PIN Mailer Security Guide

21 June 2022
Bill Reding
bill.reding@ukfinance.org.uk

1 Background

UK Finance originally operated a scheme for assuring an appropriate level of security for PIN mailers sent to UK cardholders. The scheme has now been scaled back to maintenance of a list of approved products and services, with evaluation and management of the process being devolved to approved laboratories.

2 The requirements

PIN mailers are required to be tamper evident.

The mailer contains tamper resistant and/or tamper evident features that should be effective against a range of unskilled attacks. Specifically, it should not be possible to circumvent the security features using equipment that is either readily available in the home or that is publicly available at minimal cost (e.g. <£100). Furthermore, some skill and practice should be required; taking an untrained individual up to 20 minutes to develop the necessary skills to perfect an attack technique. The attacker may be a creative individual or a small organisation with some special knowledge.

Products are the base stationery or element on which the PIN is applied. For testing, the supplier must apply test PINs to a set of samples (as agreed with the laboratory) and submit them to the laboratory. They are assessed on a one-off basis against a range of tests that show that they are robust against all relevant attacks; they must fully pass all tests. The devices used to apply test PINs to the product for testing can be chosen by the supplier. Each product must have a distinct product name. If it is intended for a specific type of printing process (such as labelling, impact, surface laser, surface inkjet), then that must be specified. Product suppliers must confirm their continued requirement for approval annually.

Print services are assessed based on the security of mailers when test PINs are applied to an approved product using production equipment. Approvals are associated with the production equipment used (the specific printer device and other devices if needed, such as labellers), and the product used. Print service providers must arrange for their approval to be renewed annually. A laboratory evaluation is required unless no printing is done within the year. After 5 years of non-use, re-assessment may be demanded. A grading scheme is used to qualify print services approvals. Approval will not be given if a sample fails to meet the most basic security

requirements, such as the PIN being clearly visible when viewed with low-angle daylight. This assessment is done by the laboratory. There is no appeal to UK Finance, but the laboratory may operate its own appeals procedure.

UK Finance retains the right to review and modify the grading scheme and other aspects of the scheme.

3 Laboratories

Laboratories are approved by UK Finance. ISO/IEC 17025 accreditation is not essential in order to achieve approval. However, to gain approval, the laboratory will be expected to demonstrate that it has in place broadly equivalent procedures, that it can handle requests methodically, prepare suitable evaluation reports, keep audit trails and maintain samples in good condition. UK Finance reserves the right to check that this remains the case by visiting laboratories, accessing evaluation reports and samples, and discussing evaluations with laboratories, with the aim of ensuring that quality and equivalence are maintained across all approved laboratories. UK Finance may withdraw its approval of a laboratory if it is dissatisfied with the results of such checks.

There is currently one laboratory that is approved for evaluation of PIN mailers:

Smithers
Olympus House, Cleeve Road, Leatherhead, Surrey KT22 7SA, UK
Contact person: Dave Stone, Senior Consultant, dstone@smithers.com

Laboratories may obtain from UK Finance the Standard developed under APACS and UK Cards that defined the tests to be performed (previously known as Standard 72), and may develop the test descriptions to allow for changing threats and new technologies. The latest version of such documents, including details of the grading scheme, will not be publicly available, but must be made available to UK Finance and must be freely shared between laboratories if more than one laboratory is approved. Note that references to level 4 tests may still exist in documentation, but only levels 1 to 3 are applicable to PIN mailer security evaluations.

4 Procedures

Suppliers should contact the laboratory in the first instance with requests for evaluations. Laboratories will manage the process by advising suppliers of how samples should be prepared and the number of samples needed. Laboratories will charge commercial rates for their services, which will cover the cost of managing the process.

A list of approvals will be maintained by UK Finance. The latest list at any time will be available to anyone on request to pinmailer@ukfinance.org.uk. It is also available on the UK Finance web site at https://www.ukfinance.org.uk/pin-mailer-security/. The list will include details of the supplier, but will not include personal contact details unless agreed by the supplier. An impersonal email address can be shown if preferred. Details of approvals and suppliers may be removed by UK Finance if approvals are not renewed or confirmed, or if UK Finance is advised of a vulnerability which a laboratory confirms would invalidate its approval.

UK Finance no longer issues product or printing certificates.

--o0o--

Company number: 10250295.
Registered address: UK Finance Limited, 1 Angel Court, London, EC2R 7HJ