



Autoident Qualified Electronic Signature Certificate Policy (ETSI EN 319 411-2)

Version 1.3


IDnow GmbH
Auenstr. 100
80469 Munich

14.04.2021

IDnow Certificate Policy (ETSI EN 319 411-2)

Version	1.3
Date	14.04.2021
Author	Armin Bauer, IDnow GmbH (armin.bauer@idnow.de)
Security Policy	IDnow Security Policy, Version 1.6
Identification Center Infrastructure Policy	IDnow Identification Center Infrastructure Policy, Version 1.0
Data Center Infrastructure Policy	IDnow Data Center Infrastructure Policy, Version 1.0
Autoident Qualified Electronic Signature Process Description	IDnow Autoident Qualified Electronic Signature Process Description, Version 1.0
Risk Assessment Autoident QUALIFIED ELECTRONIC SIGNATURE	IDnow Autoident Qualified Electronic Risk Assessment Signature, Version 1.4
Identification Services Infrastructure Policy	IDnow Identification Services Infrastructure Policy, Version 1.0
HR Policy	IDnow HR Policy, Version 1.0
Role Concept	IDnow Role Concept, Version 1.0
Quality Management Policy	IDnow Quality Management Policy, Version 1.1

History		
Date	Version	Comment
14.04.2021	1.3	3.4: Added information how the availability of the revocation process is ensured 4.9.3: Added details what is logged regarding revocations
16.03.2021	1.2	Changed references to reflect the new documents
03.11.2020	1.1	Detailed which part of the process is done by the CA
07.10.2020	1.0	- Renamed product to Autoident Qualified Electronic Signature

DocuSigned by:

 099A322C8F74462...

DocuSigned by:

 936A2205AE20499...

Table of Contents

1. PURPOSE OF THE DOCUMENT	5
1.1. DOCUSIGN FRANCE	6
1.2. OTHER CAS.....	6
1.3. PKI PARTICIPANTS.....	7
1.3.5. OTHER PARTICIPANTS.....	7
1.5. POLICY ADMINISTRATION	7
1.5.1. ORGANIZATION ADMINISTERING THE DOCUMENT	7
1.5.2. CONTACT PERSON	8
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	9
3. IDENTIFICATION AND AUTHENTICATION	10
3.1. NAMING.....	10
3.1.2. NEED FOR NAMES TO BE MEANINGFUL.....	10
3.1.3. ANONYMITY OR PSEUDONYMITY OF CERTIFICATE	10
3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS	10
3.1.5. UNIQUENESS OF NAMES	11
3.2. INITIAL IDENTITY VALIDATION.....	11
3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY	11
3.2.3. AUTHENTICATION OF PHYSICAL PERSON IDENTITY	11
3.2.4. NON-VERIFIED SUBSCRIBER INFORMATION	12
3.2.5. VALIDATION OF AUTHORITY.....	12
3.2.6. CRITERIA FOR INTEROPERATION	13
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	13
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	13
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	14
4.1. CERTIFICATE APPLICATION	14
4.1.1. WHO CAN SUBMIT A CERTIFICATE APPLICATION.....	14
4.1.2. ENROLLMENT PROCESS AND RESPONSIBILITIES	14
4.2. CERTIFICATE APPLICATION PROCESSING	14
4.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS	14
4.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATION	15
4.2.2.2. SUBSCRIBER	16

4.3. CERTIFICATE ISSUANCE.....	16
4.3.1. CA ACTIONS DURING CERTIFICATE ISSUANCE.....	16
4.4. CERTIFICATE ACCEPTANCE	17
4.4.1. CONDUCTING CERTIFICATE ACCEPTANCE.....	17
4.5. Key pair and certificate usage	17
4.6. CERTIFICATE RENEWAL.....	17
4.7. CERTIFICATE RE-KEY	17
4.8. CERTIFICATE MODIFICATION.....	17
4.9. CERTIFICATE REVOCATION AND SUSPENSION	18
4.9.1. CIRCUMSTANCES FOR REVOCATION	18
4.9.2. WHO CAN REQUEST REVOCATION	18
4.9.3. REVOCATION REQUEST PROCEDURE	18
4.9.5. TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST	19
4.9.6 REQUIREMENTS REGARDING CHECKING THE REVOCATION FOR CERTIFICATE USERS.....	19
5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS	20
5.1. PHYSICAL CONTROLS	20
5.2. PROCEDURAL CONTROLS	21
5.3. PERSONNEL CONTROLS	21
5.3.7. INDEPENDENT CONTRACTOR REQUIREMENTS.....	22
5.3.8. DOCUMENTATION SUPPLIED TO PERSONNEL.....	22
5.4. AUDIT LOGGING PROCEDURES.....	22
5.5. RECORDS ARCHIVAL	23
5.6. Certificate renewal	23
5.7. DISASTER RECOVERY	23
5.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES.....	24
5.8. TERMINATION	24
6. TECHNICAL SECURITY CONTROLS.....	26
6.1. Key pair generation and installation	26
6.2. Private Key Protection and Cryptographic Module Engineering.....	26
6.3. Other aspects of key pair management	26
6.4. ACTIVATION DATA.....	26
6.5. COMPUTER SECURITY CONTROLS	26
6.5.1. SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS.....	26
6.6. Life cycle technical controls.....	27
6.7. NETWORK SECURITY CONTROLS	27

6.8. TIME STAMPING 28

7. CERTIFICATE, CRL, AND OCSP PROFILES 29

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 30

8.3. TOPICS COVERED BY ASSESSMENT..... 30

9. OTHER BUSINESS AND LEGAL MATTERS 31

9.2. FINANCIAL RESPONSIBILITY..... 31

9.4. PRIVACY OF PERSONAL INFORMATION..... 31

9.4.1. PRIVACY PLAN..... 31

9.6. REPRESENTATIONS AND WARRANTIES 31

9.6.3. RA REPRESENTATIONS AND WARRANTIES..... 31

9.8. LIMITATIONS OF LIABILITY..... 32

9.9. INDEMNITIES 32

9.13. DISPUTE RESOLUTION PROVISIONS 32

9.14. GOVERNING LAW 32

9.16. MISCELLANEOUS PROVISIONS 32

1. PURPOSE OF THE DOCUMENT

IDnow GmbH acts as the Registration Authority (RA) and as such identifies subscribers requesting personal signatures based qualified certificates with SSCD from a Certificate Authority (CA, CSP). IDnow only performs the identification of subscribers, if

- The subscriber and the subject are the same natural person.
- The subscriber requests the qualified certificate for signing documents on its own behalf and not on behalf of a third person.

or, if

- The subscriber is a legal person and the subject is a natural person and an authorized representative of the legal person.
- The subscriber requests the qualified certificate for signing documents on its own behalf and not on behalf of a third person.
- IDnow will not check if the subject is an authorized representative of the legal person. This check has to be performed by the CA.

This document is not a full CP itself but includes comments and explanations to proof that and how the requirements for the RA in the CA's CP are fulfilled under the standards ETSI EN 319 411-2, ETSI EN 319 411-1 and ETSI EN 319 401. As IDnow is only fulfilling the RA part, any missing chapters of this documents are considered as not applicable in the context of a RA.

For the purpose of this document there is a contact to the CA for the RA part at IDnow. This contact is responsible for the following duties:

- Report all security incidents to the CA,
- manage the changes within this document upon validation of the CA,
- control that the operational procedures regarding the RA activities are performed in compliance with the present registration policy.

IDnow performs the following four process steps to assure that the identification of a natural person online has an "equivalent assurance" to a face-to-face identification:

- 1) Check of the actual existence of the person in real life
- 2) Check whether the ID document belongs to this specific person
- 3) Proof that the present person is the same as specified before
- 4) Check the legal validity of the ID document

The process description is attached to this document.

IDnow acting primarily as Registration Service acts

- on behalf of a relying party (e.g. financial institute) to transmit documents that need a signature of the subscriber to the subscriber
- on behalf of the subscriber as an agent to request a qualified certificate to be issued by the CA,
- on behalf of the subscriber as an agent to request the electronic signature of one or more documents delivered together with the request,

- on behalf on behalf of the relying party as an agent receiving the signed documents, performing all required checks requested by the applicable law and creating a quality report allowing the relying party to identify the new customer according to the law,
- on behalf of the CA as contact place to start a revocation process

The ETSI standards cited above request in chapter 7.3.1 e) that a subscriber has to be identified either directly (face-to-face) or “indirectly using means which provides equivalent assurance to physical presence”.

The current version of the Certificate Policy and the terms and conditions can be retrieved at <https://www.idnow.io/certification-policies>.

This CP references the IDnow Security policy, the IDnow Identification Center Infrastructure Policy, IDnow Data Center Infrastructure Policy, IDnow Autoident Qualified Electronic Signature Process Description, IDnow Identification Services Infrastructure Policy, IDnow HR Policy, IDnow Role Concept, IDnow Quality Management Policy, as well as the Risk Assessment Autoident Qualified Electronic Signature. They provide further details but have been outsourced due to the sensitivity of the content. The correct version of those documents for this CP is mentioned at the beginning of this document.

1.1. DOCUSIGN FRANCE

Under this CP, IDnow can act as the RA for DocuSign France. According to the Certificate Policy of DocuSign France, DocuSign France manages the overall Policy Management Authority. The relevant OID to consider for this document is OID 1.3.6.1.4.1.22234.2.8.3.20.

According to DocuSign France’s CP document IDnow GmbH is the Customer, the Registration Authority and the Operational Authority for the RA.

The existing certificates of the Protect and Sign Personal Signature solution that DocuSign France offers as a CA do not cover the registration services but include requirements for registration authorities to be fulfilled.

1.2. OTHER CAS

Under this CP, IDnow can act as the RA for additional CAs as long as the requirements for personal signatures based on qualified certificates with SSCD or signatures issues to a legal person based on qualified certificates with SSCD are fulfilled.

1.3. PKI PARTICIPANTS

1.3.5. OTHER PARTICIPANTS

IDnow uses a supplier for the operation of the datacenter. The supplier provides the server hardware, racks, firewall, electricity, Internet, etc. IDnow then takes over at the hardware level (operating system and higher layers).

IDnow has 2 main contacts with the operator of datacenters. One for business/contract questions and one for technical questions.

In addition, there is a technical emergency hotline.

In the other direction, there is a notification system (e.g. mailing list) provided by the datacenter operators, which notifies IDnow about forthcoming maintenance work.

There is a contract that governs the commercial relationship between the datacenter operators and IDnow. The scope of services provided is regulated in this contract. There is also a commissioned data processing agreement with the associated technical and organizational measures.

Details can be found in the document "IDnow Identification Services Infrastructure Policy", section 4.4 and the document "IDnow Data Center Infrastructure Policy", section 3.

In addition to its own Identification Center, IDnow partners with other call center providers to provide the identification service.

To further improve the quality of the face recognition and liveness detection IDnow uses SDKs from experts in those fields.

There are contracts for all sub-contractors in place that regulate the scope of service and liabilities. The implemented controls that are required to provide this service are documented in the "IDnow Identification Center Infrastructure Policy", section 3 and are part of the contract.

1.5. POLICY ADMINISTRATION

1.5.1. ORGANIZATION ADMINISTERING THE DOCUMENT

This document is published and maintained by IDnow GmbH, Germany. IDnow makes its CP, CPS, publicly available through our website: <https://www.idnow.io/certification-policies/>

It is regularly reviewed at least once a year or on the basis of changes and approved by a member of the management board. The IT Security Officer is responsible for the implementation of the practices. Changes to the document will be published on the IDnow website after approval from the management board.

1.5.2. CONTACT PERSON

Address:

IDnow GmbH
Auenstr. 100
80469 Munich
Germany

Contact:

Service Desk Portal (24x7): <https://support.idnow.de>

Telephone (9am – 6pm, Low & Medium Priority only): +49 89 413 24 600 (select language -> press 3)

Email (9am – 6pm, Low & Medium Priority only): tickets@idnow.de

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The terms and conditions are shown to the Subscriber during the Consent Protocol and signed by Subscriber during the Consent Protocol and are included in the proof file.

IDnow makes its Terms and conditions publicly available through our website: <https://go.idnow.de/terms>

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

Within the Autoident Qualified Electronic Signature process, the name of the subscriber is being checked against a copy of the passport or identity document.

IDnow collects the data of the user and checks them. The following data will be collected at the minimum if applicable to the document:

- Full Name
- Place of birth
- Date of birth
- Nationality
- ID card number
- Issuing country
- Type of identity document
- Mobile phone number
- Information about the agent performing the identification
- Information when the identification was performed

Details can be found in the document “IDnow Autoident Qualified Electronic Signature Process Description” section 3.4. The allowed documents for identification can found in section 3.7.

3.1.3. ANONYMITY OR PSEUDONYMITY OF CERTIFICATE

All names are real names and have been checked against evidence in form of a copy of the passport or identity document. Anonymity or pseudonymity will not be accepted by IDnow.

3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

The subject name must contain the full name of the subscriber. The name used is the name of the subject at the time the certificate was issued. The name will always be taken from the identity document used to identify the subscriber.

RA name is contained in the DN of the Subscriber.

3.1.5. UNIQUENESS OF NAMES

The uniqueness of each subject name is ensured by providing the full name of the subscriber as well as a unique transaction number.

In addition, IDnow stores additional tokens:

- A transaction number provided by the client which enables the signed documents to be linked to a request from the client
- An internal transaction number from IDnow which allow to uniquely identify the process in the systems of IDnow.

These unique tokens are linked to the signature transaction for one or more documents.

Details about this process can be found in the IDnow Autoident Qualified Electronic Signature Process Description, chapter 3.5.

3.2. INITIAL IDENTITY VALIDATION

3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY

This paragraph does not apply as IDnow only accepts natural persons as identities for qualified electronic signatures.

3.2.3. AUTHENTICATION OF PHYSICAL PERSON IDENTITY

IDnow uses its Autoident Qualified Electronic Signature process to authenticate the physical identity of a person (see 3.4).

The full name, the date and the place of birth and other data (see 3.1.2) are provided as evidence by IDnow. The number of the passport or the identity document is being checked against the ICAO standard.

All verification steps are documented and stored by IDnow. The document “Autoident Qualified Electronic Signature Process Description” provide details about the process in the following sections:

- 3.2: General identification process
- 3.3: Detailed steps of the identification process
- 3.7: Accepted identification documents
- 3.8: Approved security features of the identity documents

The IDnow Risk Assessment Autoident Qualified Electronic Signature provides an analysis of attack scenarios and their counter measures in chapter 10 Annex A: Threat Matrix.

The R&D department of IDnow regularly develops and tests new countermeasures against attacks. In addition IDnow has processes in place to ensure that information about undetected fraud cases is received from customers, users or law enforcement. Details can be found in the IDnow Quality Management Policy.

If the identity of the person is based on a subsequent remote authentication, the authentication uses at least two factor authentication as defined in ISO 29115. The authentication factors can be:

- something the person has (e.g., device signature, passport, hardware device containing a credential, private key, access to a registered device)
- something the person knows (e.g., password, PIN)
- something the person is (e.g., biometric characteristic).

Any secret information exchanged in authentication protocols shall be cryptographically protected in transit. Two or more credentials implementing different authentication factors shall be used (e.g., something you have combined with something you know).

In the case of chain of remote authentication, the authentication factors are created during the initial identification which was performed in a way which provides equivalent assurance in terms of reliability to the physical presence.

If one of the authentication factors becomes unavailable (e.g. the user forgets a password), the user must either perform a new identification process which provides equivalent assurance in terms of reliability to the physical presence and must establish new authentication factors during this process.

IDnow has taken additional measures to support users with disabilities like ensuring high contrast. Due to the nature of the process (video recording), there are certain limitations regarding the disabilities that can successfully perform the process (e.g. blind users).

All authentication steps are documented and stored by IDnow. The document “Autoident Qualified Electronic Signature Process Description” provide details about the process in section 3.6.

3.2.4. NON-VERIFIED SUBSCRIBER INFORMATION

There is no non-verified information used by the RA to fill a certificate.

3.2.5. VALIDATION OF AUTHORITY

This paragraph does not apply as IDnow only accepts natural persons as identities for qualified electronic signatures.

3.2.6. CRITERIA FOR INTEROPERATION

Certificates generated based on the information provided by IDnow are compliant with ETSI EN 319 411-2 QCP-n-qscd or QCP-l-qscd.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

Re-Keying requests are not supported by IDnow.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

A subscriber may request a revocation of the certificate. The request has to be performed in person and by the subscriber himself. For such case, the subscriber has to request the revocation through the revocation request form at <https://www.idnow.io/revocation> by providing personal details used during the identification process, as well as a reason for the revocation, which is used for documentation of the request. Upon requesting the revocation, the subscriber will get an email receipt confirming the reception of the request. The revocation request form is available from 00:00 am to 24:00 pm, seven days a week. IDnow will authenticate the person submitting the revocation request using a video-identification to ensure the person requesting the revocation is the subscriber if necessary. The instructions for performing the identification are sent to the subscriber by email.

IDnow will then request the revocation of the certificate based on a documented process between the CA and IDnow. For this, IDnow transmits the request and the CA authenticates the responsible person at IDnow.

IDnow ensures that enough personnel are available (both regarding the number of employees and regarding the individual shift planning) that the identification and authentication can be performed in due time. In addition, IDnow ensures the availability of the necessary technical components (e.g., backend systems) and physical locations which are required to perform the identification and authentication.

If IDnow has detected that a certificate was issued with incorrect data as described above, IDnow will request the revocation of the certificate. For this, IDnow transmits the revocation request and the CA authenticates the responsible person at IDnow.

The detailed process is described in the “IDnow Autoident Qualified Electronic Signature Process Description”, chapter 3.11.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. WHO CAN SUBMIT A CERTIFICATE APPLICATION

After the successful enrollment process of the subscriber, only IDnow can submit a certificate request to the CA.

The subscriber's personal data are usually transmitted by IDnow's clients and usually not being entered directly on the IDnow website or mobile app by the subscriber. IDnow identifies and authenticates its clients.

The client may also send the documents to be signed to IDnow. If the document(s) or hashes of the document(s) are not provided by the client, the subscriber can upload the document to be signed on the website of IDnow.

Details about this are in the "Autoident Qualified Electronic Signature Process Description", section 3.2.1.

4.1.2. ENROLLMENT PROCESS AND RESPONSIBILITIES

IDnow will provide at least the following information for the enrollment process:

- mobile phone
- full name (included surname and given names consistent with the applicable law and national identification practices)

In order to use the registration service, the subscriber has to accept the following terms prior to the start of this process:

- The General Terms & Conditions of IDnow
- The data privacy rules
- The subscriber's consent that the qualified certificate will not be published and only contained in the signed document
- Information about the purpose of the identification

The subscriber signs the General Terms & Conditions of the CA during the signature process (see 4.3).

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

For the matter for this document, the subscriber is always the same physical person that is subject of the requested certificate.

Before submitting a certificate request to the CA, IDnow checks the personal details of the subscriber using its Autoident Qualified Electronic Signature technology (refer to section 3.2).

The document “IDnow Autoident Qualified Electronic Signature Process Description” provides details about the process in the following sections:

- 3.2: General identification process
- 3.3: Detailed steps of the identification process
- 3.7: Accepted identification documents
- 3.8: Approved security features of the identity documents

The Risk Assessment Autoident Qualified Electronic Signature provides an analysis of attack scenarios and their counter measures in chapter 10 Annex A: Threat Matrix.

If the identity of the person is based on a subsequent remote authentication, the authentication uses at least two factor authentication as defined in ISO 29115. The authentication factors can be:

- something the person has (e.g., device signature, passport, hardware device containing a credential, private key, access to a registered device)
- something the person knows (e.g., password, PIN)
- something the person is (e.g., biometric characteristic).

Any secret information exchanged in authentication protocols shall be cryptographically protected in transit. Two or more credentials implementing different authentication factors shall be used (e.g., something you have combined with something you know).

In the case of chain of remote authentication, the authentication factors are created during the initial identification which was performed in a way which provides equivalent assurance in terms of reliability to the physical presence.

If one of the authentication factors becomes unavailable (e.g. the user forgets a password), the user must either perform a new identification process which provides equivalent assurance in terms of reliability to the physical presence and must establish new authentication factors during this process.

All authentication steps are documented and stored by IDnow. The document “IDnow Autoident Qualified Electronic Signature Process Description” provides details about the process in the section 3.6.

4.2.2. APPROVAL OR REJECTION OF CERTIFICATE APPLICATION

The subscriber’s personal data are usually transmitted by IDnow’s clients and usually not being entered directly on the IDnow website or mobile app by the subscriber. Before approving a certificate application, IDnow ensures that the request came from IDnow’s client and that the subscriber has been correctly identified by IDnow.

Details about this are in the “IDnow Autoident Qualified Electronic Signature Process Description”, section 3.2.1.

4.2.2.2. SUBSCRIBER

If the subscriber cannot be identified according to IDnow Autoident Qualified Electronic Signature process or if IDnow has doubt in the validity of the identification data, no certification request will be sent to the CA. In this case, the application of this subscriber will be rejected.

Details about this are in the “IDnow Autoident Qualified Electronic Signature Process Description”, section 3.13.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA ACTIONS DURING CERTIFICATE ISSUANCE

After having successfully identified the natural person, IDnow transmits one or more documents or hashes of documents to be signed to the CA.

Before transmitting the documents or hashes, IDnow issues a technical certificate request which includes at least the following subscriber data: the document(s) to be signed, name and first name, mobile phone number, unique identification of the transaction and the GTC of the CA.

The unsigned document is shown to the subscriber by the RA or by the client. The Subscriber can then accept to sign the document and GTC according to the consent protocol by clicking (first approval) in a check box and by entering an OTP (second approval) that the CA has sent to the mobile phone of the Subscriber. This consent protocol is performed by the CA. The mobile phone number is included in the data, which IDnow transmits with the certificate request.

The CA authenticates the Subscriber with an OTP sent to the mobile phone of the Subscriber. After having successfully authenticated the Subscriber, the CA performs the signature on the document(s) and GTC shown to the Subscriber.

After that, the CA transfers the signed documents or signed hashes to IDnow.

This process is described in detail in the process description “Autoident Qualified Electronic Signature Process Description”, chapter 3.3.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. CONDUCTING CERTIFICATE ACCEPTANCE

After having received the signed documents or hashes from the CA, IDnow checks whether the personal data included in the certificate matches the data gathered from the subscriber. If the data or parts of the data do not match, IDnow cancels the signed documents by requesting a certificate revocation. The subscriber as well as the client will be notified.

If an identification has been performed, IDnow additionally conducts a review of the identification data before accepting the certificate. The review for AutoIdent Qualified Electronic Signature is conducted by an ident center employee. If it is determined that the identification data used to sign was not correct, the signed documents or signed hashes are canceled by requesting a certification revocation using the revocation process.

If the check of the personal data could be performed successfully, the signed documents will be sent to the subscriber and the client. Alternatively, the client delivers the signed documents to the subscriber. If the check of the personal data was not successful, the revocation process will be triggered by IDnow.

4.5. Key pair and certificate usage

Not applicable in the context of an RA.

4.6. CERTIFICATE RENEWAL

Not possible for subscriber certificates.

4.7. CERTIFICATE RE-KEY

Rekeying is not supported.

4.8. CERTIFICATE MODIFICATION

Not possible for subscriber certificates.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. CIRCUMSTANCES FOR REVOCATION

It may occur that IDnow receives information that the personal data of the subscriber does not belong to the ID document or that there have been errors in the registration process of the subscriber. In such cases, IDnow notifies the CA and transmits the unique identifier of the business transaction, subscriber data as well as the signed documents. The CA is then able to revoke the previously issued certificate. IDnow informs the subscriber and the client via email about such incident.

4.9.2. WHO CAN REQUEST REVOCATION

Only the subscriber can request the revocation of the certificate from IDnow.

4.9.3. REVOCATION REQUEST PROCEDURE

A subscriber may request a revocation of the certificate. The request has to be performed in person and by the subscriber himself. For such case, the subscriber has to request the revocation through the revocation request form at <https://www.idnow.io/revocation>. Upon requesting the revocation, the subscriber will get an email receipt confirming the reception of the request. The revocation request form is available from 00:00 am to 24:00 pm, seven days a week. IDnow will authenticate the person submitting the revocation request using a video-identification to ensure the person requesting the revocation is the subscriber if necessary. The instructions for performing the video-identification are sent to the subscriber by email.

IDnow will then request the revocation of the certificate based on a documented process between the CA and IDnow. For this, IDnow transmits the request and the CA authenticates the responsible person at IDnow.

If IDnow has detected that a certificate was issued with incorrect data as described above, IDnow will request the revocation of the certificate. For this, IDnow transmits the revocation request and the CA authenticates the responsible person at IDnow.

IDnow logs the following information regarding a revocation process:

- Who has requested the revocation and why
- Who has performed the revocation
- When the revocation was performed
- Which identification / certificate was revoked
- The steps and results of the revocation process

This process is described in the “AutoIdent Qualified Electronic Signature Process Description”, chapter 3.11.

4.9.5. TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The maximum delay to revoke a certificate is 24 hours.

4.9.6 REQUIREMENTS REGARDING CHECKING THE REVOCATION FOR CERTIFICATE USERS

The certificate users are responsible for checking the state of validity of a certificate using all of the CRLs issued and/or the OCSP service implemented by the CA.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

Physical controls have been implemented for the locations, which are used to process and store the personal data of the enrollment process in order to prevent unauthorized access to such facilities: The identification center and the data center.

The following measures (see IDnow Identification Center Infrastructure Policy, chapter3) have been implemented for the identification center:

- Closed windows and doors
- Physical access restriction, authentication only by chip + pin
- Records of access by door to the identification center
- Video surveillance
- Supervision or monitoring of third parties
- Control of ident center access

In addition, IDnow uses several separate ident center locations to minimize the impact of water and fire exposure. No data is permanently stored at the identification centers.

IDnow uses a sub supplier for the operation of the datacenter. It provides the hardware, racks, grid connection, electricity and climate control for the operation of the servers. IDnow takes over the operation including the operating-system level upwards.

The following measures (see Data Center Infrastructure Policy, chapter 3) have been implemented for the data center:

- Closed windows and doors
- Fire / Water controls
- Redundant connections / power supplies
- Door access records
- Danger alarm system
- Video surveillance
- Perimeter protection / porter cabins
- Supervision or monitoring of third parties
- Control of datacenter access
- Control tours
- Secure destruction / disposal

In addition, all data at the data center is backed up to an off-site location.

IDnow operates an asset management and classification system in which all relevant systems are recorded and categorized based on their required level of security. The IT security manager is responsible for this and checks the asset management twice a year.

It is ensured that the physical controls are in place to protect assets in accordance with their classification.

5.2. PROCEDURAL CONTROLS

IDnow has implemented a role concept that ensures that the relevant tasks are separated in such a way to ensure effective controls. Personnel in a trusted role is named and accepted by the management. The person to fulfil the role also has to accept it. Evidence are documented accordingly. For each trusted role, responsibilities are defined in the respective job descriptions. Data access is only granted to employees with the respective roles after the necessary checks are completed. Such rights are only granted if the specific role was assigned with a task which requires such data access in accordance with the least privileges principle

A segregation of conflicting duties and areas of responsibility is implemented.

Details can be found in chapter 3 “Role concept” in the “IDnow Role Concept”.

5.3. PERSONNEL CONTROLS

IDnow ensures that the agents reviewing the enrolment process possess the necessary qualifications and skills. This is implemented by conducting a multi-day training after the recruitment and before deployment in production operations. IDnow provides a detailed training plan in which all initial training and recurrent training is listed. The training plan also includes training on new threats and current security practices which is done at least every 12 months. The documentation of the training takes place in the HR management system and in a fireproof safe. The responsibility for carrying out the training rests with the team lead of the identification center and the HR Manager.

The reliability of the employee is determined by IDnow by requiring all relevant documents (in particular police clearance certificate, credit worthiness information and CV) of that employee. In the examination of the police clearance certificate every entry of the employee in the certificate must be checked separately by the HR Manager and the IT security officer and approved or rejected and, if no entry should exist, no separate authorization is required. If a country does not have one of the mechanisms listed above (e.g. no credit worthiness information), IDnow shall use other measures with an equivalent level of assurance regarding the reliability of the employee.

IDnow ensures that all personal with trusted roles relating to the RA operations are free from conflicting interests that might prejudice the impartiality of the operations. The HR manager is responsible for disciplinary sanctions (including up to termination of contract) if personnel violates IDnow policies or procedure. This is also the case for employees of third parties IDnow outsources to. Employees with trusted roles of those parties must fulfill the same requirements as internal employees with regard to trustworthiness.

IDnow uses a review process to detect incorrect identifications and to check if the identification policies and procedures have been adhered. Additionally, IDnow conducts test identifications for quality control. Goal of these test identifications is to check of all procedures are followed. These test identifications are done at least yearly. Responsible is the team lead identification center.

The details regarding the personal controls can be found in chapter 3 “Human Resources” in the “IDnow HR Policy”.

5.3.7. INDEPENDENT CONTRACTOR REQUIREMENTS

IDnow uses a sub supplier for the housing of the server hardware. It provides the hardware, racks, grid connection, electricity and climate control for the operation of the servers. IDnow takes over the operation including the operating-system level upwards.

IDnow uses a sub supplier for the long term archival of the proof files (7 years' minimum archival duration).

IDnow uses both internal identification centers as well as sub suppliers for external identification centers.

5.3.8. DOCUMENTATION SUPPLIED TO PERSONNEL

IDnow makes available to their personnel the present CP and the corresponding CPS, and any relevant statutes and policies. Other technical, operational and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided to enable the trusted personnel to perform their duties.

5.4. AUDIT LOGGING PROCEDURES

Audit log files are generated by IDnow for all events related to security and RA services. Where possible, security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits. The logs contain also the following information:

- start-up and shutdown of the logging functions; and
- availability and utilization of needed services with the RA network; and
- system start-up and shutdown; and
- system crashes and hardware failures; and
- firewall and router activities

IDnow operates external logging and monitoring which is protected against unauthorized access. Logging is controlled regularly for critical or personal data. The logs and monitoring are regularly checked for discrepancies. A system administrator checks the logs in the case of a security incident.

IDnow performs itself internal security audits of all systems and networks to find vulnerabilities. This is done at least twice a year. The IT security officer is responsible.

Any alteration, deletion, or copying of data is logged with the help of log files through the IDnow software so that alterations in personal data are always traceable. The allocation to the appropriate employee and client accounts is guaranteed at all times.

In addition, it is ensured that IDnow logs the following events:

- Physical facility access

- Changes to trusted roles
- Backup management
- Log management
- Date, time, phone number used, persons spoken to, and end results of verification processes
- Acceptance and rejection of certificate requests
- IT and network management, as they pertain to the RA systems
- Security management

In addition to that, IDnow records all the information used:

- To verify the subscriber's identity
- If applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity (refer to section 3.2 above)
- To create the certificate request (means all information described in section 4.1.2.2 above)
- The list of all RA Operator that are authorized to enroll and manage subscribers
- Proof file generated by the CA
- The technical Consent Protocol

5.5. RECORDS ARCHIVAL

A PDF document, created by IDnow and transmitted to CA along with Document(s) and GTC to be signed, detailing the performed identification and the identity of the subscriber is included by the CA in the proof file after successful signature operation made by the Subscriber. After the end of the signature process the proof file is delivered to long term storage which can be operated by a third party.

The long term storage ensures that,

- All media used for archiving are protected against damage and unauthorized access
- Media is available for the required lifetime
- All media are properly disposed at the end of its lifetime

Details about the process like results of performed checks, involved employees and applications used are archived by IDnow.

5.6. Certificate renewal

Not applicable in the context of an RA.

5.7. DISASTER RECOVERY

IDnow regularly conducts risk analysis to identify any risk and countermeasures in the business and processes which covers assets relevant for the Trust Services. Taking into account the risk assessment results, IDnow selects appropriate technical or organizational risk treatment measures to be implemented. Risks are regularly reviewed and revised. The management board is responsible for

approving the risk assessment and the acceptance of residual risks. In addition, IDnow has defined an incident management process.

IDnow ensures that all necessary data for the RA operations, essential information and software are backed up and stored in a safe place, more than 5km from the primary site, suitable to allow IDnow to timely go back to operations in case of incident/disasters.

Back-up arrangements are regularly tested to ensure that they meet the requirements of business continuity plans and are performed by the relevant trusted roles.

IDnow maintains a business continuity plan (BCP) which list the applicable risks, remediation measures and acceptable recovery times. A key part of the BCP is also how to avoid repetition of the cause that triggered the BCP.

Details can be found in the "IDnow Security Policy", chapter 11.2, "IDnow Incident Management" and "IDnow Risk Assessment AutoIdent Qualified Electronic Signature", chapter 7.3 "Residual Risks".

5.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

Incidents are submitted via the contacts defined in Section 1.5.2 and processed in the context of service management. For any vulnerability, given the potential impact, IDnow either creates and implement a plan to mitigate the vulnerability; or documents the factual basis for the determination that the vulnerability does not require remediation. Critical vulnerabilities are addressed within 48 hours after its discovery.

IDnow will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies of any breach of security or loss of integrity that has a significant impact on the Trust Service provided. The IT Security Officer is responsible for this process as part of his/her overall responsibility for security.

IDnow will also inform natural persons in case a breach of security or loss of integrity is likely to adversely them without undue delay.

5.8. TERMINATION

At the moment when IDnow notifies the discontinuation of its services as RA, IDnow will:

- promptly inform the CSP and implement decommissioning activities on the basis of the contract concluded with the CSP,
- send a registered letter to the "technical contact",
- return or destroy all keys, API keys etc. existing and received privately up to the cessation of operations,
- authorize the CA to keep the proof file,
- stop sending identification results to the CSP and
- inform business partners and clients, as far as they are affected by the closure of the business area.

IDnow aims to reduce potential disruptions as a result of the cessation of the RA services. IDnow has an internal up-to-date termination plan.

IDnow has arrangements to cover the costs to fulfil these minimum requirements in case the TSP goes bankrupt, or for other reasons, is unable to cover the costs by itself.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

Not applicable in the context of an RA.

6.2. Private Key Protection and Cryptographic Module Engineering

Not applicable in the context of an RA.

6.3. Other aspects of key pair management

Not applicable in the context of an RA.

6.4. ACTIVATION DATA

The CA is responsible for the consent protocol and the document viewer.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

User management is performed for all data processing systems which require protection. The user management is carried out using personal accounts only. No impersonal collection accounts are used.

The general guidelines for creating passwords (such as minimum length and password complexity) are the basis of the password policy. All employees are informed about the proper handling of passwords and have signed an appropriate guideline.

There is a defined timeout for sessions.

The consciousness of security of their work environment is refreshed for all employees in regular security awareness trainings.

Only system administrators can access the server system and always through encrypted connections. All accesses are personalized and protected by passwords + 2-factor authentication.

Security requirements shall be analyzed during the design and requirements specification stage of system development projects to ensure that security is built into IT systems.

Network components are in locked racks to secure them physically. The networks used for the identification services are logically separated from other components to prevent unauthorized access. Firewalls protect those networks from attacks and unauthorized access. The configuration and hardening measures of those components is regularly reviewed.

Administrative accounts are used for administrative purposes only.

Human Resources management issues with the respective superiors the appropriate rights which are specified according to the HR processes. The rights are then reviewed by the IT security officer. When leaving the company, the withdrawal of access rights takes place within maximum 24 hours.

Details can be found in the “IDnow HR Process Policy”, chapter 3.

6.6. Life cycle technical controls

Not applicable in the context of an RA.

6.7. NETWORK SECURITY CONTROLS

The connection to the TSP is the only PKI component used by IDnow that is being delivered by the CA.

All systems use virus scanners that run automatically in the background and are also automatically updated.

IDnow uses security gateways (firewalls) or if necessary appropriate additional solutions such as application firewalls, next generation firewalls, etc. which, in turn, can perform (for example by Portscans, etc.) intrusion prevention or intrusion detection.

Security checks, such as through vulnerability scans with subsequent evaluation, are carried out:

- at least once per quarter or
- if IDnow receives a request for a vulnerability scan from the CA or the CA/Browser Forum or
- after any system or network changes that the CA determines are significant.

The vulnerability scans will be conducted by a specialized external company.

In addition, IDnow performs penetration tests through an external specialized company:

- at least once per year or
- if IDnow receives a request for a penetration test from the CA or the CA/Browser Forum or
- after any system or network changes that the CA determines are significant.

All personal data that are sent between the identification center and the datacenter is encrypted through a VPN, and in addition TLS. The network for the processing of identification data is physically separated from the network of offices.

The transfer of the data to the client is always encrypted (TLS, SFTP, S/MIME, etc.).

The transfer of data between the user and IDnow during identification is also always encrypted (TLS, DTLS for video).

There is no physical shipment of data.

IDnow ensures the secure operation of all technical systems by "hardening". This includes in particular:

- Removal of unnecessary software/services
- Removal of unnecessary accounts
- Modifying the configuration in regards to security
- If necessary activation of security components
- Protection of network ports

Details can be seen in "Identification Services Infrastructure Policy", chapter 3.

6.8. TIME STAMPING

All systems have their time with a time zone reference against UTC synchronized through NTP at least daily.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Not applicable in the context of an RA.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Prior to performing the role as Registration Service for the CA, an external auditor has to confirm the compliance with ETSI standards EN 319 411-2, EN 319 411-1 and EN 319 401.

The audit program is planned according the following with an audit each year for RA:

- First audit is realized by external auditor
- First year after the initial audit, the audit is realized according to the CA audit program
- Second year after the initial audit, the audit is realized according to the CA audit program
- Third year after the initial audit, the audit is realized again by external auditor

In case of major findings discovered during internal audit made by the CA, RA (Partner) as to fix it and an external audit will be conduct during the same year in order to check the findings.

8.3. TOPICS COVERED BY ASSESSMENT

The following topics will be covered in an audit of IDnow as a registration service:

- Protection, use and management of the key pairs used to protect the communication with the CA
- Creation of the technical certificate request
- RA records against requirements set in the CP
- "RA procedure" defined by Customer to identify, authenticate and manage certificate request to the CA
- Subscriber personal data protection and management

9. OTHER BUSINESS AND LEGAL MATTERS

9.2. FINANCIAL RESPONSIBILITY

IDnow maintains sufficient financial resources and obtained appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. PRIVACY PLAN

IDnow has a privacy plan that is shown to the subscriber at the start of the process and has to be confirmed by the subscriber. The privacy plan is according to the GDPR.

IDnow can optionally work in accordance with a commissioned data processing agreement with the client. The client is then the responsible entity in the sense of Art. 4 No. 7 GDPR. The supplier must observe the principles of proper data processing. The supplier must ensure the contractually agreed and legally prescribed information security measures, in particular compliance with the principles in Art. 5 I lit. f, 25 and 32 GDPR.

In addition, IDnow has appointed a privacy officer.

Every new agent, newly recruited at IDnow, goes through privacy training during his period and takes an online test on data protection.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.3. RA REPRESENTATIONS AND WARRANTIES

IDnow insures as Registration Authority that each subscriber has been identified and authenticated properly prior to a certificate request for such subscriber. Furthermore, IDnow is responsible for the correct performance and authorization of the certificate request. For this matter, IDnow uses a large array of automated checks which are performed by the IDnow software as well as further manual checks performed by a trained IDnow agent.

Before submitting a certificate request to the CA, the subscriber can review the terms and conditions regarding the use of a certificate. Furthermore, the subscriber has to accept such terms and conditions by clicking on a check box shown on the screen. The subscriber can access the terms and conditions via IDnow's website.

IDnow ensures that data contained in the certificate request is complete and accurate. IDnow supports the audit teams and has to make any reasonable effort to complete an audit and to communicate the results.

In case of a loss, stolen or compromised subscriber's private key, IDnow will notify the subscriber. If the CA notifies IDnow that a subscriber's certificate has been compromised, IDnow ensures that no certificate is being used by the subscriber or the client.

IDnow ensures that records concerning the operation of services will be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

9.8. LIMITATIONS OF LIABILITY

IDnow guarantees to have performed the enrollment process and the transmission of the resulting data to the CA. IDnow is not liable regarding the suitability or the authenticity of certificates issued under this CP.

9.9. INDEMNITIES

IDnow makes no claims as to the suitability of certificates issued under this CP for any purpose whatsoever. Relying parties use these certificates at their own risk. IDnow has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this CP.

9.13. DISPUTE RESOLUTION PROVISIONS

In the event of disputes, the parties shall come to an agreement taking into account any applicable laws, regulations, and agreements made.

9.14. GOVERNING LAW

German law shall apply.

9.16. MISCELLANEOUS PROVISIONS

IDnow operates its business in accordance with the German non-discriminatory law.