<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>COMPANY PROFILE</td>
<td>4</td>
</tr>
<tr>
<td>1.1</td>
<td>WHY IDNOW</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>AUTOIDENT</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>VIDEO IDENT</td>
<td>10</td>
</tr>
</tbody>
</table>
ID Verification Is Becoming the Standard In Almost Every Industry
1 COMPANY PROFILE

Founded in 2014, IDnow provides the world’s most advanced machine-learning technology for its Identity-as-a-Service platform that can verify in real time the identities of more than 7 billion potential customers from 193 different countries. Its patent-protected auto and video identification and e-signing solutions help its clients save money, improve customer conversion rates and streamline the onboarding process. IDnow is backed by a consortium of well-known venture capital investors and business angels. Its 400 clients include international blue-chip companies such as Commerzbank, UBS, Erste Bank and Telefonica Deutschland, as well as fintechs including Fidor, N26 and smava and also the German Government.

IDnow’s products are delivered from a common platform, which means different business units within an enterprise can leverage them with a central identity repository.

IDnow technology uses artificial intelligence to verify that all security features are present on the identity document and is therefore able to reliably detect forged documents. Its AutoIdent and VideoIdent products can finish up the identification process 24/7 in seconds.

Furthermore, IDnow recently got the official approval from the ANSSI to offer Video Identification on the French market and is therefore the first and only provider to do so.

IDnow is committed to make the connected world a safer place whether this is for private organisations or the Public sector – we are here to help with our expertise and knowledge. We provide the highest standard security identity verification in Europe.
1.1 WHY IDNOW

Ensure best-in-class conversion rates on any device let you win more customers. IDnow provides fast, paperless and secure customer onboarding. We also provide advanced artificial intelligence (AI) driven security checks to avoid fraud, delivering the highest level of security.

We are also compliant to the highest levels of Regulations. Modular identity verification process can be adapted to match any legal requirements.

END-USER EXPERIENCE:

- Second to none offering of high security and end user convenience for customers and end-users
- Images are captured automatically, users do not have to manually take images resulting in better user experience and higher image quality
- IDnow recognises IDcards (National IDs, passports, Driver Licenses) automatically, user does not have to select manually from long and inconvenient lists of documents
- Reading data from the backs of driving licences incl. validity dates
- Results delivered in less than 5 minutes
- Excellent end-user experience proven by an 8.8/10 Ranking on Trust Pilot
  And a 4.6 ranking in the app store

SAFE AND PROVEN TECHNOLOGY:

- Use of Videos and not individual images leading to a higher security level
- Geo-redundant German Data Centers
- Completely aligned with the requirements of the GDPR
- Automatic blacklist across our customer base, if fraud is detected
- Real recognition of security features, based on video stream (holograms, kinegrams, Identigrams, etc.)
- Automatic additional security checks like checksum verification, consistency of data, etc.
CUSTOMERS:
- Big and traditional companies rely on our solution (Banking Industry) as well as Challenger Banks and customers from many other Industries
- Large footprint and experience in the Gaming industry

WHAT ELSE:
- IDnow VideoIdent
- Support of eID / NFC (ID cards, passports) for higher conversion rates, better data quality and lower fraud rates
- Ease of integration, great documentation for developer for simple implementation
- Native SDKs for iOS and Android

TECHNICAL DESCRIPTION OF AUTOIDENT
The AutoIdent Product is made possible through Artificial Intelligence and Machine Learning Technology. IDnow’s background in digital online identifications and knowledge acquired through millions of verifications done through its VideoIdent product enabled us to train neural networks, leading to an automated identification process. We have networks trained for:

- Segmentation, finding the ID Documents;
- Classification, automatically detecting which sub-type of an ID Document is being used;
- Security features detection, determining if a Security Feature is behaving in the correct manner.

Additionally, we utilise a specialised OCR engine to extract the data from any ID document. Due to our vast experience with different ID documents, we understand where and how information on these documents are displayed and can accurately read and check the data to provide the highest level of data quality.

We also integrate world renowned solutions, like DERMALOG to enable face comparison and build 3D models of users’ faces.
2 AUTOIDENT

1.2 USER JOURNEY

After signing up for your service on your website, end user will start the verification process using AutoIdent

1.3 RETRIEVED DATA

- Real Time result: Success, Pending, Fraud_Suspicion_Pending
- Final result: Success, Cancelled (+reason, seen in API documentation), Fraud (+reason, seen in API documentation),
- Image of the front side of the ID document
- Image of the back side of the ID document
- Image of the user’s face on the ID document
- Image of the Selfie *
- Image of the Left side of user’s face *
- Image of the Right side of user’s face *
- Image of the Security feature shown and not shown on the document * **
- XML file of all read out data
- Data read out is configurable per customer and is dependent on the fields available on the document
- PDF file of all read out data and images
- Data read out is configurable per customer and is dependent on the fields available on the document
1.4 TECHNICAL INFRASTRUCTURE

IDnow has organizational and technical measures in place in order to protect the data assets of our customers. The organizational and technical measures are documented in the IDnow Security Concept which implements the ETSI EN 319 411-2 (Qualified Electronic Signature). IDnow is regularly audited against the compliance with the Security Concept.

All IT systems, such as the application server, the databases, and other components such as switches, are redundant. The hard drives are mirrored through a RAID process and the stored data continuously backed up in a daily backup process. The backup is stored in a physically separate datacenter. Regular checks of the restore capacity of the backups take place. In the datacenters which IDnow uses, an uninterruptible power supply is guaranteed.

Data-in-transport is encrypted according to BSI TR 02102 by using TLS 1.2 with a fixed set of cipher suites. The Video-/Audio-Communication is secured using DTLS 1.2 according to BSI TR 02102.

Data-at-rest resides in our secure data center hosted in Nuremberg, Germany. Data-at-rest can be encrypted according to NIST standards with AES256/GCM. We use a NIST recommended key-derivation method to generate unique keys per business process (identification) using the PBKDF2 key derivation method.
1.5 SCOPE OF SERVICES

Dedicated Customer Success Manager + Account Manager

- A main technical contact person is named as first point of contact for the entire contract duration for all technical questions and inquiries.

Support during Integration

- The technical integration is supported by the CS Team. During this process, the CS Team is also coordinating the communication with other IDnow teams, such as IT or Operations.
- Kick off workshop with IDnow Product Specialist (remote/onsite)
- The integration phase is finalized with a successful acceptance test by Cubic Telecom.

Support after Integration

- Daily status update calls during the soft launch
- Regular remote provider meetings
- Onsite provider meetings
- Access to our Datawarehouse for a full integration into the existing BI-Software
- Access to our BI-Software “Tableau” where customer can access a broad range of KPI Reports that will be updated daily
- Access to our “Live”-Reporting in addition
- Sophisticated Incident Management Policy
- Access to our Jira Service-Desk Ticket Board

Onsite conversion workshops with UX Specialists

- The workshop can be done either remotely by Videoconference or onsite at IDnow site. Attendees of the workshop are at least one member of the CS team, and possibly further experts of IDnow (e.g UX-Designer).
- The workshop will include the Following:
  a. Review of the customers process by an IDnow expert
  b. Comparison with best-practices in industry
  c. Development of suggestions for improvement of conversion
- The workshop result will be reflected in a presentation, created by IDnow.

Other functionalities
1.5.1 PRODUCT DELIVERABLES

- **Full SDK documentation**
  - Our SDK is available for Android and iOS. Android versions support is from 5.0 up and iOS from 10.0. This doesn't affect quality of the product. All documentation is provided with the SDK, with consistent upgrades provided to the customer on a monthly basis.
  - During the SDK integration process our clients have dedicated Client Success Managers to support in the process.

**API documentation**, as through API we deliver the results files with all information regarding identification.

3 VIDEOIDENT
The German Federal Ministry of Finance published the latest circular on 12th December 2017. In it the requirements under the Money Laundering Act regarding identification via video transmission are laid out in detail. IDnow operates an electronic identification system (identification service), which implements these requirements as outlined below. IDnow is the leading service provider for video-identifications in Europe - with the largest number of customers and the most advanced technology. As such, we are the first choice for companies of all sizes. Our list of references includes:

- Institutional banks: E.g. Commerzbank (Germany’s 2nd largest bank with 11.5M customers)
- Cooperative banks: We are the premium partner for the entire VR bank group with over 1.200 banks in DE
- Payment service providers: Companies as ConCardis (cashless payments leader) and Paysafecard offer IDnow to their customers
- FinTechs: IDnow is the preferred partner for all FinTech-Companies, as e.g. Number26, CMC Markets and more
- Several other segments in AML and mobility

1. Deliverables

1.1. Process description Online-Identification
IDnow identifies persons (end users) for the Customer. To this end, IDnow uses its identification service, which facilitates the identification of end users via video transmission. End users have access to the identification service via mobile devices or computers if they can connect to the Internet and this connection permits a video chat.

1.2. Integration in the existing “Becoming Customer” process

1.2.1. Access channels of the identification service for end users
The end user may use the identification service via a smartphone app or web browser. These channels shall be accessed via a website provided by IDnow which the Customer can integrate into its own websites or in e-mails via iFrame, Popup or hyperlink. Regardless of the hardware of the end user detected by IDnow, IDnow shall offer the end user various access channels on the website provided.

**Smartphone APP**

- IDnow provides a smartphone app (IDnow app) for this purpose. The end user may download and install the IDnow app from the respective app store.
- IDnow provides a technical interface (SDK), with which the customer can integrate the functionality of the identification software in its own app.
- The smartphone app operates on smartphones with sufficient computing power and camera resolution and the iOS (Apple) or Android (Google) operating systems.

**Web browser**

End users can also access the service via web browser on a PC. IDnow operates a website to this end, which contains its own video transmission program.

### 1.2.2. User data transfer to IDnow

**IDnow provides several options to transfer the initial user data:**

- Date transfer via Representational State Transfer (REST) API
  
  The data can be transmitted and requested. Authentication is performed via shared secrets. Encryption via the standard TLS protocol.
- Get Parameter
  
  User data is transferred via URL
- User Data Form
  
  IDnow provides a website with a user data form that is filled by the user

### 1.2.3. Look and feel

- Individual texting
- Co-Branding on channel selection website
- Complete white label solution for web frontend
To realize a full, seamless and smooth integration, IDnow suggests the following technical solutions:

- **Data transfer via Representational State Transfer (REST) API**
  The data can be transmitted and requested. Authentication is performed via shared secrets. Encryption via the standard TLS protocol.

- **Frontend integration via iFrame (web) and SDK (mobile)**
  The end user can access the services via his/her smartphone app or via a Web browser. Access to these channels happens via a Website operated by IDnow, which companies can integrate in his/her own Websites through iFrame or Popup or use in his/her emails via a hyperlink.
  For integration into an external mobile application, IDnow provides a Software Developers Kit (SDK) that can be implemented. The SDK is provided here freely via IDnow website: [www.idnow.eu/developers](http://www.idnow.eu/developers). Alternatively, IDnow can provide a complete white label app (will be charged extra).

- **Custom abort / success URL / individual Texting:**
  After a finished identification or if the identification is aborted, the user is led to specific websites that can be customized by the company (custom URL). During the process, the user will be addressed by the identification specialist with a custom texting for any organisation.

### 1.2.4. Partial integration

For a partial integration IDnow operates a website which contains its own video transmission program.

- The initial user data can be entered into a user data form, that is provided by IDnow. The identification result can be provided by encrypted e-mail, SFTP server or download portal

- The end user can access the legitimation either via IDnow website (browser must support WebRTC as mentioned in 2.2.1) or via IDnow mobile app that is available for Android and iOS. The user can request for an installation SMS to
easily access the mobile app.
- Flexible access to the service, custom URL and custom texting are also available for partial integration.

1.3. **User Handling**

**Language**
IDnow service is available in German and English (frontend, in-line texting and conversation with the ident specialist).

**Data transfer**
As stated in 2.2 the data already entered by the user can be transferred to IDnow via REST API, when the user initializes the process. This applies both for a full integration and a partial integration scenario.

**Availability**
The IDnow identification service hours are between 8am and 12pm CET. 24/7 is optional.

**Customer support**
The end user support is available via mail or via phone.

**Technical Requirements**
IDnow provides the service for notebooks / desktops and mobile devices as tablets or smartphones.

Requirements:
- Standard browsers are supported (e.g. Firefox, Opera, Chrome) in their latest versions. The Web browsers must support WebRTC (Web-Real-Time-Communication).
- IDnow supports iOS (iOS 7.0 & min. iPhone 4S/ iPad 2) and Android devices (Android 4.0 & device generation 2013 or newer)

1.4. **Transfer of legitimation results**
IDnow provides the results of the legitimations in a zip-archive (*see example file delivered with this proposal*). This contains:
1.5. General specifications

1.5.1. Server/Computer Centre

IDnow hosts its IT processes for the service with noris network AG, Nuremberg, Germany.

The server system used consists of redundant data bank servers, redundant application servers, routers, load balancers and a backup system. A firewall protects the server system. All servers deployed feature mirrored disks, redundant power supply units and multiple power connections.

IDnow may change the computer centre, insofar as the server of another computer centre provider offers similar failsafe performance.

1.5.2. Data Backup

IDnow operates continuous data backup for all data collected while operating the services. IDnow keeps these data for a 90-day period. After 90 days the data are deleted. This backup safeguards the redundant design of server components, a switch from master to redundant slave database in the event of failure, and a daily backup of the database on an external backup storage system.

1.5.3. Data Protection

IDnow takes measures to ensure data protection according to data protection law.
(see IDnow TOMs attached in the information package). IDnow appoints an external data protection officer to certify that TOMs are fulfilled. In addition, IDnow ensures its clients the possibility to audit processes due to data protection.

IDnow also has been certified for PS 951 (see certification attached in the information package) has been certified by TÜV-IT for the qualified electronic signature according to German signature law (see certification attached in the information package).

1.5.4. Test/Staging Environments
IDnow offers the Customer a test or staging environment. The interface (API) of this test environment is identical to the production environment. The test environment does not carry out – subject to agreements to the contrary – any events with Ident specialists, instead it provides positive or negative results depending on the cue entered. IDnow provides Customers with the test environment upon request. Should the Customer request a live test using Ident specialists, this can be arranged but it is charged extra.

1.5.5. Availability – Waiting Periods (SLA)
A waiting period in the sense of this proposal is the time between receipt of a connection request on the Webpages of the IDnow server and the definite establishing of a connection between end user and IDnow Ident specialists. The standard SLA is 80/2: IDnow accepts 80 % of the service requests received during the service time within a waiting period of two minutes. SLA 90/1 is optional.

1.5.6. Maintenance Works
IDnow shall carry out maintenance works during periods when a low frequency of events is to be expected. The effects on the systems are kept as minimal as possible. Normal maintenance works are usually scheduled between midnight and 6.00 am. In general, maintenance works do not exceed 4 hours per month. In the event of required maintenance works foreseeably leading to more than 4 hours,
the Technical Service Manager shall first agree the timing of these works with the Customer.

1.5.7. Monitoring / Incident Management

IDnow constantly monitors the technical and operative systems through internal and external availability checks testing systems, applications, databases and APIs. In the event of a failure of the IDnow service, the IDnow Network Operations Team automatically receives an alarm message. The team then initiates a fault isolation and a cause analysis. Should the failure result in considerable impairment of the service, IDnow shall email the Customer information regarding the type of failure and its expected duration, and the counter measures implemented.

The Network Operation Team accepts technical reclamations or fault reports 24 hours a day, seven days a week. IDnow shall advise the Customer as to the Network Operation Team’s contact details, especially their email address.

1.5.8. Documentation

IDnow documents the overall solution and the technical setting of the systems as well as any alteration requests and maintenance works. IDnow makes the documentation available in electronic format insofar as this is necessary for a reliable and secure operation.

1.5.9. Client Separation

IDnow executes the data processing for the Customer in a logically separate way from other data processing for other customers, so that no data nor their assignment to a waiting end user (waiting queue) in any one event can get mixed up. Surplus volumes for another customer shall not result in delays in the processing of the Customer’s waiting queue.

1.6. Additional remarks
Unique token

An identification token is active in the system for a standard time period of 90 days. The identification can be accessed by the user by a unique transaction code.

IDnow eSign

In addition to the IDnow VideoIdent, IDnow eSign offers a service with which the end customer can be identified via an online video chat, allowing him/her subsequently to sign his/her declaration of intent with a qualified electronic signature.

With eSign, IDnow enables clients a complete paperless application process that allows end user to sign contracts for financial product. During the process, the end user is connected to an IDnow ident specialist from the beginning to the end, enabling a safe, quick and convenient user experience. Due to the qualified electronic signature (QES), IDnow eSign fulfills written form requirements and is therefore valid for products like e.g. consumer loans.

With the new European regulation framework in effect (eIDAS), IDnow eSign is valid across all the EU.

(24 April 2020)