VISA CEMEA SCA TESTING

Guidelines and Frequently Asked Questions (FAQ) Version 1.0

This document outlines Visa's guidelines for CEMEA SCA testing and provides frequently asked questions (FAQ). It is intended for acquirers, processors, merchants, or their agents.

CEMEA SCA testing helps ensure that a contactless-enabled chip terminal is ready to receive and act on the Strong Customer Authentication (SCA) response codes. This helps prevent interoperability problems related to the introduction of SCA in CEMEA.

Important Information:

Build-001 is the current build for CEMEA SCA testing (Series 03).

CEMEA SCA testing is mandatory testing which applies additionally to L3 testing to contactless-enabled chip terminals (e.g., POS, mPOS, and Tap to Phone) in the CEMEA SCA impacted countries[1] and encompasses regional regulatory requirements on SCA.

Note: While an acquirer must successfully complete CEMEA SCA testing, it is understood that another party (e.g., a merchant, Value-Added Reseller (VAR), Independent Software Vendor (ISV), Independent Service Organization (ISO), Gateway, etc.) may be performing CEMEA SCA testing based on the acquirer/processor's process and requirements.

Summary

Starting in **September 2025**, newly deployed or updated terminals in CEMEA SCA countries[1] must perform standard L3 testing plus CEMEA SCA testing.

CEMEA SCA testing applies to transactions where both the acquirer and issuer country codes are within the regulated area of a specific SCA jurisdiction (for example, within each individual country in the CEMEA region that has a legal requirement for the implementation of SCA).

L3 test tool vendors will be providing the CEMEA SCA test set to their clients during the month of September. For the specific date of availability, contact your L3 test tool provider.

[1] CEMEA SCA countries: Albania, Azerbaijan, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, Serbia. Although there are no SCA requirements for Card Present transactions in Ukraine so far, participants in Ukraine may be enabled for CEMEA SCA testing at their own discretion.

How Does the New CEMEA SCA testing Process Work?

1. The tester uses an L3 test tool that has been qualified by EMVCo and confirmed by Visa to perform both standard L3 testing (Series 01) and CEMEA SCA testing (Series 03).
2. For CEMEA SCA testing, the tester completes the CEMEA SCA test tool questionnaire based on terminal/reader capabilities and acquirer requirements. The answers to the questionnaire (e.g., whether or not the device supports contact chip in addition to contactless and whether or not the device supports Online PIN) will be used to generate the applicable test cases.

   Note: The following transport and parking Merchant Category Codes (MCCs) are exempted from CEMEA SCA Test Set:

   - 4111 (Local and Suburban Commuter Passenger Transportation, including Ferries)
   - 4112 (Passenger Railways)
   - 4131 (Bus Lines)
   - 4784 (Tolls and Bridge Fees)
   - 7523 (Parking Lots, Parking Meters and Garages
3. Once testing has been successfully completed, the tester creates a report from the test tool.
4. The acquirer logs in to Visa Access and submits the report to the Visa Chip Compliance Reporting Tool (CCRT).

At this point, CEMEA SCA testing is completed from Visa's perspective.

Acquirer Requirements

Acquirers must ensure that they:

- Use an L3 test tool for their testing that has been qualified by EMVCo and confirmed by Visa. Refer to EMVCo–Qualified and Visa-Confirmed L3 Test Tools for a list of confirmed L3 test tools.
- Prepare their environment for testing.
  - The terminal needs to be connected to an acquirer and through to the VisaNet Certification Management Service (VCMS) or a Visa-confirmed host simulator.[2] For more information on Visa confirmed host simulators, refer to EMVCo-Qualified and Visa-Confirmed L3 Test Tools.
- Ensure their device is ready for L3 and CEMEA SCA testing. Refer to FAQ #2.3 in this document.

[2] For information on Online Message Logs (OML) and NET pass criteria, see Section 5.0 of the FAQ.

This section provides a list of Frequently Asked Questions (FAQ):

1.0 General	
1.1	**What is L3 Testing?** L3 testing is a phase of terminal testing that helps ensure that chip terminals that have been configured for deployment by acquirers are correctly integrated into the Visa payment acceptance environment and do not unduly contribute to interoperability problems. It improves acceptance of Visa-branded products. It is performed on the terminal in an environment which is as near as possible to the live one and where the connectivity to the acquirer host mirrors production.
1.2	**What is CEMEA SCA testing?** CEMEA SCA testing is an additional mandatory set of test cases for participants in CEMEA SCA impacted countries that helps ensure that contactless-enabled chip terminals can properly support and process two new response codes: • '70' (PIN data required) • '1A' (Additional customer authentication required) The CEMEA SCA test cases are in a separate series (Series 03) from the standard Visa L3 testing (Series 01).
1.3	**Who performs CEMEA SCA testing?** The acquirer, processor, or their agent in CEMEA SCA countries performs CEMEA SCA testing. An agent may be a merchant, VAR, ISV, ISO, Gateway, etc.
1.4	**Does CEMEA SCA testing include both global and regional CEMEA SCA requirements?** CEMEA SCA testing includes CEMEA SCA local requirements. CEMEA SCA Test Set applies to transactions where both the acquirer and issuer country codes are within the regulated area of a specific SCA jurisdiction (for example, within each individual country in the CEMEA region that has a legal requirement for the implementation of SCA).
1.5	**Do CEMEA SCA participants need to perform L3 testing when performing CEMEA SCA testing?** Yes. Newly deployed or updated terminals must perform both standard L3 testing and CEMEA SCA testing. There is an optional question in the questionnaire of CEMEA SCA Test Set, so that the tester can provide their CCRT Report # for their L3 testing. This question is optional as the tester might not have submitted their L3 CCRT report yet and therefore may not have the Report #.

1.0 General	
1.6	**Does the entity performing CEMEA SCA testing need to schedule CEMEA SCA testing with Visa?** No. Visa CEMEA SCA testing is considered self-service testing and does not require scheduling with Visa. You can perform the testing at your convenience. However, new acquirers need to ensure chip parameters are set up in Visa's test environment.
1.7	**Can I submit CEMEA SCA test results without using the Chip Compliance Reporting Tool (CCRT)?** No. CCRT must be used to submit test results.
1.8	**Does Visa provide me with a Letter of Approval (LOA) when I complete CEMA SCA testing?** No. Visa does not provide an LOA for CEMEA SCA testing. CCRT will provide you with a confirmation email letting you know that your test results have been received, and this email signifies that testing has been completed from Visa's perspective.
1.9	**What do I do if I fail a test?** When a test tool indicates a test case failure, it is anticipated that the acquirer will work with their technical support team and the terminal vendor or integrator (and Visa, if necessary) to correct the problem. The acquirer will continue to perform the test until the problem is resolved.
1.10	**Who should I contact if I need help with CEMEA SCA testing?** Merchant, ISVs, VARs, ISOs, etc. should contact their acquirer with any questions regarding their process and requirements to perform CEMEA SCA testing. Specific questions around L3 test tools should be handled between the client and their test tool vendor. For specific questions related to Visa CEMEA SCA test cases and/or CCRT, acquirers/processors can contact itest@visa.com or use the Visa Support Hub (VSH) on Visa Access. For more information regarding Visa's process and requirements for CEMEA SCA testing, contact your Visa representative.
1.11	**Are magnetic-stripe transactions in scope of CEMEA SCA testing?** No. CEMEA SCA testing focuses on contactless chip-based transactions. Magnetic-stripe and contact chip-based transactions are not in scope.
1.12	**Can I use the Visa Test System (VTS) as my host simulator for CEMEA SCA testing?** No. During CEMEA SCA testing, the acquirer environment must be connected to the VisaNet Certification Management Service (VCMS) or a Visa confirmed host simulator. VTS cannot be used. For a list of Visa confirmed host simulators, refer to EMVCo-Qualified and Visa-Confirmed L3 Test Tools.

2.0 Terminals	
2.1	**What types of devices and merchant types are covered under CEMEA SCA testing?** Visa CEMEA SCA testing covers the following devices accepting contactless chip: POS, mPOS, Tap to Phone. It applies to all merchants except those in the following Merchant Category Codes (MCCs): • 4111 (Local and Suburban Commuter Passenger Transportation, including Ferries) • 4112 (Passenger Railways) • 4131 (Bus Lines) • 4784 (Tolls and Bridge Fees) • 7523 (Parking Lots, Parking Meters and Garages
2.2	**How do I know what tests apply to my terminal?** In the beginning of your testing session, you will complete a questionnaire and the answers to your questionnaire will automatically be used by your L3 test tool to determine which test cases apply to your terminal. For CEMEA SCA, you will need to complete a maximum of 15 test cases.
2.3	**How do I set up my terminal for CEMEA SCA testing?** Prior to beginning CEMEA SCA testing, the terminal needs to be configured with all applicable parameters required for deployment based on Visa global and regional requirements. This includes the following: • The terminal has been Level 1 and Level 2 certified with associated Letters of Approval (LOAs)[3] • The terminal has been configured for deployment and the following are set correctly: – Applicable Visa Application Identifiers (AIDs) – Country codes and currency codes – VSDC Certificate Authority (CA) Test Public Keys (for devices that support Offline Data Authentication) (see the *Visa Smart Debit/Credit (VSDC) Certificate Authority Public Keys*)[4] – Terminal Transaction Qualifiers (TTQs) • The terminal is ready to act on the CEMEA SCA response codes of '70' and '1A'. For more details, see the Visa Rules and the *Transaction Acceptance Device Guide (TADG)*.
2.4	**I am deploying a terminal where the L1 and/or L2 approval has expired. Can I deploy this terminal?** Visa supports CEMEA SCA testing to be performed on an expired L1 and/or L2 approved product for **2 years** from the expiration of the approved product. Refer to the Visa Global L3 Testing Guidelines and FAQ for details.

[3] There may be exceptions for certain types of devices such as Tap to Phone. For Tap to Phone requirements, see the *Visa Ready Tap to Phone Solution Requirements* on Visa Access.

[4] Prior to deployment, the VSDC CA Test Public Keys must be removed from the device and replaced with VSDC CA Production Public Keys.

3.0 PINs and BINs for CEMEA SCA Testing

3.1 What PINs and which Account Ranges are used for the CEMEA SCA test card images?

Test cards use a Personal Identification Number (PIN) of 1234 unless otherwise noted in the test case.

The following Account Ranges are used for the CEMEA SCA test card images:

#	SCA impacted country	Account Ranges
1	Albania	478707040, 478707041
2	Azerbaijan	478764064, 478764065
3	Georgia	478764060, 478764061
4	Kosovo	478707048, 478707049
5	Moldova	478764066, 478764067
6	Montenegro	478707042, 478707043
7	North Macedonia	478707044, 478707045
8	Serbia	478707046, 478707047
9	Ukraine	478764062, 478764063

4.0 Online Message Logs (OML) and NET Pass Criteria

4.1 What are Online Message Logs (OML) and NET pass criteria?

- OML are host logs of CEMEA SCA test transactions (e.g., 0100/0110 and 0200/0210) provided by Visa (for clients connected to VCMS) or provided by a Visa confirmed CEMEA SCA host simulator (for clients connected to a host simulator).
- Network (NET) pass criteria are automated pass criteria that check OML for the presence of fields and/or field values in 0100/0110 and 0200/0210 messages.

4.2 My tool automatically obtains the OML. Is there anything I need to do?

These solutions already automatically obtain the OML. Please contact your preferred L3 test tool vendor for further information.

4.3 My tool does not automatically obtain the OML. What do I need to do?

If your L3 test tool does not automatically obtain the OML, you will need to obtain the OML from one of the following and upload it into your test tool:

- Clients connected to VCMS during CEMEA SCA testing will need to download the OML from the Chip Compliance Reporting Tool (CCRT) (use the "Search L3-OML" tab on CCRT) on Visa Access using the Authorization Request Cryptogram (ARQC) value from each test transaction
- Clients connected to a third-party host simulator during CEMEA SCA testing will need to obtain the OML from their host simulator

Please contact your CEMEA SCA test tool vendor and, for clients using a host simulator, your host simulator vendor for further information.

5.0 Documentation	
5.1	**Are there separate User Guides for CEMEA SCA testing?** There are no separate user guides. With the new CEMEA SCA process, documentation for each test case is built into the CEMEA SCA test tool and the test tool contains all the information on the test case including the objective, the applicability, the pass criteria, and help information.

Testing and Re-Testing Requirements

An acquirer from a CEMEA SCA country must successfully complete Visa Level 3 (L3) testing (Series 01) and CEMEA SCA testing (Series 03) before deploying a new chip-reading device, after a significant change to a chip-reading device (including adding SCA functionality), or to address an interoperability issue, as required by Visa.

Once you have completed CEMEA SCA for one of the CEMEA SCA countries or for one of the EEA SCA countries and the only change to the terminal is the country/currency codes, additional CEMEA SCA or EEA SCA testing is not required.

References

This section provides a list of EMVCo references available on the EMVCo website:

- *EMV Level 3 Testing Framework Implementation Guidelines (FIG)*, v1.1 or higher
- *EMV Level 3 Terminal Pseudo Functions,* v1.5 or higher

This section provides a list of Visa references:

- *EMVCo Qualified and Visa Confirmed L3 Test Tools and Components**
- *Chip Compliance Reporting Tool (CCRT) User Guide for Chip Acquirers*
- *Global Chip Acquirer Self Accreditation Program*
- *Transaction Acceptance Device Guide (TADG)**
- *Transaction Acceptance Device Requirements (TADR)*
- *Visa-Accredited Chip Vendor Enabled Service (CVES) Providers**
- *Visa Ready Tap to Phone Solution Requirements*
- *Visa Smart Debit/Credit Certificate Authority Public Keys**
- *Visa Smart Debit/Credit Contact and Contactless Global Acquirer Implementation Guide*

Note: Documentation is available for Visa clients on Visa Access. Merchants are advised to contact their acquirer for any documentation that is not on the Visa Chip website or the Visa Digital Partner Services website.

* Vendors may access these documents on the Visa Digital Partner Services website.