COMPLIANCE

Compilation of Rocket® Terminal Emulator Compliance Documents

Rocket®

Table of contents

Basel III Compliance with Rocket® Terminal Emulator

Basel III is a set of international standards for financial institutions that focus on financial strength and stability. Although focused on financial risks, Basel III also establishes several principles for internal controls intended to reduce the likelihood of fraud, misappropriation, errors, or misstatements that may involve technology systems. No specific, prescriptive control requirements are given, so institutions must determine the exact structure of their controls designed to satisfy the Basel III principles. From a technology perspective, Basel III is most concerned with the availability and integrity of financial data.

Rocket® Terminal Emulator (TE) may be used to support key information systems in a financial institution, and in that capacity, its remote access capabilities enable effective contingency planning to ensure the availability of key systems and data. Rocket TE also supports strong security and integrity controls to protect information systems from unauthorized access or modification. The relevant Basel III Internal Controls Principles, along with Rocket TE's related capabilities, are listed below.

BASEL III PRINCIPLES	ROCKET TERMINAL EMULATOR CAPABILITIES
Principle 6 An effective internal control system requires there be an appropriate segregation of duties and that an organization not assign personnel conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimized, and subject to careful, independent monitoring.	Rocket TE provides communication between clients and backend host systems by utilizing the user access permissions inherent in the backend host system environment. Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host O/S.

BASEL III PRINCIPLES	ROCKET TE CAPABILITIES
Principle 8 An effective internal control system requires reliable information systems are in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently, and supported by adequate contingency arrangements.	• Performs authentication against the host system directly by applying password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems. • Uses a second layer of authentication directly against the Security Server before a user may attempt to authenticate to the host system. Security Server supports integration with RSA SecurID and Active Directory for user credentials and authentication. • Record all activities initiated through Rocket TE sessions with the built-in logging mechanisms inherent within the host system environment. This eliminates the need to maintain a separate log management function specifically for Rocket TE. • Records a log of all client connections to the web server as a supplemental logging mechanism. This does not record commands issued through the sessions, which would be logged through the built-in host system functionality, but instead provides an additional layer of security by showing how many users and terminals are connecting, when, and from where. • Allows administrators to connect to the host system environment from anywhere, to anywhere, in order to perform routine maintenance or emergency corrections. During a technical incident or disaster scenario, Rocket TE can help continue or restore operations and data access. • Enables clients to specify alternate hosts for instant, automatic cutover to disaster recovery facilities. • Support redundant web servers to withstand a technical incident and continue operating in other environments, while allowing administrators from any location to continue working.

Gramm-Leach-Bliley Act (GLBA) Compliance with Rocket® TE

The Gramm-Leach-Bliley Act (GLBA) establishes a number of control requirements to protect the security and privacy of individuals' financial information. The privacy requirements include disclosures of information that is collected, stored, or distributed, and the ability for a customer to optout of certain information usages. The security requirements apply to any location of a customer's financial data, physical or electronic, and require both proactive protection measures and breach response procedures.

Specific control implementation requirements related to GLBA are described in "Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards."

Rocket TE terminal emulation solutions offer key control capabilities for protecting customers' non-public personal information (NPPI). Rocket TE does not store any data directly and leverages host system environments for access controls to protect the confidentiality of NPPI. Enhanced logging and remote access security build upon these logical security controls, and strong encryption capabilities protect all data throughout its usage. Relevant GLBA standards and the capabilities Rocket TE offers are listed below.

GLBA REQUIREMENTS	ROCKET TE CAPABILITIES
III(C)(1)(a) Access controls on customer information systems, include controls to authenticate and permit access only to authorized individuals, and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.	• Rocket TE provides communication between clients and backend host systems by utilizing the user access permissions inherent to the backend host system environment. Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host O/S . • Security Server provides an additional, optional layer of security by acting as a proxy between the host system and clients. Clients must first authenticate and connect to Security Server using an established user ID, which may be integrated with other Identity Access Management systems including RSA and Active Directory. • Security Server performs authentication against the host system directly, and automatically applies password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems. • After authenticating to Security Server, users must log into the host system directly, and apply level access permissions to the host system.

GLBA REQUIREMENTS	ROCKET TE CAPABILITIES
III(C)(1)(c) Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.	• Rocket TE products support state-of-the-art encryption methods for all communications between clients and the backend host system environment, including the TLS1.2 and SSHv2 protocols with FIPS-compliant encryption algorithms. • Rocket TE (Web Edition) applies this level of encryption to both the end user-to-web server session, and the web server-to-host system session. • While support for older protocols is available to support legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. • In environments where the host system cannot support encrypted sessions, the optional Security Server allows for plaintext communications to be isolated within a secure, local network, while applying strong encryption methods to all external connections with clients.
III(C)(1)(f) An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently, and supported by adequate contingency arrangements.	• The built-in logging mechanisms inherent within the host system environment record all activities initiated through Rocket TE sessions. There is no need to maintain separate log management functions specifically for Rocket TE. Users can design alerting and monitoring controls around these logs to identify unauthorized access attempts to NPPI. • As a supplemental logging mechanism, Rocket TE (Web Edition) records a log of all client connections to the web server. This does not record commands issued through the sessions that are logged through the built-in host system functionality, but provides an additional layer of security by showing how many users and terminals are connecting, when and from where.
Supplement A, II(A)(1)(a) At a minimum, an institution's response program should contain procedures that assess the nature and scope of an incident, and identify accessed or misused customer information systems and types of customer information.	• In the event of a breach, any Rocket TE activity from the affected time period is available in host system logs for a forensic investigation. • Rocket TE (Web Edition) logs help identify all terminals and users who have connected to an organization's systems, along with the dates, times, and source addresses.

Health Information Portability and Accountability Act (HIPAA) Compliance with Rocket® TE

The Health Information Portability and Accountability Act (HIPAA) requires organizations to safeguard patients' protected health information (PHI) by restricting and monitoring access to any systems that house it. HIPAA includes a privacy rule, which concerns appropriateness and disclosures of information that is collected, stored, or distributed, and the ability for a patient to opt-out of certain information usages. The HIPAA security rule includes a number of control requirements intended to protect the confidentiality, availability, and integrity of PHI.

The HIPAA security rule is available at 45 C.F.R. 164.302-316, and implementation guidance is provided in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66.

Rocket TE terminal emulation solutions do not store any data directly, and leverages the host system environment for access controls to protect the confidentiality of PHI. Organizations don't need to manage additional user credentials or authorization processes for Rocket TE to maintain effective logical security. Rocket TE also provides enhanced logging and remote access security capabilities, and strong encryption to protect all data throughout its usage. Below are the relevant HIPAA requirements and capabilities Rocket TE offers.

HIPAA REQUIREMENTS	ROCKET TE CAPABILITIES
Workforce Security: 164.308(a)(3) Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	• Rocket TE provides communication between clients and backend host systems by utilizing the user access permissions inherent in the backend host system environment. Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host O/S .
Information Access Management: 164.308(a)(4) Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of subpart E of this part.	• Rocket TE leverages host system credentials and permissions. There is no need to maintain a separate user account list in Rocket TE or to authorize PHI access separately.

HIPAA REQUIREMENTS	ROCKET TE CAPABILITIES
Security Incident Procedures: 164.308(a)(6) Implement policies and procedures to address security incidents.	• In the event of a breach, any Rocket TE activity from the affected time period is available in the host system logs for a forensic investigation. • Logging capability is enhanced with Rocket TE (Web Edition), as users can identify not only which commands were executed against the host system, but also all terminals and users who have connected to systems, along with the dates, times, and source addresses. This information can be critical to an effective response process.
Contingency Plan: 164.308(a)(7) Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, or natural disaster) that damages systems that contain electronic PHI.	• The distributed nature of Rocket TE's architecture allows administrators to connect to the host system environment from anywhere, to anywhere. • During a technical incident or disaster scenario, Rocket TE helps continue or restore operations and access to PHI. • Rocket TE clients can specify alternate hosts for instant, automatic cutover to disaster recovery facilities
Access Control: 164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	• All user accounts and access permissions are inherited from the host system. Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host system O/S. • Security Server provides an additional, optional layer of security by acting as a proxy between the host system and clients. Clients must first authenticate and connect to Security Server using an established user ID, which may be integrated with other Identity Access Management systems including RSA and Active Directory. • After authenticating Security Server, users must log into the host system directly, applying level access permissions to the host system.

HIPAA REQUIREMENTS	ROCKET TE CAPABILITIES
Audit Controls: 164.312(b) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.	• The built-in logging mechanisms inherent within the host system environment record all activities initiated through Rocket TE sessions. There is no need to maintain separate log management functions specifically for Rocket TE. • As a supplemental logging mechanism, Rocket Rocket TE (Web Edition) records a log of all client connections to the web server. This does not record commands issued through the sessions, that would be logged through the built-in host system functionality, but which provide an additional layer of security by showing how many users and terminals are connecting, when and from where.
Integrity: 164.312(c)(1) Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Encryption of data in transit protects the integrity of all such data, preventing technical errors, corruption, or malicious alteration in transit that could impair its accuracy and reliability.
Person or Entity Authentication: 164.312(d) Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.	• Authentication is performed against the host system directly by applying its password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems. • When using Security Server, a second layer of authentication must be conducted against the Security Server directly before a user may attempt to authenticate the host system. Security Server supports integration with RSA SecurID and Active Directory for user credentials and authentication.
Transmission Security: 164.312(e)(1) Implement technical security measures to guard against unauthorized access to electronic PHI that is transmitted over an electronic communications network.	• Rocket TE products support state-of-the-art encryption methods for all communications between clients and the backend host system environment, including the TLS1.2 and SSHv2 protocols with FIPS-compliant encryption algorithms. • Rocket TE (Web Edition) applies this level of encryption to both the end user-to-web server session, and the web server-to-host system session. While support for older protocols is available to support legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. In environments where the host system cannot support encrypted sessions, the optional Security Server allows for plaintext communications to be isolated within a secure, local network, while applying strong encryption methods to all external connections with clients.

Payment Card Industry Data Security Standard (PCI-DSS) Compliance with Rocket® TE

The Payment Card Industry requires all organizations who store or process credit card data and transactions to implement technical security requirements over all systems involved in data storage and transmission.

The scope of these control requirements range from encryption methods to access rights management to vulnerability testing.

Rocket TE terminal emulation solutions do not typically store or transfer Cardholder Data (CHD) directly, which reduces the impact on PCI compliance requirements. However, some of Rocket TE's security features do have a direct impact on an organization's ability to satisfy certain PCI-DSS requirements for the overall Cardholder Data Environment (CDE). For these areas, Rocket TE provides strong encryption, multifactor authentication, and remote access security capabilities for administrative access to host system environments. Relevant requirements, and the capabilities Rocket TE offers in order to achieve each, are listed below.

PCI-DSS REQUIREMENTS	ROCKET TE CAPABILITIES
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	• Security Server can function as a proxy in the DMZ between the host system and remote clients, which eliminates the need for direct access, and ensures secure, encrypted communications throughout the transmission.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	• Rocket TE leverages the host system credentials and all associated authentication mechanisms. There is no need to maintain a separate user account list in Rocket TE.

PCI-DSS REQUIREMENTS	ROCKET TE CAPABILITIES
2.3 Encrypt all non-console administrative access using strong cryptography.	• Rocket TE products support state-of-the-art encryption methods for all communications between clients and the backend host system environment, including the TLS1.2 and SSHv2 protocols with FIPS-compliant encryption algorithms. **Rocket TE (Web Edition)** applies this level of encryption to both the end user-to-web server session, and the web server-to-host system session. • While support for older protocols is available to support legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. • In environments where the host system cannot support encrypted sessions, the optional Security Server allows for plaintext communications to be isolated within a secure, local • network, while applying strong encryption methods to all external connections with clients.
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all CHD storage: • Limit data storage amounts and retention times to that which is required for legal, regulatory, and business requirements. • Process secure deletion of data when no longer needed. • Specify retention requirements for cardholder data. • Establish a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	• Rocket TE does not store any CHD directly; it provides a command interface between clients and the backend host system. No additional data storage and retention controls are needed for using Rocket TE.
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Accept only trusted keys and certificates . • Ensure protocol in use only supports secure versions or configurations. • Confirm the encryption strength is appropriate for the encryption methodology in use.	• Rocket TE does not transmit any CHD directly. While all communications are strongly encrypted, there is no direct exposure to this control requirement.

PCI-DSS REQUIREMENTS	ROCKET TE CAPABILITIES
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Define access needs for each role, including system components and data resources that each role needs to access for their job functions and levels of privilege required (for example, user, administrator, etc.) for accessing such resources. Restrict access to privileged user IDs to the lowest level of privileges necessary to perform job responsibilities. Assign access based on each individual personnel's job classification and function. Require documented approval by authorized parties specifying required privileges.	• All access permissions are inherited from the host system. There is no separate user access schema to maintain within Rocket TE, and Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host O/S.
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: • Assign all users a unique ID before allowing them to access system components or CHD. • Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. • Revoke access for any terminated users immediately. • Remove/disable inactive user accounts at least every 90 days. • Manage IDs used by vendors to access, support, or maintain system components via remote access • Limit repeated access attempts by locking out the user ID after not more than six attempts. • Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. • Require the user to re-authenticate to re-activate the terminal or session if a session has been idle for more than 15 minutes.	• Rocket TE leverages host system credentials. There is no need to maintain a separate user account list in Rocket TE. • Session security settings, including account lockout and session timeout, are inherited from the host system configurations.

PCI-DSS REQUIREMENTS	ROCKET TE CAPABILITIES
8.2 In addition to assigning a unique ID, ensure proper user authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric.	• Authentication is performed against the host system directly, applying its password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems. • When using Security Server, employ a second layer of authentication against the Security Server directly before a user may attempt to authenticate to the host system. Security Server supports integration with RSA SecurID and Active Directory for user credentials and authentication.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multifactor authentication.	• Rocket TE supports multifactor authentication for client access, supplementing passwords with additional authentication factors including physical tokens, and digital certificates.
10.1 Implement audit trails to link all access to system components to each individual user.	• The built-in logging mechanisms inherent within the host system environment record all activities initiated through Rocket TE sessions. There is no need to maintain separate log management functions specifically for Rocket TE. • As a supplemental logging mechanism, Rocket Rocket TE (Web Edition) records a log of all client connections to the web server. This does not record commands issued through the sessions, which would be logged through the built-in host system functionality, but provides an additional layer of security by showing how many users and terminals are connecting, when, and from where.

Rocket® TE 508 Compliance

Section 1194.21: Software Applications and Operating Systems

Detailed Voluntary Product Accessibility Template

Criteria A When software is designed to run on a system that has a keyboard, product functions shall be executable from the keyboard where the function itself or the result of performing a function can be discerned textually.	**Supporting Features** Rocket TE runs on the Windows platform and employs Windows 508 compliance to support use by disabled features. **Remarks & Explanations** Rocket TE has been modified to be completely 508 compliant.
Criteria B Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of the operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.	**Supporting Features** Rocket TE runs on the Windows platform and employs Windows 508 compliance to support use by disabled features. **Remarks & Explanations** Rocket TE has been modified to be completely 508 compliant.

Criteria C A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.	**Supporting Features** Rocket TE offers a number of features that indicate the current focus of the screen. **Remarks & Explanations** Field focus can be indicated by a user-defined cursor size, varying blink rate of the cursor, and by displaying the crosshairs of the cursor's placement on the screen. Any supporting dialog the user receives will change and be brought to the "front" to indicate its focus. Focus is exposed through Windows API calls.
Criteria D Sufficient information about a user interface element including the identity, operation, and state of the element shall be available to assistive technology. When an image represents a program element, the information conveyed by the image must also be available in text.	**Supporting Features** All user interface elements are by default identified with text. Secondarily, it may use a bitmap. **Remarks & Explanations** Rocket TE is completely compatible with assistive technology.
Criteria E When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	**Supporting Features** All textual and graphical indicators are consistent throughout the Rocket TE emulator.
Criteria F When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	**Supporting Features** All textual and graphical indicators are consistent throughout the Rocket TE emulator.

Criteria G Applications shall not override user selected contract color selections and other individual display attributes.	**Supporting Features** All Rocket TE color schemes are user-definable, but do not override the accessibility features of the operating system. Rocket TE supports the accessibility features of Windows and conforms to the colors and contrasts specified.
Criteria H When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	**Supporting Features** As a text-based emulator, Rocket TE does not utilize animation.
Criteria I Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	**Supporting Features** Rocket TE does not rely solely on the use of color-coding. The predominant indicators are cursor location, screen, text, and window focus.
Criteria J When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.	**Supporting Features** Rocket TE provides a wide array of color choices, but does not override the color and contrast settings of the operating system.
Criteria K Software shall not use flashing or blinking text, objects, or other elements that have a flash or blink frequency greater than 2 Hz and lower than 55 Hz.	**Supporting Features** Rocket TE offers a user-definable blink rate for the carat. The entire adjustable range is below 2 Hz.
Criteria L When electronic forms are used, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	**Supporting Features** Rocket TE does not utilize electronic forms.

General Data Protection Regulation (GDPR) and Rocket® TE

The General Data Protection Regulation (GDPR) that went into effect on 25 May 2018 attempted to "harmonize" data privacy laws across Europe, and give individuals greater protection and rights. GDPR drove sweeping changes for the public and for organizations that handle Personally Identifiable Information (PII). The regulation gave individuals new powers over their data, with enhanced rights to access, rectify, and erase it, and the ability to freely request the transfer of their information to other platforms. Along with issuing increased rights for data subjects to control their information, GDPR also mandated technical security controls to protect the confidentiality, availability, and integrity of individuals' data: 'Data protection by design and by default'.

Organizations cannot achieve full compliance with GDPR solely through technical means. The regulation's scope is broad, encompassing organizational, procedural, and technical security requirements. Rocket® Rocket TE enables users to minimize regulatory exposure to GDPR's articles, while providing strong, built-in technical capabilities that allow them to conform to applicable articles easily. The specific Rocket TE security controls and specifications, along with the GDPR articles they satisfy, are described below.

It is important to note that GDPR compliance will ultimately depend on an effective implementation of these capabilities, as well as other organizational and procedural controls to address all GDPR articles.

Article 5: Principles Relating to Personal Data Processing

GDPR REQUIREMENTS	ROCKET TE CAPABILITIES
1.d Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage by using appropriate technical or organizational measures ('integrity and confidentiality').	• Rocket TE provides communication between clients and back-end mainframe systems by utilizing user access permissions inherent to the back-end mainframe environment. Rocket TE cannot provide any capability for data access to the logged-in user not already specifically authorized within the mainframe O/S. • All data transfers to and from the mainframe environment are encrypted to protect against unauthorized access to the data in transit, or disclosure of user credentials that could be utilized for unauthorized system access.

Article 30: Records of Processing Activities

GDPR REQUIREMENTS	ROCKET TE CAPABILITIES
1 Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under their responsibility. That record shall contain all of the following information: a) Name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer b) Purposes of the processing c) Description of the categories of data subjects, and of the categories of personal data; d) Categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organizations e) Where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards f) Where possible, the envisaged time limits for erasure of the different categories of data g) Where possible, a general description of the technical and organizational security measures referred to in Article 32(1).	• The built-in logging mechanisms inherent to the mainframe environment record all activities initiated through Rocket TE sessions. These logs may include all the necessary information, depending on system configurations. There is no need to maintain separate log management functions specifically for Rocket TE. • As a supplemental logging mechanism, Rocket TE (Web Edition) records a log of all client connections to the web server. This does not record commands issued through the sessions, which would be logged through built-in mainframe functionality, but provides an additional layer of security by showing which endpoints are connecting, when, and from what source.

Article 32: Security of Processing

GDPR REQUIREMENTS	ROCKET TE CAPABILITIES
1.a Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the pseudonymisation and encryption of personal data.	• Rocket TE products support state-of-the-art encryption methods for all communications between clients and the back-end mainframe environment, including TLS1.2 and SSHv2 protocols with FIPS-compliant encryption algorithms. • Rocket TE (Web Edition) applies this level of encryption to both the end user-to-web server session, and the web server-to-mainframe session. While support for older protocols is available for legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. • In environments where the mainframe cannot support encrypted sessions, the optional Security Server allows for plain text communications to be isolated within a secure, local network with mainframe, while applying strong encryption methods to all external connections with clients.
1.b Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.	• Rocket TE leverages the built-in authentication mechanisms and user access permissions schemas within the mainframe environment, and can support multifactor authentication methods. There is no need to maintain separate access rights management functions for Rocket TE, as existing mainframe controls will apply. • Rocket TE also offers optional X.509 certificates to authentication endpoint devices that attempt to connect to the mainframe. • Encryption of all data in transit to and from the mainframe prevents unauthorized access through eavesdropping, and protects the administrative credentials used to establish sessions. • Encryption of data in transit also protects data integrity, preventing technical errors, corruption, or malicious alteration in transit that could impair data accuracy and reliability.
1.c Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	• The distributed nature of Rocket TE architecture lets administrators connect to the mainframe environment from anywhere to perform routine maintenance or emergency corrections. During a technical incident or disaster scenario, Rocket TE helps continue or restore operations and data access. • Rocket TE clients can specify alternate hosts for instant, automatic cutover to disaster recovery facilities. • Rocket TE (Web Edition) supports redundant web servers to withstand a technical incident and continue operating in other environments, while allowing administrators from any location to continue working.

Trust Services Principles for Service Organization Controls Reports with Rocket® TE

Service Organization Controls (SOC) reports are an effective way for companies to provide assurances to their customers and prospects regarding the security, availability, confidentiality, integrity, and/or privacy of the systems they offer. SOC 2 and SOC 3 reports are popular with Software-as-a- Service (SaaS) providers and any company with access to its customers' critical systems and data.

Each Trust Services Principle includes a number or criteria that must be satisfied by the service organization, as well as illustrative controls for how an organization may achieve the criteria.

Rocket TE terminal emulation solutions effectively leverage the security of the host system environment, while adding strong encryption for all data transfers and enhanced remote access and authentication capabilities, to achieve logical security, integrity, and confidentiality objectives. Rocket TE's distributed architecture also serves availability and continuity goals. Relevant Trust Services principles and criteria, along with Rocket TE's capabilities to meet them, are detailed on the following pages.

CRITERIA	ROCKET TE CAPABILITIES
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	• Rocket TE provides communication between clients and backend host systems by utilizing the user access permissions inherent within the backend host system environment. Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host system O/S. • Security Server provides an additional, optional layer of security by acting as a proxy between the host system and its clients. Clients must first authenticate and connect to Security Server using an established user ID, which may be integrated with other Identity Access Management systems including RSA and Active Directory. • After authenticating to Security Server, users must then also log into the host system directly, applying system-level access permissions to the host. • The built-in logging mechanisms inherent within the host system environment record all activities initiated through Rocket TE sessions. There is no need to maintain separate log management functions specifically for Rocket TE. • As a supplemental logging mechanism, Rocket Rocket TE (Web Edition) records a log of all client connections to the web server. This does not record commands issued through the sessions, which would be logged through the built-in host system functionality, but provides an additional layer of security by showing how many users and terminals are connecting, when, and from where.
CC5.2 New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	• Rocket TE leverages host system credentials and all associated authentication mechanisms. There is no need to maintain a separate user account list in Rocket TE.

CRITERIA	ROCKET TE CAPABILITIES
CC5.3 Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	• Authentication is performed against the host system directly by applying its password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems. • When using Security Server, a second layer of authentication must be conducted against the Security Server directly before a user may attempt to authenticate to the host system. Security Server supports integration with RSA SecurID and Active Directory for user credentials and authentication.
CC5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them. All access permissions are inherited from the host system.	• Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host system O/S.
CC5.6 Logical access security measures have been implemented to protect against security, availability, processing integrity, or confidentiality threats from sources outside the boundaries of the system.	• To insulate host systems from direct external access, Security Server may be implemented as a proxy within the DMZ to enhance the security of remote access.
CC5.7 The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security, availability, processing integrity, or confidentiality.	• Rocket TE products support state-of-the-art encryption methods for all communications between clients and the backend host system environment, including the TLS1.2 and SSHv2 protocols with FIPS-compliant encryption algorithms. • Rocket TE (Web Edition) applies this level of encryption to both the end user-to-web server session, and the web server-to-host system session. • While support for older protocols is available to support legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. • In environments where the host system cannot support encrypted sessions, the optional Security Server allows for plaintext communications to be isolated within a secure, local network, while applying strong encryption methods to all external connections with clients.

CRITERIA	ROCKET TE CAPABILITIES
A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	• The distributed nature of Rocket TE's architecture allows administrators to connect to the host system environment from anywhere, to anywhere in order to perform routine maintenance or emergency corrections. During a technical incident or disaster scenario, Rocket TE can help continue or restore operations and data access. • Rocket TE clients can specify alternate hosts for instant, automatic cutover to disaster recovery facilities. • Rocket TE (Web Edition) can support redundant web servers to withstand a technical incident and continue operating in other environments, while allowing administrators from any location to continue working.
PI1.6 Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	• All access permissions are inherited from the host system. Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host O/S. • Encryption of data in transit protects the integrity of all such data, preventing technical errors, corruption, or malicious alteration in transit that could impair its accuracy and reliability.
C1.2 Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality requirements.	• All access permissions are inherited from the host system. Rocket TE cannot provide any capability for data access to logged in users not already specifically authorized within the host O/S.
C1.3 Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements.	• The encryption of all data in transit to and from the host system prevents unauthorized access via eavesdropping to the data itself, as well as protecting the administrative credentials used to establish sessions.

Legal Disclaimer (Rocket Software)

Note: This document is provided for information purposes only and the contents hereof are subject to change without notice. Rocket Software, Inc., does not warrant that this document is error free, nor does it provide any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Rocket Software, Inc., specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. Rocket further makes no representation concerning the ability of Rocket Terminal Emulation to foster compliance with abovementioned regulations. This document addresses the named product(s) only.

Rocket_ComplianceDoc_Jan2022_v5