modo

ENCRYPTION & CRYPTOGRAPHY AT MODO

Encryption & Cryptography is no joke at Modo. Seriously. We know you care about your data security, and we do too. At Modo, it's our goal to think through everything to do with security so you can rest assured that you're covered - even when reducing friction between payment systems.

There are three different states in which Modo encrypts data:

1. In-flight
2. At-rest
3. During authentication

"In-flight" is when you're sending data in, "At-rest" is when you're storing data, and "During authentication" is when you're proving who you are when you're storing and accessing payments data.

IN-FLIGHT

All data that is in transit from any one system to another is considered "in-flight". Modo encrypts all in flight data, using the encryption standard RSA4096, facilitating the submission of payment credentials through non-PCI intermediate systems. It also enables secure sharing of shared auth secrets using HSMs or other keystores, allowing the sharing of a secret without any human ever seeing it.

AT-REST

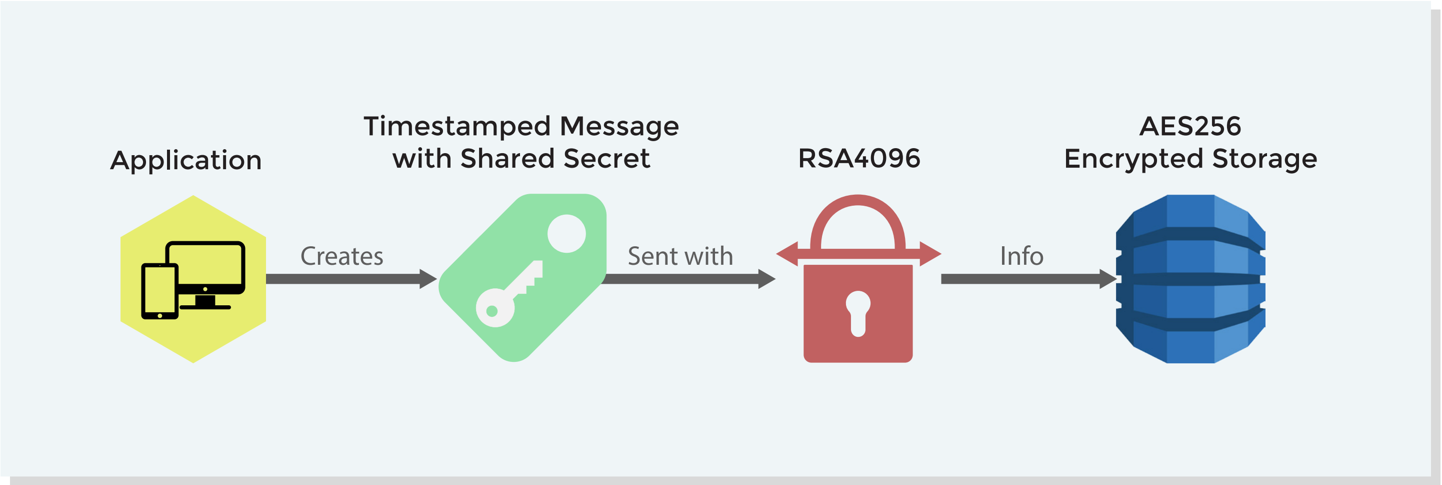
All data stored for later use is considered "at-rest". Modo encrypts all sensitive data at-rest using the encryption standard AES256. Modo utilizes a versioned encryption schema allowing us to easily switch to new algorithms, ensuring the latest and greatest security is available.

DURING AUTHENTICATION

All data that is used to prove the identity of a user when storing and accessing is encrypted during authentication. When an application makes a request to Modo with a shared secret, is assigned a unique identifier and timestamp to prevent replay and spoofing attacks. Each request is unalterable and valid only for a very short time.

WHY IS MODO BETTER?

Modo is working to reduce the friction that occurs between payment systems. We don't skimp out when it comes to security in order to do that. We use best practice cryptography techniques and deal with complex technology like HSMs so you don't have to. And, not to brag, but we're trusted and audited by some of the largest financial institutions in the world. That's just one of the reasons why we're the better way to connect payment systems.



An application creates a time-stamped message with shares secret to send to Modo, protecting it while in-flight with RSA4096. Modo then stores it at rest using AES256 encrypted storage. This ensures your data is protected at all times during the transaction.

We're a team of #paymentsgeeks that are dedicated to doing the most good for the most people by reducing friction in payments. We would love to enable interoperability and reduce payments friction for you. Reach out to us.