Visa Secure

Visa Secure Root Certificate Update: MPI/3DSS - Frequently Asked Questions (FAQs)

Version 6.0

12 May 2022

Visa Public

Contents

Summary of Changes

Version	***Version Date***	***Revision Reason/Purpose***
1.0	15 July 2021	Initial Release
2.0	12 August 2021	Updated tasks/timeline table. Updated Webinar details. Minor edits.
3.0	18 October 2021	Edits to existing FAQs for clarification. Additional FAQs added.
4.0	19 April 2022	Edits to existing FAQs for clarification Added Troubleshooting Tips Updated 3DS 1.0.2 and EMV 3DS 2.x Directory Server section, and include timeline table
5.0	29 April 2022	Updated to include information regarding the length/size increase of G2 Encryption Keys.
6.0	12 May 2022	Updated Timeline Table Dates for DS Migration

New Root Certificate for Visa Secure

This document is an FAQ is to accompany the Vendor Bulletin regarding the Visa Secure Root Certificate Update.

Attention: Increase in Size/Length of G2 Encryption Key

***The following is being communicated for endpoint awareness and for endpoints to assess if any actions are required. ***

Some 3DS 1.0.2 MPI endpoints have recently reported issues related to receiving PARes messages that exceed their expectations for maximum number of bytes, with examples of messages exceeding 8,192 bytes. This issue appears to be related to the increased key length of the new Visa G2 ACS Signing certificate which is embedded within the PARes message for 3DS 1.0.2.

The increase in length between the G1 encryption key and the length of the G2 encryption key has been identified as a potential contributing factor that have resulted in impacts for a small number of 3DS 1.02 MPI endpoints that have imposed limitations on the length or size of PARes messages. It is advised that all endpoints take the necessary steps to ensure that their software is capable of parsing and storing larger size PARes messages or acsSignedContent data. More detailed information can be found below.

G1 vs G2 Observations/Differences

Change in Encryption Key Length Size

The Visa eCommerce [G1] uses an encryption key length of 2048 bits. The Visa eCommerce G2 uses an encryption key length of 4096 bits. This increase in length may be impacting 3DS components as follows:

MPI:

MPI endpoints should check their software to confirm they will not have any problems parsing and storing larger size PARes messages, for example if the total PARes message length exceeds 8,192 bytes.

3DSS Continued on next page…

3DS SDK and 3DS Servers that process SDK transactions:

It is noted that the Signing certificate is also used for the data contained in the *acsSignedContent* in the ARes message for EMV 3DS 2.X.

3DS SDK and 3DS Server endpoints should check their software to confirm they will not have any problems parsing and storing larger size *acsSignedContent* data.

Note that *acsSignedContent* is defined as variable length in the EMV® 3-D Secure Protocol and Core Functions Specification so the increase in size should not present an issue.

1.1 What is Visa Secure?

Visa Secure provides merchants and issuers with cardholder authentication on e-commerce transactions. Visa Secure helps reduce e-commerce fraud by helping to ensure that the transaction is being initiated by the rightful owner of the Visa account.

1.2 What are we announcing?

Visa Secure, 3DS SDK, access control server (ACS), Merchant Plug-in (MPI) and 3DS Server (3DSS) endpoints use digital certificates to authenticate during a Visa Secure online transaction.

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 (CA). This will be a multi-step process for all endpoints starting 1 July 2021 with individual deadlines associated to individual steps.

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

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

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

Endpoints that do not obtain and install new certificates according to the process below will be **<u>unable to process</u>** Visa Secure transactions.

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

1.3 What is the timeline for the endpoints to update to the new root and end-entity certificates?

MPI/3DSS

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	MPI and 3DSS endpoints
Step 2	1 August 2021	30 April 2022	• **Request and install/use** new **end-entity certificates** issued from/signed by the **new eCommerce G2 Issuing CA.** ○ Connectivity Certificate(s)	MPI and 3DSS endpoints
Endpoints must not remove the current eCommerce (G1) certificate chain from their trust store until notified.				

1.4 What is the timeline to download the new root?

As of 1 July 2021, all endpoints (SDK, MPI, 3DSS, ACS) can begin downloading the new eCommerce G2 certificate chain into their trust store.

31 October 2021 is the deadline for all endpoints to have installed (trusted) the new eCommerce G2 certificate chain into their trust store.

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

1.5 What happens if I don’t install the new root by 31 October 2021?

Endpoints that do not install the new eCommerce G2 certificate chain into their trust store may experience Visa Secure service disruptions. This could come in the form of connectivity issues, crypto validation failures, and message failures.

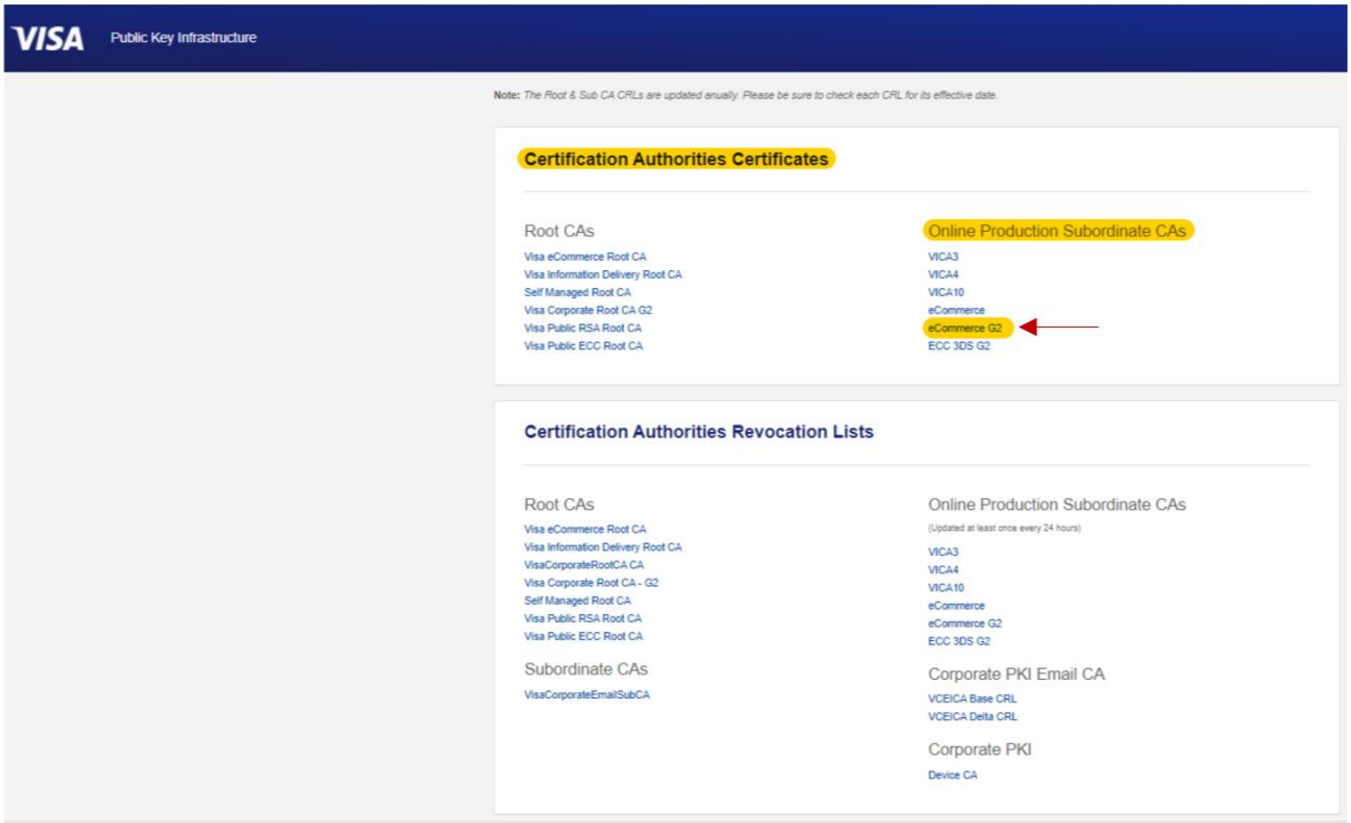
Endpoints must not remove the current eCommerce (G1) certificate chain from their trust store until notified by Visa.

1.6 Where do I download the new root certificate?

The new eCommerce G2 certificate chain can be found on the Visa Public Key Infrastructure website under > “Certification Authorities Certificates”
> “Online Production Subordinate CAs”
> “eCommerce G2.”

Quick 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).



Note: *The Root & Sub CA CRLs are updated anually. Please be sure to check each CRL for its effective date.*

Certification Authorities Certificates

Root CAs
- Visa eCommerce Root CA
- Visa Information Delivery Root CA
- Self Managed Root CA
- Visa Corporate Root CA G2
- Visa Public RSA Root CA
- Visa Public ECC Root CA

Online Production Subordinate CAs
- VICA3
- VICA4
- VICA10
- eCommerce
- eCommerce G2
- ECC 3DS G2

Certification Authorities Revocation Lists

Root CAs
- Visa eCommerce Root CA
- Visa Information Delivery Root CA
- VisaCorporateRootCA CA
- Visa Corporate Root CA - G2
- Self Managed Root CA
- Visa Public RSA Root CA
- Visa Public ECC Root CA

Subordinate CAs
- VisaCorporateEmailSubCA

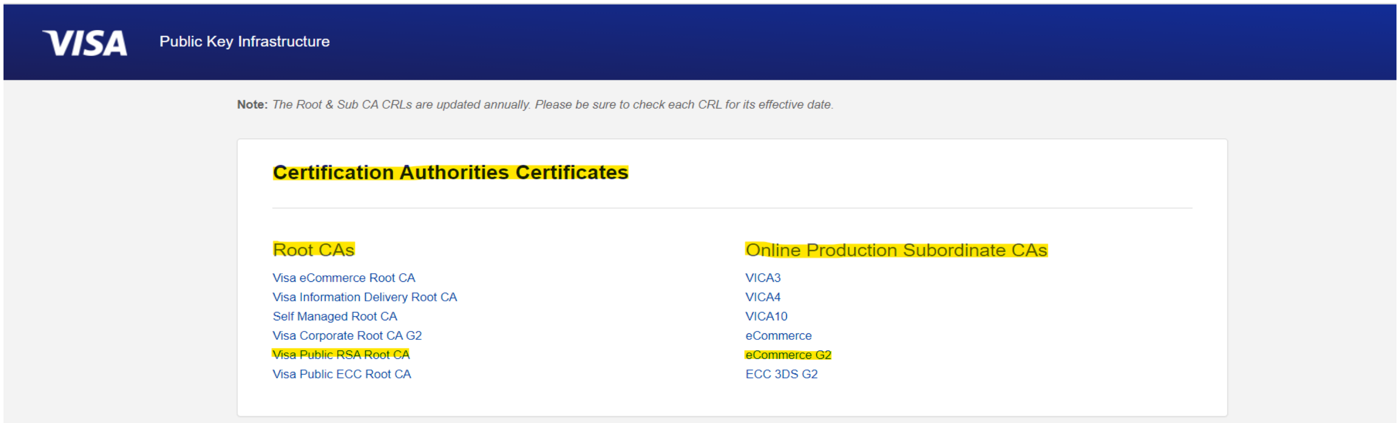
Online Production Subordinate CAs
(Updated at least once every 24 hours)
- VICA3
- VICA4
- VICA10
- eCommerce
- eCommerce G2
- ECC 3DS G2

Corporate PKI Email CA
- VCEICA Base CRL
- VCEICA Delta CRL

Corporate PKI
- Device CA

Continued on next page…

Or you can locate both the root and intermediate certificate on the Visa Public Key Infrastructure website and download each separately.



VISA Public Key Infrastructure

Note: *The Root & Sub CA CRLs are updated annually. Please be sure to check each CRL for its effective date.*

Certification Authorities Certificates

Root CAs

- Visa eCommerce Root CA
- Visa Information Delivery Root CA
- Self Managed Root CA
- Visa Corporate Root CA G2
- Visa Public RSA Root CA
- Visa Public ECC Root CA

Online Production Subordinate CAs

- VICA3
- VICA4
- VICA10
- eCommerce
- eCommerce G2
- ECC 3DS G2

New eCommerce G2 Root CA Certificate

Serial Number	51:3e:96:00:00:00:db:44:27:ee:ac:e0:be:e1:48
Validity Date	Monday, March 15, 2021 5:00:00 PM thru Thursday, March 14, 2041 5:00:00 PM

Subject Name and Issuer Name	CN = Visa Public RSA Root CA
	OU = Visa International Service Association
	O = VISA
	C = US

New eCommerce G2 Intermediate CA Certificate

Serial Number	51:3e:96:00:00:00:e5:a3:6d:84:f4:dd:e4:80:65
Validity Date	Wednesday, June 2, 2021 5:00:00 PM thru Sunday, March 10, 2041 5:00:00 PM

Subject Name and Issuer Name	CN = Visa eCommerce Issuing CA - G2
	OU = Visa International Service Association
	O = VISA
	C = US

1.7 How do I request new end-entity certificates signed by the new eCommerce G2 Issuing CA?

MPI and 3DSS: To request new end-entity certificates signed by the new eCommerce G2 Issuing CA, MPI and 3DSS endpoints will need to fill out the Certificate Request Form, which is available on the Certificate Request Forms page at Visa Online since 1 August 2021. The completed form(s) should be emailed to Certificates@visa.com.

Email Certificates@visa.com if you do not have access to Visa Online to access the forms.

Note: For EMV 3DS, 3DSS endpoints must ensure their Visa product certification for their 3DS product is valid at the time of the 3DS certificate renewal. 3DSS 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, 3DSS 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.

1.8 How long does it take to get a new end-entity certificate?

The Certificate Request Form provides specific directions and requirements for completing the form completely and accurately.

Estimated Timeframe: 10 business days from the time the Visa CA receives the certificate request to the time that the certificates are created and returned to the requestor as long as all documents and verifications are done correctly.

Note: For EMV 3DS, 3DSS endpoints must ensure their Visa product certification for their 3DS product is valid at the time of the 3DS certificate renewal. 3DSS 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, 3DSS 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.

1.9 What happens if my product is expired and I try to request a new end-entity certificate?

Your certificate request form will be rejected.

For EMV 3DS, 3DSS endpoints must ensure their Visa product certification for their 3DS product is valid at the time of the 3DS certificate renewal. 3DSS 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, 3DSS 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.

1.10 What is the deadline for installing/using the new end-entity certificates signed by/issued from the new eCommerce G2 Issuing CA?

MPI/3DSS: As of 1 August 2021, the MPI/3DSS endpoint must obtain replacement end-entity (connectivity) certificate(s) signed by/issued from the eCommerce **G2** Issuing CA and install and use by/no later than **30 April 2022**.

1.11 How do I install the certificates?

Visa cannot advise directly how to add certificates to your specific system. Refer to your application or operating system specific documentation for instructions on how to update the certificate trust store and key store, as the process for updating varies per system.

Visa strongly encourages your key management team to validate the certificates before loading them into the application/system.

1.12 When will the Visa Secure 3DS 1.0.2 and EMV 3DS 2.X Directory Servers be updated?

The new eCommerce G2 certificate chain has been added to the Visa Secure 3DS 1.0.2 and EMV 3DS 2.X Directory Server trust store.

The Visa Secure 3DS 1.0.2 and EMV 3DS 2.X Directory Servers can support endpoint connectivity certificates that are issued from the new Certificate Authority.

The Visa Secure EMV 3DS 2.X Directory Server has been updated to support the 3DS SDK Encryption Key that is issued from the new Certificate Authority.

Visa Secure's Directory Server began installing its G2 connectivity certificates across its instances on May 2nd and was to be fully completed on May 16th. However, it was determined a number of endpoints were still not compliant, so the remaining installations have been rescheduled to the dates below.

The updated dates are as follows:

Date	DS Certificate Type	Protocol
2-3 May COMPLETE	Server Certificate Presented by AHS when ACS is initiating connection to the AHS for PATransReq/PATransRes	3DS 1.0.2 AHS
~~4-5 May~~ 6-7 June	Server Certificate Presented by DS when MPI is initiating connection to the DS for VEReq/VERes	3DS 1.0.2 DS
~~6-9 May~~ 25-26 May	Client Certificate Presented by DS when DS is initiating connection to the ACS for VEReq/VERes	3DS 1.0.2 DS
16 May	Signing Certificate AACS signs the PARes during Attempts	3DS 1.0.2 AACS
~~10-11 May~~ 8-9 June	Server Certificate Presented by DS when 3DSS is initiating connection to the DS for AReq/ARes Presented by DS when ACS is initiating connection to the DS for RReq/RRes	EMV 3DS 2.X DS
~~12-13 May~~ 23-24 May	Client Certificate Presented by DS when DS is initiating connection to the ACS for AReq/ARes Presented by DS when DS is initiating connection to the 3DSS for RReq/RRes	EMV 3DS 2.X DS

Continued on next page…

These changes will be transparent to compliant endpoints that have added the G2 root certificate to their trust store as advised since July 2021.

Any end points that are non-compliant and have not yet added the G2 root certificate to their trust store will no longer be able to connect to the Directory Server after this change.

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

Additional reminder: all endpoints must have their G2 end entity certificates installed by 30 April 2022

1.13 If I use a hosted solution do I need to request new certificates?

Merchants/acquirers need to ensure that their host systems (MPI or 3DS Server providers) follow the tasks and timelines outlined here and in the VBN, as well as forthcoming Vendor Bulletins and communications.

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.

In some cases, if a client uses a hosted solution, the client does not need to request certificate(s). The hosted solution provider will request and update the certificates on the client’s behalf.

Refer to Appendix A Digital Certificates in the Visa Secure Merchant/Acquirer Implementation Guide for 3-D Secure 1.0.2.

Refer to Appendix B Digital Certificates in the Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure.

1.14 When will ACS endpoints begin using ACS Signing Certificates issued from the new eCommerce G2 Issuing CA?

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 chain to their trust store. This ensures 3DS SDK validation of ACS Signed Content and MPI validation of PARes continues to work as expected.

1.15 Does this impact both versions of 3-D Secure?

Yes, this impacts certificates used for 3-D Secure 1.0.2 and EMV 3-D Secure (2.X).

1.16 Will there be any Visa testing provided?

There is no required testing.

1.17 What if my certificate expires?

If the certificate expires it will be considered invalid and may cause a service disruption.

The endpoints must add the eCommerce **G2** certificate chain to their trust store by **31 October 2021**.

The endpoints must replace their end-entity certificate(s) prior to expiry but in line with the tasks and timelines outlined in this plan.

The MPI/3DSS endpoints must request a replacement certificate signed by/issued from the eCommerce **G2** Issuing CA and install and use by/no later than **30 April 2022**.

It is imperative that endpoints do not remove the current eCommerce (G1) certificate chain from their trust store until notified by Visa.

1.18 What is the last day to request a G1 certificate?

It is advised that all new or renewal end-entity certificates are signed by the eCommerce (G2) Issuing CA. Certificate Request Forms are being updated make the only option G2 (New eCommerce CA).

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 a G2 certificates by 30 April 2022. Requests for G1 certificates will be considered on an exception basis.

1.19 Will Visa host webinars or overview sessions?

In August and September 2021 and in January 2022, Visa hosted a series of webinars to review the Visa Secure Root Certificate update plan and answer questions. The sessions provided an in-depth review of the plan for each of the endpoints and an in-depth look at the potential impact areas and what endpoints should be doing to reduce the risk of service disruption.

The webinar presentation deck and a recording of the webinar for replay are available on the Visa Technology Partners (VTP) site.

1.20 What is the direction for new projects/endpoints?

The MPI/3DSS endpoint must add both the eCommerce **G1** certificate chain and the eCommerce **G2** certificate chain to their trust store by **31 October 2021**.

If implementing after 31 October 2021, MPI/3DSS endpoints must still add both the eCommerce **G1** certificate chain and the eCommerce **G2** certificate chain to their trust store.

MPI/3DSS endpoints must obtain the new end-entity certificate(s) signed by/issued from the new eCommerce **G2** Issuing CA and install and use by/no later than **30 April 2022**.

It is imperative that endpoints do not remove the current eCommerce (G1) certificate chain from their trust store until notified by Visa.

1.21 Does this update impact the certificates used for Visa Secure Testing Suite (VSTS)?

This Visa Secure Root Certificate Update/migration to G2 does not apply to VSTS. VSTS certificates are issued from *Visa eCommerce QA Issuing CA* (intermediate) – *Visa ecommerce QA* (root) and will not change because of the Production Visa Secure G1 to G2 certificate migration.

1.22 What are the validity periods for the G2 certificates?

The *Visa Public RSA Root CA* (root) is valid from 15 March 2021 thru 14 March 2041.

The *Visa eCommerce Issuing CA - G2* (intermediate) is valid from 2 June 2021 thru 10 March 2041.

The G2 end-entity certificates are valid for 1 year.

1.23 Inquiry Example: My end-entity certificate expires in May 2022. Do I need to obtain a new G2 end-entity certificate before May 2022?

Yes, you must replace the current G1 end-entity certificate with a new G2 end-entity certificate and install and use it by **30 April 2022**.

Endpoints cannot assume to use G1 certificates up until they expire. If an endpoint has a G1 end-entity certificate, they must replace it with a G2 end-entity certificate by the dates outlined in the plan.

1.24 Inquiry Example: We just renewed our certificates in August 2021 and received certificates signed by the G1 CA. Do we have to get new certificates?

Yes, you must replace the current G1 end-entity certificate(s) with new G2 end-entity certificate(s) and install and use them by **30 April 2022**.

1.25 Best Practices

When applicable, implement the change in only one system/server to ensure everything is working before updating others. Rotate/stagger the implementation.

For high-risk and/or high complexity changes, execute change during a low-traffic/low-volume period.

Ensure the ability to revert to the last known good configuration.

MPI endpoints should check their software to confirm they will not have any problems parsing and storing larger size PARes messages, for example if the total PARes message length exceeds 8,192 bytes.

3DS Server endpoints should check their software to confirm they will not have any problems parsing and storing larger size *acsSignedContent* data.

Note that *acsSignedContent* is defined as variable length in the EMV® 3-D Secure Protocol and Core Functions Specification so the increase in size should not present an issue.

1.26 In Summary

- By **31 October 2021**, you must add the new G2 root and intermediate certificates (the chain) to your trust store, in addition to retaining the current eCommerce (G1) chain.

- All end-entity certificates (connectivity and/or ACS Signing) will need to be replaced with new end-entity certificates signed by the new eCommerce G2 Issuing CA.
    - You must submit new Certificate Request Forms to be issued the new end-entity certificates.
    - For MPI/3DSS endpoints, this step was made available August 2021 and must be completed by **30 April 2022**.
    - For ACS endpoints, this step was made available **1 February 2022** and must be completed by **30 April 2022**.

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.

1.27 Additional Resources

For more information, refer to the program documentation available, including the Visa Secure implementation guides, from the Visa Secure section at Visa Online.

Note: For Visa Online resources, you will be prompted to log in.

1.28 More Information

Visa regional support teams are available to answer your questions. Contact the team for your region using the email address below.

North America: esupport@visa.com

Asia Pacific (AP): isupport@visa.com

Central Europe, Middle East, and Africa (CEMEA): csupport@visa.com

European Region: customersupport@visa.com

Latin America, and Caribbean (LAC): Visa's Account Support Center (ASC) through the Visa Client Support Application (VCSA), available via Visa Online

1.29 Troubleshooting Tips

If you are experiencing issues related to the G2 Certificate Migration effort. Please refer to the below suggested troubleshooting tips:

- Confirm the eCommerce G1 root certificate chain is still trusted. It has not been removed.
- Confirm the eCommerce G2 root certificate chain has been added/trusted.
- Verify that the fully qualified domain name (FQDN) matches the certificate issued.
- Verify that all the CA certificates in the CA chain are trusted. For both G1 and G2.
- Verify end-entity certificates are in the key store and CA chain is in the trust store.
- Verify that the certificates in use are not expired.
- Confirm end-entity certificates were installed correctly (for most systems this is the key store)
- Verify End Entity or Leaf CSR (Certificate Request) and Signed Certificate
- Confirm newly Signed End Entity or Leaf Certificate is correctly chained
- Confirm newly Signed End Entity or Leaf Certificate is installed on appropriate host
- Confirm, if your SAN (Subject Alternative Name) looks correct (if applicable)
- Confirm, if your DNS record and configuration looks correct

- **It is imperative that endpoints do not remove the current eCommerce (G1) certificate chain from their trust store until notified by Visa.**

1.30 Further Troubleshooting/Support

If the above troubleshooting tips did not resolve the issue, please reach out to the appropriate regional support team (as referenced in Section 1.28 of this document).

If you are experiencing critical production issues or it is outside of standard business hours, and you have exhausted the above troubleshooting suggestions. Please contact the VOCC by calling the appropriate number below **and** sending an email to VOCC-CVAS@visa.com.

Please refer to the next page (p.18) for information required by the VOCC for troubleshooting.

- VOCC 1-877-847-2577. Then select option 2.
- VOCC for LAC:1-305-328-1200. At the prompt enter 1 for English or enter 2 for Spanish or Portuguese. Then choose option 2.
- VOCC for Europe. Clients should call their country specific number below:

Andorra	+44 20 7297 14 37
Austria	+44 20 7297 14 43
Belgium	+44 20 7297 14 32
Bulgaria	+44 20 7297 14 59
Croatia	+44 20 7297 14 64
Cyprus	+44 20 7297 14 57
Czech Republic	+44 20 7297 14 42
Denmark	+44 20 7297 14 45
Estonia	+44 20 7297 14 72
Finland	+44 20 7297 14 58
France	+33 1 53 05 39 28
Germany	+49 699 201 12 11
Gibraltar	+44 20 7297 14 50
Greece	+44 20 7297 14 30
Hungary	+44 20 7297 14 36
Iceland	+44 20 7297 14 54
Ireland	+44 20 7297 14 53

Israel	+44 20 7297 14 97
Italy	+39 02 762 90 60
Latvia	+44 20 7297 14 71
Lithuania	+44 20 7297 14 70
Luxembourg	+44 20 7297 14 52
Malta	+44 20 7297 14 56
Netherlands	+44 20 7297 14 31
Norway	+44 20 7297 14 47
Poland	+48 22 164 57 55
Portugal	+351 213 58 45 09
Romania	+44 20 7297 14 40
Slovakia	+44 20 7297 14 21
Slovenia	+44 20 7297 14 38
Spain	+34 91 418 92 26
Sweden	+46 8440 35 75
Switzerland	+44 20 7297 14 41
Turkey	+90 212 290 22 20
UK	+44 20 7297 14 44

Clients must provide the following information to VOCC:

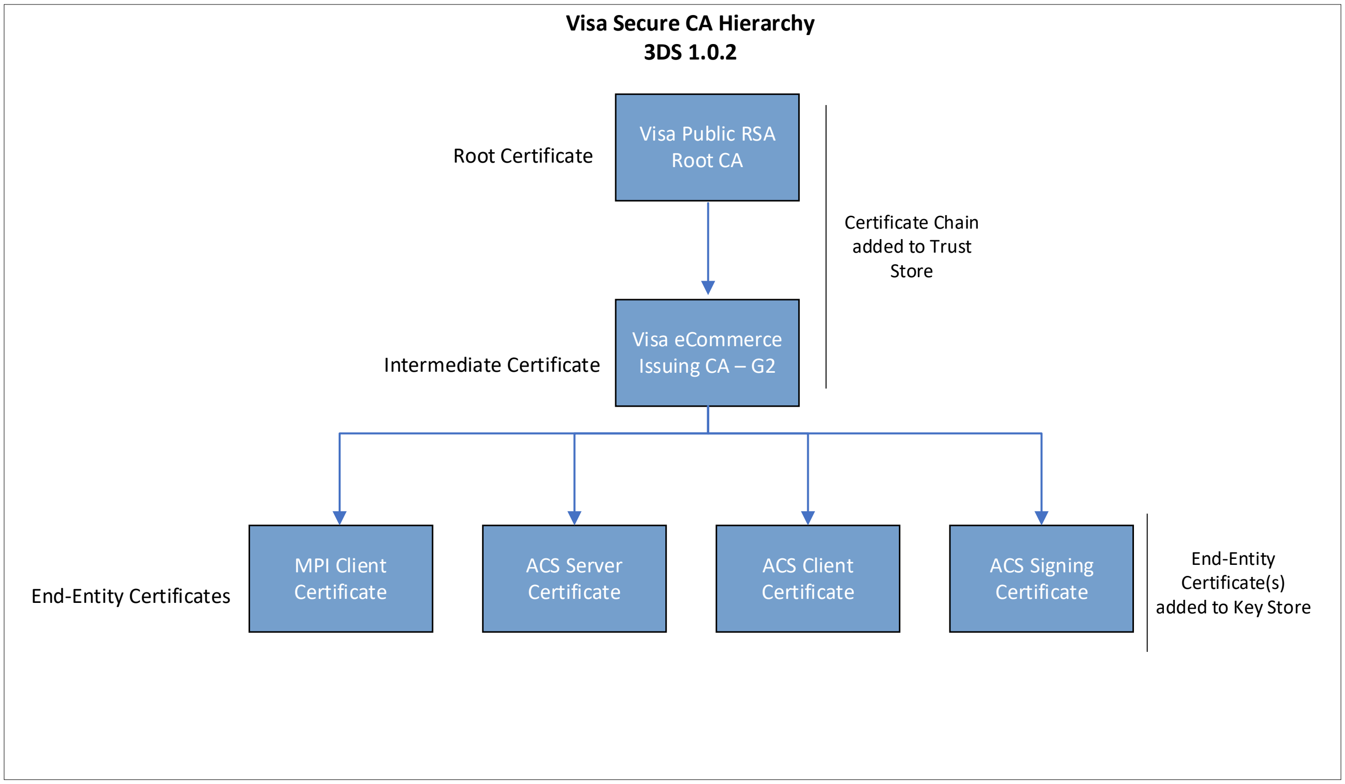
- Application URL: URL used Connect to Visa with (for example: dsec.visa3dsecure.com)
- Protocol Version: 3DS Version (3DS 1.0 or EMV 3DS)
- Client Type (Merchant or Issuer)
- Client IP (IP address of connecting client)
- Enter the Clients Port(s) (for example: 9443; 6705)
- Client Region
- Certificate Used
- TLS Version & Cipher Used (SSL - example: TLS 1.0, TLS 1.1 or TLS 1.2. Cipher - example: TLS_RSA_WITH_AES_256_GCM_SHA384)
- Detailed Error Information
  - Can you provide any sample vbvTransactionId (for 3DS 1.0) or dsTransactionId (for EMV 3DS)?
  - What transaction flow is having the issue (3DS 1.0 – VERes/Res or EMV 3DS – AReq/Res or RReq/Res)
  - Provide a screenshot of the public certificate chain used by the client to include root, intermediate, and leaf.
- Error Start Time (GMT)
- Error End Time (GMT)
- Enter TCP Packet Information (optional)

1.31 How do I install the certificates?

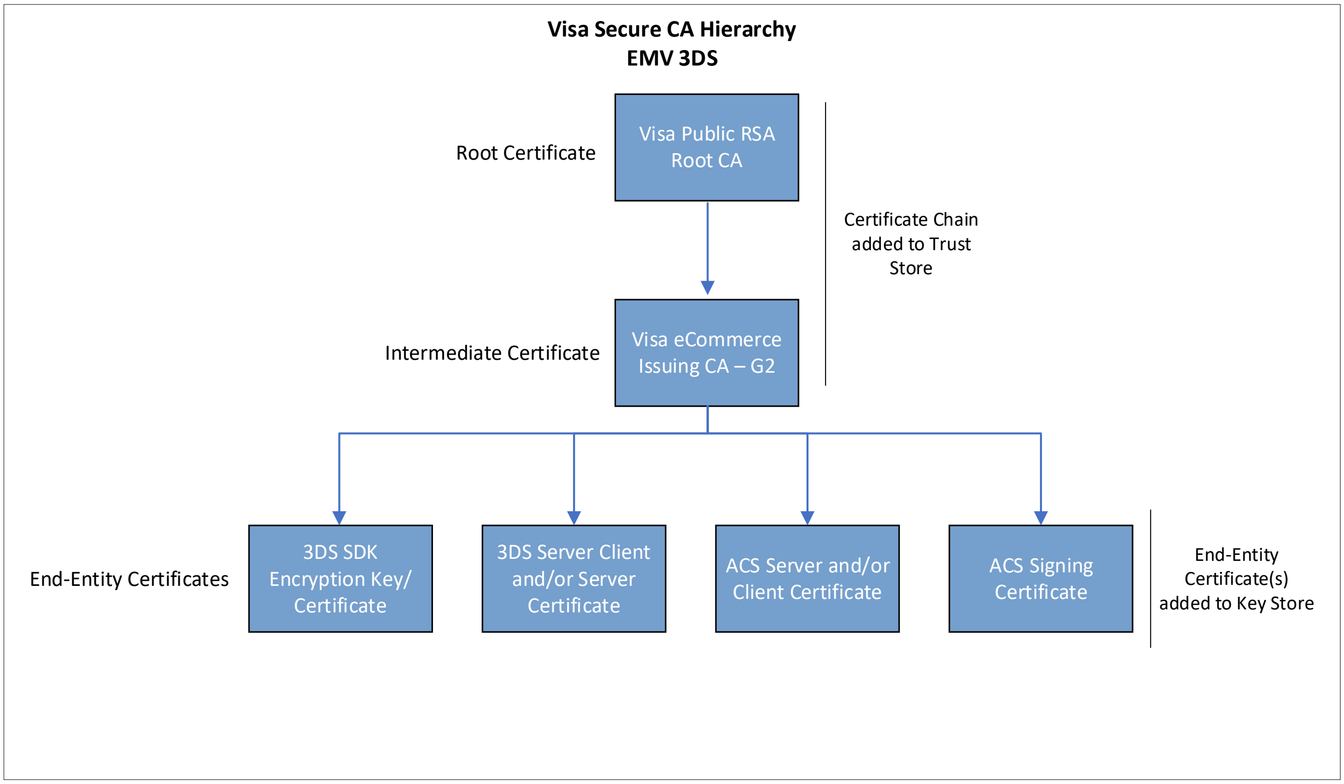
Visa cannot advise directly how to add certificates to your specific system. Refer to your application or operating system specific documentation for instructions on how to update the certificate trust store and key store, as the process for updating varies per system.

Visa strongly encourages your key management team to validate the certificates before loading them into the application/system.

1.32 Visa Secure CA Hierarchy – 3DS 1.0.2



1.33 Visa Secure CA Hierarchy – EMV 3DS



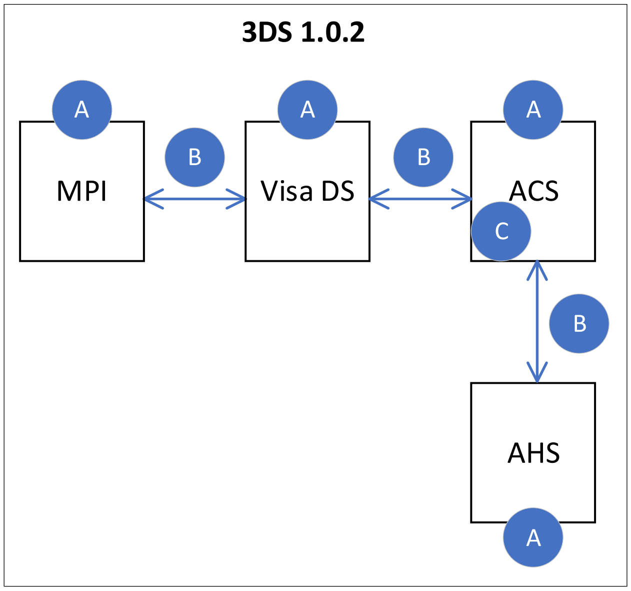
Visa Secure CA Hierarchy
EMV 3DS

Root Certificate
Visa Public RSA Root CA
Certificate Chain added to Trust Store
Intermediate Certificate
Visa eCommerce Issuing CA – G2
End-Entity Certificates
3DS SDK Encryption Key/ Certificate
3DS Server Client and/or Server Certificate
ACS Server and/or Client Certificate
ACS Signing Certificate
End-Entity Certificate(s) added to Key Store

1.34 Additional Certificate Information – 3DS 1.0.2

KEY

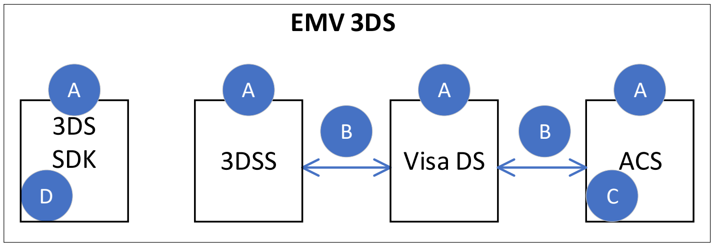
A: Visa DS Public Certificate (eCommerce G1, eCommerce G2)
B: Connectivity Certificate
C: ACS Member Signature or ACS Processor Signature Certificate



Endpoint		Certificate Type	Function
MPI, ACS	Publicly available for download	A Visa DS Public Certificate (eCommerce G2) (contains Visa DS public key, certificate chain includes root and intermediate certificates) also referred to as: Visa DS Public Key, Visa Root certificate, Root CA certificate	Used by the MPI and ACS to verify/authenticate the DS when establishing a connection (2-way TLS/SSL)
MPI	Requires Certificate Request Form submitted to Certificates@visa.com	B MPI Connectivity (Client)	Connectivity with DS (For MPI to post VEReq/CRReq to and receive VERes/CRRes from Visa DS)
ACS	Requires Certificate Request Form submitted to Certificates@visa.com	B ACS Connectivity (Server Only)	Connectivity with DS (For Visa DS to post VEReq to and receive VERes from ACS)
		ACS Connectivity (Client Only)	Connectivity with AHS (For ACS to post PATranReq to and receive PATranRes from Visa AHS)
		C S Member Signature -or- ACS Processor Signature	Used by ACS to sign the PARes in the authentication flow

1.35 Additional Certificate Information – EMV 3DS

KEY
A: Visa DS Public Certificate (eCommerce G1, eCommerce G2)
B: EMV Connectivity Certificate
C: EMV ACS RSA Signing Certificate
D: EMV 3DS SDK Encryption Key



Endpoint		Certificate Type	Function
3DS SDK 3DSS ACS	Publicly available for download	A Visa DS Public Certificate (eCommerce G2) (contains Visa DS public key, certificate chain includes root and intermediate certificates) also referred to as: Visa DS Public Key, Visa Root certificate, Root CA certificate	Used by the 3DS SDK to validate the signed content sent from the ACS for a challenge flow -- Used by the 3DSS and ACS to verify/authenticate the DS when establishing a connection (2-way TLS/SSL)
3DS SDK	Available for download. Link provided as requested.	D 3DS SDK Encryption Key Also referred to as: Device Info Encryption Key	Used by the 3DS SDK to encrypt device info content
3DSS	Requires Certificate Request Form submitted to Certificates@visa.com	EMV 3DSS RSA Connectivity (Combined Server & Client)	Connectivity with DS
		B EMV 3DSS RSA Connectivity (Server Only)	
		EMV 3DSS RSA Connectivity (Client Only)	
ACS	Requires Certificate Request Form submitted to Certificates@visa.com	EMV ACS RSA Connectivity (Combined Server & Client)	Connectivity with DS
		B EMV ACS RSA Connectivity (Server Only)	
		EMV ACS RSA Connectivity (Client Only)	
		C EMV ACS RSA Signing	Used by ACS to sign content between the ACS and the 3DS SDK for a challenge flow