National Cyber Security Centre
a part of GCHQ

Smart Metering CPA

CPA Risk Review of smart metering devices

Version 1.0

About this document

This document defines the process for performing Risk Review of smart metering devices and is used when approaching the expiry date or next risk review date of the CPA certificate for a smart metering device. Comments on the process should be sent to the NCSC.

This document is an annex to The Process for Performing CPA Foundation Grade Evaluations[1].

The process described in this document is the intended long-term version (the 'enduring version') of the Risk Review process.

Document history

The CPA Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time. Soft copy location: 1968710376-6250

Version	Date	Notes
1.0	17 February 2023	Draft for publication.

Contact NCSC

This document is authorised by: the Technical Director (Assurance), NCSC.

NCSC Contact Details
(For specific queries about the CPA Scheme)

Industry Assurance Team
NCSC, A2i,
Hubble Road,
Cheltenham,
Gloucestershire,
GL51 0EX,
UK.
Email: cpa@ncsc.gov.uk
Tel: +44 (0) 300 020 0964

[1] https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa

Contents

1 Overview

1.1 Introduction

1. This document describes the process for CPA Risk Review of smart metering Devices, to be carried out when their initial certificate expires, and at defined intervals (normally 6-yearly) thereafter. When CPA is used for smart metering Devices, this process replaces the 'Certificate expiry' subsection of section VI (Assurance maintenance) in the main body of [PPFGE].
2. The Risk Review process for smart metering Devices has been modified (from the original CPA Re-certification process) to take account of the expected lifetime of smart metering Devices, balanced with the need to provide information on the current risk posture of the deployed devices against the latest versions of the SCs. The Risk Review process is therefore based on both a review of the change history (and its resulting evidence chain) for the Device since its original certification, and a risk analysis against the latest version of the relevant SC.
3. By default the Risk Review process is not expected to require new evaluation activities by the Test Laboratory to evaluate DEV, VER or DEP mitigations. However, in some cases NCSC may request additional evaluation activities as a result of reviewing the Risk Review evidence (see section 2.1.5).
4. Risk Review is distinguished from Re-evaluation as follows:
    a. In Re-evaluation a version of a previously certified product is subject to a new set of formal evaluation activities (defined in an Assurance Plan) by a CPA Test Laboratory, to confirm that it meets each of the DEV, VER and DEP requirements in the relevant SC. This follows the CPA process defined in the main body of [PPFGE] and covers the full scope of the SC. Re-evaluation would typically be used to create a new starting point for Assurance Maintenance and a new Root version for a 'certification chain' (see section 2.1), or to create a new certificate against a later version of the Security Characteristic for that Device type. The output of a successful Re-evaluation is a new lifetime CPA certificate with a 6-year period until it is next reviewed under the Risk Review process.
    b. In Risk Review a number of versions of a previously certified product are subject to examination by a CPA Test Laboratory, covering (a) the change history and evidence chains for the product versions, and (b) their compliance with the latest version of the relevant SC for that device type, followed by a risk analysis by NCSC of any compliance gaps identified. These activities follow the process described in the relevant sections of this document, and do not follow the CPA evaluation process defined in the main body of [PPFGE]. Where full or risk-accepted compliance is found then the output of a Risk Review is a new (or updated) lifetime CPA certificate with a defined (normally 6-year) period until it is next reviewed under the Risk Review process. Where risks are determined to be unacceptable, then the certificate is not renewed or is withdrawn from one or more versions of the product.
5. When this Risk Review process has an outcome of 'Full compliance' or 'Risk-accepted' then it constitutes what is referred to in the Smart Energy Code as "renewal" of the CPA certificate.

1.2 The certification chain, Targets of Analysis, and evidence chains

6. Note: this section explains key concepts underlying the Risk Review process; readers should also familiarise themselves with the terminology in the Glossary (section 4) for clarification of terminology in this document.

1.2.1 Certification chains

7. The Risk Review process examines a number of product versions related to a single CPA certificate in a 'certification chain'. The certification chain includes all versions of the product that have been subject to CPA, either in a full CPA evaluation (leading to a CPA certificate) or under Assurance Maintenance (leading to a Security Impact Reviewed (SIR) or Security Impact Evaluated (SIE) outcome for the version that is being updated, as described below). Both of these types of version (SIR & SIE) are referred to in this process as 'CPA-certified'.
8. Note: a product version is defined in terms of a specific model identifier, a hardware version and a specific firmware version (i.e. the parameters used for entries on the CPL[2]).

[2] Even when a version has never been placed on the CPL, these parameters are still expected to be defined, as in Requirement 3 of the CPA Build Standard.

9. An example certification chain, including its basic CPA attributes, is shown in Figure 1. (The CPA attributes are explained in the text below.)

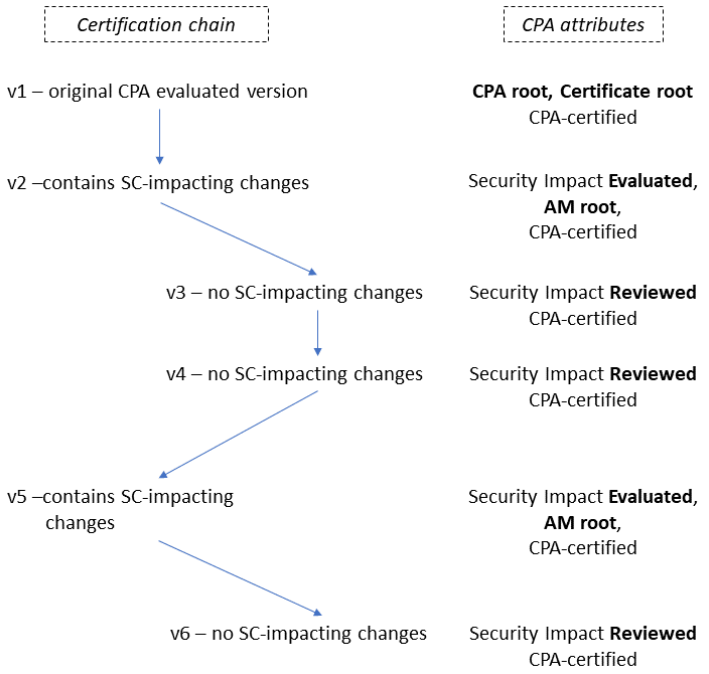


Figure 1: Certification chain example 1 – CPA attributes

10. The version at the start of the certification chain always has its own CPA certificate (i.e. it was subject to a full CPA evaluation), and is referred to as the 'CPA root' of the certification chain[3]. Each other version in the chain will have been examined under Assurance Maintenance at some point in time, and may or may not be currently covered by a CPA certificate (individual versions may have had their certification withdrawn, either as described in section 2.4 or due to the discovery of a vulnerability).

11. Where a product has been subject to a previous Risk Review, the certification chain considered in subsequent risk reviews still extends back to the CPA root (it does not start from the latest version considered in the previous Risk Review).

12. The certification chain also distinguishes which of two types of Assurance Maintenance apply to each version (below the CPA root version):

    a. Where the Security Impact Analysis (SIA) for a version indicated that there are no SC-impacting changes in the target version, and where this has been agreed with a CPA Test Laboratory, then no CPA evaluation activities are undertaken, there is no NCSC involvement in the process, and no Certification Letter is produced for the target version. This is referred to as "Security Impact Reviewed"

    b. Where the Security Impact Analysis (SIA) indicated that there *are* SC-impacting changes in the target version then an Assurance Maintenance Activity Plan (AMAP) will have been produced by the Test Laboratory, agreed with NCSC, and the relevant evaluation activities carried out. The Test Laboratory will then have produced an Assurance Maintenance Report (AMR), which is agreed with NCSC and, if successful, will have resulted in NCSC issuing a Certification Letter for the target version. This is referred to as "Security Impact Evaluated".

13. Versions with different types of AM are grouped together in the following way for the purposes of describing the evidence chain in the Security Analysis document (see section 2.1.2). An SIE version creates an 'AM root' version which is then grouped with all the subsequent SIR versions until the next SIE version (the next AM root) in the chain is reached. The principle here is that the earlier SIE version

[3] The CPA root in a certification chain never changes, even if the certificate for that version is subsequently withdrawn (in which case it will have been replaced by a certificate associated with a later version in the chain, as described in section 2.4). This is because the CPA Root represents the beginning of the chain of evaluation evidence, and contains evidence relevant to later versions certified under Assurance Maintenance (since an AMR only contains evidence for the relevant SC-impacting updates). If a new full evaluation takes place for a product version then that will create a new CPA root and a new certification chain under it.

represents a baseline state of the SC mitigations for the SIR versions that follow (because, by definition, the SIR versions do not make any SC-impacting changes).

14. The version in the chain that is identified in the current CPA certificate is called the “Certificate root”. This may be the same as the CPA root, but if the CPA root has had its certification withdrawn then the Certificate root will be a later SIE version. The choice of this version is also related to other attributes that are described in Figure 2 below (and in section 2.4).

15. The certification chain also includes other attributes, related to more operational aspects of the devices, which are relevant to the Risk Review process. These are referred to as ‘SEC attributes’, and are illustrated in Figure 2 (note that compared to Figure 1, the chain in Figure 2 has a version v1 – the CPA root – that is no longer certified). The SEC attributes are described in the text below Figure 2.

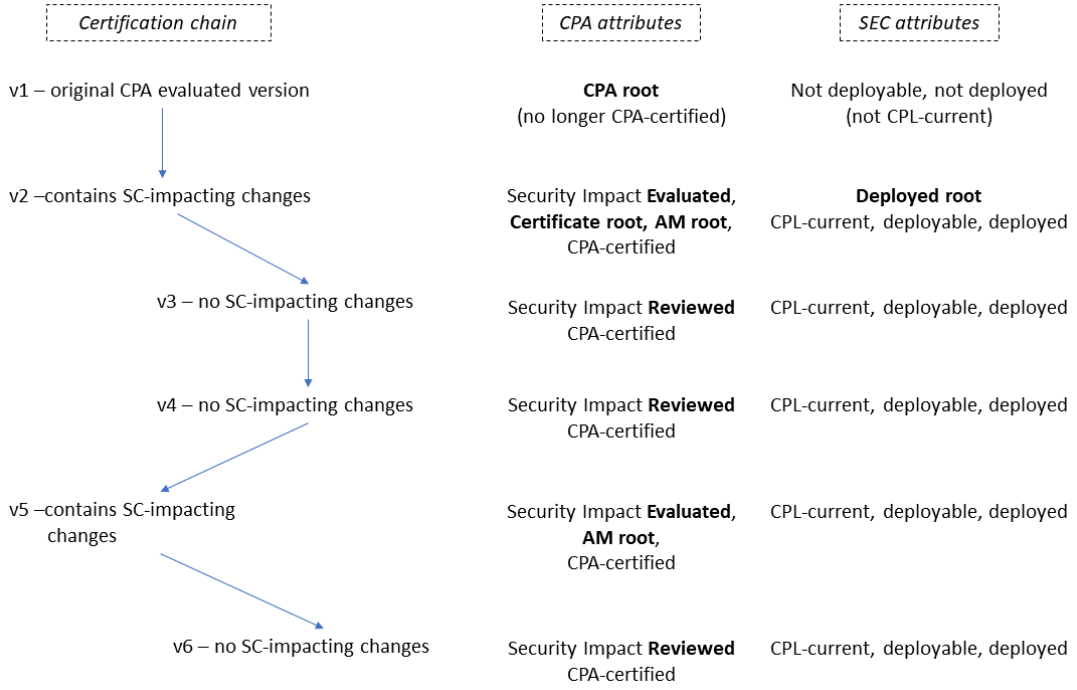


Figure 2: Certification chain example 2 – CPA & SEC attributes

16. Each version in the chain may be active (or not) on the Central Products List (CPL). A version that is included on the CPL with a status of ‘current’ is referred to in this document as ‘CPL-current’. Some CPL-current versions may not be covered by a CPA certificate: this situation will have arisen because they were originally certified, but have subsequently had their certification withdrawn and are kept on the CPL by SSC under a CPA Certificate Remedial Plan (as described in section 2.4).

17. The other attributes of each version are:

    a. Whether it currently has any deployed instances in the smart metering system[4]

    b. Whether it is currently allowed to be deployed into the smart metering system (referred to as “deployable” if it is allowed)[5].

[4] Information on the number of deployed instances of a version may be obtained by the Manufacturer for these purposes from SSC.

[5] In general a version may be: (a) deployed but not deployable (i.e. no further deployments are allowed), (b) deployable but not deployed (e.g. where the version is new and no instance has yet been deployed, or where all instances are currently in inventory but are still allowed to be deployed), or (c) both deployed and deployable.

18. Note: in general[6], any version that is deployable will also be CPL-current, but not all CPL-current versions will be deployable: this might be, for example, because a CPA certificate has been withdrawn or because a limited deployment volume has been reached and the version is being risk managed in a way that disallows adding to the deployed population, or because the manufacturer will soon stop supporting the version. Similarly, any version that is deployed will also be CPL-current, but not all CPL-current versions will be deployed.
19. Figure 2 shows these attributes for an example certification chain in which version v1 – the CPA root – is no longer certified. The Certificate root is then the earliest version in the certification chain that is CPA-certified and either deployed or deployable (or both) when the Risk Review commences (see section 2.1.1).
20. Each product version in the certification chain is a unique combination of hardware and firmware (a unique Device Model in the language of the CPL). The Manufacturer's description of the certification chain should therefore include both the hardware and firmware identifiers for that version. If a single evaluation report (ESR or AMR) covers multiple combinations of hardware and firmware (e.g. if it covers a single firmware that can be deployed on more than one hardware platform) then this can be represented in the chain by listing these combinations in a single node (in the terminology introduced below, the multiple hardware versions are part of the same Target of Analysis). However, each hardware-firmware combination that is CPL-current must be separately identified (i.e. visible) in the description of the certification chain (in the [SAT] Information Requirements). For example, adding some hypothetical hardware change details to the example in Figure 2, gives Figure 3 in which an additional hardware version is added as one of the non-SC-impacting changes in v4, and subsequent AM activities cover firmware running on all of the extended set of hardware platforms.

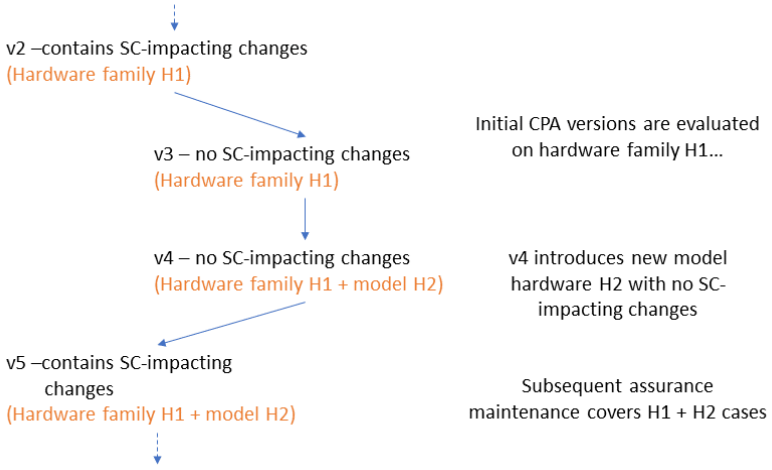


Figure 3: Certification chain example 2 extract – hardware details added

[6] The statements about CPL status and deployment in this section are generally expected to be true, but there may be exceptions in particular cases where a case-by-case risk management approach has been applied. Even where such cases exist, the focus of the CPA Risk Review will be on versions that are CPA-certified, CPL-current, and Deployed and/or Deployable at the start time of the Risk Review (as described later in this section). Outside of the Risk Review process, case-by-case exceptions in the CPL will also tend to have case-by-case consideration of CPA-related risk factors.

1.2.2 Targets of Analysis and evidence chains

21. The Risk Review process will update the certification status for all versions in the chain that, at the commencement of the Risk Review, are:

    - CPA-certified, and
    - CPL-current, and
    - deployed or deployable (or both)[7, 8].

    These versions are referred to as the 'Targets of Analysis' (ToA) for the Risk Review and for the example chain in Figure 2: v2, v3 and v4 would constitute one ToA; v5 and v6 constitute a second ToA; and v1 is not included in any ToA – this is illustrated in Figure 4.

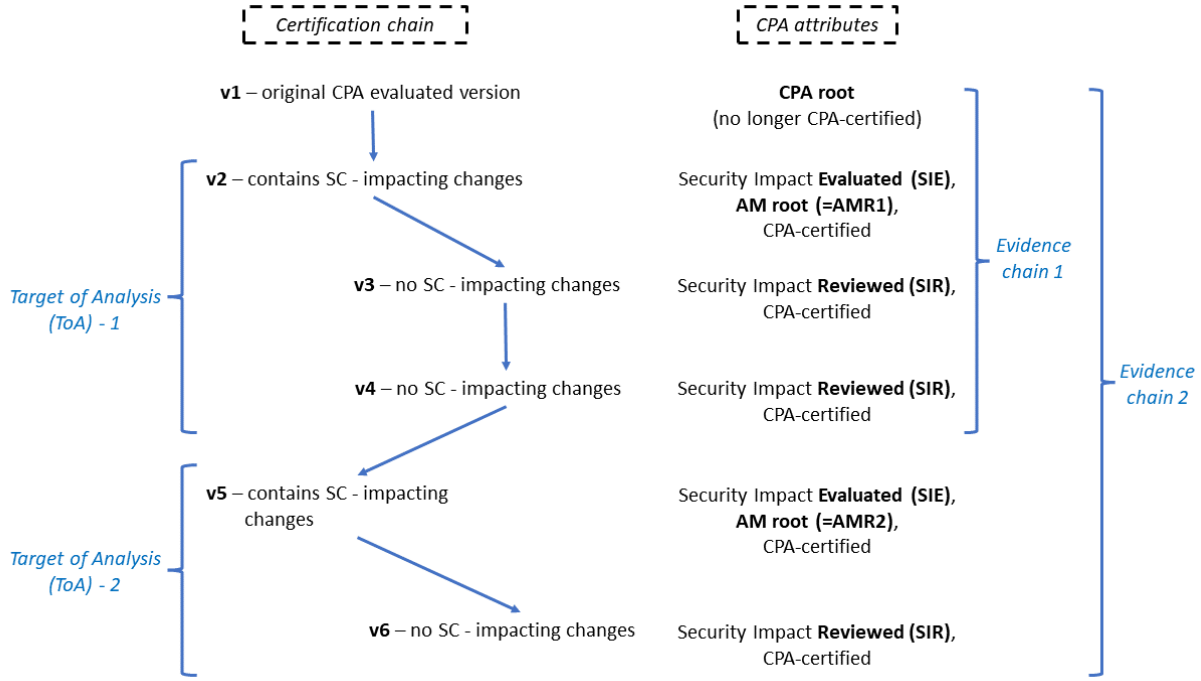


Figure 4: Targets of Analysis in an example certification chain

22. Note that each ToA requires a separate set of tables in the Security Analysis document, and that this set of tables covers the complete evidence chain for the relevant ToA (i.e. each evidence chain starts from the CPA root). Additional tables are needed to describe the evidence status of the CPA root (i.e. to capture its status relative to the latest version of the SC and Agreed Interpretations): the two cases for this are illustrated in Figure 5[9]. If the CPA root is immediately followed by an SIE version as in certification chain 1, then an additional instance of Table 1 is needed for the CPA root. If the CPA root is immediately followed by an SIR version as in certification chain 2, then the Security Analysis document requires additional instances of both Table 1 and Table 3 (i.e. to describe the non-SC-impacting changes in the directly connected SIR versions).

[7] This means that if a CPA-certified version has never been included in the CPL and will never be deployed, then it would not have an outcome from the Risk Review (i.e. it would not be issued with a new Certification Letter referencing the new lifetime certificate and its CPA certification would therefore expire with the original (non-lifetime) certificate). However, if this version has descendants in the certification chain, and some or all of these descendants are included in a ToA then the version would still form part of the evidence chain and be included in the Security Analysis document tables.

[8] There can be an exception case in a certification chain where an SIE version is not Deployed and not Deployable, but is the AM root for other SIR versions that are Deployed and/or Deployable. In this case the SIE version may need to be included in a ToA to provide a Certification Letter to which the SIR versions can be linked.

[9] Strictly speaking there is a third scenario in which the chain consists only of the CPA root: in this case, since there are no SIR versions dependent on the assurance in the CPA root, the situation would be the same as for certification chain 1 in Figure 5.

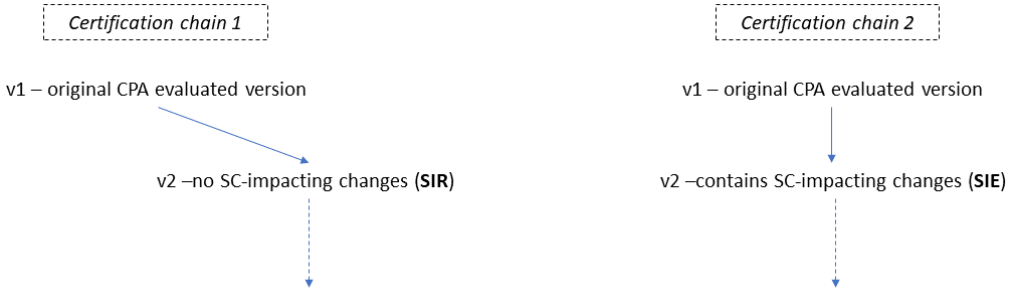


Figure 5: Differences in CPA Root security analysis tables required

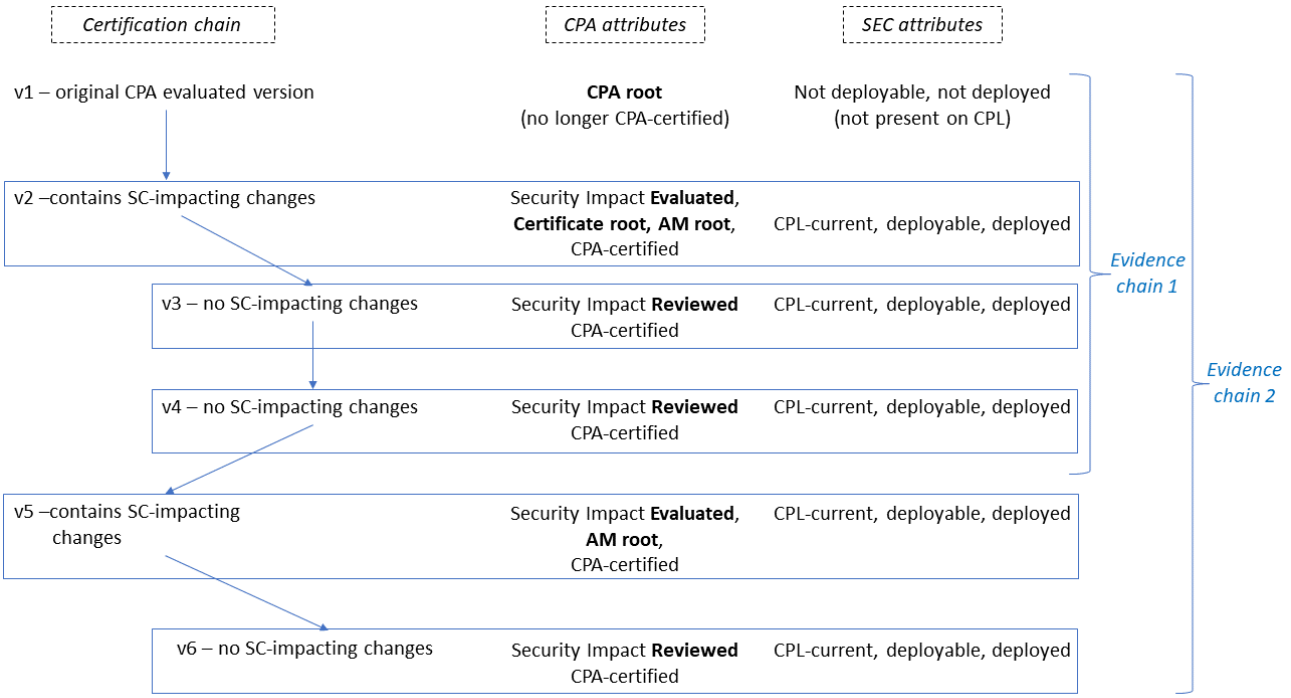
23. If a Manufacturer wishes to withdraw support for a version then they should contact SSC. If this dialogue with SSC results in a version no longer being deployed (or deployed under risk management) before the Risk Review starts, then this would mean that the version is not included in a Target of Analysis for the Risk Review[10].

24. Note that a ToA identifies versions for which the Risk Review will state an outcome (section 2.1.5). A version that is not included in a ToA will not have an outcome from the Risk Review, but the details of changes in that version will still be needed in the Security Analysis document if there are any later versions that are derived from it (because in this case the non-included version is still part of the evidence chain from the CPA Root to the latest version).

25. Appendix A includes a case study of a certification chain with more complex ToAs and evidence chains, and illustrates situations in which some product versions are not included in a ToA, and some AMRs are not included in evidence chains. It is noted that the initial evidence chains defined for a Risk Review might be expanded later to include other AMRs if there are findings (such as evidence gaps) that need to be further investigated.

1.2.3 Examples

26. This section considers some example variations of the basic certification chain and ToA scenario introduced in Figure 4. This is reproduced in a slightly different form (with a box drawn around each version that is part of a ToA) in Figure 6.



[10] If the Manufacturer withdraws support for the CPA root or the Certificate root then this will change these roots for the next Risk Review, and may necessitate various other actions as described for certification withdrawal in section 2.4.

Figure 6: ToAs and evidence chains for an example certification chain – case 1

27. If versions v2-v4 from this certification chain become no longer certified, then the required evidence chain is illustrated in Figure 7.

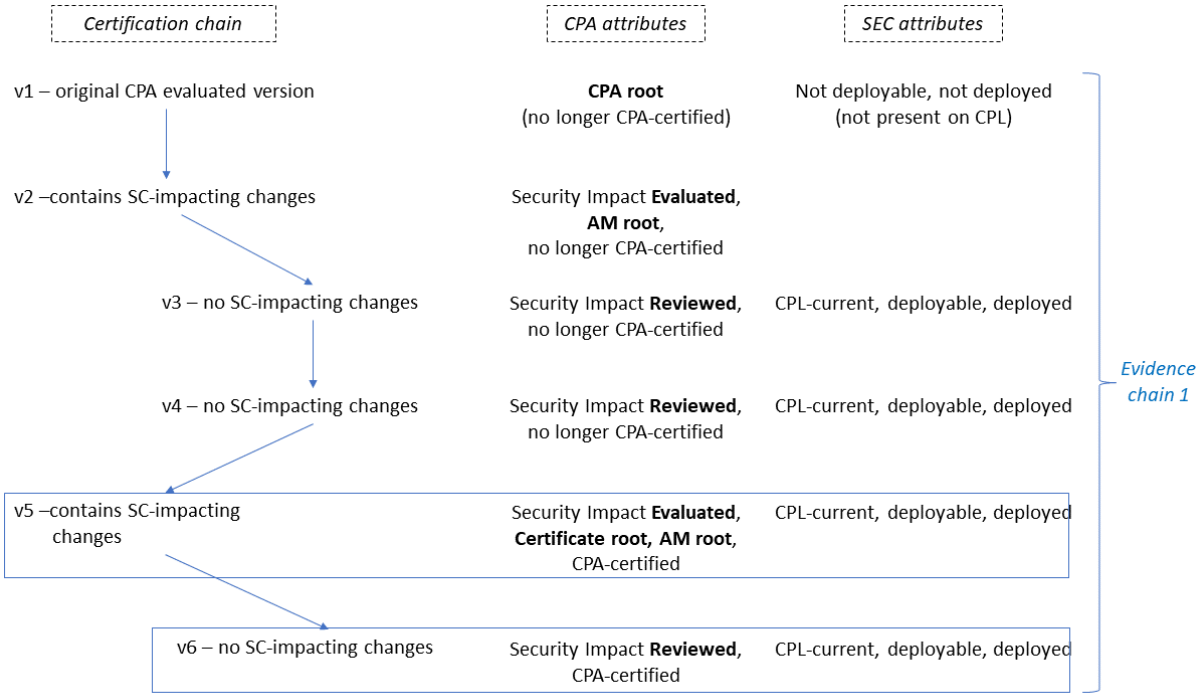


Figure 7: ToAs and evidence chains for an example certification chain – case 2

28. If v3 were to be removed from the CPL, which means that it no longer meets the criteria for update in the Risk Review, then the evidence chain becomes as shown in Figure 8. In this case, compared to Figure 4, v3 is not part of ToA 1 (so it will not have an outcome[11]), but is still part of evidence chain 1 (so its change details must be included in the tables in the Security Analysis document).

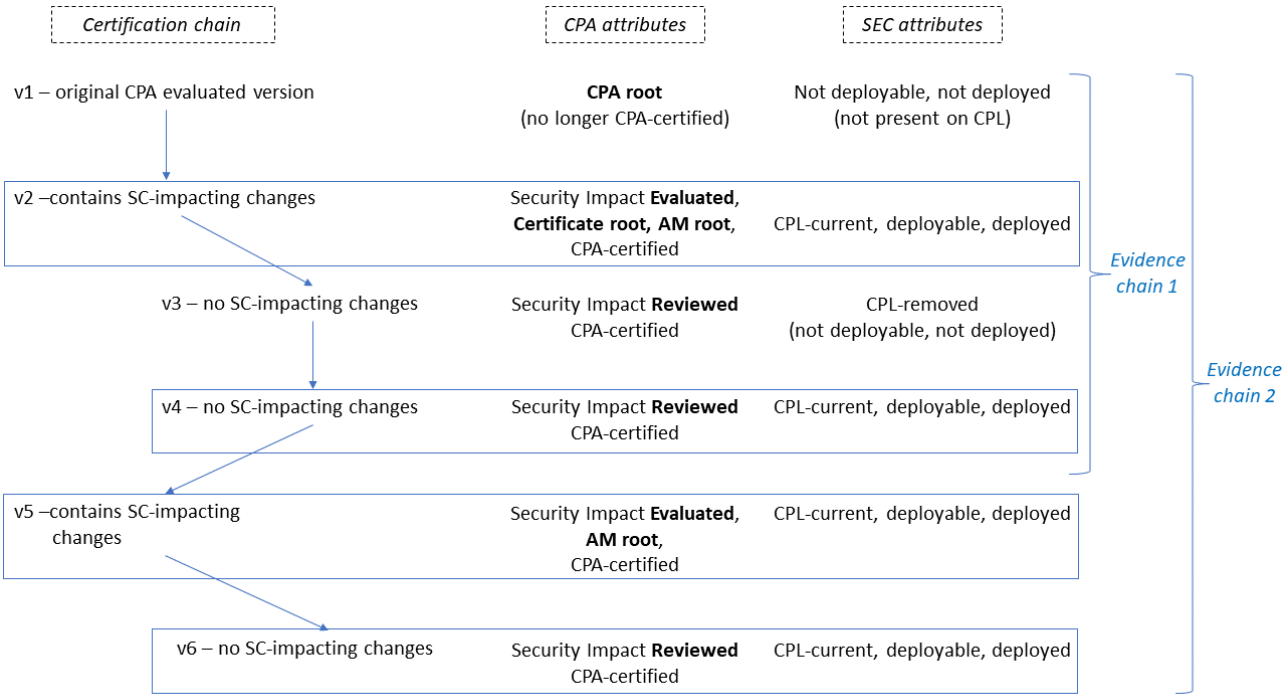


Figure 8: ToAs and evidence chains for an example certification chain – case 3

29. The examples in this section serve as an introduction to certification chains, to enable a general understanding of the Risk Review process steps. A larger example, with more complex situations, is included in Appendix A, and this may be of additional help when applying the process to real products.

[11] In CPA terms, because v3 is an SIR version, it will remain CPA-certified as long as its AM root (v2 in the examples) is CPA-certified.

2 Process description

2.1 Risk determination process

30. The initial Risk Review process stages, up to the determination of the risk analysis outcome by NCSC, are described in this section. The next part of the process is then described separately for each of the three possible outcomes in sections 2.2 – 2.4 below.

31. Figure 9 below illustrates the process for determination of the risk analysis outcome.

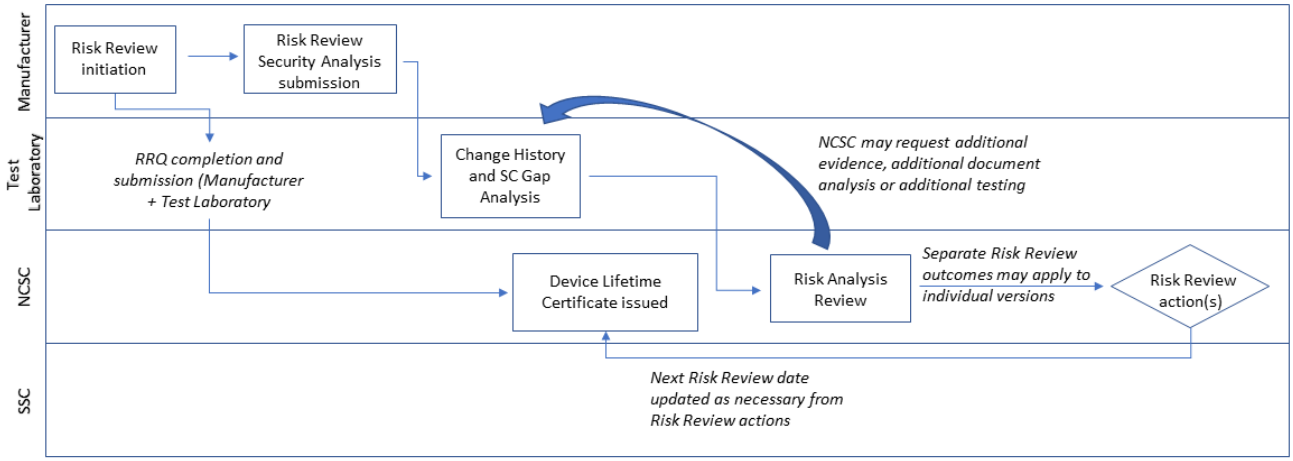


Figure 9: Risk Review – Determination process stages

32. The subsections below describe each of the stages in Figure 9 in more detail.

2.1.1 Initiation by Manufacturer

Inputs: Current CPA certificate approaching expiry/next risk review date

Scope: The Manufacturer initiates the Risk Review process by submitting a Risk Review Questionnaire (RRQ) through a Test Laboratory and starting to prepare the Risk Review Security Analysis document

Actors: Manufacturer, Test Laboratory, NCSC

Outputs: RRQ

33. The key dates for formal initiation of the Risk Review by the Manufacturer are shown in Figure 10

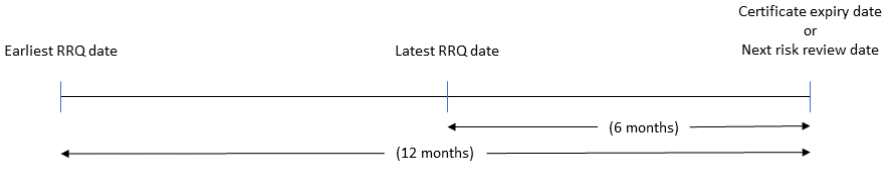


Figure 10: Risk Review –timing for initiation

34. The Manufacturer is responsible for initiating the Risk Review process, and may make the formal initiation a maximum of 12 months before the expiry/next risk review date of the current certificate for the relevant product. The Risk Review must be formally initiated at least 6 months before the expiry/next risk review date of the current certificate, and must be completed by the date given by NCSC in response to the RRQ (when converting a non-lifetime certificate to a lifetime certificate), or by the next risk review date (when renewing an existing lifetime certificate). The Manufacturer engages a Test Laboratory for the Risk Review and the Test Laboratory will then complete the RRQ in consultation with the Manufacturer and submit it to NCSC. For the purposes of meeting the required process dates, the relevant *formal* initiation action is the submission of the completed RRQ by a Test Laboratory to NCSC. If the current product certificate is not a lifetime certificate, then NCSC will respond to the RRQ by

issuing a new lifetime certificate for the product 1 month before expiry of the current certificate (see section 2.1.4). If the current product certificate is already a lifetime certificate then no action is required from NCSC since the required date for completion of the Risk Review was already defined in the previous Risk Review.

35. Once the Risk Review has been completed, the next Risk Review date (i.e. the date by which the next Risk Review must be *completed*) will normally be 6 years from the date of expiry of the original certificate (or from the risk review date set in the previous Risk Review, if this is not the first Risk Review)[12,13]. This applies even if the Risk Review process completes before that expiry/next risk review date (so in this case the period before the next risk review will be slightly longer than 6 years).
36. A separate Risk Review process must be initiated for each certification chain.
37. During this stage, a project is also initiated by the Manufacturer with a Test Laboratory to perform the Change History and SC Gap Analysis (this enables planning and scheduling to ensure that the Risk Review can be completed within the available timeframe).

2.1.2 Risk Review Security Analysis submission

Inputs: Product change history and evidence chains

Scope: The manufacturer completes their Security Analysis document, using the Security Analysis Template, and submits it to the Test Laboratory.

Actors: Manufacturer

Outputs: Completed Security Analysis document

38. The Manufacturer prepares their Security Analysis document, using the Security Analysis Template [SAT], and submits it to a Test Laboratory to enable the laboratory to perform the Change History and SC Gap Analysis. As part of preparing the Security Analysis document, the Manufacturer needs to:
    a. Describe the certification chain, identifying all the versions in the chain and their CPA attributes, and identifying each of the Targets of Analysis for the Risk Review
    b. Identify the version of the SC that the evaluation and each Assurance Maintenance process was carried out against
    c. Identify all changes to the device since the CPA root version, and the versions in which the changes are present
    d. identify which changes are security impacting (and which mitigations they affect)
    e. For SC-impacting changes, summarise the evidence demonstrating compliance with the relevant SC mitigation.
39. Note: the certification chain, to be described in the Information Requirements section of the Security Analysis, includes any versions that are no longer CPA-certified (e.g. as a result of previous Risk Review outcomes or withdrawn Certificates) and includes all versions that have been evaluated irrespective of whether they are still Certified or not. This is to ensure that the sequence of CPA evidence from the CPA root is complete and visible. (See also the description of the certification chain in section 1.2 above.)
40. Note: SEC attributes are not required to be shown for the certification chain in the Security Analysis document, but they will need to be used by the Manufacturer when identifying the Targets of Analysis (which then identifies the number and scope of [SAT] tables that are needed in the Manufacturer's Security Analysis document).
41. The Security Analysis document for a certification chain must include a separate set of the change history tables in [SAT] for each sequence from the CPA root down to (but not including) an AM root (see the evidence chains and Targets of Analysis in Figure 4, and further examples of evidence chains in Figure 6, Figure 7 and Figure 8).
42. Further details on how to create the Security Analysis documents are included in [SAT].

[12] The next Risk Review date for an SIE or fully evaluated version will be stated in the Certification Letter for that version; the next Risk Review date for an SIR version is the date given in the Certification Letter for its nearest SIE parent version.

[13] See section 2.1.6 for explanation of why some versions may be given shorter periods until their next Risk Review.

43. Note: A Manufacturer may engage a Test Laboratory to help in completion of the Manufacturer information in the Security Analysis document. However, the responsibility for accuracy and completeness of this information remains with the Manufacturer.

44. The Manufacturer also needs to provide any further evidence and explanation required by the Test Laboratory as part of their Change History and SC Gap Analysis.

45. Assurance Maintenance is not included as part of a Risk Review, but it may be carried out separately in parallel with the Risk Review process. The target version of the Assurance Maintenance in this case shall not be included in the certification chain for Risk Review, but it must be generated from a version that is present in that certification chain[14] (see Figure 11). The version undergoing Assurance Maintenance will therefore not be included in the current Risk Review (even if the Assurance Maintenance process completes before the Risk Review process). However, relevant outcome information may be communicated between these separate tasks.

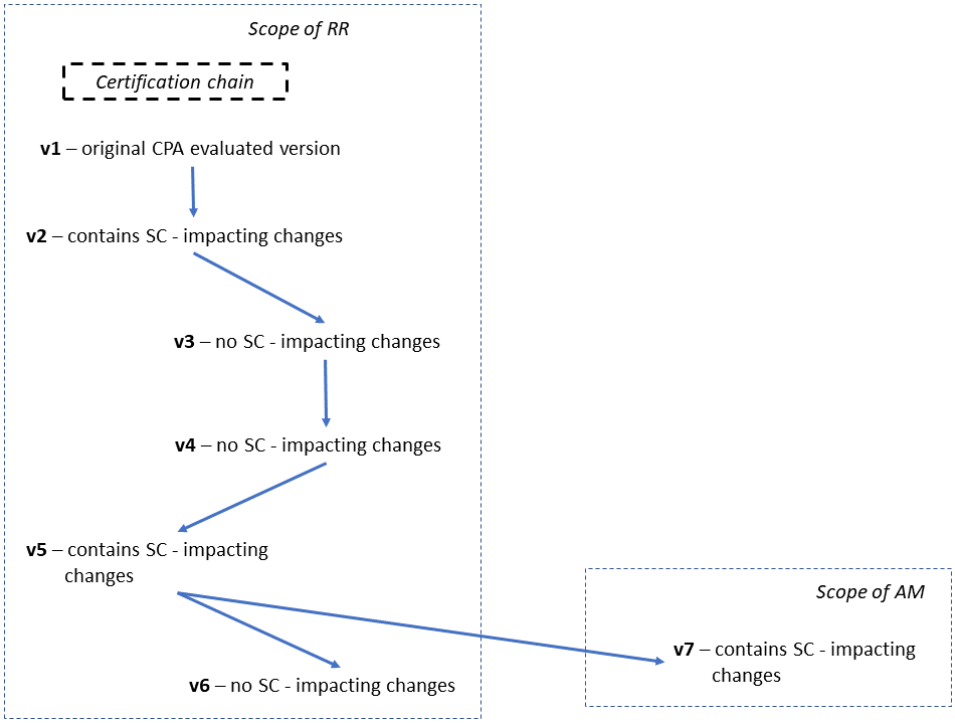


Figure 11: Risk Review and Assurance Maintenance in parallel

2.1.3 Change History and SC Gap Analysis

Inputs: Security Analysis document from Manufacturer
Certification letters for CPA root and each SIE version in the certification chain

Scope: The Test Laboratory examines the Security Analysis documents provided by the Manufacturer, and uses them to identify any cumulative risks arising from the change history (and the resulting evidence chain), to perform its own analysis of the current evidence of compliance with the latest version of the relevant SC, and reports on the conclusions to NCSC.

Actors: Test Laboratory

Outputs: Updated Security Analysis document to NCSC

46. The Test Laboratory must be provided with the Certification Letter for each relevant product version in the certification chain (i.e. the CPA root and each subsequent SIE version). This enables the laboratory

[14] In practice this means that the SIA for the Assurance Maintenance must address all changes between a version in the Risk Review certification chain, and the target version for Assurance Maintenance. The CPA-certified status of the parent version (v5 in the example in Figure 11) forms the basis for evaluating changes in the target version (v7 in the example in Figure 11), as is the usual situation for Assurance Maintenance.

to take into account any advisories or other recommendations that may be included in the Certification Letters.

47. The Test Laboratory must then use the summary of evidence in the Security Analysis documents to complete the fields in the Security Analysis document tables that are designated in [SAT] for the Test Laboratory (this is the only output from the laboratory – no other report is required). This may involve reference to content from the relevant ESR/AMRs, and/or additional discussions with the Manufacturer as necessary for the Test Laboratory to complete its analysis. The essence of the laboratory's analysis is:

    a. (Table 1) Identifying any gaps in the evidence available for each mitigation against the original SC mitigation and any relevant Agreed Interpretations published for that mitigation (as at the time the Risk Review commences).

    b. (Table 1) Identifying any gaps in that evidence relative to the version of each mitigation in the *latest* version of the relevant SC (as at the time the Risk Review commences).

    c. (Table 1) Identifying possible ways to gather additional evidence that would fill the identified gaps (for original and/or current mitigation, according to the findings above).

       Note 1: this is intended to support NCSC in deciding whether or not to ask for additional evidence to be generated. The laboratory may identify more than one way of gathering the evidence if appropriate, either because of different advantages and disadvantages, or because of different product versions involved.

       Note 2: an example might be performing additional fuzz testing where the fuzz testing expectations have been updated in the Agreed Interpretations or in a later version of the SC. The additional evidence discussion should also identify cases where the laboratory believes that it is not possible to gather additional evidence – e.g. because the hardware does not support the latest SC mitigations.

       Note 3: other examples of completion of the tables are provided by NCSC in the form of worked examples using the SAT.

    d. (Table 2) Identifying any gaps in the evidence available for each SC-impacting change against the affected mitigations in the original SC mitigation and any relevant Agreed Interpretations published for that mitigation (as at the time the Risk Review commences).

       Note: this is similar to item a above, but focussed on the change rather than the mitigation.

    e. (Table 2) Identifying any gaps in that evidence relative to the *latest* version of the relevant SC (as at the time the Risk Review commences).

    f. (Table 2) Identifying possible ways to gather additional evidence that would fill the identified gaps (for original and/or current SC, according to the findings above).

    g. (Table 3) Identifying any of the changes that were previously not SC-impacting (based on the original version of the SC for this certification chain) but that have become SC-impacting because of changes in later SC versions.

       Note: for clarity it is noted here that Table 3 lists all changes that are not SC-impacting, but the laboratory only comments on changes that are found (as part of the Change History and SC Gap Analysis) to be SC-impacting due to SC changes.

48. Since the versions covered by each table instance will be part of the same ToA, the laboratory conclusions will generally be the same for all the versions in a table. However, the laboratory may report different conclusions for different CPL-current versions, if necessary, provided a justification is given for the difference.

49. The Test Laboratory assessment must also check that:

    a. the information reported in the SA documents includes all versions of the relevant product that are associated on the CPL with the certificate identifier of the Certificate root

    b. all relevant versions have been included in a ToA (based on the version attributes in the particular certification chain)

    c. all relevant mitigation rows (for both the original and latest SC versions) have been included in each Table 1 instance

       Note: this check is simply to confirm that all expected rows are present (where an NCSC template is available for the relevant product and SC versions then it will be a check against the rows in the template).

    d. all relevant hardware and firmware combinations have been correctly included

Note: see the description of how to deal with multiple hardware and firmware versions in section 1.2 above.

e. any notifications to customers and / or the SSC of any material security vulnerabilities or incidents, including ongoing investigations or items awaiting investigation, have been identified (along with the versions that they affect).

50. Note that during, or as a result of, the NCSC Risk Analysis Review in the next stage, the Test Laboratory may be tasked with generating additional evidence (by document analysis or product testing). In general, NCSC will only ask for generation of additional evidence where the Risk Analysis Review indicates that the evidence could significantly affect the risk conclusion for the product version(s).

2.1.4 Device Lifetime Certificate issued

Inputs: Current Device (non-lifetime) CPA certificate
Completed RRQ from Test Laboratory

Scope: This stage only applies when an existing non-lifetime CPA certificate is expiring. In this case, provided that an RRQ has been received by NCSC to initiate the Risk Review process (as in section 2.1.1), NCSC issues a new lifetime certificate one month before the expiry date of the existing certificate and, on completion of the NCSC Risk Analysis Review, confirms the next Risk Review date to the manufacturer and the SSC.

Actors: NCSC

Outputs: Lifetime CPA certificate
Updated Certification Letter for Certificate root version
Required Risk Review completion date
Updated NCSC website entry

51. When the Risk Review is for a non-lifetime CPA certificate, then after receiving a completed RRQ, and 1 month before the expiry of the current certificate, NCSC will issue a new lifetime certificate for the device, along with a new Certification Letter for the Certificate root. A lifetime certificate does not have an expiry date, but the Certificate root and all other SIE versions in the certification chain (or at least all that are still CPA-certified) will at the end of the Risk Review process each have their own Certification Letter that states the next risk review date for the lifetime certificate[15]. In this case (i.e. replacing a non-lifetime certificate) the new Certification Letter for the Certificate root will state the required completion date for the current Risk Review as the 'next Risk Review Date' in the Certification Letter (this date will be replaced at the end of the Risk Review, as described in section 2.1.6). New Certification Letters for the other SIE versions in the certification chain will be issued at the end of the Risk Review.

52. Note: lifetime CPA certificates are not replaced with new CPA certificates in future. However, the risks of deploying versions in the certification chain that are CPL-current, Deployed, and/or Deployable will still be reviewed at least every 6 years by repeating this Risk Review process. The Certification Letters associated with the lifetime certificate therefore include a 'next risk review date' when the next Risk Review is due.

53. When the Risk Review is for an existing lifetime CPA certificate, then no further NCSC action is required at this stage since the required date for completion of the current Risk Review will already have been defined as part of the previous Risk Review.

54. The continuing validity of a lifetime certificate depends on successful completion of Risk Review steps by the 'next Risk Review date' stated in Certification Letters related to that certificate. If the steps are not completed by this time[16] then the certificate may be withdrawn.

[15] For an SIR version, the next Risk Review date will be that of its AM root (i.e. its nearest SIE ancestor in the certification chain)

[16] Any extension to the original time period for completion is granted solely at NCSC's discretion.

2.1.5 Risk Analysis Review

Inputs: Security Analysis document with Test Laboratory updates

Scope: NCSC perform a risk analysis based on the Security Analysis document with the evaluator content added, to reach a conclusion about the risks from any cumulative change effects and/or compliance evidence gaps with respect to the latest SC version.

Actors: NCSC

Outputs: Risk Review outcome (full compliance, risk-accepted, or certification withdrawal)
Certification chain limit decision

55. NCSC will use the Security Analysis document, with the information added by the Test Laboratory in the Change History and SC Gap Analysis, to develop a risk view for the continued deployment of the ToA versions in the certification chain, taking into account:
    a. the current threat landscape, particularly relating to the energy industry
    b. SSC details relating to reported security vulnerabilities and security incidents
    c. the nature of the changes between the different versions of the CPA SCs
    d. any other factors that NCSC deem appropriate to define the risks.
56. NCSC may engage with the Manufacturer as necessary to reach their risk conclusions.
57. The Risk Review outcome may be different for different ToAs, based on the evidence, the Test Laboratory conclusion, and the risk review factors.
58. The NCSC Risk Analysis Review will distinguish between absence of evidence for compliance, and evidence of non-compliance or potential vulnerabilities. It is also noted that lack of compliance of a product version with the current version of the SC does not automatically mean that certification will be withdrawn for that version.
59. During the NCSC Risk Analysis Review, further evidence may be requested from the Manufacturer, and in some cases this might require evidence generation by a Test Laboratory. However, this is expected to be an exceptional situation rather than the normal case. It would occur where the additional evidence could be used to avoid a certificate withdrawal outcome for one or more versions, and the Manufacturer would have the option to accept the certificate withdrawal rather than to undertake the additional work to provide the evidence.
60. NCSC will also define and review any limits that are to apply to the future extension of the certification chain. This will include limits on adding future versions to the current certification chain (and/or may update any previously set limits)[17]. This will take account of the number of versions in the chain since the last full CPA evaluation, and the outcomes of the current Risk Review (e.g. whether certification is being withdrawn from some versions). After the limit has been reached, then a full CPA evaluation (with reuse of previous results where applicable) will be required for the next version, and this will start a new certification chain.
61. Note: details of outputs from the Risk Analysis Review associated with each particular outcome are described in sections 2.2 – 2.4.

2.1.6 Risk Review action

Inputs: Risk Review outcome

Scope: NCSC and SSC collaborate on the actions required to update certification records and apply the Risk Review outcome to deployed Devices.

Actors: NCSC, SSC

Outputs: (see individual outcome sections below)

62. For each ToA in the certification chain, the Risk Review outcome will be one of the following:

[17] The application of a limit to *future* versions, rather than to the total number of versions in the chain, means that earlier versions cannot be removed from the chain to allow additional versions to be added,

a. Full compliance

b. Risk-accepted

c. Certification withdrawal.

63. The actions and outputs in each of these cases are described in sections 2.2 – 2.4.

64. All outcomes will include updated Certification Letters for the Certificate root and all other SIE versions in the certification chain (or at least all that are still CPA-certified)[18].

65. Different outcomes may apply to different ToAs in the certification chain, in which case more than one set of these actions and outputs will be applicable in the Risk Review process. Where outcomes other than full compliance have been determined for a version, this may require one or more additional Certification Letters to be created to describe advisories for the relevant versions (see section 2.3) and/or to indicate the exclusion of certain versions from the certification (see section 2.4). Note that the actions resulting from a Certification withdrawal outcome for one of the versions in the certification chain may affect the outputs for other versions (see section 2.4 for details).

66. If an Assurance Maintenance activity has been carried out in parallel with the Risk Review outcome (cf. section 2.1.2), then relevant outcome information may be communicated between these separate tasks.

67. Normally the next Risk Review date for Full compliance and Risk-accepted outcomes will be 6 years from the date of expiry of the current certificate (or from the Risk Review date set in the previous Risk Review, if this is not the first Risk Review). Depending on the findings of the Risk Review, the next Risk Review date might be less than 6 years. The following are examples of when a shorter period might be specified:

    a. Where the Risk-accepted outcome applies to one or more versions in the chain then the Risk-accepted versions may need an earlier than normal review e.g. if there is a vulnerability that needs to be monitored. If the same or similar risk factors are also relevant to other versions then these may also need earlier than normal review

    b. Where a chain has grown long and there are many versions or a long time period since the last Assurance Maintenance evaluation (i.e. a Security Impact Evaluated version) and/or evaluation of the CPA root then some or all versions in the chain may need an earlier than normal review.

68. In general, CPL entries for all versions in the certification chain that were CPL-current and either deployed or deployable (or both) at the commencement of the Risk Review will be updated by SSC based on the outcome that is applicable to that version. The updates will record the latest CPA certificate identifier and next risk review date. An exception to this situation may occur in the case of a certification withdrawal outcome: if SSC decide (as a result of their risk decision and the CPA Certificate Remedial Plan) not to remove the relevant version from the CPL then it will continue to refer to the previously associated certificate (which at that point, or shortly after, will have passed its expiry date).

[18] As noted in section 2.1.4, at the initial issuance of a new lifetime certificate, only the Certification Letter for the Certificate root is updated. This needs a further update at the end of Risk Review in order to specify the next Risk Review date.

2.2 Full compliance outcome

Outputs: Certification letter updates
CPL entry updates
Updated NCSC website entry

69. Figure 12 below illustrates the steps in processing a version with a full compliance outcome.

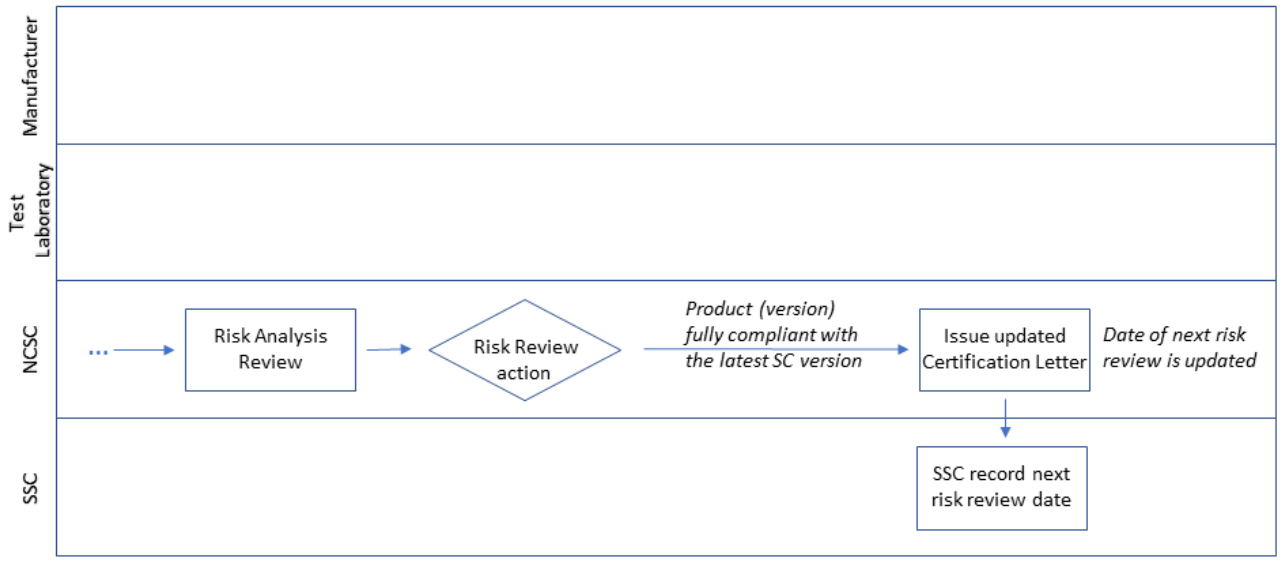


Figure 12: Risk Review steps for 'Full compliance' outcome

70. A full compliance outcome applies when there is sufficient evidence from the Risk Review process (either from the Security Analysis documents or from additional evaluation activities by the Test Laboratory) that a CPL-current version in the certification chain complies with all of the mitigations in the latest version of the relevant SC for the device type.

71. Note: a full compliance outcome from the Risk Review process is not the same as a 'Pass' result from a full CPA evaluation (as explained in section 1.1). A full CPA evaluation gives a higher level of assurance and starts a new certification chain.

72. For each ToA version in the certification chain (including the Certificate root) for which the NCSC Risk Analysis Review determines a full compliance outcome, NCSC will:

    a. Notify the manufacturer and SSC of the outcome

    b. Issue an updated Certification Letter, recording the next Risk Review date[19].

73. The next Risk Review date will usually be 6 years from the previous certificate expiry date or risk review date. However, if other versions in a certification chain are subject to Risk-accepted or Certification withdrawal outcomes (or have been in the past) then NCSC may decide on a shorter period.

74. SSC will record the next risk review dates for the relevant versions, and will request changes to the CPL to record the updated risk review date against entries that include the relevant CPA Certificate identifier.

[19] As noted in footnote 15: for an SIR version, the next Risk Review date will be that of its AM root (i.e. its nearest SIE ancestor in the certification chain).

2.3 Risk-accepted outcome

Outputs: Certification letter updates
NCSC risk conclusions report
CPL entry updates
Updated NCSC website entry
Remediation plan for deployed Devices (if applicable)

75. Figure 13 below illustrates the steps in processing a version with a risk-accepted outcome.

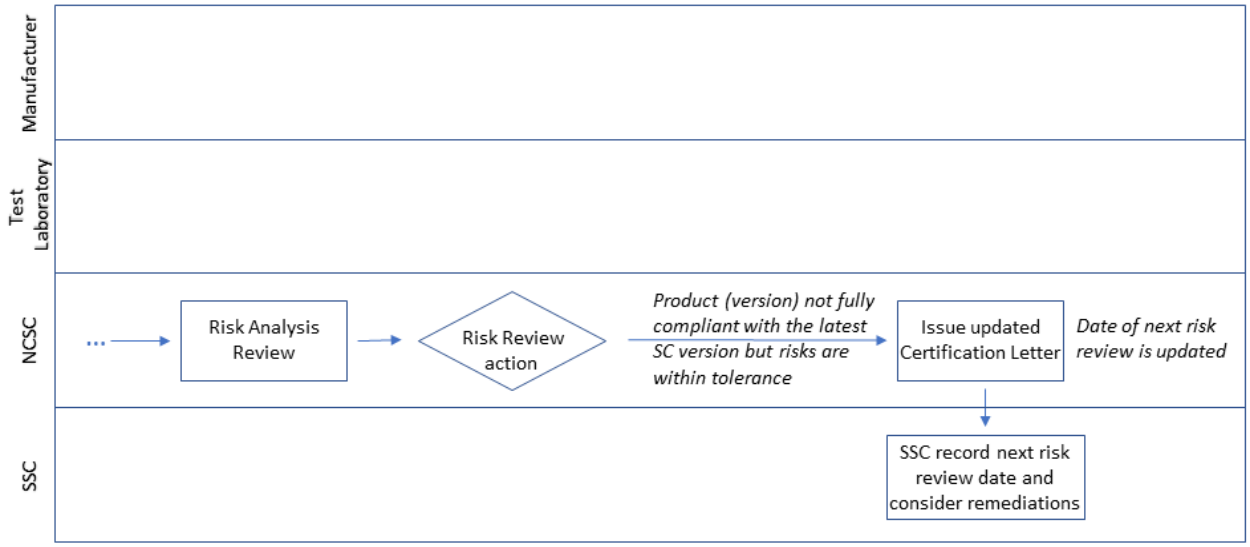


Figure 13: Risk Review steps for 'Risk-accepted' outcome

76. A risk-accepted outcome applies when there is not sufficient evidence from the Risk Review process to determine that a CPL-current version in the certification chain complies with all of the mitigations in the latest version of the relevant SC for the device type, but the NCSC Risk Analysis Review has concluded that the residual risk is within risk tolerance.

77. The lifetime certificate remains valid in this case, requiring only an update to the date of the next risk review in the Certification Letter (in general this will be the usual 6 year period from the previous expiry/next risk review date, unless the NCSC Risk Analysis Review determines that a shorter period should apply as part of the risk mitigation actions).

78. For each ToA version in the certification chain for which the NCSC Risk Analysis Review determines a risk-accepted outcome, NCSC will:

    a. Notify the manufacturer and SSC of the outcome

    b. Issue an updated Certification Letter to the manufacturer and the SSC, recording any advisories and the next risk review date

79. NCSC will report the outcomes and risk conclusions of the Risk Review to SSC, to inform and support SSC in its understanding of risks to the smart metering system. The report will identify the mitigations where full compliance has not been determined, and the nature of any specifically known non-compliances or potential vulnerabilities. The report may include advice and/or notes for SSC on the risks identified, including any significant assumptions made in the risk analysis, and potential mitigation actions by various parties. The report may also identify remedial actions that have been advised to the manufacturer as part of the outcome (including all advisories to be included in the Certification Letter). Although the NCSC report will not be routinely distributed to the Manufacturer, relevant findings will be notified to the Manufacturer in advisories (in the Certification Letter) and other feedback.

80. The updated Certification Letter will include the next Risk Review date (which may be less than 6 years in some cases, as noted above) and any requirements, recommendations and/or advice for the manufacturer as a result of the NCSC Risk Analysis Review. These requirements, recommendations or advice in the Certification Letter are referred to as 'advisories' which, if not actioned, may adversely affect the outcome of the next Risk Review.

2.4 Certification withdrawal outcome

Outputs: Lifetime certificate updates
Certification Letter updates
NCSC risk conclusions report
CPL entry updates
Updated NCSC website entry
CPA Certificate Remedial Plan

81. Figure 14 below illustrates the steps in processing a version with a certification withdrawal outcome.

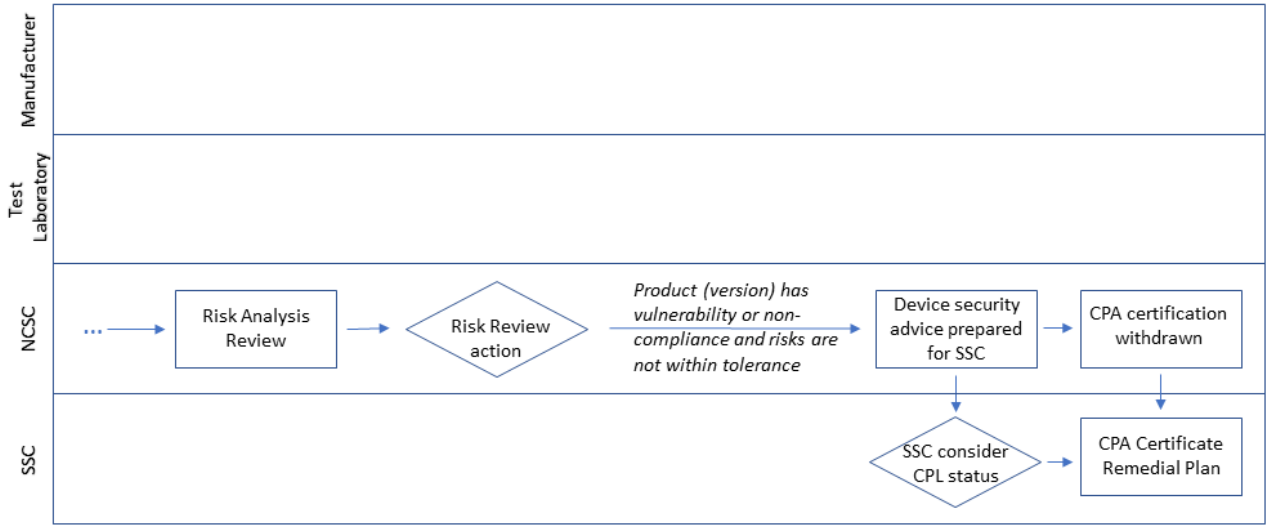


Figure 14: Risk Review steps for 'Certification withdrawal' outcome

82. A certification withdrawal outcome applies when one or more non-compliances and/or vulnerabilities has been identified for the version, and the NCSC Risk Analysis Review has concluded that the residual risk is not within risk tolerance.

83. As a result of this outcome, the certification information is updated so that the lifetime CPA certificate is withdrawn from this version of the product, and from any other versions in the same ToA (cf. Figure 4)[20]. If other versions in the certification chain achieved different outcomes then the lifetime certificate will still apply to them. This means that NCSC will issue an updated Certification Letter for the version, stating that certification has been withdrawn. Where certification has been withdrawn from the Certificate root version then other actions are taken as described below.

84. If certification is withdrawn from the Certificate root version then:

    a. the current certificate will itself be withdrawn

    b. certification will be withdrawn from any SIR versions from the Certificate root down to (but not including) the next SIE version in the chain

    c. a new lifetime certificate will be issued for the next SIE version in the certification chain that is CPA-certified and for which the current outcome is Full compliance or Risk-accepted – this version becomes the new Certificate root

    d. Certification Letters for all relevant versions in the certification chain will be updated to state the withdrawal of certification or to refer to the new certificate.

85. For each ToA version in the certification chain for which the NCSC Risk Analysis Review determines a certification withdrawal outcome (including SIR versions linked to an AM-root that has its certification withdrawn), NCSC will:

    a. Notify the manufacturer and SSC of the outcome

[20] In terms of Figure 6, this means that if certification is withdrawn from v2 then v3 and v4 would also have certification withdrawn, leaving the chain shown in Figure 7.

b. Issue Certification Letter(s) for the relevant version(s) stating that the certification is withdrawn

c. Update the certification entry on the NCSC website list of CPA certified products.

86. The decision to withdraw CPA certification is taken by NCSC alone. However, this outcome then requires SSC to decide what action to take to deal with deployed instances of the affected version(s).

87. NCSC will report the outcomes of the Risk Review to SSC, to inform and support SSC in its understanding of risks to the smart metering system. The report will identify the non-compliances and vulnerabilities that have led to certification being withdrawn, and any significant assumptions made in the risk analysis. The report may also identify potential mitigation actions by various parties, although for cases of certification withdrawal these are likely to be only partial mitigations of the risk that (by definition of the outcome) do not bring the level of risk within the tolerance margin. Such partial mitigations may nonetheless support the subsequent deliberations by SSC to require a CPA Certificate Remedial Plan to specify remediation/removal actions for deployed Devices.

88. After receiving notification of the certification withdrawal outcome, SSC will then use the risk advice from NCSC's report to decide whether or not to remove the relevant version(s) from the CPL and to require a CPA Certificate Remedial Plan (the required actions and processes for this stage are described in section 6 of the Smart Energy Code Appendix Z).

3 References

This document references the following resources.

Label	Title	Location	Notes
[PPFGE]	Process for Performing CPA Foundation Grade Evaluations	https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa	This document was written at the time of issue 2.5, but in general the latest version should be used
[SAT]	Security Analysis Template	On request from cpa@ncsc.gov.uk	This template defines the format and content for the Manufacturer's Security Analysis document for each certification chain.

4 Glossary

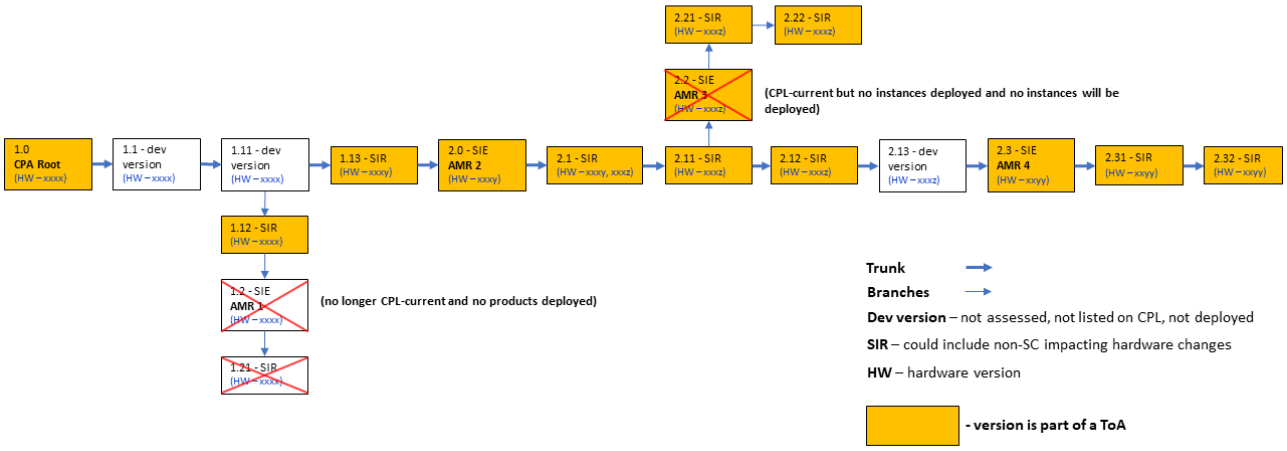
This document also uses the terms defined in the CPA methodology and the smart metering Security Characteristics, and in general these definitions are not repeated here.

Term	Definition
Advisories	Requirements, recommendations and/or advice (directed to the manufacturer) included in a Certification Letter as a result of the NCSC Risk Analysis Review.
AM root	A version of the product that contains SC-impacting changes that were successfully evaluated under Assurance Maintenance, and that has subsequent SIR versions in the certification chain that depend on it (and its AMR) for their CPA evidence. Note: an AM root is also an SIE version.
Central Products List (CPL)	The list of Devices that are approved to communicate with the DCC, which requires that the Device has met the requirements as set out in SEC Appendix Z – The CPL Requirements Document, including the requirement for the version to have a CPA certificate associated with it.
Certificate root	The version in the certification chain to which the current CPA certificate refers. Note: this will initially be the same as the CPA root, but will be different if the CPA root has had its certification withdrawn. The Certificate root will always be an SIE version.
Certification chain	The sequence of versions of a CPA certified product, beginning with a “CPA root” that is a version that underwent a successful full CPA evaluation (i.e. not Assurance Maintenance), resulting in its own CPA certificate (i.e. where the certificate specifically identifies that version as the one to which it applies). All subsequent versions in the chain have been certified under Assurance Maintenance.
CPA root	See ‘Certification chain’.
CPA-certified	A term including any version in a certification chain that has been the subject of an ESR (i.e. from a full CPA evaluation), or is an SIE or SIR version.
CPL-current	A version, in the product certification chain, that is included on the CPL and has a status (in column C of the CPL) of ‘current’. A version that has a status of ‘removed’ is referred to as being “not CPL-current” or “CPL-removed”.
Data Communications Company (DCC)	The entity that manages the smart metering data and communications infrastructure, as described in the Smart Energy Code.
Deployable	A version, in the certification chain, that is CPL-current, certified under CPA (either with its own certificate or via Assurance Maintenance), and that is allowed to be deployed into the smart metering system. Note: some versions may only be deployable under risk-managed conditions, such as when a device with old firmware is allowed to be deployed for a limited time in order to use the OTA mechanism to update its firmware to a later version.
Deployed	A version, in the certification chain, that has deployed instances in the smart metering system.
Evaluation Facility	The NCSC approved Test Laboratory that performs CPA evaluations and the Change History and SC Gap Analysis parts of the Risk Review process. Also referred to as “Test Laboratory”.
Lifetime Certificate	A CPA certificate that is valid for the lifetime of the product that it relates to, subject to 6-yearly risk reviews using the Risk Review process.

Term	Definition
Risk Review Questionnaire (RRQ)	The document issued by NCSC, that is completed by a Test Laboratory in consultation with the manufacturer, and then returned to NCSC to formally initiate a Risk Review.
Security Analysis Template (SAT)	The template that identifies the required content of Security Analysis documents to be produced by the Manufacturer and updated during the Risk Review process by the Test Laboratory and NCSC.
SC-impacting	The hardware, software, and/or firmware parts of a product that directly implement all or part of any mitigation in the SC against which the product is evaluated. Note1: directly implementing an SC mitigation means that the relevant part of the product (hardware, software, and/or firmware) is responsible for the specific decisions and behaviour that implement the mitigation. Note2: a new product version that contains SC-impacting changes requires an Assurance Maintenance evaluation (or else it may be submitted for a full re-evaluation) to maintain its certified status.
Security Impact Analysis (SIA)	The part of the CPA Assurance Maintenance process that uses a Security Impact Analysis document supplied by the manufacturer to a Test Laboratory, to enable the Test Laboratory to determine whether changes in a product version require formal CPA evaluation activities, and the involvement in NCSC in updating the CPA certificate. The determination is based on whether or not mitigations in the relevant SC for the device type are affected by the changes in that version.
Security Impact Evaluated (SIE)	A version in the certification chain that has been subject to Assurance Maintenance and found to have SC-impacting changes, leading to a CPA Assurance Maintenance Report and assertion that the changes do not impact the existing certification of the version.
Security Impact Reviewed (SIR)	A version in the certification chain that has been subject to Assurance Maintenance and found to have no SC-impacting changes, leading to the listing of the version on the CPL without a CPA Assurance Maintenance Report.
Security Sub-Committee (SSC)	The entity described in section G of the Smart Energy Code, with responsibilities including the maintenance and monitoring of assurance in various aspects of the smart metering system.
Test Laboratory	See “Evaluation Facility”
Target of Analysis (ToA)	The versions of the product (deployed or deployable) that have the same AM root. A ToA will comprise the AM root version and the subsequent SIR versions in the certification chain that depend on it (and its AMR) for their CPA evidence. Tables 1, 2 and 3 are to be completed for each ToA identified in the certification chain.

Appendix A Certification chain case study

89. Figure 15 illustrates a larger example of a certification chain, based on real-world examples of certification chains, and contains some more complex situations. These are discussed below, and examples given of dealing with these situations in a Risk Review.



ToA	Product versions	Evidence chain
1	1.0, 1.12, 1.13	ESR
2	2.0, 2.1, 2.11, 2.12	ESR, AMR 2
3	2.2, 2.21, 2.22	ESR, AMR 2, AMR 3
4	2.3, 2.31, 2.32	ESR, AMR 2, AMR 4

Figure 15: Certification chains - a more complex example

90. The chain in Figure 15 includes several different types of product version:
    - 'dev' versions: these are versions that exist in a manufacturer's version control system, but which have not been submitted for CPA evaluation (including Assurance Maintenance); they are not CPL-current, are not deployed, and are not deployable – these are not eligible for inclusion in a ToA
    - SIR and SIE versions with no instances deployed and that are no longer deployable: these are indicated by a cross in the box representing the version (e.g. v1.2) – these are generally only included in a ToA if they are needed as part of the evidence chain for later versions in a ToA
    - SIR and SIE versions that continue to be deployed and/or deployable – these are always included in a ToA.
91. The chain includes multiple branches, which have been evaluated under a number of separate Assurance Maintenance tasks, in particular:
    - there is an early branch creating v1.12 from v1.11, but this branch is no longer being actively extended with further versions, and in fact contains mainly versions that are no longer deployed (this branch represents a variant of the product that was not continued)
    - there is an additional branch creating v2.2 from v2.11, which might be further extended in future and currently has deployed and deployable instances
    - the main trunk development proceeds to v2.3, which is the latest SIE version.
92. The branching structure shows that such situations can be included in Risk Review, and Figure 15 identifies how the combination of the branches and SIE versions leads to the definition of four ToAs. The rationale for each ToA is as follows:
    a. ToA1 represents the early versions that are all covered by the original CPA certificate for the CPA root (v1.0). This covers different firmware branches on different hardware versions (xxxx & xxxy), where one of the hardware versions (xxxy) was introduced in an SIR version (v1.13) as a non-SC-impacting change
    b. ToA2 represents the subsequent trunk development up to SIR version 2.2. The later v2.13 is not included in a ToA because it is a dev version (not intended for deployment)
    c. ToA3 represents the variant branch for versions 'v2.2n' on hardware version xxxz (introduced as a non-SC-impacting change in v2.1). These are covered by AMR3, which addresses the SC-impacting changes from v2.0 that lead to v2.2

d. ToA4 represents the continuation of the trunk via the SC-impacting changes in v2.3 (this includes SC-impacting hardware changes in hardware version xxyy, which becomes the main trunk hardware version).

93. The following additional features of the chain are noted:

a. ToA1 includes versions from the trunk and from a discontinued branch (i.e. v1.12). This discontinued branch contrasts with the active branch that forms the separate ToA3. The relevant difference is the presence of CPL-current, deployed and deployable versions (v2.21 & v2.22) that depend on evidence established in the evaluation of an SIE version on the branch (v2.2)

b. AMR3 was produced for a version (v2.2) that is part of a ToA and has deployed and deployable successors, even though v2.2 itself is no longer deployed and is not intended to be further deployed. Even though there is no *intention* to deploy v2.2 in future, it remains CPL-current and *potentially* deployable. In addition, the Certification Letter for v2.2 covers the subsequent deployed and deployable v2.21 and v2.22 (since these are SIR versions, they do not have Certification Letters of their own). Both of these are reasons why v2.2 is included in a ToA.

c. AMR1 is not included in any evidence chain because it relates to a sequence in the chain consisting only of versions that are not CPL-current, not deployed, and not deployable. (Although this shows that AMR1 is not needed as an initial input, it is possible that investigation of Risk Review findings (such as evidence gaps) mean that it might be included later)

d. AMR4 is the only evidence document that covers potentially SC-impacting hardware changes (the other new hardware versions all appear in SIR versions).