

Prisoner Identification Solution (Biometric Identification and Release)

1. Service Summary

Unilink's Prisoner Identification Solution is a cloud-hosted biometric identity assurance service designed for secure environments such as prisons, immigration detention centres and secure hospitals. It strengthens identity checks at the two highest-risk control points: reception into custody and the point immediately prior to release or discharge.

The service provides positive biometric identification using high-quality fingerprint capture, supported by a prisoner photograph for manual or automated visual verification. Optional multi-factor can be enabled by matching a live facial image against the prisoner photograph already held on the system. Fingerprint identity checks can be performed as verification (1:1) and, where operationally required, identification (1:N).

The System can be deployed locally on premise, in an approved customer data centre, customer cloud environment or in Unilink's secure cloud (subject to customer assurance requirements). The cloud-hosted option provides consistent configuration, centrally managed matching and reporting, central auditability, and reduced local management overhead.

2. Service Features

The service includes:

- Reception enrolment: capture fingerprints, associate prisoner photograph and key identity markers.
- Release/discharge: final biometric check immediately prior to release or discharge.
- Fingerprint verification (1:1) and identification (1:N), configurable to policy.
- Optional live facial match against stored prisoner photograph for multi-factor assurance.
- Secure web service-based capture enabling flexible use of approved devices (PCs or MoJo devices) with fingerprint readers and cameras.
- Custody status association (e.g., in custody, released, on ROTL, temporarily absent) supporting operational assurance and reporting.
- API integration with operational systems (e.g., NOMIS/DPS) to receive release/status events and return confirmation of identity checks.
- Role-based access control, audit logging and data minimisation built in by design.
- Optional support for contactless fingerprint capture (e.g., MorphoWave) using the same centrally hosted identity and reporting services.

3. Service Benefits

- Reduces the risk of erroneous release by introducing consistent, positive biometric identification immediately prior to release.
- Strengthens discharge assurance with simple workflows focused on reception and release.
- Enables consistent identity checks across multiple establishments through centrally governed configuration and management.
- Improves auditability through central reporting and traceable identity checks at key control points.
- Reduces local infrastructure and software management overhead compared with locally managed biometric databases.
- Provides a pathway towards an 'enrol once' model and national service capability over time, if desired.

4. Service Scope

The service covers biometric identity assurance at reception and at release/discharge. Typical users include reception staff, discharge/release officers, duty managers and operational assurance teams.

- Enrolment at reception (fingerprints and photograph association).
- Biometric identity check immediately prior to release/discharge (and other custody exit events as required).
- Central matching, reporting and audit functions.
- Local device enablement for approved capture devices.
- Integration to customer systems for release/custody status events where required.

5. How the Service Works

At reception, the service supports biometric enrolment by capturing fingerprints and associating the individual's photograph and identity markers. Prior to release or discharge, a final fingerprint check is performed to confirm identity, with the option to include a live facial match against the stored photograph where required. Biometric matching, identity management and reporting are provided through a centrally hosted service, governed consistently across establishments. Secure APIs support the exchange of identity verification outcomes and release, discharge or status information with operational systems. Where throughput or hygiene considerations apply, contactless fingerprint devices can be used to support efficient processing.

6. Onboarding and Offboarding

6.1 Onboarding

- Agree scope, sites, workflows, user roles and assurance policy.
- Confirm device model(s) and connectivity (approved PCs or MoJo devices; optional contactless capture).
- Configure service tenant, security controls and role-based access.
- Implement integrations (e.g., NOMIS/DPS) and data exchange where required.
- Pilot rollout and phased expansion to additional sites.

6.2 Offboarding / exit management

- Agree termination plan, data export/retention/deletion and reporting requirements.
- Provide agreed extracts (e.g., audit logs and reports) and decommission integrations in a controlled manner.

7. Support and Service Management

Incidents and service requests are managed in accordance with the agreed contractual service levels and the operational requirements of custodial environments.

Initial response times are:

- High and Medium priority incidents: within 1 hour
- Low priority incidents and general service requests: within 2 hours

Standard support hours are Monday to Friday, 8:00am–5:00pm (UK time). In recognition of the critical nature of custodial systems, High priority incidents are supported 24 hours a day, 365 days a year.

Support is delivered using an ITIL-aligned service management framework. All requests are logged through a central service desk and assessed by a triage function, which assigns priority and routes issues to the appropriate resolver group. Resolution is provided through structured 1st, 2nd and 3rd line support, with clear escalation procedures in place.

8. Service Constraints and System Requirements

8.1 Service constraints

- Requires connectivity between approved capture devices and the centrally hosted service (cloud-hosted model).
- Optional facial matching depends on camera quality, lighting and operational capture practice.
- Customer-system integrations depend on interface availability, approvals and change control.

8.2 System requirements

- Approved endpoint device(s) (PCs or MoJo devices) with supported fingerprint readers and a camera.
- Secure network connectivity to the hosting environment (customer cloud or Unilink secure cloud).
- User accounts and roles managed in line with customer security policy.

9. Security and Compliance

The service supports privacy and data protection controls built in by design, including role-based access control, audit logging and data minimisation, supporting UK GDPR and relevant information assurance requirements.

Where Unilink provides the managed service, it operates within ISO 27001-certified information security controls and GDPR-compliant data handling, with controlled access to sensitive data and regular external security testing aligned to customer governance.

10. Training

Training is available for operational users and support teams, covering workflows, device use, exception handling, and audit/reporting (remote or on-site).

11. Ordering and Invoicing

This service is ordered via the Digital Marketplace in line with G-Cloud call-off procedures. Pricing is provided separately in the G-Cloud pricing document.

12. Trial Service

A time-limited pilot/proof-of-concept can be provided to validate workflows, integrations and device choices prior to broader rollout.