EMV 3-D Secure 2.0 Verified by Visa Test Suite (VbVTS) User's Guide

Verified by Visa

Version 1.0
Effective: 21 June 2017

6/8/2017 Draft

Important Note on Confidentiality and Copyright

Contents

Chapter 1 • Setup and Testing Guides

Introduction to VbVTS 1–2

VbVTS Testing Process Overview 1–3

3DS Server Setup Guide 1–4

3DS Server Certificate Request and Installation: 1–4

ACS Setup Guide 1–5

VbVTS Enrollment 1–5

Configuration Parameters 1–5

ACS Certificate Request and Installation 1–5

PAN Usage and ACS Enrollment: 1–6

Technical Support Contact Information 1–6

Appendix A • 3DS Server Test Cases

Required 3DS Server Certification Testing A–1

Optional 3DS Server Certification Testing A–3

Appendix B • ACS Test Cases

Required ACS Certification Testing B–1

Optional ACS Certification Testing B–3

Appendix C • CAVV Validation

Appendix D • Review Test Results

3DS Server D–1

ACS D–1

Glossary

Setup and Testing Guides 1

Introduction to VbVTS 1–2

VbVTS Testing Process Overview 1–3

3DS Server Setup Guide 1–4

ACS Setup Guide 1–5

Technical Support Contact Information 1–6

The following subsections detail the procedures to be followed when testing with Verified by Visa Test Suite (VbVTS).

- The Introduction to VbVTS provides an overview of VbVTS and VbVTS's testing process.
- VbVTS Testing Process Overview provides an overview of the testing process.
- The 3DS Server Setup Guide details the setup process to prepare for 3DS Server testing.
- The ACS Setup Guide details the setup process to prepare for ACS testing.
- The Technical Support Contact Information section gives support team details for users.

Introduction to VbVTS

The goal of the Verified by Visa Test Suite (VbVTS) is to ensure that new 3DS Server (3DSS) and Access Control Server (ACS) implementations of the Verified by Visa (VbV) program meet technical and business requirements, and will provide a consistent user experience for Visa cardholders before going live in production. Only after completing EMV 3-D Secure 2.0 Protocol testing will endpoints be allowed to test in VbVTS. VbVTS provides a standard set of 3DSS and ACS required and optional test cases that allow entities implementing Visa's version of the 3-D Secure 2.0 protocol to verify their implementations meet VbV product and business rules.

All Visa Regions have mandated that new VbV 2.0 implementations must successfully pass all of VbVTS's required test cases prior to going live in production.

Each message VbVTS sends and receives is stored, by test case instance, under the tester's ID. Testers are responsible for reviewing the results for each of their test cases to ensure that VbVTS has not found errors during message evaluation. Testers are also responsible for ensuring that their implementation responds to VbV processing appropriately from a business and product perspective as specified in the documentation for each test case. VbVTS will validate that all required fields are valid per the EMV 3-D Secure 2.0 protocol spec, while also doing specific field-level element validation for a number of fields detailed in each test case. The tester must ensure that they have performed each test case successfully from both a technical and business perspective; if not, the tester must correct the error and rerun the test case until all aspects of the test case as specified are successfully performed.

VbVTS Testing Process Overview

Each testing entity must perform the following steps, regardless of whether an a 3DS Server or ACS is being tested.

1. Enrollment: As a first step, the tester must enroll in VbVTS by providing contact information about themselves and information about the component(s) that they are testing. Global Client Testing (GCT) is notified of the tester's desire to enroll and validates the tester's EMVCo-assigned reference number. Upon validation, GCT will then grant the tester access to VbVTS.
2. Request Test Certificates: Using VbVTS's online certificate issuance facility, the tester must request the TLS client, server, and/or signing certificates required for the component for which they are performing testing. For more information on certificate setup, please refer to the Setup Guide subsection for your component type and to the Help on VbVTS Certificate Request page.
3. Run Test Cases: The tester must run all of the required test cases. For added benefit, the tester may also choose to run any number of the optional test cases.
4. Review Test Results/Rerun Test Cases as Necessary: The tester must review the View Test Results tab in VbVTS to confirm that they correctly passed all required test cases. If any test cases are failed, the tester must rerun them until they are successfully completed.
5. Successful Completion/Request Production Certificate(s): Upon completion of the required test cases, the tester should contact Global Client Testing (GCT) to request a VbVTS Compliance Letter. This will also begin the process of obtaining production certificates (if applicable).

   NOTE: *GCT will send VbVTS Compliance Letter in an email back to the vendor. The email will also inform that vendor that should they want production certificates, they should contact their regional CSS representative to request the certificates.*

   Not all software vendors will need production certificates. Only those who also function as an operator of their software will need them.

3DS Server Setup Guide

3DS Server Certificate Request and Installation:

The 3DS Server tester must install testing certificates in order to conduct test cases. If a user is signed up as a 3DS Server tester only, they will be presented with one link after they click on the "Request Testing Certificate" link on the left-hand menu:

1. Request certificates for SSL Communication: This link is used by a 3DS Server tester to obtain the SSL certificates signed by VISA VbVTestSuite CA. Currently we only support RSA certificates for SSL Communication. The tester can either upload a Certificate Signing Request (CSR) as a .bin file in DER format or place the encoded CSR in PEM format in the text area as a string. The tester then submits to obtain the signed CSR, which will be sent to the email address provided on the screen.

NOTE: *If a tester is signed up as both a 3DS Server and ACS tester, they will be presented with two links after they click on the "Request Testing Certificate" link on the left-hand menu*

1. Request certificates for SSL Communication
2. Request Signing Certificate (PbACS)

ACS Setup Guide

VbVTS Enrollment

During enrollment in VbVTS, the ACS tester must click the Component Type: ACS check box in the form. The tester must also provide their ACS URL (at which the tester's ACS expects to receive AReq, CReq, and RRes messages from VbVTS) in the ACS URL section of VbVTS enrollment form. Be sure to input the correct ACS URL (including port number, if applicable) or VbVTS will fail to communicate with your ACS.

Configuration Parameters

The ACS tester will need to perform certain configuration steps in order to connect to, send, and receive messages from VbVTS. The following configuration parameters must be set in the ACS:

- VbVTS currently supports the ciphersuites supported by the EMV 3-D Secure 2.0 Protocol Specification.

ACS Certificate Request and Installation

The ACS tester must install testing certificates in order to conduct test cases. If a user is signed up as an ACS tester only, they will be presented with two links after they click on the "Request Testing Certificate" link on the left-hand menu:

1. Request certificates for SSL Communication: This link is used by an ACS tester to obtain the SSL certificates signed by VISA VbVTestSuite CA. Currently we only support RSA certificates for SSL Communication. The tester can either upload a Certificate Signing Request (CSR) as a .bin file in DER format or place the encoded CSR in PEM format in the text area as a string. The tester then submits to obtain the signed CSR, which will be sent to the email address provided on the screen.
2. Request Signing Certificate (PbACS): This link is used by an ACS tester to obtain the PbACS certificate, which is used to sign the "acsSignedContent" in the ARes message populated for app-based challenge flows. ACS will create EC Keystore on their end and provide the Certificate Signing Request (CSR) on the screen to be signed by VISA VbVTestSuite Signing CA.

NOTE: *If a tester is signed up as both a 3DS Server and ACS tester, they will be presented with two links after they click on the "Request Testing Certificate" link on the left-hand menu*

1. Request certificates for SSL Communication
2. Request Signing Certificate (PbACS)

PAN Usage and ACS Enrollment:

ACS testers may either use VbVTS's default test card numbers (PANs), as provided by VbVTS in the AReq for each specific test case, or may use PANs that have already been enrolled on their ACS. If the ACS tester wants to use their own PANs, the tester must edit the <PAN> field in the AReq for each test case before clicking the Send AReq button. To use VbVTS's default PANs, the ACS tester must enroll VbVTS's PANs on the tester's ACS.

For those ACS testers that elect to use VbVTS's default PANs, please review Appendix B to see the PANs that must be enrolled on the ACS to conduct testing.

Technical Support Contact Information

For administrative and general testing procedure related questions, please contact Global Client Testing (GCT) at gctv3dsts@visa.com.

For test case related questions, connectivity problems, or any other specific technical issues please contact:

VbVTestSuite2@visa.com.

3DS Server Test Cases A

Required 3DS Server Certification Testing

The 3DS Server Test Cases in this chapter are required for 3DS Server implementations in all Visa Regions.

Test Case 3DSS-100–Complete a Frictionless PA Browser Flow

Description	The 3DS Server will send an AReq with the 16-digit test PAN to VbVTS DS. If the AReq is well-formed, VbVTS DS will return the 3DS Server a well-formed ARes with status Y in response. 3DS Server accepts ARes, this completes the test case.
Action	1. 3DS Server builds AReq as follows: a. PAN (Cardholder Account Number): "4012001000000100" b. Device Channel: "02" c. 3DS Requestor ID: "VbVTSReqTestID" (static, provided in the user guide) d. 3DS Requestor Name: "VbVTSReqTestName" (static, provided in user guide) e. 3DS Server Reference Number: Value provided by EMVCo after testing f. Acquirer BIN: 400000 g. Acquirer Merchant ID: "VbVTestSuite-12345678" h. Message Category: "01" ***Note:*** *all other required fields must be included in the AReq and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* 2. 3DS Server POSTs AReq to VbVTS DS
Expected Results	• VbVTS DS responds with ARes to 3DS Server, transaction status = "Y" • 3DS Server confirms the ARes is well-formed • Test case complete

Test Case 3DSS-101–Complete A Challenge PA Browser Flow

Description	The 3DS Server will send an AReq with the 16-digit test PAN to VbVTS DS. If the AReq is well-formed, VbVTS DS will send the 3DS Server a well-formed ARes with status C in response. Challenge flow initiates. 3DS Server sends a CReq through the browser to the ACS simulator. ACS simulator sends RReq through VbVTS DS with transaction status Y to 3DS Server. 3DS Server sends RRes through VbVTS DS to ACS simulator. ACS simulator sends final CRes with transaction status Y to 3DS Server, complete test case.
Action	1. 3DS Server builds AReq as follows: a. PAN (Cardholder Account Number): "4012001000000101" b. Device Channel: "02" c. 3DS Requestor ID: "VbVTSReqTestID" (static, provided in the user guide) d. 3DS Requestor Name: "VbVTSReqTestName" (static, provided in user guide) e. 3DS Server Reference Number: Value provided by EMVCo after testing f. Acquirer BIN: 400000 (check if this is a real acquirer BIN or if we can use as a test) g. Acquirer Merchant ID: "VbVTestSuite-12345678" h. Message Category: "01" ***Note:*** *all other required fields must be included in the AReq and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* 2. 3DS Server POSTs AReq to VbVTS DS
Expected Results	• VbVTS DS responds with ARes to 3DS Server, transaction status = "C" • 3DS Server confirms the ARes is well-formed • 3DS Server builds a CReq as follows – 3DS Server Transaction ID: (Same 3DS Server Transaction ID as AReq) • 3DS Server sends CReq through the browser to VbVTS ACS simulator • VbVTS POSTs RReq to 3DS Server with transaction status = "Y" through VbVTS DS • 3DS Server builds an RRes, sends to ACS simulator through VbVTS DS • VbVTS ACS simulator sends final CRes to 3DS Server with transaction status = "Y" • 3DS Server confirms the CRes is well-formed • Test case complete

Optional 3DS Server Certification Testing

Test Case 3DSS-200–Complete a Frictionless PA Browser Flow (Attempted Authentication)

Description	The 3DS Server will send an AReq with the 16-digit test PAN to VbVTS DS. If the AReq is well-formed, VbVTS DS will return the 3DS Server a well-formed ARes with status A in response. 3DS Server accepts ARes, this completes the test case.
Action	1. 3DS Server builds AReq as follows: a. PAN (Cardholder Account Number): "4012001000000200" b. Device Channel: "02" c. 3DS Requestor ID: "VbVTSReqTestID" (static, provided in the user guide) d. 3DS Requestor Name: "VbVTSReqTestName" (static, provided in user guide) e. 3DS Server Reference Number: Value provided by EMVCo after testing f. Acquirer BIN: 400551 g. Acquirer Merchant ID: "VbVTestSuite-12345678" h. Message Category: "01" ***Note:*** *all other required fields must be included in the AReq and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* 2. 3DS Server POSTs AReq to VbVTS DS
Expected Results	• VbVTS DS responds with ARes to 3DS Server, transaction status = "A" • 3DS Server confirms the ARes is well-formed • Test case complete

Test Case 3DSS-201–Send a PReq With Blank Serial Number

Description	The 3DS Server vendor will send a PReq to VbVTS DS. If the PReq is well-formed, VbVTS DS will return the 3DS Server a well-formed PRes with 10 ranges (all ranges currently in the DS, due to the blank Serial Number passed in). 3DS Server accepts PRes, this completes the test case.
Action	1. 3DS Server builds PReq as follows: a. 3DS Server Reference Number: Value provided by EMVCo after testing b. Serial Number = not present ***Note:*** *all other required fields must be included in the PReq and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* 2. 3DS Server POSTs PReq to VbVTS DS
Expected Results	• VbVTS DS responds with PRes to 3DS Server, includes card ranges 1-10 • 3DS Server confirms the PRes is well-formed • Test case complete

Test Case 3DSS-202–Send a PReq With Serial Number

Description	The 3DS Server vendor will send a PReq to VbVTS DS. If the PReq is well-formed, VbVTS DS will return the 3DS Server a well-formed PRes with 3 ranges (the ranges that have changed or been added since the given Serial Number was last returned). 3DS Server accepts PRes, this completes the test case.
Action	1. Run test case 3DSS-201 and store returned Serial Number 2. 3DS Server builds PReq as follows: a. 3DS Server Reference Number: Value provided by EMVCo after testing b. Serial Number = the value returned in 3DSS-201 ***Note:*** *all other required fields must be included in the PReq and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* 3. 3DS Server POSTs PReq to VbVTS DS
Expected Results	• VbVTS DS responds with PRes to 3DS Server, includes card ranges 11-13 • 3DS Server confirms the PRes is well-formed • Test case complete

ACS Test Cases B

Required ACS Certification Testing

The ACS Test Cases below are required for Issuer ACS implementations in all Visa Regions. Each Visa Region may also require additional test cases.

Test Case ACS-100–Complete a Frictionless PA Browser Flow

Description	VbVTS DS will send an AReq with the 16-digit test PAN to the ACS vendor. The ACS will validate the AReq and return VbVTS DS a well-formed ARes with status Y in response. VbVTS DS validates the ARes is well-formed, complete test case.
Action	1. ACS user logs in to VbVTS and runs the test case 2. VbVTS DS builds an AReq as follows and sends to ACS a. PAN (Cardholder Account Number): "4012002000000100" (default to this PAN but editable) b. Expiration Date: (Default to current month/year but editable) c. Device Channel: "02" d. Message Category: "01"
Expected Results	• ACS confirms the AReq is well-formed • ACS creates ARes with the following – Transaction Status: "Y" – ACS Reference Number: EMVCo-assigned ACS Reference Number ***Note:*** *all other required fields must be included in the ARes and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* • ACS sends ARes to VbVTS DS • VbVTS confirms the ARes is well-formed • Test case complete

Test Case ACS-102–Complete a Frictionless PA App Flow

Description	VbVTS DS will send an AReq with the 16-digit test PAN to the ACS. The ACS will validate the AReq and return VbVTS DS a well-formed ARes with status Y in response. VbVTS DS validates the ARes is well-formed, complete test case.
Action	1. ACS user logs in to VbVTS and runs the test case 2. VbVTS DS builds an AReq as follows and sends to ACS a. PAN (Cardholder Account Number): "4012002000000102" (default to this PAN but editable) b. Expiration Date: (Default to today's date but editable) c. Device Channel: "01" d. Message Category: "01"
Expected Results	• ACS validates AReq • ACS creates ARes with the following – Transaction Status: "Y" – ACS Reference Number: 'EMVCo-assigned ACS Reference Number ***Note:*** *all other required fields must be included in the ARes and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* • ACS sends ARes to VbVTS DS • VbVTS DS validates ARes • Test case complete

Optional ACS Certification Testing

Test Case ACS-101–Complete a Challenge PA Browser Flow

Description	VbVTS DS will send an AReq with the 16-digit test PAN to the ACS. The ACS will validate the AReq and return VbVTS DS a well-formed ARes with status C in response. Challenge flow initiates. 3DS Server simulator sends a CReq through the browser to the ACS. ACS sends a HTML page with challenge screen(s). User authenticates successfully. ACS sends RReq with transaction status Y to VbVTS DS. VbVTS DS sends RRes to ACS. ACS sends final CRes with transaction status Y to 3DS Server simulator, complete test case.
Action	1. ACS user logs in to VbVTS and runs the test case 2. VbVTS DS builds an AReq as follows and sends to ACS a. PAN (Cardholder Account Number): "4012002000000101" b. Expiration Date: (Default to current month/year but editable) c. Device Channel: "02" d. Message Category: "01" 3. ACS confirms the AReq is well-formed 4. ACS creates ARes with the following a. Transaction Status: "C" b. ACS Reference Number: EMVCo-assigned ACS Reference Number 5. ACS sends ARes to VbVTS DS 6. VbVTS confirms the ARes is well-formed 7. VbVTS 3DS Server simulator builds and sends CReq through the browser to the ACS 8. ACS presents challenge screen(s) 9. User authenticates successfully 10. ACS builds and sends RReq to VbVTS DS with: a. Transaction status = "Y" b. CAVV c. ECI value = 05 d. Authentication type e. Authentication method
Expected Results	• VbVTS DS confirms the RReq is well-formed • VbVTS DS builds and sends RRes to the ACS • ACS confirms the RRes is well-formed • ACS sends CRes with transaction status = "Y" to 3DS Server simulator • Test case complete

Test Case ACS-103–Complete a Challenge PA App (Native) Flow

Description	VbVTS DS will send an AReq with the 16-digit test PAN to the ACS. The ACS will validate the AReq and return VbVTS DS a well-formed ARes with status C in response. Challenge flow initiates. 3DS Server simulator sends a CReq to the ACS. ACS sends a CRes to 3DS Server simulator with challenge screen. This process continues until the user has authenticated successfully. ACS sends RReq with transaction status Y to VbVTS DS. VbVTS DS sends RRes to ACS. ACS sends final CRes with transaction status Y to 3DS Server simulator, complete test case.
Action	1. ACS user logs in to VbVTS and runs the test case 2. VbVTS DS builds an AReq as follows and sends to ACS a. PAN (Cardholder Account Number): "4012002000000103" b. Expiration Date: (Default to current month/year but editable) c. Device Channel: "01" d. Message Category: "01" 3. ACS confirms the AReq is well-formed 4. ACS creates ARes with the following a. Transaction Status: "C" b. ACS Reference Number: EMVCo-assigned ACS Reference Number c. ACS Rendering Type (Position 1, for Position 2, ACS can send any valid value): “01” 5. ACS sends ARes to VbVTS DS 6. VbVTS DS confirms the ARes is well-formed 7. VbVTS 3DS SDK simulator builds and sends CReq to the ACS 8. ACS should send a CRes with choice of Phone Number or Email. The user's choice will determine where the OTP is sent. a. VbVTS will display the message sent on the screen so the ACS can verify the message they sent. 9. VbVTS 3DS SDK simulator builds and sends second CReq to ACS. 10. ACS parses this CReq and will then send a second CRes with information to populate an OTP entry screen. 11. VbVTS parses this message and will display a screen that asks the ACS tester to enter an OTP. a. Note: this again gives the ACS tester a chance to validate their screen. b. Upon submission of the OTP screen, VbVTS 3DS SDK simulator sends final (third) CReq to the ACS. 12. ACS verifies that the final CReq has the OTP value. Above process [Steps 8-12] repeats as necessary until the ACS determines the user has authenticated successfully.

Test Case ACS-103–Complete a Challenge PA App (Native) Flow

Expected Results	• ACS builds and sends RReq to VbVTS DS with: – Transaction status = "Y" – CAVV – ECI value = 05 – Authentication type – Authentication method • VbVTS DS confirms the RReq is well-formed • VbVTS DS builds and sends RRes to the ACS • ACS confirms the RRes is well-formed • ACS sends CRes with transaction status = "Y" to 3DS Server simulator • Test case complete

Test Case ACS-104–Complete a Challenge PA App (HTML) Flow

Description	VbVTS DS will send an AReq with the 16-digit test PAN to the ACS. The ACS will validate the AReq and return VbVTS DS a well-formed ARes with status C in response. Challenge flow initiates. 3DS Server simulator sends a CReq to the ACS. ACS sends a CRes to 3DS Server simulator with challenge screen. This process continues until the user authenticates successfully. ACS sends RReq with transaction status Y to VbVTS DS. VbVTS DS sends RRes to ACS. ACS sends final CRes with transaction status Y to 3DS Server simulator, complete test case.
Action	1. ACS user logs in to VbVTS and runs the test case 2. VbVTS DS builds an AReq as follows and sends to ACS a. PAN (Cardholder Account Number): "4012002000000104" b. Expiration Date: (Default to current month/year but editable) c. Device Channel: "01" d. Message Category: "01" 3. ACS confirms the AReq is well-formed 4. ACS creates ARes with the following a. Transaction Status: "C" b. ACS Reference Number: EMVCo-assigned ACS Reference Number c. ACS Rendering Type (Position 1, for Position 2, ACS can send any valid value): “02” 5. ACS sends ARes to VbVTS DS 6. VbVTS DS confirms the ARes is well-formed 7. VbVTS 3DS SDK simulator builds and sends CReq to the ACS 8. ACS should send a CRes with choice of Phone Number or Email. The user's choice will determine where the OTP is sent. a. VbVTS will display the message sent on the screen so the ACS can verify the message they sent. 9. VbVTS 3DS SDK simulator builds and sends second CReq to ACS. 10. ACS parses this CReq and will then send a second CRes with information to populate an OTP entry screen. 11. VbVTS parses this message and will display a screen that asks the ACS tester to enter an OTP. a. Note: this again gives the ACS tester a chance to validate their screen. b. Upon submission of the OTP screen, VbVTS 3DS SDK simulator sends final (third) CReq to the ACS. 12. ACS verifies that the final CReq has the OTP value. Above process [Steps 8-12] repeats as necessary until the ACS determines the user has authenticated successfully.

Test Case ACS-104–Complete a Challenge PA App (HTML) Flow

Expected Results	• ACS builds and sends RReq to VbVTS DS with: – Transaction status = "Y" – CAVV – ECI value = 05 – Authentication type – Authentication method • VbVTS DS confirms the RReq is well-formed • VbVTS DS builds and sends RRes to the ACS • ACS confirms the RRes is well-formed • ACS sends CRes with transaction status = "Y" to 3DS Server simulator • Test case complete

Test Case ACS-200–Complete a Frictionless PA Browser Flow (Attempted Authentication)

Description	VbVTS DS will send an AReq with the 16-digit test PAN to the ACS vendor. The ACS will validate the AReq and return VbVTS DS a well-formed ARes with status A in response. VbVTS DS validates the ARes is well-formed, complete test case.
Action	1. ACS user logs in to VbVTS and runs the test case 2. VbVTS DS builds an AReq as follows and sends to ACS a. PAN (Cardholder Account Number): "`4012002000000200`" (default to this PAN but editable) b. Expiration Date: (Default to current month/year but editable) c. Device Channel: "02" d. Message Category: "01"
Expected Results	• ACS confirms the AReq is well-formed • ACS creates ARes with the following – Transaction Status: "A" – ACS Reference Number: EMVCo-assigned ACS Reference Number ***Note:*** *all other required fields must be included in the ARes and have a valid value per the EMV 3-D Secure 2.0 Protocol Specification. Any optional fields which are included must also present a valid value per the EMV 3-D Secure 2.0 Protocol Specification.* • ACS sends ARes to VbVTS DS • VbVTS confirms the ARes is well-formed • Test case complete

6/8/2017 Draft

CAVV Validation C

ACS software vendors are required to execute the CAVV validation test cases in VBVTS. The software vendors must be able to correctly connect to the VbV service, VBVTS, and process 3-D Secure 2.0 transactions, including the generation of the CAVV value with the Issuer's CAVV key.

ACS software vendors shall use the CAVV validation feature available in VbVTS to accomplish the below two objectives:

- To confirm that the ACS is able to generate a properly formatted CAVV.
- To confirm that the ACS is capable of selecting the correct CAVV position 2 value to match the authentication method used to authenticate the consumer.

Steps involved in performing CAVV validation and the expected results:

Step 1: ACS user clicks the link named"CAVV validation" on the left hand side menu and a form is presented to the user.

Step 2: The ACS user provides all the required data fields mentioned below and clicks submit:

a. CAVV

b. ECI

c. Account #

d. Expiry Date

e. Authentication Method[1] (user chooses the method from the drop down that they support)

NOTE: *The easiest way for an ACS tester to obtain a CAVV, ECI, and Account # is to run required test case ACS-100. These data fields will be a part of the ARes message available to the user when the required test case is successfully completed in VbVTS.*

The ACS tester may also use a CAVV, ECI, and Account # from any other test transaction they conduct that provides these values.

NOTE: *If an ACS software vendor does not have any issuers who use their software, then the ACS can use the VisaNet Certification Management Service (VCMS) test bins and keys. Please contact gctv3dsts@visa.com for more information.*

Step 3: VbVTS sends the above fields to VCMS. Visa will provide the validation results. If any of the above fields are not provided in the basic format expected, there will be an error displayed on the screen.

Step 4: Based on the validations above, VCMS sends the results to VBVTS and VBVTS displays the CAVV validation results to the user.

Step 5: User is provided with the below results and the fields displayed below are based on the CAVV and other fields that are provided in the previous step.

a. Response Source

b. Action Code

c. CAVV results Code.

NOTE: *If you receive a results code other than 2, 3, 8, A, B, C, or D, please refer to CAVV guide and VIP tech manual for more details on the result codes and the related fields. These guides and manuals are available on the tech partner's website that hosts 3-D Secure 2.0 materials: https://technologypartner.visa.com/Library/3DSecure2.asp*

Step 6: The user emails the screenshot of the CAVV results to gctv3dsts@visa.com along with a confirmation that they have completed other required test cases to obtain the compliance letter.

Step 7: GCT reviews the CAVV results and provides the compliance letter to the user.

[1] The ACS must test at least one of the authentication methods in order to pass the CAVV validation test case.

Review Test Results D

3DS Server

3DS Server vendors drive their test cases by sending AReq messages with the required cardholder account number to VbVTS Directory Server. After running their test cases, they must review the Testing Status page. If there are any required test cases that they have not passed, they must review their results to see why they failed - VbVTS will specify when and why the vendor failed a test case. In order to successfully complete testing and request their VbVTS Compliance Letter, they must rerun their test cases until they have passed them all. Successful completion of optional test cases is not required to obtain a compliance letter. It is highly recommended that 3DS Server vendors run optional test cases 3DSS-201 and 3DSS-202.

NOTE: *Note: The Testing Status page lists test cases and their most recent status (e.g. Passed, Pending, Failed, etc.). The Testing History page shows all attempts of a test case.*

ACS

ACS vendors drive their test cases through VbVTS UI. After running their test cases, they must review the Testing Status page. If there are any required test cases that they have not passed, they must review their results to see why they failed - VbVTS will specify when and why the vendor failed a test case. In order to successfully complete testing and request their VbVTS Compliance Letter, they must rerun their required test cases until they have passed them all.

In addition, ACS vendors must test their ability to correctly create a CAVV. They must submit a CAVV on the "CAVV Test" page. If they are successful, they must take a screenshot of their success and send it to GCT when requesting their compliance letter. Successful completion of optional test cases is not required to obtain a compliance letter.

NOTE: *Note: The Testing Status page lists test cases and their most recent status (e.g. Passed, Pending, Failed, etc.). The Testing History page shows all attempts of a test case.*

6/8/2017 Draft

Glossary

Frictionless

No cardholder interaction is needed for authentication.

Challenge

Cardholder interaction is required by the issuer to complete authentication.

PA

Payment Authentication.

VbVTS

Verified by Visa Test Suite

VbV

Verified by Visa

VCMS

VisaNet Certification Management Service. It is the VisaNet BASE II Testing System.

6/8/2017 Draft