Infraxis

PayStorm

Financial Processing

Infraxis

PayStorm

Financial Processing


API
PayStorm

The diversity of today's retail landscape where customers expect fast and reliable services across multiple channels and where payments are made using cards, apps and online accounts, is a mix of challenges and opportunity for participating businesses.

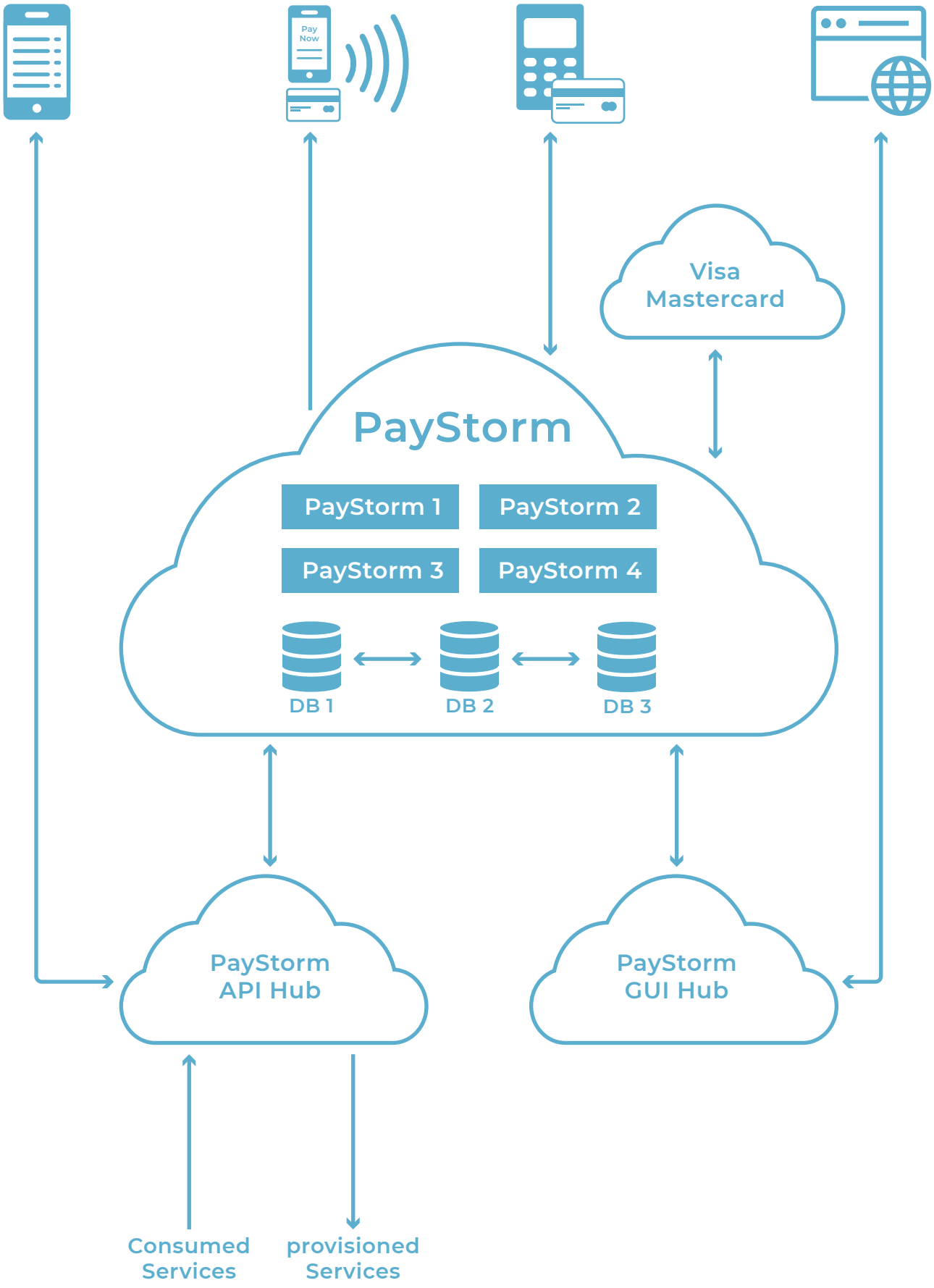
PayStorm is helping Infraxis customers to keep ahead of the latest industry trends by enabling rapid delivery of new services with the minimum of effort.

Delivering modern customer facing services within acceptable time frames doesn't necessarily require replacement of existing solutions. PayStorm can encapsulate legacy systems, enabling businesses to extract further value from existing technical investments, while presenting exciting new services to customers.

PayStorm offers a range of financial solutions including

- Credit, prepaid, debit and fuel card authorisation
- Mobile-First customer app management, onboarding and KYC
- Fuel card issuance, acquiring and switching
- Immediate Payment switching
- Service API management

:


Pay Now
Visa
Mastercard
PayStorm
PayStorm 1
PayStorm 2
PayStorm 3
PayStorm 4
DB 1
DB 2
DB 3
PayStorm
API Hub
PayStorm
GUI Hub
Consumed
Services
provisioned
Services

Microservices and Workflows

PayStorm is an omni-channel solution built upon the Infraxis Service Grid, where transactions are processed using microservices and workflows.

PayStorm channels process transactions using specific protocols built on standards such as ISO 8583, ISO 20022, JSON, XML and SOAP.

Channel services support a specific protocol and select the correct workflow to provide designated business functions.

Workflows can consume services provided on PayStorm as well as those provided by third-parties, making it quick and easy to support collaborative business approaches, where components of an offering are provided by multiple organisations.

Examples of existing business functions provided PayStorm's workflows include financial authorisation, financial product management, reformatting transactions and switching, app management, Immediate Payment connectivity, customer signup, identity and address verification, POS acquiring and fuel card payment processing.

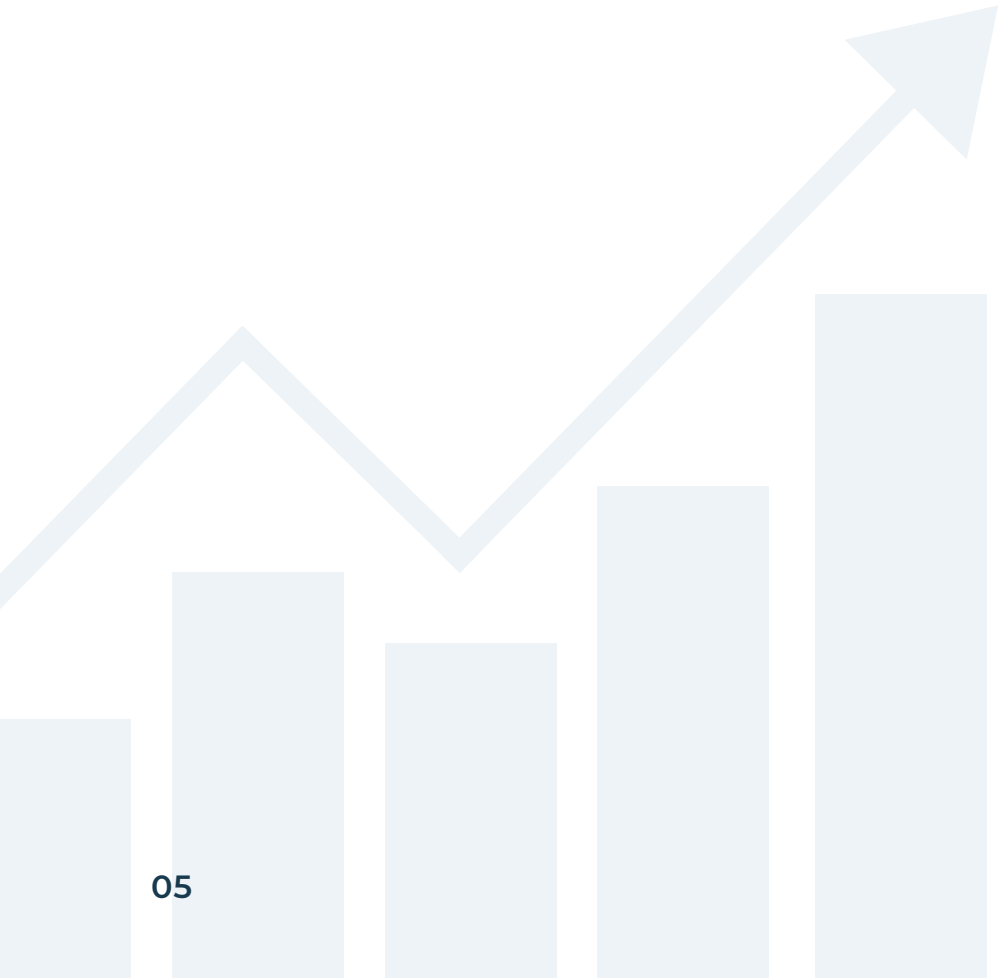
Elastic Scalability

As PayStorm operates within a virtual processing cloud, configurations can seamlessly span multiple servers where containers are loaded to support designated services. PayStorm uses JDBC database access, so databases can be selected based on vendor preference and deployed using clustered configurations to meet the relevant processing requirements.

The number of copies of each mircoservice used to deliver a business function is configured to ensure that processing times and overall throughput remain within the designated service levels.

Additional microservices can be added to the configuration while PayStorm remain in operation, providing targeted increases in processing power.

PayStorm self-monitors its performance and supports dynamic load balancing for true elastic scalability.



Business Continuity

PayStorm provides the non-stop technical platform for non-stop financial businesses. Applications and databases are deployed on securely clustered servers that normally span multiple physical locations. Unrestricted numbers of replicated services and replicated databases can exist within the configuration.

Data replication between database instances can be provided by the database vendor or alternatively, PayStorm provides native replication for use when vendor options are unavailable.

PayStorm fully utilises the available service configuration, with all services within the cluster being considered active. There is no need for any backup or redundancy, but the configuration will consider infrastructure deployment to achieve non-stop processing.

Elements of a suitably configured PayStorm cluster can be removed for scheduled maintenance without any loss of service whatsoever. Should a network, server or even a complete data centre fail for any reason, then PayStorm will continue delivering the business using the remaining configuration. When an infrastructure outage has been addressed, the expected PayStorm components are brought back online, again with no interruption to the ongoing processing.

Furthermore, as each step within a workflow can have an alternative action for use if the expected step cannot be completed, non-stop characteristics can be built in at the functional level too.

API Management

PayStorm makes both exposing APIs and consuming services over APIs a very simple process. Using PayStorm's API management dashboard, APIs can be defined, secured and the supporting workflows configured dynamically.

Exposed APIs enable businesses to open up services for consumption by external partners and internally across the enterprise.

External APIs can be configured for use in workflows when including services provided by partners and external systems.

Permanent & Stand-in Financial Authorisation

PayStorm can provide financial authorisation functions that operate using its highly adaptable internal account configurations or transactions can be switched out for external authorisation.

Stand-in authorisation against preconfigured limits can also be provided by PayStorm, if the expected external authorisation service is unavailable.

Flexible Financial Products

PayStorm's highly adaptable financial product configurations can support any method or technology used to conduct financial transactions, including payment cards of any form factor, apps, accounts and tokens.

Financial products are defined through the PayStorm configuration dashboard, where the product type, associated workflows and default usage controls are configured. Transactions associated with each product type are configured to make them uniquely identifiable when processing, using methods such as BIN ranges, AIDs or any combination of content from within the transaction data.

Multipurpose Customer Accounts

Any aspect of customer data can be securely held to exactly match the requirements of any business case.

Customer account data can be held for both individuals and companies. Accounts can be linked to form relationships and hierarchies, such as family groups and corporate structures.

Financial authorisation can utilise funds and consider limits present within all types of account structure, allowing PayStorm to support a very wide range of customer combinations. For example, company limits, department limits and individual limits can all be considered when processing within a corporate hierarchy.

Customer data can be entered through exposed APIs, over the customer management dashboard or through a batch load mechanism.

Financial Accounts

Financial accounts are attached to a specific customer account when a financial product is issued to that customer. Financial accounts may hold balances for both credit and debit products, together with any personalised usage limits applied to the specific customer.

PayStorm provides enormous flexibility for defining customer bases, where a single customer can have multiple financial accounts, each having limits and balances managed individually or in combination with other accounts.

Financial Instruments

Any number of financial instruments can be attached to a single financial account and these represent the payment cards and tokens used to access that specific account.

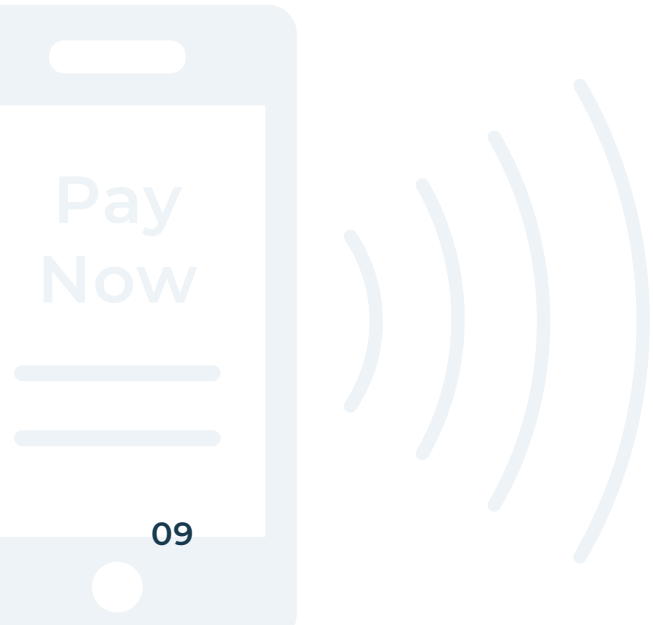
Instruments can be controlled, issued and replaced discretely, without impacting the financial account or any associated limits and balances.

The financial instrument object contains data specific to the instrument type, for example, EMV issuance data.

PayStorm manages instruments over the full lifecycle, for example, card issuance, shipping, activation, blocking due to loss, theft or fraud, expiration, replacement cards and temporary card issuance are all supported events.

Instrument lifecycle events can be managed through PayStorm's customer dashboard or by external systems, for example, card management and fraud management solutions.

Being PA-DSS certified, PayStorm manages all PCI relevant data to meet stipulated PCI rules, including SAD storage and key management.



Customer Onboarding & KYC via Apps

PayStorm simplifies the process of customer onboarding by providing APIs to support the direct signing-up of customers and KYC processing. Customer data is simply added using mobile-first app solutions, where the necessary data is captured and verification processes are performed following standard workflows. PayStorm supports document uploading, online identity checks and the setting up OAuth delegated access.

With data entry and customer verification complete, PayStorm can also automatically issue financial products to new customers. Issuance can involve loading tokens on to mobile devices and embossing standard cards.

Apps make use of these standard PayStorm features by consuming exposed APIs.

Issuer & Acquirer Card Scheme Support

PayStorm processes both issuer and acquirer transactions on the Visa and Mastercard networks. There are numerous options available on each network which are selected based upon the type of card products being managed or processed.

Settlement with the card scheme can either be processed directly through PayStorm or it can occur on an external system, with relevant data being exchanged with PayStorm.

EMV & SECCOS

PayStorm fully supports EMV and the German SECCOS card standards, including scripting and PIN management. Embossing data can be generated for these card types when required.

VISA & Mastercard Token Provisioning

PayStorm fully supports Visa VTS and Mastercard MDES tokenisation. Step-up authentication is defined to meet the issuer's requirements and this can include SMS messaging, email and call centre options using data held on PayStorm.

Tokens are linked to an underlying card, allowing card lifecycle events to be reflected on the attached tokens in keeping with card scheme rules.

PayStorm can process all tokenised card channels including Apple Pay, Android Pay, Google Pay and Samsung Pay.

Fuel Card Issuance & Authorisation

PayStorm manages fuel cards within its standard financial instrument framework. The control of product codes has been implemented generically, allowing each fuel scheme to select its own codes.

Full authorisation of fuel card transactions can be supported against PayStorm's financial accounts or alternatively, transactions can be preprocessed and switched out for financial authorisation by the issuing scheme.

Multiple fuel related protocols are supported, such as IFSF and EP2 Fuel, enabling PayStorm to acquire, authorise, preauthorise and switch fuel based transactions regardless of the technologies involved.

Fraud Protection

PayStorm provides “stop” and “go” list management for controlling the authorisation and switching of transactions. These control lists can be updated via exposed services, using the PayStorm configuration dashboard or through a batch load mechanism.

Usage of instruments and accounts can be tracked and managed by external fraud management services. PayStorm supports realtime fraud scoring and can post transaction data to external fraud management solutions for inclusion in data models.

Instruments and accounts can be temporarily or permanently blocked based upon responses from integrated fraud management services.

Automatic blocking of instruments can be applied by PayStorm when certain events occur, for example, a number of incorrect PIN entries.

Manual blocking of accounts and instruments can occur through PayStorm’s customer dashboard or through APIs attached to external customer helpdesk facilities, self-management portals and apps.

Merchant Onboarding & Management

PayStorm manages merchant bases consisting of small individual businesses through to large retail groups with national and international outlets.

PayStorm offers merchant onboarding through workflows that cover the initial signing up of new merchants, document uploading with secure storage and online verification checks.

Merchant onboarding and management can be controlled via PayStorm's merchant dashboard, via API/network requests or via a batch load mechanisms.

PayStorm provides merchant configuration for all types of businesses with options to control accepted cards types, financial limits, default terminal configurations and cutover configurations.

Merchant Self-Management

Selected functions can be made available to the merchant directly over a PayStorm self-management portal, allowing merchants to view their transactions, manage chargeback events arriving from card schemes, manage maintenance requests and to update merchant controllable configurations.

Terminal Management

Multiple payment terminals types can be configured for any merchant, with each possessing varying capabilities and controls. New terminal types can be added with ease to the existing portfolio which includes indoor and outdoor fuel terminals, virtual terminals and SmartPos devices.

Terminal configuration parameters can be applied at the terminal level to override or supplement default merchant level configurations.

Terminals are managed throughout the full lifecycle, from initial ordering to the return for decommissioning. Where terminals are managed by third-party service providers, PayStorm enables ordering of new or replacement terminals and general service requests over the merchant dashboard. Requests can be forwarded to terminal management service providers either by automated email or via APIs.

PayStorm fully supports the EP2 acquirer protocol, including COI for dynamic merchant and terminal configuration via the service centre.

Get in Touch

Please contact us to learn more about PayStorm and the associated services from Infraxis.

Infraxis Switzerland
Thunstrasse 68
CH-3074 Muri bei Bern
Switzerland
Email: info@infraxis.com
Tel: +41 (0) 31 951 4011

Infraxis United Kingdom
Suite 20, 6 – 8 York Place
Leeds
LS1 2DS
Email: uk@infraxis.com
Tel: +44 (0)113 451 0151

www.infraxis.com