

G-Cloud15

Service Definition

Access PaySuite – Secure Card Payment Gateway (SCP) for local government, housing, health and education

Contents

1	Service Overview	3
2	Onboarding.....	5
3	Additional Service Options	7
4	Service & Support Management Details	8
5	Account Management & Customer Success	10
6	Backup and Disaster Recovery	11
7	Business Continuity statement/plan.....	12
8	ISO27001 Accreditation.....	12
9	Development Life Cycle	12
10	Technical Requirements	13
11	Service Constraints	13

1 Service Overview

Access PaySuite ("PaySuite") is a PCI Level 1 payment service provider and is ideally positioned to help your organisation succeed in delivering a programme of change by simplifying income streams through the unification of payments and income management services. PaySuite offers a flexible, secure and compliant payments platform for customer-present, customer-not-present and self-service payments that can scale with your needs.

As an organisation that processes card transactions and with the UK implementation and introduction of GDPR and Data Protection Act 2018, card payment data is now classed as 'personally identifiable' and, as such, must be processed and secured to the highest standards. This, coupled with the Payment Card Industry Data Security Standards (PCI DSS), can place a large amount of strain on costs to your organisation.

PaySuite can help to reduce your scope of PCI and GDPR by -moving card data from your systems into our fully hosted and managed PCI Level 1 certified infrastructure

The PaySuite Secure Card Portal Gateway supports (primarily) online card payments, with a front-end form or system capturing customers' details and the goods or services they are paying for. It provides card entry and authorisation through seamless integration. Alternatively, via an API, front-end captures card details and this solution carries out purely authorisation and settlement.

The PaySuite Secure Card Portal gateway gives a single integration point to access a suite of online payment services, that include the following payment methods.

- Credit card
- Debit card
- Tokenisation for Planned or Recurring Payments
- Visa Click to Pay
- Apple Pay
- PayPal
- Direct Debit (see section 3 Additional Service Options)
- Optional Open Banking (see section 3 Additional Service Options)

A number of other Alternative Payment Methods are available from PaySuite.

How it works

The interface uses a combination of B2B web service calls and browser redirects to allow data and control of the browser to be passed from the client application to the PaySuite Secure Card Portal gateway and back again. The typical flow of a transaction is as follows:

The interface uses a combination of B2B web service calls and browser redirects to allow data and control of the browser to be passed from the client application to the PaySuite Secure Card Portal gateway Gateway and back again. The typical flow of a transaction is as follows:

1. The client makes an “invoke” web service call, providing details of a payment and / or store card transaction that it requires the PaySuite Secure Card Portal gateway to process.
2. The PaySuite Secure Card Portal gateway validates the request, starts a new transaction, and returns a response containing two items of data:
 - A unique identifier for the transaction
 - A URL to which the user’s browser should now be redirected. (This URL points to a location within the PaySuite Secure Card Portal gateway web application.)
3. The client redirects the user’s browser.
4. On receiving the redirect, the PaySuite Secure Card Portal gateway:
 - Retrieves the transaction (which is identified by a key within the redirect URL)
 - Processes the transaction, displaying pages on the user’s browser and prompting for input as necessary
 - Stores the result of the processing (success, card declined, etc)
 - Redirects the browser back to the client application. (The redirect URL is specified by the <returnUrl> element in the original request.)
5. The client makes a “query” web service call to the PaySuite Secure Card Portal gateway, inputting the request identifier that was returned in step 2.
6. The PaySuite Secure Card Portal gateway retrieves the transaction status and returns it.

Service description

Supports online card payments for third party solutions with a front-end form or system capturing the customer’s details and the goods or services they are paying for. It provides card entry and authorisation through seamless integration via API we services. Customers to make self-service payments online 24 / 7 for both invoiced and non-invoiced services using their credit or debit card, with optional Alternative Payment Methods including Open Banking as well as wallets (Apple Pay, Google Pay, Visa Click to Pay).

Service benefits

- Increase collection rates through your third-party online solutions
- Hosted in a PCI DSS data centre, removing PCI implications
- Removes card data from your organisation’s infrastructure
- Supports the latest card security measures
- Enables organisations to have a single corporate payment service
- Compliant to WCAG 2.1 standards
- Online card payments easily integrated with front-end systems.

Service features

- Supports payment by debit/ credit card online
- 3D Secure Strong Customer Authentication (SCA) validation (MasterCard SecureCode and Verified by Visa)

- Validation by card security code and address validation service
- Supports multiple funds / items within a single request
- Pages automatically presented in either desktop or mobile-friendly format
- Email receipt to payer and an internal address for notification
- Refunds and reporting available for the organisation's authorised employees
- Securely stores card details for quick retrieval on future payments
- Option to pay by PayPal or using Visa Click to Pay
- Gives flexibility through multiple methods, for example Pay and Store.

Service purpose

PaySuite Secure Card Portal gateway provides a real-time web service that will enable your third-party systems to interact with customers before linking to the PaySuite fully managed and hosted card forms, where customers enter their card details to make a payment with the option to pay using Alternative Payment Methods including Open Banking as well as wallets (Apple Pay, Google Pay, Visa Click to Pay) and to set up an online direct debit. Payment updates are passed back in real time, enabling onward processing.

2 Onboarding

Access Implementation Methodology (AIM)

Our consultants follow a 4-phase, 12-step process and we propose a scale of project, management and administration that's appropriate for your specific needs. From evaluation, planning and design, through to implementation of your business solution.

Phase 1, Pre-project planning

Step 1: Needs analysis

After detailed consultation we will clearly define your needs in a proposal document that identifies the benefits you will experience by updating your systems.

Step 2: Solutions demonstration

We will take you through a tailored demonstration of your proposed solution and work with you to agree which elements will be included in the initial project. We listen and take account of all your feedback and will provide a quotation outlining the anticipated cost of your project

Step 3: Sales handover

Having finalised the project's scope and agreed commercial terms, we prepare a handover document from sales to the project team who will partner you throughout implementation. They will meet with all appropriate members of your team to ensure continuity throughout the process.

Phase 2, Configure & Install

Step 4: Definition

The Access project team will work with you to define the structure and control processes that will guarantee the success of your project. Documents that we provide you at this stage will cover all your project objectives, the full specification and success criteria. This gives total clarity over individual tasks and responsibilities to ensure you're fully informed going forward.

Step 5: Solutions workshops

This step helps your project team become fully immersed in the proposed software. We map business processes to functionality so that you can understand how the solution will look and feel.

Step 6: Confirmation of requirements

Following your feedback from the solutions workshops, we will confirm the detailed actions and solution components necessary to meet the project success criteria we identified earlier.

Phase 3, Training

Step 7: Configuration

The components identified in Step 6 are delivered and a User Acceptance Test (UAT) system is built ready for you to carry out a pilot test. We configure and tune all the variables within the system to match your specific requirements.

Step 8: User Acceptance Test (UAT)

The UAT is conducted in a workshop environment for your staff against an agreed test plan. At the end of this step you will be ready to go live.

Step 9: Education

With a fully designed, installed and tested system now in place, we will train your staff on all relevant areas of the software. We are highly skilled at adapting our training to the learning styles of each of your staff members. We can train all of your staff or, if preferred, we will train your in-house trainers.

Phase 4, Support

Step 10: Go Live

The test system is converted into a live working environment ready for the processing of real-time business transactions. This is managed by a pre-agreed go live check list to ensure all possible circumstances are considered and addressed. We will be available to answer your questions and support your users throughout this time, helping them to get maximum clarity and impact from the software as they become increasingly confident.

Step 11: Support handover

We prepare a handover document and deliver it to our ongoing support team. This document contains all the information our support consultants need to answer any future queries you may have.

Step 12: Post project review

Your experience is extremely important to us. Shortly after you go live we will request feedback on your experience of the implementation process to help us further refine our delivery processes. We then agree sign-off for the project.

3 Additional Service Options

The table below highlights the additional value added services that our consulting teams can provide. Please take some time to review these.

Open Banking	Open Banking is revolutionising the way customers and consumers make payments. It allows individuals to pay directly by bank transfer from their bank to another business or organisation's account. Open banking payments offer a fast and secure way to make transactions without the requirement to input card details. Customers can conveniently select their bank from a list and authorise their purchase, streamlining the payment process. This method not only enhances speed and security but also provides a seamless and efficient way to conduct financial transactions. The use of open banking payments facilitates quicker fund transfers, reduces the risk of errors and fraud, and simplifies the payment process for both consumers and businesses. Additionally, this method empowers users to manage their finances more effectively and gain greater control over their transactions.
ELMS Portal	European Licensing portal for online payments linked to the PaySuite payment gateway
Direct Debit	Access PaySuite is a Bacs approved bureau and with this additional option, can facilitate the creation of Direct Debit mandates using our Direct Debit and Credit Management System (DDCMS).

4 Service & Support Management Details

Raising a Ticket

When contacting the Service Desk about any issue, you will need to provide as much information as possible including:

- Identify yourself
- The users, businesses or customer name this is affecting
- The specific product(s) affected
- The release version you are on including Service Packs or Hotfixes
- What impact this is having on your business in real terms e.g. deadlines
- Environmental issues that may be contributing factors
- A reference number (if calling about an existing matter)

As much detail as possible about what you are reporting including:

- Error messages (and the steps taken which cause the error message to appear)
- Time/date when these errors occur(ed)
- If the issue is intermittent or replicable, has this occurred more than once?
- Screenshots
- Which environments are affected e.g. Live/Test?. We will always strive to resolve your query immediately, but sometimes a deeper level of investigation is required. The time required to do this will depend on the complexity of the issue and the factors involved. It may be necessary to ask you a few questions in order to establish additional information or even to request a copy of some data for further investigation. While your case is being investigated, you can expect regular contact, with higher frequency depending on its priority.

Changes to a case status may be made in the following circumstances:

- Where you have been asked to provide further information, to test software, or to undertake any other action
- Where you or a third-party support agency has returned the case to PaySuite the severity will be re-assigned as deemed necessary.
- Where the significance of the fault diminishes, either because of partial fix or elimination of some elements, the case category may be downgraded.

How we intend to resolve your issues?

Software Defects

If we determine that a problem or fault reported by the customer relates to PaySuite software, we will attempt to provide a solution. The solution may take the form of additional corrective software or an updated version of PaySuite software in which the problem has occurred. We will use reasonable endeavours to provide a full resolution when the next version of the relevant PaySuite software is released. Incident resolution may take different forms e.g. advice, workaround or upgrade to later version – regardless of whether this version is released yet.

When will you respond to me?

We aim to resolve cases according to their Priority, usually with the most Urgent

and Impactful cases being addressed first. The following is the Key Performance Indicator we use to target how quickly we aim to resolve an Incident or escalate it as a problem.

*Target resolution time excludes delivery of product or software resolution.

Priority	Target Response Time
1	1 Hour
2	2 Hours
3	1 Working Day
4	2 Working Days

Priority	Target Resolution Time
1	4 Hours
2	1 Working Day
3	5 Working Day
4	10 Working Days

Priority Level	Examples
Priority 1 – System Down	A service interruption which has a critical impact on the activities of the authority; causes significant financial loss and/or disruption to the authority or results in any material loss or corruption of authority data.
Priority 2 Critical	A service interruption which can or could have a major (but not critical) adverse impact on the activities of the authority and no workaround is available.
Priority 3 - Major	A service interruption which has a major adverse impact on the activities of the authority which can be reduced to a moderate adverse impact due to the availability of a workaround.
Priority 4 - Low	Service or change request

Service Levels

Availability

Monthly Availability Target = 99.95%

3 Month Rolling availability Target- 99.95%

% availability of each managed service component is calculated as follows:

$$\frac{\text{Total Agreed Availability Hours} - \text{Unscheduled Outage Hours}}{\text{Total Agreed Availability Hours}} \times 100$$



Notes

Total Agreed On-line Availability Hours is defined as 7 days by 24 hours minus any agreed scheduled maintenance periods.

Service outages caused by other service providers are excluded from this target e.g. loss of internet connection and other telecoms failures and links to 3rd parties.

Alerts

We intensively monitor our service 24*7 with real-time alerting of any problems with the service.

If a service-affecting issue is identified during business hours, a service notification email will be sent out to your list of company contacts, advising of the issue and any subsequent updates pertaining to the issue. It is important that you supply and keep us updated with a list of contacts – you can do this by contacting the Service Desk.

Notifications

At PaySuite, we aim to provide our customers with accurate information, advice and guidance regarding service and product related changes under the form of notifications.

These may be:

- New releases, software upgrades or weekly maintenance related work;
- 2-4 weeks' notice on changes that may impact your integration and require you to operate specific changes on your systems;
- Scheme, Vendor or Acquirer changes that may impact you;
- New products or changes to existing PaySuite products.

Scheduled Maintenance

As we are continually improving our service, we have scheduled a regular maintenance window to ensure any scheduled upgrades or infrastructure changes take place at a time you can expect and prepare for.

Our maintenance window is the 3rd Sunday of every month between 04:30am and 06:30am. Whilst we strive to minimise any impact to clients during this time, please be prepared for potential intermittency while system changes are implemented.

If we need to make urgent changes, for example related to security or performance, outside of this window which we feel may impact your service, we will notify you as soon as possible, and aim to provide 48 hours' notice wherever possible.

5 Account Management & Customer Success

With over 160,000 customers using products supplied by the Access Group we have a large team involved with ensuring that our customers are able to build on their investment with Access.

This includes the Customer Success team who are specialists in specific products whose role is to ensure that our customers on Standard and Premier Success plans benefit from

educational webinars to ensure that you are always taking advantage of new functionality and most importantly continuing to adopt best practice in the day to day use and set up of the software.

Our Account Management team work with our customers specializing in vertical sectors or specific products. Depending on the complexity of the customer these are either office based using the latest technology to provide our customers with the highest possible levels of service or will visit sites for face to face meetings.

Our Account managers work with you keeping our customers informed on the way emerging technologies can help their business. They prepare briefings on the business, technical and financial benefits of technology and collaborate with customers to ensure the customer is aware of the breadth of software and support that Access can provide.

6 Backup and Disaster Recovery

PaySuite utilises multiple data centres that host our systems, this is to separate PCI data and environment. Our Disaster Recovery (DR) solution(s) are based on Primary and Secondary datacentres where all data is replicated from Primary to Secondary for DR. PaySuite also has backup/storage clusters in each datacentre running HYCU backup software for data backups away from the payment clusters, resulting in data being in 4 locations for increased resiliency. Backups are also stored offsite and are SAN stored so involve no physical devices.

In the unlikely event that the primary datacentre goes completely dark, an investigation period will be undertaken to determine the cause and decide if a datacentre promotion is required to make the secondary datacentre the primary one.

In the event of a disaster, PaySuite shall:

- Recover data stored off site
- Recover the service at the nominated disaster recovery site
- Procure and implement, at the expense of PaySuite, other equipment necessary to supply the service
- Aim to, where possible, provide a minimum service within 24 hours
- Provide a fully functional system as soon as is logistically possible.

Backups

- Synchronised high availability primary and secondary sites
- Two separate dedicated backup clusters (HYCU)
- Database mirroring – real-time synchronisation
- Hourly database logs
- Daily full database and files system/server

Backup Retention

- Daily for 1 week
- Weekly for 1 month
- Monthly for 3 months

Restores

- Recovery Point Objective (RPO) – <5 seconds
- Recovery Time Objective (RTO) – 2 hours core systems; 4 hours non-core systems

NB/ Targets for the restoration of the service do not apply in the event of a customer site disaster such as loss of equipment or premises.

7 Business Continuity statement/plan

The Access Group's full and most up to date business continuity plan can be requested by emailing buyer.enablement@theaccessgroup.com

8 ISO27001 Accreditation

The Access Group holds ISO27001:2022 accreditation across the entire organisation. This independently verified certification demonstrates our commitment to protecting your data. Maintaining this accreditation requires us to demonstrate effective security controls, regular staff training, and documented processes that are tested through independent annual audits.

9 Development Life Cycle

As one of our core products PaySuite has a detailed roadmap of improvements driven both by customers and by our own roadmap. Ongoing development against each application is supported by a development plan that has high levels of details for the next 3 months including user stories. Beyond that top line plans are in place by quarter for a further 12 month with a list of additional options waiting to be added.

There will always be a requirement to continually improve and enhance our products. Part of this can also mean products will reach end-of-life and be decommissioned. These outcomes are recognised as having different drivers, all of which are taken in to consideration:

Business-led:

- Legislative changes (including safety and security)
- Strategic business decisions
- Technological advances

Customer-led:

- Requests from individual customers
- Requests from User Groups

10 Technical Requirements

- End customer access via HTTPS:// over the internet
- Supports industry-standard browsers
- Organisation connections into our service are by public internet using TLS in line with PCI guidelines
- End of Day files are provided in a CSV format.

The PaySuite Secure Card Portal Gateway interface is designed to meet the following requirements:

- Use an industry standard web-service interface
- Provide a minimal request format for simple payment requests, but allow this to be extended with further information (such as line items and delivery details) if required
- Support local authority specific data (for example fund code) but do not require it to be provided. This will ensure that existing portal customers can switch to the SCP without loss of functionality.

Secure environment

All card details are stored behind a firewall with data access limited to dedicated support staff only. There is no sensitive information held at the data centre so that, in the unlikely event of someone breaching the system, they would not be privy to any information about customers. PCI DSS-certified, the multi-site data centre has passed the strictest of tests beyond the industry standards to ensure card data is stored securely. PaySuite provides its services from a PCI DSS Certified Level 1 data centre.

Other protection within supplier network

Applications in the DMZ pass data over SQL direct connections and HTTPS to the authorisation service and the SQL server. We protect the data by ensuring that this traffic is only internal to the network and not externally accessible or transmitted; our internal PCI network is 'ring fenced' from all other users' network traffic.

11 Service Constraints

Maintenance windows as detailed above are minimal with the service so that we use all reasonable efforts to ensure that the SaaS Services are available for 99.70% of each calendar month.

As a true SaaS solution customisation is not available although the product can be configured to meet all standard set up requirements.