GLB 11284.2 Enhancing Transport Layer Security

Type:
Switching Release Announcement

Audience:
Acquirer
Issuer
Processor
Network Enablement Partner

Region:
Global

Brand:
Mastercard®
Debit Mastercard
Maestro®
Cirrus®

Release:
25.Q4

Action indicator:
Opt-in: Acquirer, Issuer

System:
Dual Message Authorization System
Dual Message Clearing System
Single Message System

Published:
17 June 2025

Effective:
4 November 2025

Executive overview

Mastercard is enhancing how customer host systems secure the connection to the Mastercard Interface Processor (MIP).

Effective date details

Date	Time	Details
4 November 2025	01:00 to 09:00 U.S. Central Time 07:00 to 15:00 UTC	Dual Message Authorization System
	18:00 to 23:59 U.S. Central Time 00:00 to 05:59 UTC (+1D)	Dual Message Clearing System
	02:00 to 05:00 U.S. Central Time 08:00 to 11:00 UTC	Single Message System

What Mastercard is doing

Mastercard is aligning to industry standards by offering Elliptic Curve Cryptography (ECC) cipher suites to encrypt transport layer security (TLS) 1.2 connections between customer hosts and the MIP. Customers may continue to use Rivest-Shamir-Adleman (RSA) ciphers, or use a combination of ECC and RSA ciphers to secure their TLS connection to the MIP.

Background

Customers connect to the Mastercard Network through the MIP, which serves as a front-end communications processor. The MIP is located on site at the customer facility or at one of Mastercard's global data centers.

Customer host systems can connect to MIP services only through specified internet protocol (IP) addresses and specified transmission control protocol (TCP) ports. The MIP permits connections only from the customer host IP addresses that Mastercard has defined. Currently, these connections are encrypted through RSA cryptography suites as a default and will continue to do so unless customers take action.

Customers wishing to encrypt connections with ECC ciphers should prepare to include these ciphers within the TLS handshake process. Customers should consult their host system documentation for more information on how to support ECC ciphers.

Customer impact

This table represents a high-level overview of the impact as detailed in later sections of this announcement.

Impact overview

Audience	Card type	System connections	Impact type	Action indicator
Acquirer	Consumer: • Credit • Debit • Prepaid Commercial: • Credit • Debit • Prepaid	Dual Message Authorization Dual Message Clearing Single Message System	Processing	Opt-in
Issuer	Consumer: • Credit • Debit • Prepaid Commercial: • Credit • Debit • Prepaid	Dual Message Authorization Dual Message Clearing Single Message System	Processing	Opt-in

Acquirer, Issuer: Opt-In

Acquirers and issuers that would like to utilize ECC must contact their Customer Implementation Services representative before beginning to include these ciphers within the TLS handshake process.

Testing

Mastercard recommends testing to support this release announcement.

Related documentation

Information relevant to this release announcement can be found in the documents available on the **Technical Resource Center** within Mastercard Connect®. Depending on timing, information provided in this release announcement may not be reflected in a manual until after the effective dates of this release announcement.

Announcements

For more information refer to *AN 4168 Mastercard Network Secured Mastercard Interface Processor (MIP) Customer Connectivity (TLS 1.2)*, Release 20.Q4.

Reference manuals

For information about Mastercard processing refer to *Secured Data Communications*.

Other media

Statements made in videos presented at the Customer Technical Conference are current when the video was recorded. Videos are currently available only for those announcements presented at the Customer Technical Conference. Mastercard may update announcements without updating the corresponding video. Refer to the most recent version of the announcement on the Technical Resource Center for the most up-to-date information.

GLB 11284 Enhancing Transport Layer Security, Customer Technical Conference, May 2025

Version history

Version history

Date	Description of change
17 June 2025	Added Other media to Related documentation
15 April 2025	Initial publication date