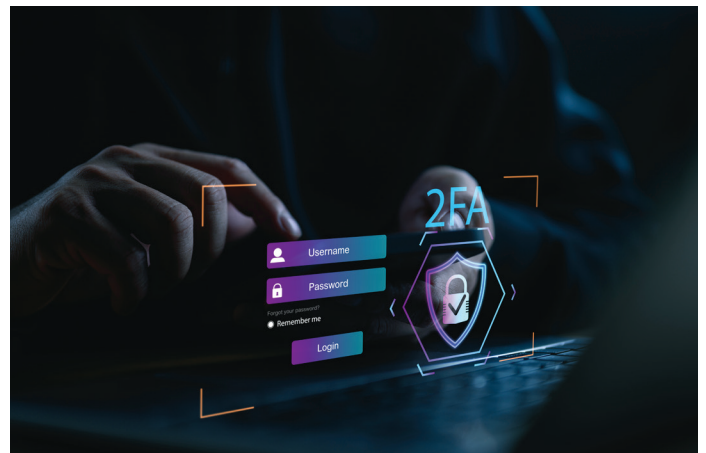


Make Modern Payments a Reality

The Ren Authorization Code Engine is used for enhanced payment security by offering an additional payment factor that is validated during payment authorizations. Used with 2-factor authentication (2FA) code, authorization code, and one-time password payment applications or to further enhance payments security from traditional channels such as ATMs or POS.

The Ren Authorization Engine includes these features:

- More Secure Payments Using 2-Factor Authentication (2FA)
 - » 2FA provides an additional layer of security by requiring consumers to perform an extra step during the payment process, typically by entering an authorization code, one-time password, or text code that is provided by their payment instrument issuing institution. Two-factor payment authentication is particularly valuable for digital payments originated using non-traditional channels.
- Generation, delivery, and validation of transaction authorization codes received for payments
- Request an authorization code for a particular “requester ID” such as a mobile phone, user ID, wallet ID, etc.
- Consumer receives SMS code on their mobile phone and supplies the code when making a payment
- Consumer registers mobile number to opt in for alerts and authorization codes using the Ren Mobile Registry feature
- Configurable authorization code validity periods (e.g., good for “X” minutes, etc.)
- Decline payments due to missing code, invalid code, expired code
- Ren API Gateway extends external consumer payment channels for:
 - » Authorization code generation and validation requests
 - » Mobile registry
 - » SMS Gateway integration



Visit us at www.renpayments.com and learn how our platform can help you revolutionize your payment operations.