iProov
Trust Service Practice Statement
(TSPS)

for the following processes:

Module 1 - Genuine Presence Assurance (GPA) and
Module 2 - Liveness Assurance (LA)

Version: 2.3
Enforcement date: 10th September 2023

ABOUT

This Trust Services Policy and Trust Services Practice Statement (TSPS) describes iProov's GPA and LA practises and procedures for remote biometric user verification through face recognition and liveness detection as part of the practises of qualified or non-qualified Trust Service Provider (TSP) issuing and managing public key certificates in compliance with the EU Regulation 910/2014 on eIDAS. The GPA and LA services described in this TSPS are meant to be used by TSP in the form of an external module coming with its own eIDAS Conformity Assessment Report (CAR). GPA provides identification of natural persons according to Article 24 1d) of the eIDAS Regulation. LA provides authentication of already known persons, e.g. in the context of remote signing or sealing to authenticate for a specific signing or sealing event.

Document control

This section tracks the changes to this document and acts as a version log. Modifications to this document can only be authorised by the CTO of iProov. All previously authorised versions of the Trust Service Practice Statement shall be rescinded with immediate effect and archived for audit trails and change trail. Minor modification to policies such as edits or additions/ deletions to policies shall be tracked with an increment of the decimal place e.g. 'version 1.2' to 'version 1.3' while major changes consisting of Section modifications shall be tracked with an increment of the units place e.g. 'version 1.7' to 'version 2.0'.

Document history

Version No.	Revision Date	Nature of Change	Document Reviewer	Document Approver
0.1	10/2021	Initial Draft	NB	--
0.2	10-11/2021	Incorporated Initial Feedback	NB	--
0.3	12/2021	Revised Details	NB	--
0.4	01/2022	Further Revisions	MD	–
1.0	10/02/2022	Public Release	MD	DF
1.1	07/02/2023	Review	NB	DF
2.0	10/02/2023	Review and approve	NB	DF

2.1	25/07/2023	Minor amendments 9.6.1, 6.5.1.5, 5.7.1 + inclusion of 1.5.4, 1.5.9,3.2.2.9, 3.2.2.10, 3.2.2.11, 3.2.2.12, 3.2.2.13	NB	DF
2.2	August 2023	Review	NB	DF
2.3	10/09/2023	Minor changes Update 3.2.2.1, 10, 2.2.1, 3.2 Inclusion 3.5,	NB	DF

Contents

1. Introduction

1.1. Document overview

The European Regulation (EU) No 910/2014 of the European Parliament and of the Council (eIDAS Regulation) regulates electronic identification and Trust Services for electronic transactions in the internal market. The eIDAS Regulation:

- ensures that people and businesses can use their own national electronic identification schemes (eID) to access public services in other EU member states, and
- creates a European internal market for Trust Services from Qualified and Non-Qualified Trust Service Providers (TSP) that provide electronic signatures, electronic seals, time stamps, electronic delivery service and website authentication services. This is accomplished by ensuring that they will work across borders and have the same legal status as traditional paper-based processes.

For Trust Services provided by an eIDAS compliant TSP, user identification is the crucial security anchor of the overall Trust Service established. iProov acts as an independent service provider contributing with its services for biometric user identification (GPA), or authentication (LA) in that context. The services provided by iProov allow face recognition and liveness detection within the overall process of secure identification or authentication of natural persons for Trust Services under the eIDAS Regulation.

iProov provides its services by form of independent modules which can be interfaced to by client companies like a Trust Service Provider. The modules undergo regular conformity assessments in order to demonstrate eIDAS compliance (see separate up-to-date eIDAS certificates and reports available at iProov for latest eIDAS compliance status).

The biometric verification services provided by iProov may also be used by other companies active in different sectors, e.g., banks, insurance companies and others. Specific requirements of such companies - other than eIDAS compliant TSPs - are however not subject of this document[1].

[1] For that reason, the term Trust Service Provider (TSP) may only be read synonymous to the following document for such client companies, not as requirements applicable to non-TSP clients making use of one of the modules.

Service fractions other than face recognition and liveness detection for secure identification (GPA) or authentication (LA) of natural persons (biometric verification), for Trust Services under eIDAS as described in this TSPS, are currently not provided by iProov.

Following the IETF RFC3647, this document consists of nine sections. Not all the sections and subsections are relevant however for the service fractions provided by iProov with their modules. To preserve the structure defined by RFC3647, sections and subsections which do not apply for the services provided by iProov carry the statement "not applicable". Sections that describe actions specific to a single service module contain only references to that service-module specific practices.

1.1.1 iProov history

iProov was founded circa 2012 by CEO Andrew Bud as a fledgling Biometric Company providing an in-house developed identity verification service. iProov as an initial concept was conceived to address the following challenges: how to assure that an online user is the right person, a real person and that they are genuinely present right now (and not a criminal or machine-driven attack). In other words, how can we trust in the genuine presence of a remote user when there is no authoritative additional person to confirm? iProov has developed solutions to create an unmatched level of trust between the organisation and the user. iProov’s face authentication enables individuals to prove their genuine presence unambiguously, and with their consent.

1.2. Document Name and Identification

This document is titled “iProov Trust Service Practice Statement (TSPS) for the following processes:

Module 1- Genuine Presence Assurance (GPA) and
Module 2 - Liveness Assurance (LA).”

iProov does not define OID for its public documents and does not refer to any OIDs of the given TSP. Any certificates issued by a TSP contain the OIDs as specified by the corresponding TSP.

The certificate Policies supported by iProov are aligned with the certificate policies defined in ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI TS 119 461 norms, as well as according to the eIDAS Regulation (EU) No 910/2014. The scope of the policies relates to the issuance of qualified and non-qualified certificates for natural persons and legal persons and iProov’s role in this endeavour, which is either for:

- Module 1, GPA – face verification and liveness detection for the purpose of identification of natural persons as of eIDAS Regulation article 24 1d) or
- Module 2, LA – face verification and liveness detection for the purpose of user authentication, for instance in the context of remote signing or sealing.

Since iProov is not a TSP itself, it uses a subset of the above-mentioned policies. Areas or sections which do not apply for the iProov modules described within this TSPS are marked as “not applicable” in the following.

The TSP making use of one of iProov’s modules shall identify which of the certificate policies defined in the documents it adopts as the basis, plus any variances it possibly chooses to apply. It’s the duty of the TSP is to make the relevant Trust Service policies, like Certificate Policies (CPs) and practises, and Certification Practice Statements (CPS) available to users and relying parties.

1.3 PKI Participants

The following participants are relevant in the context of the service modules established by iProov:

1.3.1. Trust Service Provider (TSP)

iProov is a biometric verification provider that supports Trust Services under the eIDAS Regulation. iProov’s obligations and warranties are outlined in section 9 of this document.

Trust Service Provider is an entity adhering to eIDAS Regulation Article 3 (19) and (20). Where a commercial agreement exists, a TSP is the client of iProov and has a contractual relationship with iProov. Alternatively, a partner company can have this contractual relationship with iProov, e.g., an ID document verification provider, which also contributes to the user identification or authentication for the Trust Service (see also section “Other Participants” below).

1.3.2. Certificate Authority (CA)

Trust Service Provider that issues electronic certificates as defined within clause 3.1, ETSI EN 319 411-1.

1.3.3. Registration Authority (RA)

Internal or external entity of a TSP as defined within clause 3.1, ETSI EN 319 411-1, which establishes enrolment procedures for end-user certificate applicants and can initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA.

1.3.4 Subscribers and Subjects

Subscribers are natural or legal persons purchasing Trust Services as defined within clause 5.4.2 of ETSI EN 319 411-1. They are in a contractual relationship with the TSP. iProov has no direct contractual relationship with subscribers. Subjects are natural or legal persons which are subject to a Trust Service. They are for instance subject to an electronic certificate issued by the TSP.

1.3.5. Relying Party

This relates to any party that acts trusting in a Trust Service, e.g. in a certificate issued by the TSP as defined in eIDAS Regulation Article 3 (6).

1.3.6 Other Participants

Cloud Service Provider: Sub-processors that iProov uses for data hosting.
Contractual agreements are in place between iProov and its sub-processors. Includes the contractual, organisational and security measures that are provided by the cloud provider meeting the relevant requirements as detailed by the eIDAS Regulation and normative requirements, like ETSI EN and CEN norms for Trust Services. Security requirements in relation to Trust Services are set for the public cloud provider e.g. by ISO/IEC 27001 certification and SOC2 reports or similar. By making use of Cloud Service Provider, iProov's technical environment is able to scale quickly to accommodate a changing load.

Partners: iProov partners for instance provide remote identity document reading and verification services for TSP. These may be used for certificate applications, renewal and reactivation of electronic certificates for natural persons.

Customers or Clients: An iProov client (or customer) is the entity buying the iProov service. Clients in the context of this TSPS are typically TSP or partner as of eIDAS Regulation Article 3 (19) and (20), providing services under the eIDAS Regulation.

1.4 Certificate Usage

Not applicable.

1.5 Policy Administration

1.5.1 Company administration

The Company administering iProov TSPS is:

iProov Ltd
10 York Road,
London
SE1 7ND
www.iproov.com
Company number: 07866563
Company registration address: 14, Bank Chambers 25, Jermyn Street, London, England, SW1Y 6HR

1.5.2 Contact person

The contact person for the TSPS is CTO/CISO, Dominic Forrest:
Dominic Forrest Compliance@iproov.com.

1.5.3. Procedure for approval

Before publishing this document, the TSPS is approved and enforced by iProov's CTO/CISO. iProov's TSPS is made available to all stakeholders involved following approval.

iProov's TSPS is reviewed at least once a year by iProov's compliance team in line with iProov's document control policy.

Compliance of iProov's TSPS with RFC 3647, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, and eIDAS is and will continue to be assessed, with any found inconsistency remediated.

Any amendments are captured in the version control, which includes the type of modification. The updated TSPS, which includes the enforcement date (which must be published 30 days before its enforcement date), is published electronically on iProov's website. iProov retains the right to publish a draft version of the TSPS prior to publishing the amended version to enable stakeholders to provide feedback on the draft TSPS.

iProov ensures that the practices described within this TSPS are properly implemented by conducting regular internal audits and conformity assessments.

Document life cycle as of iProov management scheme:

- Need for documentation established
- Planning in relation to content
- Document development that includes consultation with the relevant stakeholders
- Document draft creation, increasing the minor version number
- Document to be submitted to the Information Security/ Compliance representative for review
- Changes implemented
- Submit to CISO for final reviewal
- Final edits made in accordance with CISO recommendations
- Document creation, increasing the major version number
- Document dissemination
- Compliance audit/ review (Annually/ in line with audit schedule)

Any deviations from the document lifecycle or any errors must be reported immediately to the Compliance Team to remedy. Where deemed necessary, iProov's CTO will be informed of the error and the change.

1.5.4 Additional TSPS document Information

iProov's management is responsible for implementing practices as described and defined within this TSPS document.

iProov defines and reviews its process and practices that comply with the TSPS on a regular basis, including the responsibilities for maintaining this practice statement.

Should iProov intend to make changes in this practice statement, that may affect the acceptance of its product and service to its subscribers and relying parties, iProov will provide due notice of changes to its subscribers and relying parties.

iProov's CTO/CISO has the overall responsibility for enforcing and approving this document. Following approval, this document will be made publicly available.

1.6 Definitions and Acronyms

1.6.1 iProov Terminology

Lexical item	**Definition**

Biometric profile	The single model for each user that captures their identity, there is exactly one for each user
Canny	Black-white face outline abstraction when starting a claim
Claim	An iProov transaction; someone "claims" to be a certain person
Enroller	Initial enrolment of customer, their first iProov
Fail Code	A code that is used to indicate the most likely reason for a capture being failed, can either be internal (used within iProov) or external (given to a customer)
Faro	Pre-flashing (canny) stage interface guiding user's gaze and phone motion (for anti-spoofing with Giotto and gaze detection)
Feedback code	A code that is returned following a fail that can be converted into a message to give to the user
Feedback message	A message shown to the user as a result of a feedback code
Flash code	The sequence of colours displayed on the screen during a capture
FODOR	The iProov system for estimating the emotional state that a user is in whilst using iProov
Giotto	A spoof test using changes in camera perspective to infer 3D face information
Management	iProov Managers and Heads of Department
Onsite deployment	A deployment of servers into a customer's data centre with iProov installed managed and run by iProov as a SAAS service
Optical ID photo	An image taken of a photo displayed on an identity document
Photo enrol	Enrolment is performed using a photo and subsequent verification is performed with an iProov capture
Rigel	A single-frame spoof classifier operating independently of the flashes

Selfie picture	A single image of a person taken with an on-device camera
Token	Internal transaction ID
Token_hash_part	External transaction ID; maps one-to-one to token
Top Management	iProov's Senior Leadership Team
Verifier	Enrolment and subsequent verification performed with iProov captures
Zorro	Tests whether the user is trying to spoof authentication with a mask

1.6.2 Definitions

Lexical item	Definition
Auditor	Person who assesses conformity to requirements as specified in given requirements documents
Certificate, Electronic Certificate	Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it, as defined within eIDAS Regulation Article 3
Coordinated Universal Time (UTC)	Time scale based on the second as defined in Recommendation ITU-R TF.460-6 [i.8]
Client / Customer	As defined within clause “1.3 PKI Participants” above: an iProov client or customer is the entity buying the iProov verification service, that can include Partners
Digital Signature	Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient, as defined within eIDAS Regulation Article 3
End User	Subject or subscriber, as defined within clause “1.3 PKI Participants” above
Extended Validation Certificate	A certificate that proves the legal entity of the owner and is signed by a certificate authority key that can issue EV certificates

Identity Document	An official and government issued identity document such as passports, driving licences, or identity cards
Partner	As defined within clause “1.3 PKI Participants” above: Associated service provider working alongside and engaging iProov technology. An iProov partner can include an integrator
Qualified Trust Service Provider	As defined within clause “1.3 PKI Participants” above: A trust service provider who provides one or more (qualified) trust services and is granted the qualified status by the Supervisory Body
Registration Authority (RA)	As defined within clause “1.3 PKI Participants” above: Entity that is responsible for identification and authentication of subjects of certificates mainly NOTE: An RA can assist in the certificate application process or revocation process or both
Relying Party	As defined within clause “1.3 PKI Participants” above: Natural or legal person relying on TSP services
Software as a Service (SaaS)	A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted on a public cloud
Subject	As defined within clause “1.3 PKI Participants” above: Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
Subscriber	As defined within clause “1.3 PKI Participants” above: Legal or natural person bound by agreement with a trust service provider to any subscriber obligations
Supervisory Body	The authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state
Trust Service	As defined within eIDAS Regulation Article 3, electronic service for: • creation, verification, and validation of digital signatures and related certificates; • creation, verification, and validation of time-stamps and related certificates; • registered delivery and related certificates;

	• creation, verification and validation of certificates for website authentication; or • preservation of digital signatures or certificates related to those services.
Trust Service Provider	As defined within clause “1.3 PKI Participants” above: entity which provides one or more trust services

1.6.3 Acronyms

Acronym	Phrase
API	Application Programming Interface
CA	Certificate Authority
CRL	Certificate Revocation List
DBS	Disclosure and Barring Service
DMZ	Demilitarised Zone
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ETSI	European Telecommunication Standards Institute
GDPR	General Data Protection Regulation
HSM	Hardware Security Modules
ISMS	Information Security Management System
NDA	Non-Disclosure Agreement
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
SaaS	Software as a Service
SDK	Software Development Kit
RA	Relying Authority

RTW	Right to Work
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSPS	Trust Service Practice Statement
TSU	Time Stamping Unit
UTC	Coordinated Universal Time

2. Publication and Repository Responsibilities

2.1 Repositories

iProov operates an online repository that can be found at:
https://www.iproov.com/eidas-compliance-repository

2.2 Publication of information

iProov provides public repositories for its TSPS and other important policy documents.
Specific policies and practices as well as terms and conditions (TAC) regarding Trust Services provided by a TSP (e.g. certificate usage) making use of iProov's modules shall be published and maintained by the corresponding TSP.

2.2.1 Publication and notification policies

iProov publishes its public information repository that holds the following easily accessible information:

I. TSPS
II. iProov's general Terms and Conditions for TSP and client companies
III. Certifications
IV. Privacy Policy

iProov publicly discloses its TSPS through an online means that is available on a 24x7 basis.

2.2.2 Items not published in the Practice Statement

Reference to clause 9.3.1 of iProov's TSPS.

2.3 Time and frequency of publication

Any new version of this TSPS is made public via iProov's website immediately by iProov's Compliance team after the new version has been approved by iProov's CTO. Publication of repositories is updated on a frequent basis whenever relevant changes are performed, and reviewed yearly.

2.4 Access control of repositories

Information shared or published within iProov’s public repository is not considered confidential information, and as such, is made readily available and publicly accessible.

Documents that are made available via iProov’s online repository are protected from unauthorised access or any attempt to modify, delete or add information into iProov’s repository. Specific iProov employees are permitted, and have the ability to modify documentation or information provided within iProov’s online repository.

3. Identification and Authentication.

3.1. Naming

This section refers to requirements for naming in electronic certificates as specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7] and the appropriate part of ETSI EN 319 412 [2], [9] and [10]. Naming is relevant for certificate issuance performed by TSP. It is not applicable in the context of the two service modules operated by iProov.

3.2 Initial Identity Validation

3.2.1 iProov's Service Modules for TSP under eIDAS

iProov offers two services with associated biometric verification services for different or associated authentication and verification use cases in form of:

- Module 1 - Genuine Presence Assurance (GPA)[2] and
- Module 2 - Liveness Assurance (LA)[3].

The modules are implemented as iProov Technology Services which comprises a hosted Software-as-a-Service (SaaS) platform, the capabilities of which can be consumed through appropriate use of defined Application Program Interface (API) endpoints in conjunction with SDKs (Software Development Kits) and iProov edge layer technology that facilitates access to the Platform.

iProov provides up-to-date guides and directories of current API integration for the Platform and Front-end Software which are available to customers as required.

The endpoints are used to access the iProov technology irrespective of the nature of the service driving the customer requirement. It is left entirely to the customers to define their own use cases and access the service as when required for their user flow under the terms of a signed contract. On iProov side the endpoints are fixed. They shall undergo a defined maintenance, and change management, for amendments or changes as required by the eIDAS Regulation - see also section on interfacing below.

[2] supports identification of natural persons according to Article 24 1d) of the eIDAS Regulation EU 910/2014 (see detailed description below).

[3] supports user authentication of already known persons for Trust Services, e.g. in the context of remote signing or sealing, but no identification in the sense of article 24 of the eIDAS Regulation (see detailed description below).

3.2.1.1 Participants in GPA or LA service

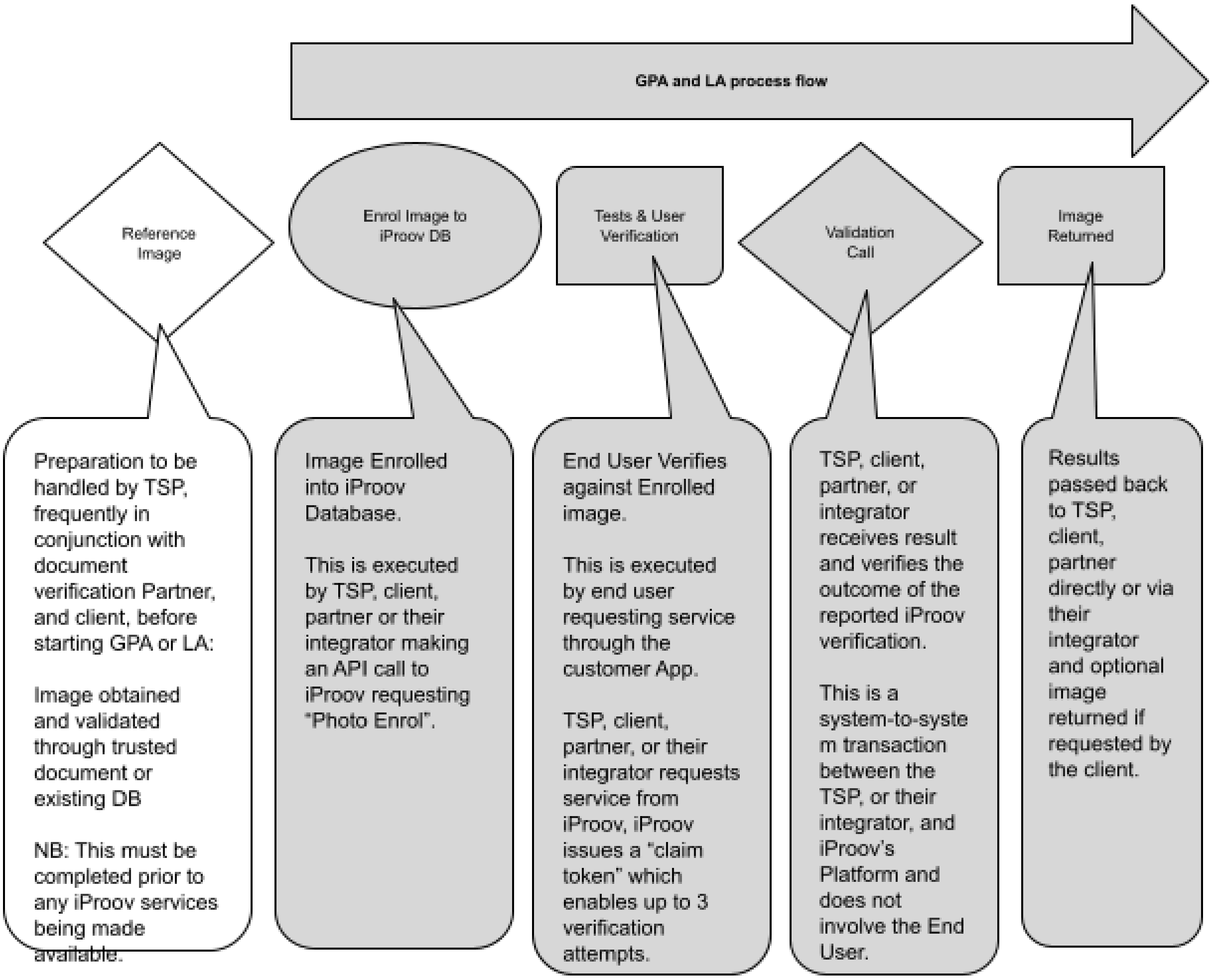
There are a number of different entities involved in delivery and consumption of an integrated service in order to meet eIDAS requirements (see also section "Definitions and Acronyms" below for explanation).

- Trust Service Provider (TSP) or client company;
  iProov's client companies in the context of this TSPS are typically Trust Service Provider (TSP), whereas TSP can be either directly iProov's customer or orchestrated via a distinguished partner service company or integrator.
- Partner service company or integrator (as far as involved);
  Partner service companies are providing other aspects of user identification or authentication, for instance checking the authenticity of a reference picture to be used by the GPA or LA process. Partners typically are service companies providing "ID document validation" for End Users wishing to enrol with a TSP. Partners can also be Registration Authorities (RA) in the definition of the eIDAS Regulation, usually in relation to the TSP itself.
  Integrators are entities such as the TSP or customer internal IT department or external IT service providers taking care of correct technical interfacing to the services provided by iProov.
- End user;
  Entity (subject/subscriber) with direct contractual relationship to the TSP. The end user typically undergoes the iProov GPA process for user identification or the LA process for user authentication in the eIDAS context (e.g. the user who applies a qualified electronic signature to an electronic document where the corresponding qualified certificate was issued by the TSP).
- Relying Parties;
  Natural or legal persons relying on TSP-provided services as third parties without direct contractual relationship to the TSP (e.g., a person relying on a document carrying a qualified electronic signature where the corresponding qualified certificate was issued by the TSP).

3.2.2.2 GPA or LA service process flow

Upon an end user wishing to obtain services of a TSP or client company (for TSP services like certificate generation, revocation, renewal, or any other scenario), a user flow will be established between the TSP client company directly, or via an integrator, invoking an end user process flow. Depending on the end user process flow coordination will be necessary between the customer/integrator and iProov.

GPA and LA process flow overview:



Preparation to be handled by TSP, frequently in conjunction with document verification Partner, and client, before starting GPA or LA:

Image obtained and validated through trusted document or existing DB

NB: This must be completed prior to any iProov services being made available.

Image Enrolled into iProov Database.

This is executed by TSP, client, partner or their integrator making an API call to iProov requesting "Photo Enrol".

End User Verifies against Enrolled image.

This is executed by end user requesting service through the customer App.

TSP, client, partner, or their integrator requests service from iProov, iProov issues a "claim token" which enables up to 3 verification attempts.

TSP, client, partner, or integrator receives result and verifies the outcome of the reported iProov verification.

This is a system-to-system transaction between the TSP, or their integrator, and iProov's Platform and does not involve the End User.

Results passed back to TSP, client, partner directly or via their integrator and optional image returned if requested by the client.

In order to use any iProov verification service, iProov will need to have obtained and stored a reference image to verify the user against. This process is called "Enrolment" which can be performed through a number of mechanisms one or more of which will be selected by the TSP.

Possible sources for the reference image are:

- NFC capture and verification from a government issued document such as a passport or Driving License
- An existing trusted database, such as National government ID scheme
- Photo enrol if the customer has authorised this alongside other security checks
- other trusted source

Note: Sourcing for reference pictures is out of scope of the two modules (GPA and LA) that iProov describes in this TSPS. The two modules expect a legitimate reference picture provided at their interface. It’s the obligation of the TSP to ensure that the sources for the reference picture are compliant with the overall applicable requirements (legal, as in eIDAS and national law and normative, as in ETSI and CEN).

When iProov are required to participate in a specific use case involving GPA or LA, the following process will be instigated:

- a call is made to the iProov API by a requester, that is the TSP or customer or the integrator, requesting a “token” to use the iProov service
    - the ID reference supplied to iProov from the requester is a pseudonym
    - the requester will store the pseudonym / real username mapping. iProov is not aware of the name or details of the end user
    - the response issued will allow up to three attempts to complete a “Claim”
- iProov will respond to the request by issuing a “token”
    - the iProov token is a string of characters 64 bits long
- the requester will receive the iProov token and pass it to the end user application
    - When an End User signed up with the TSP, the TSP app will include a copy of the iProov SDK.
    - the token will be injected into the integrated iProov SDK on the user device
    - the user device will begin the identification (GPA) or authentication (LA) process and establish a stream of image transfers.
    - iProov will inspect the received images and perform a battery of tests to identify if it's a genuine feed from a live device with a real person
- iProov will produce a result, and then send the result to the user’s device
- Communication between the user device and the TSP or customer or integrators server will result in the customer server obtaining the result of the session with the server subsequently checking the validity of the reported outcome with iProov via a backend system to system / B2B call.
- Details and records of the transaction are stored by iProov securely as determined by the customer.

3.2.2.3 General provisions applicable to iProov services

iProov GPA and LA services are delivered by iProov servers which are controlled by and may only be accessed by iProov.

iProov GPA and LA services use automated technology in the endeavour to detect impersonation and spoofing attempts. Since it relies on a probabilistic automated decision-making system there can be no guarantee that all impersonations and spoofs will be detected. There is also a chance that genuine users may have verification attempts refused.
iProov has however implemented a process management and quality control system which guarantees that:

- the assurance level for user identification reached by GPA remains at least at the level required by the eIDAS Regulation article 24 1d) and
- the assurance level reached by LA remains at least at the level required for user for authentication under the eIDAS Regulation as it is necessary for instance to authenticate for remote signing and sealing.

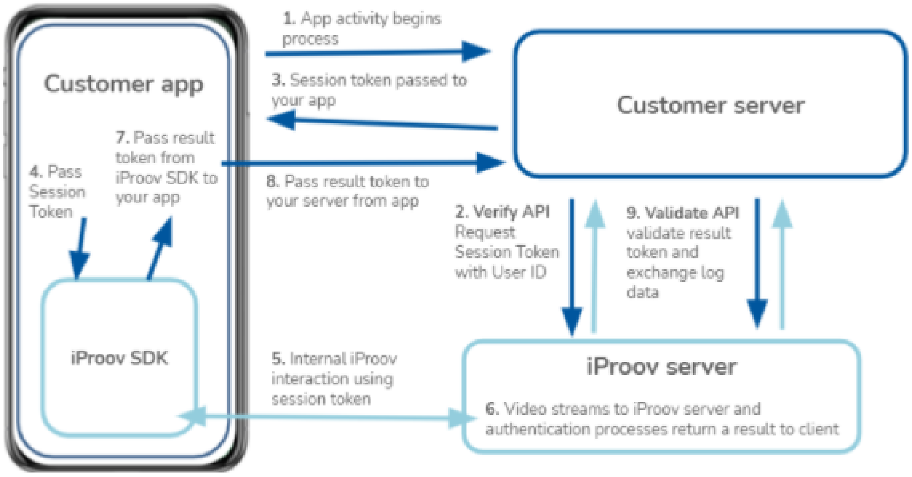
Where mention is made in this document of

- iProov's servers, these servers may be provided by contracted service providers.
- Pseudonyms, these are pseudonyms generated by the TSP or TSP's integrator. The record of the real name these relate to is wholly owned by the TSP/Integrator the details of which iProov has no knowledge or need of. This received pseudonym is associated by iProov with a separate randomly generated internal iProov pseudonym which is used to reference "Claim" credentials.
- risk profile, this is a risk profile selected by the client from a menu of such profiles provided by iProov during implementation of the GPA and LA service and establishes different criteria for the service to measure a client against.

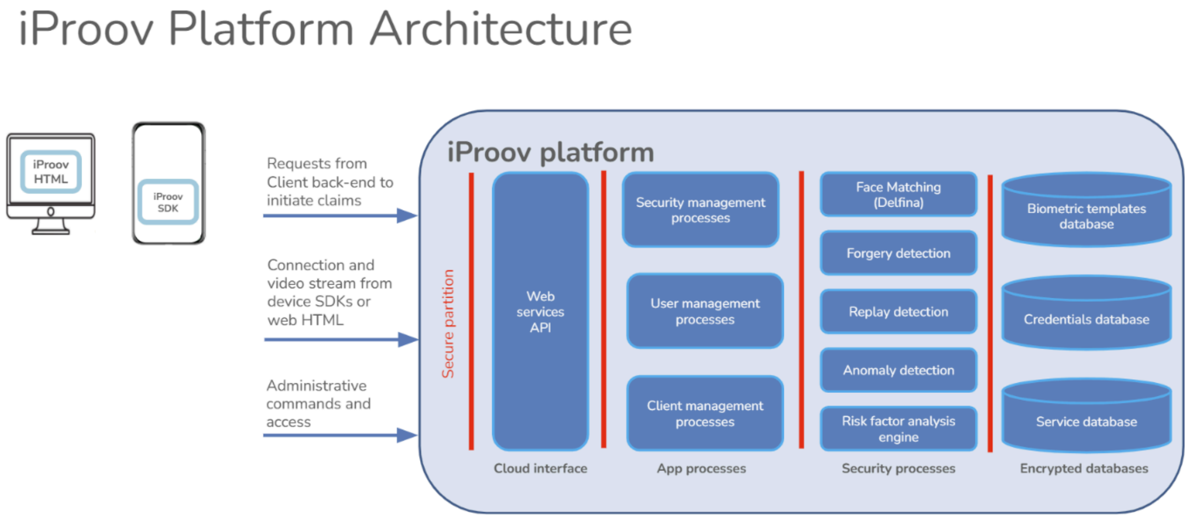
Unless otherwise provided, terms used in this document bear the meanings given to them in the clients' agreement with iProov (including the relevant Billing Profiles). References to Customer include Client and analogous terms.

3.2.2.4 General verification workflow (GPA and LA)

iProov offers its services to its clients / TSP via a mobile SDK with the following typical process flow:


Customer app
1. App activity begins process
Customer server
3. Session token passed to your app
7. Pass result token from iProov SDK to your app
4. Pass Session Token
8. Pass result token to your server from app
2. Verify API Request Session Token with User ID
9. Validate API validate result token and exchange log data
iProov SDK
5. Internal iProov interaction using session token
iProov server
6. Video streams to iProov server and authentication processes return a result to client

At the backend, iProov has implemented the following platform architecture:


iProov Platform Architecture
iProov HTML
iProov SDK
Requests from Client back-end to initiate claims
Connection and video stream from device SDKs or web HTML
Administrative commands and access
iProov platform
Secure partition
Web services API
Security management processes
User management processes
Client management processes
Face Matching (Delfina)
Forgery detection
Replay detection
Anomaly detection
Risk factor analysis engine
Biometric templates database
Credentials database
Service database
Cloud interface
App processes
Security processes
Encrypted databases

The specific implementation of GPA and LA depends on the client's TSP use case – identification of natural persons (GPA) or user authentication (LA). Further information regarding differences between the services can be found in iProov's GPA and LA product documentation.

3.2.2.5 Interfacing (GPA and LA)

Both modules interface to client TSP via predefined interfaces as they are described in this TSPS document and refined within the clients contract and iProov internal interface specification. Module interfacing to clients in the sense of this TSPS comprises the following aspects:

Interfacing at organizational level defining the following:

- general contractual aspects (service content)
- TSP end user Terms and Conditions (TAC) management
- TSP information of end users and consent in iProov TAC
- duties and limitations of iProov services
- duties and limitations on customer side (eIDAS TSP perspective)
- contact persons and responsibilities
- TSPS and change management of services provided as well as of the TSPS document from both perspectives: TSP and iProov eIDAS Modules for GPA or LA respectively
- service level agreement (SLA)

Interfacing at IT level defining the following:

- expected data input at the interface to iProov GPA or LA
- provided data output at the interface from GPA or LA
- meaning of input/output values
- data interface security (encryption, options and limitations)
- iPortal client functions and iPortal manual

3.2.2.6 Module 1 - Genuine Presence Assurance (GPA)

GPA provides identification of natural persons according to Article 24 1d) of the eIDAS Regulation EU 910/2014. It enables TSP to securely identify its end users online, in other words, confirming that the person they are interacting with is: the right person compared to a given picture (e.g. taken from an ID document)[4], a real person and is currently acting in the process and authenticating now. GPA delivers identification of a natural person at a security and assurance level appropriate for qualified Trust Services under eIDAS.

iProov GPA may be used by qualified TSP to identify natural persons in the context of the issuance of electronic certificates under the following policies:

- NCP as of ETSI EN 319 411-1

and

- QCP-n and QCP-n-qscd
- QCP-l and QCP-l-qscd as well as
- QCP-w as of ETSI EN 319 411-2.

When identifying and enrolling an end user through GPA, a high level of confidence is provided within the biometric, and therefore the biometric that is being enrolled is ensured to be real and trustworthy. GPA in this instance offers the highest levels of assurance for biometrics.

iProov GPA uses powerful deep learning AI methods to combine camera imagery with contextual and device sensor data generated during the identification process. This creates a complex and rich source of biometric analysis. iProov then applies several proprietary AI-based algorithmic biometric checks to assess the probability that the presented face is real, and not a presented object such as a screen, mask or cut-out. iProov GPA technology is designed to detect different types of spoof attacks commonly used to try and defeat secure authentication, through methods which include using artefacts or images presented to the camera, synthetic videos or replayed imagery of previous enrolment or verification

[4] ID document handling and read out is **not** part of the processes provided by iProov.

sessions injected into a device's sensors. iProov's Flashmark method uses controlled illumination, with light generated by the device screen, to ensure the user is Genuine and present at the point of challenge.
The user is presented on the screen of their device with an abstracted rendering of the image of their face captured by their device's front-facing camera. Visual feedback is provided to the user during the alignment process. The screen flashes a sequence of colours, to illuminate the user's face; this colour sequence changes for each verification attempt from the same user. This sequence is determined by a sequence generated and sent from servers deployed by iProov before the Verification attempt begins. The combination of the user's face and the unique illumination sequence creates a short video which is captured and sent to iProov during the user session. The information in the transmitted video is processed by iProov servers to determine the likelihood, as determined by iProov's technology, that the user is genuinely present, and to provide a response to the TSP or client based on this likelihood. The scores and signals from these checks are used by iProov to determine a pass/fail result and then communicates this result to the TSP.

Note: iProov offers the products "iProov Enroller" and "iProov Face Verifier" using GPA Technology. These parent products when used outside of an eIDAS environment are not subject of this TSPS.

3.2.2.7 Module 2 - Liveness assurance (LA)

LA provides user authentication of already known persons for Trust Services, e.g. in the context of remote signing or sealing. As such, LA cannot be used as identification means according to Article 24 of the eIDAS Regulation EU 910/2014.

iProov LA may be used by qualified TSP for user authentication[5], for instance in the context of remote signing[6] or sealing[7] under the following policies:

- NCP as of ETSI EN 319 411-1
- QCP-n and QCP-n-qscd
- QCP-l and QCP-l-qscd as of ETSI EN 319 411-2.

[5] it's the duty of the TSP or client company to ensure overall compliance of its processes with applicable rules and regulations when implementing LA for user authentication. See also section "TSP overall responsibility for eIDAS compliance" below.

[6] It's the duty of the TSP in conjunction with its remote signing system provider to ensure compliance of the LA process for user authentication to establish a remote signature. Note, that LA cannot (!) be used to identify natural persons for issuance of a signing certificate used in remote signing environments.

[7] It's the duty of the TSP in conjunction with its remote sealing system provider to ensure compliance of the LA process for user authentication to establish a remote seal. Note, that LA cannot (!) be used to identify natural persons in conjunction with the issuance of a sealing certificate used in remote sealing environments.

iProov uses Liveness Assurance technology (LA) to confirm that the face of a natural person which undergoes the overall authentication process for a Trust Services under eIDAS is real. Furthermore, the process provides assurance that the user is the right person. It delivers a low ceremony, passive user experience for safe and secure authentication.

The liveness ceremony uses user device interaction (e.g. mobile phone) and imagery to ensure the behaviour of a person accessing the services are consistent with that of a real human being. The user is presented on the screen of their device with an abstracted rendering of the image of their face captured by their device's front-facing camera. Visual feedback is provided to the user during the alignment process. As the user aligns their face a number of images are captured. These images, together with other information from the user's device, are sent to the iProov platform where they are processed by a number of platform subsystems which aim to establish whether the appearance of the face in front of the camera, the change in the appearance across the frames, and other data from the user device, are or are not consistent with a bona fide user. Unlike GPA, LA is not intended to determine whether the user is genuinely present and acting in real-time. Therefore the LA service does not include the use of "controlled illumination flashmark". The battery of checks conducted on a short video stream received from the device ensures that no coercion or imitation of a real user has occurred. Using the scores and signals from these checks, iProov determines a pass/fail result and then communicates this result to the TSP.

Note: iProov offers the services "iProov Basic Enroller" and "iProov Basic Face Verifier" using LA Technology. These services are not specifically tailored for TSP under the eIDAS Regulation and therefore are not subject to this TSPS.

3.2.2.8 TSP overall responsibility for eIDAS compliance

It's the obligation of the TSP to ensure that the overall identification or authentication process involving one of the iProov modules GPA or LA is compliant to the applicable requirements. These include the eIDAS Regulation with their connected normative requirements (like ETSI EN 319 401, EN 319 411-1/2, ETSI TS 119 461 as applicable) as well as additional local national laws and regulations as required by the Supervisory Body (SB) responsible for the TSP involving iProovs services.

3.2.2.9 Attribute and Evidence Collection

The identity attributes required for the identity proofing context is defined in iProov's service offerings and agreed between iProov and its customers/ partners/relying parties.

The evidence collected shall meet the requirements of the identity proofing context such as legal and contractual requirements.

The identity proofing process provided by iProov verifies that the evidence is of a type accepted according to the identity proofing context.

iProov's identity proofing process, as possible, verifies that the person is a real person, the right person in real time, at the time of the identity proofing.

3.2.2.10 Binding to applicant

iProov forms part of the overall identity proofing process, and enables the overall service/ scheme to verify whether the end-user is who they claim to be as evidence within the documents verified by iProov's partner within the scheme.

3.2.2.11 Capture of face image of the applicant

Where iProov is part of the identity proofing process, that is carried out remotely, the following requirements are met:

- A video stream of the applicant's face is captured
- The video capture process applies liveness detection measures to ensure that the video stream is of a real living person that is present in front of the camera at the time of the identity proofing.
- The video stream capture applies measures to detect artificially generated or manipulated face appearance.
- iProov does applies a zero trust policy to the device, however, if the video stream is captured on the applicant's device, the identity proofing process will ensure that the video stream is transmitted to an environment controlled by the entity responsible for the identity proofing process to ensure: authenticity, integrity, and confidentiality of the video stream.
- In instances where face biometrics is used for binding to applicant, at least one image of sufficient quality for binding to applicant shall be extracted from the video stream.
- The video stream capture applies PAD measures in compliance with ISO/IEC 30107-3.
- The PAD is evaluated in accordance with ISO/IEC 19989-3.

- Test results for the PAD achieves an APCER (attack presentation classification error rate) as defined by ISO/IEC 30107-3 at the level of industry best practice.
- Test results for the PAD achieves BPCER (bona fide presentation classification error rate) as defined by ISO/IEC 30107-3 at the level of industry best practice.
- The PAD measures and APCER and BPCER rates are kept up to date concerning advances in the threat landscape and available technology.

3.2.2.12 Result of the Identity Proofing and evidence

iProov passes a pass or fail result back to its customer as part of the overall identity proofing service.

The result is delivered and transmitted securely to the trusted service provider.

Evidence is gathered and retained for a specified period in compliance with the identity proofing context, this includes elements such as the pass/fail result, audit logs and transaction logs. Such evidence will be retained for the retention time given by the identity proofing context. The evidence of the identity proofing part of the process that pertains to iProov's services is stored in a tamper-proof way that enables the confidentiality of the information, and is stored in a way that ensures the possibility to retrieve, the identity proofing result.

At the end of the retention period, the evidence of the personal data on the applicant is deleted.

The identity proofing context conforms to the: issuing of proof (8.5).

3.2.2.13 Use cases automated operations

A face image of the end user is captured that complies with the requirements of ETSI TS 119 461 within the overall scheme.

As iProov is a part of the overall identity proofing process, iProov's partner obtains at least one digital identity document obtained as evidence.

3.3 Identification and Authentication for Re-Key Requests

TSP supporting re-key may make use of iProov's service modules as described in section 3.2 of this TSPS.

3.4 Identification and Authentication for Revocation or Suspension Requests

TSP may make use of iProov service modules as described in section 3.2 of this TSPS.

3.5 Binding to applicant by automated face Biometrics

The biometric algorithms and technologies applied are systematically tested against reference datasets and kept updated to cope with changes in the threat landscape as well as various risk situations.

The test results for the biometric face recognition show a FAR (false acceptance rate) at the level of industry best practice.

The test results for the biometric face recognition show a FRR (false rejection rate) at the level of industry best practice.

The biometric facial recognition applies measures to detect morphed photos in identity documents.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Applying for a certificate through a chosen TSP will require absolute confirmation of the applicant's authenticity. iProovs Module 1 - Genuine Presence Assurance (GPA) will be used for certificate applications. An applicant (end user) wishing to use eIDAS services must register with the RA of a TSP. Applicants in that sense are natural persons. During the application process, the applicant's consent in the terms and conditions (TAC) of the TSP or client must be registered.

It's the duty of the TSP and client to ensure that all relevant aspects related to the services provided by iProov are included in their up-to-date version of the TAC presented to the applicant for consent taking. It is also the duty of the TSP or client to keep proper evidences that consent has been given by the applicant.

4.2 Certificate Application Processing

iProov's Module 1 - Genuine Presence Assurance (GPA) may be used for certificate applications. GPA provides a return value (score) back to iProov which is in turn passed back in the form of a pass/fail, and validated by the TSP. The scores are used by iProov to determine a pass/fail result in relation to the risk profile required. Depending on the score and the pass/fail result, the TSP shall either approve or refuse a certificate application. The TSP shall at least refuse to issue a certificate if the result was fail. It is however required that all other relevant identity assurance, security and quality related variables are validated by the TSP in addition and are incorporated in its decision (e.g. information on the ID document validation). It is the duty of the TSP to ensure eIDAS compliant validation, and acceptance decision taking, regarding the overall certificate application process.

4.3 Certificate Issuance

Not applicable.

4.4. Certificate Acceptance

Not applicable.

4.5 Key Pair and Certificate Usage

Not applicable.

4.6 Certificate Renewal

Not applicable.

4.7 Certificate Re-Key

Not applicable.

4.8 Certificate Modification

Not applicable.

4.9. Certificate Revocation and Suspension

Not applicable.

4.10 Certificate Status Services

Not applicable.

4.11 End of Subscription

Not applicable.

4.12 Key Escrow and Recovery

Not applicable.

5. Management, Operational, Facility and Physical Controls

5.1. Physical Security Controls

5.1.1 Site Location & construction and general infrastructure

iProov's corporate office infrastructure is located at

10 York Road,
London
SE1 7ND

within a shared multi-tenancy, managed building operated by WeWork who are the building managers.

iProov Ltd has designed and applied physical security for offices, rooms, and facilities. The office is unobtrusive and gives minimum indication of the purpose of the organisation or the presence of commercial information processing activities. The layout of the office is configured to prevent confidential information or activities being visible and audible from the outside.

iProov Ltd conducts risk assessments of individual offices, rooms and facilities that contain confidential or high-risk information assets to identify the controls that might be necessary to secure them. There are no sites where confidential information processing facilities are shared with a third-party organisation, other than under the terms of a contract.

The iProov Ltd office has a secure perimeter which ensures that persons not in scope do not have ready access to secure areas.

Entry to the building during normal working hours is controlled by a manned shared security company who require all visitors to sign-in and be accompanied when visiting any organisation located in the building.

Visitors are not allowed access to the secure area of the office. The offices are locked out of hours and there is 24x7 CCTV covering the approach to the secure area.

Any unwanted visitors are requested to leave with recourse to security, if necessary, should any visitor not leave when requested.

The Office is secured automatically when no staff are present.

Staff have keycards to the office which are disabled and/or returned when employment ceases.

The layout of the office is configured to prevent confidential information or activities being visible and audible from the outside.

iProov Ltd conducts risk assessments of individual offices, rooms and facilities that contain confidential or high-risk information assets to identify the controls that might be necessary to secure them.

There are no sites where confidential information processing facilities are shared with a third-party organisation, other than under the terms of a contract.

Third-party support personnel are allocated a room to work which is external to the areas where confidential or restricted information could be processed. Where they need to access confidential areas (maintenance) they are escorted at all times.

Protection against external and environmental threats are implemented as follows:

- The building is protected from environmental hazards due to its modern construction.
- Further the location of the building is such that environmental hazards such as floods are reduced.
- iProov Ltd has assessed the risk of external and environmental threats and has applied controls that are included in this document or that are part of the Business Continuity Management framework.

iProov’s commercial offices are segregated and kept secure from visitor zones, other offices, and data centres.

iProov’s IT infrastructure is cloud based and all cloud-based services are certified to adhere to the highest current standards. These include ISO27001 controls which cover all aspects of iProov’s operations (ISO 27001 registration utilises a “Statement of Applicability” where organisations can declaratively include or exclude areas of their business. iProov has placed everything in scope and is audited against every aspect of commercial and technical activities).

iProov has both physical and environmental security controls in place to ensure the preservation of information by preventing unauthorised physical access, damage, interruption, and interference with iProov's information, assets and Information Processing facilities. Such controls include:

I. Physical security perimeters
II. Physical entry controls
III. Securing Offices, rooms, and facilities
IV. Protecting against external and environmental threats
V. Working in secure areas
VI. Delivery and loading areas

Equipment security is also imperative in the prevention of damage, theft and/or compromise of assets/ information. iProov takes a preventative approach with its equipment security by means of the following practices:

- No laptops or information assets are left unattended between work days.
- Employees are responsible for the safe transport and storage of all personal company assets.
- Commercial information is cloud based with only limited files stored on end point devices.
- Company handbook and other publications within iProov describe policies to avoid information security, and asset breaches.
- Remote management of all end point devices is enabled.

iProov Ltd has adopted a clear desk policy for highly confidential papers, prohibits the use of removable storage media, and a clear screen policy for information processing facilities, as described in the Staff Handbook.

Information processing and storage equipment are located in Data Centres only.

iProov's office and the utilities serving it are managed by WeWork who are the building managers.

Printers used for confidential information are sited in secure areas so that it is not possible for confidential information to be seen by unauthorised people. Where shared WeWork printers are used these require a password to be input while physically present at the printer before the print takes place. iProov discourages the use of printed materials.

5.1.2 Physical access

5.1.2.1 Physical entry controls - iProov Offices

iProov Ltd has designed and applied physical security for offices, rooms and facilities. The physical security for the office has been described in detail in clause 5. The office is unobtrusive and gives minimum indication of the purpose of the organisation or the presence of information processing activities. The layout of the office is configured to prevent confidential information or activities being visible and audible from the outside.

Entry to the office is by proximity access RFID card.

Visitors are escorted from the WeWork reception on the ground floor, where they must first register attendance via iPad terminals linked to building control systems. This then notifies the host they have arrived.

Lifts cannot be accessed without an approved access card, visitor passes do not allow access.

5.1.2.2 Physical entry controls - Cloud Data Centres

iProov uses major cloud Infrastructure as Services (IaaS) providers such as Microsoft Azure, Google Cloud Platform and Amazon Web Services. Their hosted data centres are a minimum of tier three and have stringent access and entry controls that include barriers, entry logging, air locks, closed circuit television and RFID entry with booked access times, restrictions and exit times.

The cloud data centres used by iProov for the hosting of its services are specifically built for resilience by the cloud service providers with internal “Availability Zones” each with segregated power, network, HVAC, and backup systems. The centres are not sited on floodplains or in areas where they are susceptible to natural disasters. Each of the three main providers, provide detailed certification of their facilities via their websites, this includes SOC 2 reports.

iProov does not have, or require, any form of access to the cloud data centres which are strictly controlled and managed by the relevant IaaS provider. Their processes and controls are regularly reviewed and audited, with certificates available for review. iProov reviews the security and controls for its cloud SaaS suppliers on at least an annual basis.

All cloud providers have gone through iProov’s procurement process, undertaken due diligence checks and have the required contracts in place. Part of such checks ensures that adequate Physical security controls are in place.

5.1.2.3 Cabling

Primary cabling throughout the Head Office building is provided by the landlord – WeWork.

iProov uses cloud-based services from large, well-established providers, who are responsible for cabling security within their respective data centres.

Our assurance relating to cabling security for both of the above is managed through controls relating to Supplier relationships.

Preferred use of wireless facilities enables minimal cabling for communications for both office and home workers. Where it is required it is protected or hidden and kept away from sources of interference wherever possible.

Homeworkers are encouraged to routinely check devices, and cabling, attached to their router to ensure they continue to be secure and are well maintained - this like many of the other general physical homeworking aspects is done via team updates and annual training/compliance. All communications with commercial or technical platforms are encrypted.

5.1.3 Power and Air Conditioning

iProov Ltd.'s central information processing facilities are separate from those used for commercial offices. Office facilities are also managed by external parties.

iProov's commercial facilities are equipped with:

i) heating, air conditioning and ventilation systems to control temperature and control humidity. iProov has direct contact with the management facility should any issues arise.

ii) iProov's serviced building is equipped with power systems to ensure continuous, uninterrupted access to electricity and power. iProov has direct contact with the facility management should any issues arise.

iProov has additional measures in place in case of an unrecoverable power outage within its commercial facility. Services can continue from other locations without any disruptions to our operations.

iProov platforms are hosted in cloud service providers who have fully resilient data centres that include power backup systems including bypass batteries and generators and have the appropriate cooling and air conditioning to meet computing cooling needs.

5.1.4 Water Exposure

iProov has taken reasonable steps to minimise the impact of water exposure to its service. iProov has designed its services to operate independently within a locality without dependence on external services.

In case of a water leak or flood, iProov have measures in place to minimise the impact of such events.

iProov Ltd.'s central information processing facilities, while hosted in public cloud provider infrastructure, are isolated from access or control from those external parties.

With regard to data centres iProov uses cloud service providers who meet international standards for business continuity management (ISO 22301) and they have the appropriate plans in place to deal with any contingencies around floods or water exposure.

5.1.5 Fire prevention and protection

iProov operates inline with measures to prevent, protect against, and extinguish fires and exposure to smoke/fames. Such measures align with the applicable safety regulations. iProov has a fire incident and evacuation plan in place.

Additional mitigations include:

- No smoking or vaping within the confines of the building.
- Fire detection systems consisting of smoke detectors and alarms.
- Firefighting equipment such as portable fire extinguishers in all areas.
- The fire protection measures are checked regularly, and records are retained by the landlord.

With regard to data centres iProov uses cloud services providers who meet international standards for business continuity management (ISO 22301) and they have the appropriate plans in place to deal with any contingencies around fire prevention and protection.

5.1.6 Media handling and off site management

It is prohibited for any equipment, information or software to be taken off-site without prior authorisation. Shared informational assets such as training laptops, team iPad, video and audio recording equipment as well as other assets like furniture, monitors etc must not be taken off site without a record made of the event within the relevant communications group, and if likely to affect others in their work, pre-warning and authorisation.

However, approved equipment that is in the day-to-day responsibility of staff for their job e.g. laptops can be taken off-site without any prior authorisation or record made of the event (end user devices are fully listed in the asset register, encrypted, do not have information stored locally, are managed by an MDM, and can be remotely tracked and wiped).

Ad hoc spot checks are undertaken periodically to detect unauthorised removal of property and may also be performed to detect unauthorised recording devices, or other unacceptable assets being brought in.

Any spot checks are carried out in accordance with relevant legislation and regulations, and any unauthorised removal issues encountered may be subject to follow-up investigation and possible use of the Disciplinary process.

All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Hard disks are cleared of all software and any Organisational information prior to disposal or re-use, as set out below.

The Head of Operations is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through their office.

iProov has a policy of not allowing the use of portable storage media apart from under exceptional circumstances and then for an agreed purpose in line with FIPS-2 standard.

All other storage media is based within iProov's cloud services provider infrastructure and is provisioned and deprovisioned in line with the policies of the relevant cloud services provider. This storage is held securely and adheres to the FIPS 140-2 standard.

All data stored within iProov's cloud services provider provisioned infrastructure is encrypted at rest and iProov manages keys - utilising the cloud provider tools - to facilitate authorised and audited access only, of any stored data.

5.1.7 Waste disposal

All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Hard disks are cleared of all software and all Organisational information prior to disposal or re-use, as set out below.

The Information Security Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through their office.

The asset inventory is adjusted once the asset has been disposed of as follows:

- Devices containing confidential information are wiped using specialised software prior to disposal and are never re-used. If necessary, the device(s) are put beyond practical use.

- Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.

- Portable or removable storage media of any description are destroyed prior to disposal.

All media are disposed of in line with WEEE (Waste Electrical and Electronic Equipment Directive – 2012/19/EU) regulations on disposal of computer equipment, through the Organization's approved contractor. The contractor is a licensed waste carrier and relevant Waste Transfer Notes are retained for a minimum of two years.

Documents containing confidential information, which are to be destroyed, are shredded by their owners or disposed of as confidential waste. WeWork is specifically approved for this role.

iProov employees are encouraged to work paperless. Where required to print information, or dispose of any note taking equipment, this must be disposed of securely either in the office paper shredding facilities or, at home in a paper shredder that has been provided by iProov HR.

5.1.8 Off-site back up

iProov uses cloud-based technologies and cloud providers infrastructure to backup to alternate cloud locations. Locations are selected in line with data governance controls and agreed contractual obligations. When routine backups are conducted within our cloud providers infrastructure the alternate locations are selected to ensure resilience for the specific operational platform.

Through our control of supplier management relationships, we ensure that backup and continuity requirements are met. Suppliers are selected on several criteria including the support for secure data replication and backup.

The company formulates its backup policies from processes including Risk Analysis and this ensures it is tailored to specific system availability, geographical, and recovery requirements.

This also takes into account Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO), that have been established to deliver customer requirements.

The Backup policy is constructed to meet the requirements established for individual systems and also supports a Disaster Recovery scenario where it may be necessary to rebuild the infrastructure on new hardware and/or location or recover data to a point in time.

5.1.9 Organisational reliability

Where applicable, should iProov make use of other parties, including trust service component providers (that may provide part of iProov's service through third party arrangements, iProov shall maintain overall responsibility for meeting the requirements as defined in this trust service policy.

Should iProov use a trust service component provided by another party, iProov shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.

In the event that iProov may use a trust service component provided by another party, iProov shall ensure that the security and functionality required by the trust service component are meeting the appropriate requirements of the applicable policy and practices.

5.2 Procedural Controls

5.2.1 Trusted roles

The following trust roles that have been deemed critical for security are:

- Information Security Team: this includes information security officers, who hold overall responsibility for administering the implementation of the security practices.
- CTO: Overall responsibility for the sign off and maintenance of the TSPS, services and practices.
- Technical team: Includes System Operators, who are responsible for operating iProov's trustworthy systems on a day-to-day basis. They are also authorised to perform system backups.
- System administrators: Such roles are authorised to install, configure and maintain iProov's trustworthy systems for its services management.
- System auditors: They are authorised to view archives, and audit logs of iProov's Trustworthy Systems.
- Compliance and information security team: advising, auditing, reviewing and improving on Compliance/information security requirements and best practices.
- Technical Operations teams: Meeting day to day security requirements as part of their role.

iProov employees who have been assigned a trusted role have received job descriptions that define functions and responsibilities associated with the trusted role. The relevant qualification, experience, and clearances that the trusted role must have has been defined. Those in trusted roles have also undergone background and clearance checks. Training requirements have been defined for the trusted roles. Personnel who have achieved trusted role status are subject to approval before they are issued access to devices and granted actress to the required facilities, and issued credentials to access and perform specific tasks on the iProov systems. The requirements and rules for the trusted roles apply to both iProov employees and any future contractors who the company may consider using.

Trusted role access is not issued immediately, further information on iProov's trusted roles process can be found in iProov's Trusted roles policy and Trusted Insider Programme.

iProov keeps a record of the persons that have achieved a trusted role status. Approval is required by senior management. Appointment of trusted roles must be conducted by the senior management who are responsible for ensuring the security processes are being utilised. iProov has implemented a trusted roles sign off sheet. Trusted roles can be revoked, roles can be upgraded, and records updated.

iProov Trusted employees do not have access to the trusted functions until the necessary checks and Trusted Roles programme has been completed.

5.2.2 Number of Persons Required per task

iProov has established and maintained controlled procedures to ensure segregation of duties and that the number of staff meets the demands of the tasks required. Trusted roles within the organisation are reviewed to ensure that such positions are identified to perform duties and tasks that are required and deemed sensitive. This is necessary to ensure adequate resources are available to meet the requirements of compliance, security, and risk management.

5.2.3. Identification and authentication of trusted roles

All iProov employees undertake background checks prior to commencing employment with iProov. This includes, but is not limited to, identity verification, DBS checks, employment, and credit checks. Employees in Trusted roles understand that this role has been assigned to them, their responsibilities in the designated process, with all criteria accepted by the trusted role employee.

iProov has access control processes and procedures in place that clearly identifies and logs iProov employees who are in trusted roles.

As a rule of thumb, only necessary access is provided to the roles in question. User accounts are created for personnel with roles that require access to specific systems necessary for the job function. All users must log in with their own credentials, whilst administrative accounts have been made available to those in a trusted function. Access to files is subject to restrictive permissions to prevent unnecessary viewing or use.

Two-factor authentication is a necessary requirement for access to iProov systems.

Only specific iProov trusted employees are granted access to production data where it has been deemed necessary for a specific purpose or task.

Once a trusted role has been terminated or a change has been made to the role, access is terminated for the user. Such rules of access are audited on an annual basis.

5.2.4 Roles requiring separation of duties

Where conflicting duties have been identified this is taken into account when assigning trusted roles. Having clearly defined roles and responsibilities facilitates the separation of duties mitigating further, opportunity of unauthorised access, misuse and unintentional modification of information.

5.3. Personnel Controls

5.3.1 Qualifications, Experience, and clearance requirements

Where the need for a new role or additional headcount has been identified by the relevant manager/head of department adherence to the process outlined below will be required. Requirements of the role, duties and responsibilities will have been defined and documented by the relevant managers along with justification and scope, and a job specification created prior to approval/sign off.

The job description details will include: The roles, responsibilities, and duties, as well as any prerequisites such as experience or qualifications required for the position. iProov employees (including, contract/temporary personnel), are provided with job descriptions that are tailored for the roles requiring fulfilment along with consideration of segregation of duties and least privilege. iProov management determines the position of sensitivity based on the duties and the required access levels to discharge the responsibilities of the role, and considers the level of screening, training, and awareness required. Where applicable, employee job descriptions differentiate between the general functions and the functions that relate to the TSP, this includes (but is not limited to) skills and experience.

Upon successful completion of the multi-level interview process and assessment, the successful candidate must undergo background checks, RTW checks, identity checks, employment verification, DBS checks and any additional clearances and checks deemed necessary. iProov verifies the identity and trustworthiness of each prospective employee. Pre-employment checks are also performed for contractors who join iProov.

Once such checks have been successfully completed, the employee is required to sign agreements that include company expectations, job requirements, confidentiality agreements, protection of confidential information and any bespoke requirement potentially requested or defined by customers.

All iProov employees have the necessary experience, expertise, reliability, and qualifications, and have been provided with the relevant training (which includes information security and personal data protection training) to undertake such duties specified within their employment contract and the job description.

Generally, iProov employees would have obtained the relevant academic qualifications, experience, and expert knowledge and skills to perform their job roles. iProov employees also undergo specific training to achieve this standard.

iProov employees exercise administrative and management processes and procedures that are in line with iProov's Information Security Management procedures.

iProov management possesses the required experience and training regarding information security and their responsibilities. iProov management are responsible for ensuring their own familiarity with the information security procedures as and when an update has been communicated to them by iProov's information security team. iProov Top Management team has the necessary knowledge, and will work with the compliance team to ensure that sufficient risk assessments are carried out for their functions.

iProov employees that are in Trusted roles are free from conflict of interest that may impact their impartiality with regards to the Trust Service operations.

5.3.2 Background Check Procedures

Background checks are conducted in compliance with applicable laws, regulations, and business needs.

Certain checks, such as DBS and/or credit checks are refreshed periodically.

5.3.3 Training requirements

iProov employees have received appropriate training to enable them to safely carry out their required duties. iProov employees have also met the requirements as specified within the job description and successfully illustrated their capabilities within the selection process so that they can competently execute the demands of the job role.

All iProov new starters conduct the following training: Information Security, Data Protection, regulations and internal processes, tools specific to their role, as well as the duties and tasks that are dictated by their position.

iProov updates its training, at least every 12 months to ensure new threats and current security practices are covered and that iProov personnel are up-to-date.

iProov maintains and regularly updates the records of training.

5.3.4 Retraining Frequency and Requirements

All mandatory training must be conducted by all iProov employees. Employee refresher training is conducted on a yearly basis or as required within a given role.

5.3.5. Job Rotation Frequency and Sequence

iProov does not use job rotation.

5.3.6 Sanctions for unauthorised actions

iProov employees who violate, or do not comply with this TSPS, are subject to iProov's disciplinary process. Such actions are in line with the severity of the unauthorised action(s).

5.3.7 Independent Contractor Controls

iProov does not generally employ contractors. If required, contractors will be subject to all background checks and alignment to suitable supervised projects. iProov will define the requirements of the contractor in accordance with the role and tasks required by iProov. The subcontractor (company) is responsible for providing any requested records supporting their own employment checks in addition to those conducted by iProov.

5.3.8 Documentation Supplied to Personnel

iProov employees are issued: Contract of employment, appropriate form of NDA, a defined job role, iProov's employment handbook, iProov training documentation and relevant policies. Such documents include the information regarding the role, procedures that relate to employment law, rights and responsibilities, and laws pertaining to employment at iProov.

5.4. Audit logging procedures

5.4.1. Types of Events Recorded

iProov ensures that information that relates to the operation of the Trust Service is recorded for the purpose of maintaining a secure environment and presenting evidence should a legal proceeding require. Such logs may include:

General Controls:

- The frequency of which the audit logs are processed or archived.
- The period that the audit logs are kept
- Audit log back up procedures
- Who has viewed, modified, or deleted an audit log
- Whether the audit log accumulation system is internal/external to the entity
- Vulnerability assessment history

Event Reporting

- Nature of attempts to access the system and requests processed
- API call history & identification of service/customer accounts accessing the API
- Logging verbosity of API operation & Timestamps
- Source and volume of incoming connection attempts
- Region where action occurred
- Handling rules for routing data
- VPC flow logs
- DNS logs (if applicable)
- Data read, written, or deleted during incident

System Operation

- System component issues that may have affected the platform
- Operating systems affected
- Firewall and router activity
- Systems crashes
- Hardware failures
- System start-up and shutdown
- Clock synchronisation events

Additional Information

- Record of individual users & administrators at time of event
- Audit level in operation - none, metadata, request, request response
- Detection/Identification of credentials relating to malicious use - across the specific region
- Findings related to unauthorised or unusual activity

Registration information recorded includes:

- Unique reference number
- Location of copies
- Where applicable - IP address

5.4.2 Frequency of Processing Log

Audit logging review is the responsibility of the system administrator of a given system. The system administrator accesses logs to investigate reported incidents and investigates these internally.

All audit data is secured and backed up. Logs are also timestamped using a trusted time source located within the data centre where the system is located.

Logs are reviewed by the Operations team as required, or by exception - if there is evidence of a potential attack.

5.4.3 Retention period for Audit logs

Audit logs are stored and available for 10 years, unless alternate agreed conditions apply, applicable law, legislation, demands of a TSP or as a part of a contractual arrangement between iProov and its customer where retention periods may be lower.

5.4.4. Protection of audit log

Events recorded are digitally signed, and any modification of the records is observable and logged. The audit data is made available in a read only format to those with limited access.

Access to the audit log is limited to authorised individuals and follows a privilege model.

Upon requirement for the purpose of legal proceedings, the audit log concerning the operation of services are made available to legal authorities or those whose right of access has been granted by the presiding law.

5.4.5 Audit log backup procedures

iProov performs backups of audit logs which are stored in a resilient manner so that any outage or business interruption can be recovered, and logs can be made available quickly as needed.

5.4.6. Audit log accumulation System (Internal vs external)

Logs are stored using encrypted storage and replicated as part of the Business Continuity process. Logs are pushed toward the storage and timestamped as part of the process of identification. Transaction logs are extracted to the iProov data warehouse where billing and other metrics are available to be consumed by relevant processes and tasks such as the preparation of reports and billing runs. System logs and associated process data are stored safely for periods of time defined in the contract for archiving in encrypted storage.

5.4.7 Notification of event-causing subject

iProov holds logs of any event-causing subject and trusted members with system administrator access are notified immediately. Upon such events, where required, iProov conducts root cause analysis and implements remediation plans derived from any identified threat.

5.4.8 Vulnerability assessments

iProov systems are assessed both internally and externally via vulnerability scans and penetration tests.

iProov logs events to keep track of system vulnerabilities. Vulnerability assessments are carried out, reviewed, and updated. These assessments are carried out on a daily, monthly, and annual basis.

Internal and external vulnerability risks are assessed inline with iProov's risk assessment policies and procedures.

Critical Vulnerabilities must be dealt with within 24 hours, whether via notification or in real time through scanner identification. More specifically, the remediation must either be: completed, investigated with an approved remediation plan, or have a decision in place.

A new vulnerability raised internally includes records such as:

- The name of the vulnerability
- Discovery date
- The criticality
- The priority
- Hosts affected
- The timeline for action
- Detailed description of the vulnerability
- Assigned to
- Due date (determined by the criticality and priority - see vulnerability timeframes)
- The outline of the plan for mitigation

The vulnerabilities are then reviewed and remediated to minimise the detrimental impact of any security incidents, breaches, or malfunctions.

iProov investigates and sets out timelines in line with the threat level.

External Penetration testing is undertaken on an at least annual basis. External companies are used to ensure independence in test performance.

External Pentest engagements are the responsibility of Operations and Compliance and are verified by the CTO.

5.5. Records Archival

5.5.1 Types of records archived

Data that has been considered as relevant for iProov's compliance audit is archived. Information that relates to the transactions, this may include data that derives from the identification and verification of the subject and aggregate information of the outcomes. Audit logs for information security are recorded, in addition to the access and transaction specific logs, and maintained to ensure continued integrity.

5.5.2 Retention period for archive

Archived information is retained for a period of 10 years.

5.5.3 Protection of archive

Archived data is subject to iProov's access control processes and procedures. Archived data is stored separately and is protected by iProov's access control processes and procedures. Archives have been made secure from modification, tampering, deletion and unauthorised access. Both organisational and technical controls are in place to achieve this goal. The archives are also safeguarded against storage media failure.

5.5.4 Archive back up procedures

iProov has archival backup procedures in place. Backups of systems are made via iProov's cloud service providers. Such suppliers have been selected based on being able to provide a high availability, replicated-data architecture, with data backup provision built in. Through supplier relationship management processes, whereby suppliers are selected on a number of criteria and considerations, including data replication and back up, iProov gains assurance that our backup and continuity requirements are met, e.g.:

- Backup of operational databases are stored on GCP
- Image and video data is stored on GCP
- Operational databases are backed up at least daily and a full restore is tested on every backup

5.5.5 Requirement for timestamping of records

Records are issued a timestamp using accurate time and date. The timestamp derives from a synchronised nuclear time source as part of NTP configuration processes.

5.5.6 Archive collection system (internal or external)

iProov uses a combined internal and external archive collection system, with records initially archived to the same availability zone where the cluster resides and then replicated to two external availability zones for resilience.

5.5.7 Procedures to obtain and verify archive information

The archived information is only made accessible to authorised iProov employees that are in Trusted Roles.

Records relating to the operation of services shall be held for an appropriate amount of time should they be required for the purposes of providing evidence of the correct operation of the services and/or legal proceedings, they are made available to legal authorities and/or persons who have a legal right of access to them via a written request

5.6 Key Changeover

Not applicable.

5.7 Compromise and Disaster Recovery.

5.7.1 Incident and Compromise Handling Procedures

iProov has implemented a disaster recovery plan, business continuity programme, as well as having risk management processes in place. iProov has a streamlined incident management process and holds regular audits to mitigate risk.

iProov’s Business Continuity programme is supported by iProov’s Senior Management to ensure that the appropriate measures, plans, and strategies are in place, defined and reviewed to ensure mitigation of potential impact from loss of business services, information assets or operations.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, iProov will notify the natural or legal person of the breach of security or loss of integrity without undue delay.

We maintain a Business Continuity Risk Register – Part of iProov's Business Continuity Management that ensures risks to the company have been identified, with the implied plans of mitigating the threat to the business. This is continually assessed.

Information security continuity is integrated with iProov's business continuity programme. As such:

- Information security requirements for continuity are at least equal to those required during ordinary operation.
- The critical information assets that are involved in each process are identified and cross referenced to the asset registers.
- For each of the services, iProov identifies the risks (from disasters, security or equipment failures, loss of service, attacks, and loss of service availability) that iProov Ltd is experiencing.

iProov identifies, for each of the risks, the possible information security continuity impacts that they may have on the business, ranging in seriousness from loss of site connectivity/availability through to loss of site(s) functionality.

Risks are prioritised in terms of their impacts on iProov Ltd, and the information security continuity planning process is designed to tackle these risks in order of priority.

The Continuity Plan addresses all the information continuity components of iProov Ltd.'s activities and ensures that adequately trained resources are available to provide continuity of all the identified information security assets, including taking appropriate steps for the protection of Employees/Staff (including information processing) and all information processing facilities.

Service level agreements are in place with all iProov customers. Service availability, levels and expected performance is agreed with iProov customers.

Recovery plans are tested at least annually.

Back up arrangements are tested regularly and reviewed by Trusted Roles.

Critical vulnerabilities are addressed within 24 hours.

In the event of an emergency, iProov will inform all relying parties without undue delay, within 24 hours of the senior management designation of an emergency and the proposed solution. communication is conducted via iProov's nominated communication channels.

iProov has established procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

In such event, iProov will record and keep accessible for an appropriate period of time, no less than 7 years (or 10 years if the activities of the TSP have ceased), the following: all relevant information concerning data issued and received by iProov, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

Information, assets, risks, and policies/controls created throughout iProov’s ISMS are used with the intention of understanding interruptions - and their impact on the business. Business continuity is designed based on the probability of occurrence with consideration to the confidentiality, integrity and availability of the information and assets on the business' ability to continue performing as expected.

As part of the broader risk assessment, events that can cause interruptions to business processes are identified, along with the probability and impact of such interruptions and their consequences for information security. This is already conducted in a documented information security risk assessment process and the Risks and Treatment Plan is an integral part of information security continuity.

Further information can be found in iProov’s Business Continuity Plan.

5.7.2 Computing resources, software, and/or data corruption

In the event of computer corruption, software corruption and/or data corruption, iProov will handle the issue in line with its incident response process and procedures.

5.7.3 Recovery Procedures after key compromise

iProov private key compromise will be handled in line with iProov’s incident response plan.

5.7.4 Business Continuity Capabilities after a disaster

iProov has a disaster recovery plan, business continuity programme and plan in place that addresses iProov’s crisis management protocol and communication within emergency situations.

As well as ensuring the safety of iProov’s employees and customers in the event of a disaster, iProov will also take measures to ensure the protection of business assets, IT resources and service to enable swift recovery of its business operations. Furthermore, the disaster recovery plan outlines the process involved in recovering the production infrastructure in the case of a catastrophic failure that requires rebuilding of the entire platform either in its original location or recovery to an alternative site.

The information in this document was verified by the performance of a simulated failure with the scenario requiring recovery to an alternative site. All actions were recorded and merged with the original process steps to produce this comprehensive process.

Low level disruption – Managed locally by the affected/ relevant department, led by the Head of Department. Low level impact incidents can be managed using existing processes and procedures. Low level disruptions will require review from the Information Security team, which will be logged, assessed with lessons learned when considering root cause analysis. Additional review or audit will be assessed on a case-by case basis.

Moderate disruption – For moderate disruption to the service delivery, this will be managed locally by the relevant Heads of Departments, and where necessary, the Senior Leadership Team. Most moderate level impact incidents can be managed using existing processes and procedures already in place, however, changes may be required within the existing process. Moderate level disruption will require review from the Compliance/ Information Security team, which will be logged and assessed with lessons learned when conducting root cause analysis. Additional review or audit will be assessed on a case-by case basis.

High impact – Incidents resulting in high level disruption will be managed by the head of department, the senior leadership team, and where applicable, employees “on call.” The CISO alongside the Compliance/ information security team will investigate and report. A complete root cause analysis will be compiled, lessons learned and follow up review following the incident. A follow-up audit may be deemed necessary.

As an organisation that primarily uses cloud-based technologies, replication and backup security is managed by iProov using primarily the responsibility of our cloud providers technologies, managed by iProov.

Through our controls relating to management of Supplier relationships, we gain assurance that our backup and continuity requirements will be met. Suppliers have been selected on several criteria for consideration including data management facilities, replication and backup.

The company operates a backup policy derived from risk analysis to develop a policy that is tailored to specific system availability and recovery requirements. This takes into account Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO), that have been established to deliver customer requirements.

The Backup policy is constructed to meet the requirements established for individual systems and in all cases also supports a Disaster Recovery scenario where it may be necessary to rebuild the infrastructure on new hardware and/or location or recover data to a point in time.

For our online services, our cloud service providers have been selected based on being able to provide a high availability, replicated-data architecture with data backup provision built in and available.

Operational databases are backed up at least daily and a full restore is tested against every backup configuration.

Backup of operational databases are stored on GCP.

Image and video data is stored on GCP.

All static data, including the configuration required for a rebuild of the operating platforms is stored local to the platforms along with a backup copy in an alternate location. Using this data combined with the data sets above it shall be possible to rebuild platforms from the ground up and maintain the current data state.

5.8 Termination

iProov has a Termination plan in place, made available upon request.

Before iProov terminates its services shall make the information of the termination available to other relying parties and will:

- Inform all entities that iProov has contracts, or other forms of established relations, along which relying parties, TSPs and relevant authorities such as supervisory bodies.
- Ensure it makes the information of the termination available to other relying parties.
- Terminate authorisation of all subcontractors who act on its behalf, in carrying out any functions relating to the overall process of supporting the issuing of trust service tokens.
- Transfer obligations for maintaining all information necessary to provide evidence of iProov operations to a reliable party for an agreed time period, unless it can be demonstrated that iProov does not hold any such information.
- Terminate or otherwise remove from use its private keys, in a manner that ensures that the private keys cannot be retrieved.

In the event of termination, including termination of business activities, company merger or acquisition, iProov status as a TSSP and so forth, iProov will notify the affected entities, as well as inform the relevant, relying parties such as subscribers, including those with contractual agreements and established relationships, and the relevant supervisory body(s).

A termination plan will be drawn up, dealing with post-contractual services that iProov may provide after the termination being made effective. The termination plan will include all iProov's dependencies. The overall purpose of the termination plan is to allow iProov to migrate to an alternative and to minimise the impact as much as possible.

In such an event, to ensure a smooth transition with minimal impact to each party iProov will implement an updated exit strategy that includes the contractual obligations, legal obligations, post-contractual services provided by iProov and so forth. Time frames of the completion of the actions will be included within the exit strategy. The aim remains for minimal impact and interruption on the relying party in the event of cessation, thus, termination shall not relieve iProov of its obligations, confidentiality, evidence storage and legal obligations until all actions have been fully discharged.

In the event of a contracted CA terminating its services, the relying parties will be informed about this, and will have the right to object.

iProov ensures that audit logging will be retained for a period of 10 years.

iProov conforms to its contractual and legal obligations.

Before the termination of service, iProov will transfer its obligations to a reliable party for maintaining all information necessary to provide evidence of its operation for a reasonable period of time, unless it can be demonstrated that iProov does not hold any such information.

Termination plan:

1) iProov will inform all relying parties, relevant authorities, sub-processors, and any other entities of which iProov has agreements in place that an exit strategy is being implemented.
2) Destruction of Service Provider keys, including backup copies and wiping of hardware appliances related to service in compliance with the security requirements to prohibit further use.
3) Termination of authorisation for iProov subcontractors.
4) Maintenance of logs, documentation and information required for verification. In an unscheduled termination event, this information will be transferred to another TSP to ensure transfer of service provision for existing customers. iProov does not assume liability for any loss or damage sustained by the user of the service as a result of termination.

Should iProov face bankruptcy, iProov has arrangements in place to cover the costs to fulfil these minimum requirements if iProov is unable to cover the costs itself.

The Termination Plan is updated on a regular basis to maintain it in a current and functional state.

5.9 Asset inventory

The asset inventory is adjusted once the asset has been disposed of as follows:

I. Devices containing confidential information are wiped prior to disposal and are never re-used. If necessary, the device(s) are put beyond practical use.
II. Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.
III. Portable or removable storage media of any description are destroyed prior to disposal.
IV. All media are disposed of in line with WEEE (Waste Electrical and Electronic Equipment Directive – 2012/19/EU) regulations on disposal of computer equipment, through the Organization's approved contractor. The contractor is a licensed waste carrier and relevant Waste Transfer Notes are retained by the Information Security Manager for minimum of two years.
V. Documents containing confidential information which are to be destroyed are shredded by their owners or disposed of as confidential waste. WeWork is specifically approved for this role.
VI. The organisation provides the opportunity for staff to work off-premises away from the Head Office, including home working and other locations.

5.10 Risk Management

iProov has determined all security requirements and operational procedures that are necessary to implement the risk treatment measures available. iProov's Senior management and Information Security team establish the security policy, which becomes the basis for the consistency and completeness of the Information security and management support.

iProov CTO is responsible for ensuring practices have been implemented and maintained, and approves policies and practices related to Information security of iProov services. iProov CTO, Top Management and Information Security Team publishes and communicates our information security policies and changes to internal and external parties, which includes subscribers, relying parties, assessment bodies, supervisory and other regulatory bodies.

iProov carries out regular risk assessments on a yearly basis and this is revised on a regular basis. Risk assessments are visited every 3 months by iProov's Senior Management and are continually updated as and when new risks have been identified. iProov Management approves risk assessment and accepts the residual risks identified.

iProov Ltd conducts risk assessments in line with ISMS DOC 6 of individual offices, rooms and facilities that contain confidential or high-risk information assets to identify the controls that might be necessary to secure them. There are no sites where confidential information processing facilities are shared with a third-party organisation, other than under the terms of a contract.

iProov has developed, implemented, and continues to maintain a comprehensive security programme that aligns with applicable standards (such as ISO 27001, 27701 and so forth), in addition to standards and compliance requirements that are required by applicable laws.

iProov has practices and procedures in place that are used to address all the requirements of the applicable trust service policy being supported, these are maintained inline with our developed policies.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

Not applicable. iProov does not generate, store and use key pairs which are directly used in any qualified trust services according to Article 3 (16) of eIDAS.

6.1.1 Key Pair generation

Not applicable.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuing Organisation

Not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

Not applicable.

6.1.5 Key Sizes

Not applicable.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.1.7 Key Usage Purpose (as per x.509 v3 Usage Field)

Not applicable.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Not applicable.

6.2.2 Private Key Multi Person Control

Not applicable.

6.2.3 Private Key Escrow

Not applicable.

6.2.4 Private Key Backup

Not applicable.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into from a Cryptographic Module

Not applicable.

6.2.7 Private Key Storage on Cryptographic Module

Not applicable.

6.2.8 Method of Activating Private Key

Not applicable.

6.2.9 Method of Deactivating Private Key

Not applicable.

6.2.10 Method of Destroying Private Key

Not applicable.

6.2.11 Cryptographic Module Rating

Not applicable.

6.3 Other Aspects of Key Pair Management

Not applicable.

6.4 Activation data

Not applicable.

6.5 Computer security controls

Security is applied to off-site equipment and assets with consideration to the different risks of working outside iProov Ltd.'s premises.

To the extent that iProov has enabled relevant equipment to be taken off site, employees are responsible for those assets whilst in their care.

Users of mobile equipment are required, as part of their User Agreements, to provide appropriate physical security for iProov equipment when off-site and to ensure that manufacturer's instructions for protecting equipment are followed.

Employees are required to ensure that equipment removed from its secure area is returned and secured when it is no longer in use.

Employees identifying unattended equipment outside its secure area are required to return the equipment to the Asset Owner.

Where appropriate, paper and computer media containing highly confidential information are stored in suitable locked cabinets when not in use.

Laptops are screen locked when unattended and protected by passwords conforming to the iProov password policy.

Printing of any information, especially Confidential or Highly Confidential information, is discouraged. Information when printed is cleared from printers immediately.

Laptops have a screen saver enabled after less than 10 minutes of inactivity.

Staff lock their screen when leaving their desk/computer.

iProov’s ISMS details the provisions, controls, and operating procedures in place.

6.5.1 Specific Computer Security Technical Requirements

iProov’s Information Security Policy details iProov’s commitment to information security. iProov’s CTO holds overall responsibility for the conformance with the procedures that are prescribed in iProov’s ISMS. iProov’s CTO approves Information and Security Practices that relate to iProov’s overall service. iProov’s Senior Management and Information Security Team establish and maintain the information security policy, which forms a basis for consistency and completeness of information security management support. A detailed list of Controls in relation to iProov’s information security controls can be found in iProov’s Statement of Applicability. iProov is certified against multiple Information security standards including ISO 27001.

iProov publishes and communicates its Information Security Policy and its controls to all employees and relevant external parties that are impacted by it. iProov retains responsibility for its Information Security Policy and its controls, even in the event of iProov’s services being undertaken by outsourcers.

System components are hardened to minimise the risk of unauthorised access or attack to the systems. Devices, tools, software and platforms are secure and operate with multiple controls. Multiple security controls are in place throughout the lifecycle, that include, but are not limited to:

- Environments are isolated
- Data Encryption at rest and in transit
- Encryption of secured connections
- Encryption of secure audit logs
- Hardening of systems
- Access control procedures
- Auditing
- Daily vulnerability scans
- Regular penetration tests
- Firewalls and Security Group Implementation
- MDM management
- Trusted roles and training for each of the platform elements.

Vulnerability management procedures are documented in an internal Vulnerability management policy. Through the use of Antivirus and MDM systems, all abnormal system activities indicating potential security breaches, including network intrusions, are monitored and investigated.

iProov ensures that sufficient security control procedures are in place which includes the separation of trusted roles, security administration and operational functions. System utility programmes are restricted and controlled.

iProov employees are identified and authenticated before using critical applications that are related to iProov services. iProov personnel remain accountable for their activities.

In line with iProov’s Access Control policy, access to the information and application system functions are restricted. User account management includes the timely removal and modification of access.

iProov protects sensitive information against being revealed through re-used storage objects such as “deleted files' ' or “trash” or media with the potential of unauthorised access. iProov employees are trained to not store information on reusable storage objects or removable media and this is further controlled by iProov’s MDM system.

The integrity of iProov’s systems and information are protected against viruses, malicious and unauthorized software.

Procedures are established and implemented for all trusted and administrative roles that impact the provision of services.

Security patches are applied in line with the timeframes set out in iProov’s vulnerability management process. This is to ensure that patches have been applied within a reasonable time after they come available. Reasons for not applying security patches are documented; this is detailed in iProov’s vulnerability management process.

The following describes a few of the security measures iProov has in place that relate to its endpoints, applications, and Platforms.

6.5.1.1 Endpoint security

Most of our information is stored in the cloud, with local devices mainly serving as a vehicle for drafting and generating content.

- All endpoints undergo iProov's endpoint management process. ICT equipment and processes are selected based on suitability and alignment to sensitivity or classification requirements. All ICT equipment is managed internally and upon completion undergoes iProov's ICT equipment sanitation and disposal process.
- All end user devices used for platform administration are built to a standard base profile. This includes antivirus, antimalware, disk encryption, and tools required for platform secure access. Windows machines use Hexnode MDM which is monitored and auditable. Machines are managed by MDM to ensure no shadow IT is possible and a process for requesting software exists. All installations need to be signed off by the head of compliance or CTO; it is prohibited to remove or install any unlicensed or non-company approved software.
- Devices are equipped with antivirus which is monitored using a dashboard to evaluate device threats and version/update status.
- SOE's are updated as required and obsolete OS upgraded in line with releases.
- All operating systems are hardened in line with best practice recommendations.
- Removal of spurious resources is performed as part of device hardening.
- All devices have a standard firewall configuration.
- Users are authenticated before they are granted access to a system and its resources.
- The principle of least privilege is applied wherever possible.
- Users would need the granting of privileges, in order to install software.
- Unlicensed software must not be installed even for learning/training purposes.
- Software is copyright protected. The employee must ensure that copyright is not violated.
- Any specific software used for any specific purpose must be licensed or authorised by the software vendors.

6.5.1.2 Endpoint - controls against malware

All MacOS and Windows laptops/desktops and Windows servers must be protected with antivirus software.

Antivirus definitions are updated automatically and monitored through an operations portal which also provides in depth threat logging statistics.

Malware detection scanning is carried out as part of the overall security footprint and deficiencies automatically addressed. The scans run at least weekly though this is configurable if a need for a shorter duration scanning interval becomes apparent.

We empower users by giving the freedom to access external information online without restriction or lockdown of sites provided they stay within the boundaries of our:

- Terms and conditions of employment

- Code of conduct; and
- Acceptable use of assets policy

We also encourage users to stay abreast of general security best-practice procedures and precautions. Staff communications and awareness on the subject is also assured through the Information security team in line with Information security awareness, training and education. Given these controls and those below we do not employ any other explicit form of software whitelisting or blacklisting.

Deliberate actions taken by users to deactivate anti-malware controls is considered “unacceptable use” and prevented by the MDM. Attempts to do so may lead to investigation and possible use of the Disciplinary Process.

For devices used by employees

- The use of anti-virus software on employee devices is mandatory to detect and eliminate common malware that is in existence.
- We use well-known and widely trusted products to minimise the risk of a user encountering malware.
- This is supported by our Mobile device policy.

6.5.1.3 Application control

- Across the application, Application restrictions are implemented using Security Groups, privilege control, and access rights and procedures.
- All file permissions are configured on a minimum privileged basis with access restricted to necessary entities. Applications are not modifiable by anyone without express consent of IT and security function under change control.
- Multi-factor authentication is used to authenticate all support personnel with additional privileges separately administered for those in trusted roles. All second factor credentials used for multi factor authentication are one-time passwords received via text or authentication application and used in addition too, and appended to an individual's personal pin. The OTP appended to the pin is only valid for a limited time before expiring. There is no reuse of passwords.. Accounts are locked after a maximum set of failed login attempts, issues are investigated before access is re-enabled. The user must be verified and deemed qualified by team Managers and systems admins before account modification to enable privileged roles.

6.5.1.4 Platforms & Virtualized hardening

- iProov does not use third parties to maintain the platform, maintenance of the platform is performed internally.

- Segregation of operating environments and secret key generation and rotation is employed on all our platforms.
- Servers are built and hardened to prevent applications running or communicating with extraneous services and restricting them to the prescribed function.
- Platform security is under constant review and secret keys and certs rotated at least annually.
- Multi-factor authentication is used to authenticate standard users.
- Software-based isolation mechanisms to share physical server hardware are utilised with managed services provided by any one of the three main cloud providers. The iProov software runs in a further “Containerised” abstraction and is purpose-built to perform the required functionality while running in a Microservice, fully orchestrated, software-based isolated environment.
- The appropriate software is required to be developed using secure coding practices. Such software is required to be tested to ensure security controls, including access controls, these are implemented to restrict access to the management interface. When using software-based isolation mechanisms, the underlying operating system running on the server is maintained by the cloud provider.
- Service software including software-based isolation mechanisms and operating systems are subject to the continuous vulnerability scanning and patch management process. This enforces the identification of missing patches and timely remediation.

iProov has a security risk management plan and records and monitors the identified risks and mitigation measures. The Security Risk Management Plan receives inputs from the following:

- Certification reports,
- threat and risk assessments,
- penetration tests, and
- compliance reviews.

The operations of the iProov platform are designed to be, and are by their very nature, independent of each other, this allows for independent operation and resilience. Any failure of hardware equipment is automatically dealt with by platform automation.

6.5.1.5 Cryptographic Controls

Appropriate security controls are in place for the management of cryptographic keys throughout their lifecycle.

iProov as a biometric verification provider uses cryptographic controls for protecting its own biometric verification services platform. iProov encryption key management is performed using cloud-based facilities, specifically “Cloud Key Management Services” on our Google eIDAS platform. This is used as a front end to Google's cloud based HSM to ensure secure management of credentials as required. iProov follows industry best practice and security standard requirements in relation to the key management lifecycle, key length, and algorithms.

Generation of key pairs is performed by Google KMS and conforms to FIPS 140-2 Level 3 certification. The following standards are employed within GCP FIPS 140-2 Level 3: AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys.

CMEK are generated on the google platform using KMS and moved across to the relevant endpoints using local commands from a privileged account.

Keys are delivered to iProov through secure encrypted channels and are then removed from the media used to deliver them. iProov can work with customer secure portals or default to “Signal Messenger” which is fully end-to-end encrypted and can be configured, by either party, to delete the message containing the keys after a configurable period of time.

iProov uses a key management service that manages symmetric and asymmetric cryptographic keys for iProov’s services. iProov can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys as required in conjunction with cloud services.

iProov raises a certificate signing request with the appropriate CA as required for its platform. Key management is maintained by Google KMS, with keys rotated at least annually and utilises available, ratified cryptographic standards as listed above.

Keys are generated using standard change request processes that require the involvement of a minimum of two people to effect the change. Personnel involved have been assessed suitable and confirmed for privileged roles. A minimum of two people is required for any key recovery of this kind.

iProov use Cloud based HSM to secure keys. Secondary HSM’s are used to backup sets of keys. Keys are generated in a HSM residing on the platform enabling deployment locally. Private keys are generated, activated and deployed, at the time of use by personnel with elevated privileges under Change Control. Any tampering with systems where keys are deployed will result in deactivation and replacement where necessary of affected keys. Facilities within the HSM are used when keys are required to destroyed.

6.5.2 Computer Security rating

iProov provides standard Endpoint computer systems.

6.6. Life Cycle Technical Controls

6.6.1 System Development Controls

System development controls are in place within the software development process to limit the risks of vulnerabilities. These include code review, design processes, testing, and deployment controls, followed by full operational monitoring and life cycle control.

The software development process is in place to standardise the process whilst ensuring that information security is implemented by design whilst mitigating the risk of coded bugs and vulnerabilities.

Before the technical phase of any Project can be initiated there are certain prerequisites to be fulfilled:

- Clearly defined goal(s), success criteria and responsibilities.
- Project Sponsor and stakeholders identified.
- For a project to succeed iProov recognises that there needs to be a holistic approach to all aspects of the undertaking starting with a clearly defined goal. This is achieved through mechanisms which include scrutinising the proposal, spending time analysing the original request, and ensuring what is being asked for is suitable and thorough enough to achieve the identified objective. It is the responsibility of the sponsor of the HLP (High Level Priority) Item to ensure that the goal is clearly understood.

6.6.1.1 Functional Requirements

Functional requirements are described as all the performance characteristics and behaviours required for the product to satisfy the defined role of the application. This includes integration with any existing production platforms required to cofunction as part of the solution i.e. database or other platform resources.

The details of the platform in terms of capacity and services required for the new application is assessed as part of understanding the total scope of the project and serves to aid the initial assessment of infrastructure requirements.

6.6.1.2 Non-Functional Requirements

Non-functional requirements are described as all the characteristics of the application not required for the integration or core function and include look and feel of the application and the behaviours it exhibits toward the end user. The presentation,ease of use, and intuitiveness are considerations for non-functional design.

Security of a new application is considered non-functional in many requirement statements; however, as a biometrics company, the security of an application is considered paramount and should be evident at the forefront of design decisions.

Capacity considerations should also form part of the non-functional design with attention paid to the new systems extensibility, scalability, and ease of upgrade should this become necessary.

6.6.1.3 Process Execution

iProov develops all of its software in house using full time staff and does not outsource. This enables close control of iProov IPR and encompasses the requirements below.

Version control is applied to all code to monitor and provide an audit trail of the changes to the code.

6.6.1.4 Source Code Management

Source code is committed early and frequently into Github. iProov uses a methodology allowing clear separation between development, test and production with clear versioning. Merges of code require peer review and automated vulnerability analysis and other testing is in place.

6.6.1.5 Change Control

A tailored change control system specifically for the development project scope should be created and signatories agreed. The main iProov change control process is not to be used as designated signatories are for the operational production platform control. Operational personnel are unlikely to be involved in projects and control for the development actions needs to remain within the project team.

At the successful completion of the project iProov production change control should be used to introduce the software onto the production platform and then from that point forward standard production control will apply on the platform.

Change control procedures are applied for releases, modifications, and emergency software fixes of any operational environment. This change procedure applies in all incidents, or configuration that are reflected in iProov's Information Security Policy. Such changes are documented.

6.6.1.6 Code Review

Code should be reviewed during the development of the service and address specific concerns around the following areas:

- Security
- Interoperability
- Functionality
- API compatibility

iProov strives to create software which integrates seamlessly with current processes, and which can be monitored and managed in line with existing procedures.

6.6.1.7 Security Review - code

All completed code is tested for security and vulnerability compliance prior to deployment. This includes any modules or existing libraries that form any part of the completed project. Code will be written with potential security considerations prominent in the design. In addition to component security the complete platform is subject to review and issues identified and addressed before the system becomes operational.

6.6.1.8 Testing Methodology

Testing should be performed on individual components as well as the end to end system. The creation or modification of testing platforms will form part of the project. Testing addresses:

- Function
- Monitoring and Reporting
- TDD results
- Additional platform related testing
- Unit tests
- OWASP top 10 requirements
- Code review outcomes
- Recovery processes

It also includes additional considerations:

- Confirming the design of a consistent user interface integrating corporate identity requirements.
- Business rules relating to the use of data, retention periods, and compliance requirements are able to be implemented into the design.
- Back-end systems conform to the appropriate standard design architecture models to enable deployment and support to be performed in line with current systems.
- Consideration should be given to elements suitable for pre-release or extended testing to bring elements to completion in a propitious manner.
- Implementation and support documentation.

6.6.1.9 Additional controls

Training to be provided covering the overall solution and the specific components that underpin the software development.

User guides produced for the end user of the system as required.

Monitoring systems configured and tested to provide system status, resource usage, and transactional throughput.

The CTO/Relevant Head needs to approve information and new visions of software.

6.6.2 Security Management Controls

iProov products, systems, software, and devices are managed, controlled, and monitored in order to ensure integrity, confidentiality and availability of information. iProov has streamlined a combination of automated and manual processes to monitor activity, detect and decline unauthorised attempts, whilst notifying the relevant trusted roles of changes and any activity that may be out of the ordinary. iProov also analyses unauthorised/fraudulent attempts to strengthen and improve detection, controls, and its automated and manual processes.

6.6.3 Life Cycle Security Controls

iProov policies, procedures, practices, and assets are reviewed at planned, periodic intervals, or when significant changes have been made to ensure adequacy, suitability and effectiveness of controls and measures are in place.

Changes must be reviewed by the designated trusted role, and should sign off be required at a higher level, this final review must be conducted by iProov's CTO.

A current and complete information asset inventory is a prerequisite for effective technical vulnerability management. The inventory of all information assets is assigned a classification that is in line with the risk assessment.

Configurations of iProov's systems are under constant review. Changes that are made follow strict measures and controls. Configurations are frequently checked for changes that do not comply with iProov's security requirements. iProov's CISO is required to sign off changes that may have an impact on the level of security provided.

iProov has processes and procedures in place to ensure that new versions of infrastructure application code are applied to its systems within a reasonable time period after they become available. This is no later than 6 months following the availability of the security patch. Violation of this requires documented reasons for not applying the security patches. For instance, a new version of software would be deployed well in advance of the older version being "out of support".

iProov has established the following timeline requirements for reacting to notifications of relevant vulnerabilities:

- Patches rated as Critical are deployed within 48 hours.
- The Chief Technology Officer may authorise emergency patching at any time.

- Once a potential technical vulnerability has been identified, the organisation identifies the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls.

The required controls are actioned through the change management procedure.

Available patches must be risk assessed, considering the balance between risks in installing and not installing, before the final decision as to necessary controls can be made.

Wherever appropriate, patches must be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls must be considered, such as:

- turning off services or capabilities related to the vulnerability
- adapting or adding access controls, e.g. firewalls, at network borders
- increased monitoring to detect actual attacks, and
- raising awareness of the vulnerability.

Systems at high risk should be addressed first.

6.7 Network Security Controls

iProov prevents unauthorised access and malicious activity by adhering to strict access control measures. Such controls are preventative, detective, corrective, preserving the integrity, confidentiality, and availability of the information.

The platform is not publicly accessible and has a single external endpoint.

Risk assessments are carried out for each network within the scope of this procedure, to ensure that all information security risks have been identified and appropriate controls selected. The risk assessment is reviewed in line with the review requirements of the ISMS.

The network architecture reflects the risk assessment, is designed to maximise security and business efficiency, and is kept under review.

Remote equipment is managed in accordance with iProov’s information security requirements.

Network access control is managed in line with iProov’s information security requirements.

Confidential and restricted information is encrypted as required and in line with iProov's information security requirements.

Network availability is maintained by the IT team.

iProov Ltd has deployed logging and monitoring controls, the configuration of which and reporting should be communicated regularly to senior management.

iProov conducts regular vulnerability scans and penetration tests performed by an individual or an entity with the required skills, proficiency, code of ethics, tools, and independence to provide reliable support and to ensure iProov's own reliability.

Scanning is a scheduled function, running daily, or can be invoked if a major platform change was to occur. This function's responsibility sits outside of platform support and is monitored by compliance and operations to ensure independence.

In addition, external penetration tests, when they occur, are cross referenced with internal results to validate any identified issues.

6.7.1 Security of network services

Risk assessments are carried out for each network service and appropriate controls including authentication, encryption, security, and appropriate network connection controls are selected.

The identified controls are included in the external party agreement/internal SLA.

External party agreements are managed in line with requirements.

Network guidelines set out the technical parameters and configuration requirements for connection with network services.

iProov does not use administrative systems that are used for security policy implementation for any other purpose(s).

Where an assured high level of availability for external access is required, the external network connection is made redundant, this is to ensure the availability of iProov's services in the event of a potential failure.

6.7.1.1 Segregation in networks

iProov keeps all systems that are critical to iProov's operation in one or more secured Zones.

iProov has separate dedicated networks for the administration of IT systems and iProov's operational network.

Cloud networks are segregated using standard cloud technologies VPC's/VNET's and organisational structures both above and below these virtual environments. Within the VPC separate and segregated availability zones and CIDR address space exist with networks isolated from each other based on routing and security group rules.

On corporate G-Suite platforms separate Organisational Units (OU's) are required to segregate iProov users from any permitted guests.

The perimeter of each domain is well defined.

Logical segregation of networks will be defined according to the zoning architecture required, ensuring secure zones, internal network zones, external network zones and Internet zones, each with tailored access and connection restrictions. Network zones are subject to the same security controls, and rules are reviewed on a regular basis.

Test environments are segregated from production environments.

The Head of Operation and Compliance is responsible for ensuring the correct evaluation of proposed changes has been completed and that auditable design documentation has been provided. IT design ensures that sensitive/critical information systems are isolated from other systems and are in discreet environments, dependent on data segregation, confidentiality, and other business requirements. Access to these environments is controlled and it should also be ensured that access is given only on a least privilege basis.

Network zones are defined to classify and subdivide the group of users and services depending on business criticality considerations, business agreements and security considerations.

iProov's security of the internal network and its external connections are constantly monitored to prevent unauthorised access. Unrequired connections and services are deactivated so connection is impossible.

iProov performs vulnerability scans daily and Penetration tests at least annually. Vulnerability scans are performed at set up, and after infrastructure or application upgrades or modifications that iProov determines are significant. iProov holds records of such tests and scans.

As we primarily use cloud-based services, the security of network services is controlled in conjunction with the cloud service providers. iProov requires the cloud provider to have certification to information security standards such as: ISO 27001, SOC2, and other relevant certifications.

Our security controls are limited to ensuring secure connections between our local devices and the cloud services and this is covered within Network controls as described below:

- The network architecture is designed to maximise security and business efficiency.
- All remote access to networks is over VPN.
- Network availability is maintained by the DevOps team.
- Network configuration is under source code control.

Internal penetration testing/ vulnerability scans are performed at setup and after infrastructure or application upgrades or modifications that the TSP determines are significant.

iProov configures its systems by removing or disabling all accounts, applications, services, protocols, and ports that are not required for use within its operations.

6.8 Time stamping

Audit logs (including availability and use of services) and transactions (including start-up and shutdowns) are time-stamped on a Reference Clock Service provided by iProov’s cloud service provider from a stratum 1 time source, this is synchronised with UTC at least once per day. This time signal derives from a synchronised time source.

All changes, database entries, and events contain accurate time and date information which is recorded.

Apart from that, time stamping in the sense of a Trust Services following the eIDAS regulation is not applicable.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate profile

Not applicable.

7.2. CRL profile

Not applicable.

7.3. OCSP Profile

Not applicable.

8. Compliance Audit and other assessments

8.1. Frequency or circumstances of assessment

To ensure conformity of information systems, policies, practices, processes, personnel, assets and facilities, iProov are assessed by the relevant assessment body to the eIDAS regulation, the relevant legislation and applicable standards.

iProov carries out multiple internal audits as outlined in iProov's internal audit plan.

iProov is also subject to external eIDAS audits at least annually by a qualified auditor.

8.2 Identity and Qualifications of the assessor

The assessment body must be accredited with Regulation EC no 765/2008 as competent to be able to carry out the assessment of qualified Trust Service Provider and qualified Trust Service it provides.

The auditor must be qualified to carry out such audits, by possessing the necessary qualifications and skills.

8.3 Assessor's relationship to assessed entity

External auditors are independent from iProov and the assessed systems. The internal auditor will not audit their own areas of responsibility.

8.4 Topics covered by assessment

iProov's assessment is to ensure conformity of the information systems, policies, practices, procedures, personnel, facilities, assets, and services in line with the eIDAS regulation, applicable legislation and standards. The assessment body audits all areas that iProov includes when providing services to a Trust service.

The areas that are audited include:

- Risk management
- Change management
- Human resource security
- Software development

- Compliance
- Network security
- Access control
- Business continuity
- Security of service
- Quality of service
- Operational processes
- Protection of data
- Logging and monitoring

8.5 Actions taken as a result of deficiency

Following an audit, for areas of non-conformity, a corrective action plan will be put in place that has been agreed with the auditor. The auditor will ensure that timescales have been outlined which iProov must meet.

8.6 Communication of results

The certificates and their scope can be viewed via iProov's website: www.iproov.com. The underlying audit reports are confidential and are given to the applicable national supervisory body.

8.7 Self audits

iProov carries out internal audits to continuously assess iProov's information security management system, its internal policies, processes, procedures and practices comply with the applicable laws, regulations, internal policies and certified standards.

9. Other Business and Legal Matters

9.1 Fees

iProov customers pay inline with the specific commercial requirements, agreed within a contract which can vary across customers, their business needs, product requirements and solutions that iProov must implement.

9.1.1 Scope of confidential information

iProov considers all data with regard to the service modules operation as described in this TSPS as confidential. See also the section “Privacy plan” below.

9.1.2 Fees for other services

Fees for services are specified in iProov’s price list or are as agreed with customers from time to time.

9.1.3 Refund

Refunds are handled on a case-by-case basis, subject to contractual agreements.

9.2 Financial responsibility

iProov has liability insurance that covers more than the needed €1.000.000 to cover the responsibilities of art. 13 of the eIDAS legislation. The contractual agreement stipulates further information on liability and any terms relating to a claim.

9.3 Confidentiality of Business information

9.3.1 Scope of Confidential information

iProov considers all data provided within the framework of the trust service, and definitions as agreed within the relevant contracts as confidential. All information that has become known whilst providing services and that is not intended for publication is confidential.

9.3.2 Information not within the scope of confidential information

Information is deemed Confidential Information if it is not considered, annotated, or otherwise designated as “public information”.

9.3.3 Responsibility to protect the confidentiality of information

iProov and all participants that are described within iProov's Trust Service Practice Statement have a responsibility to ensure that they protect confidential information.

9.4 Privacy of personal data

Within the scope of this TSPS, iProov does not operate as a Controller of personal data and instead functions as a processor of data provided by the controller. An iProov biometric authentication service (iProov Technology Service) is generally made available to users by a Third-Party Provider, such as a business, charity, or governmental service etc. in their capacity as controller of the data and process.

The third party provider is the controller (for the purposes of data protection laws) of the user's personal data that is processed by iProov Technology Services, while iProov acts as a processor of that data; the Controller remains responsible for the data, and is contractually obliged for the provision of controller processes to ensure the personal data is processed in compliance with the applicable law and legislation. As a processor, iProov is generally not permitted to intervene in the organisation of the end user's rights.

iProov has a data protection officer and has an EU representative.

iProov ensures that it has the relevant contracts (including DPAs and SCCs) in place with its sub-processors and suppliers, whilst complying with the requirements of GDPR, UK GDPR and DPA 2018.

iProov sub-processors must also be certified to an appropriate information security standard such as ISO 27001, SOC 2 etc and must be able to demonstrate adherence to these standards, and applicable policies and practices via initial and continued supplier review.

iProov does not hold any other identifiers other than those supplied by the controller when requesting iProov to process an end user image. On completion of the transaction the image is retained or deleted inline with the client requirements.

Where applicable, and where iProov has assessed a relevant DPIA needs to be in place, iProov has created and maintained the relevant DPIA with its Controller partner / customer to ensure that the data protection requirements have been met, to assess security requirements and to ensure that necessary controls are in place to protect data.

iProov has implemented several key security and privacy policies, controls, and measures to adhere to and to meet the requirements of the GDPR / Data Protection Act 2018 and other applicable laws. These measures include regular security tests, independent assessment, and certification to relevant international information security standards. iProov is certified to the ISO 27001 standard. iProov has all the relevant documentation in place, to address how it complies with the data protection laws.

9.4.1 Privacy plan

iProov's privacy policy can be accessed via iProov's website. For further information refer to iProov's Data management plan.

9.4.2 Information treated as private

Please refer to section 9.4.1.

9.4.3 Information not deemed as private

Please refer to section 9.4.1.

9.4.4 Responsibility to protect private information

iProov protects personal information by implementing strict security measures, controls, policies, processes and procedures. iProov also has a DPO who is tasked to ensure that the company's data that it derives from its customers, staff, providers and any other individual's, has appropriate data protection control measures in place such as: policies, practices, data handling, contracts and so forth all comply with the applicable data protection laws and regulations.

9.4.5 Notice and consent to use private information

Please refer to iProov's privacy policy that can be accessed via iProov's website.

9.4.6 Disclosure pursuant to judicial or administrative process

iProov is required to fulfil the requirements to supply data for purposes as required by applicable law and judicial process inline with the legal administrative procedures. iProov uses suitable safeguards including legal instruments to assess whether a request is lawful and from a prescribed authority, and where it is not will not disclose data.

9.4.7 Other information disclosure circumstances

Where iProov is requested by a customer to disclose information, iProov assesses the disclosure on a case by case basis and only discloses data if it does not prejudice iProov, its customers or the rights of a data subject and there is a substantiated reason for disclosure.

9.5 Intellectual property rights

iProov owns its service/product confidential information and all related documentation. Information regarding conditions pertaining to intellectual property rights can be found in the associated terms and conditions within iProov's contracts.

9.6 Representations and Warranties

9.6.1 Trust service provider representations and warranties

iProov identifies and meets the legal and contractual obligations of all external organisations supporting iProov services, which includes the applicable policies and practices. As such, iProov provides its services consistent to the requirements and procedures as defined in this TSPS and its service-based policies and procedures.
iProov publishes its practice statements, relevant documentation as necessary, terms and conditions for customers, subscribers and relying parties. iProov guarantees its availability within the public domain, in order to demonstrate conformance with the trust service policy.

iProov makes its services accessible to all relying parties whose activities fall within its operations, and agree to comply with its obligations as set forth in iProov's Terms and Conditions.

iProov informs relying parties of its terms and conditions before entering a contractual relationship. iProov provides its services to those which are consistent with the requirements and the procedures as described in this TSPS and policies. iProov remains responsible for its conformance with its procedures defined in this TSPS. iProov complies with the eIDAS regulation and related legal obligations as defined in this TSPS.

iProov partners are required to accept terms and conditions upon using iProov services, which includes iPortal.

Subjects/end-users are required to comply with iProov's partner's terms and conditions and as such, iProov ensures that it has its own Terms and Conditions with its Partners.

Subject/end-users who interact with iProov's website are subject to iProov's website terms and conditions.

iProov Terms and conditions are made available in a durable means of communication and shall be available in English. Terms and Conditions will be transmitted electronically. In the form of terms and conditions, iProov meets its claims for subscribers and guarantees their availability and access.

iProov maintains confidentiality of the information that has come to iProov's knowledge through providing its service, which is not subject to publication.

iProov will without undue delay, within 24 hours of becoming aware of an event, inform the supervisory body, the Trust Service Provider and applicable bodies of any breach of security, loss of integrity or significant impact on its service. Similarly, iProov will, without any undue delay and within 72 hours of discovery, notify the ICO of a data breach that impacts the rights and freedoms of the natural person(s). iProov will also ensure that the natural person has been informed without undue delay.

iProov preserves all the documentation, records and logs that relate to its biometric verification services and the trust services inline with contractual and legal requirements.

iProov ensures conformity assessment in accordance with the requirements and present the conclusion of conformity assessment to the Trust Service Provider to ensure the continual status of Trust Service within the Trusted Service List. iProov has the financial stability and resources that are required to conform with the requirements of this TSPS.

iProov warrants that (a) the iProov Services, when used in accordance with iProov's instructions, performs the functions set out in Schedule 1 and will meet their technical specifications as documented by iProov, and (b) it will use its reasonable endeavours to provide Services in accordance with the applicable requirements of Schedule 2 (Service Availability & Support). In the event of any failure to meet such requirements, iProov's liability and the Client's remedy for that failure shall be limited to iProov using its reasonable endeavours to comply with the relevant requirements in its subsequent delivery of the relevant Services.

Additionally, where applicable, iProov's terms and conditions shall specify for each trust service policy supported by iProov: whether iProov's service has been assured conformant with the trust service policy, and if so the conformity scheme and iProov's contact information.

Subscribers and relying parties shall be informed of precise terms and conditions, including the aforementioned items in this section prior to entering into a contractual relationship.

Terms and conditions shall be available in a readily understandable language.

iProov Trust Service Practices aim to operate in a non-discriminatory manner to assure all users, especially those with disabilities, have equal access to its services.

If the subject is a person, and not the same as the subscriber, the subject shall be informed of their obligations.

9.6.2 RA Representations and Warranties

RA operation is the duty of the TSP. In order to comply with the eIDAS Regulation as well as to comply with iProov policies applicable with operation on the modules described within this TSPS, the TSPs RA shall:

- provide its services consistent with the contractual requirements, this TSPS and GPA and/or LA service based policies and practice statements as well as with the relevant parts of the eIDAS Regulation.
- provide its employees necessary training to enforce the iProov security policy relevant for the modular services GPA and/or LA and for appropriate supply of high-security relevant service.
- Without undue delay after becoming aware of a breach or loss of integrity that impacts iProov, must inform/notify iProov.

9.6.3 Subscriber Representations Warranties

Subscribers in the sense of the following are entities subscribing for Trust Services with a TSP incorporating one or more of the service modules GPS/LA as described within this TSPS.
The subscriber shall:

- Understand and enforce the requirements provided by the TSP including the iProov GPA and/or LA related ones and the respective service - based policies/practice statements, and
- Supply true and adequate information, including within an event of change in the data submitted.

9.6.4 Relying Party Representation and Warranties

Relying parties in the sense of the following are entities relying on the results of the Trust Services operated by a TSP incorporating one or more of the service modules GPS/LA as described within this TSPS.

A relying party shall:

- Understand the risks and liabilities that relate to the contract and services provided.
- Implement the appropriate information security measures, including cryptography.

9.6.5 Representation and warranties of other participants

This is specified in the relevant contracts.

9.7 Disclaimers of warranties

The preceding section 9.1 is iProov's only warranty concerning the services and any deliverables and is made expressly in lieu of all other warranties and representations, express or implied, including any implied warranties of fitness for a particular purpose, merchantability or otherwise, or otherwise providing any condition regarding the services.

9.8 Limitations of liability

No limitations of liability apply other than those mentioned in section 9.2 or contractually specified.

9.9 Indemnities

Indemnities are regulated within the service-based terms and conditions.

9.10 Term and termination

9.10.1 Term

TSPS Version.2.3 is effective 10th September 2023 and published by iProov on their webpage into the public domain and remains current until a new version overrides the published version.

9.10.2 Termination

Termination in this sense refers to termination of the services provided through one of iProov's modules GPA/LA as described within this TSPS. Service termination directly requires termination of the Agreements between iProov and the TSP.

Either party may terminate the Agreement for convenience upon 90 days written notice in the event no Order Form is in effect. In addition, either party may terminate the Agreement, or the applicable Order Form, if the other party breaches any material term or condition of this Agreement and fails to cure such breach within 30 days after receipt of written notice of the same. In addition, if iProov's cost of providing the Services (e.g., insurance costs) materially increases, iProov may terminate this Agreement, or just the affected Order Form(s), on 30 days' notice to Client. On termination of this Agreement or the applicable Order Form, all fees and other sums invoiced by iProov to Client shall become immediately payable.
No Liability for Termination. Neither party will be liable to the other for any termination or expiration of this Agreement in accordance with its terms.

Effect of Termination; Survival. Termination shall not relieve either party of any obligation accrued prior to the date of termination. The following Sections will survive any expiration or termination of the Agreement: Order Form (excluding Term):

Unless expressly stated otherwise in the Agreement, upon termination of the Agreement, iProov shall, and shall procure that each processor engaged by iProov to process Personal Data shall, cease as soon as is reasonably practicable to use the Personal Data and delete the Personal Data unless required or entitled to retain a copy in accordance with any law of the UK, any European Union country or the USA or permitted to retain or continue processing the Personal Data under any provision of this PoC Agreement, unless required to do so by any Data Protection Law.
On expiry or termination of this PoC Agreement (however arising) this Data Protection Schedule shall survive and continue in full force and effect.

9.10.3 Effect of termination and survival

Communication of the conditions is communicated by iProov via its website.

At the very least, all responsibilities relating to the protection of personal and sensitive information, as well as the preservation of repository public information, iProov archives for a set amount of time, and logs, will survive termination. Even if this iProov and/or service-based Practice Statements expire, all Subscriber agreements continue in effect until the certificate is withdrawn or expires.

9.11 Individual notices and communications with Participants

In addition to other means of customer-specific communication as agreed within iProov contracts, iProov notices can also be found on its website: www.iproov.com, where communications are updated.

When changes are made in the Practice Statement that potentially affect service acceptance, iProov notifies and communicates with subscribers and relying parties with due notice.

Any planned changes to the TSPS will be examined by iProov's Compliance team and reviewed by iProov's CTO before notifying subscribers and relying parties of the change through iProov's website prior to the changes becoming effective.

9.12 Amendments

9.12.1 Procedure for amendments

Amendments will follow iProov contract amendment process and approval procedures.

9.12.2 Notification Mechanism and period

Notifications complies with the customer contractual agreements and iProov's website.

9.12.3 Circumstances under which OID must be changed

Not applicable.

9.13 Dispute Resolution Provisions

In the case of any dispute, including disputes received from any relying parties or regarding service provisioning, negotiations are used to resolve all disagreements between the parties. Should the parties be unable to reach an amicable resolution, the dispute will be resolved in a court of the iProov location.

The other party will be informed of any claim/ complaint no later than 30 days following the detection of the basis of the claim, unless otherwise provided by law.

The Subscriber or any other party can submit their claim or complaint to the following email: Compliance@iproov.com.

9.14 Governing law

iProov Ltd operates in the UK, under the governing laws of England and Wales. All updated versions will be made publicly available, for example, iProov's latest website terms and conditions will be published on iProov's website with version control.

9.15 Compliance with applicable laws & standards

iProov provides genuine presence assurance and identity verification services and ensures compliance with the legal requirements that derive from the applicable laws that protect records from loss, destruction, modification and falsification, and the requirements of the following:

- eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market and repealing Directive 1999/93/EC [1]
- Electronic Identification and Trust Service for Electronic Transactions Act [13]
- Personal Data Protection Act [7]
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) effective from 25.05.2018 [11]
- UK GDPR

Related European Standards:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 - 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
- GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

iProov also aligns with the following standards:

- ISO/IEC 27001:2013 Information Security Management System (ISMS)

- ISO/IEC 27701:2019 Extension to Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (PIMS)

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

For damages, losses, and expenses due to that party's actions, iProov may seek indemnity and attorneys' costs from that party. The failure of iProov to enforce a provision of this iProov does not forfeit iProov's right to enforce that provision or any other provision of this iProov in the future. Waivers must be provided in written format and signed by iProov in order to be effective.

9.16.5 Force Majeure

Neither party will be liable for any failure or delay in its performance under this Agreement due to any cause beyond its reasonable control, including act of war, acts of God, pandemic, epidemic, earthquake, flood, embargo, riot, sabotage, labour shortage or dispute, governmental act or failure of the Internet, provided that such cause is not in the reasonable knowledge of the parties at the time of entering into this Agreement and the delayed party: (a) gives the other party prompt notice of such cause, and (b) uses its reasonable commercial efforts to correct promptly such failure or delay in performance.

9.17 Other Provisions

Any provision within this document that is declared invalid or unenforceable will be outside operation. This does not affect the applicability of the remaining provisions in this TSPS.

10. References

(1) eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market and repealing Directive 1999/93/EC

(2) ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

(3) ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

(4) ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates

(5) Electronic Identification and Trust Service for Electronic Transactions Act, RT I, 25.10.2016, 1

(6) ISO/IEC 27001: 2013 Information technology - Security techniques -Information security management systems – Requirements

(7) General Data Protection Regulation

(8) United Kingdom General Data Protection Regulation, Data Protection act 2018

(9) ISO/IEC 30107-3: 2023. Biometric Presentation Attack Detection

(10) ISO/IEC 19989-3: 2020 Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection