



Leitfaden für die Datensicherheitsprüfung nach Artikel 8b Stromversorgungsverordnung

1. Zweck

Dieser Leitfaden informiert über die Datensicherheitsprüfung nach Artikel 8b Stromversorgungsverordnung (StromVV; SR 734.71). Er richtet sich hauptsächlich an Personen wie Hersteller oder Importeure, die Elemente eines intelligenten Messsystems auf Datensicherheit prüfen lassen wollen.

2. Begriffe

In diesem Leitfaden bedeuten:

- a. *Antragsteller*: Die Person, die METAS-Cert beantragt, ein Element eines intelligenten Messsystems auf die Gewährleistung der Datensicherheit hin zu prüfen.
- b. *METAS-Cert*: Die Organisationseinheit des METAS, die bei Datensicherheitsprüfungen für die Verfahrensleitung zuständig ist.
- c. *Prüflabor*: Das Labor des METAS oder von Dritten, das ein Element eines intelligenten Messsystems fachlich auf die Gewährleistung der Datensicherheit hin prüft.
- d. *Datensicherheitsprüfung*: Das Verfahren, in dem ein Element eines intelligenten Messsystems auf die Gewährleistung der Datensicherheit hin geprüft wird.
- e. *Datensicherheitszertifikat*: Die Verfügung des METAS, die bestätigt, dass ein Element eines intelligenten Messsystems erfolgreich auf die Gewährleistung der Datensicherheit hin geprüft wurde.

3. Ablauf der Datensicherheitsprüfung

- 3.1 Der Antragsteller eröffnet die Datensicherheitsprüfung mit einer Anfrage an METAS-Cert. Er legt dafür in dem von METAS-Cert zur Verfügung gestellten Formular dar, welches Element eines intelligenten Messsystems nach Artikel 8a StromVV er auf Datensicherheit prüfen lassen und mit welchem Prüflabor er zusammenarbeiten will.
- 3.2 METAS-Cert prüft die Anfrage und nimmt mit dem Antragsteller Rücksprache, wenn Unklarheiten bestehen. Anschliessend stellt METAS-Cert dem Antragsteller die Unterlagen zu, die für den Antrag auf Datensicherheitsprüfung nötig sind.
- 3.3 Der Antragssteller stellt METAS-Cert gestützt auf die ihm zur Verfügung gestellten Unterlagen den Antrag auf Datensicherheitsprüfung.
- 3.4 METAS-Cert prüft den Antrag formell und nimmt mit dem Antragsteller Rücksprache, wenn Unklarheiten bestehen. Anschliessend stellt METAS-Cert dem Antragsteller eine Mandatsbestätigung zu. Die Mandatsbestätigung legt insbesondere fest, was der Antragsteller für das weitere Verfahren beizutragen hat und wer bei METAS-Cert seine Ansprechperson ist.
- 3.5 Der Antragsteller prüft die Mandatsbestätigung und erklärt sein Einverständnis oder nimmt mit METAS-Cert Rücksprache, wenn Unklarheiten bestehen.
- 3.6 Wenn der Antragsteller sein Einverständnis mit der Mandatsbestätigung erklärt hat, prüft METAS-Cert den Antrag materiell. METAS-Cert informiert den Antragsteller wie folgt über das Ergebnis der Prüfung:
 - a. Mit Zustellung eines Entwurfs zum Datensicherheitszertifikat, wenn die Prüfung erfolgreich war.
 - b. Mit Mitteilung der Ergebnisse, wenn die Prüfung nicht erfolgreich war.

-
- 3.7 Der Antragsteller prüft die Information von METAS-Cert und teilt METAS-Cert mit, wie er weiter vorgehen will:
- a. Bei erfolgreicher Prüfung erklärt er entweder, dass er mit dem Entwurf zum Datensicherheitszertifikat einverstanden ist, oder er legt dar, welche Änderungen er darin wünscht.
 - b. Bei nicht erfolgreicher Prüfung legt er dar, welche Schlüsse er aus dem Prüfungsergebnis zieht. Insbesondere kann er seinen Antrag zurückziehen oder Vorschläge zur Behebung der festgestellten Mängel vorlegen.
- 3.8 METAS-Cert prüft die Mitteilung des Antragstellers und geht wie folgt vor:
- a. Bei erfolgreicher Prüfung stellt METAS-Cert das Datensicherheitszertifikat aus, sobald ein Entwurf vorliegt, der mit dem Antragsteller bereinigt ist.
 - b. Bei nicht erfolgreicher Prüfung beendet METAS-Cert das Verfahren, wenn der Antragsteller den Antrag zurückgezogen hat, oder nimmt mit dem Antragsteller Rücksprache, wenn er das Verfahren weiterführen will.
4. Prüflabors
- 4.1 METAS-Cert kann sich bei der Datensicherheitsprüfung auf die Arbeit von Prüflabors von Dritten stützen, wenn diese Prüflabors nach der Norm ISO/IEC 17025 mit einem für die Datensicherheitsprüfung relevanten Geltungsbereich akkreditiert sind, Referenzprojekte zu Penetrationstests von Komponenten des Internet of Things vorweisen können und eine der folgenden Voraussetzungen erfüllen:
- a. Das Prüflabor ist nach der Norm ISO/IEC 27001 zertifiziert.
 - b. Das Prüflabor ist nach den Common Criteria for Information Technology Security Evaluation zertifiziert.
 - c. Das Prüflabor verfügt über eine andere äquivalente Qualifikation.
- 4.2 Prüflabors werden beauftragt:
- a. Vom Antragsteller auf seine Kosten, wenn es sich um ein Prüflabor von Dritten handelt.
 - b. Von METAS-Cert auf Kosten des Antragstellers, wenn es sich um ein Prüflabor des METAS handelt.
- 4.3 Beauftragt der Antragsteller ein Prüflabor von Dritten, so vereinbart er mit diesem Prüflabor Folgendes:
- a. Das Prüflabor erklärt sich einverstanden, gegenüber METAS-Cert den Nachweis seiner Kompetenz zu erbringen, Rückfragen von METAS-Cert zu beantworten und allfällige Begutachtungen durch METAS-Cert vor Ort zuzulassen.
 - b. Das Prüflabor verpflichtet sich, Unterlagen für die Datensicherheitsprüfung entsprechend den Vorgaben von METAS-Cert zu übermitteln.
- 4.4 Das beauftragte Prüflaborlabor verfasst einen Bericht über die durchgeführten Prüfungen und reicht ihn im Namen des Antragstellers bei METAS-Cert ein.
5. Gültigkeit des Datensicherheitszertifikats
- 5.1 Das Datensicherheitszertifikat ist 5 Jahre ab seinem Ausstellungsdatum gültig. Danach kann es jeweils für weitere 5 Jahre verlängert werden, wenn die Datensicherheit gewährleistet ist. Das METAS kann die Fristen verkürzen, wenn die Gewährleistung der Datensicherheit dies verlangt.
- 5.2 Während der Gültigkeit des Datensicherheitszertifikats unterrichtet der Antragsteller METAS-Cert über alle Änderungen, die die Gewährleistung der Datensicherheit gefährden können. METAS-Cert entscheidet, ob die Änderung eine Ergänzungsprüfung und die Ergänzung des Datensicherheitszertifikats erfordert.
- 5.3 Das METAS kann das Datensicherheitszertifikat während dessen Gültigkeit entziehen, wenn die Datensicherheit nicht mehr gewährleistet ist.

5.4 Das METAS veröffentlicht die Erteilung, die Ergänzung, den Entzug und das Erlöschen der Datensicherheitszertifikate.

6. Übermittlung der Unterlagen

Der Antragsteller und die Prüflabors übermitteln die Unterlagen für die Datensicherheitsprüfung entsprechend den Vorgaben von METAS-Cert.

7. Kosten der Datensicherheitsprüfung

Das METAS erhebt für die Datensicherheitsprüfung Gebühren nach der Verordnung vom 5. Juli 2006 über die Gebühren des Eidgenössischen Instituts für Metrologie (GebV-METAS; SR 941.298.2).

8. Vorgehen bei Differenzen

8.1 Bei Differenzen über die Datensicherheitsprüfung suchen METAS-Cert und der Antragsteller eine einvernehmliche Lösung.

8.2 Kommt keine Einigung zu Stande, so erlässt das METAS eine Verfügung. Das Verfahren richtet sich nach dem Verwaltungsverfahrensgesetz vom 20. Dezember 1968 (VwVG; SR 172.021).

9. Haftung

Das METAS haftet nach dem Verantwortlichkeitsgesetz vom 14. März 1958 (VG; SR 170.32).

Bern-Wabern, 27. Mai 2019