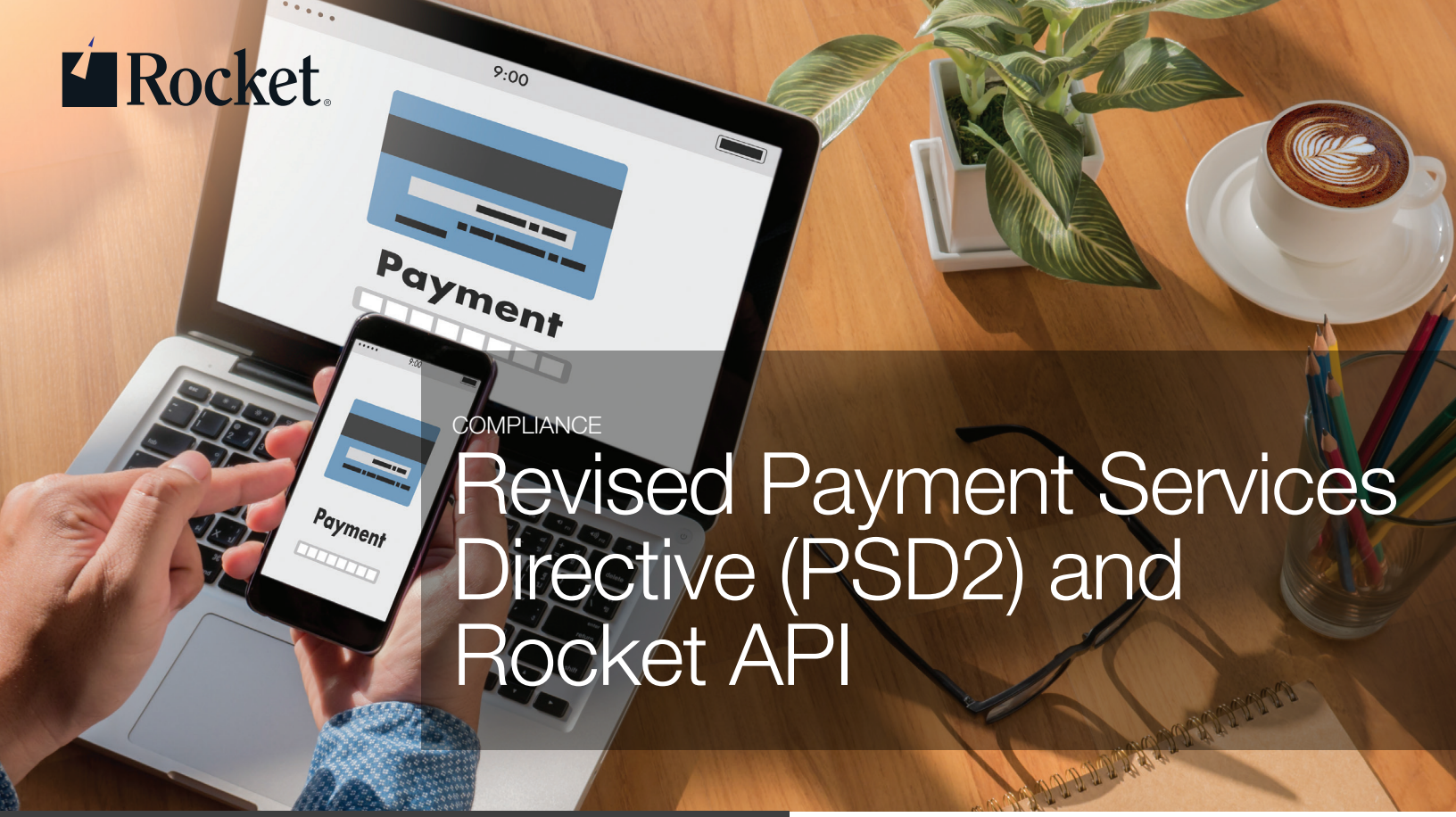

COMPLIANCE

Revised Payment Services Directive (PSD2) and Rocket API

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® API provides the tools for an organization to build these capabilities while still maintaining security. Effective management of API design and deployment to public gateways is critical to compliance. The relevant articles of PSD2 and the RTS on Strong Customer Authentication and Secure Communication, along with the associated capabilities of Rocket API, are described on subsequent pages.

Revised Payment Services Directive (PSD2)

PSD2 REQUIREMENTS	ROCKET API CAPABILITIES
66.3(e) The payment initiation service provider shall not store sensitive payment data of the payment service user.	Rocket API does not by default store any data involved with API calls, limiting the storage of such data. Customers can cache common API calls for performance reasons. Cached data is retained in memory only—not written to any permanent storage mechanism—and is erased when the Rocket API service is stopped, or at preconfigured time intervals.
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 Rocket API 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 Rocket API are secured through encrypted protocols, including TLS1.2 and SSHv2. Strong encryption provides for data security and confidentiality.
77.1 Member States shall require that, where a payment service user denies having authorized an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider. If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.	In the event of a dispute over the authenticity and integrity of a transaction, detailed system logs can provide evidence that the transaction was authenticated and accurately processed. The Regulatory Technical Standards (RTS) specify that transaction number, timestamps, and all relevant transaction data must be logged. All API calls through Rocket API are captured by your mainframe system logs, showing details of the user accessing the function, data being accessed, and data values being read and/or written. Any changes to the coding of an API that could affect the integrity of a transaction are reflected in your source control system. Any changes to the deployment of APIs are evidenced in the Rocket Access and Connectivity Hub (RACH) application logs.
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.	The RTS on Secure Customer Authentication describes multifactor authentication comprising the elements of knowledge, possession, and inherence. Rocket API leverages authentication mechanisms already configured within your mainframe environment, inheriting the security policies and configurations you have deployed. On top of the authentication security enforced through the mainframe, RACH can add an additional layer of access control through user credentials or tokens.
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 Rocket API—which may include security credentials—is encrypted according to your organization's standards, to ensure confidentiality and integrity. Rocket API supports the latest encryption protocols, including TLS1.2 and SSHv2 with strong ciphers. Rocket API does not by default store any data involved with API calls, limiting the storage of such data. RTS specifications also mandate masking of credentials upon display or input. Rocket API supports data masking and anonymization capabilities 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 API 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. Rocket API development and deployment capabilities can enable account information and payment initiation service providers the necessary access to payment accounts. The RACH extends API management capabilities, so you can easily manage all your custom-developed or open-source APIs and deploy them to all necessary API gateways. The APIs and deployment configuration can be published as necessary for third parties to utilize.
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.	Rocket API leverages access credentials from the back-end mainframe operating system, inheriting all access rights and restrictions associated with those credentials. These include read and write capabilities. In addition to access rights controlled through the back-end mainframe, Rocket API provides application-layer security that can further restrict API calls by user, by function, and by data being accessed. All data transfers using Rocket API 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 data being transferred, to prevent technical errors or malicious interference.

27.4

Account servicing payment service providers shall ensure that their interface(s) follows standards of communication which are issued by international or European standardization organizations. Account servicing payment service providers shall also ensure that the technical specification of the interface is documented and, as a minimum, available, at no charge, upon request by authorized payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied with their competent authorities for the relevant authorization. This documentation shall specify a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the account servicing payment service providers. Account servicing payment service providers shall make the summary of the documentation publicly available on their website.

Rocket API enables you to utilize public, third-party APIs developed in compliance with ISO standards, as well expose your own APIs to third parties, using standard definitions such as swagger (for REST) and WSDL (for SOAP).

27.5

Account servicing payment service providers shall ensure that, except for emergency situations, any change to the technical specification of their interface is made available to authorized payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments (or payment service providers that have applied with their competent authorities for the relevant authorization) in advance as soon as possible and not less than 3 months before the change is implemented. Payment service providers shall document emergency situations where changes were implemented and make the documentation available to competent authorities on request.

RACH manages all APIs and deployments. Strong access controls within the application, including granular role-based user access rights and integrated authentication, prevent unauthorized or inadvertent changes to API deployments.

RACH records detailed application-level audit logs that can evidence any changes to APIs and any changes to their deployment, in the event of an inquiry.

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