Payter's Information Security Risk Management (ISRM)

Document Name: Payter's Information Security Overview	**Document Owner:** Cyber & Information Security Manager	**Effective Date:** 18-03-2026
Document No. PTR-00-03-PG-P-0007 **Document Classification:** Public	**Version:** 1.3	**Access List:** Read only access to employees, contractors, vendors and clients, as appropriate

Contents

1 Executive Summary

Payter operates a risk-based Information Security & Risk Management (ISRM) programme aligned with internationally recognised standards and sector-specific requirements, including:

- ISO/IEC 27001, 27002
- PCI DSS, PCI PTS, PCI PIN & PCI P2PE
- GDPR data protection principles
- RED Cyber (EN 18031) and
- ISO 9001 quality governance.

Security and quality are embedded into Payter's operating model across terminal design, development, manufacturing, provisioning, support, and operational management.

Payter's unattended payment terminals are PCI PTS-certified devices designed to securely capture payment credentials within the device's secure boundary and transmit protected transaction data for downstream processing.

Payter does not store, view, or expose clear-text cardholder data within the customer environment, the terminal management platform (i.e. MyPayter) and its supporting backend infrastructure, or Payter corporate IT environments.

Sensitive Authentication Data (e.g. PIN, CVV) is never stored after authorisation.

Payment authorisation processing, acquiring connectivity, card network routing, and issuer-side approval are performed by the payment processing partner and associated payment ecosystem participants, **outside the direct operational scope of Payter**.

Payter's role is focused on secure terminal operation, controlled device lifecycle management, and secure operational visibility through its management platforms.

2 Security Overview

2.1 Security Governance, Assurance & Risk Management

Payter maintains a structured Information Security & Risk Management (ISRM) framework that governs how security risks are identified, assessed, managed, and monitored across its business and technology. This framework supports consistent decision-making across product development, terminal lifecycle management, backend services, cloud infrastructure, and operational processes.

Security assurance is embedded throughout the lifecycle of systems and services. This includes architecture and design reviews to ensure security is incorporated at an early stage, structured risk assessments for new implementations and changes, and continuous vulnerability identification through scanning and penetration testing. These activities are complemented by compliance

validation, controlled change and release governance, and ongoing monitoring and incident oversight.

Risks are evaluated based on their potential impact and likelihood, and are managed through clearly defined treatment approaches such as mitigation, transfer, or formal acceptance. High-impact risks are escalated to management for visibility and oversight.

Importantly, risk management is not treated as a periodic or compliance-driven exercise, but is integrated into day-to-day operational processes and continuous improvement activities.

Control Summary:

- ✓ Defined ISRM framework governing security and risk management
- ✓ Formal risk assessment and risk treatment methodology
- ✓ Integration of security into architecture and design reviews
- ✓ Regular vulnerability scanning and penetration testing
- ✓ Compliance validation against applicable standards
- ✓ Controlled change and release governance
- ✓ Continuous monitoring and incident oversight
- ✓ Management escalation for high-impact risks
- ✓ Periodic ISRM Steering Committee review and oversight

2.2 Solution Architecture

Payter provides secure payment terminals for unattended and self-service environments such as EV charging stations, vending machines, parking systems, and other automated payment points. The Payter solution consists primarily of payment terminal devices, terminal firmware/software, communication interfaces, host integration mechanisms, terminal management infrastructure and supporting cryptographic key management processes.

The principal architecture components include:

2.2.1 Payment Terminal Devices

Payter terminals, including the Apollo family, are secure payment terminals designed to capture payment credentials and initiate payment transactions. These terminals support contactless payment technologies and operate as secure PIN Entry Devices certified under PCI PTS requirements.

2.2.2 Terminal Firmware and Software Platform

Each terminal operates using embedded firmware and payment application components responsible for transaction handling, communication protocols, security controls, terminal user interaction, and device integrity protections.

2.2.3 Machine / Host Integration Interfaces

Depending on deployment use case, Payter terminals may support integration with host machines or controllers through interfaces such as:

- MDB (Multi-Drop Bus)
- Payter Session Protocol over TCP/IP or serial connections
- pulse-based or free-pulse signalling
- cloud-based integration APIs and terminal communication models

2.2.4 Network Connectivity

Terminals may use Ethernet (LAN) or cellular connectivity, including optional 4G communication, depending on the installation environment. Active internet connectivity is required for transaction verification, secure communication, remote management, telemetry, and controlled configuration updates.

2.2.5 Terminal Management Infrastructure

Payter operates terminal management and customer visibility capabilities through MyPayter and associated backend services. These services support secure device configuration, firmware and software updates, operational monitoring, device lifecycle management, and visibility of operational transaction metadata. Cryptographic key management is governed through dedicated controlled processes described separately in the Appendix.

2.2.6 Payment Processing Boundary

It is important to note that payment processing functions such as PIN handling, authorisation, acquiring connectivity, and card network routing are performed by external Payment Gateway, PSP, or Acquirer systems. These functions remain outside Payter's direct operational scope.

Controls Summary:

- ✓ Segregated architecture components (terminal, backend, interfaces)
- ✓ Secure embedded firmware with integrity validation
- ✓ Controlled and limited host integration interfaces
- ✓ Secure communication channels for terminal connectivity
- ✓ Terminal management platform with controlled access
- ✓ Secure key management with controlled key provisioning, DUKPT-based transaction key control, and protection of root keys within HSM environments
- ✓ Clear separation of Payter scope vs external payment processing

2.3 Payter Terminal Security

Payter terminals are purpose-built to operate securely in unattended environments and to protect payment credentials within a controlled cryptographic boundary. Security is embedded at both the hardware and software levels.

Payter payment terminals incorporate built-in security event detection mechanisms. These include physical tamper detection controls designed to identify any unauthorized attempt to access or manipulate the device.
In the event of a tamper condition, the terminal automatically triggers a security response, including the immediate zeroisation of sensitive cryptographic key material stored within the device. The terminal then transitions into a secure inactive state and displays a security violation indication. Tamper events are treated as high-severity security incidents and are surfaced through operational monitoring processes where applicable, enabling investigation and appropriate response actions.

Secure cryptographic processing is performed within the protected security boundary of the device, ensuring that sensitive data is not exposed outside controlled cryptographic environments.

Additional protections include trusted boot processes that ensure only authorized firmware can run on the device, as well as restrictions on debug and service interfaces to prevent unauthorized access. Terminals are configured following least functionality principles, with unnecessary services and ports disabled. Firmware updates are controlled and require validation through signed or approved software mechanisms.

Controls Summary:

- Physical tamper protection and tamper detection
- Secure cryptographic processing and key handling
- Automatic key zeroization upon tamper event
- Trusted boot and integrity validation
- Restriction of debug interfaces
- Hardened device configuration
- Least functionality, including disabling unnecessary services and ports
- Signed or approved firmware and controlled software loading

Together, these controls ensure the integrity of the device, the protection of cryptographic material, and the secure handling of payment data.

2.4 Network Security & Connectivity Model

Payter implements a secure-by-design network architecture based on zero-trust principles, ensuring that communication between payment terminals, backend systems, and supporting infrastructure is tightly controlled, authenticated, and encrypted. The design does not rely on customer network security and instead enforces security controls at the device, platform, and infrastructure levels.

Network security controls are applied consistently across both terminal-level communication and Payter's managed cloud & corporate environments, with clear separation of responsibilities and control boundaries.

2.4.1 Terminal-Level Network Security & Connectivity

Payter payment terminals are designed to operate in untrusted and public network environments while maintaining strong security controls.
Terminals initiate all communication and operate under an **outbound-only connectivity model**, meaning that no inbound connections to the device are permitted. This significantly reduces the attack surface and prevents direct remote access to deployed terminals.

Communication from the terminal is restricted to **predefined and allow-listed endpoints and ports**, ensuring that the device can only interact with authorized backend services and payment processing infrastructure. Communication outside approved destinations and parameters is restricted by design and supporting network controls.

All communication between the terminal and backend systems is protected using strong transport encryption protocols, such as **TLS 1.2 or higher**, ensuring confidentiality and integrity of transmitted data. Where applicable, mutual authentication mechanisms may be implemented to ensure that both the terminal and the receiving system can verify each other's identity before establishing communication.

Terminal communication is limited strictly to required functions, including:

- transaction processing and authorisation requests
- device telemetry and health monitoring
- configuration updates and remote management instructions
- firmware and software update retrieval

The terminal does not expose any externally reachable services or open ports that could be used for inbound communication, thereby preventing unauthorized scanning, probing, or exploitation.
This architecture ensures that terminals can securely operate even in environments where the surrounding network cannot be trusted.

2.4.2 Cloud Infrastructure - Network Security

Payter backend systems, including MyPayter and supporting infrastructure, are hosted within secure cloud environments designed with layered network protection and segmentation.
The network architecture enforces **logical separation between internet-facing services and internal systems**, ensuring that publicly exposed components are isolated from sensitive backend services and data processing environments.

Security controls implemented within the cloud and backend environment include (not limited to):

- **Firewall controls** to restrict inbound and outbound traffic based on defined rules
- **Web Application Firewall (WAF)** protections for internet-facing applications to detect and block common web-based attacks
- **Secure network gateways and routing controls** to manage traffic flow between network segments
- **Network segmentation** to isolate application layers, management interfaces, and data processing components
- **Intrusion Detection and Prevention capabilities (IDS/IPS)** to monitor and detect suspicious or malicious traffic patterns
- **API gateway controls** where integrations require managed API access

All external communication into Payter-managed environments is routed through controlled entry points, where traffic is validated, filtered, and monitored.
Internal service-to-service communication is also controlled and restricted to only what is required for system functionality, reducing the risk of lateral movement within the environment. Network access between components is governed through controlled policies and service-level restrictions.

Traffic is continuously monitored through centralized logging and monitoring systems, enabling detection of anomalies, unauthorized access attempts, or unusual traffic behaviour. These controls support proactive threat detection and incident response.

Administrative access to cloud and operational systems is restricted through controlled access paths and protected through strong authentication mechanisms, ensuring that only authorized personnel can access systems required for their role.

2.5 Environment Segregation

Payter enforces strict segregation between Production and Non-Production environments to protect live services, ensure system stability, and support secure development and change processes.

This segregation is implemented through a combination of logical separation, controlled access mechanisms, and governed deployment procedures.
Production environments are dedicated to live service operation, including terminal management, transaction-related processing, and customer-facing platforms.

Non-Production environments are used exclusively for development, testing, validation, and pre-release activities. This separation ensures that development and testing activities do not adversely impact operational systems or customer services.

Logical segregation is enforced through network segmentation and controlled interfaces, ensuring that Production systems are isolated from Non-Production environments.

Access to each environment is strictly governed through role-based access control (RBAC) and strong authentication mechanisms, including Multi-Factor Authentication for administrative and privileged

access. Separate access paths and permissions are maintained to prevent unauthorized cross-environment access.

All changes are developed, tested, and validated within Non-Production environments before being promoted to Production. Deployment into Production is performed through controlled release and change management procedures, including approval workflows, validation steps, and rollback capabilities where required. This ensures that only tested and authorized changes are introduced into live environments.

Centralised logging and monitoring are implemented across both Production and Non-Production environments to provide visibility, traceability, and auditability of activities. Security-relevant events, administrative actions, and system changes are logged and monitored to support operational oversight and incident response.

This structured approach to environment segregation ensures that:

- development and testing activities remain isolated from live services
- access to environments is controlled and restricted to authorized personnel
- changes are validated prior to Production deployment
- activities across environments are monitored and traceable

2.6 Identity & Access Management

Payter enforces strong identity and access management controls across its systems, applications, infrastructure, and terminal management platforms to ensure that access to resources is restricted to authorized users and aligned with business and operational requirements.

Access to systems is governed through a centrally managed identity and access management framework, where permissions are assigned based on defined roles and responsibilities.

Role-Based Access Control (RBAC) is implemented to ensure that users are granted access strictly on a least-privilege basis, limiting access to only the systems and functions required for their role.

Authentication to Payter systems, particularly for administrative, remote, and sensitive access, is protected through Multi-Factor Authentication (MFA). This ensures an additional layer of security beyond standard credentials and reduces the risk of unauthorized access.

User access is managed through structured lifecycle processes, including joiner, mover, and leaver procedures. Access rights are provisioned, modified, and revoked in line with role changes and employment status. Periodic access reviews and recertification activities are performed to ensure that permissions remain appropriate and aligned with current responsibilities.

Credential management follows secure practices, including strong password policies, secure storage mechanisms such as hashing, and protection against brute-force attacks through controls such as rate limiting and account lockout after repeated failed login attempts.

All authentication events and privileged activities are logged and monitored through centralized logging mechanisms. This provides traceability and supports detection of unauthorized or suspicious access attempts, as well as audit and forensic requirements.

Remote access and operational actions are secured through controlled authentication mechanisms and governed workflows, ensuring that sensitive operations are performed only by authorized personnel under controlled conditions.

Payter-managed platforms, including MyPayter, operate within Payter's controlled identity environment. Integration with external customer identity providers is not required, as authentication and access management are handled within Payter's own managed infrastructure.

Payter's identity and access management controls ensure that:

- access to systems is restricted based on roles and least privilege
- strong authentication mechanisms protect sensitive and administrative access
- user access is governed throughout its lifecycle
- authentication and privileged activities are logged and monitored
- unauthorized access attempts are prevented and detectable

These controls collectively support secure system access, accountability, and compliance with industry security standards.

2.7 Secure Software Development & Change Management

Payter follows a structured Secure Software Development Lifecycle (SDLC) to ensure that security is embedded throughout the design, development, testing, and release of software components supporting payment terminals, backend platforms, and operational services.

Security requirements are defined and integrated at the earliest stages of the development lifecycle, ensuring that security considerations are incorporated into system architecture, application design, and feature development.

This includes controls related to data protection, authentication, access control, secure communication, and system resilience.

During development, secure coding practices are applied to reduce the risk of common application vulnerabilities. Developers follow established development standards and guidelines (e.g. OWASP secure coding practices), and security considerations are incorporated into implementation activities.

All code changes are subject to peer review processes to ensure correctness, security, and adherence to defined standards before being approved for further stages.

Security testing is integrated into the development lifecycle to identify and remediate vulnerabilities prior to deployment. This includes a combination of automated and manual validation approaches such as secure code analysis, application behaviour testing, and vulnerability detection techniques.

Identified issues are assessed, prioritised, and remediated through structured defect management processes.

As part of Payter's DevSecOps practices, security controls are embedded within development and release pipelines. This enables continuous validation of code quality and security posture, supports early detection of vulnerabilities, and ensures consistent enforcement of security requirements throughout the lifecycle.

Dependencies and third-party components used within software development are subject to controlled selection, validation, and monitoring processes. Known vulnerabilities in libraries, frameworks, or external components are identified through vulnerability monitoring and are remediated through updates, patches, or replacement as required.

This reduces exposure to supply chain and third-party software risks.
Testing and validation activities are performed in controlled Non-Production environments prior to any Production deployment. These include functional testing, integration testing, and security validation to ensure that software behaves as expected and does not introduce vulnerabilities or operational risks.

Prior to release, software is subject to defined security and quality gates. These gates act as Go/No-Go decision points and require that critical security, testing, and validation criteria are met before deployment into Production environments. This ensures that only validated and approved changes are introduced into live systems.

Segregation of duties is enforced between development, testing, and production environments to ensure that no single individual has uncontrolled ability to introduce changes directly into Production systems. Access to deploy or approve changes is restricted to authorized roles and governed through controlled processes.

Software releases are managed through defined change and release procedures, which include classification of changes (e.g., standard, normal, emergency), controlled approvals, and documented deployment steps. Releases are validated prior to deployment and are executed in a controlled manner to minimise operational disruption.

To ensure software integrity, firmware and application releases are cryptographically signed or otherwise protected against unauthorized modification. Only approved and validated software components are permitted to be deployed to Production environments and terminal devices.

For terminal devices, Payter applies additional controls specific to firmware lifecycle management. Firmware updates are securely developed, tested, signed, and distributed through controlled mechanisms. Terminals validate the integrity and authenticity of firmware before installation, ensuring that only trusted and authorized software is executed on the device.
For high-impact changes, rollback mechanisms and recovery procedures are defined to allow restoration to a known stable state in case of unexpected issues during or after deployment.

2.8 System Hardening

Payter implements system hardening and protective controls to reduce attack surface, prevent unauthorized access, and ensure secure operation of infrastructure, applications, and payment terminals. These controls are aligned with industry-recognised security benchmarks, vendor best practices, and internal security standards.

Secure configuration baselines are established and maintained for infrastructure, cloud platforms, applications, and supporting services. These baselines are developed with reference to recognised industry standards such as the Center for Internet Security (CIS) Benchmarks, as well as vendor-specific security guidance and platform best practices.

Configurations are regularly reviewed and continuously monitored to detect deviations from approved baselines or the presence of insecure settings. Where misconfigurations or weaknesses are identified, remediation actions are prioritised and implemented through controlled change and risk management processes.

System hardening measures are applied across different layers of the environment and include:

- implementation of secure baseline configurations for infrastructure, operating systems, and applications
- removal or disabling of unnecessary services, ports, and interfaces
- enforcement of least functionality and minimisation of exposed system components
- hardened firmware and embedded security protections within payment terminals
- protection of web-facing services through application-layer security controls where applicable
- endpoint protection and monitoring capabilities (e.g., EDR) for corporate systems and user devices
- validation and filtering of application inputs to prevent malformed or malicious data processing

In addition, software components, libraries, and dependencies are maintained through vulnerability and patch management processes to ensure that known weaknesses are addressed in a timely manner.

These hardening and protective controls are designed to ensure that systems operate in a secure state by default, limit exposure to potential threats, and provide resilience against unauthorized access, misconfiguration, and malicious activity.

2.9 Logging & Monitoring

Payter implements centralized logging, monitoring, and alerting capabilities across its systems, applications, infrastructure, and terminal management platforms to support operational oversight, security monitoring, auditability, and incident response.
Logging is enabled across all relevant system components to capture security, operational, and administrative activities. Logged events include, where applicable, authentication and access events, administrative and privileged actions, configuration changes, operational support activities, system and service health events, and transaction-related operational metadata required for reporting and monitoring.

Log records are designed to contain sufficient contextual information, such as timestamps, user identifiers, system references, and event details to support traceability, audit requirements, and forensic investigations.

Access to logging systems and log repositories is strictly controlled through role-based access control (RBAC) and strong authentication mechanisms, including Multi-Factor Authentication for administrative access.

Log data is protected against unauthorized access, modification, or deletion through controlled storage and access restrictions.

Monitoring capabilities are implemented to provide continuous visibility into system behaviour, service performance, and potential security events. This includes monitoring of system health, service availability, and operational performance, as well as detection of anomalies, suspicious activities, and inconsistencies in system or transaction-related data.

Automated alerting mechanisms are in place to notify relevant teams of identified issues or deviations from expected behaviour. Alerts are prioritised and managed through defined incident management processes, enabling timely investigation, escalation, and resolution of potential security or operational incidents.

These logging, monitoring, and alerting controls ensure that Payter maintains visibility over its environment, supports rapid detection of issues, and provides the necessary audit trail for compliance and forensic analysis.

Controls Summary:
Payter's logging and monitoring framework ensures that:

- security and operational events are comprehensively recorded
- logs are protected, access-controlled, and audit-ready
- system and service behaviour is continuously monitored
- anomalies and suspicious activities are detected
- alerts are generated and managed through structured processes

These controls support accountability, incident response, and compliance with industry security standards.

2.10 Cryptography

Payter uses industry-standard cryptographic controls to protect payment-related information during capture, transmission, processing, and storage of operational data.
Cryptographic protections are applied in line with the nature of the data and the system component involved.

Within the payment terminal, sensitive payment data is protected inside the secure cryptographic boundary of the device using PCI PTS-certified mechanisms, including Secure Reading and Exchange of Data (SRED), to prevent exposure of cardholder data outside the secure environment.

Data transmitted between terminals, backend services, and supporting platforms is protected using strong transport encryption, including TLS 1.2 / 1.3 or higher, to ensure confidentiality and integrity during transmission. Where applicable, secure endpoint authentication controls are used to restrict communication to trusted systems and approved interfaces.

For operational data retained within Payter-managed systems, such as transaction metadata and device management information, encryption at rest is applied using platform-standard strong encryption controls (eg. AES 256) together with strict logical access restrictions.

Cryptographic controls are designed to ensure that:

- sensitive payment data is protected at the point of capture
- data in transit is encrypted and integrity-protected
- operational data is protected at rest where stored
- cryptographic processing occurs only within trusted and controlled security boundaries
- clear-text Sensitive Authentication Data is never stored after authorisation

These measures support the confidentiality, integrity, and secure handling of payment-related information across the Payter environment.

2.11 Key Management

Payter applies controlled key management practices to support the secure use, provisioning, protection, and lifecycle management of cryptographic material associated with payment terminals and supporting environments.

Key management is governed through defined procedures covering:

- key generation
- secure exchange
- injection
- storage
- use
- rotation
- revocation and
- retirement

with segregation of duties and restricted access applied to sensitive cryptographic operations.

For transaction-related PIN protection, Payter terminals operate using DUKPT-based key management, ensuring that a unique cryptographic key is used per transaction.

Root cryptographic key domains remain protected within secure Hardware Security Module (HSM) environments operated by the relevant payment processing domain, while terminal-specific cryptographic material is securely provisioned into devices through controlled key-loading processes.

Payter's key management approach is designed so that:

- root cryptographic keys remain within certified secure cryptographic environments
- terminal key provisioning is performed through controlled and auditable processes
- cryptographic keys are protected against unauthorized access, disclosure, or modification
- transaction-level key usage limits the impact of compromise to individual transactions or devices
- plaintext PIN data is never exposed outside secure cryptographic boundaries

Detailed transaction-level key flow, DUKPT hierarchy, and HSM processing are documented separately in the Appendix.

2.12 Threat, Vulnerability & Patch Management

Payter operates a formal Threat, Vulnerability and Patch Management process governed through its ISRM framework.

Vulnerabilities are identified through multiple channels, including:

- automated vulnerability scanning
- ASV scans for internet-facing services where applicable
- penetration testing
- configuration reviews
- threat intelligence and advisories
- product, firmware, and infrastructure assessments

Identified findings are assessed based on severity, exploitability, asset criticality, and potential business impact. Remediation activities are prioritized accordingly and tracked through controlled operational processes.

Payter follows a risk-based remediation approach, with indicative timelines aligned to the severity of identified vulnerabilities:

- **Critical and High severity vulnerabilities** are prioritized for immediate remediation and are addressed **as soon as possible**, typically within a maximum of 30 days depending on risk context and operational constraints.

- **Medium and Low severity vulnerabilities** are remediated within planned remediation cycles, typically within 90 days.

These timelines are applied flexibly based on operational context, system criticality, and risk exposure, ensuring that remediation efforts are proportionate and effective. Where immediate remediation is not feasible, compensating controls may be applied and tracked until full remediation is completed.
Patches and updates are tested in Non-Production before deployment to Production. Operational continuity during rollout is protected through controlled scheduling, monitoring, and rollback mechanisms.

Where vulnerabilities may materially affect customer services or products, customer communication is handled through defined contractual and operational channels.

2.13 Incident Response & Problem Management

Payter maintains incident and problem management procedures to support detection, escalation, containment, remediation, and restoration of affected services.

Incidents are assessed and escalated based on severity, business impact, and customer impact.
Incident handling includes:

- detection and reporting
- initial assessment and classification
- investigation and containment
- remediation and service restoration
- documentation and post-incident review

Recurring or systemic issues are reviewed through problem management to identify root causes and implement corrective actions.
Where incidents affect customer-facing services or operational functionality, Payter communicates relevant information to affected customers through defined operational and contractual communication channels.

2.14 Supply Chain, Manufacturing & Provisioning

Payter applies controlled supply-chain, manufacturing, and device provisioning processes to ensure device integrity across manufacturing, logistics, deployment, support, and return handling.

Controls include:

- secure manufacturing and provisioning practices
- controlled serialisation and device lifecycle tracking
- controlled device handling procedures
- secure RMA processes, including wipe and re-provisioning where applicable
- secure key injection practices
- prevention of unauthorized access or modification during handling and provisioning

These controls are designed to reduce the risk of tampering, unauthorised modification, or loss of device integrity throughout the lifecycle.

2.15 Data Handling & Retention

Payter applies data minimisation and secure handling principles to all payment-related and operational data processed within its environment.

The design of Payter services ensures that only the minimum data required to operate, monitor, and support the service is processed and retained.

Payter does not store full cardholder data, clear-text Primary Account Number (PAN), or Sensitive Authentication Data (SAD) within MyPayter, terminal management systems, or corporate IT environments.

Payment authorisation data and sensitive cardholder information are processed exclusively by the configured payment gateway, processor, or acquirer within the broader payment processing domain.

Within Payter-managed systems, only limited operational and transaction-related metadata is retained. This data supports device management, operational monitoring, customer reporting, and reconciliation visibility.

Such data may include:

- terminal identifiers
- transaction timestamps
- transaction status
- authorisation results
- merchant references
- masked PAN and
- device telemetry or operational metadata

Where transaction-related data is presented to customers or internal support teams, card-related information is restricted to masked PAN and non-sensitive transaction details. This ensures that sensitive payment information is not exposed within Payter systems or interfaces.
Access to stored data is strictly controlled through role-based access control (RBAC), least privilege principles, and strong authentication mechanisms, ensuring that only authorized personnel can access relevant information based on their responsibilities.

Customers may access and export available transaction-related data through the MyPayter platform, subject to service scope and platform functionality.

Data retention is governed by defined lifecycle management procedures, as well as applicable contractual, legal, and regulatory requirements.

Operational data is retained only for the period necessary to fulfil business, reporting, and compliance obligations, which may extend up to 7 years, or longer where required by law or contract.

When data is no longer required, it is securely deleted through controlled processes. This includes removal from active systems and associated storage locations. Temporary files, intermediate processing data, and decommissioned storage media are handled through secure deletion or disposal procedures designed to prevent unauthorized recovery.
This approach ensures that Payter limits data exposure, protects sensitive information, and maintains compliance with applicable security and data protection requirements.

Controls Summary:
Payter's data handling and retention practices ensure that:

- only minimal operational data is stored and processed
- sensitive cardholder data and authentication data are not retained

- access to data is restricted and controlled
- customers can securely access and export relevant data
- retention is aligned with legal, contractual, and operational requirements
- data is securely deleted when no longer required

These controls collectively reduce data exposure risk and support compliance with payment security and data protection standards.

2.16 Privacy & GDPR

Payter applies data protection controls proportionate to the nature, scope, and sensitivity of the personal data processed.

Payter processes very limited personal data primarily related to:

- business contacts
- support and service communications
- employee and contractor administration

Payter does not process consumer personal data as part of payment transactions.
Where third parties are used, such as cloud providers or support services, processing is governed through contractual obligations, data protection terms, and security controls.

Privacy governance is aligned to the nature and scale of Payter's processing activities and includes secure handling expectations and contractual safeguards.

2.17 Business Continuity-Disaster Recovery

Payter maintains backup, recovery, and business continuity practices designed to support the resilience and recoverability of systems that support terminal management services and related operational platforms.

These practices are intended to ensure that critical services can be restored in a controlled and timely manner in the event of an operational disruption, while maintaining the integrity and availability of operational data managed by Payter.

Backups are performed for Payter-managed operational platforms and associated metadata in accordance with internal procedures. Backup repositories are protected through secure storage mechanisms and access restrictions aligned with Payter's authorisation model. Security and audit-related records are retained in accordance with applicable compliance requirements, including PCI DSS expectations for audit log retention.

Recovery capabilities are periodically validated through structured recovery testing activities. These activities include restoration testing, infrastructure recovery validation, and review of operational recovery procedures and runbooks to ensure that recovery arrangements remain effective and aligned with the current service environment.

Detailed business continuity policies, recovery procedures, and operational runbooks are maintained as controlled internal documents and are not distributed externally.

2.17.1 Operational Recovery Objectives

For critical terminal management and payment service components, including CPS, Payter defines operational recovery targets aligned with the contracted service scope.

- **RTO:** up to 4 hours
- **RPO:** Not Applicable / no data loss expected under normal operating conditions

The CPS service is a critical component for transaction initiation and service availability from Payter terminals. However, CPS and MyPayter do not act as the systems of record for payment transaction processing or financial settlement data.
Payment authorisation, transaction processing, and authoritative financial records are maintained by external payment gateway providers, processors, acquirers, and card networks.

The RPO is considered not applicable due to the nature of the service and underlying system design. In particular, CPS supports transaction initiation and operational control, but does not store sensitive payment data or act as the authoritative source of transaction records.

Payter-managed systems primarily maintain operational metadata and reporting information, while authoritative transaction records remain within the external payment processing ecosystem.

Accordingly, in the event of Payter platform unavailability, authoritative transaction records remain available through the relevant external payment processing participants, and no data loss is expected within Payter-managed systems under normal operating conditions. These recovery objectives apply specifically to Payter-managed CPS and associated operational platforms and do not extend to payment processing components operated by third-party processors, acquirers, or card networks.

2.18 Security Architecture Summary

Payter's security architecture is designed to protect payment credentials, ensure secure transaction processing, and clearly separate Payter-managed responsibilities from external payment processing domains.

The architecture follows a defence-in-depth approach, combining secure device design, controlled communication, strong cryptographic protections, and governed operational processes.

Key security principles include:

- payment credentials are protected at the point of capture within PCI PTS-certified terminal devices
- Sensitive Authentication Data is never stored after authorisation
- PIN data is never exposed outside secure cryptographic boundaries
- Each transaction is protected using unique cryptographic keys
- Root cryptographic key domains remain protected within secure HSM environments
- Terminal communication follows an outbound-only model with restricted endpoints
- Backend systems are logically segmented and securely exposed
- Access to systems and data is controlled, authenticated, and monitored
- Production and non-production environments are strictly segregated
- Payter systems do not store full cardholder data and are not systems of record for payment transactions

These controls collectively ensure the confidentiality, integrity, and availability of Payter-managed systems while maintaining alignment with industry security standards and clearly defined responsibility boundaries within the payment ecosystem.

3 Certifications and Security Assurance

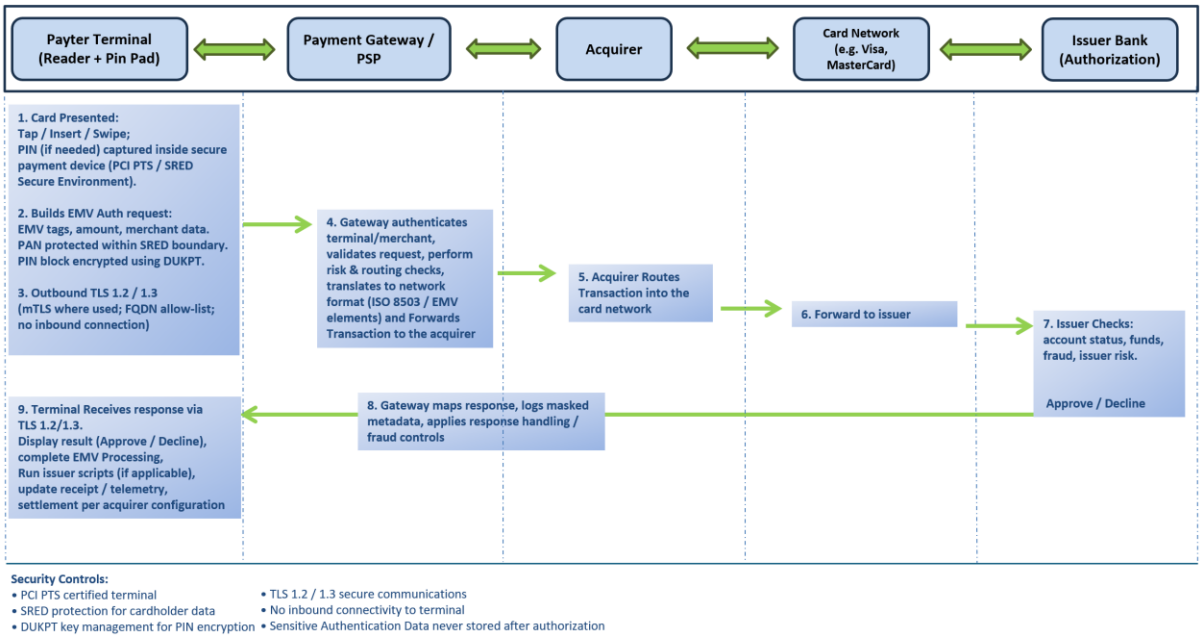
Payter's security posture is supported by recognised certifications and compliance activities, including:

- **PCI PTS**
- **PCI DSS**
- **ISO 9001 Quality Management System**
- **RED Cyber (EN 18031)**

Security and operational controls are continuously reinforced through ongoing assessment, governance, testing, and controlled operational processes.

4 Appendix

4.1 Payter Payment Terminal Card Flow



Step-by-step Terminal Card Flow

1. **Card presented; PIN (if needed) captured inside the secure payment device.**
   Card data is read within the PCI PTS-certified secure environment of the terminal, and PIN entry, where required, occurs within the secure PIN entry function.

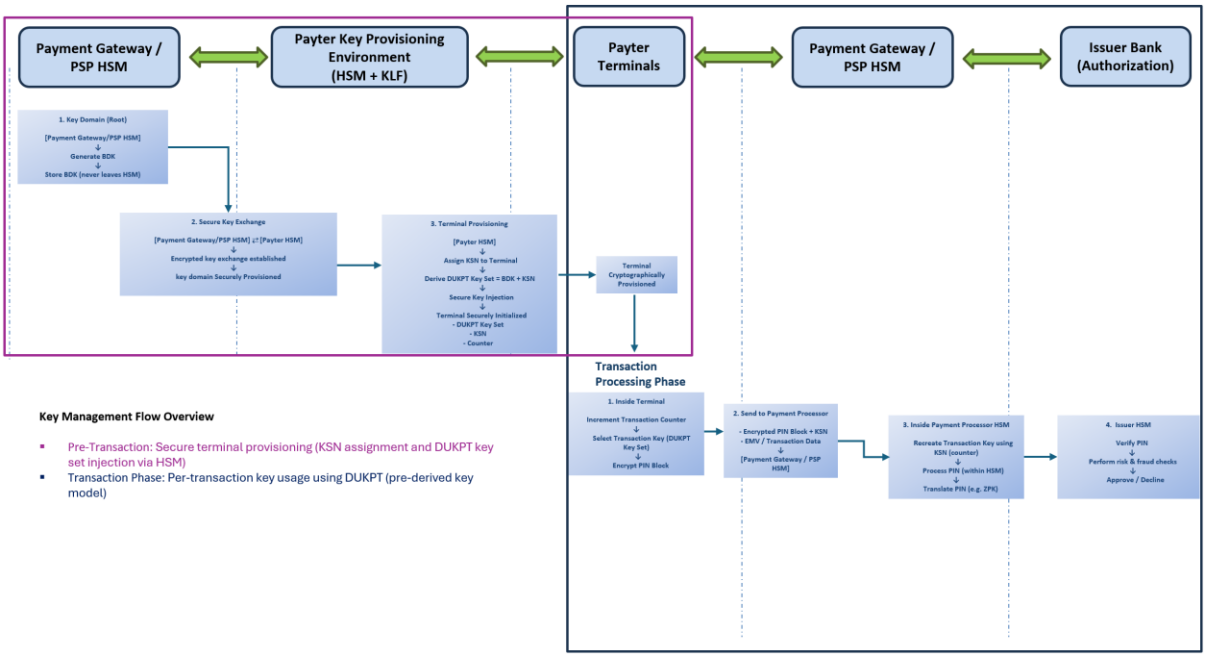
2. **Terminal constructs the authorization request (EMV data, amount, merchant and terminal data).**
   PAN and any PIN-related data never leave the device's secure boundary in clear text. Account data is protected within the SRED environment, and PIN-related cryptographic protection uses DUKPT-based key management where applicable.

   - **SRED enforces:**
     - PAN / PIN are never exposed in clear outside the device's secure module
     - Tamper detection and automatic key zeroization, so a physical tamper attempt destroys keys and disables secure operation
     - Only approved / signed firmware and locked-down configuration can run
     - No clear-text PAN / PIN in receipts, logs, telemetry, or diagnostics
   - **DUKPT enforces:**

- The device is provisioned for per-transaction derived key usage under a controlled key-management scheme
- A unique working key is derived for each transaction
- The KSN enables only the authorized downstream HSM environment to derive the corresponding key using the BDK.
- Compromise of one derived key does not expose past or future transactions

3. **Terminal opens an outbound-only TLS 1.2 / 1.3 connection to the Payment Gateway / PSP.** Communication is terminal-initiated only, using allow-listed destinations and ports. No inbound connectivity to the terminal is required.
4. **Gateway authenticates the terminal / merchant, performs validation, risk checks, routing decisions, and network message formatting.** The gateway validates the terminal and merchant context and translates the transaction into the required downstream processing format, such as ISO 8583 / EMV-related message structures.
5. **Gateway forwards the transaction to the configured processor / acquirer.**
6. **The processor / acquirer then routes the authorization request** through the applicable card network to the issuer bank.
7. **Issuer performs authorization checks and returns approve / decline.** These checks typically include account status, available funds, fraud screening, and issuer risk controls.
8. **The response returns through the payment chain back to the terminal.** The authorization response travels back from issuer to card network to acquirer / processor to gateway and finally to the terminal.
9. **Terminal displays the outcome and completes the transaction.** The terminal displays approve / decline, performs any applicable EMV completion steps, and logs only masked transaction data and operational metadata. No Sensitive Authentication Data is stored after authorization. Settlement occurs later through the acquirer clearing and settlement process.

4.2 Key Management Flow



4.2.1 Overview

The Payter payment solution uses industry-standard cryptographic mechanisms to protect PIN and cardholder data during payment transactions. The architecture incorporates multiple layers of security, including:

- PCI PTS / SRED-certified payment terminals
- Derived Unique Key Per Transaction (DUKPT) key management for PIN protection
- Hardware Security Modules (HSMs) operated by Payter and the Payment Gateway / Payment Service Provider (PSP)
- Secure inter-domain key exchange mechanisms
- TLS encryption for secure communication between terminals and backend systems

Sensitive Authentication Data (SAD), including PIN values, is never transmitted or stored in clear text outside secure cryptographic environments.

Within this model:

- Payter is responsible for secure terminal key provisioning
- The Payment Gateway / PSP performs transaction-time cryptographic processing within its HSM infrastructure

4.2.2 Key Ownership and Storage

Cryptographic keys are maintained only within controlled components of the payment architecture and are protected using certified HSMs or secure cryptographic devices.

Component	Key Material
Payter Terminal	DUKPT cryptographic key material (pre-derived transaction key set), KSN, transaction counter
Payter Provisioning HSM	Secure key exchange material, provisioning keys
Payment Gateway / PSP HSM	Root DUKPT key domain (BDK), network processing keys

Component	Key Material
Issuer Bank HSM	PIN verification keys (e.g. PVK), issuer cryptographic keys

The DUKPT key domain used for transaction processing is owned and managed by the Payment Gateway / PSP.

Payter:

- Does not store or process plaintext PIN data
- Does not perform PIN processing during live transactions

4.2.3 Secure Key Exchange

Prior to terminal provisioning, Payter establishes a secure key exchange relationship with the Payment Gateway / PSP HSM environment.
This enables Payter to provision terminals that operate within the gateway's DUKPT key domain.

Key characteristics:

- Secure exchange performed using industry-standard key exchange procedures
- Key material always remains within HSM boundaries
- Root key material (BDK) is never exposed outside the Payment Gateway / PSP HSM

This ensures cryptographic alignment between:

- Payter Terminal
- Payter provisioning environment
- Payment Gateway / PSP processing environment

4.2.4 DUKPT Key Hierarchy

The solution uses the DUKPT scheme as defined in ANSI X9.24.

The architecture consists of:

- Root key domain (BDK) managed by the Payment Gateway / PSP
- Terminal-specific cryptographic material provisioned during initialization
- Transaction-specific keys used per transaction

This model ensures:

- Each terminal operates with a unique cryptographic context
- Each transaction uses a unique encryption key
- Compromise of one device does not impact other devices or transactions

4.2.5 Terminal Provisioning and Key Injection

Before a terminal can process transactions, it is securely provisioned with terminal-specific cryptographic material.

- **Terminal Identification**

Each terminal is assigned a **Key Serial Number (KSN)**, uniquely identifying the device within the DUKPT domain.
The KSN range is registered with the Payment Gateway / PSP.

- **IPEK Generation**

Using the securely exchanged DUKPT key domain, the Payter HSM derives a terminal-specific Initial PIN Encryption Key (IPEK) based on the assigned Key Serial Number (KSN).
This operation occurs entirely within the secure boundary of the HSM.

- **Secure Key Injection**

Derived terminal cryptographic material is provisioned through Payter's controlled key injection process.

- Key injection is performed using Remote Key Injection (RKI)
- Communication occurs over mutually authenticated secure channels
- Confidentiality and integrity of key material are ensured during transfer

Following provisioning, the terminal is securely initialized with:

- DUKPT cryptographic key material (pre-derived transaction key set)
- Key Serial Number (KSN)
- DUKPT transaction counter

All cryptographic material is stored within the secure boundary of the PCI PTS-certified device.
The terminal:

- Does not store or access the Base Derivation Key (BDK)
- Does not have access to any root key material

4.2.6 Transaction Key Usage

For each transaction:

- The terminal increments the DUKPT transaction counter
- The counter is used to select the corresponding key from the provisioned key set
- Each key is used once per transaction

This ensures:

- Unique key usage per transaction
- No key reuse
- Synchronization with the Payment Gateway / PSP HSM

4.2.7 PIN Block Creation and Encryption

When a end customer enters a PIN:

- The PIN is formatted into a PIN block using ISO standards
- The PIN block is encrypted using the transaction-specific key

All operations occur within the secure boundary of the terminal.
At no point is the PIN exposed in plaintext outside the device.

4.2.8 Transaction Transmission

The terminal transmits transaction data to the Payment Gateway / PSP over TLS 1.2 or higher.

The message includes:

- Encrypted PIN block
- KSN (including transaction counter)
- Card / EMV data
- Transaction metadata

All sensitive data remains encrypted during transmission.

4.2.9 Payment Gateway/PSP HSM Processing

Upon receipt, the Payment Gateway / PSP processes the transaction within its HSM environment.

The HSM:

- Identifies the correct transaction key using the KSN and counter
- Processes encrypted PIN data within the secure boundary
- Performs PIN translation where required (e.g., to ZPK format)

All cryptographic operations are performed within certified HSM environments.

4.2.10 Issuer Authorization

The transaction is routed through the card network to the issuing bank.

Within the issuer HSM:

- PIN verification is performed
- Fraud and risk checks are executed
- Authorization decision is generated

The response (approve/decline) is returned to the Payment Terminal.

4.2.11 Summary

The Payter payment architecture ensures that:

✓ PIN data is encrypted at the point of entry
✓ Each transaction uses a unique cryptographic key
✓ Root keys remain protected within certified HSM environments
✓ Payter system never process plaintext PIN data
✓ Compromise of a single device doesn't affect other devices or transactions

This model aligns with PCI PTS, PCI PIN, PCI P2PE Security, and industry-standard cryptographic practices.

4.3 PCI PTS Certification / Assurance

➢ Payter Apollo Family Terminals

- **Approved PTS Devices link** - https://listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true)

➢ Payter P6X Series Terminals

The Payter P6X series is a contactless-only payment device designed for use cases where PIN entry is not required.

Applicability of PCI PTS:
PCI PTS POI (Point of Interaction) standards primarily apply to devices that support PIN entry (PIN Entry Devices - PEDs). As the P6X does not support PIN entry, it does not fall within the scope of PCI PTS POI certification requirements applicable to PIN-accepting devices.

At the time of introduction of the P6X series, applicable PCI program rules did not mandate PCI PTS certification for contactless-only devices without PIN entry functionality.

Security Design and Controls:
Although not a PIN-entry device, the P6X is designed in accordance with Payter's secure device and platform security principles, including:

- Secure firmware and software integrity controls (e.g. signed firmware, controlled updates)

- Protection against unauthorized modification and tampering
- Hardened configuration and restricted system interfaces
- Secure communication using encrypted protocols (e.g. TLS)
- Payment data protection aligned with EMV contactless security mechanisms

All payment data processed by the device is protected within the secure execution environment and transmitted securely to the payment processing infrastructure.

Scheme Approvals:
The P6X terminal is approved by major payment schemes (e.g. Visa, Mastercard).
Scheme approval includes validation of:

- Security requirements
- Functional correctness
- Interoperability within the payment ecosystem

These approvals are based on rigorous scheme-specific testing and certification processes.

Platform Integration:
The P6X operates within the same Payter terminal ecosystem, including:

- MyPayter terminal management platform
- Secure backend infrastructure and communication model
- Centralized monitoring, configuration, and operational controls

Security controls at the platform, network, and operational levels are consistently applied across Payter terminal products.

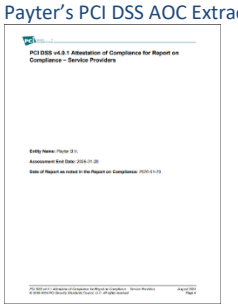
Summary:
The P6X is a contactless-only payment device that does not require PCI PTS POI certification due to the absence of PIN entry functionality. Security assurance is achieved through a combination of secure device design, EMV contactless protections, scheme approvals, and integration within Payter's controlled and monitored payment ecosystem.

4.4 PCI DSS AOC

Payter maintains PCI DSS certification covering its applicable systems and services. A copy of Payter's PCI DSS Attestation of Compliance (AOC) can be provided upon request via the Payter Sales or Support team.

Where payment processing is performed by designated third-party payment processors/gateways, Payter maintains the relevant PCI DSS AOC documentation for these providers. Such documentation can also be shared upon request via the Payter Sales or Support team.

Payter's PCI DSS AOC Extract


PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

4.5 ISO 9001 Certification

Payter is ISO 9001 certified, reflecting its commitment to structured quality management, operational excellence, and continuous improvement of its services.

TÜVNORD

Certificate

for the quality management system according to

NEN-EN-ISO 9001:2015

The certification body TÜV NORD Nederland hereby confirms that the certification took place in accordance with its certification regulations for the organisations

Payter B.V.
Rozenlaan 115
3051 LP Rotterdam
The Netherlands

Payter B.V.
Eglantierbaan 4
2908 LV Capelle aan den Ussel
The Netherlands

The management system and the application thereof complies with the requirements of the standard.
The certification is subject to annual evaluation by TÜV NORD Nederland.

Field of application

Designing and developing terminals for contactless and cashless payments, savings and other contactless interactions, including NFC. Advising companies and organisations on securely integrating cashless and contactless technologies.

Registration number 32451-1.2

Start date certificate 23-09-2024
Certificate valid until 22-07-2027
Date of first certificate 22-07-2024

Mr. E.W.A.C. Franken
Managing Director

TÜV NORD Nederland B.V.
Ekkersrijt 4401, 5692 DL Son en Breugel
The Netherlands

TÜVNORDGROUP

4.6 RED Cyber Certification

Payter is compliant with the RED Cybersecurity requirements (EN 18031-1,-2,-3) and has successfully passed the corresponding conformity testing, demonstrating alignment with EU cybersecurity requirements for radio equipment.

Please contact Payter Sales or Support Team to receive a copy of RED Cyber Certificate.