

ICS 35.030; 35.240.95

**Informationstechnik –  
IoT-fähige Geräte –  
Mindestanforderungen zur Informationssicherheit**

Information Technology –  
IoT capable devices –  
Minimum requirements for Information security

Technologies de l'information –  
Appareils compatibles avec l'IoT –  
Exigences minimales de sécurité de l'information

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:  
Das vorliegende Dokument wurde nach den Verfahrensregeln einer Vornorm erstellt.

Gesamtumfang 16 Seiten

Inhalt

|                                                                         | Seite |
|-------------------------------------------------------------------------|-------|
| Vorwort .....                                                           | 3     |
| 1    Anwendungsbereich .....                                            | 4     |
| 2    Normative Verweisungen .....                                       | 4     |
| 3    Begriffe .....                                                     | 5     |
| 4    Anforderungen .....                                                | 8     |
| 4.1   Allgemeines .....                                                 | 8     |
| 4.2   Sicherheitsarchitektur .....                                      | 9     |
| 4.3   Konfiguration.....                                                | 10    |
| 4.4   Kommunikation .....                                               | 11    |
| 4.5   Update.....                                                       | 13    |
| Anhang A (informativ) Übersicht der Anforderungen und Empfehlungen..... | 14    |
| Literaturhinweise.....                                                  | 16    |

## Vorwort

Dieses Dokument wurde vom Arbeitsausschuss NA 043-01-41-01 AK „Security by Design Anforderungen für IoT-Geräte im Small Business/Home Umfeld“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) erarbeitet.

DIN SPEC sind nicht Bestandteil des Deutschen Normenwerks.

Eine DIN SPEC nach dem Vornorm-Verfahren ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden DIN SPEC wurde kein Entwurf veröffentlicht.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Erfahrungen mit dieser DIN SPEC sind erbeten.

- vorzugsweise als Datei per E-Mail an [nia@din.de](mailto:nia@din.de) in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter <http://www.din.de/de/mitwirken/norm-entwurfs-portal> abgerufen werden;
- oder in Papierform an Normungsausschuss Informationstechnik und Anwendungen im DIN Deutsches Institut für Normung e. V., 10772 Berlin (Hausanschrift: Burggrafenstraße 6, 10787 Berlin).

## 1 Anwendungsbereich

Diese Spezifikation legt generische Mindestanforderungen an vernetzungsfähige Geräte, sogenannte Internet of Things (IoT)-Geräte, fest. Dabei wird ein Basissicherheitsniveau adressiert, das gegen elementare Angriffe auf grundlegende Designschwächen (wie Verwendung von Standardpasswörtern) schützen soll. Dabei soll der Schutz der bereitgestellten Informationen sowie der zuverlässige Betrieb des IoT-Geräts sichergestellt werden. Dieses Dokument betrachtet ausschließlich die IT-Sicherheit (security) eines IoT-Gerätes. Es werden keine Aspekte der funktionalen Sicherheit (safety) adressiert.

Die in diesem Dokument benannten Anforderungen richten sich grundsätzlich an IoT-Geräte aus dem Consumer-Bereich (Small Business/Home Umfeld) und sind anwendungsunabhängig. Diese Spezifikation definiert Mindestanforderungen an grundlegende IT-Sicherheitseigenschaften von IoT-Geräten, die bei deren Konzeption berücksichtigt werden sollen (Security-by-Design). Je nach Funktionalität des Gerätes und dem zugehörigen Anwendungsbereich müssen ggf. zusätzliche IT-Sicherheitsanforderungen an das IoT-Gerät vom Hersteller umgesetzt werden.

Ein IoT-Gerät ist häufig keine Stand-Alone Lösung, sondern ist in ein IoT-Ökosystem eingebunden. Die IT-Sicherheit folgender Komponenten des IoT-Ökosystems, die mit dem IoT-Gerät in Verbindung stehen, werden in diesem Dokument nicht betrachtet:

- Zugehörige Services zum IoT-Gerät
- Apps, die mit dem IoT-Gerät bzw. den zugehörigen Services kommunizieren
- Desktop-Software zu dem IoT-Gerät
- Benutzer Software, die nach Inbetriebnahme vom Nutzer auf das IoT-Gerät geladen wird
- Non-IP Kommunikationsschnittstellen des IoT-Gerätes.

Entsprechend betrachtet diese DIN SPEC nicht das komplette IoT-Ökosystem, in dem das IoT-Gerät betrieben wird, auch wenn eine übergreifende IT-Sicherheitsbetrachtung des gesamten IoT-Ökosystem zur Beurteilung der ganzheitlichen IT-Sicherheit von zentraler Bedeutung ist. Darüber hinaus wird die nachträgliche Installation von Software, die nicht Teil der Updatefunktionalität des IoT-Geräts ist nicht betrachtet. Dazu gehört z. B. die Installation von Apps durch den Nutzer nach Inbetriebnahme. Ebenso werden Sicherheitsanforderungen zum Schutz von geistigem Eigentum nicht berücksichtigt. Fokus dieser Spezifikation ist die Absicherung der IP-basierten Kommunikation eines IoT-Gerätes und die dahinterliegende Architektur. Dabei sollen die Geräte insbesondere gegen skalierbare Cyberangriffe aus dem Internet geschützt werden, z. B. Angriffe durch die Schadsoftware Mirai. An den nicht netzwerkbasieren Zugriff auf ein IoT-Gerät über ein lokales Interface, wie eine Taste oder ein Tastbildschirm, werden in diesem Dokument keine Anforderungen definiert. Hierzu wird davon ausgegangen, dass der Nutzer die Umgebung des IoT-Geräts kontrolliert, wodurch unberechtigte Zugriffe vermieden werden.

## 2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

### 3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- DIN-TERMinologieportal: verfügbar unter <https://www.din.de/go/din-term>
- DKE-IEV: verfügbar unter <http://www.dke.de/DKE-IEV>

#### 3.1

##### **IoT-Gerät**

physisches Objekt, mit integriertem IT-System, das über hinreichende Rechenleistung und Stromversorgung für eine IP-basierte Kommunikation mit anderen Geräten und Services verfügt und auch kryptografische Protokolle (z. B. Transport Layer Security, TLS) nutzen kann

Anmerkung 1 zum Begriff: Unter IoT-Gerät werden hier typische IT-Produkte aus dem Consumer<sup>1)</sup> und SOHO Bereich verstanden.

Anmerkung 2 zum Begriff: IoT-Geräte können ggf. auch weitere Non-IP-Kommunikationsschnittstellen besitzen, die jedoch in diesem Dokument nur im Rahmen der IT-Sicherheitsarchitektur (z. B. Schutz von kryptografischen Schlüsseln) betrachtet werden.

BEISPIEL IP-Kameras, Kopierer/Drucker, Breitbandrouter, Smart TVs u.Ä.

#### 3.2

##### **Small Office, Home Office**

##### **SOHO**

Kundengruppe im IT-Bereich, dient zur Unterscheidung zwischen einerseits überwiegend privaten, kleingewerblichen (Kleinstunternehmen) oder freiberuflichen Kunden (en: „Home“ oder „Consumer“) und andererseits Unternehmen (en: „Enterprise“ oder „Corporate“)

Anmerkung 1 zum Begriff: In einem SOHO-Umfeld kann im Gegensatz zu einem Unternehmen nicht davon ausgegangen werden, dass die Einrichtung, Wartung und der Betrieb von IoT-Geräten durch einen fachkundigen Administrator erfolgt.

#### 3.3

##### **IP-Netzwerk**

Kommunikationsinfrastruktur, welche die Internet Protokollfamilie, wie z. B. IPv4, IPv6, ICMP, DNS oder DHCP, zur Kommunikation nutzt

Anmerkung 1 zum Begriff: Non-IP-Netzwerke (z. B. Bluetooth, DECT und andere) sind nicht Teil der Betrachtung dieses Dokuments.

#### 3.4

##### **Remote Interface am IoT-Gerät**

##### **RI**

logische Schnittstelle, über die über ein IP-Netzwerk auf Funktionsmodule eines IoT-Geräts zugegriffen werden kann

Anmerkung 1 zum Begriff: Beispiele hierfür sind Web-Interfaces über WAN oder LAN, Steuerung per APP über WAN oder LAN, Steuerung per Desktop-Software, IP-basierte Fernbedienung.

Anmerkung 2 zum Begriff: Ein IoT-Gerät kann über mehrere RI in Abhängigkeit zu den betriebenen Diensten verfügen.

---

1) Der in der Fachsprache verbreitete Begriff „Consumer“ wird im Deutschen mit „nichtgewerblicher Endverbraucher“ übersetzt.