***Designated bodies for the conformity inspection of SSCD***

***Requirements for the designation procedure***

The Commission Decision 2000/709/EC lays the following general requirements for DBs:

If the DB is part of a (bigger) organisation also involved in other activities, the DB must be identifiable within that organisation and the different activities must be clearly distinguished. (Article 2)

The independence of the DB and its staff must be ensured. This includes that neither the DB nor its staff are engaged in any activities that may conflict with their independence of judgement and integrity in relation to their task, and that the DB is financially independent. (Article 3)

The DB and its staff must be able to determine the conformance with a high degree of professional integrity, reliability and sufficient technical competence. (Article 4)

The DB shall be transparent and non-discriminatory in its assessment. All interested parties must have access to the services of the body. (Article 5)

The DB must have at its disposal the necessary staff and facilities to enable it to perform properly and swiftly the technical and administrative work. (Article 6)

The personnel responsible for conformance assessment must have sound technical and vocational training in the field of electronic-signature technologies and related IT security aspects, and satisfactory knowledge of the requirements of the assessments out and adequate experience to carry out such assessments. (Article 7)

The impartiality of DB staff shall be guaranteed. Their remuneration shall neither depend on the number nor on the results of conformance assessments. (Article 8)

The DB must have arrangements to cover liabilities from its activities. (Article 9)

The DB must have adequate arrangements to ensure the confidentiality of the information obtained in carrying out its tasks. (Article 10)

In case that part of the conformance assessment is carried out by another party, the DB must take the full responsibility and must ensure and must be able to demonstrate that is party is competent. (Article 11)

Although the Directive doesn't directly suggest specific standards, these minimum criteria are covered by existing and internationally recognised standards, especially EN 45011 for bodies operating product certification systems (certification bodies) and ISO17025 or testing and calibration laboratories (evaluation facilities) with the exception of the requirements of:

Article 4: competence regarding the conformance assessment of SSCD according to annex III of the directive and

Article 7: knowledge in e-signatures techniques and legislation

which are dedicated requirements on the knowledge and competence in the field of the EU-Directive for electronic-signatures and IT security evaluation/certification. These dedicated requirements are contained in EN45011 and ISO17025 as general requirements on the “relevant” qualification and training of the staff. For instance in EN45011 it is defined that the certification body shall employ a sufficient number of personnel having the necessary education, training, technical knowledge and experience for performing certification functions relating to the type, range and volume of work performed, under a responsible senior executive.

Therefore, DB for conformance assessment of SSCD shall comply with requirements of the standard EN45011. Further guidance on how this standard should be applied is provided by «EA Guidelines on the Application of EN 45 011, European co-operation for Accreditation, June 1999». Compliance is usually proved through accreditation by a national accreditation organisation to the relevant standard (EN45011 or ISO17025) and within a dedicated scope. For conformance assessment of SSCD the scope should be: IT security evaluation and certification of IT products (here SSCD) as well as e-signature techniques.

The most common and internationally recognised standards used within the framework of security evaluation and certification are ITSEC and Common Criteria (CC) In the context of Common Criteria, Article 9 Committee has published CEN-CWA14168 and CEN-CWA14169 which define the Protection Profile for SSCDs where the SSCD represents a so called Target of Evaluation (TOE). Designated bodies are expected to be familiar with the concepts of the above publications, which are hot candidate for standardization, as well as with the guidelines defined in CEN-CWA14172-5.

In summary the candidate body and its personnel, in order to fulfil Article 4 and 7 requirements, should provide, for their accreditation, evidence that they possess:

Sufficient knowledge in formal evaluation processes (ITSEC /CC)

Sufficient knowledge in key-generation and key-usage-processes

Sufficient knowledge in electronic signatures legislation

*Designated bodies for the conformity inspection of Certification Service Providers (CSPs)*

*Requirements for the designation procedure*

*A candidate body for the conformity inspection of CSP must fulfil the minimum criteria for designated bodies specified in the Commission Decision of 6/11/2000). Apart from articles 4 and 7, this can be explicitly proved if the candidate body has an accreditation according to either:*

*a) EN45012 with scope Information Security Management Systems (like in BS7799),*

*b) ISO17025 with scope ITSEC/CC (Evaluation Body),*

*c) EN45011 with scope ITSEC/CC (Certification body).*

*The correspondence between Minimum Criteria and the respective standards is shown in the following table (Table 1).*

| *2000/709/EC* | | *ISO17025* | *EN45011* | *EN45012* |
|---|---|---|---|---|
| *1* | *The purpose of this Decision is to establish the criteria for Member States to determine whether a national body should be designated as responsible for the conformity assessments of secure signature-creation-devices.* | *not relevant (#)* | *1.1, 4.1.3 (#)* | *not relevant (#)* |
| *2* | *Where a designated body is part of an organisation involved in activities other than conformance assessment of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC it must be identifiable within that organisation. Different activities must be clearly distinguished.* | *4.1.4, 5.3* | *4.2d;e;l* | *2.1.2d;e;l* |

| | | | | |
|---|---|---|---|---|
| *3* | *The body and its staff must not engage in any activities that may conflict with their independence of judgement and integrity in relation to their task. In particular, the body must be independent of the parties involved. Therefore, the body, its executive officer and the staff responsible for carrying out the conformance assessment tasks must not be a designer, manufacturer, supplier or installer of secure signature-creation-devices, or a certification service provider issuing certificates to the public, nor the authorised representative of any of such parties.*<br><br>*In addition, they must be financially independent and not become directly involved in the design, construction, marketing or maintenance of secure signature-creation-devices, nor represent the parties engaged in these activities. This does not preclude the possibility of exchange of technical information between the manufacturer and the designated body.* | *4.1.5b* | *4.2n;o, 9.3* | *2.1.2n;o, 2.2.3* |
| *4* | *The body and its personnel must be able to determine the conformity of secure signature-creation-devices with the requirements laid down in Annex III to Directive 1999/93/EC with a high degree of professional integrity, reliability and sufficient technical competence.* | *(*)* | *4.2j (*)* | *2.1.2j (*)* |
| *5* | *The body shall be transparent in its conformity assessment practices and shall record all relevant information concerning these practices. All interested parties must have access to the services of the body. The procedures under which the body operates must be administered in a non-discriminatory manner.* | *4.4, 4.12* | *4.1.1, 4.1.2, 4.1.3, 4.8* | *2.1.1.1, 2.1.1.2, 2.1.1.3, 2.1.7* |

| | | | | |
|---|---|---|---|---|
| *6* | *The body must have at its disposal the necessary staff and facilities to enable it to perform properly and swiftly the technical and administrative work associated with the task for which it has been designated.* | *5.2, 5.5* | *5* | *2.2* |
| *7* | *The personnel responsible for conformity assessment must have:*<br>*sound technical and vocational training, particularly in the field of electronic signature technologies and the related IT security aspects,*<br>*satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate experience to carry out such assessments.* | *5.2(*)* | *5 (*)* | *2.2 (*)* |
| *8* | *The impartiality of staff shall be guaranteed. Their remuneration shall not depend on the number of conformity assessments carried out nor on the results of such conformity assessments.* | *4.1.5b* | *4.2m;n* | *2.1.2m;n* |
| *9* | *The body must have adequate arrangements to cover liabilities arising from its activities, for example, by obtaining appropriate insurance.* | *4.1.5h* | *4.2h* | *2.1.2h* |
| *10* | *The body must have adequate arrangements to ensure the confidentiality of the information obtained in carrying out its tasks under Directive 1999/93/EC or any provision of national law giving effect thereto, except vis-a-vis the competent authorities of the designating Member State.* | *4.1.5c* | *4.10* | *2.1.9* |
| *11* | *Where a designated body arranges for the carrying out of a part of the conformity assessments by another party, it must ensure and be able to demonstrate that this party is competent to perform the service in question. The designated body must take full responsibility for the work carried out under those arrangements. The final decision remains with the designated body.* | *4.5.1, 4.5.3* | *4.4* | *2.1.3* |

| | | | | |
|---|---|---|---|---|
| 12 | This Decision is addressed to the Member States. | (foreword) not relevant | (foreword) not relevant | (foreword) not relevant |

(#) only EN45011 is suitable for conformity assessments for products:

EN45012 is suitable for conformity assessments for quality management systems (2.1.1.3)

ISO17025 is suitable for tests and calibration (1.2)

(*) The following articles are not completely covered by existing standards:

article 4: specific competence regarding the conformity assessment of SSCD according to annex III of [EU-Dir-99/93]

article 7: specific knowledge in e-signatures techniques and legislation

*Table 1. Minimum Criteria / Relevant Standards*

*Additionally, as far as sufficient knowledge is concerned (article 4 and 7 of decision 2000/709/EC) the candidate body must especially possess specific knowledge about the following:*

*Organizational and procedural security measures*

*Usual proceedings for threat / risk analysis*

*Best practices of security management*

*Security audit of trustworthy systems (including network penetration tests)*

*Environmental requirements for evaluated security products (i.e. that evaluated products have such requirements which must be fulfilled by the user/CSP)*

*Constructional security measures*

*Electronic signatures legislation*

*CSP services and processes*

*The knowledge can be proved by submitting training certificates or proofs of participating in special workshops, former projects, etc. Some of the above points are considered covered if the candidate body has an accreditation according to a), b) or c). This is depicted in the following table (Table 2).*

| Candidate body has | | | | |
|---|---|---|---|---|
| Nothing | EN45012 scope ISMS | EN45011 scope ITSEC/CC | ISO17025 scope ITSEC/CC | |
| x | | | | Everything out of the minimum criteria |

| *Candidate body has* | | | | |
|---|---|---|---|---|
| *Nothing* | *EN45012 scope ISMS* | *EN45011 scope ITSEC/CC* | *ISO17025 scope ITSEC/CC* | |
| | *x* | | | *they must know about security audit of (trust worthy) systems (including network penetration tests)*<br>*they must have knowledge about environmental requirements for evaluated security products (they must simply know, that evaluated products have such requirements which must be fulfilled by the user/CSP)*<br>*they must know about constructional security measures*<br>*they must have knowledge in electronic signatures legislation*<br>*they must have knowledge in CSP services and processes* |
| | | *x* | | *they must know about organizational and procedural* |
| | | | *x* | |

| *Candidate body has* | | | | |
|---|---|---|---|---|
| *Nothing* | *EN45012 scope ISMS* | *EN45011 scope ITSEC/CC* | *ISO17025 scope ITSEC/CC* | |
| | | *x* | *x* | *security measures*<br>*they must have knowledge in usual proceedings for threat analysis*<br>*they must have knowledge in best practices of security management*<br>*they must know about constructional security measures*<br>*they must have knowledge in electronic signatures legislation*<br>*they must have knowledge in CSP services and processes* |
| | *x* | *x* | | *they must know about constructional security measures*<br>*they must have knowledge in electronic signatures legislation*<br>*they must have knowledge in CSP services and processes* |
| | *x* | | *x* | |
| | *x* | *x* | *x* | |

*Table 2. Alternatives for the designation of DBs for CSP*