iProov GPA
LOA Mapping for eID

for the following processes:

Module 1 - Genuine Presence Assurance (GPA)

Version: 1.6
Enforcement date: 10 September 2023

ABOUT

This document highlights the characteristics of the identification verification services provided by iProov inline with the requirements of the eIDAS level of Assurance - High. The definition of which is outlined in Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of the eIDAS Regulation [eIDAS]. This document refers to iProov's GPA (Genuine Presence Assurance) service.

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 All previously authorised versions of the Trust Service Practice Statement shall be rescinded with immediate effect and archived for audit trails and change trail.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	04/2022	Initial Draft	NB	--
0.2	05/2022	Review and comments	TUV	
1.0	05/2022	Comments and changes update	NB	DF
1.2	02/23	Review	NB	DF
1.3	08/23	Review, minor changes	NB	DF
1.4	08/23	Review	TUV	
1.5	09/23	Minor changes	NB	DF
1.6	09/23	Minor changes	PB	DF

Contents

1. Introduction

iProov's GPA remote biometric identity verification service meets the requirements of the eIDAS Level of Assurance High, in order to serve eIDAS compliant eID schemes to be employed by the scheme operator in the form of a module. This document outlines how iProov meets the requirements as depicted in the Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of the eIDAS Regulation [eIDAS].

1.1 About iProov

iProov is a biometric identity verification service provider that uses its own proprietary technology to verify the identity (Matching) and liveness of an individual enrolling onto or using a service that needs a positive identification to be made against a recognised identity document such as passport or national identity card and a verification that the person enrolling is a live person and not an attacker.

1.1.1 iProov GPA product

iProov Genuine Presence Assurance technology provides effortless and highly secure remote identity assurance to support automated digital onboarding. iProov verifies that an online customer is the right person using face matching technology, a real person using liveness detection, and is authenticating right now using patented Flashmark technology to create a one-time face biometric.

The solution delivers market leading biometric authentication and anti-spoofing to detect and protect against potential risks such as:

• highly scalable digital injection attacks (replayed or synthetic imagery that bypasses the device camera or is
injected into the data stream)

• presentation attacks (physical or digital artefacts presented to the device camera)

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.

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), 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
IA 2015/1502

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
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.

1.1.2 iProov as SaaS

iProov is a SaaS service provider offering its customers with both single tenant and multi-tenant environments to its customers hosted by a public cloud service provider. For EU customers, iProov uses Google Cloud Provider.

1.1.3 iProov's SDKs

iProov Biometrics Android SDK enables iProov customers and partners to integrate iProov into the relying party's Android application. iProov also has an iOS Biometrics SDK, Xamarin bindings and Web Biometrics SDK.The iProov Biometrics Android SDK is provided in AAR format (Android Library Project) as a Maven dependency.
The general requirements are as follows:

- Android Studio
- API Level 21 (Android 5 Lollipop) and above
- Compilation target, build tools and Android compatibility libraries must be 29+
- AndroidX
- Contents

API credentials can be obtained by registering on the iProov's Portal.

1.1.4 iProov Management Portal

Iproov offers its customers a management portal, iPortal.iPortal provides its customers with the depth of visibility and control that is obtained from having developed its own in-house technology. Features such as: reporting, user administration, provisioning, and integration are all accessible 24/7. Products and solutions are fully supported, enhanced and upgraded without additional time, cost or resources. The following key features are highlighted below:

iPortal: Reporting and Performance Data
iPortal provides its customers access to data on: availability, performance, and capacity. The reports provide:

- Utilisation statistics and performance data
- Business outcomes and success rates
- Breakdown of error reasons

iProov Resources and Documentation
We ensure that our customers have 24/7 access to all of the resources and documentation that is required for a successful implementation.

1.1.5 Science and innovation

iProov's Science and Innovation team use cutting edge academic research to solve real problems. This includes:

- Advanced Machine Learning
- Behavioural Science
- Optics
- Computer Vision
- Cryptography

External academic researchers are regularly involved in assessments and enhancements of iProov's systems. This includes: Supporting the development of innovative technologies, using the latest in AI and machine learning, Combined with a team of researchers and data scientists, who deliver continual innovation programs, such as :

- Delivering enhancements to respond to new attack methodologies
- Creating anti-spoof techniques for new (and as yet unknown) delivery mechanisms
- Identifying, testing and enhancing biometric security

1.1.6 Flashmark technology

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 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.

1.1.7 Android Support

In accordance with our commitment to security best practice, iProov promotes TLS 1.2 as the standard for client-server encryption.

1.1.8 iOS Support

iOS 5's TLS implementation has been upgraded to support TLS protocol version 1.2.

1.1.9 Web/Kiosk Support

iProov’s Kiosk enables companies to provide robust Identification verification on kiosks. This is accessible and inclusive, by enabling access to services for citizens without access to a smartphone. Kiosk can be adaptable, through mobile use or fixed terminals in a semi-supervised or supervised environment. End users will stand in front of the kiosk screen, whilst their identity is verified within 30 seconds.

iProov's Web SDK makes use of the following technologies:

WebGL
WebSockets
WebAssembly
WebComponents

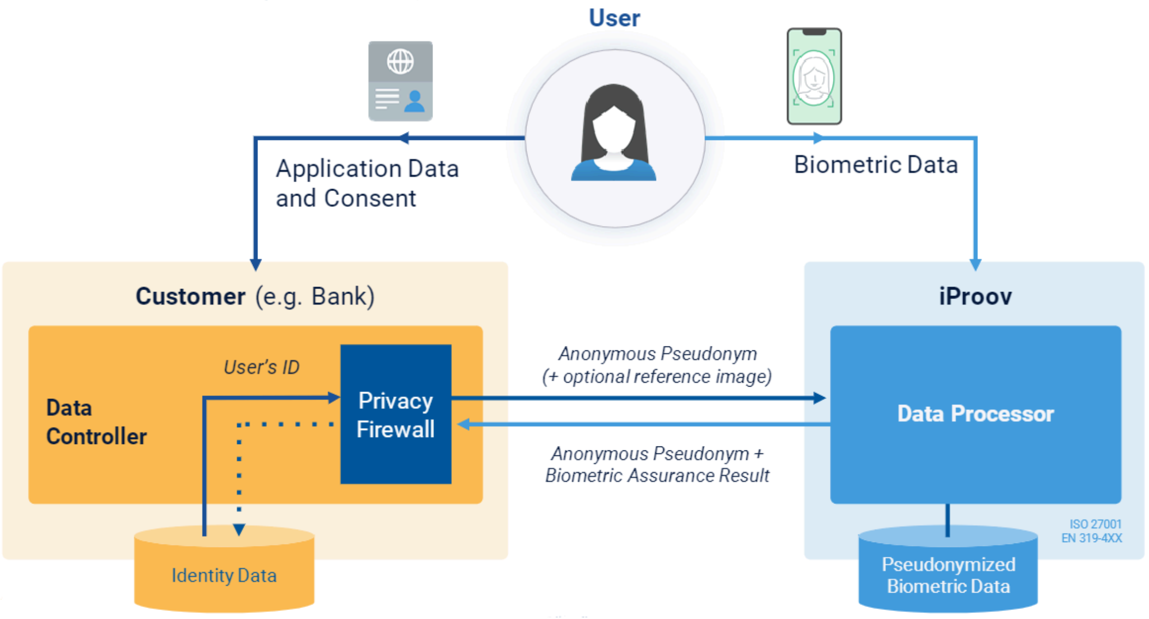
iProov Biometrics Web SDK requires access to a front-facing camera, WebGL, WebAssembly and the ability to enter full screen. A network connection is required that allows WebSockets. Provided there's a suitable webcam available, most modern desktop browsers fall within these criteria.

iProov Biometrics Web SDK requires access to a front-facing camera, WebGL, WebAssembly and the ability to enter full screen. A network connection is required that allows WebSockets. Provided there's a suitable webcam available, most modern desktop browsers fall within these criteria.

1.1.10 Data Processing

iProov uses a privacy firewall and strong encryption techniques to protect and safeguard the users confidentiality.

Communications from the SDK to the iProov SaaS cloud passes through an edge firewall, through other mechanisms before reaching the web server that authenticates the connection and cryptographic signing of the access token. This authentication process is made via a call to the Database that is storing a copy of the token previously issued to the customer in advance of the session.


User
Application Data and Consent
Biometric Data
Customer (e.g. Bank)
Data Controller
User's ID
Privacy Firewall
Identity Data
Anonymous Pseudonym (+ optional reference image)
Anonymous Pseudonym + Biometric Assurance Result
iProov
Data Processor
ISO 27001
EN 319-4XX
Pseudonymized Biometric Data

Data is encrypted in transit, and the unique identification that is produced by the client is pseudonymised. The end-user's identity is not revealed or identifiable to iProov. The end customer controls this pseudonym, and while iProov knows who the end customer is, it is unable to identify the data subject.

1.2 Typical iProov Flow

When iProov are required to participate in a specific use case involving GPA 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) 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.

1.3 Scope of Assessment

This eIDAS electronic identification self-assessment is scoped to tiProov’s Genuine Presence Assurance (GPA) service.

1.4 Definitions

Lexical item	Definition
Auditor	Person who assesses conformity to requirements as specified in given requirements documents
Applicant	Someone who tries to authenticate/ has yet to be proven to be the legitimate natural or legal person.
Authentication factor	Factor(s) that are confirmed as being bound to a person.This can be: “Possession based authentication factor, knowledge-based authentication factor or inherent authentication factor.
Authoritative source	Any source irrespective of its form that can be relied upon to provide accurate data, information/ evidence that can be used to prove identity.
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
Dynamic authentication	Electronic process using cryptography/ other techniques to provide a means of creating an on-demand, electronic proof that the subject is in control/possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity.
End User	Subject or subscriber
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
Information security management system	A set of processes and procedures designed to acceptable levels of risk related to information security.
Partner	: Associated service provider working alongside and engaging iProov technology. An iProov partner can include an integrator
Qualified Trust Service Provider	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)	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	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	The legitimate natural or legal person that is, or to be, represented by the electronic identification means.
Subscriber	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	An entity which provides one or more trust services

1.4.1 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. Technical Specifications

2.1 Enrolment

2.1.1 Application and Registration

Low

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

iProov's customers communicate terms and conditions to the applicant, through their user interface. iProov has terms and conditions in place with its customers. Where DPAs are in place with iProov customers, the customer acts as a Controller of personal data. DPAs are in place with which both parties are subject to, and must adhere to the applicable data protection laws. Where iProov acts as a processor, the Controller has privacy notices and terms of use in place with the applicant/ end user. Where iProov is a Controller, iProov has its own privacy policies.

iProov's privacy policy can be found here: https://www.iproov.com/privacy-policy

iProov's terms are also available and accessible within its online repository, which can be found here: https://www.iproov.com/compliance-repository

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

iProov's customers ensure that the applicant is aware of the recommended security precautions that relate to the electronic identification means.

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

iProov verifies the image against the verified image provided by the partnering company. Following the enrolment to the service, GCP verifies the identity (matching) against a recognised identity document such as a passport or national identity card, whilst verifying that the person enrolling is a live person and not an attacker. GPA offers powerful deep learning AI methods and additional checks for its proofing and verification capabilities."

Substantial

Same as level low

High

Same as level low.

2.1.2 Identity Proofing and Verification (Natural Person)

Low

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

iProov's GPA process does not handle ID documents and as such this section is not applicable.

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

iProov's GPA process does not handle ID documents and as such this section is not applicable.

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

Although iProov does not handle the ID documentation, the documentation required for "matching" is a recognised identity document, such as a passport or national identity card, which is produced during enrolment.

Substantial

1. "The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence."

The identity document is known to exist and relates to a real person. Steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence. iProov authenticates the individual using their face biometric against an authorised photo ID document. Genuine Presence Technology is used to determine whether the individual is a real person, the right person and one who is authenticating right now. The photo ID source are government-approved documents such as passports, driving licence, national ID cards or against a centralised database. Such measures ensure that the person in real time is matched against the enrolled document that the individual is in possession of at the time.

"or

2. *“An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;"*

iProov’s GPA process does not handle ID documents and as such this section is not applicable.

"or

3. *“Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council(1) or by an equivalent body;"*

iProov’s GPA process does not handle ID documents and as such this section is not applicable.

or

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

iProov's GPA process does not handle ID documents and as such this section is not applicable.

High

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

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

"(a)Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;
and
the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;"

iProov customers ensure that the identification used for evidence is recognised by the Member State in which the application for the electronic identity means is being made. The applicant is identified as the claimed identity using iProov's flashmark technology that ensures the liveness and genuine presence of remote users. Facial authentication uses pattern matching through a number of metrics to confirm that a selfie face scan done by a live human on a mobile device or computer matches a photograph in a trusted identity document. The biometric evidence provided undergoes a series of checks to validate that the person is the right person and not an imposter. Examples of such attacks may include, but are not limited to imposter attacks, use of artifacts such as photos, videos, masks etc, or digitally injected media. The use of GPA ensures that the person is the right person, a real person and a person that is authenticating in real time.

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

This section is not in scope as iProov meets the requirements of level substantial plus 1.A.

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

This section is not in scope as iProov meets the requirements of level substantial plus 1.A.

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

This section is not in scope as iProov meets the requirements of level substantial plus 1.A.

2.1.3 Identity Proofing and Verification (Legal Person)

Low

> “1.The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made.”

This section is not applicable as under eIDAS legal persons are organisations such as: companies, public authorities, private clubs and so forth who are not typically in possession of a photo ID document that iProov could make use of for GPA.

> “2. The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source, where the inclusion of a legal person in the authoritative source is voluntary and is regulated by an arrangement between the legal person and the authoritative source.”

This section is not applicable as under eIDAS legal persons are organisations such as: companies, public authorities, private clubs and so forth who are not typically in possession of a photo ID document that iProov could make use of for GPA.

Substantial

> “3. The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.
>
> Level low, plus one of the alternatives listed in points 1 to 3 has to be met:”

This section is not applicable as under eIDAS legal persons are organisations such as: companies, public authorities, private clubs and so forth who are not typically in possession of a photo ID document that iProov could make use of for GPA.

> "1.The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable) its registration number
>
> and the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source, where the inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector
>
> and steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;"

This section is not applicable as under eIDAS legal persons are organisations such as: companies, public authorities, private clubs and so forth who are not typically in possession of a photo ID document that iProov could make use of for GPA.

> "or
> 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment

> body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body."

This section is not applicable as under eIDAS legal persons are organisations such as: companies, public authorities, private clubs and so forth who are not typically in possession of a photo ID document that iProov could make use of for GPA.

High

> Level substantial, plus one of the alternatives listed in points 1 to 3 has to be met:
>
> "1.The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context
> and
> the evidence is checked to determine that it is valid according to an authoritative source;"

This section is not applicable as under eIDAS legal persons are organisations such as: companies, public authorities, private clubs and so forth who are not typically in possession of a photo ID document that iProov could make use of for GPA.

> "or
> 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body
> and
> steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid."

This section is not applicable as under eIDAS legal persons are organisations such as: companies, public authorities, private clubs and so forth who are not typically in possession of a photo ID document that iProov could make use of for GPA.

2.1.4 Binding Between the Electronic Identification Means of Natural and Legal Persons

> "Where applicable, for binding between the electronic identification means of a natural person and the electronic identification means of a legal person ('binding') the following conditions apply:
> (1) It shall be possible to suspend and/or revoke a binding. The life-cycle of a binding (e.g. activation, suspension, renewal, revocation) shall be administered according to nationally recognised procedures."

iProov's GPA does not conduct binding between the electronic identification means of a natural person and the electronic identification means of a legal person, and as such 2.1.4 is not applicable.

> "(2) The natural person whose electronic identification means is bound to the electronic identification means of the legal person may delegate the exercise of the binding to another natural person on the basis of nationally recognised procedures. However, the delegating natural person shall remain accountable."

iProov's GPA does not conduct binding between the electronic identification means of a natural person and the electronic identification means of a legal person, and as such 2.1.4 is not applicable.

Low

> (3) Binding shall be done in the following manner:
> 1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above.
> 2. The binding has been established on the basis of nationally recognised procedures.
> 3. The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.

iProov's GPA does not conduct binding between the electronic identification means of a natural person and the electronic identification means of a legal person, and as such 2.1.4 is not applicable.

Substantial

> "Point 3 of level low, plus:

> 1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high."
> 2. The binding has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source.
> 3. The binding has been verified on the basis of information from an authoritative source.

iProov's GPA does not conduct binding between the electronic identification means of a natural person and the electronic identification means of a legal person, and as such 2.1.4 is not applicable.

High

> "Point 3 of level low and point 2 of level substantial, plus:
> 1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high."
> 2. The binding has been verified on the basis of a unique identifier representing the legal person used in the national context; and on the basis of information uniquely representing the natural person from an authoritative source.

iProov's GPA does not conduct binding between the electronic identification means of a natural person and the electronic identification means of a legal person, and as such 2.1.4 is not applicable.

2.2 Electronic Identification Means Management

2.2.1 Electronic Identification Means Characteristics and Design

Low

> "1. The electronic identification means utilises at least one authentication factor."

The eID means are operated by an eID scheme provider, which is not part of iProov's services, however, iProov may support the eID scheme provider through iProov's GPA service for user authentication against the eID means. iProov's GPA service is used as an authentication factor.

> "2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs."

The eID means are operated by an eID scheme provider, which is not part of iProov's services, however, iProov may support the eID scheme provider through iProov's GPA service for user authentication against the eID means. iProov's GPA service is used as an authentication factor where it is designed so that it is used only under the control or possession of the person to whom it belongs to. When identifying and enrolling an end user through GPA, a high level of confidence is provided within the biometric image dataset, and therefore the biometric image dataset that is being enrolled is ensured to be real and trustworthy. GPA offers the highest levels of assurance for biometrics.

Substantial

> 1.The electronic identification means utilises at least two authentication factors from different categories.

The eID means are operated by an eID scheme provider, which is not part of iProov's services, however, iProov may support the eID scheme provider through iProov's GPA service for user authentication against the eID means. iProov's GPA service is used as an authentication factor.

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

The eID means are operated by an eID scheme provider, which is not part of iProov's services, however, iProov may support the eID scheme provider through iProov's GPA service for user authentication against the eID means. iProov's GPA service is used as an authentication factor.

High

> "Level substantial, plus:
> 1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential"

The eID means are operated by an eID scheme provider, which is not part of iProov's services, however, iProov may support the eID scheme provider through iProov's GPA service for user authentication against the eID means. iProov's GPA service is used as an authentication factor. Through iProov's Genuine Presence Assurance, this protects against attackers with high attack potential.

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

The eID means are operated by an eID scheme provider, which is not part of iProov's services, however, iProov may support the eID scheme provider through iProov's GPA service for user authentication against the eID means. iProov's GPA service is used as an authentication factor. Through iProov's Genuine Presence Assurance is designed so that it can be reliably protected against others using it. iProov's platform is used to provide its customers and end users with increased security and convenience. When identifying and enrolling an end user through GPA, a high level of confidence is provided within the biometric image dataset, and therefore the biometric image dataset that is being enrolled is ensured to be real and trustworthy. GPA offers the highest levels of assurance for biometrics.

2.2.2 Issuance, Delivery, and Activation

Low

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

This section does not apply to iProov's GPA service as GPA does not support the security of the eID's issuance and delivery.

Substantial

"After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs."

iProov's GPA service is used after issuance of the electronic identification means as a way in which it can be assumed that it is delivered only into the possession of the person to whom it belongs. iProov GPA uses powerful deep learning AI methods to combine camera imagery with both contextual and device sensor data generated during the identification process. This creates a complex and rich source of biometric analysis. iProov then applies a number of 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 sessions injected into a device's sensors. iProov's paintented Flashmark technology is used to ensure that the user is Genuine and present at the point of challenge.

The information 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 integrator 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 integrator or customer as previously described.

High

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

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

When identifying and enrolling an end user through GPA, a high level of confidence is provided within the biometric image dataset, and therefore the biometric image dataset 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 both contextual and device sensor data generated during the identification process. This creates a complex and rich source of biometric analysis. iProov then applies a number of 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 sessions injected into a device's sensors. iProov's paintented Flashmark technology is used to ensure that the user is Genuine and present at the point of challenge.

The information 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 integrator 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 integrator or customer as previously described.

2.2.3 Suspension, revocation, and reactivation

Low

> "1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner."

This section is not applicable to iProov as iProov's GPA service does not suspend or revoke an electronic identification means.

> "2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation."

This section is not applicable to iProov as iProov's GPA service does not suspend or revoke an electronic identification means.

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

This section is not applicable to iProov as iProov's GPA service does not suspend or revoke an electronic identification means.

Substantial

> "Same as level low".

This section is not applicable to iProov as iProov's GPA service does not suspend or revoke an electronic identification means.

High

> "Same as level low."

This section is not applicable to iProov as iProov's GPA service does not suspend or revoke an electronic identification means.

2.2.4 Renewal and Replacement

Low

> "Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level."

This section is not applicable to iProov's GPA service as iProov does not act as an eID scheme operator.

Substantial

> "Same as level low"

This section is not applicable to iProov's GPA service as iProov does not act as an eID scheme operator.

High

> "Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source."

This section is not applicable to iProov's GPA service as iProov does not act as an eID scheme operator.

2.3 Authentication

"This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls shall be understood to be commensurate to the risks at the given level."

2.3.1 Authentication Mechanism

Low

> "The following sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party."

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

In the context of iProov's customer's making use of GPA, a secure method of authentication is in place. iProov's GPA service that uses its own proprietary technology hosted in a public cloud to verify the identity (Matching) and liveness of an individual enrolling onto or using a service that needs a positive identification to be made against a recognised identity document such as passport or national identity card and a verification that the person enrolling is a live person and not an attacker. As such, the GPA service is used to verify that the person identified on the document is the same person attempting to authenticate.

> 2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.

In the context of GPA being used as the secure authentication method, iProov securely stores the obtained information (such as Imagery, biometric template, and where applicable IP address) to protect against loss and being compromised, including analysis offline. All data is encrypted in transit and at rest. iProov uses Google Key Management Service to create, store and rotate and issue keys for password, secret and workload protection. Keys are stored within Google's infrastructure and are AES256. Keys are rotated frequently. The SDK and edge layers are cryptographically controlled, passwords are encrypted throughout build and support, production databases are encrypted, VPN solutions are used. Iproov systems are audited against ISO 27001 principles and are subject to frequent external pentests to validate and continuously improve upon its information security.

> 3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.

In the context of GPA being used as a secure authentication method, an integral part of iProov Genuine Presence Assurance is the iProov Security Operation Centre (iSOC) which detects biometric threats and anomalies from a range of devices and platforms. It combines advanced technology, with appropriate processes and experts, to provide resilience against the most sophisticated attacks. iSOC provides a level of added value that secures and reassures our customers and their end users. iSOC helps identify novel or evolving attack methods and enables the creation of new defences if necessary to maintain the highest level of protection against known and unknown attack types. Rapidly detecting evolving threats ensures prompt recovery and response to support the security of the solution and the protection of the customer organisation and their users.

Substantial

"Level low, plus:

1.The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through dynamic authentication."

In the context of GPA being used as a secure authentication method, GPA is used as a means of reliable verification to validate that the person is who they claim to be. iProov's GPA service is to determine whether the right person, the real person, is present at the time of verification.

2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.

In the context of GPA being used as a secure authentication method, an integral part of iProov Genuine Presence Assurance is the iProov Security Operation Centre (iSOC) which detects biometric threats and anomalies from a range of devices and platforms. It combines advanced technology, with appropriate processes and experts, to provide resilience against the most sophisticated attacks. iSOC provides a level of added value that secures and reassures our customers and their end users. iSOC helps identify novel or evolving attack methods and enables the creation of new defences if necessary to maintain the highest level of protection against known and unknown attack types. Rapidly detecting evolving threats ensures prompt recovery and response to support the security of the solution and the protection of the customer organisation and their users.

As iProov's GPA service is to determine if a person is present at the time of verification checks need to be undertaken to ensure that the biometric image stream is provided by a live device and person (identifying a live person). This is the heart of Genuine Presence Assurance

In a Replay Attack, hackers or fraudsters try to attempt to mimic liveness via replay attacks of videos or computer-generated images. The iProov process looks for specific parameters and patterns that are often associated with these types of replay attacks.

High

> "Level substantial, plus:
> The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms."

In the context of GPA being used as a secure authentication method, iProov implements security controls for the verification so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation can be performed by an attacker with high attack potential to subvert the authentication mechanisms.

Once the biometric image exists within iProov's database, then GPA performs a matching function to an existing image stored in iProov's biometric templates database.

As additional security and integrity measures, a number of security processes are implemented to protect the biometric data and customer environments or services. These are measures to detect different types of attacks that could come from bad actors seeking to defeat the iProov SDK or customer environments or processes. Such measures include:

- Forgery Detection - where the process examines a series of parameters known to co-exist with these attack vectors to verify whether the photo or image stream has been tampered with.
- Replay Detection - which determines if a person is present at the time of verification checks are being conducted to ensure that the biometric image stream is provided by a live device and person (identifying a live person).

- In a Replay Attack - where hackers or fraudsters try to attempt to mimic liveness via replay attacks of videos or computer-generated images. The iProov process looks for specific parameters and patterns that are often associated with these types of replay attacks.

- Further Anomaly Detection - There are several genuine parameters that are associated with a live stream and living person and these are difficult to replicate. The iProov platform has numerous security measures in place to look at these parameters and is configured to detect anything that is different to normal characteristics and measurements.

- Risk Factor Analysis Engine - This iProov process looks at general and aggregated parameters associated with the data and security processes and flags anything as unusual and generates an alert based upon assumed or detected risks. These alerts are then investigated to determine if there is an anomaly with the data being processed or whether it is a new form of attack that has been detected. The investigations are manual and involve human oversight so that system errors cannot allow for onward processing of data that is assessed as high risk.

An integral part of iProov Genuine Presence Assurance is the iProov Security Operation Centre (iSOC) which detects biometric threats and anomalies from a range of devices and platforms. It combines advanced technology, with appropriate processes and experts, to provide resilience against the most sophisticated attacks. iSOC provides a level of added value that secures and reassures our customers and their end users. iSOC helps identify novel or evolving attack methods and enables the creation of new defences if necessary to maintain the highest level of protection against known and unknown attack types. Rapidly detecting evolving threats ensures prompt recovery and response to support the security of the solution and the protection of the customer organisation and their users.

2.4 Management and Organisation

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

2.4.1 General Provisions

Low

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

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

iProov complies with the requirements of DPA 2018, UK GDPR & GDPR and any other specific legislation that iProov must comply with as detailed in its customer contracts that are incumbent to iProov’s operation and delivery of service.

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

iProov has liability insurance with sufficient financial coverage.

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

iProov uses sub-processors, such as cloud providers for its hosting. It is contractually, organisationally and technically ensured that this cloud provider fulfils the relevant requirements to remain compliant with eIDAS CIR 2015/1502

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

Although iProov is not an eID scheme operator, and provides its service in the context of the eID scheme. To this extent, contractual provisions are in place to cater for controlled termination of iProov’s services. 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.

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

iProov conforms to its contractual and legal obligations.

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.
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.

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.

Substantial

Same as level low.

High

Same as level low.

2.4.2 Published Notices and User Information

Low

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

iProov’s published documents can be found within the following on-line repository:www.iproov.com/compliance-repository. iProov details its standards that it complies with, its general terms, privacy policy and TSPS.

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

iProov does not have direct contact with the end user, however, contracts are in place with iProov and its customers that cover the applicable terms and conditions of service. As such, this section does not directly apply to iProov or its GPA service.

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

This is embedded within the contracts between iProov and its customers. In the case of a data breach, iProov will notify the customer and comply with its requirements under the GDPR.

Substantial

Same as level low.

High

Same as level low.

2.4.3 Information Security Management

Low

> “There is an effective information security management system for the management and control of information security risks.”

iProov has an effective information security management system for the management and control of information security risks. iProov’s information security management system adheres to the ISO 27001 principles for the management and control of information security risks.

Substantial

"Level low, plus:

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

iProov complies with the requirements of the ISO 27001 standard, and also draws on practices within the risk management focused ISO 31000. Further information can be found in iProov's risk management methodology policy. iProov uses ISMS online to manage, store and update its Information Security Risks.

iProov operates as a SaaS service provider, where it's cloud providers have certification to information security standards such as SOC -2, ISO 27001 or similar.

High

Same as level substantial

2.4.4 Record-Keeping

Low

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

Storage, management and maintenance of records take into account the applicable legislation, and good practice in relation to the data protection and data retention. iProov does not hold records for any longer than considered necessary or required in its client contractual agreements.

Where an attempted fraud by a person verifying genuine presence is detected, the customer is informed of the attempt and a record of the attempt is kept so that should the customer require further investigation or evidence, it is available as needed. After an agreed period of time, inline with its contractual obligations, this data will be deleted.

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

iProov retains information as far as it is permitted by the applicable laws and protects the records for as long as required for the purpose of auditing and investigation of security breaches and retention, after which the records are securely destroyed.

Where an attempted fraud by a person verifying genuine presence is detected, the customer is informed of the attempt and a record of the attempt is kept so that should the customer require further investigation or evidence, it is available as needed. After an agreed period of time, inline with its contractual obligations, this data will be deleted.

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.

Substantial
Same as level low.

High
Same as level low.

2.4.5 Facilities and Staff

“The section represents the requirements with respect to facilities and staff and subcontractors, if applicable, who undertake duties covered by this Regulation. Compliance with each of the requirements shall be proportionate to the level of risk associated with the assurance level provided.”

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

Procedures are in place to ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills required to perform their roles and responsibilities.

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's Top Management team have 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. Trusted role training is in place.

Further information regarding iProov's training can be found in iProov's training policy.

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

iProov's availability requirements include that of staff and subcontractors to adequately meet the operational and resource requirements relevant to iProov's services in accordance to the requirements of the ISO 27001 and identified risks.

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

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 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:

Physical security perimeters
Physical entry controls
Securing Offices, rooms, and facilities
Protecting against external and environmental threats
Working in secure areas
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:

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.

Further information can be found in iProov's ISMS inline with the requirements of: A.11 Physical and Environmental security, A.12 Operations security and A.9 Access control of the ISO 27001 standard.

> “4. Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.”

Access control, cryptographic controls and physical and environmental security is covered as part of the controls of the following ISO 27001 standard: A.9 Access control, A.10 Cryptography, A.11 Physical and environmental security and A.12 Operations security. Relevant controls are also covered inline with the requirements of the ETSI standards (EN 319 - 411-1, EN 319 411-2, EN 319 401).

Iproov uses cloud hosted infrastructure for the provision of its identity services to its customers. Providers include Google Cloud Platform and Microsoft Azure. As hosted services, iProov staff do not have any physical access to the data centres providing the services to iProov. Microsoft and Google have policies and processes in place to limit access to their facilities and these are evidenced by their ISO27001 and SOC2 documents that are reviewed by iProov regularly. Where iProov needs to access services within the data centres that relate to the identification process they are accessed remotely via VPN.

Where personal, cryptographic or other sensitive information is accessed, only authorised iProov staff can do so. Trusted role staff are the only team members with access to cryptographic material and this is held in the GCP data centres via an iProov managed HSM. All access is logged and controlled via the VPN and via Google Authentication. Other team members who access sensitive data are restricted to specific system access based upon role and use Google Authentication and have specific access permissions associated with their unique account used for data access. Access is also monitored via logs that are analysed by iProov’s security team.

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

The iProov controlled office also referred to in this document as “secure area” is only accessible by iProov staff members,with key cards, any guests/ external parties who may be on premises for meetings are not granted access into the main office space as such meetings are conducted in a separate room outside of the controlled office space.

iProov staff are also required to book their space into the internal office, otherwise their passes will not work on the day.

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.

All floors have specific key cards to enable access based on where the individual works.

All visitors must identify themselves at the reception of the Wework building. This is then verified by an iProov member of staff who will meet the Visitor at the reception and will escort them into the shared premises or iProov meeting room. Visitors must be with their host throughout the time within the office and are restricted from any other floor(s) - their passes do not grant them any access to floors and therefore must be supervised.

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

Substantial
Same as level low.

High
Same as level low.

2.4.6 Technical Controls

Low

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

iProov has technical controls in place as highlighted in iProov's ISMS, which is inline with the requirements of the ISO 27001 standard. Such controls include: Cryptography, operations security, system acquisition, development and maintenance and information security aspects of business continuity management.

iProov has Risk management processes in place and has implemented risk management that identifies, assesses and takes appropriate steps to reduce risks to an acceptable level.

Following the CIA triad, iProov maintains, updates and prioritises its risks on a risk register that is available on ISMS online.

Regular risk assessments are in place to manage the potential and current risks posed to the security of the services. Risks are updated on a regular basis. Risk assessments are visited at least 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.

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

The electronic communication channels used to exchange personal or sensitive information between iProov and its customers or partners are protected against eavesdropping, manipulation and replay. THis is covered in iProov's ISMS under A.10 cryptography, A.13 Communication security of the ISO 27001 standard. All communications with commercial or technical platforms are encrypted.

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

The access control for accessing sensitive cryptographic material is covered by iProov's ISMS inline with the requirements of the ISO 27001 standard, which includes: A.9 Access control, A.10 cryptography and the requirements of the ETSI standards (EN 319 - 411-1, EN 319 411-2, EN 319 401).

Only a trusted role, that strictly requires access and who has the specific administration access within the technology team has granted access applicable to their roles and responsibilities to the platform environment. Any access to cryptographic material is restricted to VPN access only for administration and control. The VPN allows only specific access to authorised material based upon the role. Access is managed via Authentication, cloud specific authentication and permissions in the VPN. Cryptographic keys are stored in an iProov managed HSM and keys are generated, managed and destroyed via this. Where applications need access to secrets or cryptographic keys, access is granted via a Secrets manager. The secrets manager allows for keys and secrets to be obtained when code is executed. This means that no cryptographic material or secrets are hard coded or stored in plain text.

Roles are granted via iProovs access control procedures and changes to the environment are only made after successful completion of iProov's change control process.

Key management is managed via Google's Key Management Service,

and iProov reviews that the necessary change control and access control measures are in place and have been evaluated as part of GCP's external audits.

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

Procedures are in place to ensure that security is maintained over time and that iProov has the ability to respond to the changes inline with the risk levels, incidents and security breaches. Technical security controls are in place that include key protection & cryptographic controls. Computer security controls are in place where systems are hardened to minimise the risk of unauthorised access or attacks to the system. Multiple security controls are in place through 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.

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.

iProov evaluates its risks regularly, but no less than once a year.

iProov has both an incident response and information security team that handle and solve incidents adequately.

iProov has an incident management process and procedures are in place.

iProov conducts DR and BCP testing on a regular basis.

iProov is subject to regular external and internal information security audits that security is maintained over time.

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

iProov’s asset management procedures are covered within iProov’s ISMS, inline with the requirements of ISO 27001 standard controls A.8 Asset management and within the applicable controls of the ETSI standards (ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 401).

iProov does not allow personal data, sensitive or cryptographic data to be stored over transportable media such as USBs/ portable disks. Any personal data, sensitive or cryptographic data is stored securely within iProov’s cloud or with a sub processor who is contracted to supply services and store data associated with the service they are providing. If data is held with a sub processor, iProov has the contractual right to request secure deletion if iProov is not not directly controlling this data. If iProov does control this data, then the data is securely deleted via overwriting the data several times so the original data is corrupted and unreadable. As iProov is a cloud based service provider, data cannot be crypto shredded and disks cannot be removed from the cloud data centres.

Sensitive and personal data are encrypted at rest and in transit with keys or certificates controlled by iProov or its contracted sub processors.

Substantial
"Same as level low, plus:
Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering."

iProov has a cryptography policy that can be accessed via ISMS online in general, the following applies:

All critical or sensitive data transferred outside of the organisation must be encrypted.

Laptop hard drives must be encrypted.

All remote access must take place via encrypted VPN services or by using a TLS encrypted connection.

Encryption of data in transit
Data classified as “Highly Confidential” must always be encrypted on the public internet and must be encrypted in transit wherever possible and practical on secure networks.
Data classified as “Confidential” must always be encrypted on the public internet and must be encrypted in transit wherever possible and practical on secure networks.

Encryption of data at rest
Data classified as “Highly Confidential” must be encrypted at rest.
Data classified as “Confidential” must be encrypted at rest.

Key management

Key management managed by Google GC is used to create, issue and destroy keys used for issuing electronic identification means.

Encryption keys are securely managed, in a central location via a highly controlled and secure Hardware Security Module (HSM). All information encrypted by the organisation can be decrypted if required.

The strength of encryption to be used is considered against the risks associated with the assets to be encrypted. As a guide, a minimum of 1024 bit encryption is used for any encryption involving electronic identification needs.

iProov uses a key management service that manages symmetric and asymmetric cryptographic keys for iProov’s production services that involve electronic identification. 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 that provide keys to manage services that provide electronic identification needs. Key management is maintained by Google KMS, with keys rotated at least annually and utilises available, ratified cryptographic standards as listed above.

Cryptographic keys are generated and stored securely in iProov’s cloud infrastructure. Cryptographic keys are stored and used in an end-to-end encrypted environment so that they cannot be exposed to anyone without access to the encrypted environment. They are transported and stored without jeopardising confidentiality and are not hardcoded into any software or system. iProov uses a secrets manager that allows for keys to be called and replaced by systems in real time at execution. This means that keys are called and deployed as needed and rotation is managed automatically. Keys are regularly backed up to ensure that no data is permanently lost as a result of lost, compromised or expired keys.

Secondary HSM's are used to backup sets of keys. Keys are generated in a HSM residing on the production platform enabling deployment locally. Private keys are generated, activated and deployed, at the time of use by personnel with elevated privileges that are granted under Change Control for the specific cryptographic activity they are undertaking.. Any generated keys cannot be tampered with as they are signed and tampering would invalidate the key.

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 be destroyed.

iProov reviews GCP's compliance and security measures on an ongoing basis.

High

Same as level substantial

2.4.7 Compliance and Audit

Low

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

iProov's compliance function conducts periodic internal audits, where the relevant functions are audited at least once a year.The schedule of iProov's internal audits can be found in iProov's internal audit plan.

Substantial

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

iProov is subject to both internal and external audits that are scoped to include all relevant parts to the supply of GPA to ensure companies with relevant policies. Internal audits are conducted inline with iProov's internal audit schedule. iProov is periodically assessed against its compliance with the requirements of ISO 27001 at least annually.

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 include 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

High

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

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. External auditors are independent from iProov and the assessed systems.

iProov is also audited by its Clients, who are regulated authorities.

iProov undergoes regular annual professional penetration tests, which is conducted at least annually.

High

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

Where a scheme is directly managed by a government body, iProov must present the conclusion of the conformity assessment to the TSP.

iProov undergoes periodical assessments against the requirements of the eIDAS regulation, which is audited by a conformity assessment body. Assessments include the eIDAS regulation, relevant legislation and applicable standards.

iProov is audited at least annually for its ISO 27001 certification.

iProov undergoes regular external penetration tests. External penetration tests are conducted at least annually.