Service Definition
Paygate Enterprise Payments Platform

Service overview

Paygate Enterprise is a cloud-hosted payments and validation platform that enables organisations to securely manage Bacs Direct Credits, Bacs Direct Debits and Faster Payments through a fully accredited Bacs Approved Software solution. The service is designed for UK public sector and regulated organisations that require a highly secure, resilient and auditable platform to initiate, control and monitor payment activity. Paygate Solutions Limited has been a Bacs Approved Software Supplier since 1977 and also operates as a Bacs Approved Bureau, allowing customers to choose between self-managed submissions using their own Service User Numbers or a fully managed bureau submission model where appropriate. The platform combines payment processing, full lifecycle Direct Debit management, Faster Payments capability, and integrated KYC-focused validation services within a single centrally managed system.

Service scope and functionality

The Paygate platform supports the end-to-end processing of Bacs payments, including the creation, validation, signing, approval and submission of Standard 18 files for Direct Credits and Direct Debits. Payment data can be ingested via secure web upload, scheduled SFTP using the Paygate Agent, or programmatically through REST APIs, allowing seamless integration with finance, payroll and ERP systems. Submissions follow a structured Validate, Create, Sign, Approve and Submit workflow, ensuring strong segregation of duties and full auditability. The service supports both smartcard-based and hosted HSM signing options, including HSM as a Service operated to FIPS 140-2 Level 3 standards, removing the need for customers to manage physical hardware if desired. As a Bacs Approved Bureau, Paygate can submit files on behalf of customers during contingency scenarios or as a fully outsourced submission model.

Direct Debit management

Paygate provides comprehensive Direct Debit management functionality covering the full lifecycle of a Direct Debit Instruction. This includes the creation, amendment and cancellation of DDIs, support for AUDDIS processing, and the handling of ARUDD and ADDACS reports. The platform enables organisations to manage advance notice requirements, track unpaid items, reconcile returned Direct Debits and respond efficiently to payer status changes in line with Bacs scheme rules. Direct Debit reporting and exception handling tools provide clear visibility of mandate status and payment outcomes, supporting compliance and reducing the risk of failed collections and indemnity claims.

Faster Payments

In addition to Bacs processing, the platform supports Faster Payments, enabling near real-time payments where faster settlement is required. Faster Payments can be initiated and managed through the same secure workflows and permission model as Bacs payments, providing a consistent user experience and centralised control across payment types. This allows organisations to choose the most appropriate payment method based on urgency and operational need while maintaining consistent governance and audit controls.

KYC, data validation and verification

The service includes integrated KYC-focused validation and verification services designed to improve data accuracy and reduce fraud risk before payments are initiated. These services include sort code and bank account modulus checking, Confirmation of Payee, address lookup and validation, email validation and phone number validation. Validation can be performed at the point of data capture or prior to submission, ensuring that errors are identified early and reducing the likelihood of failed or misdirected payments. These checks support regulatory expectations, Bacs scheme responsibilities and good practice around customer due diligence.

User access, permissions and workflows

Access to the platform is controlled through a single, consistent user model with granular role-based access control aligned to the principle of least privilege. Permissions can be configured at group and function level, allowing organisations to separate responsibilities across departments, payment types and approval stages. Authentication requires username and password with mandatory multi-factor authentication, with support for MFA applications, email, SMS and hardware tokens. The platform integrates with Microsoft Entra ID to provide single sign-on, allowing organisations to mandate SSO, restrict access by domain and centralise identity management. Automation workflows are available across the solution, enabling partial or full automation of payment processes, including file ingestion, validation, signing, approval routing and report distribution, while retaining human approval where required.

Operational monitoring, reporting and audit

The platform provides extensive operational reporting and monitoring capabilities. Users can access real-time and historical views of submissions, including status, totals, processing dates and detailed line items where retained. All actions are logged in a tamper-proof audit trail that records who performed each action and when, providing strong evidential support for internal and external audits. Reports can be exported in common formats and filtered by a range of criteria. Alerts and notifications inform users of outstanding actions, errors or exceptions, ensuring timely intervention where required.

Security and compliance

Security is embedded by design and by default across the Paygate service. The platform is developed and maintained in-house using a controlled Agile development lifecycle and OWASP secure coding practices. Paygate is ISO 27001 certified and Cyber Essentials Plus certified, with an Information Security Management System aligned to ISO 27001:2022 principles. The service operates within Amazon Web Services using a multi-availability zone architecture, with infrastructure aligned to recognised security standards and independently audited. Data in transit is protected using TLS encryption, and data at rest, including backups and replicas, is encrypted. Continuous monitoring, logging, vulnerability scanning and external penetration testing are performed, and access to customer data is strictly controlled, logged and audited on a need-to-know basis.

Data protection and privacy

Customers remain the data controllers for all payment and customer data processed within the platform, with Paygate acting as data processor. Personal data is processed solely for the purpose of delivering the contracted services and is not shared with third parties or used for marketing. Data is logically segregated between customers. The platform supports configurable data retention policies, secure deletion, and GDPR tooling to support subject access requests and the redaction of historical payment data where no longer required. Data handling and disposal processes are aligned with recognised standards and internal data protection policies.

Business continuity and resilience

The service is designed to be highly resilient, with automated failover across multiple AWS availability zones and continuous monitoring of system health. Paygate maintains formal business continuity and incident response frameworks aligned to ISO 27001, ensuring rapid response and recovery in the event of disruption. Customers are kept informed through defined communication channels, including a public service status page. The optional Goldstar contingency service provides additional assurance by enabling continued payment processing during exceptional scenarios.

Integration and interoperability

The platform is designed to integrate easily with existing customer systems. Secure APIs provide programmatic access to validation services, submission management, approvals and report retrieval using OAuth2 and OpenID Connect. SFTP integrations can be scheduled and automated, supporting high-volume and lights-out processing models. This enables organisations to embed Paygate into their existing operational workflows without major changes to upstream systems.

Exit and portability

Paygate supports customers throughout the full service lifecycle, including orderly exit and data portability. During the term of the contract, customers can access and export operational reports, submission summaries, audit logs and supporting information using built-in reporting and export functionality. At the point of contract termination, Paygate will work with the customer to agree an exit plan that minimises operational risk and disruption. Customer data is retained only for the agreed contractual and regulatory retention periods and is securely deleted thereafter in line with Paygate's data retention, handling and disposal policies and recognised standards for secure media destruction. Where required, Paygate can provide confirmation of data deletion. Exit processes are designed to ensure continuity of service, clear handover and compliance with data protection obligations.

Public sector suitability

Paygate Enterprise is well established within the UK public sector and is used by local authorities, housing bodies, shared service centres and other publicly funded organisations to process large-scale, business-critical payment operations. The platform is designed to align with public sector expectations around security, governance, auditability and resilience, including strong segregation of duties, tamper-proof audit trails, robust access controls and transparent reporting. Paygate's long-standing experience with public sector customers ensures familiarity with procurement, audit and compliance requirements, while the non-transactional pricing model and scalable cloud architecture support long-term financial planning and service stability.

Pricing approach

Pricing for Paygate Enterprise is subscription-based and modular, aligned to the number of users, organisational groups and the functional modules required rather than transaction volumes or payment values. This approach provides predictable and transparent costs, enabling public sector organisations to scale usage, increase payment volumes or expand services without incurring unexpected per-transaction charges. Optional services, such as bureau submission, validation modules or extended support, can be added as required, allowing customers to tailor the service to their operational needs while maintaining budgetary control.

Accessibility

The service is delivered through a modern, web-based user interface accessible via standard supported browsers, with no requirement for specialist hardware for normal operation. Accessibility considerations are incorporated into the ongoing design and development of the platform to ensure it can be used effectively by a broad range of users across finance and operational teams. The browser-based delivery model supports flexible working arrangements and reduces barriers to access, while consistent layouts and workflows help users perform tasks efficiently and accurately.

Service updates and roadmap

Paygate Enterprise is provided as a fully managed service, with enhancements, security updates, performance improvements and regulatory or scheme-driven changes delivered as part of the subscription at no additional cost. Updates are planned and deployed in line with Paygate's controlled change management and release processes, with a focus on minimising customer impact. Customers are informed in advance of material changes through release notes and service communications, ensuring transparency and allowing organisations to plan accordingly. Continuous improvement is informed by customer feedback, regulatory developments and evolving security threats, ensuring the service remains current, compliant and fit for purpose over time.

Benefits and outcomes

The Paygate Enterprise platform provides secure and compliant processing of Bacs Direct Credits, Bacs Direct Debits and Faster Payments, supports high payment volumes without transactional pricing penalties, and offers optional use of a Bacs Approved Bureau. Integrated validation and Confirmation of Payee checks reduce fraud risk and improve data accuracy before payment initiation. Granular permissions and secure workflows ensure that only authorised personnel can access or approve payment activity, enforcing consistent processes across finance teams. Automation reduces operational workload, while comprehensive reporting and audit trails provide clear visibility, control and assurance for public sector and regulated organisations.