

Inhaltsverzeichnis

Abkürzungsverzeichnis	XVII
Abbildungsverzeichnis	XXI
1 Sicherheit im Cloud Computing (Einleitung)	1
2 Technische Grundlagen	7
2.1 Cloud Computing	7
2.1.1 Definition	7
2.1.2 Cloud-Modelle	7
2.1.3 Cloud-Leistungen	8
2.1.4 Cloud-Strukturen	9
2.1.4.1 Basisstruktur	9
2.1.4.2 Besonderheiten auf Cloud-Kunden-Seite/Cloud-Nutzer-Seite	10
2.1.4.3 Besonderheiten aufseiten des Cloud-Diensteanbieters	10
2.1.5 Ausgewählte Beispiele	11
2.1.5.1 Cloud-Diensteanbieter	12
2.1.5.1.1 Amazon Cloud Drive, iCloud, Facebook	12
2.1.5.1.2 Salesforce	12
2.1.5.1.3 Microsoft Sharepoint Online	13
2.1.5.2 Cloud-Kunden/Cloud-Nutzer	13
2.1.5.2.1 Automotive Cloud	13
2.1.5.2.2 Versicherungs-Cloud	14
2.1.5.2.3 Verwaltungs-Cloud	15
2.1.5.2.4 Gesundheits-Cloud	17
2.1.5.2.5 Universitäts-Portal	17
2.1.6 Zusammenfassung	18
2.2 Grundbegriffe des Identitätsmanagements	19
2.2.1 Authentifizierung, Authentisierung und Autorisierung	19
2.2.1.1 Authentifizierung und Authentisierung	19
2.2.1.2 Autorisierung	21
2.2.1.3 Erstregistrierung und wiederholter „Login“	21
2.2.1.4 Interne und externe Authentifizierung	22
2.2.2 Identität, Identitätsattribute, Identitätsdaten	23
2.2.3 eID-Diensteanbieter	24
2.2.4 Identitäts-Föderation	25
2.2.4.1 Begriff und Nutzen	25
2.2.4.2 Single-Sign-On	26
2.2.4.3 SAML	27
2.2.5 Identitätsmanagement	29
2.2.6 Das Identitätsmanagement-System der Universität Passau	30
2.2.7 Zusammenfassung	33
2.3 Elektronische Chipkarten-Ausweise	33
2.3.1 Hintergrund: Die E-Card-Strategie der Bundesregierung	33
2.3.2 Funktionsweise der eID-Funktion des neuen Personalausweises	34

2.3.2.1 Technische Richtlinien des BSI	34
2.3.2.2 Authentisierungsfunktion	34
2.3.2.3 Signaturfunktion	39
2.3.3 Die elektronische Gesundheitskarte (eGK)	39
2.4 Referenzarchitektur: Das Forschungsprojekt SkiIdentity	41
2.4.1 SkiIdentity-Vision	41
2.4.2 Technische Umsetzung	43
2.5 Zusammenfassung und Darstellung relevanter Rechtsbeziehungen	45
2.5.1 Relevante Stellen	46
2.5.1.1 Der Cloud-Kunde	47
2.5.1.2 Der Cloud-Diensteanbieter	47
2.5.1.3 Der Cloud-Nutzer und Ausweisinhaber (Betroffener)	47
2.5.1.4 Der eID-Diensteanbieter	48
2.5.1.5 Der Broker-Diensteanbieter	48
2.5.2 Relevante Rechtsverhältnisse	48
3 Rechtsrahmen und Relevanz für den Umgang mit Identitätsdaten	51
3.1 Datenschutzrecht	51
3.1.1 Anwendungsbereich	52
3.1.1.1 Anwendbares Gesetz	52
3.1.1.1.1 Europäische Union	52
3.1.1.1.2 Deutschland	53
3.1.1.1.2.1 Bundesdatenschutzgesetz und Subsidiaritätsgrundsatz	53
3.1.1.1.2.2 Telekommunikationsgesetz	54
3.1.1.1.2.3 Telemediengesetz	55
3.1.1.1.2.3.1 Telemediendiensteanbieter	55
3.1.1.1.2.3.2 Datenschutzrechtliche Verantwortlichkeit	57
3.1.1.1.2.3.2.1 Begriff der verantwortlichen Stelle	57
3.1.1.1.2.3.2.2 Anbieter-Nutzer-Verhältnis/Bestands- und Nutzungsdaten	58
3.1.1.1.2.3.2.3 Konsequenzen für das Identitätsmanagement	62
3.1.1.1.2.3.3 Ausnahmen vom Anwendungsbereich des TMG	64
3.1.1.1.2.3.4 Öffentlich-rechtlicher Bereich	65
3.1.1.1.3 Zwischenergebnis	65
3.1.1.2 Sachlicher Anwendungsbereich: personenbezogene Daten	66
3.1.1.2.1 Relevanz	66
3.1.1.2.2 Problematik und Streitstand	67
3.1.1.2.3 Stellungnahme und Konsequenz für das Identitätsmanagement	70
3.1.1.3 Verbotsprinzip und Formen des Datenumgangs	73
3.1.1.4 Räumlicher Anwendungsbereich	75
3.1.1.4.1 Dispositives Recht?	76
3.1.1.4.2 Keine spezialrechtlichen Regelungen	77
3.1.1.4.3 Datenumgang innerhalb und außerhalb der EU/ des EWRs	77

3.1.1.4.3.1 Innereuropäische Sachverhalte, § 1 Abs. 5 Satz 1 BDSG.....	78
3.1.1.4.4 Sachverhalte mit Drittstaatenbezug § 1 Abs. 5 Satz 2 BDSG.....	82
3.1.1.4.5 Ausblick auf die DS-GVO	86
3.1.1.4.5 Zwischenergebnis	87
3.1.1.6 Zusammenfassung.....	89
3.1.2 Datenschutzrechtliche Legitimation.....	90
3.1.2.1 Legitimation durch Gesetz.....	91
3.1.2.1.1 Vorschriften für öffentliche und nicht-öffentliche Stellen aus dem TMG	91
3.1.2.1.1.1 § 12 Abs. 1 TMG in Abgrenzung zu den Vorschriften des BDSG	91
3.1.2.1.1.2 Anforderungen an den Datenumgang.....	91
3.1.2.1.1.2.1 Zweckbindung und Erforderlichkeit	91
3.1.2.1.1.2.2 Sonderfall Übermittlung von Nutzungsdaten	95
3.1.2.1.1.2.3 Weiterer Umgang mit Abrechnungsdaten	96
3.1.2.1.1.2.4 Profilbildung zu Werbezwecken etc.	96
3.1.2.1.1.2.5 Verwendung zu Zwecken der Rechtsverfolgung, § 15 Abs. 8 TMG.....	97
3.1.2.1.2 Legitimationsgrundlagen des Bundesdatenschutzgesetzes	97
3.1.2.1.2.1 §§ 28, 29 BDSG	98
3.1.2.1.2.1.1 Abgrenzung	98
3.1.2.1.2.1.2 Anforderungen im Einzelnen.....	99
3.1.2.1.2.2 §§ 12 ff. BDSG	101
3.1.2.1.2.3 § 32 BDSG und die Besonderheiten des Beschäftigtendatenschutzes	101
3.1.2.1.2.4 Umgang mit besonderen Arten personenbezogener Daten.....	105
3.1.2.2 Legitimation durch Einwilligung und Informationspflichten.....	105
3.1.2.3 Des Auftraggebers Privilegierung durch Auftragsdatenverarbeitung....	108
3.1.2.3.1 Die Bedeutung der Auftragsdatenverarbeitung	108
3.1.2.3.2 Anwendbarkeit im TMG	109
3.1.2.3.3 Definition der Auftragsdatenverarbeitung	110
3.1.2.3.3.1 Abgrenzung zur Funktionsübertragung.....	110
3.1.2.3.3.2 Keine Auftragsdatenverarbeitung in Drittstaaten.....	113
3.1.2.4 Zusammenfassung.....	114
3.1.3 Technische und organisatorische Maßnahmen.....	115
3.1.3.1 IT-Sicherheit: Schnittstelle zwischen Recht und Technik.....	115
3.1.3.2 Katalog der technischen und organisatorischen Maßnahmen im Einzelnen	118
3.1.3.2.1 § 9 BDSG.....	118
3.1.3.2.1.1 Erforderlichkeit und Verhältnismäßigkeit der Maßnahmen	118
3.1.3.2.1.2 Anlage zu § 9 BDSG.....	119
3.1.3.2.1.2.1 Zutrittskontrolle (Nr. 1).....	119
3.1.3.2.1.2.2 Zugangs- und Zugriffskontrolle (Nr. 2 und Nr. 3).....	120
3.1.3.2.1.2.3 Weitergabekontrolle (Nr. 4).....	122
3.1.3.2.1.2.4 Eingabekontrolle (Nr. 5).....	124

3.1.3.2.1.2.5	Auftragskontrolle (Nr. 6)	126
3.1.3.2.1.2.6	Verfügbarkeitskontrolle (Nr. 7)	126
3.1.3.2.1.2.7	Datentrennung (Nr. 8)	128
3.1.3.2.1.3	Verschlüsselung	128
3.1.3.2.1.4	Personenbezug verschlüsselter Daten?.....	132
3.1.3.2.2	Technische und organisatorische Anforderungen aus § 13 TMG	133
3.1.3.2.2.1	§ 13 Abs. 4 TMG.....	134
3.1.3.2.2.1.1	Jederzeitige Beendigungsmöglichkeit des Nutzers (Satz 1 Nr. 1).....	134
3.1.3.2.2.1.2	Lösch- und Sperrpflichten (Satz 1 Nr. 2).....	134
3.1.3.2.2.1.3	Schutz gegen Kenntnisnahme Dritter (Satz 1 Nr. 3)	136
3.1.3.2.2.1.4	Getrennte Verwendung (Satz 1 Nr. 4)	137
3.1.3.2.2.1.5	Beschränkte Zusammenführung von Nutzungsdaten (Satz 1 Nr. 5).....	138
3.1.3.2.2.1.6	Keine Identifikation bei der Erstellung von Nutzungsprofilen (Satz 1 Nr. 6).....	138
3.1.3.2.2.2	Pflicht zur Anonymisierung und Pseudonymisierung, § 13 Abs. 6 TMG	138
3.1.3.3	Technische und organisatorische Maßnahmen nach DS-GVO.....	141
3.1.3.4	Zusammenfassung und Bedeutung für das Identitätsmanagement.....	142
3.1.4	Anforderungen an eine wirksame Auftragsdatenverarbeitung	143
3.1.4.1	Sorgfältige Auswahl des Auftragnehmers und Festlegung der technischen und organisatorischen Maßnahmen	143
3.1.4.2	Schriftlicher Vertrag	145
3.1.4.3	Festlegung von Gegenstand und Dauer des Auftrags (Nr. 1)	146
3.1.4.4	Festlegung von Umfang, Art und Zweck des Datenumgangs, Datenart und Betroffenenkreis (Nr. 2).....	146
3.1.4.5	Löschen, Berichtigen und Sperren (Nr. 4).....	148
3.1.4.6	Unterauftragsverhältnisse (Nr. 6).....	148
3.1.4.7	Weisungsbefugnisse (Nr. 9)	150
3.1.4.8	Kontrollen des Auftraggebers (Nr. 5, Nr. 7 i. V. m. Satz 4 und Satz 5).	151
3.1.4.8.1	Problematik im Cloud Computing allgemein	151
3.1.4.8.2	Konsequenzen für das Identitätsmanagement	155
3.1.4.9	Rückgabe und Löschung nach Beendigung des Auftrags.....	155
3.1.4.10	Zusammenfassung.....	156
3.1.5	Datenübermittlung in Drittstaaten	157
3.1.5.1	Rechtslage.....	158
3.1.5.1.1	Ausgangspunkt	158
3.1.5.1.2	Angemessenes Datenschutzniveau in Drittstaaten	158
3.1.5.1.3	Ausnahmen in Verbindung mit geeigneten Garantien für ein angemessenes Datenschutzniveau	159
3.1.5.1.3.1	Die Standardvertragsklauseln der EU-Kommission	160
3.1.5.1.3.2	Verbindliche unternehmensinterne Regelungen	161
3.1.5.1.3.3	Die „Safe-Harbor-Zertifizierung“	161
3.1.5.1.4	Garantie durch Zertifizierung entsprechend DS-GVO.....	163
3.1.5.1.5	Versagen der Garantien bei Datentransfers in die USA	163
3.1.5.1.6	Einwilligung des Betroffenen	168
3.1.5.2	Zusammenfassung und Konsequenzen für das Identitätsmanagement	169

3.1.6 Gesamtzusammenfassung Datenschutzrecht	170
3.2 Personalausweisrecht	172
3.2.1 Rechtliche Grundlagen der eID-Funktion des nPAs	172
3.2.2 Auswirkungen auf das Identitätsmanagement	174
3.2.2.1 Anforderungen aus § 21 Abs. 2 Satz 1 PAusWG im Einzelnen	175
3.2.2.1.1 Kein rechtswidriger Geschäftszweck (Nr. 1) und keine Anhaltspunkte für missbräuchliche Verwendung (Nr. 5)	175
3.2.2.1.2 Kein auf eine geschäftsmäßige Datenübermittlung gerichteter Geschäftszweck (Nr. 2 und Nr. 2a)	176
3.2.2.1.2.1 Begriff der Übermittlung	177
3.2.2.1.2.2 Begriff der Geschäftsmäßigkeit	177
3.2.2.1.3 Anforderungen der Personalausweisverordnung	183
3.2.2.1.3.1 Insbesondere Datenschutz und Datensicherheit	183
3.2.2.1.3.2 Weitere Anforderungen der Personalausweisverordnung	184
3.2.2.1.4 Erforderlichkeit	186
3.2.3 Zusammenfassung	188
3.2.4 Exkurs: Obligatorische Nutzung des nPAs	190
3.2.4.1 Problemstellung	190
3.2.4.2 Entscheidung des BAG	190
3.2.4.3 Übertragbarkeit auf nPA-Nutzung	191
3.2.4.3.1 Gemeinsamkeiten	191
3.2.4.3.2 Unterschiede	192
3.2.4.3.3 Zusammenfassung	193
3.3 Beweisrechtliche Fragestellungen im Zusammenhang mit der Nutzung des nPAs	193
3.3.1 Ausgangspunkt und Problemstellung	193
3.3.1.1 Datenschutz und Beweisrecht	193
3.3.1.2 Beweisrelevante Tatsachen	194
3.3.1.3 Beweisrechtliche Fragestellungen	196
3.3.2 Allgemeine Beweisregeln und elektronische Dokumente	196
3.3.2.1 Die unterschiedlichen Prozessordnungen und ihre Grundsätze	196
3.3.2.2 Beweismittel und Beweisregeln im Hinblick auf elektronische Dokumente	197
3.3.3 Beweiswirkung einzelner Authentisierungswerkzeuge	199
3.3.3.1 Authentisierung durch Nutzernamen und Passwort	199
3.3.3.2 Authentisierung im Rahmen von Banking-Verfahren	200
3.3.3.2.1 EC-Karten an Bankautomaten	201
3.3.3.2.2 Online-Banking	201
3.3.3.3 Authentisierung mittels nPA	203
3.3.3.3.1 Nachweis einer Authentifizierung nach § 18 PAusWG	204
3.3.3.3.2 Beweiswert der Authentifizierung mittels nPA	205
3.3.3.3.2.1 Nutzung des Ausweises und der PIN	205
3.3.3.3.2.2 Vornahme einer Handlung und Schriftformersatz	207
3.3.3.3.2.2.1 Voraussetzungen der Richtlinie BSI TR-03107-2	208
3.3.3.3.2.2.2 Konsequenzen für den privatrechtlichen Bereich?	209
3.3.4 Auswirkungen auf die Referenzarchitektur	210

3.3.4.1	Nachweis der Authentifizierung	210
3.3.4.2	Nachweis weiterer Handlungen	212
3.3.4.3	Exkurs: Erweiterung durch Token-Mapping	213
3.3.5	Zusammenfassung.....	213
3.4	Der Einsatz der eGK	216
3.4.1	Rechtliche Grundlagen der Authentisierung	216
3.4.1.1	Beschränkter Anwendungsbereich der eGK	216
3.4.1.1.1	Auf der Karte gespeicherte Angaben	218
3.4.1.1.2	Unterstützte Anwendungen	218
3.4.1.1.3	Verarbeitungszwecke	218
3.4.2	Besondere Anforderungen an Authentisierung und Autorisierung.....	219
3.4.3	Rechtliche Vorgaben für cloudspezifische Elemente der Telematikinfrastruktur.....	220
3.4.3.1	Identitätsdaten als Sozialdaten und Sozialgeheimnis.....	220
3.4.3.2	Besondere Vorgaben bei der Auftragsdatenverarbeitung	221
3.4.3.3	Übermittlungen ins Ausland	222
3.4.3.4	Beschlagnahmeschutz	223
3.4.3.5	Besondere Geheimhaltungspflichten.....	224
3.4.3.5.1	Problematik.....	224
3.4.3.5.2	Reformbestrebungen	225
3.4.3.6	Besondere Anforderungen an den Umgang mit Gesundheitsdaten.....	227
3.4.4	Zusammenfassung und Konsequenzen für das Identitätsmanagement	228
3.5	Europarechtliche Vorgaben für die elektronische Identifizierung.....	228
3.5.1	Wesentlicher Inhalt der eIDAS-VO in Bezug auf elektronische Identifizierung	229
3.5.1.1	Anerkennungspflicht notifizierter eIDs	229
3.5.1.2	Voraussetzung für die Anerkennung im Einzelnen	229
3.5.1.2.1	Staatliche eIDS	229
3.5.1.2.2	Verwendung im Rahmen eines öffentlichen Dienstes.....	230
3.5.1.2.3	Sicherheitsniveau.....	230
3.5.1.2.4	Gewährleistung der Interoperabilität und Gebührenfreiheit	231
3.5.1.3	Haftung	232
3.5.2	Verhältnis von eIDAS-VO zu nPA und Bewertung	234
3.5.3	Chancen durch einen Broker-Diensteanbieter	236
3.5.4	Zusammenfassung.....	238
4	Untersuchung relevanter Rechtsverhältnisse	241
4.1	Rechtsverhältnisse mit dem Betroffenen	243
4.1.1	Betroffener – Cloud-Kunde	243
4.1.1.1	Personalausweisrecht	243
4.1.1.2	Datenschutzrecht	244
4.1.1.2.1	Typ-1-Modell: Cloud-Anbieter im Hintergrund.....	244
4.1.1.2.1.1	Verantwortlichkeit.....	244
4.1.1.2.1.2	Legitimation und Anforderungen im Einzelnen.....	244
4.1.1.2.1.3	Drittstaatenverkehr	247
4.1.1.2.2	Typ-2-Modell: Cloud-Diensteanbieter mit Außenauftritt	247
4.1.1.3	Beweisrecht	248
4.1.2	Betroffener – Cloud-Diensteanbieter	249

4.1.2.1	Personalausweisrecht	249
4.1.2.2	Datenschutzrecht	249
4.1.2.2.1	Typ-1-Modell: Cloud-Diensteanbieter im Hintergrund	249
4.1.2.2.1.1	Verantwortlichkeit.....	249
4.1.2.2.1.2	Legitimation	250
4.1.2.2.1.3	Pflichten als Auftragnehmer	250
4.1.2.2.2	Typ-2-Modell: Cloud-Diensteanbieter mit Außenauftritt	251
4.1.2.2.2.1	Verantwortlichkeit.....	251
4.1.2.2.2.2	Legitimation	252
4.1.2.3	Beweisrecht	253
4.1.3	Betroffener – Broker-Diensteanbieter	254
4.1.3.1	Personalausweisrecht	254
4.1.3.2	Datenschutzrecht	255
4.1.3.2.1	Verantwortlichkeit	255
4.1.3.2.2	Legitimation.....	255
4.1.3.2.3	Anforderungen im Einzelnen	256
4.1.3.3	Beweisrecht	257
4.1.4	Betroffener – eID-Diensteanbieter	257
4.1.4.1	Personalausweisrecht	257
4.1.4.2	Datenschutzrecht	258
4.1.4.2.1	Verantwortlichkeit	258
4.1.4.2.2	Legitimation und Pflichten im Einzelnen.	258
4.1.4.3	Beweisrecht	258
4.2	Rechtsverhältnisse sonstiger Beteiligten untereinander	258
4.2.1	Cloud-Kunde – Cloud-Diensteanbieter	259
4.2.1.1	Personalausweisrecht	259
4.2.1.2	Datenschutzrecht	259
4.2.1.2.1	Typ-1-Modell: Cloud-Diensteanbieter im Hintergrund	259
4.2.1.2.2	Typ-2-Modell: Cloud-Diensteanbieter mit Außenauftritt	260
4.2.2	Cloud-Diensteanbieter – Broker-Diensteanbieter	261
4.2.2.1	Personalausweisrecht	261
4.2.2.2	Datenschutzrecht	261
4.2.2.3	Beweisrecht	261
4.2.3	Cloud-Kunde – Broker-Diensteanbieter.....	262
4.2.3.1	Personalausweisrecht	262
4.2.3.2	Datenschutzrecht	262
4.2.3.3	Beweisrecht	262
4.2.4	Cloud-Kunde – eID-Diensteanbieter	263
4.2.4.1	Personalausweisrecht	263
4.2.4.2	Datenschutzrecht	263
4.2.4.3	Beweisrecht	263
4.2.5	Cloud-Diensteanbieter – eID-Diensteanbieter	263
4.2.5.1	Personalausweisrecht	263
4.2.5.2	Datenschutzrecht	263
4.2.5.3	Beweisrecht	264
4.2.6	Broker-Diensteanbieter – eID-Diensteanbieter.....	264
4.2.6.1	Personalausweisrecht	264

4.2.6.2	Datenschutzrecht	264
4.2.6.3	Beweisrecht	265
4.2.7	Annex: Verhältnis unterschiedlicher Cloud-Kunden untereinander	265
5	Gestaltungsvorschläge	267
5.1	Technische und organisatorische Gestaltungsvorschläge	267
5.1.1	Durchgehend getrennte Behandlung von Identitätsdaten und Cloud-Inhaltsdaten	267
5.1.2	Auslagerung des Identitätsmanagements	267
5.1.3	Trennung von Authentifizierung und Rechtemanagement	268
5.1.4	Bildung von Pseudonymketten	268
5.1.5	Löschen von nicht benötigten Daten beim Broker-Diensteanbieter	268
5.1.6	Speicherung des DKKs bei sämtlichen involvierten Stellen	269
5.1.7	Vergabe unterschiedlicher Zertifikate	269
5.1.8	Verwendung von Hardware-Token	269
5.1.9	Broker-Dienste innerhalb der EU bzw. des EWRs (auch personalausweisrechtliche Vorgabe)	270
5.1.10	Eingeschränkte Übermittlung von personenbezogenen Identitätsdaten zum Cloud-Diensteanbieter	270
5.1.11	Zurverfügungstellung der Identitätsdaten an den Ausweisinhaber	270
5.1.12	Kommunikation über Client	270
5.1.13	Sichere Kanäle und Verschlüsselung	271
5.1.14	Vermeidung eines „Kanalmergers“ bei Zwei-Faktor-Authentisierung	271
5.1.15	Beweissichere Verknüpfung von Erklärung und Authentifizierung	271
5.2	Rechtliche Gestaltungsvorschläge	271
5.2.1	Ausgestaltung des Broker-Diensteanbieters	271
5.2.2	Vertragliche Regelung zwischen Broker-Diensteanbieter und Cloud-Diensteanbieter	272
5.2.3	Datenschutzerklärung des Broker-Diensteanbieters	272
5.2.4	Ausgestaltung der Einwilligung	272
5.2.5	Vertragliche Regelungen zwischen Broker-Diensteanbieter und Betroffenen	273
5.2.6	Vermeidung von eigenständigen Nutzungsverträgen mit dem Betroffenen	273
5.2.7	Keine Auftragsdatenverarbeitung zwischen Broker- und Cloud-Diensteanbieter bzw. Cloud-Kunden	273
5.3	Konkretes Modell: Konzept der abgeleiteten Identität	274
5.3.1	Bestehende Konzeption	274
5.3.2	Anwendungsszenario: Salesforce-Anbindung	276
5.3.3	Ergänzungen	277
6	Fazit	278
	Literatur	281