Visa Secure FAQs:

Platform Updates

Version 1.0

December 2022

Visa Public

Contents

1 Overview

Visa is announcing changes to the previously communicated schedule for Visa Secure platform updates. The updated schedule will help ensure Access Control Server (ACS) Providers and EMV 3DS Server (3DSS) providers have sufficient time to prepare their associated enhancements and avoid service interruptions. Visa is also reminding endpoints of required actions that are recommended to be taken immediately to ensure compliance prior to the platform updates. The upcoming platform updates are:

- Implementation of Visa EMV 3DS 2.X Directory Server (DS) instance in Basingstoke, UK Data Center (OCB)
- Implementation of Visa EMV 3DS 2.X Directory Server (DS) instances in India Data Centers (OCIB and OCIM)
- Implementation of India-specific URLs for India based EMV 3DS 2.X 3DS Server endpoints
- Inclusion of US Token Ranges in the Preparation Response (PRes) Message
- Guidance for the DS Reference Number field

This document contains frequently asked questions regarding these upcoming platform updates.

1.1 Audience

This document will provide useful information and action steps on upcoming Visa Secure platform updates.

- Endpoints using EMV 3DS
- Issuer ACS Providers
- 3DSS Providers

1.2 External Communications

These platform updates have been communicated in previous Release Notes, Endpoint Communications, and Visa Business News (VBN) articles.

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

1.2.1 Visa Business News

"Changes to the Implementation Schedule for Visa Secure Platform Updates and Reminders of Required Actions" *Visa Business News, 6 October 2022*

"Implementation of Visa EMV 3DS 2.X Directory Server Instances in India Data Centers" *Visa Business News, 11 August 2022*

"Enhancements to India Processing" *Visa Business News, 16 June 2022*

"New EMV 3DS Directory Server for Visa Secure in the UK" *Visa Business News, 2 June 2022*

"Visa Secure Platform: May 2022 Update and Release Notes" *Visa Business News, 3 March 2022*

"Visa Secure Platform: August 2021 Update and Release Notes" *Visa Business News, 8 July 2021*

1.2.2 Visa Secure Related Documents

- Visa Secure May 2022 Release Notes
- Visa Secure August 2021 Release Notes
- Technical Specification Guide for Enhancements in India Processing

1.3 Region Contacts

For questions about the platform updates in your locality, contact your Visa Secure Regional Contact as shown below:

North America: esupport@visa.com

Latin America and Caribbean (LAC): Open Ticket through ASC on VOL

Asia Pacific (AP): isupport@visa.com

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

European Region: customersupport@visa.com

1.4 Required Actions

Required Actions by Platform Update:

Platform Update	*ACS Providers*	*3DSS Providers*	*Issuers, Acquirers, and Merchants*
New Directory Server Instances (One in the UK and Two in India)	**All** ACS providers must be able to support inbound and outbound connections with the new instances of the Visa Secure DS. **Action**: Firewall rules or allow lists must be updated with the new IP addresses. Please make the required changes **immediately** to ensure readiness by **15 February 2023**	**All** 3DSS providers must be able to support inbound and outbound connections with the new instances of the Visa Secure DS. **Action**: Firewall rules or allow lists must be updated with the new IP addresses. Please make the required changes **immediately** to ensure readiness by **15 February 2023**	**Action**: **Contact and confirm** that your service provider has completed **all** their required actions. Failure to complete the required changes will result in failed transactions.
India specific URLs	*No required changes.*	**Non-India Based 3DSS Providers:** *No required changes.* Continue to use the existing single global URL to connect to the DS. **India Based 3DSS Providers:** Prepare systems to use the new India-specific URLs to process domestic and cross-border authentication transactions. India-located 3DSS must use the India specific URLs effective **June 2023. (Exact date to be announced)**	
Inclusion of US Token Ranges in the PRes Message	*No required changes*	**Action**: **All** 3DSS providers should plan for the overall size of the PRes to be as many as 2 million ranges and be prepared for this volume to grow to at least 5 million ranges by July 2023 **Action**: **All** 3DSS providers should implement fallback logic to proceed with submitting an EMV 3DS 2.1 authentication request in the event they are unable to successfully process the PRes message.	
Guidance for the DS Reference Field	**Does not treat dsReferenceNumber as a static value:** *No required changes.* **Treats dsReferenceNumber as a static value:** **Action**: Make changes to support the DS Reference Number value changing over time. **This field must not be treated as a static value.**		

2 Summary of Platform Updates

2.1 What platform updates are clients getting additional time to prepare for?

Clients are getting more time to prepare for the following upcoming platform updates:

- Implementation of Visa EMV 3DS 2.X DS instance in Basingstoke, UK Data Center (OCB)
- Implementation of Visa EMV 3DS 2.X DS instances in India Data Centers (OCIB and OCIM)
- Implementation of India-specific URLs for India based EMV 3DS 2.X 3DS Server endpoints
- Inclusion of US Token Ranges in the Preparation Response (PRes) Message
- Guidance for the DS Reference Number field

These updates have been communicated in previously sent Release Notes, Endpoint Communications, and VBNS listed in section 1.2 of this document.

2.2 When will the platform updates be enabled?

Platform Update	Target Go Live Date[1]
New DS instance in Basingstoke, UK (OCB)	Week of 24 April 2023
New DS instances in India (OCIB and OCIM)	June 2023
India-specific URLs for India EMV 3DS 2.X	June 2023
Inclusion of US Token Ranges in the Preparation Response (PRes) Message	After June 2023
Guidance for the Visa EMV 3DS DS Reference Number field	N/A Endpoints should implement required changes as soon as possible

[1] The schedule for all features, changes, enhancements, and product releases are subject to change at Visa's discretion.

2.3 Why were these changes delayed?

Validation runs for these platform changes have indicated that the Visa Secure ecosystem participants are not prepared for the updates to go live during 2022. To prevent service impacts, Visa is allowing additional time for the ecosystem participants to prepare.

3 3DSS Frequently Asked Questions

3.1 New Directory Server (DS) Instances

3.1.1 What are the new DS instances?

Visa's Interoperability Domain Directory Server (DS) will now be hosted in three additional data centers to further support operational resiliency and availability. One instance (OCB) will be established in the Basingstoke Data Center and the remaining two instances (OCIB and OCIM) will be established in the Mumbai and Bangalore Data Centers in India. These additional DS instances are in addition to the two existing instances in the US.

3.1.2 What actions are required by the 3DSS for this update?

All 3DSS should always perform a DNS look-up to determine the Visa Secure EMV 3DS DS IP addresses.

New DS in Basingstoke, UK (OCB)

All EMV 3DS endpoints must be able to support inbound and outbound connections with the Basingstoke instance of the Visa Secure DS. 3DSS must add or update any firewall rules and allow lists with the new IP addresses. The Basingstoke DS (OCB) IP addresses are available in the *Visa Secure May 2022 Release Notes* located on the Visa Secure Documentation page of Visa Online.

The existing global URL will continue to be used by the non-India-located endpoints to connect to the Visa Secure DS. This will not change with the addition of the new DS instance (OCB) in the UK. The global URL can be found in the Visa Secure Implementation Guides located on the Visa Secure Documentation page of Visa Online.

New DS instances in India (OCIB and OCIM):

All India-located 3DSS must be able to support inbound and outbound connections with the new India instances (OCIB and OCIM) of the Visa Secure DS. India-located 3DSS must add or update any firewall rules and allow lists with the new IP addresses.

More detailed information regarding the India-specific URLs and the India DS instances (OCIB and OCIM) IP addresses can be found in the Technical Specification Document for Enhancements in India Processing located on the Visa Secure Documentation page of Visa Online.

Note that the additional IP addresses are in addition to the existing IP addresses and will not be replacing them.

3.1.3 Where can I find the IP addresses?

The Basingstoke DS (OCB) IP addresses are available in the updated Visa Secure May 2022 Release Notes[2], Version 2.0. The India (OCIB and OCIM) IP addresses are available in the Technical Specification Document for Enhancements in India Processing , Version 2.0.

These documents can be found on Visa Online, where you will be prompted to log in. If you do not have access to Visa Online, please contact your issuer or acquirer to retrieve this information.

3.1.4 What will happen if these changes are not completed in time?

Failure to update any firewall rules and allow list with the new IP addresses will result in connection failures, intermittent service disruptions, and authentication transaction failures.

3.1.5 Is Visa removing or replacing any of the existing DS instances?

No, Visa will not be removing or replacing the existing DS instances or their IP addresses. The new DS instances are in addition to the existing instances.

3.1.6 As the DS instance changes impact ACS and 3DSS, is there anything issuers, acquirers or merchants need to do?

Issuers, acquirers, and merchants should contact their service provider to confirm all the required actions have been completed. Failure by the service provider to complete the required changes will result in service interruptions and failed authentications for the issuers, acquirers, and merchants.

3.1.7 We already perform a DNS look-up prior to connecting to the DS. Do we need to perform any additional actions regarding our firewall rules or allow lists?

A DNS look-up should always be performed to determine the Visa Secure EMV 3DS DS IP addresses.

[2] Direct download to document

However, there may still be firewall rules or allow lists in place that could restrict or hamper connections to the new DS instances.

It is required that all endpoints verify that both their firewalls and allow lists are configured to allow both outbound and inbound traffic to and from the new IP addresses. As the new instances of the DS are enabled, the DNS look-up could return the new IP addresses of the new instances.

3.1.8 If an endpoint is not located in either the UK or India, are they required to make any changes?

Yes, **all 3DSS globally** must be able to establish inbound and outbound connections with the Basingstoke DS (OCB). These actions are in addition to maintaining connections to the existing DS instances.

All India-located 3DSS are required to take the necessary actions to establish inbound and outbound connections to the India instances of the Visa Secure DS (OCIB and OCIM).

3.1.9 Can 3DSS send all authentication requests to the Basingstoke DS as their primary connection?

No, Visa does not allow primary or preferred connections to specific instances of the Directory Servers.

All non-India located 3DSS will continue to connect to the Visa Secure Directory Sever using the **existing single global URL**.

When instructed to, only 3DSS located in India will begin to use the India-specific URLs as their primary connection.

3.1.10 Should 3DSS located in India send all authentication requests to the India instances?

Yes, India-located 3DSS should send all Authentication Requests (AReq) to the India DS instances (OCIB and OCIM) using the India-specific URL for AReq processing, once the India DS instances are live.

Also, India-located 3DSS should send all Preparation Requests (PReq) to the India DS instances (OCIB and OCIM) using the India-specific URL for PReq processing, once the India DS instance are live.

3.1.11 Will endpoints have to update the IP addresses in the future if Visa changes them or adds additional instances of the DS?

Yes, all Visa Secure IP addresses are subject to change. EMV 3DS endpoints should always perform a DNS lookup to determine the Visa Secure Directory Server IP addresses.

3.1.12 What types of testing is Visa executing related to the new DS instances?

Visa will be conducting limited scope outbound (from the DS) testing to determine endpoint readiness for this change.

As the EMV 3DS transactional flows are bidirectional it is important that endpoints perform their own tests to ensure that both inbound and outbound connections can be established to the new Directory Server instances.

3.1.13 Is there going to be heightened monitoring after the new DS instances go live?

Yes there will be heightened monitoring as there is with any major change to the Visa Secure platform. Visa will be increasing the monitoring of the ecosystem both during and following the implementation period. Additionally, all endpoints should continue to closely monitor their systems and pay close attention to any communications from Visa.

3.1.14 When will Visa enable the new Directory Server instances?

The Basingstoke, UK DS instance (OCB) is scheduled to be enabled in April 2023.

The India DS instances (OCIB and OCIM) are scheduled to be enabled in June 2023.

3.1.15 When should endpoints complete their required changes?

All endpoints should have all changes complete by **15 February 2023** to comply with readiness and prevent service interruptions once the DS instances are live. This will allow endpoints to be prepared for Visa's validation executions which may begin as early as16 February 2023 to confirm ecosystem readiness for the new DS instances.

3.2 Endpoint Self-testing for DS Connectivity

3.2.1 Are there any additional actions endpoints can take to ensure their readiness for the new instances of the DS?

Endpoints have the ability to execute limited self-testing to determine their ability to connect to the new instances of the DS. Additionally, endpoints may have their own internal tools or functions to test the EMV 3DS flows (PReq/PRes, AReq/ARes, RReq/RRes).

Visa also recommends endpoints execute telnet commands to verify that connectivity can be established. Endpoints will need to perform a separate telnet command for each IP Address or URL that

they are trying to verify connectivity to. For further details about self-testing endpoints should contact their Issuer or Acquirer.

3.2.2 What response should the endpoint expect to receive if the connection is successful?

When executing the self-testing telnet commands endpoints should receive a "Connected to" response indicating the domain IP address and port number. Examples of potential responses are below[3]:

A Successful connection response to the OCB instance of the Visa Secure DS:

** Trying 123.456.789.111:222...*
** TCP_NODELAY set*
** Connected to 123.456.789.111 (123.456.789.111) port 222 (#0)*

A Successful connection response to the India-specific URL:

** Trying 123.456.789.111:222...*
** TCP_NODELAY set*
** Connected to xxx.visa.com (123.456.789.111) port 222 (#0)"*

3.2.3 What should an endpoint do if they do not receive the "Connected" response?

If a "connected" response is not received, endpoints should verify they do not have any firewall rules, allow list, or other configurations that could interfere with the connection inbound or outbound to the Visa DS.

3.3 India-Specific URLs for India 3DS Servers

3.3.1 What will the India-specific URLs be used for?

The India-specific URL will be required to process India domestic and any cross-border authentication transactions that originate in India.

Additionally, the new India-specific URL for PReq/PRes will be required for the PReq/PRes message flow. This requirement will apply to all India-located 3DSS.

[3] These are examples and are not the actual values.

3.3.2 What are the required actions to prepare for the India-specific URLs?

See the table below for more information and required actions:

3DS Server Providers	ACS Providers	Issuers and Merchants
• **Non-India-located 3DS Server providers:** No changes. Continue to use the existing single global URL to connect to the Visa Secure DS. • **India-located 3DS Server providers:** Prepare systems to use the new India-specific URLs to process domestic and cross-border authentication transactions. The deadline for this action is **June 2023 (exact date to be announced)**.	Not Applicable	• **Issuers:** Not applicable. • **Merchants:** Contact and confirm your service provider has completed all required actions. • Failure to complete the required changes will result in service interruptions. The exact dates for implementation will be communicated in 2023.

3.3.3 Are the above actions in addition to the changes required for the new IP addresses?

Yes India-located 3DSS must use the new India specific URLs in order to process India domestic and cross-border authentication transactions after the India DS instances (OCIB and OCIM) go live.

3.3.4 When should India-located endpoints start connecting to the India-specific URLs?

Visa will be communicating the implementation date in future communications. It is currently planned for implementation shortly after the go-live of the India DS instances (OCIB and OCIM) in June 2023.

3.4 Guidance for the DS Reference Number field

3.4.1 Why is Visa updating the guidance for the DS Reference Number field?

The DS Reference Number value is subject to change each time Visa certifies or recertifies its DS product with EMVCo, thus, Visa recommends that the dsReferenceNumber field is not treated as a static value. To prepare for updates to the DS Reference Number all ACS and 3DSS that currently treat this field as a static value must make changes to support the value changing over time. Clients will be notified before a new DS Reference Number is utilized by the DS.

3.4.2 What are the required actions to support the DS Reference Number?

It is mandatory that any 3DSS Providers who currently treat this field as a static value (i.e., to identify Visa) make changes to that support the value changing over time. Thus, the value of the dsReferenceNumber field should not be treated as static.

3.4.3 Will there be any Visa testing provided or required for this update?

Testing is not available for this update.

3.4.4 If an endpoint has already made changes to treat the DS Reference Number as a non-static value, are there any additional steps required?

If an endpoint is enabled to **not** treat the dsReferenceNumber field as **static** and can support changes to Visa's DS Reference Number value, no additional steps are required.

3.5 US Token Ranges in PRes Message

3.5.1 What is the Preparation Request / Response Message (PReq/PRes)

The Preparation Request (PReq) message is a 3-D Secure message sent from the 3DS Server to the DS to request the ACS and DS Protocol Version(s) that correspond to the DS card ranges as well as an optional 3DS Method URL to update the 3DS Server's internal storage information.

The Preparation Response (PRes) message is the response to the PReq message that contains the DS Card Ranges, active Protocol Versions for the ACS, and DS and 3DS Method URL so that updates can be made to the 3DSS internal storage.

3.5.2 What is the impact for 3DSS on the inclusion of US Token Ranges into the PRes Message?

After the inclusion of the US token ranges, endpoints should plan for an estimated 300k additional token ranges in the PRes message. 3DSS should plan on the number of card ranges in the PRes to continue to grow in size and be able to handle at least 5M ranges in the next 12 months.

3DSS providers will need to account for these changes and update their cache or memory allocation accordingly for the additional token ranges shared by the DS. Visa recommends 3DSS update their systems accordingly as soon as possible and perform a full download after the US region's token ranges are added. 3DSS should also consider increasing the current PRes timeout setting to handle the additional data.

3.5.3 Are non-US based 3DSS providers required to make changes to support this update?

Yes, 3DSS providers globally are required to make this change to process the PRes message correctly.

3.5.4 Will this change be implemented for the other regions as well?

The inclusion of token ranges for all other regions was enabled February 2022 through April 2022.

3.5.5 What happens if an error code is received?

If a full download is not completed, the Visa Secure Directory Server will return error code "307" (Serial Number Not Valid) whenever the number of changes in a given response exceeds a threshold which is configurable in the DS. If a 3DSS receives this error message they should resend a PReq without a Serial Number to download the list of all current ranges.

Additionally, it is recommended that 3DSS implement fallback logic to proceed with submitting an EMV 3DS 2.1 authentication request in the event they are unable to successfully process the PRes message.

3.5.6 Where can I find documentation about the PReq/PRes?

Please refer to the EMVCo website for the EMV 3D-Secure Specifications.
https://www.emvco.com/emv-technologies/3d-secure/

3.5.7 Will there be any Visa testing provided or required for this update?

There is no testing available through Visa for this update. However, 3DSS must test their systems ability to process an increased sized PRes message.

3.5.8 Is there going to be heightened monitoring after this update is enabled?

Yes, there will be heightened monitoring as there is with any major change to the Visa Secure platform. Visa will be increasing the monitoring of the ecosystem both during and following the deployment period.

Additionally, all endpoints should continue to closely monitor their systems and pay close attention to any communications from Visa.

3.5.9 Can Visa provide endpoints with a sample load file to test with?

No, Visa will not provide a sample PRes file for testing.

4 ACS Frequently Asked Questions

4.1 New Directory Server Instances

4.1.1 What are the new Directory Server instances?

Visa's Interoperability Domain Directory Server (DS) will now be hosted in three additional data centers to further support operational resiliency and availability. One instance (OCB) will be established in the Basingstoke Data Center and the remaining two instances (OCIB and OCIM) will be established in the Mumbai and Bangalore Data Centers in India. These additional DS instances are in addition to the two existing instances in the US.

4.1.2 What actions are required by ACS for this update?

All ACS should always perform a DNS lookup to determine the Visa Secure EMV 3DS DS IP addresses.

New DS in Basingstoke, UK (OCB)

All EMV 3DS endpoints must be able to support inbound and outbound connections with the Basingstoke instance (OCB) of the Visa Secure DS. ACS must add or update any firewall rules and allow lists with the new IP addresses. The Basingstoke (OCB) IP addresses are available in the *Visa Secure May 2022 Release Notes* located on the Visa Secure Documentation page of Visa Online.

The existing global URL will continue to be used to connect to the Visa Secure DS; this will not change with the addition of the new DS in the UK (OCB). The global URL can be found in the Visa Secure Implementation Guides located on the Visa Secure Documentation page of Visa Online.

New DS instances in India (OCIB and OCIM):

All ACS must be able to support inbound and outbound connections with the India instances (OCIB and OCIM) of the Visa Secure DS to facilitate cross-border transactions in India.

All ACS must add or update any firewall rules and allow lists with the new India DS instances (OCIB and OCIM) IP addresses.

More detailed information regarding the India-specific URLs and the India DS instances (OCIB and OCIM) IP addresses can be found in the Technical Specification Document for Enhancements in India Processing located on the Visa Secure Documentation page of Visa Online.

Note that the new IP addresses are in addition to the existing IP addresses and will not be replacing them.

4.1.3 Where can I find the IP addresses?

The Basingstoke DS (OCB) IP addresses are available in the updated Visa Secure May 2022 Release Notes[4], Version 2.0. The India DS (OCIB and OCIM) IP addresses are available in the Technical Specification Document for Enhancements in India Processing.

These documents can be found on Visa Online, where you will be prompted to log in. If you do not have access to Visa Online, please contact your issuer or acquirer to retrieve this information.

4.1.4 What will happen if these changes are not completed in time?

Failure to update any firewall rules and allow list with the new IP addresses will result in connection failures, intermittent service disruptions, and authentication transaction failures.

4.1.5 Is Visa removing or replacing any of the existing DS instances?

No, Visa will not be removing or replacing the existing Directory Server instances or their IP addresses. The new Directory Server instances are in addition to the existing instances.

4.1.6 As the DS instance changes impact ACS and 3DSS, is there anything issuers, acquirers or merchants need to do?

Issuers, acquirers, and merchants should contact their service provider to confirm all the required actions have been completed. Failure by the service provider to complete the required changes will result in service interruptions and failed authentications for the issuers, acquirers, and merchants.

4.1.7 We already perform a DNS look-up prior to connecting to the DS. Do we need to perform any additional actions regarding our firewall rules or allow lists?

A DNS look-up should always be performed to determine the Visa Secure EMV 3DS DS IP addresses.

However, there may still be firewall rules or allow lists in place that could restrict or hamper connections to the new DS instances.

[4] Direct download to document

It is required that all endpoints verify that both their firewalls and allow lists are configured to allow both outbound and inbound traffic to and from the new IP addresses. As the new instances of the DS are enabled, the DNS look-up could return the new IP Addresses of the new instances.

4.1.8 If an endpoint is not located in either the United Kingdom or India, are they required to make any changes?

Yes, **all ACS globally** must be able to establish inbound and outbound connections with the Basingstoke DS (OCB). These actions are in addition to maintaining connections to the existing DS instances.

All ACS globally are required to take the necessary actions to establish inbound and outbound connections to the India instances of the Visa Secure DS (OCIB and OCIM).

4.1.9 Can ACS send all authentication requests to the Basingstoke DS (OCB) as their primary connection?

No, Visa does not allow primary or preferred connections to specific instances of the Directory Servers.

4.1.10 Will endpoints have to update the IP addresses in the future if Visa changes them or add additional instances of the DS?

Yes. All Visa Secure IP addresses are subject to change. EMV 3DS endpoints should always perform a DNS lookup to determine the Visa Secure Directory Server IP addresses.

4.1.11 What types of testing is Visa executing related to the new DS instances?

Visa will be conducting limited scope outbound (from the DS) testing to determine endpoint readiness for this change.

As the EMV 3DS transactional flows are bidirectional it is important that endpoints perform their own tests to ensure that both inbound and outbound connections can be established to the new Directory Server instances.

4.1.12 Is there going to be heightened monitoring after the new DS instances go live?

Yes, there will be heightened monitoring as there is with any major change to the Visa Secure platform. Visa will be increasing the monitoring of the ecosystem both during and following the implementation period. Additionally, all endpoints should continue to closely monitor their systems and pay close attention to any communications from Visa.

4.1.13 When will Visa enable the new Directory Server instances?

The Basingstoke, UK DS instance (OCB) is scheduled to be enabled in April 2023.

The India DS instances (OCIB and OCIM) are scheduled to be enabled in June 2023.

4.1.14 When should endpoints complete their required changes?

All endpoints should have all changes complete by **15 February 2023** to comply with readiness and prevent service interruptions once the DS instances are live. This will allow endpoints to be prepared for Visa's validation executions beginning 16 February 2023 to confirm ecosystem readiness for the new DS instances.

4.2 Endpoint Self-testing for DS Connectivity

4.2.1 Are there any additional actions endpoints can take to ensure their readiness for the new instances of the DS?

Endpoints have the ability to execute limited self-testing to determine their ability to connect to the new instances of the DS. Additionally, endpoints may have their own internal tools or functions to test the EMV 3DS flows (PReq/PRes, AReq/ARes, RReq/RRes).

Visa also recommends endpoints execute telnet commands to verify connectivity can be established. Endpoints will need to perform a separate telnet command for each IP Address or URL that they are trying to verify connectivity to. For further details about self-testing endpoints should contact their Issuer or Acquirer.

4.2.2 What response should the endpoint expect to receive if the connection is successful?

When executing the self-testing telnet commands endpoints should receive a "Connected to" response indicating the domain IP address and port number. Examples of potential responses are below[5]:

A Successful connection response to the OCB instance of the Visa Secure DS:

** Trying 123.456.789.111:222...*
** TCP_NODELAY set*
** Connected to 123.456.789.111 (123.456.789.111) port 222 (#0)*

[5] These are examples and are not the actual values.

A Successful connection response to the India-specific URL:

** Trying 123.456.789.111:222...*
** TCP_NODELAY set*
** Connected to xxx.visa.com (123.456.789.111) port 222 (#0)"*

4.2.3 What should an endpoint do if they do not receive the "Connected" response?

If a "connected" response is not received, endpoints should verify they do not have any firewall rules, allow lists, or other configurations that could interfere with the connection inbound or outbound to the Visa DS.

4.3 Guidance for the DS Reference Number Field

4.3.1 Why is Visa updating the guidance for the DS Reference Number field?

The DS Reference Number value is subject to change each time Visa certifies or recertifies its DS product with EMVCo, thus, Visa recommends that the dsReferenceNumber field is not treated as a static value. To prepare for updates to the DS Reference Number all ACS and 3DSS who currently treat this field as a static value must make changes to support the value changing over time. Clients will be notified before a new DS Reference Number is utilized by the DS.

4.3.2 What are the required actions to support the DS Reference Number?

It is mandatory that any ACS Providers who currently treat this field as a static value (i.e., to identify Visa) make changes to that support the value changing over time. Thus, the value of the dsReferenceNumber field should not be treated as static.

4.3.3 Will there be any Visa testing provided or required for this update?

Testing is not available for this update.

4.3.4 If an endpoint has already made changes to treat the DS Reference Number as a non-static value, are there any additional steps required?

If an endpoint is enabled to **not** treat the dsReferenceNumber field as **static** and can support changes to Visa's DS Reference Number value, no additional steps are required.

Glossary

0 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Term	Definition
0-9	
3-D Secure (3DS, Three Domain Secure)	The protocol developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance. Visa owns 3DS 1.0.2 and licenses it to other payment providers. EMVCo owns 3DS EMV 3DS. Visa's offering of 3DS is called Visa Secure.
A	
Access Control Server (ACS)	A server hardware/software entity that supports Visa Secure authentication and other functions. The ACS is operated by the issuer or the issuer's processor. In response to Visa's Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the cardholder during online purchases, and provides digitally signed authentication response messages (containing the authentication results and other Visa Secure data) to the merchant.
Acquirer	A Member that signs a Merchant or payment facilitator or disburses currency to a cardholder in a cash disbursement, and directly or indirectly enters the resulting transaction receipt into interchange.
Authentication	The process used to ensure that the transaction is being initiated by the rightful owner of the Visa account.
Authentication Request	A request for cardholder authentication from a Visa Secure Merchant.
Authentication Response	A response from a Visa Secure Issuer, or Visa on behalf of an Issuer, in response to an Authentication Request. Authentication Responses include: – Attempt Responses – Authentication Confirmations – Authentication Denials – Unable-to-Authenticate Responses

Term	Definition
I	
Issuer	A Member that enters into a contractual relationship with a cardholder for the issuance of one or more card products.
India-located	An entity who is primarily located/has a host server in India.
M	
Member	A client of Visa U.S.A., Visa International, Visa Worldwide, Visa Europe Limited, or Visa International Servicios de Pago España, S.R.L.U. or a customer that has entered into a Services Agreement with Visa Canada. Requirements for membership are defined in the applicable Visa charter documents.
Merchant	An entity that accepts a Visa Card for the sale of goods or services and submits the resulting transaction to an Acquirer for interchange, directly or via a payment facilitator. A Merchant may be a single merchant outlet or represent multiple merchant outlets.
P	
Preparation Request (PReq) Message	The PReq message is sent from the 3DS Server to the Visa Directory Server to request information about the versions supported by available ACSs and, if one exists, any corresponding 3DS Method URL.
Preparation Response (PRes) Message	The PRes message is the Visa Directory Server response to the PReq message. The 3DS Server can utilize the PRes message to cache information about the versions supported by available ACSs, and if one exists, about the corresponding 3DS Method URL.
R	
Results Request (RReq) message	EMV 3DS message sent from the Issuer ACS to the 3DS Server via the Visa Directory Server to transmit the results of the authentication transaction.
Results Response (RRes) message	The EMV 3DS 3DSS response to the Results Result (RRes) message used to acknowledge receipt of this message.
V	
Visa Directory Server	A server hardware/software entity that is operated by Visa, whose primary function is to route authentication requests from merchants to specific ACSs and to return the results of authentication.

Term	Definition
Visa Secure	Visa's customer authentication program that is built off of the 3-D Secure protocol. The program contains all the rules and mandates that ACS, issuers, and merchants must follow to participate