COMPLIANCE

Revised Payment Services Directive (PSD2) and Rocket LegaSuite

The Revised Payment Services Directive (PSD2) goes into effect in January 2018. This new set of regulations drives significant changes in the banking and payment technology industries. While much of PSD2 concerns the operational aspects of monetary transfers, there are also specific technical requirements. Notably, the companion document Regulatory Technical Standards (RTS) on Strong Customer Authentication and Secure Communication requires that banks allow third-party technology providers access to their systems through a secure, designated communications interface. The specific provisions of this RTS are effective as of November 2018.

Rocket® LegaSuite is inherently designed to satisfy the technical requirements of PSD2 surrounding authentication and secure communications, enabling you to take advantage of the open communications interfaces. The relevant articles of PSD2 and the RTS on Strong Customer Authentication and Secure Communication, along with the associated capabilities of LegaSuite, are described below.

Revised Payment Services Directive (PSD2)

PSD2 REQUIREMENTS	ROCKET LEGASUITE CAPABILITIES
66.3(e) The payment initiation service provider shall not store sensitive payment data of the payment service user.	LegaSuite does not store or cache data, limiting exposure to potential breaches.
66.4(a) The account servicing payment service provider shall communicate securely with payment initiation service providers in accordance with point (d) of Article 98(1).	All data transfers using LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality.
67.3(a) In relation to payment accounts, the account servicing payment service provider shall communicate securely with the account information service providers in accordance with point (d) of Article 98(1).	All data transfers using LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality.
97.1 Member States shall ensure that a payment service provider applies strong customer authentication where the payer: 　(a) accesses its payment account online; 　(b) initiates an electronic payment transaction; 　(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.	LegaSuite leverages user credentials, access rights, and authentication mechanisms defined by your mainframe O/S, extending those security controls to your web platform. LegaSuite also supports single sign-on authentication. Credentials are transmitted in encrypted form. LegaSuite provides configuration options that can further limit data values and form types presented to end users. These can be used to provide additional confidentiality for sensitive data, and to protect the integrity of data in the system from invalid inputs.
97.3 With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalized security credentials.	Any data transferred through LegaSuite—which may include security credentials—is encrypted according to your organization's standards to ensure confidentiality and integrity. LegaSuite supports the latest encryption protocols, including TLS1.2 and SSHv2 with strong ciphers. LegaSuite does not store or cache data, limiting exposure to potential breaches. RTS specifications also mandate masking of credentials upon display or input. LegaSuite data presentation configuration options can support masking and pseudonymization to limit the exposure of sensitive data, including credentials.

Regulatory Technical Standards on Strong Customer Authentication and Secure Communication (RTS on SCA and CSC)

PSD2 REQUIREMENTS	ROCKET LEGASUITE CAPABILITIES
27.1 Account servicing payment service providers that offer to a payer a payment account that is accessible online shall have in place at least one interface which meets each of the following requirements: (a) account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments can identify themselves towards the account servicing payment service provider; (b) account information service providers can communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions; (c) payment initiation service providers can communicate securely to initiate a payment order from the payer's payment account and receive information on the initiation and the execution of payment transactions.	All internet banking systems must make their functions available to third-party payment services through a published, available, secured API gateway. LegaSuite provides tools for securely presenting the output from these API calls to your web application users, and for formatting user input to the back-end systems.
27.3 For the purposes of authentication of the payment service user, the interfaces referred to in paragraph 1 shall allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user. In particular the interface shall meet all of the following requirements: (a) a payment initiation service provider or an account information service provider shall be able to instruct the account servicing payment service provider to start the authentication; (b) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and the payment service user(s) shall be established and maintained throughout the authentication; and (c) the integrity and confidentiality of the personalized security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider shall be ensured.	LegaSuite leverages user credentials, access rights, and authentication mechanisms defined by your mainframe O/S, extending those security controls to your web platform. LegaSuite also supports single sign-on authentication. Credentials are transmitted in encrypted form. In addition to access rights controlled through the back-end mainframe, LegaSuite provides configuration options that can further limit data values and form types presented to end users. These can be used to provide additional confidentiality for sensitive data, and to protect the integrity of data in the system from invalid inputs. All data transfers using LegaSuite are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality. The encryption protocols also ensure the integrity of the data being transferred, to prevent technical errors or malicious interference.

Rocket

rocketsoftware.com

info@rocketsoftware.com

US: 1 855 577 4323
EMEA: 0800 520 0439
APAC: 612 9412 5400

twitter.com/rocket

www.linkedin.com/
company/rocket-software

www.facebook.com/
RocketSoftwareInc

blog.rocketsoftware.com