HCLTech | Supercharging Progress™

# G-Cloud 15 – RM1557.15

## Lot 2 - Cloud Software

## Biometric Solution (Police Mobility)

## Service Description

# Foreword

This proposal has been prepared by HCLTech, for the sole use of Crown Commercial Service (CCS). The contents of this document shall remain the confidential property of HCLTech and should not be communicated to any other party without the prior written approval of HCLTech.

The furnishing of this document shall be subject to contract and shall not be construed as an offer or as constituting a binding agreement on the part of HCLTech to enter into any relationship.

HCLTech warrants that, to the best of their knowledge, those who prepared this document have taken all reasonable care in preparing it, have made all reasonable enquiries to establish the veracity of the statements contained in it and believe its contents to be true. (HCLTech cannot however warrant the truth of matters outside of its control and accordingly does not warrant the truth of all statements set out in this document to the extent that such statements derive from facts and matters supplied by other persons to HCLTech. The statements in this document are qualified accordingly.)

# Validity

This proposal and all information contained within are valid for a period of 180 days from January 30, 2026.

# HCLTech Contact

| | |
|---|---|
| **Name** | Paul Montgomery |
| **Address** | 6th Floor<br>70 Gracechurch Street<br>London<br>EC3V 0XL |
| **Email** | eas-hclsalessup@hcltech.com<br>or<br>Paul.Montgomery@hcltech.com |
| **Phone** | +44 (0) 7747 828480<br>or<br>+44 (0) 20 7105 8600 |

# Table of Contents

## About HCLTech

HCLTech is a next-generation global technology company that helps enterprises reimagine their businesses for the digital age. Our technology products, services and engineering are built on four decades of innovation, with a world-renowned management philosophy, a strong culture of invention and risk-taking, along with a relentless focus on customer relationships.

With a worldwide network of Research and Development (R&D), innovation labs and delivery centres and over 225,000+ 'Ideapreneurs' working in more than 60 countries, HCLTech serves leading enterprises across key industries. HCLTech generated consolidated revenues of USD 13.8 billion for 12 Months ended 31st March 2025 with 4.5% Increase YoY. For latest figures, please refer to the link below:

About our Company: HCLTech – Supercharging Progress
HCLTech' s Annual Report 2024-25 | HCLTech

We offer an integrated portfolio of products, solutions, services, and Intellectual Property (IP) through our Mode 1-2-3 strategy built around Digital, Internet of Things (IoT), Cloud, Automation, Cybersecurity, Analytics, Infrastructure Management and Engineering Services, amongst others, to help enterprises reimagine their businesses for the digital age.

## Service Description

HCLTech started working with UK Police Forces around ten years ago and has delivered mobilisation to over 20,000 frontline Police Officers. The service enables officers to be more productive and safer, by providing role based mobile access to critical information from in-force backend systems and national police applications.

The service is designed to enable police forces to achieve and demonstrate real benefits from a mobile data investment. The service integrates with existing force national and local backend applications and provides remote access to these from the streets.

The HCLTech Biometric solution is the next generation tool in the OPTIK (Operational Policing Tool and Information Kit) Solution for police forces to perform nominal check using their fingerprints. HCLTech's Biometric solution seamlessly integrates with the Home Office BSG (Biometric Service Gateway) service to perform biometric identification from IDENT1 (UK national criminal biometrics system) and IABS (Immigration Asylum Biometric Database) databases.

This solution has been developed on the HCLTech 'One Code' platform, which makes it platform and device agnostic.

The HCLTech Biometric Solution enables officers in the field to identify nominals, criminals and wanted suspects, etc. It can also help officers to identify individuals in emergency situations and to contact next of kin when appropriate.

The HCLTech Biometric solution integrates with IDENT1 and IABS database to perform nominal checks using their fingerprint. It displays Forename, Surname, Date of Birth, Gender, Nationality, etc.

The result list for the IABS database also displays the thumbnail image of the nominal along with the option to view the image in a larger display. The solution is available across the full range of platforms, e.g. Microsoft, Android and IOS, along with the associated mobile devices.

## Features

The HCLTech Biometric solution provides:

- Biometric fingerprint search in national databases – IDENT1 & IABS
- Detailed audit trail for all the transactions
- Management dashboard reports
- Integration with national and police force systems like PNC (Police National Computer), Athena, Niche, etc. when integrated with the HCLTech OPTIK Solution (separate application).
- Offline working

- Police forces with the capability to securely capture, record and have role-based access to secure data on the move.

## Benefits

- Retrieve nominal details from IDENT1 and IABS systems on handset
- Access to real time information at the point of decision
- Saves time not returning to station/ custody to establish identity
- May identify those trying to escape investigation
- Increase police visibility out of the station
- Fewer arrests required to establish the identity
- Innocent parties dealt with quickly and with less inconvenience.

## Technical Specifications

The HCLTech Biometric solution is available across a variety of devices and platforms as listed below:

- Smart Phone – Android smart phone (Android 0S 6 and above), iOS (iPhone 4 and above), Windows 8, 8.1
- Tablet – Android tablet (Android OS 6 and above), iOS (iPAD3 and above), Windows 8, 8.1.

Connectivity is based on trust which is created by using the certificates shared by the Home Office.

Any data transferred between HCLTech services and (Biometric Service Gateway (BSG) are encrypted over Secure Sockets Layer (SSL). The BSG is presented to subscribing organisations via the Public Services Network (PSN). Home Office has set out requirements in the PSN Code of Connection for any organisation wishing to connect to BSG.

A single connection will be established between each Mobile Application Server and the Biometric Services Gateway (BSG), as opposed to multiple servers being routed via a Force gateway, for example.

This meets HOB security principles but does mean that BSG may need to manage multiple routing connections, depending on the architectural environment of the Force in question. However, all such connections will adhere to the Code of Connection (CoCo).

The HCLTech Biometric solution interfaces with the Home Office Biometric Service Gateway (BSG) service. This requires handling the semantics to communicate with this service. Specifically, it uses the correct communication Application Programming Interface (API) to call the service and perform the necessary translation between the data formats used by the BSG service.

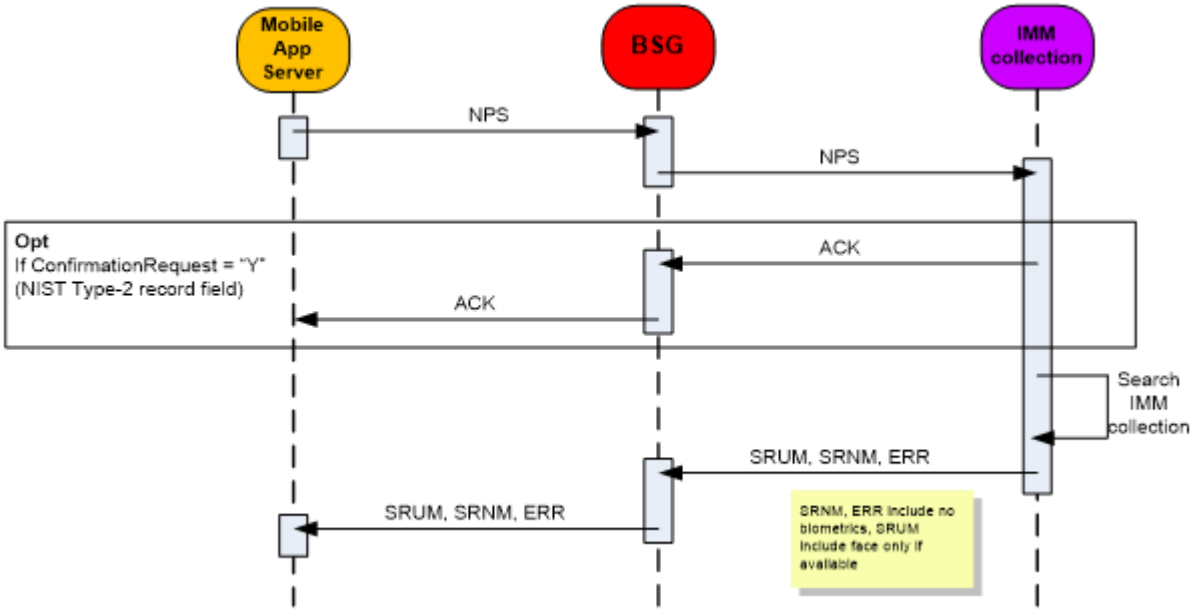
The BSG service contract consists of a long running conversation, it keeps the intermediate state while waiting for a response.

The Service Adaptors have been used to implement the logic necessary to encapsulate these tasks and to initiate and manage a messaging-based conversation with the BSG service.

BSG undertakes the orchestration of the separate immigration and police collection search requests, based on what is set in the Type-2 Request Collection field of the message.

The diagram below shows the basic request and response and how asynchronous “NIST ACK” works.

The sequence diagram below provides an end-to-end view of a search request from a Mobile App Server to search the immigration and police biometric collections, which is routed via the BSG.




*Basic request and response and how asynchronous "NIST ACK" works*

This functionality allows a field ("Confirmation Request") in the Type-2 record of the message to be set to request an asynchronous confirmation message that the request has reached the end system. In other words that BSG has successfully delivered it to the required end point.

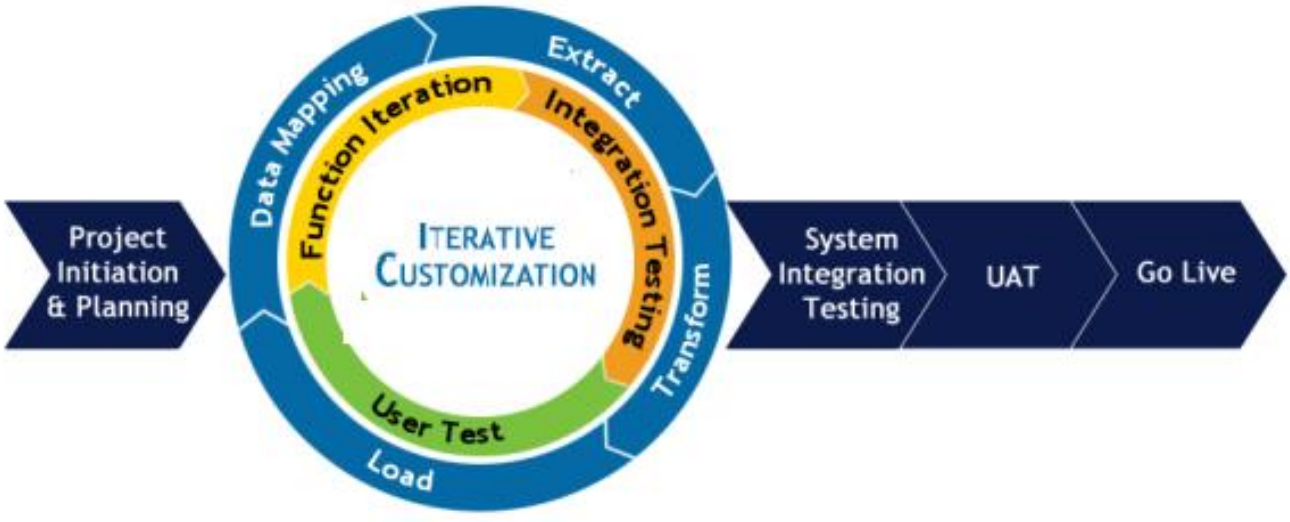
## Implementation

HCLTech uses a hybrid approach (mix of iterative and agile) to deliver best value to the customer for implementation.

Using this Hybrid approach, HCLTech will carry out due diligence activities to understand the current landscape that we will operate within. This will include understanding the backend systems and their interfaces, as well as the infrastructure in place to support it.

This enables HCLTech to define the most appropriate implementation approach/ plan and infrastructure design, making use of existing/ future IT investments. This ensures that the project is delivered with the highest quality, in the quickest time and to budget.

The high-level chronological representation of the project level execution activities is provided below:




*High-level chronological representation of the project level execution activities*

### Implementation Plan

The detailed project implementation plan demonstrating key deployment stages, activities and resourcing requirements for the complete project can be provided to the customer on request. All the dependencies will also be mentioned against the activities in the project plan.

Key dates in a detailed project plan incorporate the following:

- Key project phases, e.g. Scoping, Construction, UAT (User Acceptance Test) and Deployment
- Project deliverables, milestones and quality standards
- Detailed work packages, tasks and dependencies
- Responsibility and accountability for deliverables
- Resource assignment and ownership
- Partner obligations and dependencies.

### Risk Planning and Mitigation

Managing and minimising risk is a key element of HCLTech's approach to managing large scale programmes, projects and services.

A joint (customer and HCLTech) team will manage risk through a formal, structured framework, so that vulnerabilities, risks and threats can be identified and managed/ avoided throughout the project lifecycle and service contract. The objective of risk management is to identify and quantify potential risks, then perform mitigating actions (including risk avoidance) before the risk materialises.

Risk management processes and tools will be integrated with other activities throughout the project and service contract lifecycle. The analysis matrix is compiled using the following process:

- Identification of risks - brainstorming session by the joint team
- Analysis and ranking using an appropriate scale assessing the probability and impact, with the product of the two indicating an overall score. The higher the overall score, the greater the priority for the identification of sound counter-measures and contingency plans to manage the risk
- Continuous review and re-assessment – the risk matrix is updated as part of the Risk Management process.

Once identified, a risk will be recorded and managed through its lifecycle, assigning owners for each stage, providing a sign off audit trail and managing reporting against due dates, as well as recording the relevant discussions, outcomes and decisions.

The standard workflow lifecycle for a risk is shown below:

- Risk logged
- Action manager accepted
- Plan defined
- Plan completed
- Closed by owner.

The HCLTech risk management process requires all risks to be assessed based on the following criteria:

- Risk score = impact of risk x likelihood of occurrence.

This provides a simple prioritisation of all risks and helps identify the most appropriate level of management required for each item, i.e. items with a low risk score can be managed within a workstream, whereas items with a high risk score require input from a Management/ Steering Group level. The appropriate risk management strategy for a given risk can only be determined following detailed review and discussion. As part of this, input and options may be sought from a number of relevant sources within (or outside of) the programme/ service contract. Based on this information, the risk management process (operating within the broader governance process) can determine the most appropriate strategy from:

- Avoidance
- Mitigation
- Transference
- Acceptance.

Actions or activities are recorded, associated to the risk and tracked to individual completion.

## Support Arrangements

HCLTech proposes to provide Level 2 and Level 3 Support as part of this Service.

The Biometric solution is underpinned by a comprehensive Information Technology Infrastructure Library (ITIL) based service model. The HCLTech Support Desk will provide the co-ordination of service management activities including:

- Incident management
- Problem management
- Configuration management
- Service level management
- Escalations
- Complaints.

The HCLTech Support Desk operates business hours and on call support for Severity 1 issues.

Officers will raise the Biometric solution related issues with their internal Helpdesk. The same will be routed to the HCLTech Support team for resolution.

If the issue subsequently turns out to be related to the Home Office services, then service desk/ Force Duty Officer would be informed by HCLTech, so that they can contact their Home Office service desk directly. HCLTech can then work collaboratively with Home Office service desk from then on.

**Minimum data set required for a support call for HCLTech support team:**

- Fault description
- Is the device connected to the internet and Virtual Private Network (VPN)?
- Last input made before the fault
- Steps taken to replicate the issue
- Error code/ message
- Convenient time to contact the user
- Date and time the error occurred
- Actions taken so far.

**Following data set are required while raising a support call with HO service desk:**

- Service: BSG-Rapid Search
- Name of the person reporting
- Contact number
- Message unique identifier reference
- Database(s) that the search was made against (IABS, IDENT or both)
- Time and date the search was made
- Any error message(s) received
- Description of the issue
- Confirmation of the triage activities done by Force.

**HCLTech Service / Support Contacts are as below**:

Email: HCLTech Policing Mobility Support <HCLMobilitySupport@hcl.com>

### Service Levels

The baseline service will come with a monthly service availability Service Level Agreement (SLA) of 99.9%.

We provide high levels of resilience and availability and commit to 99% over the contract term.

The Service will be available 365 days a year, 24 hours a day.

The items below highlight the key technical design considerations of the HCLTech solution to keep the system highly available throughout 365 days a year and 24 hours a day:

- Loosely coupled architecture, all components can be hosted independently

- No single point of failure; every component equipped with exception handling and logging frameworks
- Fault tolerance at all levels - The system will continue to operate when a failure at any layer occurs, such as receiving, processing, data storages, networks, etc.
- Isolation of the data and hosting - The system is de-coupled from processing, integration and the data storage
- Availability of reserved nodes - All the points in the system can be backed-up with the reserved nodes that have been kept in the passive but ready to serve state
- Fail-over and replicating identical instances to other systems
- During any mode of failure in the application or the hardware, an identical system is replicated, so that normal operation continues as before
- Logical categorisation of data to avoid data redundancy
- Administrating the deployed components from a single window at runtime
- The hosting site will be enabled with monitoring tools - HCLTech uses Microsoft's System Centre Operation Manager (SCOM) to monitor.

**Outage and Maintenance**

Planned works are any activities undertaken by HCLTech as part of routine maintenance and preventative actions to support the continued running of the service.

HCLTech will ensure that we give at least 10 Working Days' notice of any planned works affecting the customer.

Customers may not refuse planned works that are required by us to ensure the integrity, supportability, security, performance or availability of any service for customers.

**Customisation**

All agreed customisations will be included within the relevant Statement of Works (SoW) and/ or Solution Design Document (SDD) documentation.

**Performance attributes**

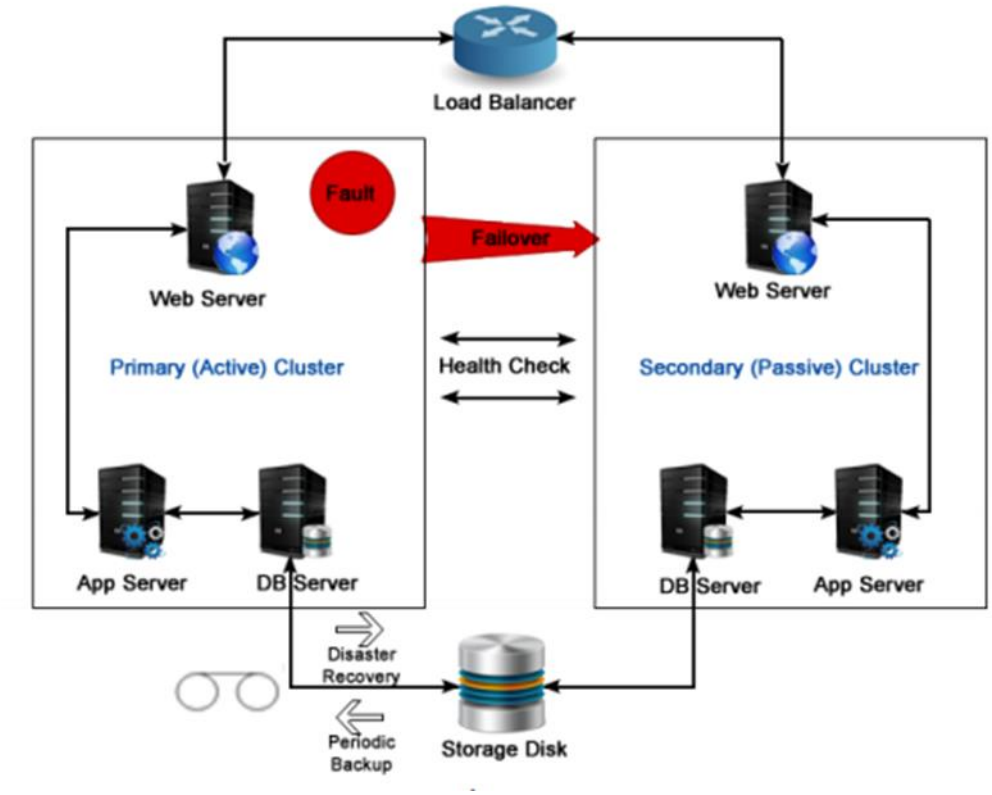
The HCLTech Biometric Solution service performance is dependent on the network connectivity and on the external system's performance. However, on a normal day with decent network connectivity we expect our transactions to complete within 5 – 6 seconds.

## Business Continuity/ Disaster Recovery

1. **For in-house installation:** As part of this service, HCLTech proposes the in-house installation within the customer's infrastructure. No infrastructure services are being offered as part of this service. We can provide guidance and support, but disaster recovery will remain as the customer's responsibility and will be managed by the customer's internal IT team.
2. **For Central Hosting:** As part of this service, HCLTech will provide the Disaster Recovery (DR). The DR plan and strategy will be shared during implementation. If any modification is required as per the customer's requirements, then this will be discussed and agreed during the implementation period.

For Business Continuity, the solution must remain available even in the face of any physical site going down. Appropriate measures will be in place in the physical architecture to ensure the required business continuity.

The networking architecture of the HCLTech solution will have two physical sites. Both sites will be active in nature and servers hosted on both sites will be connected with a dedicated secure link as shown in the diagram below.




*Active/ Passive Clustering*

## Data Backup/ Restore

1. **For in-house installation:** As part of this service, HCLTech proposes the in-house installation within the force infrastructure. No infrastructure services are being offered as part of this service. We can provide guidance and support but backup will remain the customer's responsibility and will be managed by the customer's internal IT team.
2. **For Central Hosting:** As part of this service, HCLTech will provide the backup. The backup plan and strategy will be shared during implementation. If any modification is required as per the customer's requirements then this will be discussed and agreed during the implementation period. The service will be hosted at a secure IL3 (Impact Level 3) compliant data centre. All the backups will be stored in a restricted place where only authorised personnel will have access to those areas.

## Security

HCLTech's Biometric Solution has been designed in a way that it is fully compliant with the Data Protection Act 1998 and fully supports the standards required to achieve the security compliance for IL3.

HCLTech's Biometric Solution has been designed in a way that fully supports the standards required to achieve the security compliance for the Association of Chief Police Officers (ACPO) Community Security Policy and local Force Security Policies.

Selection of application interface design patterns, choice of protocols for secure data communication, implementation of business rules for smooth integration with the customer's backend systems are all designed keeping security at the core.

This helps us to ensure the confidentiality, evidential integrity and availability of the service as explained below.

HCLTech's Biometric Solution comes with a three-layered security architecture/ framework, thus:

- Encryption of data before transmission
- Implementation of SSL (Secure Sockets Layer) encryption
- Secure/ VPN Tunnel.

The service is split into the following security domains:

- End point security
- Communications
- Authentication
- Audit
- Hosting.

### Authentication in Biometric Solution

There is no authentication mechanism in the Home Office BSG. Connectivity is based on trust which is created by using the certificates shared by the Home Office. The officer will authenticate in the HCLTech OPTIK application and appropriate roles will be assigned via Access Management in the HCLTech Admin Desktop solution. Any data transferred between HCLTech services and BSG are encrypted over Secure Sockets Layer (SSL).

### Access Management

Access to the application will be managed by the Manage Group functionality in the HCLTech Admin Desktop solution. Access to officers will be controlled by the customer's project team and can be revoked directly from the Manage Group function.

### Logging & Audit

Complete audit trails are maintained with the HCLTech administration module and this information is accessible to administrators via dashboards.

The HCLTech Biometric Solution implements logging at various levels that can be used for audit purposes.

The first level of logging is implemented at the level where every attempt to access the network servers are logged in appropriate log files. The logging at this level provides information on who attempted to access the network, which device or workstation was used for the access.

The second level of logging is implemented at the Web Server level - which is Microsoft Internet Information Server (IIS) - where the Web Application of the HCLTech Biometric Solution is hosted. At this level, all access attempts to the HCLTech Biometric solution are logged including any unauthorised access attempt.

The third level of logging is implemented in the HCLTech Biometric solution components. At this level there are the following categories of events that the HCLTech Biometric solution logs:

- Debug – this category will be used to log messages that describe flow of control in the programme
- Information – this category will be used to log any general information
- Warning – this category will be used wherever the programme suspects something that needs to be corrected but does not come under the category of errors
- Error – this category will be used to log all application exceptions
- Fatal – this category will be used to log all system exceptions.

The logging at this level provides information on which functionality was accessed, errors occurred during the processing and debug/ information/ warning messages useful for support staff.

Analysing the log files generated at various levels and correlating the log information, helps in finding answers on general security audit questions, such as:

- Who attempted the access?
- When was the access attempted?
- Which device or workstation was used for the access?
- Which services and functionalities were accessed?

## Exclusions

The services listed below are out of scope of the contract terms.

- Infrastructure and associated infrastructure support
- Remote connectivity to enable shared support

- Load balancer configuration
- Third party software licences
- Firewall settings for associated ports of the Biometric Service for all the environments, e.g. test, training and live, etc.
- Maintenance and connectivity to the Biometric Service Gateway (BSG) service.
- Devices Management
- Devices and fingerprint scanner – Optional.
- HCLTech can help arrange devices and scanners, as per mutual agreements. However, they are not delivered as part of this service.
- Network connections are not offered as part of this services.
- However, the HCLTech Biometric service can connect via Public Services Network (PSN) and individual force's Police National Network (PNN) connection.

## Account Management

A dedicated Account Manager and Service Delivery Manager will be appointed to discuss and manage issues, changes and enhancements to the service.

HCLTech | Supercharging Progress™

hcltech.com