Programme Guideline G6

End-to-End Certification Process for Point of Sale Equipment

AMENDMENT HISTORY

Version	Date	Remarks
0.1	29/11/02	First draft
0.2	16/01/03	Revised following comments from schemes and acquirers
0.3	20/01/03	Further revision following comment from scheme
0.4	14/02/03	Revised following workshop on 5/02/03
0.5	10/03/03	Further revisions following workshop on 3/03/03; issued for final review prior to approval
0.9	27/03/03	Version incorporating suggested changes/amendments from APACS and Amex
1.0	11/04/03	Approved
1.1	11/6/03	Changes made to sections, 3.1, 4.2.2, 4.4, 4.4.1, 4.4.3
1.2	26/03/04	Revised for changes to certification process
1.3	16/04/04	Revised following comments
1.3a	19/04/04	Revised following additional comments
1.4	20/05/04	Revised for updated PED requirements and process
2.0	27/05/04	Approved by ISC

DOCUMENT IDENTIFICATION

Location on shared area: Shared Directories/Programme Documentation/Tech & Ops/Guidelines

AUTHOR

Name	Position
Nick Green	Technical Consultant
Mike Hendry	Technical & Operations Director
Jo Down	Technical & Operations Consultant

DISTRIBUTION

Name	Position	Reason for distribution

FORECAST LIFECYCLE

Version	Owner	Anticipated movement
2.0	Mike Hendry	

SIGN OFF / ACCEPTANCE

Name	Date	Signature
Mike Hendry		
ISC		

TABLE OF CONTENTS

1 Scope

The purpose of this paper is to describe the End-to-End certification process which must[1] be completed by all vendors and retailers, in order for their Point of Sale terminal products, software and systems to be usable for processing payment scheme transactions in the context of the UK Chip and PIN Programme. Some parts of the process are applicable to vendors and others to retailers. This distinction is made clear in the text.

This Guideline does not cover the certification processes for cards, card issuing and personalisation systems, acquirer systems, ATMs and ATM acquirer systems, nor the optional card personalisation verification services operated by the card schemes. These are in general applicable to banks and bank suppliers only.

The document was discussed at two workshops in 2003 by schemes, acquirers and vendors and retailers with experience of the process. This revision represents the current understanding of the process, following changes over time and specifically to the MasterCard ETEC process.

The document is now offered for final review prior to approval by the Technical and Operations Steering Committee as an updated Programme Guideline.

This paper has the status of a Guideline. It is not mandatory on participants, but following this Guideline is likely to lead to a more consistent approach across the Programme and should minimise user confusion. In addition, schemes and acquirers may have their own requirements that may be mandatory.

The Guideline covers the requirements for Point of Sale terminals processing Visa, MasterCard, Switch, American Express and JCB transactions. It covers the requirements for the Transition period in which users are becoming familiar with Chip and PIN technology and for the mature chip and PIN environment. It includes both attended and unattended devices, but excludes PC-connected devices for e-commerce, ATMs and bank branch terminals. Although most of the requirements would also apply to acquirer-owned terminals, the focus of this Guideline is on retailer-owned terminals and systems.

The certification processes described in this Guideline are not a replacement for functional testing processes, nor should they be used for debugging. The processes described should only be used once the relevant hardware, software and systems are judged to be fully working and fit for purpose.

All timescales and costs quoted in this Guideline are approximate and as of March 2004; they may be updated at any time.

Sections 3 - 6 describe the tests that must be carried out and the processes that must be followed. Section 7 gives an indication of the best timescales achievable.

[1] Not all the individual elements described in this guideline are mandatory

2 Structure of certification

The certification process consists of four distinct phases:

- EMV Level 1 type approval (hardware)
- EMV Level 2 type approval (software)
- Scheme-specific integration tests
- Acquirer testing

Within the second and third phases, several tests may be carried out. PINpad security testing will normally take place during the second phase, but could be carried out earlier. Phases 3 and 4 may overlap, particularly where acquirers have delegated authority.

Phase 1	EMV Level 1 type approval MasterCard Terminal Quality Management
Phase 2	EMV Level 2 type approval PINpad security certification JCB Manufacturer Test
Phase 3	MasterCard Environment of Use Testing Visa Acquirer Device Validation Toolkit (ADVTK) American Express device Testing Other scheme tests (if required)
Phase 4	Acquirer end-to-end testing

Each of these testing stages is described in the following sections.

3 Phase 1

3.1 EMV Level 1 Type Approval

All devices that come into electrical contact with EMV Cards (e.g. Card Readers or combined PINpad - Card Readers) must use an Interface Module (IFM) type-approved to EMV Level 1 by an approved EMV testing laboratory. The purpose of this certification is to protect chips on cards. Laboratories are available in a number of countries and a list can be found at www.emvco.com and using the menu: Type Approval -> Laboratories.

Retailers and Systems Integrators may select devices incorporating IFMs that have already achieved Level 1 Type Approval – these IFMs are listed at www.emvco.com using the menu: Type Approval -> Level 1 Approved Interface Modules. Selection of devices that do not have this approval will increase considerably the total time required for certification and the risk that hardware design changes will be required.

3.1.1 Versions

From 1 April 2004 EMV Level 1 Certification may only be carried out against EMV 4.0 specifications.

Devices that have received certification against EMV 3.1.1 (with Errata) may continue to be used without limitation. However, if they are submitted for recertification, they will be subjected to extra testing in line with the EMV 4.0 and this may result in a failure and a requirement to retest. There is no requirement that devices in the field be withdrawn in this situation (although retailers may consider the failure to be of sufficient severity that it will affect their business and seek to upgrade the equipment.)

3.1.2 Test tools and scripts

Vendors are advised to acquire one of the test tools recommended by the card schemes[2]. These are updated regularly when new test scripts are released.

3.1.3 Responsibility

It is the responsibility of the device manufacturer / vendor to obtain this certification.

3.1.4 Impact

No equipment can be used to process chip card transactions from any of the international card schemes that does not have this certification.

3.1.5 Timescales

The lead time for obtaining a testing slot with an approved laboratory is currently around 1 week.(March 2004). Before booking with the laboratory, vendors must register with EMVCo

[2] E.g. Integri (functional only), Orga (electrical only), VXI ATE

(using the documents on the EMVCo website). Two weeks should be allowed for this. The testing takes 1 - 2 weeks, and the production of a test report a further 2 weeks. This test report must be sent to EMVCo in New York either by the vendor or by the test lab and can be sent in electronic format; if the report is clean and the fee has been paid then a certificate is issued in 2 - 3 weeks. If the report contains any failures, a full re-test will normally be required.

Disputed reports may take some time to resolve, and there have been many reported issues with the test tools. Laboratories report that approximately 50% of systems pass first time, however nearly all pass at the second attempt following minor modifications. Most laboratories offer a pre-certification process to increase the chances of a first-time pass.

3.1.6 Recertification

EMVCo have defined (in Type Approval Bulletin no 11) major and minor changes which determine whether the change requires recertification. EMVCo Type Approval Bulletin no 11 states that 'examples of a major change would include change of firmware, change of contacts, change of clock crystals and change of PCB layout. Major changes require the new component to be submitted to EMVCo for a new Type Approval. Minor changes would include a change of connector, change of transistor or change in capacitor'. It is the vendor's responsibility to determine whether a change is major or minor, but anything which significantly impacts the functionality of the IFM must be considered a major change.

3.2 MasterCard Terminal Quality Management

MasterCard's Terminal Quality Management (TQM) programme is complementary to the EMVCo Level 1 Interface Module tests and has been mandated by MasterCard since July 2003. However vendors have up to 12 months in production to comply and the label can be obtained in parallel with TIP testing. Vendors sign an agreement with MasterCard to enrol in the programme.

MasterCard grants a TQM label when the terminal vendor complies with the quality requirements and may be granted to terminals having EMVCo type approved IFM. EMVCo Level 1 covers the sample testing process while TQM covers the entire product life cycle.

4 Phase 2

4.1 EMV Level 2 Type Approval

To process transactions a device must have a supporting software application. Where this application resides will depend on the configuration of equipment implemented. The EMV application must be certified to EMV level 2 by an approved EMV testing laboratory. The purpose of this certification is to protect the integrity of the overall Chip and PIN environment. Laboratories are available in a number of countries and a list can be found at www.emvco.com and using the menu: Type Approval -> Laboratories. Where any part of the level 2 functions is carried out within the PINpad, the level 2 type approval must include the PINpad; where the PINpad only performs PIN entry, display and local encryption any approved PINpad (including level 1 approval where appropriate) may be used (see EMVCo Type Approval Bulletin no 11).

Where possible, a "kernel" providing the EMV functions should be identified within the overall software implementation. This allows the kernel to be certified and provides isolation from changes which need to be made to the actual implementation environment. It also permits a certified kernel provided by a specialist payment software company to be used in conjunction with EPOS application software developed by a retailer or a third party software house.

4.1.1 Versions

All vendors seeking Level 2 certification should use EMV 4.0. Applications type-approved under EMV 3.1.1 may continue to be used provided they have passed the "Errata tests" carried out in the second half of 2003, however if applications certified under EMV 3.1.1 are submitted for recertification they will be subject to extra testing in line with EMV 4.0 and this may result in a failure and a requirement to retest. It is possible to use an EMV 3.1.1 compliant IFM in conjunction with an EMV 4.0 application kernel providing that the combining of the components did not require additional modifications that could negatively impact the functionality of either component. The process of combining them would be a minor change as long as neither component is affected by a major change.

4.1.2 Test tools and scripts

Again, vendors are likely to require one of the approved test tools[3], and must arrange for these to be updated with the latest scripts when they are produced. Schemes and test tool vendors must liaise regularly with their customers to ensure that users are aware of updated cards and test scripts as soon as possible.

4.1.3 Responsibility

It is the responsibility of the software vendor to obtain this certification. Merchants must not used uncertified software, and the acquirer is required to ensure that uncertified software is not used.

[3] ICC SIM, KaSYS, Collis or MasterCard EVAL

4.1.4 Impact

No equipment can be used to process MasterCard, Visa, JCB or American Express chip card transactions that does not have this certification. MasterCard will fail the TIP process if the relevant PED is not quoted on the EMV Level 2 Certificate. From Q2 2004 it is possible for venors to obtain certification of software with multiple PEDs.

4.1.5 Timescales

The lead-time for obtaining a testing slot with an approved laboratory is approximately 1 week (March 2004).. Before booking with the laboratory, vendors must initiate registration with EMVCo (using the documents on the EMVCo website). Registration takes 2-3 weeks, but registration covers a vendor and may be for Level 1 and Level 2 simultaneously. Testing takes 1 week (best case), typically 2-3 weeks including re-tests, and the production of a test report a further 2 weeks. This test report must be sent to EMVCo in New York either by the vendor or by the test lab and can be sent in electronic format;; if the report is clean and the certification fee has been paid then a certificate is issued in 2-3 weeks.

4.1.6 Recertification

If the defined kernel is modified in any way that could affect its EMV functions, it must be recertified. Refer to section 3.1.6 for examples of major and minor changes.

4.2 Visa & MasterCard PINPad Certification

Visa and MasterCard have agreed to a standard methodology for how PIN Entry devices are tested and approved. These requirements ensure that the cardholder's PIN is protected at the point of sale.

To retain protection from liability of PIN compromise with Visa and MasterCard PIN pads being deployed must have passed a laboratory evaluation and be approved by the central approval centre[4]. Vendors can reduce the complexity of new product development by now undergoing security testing at one organised approval centre.

The new program is effective 1 October 2004 and will replace the current programs that Visa and MasterCard have in place. All POS PED vendors must meet the aligned requirements starting from this date. MasterCard have agreed to grandfather and accept all PEDs previously approved by Visa. Vendors have the option of submitting their PED for testing against Visa original requirements prior to 1 October 2004 and if approved by Visa, then they will be accepted by MasterCard. From 1 October the laboratories will only be evaluating PEDs against the new aligned requirements.

4.2.1 Responsibility

It is the responsibility of the vendor to obtain this certification.

4.2.2 Impact

Any devices newly installed, repaired or replaced after 1st October 2004 to process PIN-based Visa or MasterCard transactions must have this certification.

[4] Current approved laboratories are InfoGuard, TNO and T Systems

4.3 American Express PIN pad certification

American Express does not currently have any separate certification requirements for PINpads..

4.4 APACS PIN pad Evaluation

APACS member banks have adopted as policy a requirement that all PINpads installed in the UK should be evaluated against a Protection Profile, in accordance with Common Criteria (ISO 15408-1:1999) procedures. In order to facilitate this policy APACS has developed a Protection Profile for a PIN Entry Device, which itself has been evaluated and certified under the Common Criteria. This Protection Profile defines the security requirements for PINpads deployed in the UK.

All new devices deployed after 1st January 2004 must have undergone or be undergoing evaluation, and existing devices must be evaluated or replaced by 1st July 2010. Repaired or replacement devices will be allowed at the acquirer's discretion.

Evaluation must be carried out by an approved testing laboratory (CLEF - Certified Laboratory Evaluation Facility), which will produce a technical evaluation report which indicates the test outcome. This evaluation report should be submitted to the acquirer, which will carry out a business risk assessment. Acquirers should consult with APACS Card Services in order to ensure consistency. Vendors may additionally submit the evaluation report to CESG (Communications and Electronics Security Group - based at GCHQ, Cheltenham) for a formal Common Criteria certification. Any such certificate is recognised by other countries with whom the UK government has a reciprocal arrangement as stipulated in the 'Arrangement on the Recognition of CC certificates'[5](although there is no guarantee that it will be accepted by banking authorities in lieu of national criteria).

With this in mind vendors should aim to follow the Common Criteria and Protection Profile in their designs and design processes and should prepare to submit devices for testing against these specifications. Pre-evaluation consultancy against the specification is available from any of the CLEFs listed in Appendix A of Recommendation 10. Such consultancy does not tie the vendor to a formal evaluation with that CLEF.

Further details on the Protection Profile testing process, including a list of approved laboratories, are given in Programme Recommendation 10.

4.4.1 Timescales and cost

The likely timescale for the laboratory to conduct testing and issue a "Vendor Technical Report from Evaluation" is 4 - 8 months. However, vendors should add to this any time required for pre-evaluation consultancy, to prepare paperwork, and (if required) 4 – 6 weeks to obtain the CESG certificate. The indicative cost is £50,000 - £80,000 per evaluation, however this is subject to individual negotiation with the laboratory. Vendors may also wish to commission pre-evaluation consultancy from the laboratory.

[5] These include Australia, New Zealand, Canada, Finland, France, Germany, Greece, Italy, Netherlands, Norway, Spain, Sweden, USA (NIST & NSA), UK (CESG)

4.4.2 Responsibility

It will be the responsibility of the vendor to contract for and have completed the evaluation.

4.4.3 Impact

UK acquirers will not certify new systems unless the PINpads are covered by a positive report from an approved testing laboratory. (A formal CESG certificate is a vendor option).

4.5 PIN encryption

Where the PIN Pad and the card reader are separate devices and the PIN is passed between the devices on communications link then the PIN must be encrypted using a minimum of Triple DES. As this is a symmetrical key system the vendors must establish a scheme that will allow the PIN Pad and Card Reader to exchange / synchronise these Triple DES keys in a secure manner. The Vendor must submit a description of the scheme that they are using to the retailer's acquirer for agreement that the vendors' scheme is robust. It is recommended that the scheme chosen uses a known algorithm and does not rely on secrecy of a proprietary algorithm[6].

Further guidance on this requirement is given in Programme Recommendation 9.

[6] APACS Acquirers POS Group has asked the Card Security Group to recommend specific security schemes; other schemes will be acceptable provided they meet the criteria but approval may take longer.

5 Phase 3

5.1 MasterCard Terminal Integration Process (TIP)

This requirement is mandated by MasterCard and must be undertaken once integration of the certified EMV components into the retailer's system has been achieved.

It is required for each configuration (combination of hardware, software, operating system etc), and therefore every retailer variation has to undergo TIP testing.

Testing is carried out by the acquirer and the results and EPSS[7] logs are reviewed by MasterCard, unless the retailer's MasterCard acquirer has secured delegated authority to approve these tests[8]. These tests are typically carried out as a precursor to the acquirer's end to end testing (see section 6).

The tests have been divided into 'off-line' and 'online' testing; off-line tests need only be carried out once for all acquirers for all systems meeting a 'similarity test'. The offline testing is network independent and can be completed in the laboratory (with or without an acquirer connection), whilst the on-line testing is host specific and needs to be completed by each acquirer. Currently there are three labs in Europe with an option to increase in number if required. Once each system configuration has been registered as fully tested, each additional implementation with another retailer will only have to go through the 'online' testing to assess the proper integration with the Acquirer system.

The test which defines if two systems are sufficiently similar for the reduced test set to be used is defined below. The reduced test set can only be performed if the offline tests have been carried out in the lab.

The "same product" is defined as having the:
- same EMVCo level 1 approval
- same EMVCo level 2 approval including the same PIN pad if the PIN pad encrypts the PIN

MasterCard holds and maintains a register of configurations already tested to avoid repetitive testing by different Acquirers.

In practice this means that for a combination of the same Product for a different Retailer or Acquirer the connectivity subset of 20 cards and 84 tests needs to be completed. Where the combination consists of a different Product for the same Retailer or Acquirer the product subset without pre-requisite testing consists of 68 cards and tests and with pre-requisite testing 49 cards and tests.

[7] EPSS is the MasterCard central switching system

[8] No UK acquirer currently has delegated authority

5.1.1 Test tools and scripts

These tests are fully scripted and the MasterCard ETEC test pack (obtainable from MasterCard – price subject to quotation) is required. This will normally be supplied by the acquirer for the tests themselves, however for pre-testing the vendor may use the ETEC test pack or obtain additional scripts for its existing test pack.

Testing is in two parts:

- Part 1 is an interoperability test for MasterCard, Maestro and Cirrus branded cards (for ATM certification); it is mandatory, and is supported by around 70 cards in subset 1 of the ETEC test pack (current version is 4.0c).
- Part 2 is a regression test of the EMV application kernel; it is supported by the 100 cards in subset 2 of the ETEC test pack, and is optional. A reduced test can be performed, using 25 cards from subset 2, depending on the perceived level of regression risk.

These subsets of cards can be purchased separately.

5.1.2 Responsibility

Acquirers will not allow implementation of a chip card system without this certification. It is the responsibility of the retailer [for EPoS systems] and the terminal placer [for standalone terminals] to obtain this certification. However, the vendor or system integrator is expected to play a significant role.

5.1.3 Impact

No equipment can be used to process a MasterCard chip card transaction that does not have this certification.

5.1.4 Timescales

Retailers are advised to book as early as possible – minimum 2-3 weeks. TIP testing is likely to take at least 4 weeks (MasterCard estimates 3 weeks if the acquirer has achieved delegated authority). MasterCard's review of the test results takes approximately 1 week.

5.1.5 Recertification

Following any significant system changes Acquirers describe the change and MasterCard will ascertain whether all or part of the MasterCard TIP tests must be repeated along with other acquirer testing.

5.1.6 Certification Incident Management

The acquirers and MasterCard have agreed to an incident management process which has been created to manage and co-ordinate any incidents which occur, which cannot be resolved quickly and directly with the vendor or Scheme in question. It aims to remove any duplication of effort and ensure that all interested parties are aware of any issues and their resolution. Incidents must be specific and must be backed up with diagnostic information. It is imperative that these incidents are reported to the PMO immediately.

5.2 Visa Acquirer Device Validation Toolkit (ADVTK)

Visa has also specified tests to be carried out by the acquirer following integration and installation. The purpose of these tests is to ensure the parameters have been correctly set up for Visa cards, and to give confidence in the end-to-end system.

These tests are not mandated by Visa, however they are mandated by some acquirers or incorporated into their acquirer test packs. This is a shorter set of tests than MasterCard Environment of Use, and Visa neither reviews the results nor issues any certificate. The 42 tests are estimated to add under 3 days to the normal acquirer testing process.

5.2.1 Test tools and scripts

Current end to end subscribers have been upgraded and new packs cost €900. They are available through chipven@visa.com.

5.2.2 Responsibility

It is the responsibility of the retailer [for EPoS systems] and the terminal placer [for standalone terminals] to obtain this approval (if required). However, the vendor or system integrator is expected to play a significant role.

5.3 American Express Device Testing

American Express mandates a set of offline device tests post EMVCo level 2. Tests are executed by the vendor, with approval by American Express. These tests are fully documented and American Express will supply documentation, test scripts and test cards, if the vendor does not have access to the ICC Solutions test tool.

Acquirers will not allow implementation of a chip card system without this certification. It is the responsibility of the retailer [for EPoS systems] and the terminal placer [for standalone terminals] to obtain this certification. However, the vendor or system integrator is expected to play a significant role.

Tests can normally be completed within 1 to 2 days. Vendors are recommended to give two weeks notice, particularly if test cards are required. American Express' review of the test results would normally be completed within 1 week, but vendors should allow two weeks. AmEx issues a letter of certification following successful completion.

Following any significant system changes, American Express will ascertain whether all or part of the AmEx offline device tests must be repeated along with other acquirer testing.

5.4 Other scheme requirements

5.4.1 Switch

Switch has no requirements other than those described for MasterCard.

5.4.2 JCB

JCB provides test tools (cards and software) directly to the terminal manufacturer/software vendor for a self-assessment test of JCB chip card acceptance. This test can normally be completed in 3-4 days. The test report is then sent to JCB for validation.

6 Phase 4

6.1 Acquirer Testing

Acquirer acceptance testing (AAT) is the final stage of the end-to-end certification process. It is conducted by acquirers to ensure that messages are passed end-to-end correctly and that scheme product rules are followed. AAT involves acquirers performing a series of tests to confirm that authorisation, clearing and settlement records all contain the appropriate data for authorisation, interchange and settlement. AAT commences after the retailer (and their suppliers have completed their AAT development and should not be viewed as a replacement to the internal testing that is undertaken during the development phase.

This testing can be undertaken as soon as the retailer integration testing has been completed and is not reliant on the certifications described above. For example, acquirer testing can take place using a PINpad that has not yet received Visa certification, however if changes are made to the system after acquirer testing, these tests must be repeated.

6.1.1 Test cards and scripts

Acquirers will normally provide, on loan, one set of test cards and scripts for testing.

6.1.2 Responsibility

It is the responsibility of the retailer to obtain approval of this interface from each of its acquirers. Acquirers will allow vendors to pre-test (using test hosts) prior to formal testing by the retailer.

6.1.3 Impact

Acquirers will not allow devices that have not achieved ‘sign off’ to connect to their systems to process transaction.

6.1.4 Timescales

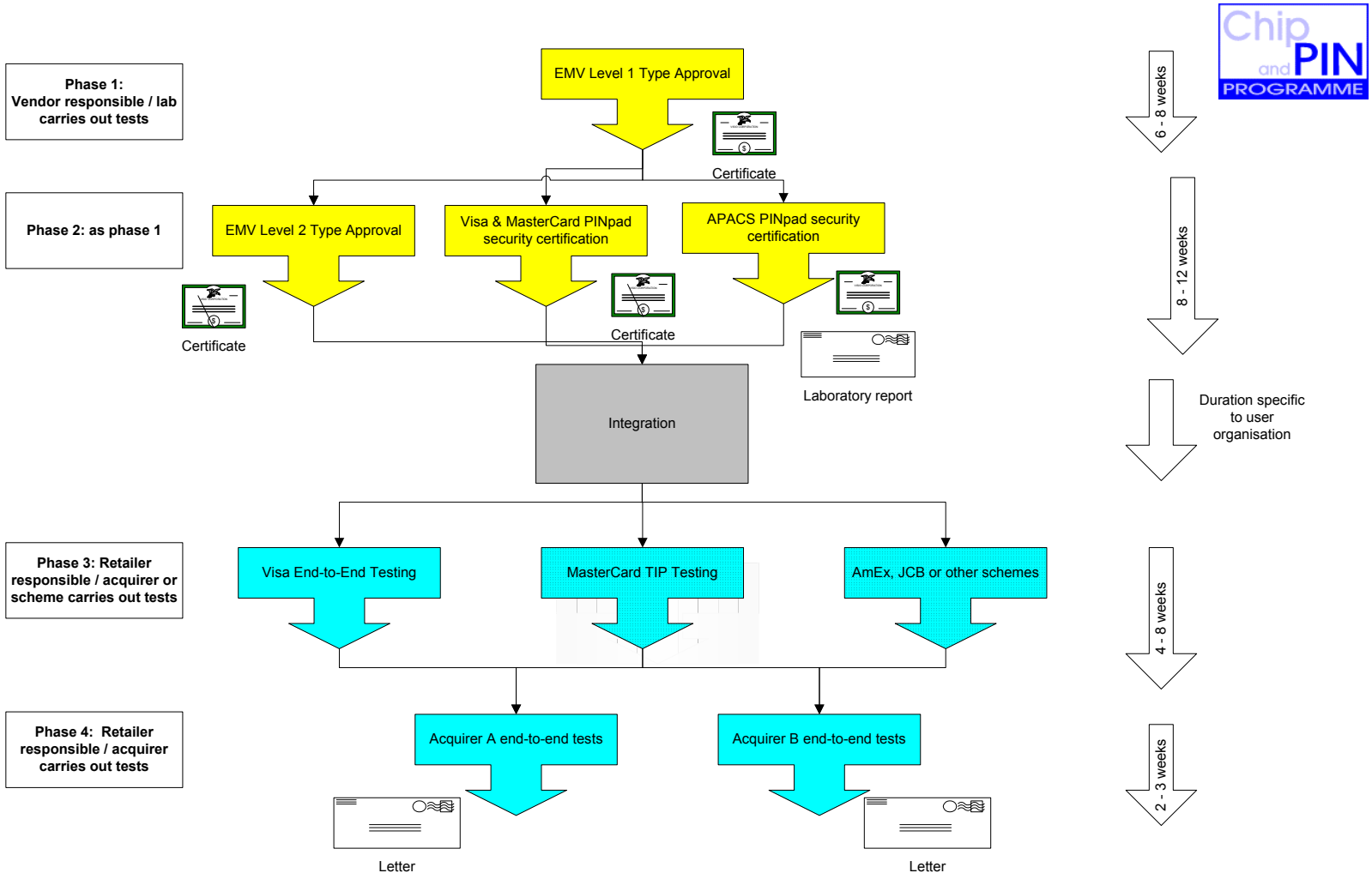
The lead-time for booking testing slots will vary by acquirer; retailers should allow not less than four weeks and probably longer during the second half of 2004. The elapsed time for each acquirer is approximately 2 weeks.

7 Timelines

The following table lists each stage in the process and shows the minimum time possible for each stage. In many cases the time required will be longer. The timescales mentioned below do not include the time required for paperwork, e.g. registration or issuance of certificates.

Most suppliers underestimate the time required for all stages of this process. The timescales quoted in Section 3 assume that the vendor has already been through a series of development and debugging cycles that may or may not have involved input from the EMV testing bureaux. This effort before reaching a point where formal certification is sought can take a number of elapsed months and could be 6 months plus depending on the in-house EMV expertise.

Figure 1 below summarises the likely timetable for the certification processes described; the integration of the software with the retailer's own systems takes place between phases 2 and 3, and the timescale for this is entirely dependent on the retailer and its vendor. The timescales shown on the right-hand side of the diagram should be regarded as "best case" and do not incorporate any contingency for re-testing, nor any allowance for delays at periods of peak demand such as are likely to occur during 2004.


Phase 1:
Vendor responsible / lab carries out tests
EMV Level 1 Type Approval
Certificate
6 - 8 weeks
Phase 2: as phase 1
EMV Level 2 Type Approval
Visa & MasterCard PINpad security certification
APACS PINpad security certification
Certificate
Certificate
Laboratory report
8 - 12 weeks
Integration
Duration specific to user organisation
Phase 3: Retailer responsible / acquirer or scheme carries out tests
Visa End-to-End Testing
MasterCard TIP Testing
AmEx, JCB or other schemes
4 - 8 weeks
Phase 4: Retailer responsible / acquirer carries out tests
Acquirer A end-to-end tests
Acquirer B end-to-end tests
2 - 3 weeks
Letter
Letter