

Bundesamt für Sicherheit in der Informationstechnik

**Risiken und Chancen des  
Einsatzes von RFID-Systemen**

Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit

<b>1. Vorwort</b>	<b>11</b>
<b>2. Geleitwort</b>	<b>12</b>
<b>3. Zusammenfassung</b>	<b>14</b>
<b>4. Einführung</b>	<b>22</b>
4.1. RFID als Schlüsseltechnologie des Pervasive Computing	22
4.2. Ziele, methodische Herangehensweise und Aufbau der Studie	24
<b>5. Grundlagen der RFID-Technologie</b>	<b>27</b>
5.1. Eigenschaften und Ausführungen von RFID-Systemen	27
5.2. Unterscheidungsmerkmale von RFID-Systemen	28
5.2.1. Frequenzbereiche	28
5.2.2. Speichertechnologie	30
5.2.3. Energieversorgung der Transponder und Datenübertragung	31
5.2.4. Mehrfachzugriffsverfahren	34
<b>6. Klassifizierung von RFID-Systemen</b>	<b>38</b>
6.1. Allgemeines	38
6.2. Klassifizierung von RFID-Systemen nach Leistungsfähigkeit	38
6.2.1. Low-End-Systeme	38
6.2.2. Systeme mittlerer Leistungsfähigkeit	38
6.2.3. High-End-Systeme	39
6.3. Klassifizierung von RFID-Systemen nach Reichweiten	39
6.4. Die Klassifizierung des Auto-ID-Centers	40
<b>7. Bedrohungslage und Bestandsaufnahme gängiger Sicherheitsmaßnahmen</b>	<b>41</b>
7.1. Übersicht	41
7.2. Grundlegende Angriffsarten	41
7.3. Angriffsarten nach Zweck	43
7.4. Exkurs: Angriffe auf das Backend	44
7.5. Bedrohungslage für die aktive Partei	45
7.5.1. Ausspähen von Daten	45
7.5.2. Einspeisen falscher Daten (Täuschen)	45
7.5.3. Denial of Service	45
7.6. Bedrohungslage für die passive Partei	46
7.6.1. Bedrohung der Data Privacy	46
7.6.2. Bedrohung der Location Privacy	47
7.7. Sicherheitsmaßnahmen	47
7.7.1. Authentifizierung	47
7.7.1.1. Prüfung der Identität des Tags	47
7.7.1.2. Prüfung der Identität des Lesegeräts	48
7.7.1.3. Starke gegenseitige Authentifizierung	49
7.7.2. Verschlüsselung	50
7.7.3. Abhörsichere Antikollisionsprotokolle	51
7.7.3.1. Silent Tree-Walking	51
7.7.3.2. Aloha-Verfahren mit temporären IDs	51

7.7.4. Pseudonymisierung	52
7.7.4.1. Randomized Hash-Lock	52
7.7.4.2. Chained Hashes	52
7.7.4.3. Verfahren von Henrici und Müller	52
7.7.5. Verhindern des Auslesens	53
7.7.5.1. Verwendung von Blocker-Tags	53
7.7.6. Dauerhafte Deaktivierung	53
7.7.6.1. Kill-Befehl	53
7.7.6.2. Deaktivierung durch Feldeinwirkung	54
7.7.7. Umsetzung der Fairen Informationspraktiken in RFID-Protokollen	54
7.8. Einschätzung der Bedrohungslage und Diskussion der Sicherheitsmaßnahmen	55
7.8.1. Gesamteinschätzung	55
7.8.2. Einschätzung einzelner Angriffsarten und Diskussion der Gegenmaßnahmen	55
7.8.3. Einschätzung der Bedrohung für die Privatsphäre und Diskussion der Gegenmaßnahmen	61
7.9. Verfügbarkeit der Sicherheitsmaßnahmen	64
<b>8. Anwendungsgebiete von RFID-Systemen</b>	<b>66</b>
8.1. Die Anwendungsgebiete im Überblick	66
8.2. Kennzeichnung von Objekten	67
8.3. Echtheitsprüfung von Dokumenten	72
8.4. Instandhaltung und Reparatur, Rückrufaktionen	74
8.5. Zutritts- und Routenkontrolle	76
8.6. Diebstahlsicherung und Reduktion von Verlustmengen	81
8.7. Umweltmonitoring und Sensorik	82
8.8. Supply-Chain-Management: Automatisierung, Steuerung und Prozessoptimierung	84
<b>9. Fördernde und hemmende Faktoren für den Einsatz von RFID</b>	<b>90</b>
<b>10. Entwicklungsperspektiven der RFID-Technologie</b>	<b>101</b>
10.1. Veranschaulichung der Risiken in Form von fiktiven Fallbeispielen	101
10.1.1. Einleitung	101
10.1.2. Anwendungsgebiet „Kennzeichnung von Produkten“	101
10.1.3. Anwendungsgebiet „Zutritts- und Routenkontrolle“	103
10.2. Erwartete Entwicklungen bis 2010	104
10.2.1. Vorbemerkung	104
10.2.2. Technologie und Standardisierung	105
10.2.3. Markt- und Preisentwicklung	106
10.2.4. Anforderungen an Informationssicherheit, Datenschutz und Privatsphäre	108
10.2.5. Gesellschaftliche Akzeptanz	110
<b>11. Abkürzungsverzeichnis</b>	<b>112</b>
<b>12. Index</b>	<b>113</b>
<b>13. Quellenverzeichnis</b>	<b>115</b>