CFCF Terminal and Acquirer Certification Policy based on nexo Specifications

Annex 2

Evaluation Procedure for Terminal & Acquirer System based on nexo Specifications and Testing Laboratory Requirements

Version 4.1, April 2023

Table of Contents

1 Glossary, abbreviations and references

This document is the Annex 2 of the “CFCF Terminal and Acquirer Certification Policy based on nexo Specifications” referred hereafter as [CFCF Policy] describing in detail

- the evaluation procedure for terminal and acquirer systems based on nexo specifications and
- the requirements applicable to the CFCF Test Laboratories including the procedure to accredit Test Laboratories to operate within the CFCF Certification infrastructure.

For information on definitions please refer to the Glossary section (section 1) of the [CFCF Policy].

For information on abbreviations please refer to the Abbreviations section (section 2) of the [CFCF Policy].

For information on reference documents please refer to the References section (section 3) of the [CFCF Policy].

2 Introduction

The goal of the present document is to describe the overall Test process applicable to POI and Acquirer Host applications developed following the nexo implementation specification (nexo IS) as defined in [CFCF References].

The requirements applicable to the CFCF Test Laboratories are also contained in this document. This document also describes the procedure to accredit Test Laboratories to operate within the CFCF Certification infrastructure.

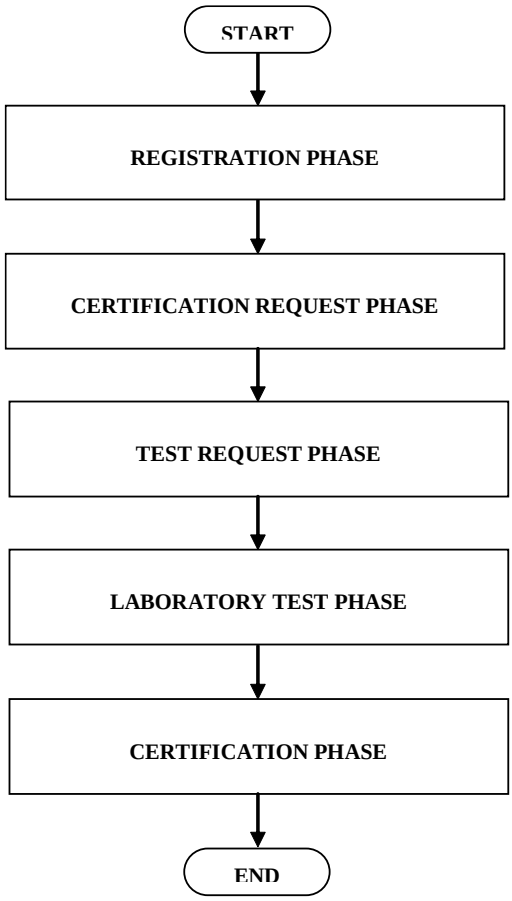
The roles of different stakeholders involved as well as the requirements for CFCF product evaluations and Laboratories are also described here. The involved parties are:

- The CFCF Certification Committee
- CFCF Accredited Certification Body(ies)
- Accredited Laboratory(ies)
- Qualified Auditors

The Accredited Laboratories performing the functional Tests of a Certification Object must be audited by a Qualified Auditor.

3 Requirements for testing

The overall certification process is made of phases as shown in the figure below.



The present section details the phases of Test Request and Laboratory Testing and their related requirements.

Prerequisite: As described in the [CFCF policy] document, the Certification Applicant must have been registered at a Certification Body and must have selected an Accredited Laboratory.

At that stage, the Certification Object's ICS can be reviewed by the Laboratory and must be validated by the Certification Body involved in the Certification process.

When the test request submission is complete, the test laboratory performs the testing of the Certification Object. Then a test report including related technical advice is issued to the Certification Applicant and copied to the Certification Body.

Based on the test report analysis, the Certification Body will grant or not a Certificate to the Certification Applicant for the Certification Object.

3.1 Test request and test phases for POI

3.1.1 Test request submission phase

Before testing of its POI the Certification Applicant must:

- Send a test request to the Accredited Laboratory
- Send the validated Implementation Conformance Statement (ICS) to the Accredited Laboratory for the certification object that it submits.

  Sign a product evaluation agreement with the Laboratory. This agreement must at least include:

  - Any Laboratory requirements needed for interfacing with the Laboratory test equipment, e.g., host emulator, etc.
  - Reference to the [CFCF policy] including its current annexes
  - reference to the Certification Body chosen by the Vendor (note: the chosen test Lab must be accredited by this Certification Body)
  - Agreement of mutual cooperation in providing information and assistance where needed.
  - Lead-time for the execution of the Tests.
  - The number of samples available for testing incl. arrangement for the preparation and delivery of samples.
  - Right to keep all samples for the duration of the Certification procedure.
  - The necessary support to the Laboratory to ensure the sample(s) remains fully functional.

- Supply the Laboratory at least with 2 POI samples or a server set-up and at least two Pin Pad samples, in case of a distributed configuration.

  All contact and contactless kernels declared in the ICS, must be installed and configured on the POI samples.

  The test environment has to ensure the integrity of the evaluated POI at all time. In case all components of the POI are not physically presentable in the Lab at the time of the Evaluation:
  - the Vendor must inform beforehand both the Laboratory and Certification Body of the Test configuration and answer to all related questions from both parties.
  - the Vendor must make sure all Tests required by the Certification process can be executed by the Laboratory.
  - the Test Laboratory or the Certification Body will conduct an audit for the elements which are not in the Laboratory to assess the integrity, e.g. a server.

3.1.2 Testing phase

The laboratory then:

- Validates that the ICS is complete and technically valid.
- Once the ICS is technically validated, the lab sends the ICS to the Certification Body for final qualification and registration.
- validates that the POI sample received is consistent with the ICS. For instance the checksum value of each application modules shall be checked by the laboratory against the value declared in the ICS and the hardware version indicated in the ICS must be validated.
- If the terminal sample is not consistent with the ICS, the laboratory notifies the ICS non-conformance to the Certification Applicant and :
    - Either requests for ICS compliant samples
    - Or update the ICS to comply with the sample features. In that case the ICS must be validated again by the laboratory and then by the Certification Body
- Identifies the list of applicable Test Cases according to the submitted and finally validated ICS
- Performs the test using qualified Test Tool(s) and a current valid Test Specification version. The latest version of the Test Specification is specified in [CFCF References] and have to be confirmed by the Certification Body.
- Note that the Certification Applicant must not be present during the testing and that no modifications are allowed to the Certification Object during the tests.
- The checksum value of each application modules shall be checked by the Laboratory against the value declared in the ICS at the end of the Test session.
- Reports the test results to the Certification Applicant using a standard test report (see requirements in section 4.1)
- Sends the test reports to the Certification Body once reviewed by the Certification Applicant.

In case of contactless POI applications, the integration of all kernels declared by the Vendor in the ICS must be tested and associated test results must be present in the test report.

3.1.3 Certification Applicant appropriateness verification

The Certification Applicant and its Certification Object are identified by a registration number given by the selected Certification Body as described in [CFCF Process].

3.1.4 Certification Applicant’s Sample identification (hardware, software)

The Certification Object sample must be identified with the following information:

- Vendor name
- Vendor Registration Number
- Sample number including its serial number
- Sample product name
- Date sample produced

- hardware identification with a hardware version number
- software identification with a software version & software module checksum
- checksum: Certification Applicant generates checksums to identify and verify the integrity of application modules (POI Application and the different interfaces). The checksum must be a unique value for each application and for each version of the application. The method or algorithm used for generating the checksum is left to the discretion of the Certification Applicant. SHA-1 or CRC might be chosen for example This value must be easily retrievable from the terminal for comparative purposes.

3.1.5 Powering the sample definition (how to operate the sample)

The POI sample must be supplied with the necessary documentation and support in order to operate the terminal sample during the testing phase. The certification applicant must make itself available in a reasonable time to answer any laboratory question about sample operation.

3.1.6 Upper Tester (UT) requirements & definition

If required by the test plan, the POI must be provided with Upper Tester capability (for example: a POS simulator for a POI application or an Issuer Accreditation simulator for a Host Acquirer System).

In that way the POI implements a software module that may also be logically located between the Application module (nexo FAST or nexo protocols) to test and the test tool. The UT has a predefined configuration, a controlled behaviour and gives expected results back to the test tool.

3.1.7 Certification Applicant's UT identification & documentation

If UT is required, the Certification Applicant must provide UT's identification and documentation as well as the necessary support to the laboratory to operate the UT.

3.2 Test request and test phases for ACQ

3.2.1 Test request submission phase

To perform testing of its ACQ the Certification Applicant must:

- Send a test request to the Accredited Laboratory
- Send the Implementation Conformance Statement (ICS) of the host to the Accredited Laboratory.
- Sign a product evaluation agreement with the laboratory.

  This agreement must at least include:

- Any laboratory requirements needed for interfacing with the laboratory test equipment, e.g., host emulator, etc.
- Reference to the [CFCF Policy] including its current annexes
- Reference to the Certification Body chosen by the Vendor (note: the chosen test lab must be accredited by this Certification Body)
- Agreement of mutual cooperation in providing information and assistance where needed.
- Lead-time for the execution of the tests.
- Configuration available for testing incl. arrangement for the preparation and delivery .
- Right to keep the test configuration installed for the duration of the certification procedure.
- The necessary support to the laboratory to ensure the configuration remains fully functional.

- Supply the laboratory with a ACQ server set-up configuration as described in the CFCF ICS or setting-up test access to a ACQ server port for the duration of the evaluation
  Remark: audit of the Acquirer System would be an option in case of remote testing.

3.2.2 Tests to be performed according to the ICS

The Test Lab will determine the Tests to be executed during the evaluation based on the validated ICS.

3.2.3 Certification Applicant appropriateness verification

The Certification Applicant and its Certification Object are identified by a registration number given by the selected Certification Body as described in the [CFCF Process].

3.2.4 Certification Applicant's Sample identification (hardware, software)

The Certification Object sample must be identified with the following information:

- Vendor name
- Vendor Registration Number
- Sample number including its serial number
- Sample product name
- Date sample produced

- hardware identification with a hardware version number
- Operating system identification (no checksum required)
- software identification with a software version & software module checksum
- checksum: Certification Applicant generates checksums to identify and verify the integrity of application modules (HAP). The checksum must be a unique value for each application and for each version of the application. The method or algorithm used for generating the checksum is left to the discretion of the Certification Applicant. SHA-1 or CRC might be chosen for example This value must be easily retrievable from the ACQ for comparative purposes.

3.2.5 Powering the sample definition (how to operate the sample)

Access to the ACQ sample must be supplied with the necessary documentation and support in order to operate the terminal sample during the testing phase. The certification applicant must make itself available in a reasonable time to answer any laboratory question about sample operation.

3.2.6 Upper Tester (UT) requirements & definition

If required by the test plan, the ACQ may be provided with Upper Tester capability (for example: Issuer authorisation simulator for a Host Acquirer System).

3.2.7 Certification Applicant's UT identification & documentation

If UT is required, the Certification Applicant must provide UT's identification and documentation as well as the necessary support to the laboratory to operate the UT.

3.3 Test case policy

The Test Specification consists of a set of test cases for POI and ACQ applications, as referenced in [CFCF References].

The implementation of POI and ACQ applications shall be based on the nexo IS and not on the test cases.

Test cases may change over time and the scope of testing covers only a certain part of the nexo IS requirements. Hence it is the Vendor's responsibility to fully implement the nexo IS specifications and to verify that all the requirements are correctly implemented.

The CFCF Certification Committee decides on the applicable versions of the Test Specifications. The valid Test Specification versions are referred in [CFCF References].

4 Requirements for test laboratories

4.1 Requirements concerning the test reports

Test results are presented in a test report, signed by a laboratory accredited by a Certification Body accredited by the CFCF Consortium.

The Test report must meet the following requirements:

- Test reports must be in electronic PDF format. When sent to the Certification Body for review, the test report must be password protected using Acrobat or equivalent pdf editing software security tools. The password may be attributed to the Laboratory by the Certification Body.
- Each test report must be signed by the laboratory that performed the tests. The signature may be digital by using the signature capabilities of Acrobat or equivalent pdf editing software.
- Test reports must include
  - the ICS reference number on the cover page and the identification of the qualified test tools used during the tests,
  - the Certification Applicant's sample identification as specified in section 3.2.4 of this document including photos of the terminal (back and front).
  - test performance dates and the date of the final test,
  - all test cases, and each must be designated as Pass, Fail, Inconclusive (Not Conclusive) or Not Applicable,
  - identification of the test tools, version and status must be provided for each test,
  - a detailed description of any exception test(s) performed or equipment used and a description of the related test results,
  - a detailed analysis from the laboratory of any test results designated as Fail or Inconclusive (technical advice).

    The detailed analysis shall at least include the "expected behavior" (requirements or pass criteria) and the "Product behavior" observed during the test.
  - If any modification was made to the ICS during the test session (without any modification to the certification object), the test report must identify the reason for the change and must include the laboratory's assessment of the impact and the tests performed showing there were no impact on the on-going evaluation.
  - Test results must be based upon the current valid Test plan as defined in [CFCF References].
  - Test results must be presented according to the test result summary for POI and ACQ application provided by the CFCF Consortium.

The Certification applicant determines whether the test results resulting from laboratory testing will be submitted to a CFCF Accredited Certification Body for evaluation.

The Certification Body does not comment in advance on acceptance of a test report until it has received the completed test report.

4.2 Requirements concerning the usage of Test Tools

The test laboratory:

- must ensure that test tools used for testing POI and ACQ have been qualified by the CFCF Consortium,
- is informed by the CFCF Consortium about the new qualified versions of test tools to be used for testing,
- identifies in its test reports the qualification reference number of the test tool used for testing,
- will inform the Certification Body of any test tool nonconformance found during a test session. The impacted test case will feature “inconclusive” as a test result.
- receives from the CFCF Consortium confirmation when a new qualified version of the test tool has to be used and/or any migration dates for implementation of new qualified versions.

The procedure of the qualification of test tools and the maintenance process of test tools as well as the responsibilities of the test tool provider is described in [CFCF Tools].

5 Requirements for lab accreditation

Preamble:

- The 1st product evaluation will serve to accredit a test laboratory.
- A pre-requisite for lab accreditation is to use a test tool qualified by the CFCF Consortium.
- Other accreditation criteria are: business, security, administrative and technical ability.

5.1 Types of Accreditation Audits

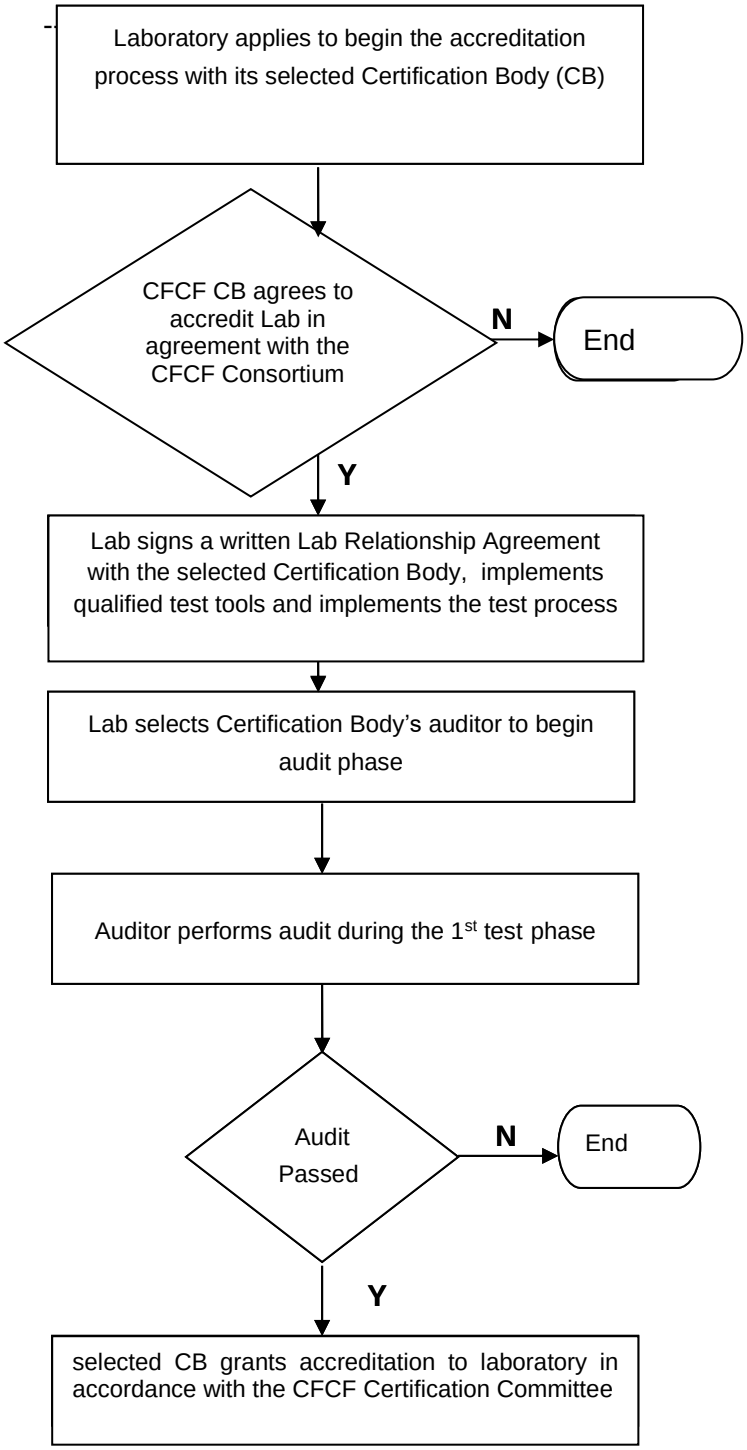
A laboratory facility must obtain and maintain the accreditation of the CFCF Consortium. Therefore, several types of audits may be required under a Laboratory's Relationship Agreement with the recognized Certification Bodies.

- Initial Accreditation Audit
- Accreditation Renewal Audit
- Incremental Accreditation Audit
- Interim Proficiency Audit

When a laboratory initially requests the accreditation by a Certification Body, the laboratory supplies the CFCF Consortium and the selected Certification Body with documentation about the laboratory including an overview of its abilities to meet the CFCF Consortium's accreditation requirements. Once the CFCF Consortium and the Certification Body have reviewed the documents supplied and have accepted the laboratory for potential accreditation, a full accreditation audit is required.

5.2 Accreditation Processes

The figure below shows the Laboratory accreditation process.



Below the laboratory accreditation process is described in detail.

Laboratory
Sends accreditation request to a selected CFCF Certification Body that will relay it to the CFCF Consortium to begin the accreditation process.

The request should include the following:

- Executive and financial summary
- Technical expertise summary
- Laboratory background
- Laboratory accreditation request
- Selected Certification Body.

The CFCF Consortium (Certification Committee)
Evaluates together with the selected Certification Body whether the laboratory facility qualifies to be accepted for consideration as a potential Accredited Laboratory.
Informs laboratory and selected Certification Body(ies) if it may proceed with accreditation.

Certification Body(ies)
Provides laboratory with:

- a written Laboratory Relationship Agreement for signature, which must include the mandate to meet the requirements outlined in sections 4 and 5 of this document.

Note: If the laboratory is already accredited as a functional testing laboratory by GBIC or by PayCert, the associated contract between GBIC/PayCert and the specific laboratory is comparable to the required Laboratory Relationship Agreement. This means that a Laboratory Relationship Agreement is not necessary. The existing contract is sufficient to meet the CFCF requirements for entering into a Laboratory Relationship Agreement and its contents.

Laboratory
Signs the Laboratory Relationship Agreement and returns two signed copies to the Certification Body.

Certification Body

- Signs the Laboratory Relationship Agreement and sends a signed version to the laboratory
- Requests a demonstration of testing capabilities as described in section 5.4.3.

Laboratory

- Purchases the necessary qualified test Tools or develops necessary test tools and applies for qualification for the tools

- Obtains adequate training on nexo IS test cases and test tools
- Contacts the Certification Body that will propose an auditor and makes legal arrangements with the auditor for the laboratory and its facility to be audited. The Certification Body will inform the CFCF Certification Committee about the application of the test lab to be accredited.
- Provides to the auditor the information required to meet the audit requirements
- plans a test session during the audit during which the lab will demonstrate its testing capabilities as described in section 5.4.3.

Laboratory

- Answers to the audit findings described in the audit report and defines a corrective action plan that will be sent to the Certification Body at the latest 2 weeks after 1st version of the audit report has been delivered to the Lab.

The qualified auditor

- Reviews and validates the action plan defined by the laboratory
- Provides a copy of the validated laboratory action plan included in its audit report to the Certification Body

Certification Body

- Reviews the audit report and the Lab test report issued after the 1st test session to determine whether the laboratory facility may be in agreement with the selected Certification Body(ies) accredited.

Note: *The Consortium reserves the right to deny accreditation at its own discretion and without detailed explanation.*

If the audit report is acceptable, the Certification Body:

- Signs the Audit Report and sends a signed version to the laboratory
- Sends to the laboratory a confirmation of Accreditation
- Adds the laboratory facility to the list of Accredited laboratories

5.3 Laboratory requirements

A laboratory must satisfy all requirements in this document. A laboratory must obtain and keep current its accreditation(s) with the Certification Body and must successfully meet all audit requirements at Certification Body's request.

This section identifies the business, security, administrative, and technical requirements which a laboratory must meet in order to obtain and maintain a CFCF accreditation.

5.3.1 Business requirements

This section describes the overall business requirements which a laboratory must meet.

Financial
The laboratory must conduct business in a manner that is consistent with the highest ethical standards and with practices that minimize risk. The laboratory must be subject to a due diligence review, with the primary focus of identifying and mitigating potential financial and goodwill risks.

- The laboratory must have a sound financial basis and be a part of a stable organization.
- The laboratory must adhere to ethical business standards and practices.
- The laboratory must have no financial dependencies on any Certification Applicant for which testing is being performed other than the Certification Applicant's payment for the service provided.
- The laboratory must have no financial dependencies on any CFCF member with regards to performance of any evaluation activity unless permitted in writing by the CFCF Consortium.
- The laboratory must be free of any past fraudulent or criminal activity.

Legal
The laboratory must be recognized as a legal entity and must be (or must be part of) an organization that is registered as a tax-paying business or as having a tax exempt status or as a legal entity in some form with a national body.

The laboratory must be able to sign and abide by all the Certification Body's legal agreements for accredited testing laboratories, including the Laboratory Relationship Agreement.

Public Communications
The laboratory agrees to abide by the CFCF Consortium 's policy that testing performed at any Accredited Laboratory is acceptable for Certification, and must make no claims to the contrary in its marketing material.

The laboratory must not, under any circumstances, communicate nor disclose to any third party, including to the Certification Applicant or other entity submitting a product for testing, that a product has or has not been certified by a CFCF Certification Body. The CFCF Certification Body, not the laboratory, shall be the final party to determine whether a particular Certification Object conforms to CFCF's requirements.

Independence

The laboratory must be able to demonstrate independence in test case analysis methodology and testing processes from the party involved in the design or manufacturing of the Certification Object under test.

The laboratory must receive communication and direction related to Certification testing only from a Certification Body.

Consistent Business Practices
Qualified test tools are supposed to produce consistent test results.

Therefore it is mandatory that any test result from any CFCF Accredited Laboratory be recognized by all other CFCF accredited laboratories, without any further investigation and without any discrimination regarding pricing for complementary testing.

5.3.2 Security requirements

This section describes the security requirements that a laboratory must meet.

Physical
The laboratory must maintain and comply with a physical security policy that includes, at a minimum, the following requirements.

Physical Layout
The laboratory must have sufficient security measures to prevent unauthorized people from entering the building(s) of the facility seeking accreditation and the laboratory's administrative offices (if separate). If the laboratory facility or administrative offices is part of a shared building or complex, there must be sufficient security measures to prevent unauthorized people from entering the laboratory's facility or offices.

Testing Areas
Areas in the laboratory facilities in which terminal products, components, or data are tested or stored are called *Testing Areas* for the purpose of this document.

In any given facility, the Testing Area is clearly delimited from the rest of other company areas and entry to the Testing Area must be restricted to authorized employees.

It must be verified during the audit for the initial authorization whether available audit results of a valid EMVCo audit can be re-used.

Storage
Test samples of the certification objects must be stored in a clearly identified and delimited Certification storage area. Entry to any Certification storage area must be restricted to authorized employees. The same requirements apply to additional storage that must be provided for all materials retained by the laboratory after testing has been completed.

Logical Security

The laboratory must maintain and comply with a logical security policy that includes, at a minimum, the following requirements.

Classified Materials and Information

As for test samples, the CFCF Consortium documents and specifications must be handled with particular care and kept within the company such that they are accessible only to persons appointed by the business management. These materials must be controlled and stored securely in electronic or paper format.

Disclosure of Certification or Certification Applicant data and documents to third parties must be authorized in writing by an officer of the company that owns the data or documents to be released. Receipt of restricted information must be acknowledged by signature of the company's official representative.

Classified material must be stored in secure containers, where unauthorized access is prevented by appropriate measures (e.g. alarms, surveillance, and/or sufficient mechanical protection).

The laboratory must hold in strict confidence any classified information received from the CFCF Certification Body or Certification Applicant. Classified documents must be stored according to their classification level. When a Certification Applicant grants permission to the laboratory to release classified information concerning the Certification object to Certification Bodies, this information may be released only to Certification Bodies. The Certification Bodies could only release the information to appropriate members and other key personnel of the CFCF Consortium.

Test Reports

All evaluation reports must be stored securely. If reports are stored electronically, they must be in an industry-recognized protected form. All back-up processes must be appropriately managed by the laboratory according to industry standards for recovery purposes.

A laboratory facility must store Certification object samples and all reports and logs from the test sessions (whether paper or electronic) for a defined period.

When issuing an electronic report to a Certification Body, the report must be password-protected using the Certification Body approved technique. Passwords must never be sent in the same email as the actual report. Passwords for a CFCF Certification Body may not be shared with third parties.

Test Equipment Access

Non-necessary personnel must not be able to gain access to CFCF test tools, test software or test networks.

It must be verified during the audit for the initial accreditation whether available audit results of a valid EMVCo audit can be re-used.

Test Equipment Hardware Maintenance
Any maintenance work on test equipment hardware and hardware systems must be authorized before work begins. The work must be performed under the control and authorization of the laboratory's staff, and there must be a documented procedure signing the equipment over to maintenance and signing the equipment back to production.

Test Equipment Software Maintenance
Test equipment software must be protected from unauthorized modification. Any update to the CFCF test tool for terminal product testing must be performed under the control and authorization of the laboratory's staff. It is also recommended to seek an approval by the Certification Body prior to a software update.

The laboratory must maintain documentation of any change to test equipment software including test system engine or individual test scripts to perform the test cases. This documentation must provide detailed information concerning the nature of the change to the test equipment software, the reason for the change, and the date of authorization by the Certification Body.

The update of the test software must be performed under continuous supervision of the laboratory's staff. If test tool equipment must be sent to the vendor or supplier to upgrade the tool software, there must be documented procedures for signing the test equipment over to the test equipment vendor or supplier and signing the equipment back to production.

Networks
Any computers used to store secure information (evaluation reports, Certification Applicant data, etc.) must not be connected to a network that allows unauthorized personnel access.

If the laboratory uses a non-dedicated network, then suitable controls must be in place to protect the integrity of the data within the laboratory. These controls include the use of firewalls and routers that offer sufficient security levels for the data being handled.

Networks linking the laboratory to third parties for the transfer of customer information must be separate and isolated from the test system, either physically or using network filters and adequate authentication.

Networks that link separate laboratory premises must use the network controls described above and all security sensitive data must be encrypted when using such networks.

The laboratory must have a secure method of transferring customer data to test samples and equipment that does not introduce security risks or vulnerabilities.

5.3.3 Administrative Requirements

This section describes the administrative requirements that a laboratory must meet.

Quality Assurance

The laboratory must have a quality system based upon ISO 17025 requirements, providing documented procedures defining processes to ensure a high quality of testing and test reproducibility. These procedures must comply with the CFCF Consortium's certification Process and must include, for example:

- Test methods and procedures
- Reporting of tests aimed at reproducibility and consistency
- Laboratory practices such as laboratory log books
- Procedures for maintaining accuracy and availability in equipment, including periodic calibration and justification of all measurement tools used for testing
- Procedures for test sample identification and secure storage
- Procedures for maintaining confidentiality of entrusted information

The laboratory must maintain an up-to-date library of technical reference material (books, papers, articles, etc.) on methods, standards, techniques, and equipment that are resident in the laboratory facility seeking accreditation and that provide information required for laboratory test performance. The laboratory must also maintain up-to-date records of equipment maintenance.

The level of the above quality requirements and other requirements has been described in various international standards. A laboratory shall comply with ISO 17025 or have a comparable quality system, and must also comply with the requirements stated elsewhere in this document.

In case the laboratory is ISO 17025 accredited, a valid accreditation must be provided each year by the Accredited Laboratory to the Certification Body.

Other comparable proof of accreditations, such as an EMVCo accreditation report, must also be provided to the Certification Body on a yearly basis.

Personnel

Each facility must maintain a list of its qualified test personnel consisting of a description of their role in the organization and facility, their qualifications, and their experience. The laboratory must have procedures to ensure an adequate match between staff training and roles in the performance of the Certification activities.

When employees are terminated, the laboratory must have designated staff members who execute and document the following:

- Recover the employee’s photo ID badge or access card, access keys, or passes and immediately deactivate any access devices.
- Ensure that the employee surrenders all property and documentation involving testing and Certification processes.
- Ensure that all computer (local area network [LAN]) access passwords are revoked or changed.
- Complete an employee termination checklist, which must include the above as a minimum.

5.3.4 Technical Requirements

Technical Expertise

An Accredited Laboratory for POI and ACQ application testing must have staff with an appropriate level of knowledge in the following areas:

- POI technology and operation
- Acquiring system technology and operation
- specification functionality

It is not necessary that each member of the laboratory facility's staff have knowledge and skills in each of these areas, but the laboratory facility staff as a whole must have an expert level of knowledge in the identified areas.

Laboratory facility personnel must be skilled in using the laboratory facility's equipment (i.e. validated test tool) and applying the laboratory techniques.

Experience

The laboratory should have several years of experience testing applications for payment systems. Laboratories with multiple facilities must be able to demonstrate that each facility for which it seeks accreditation has sufficient access to this testing expertise.

Equipment

The laboratory facility must have a CFCF qualified Test Tool to verify whether the Certification Object is compliant with the specifications referenced by CFCF. The list of qualified Test Tools is published on the CFCF website (www.cfcf.eu).

The laboratory must archive previous versions of test plans, test suites and test tools during the pilot phase.

Involvement to improve the quality of certification infrastructure

The laboratory must commit to make its best effort to improve the certification infrastructure by reporting all known discrepancies and eventual dysfunctions to its Certification Body.

The Laboratory must also cooperate in the test tools qualification procedures and accepts to share information with other laboratories and test tool providers during such procedures.

5.4 Audit requirements

In order to demonstrate sufficient conformance with the laboratory requirements in section 5.3, the laboratory must do the following:

- Provide written evidence to the CFCF auditor before the audit
- Complete a site visit
- Demonstrate testing capabilities during the 1st test session
- Complete a corrective action plan, if applicable

This section describes information that the laboratory is required to supply to the auditor, and the level of detail required in the audit reports. The auditor, in reviewing the documentation, may request additional information from the laboratory prior to or during the site visit and/or the demonstration of testing capabilities.

In preparation for the audit, the laboratory will provide written consent for disclosure of this information to the CFCF Consortium, the Certification Body and to the auditor during the site visit.

The audit report that the Certification Body receives from the auditor must have the level of detail specified in this section and must satisfy the audit report requirements.

5.4.1 Written evidence

In case the laboratory has been accredited by EMVCo (Level 2 testing) the written evidence provided to EMVCo can be reused for the laboratory accreditation process.

Business conformance
The laboratory provides the auditor with evidence of conformance with the laboratory business requirements. This evidence may be in the form of a written report describing:

- Services of the organization
- Structure of the organization, demonstrating the isolation between the laboratory and other areas of the organization (e.g. design area)
- Organization legal information
- Certificate of ownership and/or tax identification number

In addition, the laboratory must provide the auditor with the following:

- Audited financial statements for the organization
- Official Annual Report as required by national or international law and/or regulation

Security Conformance

The laboratory provides to the auditor evidence of physical and logical security conformance. This evidence must be in one of the following forms:

1. Included within laboratory procedures and documentation, or
2. A written report describing:

    - Laboratory security policy with particular focus on the physical and logical network security measures
    - Personnel background check security policies
    - Confidential data protection practices

Administrative Conformance

The laboratory provides to the auditor evidence of administrative conformance. This evidence may be in the form of a written report describing:

- other formal accreditations (ISO 17025, ISO 9001…)
- Experience relevant to the desired laboratory role within the European payments area
- Description of the laboratory's quality assurance system

The quality assurance system must comply with the requirements of the CFCF Certification Process and must be in line with to ISO 17025. As such, the Quality assurance system must feature written descriptions such as, for instance:

- Overview of the laboratory personnel and the qualifications of laboratory personnel involved in the performance of any testing or administrative duties connected with Certification to be conducted at the facility seeking accreditation,
- Overview of the laboratory facility's equipment and techniques,
- Description of the laboratory security policy with particular focus on the procedures for identification and recording of test samples,
- Overview of laboratory asset management system for documentation and equipment.

The laboratory shall also implement personnel management procedures or equivalent and be able to provide written evidence that each employee or subcontractor complies to the CFCF Consortium requirements regarding personnel management (§ 5.3.3 and 5.3.4).

5.4.2 Site visit

The Consortium requires a site visit at each facility for which the laboratory is seeking an accreditation.

The objectives of the site visit are to:

- Verify that laboratory documentation and actual laboratory implementation are in agreement,
- Observe the physical environment of the organization and the physical security and organizational measures taken,
- Verify that the laboratory's personnel information is on file (to the extent it is legally permissible for the auditor to examine this information),
- Verify the laboratory's technical expertise,
- Verify the laboratory's quality assurance procedures. CFCF's efforts will depend on the availability of an ISO 17025 certificate.

If the laboratory has an ISO 17025 certificate covering the facility performing the testing:

- Evidence that the evaluations are carried according to equivalent methods and procedures to the ones that are in the scope of the ISO 17025.
- The laboratory provides a copy of the audit report corresponding to the ISO 17025 certificate to the auditor.
- The auditor reviews the audit report to use as evidence of compliance in the audit report for Certification Body and audits the laboratory for the requirements not covered by the ISO 17025 certificate.
- In the absence of an ISO 17025 certificate, a full audit of the laboratory must be conducted to assess that all CFCF Consortium requirements for laboratories are met.

5.4.3 Demonstration of Testing Capabilities

The Certification Body will require a demonstration of the laboratory facility's actual testing capabilities. This will be done through witnessing the laboratory facility's testing during its 1st certification testing.

Certification testing is defined as the laboratory facility's certification testing of a POI or an ACQ Application that is candidate to Certification or that was previously certified by a Certification Body, and providing a test report to the auditor to review. The choice of subject for this certification testing is at the discretion of the CFCF Consortium in agreement with the Certification Body and both reserves the right to witness a part of this evaluation.

The format and presentation of assurance evidence will be an essential part of this exercise, in addition to the demonstration of testing capability. Results are expected to be prepared in accordance with ISO 17025 standards and the Consortium requirements.

The test report, corresponding to the demonstrated certification testing, will be provided to the auditor and/ the Certification Body as written element to assess the laboratory compliance statement.

Note: If the audit is performed to maintain a lab's accreditation, the demonstration of the laboratory facility's testing capabilities will be optional and the decision to demonstrate or not will be left at the discretion of the CFCF Certification Committee in agreement with the Certification Body.

5.4.4 Corrective action plan

An audit report may indicate that the laboratory does not meet all necessary requirements for a facility, but has demonstrated sufficient capabilities that with specific corrective actions, it would meet such requirements. If so, in a delay of 2 weeks:

- The laboratory will define an action plan with deliverables and due dates to meet all Consortium requirements.
- The auditor will review and validate the action plan to be included in the audit report to the Certification Body.

5.4.5 Fast-track accreditation (re-use of an EMVCo Accreditation)

In case of an initial accreditation request, a Test Laboratory could choose to benefit of a fast-track accreditation procedure enabling to re-use a valid EMVCo accreditation for terminal evaluation (contact or contactless kernels).

In order to validate its "Fast-track accreditation" the candidate laboratory will join to its application letter a valid EMVCo Accreditation letter as well as an EMVCo Audit report dating from less than 2 years.

When being notified that its "Fast-track accreditation" request has been accepted the candidate lab will be dispensed from the following steps :

- Security conformance as in § 5.4.1
- Administrative conformance in § 5.4.1
- Site visit in § 5.4.2

The lab will still have to provide justification for the Business Requirements (as in 5.4.1) if requested by the Certification Body and will have in any case to demonstrate its testing capabilities (as in § 5.4.3).

The lab will also have to provide the following elements to the Certification Body prior to its first evaluation :

- reference and supplier of the Qualified Test Tool(s),
- draft of a test report,
- elements proving that its staff possesses the necessary technical expertise,
- documented process about the testing activities.

5.5 Non-conformance, modification or termination of Accreditation

5.5.1 Non-conformance Investigation

Retesting at an Accredited Laboratory
At any time, based on the terms of the Laboratory Relationship Agreement with the Certification Body, the Certification Body, eventually upon request from the Consortium, at their common discretion, may require a retesting exercise to confirm whether results from Certification object testing at the laboratory's facility are correct. Retesting may include testing of Certification object sample(s) originally tested at the laboratory facility and Certification object sample(s) from the field.

Cross Testing between accredited laboratories
At any time under the Laboratory Relationship Agreement with the Certification Body, both, at their common discretion, may organise a cross testing exercise to evaluate whether test results for Certification Object tested at the laboratory's facility are the same as test results for the same Certification Object tested at another Accredited Laboratory.

Corrective Action for Non-conformance
Based on the results of retesting or cross testing, one of the following may occur:

- The Certification Body may require for an update of the test case documentation from the specification provider.
- The Certification Body may require that a test tool be re-qualified.
- The Certification Body may revoke a product's certification.

5.5.2 Modification or Termination

At any time, a laboratory's accreditation may be modified or terminated:

- A laboratory or facility may decide to add or cease offering a specific testing service.
- A laboratory or facility may decide to terminate its accreditation.
- A Certification Body may decide to revoke a laboratory's accreditation

Change in Testing Services Offered
If a facility or the laboratory generally, decides to change the Consortium's specific testing service, the laboratory must inform the Certification Body. Upon receipt of such request, the Certification Body will modify the applicable exhibit to the Laboratory Relationship Agreement accordingly, re-issue a letter of accreditation (without changing the accreditation expiration date), and update the list of accredited laboratories.

Termination of accreditation
At any time, a laboratory can inform the Certification Body of the termination of its Laboratory Relationship Agreement or one or more accreditation(s), in accordance with the terms of the Laboratory Relationship Agreement or of the Letter of Accreditation.

Upon receipt of such information, the Certification Body will confirm termination of the Laboratory Relationship Agreement and/or accreditation(s) and remove the laboratory's and/or applicable facility's name from the list of accredited Laboratories in agreement with the Consortium.

Upon termination of a facility's accreditation, the facility must promptly deliver to Certification Body all of its test reports, test logs, and Certification Object samples for products already approved by a Certification Body or currently in testing for Certification. The facility must also promptly return to the Certification Body all property and all confidential information. Alternatively, if so directed by the Certification Body, the facility must destroy all confidential information, and all copies thereof, in the facility's possession or control, and must provide a certificate signed by an officer of the laboratory that certifies such destruction in detail acceptable to the Certification Body.

The Certification Body informs the Consortium about this process immediately.

Suspension of Accreditation
At any time, at the Certification Body's own discretion, but in close coordination with the Certification Committee, the Certification Body may suspend a laboratory's accreditation:

- Based on the results of an audit report
- Due to the laboratory's or a facility's nonconformance

If the accreditation of a laboratory is suspended the name of the Laboratory and/or facility will be removed from the list of accredited laboratories.

Revocation of Accreditation
At any time and at the Certification Body's own discretion, but in close coordination with the Consortium the Certification Body may revoke a laboratory's accreditation:

- Based upon the results of an audit report
- Due to the laboratory's or a facility's nonconformance

Upon request of revocation of an accreditation made by the Consortium, the Certification Body may terminate the Laboratory Relationship Agreement with the laboratory, with or without cause, in accordance with its terms. The Certification Body may also remove the laboratory's and/or facility's name from the list of Accredited Laboratories.

Upon revocation of a laboratory facility's accreditation, the laboratory must make available to the Certification Body all test reports, test logs, and Certification object samples for products

already certified by a Certification Body or currently in testing for Certification. The laboratory must also promptly return to the Certification Body all property and all confidential information. Alternatively, if so directed by Certification Body, the laboratory must destroy all confidential information, and all copies thereof, in the laboratory's possession or control, and must provide a certificate signed by an officer of the laboratory that certifies such destruction in detail acceptable to the Certification Body.

The Certification Body informs the Consortium about this process immediately.