Identity Proofing Service Provider

Practice Statement

Checkin.com ID Verification

-

Version 1

1st Effective date: 28.05.2025

Document Change History:

Date:	**Change description:**	**Version:**
13.05.2025	Document creation	v. 1
28.05.2025	Management review and approval	v. 1.1

–

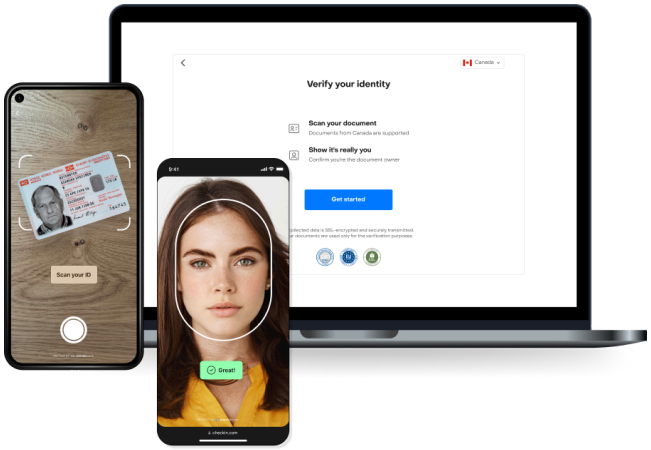
Content

1. Introduction **4**
1.1. Overview 4
1.2. Scope: Identity Proofing Service Policy (IPSP) 4
1.3. Identity Proofing process 5
1.4. Identity Proofing context 5
2. Policy administration **5**
2.1. Organization administering the document 5
2.2. Contact person 6
2.3. Time or frequency of publication 6
2.4. Terms and Conditions 6
3. Definition of Terms and Abbreviations **6**
3.1. Terms 6
3.2. Abbreviations 7
4. Risk Assessment **8**
5. Policies and Practices **8**
6. Internal Organisation **8**
7. Human Resource Security **8**
8. Asset Management **9**
9. Access Control **9**
10. Cryptographic Controls **9**
11. Physical and environmental security **9**
12. Operation Security **9**
13. Network Security **10**
14. Incident Management **10**
15. Business Continuity **10**
16. Termination **10**
17. Identity proofing service requirements **10**
17.1. Initiation 10
17.2. Attribute and evidence collection general requirements 10
17.3. Attribute collection for natural person 11
17.4. Attribute and evidence validation general requirements 11
17.5. Validation of physical identity document 12
17.6. Binding to applicant general requirements 12
17.7. Capture of face image of the applicant 12
17.8. Binding to applicant by automated face biometrics 13
17.9. Issuing of proof 13
17.10. Evidence of the identity proofing process 13
18. Identity proofing use cases **14**
18.1. Identity proofing of natural person 14
18.2. Remote identity proofing 14

1. Introduction

This document contains the Trusted Service Practice Statement (TSPS) of Checkin.com Group AB (Checkin) identity verification service covering the aspects of identity proofing. For Checkin.com this is also the IPSP Practice statement.

The Checkin.com ID Scan service scans identity (ID) documents (passports, driving licenses, residence cards, etc.), and ensures that the person carrying out the process is a natural person and the rightful owner of the document using biometrics and other security measures. The attributes collected uniquely identify the applicant as a natural person in the identity proofing context.



The purpose of this document is to serve as a base for compliance with eIDAS, the Regulation (EU) No 910/2014 & Regulation (EU) 2015/1502 of the European Parliament and ETSI standards ETSI TS 119 461 [1] and ETSI EN 319 401

1.1. Overview

Identity proofing is the process of verifying with the required degree of certainty that the identity of an applicant is correct. Checkin.com has developed a remote identification service for identity proofing of trust service subjects as well as onboarding and know-your customers (KYC) processes.

In particular, Checkin.com verifies the identity of natural persons amongst other methods in accordance with eIDAS, Article 24, paragraph 1 d) by using "other identification methods" which provide equivalent assurance in terms of reliability to physical presence. Conformance with eIDAS at assurance level "Substantial" allows certification service providers to use these services for identity verification in their processes.

1.2. Scope: Identity Proofing Service Policy (IPSP)

The present document (the "Identity Proofing Service Provider Practice Statement") describes the applied practices employed in delivering the service and in meeting the applicable requirements for identity proofing.

More specifically, the practices adopted for fulfilling the general policy requirements given in ETSI EN 319 401 and ETSI TS 119 461 V2.1.1 (2025-02) describing the policy and security requirements adopted for implementing an "Identity Proofing Service Component" supporting identity proofing in European and other regulatory framework. This standard has been developed taking into account the following:

- ETSI EN 319 401 v2.3.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

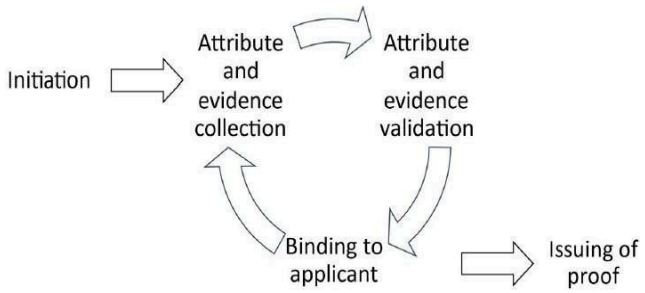
- ETSI TS 119 461 v2.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects. Level of Assurance "Baseline Level of Identity Proofing"

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market Art. 24.1d Remote identification service component. Level of Assurance "Substantial"

1.3. Identity Proofing process

Checkin.com conforms to the following identity proofing service requirements as specified in ETSI TS 119 461 [1], Chapter 8:

- 8.1 Initiation
- 8.2.1 Attribute and evidence collection general requirements
- 8.2.2.1 Attribute collection for natural person
- 8.3.3 Validation of physical identity document
- 8.3.1 Attribute and evidence validation general requirements
- 8.4.1 Binding to applicant general requirements
- 8.4.2 Capture of face image of the applicant
- 8.4.3 Binding to applicant by automated face biometrics
- 8.5 Issuing of proof



1.4. Identity Proofing context

Identity proofing context refers to the surrounding external factors that influence and set limitations on the identity proofing process. A key aspect of this context is the legal and regulatory obligations specific to the intended use of the identity proofing. It is often the customer's responsibility to adhere to local regulations relevant to their particular identity proofing context.

The Checkin.com identity proofing context is not uniform and changes based on the purpose of verification and the country. Key areas of divergence are: the necessary level of assurance (such as eIDAS Substantial), the identity attributes that are collected (including mandatory, prohibited, and optional ones), and the country's unique laws and governmental policies concerning applicable technologies

2. Policy administration

2.1. Organization administering the document

Checkin.com Group AB is a Sweden-based holding company, founded in 2017, that unifies subsidiaries Checkin.com International AB and GetID OU, which provide Software as a Service (SaaS) services in Sweden and Estonia specializing in digital onboarding. The companies aim to redefine how users register,

identify themselves, and log in to digital services. By integrating multiple user experience systems, data sources, and identity solutions, Checkin.com delivers a seamless, secure, and scalable check-in experience that enhances conversion rates and ensures regulatory compliance. Operating globally, Checkin.com serves a diverse range of industries, including financial services, iGaming, and travel.

This document is periodically reviewed and updated. Approval and discussions of the current scope is performed in management reviews, similarly to ISO maintenance and recertification procedures.

2.2. Contact person

Checkin.com Group AB
559096-3087
Grev Turegaten 30, 114 38
Stockholm, Sweden
support@checkin.com

2.3. Time or frequency of publication

The latest version of this IPSP approved by management is available for download on the website.

2.4. Terms and Conditions

This IPSP becomes effective from the date of publication on the website.
Amendments become effective upon publication. This IPSP remains in force until it is replaced by a new version.

Applicable terms and conditions towards partners for the provision of the identification service are regulated in the terms and conditions and service agreement.

Applicable terms and conditions towards the End user are regulated in the Privacy Statement.

3. Definition of Terms and Abbreviations

3.1. Terms

Term:	Definition:
Applicant	natural person whose identity is to be proven
(identity) attribute	quality or characteristic ascribed to a person.
LoA	Level of Assurance (LoA) according to eIDAS Regulation (EU) 910/2014 which distinguished between High, Substantial and Low level.
Binding to applicant	part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence.
Physical identity document	A government-issued, tangible document, that physically exists and is used to establish a person's legal identity.
End user	Person/Customer using the ID service. I.e. a person who wants to be identified.

(identity) evidence	information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct.
Identity document	physical document issued by an authoritative source and attesting to the applicant's identity.
Identity proofing context	external requirements affecting the identity proofing process
Identity proofing (process)	process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes.
Identity proofing policy	set of rules that indicates the applicability of an identity proofing service to a particular community and/or class of application with common security requirements.
Identity proofing practice service statement	Alternative name given in ETSI 119 461 [1], clause 6 for the trust service practice statement defined in ETSI EN 319 401 [1], clause 6.1
Liveness detection	measurement and analysis of biometric characteristics to detect that the person is not recorded and live
Partner	the legal entity/Company subscribing to the service. I.e. the company that uses Checkin.com as a third party identity solution
Service Agreement	Service Agreement for the provision of the verification Service with a Partner
Remote identity proofing	identity proofing process where the applicant is physically distant from the location of the identity proofing.
Trust service component	one part of the overall service of a TSP according to ETSI EN 319 403-1 [i.6].
Trust Service Practice Statement	statement of the practices that a TSP employs in providing a trust service.
Service	the service provided by Checkin.com which is in scope with this identity proofing practice statement.

3.2. Abbreviations

IPSP Identity Proofing Service Policy

LoA Level of Assurance

MRZ Machine Readable Zone

OCR Optical Character Recognition

TSP Trust Service Provider

TSPS Trust Service Practice Statement

VIZ Visual Inspection Zone

FAR False Acceptance Rate

FRR False Rejection Rate

4. Risk Assessment

Checkin.com Group AB ’s risk assessment process identifies and manages risks that could potentially affect Checkin.com Group AB ’s ability to provide reliable and secure services to our customers. As part of this process, Checkin.com Group AB maintains a risk register to track all systems and procedures that could present risks to meeting the company’s objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Checkin.com Group AB product development process so they can be dealt with predictably and iteratively.

5. Policies and Practices

Checkin.com Group AB maintains an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022 and supports SOC 2 Type 2 compliance. The ISMS governs all systems, personnel, and locations involved in identity proofing services, ensuring appropriate technical and organizational measures are in place to protect confidentiality, integrity, and availability.

Policies and procedures are designed to meet legal, regulatory, contractual, and internal compliance requirements. These controls are reviewed and updated annually as part of the management review process and are overseen by the Chief Technology Officer (CTO).

Data protection practices follow applicable privacy regulations, including the General Data Protection Regulation (GDPR). Customer commitments are defined in Service Level Agreements (SLAs) and contracts, and are supported by the ISMS, operational controls, and periodic independent audits to ensure service integrity and compliance.

6. Internal Organisation

Checkin.com Group AB has established a clear internal structure to ensure the secure and reliable delivery of its identity proofing services. The organization applies non-discriminatory practices and segregation of duties in line with its ISO/IEC 27001:2022-based information security framework.

Roles and responsibilities are clearly defined, and access to sensitive systems is restricted based on the principle of least privilege, managed centrally through Identity and Access Management (IAM). All suppliers, including subcontractors and external service providers involved in identity verification, are subject to risk assessments and contractual security obligations. These providers operate under strict contractual control with oversight from Checkin.com.

Organizational and financial stability is supported by formal governance structures and documented reporting. Internal policies govern vendor selection, outsourcing, and third-party management. Services are designed to meet high assurance levels and reflect recognized industry best practices.

7. Human Resource Security

Checkin.com Group AB applies structured onboarding and oversight processes to all employees to ensure a high standard of competence, integrity, and reliability across the organization. Qualifications and relevant experience are verified during onboarding, and personnel are assigned roles in line with their responsibilities and skills. Ongoing performance is reviewed as part of the company’s regular performance review process.

Security awareness training is mandatory for all staff and is regularly updated to reflect evolving risks, compliance requirements, and best practices. Personnel with elevated responsibilities—such as system administrators and operations staff—are granted access rights in accordance with their roles and these are reviewed periodically as part of the company’s information security governance.

8. Asset Management

Checkin.com Group AB manages all its assets—software, hardware, data centre IT, and end-user computing assets—according to a comprehensive asset management policy which is part of ISO27001:2022 and audited yearly. A complete inventory is maintained, and assets are classified and protected based on risk assessments.

9. Access Control

Checkin.com determines the type and level of access granted to individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by Checkin.com's business and security requirements.

Permissions and access rights not expressly granted shall be, by default, prohibited. Checkin.com's primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible, rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production infrastructure shall use Multi-Factor Authentication (MFA).

10. Cryptographic Controls

Checkin.com evaluates the risks inherent in processing and storing data and implements cryptographic controls to mitigate those risks. Where encryption is in use, strong cryptography with associated key management processes and procedures shall be implemented and documented. All encryption is performed in accordance with industry standards, targeting best practices in NIST SP 800-57. Customer or confidential company data must utilize strong ciphers and configurations in accordance with the vendor recommendations.

11. Physical and environmental security

AWS oversees and strictly manages physical access to data centres through rigorous protocol, permitting entry exclusively to authorised personnel. This stringent control prohibits any physical entry by Checkin.com staff or any of its partners. There is no processing or storage of data on any on-premise or hybrid clouds.

The AWS Cloud premises are highly secure and heavily monitored including proper entry controls, protection against external and environmental threats, cabling security, and maintenance of equipment are in place.

12. Operation Security

Checkin.com Group AB maintains documented operational security processes to ensure the secure and continuous operation of its identity proofing services. Change management procedures are in place to assess, test, and approve system changes before deployment, and development, staging, and production environments are strictly separated.

Security patches and updates are applied based on risk and vendor guidance, while technical vulnerabilities are prioritized and remediated within defined timeframes. System activity, administrator access, and configuration changes are logged and monitored to detect unauthorized behavior.
Additional controls include malware protection, automated backups, network segmentation, and file integrity monitoring. These measures are aligned with ISO/IEC 27001:2022 and SOC 2 Type 2, supporting Checkin.com's commitment to operational resilience and data protection.

13. Network Security

Checkin.com Group AB's infrastructure is segmented into security zones protected by multiple firewalls based on the functional, logical, and physical relationship between the systems and services. Processing servers are running on a separate subnetwork accessible to authorized personnel only. As an ongoing commitment to enhance security, the system undergoes an external penetration test conducted by a certified security firm at least once a year.

14. Incident Management

Checkin.com uses the ISO27001:2022 framework and has a comprehensive ISMS in place for handling incidents and minimizing disruptions. The framework and incident handling include polices, processes, communications and preparations for security or IT related incidents.

15. Business Continuity

Checkin.com tests and validates its BCD plan and corresponding policies at least annually. It includes standby processing clusters, backup recovery plans and ability to swiftly get back on track in case of very big disruptions to the service. This is all controlled and audited by ISO27001:2022.

16. Termination

Checkin.com has developed a termination plan to be executed if a decision is made to terminate Checkin.com Service Agreement. Termination procedures include notification of affected entities; and where applicable active obligations will be reviewed and either fulfilled, transitioned, or terminated according to respective terms and conditions

17. Identity proofing service requirements

17.1. Initiation

Checkin.com provides an automated remote identity proofing service for natural persons.

The applicant is presented with a privacy notice prior to an identity proofing. The applicant has to read and accept these terms. This includes a full overview of what will happen, the process, the captured/processed data, data storage, deletion, retention policy, applicable law incl. GDPR:

The application supports and can handle persons with disabilities. Autocapture functionality is available to reduce the need for manual user interaction, helping ensure a smoother flow for all applicants. In edge cases (e.g. document issues or poor lighting), some actions may still require the applicant's manual interaction.

17.2. Attribute and evidence collection general requirements

The applicant’s physical identity document is scanned during the identity proofing process. The identity proofing context defines the attributes to be collected and may include both mandatory and optional fields. Only attributes needed for the specific context are collected.
Multiple types of evidence may be used, combining the physical document with biometric data such as a facial image or liveness check. The collected data is checked for correctness and consistency. Documents must be valid at the time of the identity proofing and issued by trusted authorities.
The identity proofing flow is configurable per use case. Partners can define required steps (e.g. document only, document and selfie, or document, selfie and liveness), accepted document types, issuing countries, minimum age, and required fields.

Anonymity or pseudonymity is not accepted; all names must reflect the real legal identity shown on the official identity document.

Evidence of the process, including captured media, timestamps, and session metadata is securely recorded to encrypted storage to support auditability and compliance.

17.3. Attribute collection for natural person

The identity proofing practice statement identifies, for each supported identity proofing context, the methods used to collect identity attributes for a natural person. This includes scanning from a physical identity document (via OCR, MRZ reading, and analysis of security features) and optional biometric capture via selfie.

Minimum attributes always collected:

- Family name(s)
- First name(s)
- Additional attribute(s) required to ensure uniqueness, i.e. document number, issuing country, date of birth, personal identification number

Additional attributes collected, depending on the identity proofing context:

- Full name
- Document type
- Expiration date
- Date of issue
- Gender
- Nationality
- Barcode (if present)
- Optional fields from the document (e.g. personal identification number, if present)
- Portrait image(s) from the document
- Biometric/liveness data (collected during video capturing to prove that the applicant is a live person)

17.4. Attribute and evidence validation general requirements

Identity attributes are extracted from both the Visual Inspection Zone (VIZ) and the Machine Readable Zone (MRZ) of the physical identity document using Optical Character Recognition (OCR) technology. The MRZ typically contains the family name, first name(s), date of birth, and other key attributes. This set of attributes aligns with the minimum data set required to uniquely identify a natural person, as defined in eIDAS CIR 2015/1501.

All extracted attributes are validated for correctness and internal consistency. Cross-checks are performed between VIZ and MRZ data. The structure and format of the fields are validated, and the document’s issuing country and expiry date are checked against the supported identity proofing context. Documents must be valid at the time of the identity proofing.

Encoding differences, such as transliteration from Cyrillic or other scripts to Latin, and the handling of diacritics, are addressed by normalizing extracted values to a unified format. Name fields are compared using logic that supports truncation, missing middle names, and reordering.

The process verifies that the identity document type and issuing country are accepted in the specific identity proofing context. Tampering and manipulation are detected using automated checks. Where relevant, document authenticity and integrity are evaluated based on security features and known structural patterns.
Validation is performed in a secure environment under the control of the identity proofing service. Captured identity data and document evidence are handled securely and stored for audit or further review in accordance with clause 8.5.2.

17.5. Validation of physical identity document

The applicant is required to present a physical identity document in real time in front of the camera. The process captures high-resolution images of the document, covering at least one image per side. No pre-recorded files are accepted; the document must be physically present and shown live during the session. The process also assesses lighting, sharpness, and visibility of captured frames, and may request the applicant to retry the capture if image quality is insufficient. A maximum retry limit logic is implemented.

Captured images and metadata are transmitted securely to a controlled environment for verification. Reference data, such as PRADO, may be used for document template validation.

Validation is performed using automated checks supported by AI models, with fallback to manual review if automatic checks fail. The process verifies printed document elements such as text layout, embedded portraits and security features. Extracted attributes from the Machine Readable Zone (MRZ) are compared with data from the visible zone for consistency.

Security features are checked where present, including optically variable elements, holograms, and printing techniques. The extent of the verification depends on the document type and the identity proofing context.

17.6. Binding to applicant general requirements

As part of the identity proofing process, a live facial image of the applicant is captured to confirm that the person presenting the identity document is its rightful holder and is physically present during the session.

Binding is established by comparing the real-time facial image of the applicant with the portrait(s) extracted from the identity document. This confirms both possession and identity match. The comparison may be performed using automated biometric matching, manual review, or both, depending on the configured identity proofing flow.

17.7. Capture of face image of the applicant

A facial image of the applicant is captured in real time during the identity proofing process. This image is securely transmitted to a controlled environment for verification. The system applies biometric liveness detection and deepfake protection to confirm that the applicant is a live person and not a presentation attack.

The system is designed to resist common attack vectors, including:

- Screen replays
- Virtual or emulated camera feeds
- Injected video content
- AI-generated media such as face swaps or morphs

Liveness detection and spoof prevention rely on Presentation Attack Detection (PAD) technology that is certified to iBeta Level 1 and Level 2, in line with ISO/IEC 30107-3. Where applicable, a 3D face representation may be created using multi-frame analysis to further enhance spoof detection. The system tested and tuned against biometric performance benchmarks that target a BPCER of 0.00% at APCER thresholds of 0.1 and 0.01. These values are reviewed regularly as part of model updates.

Image quality is evaluated during the session. If lighting, sharpness, or visibility are below acceptable thresholds, the applicant is prompted to retry. A retry limit is enforced to prevent abuse or excessive attempts.

Captured images and metadata are stored and processed in accordance with the identity proofing context and applicable privacy regulations.

17.8. Binding to applicant by automated face biometrics

During processing of the application the face biometrics image captured from the document is compared to the face of the applicant captured as part of the liveness and selfie steps. The images are then automatically compared using a trained AI network that can distinguish human features and compare the similarity between two face images. If the image on the document matches the applicant this step is evaluated as successful. If both the automated biometric check and fallback methods failed or were not performed, the identity proofing process is marked as declined.

The biometric comparison is processed and conducted at Checkin.com controlled infrastructure and has been thoroughly tested. The goal is to achieve a False Rejection Rate (FRR) and False Acceptance Rate (FAR) as close to 0% as possible, recognizing that while absolute 0% may be theoretically ideal, practical systems aim to minimize these rates to the lowest feasible levels to ensure optimal accuracy and security. The confidence score calculated by the face biometrics comparison is evaluated against a test threshold to receive as low FAR ratings as possible without increasing FRR. For 1-1 matching of faces the FAR and FRR is very low provided that the image quality is sufficient. The FAR rating is set to be below 0.01% for biometrics checks which gives a FRR of less than 0.5%. For FRR the rate is much more dependent on the captured images quality. The captured image quality is also assessed as part of a prerequisite of the image evaluations. The confidence thresholds for FAR are updated based on need and when new and improved models are put in use.

Several mechanisms are used to detect and minimize the use of deep-fakes, morphed images and digitally altered images. These detection models and methods are updated and improved often as the risks of such attacks are evaluated.

17.9. Issuing of proof

At the end of the identity proofing process, Checkin.com issues a structured result with a final status of Approve/Needs-review/Decline based on verification rules set by a partner. The result reflects the outcome of automated and/or manual verification steps and is made available through the backoffice, API, or as a downloadable PDF within the backoffice application details view.

The result includes the following elements:

- Application ID
- Timestamps
- Overall verification status
- Document verification status
- Face comparison verification status
- Captured media (images and/or video, if applicable)
- Metadata
- External ID (if provided by partner for system cross-reference)

The applicant cannot access or modify the issued result. All data is securely stored and protected, with access limited to authorized persons. Retention, access, and delivery settings are configurable based on the identity proofing context and the agreement with the partner.

The partner can access the details of the results through a process. A separate JWT signed webhook is sent to the partner when the status of the identification is completed. The webhook authenticity can then be validated towards the Checkin.com public signing token. The results and information shared by the webhook can be retrieved from Checkin.com backend servers with a pre-shared partner specific secret API key. The full transmission is encrypted using SSL/HTTPS with modern encryption.

17.10. Evidence of the identity proofing process

In addition to the result issued to the partner, Checkin.com retains internal evidence of the identity proofing process to support auditability and regulatory compliance. This includes the full decision trail, system logs, and fraud detection signals linked to the application.

If manual fallback was triggered, operator actions and timestamps are also recorded. The time of completion is part of the stored data. All evidence is stored securely in an access-controlled environment.

This data is not visible to the applicant or exposed via API and is retained according to the configured retention policy. Once the retention period ends, all related data is securely and permanently deleted.

18. Identity proofing use cases

The Checkin.com identity proofing flow is configurable to support a range of use cases, including onboarding and access control. Partners define the use case and can configure the verification steps to meet their specific legal, regulatory, or business requirements

18.1. Identity proofing of natural person

Checkin.com identity proofing process for natural persons is designed as a hybrid model, combining automated decision-making with manual review fallback in case automated checks fail. The process is fully remote, with unattended online communication and no physical presence required from the applicant.

The applicant interacts with the system through guided flows that collect and validate attributes and evidence in real time. The binding of identity evidence to the applicant is performed using face biometrics and certified liveness detection, ensuring that the person presenting the document is physically present and matches the identity document holder.

18.2. Remote identity proofing

Checkin.com performs remote identity proofing under the hybrid model defined in ETSI TS 119 461 clause 9.2.3.3. The applicant is remotely present and completes the process through an unattended online flow.

As described in sections 17.5 and 17.8, evidence validation is performed using a combination of automated and manual methods, and binding to the applicant is achieved using face biometrics with fallback to manual verification if needed.