# AutoIdent eIDAS Substantial LoA Mapping

# 1.1

IDnow GmbH
Auenstr. 100
80469 Munich

29.10.2020

# 1. Contents

# 2. Introduction

## 2.1. Purpose of this document

This document maps the characteristics of the AutoIdent eIDAS Substantial product to the eIDAS Level of Assurance defined in Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of the eIDAS Regulation [(EU) 910/2014]. For that purpose, we consider each requirement of the Implementing Regulation and explain how AutoIdent eIDAS Substantial meets the requirements for Level of Assurance 'substantial'.

As creators of the best-in-class identification products, we are proud of our mission to make the connected world a safer place, leading in compliance and security. This is not just earned through our distinguished results, but our corporate culture and team structure aimed at quality control and identification of new threats.

Today's daily social and business world is increasingly moving into the realm where digital identity is a basis for interaction or accessing services. As new markets enter the digital space, challenges arise surrounding digital identity, privacy, and cybersecurity. Such developments require solutions and technologies built on systems that enable trust.

Since IDnow's founding in 2012, our goal has been to create products that offer the same level of confidence and trust in remote identification as exists with a physical face-to-face identification. In 2014, we were selected as part of an exclusive group of companies to provide remote identification by the Germany's Federal Financial Supervisory Authority (BaFin). Under a tight mandate, our product provides an equivalent assurance of reliability to physical presence with our VideoIdent product.

With these years of experience, we have incorporated what we have learned into our new generation of machine learning products that meet the highest requirements of today's environments. Given this document's class of requirements, we are confident that the AutoIdent eIDAS Substantial system meets security requirements for low and substantial. The level of guarantee will depend on the system's resistance to attacks, such as counterfeit identity documents, manipulating images or video captured, manipulating the user's environment or that of the service provider's system.

AutoIdent is based on optical technology. Our team of experts also contribute to building stronger technical criteria in identity proofing standards, such as our work with The European Technical Standards Institute (ETSI) the G7's Financial Action Task Force (FATF), and the FIDO Alliance, which ultimately can serve as a blueprint for more effective regulation. IDnow is committed to making the connected world a safer place.

## 2.2. Review frequency

This document will be reviewed yearly or based on changes that require a new review.

## 2.3. Current version

The current version of this document is 1.1 of 29.10.2020.

## 2.4. Versioning

| Version | Date | Changes |
|---|---|---|
| 1.1 | 29.10.2020 | • Added more details regarding the security feature checks |
| 1.0 | 16.10.2020 | • Initial Version |

## 2.5. Responsible roles

The following persons are responsible for this security concept:

| Position |
|---|
| IT Security Officer |

## 2.6. Classification

This document is classified as

Public

The document can be freely distributed inside and outside of IDnow.

## 2.7. Distribution

The document should be distributed to the following recipients

| Recipient | Responsible Role |
|---|---|
| IDnow Management | IT Security Officer |

DocuSigned by:
Armin Bauer
099A322C8F74462...

DocuSigned by:
Christoph Jung
936A2205AE20499...

# 3. LoA mapping

**2.1.1. Application and registration - LOW, SUBSTANTIAL, AND HIGH**

**1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means**

The terms and conditions related to the use of AutoIdent eIDAS Substantial are available during the process and publicly on the website of IDnow at https://idnow.io/terms. Before a user enters the identification process, the user agrees to the data collection by IDnow and accepts the terms and conditions of IDnow. The terms and conditions are versioned are logged and properly archived as evidence that a certain user accepted the terms and conditions for an identification process at a point in time.

The terms and conditions are publicly available.

Hence, this control is fulfilled.

**2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.**

The applicant is made aware of recommended security precautions related to the electronic identification means through the terms and conditions.

**3. Collect the relevant identity data required for identity proofing and verification.**

IDnow collects relevant identity data required for proof and verification of identity through the AutoIdent eIDAS Substantial product required to verify the identity of the person beyond doubt at the time of application.

A user launches the verification App and uses his or her smartphone camera to take a picture of the identification document. The App recognizes the picture on the ID card / passport and extract the data from the document.

The App recognizes the data on the card and reads it via OCR. The following minimum data is read from ID documents:

- First name
- Last name
- Date of birth
- Nationality
- ID number
- Issuing country
- Validity of the document

Depending on the country and the type of identification document, more data can be read. Further data fields are to be agreed on between the Customer and IDnow. We comply with the requirements of the GDPR and are audited yearly for the compliance by an external data privacy auditor.

Details can be found in the document "AutoIdent eIDAS Substantial Process Description Version 1.0" chapter 3.4 "Data collected".

Hence, this control is fulfilled.

### 2.1.2. Identity proofing and verification (natural person) - LOW

**1. The person can reasonably be assumed to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.**

IDnow AutoIdent eIDAS Substantial offers an automated solution to identify a person and the person's official identification document are a match. IDnow only accepts official document as evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.

The user must present the identity document. The system then determines the document type, version (i.e. nationality), is able to retrieve data, execute liveness and security checks, and – if deemed necessary by the system - an agent performs a manual review to further ensure the system has run properly and the applicant matches to the document.

The process automatically performs these steps:

- Determines the kind of document used (e.g. passport, ID-card, driver license)
- Determines the version of the document (e.g. French passport)
- Retrieves the data from the document
- Performs a biometric comparison
- Executes a liveness detection
- Verifies the genuineness of the document used during the process by doing a security verification of the document. AutoIdent eIDAS Substantial uses an optical process for verifying the documents during the process. For details please see section "2.1.2. Identity proofing and verification (natural person) – SUBSTANTIAL" of this document.

Details can be found in the documents "AutoIdent eIDAS Substantial Process Description Version 1.1".

Hence, this control is fulfilled.

**2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.**

IDnow supports ID Documents (passports, national ID cards, Residency Permits, and Driver's Licenses for specific use cases i.e. car sharing) in accordance with the common ICAO standard.

IDnow has classified ID documents into "document tiers" which define the required security level of the document. The AutoIdent system reads Tier 1-2 documents with multiple security features embedded into the document. (Please refer to section 6.7 Document Tiers, in our AutoIdent Qualified Electronic Signature Risk Assessment for further details).

The AutoIdent system verifies that the identity document is legible, consistent with data transmitted, and has not been falsified or counterfeited, and the photograph on the document does not appear to have been altered.

Details can be found in the documents "AutoIdent eIDAS Substantial Process Description Version 1.1".

Hence, this control is fulfilled.

**3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.**

IDnow uses official ID documents as authoritative source. These have been issued by government bodies according to the local state laws. The AutoIdent system verifies that the identity document is legible, consistent with data transmitted, and has not been falsified or counterfeited, and the photograph on the document does not appear to have been altered. The existence of the user's identity is verified to be the person he or she claims to be with a face comparison between the ID document and the user and a liveness check.

Details can be found in the documents "AutoIdent eIDAS Substantial Process Description Version 1.1".

Hence, this control is fulfilled.

### 2.1.2. Identity proofing and verification (natural person) - SUBSTANTIAL

**Level low, plus one of the alternatives listed in points 1 to 4 has to be met:**

**1. The person has been verified to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity**

**and**

**the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person**

**and**

**steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;**

**"Steps have been taken to minimize the risk that the person's identity is not the claimed identity"**

Not every document in the world is produced in the same way. The security of the document can vary from country to country and from version to version. The security of an identification process depends on the security of the underlying document and how easily the document can be assessed. Documents are split up into tiers that define the quality of each document. Tiers define the quality of the document.

For details about the document tiers please refer to the document "IDnow AutoIdent Qualified Electronic Signature Risk Assessment", chapter 6.7. "Document Tiers".

To assess the document, it must contain security features the can be checked in white light. In this analysis only those security features are considered (e.g. no UV light). As single security features can sometimes be forged, the document must contain security features from different categories.

The quality of the photo can be a strong factor in the quality of the face comparison / biometrics. In general, there exist 2 types:

- Biometric Photo: The photo is taken under defined settings that allow good biometric comparison (e.g. face straight in the camera, mouth closed, eyes open, etc. For details the ICAO guidelines are consulted)
- Non-biometric Photo: The photo has no special requirements as to how it is taken. Often users do not look straight into the camera, smile, etc.

The AutoIdent Level 4 system accepts Tier 1 and Tier 2 documents, with biometric or non-biometric photos as identification evidence. In any case, the biometric algorithm is configured to ensure a False Acceptance Rate (FAR) < 0.5%.

In comparison, in a physical face- to-face identification, more unsecure documents such as Tier 3 and Tier 4 documents (paper-based documents) are accepted. This leads to more security issues as attackers typically do not attack the most secure document but instead go for the less secure documents, and strongly increases the risk for physical encounters.

**"Evidence recognized by the Member State"**

AutoIdent eIDAS Substantial only accepts official ID documents recognized by the member state as evidence.

**"Evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person"**

**And**

**"taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence"**

The AutoIdent system verifies that the identity document is legible, consistent with data transmitted, and is checked to not been falsified or counterfeited, and the photograph on the document does not appear to have been altered. The system verifies the genuineness of the document presented and ensures the ID relates to the user through several automated checks. The verification process inspects the security of the document

An identity document must be presented at the beginning of the AutoIdent process for a face comparison. The system verifies that the ID document relates to the applicant using several automated checks and – if deemed necessary by the system – a manual check by a human agent.

- These measures (i.e. document and security checks with inspection of holograms, kinegrams, microprinting, guilloche structure, checksum, a face comparison and liveness checks, plus optionally a manual review) minimize the risk that the identity of the person does not match the document.

- IDnow does rely on official sources such as the European Union's PRADO database, as reference databases is used in the case of a manual verification by the agents. In addition, IDnow has its own blacklist of ID documents, this list is updated continually and shared with our customers only.
- The system automatically retrieves the kind of document used (e.g. passport, ID-card, driver license), the document type, version (i.e. nationality), and is able to retrieve data from the document.
- Automatic security checks like checksum verification and verifying the consistency of data minimize the risk that the document is not genuine.
- The MRZs in the document have checksums that are calculated based on user information. These checksums are validated and marked as a fraudulent document if they do not match with the expected checksum.
- The system also compares MRZ information with the visible printed information in order to detect any manipulations done to the data.
- Regarding lost and stolen documents: This is taken care of by the biometric algorithm which ensures that such documents cannot be used by other person.
- Regarding suspended, revoked, or expired documents: This is checked directly based on the document (e.g. expiration date, cut corners, punch holes).

Thereafter, IDnow optionally performs a manual follow-up check on all of the identifications that have gone through the identification process of the AutoIdent product. An ident specialist checks the data collected and matches it with the ID document, verifies the security features on the ID card, and performs a face comparison between the user's photo and the photo on the ID card. The verification by the ident specialist is performed based on the images taken during the process and by checking the result of the algorithm.

In addition, identifications that have been carried out, are checked for quality, suspicion of fraud and errors. In the case of an emergency (e.g. if fraud is detected after the identification was finished), the Customer shall receive information about this, and eID shall not be issued.

**"The person has been verified to be in possession of evidence"**

**And**

**"Steps have been taken to minimize the risk that the person's identity is not the claimed identity"**

IDnow begins with process steps to assure that the identification of a natural person is equivalent to a face-to-face identification. It identifies whether the image in front of the camera is a real person or manipulated images. This is done by using liveness detection where the person has to perform system-defined movements in front of the camera which are then checked to verify that no picture or video of a person are in front of the camera.

- Check of the actual existence of the person in real life

- Check whether the ID document belongs to this specific person
- Proof that the present person is the same as specified before

The system performs a biometric face comparison of the user to identify whether the image in front of the camera is a real person or a manipulation of images. The comparison is carried out with a reliability that meets and even exceeds a face to face encounter. This is done by comparing the false acceptance rate (FAR) of the biometrics algorithm to the performance of a trained human operator. The AutoIdent system ensures the user ID matches his or her own identity. In any case, the biometric algorithm is configured to ensure a False Acceptance Rate (FAR) < 0.5%.

AutoIdent's 3D face recognition protects against presentation attacks and uses a short video stream rather than a selfie to compare physical characteristics with color images with a resolution larger than 600 DPI.

Security checks, face comparison and liveness checks are optionally further supported by a manual review. Our agents are specifically trained to perform security checks and evaluate the comparison criteria of the user to their official document. These mechanisms are proven to be resistant to know attacks.

Through the assistance of technology, fraud also depends on the level of sophistication an attacker chooses to engage. The system identifies whether the image in front of the camera is a real person or a manipulation of images. AutoIdent eIDAS Substantial is a face-based authentication solution, it matches the individual to the photo on the user's ID document.

All checks have to be completed before the creation of the eID.

Details can be found in the documents "AutoIdent eIDAS Substantial Process Description Version 1.1".

Hence, this control is satisfied.

**or**

**2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it**

**and**

**steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;**

Not applicable.

**or**

**3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such**

**equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council(1) or by an equivalent body;**

Not applicable.

**or**

**4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.**

Not applicable.

**2.1.2. Identity proofing and verification (natural person) - HIGH**

**Requirements of either point 1 or 2 have to be met:**

**1. Level substantial, plus one of the alternatives listed in points a to c has to be met:**

**a. Where the person has been verified to be in possession of photo or biometric identification evidence recognized by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;**

**and**

**the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;**

**or**

**b. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for the registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council or by an equivalent body**

**and**

**steps are taken that the results of this previous procedure remain valid;**

Not applicable

**or**

**c. Where, electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body**

**and**

**steps are taken that the results of this previous issuance procedure of a notified electronic identification means remain valid.**

Not applicable

**OR**

**2. Where the applicant does not present any recognized photo or biometric identification evidence, the very same procedures used at the national level of the Member State of the entity responsible for the registration to obtain such recognized photo or biometric identification evidence are applied.**

Not applicable

**2.1.3 Identity proofing and verification (legal person)**

**(…)**

As the eID is only used for the identification of natural persons, this section is not applicable.

**2.1.4 Binding between the electronic identification means of natural and legal persons**

**(…)**

As the eID is only used for the identification of natural persons, this section is not applicable.

**2.2.1 Electronic identification means characteristics and creation - LOW**

**1. The electronic identification means utilizes at least one authentication factor.**

**2. The electronic identification means is designed so 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.**

For details, see rationale 2. of level 'SUBSTANTIAL' (below).

**2.2.1 Electronic identification means characteristics and creation – SUBSTANTIAL**

**1. The electronic identification means utilizes at least two authentication factors from different authentication factor categories.**

**2. The electronic identification means is designed so that it can be assumed to be used only if under the control of the subject to whom it belongs.**

The eID does not provide authentication options. Instead it can only be used once in the same session as the identification. So, it is always ensured that the eID is under control of the person to whom it belongs. After the eID is used, it cannot be used again.

Hence, this control is satisfied.

**2.2.1 Electronic identification means characteristics and creation - HIGH**

**Level substantial, plus:**

**1. The electronic identification means protects against duplication and tampering against attackers with high attack potential.**

Not applicable.

**2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.**

Not applicable.

**2.2.2 Issuance, delivery and activation – LOW**

**After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.**

See rationale of level 'SUBSTANTIAL'.

**2.2.2 Issuance, delivery and activation – SUBSTANTIAL**

**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.**

As AutoIdent eIDAS Substantial only provides access to the person who was identified in a seamless process there is no separate "Issuance, delivery and activation" process necessary.

Hence, this control is satisfied.

**2.2.2 Issuance, delivery and activation – HIGH**

**The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.**

Not applicable

**2.2.3 Suspension, revocation and reactivation - LOW, SUBSTANTIAL, and HIGH**

**1. It is possible to suspend and/or revoke an electronic identification means in a timely and efficient manner.**

**2. The existence of measures taken to prevent unauthorized suspension, revocation and/or reactivation.**

**3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.**

As the eID can only be used during the identification, a revocation or reaction process is not possible. Hence, this section is not applicable.

**2.2.4 Renewal and replacement**

**(…)**

The eID can be neither renewed nor replaced (without new enrolment). Hence, this section is not applicable.

**2.3.1 Authentication mechanism - LOW**

**1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.**

**2. Where person 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 activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.**

Not applicable as the system does not provide authentication options.

**2.3.1 Authentication mechanism - SUBSTANTIAL**

**Level low, plus:**

**1. The release of person identification data shall be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process.**

The underlying encryption methods used by IDnow provide the required dynamic authentication by using protocols based on a static-ephemeral Diffie-Hellman based on at least TLS v1.2 according to BSI TR-02102. It is ensured that a cryptographically secure random number generator is used.

Hence, this control is satisfied.

**2. 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 manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.**

In the AutoIdent system, all data is encrypted and transmitted securely. It fulfils end-to-end encryption as well as requirements of BSI TR-02102 and uses at least TLS v1.2. Strong cryptographic protocols and appropriate key lengths are selected. IDnow uses CAs whose root certificate is contained in the trust store of the browser of the user.

Hence, this control is satisfied.

**2.3.1 Authentication mechanism - HIGH**

**Level substantial, plus:**

**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 manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.**

Not applicable

**2.4 Management and organization**

**All participants providing a service related to electronic identification in a cross-border context ("providers") shall have in place documented information security management practices, policies, approaches to risk management, and other recognized controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.**

IDnow has an effective information security management system in place to manage and control all information security risks. The organizational and technical measures are documented in the IDnow Security Policy. IDnow is regularly audited against compliance with the Security Concept according to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2

IDnow operates at the highest levels of processes and procedures to manage information security risks to acceptable levels. Our security policy document IDnow Security Policy is available upon request and has been approved by management. The security policies are communicated to our employees and is further supplemented with detailed policies and procedures for all personnel involved in identity verification (i.e. Ident agents).

The IDnow Security Policy defines information security, the overall objectives and scope, and the importance of security as a secure mechanism for information sharing. It contains a statement of management commitment, support of these goals and IDnow's principles of information security. The document provides an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the company and our function as an identification solution provider.

The Security Policy lists both general and specific responsibilities within information security management, including reporting security incidents, referencing documentation and standards that support the policy, duties to protect individual assets, and responsibilities to carry out specific security processes. These are clearly outlined and defined.

IDnow ensures that there are clear directions with active management support for all security initiatives. Our CISO is responsible for maintaining the security policy and coordinating the implementation of these measures, including regular reviews of the information security policy, any processes and supporting documentation, which includes our risk assessments.

Hence, this control is satisfied.

**2.4.1 General provisions - LOW, SUBSTANTIAL, and HIGH**

**1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognized as such by national law of Member State, with an established organization and fully operational in all parts relevant for the providing of the services.**

IDnow is a legal entity and is recognized as such by national law of Member State, with an established organization and fully operational in all parts relevant for the providing of the services.

Hence, this control is satisfied.

**2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service including, the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.**

As a audited and certified entity according to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2, IDnow complies with any legal requirements incumbent on them in connection with operation and delivery of the service including, the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.

Hence, this control is satisfied.

**3. Providers are able to demonstrate the ability to assume the risk of liability for damages, as well as having sufficient financial resources for continued operations and providing of the services.**

IDnow has customers worldwide, operations in multiple European countries and is one of the leading identity providers in Europe. In addition, IDnow has the backing of investors and has insurances covering the relevant risks.

Hence, this control is satisfied.

**4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.**

Contracts are in place to ensure high level of compliance. IDnow is still fully responsible for the outsourced commitments.

**5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.**

Please see section 10 “End of operation” of the document “IDnow Security Policy Version 1.5”.

Hence, this control is satisfied.

**2.4.2 Published notices and user information - LOW, SUBSTANTIAL, and HIGH**

**1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.**

The terms and conditions related to the use of AutoIdent eIDAS Substantial are available during the process and publicly on the website of IDnow at https://idnow.io/terms. The terms and conditions are publicly available and include a privacy policy.

Hence, this control is fulfilled.

**2. Appropriate policy and procedures are in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions and privacy policy for the specified service.**

Any changes of any service definition are made public on the website of IDnow under the same URLs at https://idnow.io/certification-policies.

Hence, this control is fulfilled.

**3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.**

IDnow provides contact by phone and email for requests for information (https://www.idnow.io/contact). There are policies in place that requests are answered by the appropriate department at IDnow.

Hence, this control is fulfilled.

**2.4.3 Information security management - LOW**

**There is an effective information security management system for the management and control of information security risks.**

See rationale of levels 'substantial and high' (below).

**2.4.3 Information security management - SUBSTANTIAL and HIGH**

**Level low, plus:**

**The information security management system adheres to proven standards or principles for the management and control of information security risks.**

IDnow has an effective information security management system in place to manage and control all information security risks. The organizational and technical measures are documented in the IDnow Security Policy. IDnow is regularly audited against compliance with the Security Concept according to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

Hence, this control is fulfilled.

### 2.4.4 Record keeping - LOW, SUBSTANTIAL and HIGH

**1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.**

Please refer to section 3.4. “Data collected” of the document “AutoIdent eIDAS Substantial Process Description Version 1.0” and section 7.4 “IT security” of “IDnow Security Policy Version 1.5”.

Hence, this control is fulfilled.

**2. Retain, as far as permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.**

IDnow stores the required records for as long as required by the applicable national laws. After the storage period has ended the records are securely destroyed.

Hence, this control is fulfilled.

### 2.4.5 Facilities and staff - LOW, SUBSTANTIAL, and HIGH

**1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.**

Staff are employed according to dedicated job profiles. Where relevant, also additional dedicated training programs for staff members exist. This ensures that procedures are performed by trained, qualified and experienced staff. The duties are performed according to formalized processes, and special obligations of due diligence exist. In particular, this holds for enrolment, identity proofing and verification.

Please refer to section 5. “Role Concept” and section 6. “HR” of “IDnow Security Policy Version 1.5”.

Hence, this control is fulfilled.

**2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.**

IDnow ensures that sufficient staff is available to operate the service.

Please refer to section 7.7. “System Planning” of “IDnow Security Policy Version 1.5”.

Hence, this control is fulfilled.

**3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorized access and other factors that may impact the security of the service.**

Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorized access and other factors that may impact the security of the service by measures as limiting physical access, access protocols, perimeter security if applicable, video surveillance, alarm system, visitor logs and control tours.

Please refer to section 7. “Infrastructure” of “IDnow Security Policy Version 1.5”, as well as section 3 of “IDnow Data Center Infrastructure Policy” and “IDnow Identification Center Infrastructure”.

Hence, this control is fulfilled.

**4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorized staff or subcontractors.**

Access to areas of facilities used for providing the service holding or processing personal, cryptographic, or other sensitive information is limited to authorized staff or subcontractors. This is ensured by appropriate access right management, limiting physical access, access protocols, and perimeter security if applicable.

Please refer to section 7. “Infrastructure” of “IDnow Security Policy Version 1.5”, as well as section 3 of “IDnow Data Center Infrastructure Policy” and “IDnow Identification Center Infrastructure”.

Hence, this control is fulfilled.

### 2.4.6 Technical controls - LOW

**1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.**

There exist appropriate technical inspections concerning the risk management with regard to the protection of confidentiality, integrity and availability of the information processed.

Please refer to section 7. “Infrastructure” of “IDnow Security Policy Version 1.5”, as well as section 3 of “IDnow Data Center Infrastructure Policy” and “IDnow Identification Center Infrastructure”.

Hence, this control is fulfilled.

**2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.**

All communication channels are protected according to BSI TR 02102 and are using at least TLS v1.2.

Please refer to section 7. “Infrastructure” of “IDnow Security Policy Version 1.5”.

Hence, this control is fulfilled.

**3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plaintext.**

Not applicable

**4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.**

IDnow follows its internal processes and policies to ensure that security is maintained over time and to respond without delay to changes in risk levels, incidents or security breaches.

**5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.**

All media is encrypted in-transit and the biometric data is encrypted at rest. No media is every transported physically.

There exists a certified disposal mechanism of media that has to be retired.

Please refer to section 7. “Infrastructure” of “IDnow Security Policy Version 1.5”.

Hence, this control is fulfilled.

### 2.4.6 Technical controls - SUBSTANTIAL

**Level low, plus:**

**Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.**

Not applicable

### 2.4.7 Compliance and audit - LOW

**The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.**

See rationale of level ‘SUBSTANTIAL’ (below).

### 2.4.7 Compliance and audit - SUBSTANTIAL

**The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.**

IDnow is externally audited and certified according to the Commission Implementing Regulation (EU) 2015/1502 for level of assurance substantial by an independent external auditor.

Hence, this control is fulfilled.

**2.4.7 Compliance and audit - HIGH**

**1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.**

**2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.**

Not applicable