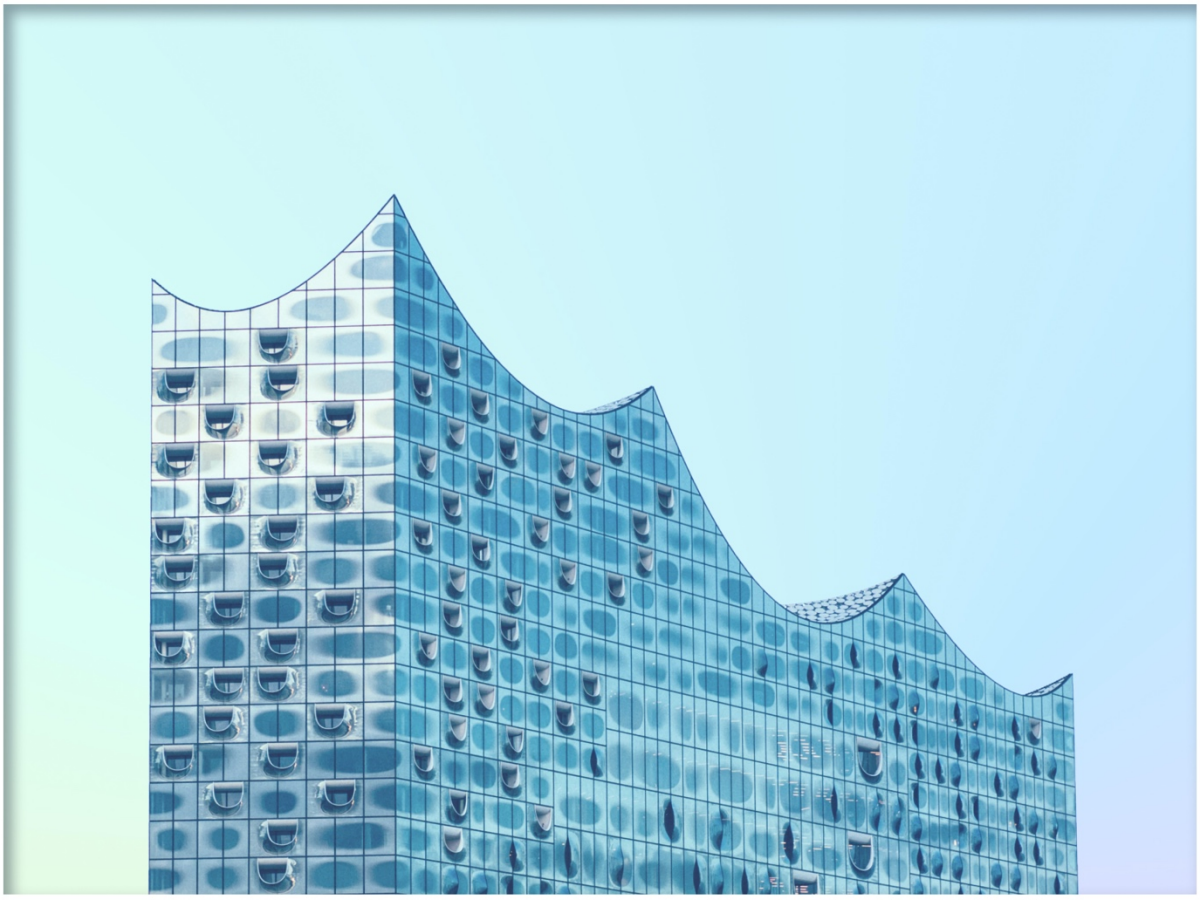
Nect GmbH

Nect Trust Services Practice Statement



Trust Services Practice Statement (TSPS)

Document History

Version	Date	Changes
1.0	March 2020	Skeleton, first content, descriptions added.
1.1	April 2020	Finalised content, consulted respective area owners and added updates.
1.2	April 2020	Updated content according to Stage 1 Report feedback
1.3	May 2020	Updated content according to Stage 2 Report feedback
1.4	November 2020	Correction to address.
1.5	June 2021	Content revised after the additional criteria were published by the Bundesnetzagentur and after review against these criteria by the CAB.
1.6	June 2022	Product rebranding *Robo-Ident* to *Nect Ident*

1. Introduction

Nect GmbH was established in 2017 in Hamburg, Germany. Nect's core product is an online services for identity verification of natural persons (in the following "persons" or "users") in order to support Nect's partners needing confidence in the real identity and/or specific parameters such as age of their users.

In addition, in collaboration with qualified trust service providers and contract partners Nect enables individual users of the contracted partners (in the following "partners") to electronically sign legally binding contracts using advanced or qualified electronic signatures according to the eIDAS regulation.

The identity verification services are compliant with the Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).

In particular, Nect verifies the identity of natural persons in accordance with eIDAS, Article 24, paragraph 1 d) by using "other identification methods" recognized in Germany which provide equivalent assurance in terms of reliability to physical presence.

As part of the official recognition according to §11 of the German Trust Services Act (Vertrauensdienstegesetz ("VDG")), Nect GmbH's Nect Ident procedure underwent an audit by an accredited conformity assessment body ("CAB"). The result is a positive, EU-wide valid conformity assessment report ("CAR"), as well as a module confirmation according to §11 VDG in Germany.

This document is the Nect's Trust Service Practice Statement (TSPS). It is not a full Certification Practice Statement (CPS) according to RFC 3647 because Nect only provides identity verification services but does not currently offer other certification services like issuing certificates or the provision of certificate validation services.

The purpose of this document is to serve as a base for compliance with eIDAS.

1.1 Overview

Nect services allow users to be reliably identified digitally, without direct physical or virtual contact to a second person ("service agent"). Nect delivers the results ("evidence") of identity verifications in the electronic form to its partners and/or to certification service providers for the issuance of qualified electronic certificates.

The qualified certificates may then be used to sign legally binding electronic documents or verify the identity of natural persons. The Nect consists of several individual verification services offered via system-native applications for various systems, e.g. Android mobile devices or iOS mobile devices, each offering full functionality.

The frontend applications are continuously being further developed. In addition to testing for possible security vulnerabilities, the security improvements of the respective operating systems are integrated.

Nect offers its services to all users of its contract partners without discrimination. Nect is committed to always take additional measures to support users with disabilities like ensuring high contrast and support voice over. Due to the nature of the processes (video recording), there are certain limitations regarding the disabilities that can successfully perform the process.

The services of Nect GmbH have been assessed for compliance with the requirements of eIDAS according to the standards

- ETSI EN 319 401,
- ETSI EN 319 411-1, and
- ETSI EN 319 411-2

as well as the

- additional criteria issued by the Bundesnetzagentur on April 1st, 2021.

The compliance to these regulations has been confirmed by an accredited CAB.

The synchronous and asynchronous legally required sample inspection and, if necessary, support of machine processing (“human-in-the-loop”) is performed according to legally admitted procedures by experienced identity verification specialists that undergo regular training.

The usage of the Nect services is defined by the Terms of Service, the Data Privacy Statement and by the declaration of consent as well as the optional consent to improve services.

1.2 Document Name and Identification

The document is the “Trust Service Practice Statement” of the Nect GmbH and bears the indication of version 1.5 as of June 2021.

1.3 PKI Participants

1.3.1 Certification Authorities

A Certification Authority (CA) is an entity authorized to issue public key certificates. A CA is also responsible for the distribution, publication, and revocation of certificates.

Nect GmbH does not operate a CA but offers identification services on behalf of CAs.

1.3.2 Registration Authorities

A Registration Authority (RA) acts on behalf of a CA. RAs are responsible for verifying both business information and personal data contained in a subscriber’s certificate.

An RA submits certificate requests to issuing CAs, approves applications for certificates, renewal, or re-keying, and handles revocation requests.

Nect GmbH does not operate an RA but offers identification services on behalf of a CAs RA

1.3.3 Subscribers

Subscribers are the end-entities of certificates issued by a CA. Subscribers are individual persons.

Nect GmbH identifies the subscribers on behalf of contracted partners or CAs.

1.3.4 Relying Parties

A Relying Party or contracted Partner; is an individual or entity that relies on a certificate. A Relying Party or contracted Partner uses a Subscriber’ s certificate to verify the integrity of a digitally signed document and to identify the signer of the document,

1.3.5 Other Parties

Nect uses 3 data centres and 2 back up servers to operate the service. The data centres provide only space while the hardware is Nect owned, managed and deployed. There is a service provider agreement in place with each data centres. The scope of service provided is regulated in the contract. There is a notification system in place provided by the data centre operators, which notify Nect about outages, maintenance or any other relevant updates.

1.4 Certificate Usage

Not applicable, Nect GmbH provides identity verification services and does not issue certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This TSPS is administered by: Nect GmbH, Großer Burstah 21, 20457 Hamburg

1.5.2 Contact Person

Compliance Officer, Nect GmbH, Großer Burstah 21, 20457 Hamburg

E-Mail: compliance@nect.com

1.5.3 Person determining CPS Suitability for the Policy

Nect's Compliance Officer determines the suitability of this TSPS with the Policy.

1.5.4 TSPS Approval Procedure

This TSPS document has been prepared for compliance with the requirements of eIDAS on identity verification.

TSPS document is approved by Nect GmbH Senior Management and published and communicated to all relevant employees and external parties immediately.

The TSPS and the Terms and Conditions are reviewed in regular intervals, at least once a year. Amendments to these documents must be approved by Nect GmbH Senior Management before becoming effective.

The Terms and Conditions are made available to all subscribers and relying parties (partners) through durable means of communication. Amended versions or updates of this TSPS, the PKI Disclosure Statement (PDS) and the Terms and Conditions are published immediately at the website.

Nect shall notify the supervisory authority of any changes in the provisions and of any intended discontinuation of the trust service activities.

1.6 Definitions and Acronyms

Not required.

1.7 References

ETSI EN 319 401	ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 4111	ETSI EN 319 4111, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 4112	ETSI EN 319 4112, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
eIDAS	Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

2. Publication and Repository Responsibilities

2.1 Repositories

Nect GmbH publishes this TSPS and other relevant documents like General Terms and Conditions (AGB) and the Data Protection Statement on its website https://nect.com.

2.2 Publication of Certificate Information

Not applicable. Nect GmbH does not issue certificates.

2.3 Time or Frequency of Publication

This TSPS and any subsequent amendments are made immediately publicly available after approval. Nect GmbH develops, implements, enforces, and annually updates this TSPS to meet the compliance standards of the documents listed in Section 1.7.

The websites of Nect are publicly available 24 hours per day, 7 days per week. Upon system failure or other kinds of outages, Nect will restore proper function without delay.

2.4 Access Controls on Repositories

The repository is publicly and internationally available. Read-only access is unrestricted.

Nect protects the integrity and authenticity of all documents in the repository. The repository is subject to access control mechanisms to protect its availability and prevent unauthorized persons from adding, deleting, or modifying information in the repository.

3. Identification and Authentication

3.1 Naming

Not applicable. Nect does not issue certificates.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

Not applicable. Nect does not issue certificates.

3.2.2 Authentication of organization entity

Not applicable. Nect does not issue certificates.

3.2.3 Authentication of individual identity

The customer's identity is checked against an official, valid, government-issued photo ID document. International passports must fulfill the ICAO 9 303 Standards.

The authentication of the individual identity is checked in different ways:

I. Nect Ident

The user is requested to record a video of their ID document as well as a selfie video. Depending on the document type further request can be made to the user, such as a recording of the back-side of the ID card, a recording of the signature page of the passport or to hold the document onto the smartphones NFC antenna to read out the data stored on the ID document's chip.

The service is generally able to optically (OCR) and/or electronically (e.g. NFC) read out all necessary information from the ID document and provide them electronically to the relying party, such as a CA. In most cases the data includes:

- full name (including surname and given names consistent with the national identification practices),
- date and place of birth,
- reference to a nationally recognized identity document,
- or other attributes which can be used to, as far as possible, distinguish the person from others with the same name.

For legally required archival, the service provide further data such as:

- copy of identity report file (incl. ID document copy and verification results),
- acceptance report of terms and conditions (audit trail).

The Nect technology is designed to provide equivalent assurance in terms of reliability to physical presence.

All data transmission to / from communicating entities is fully encrypted (without exception) in accordance with TR-03116-4 (*Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4*, issued 10.01.2020, BSI).

3.3 Identification and Authentication for Re-key Requests

Not applicable. Nect does not issue certificates.

Therefore, Nect does not differentiate between identifications for initial certificate issuance or re-key requests.

3.4 Identification and Authentication for Revocation Requests

Not applicable. Nect does not issue certificates and does not handle revocation requests.

4. Certificate Life-Cycle Operational Requirements

Not applicable.

Nect performs identification services according to chapter 3.2.3. Nect does not issue certificates, does not process certificate applications, and does not provide certificate status validation services.

5. Facility, Management, And Operational Controls

Nect carries out regular risk assessments to identify, analyse, and evaluate risks related to its services taking into account business and technical issues.

Nect then selects appropriate risk treatment measures taking into account the results of the risk assessment.

The risk treatment measures chosen to ensure that the level of security is commensurate with the degree of risk.

The risk assessment is approved by Nect's management who accepts the residual risks identified in the risk assessment with this approval.

5.1 Physical Security Controls

Nect has implemented a general security policy which supports the security requirements of the services, processes, and procedures covered by this TSPS. Nect enforces measures to deny unauthorized persons access to the buildings and data processing facilities where personal data are processed.

These security mechanisms are commensurate with the level of threat in the identity validation environment.

5.1.1. Site Location and Construction

Nect operates its platform from the main location in Hamburg.

All operations related to identity verification are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

Several layers of physical security controls restrict access to the sensitive hardware and software systems used for performing operations. The systems used for identity validation services are physically separated from other systems so that only authorized employees can access them.

All services operated by Nect GmbH are hosted in German data centers on devices in possession of Nect GmbH, deployed in Hamburg, Hannover and Bremen. All data centers are certified by ISO 27001 standards. Nect has with every data center, which are service providers, an effective service provider agreement.

All Data centers in use by Nect are Tier Level 3, the one in Bremen is Tier Level 4. All data centers are equipped with redundant servers, storage, network links and other IT components that corresponds to Level 3, where data center IT components are powered with multiple, active and independent sources of power and cooling resources.

5.1.3 Physical Access

Nect protects its relevant systems, especially database servers and the systems used by the identity validation specialists with physical security mechanisms to:

- permit no unauthorized access to the hardware,
- store all identity validation data in encrypted form,
- monitor, either manually or electronically, for unauthorized intrusion at all times,
- maintain and periodically inspect access logs.

Nect has implemented physical access controls to reduce the risk of unauthorized persons being able to access Nect's premises. This includes the workplaces of identity validation specialists as well as database servers, routing and switching components, and firewalls.

Access to Nect's premises is guarded by CCTV surveillance.

5.1.4 Water Exposure

All systems have reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire Prevention and Protection

All systems have industry-standard fire prevention and protection mechanisms in place. Nect has appointed several members as BET (Building Evacuation Team) who are also trained to work with fire extinguishers.

5.1.6 Waste Disposal

Sensitive documents and materials occur only in electronic form. Media used to collect or transmit sensitive information are securely erased before disposal. Regulations for the disposal of paper documents (shredder or by a certified service provider with disposal certificate). Data medium destruction according to DIN 66399 with at least protection class 3.

5.1.7 Off-site backup

Nect performs regular routine backups of critical system data, audit log data, and other sensitive information to two redundant off-site locations in different ISO-27001 certified data centers. All data is protected by an additional layer of encryption.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted persons include all employees that have access to or control video identification data. For the services provided by Nect these roles are identity verification specialists (or identity verification agents), system administrators, security officer, and auditor. Special roles include:

Security Team

The Security Team consists of the Head of Technology & Security and several security experts. In addition to developing personnel, organisational, technical and infrastructural security measures, the security team is also responsible for implementing these measures and maintaining them during ongoing operations. This requires not only regular training of all Nect employees but also adjustments to the current security situation in order to be able to react to any security incidents that may occur.

Data Protection Officer

In line with the European Commission's general data protection regulation (GDPR), Nect has appointed a Data Protection Officer. The data protection officer is supported by a team of qualified employees. With respect to data security, the Privacy Team works closely with the Nect’s Security Team as well as with the Management Team.

Identity Specialist Team

The Identity Specialist Team consists of highly qualified and trained individuals in the area of document verification and fraud detection. It provides support and checks the identity cases which

- are selected for random and/or legally required quality sampling,
- are selected for asynchronous human verification (up to 100%, based on contractual or legal requirements),
- require human intervention (human-in-the-loop).

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

Personnel in trusted roles is named and approved by senior management of Nect GmbH before being permitted to access CA relevant systems.

Identification and authentication during operations for each role are based on individual passwords and individual access tokens and PINs.

Personnel have no access to trusted functions until the necessary checks are completed.

Personnel in trusted roles is named and approved by senior management of Nect GmbH before being permitted to access relevant systems requiring the principle of "least privilege" when accessing or when configuring access privileges.

All employees of Nect are thoroughly checked for their qualifications for the tasks for which they are responsible before being hired. Training and previous employment are examined on the basis of training and work certificates.

5.2.4 Roles Requiring Separation of Duties

All personnel performing sensitive operations are assigned a trusted role. Segregation of conflicting duties and areas of responsibility is implemented to reduce opportunities for modification and misuse to its minimum.

5.3 Personnel Controls

5.3.1 Qualification, Experience, and Clearance Requirement

All employees involved in the operation of Nect systems and all identity verification specialists have appropriate knowledge and experience related to their duties.

They must have demonstrated security consciousness and awareness regarding their duties and receive the appropriate training in organizational policies and procedures.

All employees of Nect have signed a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment.

Managerial personnel possess professional experience and are familiar with security procedures for personnel with security responsibilities. Personnel in trusted roles are held free from conflict of interest that might prejudice the impartiality of operations.

5.3.2 Background Check Procedures

All employees of Nect are thoroughly checked for their qualifications for the tasks for which they are responsible before being hired. The check consists at a minimum of the following areas:

- employment,
- education,
- place of residence,
- criminal background check (*Führungszeugnis* according to § 30 *Bundeszentralregistergesetz* for all employees of Nect),
- references (if available).

Training and previous employment are examined on the basis of training and work certificates.

The checks must be clear of records related to trustworthiness. Regular periodic reviews are performed to verify the continuous trustworthiness of all personnel.

5.3.3 Training requirements

All employees performing duties with respect to the operation of the Nect GmbH systems and services receive comprehensive training. Training is conducted in the following areas:

- information security,
- compliance,
- data protection,
- fraud detection and prevention,
- relevant norms and standards,
- security principles and mechanisms,
- use and operation of the Nect platform and systems,
- incident handling and reporting,
- disaster recovery procedures.

Nect conducts regular security training sessions to raise awareness of Information Security and Data Protection. Training is mandatory not only for Nect's technical staff (e.g. system administrators, data scientists and developers), but for all employees. The courses cover all relevant topics of Information Security and Data Protection, from current threats to attacker procedures (including social engineering) to the consequences of successful attacks and methods for risk minimization.

In addition to the Identity Specialist all employees (e.g. developers) are being offered and sometimes required to participate in an ID document verification and fraud detection training.

5.3.4 Retraining Frequency

Retraining is performed to the extent and frequency required to ensure that the required level of proficiency is maintained.

The Identity Specialists are retrained externally once a year to ensure the latest and up to date information on identity fraud and prevention while regular retraining is offered internally to the extent and frequency required to ensure that the required level of proficiency is maintained.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions are taken in case of unauthorized actions.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures.

5.3.7. Independent Contractor Requirements

Not applicable as Nect does not work with independent contractors for the development or operation of its trust services.

Should independent contractors be required to support the regular employees they must fulfill the same requirements as regular employees.

5.3.8 Documentation Supplied to Personnel

This TSPS, applicable system operations documents, operations procedures documents, and any relevant other documents required to perform their jobs have been made available to Nect employees.

5.4 Audit Logging Procedures

5.4.1 Types of Events Logged

Nect keeps audit trails and system log files that document actions taken as part of the identity verification services. All relevant events related to the services provided are logged.

Log entries include the following elements:

- date and time of the entry,
- serial or sequence number of entry, for automatic journal entries,
- identity of the entity making the journal entry,
- description/kind of entry.

The identity verification logs include, but are not limited to:

- interaction with the identification Service (by customers and end-users, e.g. via a mobile application),
- kind of identification document presented by the end user,
- information about the automatic processing of the documents and other information presented by the end user,
- record of unique identification data of identification document (e.g. ID document serial number),
- identity of the identity verification specialist performing the identity proofing.

All security audit logs are automatically collected.

5.4.2 Frequency of Processing Log

Nect‘s system and its components are continuously monitored and can provide real time alerts if unusual security and operational events occur and allow an immediate review by system security administrators.

5.4.3 Retention Period for Audit Log

Logs and records are archived for as long as required by the respective legislation and specific regulations.

5.4.4 Protection of Audit Log

Procedures are implemented to protect archived data and audit data from destruction or modification prior to the end of the audit log retention period.

Audit logs are moved to a safe, secure storage location separate from the component which produced the log. Access to audit logs is strictly restricted to authorized personnel and all access is monitored and logged independently.

5.4.5 Audit Log Backup Procedures

Nect performs regular routine backups of audit log data to two redundant off-site locations in different ISO-27001 certified data centers. All data is protected by an additional layer of encryption.

5.4.6 Audit Collection System (Internal vs. External)

Audit data is generated and recorded automatically at the application, network, and operating system level.

Where this is not possible audit data is generated manually and recorded by personnel.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessment

The security team regularly checks the effectiveness of the implemented measures, also by simulating its own attacks (hacking, but also e.g. phishing attacks), and thus tests the effectiveness of the security measures and security training courses. A daily automated security scan is performed to proactively detect and respond to new potential vulnerabilities. External security audits are performed at regular intervals.

In addition, based on events in the log files the security team initiates vulnerability assessments.

5.5 Records Archival

5.5.1 Types of Records Archived

At a minimum, Nect records the following data for archival:

- the TSPS (this document),
- contractual obligations,
- system and equipment configuration,
- modifications and updates to systems or configurations,
- audit logs mentioned in section 5.4,
- documentation required by compliance auditors.

5.5.2 Retention Period for Archive

Long term archival of identification data according to the requirements of eIDAS is regulated by contractual agreements with the CA. Either the CA is responsible for archival of identification or the CA contractually agrees with Nect GmbH that long-time archival is in the responsibility of Nect GmbH.

5.5.3 Protection of Archive

Nect protects the archive so that only authorized persons in trusted roles are able to access the archive. The archive is stored in a trustworthy system protecting it against unauthorized viewing, modification, deletion, or another tampering. The media holding the archive data and the applications required to process the archived data is maintained to ensure that the archive data can be accessed for the time period defined above.

5.5.4 Archive Backup Procedures

Nect performs daily database and storage backups.

5.5.5 Requirements for Timestamping of Records

No stipulation.

5.5.6 Archive collection Systems

The archive collection systems are internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to the archive is restricted to personnel in trusted roles.

Information in the archive is verified in regular intervals as described in section 5.4.2

5.6 Key Changeover

Not applicable. Nect does not handle CA keys.

5.7 Compromise and Disaster Recovery

Nect has implemented a disaster recovery and business continuity plan intended to allow restoration of business operations in a reasonably timely manner following an interruption to, or failure of, critical business processes.

On the basis of mobile communication and VPN-based use of internal IT-systems and data, Nect employees can work in a decentralized manner from different locations and even from home until the availability of the primary office location is restored or a contingent location ready for use.

5.7.1 Incident and Compromise Handling Procedure

Backups of essential business information are performed on a regular basis. Nect tests internal disaster recovery procedures regularly. Incidents affecting the security or the integrity of Nect's services are reported to the relevant CA(s) and to the supervising authority without unnecessary delay (in any case within 24 hours) after Nect has become aware of the incident.

Impacted users are notified without unnecessary delay.

Head of Technology and Security and C-Level as well as the Data Protection officer are informed and involved accordingly and act in accordance with the incident and notification plan.

Bundesnetzagentur (BNetzA) shall be notified without delay of any severe incidents and/or changes to TSPS via tsp-incidents@bnetza.de. Additionally, impacted persons shall be notified without delay.

5.8 CA or RA Termination

Not applicable. Nect does not operate a CA or RA Services.

6. Technical Security Controls

Nect has implemented and operates a number of security controls in order to protect user's data and the application

6.1 Key Pair Generation and Installation

Not applicable. Nect does not generate keys.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Not applicable. Nect does not generate and manage keys.

6.3 Other Aspects of Key Pair Management

Not applicable. Nect does not generate and manage keys.

6.4 Activation Data

Not applicable. Nect does not generate and manage keys.

6.5 Computer Security Controls

A general information security policy document (security policy) is available and has been approved by management. It is published, and communicated, as appropriate, to all employees affected by it. This policy may be supplemented by detailed policies and procedures for personnel involved in identity verification.

The information security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing. It contains a statement of management intent, supporting the goals and principles of information security, and gives an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization.

The information security policy lists general and specific responsibilities for information security management, including reporting security incidents, and contains references to documentation which supports the policy. Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.

Nect's management ensures that there are clear direction and visible management support for security initiatives. Nect's management is responsible for maintaining the security policy and coordinates the implementation of information security measures. This includes regular reviews (at least yearly) of the information security policy and associated documents like the risk assessment, the inventory of assets, and the TSPS.

The risk assessment is approved by Nect‘s management, reviewed regularly and revised if necessary. The management accepts with this approval the residual risks identified in the risk assessment.

6.5.1 Specific Computer Security Technical Requirements

All Nect systems were designed from the outset with a view to the secure implementation of the Nect service (Security by Design). These include not only the cryptographic methods used, but also the technical infrastructural, software-side and overarching elements for securing the platform. Consequently, the systems storing and processing software and data are trustworthy systems protected against unauthorized access with multi-layer protection and multi-factor authentication mechanisms.

All data transmission to / from communicating entities is fully encrypted (without exception) and in accordance with TR-03116-4 (*Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4*, issued 10.01.2020, BSI).

All systems are protected against viruses, malicious, and unauthorized software.

Patches or updates for network security software components or operating system components are applied after their relevance and applicability have been verified.

All systems are hardened, i.e. all unnecessary user accounts, applications, protocols, and ports are removed or disabled.

Access to systems is restricted to individuals with a valid business reason for such access. General application users have no accounts on production systems.

User and account management has been implemented. Access rights are granted based on the role concept. Rights are immediately removed if no longer required. In addition, user accounts, roles, and access rights are regularly reviewed.

All data is stored in encrypted form to protect is against manipulations and unauthorized access.

The network with systems for identity verification is logically separated from other components. This separation prevents network access to critical systems except through defined application processes and network paths. Firewalls are installed to protect the production network from internal and external intrusion or other forms of attacks.

Direct access to databases supporting identity verification and storing customer’s identity data is limited to persons in trusted roles having a valid business reason for such access. The workplaces of the identity verification specialists must be physically separated from each other.

6.6 Life Cycle Security Controls

6.6.1 Life Cycle Technical Controls

Development and test systems are separated from production systems.

New software or new applications, releases, modifications and emergency software fixes are installed on production systems only after they have been successfully tested according to the change control policy. Installation of new software or applications prior to approval is not permitted.

6.6.2 Security Management Controls

The configuration of Nect’s systems and any modifications and upgrades must be documented and controlled. Access to and modification thereof is limited to authorized personnel.

Nect’s information security management system is based upon ISO 27001 Standard. It ensures that proper security controls adequate to manage the risks are taken.

6.7 Network Security Controls

Nect has installed adequate protection from both inside and outside attacks such as firewalls, intrusion detection mechanisms, etc.

Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy.

Access to all servers is subject to multi-factor authentication. All access and interaction with administrative systems are logged and monitored.

Regular vulnerability scans and penetrations test are performed by an independent third party as well as internally for all of Nect‘s network components and systems. In addition, attack prevention mechanisms are in place, including brute force attack detection/rate limiting, intrusion detection and network traffic monitoring.

6.8 Timestamping

Cryptographic time-stamps are not required. However, database entries about identification sessions contain time and date information. File names of protocols and other relevant records like log files must include at least the date of creation

7. Certificate, CRL, and OCSP Profiles

Not applicable. Nect does not issue certificates or CRLs and does not operate OCSP responders.

8. Compliance Audit and Other Assessment

Nect is subject to regular external audits. These include audits pursuant to ETSI EN 319 411-1 and ETSI EN 319 411-2 which are required to prove conformity with the regulations made in eIDAS.

These audits require demonstration of a maximum level of security and conformity to well-recognized policies and practices.

In addition, Nect performs internal self-audits. Topics covered by these audits include checks of proper implementation of applicable policies and extensive checks on the quality of identifications performed and on the quality of collected evidence collected during identifications.

The results of these compliance audits are documented and archived. They may be released at the discretion of Nect management to compliance auditors and if required by government authorities for the purpose of legal proceedings.

8.1 Frequency and Circumstances of Assessment

According to eIDAS, article 20 (1) compliance audits according to section 8 must be performed at least every 24 months. Surveillance audits are made 12 months after each full audit.

Additional assessments are required if substantial changes are made to Nect's systems, configurations, or processes that might affect the overall security if the services.

8.2 Identity/Qualifications of Assessor

The conformity assessment required by eIDAS is performed by an accredited assessment body ("CAB").

8.3 Assessor's Relationship to Assessed Entity

Compliance audits must be performed by a public firm that is independent of Nect GmbH.

8.4 Topics Covered by Assessment

The purpose of a compliance audit is to verify that Nect's components comply with the statements of this TSPS, with the eIDAS regulation, and with the requirements specified in the audit standard under consideration.

Thus, all applicable aspects of this TSPS are covered by the compliance audits.

The scope of the ETSI audit includes (but is not limited to) environmental controls, infrastructure and administrative CA controls, network controls, and identity verification processes and procedures.

The assessment by the CAB has included the additional criteria issued by Bundesnetzagentur regarding the conformity assessment of Video-identification with automated means.

8.5 Actions Taken as a Result of Deficiency

If significant exceptions or deficiencies are identified during the compliance audit as defined in section 8 this will result in a determination of actions to be taken. This determination will be made by Nect's management in cooperation with the auditor. Nect's management is responsible for developing and implementing a corrective action plan.

If it is determined that such exceptions or deficiencies pose an immediate threat to identity verification services a corrective action plan must be developed within a period of time agreed upon with the auditor and implemented within a reasonable period of time. For less serious exceptions or deficiencies, the management evaluates the significance of such issues and determines the appropriate actions.

8.6 Communication of Results

No stipulation.

9. Other Business and Legal Matters

9.1 Fees

Fees for the identity verification services are subject to contractual agreements between Nect and its business partners.

Nect does not charge a fee for access to this TSPS. Any use other than viewing, such as reproduction, redistribution, modification, or creating derivatives is not permitted.

9.2 Financial Responsibility

For both contractual and non-contractual customers and business partners, the regulations of indemnification of German law are binding.

Nect GmbH undergoes regular financial assessments to verify that it has the financial stability and resources required to operate in conformity with this TSPS and the requirements of eIDAS.

9.2.1 Insurance Coverage

Nect maintains a Professional Liability insurance coverage.

9.2.2 Other Assets

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Confidential information includes any information provided by customers for purposes of identity verification.

9.3.2 Information Not Within the Scope of Confidential Information

Documents and other information in the repository are not considered confidential/private information.

9.3.3 Responsibility to Protect Confidential Information

All of Nect‘s personnel are responsible for protecting the confidential information in their possession in accordance with this TSPS, in accordance with contractual agreements, and in accordance with the German data protection regulations.

9.4 Privacy of personal information

9.4.1 Privacy Plan

All information that allows the identification of users is protected from unauthorized disclosure.

9.4.2 Information Treated as Private

German statutory data privacy law defines which information must be treated as private.

Further information to be treated as private can be contractually agreed upon.

9.4.3 Information not Deemed Private

The information included in the certificates that are issued by a CA based on identity verifications performed by Nect is considered not to be private.

9.4.4 Responsibility to Protect Private Information

All employees of Nect GmbH receiving private information are obliged to protect it from compromise and disclosure to third parties. All employees must adhere to German privacy laws.

9.4.5 Notice and Consent to use Private Information

Unless otherwise stated in this TSPS Nect GmbH will not use private information without the owner’s consent.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If disclosure of private information about customers is necessary in response to judicial, administrative, or other legal proceedings the information shall be given only to the requesting authority or the customers themselves.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

9.6.1 CA Representation and Warranties

Not applicable.

9.6.2 RA Representations and Warranties

Nect has overall responsibility for all technical and organizational processes and procedures of its identification services.

Nect warrants that it performs identity verification functions as described in this TSPS.

Nect forwards complete, accurate, and verified data about subjects for further processing to the CA.

Retention, archiving, and protection of data are performed according to the stipulations of this TSPS.

Archived subscriber data is protected in compliance with German and European data protection legislation, all data is stored in encrypted form.

Technical services are performed by reliable third party data center personnel. Data center personnel have no access to user data. There is a contractual agreement (Auftragsverarbeitung) between Nect and the Data Centers, which are ISO 27001 certified. These data centers fulfill the redundancy requirement.

9.6.3 Subscriber Representations and Warranties

User warrant that all representations made by Nect on its website and on its platform are true.

9.6.4 Relying Party Representations and Warranties

Not applicable. Nect does not issue certificates.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

Limitations of Liability are subject to contractual agreements between Nect and its business partners. In any case, limitations of liability contained in Nect's General Terms of Service shall apply. Limitations of Liability as specifically agreed on in each individual case, where applicable, remain unaffected.

9.9 Indemnities

The regulations of indemnification of German law are binding

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, customers and CAs issuing qualified certificates based on the identity verification performed by Nect may be required to indemnify Nect for:

- submitting false facts or misrepresenting facts on the user's identity,
- failure to disclose a material fact on the identity verification with intent to deceive any party,
- failure to protect the user's private data, use of an untrusted system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the user's private data.

9.10 Term and Termination

9.10.1 Term

The TSPS becomes effective upon publication on Nect's web site. Amendments to this TSPS become effective upon publication.

9.10.2 Termination

This TSPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Despite the fact that this TSPS may eventually no longer be in effect, the following obligations and limitations of this TSPS shall survive: section 9.6 (Representations and Warranties), section 9.2 (Financial Responsibility), and section 9.3 (Confidentiality of Business Information).

9.11 Individual notices and communication with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this TSPS may be made by Nect's management. Amendments shall either be in the form of a document containing an amended form of the TSPS or an update. Amended versions or updates shall be published in the repository.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances under which OID must be changed

Not applicable.

9.13 Dispute Resolution Provisions

For disputes with end-users and customers the dispute resolution procedures of the issuing QTSPs apply.

Complaints regarding Nect's services can be submitted to compliance@nect.com.

9.14 Governing Law

The applicable law is the law of the Federal Republic of Germany.

9.15 Compliance with Applicable Law

This TSPS is subject to applicable national law, in particular the eIDAS regulation in Germany.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If parts of any of the provisions in this TSPS are incorrect or invalid, this shall not affect the validity of the remaining provisions until the TSPS is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The Nect GmbH shall not be responsible for any breach of warranty, delay, or failure in performance under this TSPS that result from events beyond its control, such as strike, acts of war, riots, epidemics, power outages, fire, earthquakes, and other disasters.

9.17 Other Provisions

No stipulation.