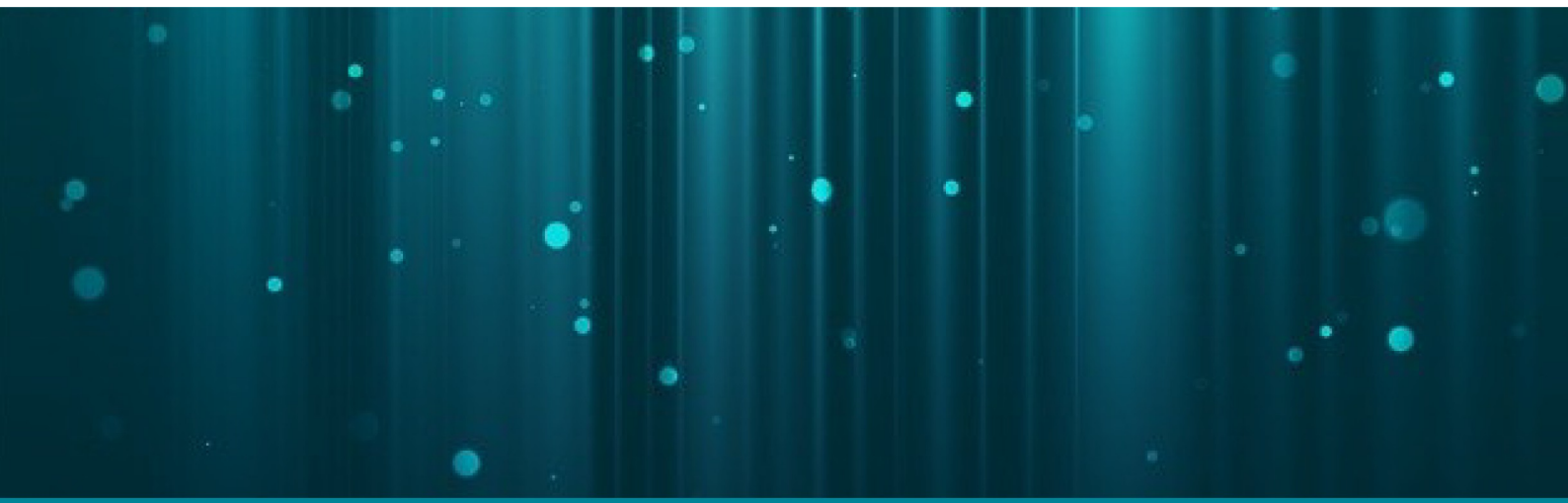

DIGIPASS FX7

Benutzerhandbuch

Version: 2024-08-01

Copyright-Hinweis

Copyright © 2024 OneSpan North America, Inc. Alle Rechte vorbehalten.

Markenzeichen

OneSpan™, DIGIPASS® und CRONTO® sind eingetragene oder nicht eingetragene Marken von OneSpan North America Inc., OneSpan NV und/oder OneSpan International GmbH (zusammen "OneSpan") in den USA und anderen Ländern.

OneSpan behält sich alle Rechte an den Marken, Dienstleistungsmarken und Logos von OneSpan und

seinen Tochtergesellschaften vor. Alle anderen Marken oder Handelsnamen sind Eigentum der jeweiligen

Inhaber.

Geistiges Eigentum

OneSpan Software, Dokumente und zugehörige Materialien ("Materialien") enthalten geschützte und vertrauliche Informationen. Alle Titel, Rechte und Anteile an der OneSpan Software und den Materialien, deren Updates und Upgrades, einschließlich der Softwarerechte, Urheberrechte, Patentrechte, Geschmacksmusterrechte, Geschäftsgeheimnisrechte, Datenbankrechte sui generis und aller anderen geistigen und gewerblichen Eigentumsrechte liegen ausschließlich bei OneSpan oder seinen Lizenzgebern. OneSpan-Software oder -Materialien dürfen nicht heruntergeladen, kopiert, übertragen, offengelegt, reproduziert, weiterverteilt oder in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch, mechanisch oder anderweitig, für kommerzielle oder Produktionszwecke übertragen werden, es sei denn, dies ist anders gekennzeichnet oder von OneSpan ausdrücklich schriftlich gestattet.

Haftungsausschluss

OneSpan übernimmt keine Haftung für die Richtigkeit, Vollständigkeit oder Aktualität der Inhalte oder für die Verlässlichkeit von Links zu und Inhalten von externen oder fremden Websites.

OneSpan haftet unter keinen Umständen für Verluste, Schäden oder Kosten, die Ihnen, Ihrem U n t e r n e h m e n oder Dritten durch die Nutzung oder die Unmöglichkeit der Nutzung der OneSpan Software oder der Materialien oder der zur Verfügung gestellten oder herunterladbaren Materialien von Dritten entstehen. OneSpan haftet nicht für Verluste/Schäden, die durch die Ä n d e r u n g dieser rechtlichen Hinweise oder des Inhalts entstehen.

Reservierung

OneSpan behält sich das Recht vor, diese Hinweise und den Inhalt jederzeit zu ändern. OneSpan behält sich ebenfalls das Recht vor, die Zustimmung zurückzuziehen oder zu widerrufen oder die Nutzung der OneSpan Software oder der Materialien anderweitig zu untersagen, wenn eine solche Nutzung nicht den Bedingungen einer schriftlichen Vereinbarung zwischen OneSpan und Ihnen oder anderen geltenden Bedingungen entspricht, die OneSpan von Zeit zu Zeit veröffentlicht.

Kontaktieren Sie uns

Besuchen Sie unsere Website: **https://www.onespan.com**
Ressourcenzentrum: **https://www.onespan.com/resource-center**
Technische Unterstützung und Wissensdatenbank: **https://www.onespan.com/support**

Wenn Sie in der Wissensdatenbank keine Lösung finden, wenden Sie sich an das Unternehmen, von dem Sie das

OneSpan-Produkt bezogen haben. Datum: 2024-08-01

Inhalt

Abbildung

Tabelle

Verfahren

Produktübersicht

1

Willkommen beim *DIGIPASS FX7 Benutzerhandbuch*! DIGIPASS FX7 ist ein phishing-resistenter Authentifikator, der sofort mit fast 1.000 FIDO2-fähigen Diensten funktioniert.

Die **FIDO Alliance** entwickelt Standards für die passwortlose Authentifizierung. Mit FIDO (Fast IDentity Online) basiert die Benutzerauthentifizierung nicht auf statischen Passwörtern oder einmaligen Passwörtern. Stattdessen werden die Benutzer über biometrische Daten und FIDO-konforme Authentifikatoren authentifiziert.

Der DIGIPASS FX7 Authentifikator funktioniert im angeschlossenen Modus über USB-C.

1.1 Übersicht der Geräte

1.1.1 Authenticator Vorderseite

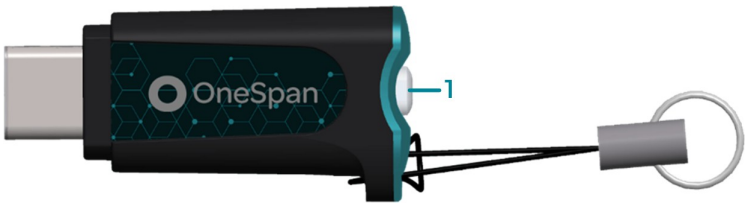

Abbildung 1: Authenticator Vorderseite

1 Taste mit integrierter LED

1.1.2 Authenticator zurück

Auf der Rückseite des Authentifikators sind die gesetzlich vorgeschriebenen Kennungen aufgedruckt. Das Etikett enthält eine eindeutige 10-stellige Seriennummer, sowohl im Textformat als auch als 2D-Barcode.

Abbildung 2: Authenticator Rückseite

1.2 PIN-Schutz

Der DIGIPASS FX7 Authentifikator führt eine Benutzerverifizierung per PIN durch.

Da der DIGIPASS FX7 Authentifikator über keine Tastatur verfügt, wird die PIN auf dem Gerät eingegeben, an das der Authentifikator angeschlossen ist (in der Regel ein Computer oder ein mobiles Gerät).

Die PIN setzt sich aus alphanumerischen Zeichen zusammen und muss den folgenden Regeln entsprechen:

- **Mindestlänge**: 4 Dezimalziffern oder 4 Zeichen
- **Maximale Länge**: 63 Bytes in UTF-8-Darstellung. Dies entspricht 63 Zeichen, wenn nur Standard-ASCII-Zeichen verwendet werden, aber weniger Zeichen, wenn Sonderzeichen verwendet werden (z.B. mit Akzent, Chinesisch,...).

HINWEIS: Nach 3 aufeinanderfolgenden falschen PIN-Versuchen muss der Authentifikator aus dem USB-Anschluss entfernt und erneut eingesteckt werden.

ACHTUNG: Nach insgesamt 8 aufeinanderfolgenden falschen PIN-Versuchen wird der Authentifikator gesperrt. Der Authentifikator muss zurückgesetzt werden, wodurch alle Daten (Zugangsdaten, Konten, PIN) gelöscht werden und der Authentifikator auf die Werkseinstellungen zurückgesetzt wird.

1.3 LED-Anzeige

Das Gerät verfügt über eine in die Taste integrierte LED.

Tabelle 1: Beschreibung der LED

LED	Beschreibung
○ ○ ○ Blinkend WEISS	Benutzeranwesenheit angefordert; warten, bis Taste gedrückt wird.
○ WEISS	Nach dem Einsetzen des Authentifikators leuchtet die LED kurz auf, um anzuzeigen, dass DIGIPASS FX7 betriebsbereit ist.

Erste Schritte

2

2.1 Erste Schritte

2.1.1 Schalten Sie den Authentifikator ein/aus

- Um den Authentifikator einzuschalten, verbinden Sie den Authentifikator mit einem Computer oder einem mobilen Gerät.
- Um den Authentifikator auszuschalten, ziehen Sie den Stecker des Authentifikators.

2.1.2 Verbinden Sie Ihren Authentifikator

Sie können Ihren Authenticator über USB-C oder über einen USB-A zu USB-C Adapter anschließen.

2.2 Erstmalige Einrichtung des Authentifikators

Mit den folgenden Anwendungen können Sie Ihren Authentifikator einrichten und verwalten:

- Unter *Windows* können Sie Ihren Authentifikator in der App Windows-Einstellungen verwalten.
- Unter *macOS* und *Linux* können Sie Ihren Authentifikator über die Sicherheitseinstellungen von Google Chrome verwalten.

Die Ersteinrichtung des Authentifikators umfasst die folgenden Schritte:

1. Legen Sie die PIN fest

2.2.1 Windows

▶So legen Sie die PIN fest (Windows Einstellungen App)

1. Verbinden Sie Ihren Authentifikator.
2. Klicken Sie auf die Schaltfläche Start auf Ihrem Computer und wählen Sie **Einstellungen**, um die Win- dows-Einstellungen-App zu öffnen.
3. Wählen Sie **Konten > Anmeldungsoptionen**.
4. Klicken Sie auf **Sicherheitsschlüssel** und dann auf **Verwalten**.
5. Wenn Sie dazu aufgefordert werden, drücken Sie die Taste auf dem Authentifikator. Der **Windows** Hello-Einrichtungsdialog wird angezeigt.
6. Klicken Sie unter **Sicherheitsschlüssel-PIN** auf **Hinzufügen**.
7. Geben Sie die Authentifikator-PIN ein, bestätigen Sie sie und klicken Sie auf **OK**. Siehe **1.2 PIN-Schutz** für PIN-Anforderungen.

2.2.2 macOS und Linux

▶So legen Sie die PIN fest (Google Chrome)

1. Verbinden Sie Ihren Authentifikator.
2. Rufen Sie in Google Chrome die Seite **Sicherheitsschlüssel verwalten** auf:
   - Klicken Sie auf ⋮ **Anpassen und Steuern von Google Chrome** und wählen Sie **Einstellungen > Datenschutz und Sicherheit > Sicherheit > Sicherheitsschlüssel verwalten**.

   -OR-

   - Geben Sie die folgende Adresse in die Adressleiste ein:

     chrome://settings/securityKeys
3. Klicken Sie auf **PIN erstellen**.
4. Wenn Sie dazu aufgefordert werden, drücken Sie die Taste auf dem Authentifikator.
5. Geben Sie die PIN ein, bestätigen Sie sie und klicken Sie auf **Speichern**. Siehe **1.2 PIN-Schutz** für die PIN-Anforderungen.
6. Klicken Sie auf **OK**, um die Erstellung der PIN abzuschließen.

2.3 Verwenden Sie den Authentifikator

Die Schritte zur Verwendung des DIGIPASS FX7-Authentifikators hängen von der Einrichtung Ihres Anwendungsanbieters ab. Unter **3 FIDO-Authentifizierung** finden Sie einen Überblick über den FIDO-Registrierungs- und Anmeldeprozess.

FIDO-Authentifizierung

3

Für die FIDO-Authentifizierung müssen Sie zunächst Ihren DIGIPASS FX7-Authentikator bei dem entsprechenden Dienst registrieren. Nach erfolgreicher Registrierung können Sie sich bei dem Dienst anmelden.

HINWEIS: FIDO-Operationen sind über kompatible Browser zugänglich.

3.1 Beginnen Sie mit der FIDO-Authentifizierung

Die Registrierungs- und Authentifizierungsabläufe variieren je nach den Optionen, die vom Browser und der Plattform verwendet werden.

3.1.1 Bevor Sie beginnen

Bevor Sie mit der FIDO-Authentifizierung beginnen können, müssen Sie sicherstellen, dass Sie die Ersteinrichtung des Authentifikators abgeschlossen haben. Weitere Informationen finden Sie unter **2.2 Erstmalige Einrichtung des Authentifikators**.

> **HINWEIS:** Es kann sein, dass das System zu Beginn des Registrierungsvorgangs automatisch den PIN-Einrichtungsvorgang einleitet, wenn im Authentifikator keine PIN festgelegt wurde.

3.1.2 Registrieren Sie den Authentifikator und melden Sie sich an

▶So registrieren Sie den Authentifikator

1. Schließen Sie Ihren Authenticator über USB-C an.
2. Folgen Sie den Anweisungen für den entsprechenden Dienst, um den Authentifikator für die FIDO-Authentifizierung zu registrieren.

   Während des Registrierungsprozesses müssen Sie in der Regel den Namen des Authentifikators angeben, die Taste drücken und Ihre PIN eingeben.

> **HINWEIS:** Der DIGIPASS FX7 Authentifikator kann bis zu 100 erkennbare Berechtigungsnachweise speichern.

▶So melden Sie sich mit der FIDO-Authentifizierung an

1. Schließen Sie Ihren Authenticator über USB-C an.
2. Folgen Sie den Anweisungen für den Dienst, bei dem Sie sich anmelden möchten.

Wenn Sie dazu aufgefordert werden, drücken Sie die Taste und geben Sie Ihre PIN zur Authentifizierung ein.

HINWEIS: Ob eine PIN für die Authentifizierung erforderlich ist, entscheidet der Dienst (Relying Party).

Verwalten Sie den Authentifikator

4

Abhängig von Ihrem Betriebssystem können Sie die folgenden Anwendungen für die Authentifikatorverwaltung verwenden:

- Unter *Windows* können Sie Ihren Authentifikator in der App Windows-Einstellungen verwalten.
- Unter *macOS* und *Linux* können Sie Ihren Authentifikator über die Sicherheitseinstellungen von Google Chrome verwalten.

4.1 Ändern Sie die PIN

4.1.1 Windows

▶So ändern Sie die PIN (Windows Einstellungen App)

1. Schließen Sie Ihren Authentifikator an und öffnen Sie den **Windows** Hello-Einrichtungsdialog in der Windows-Einstellungen-App. Anweisungen zum Öffnen des Dialogs finden Sie unter **2.2 Ersteinrichtung des Authentifikators**.
2. Klicken Sie unter **Sicherheitsschlüssel-PIN** auf **Ändern**.
3. Gehen Sie wie folgt vor:
   a. Geben Sie die alte PIN ein.
   b. Geben Sie die neue PIN ein und bestätigen Sie sie.

   Siehe **1.2 PIN-Schutz** für PIN-Anforderungen.
4. Klicken Sie auf **OK**.

4.1.2 macOS und Linux

▶So ändern Sie die PIN (Google Chrome)

1. Verbinden Sie Ihren Authentifikator.
2. Klicken Sie auf der Seite **Sicherheitsschlüssel verwalten** in den Sicherheitseinstellungen von Google Chrome auf **PIN erstellen**. Anweisungen zum Öffnen der Seite finden Sie unter **2.2 Erstmalige Einrichtung des Authentifikators**.
3. Wenn Sie dazu aufgefordert werden, drücken Sie die Taste auf dem Authentifikator.

4. Gehen Sie wie folgt vor:

    a. Geben Sie die alte PIN ein.

    b. Geben Sie die neue PIN ein und bestätigen Sie sie.

    Siehe **1.2 PIN-Schutz** für PIN-Anforderungen.

5. Klicken Sie auf **Speichern**.

4.2 FIDO-Anmeldeinformationen entfernen

4.2.1 Windows

Die Windows-Einstellungs-App unterstützt das Entfernen von FIDO-Anmeldeinformationen nicht.

4.2.2 macOS und Linux

In Google Chrome können Sie die Liste der auffindbaren Anmeldeinformationen anzeigen und bei Bedarf Anmeldeinformationen löschen.

▶So entfernen Sie FIDO-Anmeldeinformationen (Google Chrome)

1. Verbinden Sie Ihren Authentifikator.
2. Klicken Sie auf der Seite **Sicherheitsschlüssel verwalten** in den Sicherheitseinstellungen von Google Chrome auf **Anmeldedaten**. Anweisungen zum Öffnen der Seite finden Sie unter **2.2 Erstmalige Einrichtung des Authentifikators**.
3. Suchen Sie den entsprechenden Berechtigungsnachweis in der Liste und klicken Sie auf das Symbol **Löschen**.
4. Klicken Sie auf **Erledigt**.

4.3 Authentifikator zurücksetzen

In manchen Situationen ist es notwendig, die Werkseinstellungen des DIGIPASS FX7 Authentifikators wiederherzustellen, z.B. wenn die PIN gesperrt ist.

Beim Zurücksetzen auf die Werkseinstellungen werden alle persönlichen Daten, die auf dem Authentifikator gespeichert sind, gelöscht:

- PIN
- Alle Berechtigungsnachweise
- Alle Konten

4.3.1 Windows

▶So setzen Sie den Authentifikator zurück (Windows Einstellungen App)

1. Schließen Sie Ihren Authentifikator an und öffnen Sie den **Windows** Hello-Einrichtungsdialog in der Windows-Einstellungen-App. Anweisungen zum Öffnen des Dialogs finden Sie unter **2.2 Ersteinrichtung des Authentifikators**.
2. Klicken Sie unter **Sicherheitsschlüssel zurücksetzen** auf **Zurücksetzen**.
3. Klicken Sie auf **Fortfahren**, um zu bestätigen, dass Sie den Authentifikator zurücksetzen möchten.
4. Wenn Sie dazu aufgefordert werden, trennen Sie die Verbindung zum Authentifikator und schließen ihn erneut an.
5. Wenn Sie dazu aufgefordert werden, drücken Sie innerhalb von 10 Sekunden, nachdem Sie den Authentifikator wieder angeschlossen haben, zweimal die Taste am Authentifikator.
6. Wenn das Zurücksetzen abgeschlossen ist, klicken Sie auf **Fertig**.

4.3.2 macOS und Linux

▶So setzen Sie den Authentifikator zurück (Google Chrome)

1. Verbinden Sie Ihren Authentifikator.
2. Klicken Sie auf der Seite **Sicherheitsschlüssel verwalten** in den Sicherheitseinstellungen von Google Chrome auf **Sicherheitsschlüssel zurücksetzen**. Anweisungen zum Öffnen der Seite finden Sie unter **2.2 Erstmalige Einrichtung des Authentifikators**.
3. Wenn Sie dazu aufgefordert werden, trennen Sie den Authentifikator und schließen ihn wieder an, dann drücken Sie die Taste am Authentifikator.
4. Wenn Sie dazu aufgefordert werden, drücken Sie die Taste auf dem Authentifikator, um das Zurücksetzen auf die Werkseinstellungen zu bestätigen.
5. Klicken Sie auf **OK**, um das Zurücksetzen auf die Werkseinstellungen abzuschließen.

Technische Daten und System Anforderungen

5

5.1 Technische Daten

Tabelle 2: Technische Daten für DIGIPASS FX7

Größe	35mm (49,5 mit Kabel) (L) x 35(B) x 10,8mm(H)
Gewicht	3g
Batterie	Keine Batterie
Anschluss	USB-C
Energieversorgung	Über USB-C, 4,40 bis 5,50 Volt
Staub- und wasserdicht	Staubgeschützt und spritzwassergeschützt
Unterstützte Protokolle	FIDO: • FIDO U2F • FIDO2.1: das Gerät implementiert die CTAP2.1 Spezifikation

5.2 Systemanforderungen

Unterstützte Betriebssysteme:

- Windows 10 Version 1903 oder höher
- macOS 13 oder höher
- Ubuntu 22.04.2 oder höher
- Android 12 oder höher

Unterstützte Browser:

- Google Chrome 111 oder höher
- Alle Browser, die die *FIDO2 WebAuthn API* unterstützen

> **HINWEIS:** Eine Liste mit kompatiblen Betriebssystemen und Browsern finden Sie unter https://www.onespan.com/digipassfx7.

Sicherheitshinweise und Vorschriften Informationen

6

6.1 Sicherheitshinweis

ACHTUNG: Die Nichtbeachtung der Sicherheitshinweise kann zu Bränden, elektrischen Schlägen und anderen Verletzungen oder Schäden am Gerät oder an anderen Gegenständen führen. Das Gehäuse besteht aus Kunststoff mit empfindlichen elektronischen Bauteilen im Inneren.

Sicherheitshinweise

- Sie dürfen das Gerät nicht durchstechen, zerbrechen, zerquetschen oder zerschneiden.
- Setzen Sie das Gerät nicht einer offenen Flamme oder extrem hohen Temperaturen aus.
- Setzen Sie das Gerät keinen Flüssigkeiten oder extrem niedrigem Luftdruck aus.
- Lassen Sie das Gerät nicht fallen.
- Das Gerät muss recycelt oder getrennt vom Hausmüll entsorgt werden.

6.2 Informationen über gesetzliche Vorschriften und deren Einhaltung

Tabelle 3: Zertifizierung und Konformität

Kurzfristige Lagertemperatur	• -10° C bis 50° C • 90% RH nicht kondensierend	• IEC60068-2-78 (feucht Hitze) • IEC60068-2-1 (kalt)
Betriebstemperatur	• 0° C bis 45° C • 85% RH nicht kondensierend	• IEC60068-2-78 (feucht Hitze) • IEC60068-2-1 (kalt)
Vibration	• 10 bis 75 Hz • 10 m/s²	• IEC60068-2-6
Ablegen	• 1 Meter	• IEC60068-2-31
Emission		• EN55032
Immunität	• 4 kV Kontaktentladungen • 8 kV Luftentladungen • 3 V/m von 80 bis 1000 MHz	• EN55035
Konform mit europäischen Richtlinien		• CE: 89/336/EWG oder 2004/108/EG • RoHS: 2002/95/EG • WEEE: 2002/96/EC
Konform mit der Federal Communications Com-mission	• Ja	

Erklärung zur Übereinstimmung mit der EU-Richtlinie

CE OneSpan NV erklärt, dass dieses DIGIPASS FX7 Gerät den grundlegenden Anforderungen und anderen relevanten Bestimmungen der Richtlinien 2014/53/EU und 2015/863/EU entspricht.

Die vollständige Konformitätserklärung kann angefordert werden

bei: Company: OneSpan NV

Adresse: De Kleetlaan 12A, 1831 Machelen

Belgien E-Mail: legal@onespan.com

FCC-Erklärung

Dieses Gerät erfüllt die Anforderungen von Teil 15 der FCC-Bestimmungen. Der Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Interferenzen verursachen und (2) dieses Gerät muss alle empfangenen Interferenzen akzeptieren, einschließlich Interferenzen, die einen unerwünschten Betrieb verursachen können.

Änderungen oder Modifikationen an diesem Gerät, die nicht ausdrücklich von OneSpan NV genehmigt wurden, können dazu führen, dass die FCC-Zulassung zum Betrieb dieses Geräts erlischt.

IC-Hinweis für Kanada

Dieses Gerät der Klasse B entspricht den kanadischen ICES-003 Anforderungen für Geräte der Informationstechnologie (einschließlich digitaler Geräte). Dieses numerische Gerät der Klasse B entspricht der kanadischen Norm NMB-003.

Dieses Gerät entspricht dem/den lizenzfreien RSS-Standard(s) von Industry Canada. Der Betrieb unterliegt den folgenden zwei Bedingungen: 1) Dieses Gerät darf keine Interferenzen verursachen und 2) dieses Gerät muss alle Interferenzen akzeptieren, einschließlich Interferenzen, die einen unerwünschten Betrieb des Geräts verursachen können.

Das vorliegende Gerät entspricht den für lizenzfreie Funkgeräte geltenden CNR von Industrie Canada. Der Betrieb ist unter den folgenden zwei Bedingungen gestattet: 1) l'appareil ne doit pas produire de brouillage; 2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Korrekte Entsorgung dieses Produkts (Elektro- und Elektronik-Altgeräte)

Anwendbar in der Europäischen Union und anderen europäischen Ländern mit getrennten Sammelsystemen

Diese Kennzeichnung auf dem Produkt oder in der dazugehörigen Literatur weist darauf hin, dass das Produkt am Ende seiner Lebensdauer nicht mit dem Hausmüll entsorgt werden darf. Um mögliche Schäden für die Umwelt oder die menschliche Gesundheit durch unkontrollierte Abfallentsorgung zu vermeiden, trennen Sie dieses Produkt bitte von anderen Abfällen und recyceln Sie es verantwortungsbewusst, um die nachhaltige Wiederverwendung von Materialressourcen zu fördern. Private Nutzer sollten sich entweder an den Hersteller des Produkts oder an ihre örtliche Behörde wenden, um zu erfahren, wo und wie sie den Artikel einem umweltgerechten Recycling zuführen können. Gewerbliche Nutzer sollten sich an ihren Lieferanten wenden und die Bedingungen des Kaufvertrags prüfen. Dieses Produkt darf nicht mit anderen gewerblichen Abfällen vermischt und entsorgt werden.