', and 'High'. Early versions of NSIS also included the level 'Limited', but it has been removed, as it has no real significance in practice. The three levels of NSIS directly correspond to the three levels of the [eIDAS] Regulation.

NSIS allows service providers to define the requirement for the desired Assurance Level for users based on a risk assessment as described in the guide [LOA-GUID] and that the ID services that delivers the identities are measured against these levels. ID services that provide identities are measured against those levels. Hereby, risks in the business service ("risk levels") can be balanced to the strength of control mechanisms ("Assurance Levels").

The requirements targeting the three Assurance Levels include both technical, organisational, economic aspects, and revision since many factors have an impact on the trust in digital identities and ID services.

1.4 Purpose and Scope

This standard applies to national, public Electronic Identification Schemes as well as Identity Brokers handling identities for natural persons, legal entities and natural persons associated with a legal entity (including employees). The standard is made available for use for both state, municipalities, and regions and across domains (e.g. health and education) and includes both private and public providers of Electronic Identification Schemes as well as Identity Brokers. Identity management for devices and the Internet of Things is currently not covered by the standard due to lack of maturity. As these areas mature, and possibly, if an international framework for this emerges, the areas may be incorporated into NSIS if deemed appropriate. The assurance levels in NSIS furthermore only addresses core Identity, and therefore no provisions have been included for other types of attributes such as rights, entitlements, authorisations etc. In these areas, there are not yet any national standards, which establish quality requirements.

NSIS only addresses matters relating to the issuance and use of Electronic Identification Means and Identity Brokers, but there are naturally a large number of other aspects to be addressed when the overall level of information security for a business service is established, for example, authorisation, confidentiality and availability.

The requirements of NSIS are based on and in line with the [eIDAS] regulation, so that a Danish Electronic Identification scheme that fulfils a certain Level of Assurance in this standard will meet the requirements of the same level in relation to the [eIDAS] Regulation. In this respect, however, it should be noted that NSIS would be adapted to national circumstances and be more detailed than the implementation act [LOA] that defines the corresponding levels under the [eIDAS] Regulation, which on certain issues will be more general. It can moreover be noted that Lov om MitID og NemLog-in (hereafter the Act on MitID and NemLog-in) [LOV] establishes that NSIS is the national trust framework for the Danish public infrastructure.

It is not within the scope of this standard to describe additional matters relating to the responsibility of service providers in the field of information security and the choice of Assurance Level for authenticated users accessing their business service:

NSIS does not set normative requirements for service providers.

The responsibility for determining the required level of assurance and risk level for each business service (in the role as identity **recipient**) lies with the individual service provider, who is responsible for the data that is displayed and can be accessed through the service at the required Assurance Level. Reference can be made to the publication [LOA-GUID], which provides examples and guidance to service providers on how to determine the required Assurance Level using a risk-based approach. However, this guide is not normative but serves as a source of inspiration.

For organisations processing personal data, the handling of risks and controls will often be a natural extension of the obligations under the applicable regulation of processing personal data. The Danish Data Protection Agency monitors compliance with the applicable regulation of personal data.

1.5 Examples of ID Services and Assurance Levels

MitID and NemLog-in	The NemLog-in and MitID solutions work with a variety of Electronic Identification Means and identity assurance processes and therefore use NSIS as a reference framework to describe the obtained Assurance Levels of these. The Act on MitID and NemLog-in [LOV] equally utilises NSIS as a frame of reference for Assurance Levels.
Private ID services	The standard defines the conditions for a known Assurance Level which private ID services can be assessed against in relation to application in the public sector. By using a common standard, co-operation across sectors is made possible.

<p>Local Identity Provider (IdP)</p>	<p>Many organisations wish to act as an identity provider and the issuer of Electronic Identification Means for users in their own organisation. This applies for instance for municipal field where almost all municipalities have Local IdPs. Using this model, an employee's log-in to a local domain could be federated to external systems through a common broker.</p> <p>The organisations have different identity proofing processes, different systems and different Electronic Identification Means. Here, NSIS provides a standardised framework against which each Local IdP can be measured so that service providers do not need to consider the specific circumstances of each individual Local IdP, but can simply request a particular Assurance Level defined in the standard.</p> <p>In most cases, an organisation with a Local IdP will both issue local identification means to its users and expose an authentication service through which service providers can request that a user be authenticated. Thus, a typical Local IdP will need to meet the requirements in chapters 3, 4, 5, and 6 (possibly excluding 3.1.3) if it is to make statements regarding an NSIS Assurance Level.</p>
<p>FullService IdP</p>	<p>A FullService IdP is a type of Local IdP as described above that is delivered as a service to an organisation. The model is defined by the provider of the FullService IdP managing all requirements of NSIS on behalf of the organisation and taking responsibility for the identity proofing and issuance of identification means. Thus, it is not necessary for the organisation to undertake an NSIS audit before utilising the FullService IdP for authentication of employees. Note that the model presupposes that the organisation itself cannot be responsible for any of the processes that is subject to NSIS requirements (e.g. identity proofing, issuance of identification means etc.) or operate any of the systems that contribute to the fulfilment of the requirements. This means that there is a strict separation from the organisation if it is to evade an NSIS audit. If there is a shared responsibility where a service provider is responsible for some (but not all) requirements regarding a Local IdP, the organisation has to undertake an NSIS audit itself of the Local IdP, but the organisation can potentially refer to the audit report of the service provider in the NSIS audit. More details in relation to audit by use of service providers is described in the audit guide for NSIS [AG-NSIS]. As a rule, a FullService IdP will have to handle the requirements in section 3.1.3 concerning verification of identities for legal entities. These requirements ensure that the FullService IdP has verified the identity of the organisation that it delivers a service to and authenticates users on behalf of.</p>

Public health sector (Security Token Services)	In the public health sector, national services rely on the token services established within the national health IT infrastructure. Where a national authentication service based on OCES employee certificates and NIST Assurance Levels were previously in place, authentication will henceforward occur only locally or via MitID, and trust in these identification schemes will be based on NSIS. Token issuance from national trust services in the healthcare sector will continue, but these tokens will function solely as Identity Brokers (and enrich them with attributes relevant to the health sector).
Field of education	There are a number of ID services and federations established in the field of education, and educational institutions often guarantee identity of their own users through participation in identity federations. Services such as Uni-Login and WAYF act as Identity providers and Proxies which federate these Identities, and NSIS will be able to provide a common framework for trust in these.
Foreign Electronic Identification Means	<p>In the [eIDAS] Regulation, EU member states are required to mutually recognise national Electronic Identification Schemes from other member states notified to the Commission after a peer-review process. Member States' national Electronic Identification schemes are very different, but mutual trust is achieved through a common trust framework that defines a number of known Assurance Levels.</p> <p>In Denmark, an eID gateway has been established, which can, among other things, facilitate the authentication of individuals from other EU countries using their local eID when accessing Danish services with a well-defined Assurance Level.</p>

1.6 Terminology

The most important concepts used in NSIS are described below. It uses the convention that defined concepts are capitalised. The terminology is largely compatible with the Danish reference architecture for user management [REF-ARK] to ensure consistency with other work in common public user management. However, in a number of areas, NSIS needs to go into greater detail, and it should also be noted that the reference architecture uses the term 'Akkreditiv' for the term that is referred to as 'Electronic Identification Means' in NSIS and eIDAS.

Access Control	A process in a service that determines which functions and data a user can access based on the user's Identity, Attributes, roles/privileges, and the service's security policy.
Attribute	Characteristics or properties of an Entity or Identity. This can e.g. be a name, username, a pseudonym, a Social Security number, a UUID, residence, role, etc.

Authentication	A process that recognises and verifies an Identity (associated with an Entity) using an Electronic Identification Means connected to the Identity. Multi-factor authentication is an authentication process in which the Electronic Identification Means uses several Authentication factors from different categories (see below).
Authentication factor	<p>An attribute of an Electronic Identification Means that binds it to the Entity and which can be in the following categories:</p> <ul style="list-style-type: none"> (a) 'possession-based authentication factor': an authentication factor which the entity must prove to be in possession of (e.g. a physical entity); (b) 'knowledge-based authentication factor': an authentication factor that the Entity must prove to have knowledge of (e.g. a password); (c) 'inherent authentication factor': an authentication factor based on a physical feature of a natural person and which the Entity must prove to have (e.g. biometrics); <p>An Electronic Identification Means may have one or more factors.</p>
Authoritative source	Any trustworthy source that, regardless of its form, can be used to obtain accurate data, information and/or evidence that can be used to establish an Identity. Authoritative sources can take many forms such as a registers or documents (e.g. passports), depending on the context.
Attack potential	<p>An authentication mechanism cannot withstand all attacks but only attacks to a certain level. A standardised way to quantify resilience to various attacks is to rank them against attacks with a particular attack potential.</p> <p>This document uses the concepts basic, moderate and high on various attack potential. The terminology is from [ISO15408] and can be consulted for further descriptions.</p>
Dynamic Authentication	An electronic process using cryptography or other techniques to create an electronic proof that an Entity has access to or is in the possession of an Electronic Identification Means and where the evidence is altered by each Authentication process between the Entity and the system that verifies the authentication. Dynamic Authentication protects against replay attacks.

<p>Electronic Identification Means</p>	<p>A Means issued to an Entity for the purpose of online Authentication. It can be both physical and virtual and must be in the control of the Entity.</p> <p>A <i>combined</i> Electronic Identification Means consists of one or more elements, each of which can also be considered an Electronic Identification Means used in combination in order to satisfy the requirements at a higher Assurance Level.</p> <p>Note that the concept (single) Electronic Identification Means is also described as an 'Authenticator' in the American [NIST] standard - and not the concept 'Credential', which is used in [NIST] as a term for the linkage between an Identity and one or more 'Authenticators'.</p>
<p>Electronic Identification scheme</p>	<p>An electronic identification scheme is a system under which Electronic Identification Means are issued to natural persons or legal entities and/or natural persons associated with legal entities. An Electronic Identification Scheme covers all processes in the life cycle of Electronic Identification Means, including registration, issuance, use, expiration, revocation and archiving. An Electronic Identification Scheme is notified to the Danish Agency for Digital Government and may use one or more ID services to handle each process in the life cycle of Electronic Identification Means.</p> <p>The requirements for an Electronic Identification Scheme are set out in Chapters 3 to 5 and is separate from the requirements of Identity Brokers set out in Chapters 4 and 6. Thus, there is no obligation to implement both sets of requirements, one only has to fulfil the requirements of the role one chooses to notify.</p>
<p>Entity</p>	<p>A natural person or legal entity who wants access to an online service through Authentication with Electronic Identification Means. Entities can have multiple Electronic Identities - for example, a natural person can have both a private identity and multiple business (employee) identities.</p>
<p>Identity (Electronic)</p>	<p>A digital persona (user identity) represented by a set of attributes, which, for example, may represent a natural person (private identity), a legal entity, or a natural person associated with a legal entity (e.g. employee identity). An Identity can accommodate Personal Identification Data but can also be pseudonymous.</p>
<p>Identity Broker</p>	<p>An ID service that asserts (or federates) an authenticated identity to third parties based on an Authentication verified by the broker itself or by another third party. An Identity Broker does not necessarily carry out identity proofing or issuance of Electronic Identification Means and thus is separate from an Electronic Identification Scheme. An Identity Broker is a service that requires trust (acting as a trusted third party) from business services and is therefore subject to requirements in this standard.</p>

Identity Registry	A register that records trustworthy information about Entities (e.g. citizens) and is considered an Authoritative Source. Examples include the Civil Registration System (CPR) and the Central Business Register (CVR) as examples among several registries.
Identity proofing	A process in which the identity of an Entity is determined (e.g. through inspection of identity documents) and where Personal Identification Data (e.g. name and social security number or association with legal entity) is verified.
ID service	<p>A trusted service that performs one or more of the processes that are subject to requirements in this standard. This may include identity proofing, issuance of Electronic Identification Means, or an Identity Broker.</p> <p>Please note that the [eIDAS] regulation uses the concept of "trust service" on services involved in issuing digital signatures / certificates, validation of certificates validity and time stamping, which is not covered in NSIS.</p> <p>NSIS covers Chapter 2 of [eIDAS] (in particular Article 8), while trust services relate to [eIDAS] Chapter 3. An NSIS ID service must not be perceived as an [eIDAS] trust service (unless it also issues certificates, performs time stamping or some of the other functions described in Chapter 3 in the [eIDAS]).</p>
A person	A natural person or legal entity.
Personal identification data	<p>A set of data (attributes) that determines the identity of a natural person or legal entity (i.e. which uniquely identifies an Entity).</p> <p>Typically, an IdP will issue a token containing personal identification data and possibly other attributes (e.g., permissions) as the result of a successful authentication. The associated NSIS Assurance Level in the token applies only to the personal identification data and not to any additional attributes.</p>

<p>Assurance Level (LoA)</p>	<p>The degree of trust in an authenticated Identity also referred to as the level of identity assurance. Assurance Levels are described in this document as three levels referred to as Low, Substantial, and High. Requirements are set for the various sub-processes in connection with identity assurance, registration, issuance and use of Electronic Identification Means, etc. When assessing LoA, all requirements in NSIS apply (except for Identity Brokers, if such have not been part of the Authentication).</p> <p>The overall Assurance Level (LoA) can be decomposed into several sub concepts:</p> <p>Identity Assurance Level (IAL) describes the strength of the Identity proofing process. For the purpose of assessment, the requirements of Chapter 5 of Section 3.1 and the general requirements set out in Chapter 4 apply.</p> <p>Authenticator Assurance Level (AAL) describes the Assurance Level of combined Electronic Identification Means used in an Authentication. For the assessment of AAL, the requirements of sections 3.2 and 3.3 and the general requirements set out in Chapter 4 apply.</p> <p>Federation Assurance Level (FAL) describes the Assurance Level of an Identity Broker that federates/claims an Identity to third parties. For the purposes of the assessment, the requirements set out in section 6.1 and the general requirements set out in Chapter 4 must apply.</p>
<p>Service provider</p>	<p>An organisation with an IT system that users log in to by using an electronic identification means – typically via an Identity Broker.</p> <p>It is also referred to as a relying party in English. The service provider consumes the electronic identity and typically requires a specific Assurance Level before access to the service can be granted. Examples of services include borger.dk, virk.dk, or municipal case management systems.</p> <p>NSIS does not set requirements for service providers.</p>

The figure below illustrates the relationships between the important concepts of Entity, Identity, and Electronic Identification Means:

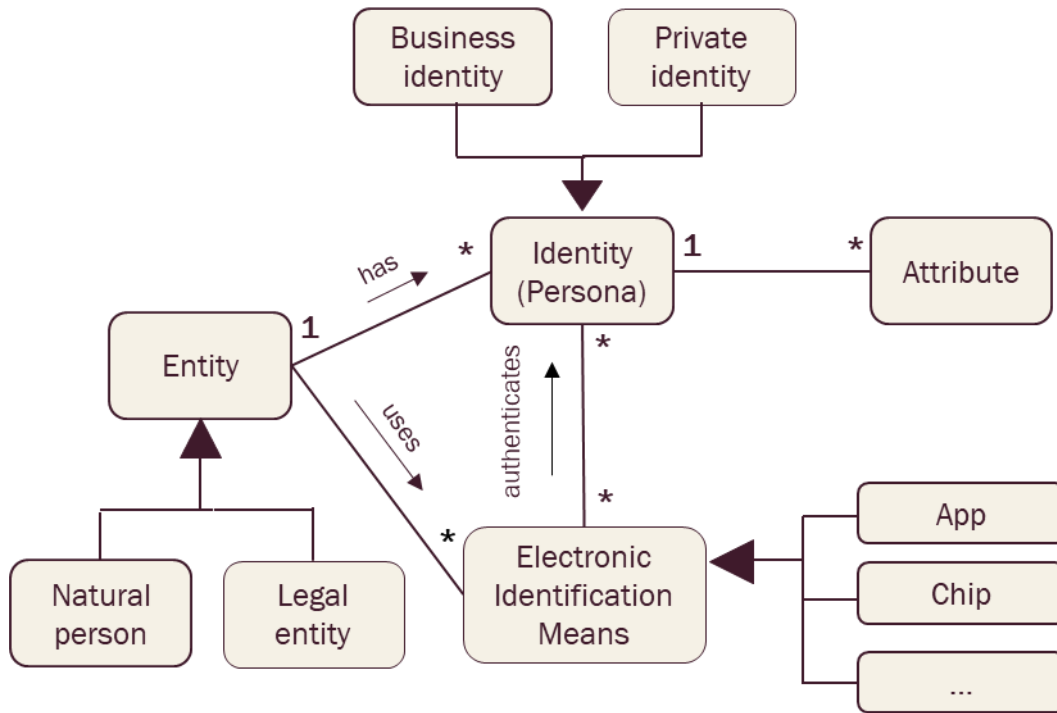


Figure 1: Relationship between the concepts of Entity, Identity, and Electronic Identification Means

The (combined) Electronic Identification Means is used by an Entity for Authentication at a given Assurance Level, while it is the individual Electronic Identification Means that is issued and administered in the life cycle of Electronic Identification Means. For example, passwords and code display in MitID can be managed separately from each other with their own life cycle.

The term "Electronic Identification Means" thus refers to both the combined Electronic Identification Means and the individual Electronic Identification Means, depending on the context of use (Authentication) or issuance / administration.

The below figure illustrates the relationship between the terms Entity, Identity, and Identification Means:

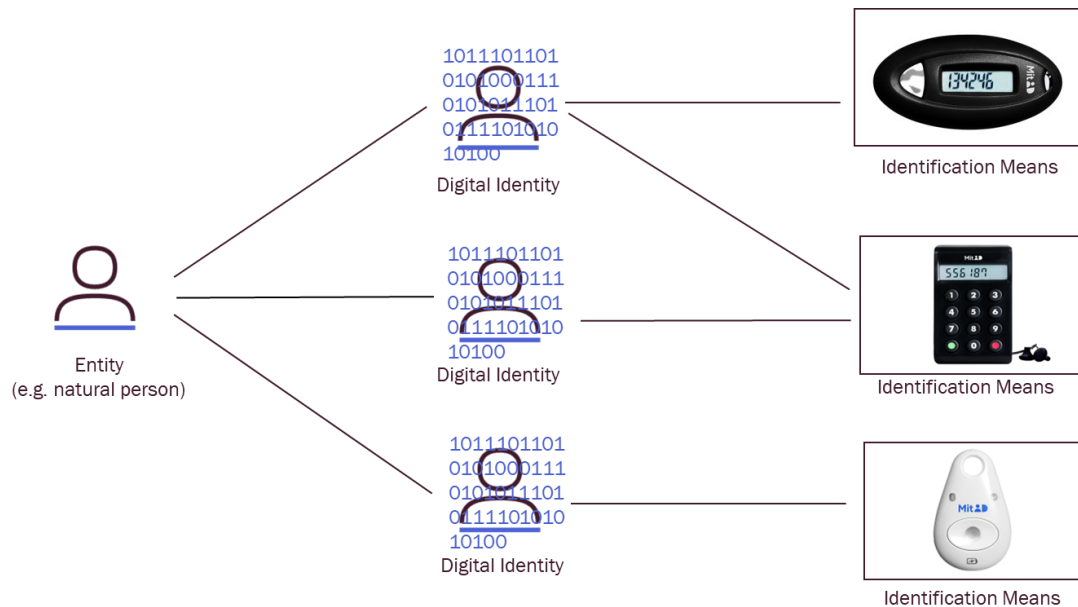


Figure 2: Core terms

1.7 Requirement Fulfilment

Where several requirements are specified at a given Assurance Level in this standard, all requirements for the given Assurance Level must be fulfilled unless it is explicitly stated that this does not apply. In addition, requirements of a lower Assurance Level must always be fulfilled in order to establish a hierarchy and a progression throughout the three Assurance Levels. The overall Level of Assurance (LoA) is dictated by the minimum Assurance Level achieved in the specific areas below. In other words, all requirements for the level 'Substantial' must be fulfilled before an Electronic Identification Scheme can be stated to fulfil NSIS at level 'Substantial'.

The requirements are written in an 'outcome-based' way so they mainly address the results of certain controls and processes (the desired quality level) rather than dictating the way to achieve the concerned Assurance Level. This allows for different technologies and solutions and is also the approach taken in [LoA]. However, there are deviations from this approach, so in reality the requirements in NSIS are a mix of several approaches.

2 Life Cycle of Electronic Means

The requirements described in the subsequent chapters target different phases of the life cycle of Electronic Identification Means – in relation to their registration, issuance and use. In order to create an understanding of the context of these requirements, it is useful to begin with an overview of the overall life cycle of Electronic Identification Means.

Different actors/services may handle the individual phases of the life cycle. For example, the registration in MitID solutions can be made in cooperation between the Citizens' Service (In Danish 'Borgerservice'), the Civil Registration System and the MitID supplier. The issuance is carried out by the MitID supplier (on behalf of the Danish Agency for Digital Government and the banks), the authentication process can be communicated by the NemLog-in solution (in the role of an Identity Broker), while the security context and authorisation can be established in borger.dk by access to a citizen-oriented service. Note that the notification of the overall Electronic Identification scheme must cover all aspects.

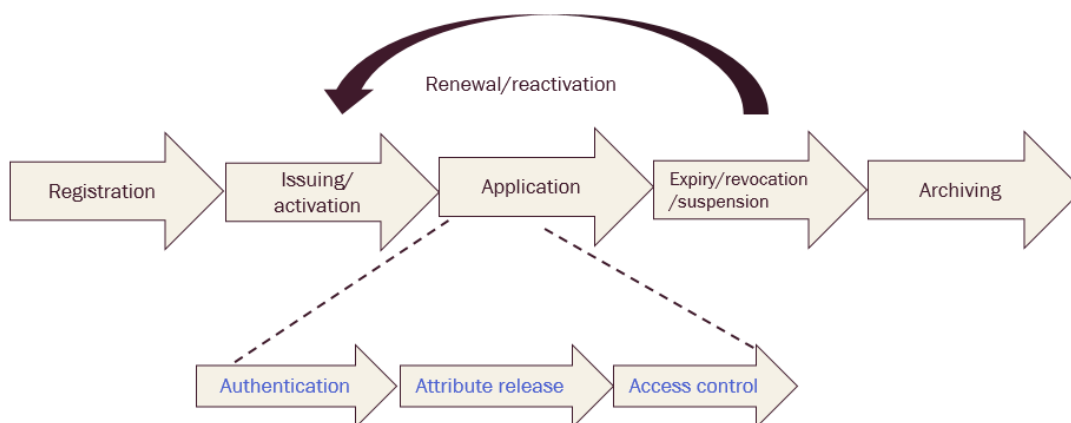


Figure 3: Life cycle of an Electronic Identification Means¹

Below is a short summary of the life cycle for an Electronic Identification Means:

- *Registration* - a process in which the Entity (user) applies for an Electronic Identification Means and identity proofing is performed.
- *Issuing* - a process in which an Electronic Identification Means is issued and handed over to the Entity.
- *Activation* - a process in which the Entity activates or prepares the Electronic Identification Means for use.
- *Application* - the processes in which the Entity uses its Electronic Identification Means for Authentication (or, where applicable, signing) in online services. This can form the basis of other processes such as release of attributes, access control, etc.

¹ NOTE: The purpose of the figure is to give the reader an overview of the different stages - the structure is reflected in the chapters with the normative requirements, but there is not a complete one-to-one relationship.

- *Expiry* - an event where an Electronic Identification Means naturally expires and no longer can be used. Not all types of Electronic Identification Means have a natural expiration date.
- *Suspension* - temporary blocking of an Electronic Identification.
- *Revocation* - an event in which an Electronic Identification Means is revoked permanently, for example, due to compromise.
- *Archiving* - a process in which an Electronic Identification Means or related data are stored long-term, for example in order to ensure probative value or decrypt data, etc.

2.1 Chain of Trust for Digital Identities

Digital identities are often used and conveyed through a chain of trust involving multiple parties, where the overall security level is determined by the ‘weakest’ link in the chain. All links in the chain (except for the end service provider) must comply with NSIS, allowing the service to trust the quality of the identity received – ensuring that it has not been compromised along the way.

In the example illustrated below, the chain of trust begins on the right side with the issuance of a local identification means via a Local IdP, which is NSIS certified as an Electronic Identification Scheme. The Local IdP provides an authentication service in the form of an ID service that can authenticate local users with the locally issued credentials. In the example, authentication is relayed through an additional broker (which could be NemLog-in, for instance) before reaching the business service, which, as previously mentioned, is not NSIS certified but simply determines the required security level for access.

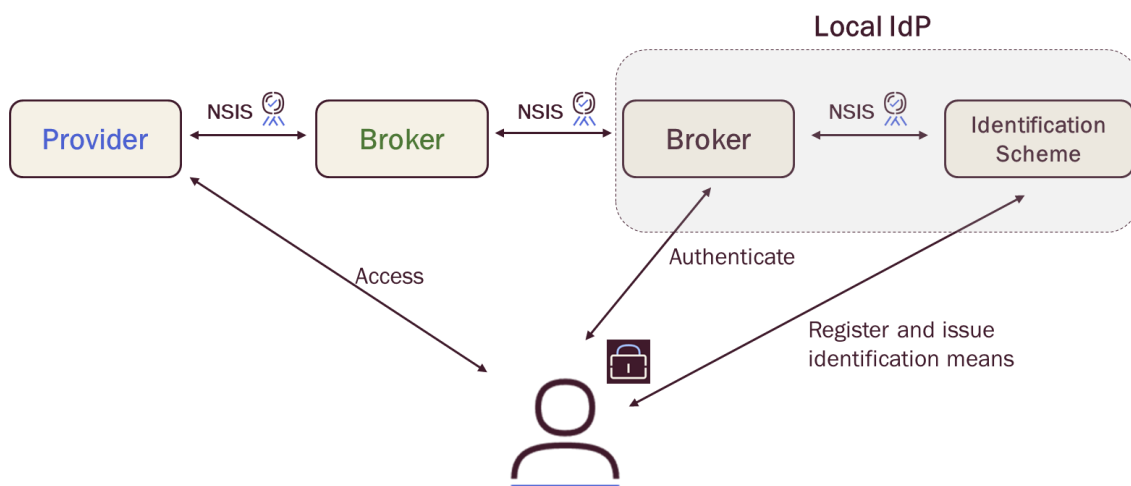


Figure 4: Example of Chain of Trust

3 Requirements for Electronic Identification Means

This chapter contains normative requirements for the issuance of Electronic Identification Means and their application in authentication process based on [eIDAS] and [LoA]. As the requirements target different steps in the life cycle, not all requirements will be relevant to all ID services – the following is the combined number of requirements.

3.1 Registration Process

This section covers requirements for Identity Proofing of an applicant, including validation and verification of the Identity prior to issuing the Electronic Identification Means. The level of Identity Assurance achieved, as described in the table below, is called IAL (Identity Assurance Level). The term 'applicant' refers to the natural person or legal entity who wishes to obtain an Electronic Identification Means.

3.1.1 Application

The following describes requirements for the application process. It should be noted that when issuing Electronic Identification Means in companies, an explicit application is not necessarily made if an Electronic Identification Means was issued automatically as part of the recruitment process. In such cases, the requirements must be fulfilled anyway.

Assurance Level	Requirements
Low	1) The applicant must be made aware of the conditions for the use of the issued Electronic Identification Means. 2) The applicant must be made aware of the required security measures related to the use of Electronic Identification Means. 3) Relevant data required for identity proofing and verification are collected in a trustworthy way.
Substantial	4) The applicant must accept conditions and to declare having read them.
High	Same as level Substantial.

3.1.2 Identity Proofing and Verification (Natural Persons)

This section covers the requirements for identity proofing of natural persons. The requirements in the table below relate to issuance based on non-electronic documentation.

Generally, it is permitted to base the identity proofing on an Authentication with a valid Electronic Identification Means on at least the same Assurance Levels with respect to eIDAS or NSIS. In this case, the requirements below will be not relevant. The Electronic Identification Means does not have to be issued by the same issuer, but it must be verified that the Electronic Identification Means in question is valid and not revoked.

If the electronic identification means used does not include all personal identification data necessary for the issuance of the new identification means, the missing personal identification data must be secured in accordance with the requirements below, and the overall Assurance Level must be adjusted according to the lowest Assurance Level achieved for all personal identification data.

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) A verification process must be carried out, and a description of the verification process must be available, including the prerequisites used. 2) The applicant (Entity) must with a high degree of probability, be in possession of generally accepted evidence of the claimed identity. 3) The documentation can be assumed genuine and valid.

Assurance Level	Requirements
Substantial	<p>4) It must be verified that the applicant has nationally recognised photo or biometric evidence of the claimed identity (e.g. passport or driving license). In situations where the applicant is not in possession of this, the identification processes used for the issuance of a Danish passports or driving licenses can be used.</p> <p>5) The documentation is verified to make sure it is genuine or that it is known according to an authoritative source that the documentation exists and is related to a natural person.</p> <p>6) Steps have been taken to minimise the risk that the identity of the person in question is not the claimed identity, taking into account the risk that the documentation submitted may have been lost, stolen, suspended, revoked or expired. The identity of the applicant must be validated according to an authoritative source and, to the extent possible, steps must be taken to ensure that the applicant is not marked as dead or disappeared.</p> <p>7) If manual checks are performed, only specially trained personnel who have received relevant instruction in verifying the authenticity of documentation and detecting fraud can perform these.</p> <p>8) If another person than the applicant carries out the registration, this person must be authenticated at Assurance Level Substantial or High.</p>
High	<p>9) The applicant can be identified as having the alleged identity by comparing one or more of the person's physical characteristics with an Authoritative Source. The comparison must be carried out either through physical presence or another mechanism providing equivalent assurance.</p> <p>10) There is a very high probability that there is a physical match between the applicant and the documentation presented (e.g. match of photo and signature).</p> <p>11) If a person other than the applicant carries out the registration, the person must be authenticated at Assurance Level High.</p>

3.1.3 Identity Proofing (Legal Entities)

This section describes the requirements for Identity Proofing of legal entities. The requirements in the table below refer to the re-issuance based on physical documentation.

Identity proofing of legal entities is relevant when issuing identification means to other organisations or employees of external organisations², such as when providing a FullService IdP. In these cases, it is important to ensure that identification means are issued to (business users in) the correct organisation. An example of this is the MitID Erhverv solution, which issues identities and/or identification means to (potentially) all organisations with a Danish company registration number. Here, MitID Erhverv's onboarding processes ensure that the organisation's identity is documented, and that administrators are appointed by management, before users can be created and identification means issued for the organisation.

If identification means are issued only within one's own organisation, the requirements in this section do not apply; see the guidelines on collective notifications in section 4.1.7 on notification and auditing.

Generally, it is permitted to base the identity proofing on an Authentication with a valid Electronic Identification Means on at least the same level as the Assurance Levels of eIDAS or NSIS. In this case, the requirements below will not be relevant. The Electronic Identification Means does not have to be issued by the same issuer, but it must be verified that the Electronic Identification Means in question is valid and not revoked.

If the electronic identification means used does not include all personal identification data required for the issuance of the new identification means, the missing personal identification data must be secured in accordance with the requirements below, and the overall Assurance Level must be adjusted according to the lowest achieved Assurance Level for all personal identification data.

² This means no temporary staff or consultants who are given an identity within the organisation.

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) The existence of the legal entity is documented with a recognised certificate (e.g. a registration certificate or equivalent) or by posting in the Danish Central Business Register. 2) The name, legal form and unique company registration number (CVR number) of the legal entity are clearly established. 3) The legal entity is not registered with a status that prevents the legal entity from acting as such (including bankruptcy, etc.). 4) It can be assumed that a person authorised by the legal entity carries out the registration. 5) The person carrying out the registration is authenticated at Assurance Level Low or higher.
Substantial	<ol style="list-style-type: none"> 6) Reasonable steps have been taken to ensure that a person authorised for this by the legal entity carries out the registration. The authenticity and validity of the authorisation must be verified. 7) The person carrying out the registration is authenticated at Assurance Level Substantial or High.
High	<ol style="list-style-type: none"> 8) A strong validation has been carried out to ensure that a person authorised for this by the legal entity carries out the registration. 9) The person carrying out the registration is authenticated at Assurance Level High.

3.2 Issuing and Handling of Electronic Identification Means

The table below sets out the requirements for Electronic Identification Means at the three Assurance Levels.

3.2.1 The Strength of Electronic Identification Means

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) The Electronic Identification Means must make use of at least one Authentication Factor. 2) The Electronic Identification Means is designed in such a way that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.

Assurance Level	Requirements
Substantial	3) The Electronic Identification Means utilises at least two Authentication factors from different categories. 4) The Electronic Identification Means is designed in such a way that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
High	5) The Electronic Identification Means protects against duplication and tampering as well as against attackers with high attack potential. 6) The Electronic Identification Means is designed in such a way that it can be reliably protected by the person to whom it belongs against use by others.

3.2.2 Delivery and Activation

The following table sets out the requirements for delivery per Assurance Level:

Assurance Level	Requirements
Low	1) After issuance, the Electronic Identification Means is delivered via a mechanism by which it can be assumed it is delivered only to the intended person.
Substantial	2) After issuance, the Electronic Identification Means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.
High	3) The activation process verifies that the Electronic Identification Means was delivered only into the possession of the person to whom it belongs. 4) The delivery must be protected against attacks in which the Electronic Identification Means is stolen during transport and insider attacks in the delivery function of the issuer by, for example, using two independent shipping channels or segregation of duties.

3.2.3 Suspending, Revocation, and Reactivation

The table below indicates the requirements for suspension and revocation per Assurance Level:

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) It must be possible for the user/owner of an Electronic Identification Means to suspend (temporarily prevent use) and/or revoke (permanently prevent use) in a timely and effective manner. 2) Measures must be put in place to ensure that Electronic Identification Means are not unduly revoked or suspended in an attempt to deny access of a legitimate person. 3) Reactivation must take place only if the same assurance requirements as established before the suspension or revocation to be met. 4) The issuer of an Electronic Identification Means must, on its own initiative, revoke this: <ul style="list-style-type: none"> ○ if there is suspicion of compromise or loss of control over this, ○ if errors are found in the Electronic Identification Means (e.g. incorrect data), ○ if there is no longer a valid agreement³ between the issuer and the applicant. 5) If possible, a receipt for revocation is given to the user/owner of the Electronic Identification Means.
Substantial	<ol style="list-style-type: none"> 6) Suspension and revocation function must be available 24 hours a day and have a high level of availability. 7) The issuer must revoke the Electronic Identification Means if it is found that the user/owner of the Electronic Identification Means has ceased to exist (e.g. death for natural person or bankruptcy of legal entity).
High	Same as level Substantial.

³ Legislation can replace an agreement.

3.2.4 Renewal and Replacement

The following table sets out the requirements for renewal and replacement per Assurance Level:

Assurance Level	Requirements
Low	1) Taking into account the risks of a change in a person's identification data, renewal and replacement processes needs to meet the same requirements as the initial identity proofing and verification (and recognise the risk of altered identification data) or is based on a valid Electronic Identification Means, or higher Assurance Level.
Substantial	Same as level Low.
High	2) Where the renewal or replacement is based on a valid Electronic Identification Means, the personal identification data and existence of Entity must be re-verified with an Authoritative source.

The above requirements relate to the renewal of an Electronic Identification Means in connection with the expiry of an Electronic Identification Means. If the renewal occurs before expiry of the Electronic Identification Means (e.g. because the owner has lost the original Electronic Identification Means or this is compromised), re-identification can be abstained up to level Substantial if there are strong checking mechanism that ensure that the Electronic Identification Means is issued to the same Person. An example could be that users should not have to go through the identity proofing process again if a person has forgotten his/her password.

3.3 Use and Authentication

3.3.1 Authentication Mechanisms

The table below describes the requirements for authentication mechanisms per Assurance Level where an Entity uses one or more Electronic Identification Means in an Authentication.

Assurance Level	Requirements
Low	1) The release of personal identification data is preceded by reliable verification of the Electronic Identification Means and its validity. 2) Where personal identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. 3) The authentication mechanism implements security controls for the verification of the Electronic Identification Means, so that it is highly unlikely that attacks such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
Substantial	4) The release of personal identification data takes place after a reliable control of Electronic Identification Means and its validity through a Dynamic Authentication Mechanism. 5) The authentication mechanism implements security controls for the verification of the Electronic Identification Means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulate communication by an attacker with a moderate Attack Potential can subvert the authentication mechanism.
High	6) The authentication mechanism implements security controls for the verification of the Electronic Identification Means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulate communication by an attacker with high Attack Potential can subvert the authentication mechanism.

4 Organisational and Cross-Cutting Requirements

4.1.1 General Requirements

The following table lists the general requirements for organisations that provide ID services, including Identity Brokers (see Chapter 6):

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) Organisations providing any ID services covered in this document must be registered as a legal entity in the European Union with an established organisation. The organisation must meet all requirements for the services offered, similar to the processes described in the life cycle of Electronic Identification Means (registration, issue, use, broker etc.). 2) This requirement has been removed. However, see section 7.3 regarding legal compliance. Organisations providing ID services are responsible for fulfilling obligations entrusted to third parties.
Substantial	<ol style="list-style-type: none"> 3) Organisations providing ID services must be able to demonstrate their ability to undertake the risk of liability for damages as well as having sufficient financial resources for continued operations and providing of the services. 4) Private organisations providing ID services must have a described termination plan ensuring the appropriate decommissioning or acquisition of third parties, as well as the notification of authorities and users. The plan must include details of how data are stored, protected and destroyed.
High	Same as level Substantial.

4.1.2 Obligation to Provide Information

The following table describes information requirements:

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) A service description must be published for Identity Brokers and Electronic Identification Schemes describing all relevant conditions, payments and limitations on the use of the service. The service description must include a privacy policy that meets the requirements of [GDPR]. 2) The Electronic Identification Scheme needs describe responsibility and prerequisites for users and service providers, relying on an Electronic Identification Means in relation to obtaining a given Assurance Level. This includes, for example, safety instructions for users. 3) For Electronic Identification Schemes, the conditions must explicitly require the user to: <ul style="list-style-type: none"> ○ use only the Electronic Identification Means in accordance with the issuer's policies (including password and, if necessary, password length policies); ○ does not transfer its Electronic Identification Means to others and ○ adequate and correct answers to all requests for information in the application process, as well as ○ take reasonable steps to protect its Electronic Identification Means (including by any backup) and ○ immediately request the revocation of its Electronic Identification Means in the event of a compromise or suspicion of compromise ○ immediately request the renewal of its Electronic Identification Means if the corresponding Personal identification data is no longer correct (including information provided during the registration process included in Electronic Identification Agents).
Substantial	Same as level Low.
High	Same as level Low.

4.1.3 Information Security Management

The following table describes information security management requirements for Organisations providing ID services:

Assurance Level	Requirements
Low	1) Organisations providing ID services must establish an effective information security management system (ISMS) covering the ID service in order to address risks associated with information security.
Substantial	2) The management system must comply with the principles set out in the [ISO 27001] standard. 3) A contingency plan must be available covering all essential areas.
High	4) The management system for the ID service must be certified according to the [ISO 27001] standard or similarly documentation for compliance with information security management requirements must be provided.

4.1.4 Logging

The following table sets out logging requirements:

Assurance Level	Requirements
Low	1) Relevant information must be logged and protected in accordance with applicable law and good data protection and management practices. 2) Relevant information is recorded and updated by means of an effective registration scheme that take into account applicable legislation and good practices in the field of the protection and storage of data. 3) Information (including logs) must be kept and protected as long as they are necessary for the audit or investigation of security breaches, and retention, after which the information must be securely destroyed.
Substantial	Same as level Low.
High	Same as level Low.

4.1.5 Facilities and Staff

The following table sets out requirements for facilities and staff:

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified, experienced in the skills needed to execute the roles they fulfil 2) There must be sufficient staff (possibly through subcontractors) to operate and maintain the service in accordance with the relevant policies and procedures. 3) Operating facilities must be continuously monitored for and protected against damage caused by environmental disasters, unauthorised access or other factors that may affect the safety of the service. 4) Operating facilities containing personal, cryptographic, or other confidential information must be limited to authorised personnel.
Substantial	<ol style="list-style-type: none"> 5) It must be verified that managers and employees performing trusted tasks are not punished for a crime that renders them unfit to perform their duties, as well as ensuring employees and managers have sufficient training and experience. The same applies to suppliers and subcontractors. 6) It must be documented who has had access to central operating premises. 7) Trusted access (including administrative access) to production facilities must be secured and monitored.
High	<ol style="list-style-type: none"> 8) It is necessary to ensure that access to and stay in the central operating rooms is video monitored. 9) Operating facilities must have a perimeter protection equivalent to [DS 471].

4.1.6 Technical Controls

The following table sets requirements for technical controls:

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) Reasonable technical controls exist to prevent threats to the security of services and ensure the confidentiality, integrity, and availability of the processed information. 2) Electronic channels of communication used for the exchange of personal data must be protected against interception, manipulation, and replay. 3) Access to cryptographic material used for the issuing of an Electronic Identification Means or Authentication must be limited to the roles and applications that have a strictly necessary need for access and cryptographic material must never be stored in clear text in persistent storage media. 4) Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk level, security incidents, and security breaches. 5) All media containing personal, cryptographic, or other confidential or sensitive information are stored, transported, and disposed of in a safe and secure manner.
Substantial	<ol style="list-style-type: none"> 6) Sensitive cryptographic material used for issuing of an Electronic Identification Means and Authentication must be protected from tampering. Cryptographic algorithms or protocols with known vulnerabilities or using insufficient key lengths must not be used.
High	Same as level Substantial.

4.1.7 Notification and Audit

Electronic Identification Schemes and Identity Brokers wishing to be recognised at a given Level of Assurance under this standard must notify their solution/scheme to The Danish Agency for Digital Government. The notifier is obligated to supply comprehensive information and answer supplementing questions if necessary.

If the notified solution or scheme meets the requirements in NSIS, the Danish Agency for Digital Government will publish a brief description of the solution and the achieved NSIS Assurance Level on its web page⁴. Only then, will a solution be allowed to claim a given NSIS Assurance Level for an authentication towards third parties.

The Danish Agency for Digital Government is solely responsible for ensuring compliance with the formalities surrounding the notification, including the availability of

⁴ www.digst.dk/NSIS

the required documentation (e.g. audit report). The Agency assumes no responsibility as to whether notified solutions continuously fulfil the requirements of the specified Assurance Level.

The following table sets out notification and audit requirements:

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) When notifying an Electronic Identification Scheme and/or Identity Broker to the Danish Agency for Digital Government, the technical and security design and the desired Assurance Level must be clearly described. 2) When notifying an Electronic Identification Scheme and/or Identity Broker to the Danish Agency for Digital Government, self-declaration must be used. In doing so, the notifier must issue a statement that the requirements for the specified Assurance Level (Low) are fulfilled. 3) For registration at level Low, an internal audit must be conducted covering all necessary areas of the offered services to ensure compliance with relevant requirements and policies. Additionally, at Assurance Level Low, the applicant must submit an annual management statement confirming that the original registration remains accurate and that the solution is active – or alternatively, update their registration or request removal from the list of registered solutions. If an external audit is conducted with respect to assurance levels Substantial or High, the requirement for an internal audit is waived.

Assurance Level	Requirements
Substantial	<p>4) The self-declaration is supplemented by a formal statement of compliance by an independent, approved⁵ auditor with the relevant competencies within it revision or an accredited conformity assessment body (cf. Article 3, 1, number 18 of eIDAS), which confirms that the technical and security design of the solution has been audited, that the required level of protection is achieved by the solution/scheme at the level of assurance indicated and that processes have been implemented to ensure an ongoing basis that the specified Assurance Level is Maintained. The notification must be supplemented by a management statement stating that all relevant requirements have been fulfilled and necessary processes for maintenance have been implemented. A new audit report must be submitted annually confirming that the requirements are continuously fulfilled.</p> <p>5) The auditor statement of assurance must be created in accordance with the Notification and Audit Guide for NSIS (see [AG-NSIS]). Notifier and auditor must complete the corresponding Excel sheet (or a corresponding document⁶) for level Substantial.</p>
High	<p>6) The auditor statement of assurance must be created in accordance with the Notification and Audit Guide for NSIS (see [AG-NSIS]). Notifier and auditor must complete the corresponding Excel sheet (or a corresponding document) for level High.</p>

Please note that the requirement for type 2 declarations entails that the organisation must be able to document that controls are carried out continuously over the period. This includes, for example, traceability for the creation and deactivation of users.

⁵ Approved auditor is used as a common description for both state authorised and registered auditors. The auditor needs to have the relevant professional competencies, see the audit guide for more details.

⁶ If the auditor includes, in a separate section of their statement, the controls and audit procedures outlined in the Excel sheet, this is considered sufficient.

5 Electronic Identification Means Associated to Legal Entities

This chapter describes requirements for Electronic Identification Means related to 'natural persons associated with a legal entity'. The Association covers, among others, employees in an organisation, but also other relationships where there is no employment relationship. An association (binding) can be implemented by issuance of a new, dedicated Electronic Identification Means (e.g. separate MitID Identification Means in MitID Erhverv), but may also consist of a logical linkage between a natural person and a legal entity without issuance of new Electronic Identification Means (e.g. marking of the natural person where the person is using his/her personal Electronic Identification Means in the context of the legal entity). The following are specific requirements for handling the life cycle for the binding.

5.1 Issuing of Electronic Identification Means

When an Electronic Identification Means is issued to natural persons associated with a legal entity, the same requirements as described in Chapter 3 must apply to natural persons. In other words, all Chapter 3 requirements apply, unless expressly stated below. In the case of reissuance, data from a previous Identity Assurance process can be reused (based on a risk assessment) if control mechanisms are established that minimise risks in this connection – e.g. by the nearest manager approving the employee's identity.

5.2 Binding (Association) between Natural Persons and Legal Entities

The following requirements apply to the binding between natural persons and legal entities:

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) It must be possible to suspend and/or terminate the binding for both parties. 2) The legal entity (e.g. via an administrator) has the right to suspend or revoke the binding, which may include suspending/revoking an associated Electronic Identification Means if the binding is established through this. 3) It must be ensured that the binding is removed when the association between the legal entity and natural person ceases. Examples include situations where employees are no longer employed or no longer have a work-related need to be associated with the legal entity, or in the event of bankruptcy or liquidation of the legal entity. 4) Verification of the natural person acting on behalf of the legal entity must be checked at Assurance Level Low or more. 5) The binding can be established based on authoritative data from the Central Business Register or other Authoritative Source, including the legal entity itself. 6) The natural person is not registered by an Authoritative Source with a status that prevents the natural person from acting on behalf of the legal entity.
Substantial	<ol style="list-style-type: none"> 7) Validation of the identity of the natural person acting on behalf of the legal entity must be carried out at Assurance Level 'Substantial' or 'High'. 8) The binding is established under the control of the legal entity, e.g. through a designated administrator or through information from an Authoritative source. 9) Procedures for establishing the binding have been subject to audit. 10) The binding has been verified based on a unique identification number (e.g. company registration number (CVR)) representing the legal entity and used in The Danish Business Association and based on information that uniquely represents the natural person from an Authoritative source. 11) The natural person and legal entity must be notified of the establishment of the binding.
High	<ol style="list-style-type: none"> 12) Verification of the identity of the natural person associated with a legal entity is performed at Assurance Level High.

6 Requirements for Identity Brokers

This chapter describes a number of requirements for Identity Brokers, a special kind of ID service that conveys an authenticated Identity to a third party by issuing and signing a Security Token. These are in some contexts referred to as 'Identity Providers' or 'Security Token Services'. Examples include the central NemLog-in solution that issues SAML Assertions to public service providers based on e.g. a MitID authentication. Another example is a local 'Identity Provider', which offers authentication and federation of e.g. employees in a municipality based on an authentication with a locally issued Electronic Identification Means.

Organisations that provide Identity Brokers generally must comply with organisational requirements set out in Chapter 4 at the Assurance Level to which the Identity Broker is classified. The Assurance Level of an Identity Broker is referred to as Federation Assurance Level (FAL).

In addition to the organisational requirements in Chapter 4, the following specific requirements apply to Identity Brokers:

Assurance Level	Requirements
Low	<ol style="list-style-type: none"> 1) Security tokens must only be issued after (a) a successful Authentication, (b) based on a valid authenticated session (Single Sign-On), or (c) by exchanging a valid security token from another (NSIS) Identity Broker with whom a trusted relationship is established. 2) The current NSIS Level of Assurance must be indicated in the issued token (LoA) so that the recipient of the token (relying party) can read it directly. The LoA in a token is calculated as the minimum value of the Assurance Level of the Authentication (see sections 2-5), the level of the broker's own Assurance Level (FAL) as referred to (see sections 4 and 6), as well as the Assurance Levels for any Identity Brokers used as subcontractors in the specific Authentication. It is thus the lowest Level of Assurance in the <i>authentication chain</i>, which will be the resulting Assurance Level conveyed by the Broker. 3) Token must be signed with the Broker's private key and may only be exchanged over encrypted channels. 4) The Broker's private key, which signs the security tokens, must be protected from unauthorised access. 5) Sessions with Identity Brokers must have a limited service life (automatic expiration), and it must be possible for the user to log out of all sessions at once (single log-out). 6) Sessions with Identity Brokers must be protected from takeover. 7) All requests to the Identity Broker and all responses to these must be written to an integrity-protected log.

Assurance Level	Requirements
Substantial	<p>8) Users of Identity Brokers, who rely on the Broker's Authentication, should in their request be able to opt out of Single Sign-On if the service wishes to enforce an Authentication with active user involvement (i.e. opt out SSO).</p> <p>9) The token must be limited to one or more specific services which must be explicitly stated in the token (e.g. as Audience Restriction).</p> <p>10) Tokens containing confidential or sensitive personal data and are transported through the user's browser must be end-to-end encrypted or encrypted at the attribute level so that the content is readable only to the recipient.</p> <p>11) The private key of the Broker signing security tokens must be protected from unauthorised access both from internal and external actors, and explicit key management procedures covering the full life cycle must be established.</p> <p>12) For national services⁷, the private key of the Broker signing security tokens must be placed in 'tamper-resistant' cryptographic hardware that meets the requirements of [FIPS 140-2] level 3 or equivalent.</p>
High	<p>13) The Broker's private key, which signs security tokens, is placed in 'tamper-resistant' cryptographic hardware that meets the requirements of [FIPS 140-2] level 3 or equivalent.</p> <p>14) The private key must be generated in hardware, and it must not be exportable in clear text.</p>

⁷ Services that act as brokers for arbitrary private citizens or individuals associated with arbitrary organisations. A broker that handles only one / a few organisations or an organisation's own local users is not considered national, and therefore the requirement does not apply to these.

7 Governance

This chapter describes rules for Electronic Identification Schemes as well as Identity Brokers wishing to make use of NSIS.

7.1 Ownership and Maintenance of the Standard

Like the OCES certificate policies, this standard is prepared by the Danish Agency for Digital Government, as is governed and maintained by the Danish Agency for Digital Government as a common public standard.

Major changes in the standard will be implemented with the involvement of state, municipalities and regions and based on a broad public consultation. However, the Danish Agency for Digital Government can make necessary security adjustments.

The document is versioned, and new editions are published on www.digst.dk/NSIS.

With each release of an updated version of this document, it will also be published how long the users must comply with new/changed requirements. Most often, the deadline will be at least 6 months, unless security conditions require a shorter implementation deadline.

7.2 Termination and Follow-Up

An organisation, which has notified an Electronic Identification Scheme or Identity Broker to the Danish Agency for Digital Government, is obliged to notify the Danish Agency for Digital Government immediately if one or more requirements of this standard no longer are fulfilled, if an ID service is planned to terminate, or if the Assurance Level is desired to change. In case of termination, the applicant is required to make a closing audit – the further details are described in [AG-NSIS].

The Danish Agency for Digital Government may at any time deprive an organisation of the right to refer to this standard and remove the Electronic Identification Scheme or Identity Broker from the NSIS trusted list of notified solutions, if it does not comply with the requirements of the standard. If an organisation either is deprived of the possibility of using NSIS or of it ceases to use NSIS, the organisation must, if possible, notify its service providers and users of this.

The Danish Agency for Digital Government is also entitled to contact an applicant for clarifications or supplementary explanations if the supervision becomes aware of matters of significant importance to the NSIS notification. An applicant must cooperate loyally and effectively in responding to such inquiries, and failure to cooperate may, in the most extreme case, result in removal from the NSIS trusted list.

7.3 Liability and Insurance

The organisation notifying of an Electronic Identification Scheme or Identity Broker bears full responsibility for complying with the requirements described in this standard. Moreover, it is expected to comply to the relevant laws. Electronic Identification Schemes or Identity Brokers at Assurance Level Substantial or High must assume liability under general rules of Danish law concerning holders of Electronic Identification Means and services relying on an Electronic Identification Means (relying parties), if the loss is due to:

- Information in the issued Electronic Identification Means or Security Tokens is incorrect at the time of issue, or failure to revoke on the basis of a valid request;
- Security tokens are issued in breach of the requirements of Identity Brokers in this standard;
- Failure to immediately revoke or suspend an Electronic Identification Means upon request for a revocation/suspension;
- Serious security breach caused by failure to fulfil security requirements unless it can be demonstrated that no negligence or intentional action has occurred.

The notifier prepares its contracts/agreements etc. with its counterparties and is entitled to limit the responsibilities in the relationship between itself and the counterparties to the extent that those counterparties are economic operators or public authorities. The notifier is not entitled to seek to limit its responsibilities to private citizens, as counterparties, other than those set out in that standard.

The Danish Agency for Digital Government assumes no liability for notified solutions and their design by publishing them on digst.dk.

Organisations notifying Electronic Identification Schemes or Identity Brokers on level Substantial and High must have the capacity to bear liability, which can, for example, be achieved through insurance arrangements (or self-insurance schemes for public authorities).

7.4 Cost

All costs for complying with the requirements of the standard are borne by the notifier.

7.5 Sharing Security Incidents

Notified Electronic Identification Schemes and Identity Brokers at level Substantial or High must share severe security incidents with the Danish Agency for Digital Government, as well as other relevant authorities, such as the Danish Center for Cybersecurity. This is done by reporting to an agreed contact point to the NSIS Supervisory Board within the Danish Agency for Digital Government when serious security incidents occur – including on reasonable suspicion that one or more requirements in the standard are no longer being complied with and/or that a security control is compromised. The ID service provider must also be available for a follow-up dialogue and clarification of any information to the problem from the Danish Agency for Digital Government. In the event of a security incident, users or other services (relying parties) must be informed, and relevant countermeasures must be taken, such as revoking an Electronic Identification Means etc.

The European Union Network and Information Security Agency (ENISA) has published guidelines for incident reporting (see [ENISA]), which should be taken into consideration.

8 References

- [DS-471] "DS 471:1993 – Technical prevention against Burglar Attack".
- [eIDAS] " Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework".
- [ENISA] "Technical guideline for Incident Reporting"
<https://www.enisa.europa.eu/publications/technical-guideline-for-incident-reporting>
- [FIPS 140-2] "FIPS PUB 140-2, Security Requirements for Cryptographic Modules", NIST.
<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- [GDPR] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)"
- [ISO15408] "ISO/IEC 15408-1:2009 "Information technology – Security techniques – Evaluation criteria for IT security" and ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation".
- [ISO 27001] "ISO/IEC 27001:2013 - Information technology – Security techniques – Information security management systems – Requirements".
- [ISO29115] "ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication security framework".
<https://www.iso.org/standard/45138.html>
- [LOA] " Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market".

- [NIST] "NIST Special Publication 800-63 Revision 3", NIST.
<https://pages.nist.gov/800-63-3/sp800-63-3.html>
- [DBL] "Data Protection Act" (in Danish: Databeskyttelsesloven), Ministry of Justice.
<https://www.retsinformation.dk/Forms/R0710.aspx?id=201319>
- [REF-ARK] "User management reference architecture", Agency for Digital Government (in Danish).
<https://arkitektur.digst.dk/rammearkitektur/referencearkitekturer/referencearkitektur-brugerstyring>
- [LOA-GUID] "Guidance for selecting assurance level for service providers – Version 2.0.3" (in Danish: Vejledning til valg af sikringsniveau for tjenesteudbydere version 2.0.3), Agency for Digital Government, which is published in:
<https://digst.dk/nsis/>
- [AG-NSIS] "Notification and Audit Guide for NSIS" (in Danish: Anmeldelses- og revisionsvejledning til NSIS – version 1.1.1), which is published in:
<https://digst.dk/nsis/>
- [VEJL] "Guide to NSIS version 2.5" (in Danish: Vejledning til NSIS – version 2.5), Agency for Digital Government, which is published in:
<https://digst.dk/nsis/>
- [LOV] "Act on MitID and NemLog-in" (in Danish: Lov om MitID og NemLog-in)
<https://www.retsinformation.dk/eli/lta/2021/783>