Solution Security Assumptions/Statements	Supporting Information
Security	The terminals are certified by MasterCard, VISA, American Express, Discover according to the latest standards and accredited through various acquirers by the same Card scheme's. The terminal incorporates the following security measures for data handling; SSL TLS 1.2, SRED and DUKPT which are compliant to the PCI regulations for data security. The routing of the transactions by gateways such as Creditcall are PCI certified. The production of the terminals is certified by MasterCard and the TüV in a Terminal Quality Management system.
PCI PTS	Payter card readers are not PCI PTS approved devices as this is not required by Visa/Mastercard for their approval (as no PIN Entry);
Uses non-PED card reading devices that are EMV level 1 certified, use the Creditcall EMV level 2 kernel and are Visa/Mastercard/Amex/Discover certified.	Account data is encrypted immediately upon entry and processed within a secure controller of the device (Payter device: SAM Secure Application Module EAL 5+); Use of the SRED function for encryption of card data is enforced at all times (devices cannot enter a state where account data is not encrypted); The SAM module containing the encryption material is equal to any EMV card with the same protections against tampering. Device does not include a tamper response mechanism (keys are not erased when attempting to tamper with the device); however the terminal does not contain any past keys due to the mechanisms of DUKPT.
Uses SRED encryption.	Payter card readers are not PCI PTS approved devices; not required by Visa/Mastercard for their approval (as no PIN Entry); Certified Lab testing confirms that Payter devices have the capacity to protect externally communicated account data from modification and disclosure.
Uses standard 3DES DUKPT encryption.	The Payter solution uses an approved algorithm (3DES) and a standard key management method (Derived Unique Key Per Transaction) commonly used in PCI-listed P2PE solutions. The DUKPT key management scheme means a unique key is used for every transaction. If a derived key is compromised, future and past transaction data are still protected since the next or prior keys cannot be determined easily. The SAM stores the device encryption and communication keys and is understood to handle all the key management and cryptography within the devices. The device will only contain unused keys not keys that have been used to encrypt any previous card holder data, this is a primary function of DUKPT as per ANSI X9.24. Only off-line stored transactions could reside in the terminal, which are encrypted and cannot be retrieved, even the terminal can not decrypt the transaction data. The key used to encrypt any stored card data is longer present in the terminal. Key management, exchange procedures are performed following the Creditcall PCI procedures resulting in a functioning ecosystem and successful transactions, both on and off-line.
Communication is secured end to end secured between Payter device and gateway. Solutions uses TLS v1.2 to encrypt all communications outside of the Payter device.	The gateway does not accept any transactions which do not comply to these standards and actively monitors this. If the protocols or encryption communication do not comply, transactions will be declined. Certified Lab testing confirms use of TLS v1.2 to secure all communications.
The solution security layer (both GPRS and LAN versions) assumes an open, untrusted network;	Payter has no expectation of or requirement for the merchant to implement any additional security controls necessary for the protection of account data. All security controls are built into the solution.

Solution management is within Payter's control	The ability to enable/disable the SRED 3DES DUKPT encryption is restricted to Payter; Device allocation is done through the terminal management system managed and controlled by Payter; The initial keys are stored into Payter SAM module which are securely injected into the SAM at SAM manufacturer. Following this the SAM's are loaded in an offline setup always with fully encrypted channels between secure elements. Payter is responsible for secure device configuration, ongoing vulnerability management and update of the deployed solution; Payter monitor for vulnerabilities affecting solution, assess for relevance and take action to address incl. ensuring remote deployment of updates (via TMS); Payter can enforce changes of any applicable device defaults and remotely update or deactivate devices; Merchant cannot change device security settings, parameters etc., merchant has no ability to amend settings/configuration that could affect the terminal encryption or protection of card data. Payter Settings Tool can only be used to configure connectivity to host machines (e.g. VDB mode), test connectivity, perform test transaction or view network connectivity diagnostics; There is no inbound remote access to devices, terminal comms is controlled by Payter and is initiated outbound to Payter Terminal Management System (TMS) and outbound to Creditcall gateway only; Merchant cannot add any remote access function to the devices; Shipping to distributors is within Payter control.
No full PAN is ever 'on display' either on device screen or in an issued receipt.	Receipts can only be generated by 3rd parties not by Payter. Payter control what is displayed on device screen or can be sent to any 'host machine': no full PAN;
Devices that are suspected of being tampered or are reported as tamper lost or stolen can be remotely deactivated.	The gateways used are PCI P2PE v.2 compliant, and at a platform level this is never turned off. Event reports are sent in the event of any security breach or malfunction. Reports include – • Unencrypted card details received • Unexpected KSN (Encryption Key Identifier) • Decryption exceptions. Failures at Creditcall H.S.M.'s to decrypt data (a platform error – e.g. H.S.M. unavailable) Decryption failures. Failures to decrypt data received due to things like – • BDK not found in H.S.M. • BDK does not match • Decrypted data is invalid Payter will respond to all notifications with remote deactivation. Devices are identified both by Terminal ID (TiD), unique serialnumber, SAM number and quite often SIM card number. Any of these identifiers but usually a combination thereof are used for identification. Creditcall would report an incident to Payter using the TID.
Sets expectations for merchant usage of the solution and security responsibilities for protecting payment card data.	Payter provides an instruction for download stating the merchant responsibilities and expectations.