VISA

Visa Secure Root Certificate Update – ACS
GLOBAL

The current Visa Secure root certificate and intermediate certificate are expiring in 2022. All Visa Secure endpoints will need to update their certificate chain in their trust store and replace current end-entity certificates with end-entity certificates issued from the new Certificate Authority. This will be a multi-step process for ACS endpoints starting 1 July 2021 with individual deadlines associated to individual steps.

Current Visa CA

Root	Visa eCommerce Root
Intermediate	Visa eCommerce Issuing CA
Referred to in this document as	eCommerce G1, G1

New Visa CA

Root	Visa Public RSA Root CA
Intermediate	Visa eCommerce Issuing CA – G2
Referred to in this document as	eCommerce G2, G2

All endpoints are required to participate in the certificate replacement process, which includes:

- New Visa DS Public Certificate (aka Visa Root CA, Visa DS Public Key)
- New Intermediate Certificate Authority
- New 3DS SDK Encryption Key/Certificate
- New MPI/3DSS Connectivity Certificate(s) (for connecting with the Visa DS)
- New ACS Connectivity Certificates(s) (for connecting with the Visa DS)
- New ACS Signing Certificate(s)

Visa Secure access control server (ACS), Merchant Plug-in (MPI), 3DS Server (3DSS) and 3DS Software Development Kit (SDK) endpoints use digital certificates to authenticate during a Visa Secure online transaction. The Visa Certificate Authority (CA), which issues the digital certificates used, is updating the root certificate due to the expiration of the current eCommerce (G1) certificate chain.

This change applies to Visa Secure endpoints using 3DS 1.0.2 and EMV® 3DS.

The production Visa Secure 3DS 1.0.2 and EMV 3DS Directory Servers (DS) have been updated to support endpoint connectivity certificates that are issued from the new Certificate Authority.

All ACS signing certificates must be replaced after **1 February 2022** but before **30 April 2022** to ensure all MPI and 3DS SDK endpoints have added the new eCommerce G2 certificate train to its trust store. This ensures 3DS SDK validation of ACS Signed Content and MPI validation of PAREs continue to work as expected.

To avoid service interruption, all Visa Secure endpoints **must abide by** the detailed timelines provided below.

Endpoints that do not obtain and install new certificates will be **unable to process** Visa Secure transactions.

Endpoints **must not remove** the current eCommerce (G1) certificate chain from their trust store until notified by Visa.

Note: If you use a hosted solution for your 3DS SDK, MPI, 3DS Server or ACS service, check with your hosted solution provider to ensure they are aware of this change and are following the actions on your behalf.

Steps	Start Date [Earliest date task can be started]	End Date [Complete task by this date]	Action/Task	To Be Performed By
			Endpoints must not remove the current eCommerce (G1) certificate chain from their trust store until notified.	

Step 1	1 July 2021	31 October 2021	• **Download and add** the **new eCommerce G2 certificate** chain (root and intermediate) into the trust store
			  ○ Visa Public RSA Root CA ← this is the root certificate
			  ○ Visa eCommerce Issuing CA – G2 ← this is the intermediate certificate
				ACS endpoints

Step 2	1 February 2022	30 April 2022	• **Request and install/use** new **end-entity certificates** issued from/signed by the **new eCommerce G2 Issuing CA.**
			  ○ Connectivity Certificate(s)
			  ○ ACS Signing Certificate(s)
				ACS endpoints

			Endpoints must not remove the current eCommerce (G1) certificate chain from their trust store until notified.	

See *Visa Secure Root Certificate Update ACS - FAQs* document for more information.

Additional Information and Important Links

- To obtain the new eCommerce G2 certificate chain:

  o **All endpoints:** The **eCommerce G2 certificate** chain is available for download on the Visa Public Key Infrastructure website under
    >"Certification Authorities Certificates"
      > "Online Production Subordinate CAs"
        > "eCommerce G2."

    This certificate can also be directly downloaded by clicking the following link: eCommerce G2

    Note: This points you to the intermediate certificate (Visa eCommerce Issuing CA-G2 - "eCommerce G2"), from which you can extract the root certificate (Visa Public RSA Root CA).

- To request new end-entity certificates:

  o **ACS: Starting 1 February 2022**, to request the new (end-entity) connectivity certificates and ACS Signing certificates signed by the new **eCommerce G2 Issuing CA**, ACS endpoints must fill out the Certificate Request Form, which will be available for G2 requests on the Certificate Request Forms page at Visa Online starting 1 February 2022. The completed form should be emailed to Certificates@visa.com.
    Estimated turnaround time is 10 business days. Refer to FAQS for details.

    Note: For EMV 3DS, ACS endpoints must ensure their Visa product certification for their 3DS product is valid at the time of the 3DS certificate renewal. ACS endpoints will not be able to renew their Visa 3DS certificate if their Visa product certification has expired. To confirm whether the Visa 3DS product is still valid, ACS endpoints should refer to the Visa EMV 3DS Compliant Vendor Product List, available on the Visa Technology Partners (VTP) site. If you have any questions in relation to your Visa product certification, please visit VTP or contact Global Client Testing (GCT) 3DS Support.

31 January 2022 is the last day to request an end-entity certificate signed by the **eCommerce (G1) Issuing CA**. These G1 certificates will expire on 22 June 2022 but must be replaced with G2 certificates by 30 April 2022.