EPSON

Sicherheitshandbuch

- Für Kunden, die POS-Drucker verwenden -

Inhaltsverzeichnis

1. Einführung 4

2. Grundlegende Sicherheitsrichtlinie von Epson 6

2-1. Grundlegende Richtlinie 6
2-2. Informationen 7
2-3. Unterstützung bei Sicherheitsrisiken 7
2-4. Einhaltung von Codes und Standards 7

3. Vorgehensweise bei der Installation des Produkts 8

3-1. Physischer Schutz für die Produkte 8
3-2. Administratorkennwort 8
3-3. Internetverbindung 9
3-4. WLAN-Netzwerk 10
3-5. Deaktivierung nicht verwendeter Protokolle und Funktionen 10
3-6. Aktualisierung auf die neueste Firm- und Software 10
3-7. Sicherheit beim Verbinden von Peripheriegeräten 10

4. Netzwerksicherheit 12

4-1. TLS-Kommunikation 12
4-2. Steuerung der Berechtigungen und Ausnahmen des Protokolls 13
4-3. IPsec/IP-Filterung 14
4-4. Authentisierung gemäß IEEE 802.1X 15
4-5. SNMP 15
4-6. WLAN-Sicherheit 16
4-7. Bluetooth-Sicherheit 17
4-8. CA-Zertifikat 17

5. Schutz Ihres Produkts 18

5-1. Umgang mit Viren, die vom USB-Speicher übertragen werden 18

6. Drucksicherheit 19

6-1. Sicheres Drucken 19

7. Nutzerdatenschutz 20

7-1. Datenverarbeitung des Produkts 20

7-2. Kennwortverschlüsselung 20
7-3. Abruf von Beleginformationen 20

8. Betriebsbeschränkungen 21

8-1. Kennwortrichtlinie 21
8-2. Audit-Protokoll 21

9. Produktsicherheit 22

9-1. Benachrichtigung über automatische Firmware-Aktualisierung 22
9-2. Schutz vor illegalen Firmware-Aktualisierungen 22
9-3. Erkennung der Infiltration von Malware 22

10. Sicherheitsmaßnahmen bei der Entsorgung Ihres Produkts 23

10-1. Wiederherstellen der Werkseinstellungen 23

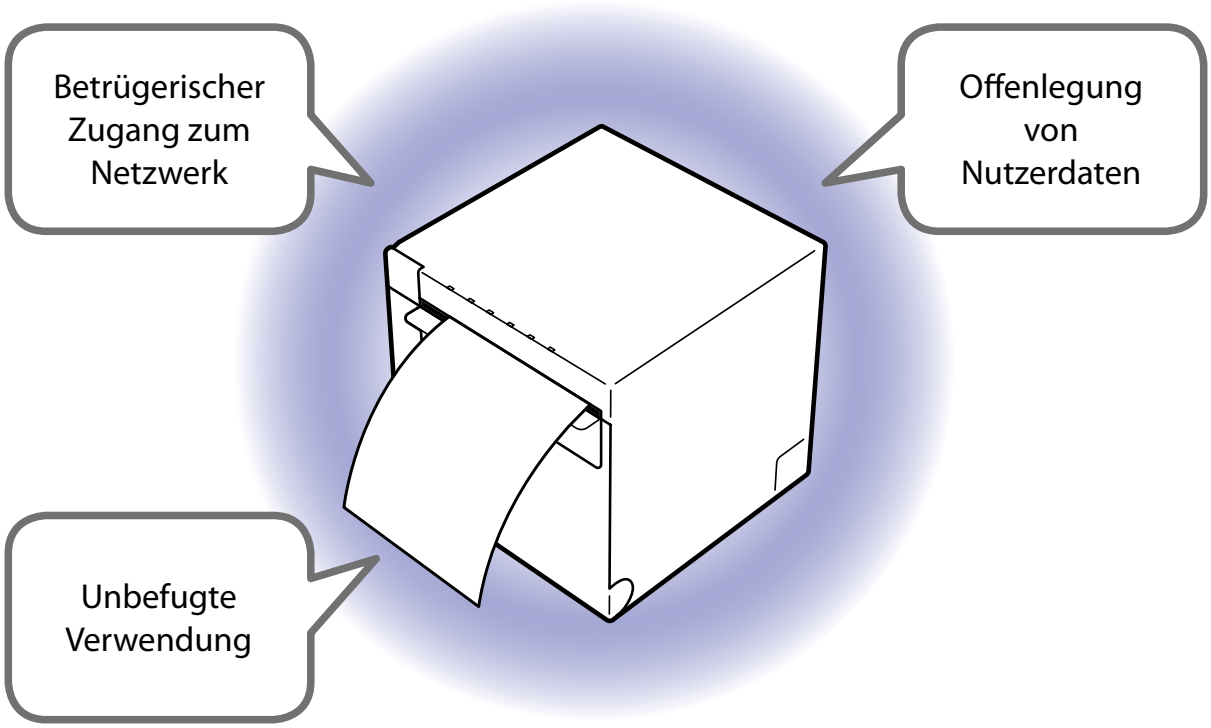
Anhang. 24

1. Einführung

Epson hat die Netzwerkkompatibilität seiner Produkt, um den Kundenkomfort zu erhöhen.

Die zunehmende Raffinesse und Komplexität von Cyberangriffen durch böswillige Dritte stellt eine neue Bedrohung für Netzwerkgeräte dar und hat die Sicherheitsbedenken weiter verstärkt.

Die Produkte von Epson sind mit vielen Merkmalen und Funktionen ausgestattet.
Bei der Verwendung von Computern und Servern sind jedoch eine Reihe von Sicherheitsaspekten zu berücksichtigen, insbesondere bei der Verbindung mit einem Netzwerk und der Nutzung des Netzwerks.



Dieses Handbuch ist eine Einführung in das Sicherheitskonzept von Epson und ein Ratgeber für die Kunden. Es führt Sie durch die verfügbaren Sicherheitsfunktionen.

Die Symbole neben der Funktion im Text haben die folgenden Bedeutungen.

: Sicherheitsfunktionen mit dieser Kennzeichnung sind die minimalen Anforderungen, die vom Administrator eingerichtet werden müssen.

: Sicherheitsfunktionen mit dieser Kennzeichnung dürfen nur vom Administrator konfiguriert werden und stehen den Benutzer in der konfigurierten Sicherheitsumgebung zur Verfügung.

: Sicherheitsfunktionen mit dieser Kennzeichnung können von Administratoren und Benutzern eingerichtet werden.

: Andere Sicherheitsfunktionen. Das sind Sicherheitsmerkmale, die Teil der Spezifikationen und in die Produkte integriert sind.

Lesen Sie in Ihrem Produkthandbuch, wie die Sicherheit eingerichtet wird.

Beachten Sie, dass die Sicherheitsfunktionen und die Einhaltung der in diesem Handbuch beschriebenen Standards je nach Produkt variieren. Bestimmte Produkte haben diese Funktionen möglicherweise nicht oder erfüllen diese Sicherheitsstandards nicht. Beachten Sie daher die separate Liste der Funktionen und Merkmale jedes Produktes.

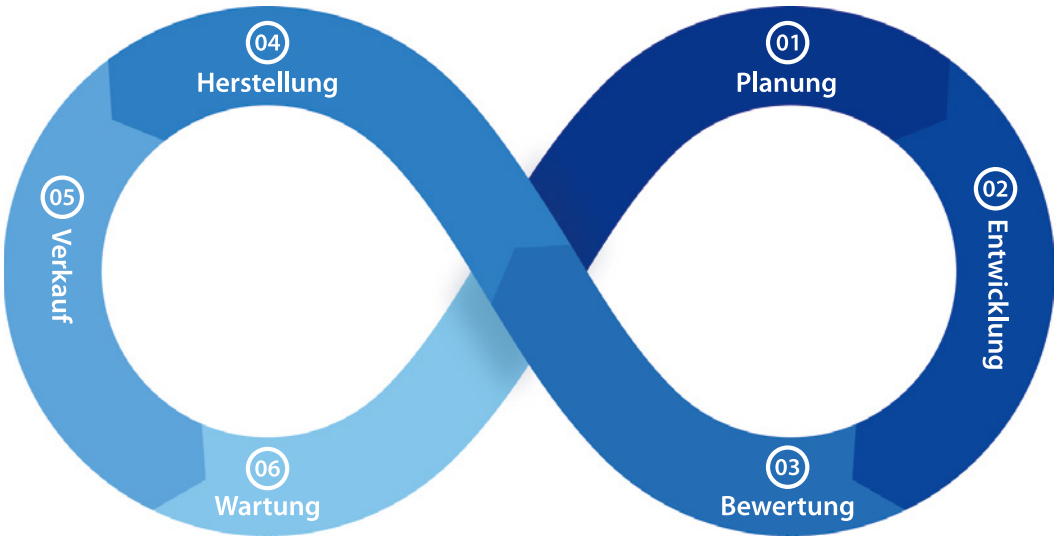
2. Grundlegende Sicherheitsrichtlinie von Epson

Das Herangehen von Epson in Sicherheitsfragen stellt sicher, dass unsere Kunden unsere Produkte sicher und leicht nutzen können.

2-1. Grundlegende Richtlinie

Epson betrachtet die Produktsicherheit als Eckpfeiler der Produktqualität.

Wir praktizieren Produktsicherheit (Endpunkt) im gesamten Produktlebenszyklus, von der Planung und Entwicklung bis zu Bewertung, Herstellung, Verkauf und Wartung und wir überprüfen die Sicherheit der unterschiedlichen Nutzungsumgebungen unserer Produktreihen, damit die Kunden die Produkte unter sicheren Bedingungen verwenden können.



① Planung
In der Produktplanungsphase überwachen wir kontinuierlich die neuesten Sicherheitstrends und potenzielle Sicherheitsrisiken. Wir hören auch auf die Anfragen der Kunden, wenn wir die sicherheitsrelevanten Anforderungen identifizieren und analysieren. Dadurch können wir potenzielle Probleme bei unseren Produkten beseitigen, bevor sich die Risiken materialisieren.

② Entwicklung
Mit den ausgereiften Plattformen und Technologien, die wir für ein breites Spektrums an Produkten, von Büro- und Heimdruckern bis zu gewerblichen und industriellen Druckern für kleine und große Formate, entwickelt haben, sind wir bestrebt, den Schutz vor Sicherheitsrisiken zu verbessern.

③ Bewertung
Zusätzlich zu den umfassenden internen Prüfungen ziehen wir auch externe Organisationen zur objektiven Sicherheitsbewertung hinzu. Wir führen mit unserem strengen Sicherheitsprüfungssystem Bewertungen aus verschiedenen Perspektiven

durch, um die hohe Sicherheit unserer Produkte sicherzustellen.

④ Herstellung
Zur Gewährleistung der hohen Qualität unserer Herstellungsprozesse haben wir in unseren Werken ein umfassendes Informations-Asset-Management implementiert und wir installieren Software, die Funktionalität unserer Produkte ermöglicht.

⑤ Verkauf
Wir unterstützen unsere Kunden beim Planen und Implementieren von Lösungen, die Sicherheitsrisiken in ihren spezifischen Nutzungs- Betriebsumgebungen verringern.
Wir sorgen auch dafür, dass mögliche Sicherheitsrisiken nach der Installation unserer Produkte schnell beseitigt werden.
Wenn Produkte ersetzt oder entsorgt werden müssen, setzen wir die Geräte aus Werkseinstellungen zurück, damit wertvolle vertrauliche Informationen nicht verloren gehen.

⑥ Wartung
Wir reagieren schnell auf sicherheitsrelevante Probleme und Bedenken, die von den Kunden gemeldet werden.

2-2. Informationen

Wir informieren unsere Kunden umfassend und machen sie bewusst auf Sicherheitsfragen aufmerksam.

2-3. Unterstützung bei Sicherheitsrisiken

Wir beseitigen kontinuierlich Sicherheitslücken und Risiken.

- Wir prüfen unsere Produkte mit den branchenüblichen Tools auf Sicherheitslücken, damit alle unsere Produkte frei von Risiken sind.
- Wir verfolgen regelmäßig die Informationen zu Sicherheitsrisiken der Open Source Software, die wir in der Firmware unserer Produkte verwenden.
- Wenn neue Sicherheitsrisiken entdeckt werden, analysieren wir sie und stellen Informationen und Gegenmaßnahmen zur Verfügung.

2-4. Einhaltung von Codes und Standards

Wir sind bestrebt, die Sicherheitsstandards einzuhalten und zu erreichen.

3. Vorgehensweise bei der Installation des Produkts

Der „Administrator“ für die Produkte bezieht sich auf den Produkteigentümer oder einen Nutzer, der einem Eigentümer entspricht. Zur Gewährleistung der Sicherheit sollten Administratoren die erforderlichen Einstellungen gemäß ihrer Nutzungsumgebung vornehmen.

3-1. Physischer Schutz für die Produkte

Der Administrator sollte das Produkt in einer Umgebung installieren, die es vor Modifikation, Zerstörung, Entfernung usw. durch Dritte schützt. Zum Schutz der Kommunikationsdaten sollten Sie zudem Netzwerkgeräte (wie Computer, Router usw.) entsprechend der Sicherheitsrichtlinie der Organisation kaufen und einrichten.

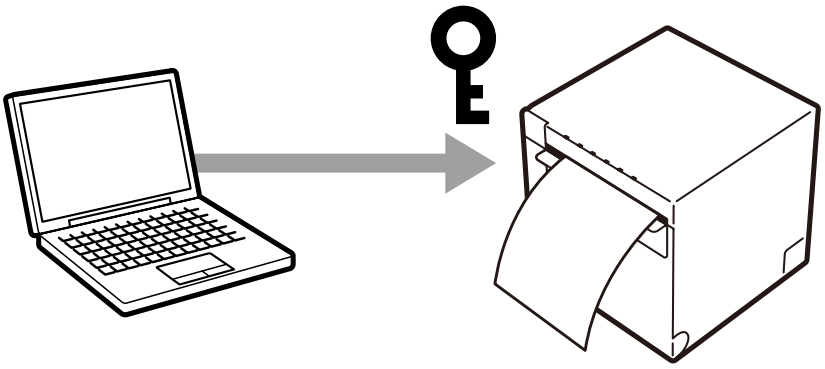
3-2. Administratorkennwort

Wir empfehlen, während der Installation jedes Produkts unbedingt ein Administratorkennwort einzurichten.

Wenn kein Administratorkennwort festgelegt ist oder die Werkseinstellungen des Produkts beibehalten werden, kann auf die allgemeinen Einstellungen oder die Netzwerkeinstellungen, die auf dem Produkt gespeichert sind, illegal zugegriffen oder sie können geändert werden. Es besteht zudem das Risiko, dass Kennwörter oder personenbezogene und vertrauliche Daten nicht geschützt werden.

Das Administratorkennwort sollte eine komplexe Zeichenkette sein, die andere Benutzer oder Gäste schwer erraten können. Sie muss aus acht oder mehr Zeichen bestehen, einschließlich englischer Buchstaben, aber auch Symbole und Zahlen enthalten.
Sie können das Administratorkennwort über verschiedene Tools über das Netzwerk einrichten.

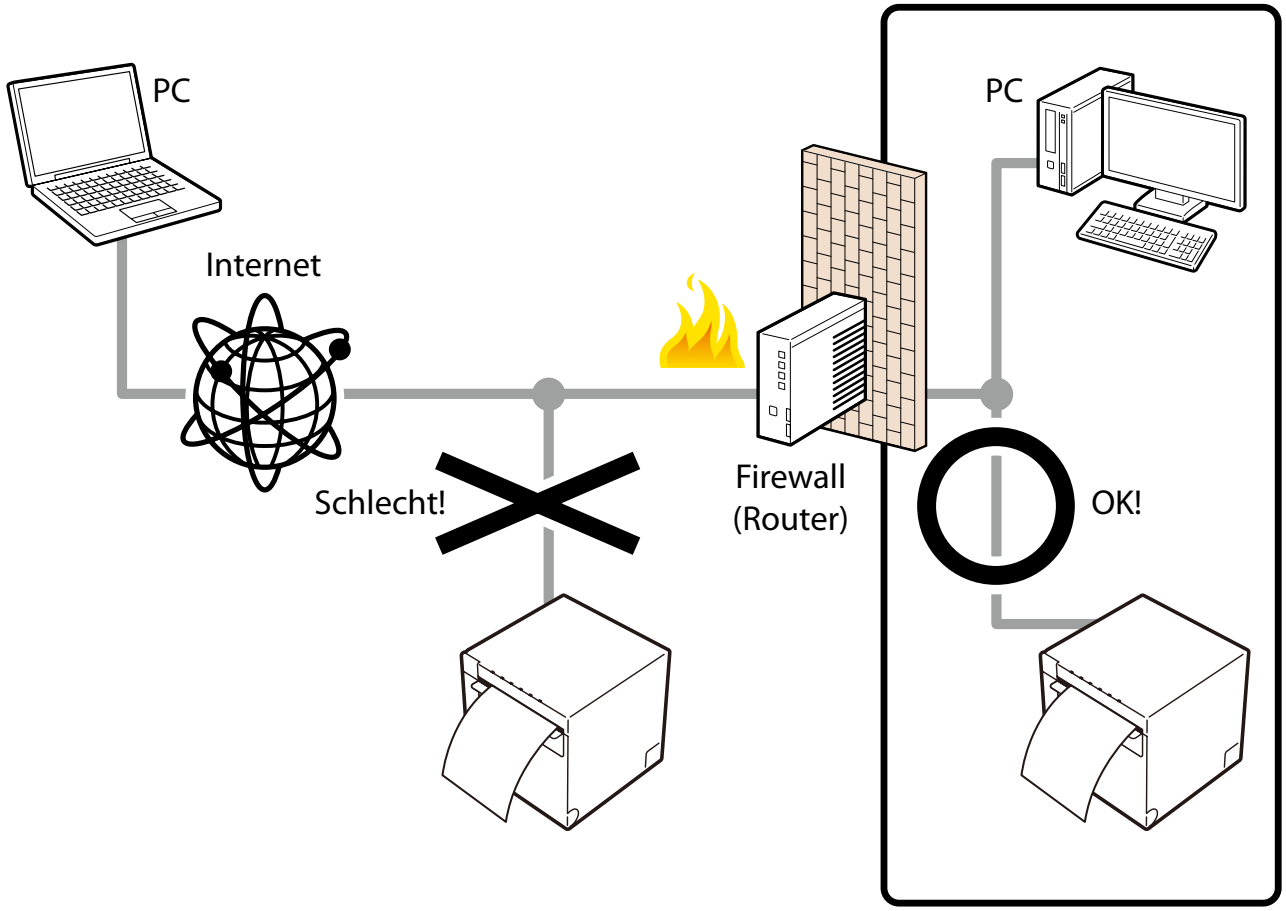
Einige Produkte haben werkseitig eingerichtete, individuelle Passwörter, um die Sicherheit zu erhöhen.



3-3. Internetverbindung

Installieren Sie Produkte in einem Netzwerk, das durch eine Firewall geschützt ist und verbinden Sie sie nicht direkt mit dem Internet. Wir empfehlen die Einrichtung und Verwendung einer privaten IP-Adresse, wenn Sie Produkte verbinden.

Auch wenn Sie das Produkt in einer IPv6-Umgebung verwenden, sollten Sie das Produkt durch eine Firewall oder andere Mittel schützen und den direkten Zugriff auf das Produkt aus dem Internet beschränken oder verhindern.



Sowohl für die Netzwerkfunktionen als auch für das Drucken enthält das Produkt eine Verwaltungsoberfläche z. B. einen Web-Verwaltungsbildschirm (Web Config oder EpsonNet Config (Web-Version)). Trotz der Sicherheitsprüfungen von Epson und unserem Bemühen, risikofreie Produkte zu liefern, birgt die direkte Verbindung zum Internet unerwartete Sicherheitsrisiken für das Kundennetzwerk und die Netzwerkgeräte z. B. durch unbefugte Bedienung und Datenverluste.

3-4. WLAN-Netzwerk

Nehmen Sie die entsprechenden Sicherheitseinstellungen für das WLAN-Netzwerk vor, wenn Sie WLAN nutzen.

Der Vorteil von WLAN ist, dass Sie sich mühelos über das Netzwerk mit dem Produkt verbinden und mit dem Computer oder Smartphone kommunizieren können, wenn Sie sich in Signalreichweite befinden. Andererseits können Probleme auftreten, die durch böswillige Drittparteien verursacht werden, wenn die Sicherheit nicht ordnungsgemäß eingerichtet wird.

- Persönliche Informationen wie z. B. Druckdaten und Kennwort können von anderen eingesehen oder abgefangen werden.
- Inhalte der Kommunikation werden möglicherweise in betrügerischer Absicht überschrieben (falsifiziert).
- Angreifer können sich als bestimmte Nutzer und Geräte ausgeben und die gestohlene Identität zur Kommunikation nutzen.

Siehe Produkthandbuch zu den Verfahren der WLAN-Einrichtung.

3-5. Deaktivierung nicht verwendeter Protokolle und Funktionen

Deaktivieren Sie Protokolle und Funktionen, die nicht verwendet werden.

Protokolle und Funktionen können individuell zugelassen oder verboten werden. Dadurch vermeiden Sie Risiken, falls sie unbeabsichtigt verwendet werden.

3-6. Aktualisierung auf die neueste Firm- und Software

Wir stellen bei Bedarf die neueste Firm- und Software bereit. Aktualisieren Sie auf die neueste Firm- und Software für Ihr Produkt.

Mit der neuesten Firm- und Software erhalten Sie nicht nur zusätzliche Funktionen, sondern es werden auch Mängel und Sicherheitsrisiken behoben. Weitere Informationen zur Firmware oder Software finden Sie im Änderungsverlauf der Firmware und Software.

3-7. Sicherheit beim Verbinden von Peripheriegeräten

Sie können die folgenden Peripheriegeräte mit dem Produkt verbinden. Verwenden Sie hochsichere Einstellungen für die Verbindung. Die vom Produkt unterstützte Peripherie können Sie der Produktanleitung entnehmen.

- Optionales WLAN-Gerät
- Geldwechsler
- Kreditautorisierungsterminal
- Magnetstreifenleser (MSR)

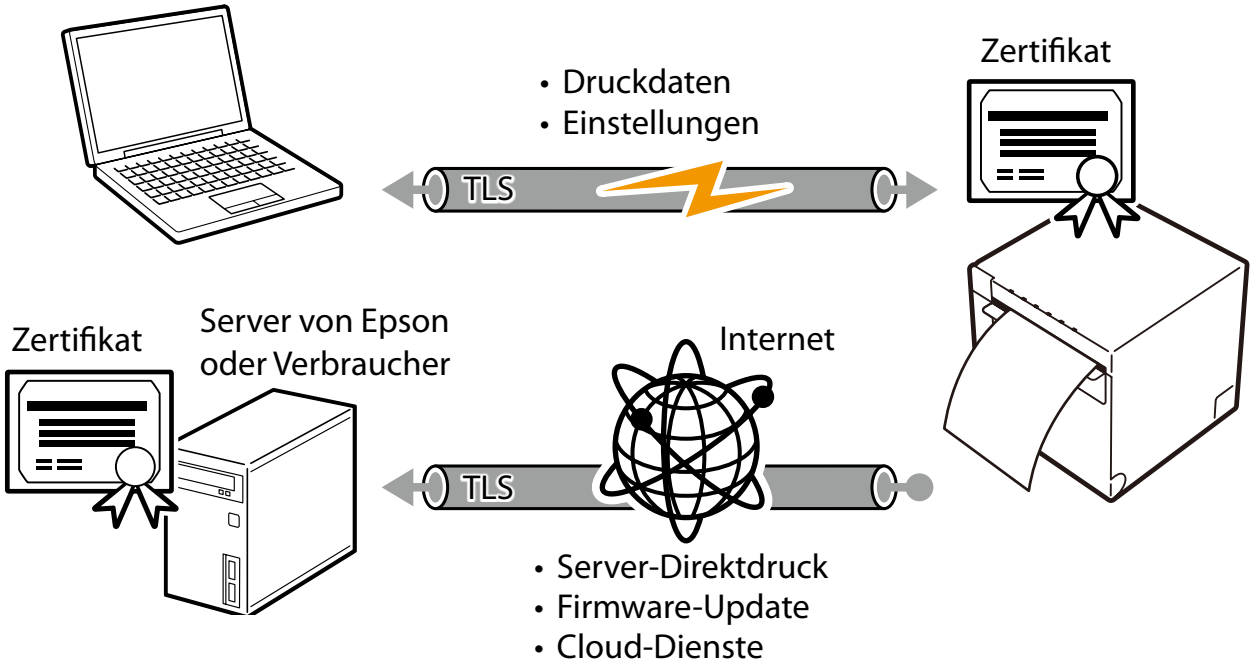
- Strichcode-Scanner
- Optionales Kundendisplay
- Tastatur
- Kassenschublade
- Optionaler externer Summer
- Kartenleser

4. Netzwerksicherheit

4-1. TLS-Kommunikation

Übertragungen sind durch TLS geschützt, deshalb können Sie die Offenlegung von Einstellungsinformationen und Inhalten beim Drucken von Daten verhindern, wenn Sie das Produkt oder den Druck über ein Netzwerk konfigurieren. Sie können auch verhindern, dass Informationen an nicht autorisierte Geräte gesendet werden. Verwenden Sie die Servervalidierungsfunktion, importieren Sie das CA-signierte Zertifikat und verwenden Sie die Public-Key-Infrastruktur (PKI). Die konfigurierte Verschlüsselungsstärke ermöglicht einen sichereren Verschlüsselungsalgorithmus. Sie sind auch durch TLS geschützt, wenn Sie mit dem Produkt für Server-Direktdruck, Firmware-Aktualisierungen und Cloud-Dienste auf den Epson-Server im Internet zugreifen. Sie können über das Internet das Produkt sicher konfigurieren und drucken, indem Sie Kommunikationsinhalte verschlüsseln und Authentifizierungen durchführen. Durch Verifizierung, dass Clients und Drucker vertrauenswürdig sind, können Sie verhindern, dass Daten an unautorisierte Geräte gesendet werden. Wir empfehlen die Verwendung von Einstellungen, die Sicherheitsrisiken reduzieren.

Wenn Sie Ihren eigenen Server aufbauen, prüfen Sie vor der Einrichtung „4-8. CA-Zertifikat".



Sie können die Version- und die Verschlüsselungsstärke des verwendeten TLS auswählen.

Unterstützte TLS-Versionen und Verschlüsselungsstärken: Je weiter oben sich der Eintrag in der Liste befindet, desto geringer ist das Sicherheitsrisiko.

TLS-Version

- TLS1.3

- TLS1.2
- TLS1.1

Verschlüsselungsstärke

Die Optionen variieren je nach Produkt.

- 256 bit
- 192 bit
- 128 bit
- 112 bit
- 80 bit

oder

- Hoch (AES256)
- Mittel (AES256, 3DES)
- Gering (AES256, AES128, 3DES)

4-2. Steuerung der Berechtigungen und Ausnahmen des Protokolls

Das Produkt kommuniziert beim Erkennen, Drucken, Abrufen von Informationen und Konfigurieren über verschiedene Protokolle. Sie können individuelle Berechtigungen und Verbote für jedes Protokoll einrichten, um Sicherheitsrisiken durch versehentliche Verwendung zu vermeiden.

Im „Anhang“ finden Sie Informationen zu den Sicherheitsrisiken, wenn Protokolle und Funktionen aktiviert sind, und zu den Einschränkungen, wenn sie deaktiviert sind.

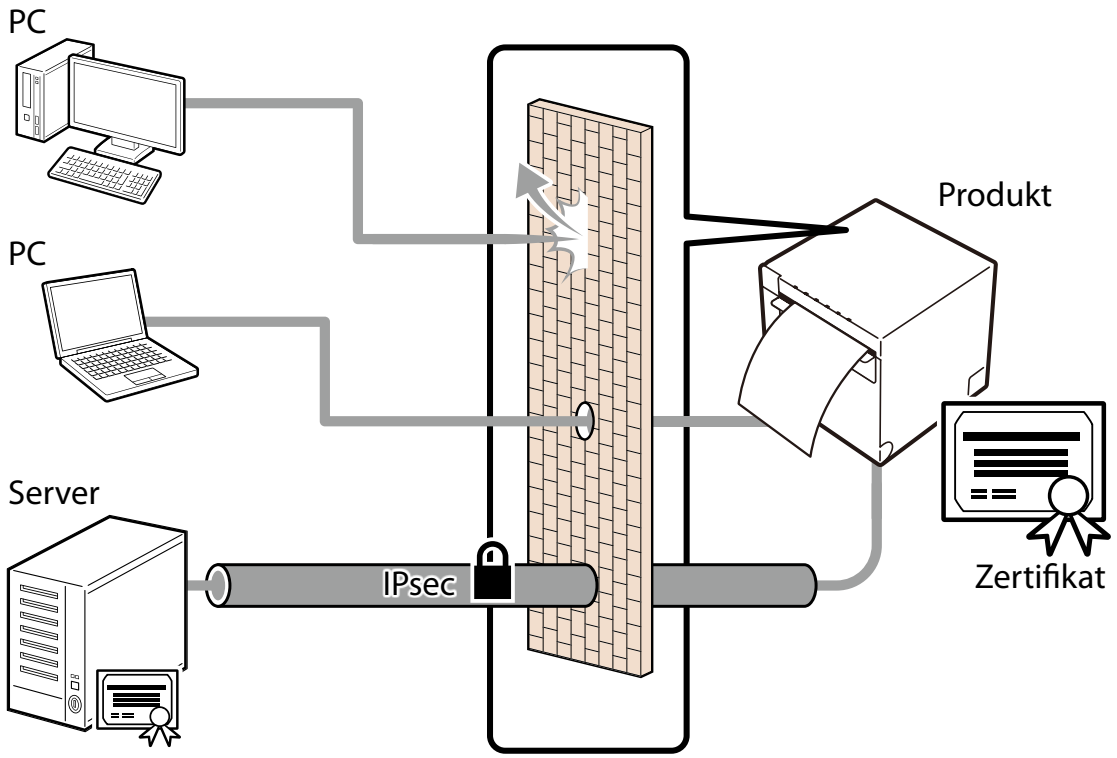
Protokolle und Funktionen können wie folgt erlaubt oder verboten werden.

- APIPA
- Bonjour
- BOOTP
- ePOS-Device
- ePOS-Print
- LLTD
- LLMNR
- LPR
- RAW (Port9100/Angepasster Port)
- SLP
- SNMP
- SSL/TLS

4-3. IPsec/IP-Filterung

Sie können IP-Adressen, Diensttypen, die Portnummern für Empfang und Übertragung usw. mit der Funktion IPsec/IP-Filterung filtern. Je nach Kombination dieser Filter können Sie festlegen, ob Daten eines spezifischen Kunden akzeptiert oder blockiert werden und spezifische Datentypen blockieren. Auf ähnliche Weise können Sie mit höherer Sicherheit kommunizieren, wenn Sie mithilfe von IPsec Schutzmechanismen kombinieren.

Auch unsichere Druckprotokolle werden geschützt, denn der Schutz in IP-Paketeinheiten (Verschlüsselung und Zertifizierung) ist Teil des Schutzes durch IPsec. Vorinstallierte Schlüssel und Zertifikate werden von der IPsec-Authentisierungsmethode unterstützt.



Folgende Algorithmen und Schlüsselaustauschmethoden werden unterstützt. Je weiter oben sich der Eintrag in der Liste befindet, desto geringer ist das Sicherheitsrisiko.

Schlüsselaustauschmethode

- IKEv2
- IKEv1

ESP Verschlüsselungsalgorithmus

- AES-GCM-256
- AES-GCM-192
- AES-GCM-128
- AES-CBC-256
- AES-CBC-192
- AES-CBC-128

- 3DES

ESP/AH Verschlüsselungsalgorithmus

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5

Die grundlegende Richtlinie gilt für alle Nutzer, die auf das Produkt zugreifen. Legen Sie individuelle Richtlinien zur Zugangssteuerung gemäß Ihren spezifischen Bedürfnissen fest.

4-4. Authentisierung gemäß IEEE 802.1X

IEEE 802.1X* ist ein Standard für die Zugangssteuerung an jedem einzelnen Port des Netzwerkgeräts. IEEE 802.1X*-Netzwerke bestehen aus RADIUS-Servern (Authentisierungsserver) und Schaltknoten, die eine Authentisierungsfunktion haben.

Die Produkte von Epson entsprechen IEEE 802.1X* und können mit einer Netzwerkumgebung verbunden werden, die vertrauliche Daten enthält. Prüfen Sie bei Verwendung dieser Funktion auch „4-8. CA-Zertifikat".

* Je nach Produkt könnte sie als WPA2-Enterprise oder WPA3-Enterprise angezeigt werden.

Unterstützte Authentisierungsmethoden und Verschlüsselungsstärken: Je weiter oben sich der Eintrag in der Liste befindet, desto geringer ist das Sicherheitsrisiko.

Authentisierungsmethode

- EAP-TLS
- PEAP-TLS
- EAP-TTLS
- PEAP/MSCHAPv2

Verschlüsselungsstärke

- Hoch (AES256, 3DES)
- Mittel (AES256, AES128, 3DES, RC4)

4-5. SNMP

SNMP ist ein Protokoll zur Überwachung des Status und zur Änderung der Einstellungen von unterstützten Geräten und Verwaltungstools.

SNMPv1 und SNMPv2c unterstützen die Verschlüsselung der Kommunikation nicht und

müssen innerhalb eines mit einer Firewall oder anders geschützten verwendet werden. Doch selbst bei Verwendung von SNMPv1 oder SNMPv2c erfolgt die Kommunikation durch Authentifizierung und Verschlüsselung bei Überwachung des Status hochgradig vertraulicher Informationen oder bei der Änderung von Einstellungen.

SNMPv3 kann zur Authentisierung und Verschlüsselung der SNMP-Kommunikation (Pakete) für die Überwachung des Produktstatus und die Konfiguration von Änderungen über kompatible Geräteverwaltungsprogramme verwendet werden.

Dadurch wird die Vertraulichkeit sichergestellt, wenn Sie Einstellungen ändern oder den Status über das Netzwerk überwachen.

SNMPv3 unterstützt die folgenden Authentisierungs- und Verschlüsselungsalgorithmen. Je weiter oben sich der Eintrag in der Liste befindet, desto geringer ist das Sicherheitsrisiko.

Authentisierungsalgorithmen von SNMPv3

- SHA-512 (nur in Europa, im Nahen Osten und in Afrika unterstützt)
- SHA-384 (nur in Europa, im Nahen Osten und in Afrika unterstützt)
- SHA-256 (nur in Europa, im Nahen Osten und in Afrika unterstützt)
- SHA-224 (nur in Europa, im Nahen Osten und in Afrika unterstützt)
- SHA-1
- MD5

Verschlüsselungsalgorithmen von SNMPv3

- AES128
- DES

4-6. WLAN-Sicherheit

Die unterstützten WLAN- (Wireless LAN) Authentifizierungs- und Verschlüsselungstechnologien sind wie folgt. Je weiter oben sich der Eintrag in der Liste befindet, desto geringer ist das Sicherheitsrisiko.

- WPA3-Enterprise
- WPA3-SAE
- WPA2-Enterprise
- WPA2-Personal
- WPA2-PSK
- WPA-PSK(AES)
- WPA-PSK
- WEP

WPA2/WPA3-Enterprise unterstützt die folgenden EAP-Methoden.

- EAP-TLS
- PEAP-TLS

- EAP-TTLS
- PEAP-MSCHAPv2

4-7. Bluetooth-Sicherheit

Sie können über die Bluetooth-Schnittstelle konfigurieren und drucken.

Wenn Sie Bluetooth Classic verwenden, wird die folgende Authentifizierung und Verschlüsselung verwendet.

- Europa, Naher Osten und Afrika:
  Einstellungsänderungen erfordern Authentifizierung und werden mit AES verschlüsselt. Druck wird ebenfalls mit AES verschlüsselt.
- Außerhalb von Europa, Nahem Osten und Afrika:
  Einstellungsänderungen erfordern Authentifizierung und werden mit E0 verschlüsselt. Druck wird ebenfalls mit E0 verschlüsselt.

Wenn Sie Bluetooth Low Energy nutzen, werden die folgenden Verschlüsselungstechnologien unterstützt. Je weiter oben sich der Eintrag in der Liste befindet, desto geringer ist das Sicherheitsrisiko.

- Sichere LE-Verbindungen (Druck mit AES-Verschlüsselung)
- Hoch (Druck mit AES-Verschlüsselung)
- Mittel (Druck ohne Verschlüsselung)
- Gering (Druck ohne Verschlüsselung)

Der Kopplungsmodus ändert sich ebenfalls entsprechend den Sicherheitseinstellungen. Einzelheiten finden Sie in der Produktanleitung.

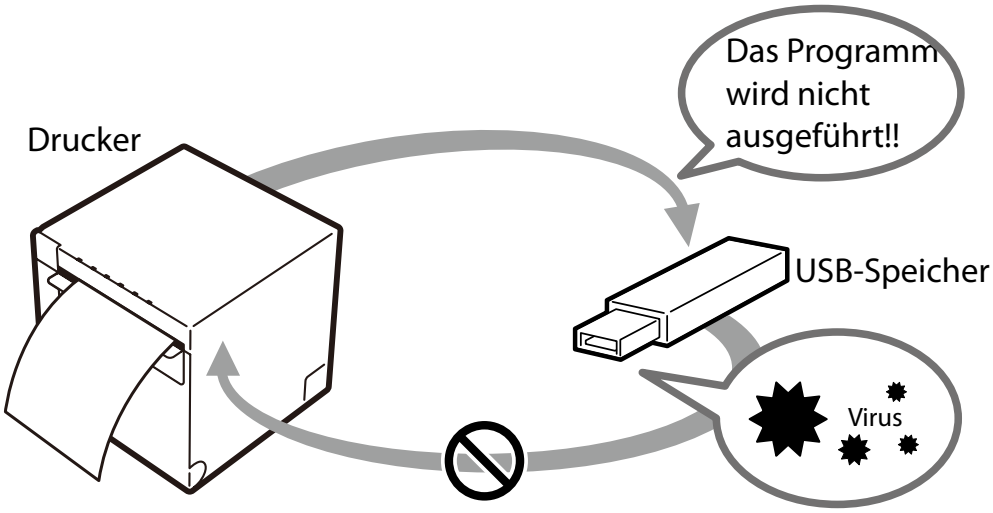
4-8. CA-Zertifikat

Ein CA- (Certificate Authority) Zertifikat ist ein von einer CA- ausgestelltes digitales Zertifikat. Das Produkt hält ein Root-Zertifikat und kann mit Servern kommunizieren (bspw. Server-Direktdruck, Statusbenachrichtigungsfunktion und Authentisierungsserver). Wenn Sie sicher mit einem Server über ein Serverzertifikat, dessen Zuverlässigkeit nicht verifiziert werden kann, wie ein angepasstes CA-Zertifikat, kommunizieren möchten, können Sie zur Verifizierung des Servers ein CA-Zertifikat hinzufügen.

5. Schutz Ihres Produkts

5-1. Umgang mit Viren, die vom USB-Speicher übertragen werden

Es gibt keine ausführbaren Funktionen auf USB-Speichern für Epson-Produkte, deshalb besteht keine Gefahr, dass das Produkt über einen USB-Speicher mit Viren infiziert wird.



6. Drucksicherheit

6-1. Sicheres Drucken

Wenn Sie den Druckkommunikationspfad sichern möchten, können Sie die folgenden Protokolle nutzen. Wenn Sie die sichere Druckfunktion deaktivieren, können Druckdaten von einem Dritten gelesen werden.

- HTTPS-Kommunikation durch TLS geschützt
- Kommunikation über den TCP-Port (8143/8043/TCPS) für durch TLS geschütztes ePOS-Device
- Bluetooth-Kommunikation durch AES-Verschlüsselung geschützt

7. Nutzerdatenschutz

7-1. Datenverarbeitung des Produkts

Druckdaten werden temporär auf einem Produkt gespeichert. Anschließend werden Sie gelöscht, wenn ein Auftrag abgeschlossen, der nächste Auftrag gestartet oder das Produkt abgeschaltet wird.

7-2. Kennwortverschlüsselung

Sie können ein Administratorkennwort verschlüsseln, das im Produkt gespeichert wird.

7-3. Abruf von Beleginformationen

Modelle mit einer Funktion zum Abrufen von Beleginformationen können Belegdaten an einen Server senden. Wenn eine Übertragung an den Server aufgrund einer Netzwerktrennung oder aus anderen Gründen fehlschlägt, werden die Belegdaten im Drucker gespeichert und bei erfolgreicher Übertragung gelöscht. Da Daten werden an einem Ort gespeichert, an dem nicht von außerhalb auf sie zugegriffen werden kann, sodass keine Gefahr von Datenlecks besteht.

8. Betriebsbeschränkungen

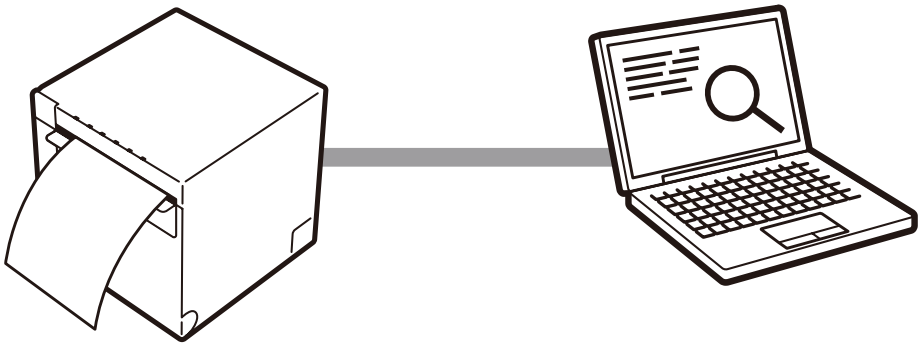
8-1. Kennwortrichtlinie

Sie können das Risiko von Datenlecks reduzieren, indem Sie die Administratorkennwortrichtlinie auf ein Minimum von acht Zeichen und die Einbeziehung von alphanumerischen Buchstaben (Groß- und Kleinbuchstaben) und Symbolen festlegen.

8-2. Audit-Protokoll

Sie können Elemente, wie Druckverläufe, Kundendisplay-Informationen, Versanddaten an Cloud-Dienste und Einstellungsänderungen, als Audit-Protokolle aufzeichnen. Mit der regelmäßigen Bestätigung dieses Protokolls können Fehlbedienungen früher erkannt und Sicherheitsprobleme aufgespürt werden.

Es werden bis zu 2.400 Audit-Protokolle aufbewahrt.



9. Produktsicherheit

9-1. Benachrichtigung über automatische Firmware-Aktualisierung

Wenn Benachrichtigungen über automatische Firmware-Aktualisierungen aktiviert sind, können Sie automatisch die Verfügbarkeit der neuesten Firmware zum jeweiligen Zeitpunkt prüfen. Sie können entscheiden, ob eine Firmware-Aktualisierung erforderlich ist, und je nach Bedarf auf die neueste Firmware aktualisieren.

9-2. Schutz vor illegalen Firmware-Aktualisierungen

Bei der Firmware-Aktualisierung wird eine Authentisierung mit Administratorkennwort durchgeführt. Die Datenkommunikation mit dem Produkt wird bei kabelgebundener LAN- und WLAN-Kommunikation über HTTPS und bei Bluetooth-Kommunikation über AES-Verschlüsselung geschützt. Zudem wird ihre Authentizität vor dem Neuschreiben der Firmware durch eine Signatur verifiziert. Dadurch wird die unbefugte Veränderung der Firmware durch böswillige Drittparteien verhindert.

9-3. Erkennung der Infiltration von Malware

Das Produkt wird ständig auf Infiltration von Malware in die Firmware überwacht, während das Produkt ausgeführt wird. Wenn Malware entdeckt wird, wird das Produkt neu gestartet, um Malware zu beseitigen.

10. Sicherheitsmaßnahmen bei der Entsorgung Ihres Produkts

10-1. Wiederherstellen der Werkseinstellungen

Wenn Sie ein Produkt übertragen oder entsorgen, können Sie alle Einstellungen und im Produkt gespeicherten Daten auf Werkseinstellungen (Initialisierung) zurücksetzen, um die Offenlegung vertraulicher Informationen zu verhindern. Verfahren zur Initialisierung finden Sie in der Produktanleitung.

Sicherheitsrisiken, wenn Protokoll-/Sicherheitsfunktionen aktiviert sind (Auswirkung auf Schutz personenbezogener Daten, unautorisierte Vorgänge), und Beschränkungen, wenn sie deaktiviert sind

Administratoren sollte sich vor der Konfiguration mit den Risiken und Beschränkungen vertraut machen.

Protokoll/ Sicherheitsfunktio-nen	Sicherheitsrisiken bei Aktivierung	Beschränkungen bei Deaktivierung
APIPA	Es gibt kein Sicherheitsrisiko.	IP-Adresseinstellung mit APIPA ist nicht möglich.
Bonjour	Es besteht die Möglichkeit, dass Informationen auf den Geräten im Netzwerk von Dritten gelesen werden.	Die Suche über Bonjour ist auf dem Computer nicht möglich.
BOOTP	Es besteht die Möglichkeit, dass eine falsche IP-Adresse zugewiesen werden kann.	IP-Adresseinstellung mit BOOTP ist nicht möglich.
LLTD	Es besteht die Möglichkeit, dass Informationen auf den Geräten im Netzwerk von Dritten gelesen werden.	Die Geräte werden in Windows in „Geräte und Drucker“ nicht angezeigt.
LLMNR	Es besteht die Möglichkeit, dass Informationen auf den Geräten im Netzwerk von Dritten gelesen werden.	Die Suche mit LLMNR ist auf dem Computer nicht möglich.
LPR	Die Kommunikation ist nicht verschlüsselt und es besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können.	Es kann nicht mit LPR gedruckt werden.
RAW (Port 9100/ angepasster Port)	Die Kommunikation ist nicht verschlüsselt und es besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können.	Es kann nicht über RAW-Port gedruckt werden. Wenn angepasster Port deaktiviert ist, sind Druckfunktionen mit ePOS-Print und ePOS-Device nicht möglich.
SLP	Da der Absender nicht authentifiziert ist, Es kann ein gefälschter Absender für einen Angriff genutzt werden, um den Dienst zu deaktivieren, weil der Absender nicht authentisiert ist.	Es ist dem Computer nicht möglich, über SLP Informationen vom Gerät abzurufen bzw. das Gerät zu erkennen.

Protokoll/ Sicherheitsfunktionen	Sicherheitsrisiken bei Aktivierung	Beschränkungen bei Deaktivierung
SNMP	Da Kommunikation bei Verwendung von SNMPv1 und SNMPv2c nicht verschlüsselt ist, besteht die Möglichkeit, dass Geräteinformationen und Einstellungsdaten von einem Dritten gelesen werden können (hochgradig vertrauliche Kommunikation wird jedoch in SNMPv1 und SNMPv2c verschlüsselt). Risiken werden durch SNMPv3 reduziert. Das Risiko steigt jedoch bei der Verwendung von Authentifizierungsalgorithmen oder Verschlüsselungsalgorithmen mit geringer Verschlüsselungsstärke.	Die Verwaltungstools, die SNMP verwenden, können nicht verwendet werden. Außerdem sind die von Epson bereitgestellten Verwaltungstools und Anwendungen nicht verfügbar.
SSL/TLS	Risiken werden durch SSL/TLS reduziert. Wenn jedoch eine geringe Verschlüsselungsstärke oder alte TLS-Versionen verwendet werden, besteht die Möglichkeit, dass ausgedruckte Daten gelesen werden können. Wenn ein selbst signiertes Zertifikat verwendet wird, besteht die Möglichkeit, dass Geräteinformationen und Einstellungsdaten von Dritten gelesen werden können.	Druck ist mit einem alten Betriebssystem nicht möglich. Zudem ist die Nutzung von Web Config oder EpsonNet Config (Web-Version) nicht möglich.
CA-Zertifikat	Risiken werden durch Einstellung des CA-Zertifikats eines anderen Servers reduziert. Wenn jedoch kein vertrauenswürdiges CA-Zertifikat verwendet wird, besteht die Möglichkeit, dass ausgedruckte Daten, Geräteinformationen und Einstellungsdaten von einem Dritten gelesen werden können.	Die Verwendung des CA-Zertifikats eines anderen Servers ist nicht möglich.
IPsec	Risiken werden durch IPsec reduziert. Wenn jedoch eine schwache Authentifizierung, Verschlüsselungsstärke oder kein Zertifikat verwendet wird, können Geräteinformationen und Einstellungsdaten von einem Dritten gelesen werden.	Kommunikation mit IPsec ist nicht möglich.

Protokoll/ Sicherheitsfunktio-nen	Sicherheitsrisiken bei Aktivierung	Beschränkungen bei Deaktivierung
IEEE 802.1X	Risiken werden durch IEEE 802.1X reduziert. Wenn jedoch eine schwache Authentifizierung, Verschlüsselungsstärke oder kein Zertifikat verwendet wird, können ausgedruckte Daten, Geräteinformationen und Einstellungsdaten von einem Dritten gelesen werden.	Nicht registrierte Dritte können dem Netzwerk beitreten.
Bluetooth	Wenn Sicherheit auf niedrigem Niveau verwendet wird, besteht die Möglichkeit, dass Geräteinformationen und Einstellungsdaten von Dritten gelesen werden können.	Kommunikation mit Bluetooth ist nicht möglich.
ePOS-Print, ePOS-Device	Das Risiko wird durch den Einsatz verschlüsselter Protokolle/Ports reduziert. Wenn jedoch nicht verschlüsselte Protokolle/Ports verwendet werden, besteht die Möglichkeit, dass ausgedruckte Daten und Steuerungsbefehle an Peripheriegeräte von einem Dritten gelesen werden können.	Steuerung von Druck und Peripheriegerät mit ePOS-Print und ePOS-Device ist nicht möglich.
Benachrichtigung über automatische Firmware-Aktualisierung	Es gibt kein Sicherheitsrisiko.	Eine Aktualisierung auf verbesserte Firmware zur Handhabung von Problemen, wie Adressierungsschwachstellen, ist nicht möglich.

EPSON

Vorsicht

- Dieses Dokument und Teile dieses Dokuments dürfen nicht vervielfältigt werden.
- Der Inhalte dieses Dokuments kann sich ohne vorherige Ankündigung künftig ändern.
- Diese Dokument dient nur internen Zwecke. Lesen Sie das Handbuch jedes einzelnen Produkts zu den Details der Verwendung.

Markennachweis

- Microsoft and Windows are trademark of the Microsoft group of companies.
- Apple, Bonjour, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Seiko Epson Corporation is under license.
- Wi-Fi® is trademarks of Wi-Fi Alliance®.
- Alle andere Marken sind das Eigentum ihrer jeweiligen Inhaber und werden nur zu Identifizierungszwecken verwendet.

NPD7629-00 DE
©2025 Seiko Epson Corporation