

DCC Notice:

IKI Certificate Policy (IKI CP)

Publication of draft SEC Subsidiary Document

1.1 Purpose of Notice

DCC sets out below a brief narrative describing the evolution of the IKI CP from the consultation version to final draft SEC Subsidiary Document.

1.2 Background

DCC submitted the draft IKI CP SEC Subsidiary Document to the Secretary of State on 29 January 2015 pursuant to Sections L9.19 to L9.21 of the Smart Energy Code (SEC).

1.3 Document status

The IKI CP to which this narrative relates is draft final version of the SEC Subsidiary Document, which is subject to the Secretary of State's approval (the Secretary of State may request that further work is undertaken, may make further changes directly or may choose to approve the document in its current form). It was therefore published for information only.

1.4 Changes / points of interest

1.4.1 This narrative is focused on responding to the bigger issues raised or where changes to the draft SEC Subsidiary Document have been made.

1.4.2 Negative responses to question 1, stating a belief that the level of detail within the IKI CP is not adequate, included:

a) a risk that the information will be used by potential attackers. DCC notes the risk, which has been subject to risk review, and is not aware that there is a strong argument for not including such information in the IKI CP. DCC clarifies that more detailed information is contained within the IKI Certification Practice Statement (CPS), which is subject to approval by the SMKI PMA (this document is not published for reasons of security).

b) the use of IKI terminology is confusing by implying a standalone key infrastructure. It should therefore be named "SMKI Infrastructure Certificates". DCC notes the comment; however the documents are defined in the SEC and therefore no change has been made.

1.4.3 In response to question 2, two respondents commented that the language used is not precise enough to be audited and there were insufficient references to applicable standards. DCC does not agree that the language is imprecise or that additional standards need to be referenced. It was also suggested that the IKI CP does not align with other SMKI documents (e.g. SMKI RAPP). In response, DCC confirms that it updated the SMKI RAPP to

include IKI terminology prior to submission to the Secretary of State on 22 December 2014. DCC has also identified a couple of minor additions to the SMKI RAPP as a result of consultation responses received. DCC is also updating the SMKI Interface Design Specification and SMKI Code of Connection to include IKI terminology as necessary.

1.4.4 In addition to the consultation responses received, DCC received a response which was not specifically in relation to the consultation. It indicated that the relatively recent introduction of IKI and DCCKI terminology could be clearer. In particular, the response indicated that there is some confusion relating to the:

- a) credentials issued under the IKI/SMKI/DCCKI Certificate Authorities
- b) credentials not issued via a Certificate Authority (e.g. usernames and passwords to access the SMKI Repository)
- c) purposes for which each credential is to be used

1.4.5 In response, DCC has issued a clarification paper to TPMAG members, which has also been made available via the Service User SharePoint site.

1.5 Contact

If you would like to discuss this Notice, please contact Richard Sullivan at richard.sullivan@smartdcc.co.uk.