Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Verfahrensbeschreibung zur Erteilung von IT-Sicherheitskennzeichen

VB Erteilung IT-SiK

Prozessverantwortung:	BSI | Referat Erteilung von IT-Sicherheitskennzeichen
Version:	1.1
Ausgabedatum:	01.03.2024
Einstufung:	öffentlich

Änderungshistorie und Freigabeinformation

Änderungshistorie

Version	Ausgabedatum	Name	Beschreibung
1.0	01.02.2022	Erteilung von IT-Sicherheitskennzeichen	**Erstausgabe**
1.1	01.03.2024	Erteilung von IT-Sicherheitskennzeichen	**Revision**

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat Erteilung von IT-Sicherheitskennzeichen

Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582 - 0
E-Mail: IT-Sicherheitskennzeichen@bsi.bund.de
Internet: www.bsi.bund.de

Inhaltsverzeichnis

Änderungshistorie und Freigabeinformation 2

1. Einleitung 4

1.1. Rechtliche Grundlagen 4

1.2. Begriffsbestimmungen 5

2. Verfahren zur Erteilung des IT-Sicherheitskennzeichens 6

2.1. Beteiligte Akteure 7

2.2. Gegenstand des Antrags 7

2.3. Beantragungsverfahren 8

2.4. Herstellererklärung 9

2.5. Antragsbearbeitung durch das BSI 9

2.6. Verfahrenskosten und Kostenlast 10

2.7. Abschließende Entscheidung 11

2.8. Antrag auf Verlängerung 11

3. Kennzeichnung und Veröffentlichungen auf der Produktinformationsseite 12

4. Laufzeit des IT-Sicherheitskennzeichens 12

5. Marktaufsicht 13

6. Pflichten des Herstellers während der Laufzeit des IT-Sicherheitskennzeichens 14

7. Widerruf und Ordnungswidrigkeiten 14

1. Einleitung

Mit dem IT-Sicherheitsgesetz 2.0 hat das BSI den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen einzuführen. Das IT-Sicherheitskennzeichen bietet Herstellern und Diensteanbietern[1] die Möglichkeit, das Versprechen in die IT-Sicherheit ihrer Produkte und Dienste[2] gegenüber dem Verbraucher transparent zu machen. Dadurch werden bereits während des Einkaufs sicherheitsrelevante Informationen zum Produkt zur Verfügung gestellt, die Verbraucherinnen und Verbraucher in ihre Kaufentscheidung einbeziehen können. Mit dem IT-Sicherheitskennzeichen erhöht das BSI das Bewusstsein für IT-Sicherheit auf dem Verbrauchermarkt, in dem es:

1. vom Hersteller zugesicherte Sicherheitseigenschaften digitaler Produkte transparent macht (Herstellererklärung) und

2. über aktuelle Sicherheitsinformationen, beispielsweise Schwachstellen und dazugehörige Updates, informiert (Sicherheitsinformation).

Das IT-Sicherheitskennzeichen wird durch das BSI für Produkte erteilt, wenn der Hersteller die Übereinstimmung mit bestimmten IT-Sicherheitsvorgaben selbst geprüft und deren Konformität durch die Abgabe einer Herstellererklärung zugesichert hat. Damit kommen Hersteller dem Informationsbedürfnis der Verbraucherinnen und Verbraucher nach, indem sie Sicherheitseigenschaften ihrer IT-Produkte transparent und leicht zugänglich darstellen. IT-Sicherheit wird dadurch zu einem entscheidungserheblichen Kaufargument.

Eine Beantragung des IT-Sicherheitskennzeichens ist nur innerhalb der vom BSI veröffentlichten Produktkategorien möglich und gesetzlich auf Produkte des Verbrauchermarkts beschränkt. Produkte aus dem B2B-Bereich fallen demnach nicht in den Anwendungsbereich des Kennzeichens.

Die vorliegende Verfahrensbeschreibung beschreibt und erläutert die diesbezüglichen Verfahren und richtet sich primär an (potenzielle) Antragsteller. Zu diesem Zweck werden die einzelnen Schritte des Verfahrens dargestellt sowie betroffene Akteure und beizubringende Unterlagen benannt. Ferner werden die Rechte und Pflichten der Beteiligten zusammenfassend aufgezeigt.

1.1. Rechtliche Grundlagen

Die Erteilung des IT-Sicherheitskennzeichens richtet sich nach § 9c des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) in Verbindung mit den Vorschriften der Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-ITSiKV).

Demnach wird die Freigabe des IT-Sicherheitskennzeichens für das jeweilige Produkt erteilt, wenn

1. das Produkt zu einer der Produktkategorien gehört, die das BSI durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt gegeben hat,

[1] nachfolgend nur als „Hersteller“ bezeichnet

[2] nachfolgend nur als „Produkt“ bezeichnet

2. die Herstellererklärung plausibel und durch die beigefügten Unterlagen ausreichend belegt ist und
3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde (§ 9c Abs. 5 Satz 1 BSIG).

Weitere Details zur Ausgestaltung des Antragsverfahrens regelt die BSI-ITSiKV.

1.2. Begriffsbestimmungen

Die nachfolgenden Begriffe sind für das Antragsverfahren von wesentlicher Bedeutung und definieren sich entsprechend § 2 BSI-ITSiKV wie folgt:

→ **Hersteller** ist jede juristische oder natürliche Person, die einen Dienst anbietet oder ein Produkt herstellt beziehungsweise entwickeln oder herstellen lässt und dieses Produkt oder diesen Dienst unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet; nicht erfasst sind die Hersteller einzelner Teile oder Komponenten davon.

→ **Verkäufer** ist jede juristische oder natürliche Person, die gewerblich ein Produkt unmittelbar Verbrauchern und Verbraucherinnen auf dem Markt bereitstellt.

→ **Branche** sind die Unternehmen und Organisationen und ihre Verbände, die für den jeweiligen Wirtschaftsbereich Produkte oder Dienstleistungen im Geltungsbereich des BSIG herstellen oder vertreiben.

→ Eine **branchenabgestimmte IT-Sicherheitsvorgabe** ist ein Anforderungskatalog, der von einer Branche erstellt und gepflegt wird und dessen Geeignetheit das BSI nach § 9c Absatz 3 Satz 1 BSIG festgestellt hat.

→ **Geeignete und qualifizierte Dritte** sind juristische oder natürliche Personen, die aufgrund ihrer fachlichen Qualifikation eine Aussage darüber treffen können, ob Sicherheitsversprechen eines Produktes eingehalten werden oder bestimmte Eigenschaften nachgewiesen werden können.

→ **Plausibilitätsprüfung** bedeutet die Sichtung der Herstellererklärung, der Angaben des Herstellers im Antrag und eventueller Unterlagen zur Ermittlung, ob die Konformität mit den vom BSI festgelegten Sicherheitsanforderungen plausibel und nachvollziehbar zugesichert wird.

→ **Produktkategorie** ist ein durch das BSI festgelegter Oberbegriff für die Erfassung einer Gruppe von vergleichbaren informationstechnischen Produkten in einem eingrenzbaren Bereich.

→ Die **zugehörige Internetseite** ist der für das einzelne Produkt angepasste Zielbereich auf der Internetseite des BSI, auf der Informationen zu diesem Produkt vorgehalten werden.

→ Das **Etikett**[3] ist die physische oder elektronische Kennzeichnung am Produkt oder seiner Umverpackung, welche produktspezifisch mit dem Verweis auf die zugehörige Internetseite angepasst wird.

[3] Die grafische Darstellung des Etiketts ist der BSI Zeichenordnung zur Zertifizierung und Anerkennung sowie IT-Sicherheitskennzeichen (BSI Zeichenordnung) zu entnehmen.

2. Verfahren zur Erteilung des IT-Sicherheitskennzeichens

Die Freigabe zur Verwendung des IT-Sicherheitskennzeichens erfolgt im Rahmen eines Antragsverfahrens beim BSI. Die Bearbeitung entsprechender Anträge erfolgt federführend durch das Referat - Erteilung von IT-Sicherheitskennzeichen. Weitere Organisationseinheiten des BSI werden anlassbezogen beteiligt. Die Antragsbearbeitung schließt mit einer positiven oder negativen Entscheidung über die Erteilung des IT-Sicherheitskennzeichens in Gestalt eines rechtsmittelfähigen Bescheids.

Der Antragsprozess stellt sich in der Übersicht wie folgt dar und wird im Weiteren durch dieses Dokument beschrieben:

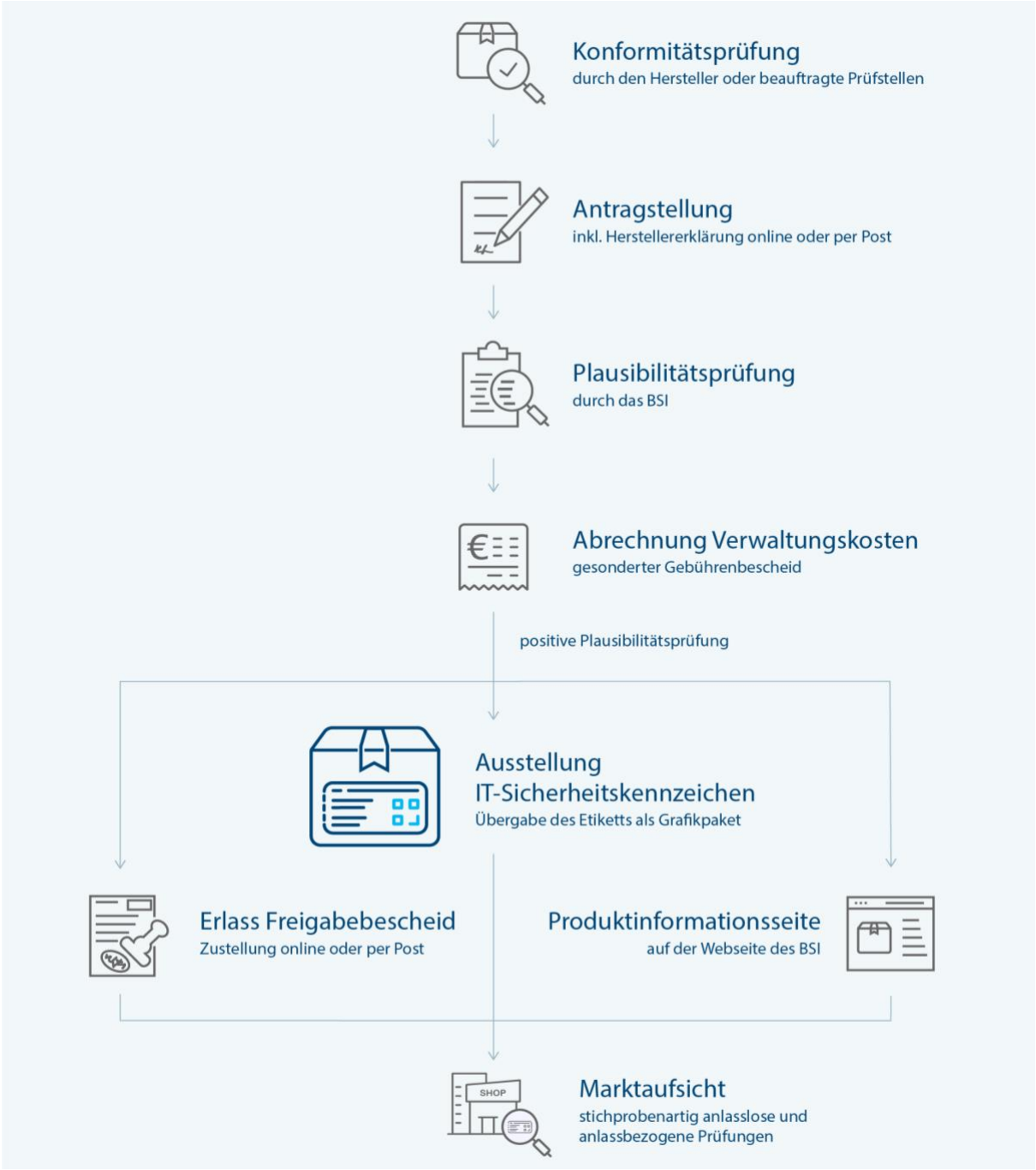

Abbildung 1 - Prozessschaubild zur Erteilung des IT-Sicherheitskennzeichens

2.1. Beteiligte Akteure

Am Verfahren können nachfolgend benannte Akteure beteiligt sein:

→ Das **Bundesamt für Sicherheit in der Informationstechnik** ist zuständige Behörde für die Beantragung, Erteilung und Aufsicht des IT-Sicherheitskennzeichens sowie zugehöriger Verwaltungsverfahren. Das BSI bearbeitet entsprechende Anträge, entscheidet über die Erteilung von IT-Sicherheitskennzeichen und übernimmt den nachgelagerten Prozess der Marktaufsicht.

→ Der Antrag auf Erteilung des IT-Sicherheitskennzeichen ist ausschließlich durch den **Hersteller** des Produkts zulässig und regelmäßig durch diesen zu stellen (§ 4 Abs. 1 Satz 2 BSI-ITSiKV). Er wird mit Eingang des Antrags beim BSI zum **Antragsteller**.

→ Sofern der Antragsteller im Einzelfall nicht zugleich Hersteller des antragsgegenständlichen Produkts ist, hat der Antragsteller eine Bevollmächtigung des Herstellers nachzuweisen, die den Antragsteller zu allen das Verwaltungsverfahren betreffenden Verfahrenshandlungen bevollmächtigt. Bedient sich der Hersteller zur Antragsstellung, zur Erfüllung seiner Pflichten aus dem BSIG oder der BSI-ITSiKV eines **bevollmächtigten Dritten**, werden ihm die Handlungen des Dritten wie eigene zugerechnet.

→ Die Konformitätsprüfung kann der Hersteller selbst durchführen (bspw. durch eine interne Auditierung) oder durch eine **Konformitätsbewertungsstelle** durchführen lassen. Konformitätsbewertungsstellen werden unmittelbar für den Antragssteller tätig und können neben der Konformitätsprüfung auch administrative Hilfe bei der Beantragung des IT-Sicherheitskennzeichen anbieten. Zur Information potentieller Antragssteller veröffentlicht das BSI eine Liste von Unternehmen/ Organisationen, die solche Konformitätsprüfungen im Rahmen des IT-Sicherheitskennzeichens anbieten. Die Veröffentlichung auf der Webseite ist dabei ausdrücklich nicht mit einer Empfehlung oder Qualitätsaussage durch das BSI verbunden (insbesondere keiner Anerkennung oder Zertifizierung).

→ Das BSI kann **qualifizierte Dritte** mit der Überprüfung von Herstellerdokumenten und -angaben beauftragen.

2.2. Gegenstand des Antrags

Ein Antrag auf Freigabe des IT-Sicherheitskennzeichens ist nur innerhalb der vom BSI bekanntgegebenen Produktkategorien zulässig (§ 4 Abs. 1 Satz 1 BSI-ITSiKV). Das Produkt (Antragsgegenstand) für das eine Freigabe zur Nutzung des IT-Sicherheitskennzeichens erteilt werden soll, muss zum Zeitpunkt der Antragstellung am deutschen Verbrauchermarkt verfügbar sein oder sich hinsichtlich der zugesicherten Eigenschaften in einem marktreifen Zustand befinden und innerhalb von drei Monaten ab Erteilung des IT-Sicherheitskennzeichens am deutschen Verbrauchermarkt verfügbar sein.

Der Antragsgegenstand wird bei Antragstellung über seine Marktbezeichnung, technischen Eigenschaften und den Anwendungsbereich der zugrundeliegenden Standards bestimmt und eindeutig identifiziert. Erteilte IT-Sicherheitskennzeichen behalten ihre Gültigkeit bei Änderungen am Antragsgegenstand nur dann, wenn diese die im Antrag erklärten Eigenschaften des Produkts nicht negativ beeinflussen. Der Hersteller ist während der Laufzeit des IT-Sicherheitskennzeichens verpflichtet, das BSI unaufgefordert zu informieren, wenn sich die erklärten Eigenschaften des Produktes ändern. Um die Gültigkeit des IT-Sicherheitskennzeichens lückenlos aufrecht zu erhalten, sollten relevante Änderungen am Produkt vorab mit dem BSI abgestimmt werden.

Das IT-Sicherheitskennzeichen wird produktbezogen vergeben, sodass eine Freigabe grundsätzlich für jedes Produkt einzeln zu beantragen ist. Produkte, die hinsichtlich ihrer

sicherheitsrelevanten Komponenten im Wesentlichen baugleich sind und für die der Hersteller übereinstimmende Sicherheitseigenschaften erklärt („Produktvarianten“), sodass nur eine einzelne Prüfung durch das BSI erforderlich ist, können unter einem Antrag zusammengefasst werden. Dies ist durch die entsprechende Angabe der jeweiligen Produktbezeichnungen im Antrag kenntlich zu machen.

Die parallele Einreichung mehrerer Anträge durch einen Antragsteller ist möglich.

2.3. Beantragungsverfahren

Der Hersteller muss vor der Antragstellung prüfen, ob das Produkt die Anforderungen der jeweiligen Produktkategorie erfüllt. Diese Konformitätsprüfung kann er entweder selbst vornehmen oder durch einen Dienstleister („Konformitätsbewertungsstelle“) vornehmen lassen. Mit der Abgabe der Herstellererklärung wird bestätigt, dass eine solche Überprüfung erfolgt ist und Konformität mit den IT-Sicherheitsanforderungen des BSI festgestellt wurde. Nach erfolgreicher Konformitätsprüfung kann das IT-Sicherheitskennzeichen beantragt werden.

Die Beantragung beim BSI erfolgt grundsätzlich elektronisch über das Bundesportal. Eine Verlinkung auf der Webseite des BSI führt direkt zum entsprechenden Onlineantrag. Für Antragsteller besteht dabei die Möglichkeit, sich entweder über das Elster-Konto ihres Unternehmens zu identifizieren oder den Antrag im Offline-Verfahren zu übermitteln. Beim Offline-Verfahren wird der Antrag ebenfalls im Bundesportal ausgefüllt, jedoch ohne elektronische Übermittlung heruntergeladen, ausgedruckt und als Brief versendet.

Sofern eine Online-Beantragung über das Bundesportal nicht erwogen wird, können weiterhin auch die auf der Webseite des BSI hinterlegten Antragsformulare per Post eingereicht werden. Gleiches gilt für neue Produktkategorien, solange diese noch nicht im Bundesportal umgesetzt sind.

Die Antragsformulare bestehen aus allgemeinen Angaben zum Antragsteller sowie produktspezifischen Anlagen. Die notwendigen Anlagen bestimmen sich nach der Produktkategorie, in der eine Beantragung erfolgen soll. Sie beinhalten auch die abzugebende Herstellererklärung. Gegebenenfalls beizufügende Unterlagen werden ebenfalls in den jeweiligen Formularfeldern benannt. Dem Antrag sind insbesondere Dokumente und Nachweise beizufügen, die das dabei zur Anwendung gekommene Vorgehen beschreiben und dokumentieren. Dies können beispielsweise externe Prüfberichte oder interne Auditierungen sein, die sich an einer vom BSI veröffentlichten Testspezifikation orientieren.

Weitere zusätzliche Unterlagen können im Bundesportal im Schritt „Ergänzende Angaben zum Antrag“ hochgeladen werden. In den nicht elektronischen Antragsformularen bietet die Anlage 4 diese Möglichkeit zur Ergänzung.

Sobald alle erforderlichen Unterlagen vorliegen, wird der vollständige Eingang des Antrags durch das BSI bestätigt. Die Eingangsbestätigung enthält eine Angabe zu den geltenden Prüfungsfristen für die Freigabeerklärung, welche in der Regel sechs Wochen beträgt, sofern keine abweichende Prüfungsfrist für die jeweilige Produktkategorie festgelegt wurde (§ 11 Abs. 1 BSI-ITSiKV).

Werden Unterlagen nicht oder nicht vollständig vorgelegt, muss der Antrag durch das BSI ohne Prüfung abgelehnt werden.

Zu beachten ist, dass für die Antragsbearbeitung eine Verwaltungsgebühr unabhängig vom Ausgang des Verfahrens erhoben wird. Es wird deshalb empfohlen, offene Fragen zur Beantragung eines IT-Sicherheitskennzeichen vor Antragstellung mit dem BSI zu besprechen.

2.4. Herstellererklärung

Zentrales Element des IT-Sicherheitskennzeichens ist die abzugebende Herstellererklärung. Die Herstellererklärung im engeren Sinne umfasst die Zusicherung des Herstellers, dass

→ der Antragsgegenstand nach Maßgabe der in der Produktkategorie geltenden Standards geprüft wurde und zum Zeitpunkt der Antragstellung alle zwingenden IT-Sicherheitsanforderungen des jeweiligen Standards erfüllt sind,

→ die Einhaltung der geltenden Standards für die Dauer der Freigabe aufrechterhalten wird,

→ empfohlene Anforderungen des jeweiligen Standards zum Zeitpunkt der Antragstellung erfüllt und für die Dauer der Freigabe aufrechterhalten werden, sofern keine gegenteilige Erklärung über begründete Abweichungen eingereicht wird,

→ das BSI für die Dauer der Freigabe unaufgefordert und unverzüglich informiert wird, wenn sich die erklärten Eigenschaften des Antragsgegenstands ändern, einschließlich (vorübergehender) Störungen der Informationssicherheit des Produktes und etwaiger Sicherheitslücken und

→ über die Dauer der Freigabe bekanntwerdende Sicherheitslücken behoben werden und der Stand der dafür erfolgten Maßnahmen dem BSI mit den in § 3 Abs. 4 Satz 2 BSI-ITSiKV genannten Informationen angezeigt werden.

Der Inhalt der Herstellererklärung ist für die Veröffentlichung auf der Produktinformationsseite vorgesehen.

2.5. Antragsbearbeitung durch das BSI

Sobald dem BSI alle erforderlichen Angaben und Unterlagen vorliegen, wird der eingereichte Antrag inhaltlich bearbeitet und geprüft. Zu beachten ist dabei, dass das BSI im Rahmen der Freigabe des IT-Sicherheitskennzeichens zunächst keine Tiefenprüfung oder technische Überprüfung der erklärten Sicherheitsvorgaben durchführt, sondern die Angaben und eingereichten Unterlagen des Herstellers nur auf Plausibilität überprüft. Die Überprüfung der zugesicherten Produkteigenschaften erfolgt in einem der Freigabe nachgelagerten Prozess, der anlasslosen und anlassbezogenen Marktaufsicht (vgl. Punkt 5., Marktaufsicht).

Das für die Erteilung von IT-Sicherheitskennzeichen zuständige Referat des BSI koordiniert die inhaltliche Antragsbearbeitung federführend unter Beteiligung einschlägiger Fachreferate sowie ggf. externer Stellen.

Die durchzuführende Plausibilitätsprüfung umfasst insbesondere:

→ die Prüfung, ob die mit der Herstellererklärung verbundenen Prüfmaßnahmen und Produkteigenschaften nachvollziehbar und glaubhaft versichert wurden.

→ die Abfrage innerhalb des BSI, ob das Produkt oder die mit dem Produkt ausgelieferte Software hier bekannte Sicherheitslücken enthält.

→ die Prüfung, ob Produkte des Herstellers bereits Gegenstand einer Warnung oder Information nach den §§ 7 oder 7a BSIG oder von Maßnahmen nach § 9c Abs. 8 BSIG betroffen waren.

→ die Prüfung, ob der Hersteller hinreichend zuverlässig erscheint, um Gewähr für die IT-Sicherheit des Antragsgegenstands über die gesamte Dauer der Freigabe des IT-Sicherheitskennzeichens zu bieten.

Ablehnungsgründe können sich dabei insbesondere aus bereits bekannten Problemen mit dem Produkt (z. B. Sicherheitslücken) oder vorherigem Fehlverhalten des Herstellers (z. B. Warnungen vor Produkten) ergeben. Das BSI kann die Freigabe des IT-Sicherheitskennzeichens auch dann verweigern, wenn der Freigabe unabhängig von den eingereichten Unterlagen ernstliche Zweifel an der Herstellererklärung entgegenstehen oder erforderliche Unterlagen nicht oder nicht vollständig vorgelegt werden.

Der Antrag kann im vereinfachten Prüfverfahren ohne Plausibilitätsprüfung bearbeitet werden, wenn für den Antragsgegenstand auf Grundlage des gleichen Prüfstandards bereits ein Zertifikat nach § 9 BSIG erteilt wurde. Die referenzierte Zertifizierung muss sich dabei nach Art und Umfang auf denselben Standard (bspw. Technische Richtlinie) beziehen, der auch für die jeweilige Produktkategorie des IT-Sicherheitskennzeichens einschlägig ist. In diesem Fall ist lediglich die Herstellererklärung abzugeben und im Übrigen auf das Aktenzeichen zu verweisen, unter dem das Zertifizierungsverfahren beim BSI geführt wird.

Ebenso ist ein vereinfachtes Antragsverfahren möglich, wenn für das antragsgegenständliche Produkt bereits ein ausländisches staatliches Kennzeichen erteilt wurde und dieses von einer bilateralen Anerkennungsvereinbarung umfasst ist. Eine Übersicht über bestehende Anerkennungsabkommen stellt das BSI auf seiner Webseite zur Verfügung.

Bei ausländischer Kennzeichnung ist für die Beantragung des IT-Sicherheitskennzeichens im vereinfachten Verfahren der Hauptantrag mit der Herstellererklärung, den Technischen Angaben zum Produkt sowie Angaben zur durchgeführten Konformitätsprüfung einzureichen. In Absprache mit dem BSI können vergleichbare Dokumente aus dem ausländischen Antragsverfahren vorgelegt werden.

2.6. Verfahrenskosten und Kostenlast

Für die Antragsbearbeitung wird durch das BSI eine Verwaltungsgebühr erhoben. Sie ergibt sich aus der Besonderen Gebührenverordnung des Bundesministeriums des Innern und für Heimat (BMIBGebV).

Die Verwaltungsgebühr fällt je nach Ausgang des Antragsverfahrens gleichermaßen vollständig an. Demnach wird eine Verwaltungsgebühr auch bei negativer Freigabeentscheidung oder bei Rücknahme des Antrages durch das BSI erhoben.

Die Plausibilitätsprüfung des Antrags kann auch durch einen vom BSI beauftragten qualifizierten Dritten erfolgen. Der Antragssteller trägt ggf. die Kosten der Überprüfung durch qualifizierte Dritte. Derzeit ist eine Hinzuziehung qualifizierter Dritter in der Regel nicht vorgesehen. Sofern dies jedoch im Einzelfall angezeigt erscheint, wird der Antragsteller hierauf hingewiesen.

Werden die Kosten von einem Dritten übernommen, muss dies mitgeteilt und eine entsprechende Kostenübernahmeerklärung vorgelegt werden.

Gemäß § 9c Abs. 5 Satz 1 Nr. 3 BSGI ist die Begleichung der erhobene Verwaltungsgebühr tatbestandliche Voraussetzung für die Erteilung des IT-Sicherheitskennzeichens. Der Antragsteller erhält deshalb vor Freigabe des IT-Sicherheitskennzeichens einen gesonderten Gebührenbescheid des BSI über die zu zahlende Verwaltungsgebühr. Erst nach vollständigem Zahlungseingang erfolgt die abschließende Freigabe des IT-Sicherheitskennzeichens.

2.7. Abschließende Entscheidung

Nach Abschluss der Antragsprüfung wird durch das BSI mit rechtsmittelfähigem Bescheid über den Antrag entschieden.

Sofern im Ergebnis der Prüfung beabsichtigt sein sollte, die Erteilung des IT-Sicherheitskennzeichens abzulehnen, wird der Antragsteller hierzu vorab nach den Vorschriften des Verwaltungsverfahrensgesetzes (VwVfG) angehört.

Im Falle einer positiven Entscheidung über den Antrag erhält der Antragsteller einen entsprechenden Freigabebescheid. Die Veröffentlichung der jeweiligen Produktinformationsseite sowie die Bereitstellung des individuellen Etiketts erfolgen nach Bekanntgabe des Freigabebescheids. Die Zustellung erfolgt regelmäßig gegen Postzustellungsurkunde.

2.8. Antrag auf Verlängerung

Trägt ein Produkt ein gültiges IT-Sicherheitskennzeichen, kann derselbe Hersteller frühestens drei Monate und spätestens sechs Wochen vor Ablauf der Gültigkeit des IT-Sicherheitskennzeichens einen Antrag auf Verlängerung stellen.

Für die Beantragung ist der Vordruck „Antrag auf Verlängerung bereits erteilter IT-Sicherheitskennzeichen“ zu verwenden.

Sofern der Hersteller bestätigt, dass die in der ursprünglichen Herstellererklärung zugesicherten Eigenschaften weiterhin erfüllt und aufrechterhalten werden, kann sich der Hersteller auf die Herstellererklärung nebst Anlagen aus dem ersten Antragsverfahren beziehen. Die Einreichung zusätzlicher Dokumente ist in diesem Fall grundsätzlich nicht erforderlich. Im Zuge der Plausibilitätsprüfung können jedoch anlassbezogen weitere Unterlagen nachgefordert werden.

3. Kennzeichnung und Veröffentlichungen auf der Produktinformationsseite

Mit der Erteilung des IT-Sicherheitskennzeichens wird das Produkt mit einer individuellen Produktinformationsseite in das zentrale Verzeichnis gekennzeichneter Produkte aufgenommen, welches über das Onlineangebot des BSI öffentlich einsehbar ist. Jedes Etikett eines IT-Sicherheitskennzeichen ist mit einem individuellen QR-Code und Link versehen, welcher unmittelbar auf die Produktinformationsseite des jeweiligen Produkts führt. Über den Verweis werden auf der Produktinformationsseite die weiterführenden Sicherheitsinformationen dargestellt.

Die Produktinformationsseite beinhaltet sicherheitsrelevante Angaben und Informationen über Eigenschaften des Produkts, den Inhalt der abgegebenen Herstellererklärung sowie den zugrundeliegenden Prüfstandard. Zentrales Element des IT-Sicherheitskennzeichens ist darüber hinaus die auf der Produktinformationsseite veröffentlichte Sicherheitsinformation. Diese informiert auf Grundlage eines vom BSI festgelegten Verfahrens (vgl. Punkt 5., Marktaufsicht) über aktuelle sicherheitsrelevante Erkenntnisse zum gekennzeichneten Produkt.

Das produktspezifische Etikett wird nach Bekanntgabe des Freigabebescheids elektronisch und in Druckauflösung zur Verfügung gestellt. Die konkrete Verwendung des Etiketts bestimmt sich nach § 9c BSIG sowie der BSI-ITSiKV und den ergänzenden Vorschriften der BSI Zeichenordnung. Hersteller dürfen gemäß ihrer Freigabe keine von diesen Vorgaben abweichende Gestaltung verwenden. Die Nutzung des IT-Sicherheitskennzeichens zu Werbezwecken ist erlaubt und erwünscht. Das Etikett des IT-Sicherheitskennzeichens ist auf dem Produkt oder dessen Umverpackung anzubringen. Sofern das Kennzeichen für einen Dienst erteilt wurde oder eine Anbringung des Etiketts aus einem sonstigen tatsächlichen Grund nicht möglich ist, kann dieses auch elektronisch genutzt werden. Dies gilt insbesondere für Produkte, an denen aufgrund ihrer Beschaffenheit kein Zeichen angebracht werden kann.

4. Laufzeit des IT-Sicherheitskennzeichens

Das IT-Sicherheitskennzeichen hat eine regelmäßige Laufzeit von zwei Jahren, sofern keine abweichende Laufzeit für die jeweilige Produktkategorie bestimmt wurde. Die Laufzeit beginnt mit dem Tag der Bekanntgabe des Freigabebescheids oder ergibt sich aus der im Freigabebescheid festgesetzten Laufzeitdauer.

Durch einen rechtzeitigen Folgeantrag (frühestens drei Monate und spätestens sechs Wochen vor Ablauf der Gültigkeit des IT-Sicherheitskennzeichens) kann der Hersteller vor Ablauf der Gültigkeit des IT-Sicherheitskennzeichens dessen Verlängerung beantragen (vgl. Punkt 2.8. Antrag auf Verlängerung). Damit wird gewährleistet, dass ein Produkt „lückenlos“ über ein gültiges IT-Sicherheitskennzeichen verfügt.

Nach Ablauf der festgelegten Dauer erlischt die Freigabe für die Nutzung des IT-Sicherheitskennzeichens. Dasselbe gilt, wenn der Hersteller gegenüber dem BSI erklärt, dass er seinen Antrag zurücknimmt bzw. auf die Verwendung des IT-Sicherheitskennzeichens verzichtet. Das BSI veröffentlicht einen entsprechenden Hinweis in der Sicherheitsinformation innerhalb der Produktinformationsseite, dass die Freigabe des IT-Sicherheitskennzeichens erloschen ist.

Der Hersteller hat dafür Sorge zu tragen, dass keine nach dem Erlöschen hergestellten Produkte mehr mit dem Etikett auf den Markt gebracht werden.

Ungeachtet dessen erlischt die Freigabe für das IT-Sicherheitskennzeichen nach einer Frist von sechs Wochen, wenn eine für die einschlägige Produktkategorie geltende IT-Sicherheitsvorgabe geändert oder für ungültig erklärt wird und der Hersteller die Herstellererklärung nicht auf einer gültigen Prüfgrundlage aktualisiert. Das BSI weist auf entsprechende Änderungen, Ungeeignetheit oder Aufhebungen auf seiner Internetseite hin.

5. Marktaufsicht

Tragen Produkte das IT-Sicherheitskennzeichen, so unterliegen diese ab Erteilung des Kennzeichens einer nachgelagerten Überwachung durch das BSI. Das BSI prüft in diesem Rahmen, ob die zugesicherten Eigenschaften des Produkts durch den Hersteller tatsächlich eingehalten werden.

Die Produkte werden hierzu stichprobenartig anlasslos oder anlassbezogen geprüft. Anlass zur Prüfung können beispielsweise bekanntgewordene Schwachstellen zum betreffenden Produkt, der verwendeten Technologie oder zu ähnlichen Produkten des gleichen Herstellers sein, die noch kein IT-Sicherheitskennzeichen tragen.

Werden bei einem Produkt Abweichungen von der Herstellererklärung festgestellt, kann das BSI geeignete Maßnahmen zum Schutz des Vertrauens der Verbraucherinnen und Verbraucher in das IT-Sicherheitskennzeichen ergreifen, zum Beispiel durch Bereitstellung entsprechender Informationen an die Verbraucherinnen und Verbraucher über die Produktinformationsseite bis hin zum Widerruf des IT-Sicherheitskennzeichens.

Durch das BSI aufgeklärte Schwachstellen und zu veröffentlichende Informationen werden in geeigneter Weise, angelehnt an das „Responsible-Disclosure-Verfahren“, dem Hersteller mit der Gelegenheit zur Rückäußerung zur Kenntnis gegeben. In der Regel wird den betroffenen Herstellern eine angemessene Frist eingeräumt, um die festgestellten Sicherheitslücken zu beheben und den zugesicherten Zustand des Produkts wiederherzustellen, bevor Maßnahmen durch das BSI ergriffen werden. Dies gilt zum Schutz der Verbraucherinnen und Verbraucher dann nicht, wenn gewichtige Gründe der Sicherheit der Produkte eine sofortige Maßnahme erfordern.

Weitere Informationen zum Prozess der Marktaufsicht können der „Verfahrensbeschreibung zur Marktaufsicht über IT-Sicherheitskennzeichen“ entnommen werden. Diese ist auf der Webseite des BSI abrufbar.

6. Pflichten des Herstellers während der Laufzeit des IT-Sicherheitskennzeichens

Die Pflichten des Herstellers während der Laufzeit des IT-Sicherheitskennzeichens ergeben sich im Wesentlichen aus

→ dem BSIG nebst BSI-ITSiKV,

→ der mit der Herstellererklärung verbundenen Selbstverpflichtung (vgl. Punkt 2.4., Herstellererklärung),

→ den in diesem Dokument benannten Nebenpflichten der Laufzeit (vgl. Punkt 4., Laufzeit) und Marktaufsicht (vgl. Punkt 5., Marktaufsicht) sowie

→ der BSI Zeichenordnung zur Anerkennung, Zertifizierung und IT-Sicherheitskennzeichen.

Eine Zusammenfassung der wichtigsten Pflichten stellt das BSI auf seiner Webseite zur Verfügung.

7. Widerruf und Ordnungswidrigkeiten

Bei einem Verstoß gegen die Herstellererklärung, die gesetzlichen Herstellerpflichten, bei unzutreffenden oder unvollständigen Angaben, sowie dem sonstigen Wegfall der Erfüllung der gesetzlichen Voraussetzungen oder Anforderungen des BSI kann die Freigabe widerrufen werden. Dem Hersteller wird im Rahmen der Anhörung eine angemessene Frist zur Stellungnahme gegeben, es sei denn, gewichtige Sicherheitsgründe erfordern eine sofortige Maßnahme.

Ordnungswidrig handelt, wer ein IT-Sicherheitskennzeichen ohne erforderliche Freigabe durch das BSI verwendet. Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfhunderttausend Euro geahndet werden.