Kompass der IT-Sicherheitsstandards

Auszüge zum Thema Elektronische Identitäten

BITKOM

DIN

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org	DIN Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik und Anwendungen (NIA) Burggrafenstraße 6 10787 Berlin Tel.: 030.2601-0 Fax: 030.2601-1231 nia@din.de www.nia.din.de
Ansprechpartner:	Marc Fliehe Tel.: 030.27576-242 m.fliehe@bitkom.org	Volker Jacumeit Tel.: 030.2601-2186 volker.jacumeit@din.de
Redaktion:	Dr. Walter Fumy (Bundesdruckerei GmbH) Lutz Neugebauer (TÜV TRUST IT GmbH) Marc Fliehe (BITKOM)	Volker Jacumeit (DIN e.V.) Martin Uhlherr (DIN e.V.)
Verantwortliches Gremium:	AK Sicherheitsmanagement	Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, Arbeitsausschuss NIA-27, IT-Sicherheitsverfahren
Redaktionsassistenz:	Miriam Taenzer (BITKOM)	
Gestaltung/Layout:	Design Bureau kokliko / Astrid Scheibe (BITKOM)	
Copyright:	BITKOM 2014	
Stand:	Februar 2014, Auszüge zum Thema Elektronische Identitäten	

Mit freundlicher Unterstützung von: BUNDESDRUCKEREI

Kompass der IT-Sicherheitsstandards

Auszüge zum Thema Elektronische Identitäten

BITKOM

DIN

Inhaltsverzeichnis

Abbildungsverzeichnis

1 »Sichere Identitäten sind unser Markenzeichen«

Ulrich Hamann, Vorsitzender der Geschäftsführung der Bundesdruckerei GmbH

Ulrich Hamann, Vorsitzender der Geschäftsführung der Bundesdruckerei GmbH, berichtet von wegweisenden Produkten und erklärt, welche Bedeutung Full-ID-Management heute hat und künftig haben wird.

Wir kaufen im Netz, unterhalten uns dort mit Freunden oder buchen eine Reise – was spricht dafür, ein Dokument wie den Personalausweis in der Online-Welt zu nutzen?

Ulrich Hamann: *Mit wem hat man es zu tun? Das ist heute eine der entscheidenden Fragen, wenn sich immer mehr Dinge des Alltags wie Einkaufen oder Behördengänge ins Internet verlagern. Uns geht es darum, wie man seine Identität sicher im Netz nachweisen kann, und zwar überall dort, wo es sinnvoll ist. Mit dem Personalausweis und seinen Online-Funktionen wurde erstmals auch für die vernetzte Gesellschaft ein Legitimationsmittel geschaffen, das ein Höchstmaß an Sicherheit bietet. Der Personalausweis ist weit mehr als nur ein Ausweisdokument – mit dem grauen Büchlein von einst hat er nur noch wenig zu tun. Künftig können Sie mit dem Personalausweis Geld abheben, Ihre aktuelle Energierechnung einsehen oder Behördengänge online erledigen. Kurz: Der Personalausweis bietet in der Online-Welt eine sichere und verlässliche Antwort auf die Frage, mit wem man es zu tun hat – für Kunden und Anbieter. Das schafft gegenseitiges Vertrauen.*

Was macht den Personalausweis zu mehr als einem ID-Dokument?

Ganz einfach: Der Personalausweis ist vielseitig einsetzbar. Wir haben gemeinsam mit der biw Bank einen EC-Bankautomaten in unserem Foyer in Berlin aufgestellt, an dem Sie mit Ihrem Personalausweis Geld abheben können. Nach der Online-Kontoeröffnung und dem Online-Abschluss von Versicherungen ist das der nächste Schritt, der den Personalausweis zu einem sicheren »Handwerkszeug« im Alltag macht. Als eine perfekte Ergänzung sehe ich auch »sign-me«, eine von der Bundesdruckerei entwickelte Web-Applikation, mit der eine Online-Unterschrift mittels einer Qualifizierten Elektronischen Signatur geleistet werden kann. Nichts macht uns so unverwechselbar wie die eigene Unterschrift. Hierzu haben wir die Pilotphase für das Nachladen von Zertifikaten auf den Personalausweis gestartet. Das Feedback der Nutzer lassen wir nun in die weitere Produktentwicklung einfließen.

Wie stellt die Bundesdruckerei sicher, dass man weiß, mit wem man es zu tun hat?

Das ist eine komplexe Aufgabe, die mehr als nur die Produktion von Dokumenten umfasst. Wir nennen es Full-ID-Management, und das heißt: Die Bundesdruckerei ist für die gesamte Prozesskette »Sichere Identität« verantwortlich. Das beginnt mit der Erfassung und Registrierung von Daten in den Behörden und Ämtern, damit sie anschließend verarbeitet, geprüft und übermittelt werden können. Mit den erfassten Daten werden in unserem Haus ID-Dokumente produziert, die mit modernsten Sicherheitsmerkmalen ausgestattet sind und an die Behörden ausgeliefert werden. Das Hochsicherheitskonzept unseres Trustcenters D-TRUST gewährleistet zudem den Aufbau eines sicheren ID-Managements sowie einen optimalen

Datenschutz beim Einsatz des Ausweises im Netz oder bei der rechtsverbindlichen Online-Unterschrift. Unter Full-ID-Management verstehen wir aber auch die stetige Arbeit an Innovationen. Nur ein Beispiel ist das dynamische Passwort, das wir mit unserem Partner Infineon entwickelt haben. Dabei handelt es sich um ein One-Time-Passwort, ein Einmalkennwort für den Zugang zu einem Online-Service oder Datensystem. Ausgangspunkt ist dabei eine feste PIN, die durch eine dynamische, immer neu konfigurierte PIN-Ergänzung zu einem sicheren Schlüssel wird.

Worin sehen Sie den Grund für den Erfolg der ID-Security-Komponenten der Bundesdruckerei?

Einen wesentlichen Grund sehe ich in den Kompetenzen, die tief in unserer Geschichte verankert sind. Seit Gründung des Unternehmens und seiner Vorgänger vor 250 Jahren, sind wir Dienstleister für Staaten und Regierungen und haben dabei das wichtigste Kapital für ID-Management und ID-Security aufgebaut: Vertrauen. Dieses Vertrauen überzeugt Kunden wie das Bundesinnenministerium, für das wir Personalausweise und Reisepässe produzieren, das Bundesverkehrsministerium, das bei uns den neuen Führerschein produzieren lässt, und nicht zuletzt auch internationale Partner wie die Vereinigten Arabischen Emirate. Das Vertrauen überzeugt aber auch den Bürger, der die Online-Ausweisfunktion nutzt, um ein neues Bankkonto zu eröffnen. Kurz gesagt: Das Thema Sichere Identitäten ist unser Markenzeichen.

Und wie prüft ein Händler im direkten Kontakt an der Ladentheke, ob es sich um ein echtes Dokument handelt?

Für Kunden aus der Privatwirtschaft haben wir das Dokumentenprüfsystem VISOCORE® Verify entwickelt. Das hilft dabei, einen möglichen wirtschaftlichen Schaden zu verhindern. Zum Beispiel passiert es nicht selten, dass Autohäusern bei Probefahrten gefälschte Dokumente vorgelegt und die Autos während der Probefahrt entwendet werden. Mit VISOCORE® Verify lässt sich leicht feststellen, ob der Ausweis echt ist. Das Gerät ist auch für Laien gut handhabbar. Es lässt sich im Übrigen auch beim Abschluss von Handy-Verträgen oder bei der Vergabe von Kleinkrediten einsetzen. Sprich: überall dort, wo ein gesicherter Nachweis der Identität meines Gegenübers erforderlich ist.

Behördengänge sind oft sehr zeitaufwändig. Wie kann beispielsweise die Beantragung von Pässen künftig noch schneller ablaufen?

Eine Möglichkeit, um die Beantragung schneller und effizienter zu gestalten, ist das von uns entwickelte Self-Service-Terminal. Das ist eine Art Automat, der in Behörden und Ämtern aufgestellt werden kann und mit dem der Bürger eigenhändig Ausweise und andere Dokumente beantragt. Als besonders nützlich erweist sich das Terminal bei der Beantragung hoheitlicher Dokumente wie zum Beispiel von Reisepässen oder eines Führungszeugnisses. Die Daten werden dabei entweder über die Tastatur eingegeben oder sie werden mit einem Lesegerät vom Sicherheitschip des Personalausweises abgerufen. Anschließend bearbeitet wie gewohnt ein Behördenmitarbeiter den Antrag. Doch durch die Selbsteingabe reduziert sich sowohl der Bearbeitungsaufwand für die Behörde als auch die Wartezeit für die Bürger. Der Einsatz der Terminals ist übrigens auch in Unternehmen für die Ausstellung von Mitarbeiter- oder Besucherausweisen sinnvoll.

Welchen Anteil am Umsatz haben ID-Dokumente wie der Personalausweis?

Seit Einführung des neuen Personalausweises 2010 haben wir mehr als 18 Millionen Personalausweise ausgegeben. Bundesweit sind bereits mehr als 70 Online-Dienste bei Behörden und Unternehmen installiert, Tendenz steigend. Es ist in der Tat so, dass ID-Systeme und ID-Dokumente inzwischen rund 85 Prozent unseres Umsatzes ausmachen. Das umfasst nicht nur Personalausweise, sondern auch Reisepässe, elektronische Aufenthaltstitel oder Führerscheine. Hinzu kommt, dass weltweit strengere Sicherheitsbestimmungen für Reise- und Ausweisdokumente für ein erhebliches Marktwachstum sorgen.

Welche Perspektiven ergeben sich für die Bundesdruckerei in den nächsten Jahren?

Wir haben im letzten Jahr unser neues Produktionsgebäude in Betrieb genommen. Das ist ein gewaltiger Einschnitt, dadurch ändern sich unsere Logistikprozesse von Grund auf. Logistik und Produktion rücken enger zusammen, und die neuen, wesentlich effizienteren Fertigungslinien und die IT-gestützte Taktung von Zulieferungen sorgen für kurze Wege beim Waren- und Rohstofftransport. Mit dem neuen Hochregallager machen wir einen enormen Modernisierungssprung. Und was unsere Geschäftsfelder angeht: Wir sind derzeit in der Lage, täglich bis zu 50.000 Dokumente herzustellen und mit der ME 8000 Inspect, der Weltneuheit unserer Tochter Maurer Electronics, jeden einzelnen Ausweis auf Sicherheitsmerkmale, Datenkonsistenz sowie Druck- und Laserqualität zu überprüfen. Das ist ein Qualitätsprozess, den es so für ID-Dokumente bisher nicht gegeben hat. Das alles sind Gründe, sehr zuversichtlich in die Zukunft zu blicken.

2 Nutzer und Nutzen von Standards

So wie der Einsatz von Informations- und Kommunikationstechnologien in Unternehmen in der Regel kein Selbstzweck ist, so sollte auch die Verwendung von Sicherheitsstandards immer mit einem – bestenfalls quantifizierbaren – Nutzen verbunden sein. Beispielsweise ist die Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001 – je nach Wahl des Geltungsbereiches – durchaus mit einem spürbaren personellen und finanziellen Aufwand verbunden. Das gilt sowohl für den Zertifizierungsprozess als auch im nachfolgenden Betrieb des Managementsystems und den notwendigen Audits zur Aufrechterhaltung des Zertifikats. Unbestritten sind aber auch die Vorteile, die eine stringente und für das Unternehmen angemessene Einführung und Betrieb eines Managementsystems für die Informationssicherheit mit sich bringt.

In der Innenwirkung kann die Verwendung von etablierten Standards dabei unterstützen, die sicherheitsrelevanten IT-Prozesse zum Vorteil des Unternehmens, der Kunden, der eigenen Produkte sowie der Mitarbeiter zu verbessern. Sie bieten Hilfestellung bei der Entwicklung von generischen Maßnahmen auf Management-Ebene bis zu detaillierten technischen Implementierungen an. Sie liefern Methoden für ein leistungsfähiges IT-Sicherheitsmanagement oder definieren die IT-Sicherheit von ausgewiesenen Produkten. Sie können sowohl eigenständig als auch methodisch eingebettet in ein anderes System fortlaufend betrieben werden.

Ein ISMS ist sinnvollerweise Teil eines unternehmensweiten Risikomanagements, durch das insbesondere auch die IT-Risiken auf ein für das Unternehmen angemessenes Niveau reduziert werden können. Dabei kommt es insbesondere darauf an, die Risiken umfassend zu ermitteln und die Schutzmechanismen aus wirtschaftlichen Gründen nicht aufwendiger zu gestalten, als es das zulässige Risiko verlangt. Die Auswahl und die Anwendung angemessener IT-Sicherheitsstandards ist ein Teil des IT-Sicherheitsmanagements.

In der Außenwirkung entwickeln die Verwendung und insbesondere der Nachweis der Verwendung von IT-Sicherheitsstandards (also eine entsprechende Zertifizierung) eine immer größere Bedeutung – dies gilt insbesondere für Standards im Bereich Management und Prozesse:

- Zunehmend wird in Ausschreibung von Unternehmen oder Behörden eine Zertifizierung gefordert, um die Gefahr zu minimieren, mit einem Partner mit hohen IT-Sicherheitsrisiken zusammenarbeiten zu müssen.

- Der Nachweis eines etablierten IT-Sicherheitsmanagement kann die Bereitstellung von Kapital bei Banken erleichtern oder die Prämie einer Cyber-Versicherung günstig beeinflussen, die von immer mehr Versicherungsunternehmen angeboten wird.

- Für Unternehmen aus dem Bereich Kritischer Infrastrukturen (KRITS) wird spätestens mit der bereits heute absehbaren Verabschiedung eines »IT-Sicherheitsgesetzes« in der 18. Legislaturperiode in Deutschland die nachweisliche Nutzung von sektorspezifischen IT-Sicherheitsstandards verpflichtend. Im aktuellen Gesetzentwurf ist unter anderem die Forderung verankert, branchespezifische Standards zu entwickeln und eine Prüfung in regelmäßigen Abständen durchzuführen. Es ist weiterhin absehbar, dass hiervon nicht nur die Unternehmen der KRITIS-Branchen, sondern auch Partner und Zulieferer betroffen sein werden.

Die Vielzahl und Vielfalt der heutigen Sicherheitsstandards hat sich aus den unterschiedlichen Bedürfnissen von Unternehmen (z.B. verschiedene Branchen) aber auch aus den Rollen und Verantwortlichkeiten von Personen im Unternehmen entwickelt.

Zieht man die tiefe Durchdringung fast aller Unternehmensprozesse mit IT in Betracht, ist die große Anzahl unterschiedlicher Rollen und Funktionen, die sich mit

IT-Sicherheit auseinandersetzen müssen nicht verwunderlich. Insbesondere ist bereits heute klar, dass sich nicht mehr nur die IT-Abteilung mit dem Thema IT-Sicherheit auseinandersetzen muss, sondern praktisch jede Unternehmensfunktion, die mit personenbezogenen oder sonstigen sensiblen Daten umgeht, bzw. mit der technischen und organisatorischen Bereitstellung von Infrastrukturen und Diensten zur Unterstützung der IT befasst ist.
Im Rahmen dieses Leitfadens soll nach drei wesentlichen Blöcken unterschieden werden.

- **Management**
  Aus der Perspektive der Anwender gehört hierzu unter anderem die Rollen Geschäftsleitung, Revision, Risikomanagement, Leiter Unternehmens-IT oder Leiter Unternehmenssicherheit.

- **Prozesse**
  Hierunter können die Geschäftsprozessverantwortlichen, zentrale Unternehmensfunktionen (z.B. Einkauf, Facility Management, usw.) gezählt werden.

- **Technik**
  Hierzu gehört der IT-Betrieb, insbesondere Administratoren, Techniker.

Das folgende Bild zeigt die Zuordnung der Rollen aus der Perspektive der Anwender, ergänzt um die Sicht auf die Anbieter von Diensten und von Produkten im IT-Umfeld. Auch für die beiden letztgenannten ist eine ganze Reihe von Sicherheitsstandards maßgeblich, da die Anbieter neben den für sie selbst geltenden auch die für Kunden relevanten IT-Sicherheitsstandards als Anforderungen an Dienste und Produkte beachten müssen.

Bei den dargestellten Rollen kann keine scharfe Trennung zwischen den Blöcken Management, Prozesse und Technik vorgenommen werden. Vielfach finden sich daher Rollen wieder, die für zwei oder drei der genannten Blöcke gelten.

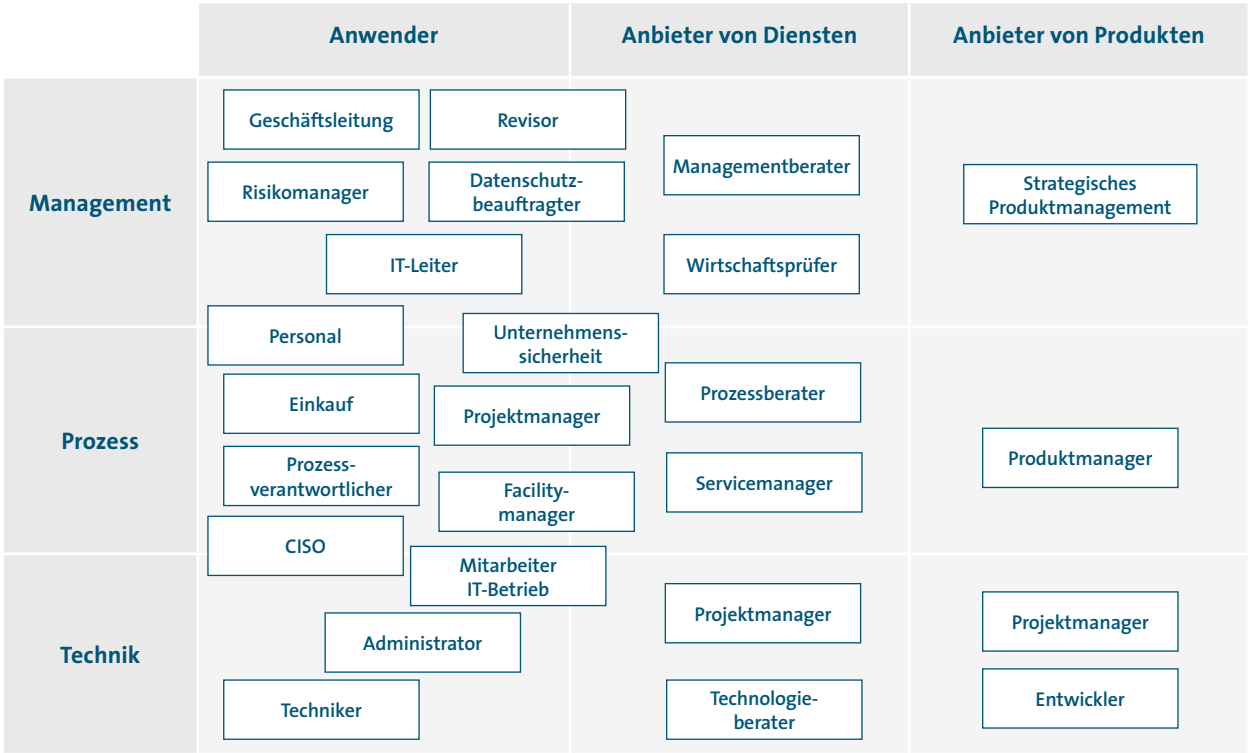

Abbildung 1: Rollen- und Funktionsmatrix

3 Arten von Standards und ihre Einsatzgebiete

3.1 Entwicklung von Normen und Standards

Weltweit gibt es zahlreiche Gremien, die sich mit der Entwicklung von Sicherheitsstandards bzw. Normen beschäftigen.

Die in diesem Leitfaden aufgeführten und beschriebenen Standards wurden von verschiedenen Gremien nach unterschiedlichen Verfahren entwickelt. In der Regel kann man das verantwortliche Gremium an der Zeichenkette zu Beginn der Kurzbezeichnung des Standards erkennen:

- **ISO/IEC-Standards**
  Bei der Mehrzahl handelt es sich um internationale Normen, die unter deutscher Mitwirkung im Subkomitee 27 »IT-Security Techniques« des Technischen Gemeinschaftskomitees »Information Technology« der Internationalen Normenorganisationen ISO und IEC, ISO/IEC JTC 1/SC 27 (http://www.jtc1sc27.din.de), nach einem Konsensverfahren entwickelt und in einer öffentlichen Umfrage bestätigt wurden. Diese Standards sind an der Zeichenkette ISO/IEC gefolgt von der Normennummer zu erkennen (Beispiel: ISO/IEC 27001).

- **DIN EN-Standards**
  Bei Standards, die mit der Zeichenkette EN beginnen, handelt es sich um Europäische Normen, die von einer der Europäischen Normenorganisationen CEN, CENELEC oder ETS, ebenfalls nach einem Konsensverfahren mit öffentlicher Umfrage, entwickelt wurden. Beginnt die Zeichenkette mit »DIN«, so handelt es sich um eine deutsche Norm. »DIN EN« bezeichnet eine Europäische Norm, die in das deutsche Normenwerk übernommen wurde.

- **Andere Standards**
  Andere Bezeichnungen (wie z.B. IT-GSHB) deuten auf Standards, die von Konsortien, Interessen-gruppen oder Behörden nach deren jeweiligen Regeln erarbeitet wurden. Diese Regeln sehen einen gegenüber den Normungsorganisationen eingeschränkten Konsensrahmen vor und legen die Mitwirkungsmöglichkeiten fest.

Die Erarbeitung deutscher Beiträge und Stellungnahmen zu internationalen Normen erfolgt durch das DIN, insbesondere durch den Arbeitsausschuss »IT-Sicherheitsverfahren« des Normenaus-schusses Informationstechnik NIA-27 (www.nia.din.de/ni27). Die Mitarbeit[1] in den Gremien des DIN ist, bei angemessener Beteiligung an den Kosten der Normungsarbeit, offen für alle interessierten Kreise – unabhängig von der Mitgliedschaft im DIN.

Die internationalen bzw. nationalen Standards werden im zeitlichen Abstand von maximal fünf Jahren einer Revision unterzogen und bei Bedarf überarbeitet. Das Veröffentlichungsdatum gibt jeweils den Abschluss der letzten Überarbeitung an. Bei der Anwendung der Standards ist es sinnvoll, bei einer aktuellen Datenbank (z.B. www.beuth.de, Verlag des DIN) die aktuelle Ausgabe anzufragen. Hier können die Standards auch bezogen werden.

[1] Anfragen zur Mitarbeit sowie zu den Projekten und Normen können gern an den Ausschuss (siehe Impressum) gestellt werden.

3.2 Wesentliche Einordnung von Standards

Standards lassen sich nach verschiedenen Kriterien sortieren. Sinnvollerweise findet eine Gruppierung nach dem Betrachtungsgegenstand (also den zu standardisierenden Inhalten statt. Die im Kompass der Sicherheitsstandards vorgesehenen Gruppen lassen sich in folgendem Bild ablesen. Im Wesentlichen orientiert sich die Struktur an der Einteilung der Standards des NIA-27 und seiner Arbeitsgruppen.

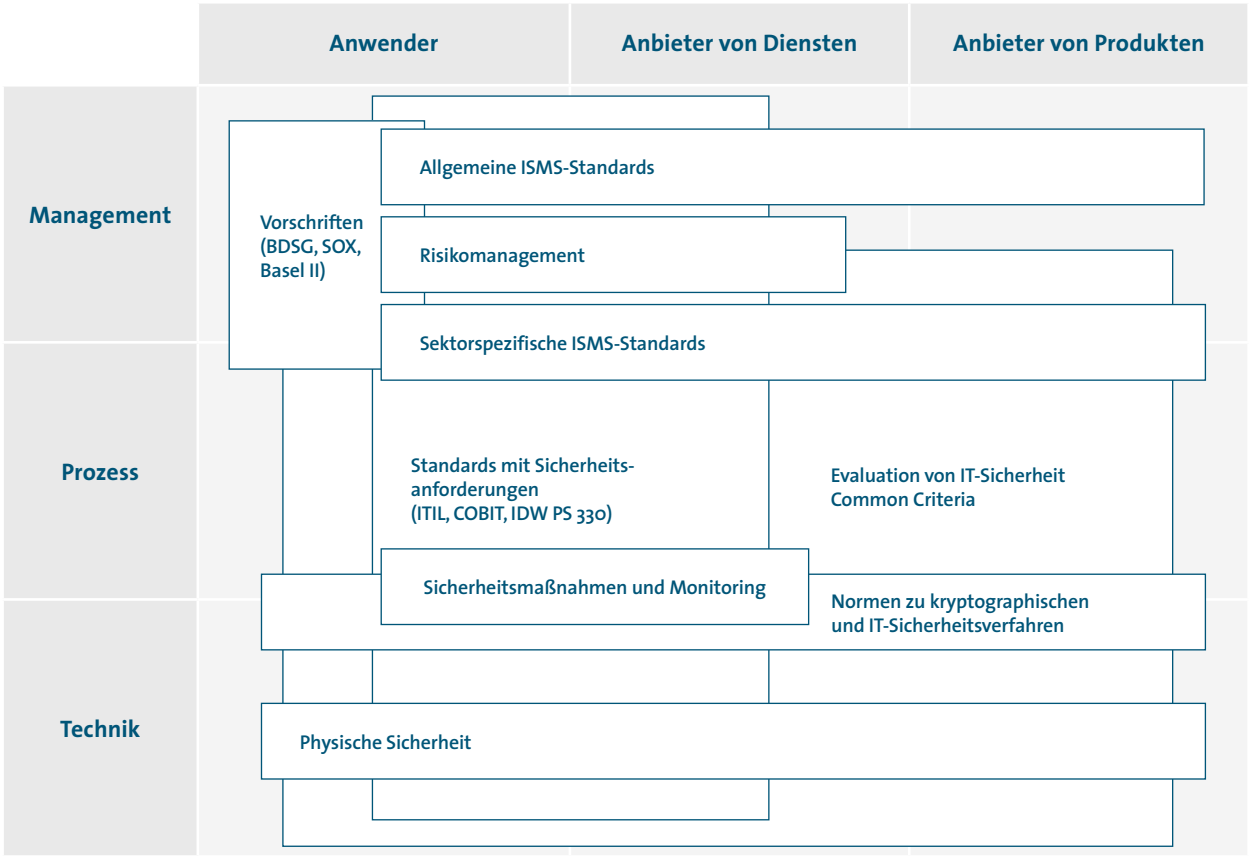

Abbildung 2: Einordnung von Standards

3.3 Zuordnung der Einzelstandards

Im Folgenden werden die grundlegenden Standards zum IT-Sicherheits- und Risikomanagement den oben dargestellten Gruppen zugeordnet

Privacy- und Identity Management

ISO/IEC 29100	Privacy framework
ISO/IEC 29101	Privacy architecture framework
ISO/IEC 24760	A framework for Identity management
ISO/IEC 29115	Entity authentication assurance framework

Biometrie

ISO/IEC 19784	Biometric application programming interface Biometrische Anwendungs-programmier-Schnittstelle(BioAPI)
ISO/IEC 19785	Common Biometric Exchange Formats Framework Rahmenbedingungen gemeinsamer biometrischer Austauschformate
ISO/IEC 19794	Biometric data interchange formats Biometrische Datenaustauschformate
ISO/IEC 30107	Presentation attack detection Presentation Attack Detection

Informationssicherheits-Managementsysteme (ISMS)

ISO/IEC 27001	Information security management systems – Requirements Informationssicherheits-Manage-mentsysteme– Anforderungen
ISO/IEC 27002	Code of practice for information security management Leitfaden zum Informationssicher-heitsmanagement

Risikomanagement

ISO/IEC 27005	Information security risk management Informationssicherheits-Risiko-management
ISO/IEC 27014	Governance of information security Governance von Informationssicherheit

Vorschriften

BDSG	Bundesdatenschutzgesetz

Evaluierung von IT-Sicherheit

Common Criteria

ISO/IEC 15408 (CC)	Evaluation criteria for IT security (Common Criteria) Evaluationskriterien für IT-Sicherheit
ISO/IEC TR 15443	A framework for IT security assurance Rahmenrichtlinien für Sicherung von IT-Sicherheit

■ ISO/IEC 18045	Methodology for IT security evaluation Methodik zur Evaluation von IT-Sicherheit
■ ISO/IEC 21827 (SSE-CMM)	System Security Engineering – Capability Maturity Model Modell der Ablaufstauglichkeit (auch ISO 21827)
■ BSI-TR-03125	Technische Richtlinie für Beweiswerterhaltung kryptographisch signierter Dokumente

Schutzprofile

■ ISO/IEC TR 15446	Guide on the production of protection profiles and security targets Leitfaden zum Erstellen von Schutzprofilen und Sicherheitsvorgaben

Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Verschlüsselung

■ ISO/IEC 18033	Encryption algorithms Verschlüsselungsalgorithmen
■ ISO/IEC 10116	Modes of operation for an n-bit block cipher Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus
■ ISO/IEC 19772	Data encapsulation mechanisms Daten verkapselnde Mechanismen
■ ISO/IEC 29192	Lightweight cryptography Leichtgewichtige Kryptographie

Digitale Signaturen

■ ISO/IEC 9796	Digital signature schemes giving message recovery Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht
■ ISO/IEC 14888	Digital signatures with appendix Digitale Signaturen mit Anhang
■ ISO/IEC 15946	Cryptographic techniques based on elliptic curves Auf elliptischen Kurven aufbauende kryptographische Techniken

Hash-Funktionen und andere Hilfsfunktionen

■ ISO/IEC 10118	Hash functions Hash-Funktionen
■ ISO/IEC 18031	Random bit generation Erzeugung von Zufallszahlen
■ ISO/IEC 18032	Prime number generation Primzahlerzeugung

Authentifizierung

■ ISO/IEC 9798	Entity authentication Authentisierung von Instanzen
■ ISO/IEC 9797	Message Authentication Codes (MACs) Nachrichten-Authentisierungscodes (MACs)

PKI-Dienste

ISO/IEC 15945	Specification of TTP services to support the application of digital signatures Spezifizierung der Dienste eines vertrauenswürdigen Drittens zur Unterstützung der Anwendung von digitalen Signaturen
ISO/IEC TR 14516	Guidelines for the use and management of Trusted Third Party Services Richtlinien für die Nutzung und das Management eines vertrauenswürdigen Dritten

Schlüsselmanagement

ISO/IEC 11770	Key management Schlüsselmanagement

Kommunikationsnachweise

ISO/IEC 13888	Non-repudiation Nicht-Abstreitbarkeit

Zeitstempeldienste

ISO/IEC 18014	Time-stamping services Zeitstempeldienste

3.4 Beschreibung der IT-Sicherheitsstandards

Jeder aufgeführte Standard bzw. Norm und jede aufgeführte Vorschrift wird in den folgenden Kapiteln kurz beschrieben:

- Die Beschreibung für jeden Standard, jede Vorschrift ist nach einem einheitlichen Schema strukturiert:
  - Inhalt und Anwendungsbereich
  - Methodik (wo sinnvoll)
  - Zertifizierung (wo sinnvoll)
  - Weitere Anmerkungen
  - Bisherige Ausgaben
  - Falls ein Abschnitt ohne Inhalte wäre, ist dieser in der Beschreibung nicht aufgeführt, z.B. können Vorschriften nicht zertifiziert werden, so entfällt bei der Vorschrift »Basel II« der Abschnitt »Zertifizierung«.
- Sofern es sich um internationale oder europäische Standards handelt, sind der Titel, das Arbeitsgebiet und der Name des Standards (englisch) aufgeführt. Englische Titel wurden verständnishalber um eine inoffizielle deutsche Übersetzung ergänzt, da nur die in das deutsche Normenwerk übernommenen Dokumente einen offiziellen deutschen Titel tragen. Bei mehrteiligen Standards bzw. einer Normenreihe wird die Nummer des jeweiligen Teils mit einem Bindestrich nach der Normennummer angefügt.
- Internationale und europäische Standards wurden formal meist nicht in das deutsche Normenwerk übernommen, weil die aufwändige Übersetzung in der Regel keinen entsprechenden Mehrwert für die Anwender schafft. Ist die Übernahme einer internationalen Norm ins deutsche Normenwerk erfolgt oder geplant, so wird dies bei den Erläuterungen im Abschnitt »Weitere Anmerkungen« ausgewiesen.

- Standards sind von anderen Standards abhängig oder beeinflussen diese. Der Bezug von Standards zu anderen Standards ist ebenfalls in der Online-Version erläutert. Diese Bezüge sind möglichst umfassend angegeben, eine Vollständigkeit kann nicht garantiert werden.

3.5 Einführung von IT-Sicherheitsstandards im Unternehmen

Die Einführung von Standards im Unternehmen erfolgt in drei generischen Schritten:

Auswahl des Standards

In der Regel entscheidet die Geschäftsführung mit Unterstützung des – falls vorhanden – IT-Sicherheitsbeauftragten, IT-Risikobeauftragten und IT-Verantwortlichen den IT-Betrieb vom Unternehmen an einem IT-Sicherheitsstandard auszurichten. Welcher Standard der richtige für ein Unternehmen ist, hängt von einigen Faktoren (siehe Kompass) ab:

- Art des Unternehmens
- Relevanter Unternehmensbereich für die Standardisierung
- Relevante Charakteristika des Standards

Einführung

Die Einführung von IT-Sicherheitsstandards im Unternehmen erfolgt nach dem jeweiligen Vorgehensmodell des ausgewählten Standards. Als Beispiel sei hier das Vorgehensmodell nach BSI IT-Grundschutz aufgeführt:

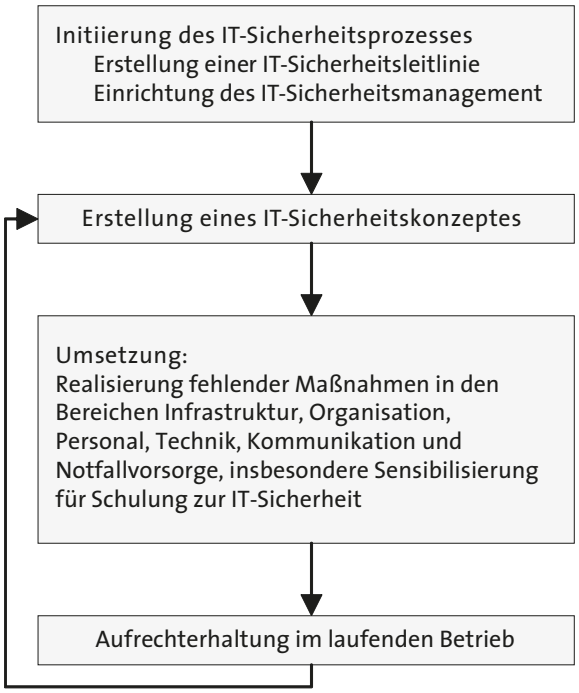

Abbildung 3: Vorgehensmodell nach BSI IT-Grundschutz

Die Notwendigkeit der einzelnen Schritte des jeweiligen Vorgehensmodell sollten vor der Einführung auf Relevanz geprüft werden. Anschließend sind die ausgewählten Schritte durchzuführen und die Maßnahmen zur Umsetzung des Standards festzulegen. Hierbei ist zu beachten, dass für die Umsetzung des Modells externes Know-how zugezogen bzw. Mitarbeiter entsprechend geschult werden sollten. Die Einführung eines Standards ohne externes oder internes Know-how führt in der Regel zu einem höheren Aufwand bei eventuell schlechterem Ergebnis.

Betrieb

Nach der Einführung des Standards müssen die getroffenen Maßnahmen (personell, organisatorisch, technisch) in den regulären Betrieb übergehen. Hierfür sind Mitarbeiterschulungen, -information sowie ggf. Prozessanpassungen notwendig. Im Rahmen des regulären IT-Betriebs kann die Einhaltung des Standards durch zwei aufeinander aufbauende Verfahren überprüft und gewährleistet werden:

- **Auditierung**
  Ein wichtiges Element des Vorgehensmodells ist, die Einhaltung und Aktualität der Sicherheitsmaßnahmen in regelmäßigen Audits von internen oder externen Partnern zu überprüfen. Mit diesem Vorgehen können Unternehmen ihre IT-Sicherheit immer weiter verbessern und sukzessive Sicherheitslücken schließen.
  Im Rahmen eines Audits kommt ein externer (zertifizierter) Auditor für einige Tage ins Unternehmen. Anhand der Vorgaben des Standards bzw. der Dokumentation des IT-Betriebs wird der Ist-Stand mit dem Soll-Konzept verglichen. Empfehlungen für die Verbesserung der IT-Sicherheit werden ausgesprochen. Diese sollten vom Unternehmen im Nachgang umgesetzt werden.
  Eine Auditierung kann den gesamten IT-Betrieb umfassen, kann sich aber auch nur auf beispielsweise neu eingesetzte Sicherheitskomponenten beschränken (z.B. neue Firewall).

- **Zertifizierung**
  Einige IT-Sicherheitsstandards können als Grundlage für eine Zertifizierung herangezogen werden. Ein Zertifikat ist eine unabhängige Bestätigung dafür, dass alle (soweit anwendbare) im Standard geforderten Sicherheitsmaßnahmen zum Zeitpunkt der Zertifizierung dokumentiert und tatsächlich umgesetzt sind. Durch die Ausstellung eines Zertifikates, mit dem die Umsetzung des Standards bestätigt wird, kann dies Dritten transparent gemacht werden. Dritte können hierbei Kunden, Banken, Versicherungen oder auch die Öffentlichkeit sein.
  Der Aufwand für die Zertifizierung ist abhängig vom Unternehmen und dem Zertifizierungs¬ziel. Hierbei kann jedoch von einem externen Aufwand von einigen Tagen bis einigen Wochen ausgegangen werden. Der interne Aufwand kann deutlich höher sein, je nach Vorbereitungs¬stand des Unternehmens. Eine generelle Aussage kann nicht getroffen werden.
  Bei der Auswahl des Zertifizierers ist zu beachten, dass einige Standards einen akkreditierten Zertifizierer fordern.

4 Für Elektronische Identitäten relevante Standards

4.1 Privacy- und Identity Management

Angesichts der umfassenden Nutzung personenbezogener oder personenbeziehbarer Informationen in immer mehr IKT-Anwendungen wächst die Herausforderung, diese Informationen und die entsprechenden Persönlichkeitsrechte zu schützen. Darum gibt es mehr Normen zu Datenschutz und Identitätsmanagement. Zuständig dafür ist seit 2006 die WG 5 »Identity Management and Privacy Technologies« bei ISO/IEC JTC 1/SC 27.

Die derzeit wichtigsten Projekte aus dem Arbeitsprogramm von WG 5 sind:

4.1.1 ISO/IEC 29100

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Privacy framework

Inhalt und Anwendungsbereich

Die Norm ISO/IEC 29100:2011 ist ein Rahmenwerk zu Privacy bzw. Datenschutz.

ISO/IEC 29100:

- definiert die einschlägige Terminologie;
- spezifiziert die Akteure und ihre Rollen bei der Verarbeitung personenbeziehbarer Daten;
- beschreibt beim Schutz der Privatsphäre zu berücksichtigende Aspekte und entsprechende technische Ansätze
- liefert Verweise wesentliche Datenschutzgrundsätze für die Informationstechnologie.

Weitere Anmerkungen

ISO/IEC 29100 ist einschlägig für Spezifikation, Beschaffung, Entwurf, Entwicklung, Test, Wartung, Verwaltung und Betrieb von Informations-und Kommunikationstechnologien, -systemen oder -dienstleistungen, die personenbeziehbare Daten verarbeiten.

ISO/IEC 29100:2011 bezieht sich auf Standing Document (SD) 2 »Privacy references«, kostenfrei erhältlich via http://www.jtc1sc27.din.de/sbe/wg5sd2 .

Bisherige Ausgaben

- ISO/IEC 29100:2011

4.1.2 ISO/IEC 29101

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Privacy architecture framework

Inhalt und Anwendungsbereich

ISO/IEC 29101 bietet ein Rahmenwerk für Datenschutzarchitekturen.

ISO/IEC 29101

- spezifiziert technische Aspekte des Datenschutzes, die bei Informations- und Kommunikationstechnologie bei der Verarbeitung personenbezogener Daten – zu beachten sind.
- listet Komponenten für die Implementierung datenschutzfreundlicher Systeme auf.

- enthält Architekturansichten, die diese Komponenten in Kontext zueinander bringen.
- enthält Leitlinien für Planung, Konzeption und Bau von IKT-Systemarchitekturen, die die Privatsphäre der Personen, deren Daten verarbeitet werden, schützen, indem sie die Verarbeitung von personenbeziehbaren Informationen kontrollierbar machen.
- zeigt, wie Privacy Enhancing Technologies (PETs) als Datenschutzkontrollmechanismen eingesetzt werden können.

Weitere Anmerkungen

Die Norm ISO/IEC 29101:2013 ist einschlägig für Spezifikation, Beschaffung, Entwurf, Entwicklung, Test, Wartung, Verwaltung und Betrieb von Informations-und Kommunikationstechnologien, -systemen oder -dienstleistungen, die personenbeziehbare Daten verarbeiten. Sie baut auf dem Datenschutzrahmenwerk ISO/IEC 29100:2011 auf und hilft Organisationen, Datenschutzmaßnahmen zu definieren.

Bisherige Ausgaben

- ISO/IEC 29101:2013

4.1.3 ISO/IEC 24760

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	A framework for identity management

Inhalt und Anwendungsbereich

ISO/IEC 24760 ist einschlägig für alle Systeme, die Identitätsinformationen verarbeiten, und wird zukünftig aus drei Teilen bestehen:

Teil 1: »Terminology and concepts«

- definiert die wesentlichen Begriffe für das Identitätsmanagement, etwa partielle Identitäten,
- spezifiziert die Kernkonzepte von Identität und Identitätsmanagement sowie ihre (oft subtilen) Beziehungen zueinander,
- enthält eine Bibliographie zu den verschiedenen Aspekten des Identitätsmanagements,
- ist kostenfrei erhältlich via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Teil 2 (in Erarbeitung): »Reference architecture and requirements« (CD 24760-2) spezifiziert eine Referenzarchitektur und die Anforderungen entlang des Lebenszyklus von Identitäten.

Teil 3 (in Erarbeitung): »Practice« (WD 24760-3) liefert Hinweise und Beispiele für »Best Practises« beim Identitätsmanagement.

Bisherige Ausgaben

- ISO/IEC 24760-1:2011

4.1.4 ISO/IEC 29115

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Entity authentication assurance framework

Inhalt und Anwendungsbereich

Die Norm ISO/IEC 29115 bietet ein Rahmenwerk zur Authentifizierung beliebiger Entitäten. Insbesondere spezifiziert sie vier Assurance Levels (LoA) für

Authentifizierung und die Kriterien und Richtlinien zur Erreichung jedes der vier Niveaus. Zusätzlich gibt sie Anleitungen

- für die Einordnung anderer Authentifizierungssicherungssysteme in den vier Niveaus,
- für den Austausch der Ergebnisse einer Authentifizierung, die auf den vier LoAs basiert,
- zu den Kontrollmöglichkeiten, um Bedrohungen in Bezug auf Authentifizierung zu mildern.

Bisherige Ausgaben

- ISO/IEC 29115:2013

4.1.5 ISO/IEC 29191

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Requirements for partially anonymous, partially unlinkable authentication

Inhalt und Anwendungsbereich

Die Norm ISO/IEC 29191 bietet ein Rahmenwerk für das Gebiet der teilweise anonymen, teilweise unverkettbaren Authentisierung und beschreibt die einschlägigen Anforderungen.

In vielen Fällen wird eine Entität, etwa ein Nutzer, bei einer Authentisierung so umfassend identifiziert, dass diese Entität bei anderen Authentisierungen gegenüber anderen Partnern als dieselbe Entität wiedererkannt werden kann. Diese Verknüpfbarkeit zweier Aktivitäten einer Entität stellt ein erhebliches Risiko für Privatsphäre und Datenschutz dar, etwa wenn die eine Authentisierung bei einer Diskussionsplattform über möglicherwiese illegale Praktiken einer Organisation erfolgt und die andere Authentisierung bei der Organisation selbst stattfindet. Dem Nutzer können dann Nachteile für seine Meinungsäußerung entstehen.

ISO/IEC 29191 behandelt Anforderungen und Technologien, die solchen Problemen abhelfen können, indem sie die möglicherweise gefährlichen Verknüpfbarkeiten reduzieren.

Bisherige Ausgaben

- ISO/IEC 29191:2012

4.1.6 ISO/IEC 24745

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Biometric information protection

Inhalt und Anwendungsbereich

ISO/IEC 24745 liefert Hinweise zum Schutz biometrischer Informationen bezüglich verschiedener Anforderungen nach Vertraulichkeit, Integrität, Erneuerbarkeit und Rückrufbarkeit während der Speicherung und dem Transfer dieser Informationen Zusätzlich enthält ISO/IEC 24745 Anforderungen und Hinweise für die sichere und datenschutzkonforme Verwaltung und Verarbeitung biometrischer Information.

Bisherige Ausgaben

- ISO/IEC 24745:2011

4.2 Biometrie

Biometrische Verfahren werden verstärkt bei Grenzkontrollen, für die Zutrittskontrolle bei Sicherheitsbereichen, sowie für einen kontrollierten Zugang zur Informationstechnologie eingesetzt. Für die sichere und effiziente Nutzung von Ausweisdokumenten mit biometrischen Referenzdaten und Sensoren in offenen Systemen sind Interoperabilität sowie ein reibungsloser Datenaustausch zwischen Anwendungen und Systemen unerlässlich.

Die internationale Normung, im Unterkomitee 37 des ISO/IEC Gemeinschafts-komitees 1 »Information Technology« (ISO/IEC JTC 1), schafft hierfür grundlegende Voraussetzungen. Im Bereich der »Biometrie« werden generische biometrische Technologien zur Unterstützung der Interoperabilität und des Datenaustausches zwischen Anwendungen und Systemen genormt. Das Arbeitsgebiet umfasst biometrische Anwendungsprogramm-Schnittstellen, biometrische Datenaustauschformate, biometrische Auswahl-Normen (sogenannte Profile), Testverfahren und Berichte für biometrische Technologien, sowie die Berücksichtigung gesellschaftlicher und juristischer Aspekte wie Schutz der Privatsphäre, Verbraucherschutz und Schutz vor Benachteiligung bei persönlichen Behinderungen.

4.2.1 ISO/IEC 19784

Arbeitsgebiet:	Informationstechnik – Biometrie
Name des Standards:	Biometric application programming interface Biometrische Anwendungsprogrammier-Schnittstelle (BioAPI)

Inhalt und Anwendungsbereich

In den Normen der Reihe ISO/IEC 19784 werden die Architektur und Schnittstellen definiert, die es erlauben Komponenten biometrischer Anwendungen verschiedener Hersteller zu kombinieren und damit die proprietären Verfahren der verschiedenen Hersteller zusammenzuführen. Die Spezifikationen umfassen die Funktion, die für die biometrische Identifikation erforderlich sind, ebenso die Schnittstellen-Spezifikationen und die Verwaltung biometrischer Daten. BioAPI ist auf ein breites Spektrum biometrischer Verfahren und Anwendungen, angefangen von persönlichen Geräten über Netzwerk-Sicherheitsanwendungen bis hin zu großen, komplexen Identifikationssystemen, anwendbar.

Die Normenreihe umfasst sechs Teile, wobei die Teile 5 und 6, die sich mit biometrischen Verarbeitungs- und Abgleichalgorithmen befassen, noch in Erarbeitung sind. Der Teil 1, in dem BioAPI 2.0 festgelegt ist, wird derzeit einer Revision unterzogen.

Teil 1: BioAPI-Spezifikation

Teil 2: Schnittstelle zum Erbringer einer biometrischen Archiv-Funktion

Teil 4: Schnittstelle zum Erbringer einer biometrischen Sensor-Funktion

Part 5: Biometric processing algorithm function provider interface (in Arbeit)

Part 6: Biometric matching algorithm function provider interface (in Arbeit)

Durch die beiden Normenreihen ISO/IEC 19784 Biometrische Anwendungsprogrammier-Schnittstelle (BioAPI) und ISO/IEC 19785 Rahmenbedingungen gemeinsamer biometrischer Austauschformate wird eine Vereinheitlichung der Schnittstelle zu den unterschiedlichen Biometrie-Anwendungen und der bei der Übertragung über diese Schnittstelle verwendeten Datenformate angestrebt.

Bisherige Ausgaben

- ISO/IEC 19784-1:2006
- ISO/IEC 19784-2:2007
- ISO/IEC 19784-4:2011

4.2.2 ISO/IEC 19785

Arbeitsgebiet:	Informationstechnik – Biometrie
Name des Standards:	Common Biometric Exchange Formats Framework Rahmenbedingungen gemeinsamer biometrischer Austauschformate

Inhalt und Anwendungsbereich

Das Common Biometric Exchange File Format (CBEFF) beschreibt die Datenelemente, die nötig sind, um biometrische Technologien systemübergreifend zu nutzen. Diese Daten werden in einer einzelnen Datei gespeichert, die für den Austausch von biometrischen Informationen zwischen verschiedenen Systemkomponenten oder unterschiedlichen Systemen verwendet wird. Dadurch wird ein Austausch der biometrischen Daten möglich und die Interoperabilität der biometrisch-basierten Anwendungen und Systeme verschiedener Hersteller gefördert.

Nachdem bereits 2006 bzw. 2007 die drei ersten Teile der Normenreihen zu technologie-übergreifenden Austauschformaten (Reihe ISO/IEC 19785, Common Biometric Exchange Formats Framework, CBEFF) veröffentlicht werden konnten, wurde in 2010 Teil 4 als Ergänzung zu den bereits veröffentlichten Normen herausgegeben, der die Spezifikation des Formates für das Sicherheitsfeld enthält. Die Normenreihe ISO/IEC 19785 besteht derzeit aus den folgenden Teilen, wobei Teil 1 und Teil 3 sich derzeit in der Revision befinden:

Teil 1: Spezifikation der Datenelemente

Teil 2: Verfahren für den Betrieb der biometrischen Registrierungsinstanz

Teil 3: Spezifikation anwendungsbezogener Formate

Teil 4: Spezifikation des Formates für das Sicherheitsfeld

Im Teil 1 des »Common Biometric Exchange Formats Framework« (CBEFF) werden allgemeine Rahmenbedingungen für Austauschformate für biometrische Daten festgelegt und ein abstraktes Rahmenformat (Biometric Information Record) für biometrische Daten beschrieben. Dieses Rahmenformat enthält einen Kopfteil (Standard Biometric Header – SBH), einen Rumpfteil (Biometric Data Block – BDB) und am Ende einen optionalen elektronischen Signaturblock (SB). Für den Kopfteil werden abstrakte Datenelemente definiert, die den Biometrietyp (z. B. Fingerabdruck), den Formatinhaber und Formattyp der im Rumpfteil enthaltenen biometrischen Daten und weitere Attribute der biometrischen Daten bezeichnen. Der Biometric Data Block ist für die eigentlichen biometrischen Daten vorgesehen, deren Struktur in der CBEFF-Spezifikation nicht näher definiert wird.

Teil 2 definiert die Registrierungsverfahren für biometrische Organisationen, Datenformate, Produkte und Patronformate. Als CBEFF-Registrierungsinstanz ist IBIA (International Biometric Industry Association) festgelegt. Eine registrierte biometrische Organisation kann sowohl biometrische Datenformate, als auch eigene Patronformate definieren und diese bei IBIA registrieren.

Im Teil 3 werden so genannte Patronformate spezifiziert. Dabei handelt es sich um konkrete CBEFF-Formate, die die abstrakten Definitionen der CBEFF-Struktur und der Header für verschiedene Anwendungsbereiche übersetzen.

Bisherige Ausgaben

- ISO/IEC 19785-1 2006
- ISO/IEC 19785-2 2006
- ISO/IEC 19785-3 2007
- ISO/IEC 19785-4 2010

4.2.3 ISO/IEC 19794

Arbeitsgebiet:	Informationstechnik – Biometrie
Name des Standards:	Biometric data interchange formats Biometrische Datenaustauschformate

Inhalt und Anwendungsbereich

Mit der Normenreihe ISO/IEC 19794 über »Informationstechnik – Biometrische Datenaustauschformate« wurde über die letzten Jahre für eine Anzahl von biometrischen Modalitäten jeweils eindeutige, harmonisierte Datenaustauschformate genormt.

Derzeit besteht die Reihe ISO/IEC 19794 aus vierzehn Teilen:

Teil 1: Rahmenbedingungen

Teil 2: Austauschformat basierend auf Finger-Minuzien

Teil 3: Spektrale(s) Muster der Finger – Daten

Teil 4: Austauschformat basierend auf Fingerabdrucksbildern

Teil 5: Austauschformat basierend auf Gesichtsbildern

Teil 6: Austauschformat basierend auf Irisbildern

Teil 7: Zeitreihendaten basierend auf Unterschriften/Kurzzeichen

Teil 8: Daten skelettierter Fingerabdrücke

Teil 9: Daten basierend auf Blutgefäßbildern

Teil 10: Austauschformat basierend auf Handgeometrie-Konturendaten

Teil 11: Verarbeitete dynamische Unterschrifts- und Kurzzeichen-Daten

Teil 13: Stimmdaten (in Arbeit)

Teil 14: Austauschformat basierend auf DNA-Daten

Part 15: Palm Crease Image Data (in Arbeit)

ISO/IEC 19794-1 enthält Informationen, die für alle folgenden Teile der Reihe relevant sind und bietet eine Einführung in das Beziehungsgeflecht der SC 37-Normen und eine Veranschaulichung eines allgemeinen biometrischen Systems nebst seiner Teilsysteme zur Datenerfassung, zur Merkmalsextraktion, zur Datenspeicherung und für den Datenvergleich und die Entscheidungsfindung. ISO/IEC 19794-1 illustriert ferner die Funktionen eines biometrischen Systems wie Enrolment, Verifikation und Identifikation und erklärt das Konzept der Einbettung der Datenaustauschformate in die CBEFF-Struktur.

Die Teile 2-15 detaillieren dann die oben genannten Spezifizierungen für das jeweilige biometrische Charakteristikum und legen die Austauschformate für den Austausch von Bildern und biometrischen Referenzen fest.

Weitere Anmerkungen

Nachdem das ISO/IEC JTC 1/SC 37 »Biometrie« im Jahre 2002 gegründet wurde, wurden nach einer sehr kurzen Vorbereitungsphase bereits in 2005 die ersten internationalen Normen veröffentlicht. In diesen Normen der ersten Generation wurden Austauschformate für Finger-, Gesichts- und Irisbilder, Unterschriften/Kurzzeichen, Blutgefäßbildern und Handgeometriedaten festgelegt. An der zweiten Generation dieser Austauschformate wird seit 2007 gearbeitet. Dabei werden die einzelnen Teile weiter gemäß den Vorgaben aus ISO/IEC 19794-1 harmonisiert und neueren technischen Entwicklungen Rechnung getragen, indem die Konformitätstests und Codierung der Datenfelder im XML-Format mit aufgenommen werden.

Bisherige Ausgaben

- ISO/IEC 19794-1:2006; 2011
- ISO/IEC 19794-2:2005; 2011
- ISO/IEC 19794-3:2006
- ISO/IEC 19794-4:2005; 2011
- ISO/IEC 19794-5:2005; 2011
- ISO/IEC 19794-6:2005; 2011
- ISO/IEC 19794-7:2007; 2014
- ISO/IEC 19794-8:2006; 2011
- ISO/IEC 19794-9:2007, 2011
- ISO/IEC 19794-10:2007
- ISO/IEC 19794-11:2013
- ISO/IEC 19794-14:2013

4.2.4 ISO/IEC 30107

Arbeitsgebiet:	Informationstechnik – Biometrie
Name des Standards:	Presentation attack detection Presentation Attack Detection

Inhalt und Anwendungsbereich

Mit der Nutzung der biometrischen Technologien geht die Notwendigkeit zur Beschäftigung mit den Sicherheitsproblemen und Gegenmaßnahmen zum Erkennen und Vereiteln von Überwindungs- und Umgehungsversuchen eines biometrischen Systems einher.

Subversionen einer beabsichtigten Funktion einer biometrischen Technologie können an jeder Stelle im Sicherheitssystem auftreten und sowohl auf einen internen als auch externen Angreifer zurückgehen. Die derzeit in der Entwicklung befindliche Norm wird sich mit den Techniken für die automatische Erkennung von »Presentation Attacks«, d. h. Versuchen bei der Präsentation und Abgabe der relevanten biometrischen Daten das biometrische System zu überwinden, beschäftigen. Diese Techniken werden in der Norm als »Presentation Attack Detection« (PAD)-Methoden bezeichnet.

Der Zweck der neu zu erarbeitenden Norm ist es, durch die Definition von Begriffen und Formaten eine Basis für die Spezifizierung, Charakterisierung und Evaluierung von »Presentation Attack Detection«-Methoden zu schaffen. Die Norm empfiehlt jedoch keinen bestimmten Algorithmus als einheitliches PAD-Tool.

Das Projekt wird in einer Normenreihe, bestehend aus drei Teilen, bearbeitet:

Teil 1: Rahmenbedingungen

Teil 2: Datenformate

Teil 3: Testen, Berichten und Klassifizierung von Attacken

Der Teil 1 der Internationalen Norm hat mittlerweile den Committee Draft-Status erreicht, Teil 2 und 3 liegen im internationalen Normungsgremium ISO/IEC JTC 1/SC 37 als Working Draft vor.

4.3 Informationssicherheits-Managementsysteme

Der bedeutendste Standard für ein Informationssicherheits-Managementsystem ist die Norm ISO/IEC 27001. Sie beschreibt die grundlegenden Anforderungen an das ISMS in einer Organisation (Unternehmen oder Behörde).

Weitere Standards aus der ISO/IEC 27000er-Familie ergänzen ISO/IEC 27001. So wird in ISO/IEC 27000:2009 die Terminologie, in ISO/IEC 27002 (zuvor ISO/IEC 17799) werden einzelne Maßnahmen erläutert. Darüber hinaus werden in ISO/IEC 27006 die Anforderungen an Stellen beschrieben, die ein ISMS auditieren bzw. zertifizieren. Eine Reihe weiterer Standards in der 27000er-Reihe befindet sich zurzeit in der Erstellung.

Das vom BSI herausgegebene IT-Grundschutzhandbuch erläutert ebenfalls die Anforderungen an ein ISMS und ist mit ISO/IEC 27001 kompatibel.

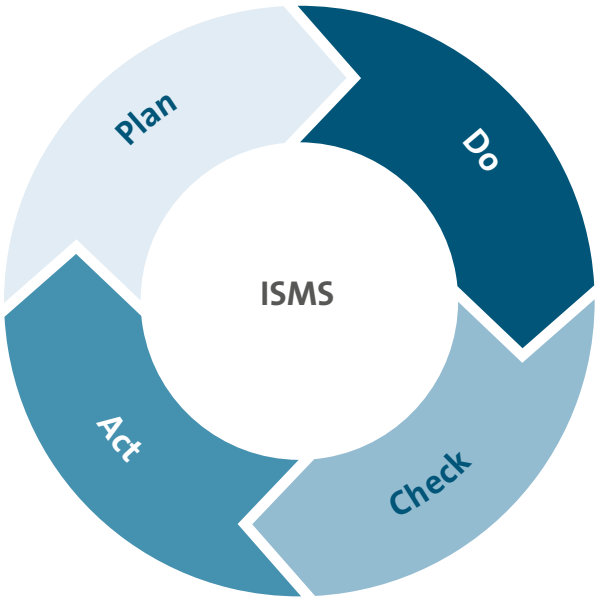

Abbildung 4: Regelkreislauf des ISMS

4.3.1 ISO/IEC 27001

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Information security management systems – Requirements Informationssicherheitsmanagementsysteme – Anforderungen

Inhalt und Anwendungsbereich

ISO/IEC 27001 legt die Anforderungen für die Errichtung, Einführung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems fest. Da das Dokument sehr generisch gehalten ist, um auf alle Organisationen unabhängig von Typ, Größe und Geschäftsfeld anwendbar zu sein, haben diese Anforderungen einen niedrigen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse wohl definiert sind. Aufbauend auf der Norm werden nationale Zertifizierungsschemata definiert.

Methodik

ISO/IEC 27001 berücksichtigt den in den ISO/IEC Direktiven Teil 1 festgeschriebenen Annex SL, der eine einheitliche Struktur und Wortwahl für Managementsysteme, bis hin zu identischen Kapiteln und einheitlichen Begriffsdefinitionen vorgibt. Die Struktur des ISMS ist damit kompatibel zu anderen Managementsystemen, die unter Berücksichtigung des Annex SL standardisiert sind wie z.B. zukünftig das Qualitätsmanagementsystem nach ISO 9000. Ein ISMS erlaubt es, ermittelte Risiken durch geeignete, in die Organisationsprozesse eingebettete Kontrollmechanismen zu reduzieren, zu verlagern oder anders zu kontrollieren. Hierbei sind die Geschäftsziele und die resultierenden Sicherheitsanforderungen als Input sowie »gemanagte« Informationssicherheit als Output anzusehen. Die transformierenden Systemprozesse sind das Aufbauen, das Umsetzen und Betreiben, das Überprüfen sowie das Aufrechterhalten und Verbessern.

Als Managementstandard richtet sich das Dokument an die Geschäftsleitung und den IT-Sicherheitsbeauftragten, weniger an die Umsetzungsverantwortlichen, Techniker oder Administratoren.

Zertifizierung

Der Grad der Umsetzung des Informationssicherheits-Managementsystems kann von internen oder externen Parteien (Auditoren) kontrolliert werden. Bisher war es in Deutschland möglich sich mit dem vom BSI herausgegebenen Zertifikat »ISO/IEC 27001 auf Basis IT Grundschutz« nach ISO/IEC 27001:2005 zertifizieren zu lassen. Durch die Neuausgabe der ISO/IEC 27001 müsste das Grundschutzzertifikat angepasst werden, was derzeit aber nicht abzusehen ist. Die Übergangsfrist für bestehende Zertifikate wurde von der IAF auf 2 Jahre festgelegt, bis Oktober 2015.

Die Zertifizierung erfolgt durch akkreditierte Unternehmen, sogenannte Zertifizierungsstellen. Eine aktuelle Liste der akkreditierten Stellen, auch für andere Zertifizierungen, kann bei der DAkkS – Deutsche Akkreditierungsstelle GmbH (http://www.dakks.de) abgerufen werden.

Weitere Anmerkungen

Wegen der engen methodischen Anlehnung an die ISO 9000 (Qualitätsmanagement) und die ISO 14000 (Umweltmanagement) kann die ISO/IEC 27001 als ein Qualitätsstandard für Managementsysteme bezüglich der Informationssicherheit angesehen werden.

ISO/IEC 27001:2013 wird im Laufe des Jahres 2014 als DIN ISO/IEC 27001 als deutsche Sprachfassung ins Deutsche Normenwerk übernommen.

Bisherige Ausgaben

- ISO/IEC 27001:2005
- ISO/IEC 27001:2013

4.3.2 ISO/IEC 27002 (zuvor 17799)

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Code of practice for information security management Leitfaden zum Informationssicherheitsmanagement

Inhalt und Anwendungsbereich

Ziel von ISO/IEC 27002 ist es, Informationssicherheit als Gesamtaufgabe darzustellen, da es »guidelines and general principles for [...] information security management in an organization« enthält. In den Prozess der Informationssicherheit sind alle Bereiche der Organisation einzubeziehen, da alle an der Erhebung, Verarbeitung, Speicherung und Löschung von Informationen beteiligt sind. Der Anwendungsbereich ist somit ohne einen konkreten Bezug zu den Anforderungen in einer Organisation nicht abgrenzbar. Das Dokument richtet sich an IT-Sicherheitsbeauftragte.

Methodik

Der Standard legt Richtlinien und allgemeine Prinzipien für das Initiieren, Umsetzen, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements in einer Organisation fest. Er ist logisch in vierzehn Überwachungsbereiche gegliedert, auf die das Sicherheitsmanagement thematisch angewendet wird:

- Sicherheitsleitlinien (information security policies)
- Organisation der Informationssicherheit (organization of information security)
- Personalsicherheit (human resources security)
- Management von organisationseigenen Werten (asset managment)
- Zugangskontrolle (access control)

- Kryptographie (cryptography)
- Physische und umgebungsbezogene Sicherheit (physical and environmental security)
- Betriebssicherheit (operations security)
- Kommunikationssicherheit (communications security)
- Beschaffung, Entwicklung und Wartung von Informationssystemen (information systems acquisition, development and maintenance)
- Lieferantenbeziehungen (supplier relationships)
- Umgang mit Informationssicherheitsvorfällen (information security incident management)
- Sicherstellung des Geschäftsbetriebs (business continuity management)
- Einhaltung von Vorgaben (compliance)

ISO/IEC 27002 ist ursprünglich als ISO/IEC 17799 aus dem Teil 1 des britischen Standards BS 7799-1 hervorgegangen. Aufgrund der Bestrebungen, alle Standards, die ISMS betreffen, als ISO/IEC 27000er-Reihe zusammenzuführen, wurde ISO/IEC 17799 im Jahr 2007 in ISO/IEC 27002:2005 umbenannt.
Die ISO/IEC 27002:2005 wurde als DIN ISO/IEC 27002:2009 ins Deutsche Normenwerk übernommen.

Bisherige Ausgaben

- ISO/IEC 17799:2000
- ISO/IEC 17799:2005 (2. Ausgabe)
- ISO/IEC 27002:2005 (textgleich mit ISO/IEC 17799:2005)
- ISO/IEC 27002:2013

Risikomanagement

Definition: Risikomanagement ist der Führungsprozess zur Bewältigung der in einer Unternehmung entstehenden Risiken. Das Ziel des IT-Sicherheitsmanagements ist die Risikoreduktion des Gesamtrisikos bis zum akzeptierbaren bzw. tragbaren Restrisiko:

- **Risikovermeidung:**
  Dabei werden Risiken, denen ausgewichen werden kann, vermieden. Dies kann beispielsweise die Wahl eines geeigneten Raums oder der Aufstellungsort eines Servers sein.
- **Risikoverminderung durch Schutzmaßnahmen:**
  Entgegen der Vermeidung, werden hier Risiken teilweise akzeptiert. Durch geeignete Schutzmaßnahmen werden diese Risiken vermindert. Dies kann beispielsweise das Patchen von Systemen sein.
- **Risikobegrenzung:**
  Durch geeignete Maßnahmen wird bei Eintreten eines Risikos der Schaden begrenzt. Dies können beispielsweise Feuerlöschsysteme in einem Raum sein.
- **Risikoüberwälzung:**
  Bei der Risikoüberwälzung wird das Risiko durch faktische oder vertragliche, teilweise oder vollständig an Dritte übertragen. Dies kann beispielsweise durch Versicherungen der Fall sein oder die Abwälzung auf Vertragspartner.
- **Risikoakzeptanz:**
  Die Vermeidung, Verminderung und Überwälzung von Risiken kann die Risiken nicht vollständig ausschliessen. Das verbleibende Restrisiko muss das Unternehmen akzeptieren und selbst tragen.

Das Risikomanagement ist ein ständiger Prozess. Es ist wichtig, regelmäßig die Risiken zu überarbeiten. Sind neue Risiken entstanden? Haben sich Risiken verändert? Es gilt diese Risiken zu erkennen und in einem weiteren Schritt diese zu bewerten.

Folgende Schritte sind daher ständig durchzuführen:

- Risiken sind zu erkennen
- Risiken sind in Bezug auf die Geschäftseinflüsse und die Eintrittswahrscheinlichkeiten zu bewerten
- Die Eintrittswahrscheinlichkeiten und Konsequenzen dieser Risiken sind abzuschätzen
- Es müssen Prioritäten zur Abschwächung der Risiken definiert werden
- Alle involvierten Parteien und Personen müssen informiert und, falls notwendig, geschult werden
- Die getroffenen Maßnahmen müssen auf ihre Effektivität überwacht werden
- Es müssen geeignete Möglichkeiten zur Abwälzung der Risiken gesucht und umgesetzt werden
- Die Restrisiken müssen bewusst getragen werden

4.3.3 ISO/IEC 27005

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Information Security Risk Management Management von Informationssicherheitsrisiken

Inhalt und Anwendungsbereich

Die ISO/IEC 27005 ist aus dem Teil 2 des bisherigen ISO/IEC 13335-2 hervorgegangen. Der Standard enthält Leitlinien für ein systematisches und prozessorientiertes Risikomanagement, das gegebenenfalls auch die Einhaltung der Anforderungen an das Risikomanagements nach ISO/IEC 27001 unterstützt.

Methodik

Ein Informationssicherheitsrisiko wird definiert als Potential, dass eine Bedrohung eine Schwachstelle eines Unternehmenswertes ausnutzt und dadurch zu einem Schaden für eine Organisation führt. Zur systematischen Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken wird ein Prozess beschrieben, der als Ergebnis eine priorisierte Liste von Risiken hat, die anschließend kontinuierlich zu verfolgen sind.

Im Einzelnen definiert der Standard die folgenden wesentlichen Schritte beim Management von Informationssicherheitsrisiken:

- **Definition der Rahmenbedingungen (Context establishment)**
  Zur Definition der Rahmenbedingungen gehören dann die Festlegung von Kriterien zur Bewertung und Akzeptanz von Risiken, die Abgrenzung des Betrachtungsbereiches sowie die Etablierung einer Organisation für das Risikomanagement.

- **Identifizierung von Risiken (Risk identification)**
  Risiken werden identifiziert, indem alle Unternehmenswerte erfasst werden, die im Betrachtungsbereich liegen. Dabei ist darauf zu achten, dass Unternehmenswerte nicht nur Hardware und Software umfasst, sondern auch Geschäftsprozesse und Informationen.
  Auch müssen alle relevanten Bedrohungen (Beispiel: Brand) sowie vorhandene Schwachstellen (Beispiel: fehlender Brandschutz) ermittelt werden.
  Weiterhin werden alle bestehenden oder bereits geplanten Sicherheitsmaßnahmen identifiziert, da diese die Risiken beeinflussen, indem sie Eintrittswahrscheinlichkeiten oder Schadensausmaß reduzieren können.
  Schließlich sind die Konsequenzen zu ermitteln, die entstehen können, wenn eine Bedrohung auf eine Schwachstelle trifft. Als Konsequenzen werden unter anderem Verlust von Geschäftsvolumen oder Reputation genannt.

- **Abschätzung von Risiken (Risk estimation)**
  Die Bewertung des Risikos kann auf der Grundlage verschiedener Einflussgrößen erfolgen wie Kritikalität der Unternehmenswerte, Ausmaß von Schwachstellen oder Auswirkungen bekannter Sicherheitsvorfälle. Grundsätzlich kann die Bewertung mit qualitativen (Beispiel: »niedrig«, »hoch«, »selten«, »oft«), quantitativen (Beispiel: »10.000 €«, »85 Prozent«) oder hybriden Methoden erfolgen. In der Praxis wird für einen Anwendungszweck eine Methode gewählt, für die hinreichendes Zahlenmaterial verfügbar ist und deren Aussagekraft dem Ziel der Risikobewertung angemessen ist.
  Für die Abschätzung von Risiken müssen zum einen die Konsequenzen bewertet werden, genauer gesagt das Schadensausmaß bei Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit. Zum anderen muss die Eintrittswahrscheinlichkeit eines solchen Sicherheitsvorfalls bestimmt werden.
  Schließlich wird durch Kombination des Schadensausmaßes und der Eintrittswahrscheinlichkeit ein Risikoniveau bestimmt.

- **Auswertung von Risiken (Risk evaluation)**
  Dieser Schritt ist im Standard zur Priorisierung der Risiken vorgesehen. Die Priorisierung kann beispielsweise dadurch erfolgen, dass Risiken für Unternehmenswerte, die weniger wichtige Geschäftsprozesse unterstützen, gering priorisiert werden.

- **Behandlung von Risiken (Risk treatment)**
  Es ist zu entscheiden, ob ein Risiko reduziert, akzeptiert, vermieden oder übertragen wird. Während zur Reduzierung geeignete Sicherheitsmaßnahmen definiert werden müssen, können Risiken, die die Akzeptanzkriterien für Restrisiken erfüllen, unbehandelt bleiben. Ein Risiko kann vermieden werden, indem bspw. ein kritisches System in einer geschützten Umgebung aufgestellt wird, wo es besser gegen Naturkatastrophen geschützt ist. Die Übertragung von Risiken an Dritte kann über Versicherungen oder durch geeignete Vertragsformulierungen erfolgen.

- **Akzeptanz von Risiken (Risk acceptance)**
  Das Ergebnis der Risikobehandlung ist ein Plan, der für jedes Risiko die entsprechenden Handlungsempfehlungen aufzeigt. Die Leitungsebene einer Organisation kann entscheiden, Risiken zu akzeptieren, auch wenn diese nicht die Akzeptanzkriterien erfüllen.
  Für diese Fälle wird eine formelle Risikoübernahme gefordert.

- **Kommunikation von Risiken (Information security risk communication)**
  Informationen über Risiken sollten mit Entscheidungsträgern und weiteren relevanten Mitarbeitern ausgetauscht werden.
  Während die oben genannten Schritte der erstmaligen Identifizierung, Bewertung und Behandlung von Risiken dienen, definiert der Standard weitere Aktivitäten, um die Aktualität der Ergebnisse und angewandten Methoden sicherzustellen.

- **Überwachung von Risiken und Risikomanagement**
  Risiken sind von geschäftlichen Anforderungen und technologischen Rahmenbedingungen abhängig und damit einem Änderungsprozess unterworfen. Daher müssen die Risiken, das heißt auch Bedrohungen, Schwachstellen und weitere Einflussgrößen wiederkehrend auf Änderungen untersucht werden.
  Ebenso ist der in der Organisation angewandte Ansatz für das Risikomanagement regelmäßig auf Angemessenheit zu überprüfen.

Weitere Anmerkungen

Die Anhänge des Standards enthalten unter anderem Einzelheiten und Beispiele zu Bedrohungen, Schwachstellen und Bewertungsansätzen.

Bisherige Ausgaben

- ISO/IEC 13335-2:1997
- ISO/IEC 27005:2008
- ISO/IEC 27005:2011

4.3.4 ISO/ IEC 27014

Arbeitsgebiet	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards	Governance of information security Governance von Informationssicherheit

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 27014 bildet die Schnittstelle zwischen der Organisation, der Geschäftsleitung sowie den Verantwortlichen für die Umsetzung und den Betrieb eines Information Security Management Systems. Es ist eine Ergänzung zu den Anforderungen aus ISO/IEC27001. Der Standard beschreibt, wie Maßnahmen zur Informationssicherheit in der gesamten Organisation umgesetzt werden sowie IT-Sicherheitsberichte in einem geschäftlichen Kontext zurück an die Geschäftsleitung gelangen. Damit sind aussagekräftige und zeitnahe Entscheidungen zur Unterstützung der strategischen Ziele der Organisation möglich.

Methodik

Die Governance der Informationssicherheit muss die Ziele und Strategien für die Informationssicherheit an den wirtschaftlichen Zielen des Unternehmens ausrichten und gleichzeitig die Einhaltung von Gesetzen, Verordnungen und Verträge sicherstellen. Dazu gehört ein Risiko-Management-Ansatz (z.B. nach ISO/IEC 27005) kombiniert mit einem internen Kontrollsystem (IKS). Zu den Ergebnissen einer effektiven Umsetzung der Governance gehört den Status der Informationssicherheit sichtbar zu machen, eine Entscheidungsfindung bei der Behandlung von Informationssicherheitsrisiken zu ermöglichen sowie eine effiziente und effektive Planung von Investitionen zu gewährleisten. Weiterhin werden externe, d.h. rechtliche, regulatorische oder vertragliche, Anforderungen bestmöglich eingehalten

Der Standard ISO/IEC 27014 definiert sechs Grundsätze:

1. Sicherstellen einer unternehmensweiten Informationssicherheit
2. Verfolgung eines risikobasierten Ansatzes
3. Richtungsentscheidungen für Investitionsentscheidungen
4. Konformität mit internen und externen Anforderungen
5. Fördern eines positiven Sicherheitsumfelds
6. Bewertung der Kosten und des Nutzens der Informationssicherheit in Bezug auf die Geschäftsergebnisse

Bisherige Ausgaben

- ISO/IEC 2014:2013

4.4 Vorschriften

4.4.1 BDSG

Für den nicht-öffentlichen Bereich, sprich für die Unternehmen in Deutschland, ist im Bereich des Datenschutzes vor allem das Bundesdatenschutzgesetz (BDSG) maßgeblich. Weitere relevante Regelungen finden sich bspw. im Telemediengesetz (TMG), wenn es um die Webpräsenz eines Unternehmens geht.

Das BDSG soll die Daten der einzelnen natürlichen Personen schützen. Personenbezogene Daten sind dabei z.B. der Name der betroffenen Person, das Geburtsdatum, aber auch besonders sensible Informationen wie zu Krankheiten, politischen Ansichten oder sexueller Ausrichtung.

Daher regelt das BDSG

- ob und wie mit personenbezogenen Daten umgegangen werden darf
- welche Rechte die natürlichen Personen bezüglich ihrer auf ihre Person bezogenen Daten haben
- welche Kontrollmöglichkeiten es bei dem Umgang mit personenbezogenen Daten gibt und
- wie Verstöße gegen den Datenschutz geahndet werden

Der Grundsatz im Datenschutzrecht besagt, dass der Umgang mit personenbezogenen Daten verboten ist, es sei denn der Inhaber (Betroffene) willigt in den Umgang mit seinen Daten ein oder eine spezielle Rechtsvorschrift außerhalb des BDSG oder das BDSG selbst erlaubt den Umgang.

Hier ist zu beachten, dass spezielle Regelungen, wie das bereits angesprochene TMG für den Internetbereich oder auch Regelungen in den Sozialgesetzbüchern für den sozialen Bereich, dem BDSG vorgehen. Erst wenn sich keine speziellen Rechtsvorschriften finden lassen, ist auf das BDSG zurückzugreifen.

Der Betroffene hat auch gegenüber dem Unternehmen, das seine personenbezogenen Daten nutzt, ein gesetzlich normiertes Auskunftsrecht, wenn es um die Frage geht, was das Unternehmen mit den Daten macht und wie es an die Daten gelangt ist. Weiterhin kann er die Löschung oder Berichtigung der Daten verlangen.

Damit der Datenschutz in den Unternehmen wirksam umgesetzt werden kann, sieht das BDSG für Unternehmen eine Selbstkontrolle vor. Damit ist das Unternehmen für die Einhaltung des Datenschutzes selbst verantwortlich. Zu diesem Zweck hat es einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn eine bestimmte Anzahl seiner Beschäftigten mit personenbezogenen Daten arbeitet. Der Datenschutzbeauftragte kann als interner oder externer Beauftragter bestellt werden. Er ist bei der Erfüllung seiner Aufgaben keinen Weisungen der Unternehmungsführung unterworfen. Damit er den Datenschutz wirksam durchsetzen kann, muss er ein gewisses Maß an Zuverlässigkeit und Fachkunde für den Datenschutz aufweisen. Neben diesem Datenschutzbeauftragten findet auch eine Überwachung der Unternehmen durch die Datenschutzaufsichtsbehörden der jeweiligen Bundesländer statt.

Sobald es um den Datentransfer eines Unternehmens an ein anderes Unternehmen geht, ist besondere Aufmerksamkeit in Hinsicht auf den Datenschutz geboten. Sollte beispielsweise die Aktenvernichtung (bspw. Personalakten) nicht selbst, sondern durch einen Dienstleister durchgeführt werden, so besteht eine sogenannte Auftragsdatenverarbeitung. Sie ist dadurch charakterisiert, dass eine solche Datenverarbeitung bzw. -vernichtung auch vom verantwortlichen Unternehmen selbst durchgeführt werden könnte, es dieses aus Kosten- und Effizienzgründen aber auslagern möchte. Das Unternehmen, das solche Vorgänge an ein anderes Unternehmen überträgt, bleibt in diesem Fall verantwortlich für den Umgang mit den personenbezogenen Daten. Das Unternehmen muss dann sicherstellen, dass der Dienstleister den Datenschutz einhält. Dies muss zwingend durch einen schriftlichen

Vertrag geregelt werden. Ebenso ist das Unternehmen während der Auftragsdatenverarbeitung verpflichtet Kontrollen auf Einhaltung des Datenschutzes beim Dienstleister durchzuführen. Im Detail sei hierzu auf die BITKOM-Publikation »Mustervertragsanlage zur Auftragsdatenverarbeitung« verwiesen.

Etwas anderes gilt dann, wenn ein Unternehmen eigene Aufgaben komplett an einen anderen Dienstleister überträgt. Dies ist bspw. der Fall, wenn die Buchhaltung an einen Dienstleister auslagert wird. In diesem Fall verfügt das Unternehmen bzw. will es in der Regel nicht über das Know-How verfügen, um die Buchhaltung steuer- und sozialabgabenkonform selbst durchzuführen. Dann spricht man von einer Funktionsübertragung. Für diese bedarf es allerdings einer rechtlichen Grundlage, bspw. aus dem BDSG.

Für eine wirksame Durchsetzung des Datenschutzes und Sanktionierung von Datenschutzverstößen, sieht das BDSG Geldbußen in Höhe von bis zu 300.000 € und bei schwerwiegenden Verstößen auch Geld- und Haftstrafen vor.

Zusammenfassend ist zu sagen, dass der Datenschutz für die Unternehmen ein nicht zu unterschätzender Bereich ist, der auch im Rahmen der Compliance Beachtung finden muss.

4.5 Evaluierung von IT-Sicherheit

IT-Sicherheitskriterien beschreiben Schemata zur Bewertung von Sicherheitsvorkehrungen in IT-Systemen und ermöglichen mit den zugehörigen Evaluationshandbüchern deren transparente Prüfung. Die europäischen Information Technology Security Evaluation Criteria (ITSEC) waren jahrelang die Grundlage für den Bewertungsstandard für IT-Sicherheit in Europa. Ab Ende 1997 konnte in Deutschland alternativ die Erteilung von Sicherheitszertifikaten auf der Grundlage der Common Criteria (CC) beantragt werden, seit 2005 erfolgt ausschließlich die Prüfung nach CC.

Common criteria

4.5.1 ISO/IEC 15408 (CC)

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Evaluationskriterien für IT-Sicherheit Evaluation criteria for IT security

Inhalt und Anwendungsbereich

Die Norm definiert ein Kriterienwerk für die Sicherheitsevaluierung von IT-Produkten und IT-Systemen. Der Standard besteht aus folgenden drei zusammengehörigen Teilen:

Teil 1: Einführung und allgemeines Modell (Introduction and general model)

Teil 2: Funktionale Sicherheitsanforderungen (Security functional requirements)

Teil 3: Anforderungen an die Vertrauenswürdigkeit (Security assurance requirements)

Teil 1 stellt das allgemeine Konzept der Evaluationskriterien vor. Grundlegende Begriffe wie Sicherheitsanforderungen, Sicherheitsziele, Schutzprofile und Evaluationsgegenstand (Target of Evaluation, TOE) werden eingeführt.

Teil 2 enthält einen Katalog vordefinierter Funktionalitäten. Die Sicherheitsanforderungen an die Funktionalität sind nach Klassen strukturiert und innerhalb einer Klasse weiter in Familien aufgeteilt. Jede Familie besitzt zumindest eine Komponente, in der die Sicherheitsanforderungen an die konkrete Funktionalität beschrieben werden. Darüber hinaus können eigene Sicherheitsvorgaben als Grundlage für die Evaluierung/Zertifizierung definiert werden.

Teil 3 spezifiziert Kriterien für die Evaluierung von Schutzprofilen und Sicherheitsvorgaben. Die Sicherheitsvorgaben werden vor Beginn der eigentlichen Evaluierung eines TOE separat evaluiert. Auch Schutzprofile können vorevaluiert werden. Die Sicherheitsanforderungen an die Vertrauenswürdigkeit sind wie in Teil 2 des Standards mittels Klassen, Familien und Komponenten strukturiert. Sie werden für jede Komponente in einem festgelegten Aufbau formuliert, der sich aus Anforderungen an den Entwickler, Anforderungen an Inhalt und Form der Prüfnachweise, sowie Anforderungen an den Evaluator zusammensetzt.

Zertifizierung

IT-Produkte und IT-Systeme können nach dem Standard, auch unter dem Namen »Common Criteria (CC)« bekannt, zertifiziert werden. Im Rahmen der Zertifizierung wird die Sicherheit durch eine unabhängige Instanz (Prüfstellen, Zertifizierungsstellen und die nationalen Behörden) überprüft. Die Nutzer des Standards sind in den folgenden Gruppen zu finden:

- Käufer von IT-Sicherheitsprodukten (Institutionen und Verbraucher) können das Vorliegen eines Zertifikats nach ISO 15408 zu einem Maßstab ihrer Kaufentscheidung machen. Dazu müssen sie zwar den Standard nicht selbst inhaltlich benutzen, sollten aber um seine Bedeutung wissen.
- Große Institutionen oder Verbände von Verbrauchern können zudem das Mittel des Schutzprofils (Protection Profile) nutzen, um selbst Anforderungen an die Sicherheit von Produkten zu definieren.
- Hersteller von IT-Sicherheitsprodukten und -systemen können die Erreichung eines Zertifikats nach ISO 15408 als Marketinginstrument nutzen, um die Vertrauenswürdigkeit ihrer Produkte zu demonstrieren. Um eine Evaluierung als Hersteller zu durchlaufen, ist eine intensive Arbeit mit dem Standard erforderlich.
- Hersteller und Herstellerverbände können das Mittel des Schutzprofils nutzen, um Mindestanforderungen an einen Produkttyp im Markt zu etablieren.
- IT-Sicherheitsberater und IT-Sicherheitsverantwortliche in Institutionen sollten die Norm ebenfalls kennen, auch wenn sie nicht selbst in Evaluationen involviert sind. Zum einen sind sie immer potentielle Nutzer evaluierter Produkte, zum anderen ist die Vorgehensweise der Common Criteria auch für andere Bereiche der IT-Sicherheit interessant.

Weitere Anmerkungen

Die Nutzung der Common Criteria erfolgt im Wesentlichen durch namhafte Hersteller etwa von Chipkarten und Chipkartenhardware oder von hochsicheren Spezialprodukten. Kleinere Hersteller von preiswerten Sicherheitslösungen scheuen oft die Kosten einer Evaluierung nach den Kriterien. Staatliche Stellen gehen zunehmend dazu über, die CC zur Grundlage für die Akzeptanz sicherer Systeme zu machen, in Deutschland wird die CC vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dass auch an deren Entwicklung maßgeblich beteiligt war, empfohlen und benutzt. Eines der Ziele des BSI ist, die Anwendung der CC auch für kleine Hersteller attraktiv zu machen.

Für Fachkreise (Hersteller von IT-Sicherheitsprodukten und professionelle Anwender solcher Produkte) gibt es in Form der jährlich stattfindenden ICCC (International Common Criteria Conference) ein internationales Forum.

Bisherige Ausgaben

- ISO/IEC 15408:1999 (Teile 1 – 3)
- DIN ISO/IEC 15408:2001 (Teile 1 – 3)
- ISO/IEC 15408:2005 (Teile 1 – 3) (2. Ausgabe)
- DIN ISO/IEC 15408:2006 (Teile 1 – 3) (2. Ausgabe)
- ISO/IEC 15408:2008 (Teile 2 – 3)
- ISO/IEC 15408-1:2009
- ISO/IEC 15408-2:2008
- ISO/IEC 15408-3:2008

4.5.2 ISO/IEC TR 15443

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	A framework for IT security assurance Rahmenrichtlinien zur Sicherung von IT-Sicherheit

Inhalt und Anwendungsbereich

Der technische Bericht 15443 soll eine Hilfestellung bei der Entscheidung geben, nach welchen Kriterien und mit welchen Methoden man die Vertrauenswürdigkeit in die Sicherheit von IT-Produkten, -Systemen oder -Dienstleistungen bewertet.

Er besteht aus drei Teilen:

Teil 1: Überblick und Rahmenrichtlinie (Overview and framework)

Teil 2: Sicherungsmethoden (Assurance methods)

Teil 3: Analyse der Sicherungsmethoden (Analysis of assurance methods)

Insofern liegt der unmittelbare Nutzen auf der Anwenderseite. Dies betrifft natürlich weniger den Endverbraucher als die Entscheidungsvorbereitung in Firmen und anderen Organisationen. Beispiele für interessierte Leser könnten daher sein: IT-Sicherheitsverantwortliche in Organisationen, insbesondere Einkaufsverantwortliche, Verfasser von Sicherheitskonzepten, IT-Sicherheits-Berater.

Neben diesen Verantwortlichen für die Nutzung von Produkten, Systemen und Dienstleistungen sind die Kriterien natürlich auch für die Anbieter solcher Leistungen von Interesse, da sie anhand des Berichtes entscheiden können, welche Arten von Verfahren sie anwenden, um Vertrauen bei ihren Kunden zu schaffen. Für sie ist also beispielsweise interessant, welche Kombination von Qualitätsnormen, ISMS-Standards und Produktevaluierungen die Vertrauenswürdigkeit ihrer Firma und deren Produkte am besten demonstriert.

Für Leser des vorliegenden Leitfadens könnte der technische Bericht 15443 besonders von Interesse sein, da er – bezogen auf das Gebiet Vertrauenswürdigkeit – ein ähnliches Ziel wie dieser Leitfaden verfolgt. Sein Ziel ist es ja, die Bedeutung und Nutzbarkeit verschiedener Standards und Methoden in diesem Gebiet einzuordnen und damit eine Grundlage für die Entscheidung zur Nutzung eines oder mehrerer dieser Standards und Methoden zu schaffen.

Bisherige Ausgaben

- ISO/IEC TR 15443-1:2005, 2012
- ISO/IEC TR 15443-2:2005, 2012
- ISO/IEC TR 15443-3:2007

4.5.3 ISO/IEC 18045

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Methodology for IT security evaluation Methodik zur Evaluation von IT-Sicherheit

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 18045 richtet sich primär an Evalutoren von IT-Sicherheitsprodukten oder -systemen nach ISO/IEC 15408 (auch Common Criteria). Er ist im Wesentlichen identisch mit der in der Common-Criteria-Gemeinschaft bereits bekannten Common Evaluation Methodology (CEM). Es hat sich gezeigt, dass die Arbeit mit dem Dokument auch für die Hersteller von Produkten und Systemen oder deren Berater sehr empfehlenswert ist, um Herstellerdokumente zu schreiben, die die Anforderungen der ISO/IEC 15408 erfüllen und damit geeignet sind, eine erfolgreiche Evaluierung zu ermöglichen.

Weitere Anmerkungen

Eine freie Version dieses Dokumentes ist bereits seit längerem verfügbar und bildet den de facto Standard für die Durchführung von Evaluierungen nach ISO/IEC 15408 respektive Common Criteria. Insofern ist die Verbreitung in der angesprochenen Nutzergemeinschaft nahezu vollständig. Dies wird auch für künftige Versionen gelten, die jeweils dem Stand der 15408 angepasst sein werden.

Bisherige Ausgaben

- ISO/IEC 18045:2005
- ISO/IEC 18045:2008 (Diese Ausgabe wurde deutlich überarbeitet in Anpassung an die gleichzeitige Version von ISO/IEC 15408.

4.5.4 ISO/IEC 21827 (SSE-CMM)

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Capability Maturity Model (SSE-CMM®) Model der Ablaufstauglichkeit

Inhalt und Anwendungsbereich

Ziel des Dokumentes ist es, Informationssicherheit mittels eines Prozess-Referenz-Modells darzustellen. Der Standard wurde Mitte der Neunziger Jahre in den USA von staatlichen Behörden und einigen Großunternehmen aus dem allgemeinen Reifegradmodell dem sog. Capability maturity model (CMM), das besonders in der Softwareentwicklung verbreitet ist, weiterentwickelt und an die speziellen Anforderungen des Sicherheitsmanagements angepasst.

Es dient dem Managen von Sicherheit in einer Organisation, indem es die einzelnen Aktivitäten – also das »Wie« – beschreibt. Der organisatorische Reifegrad in Bezug auf das Sicherheitsmanagement wird betrachtet. Das Dokument richtet sich an den IT-Sicherheitsbeauftragten einer Organisation.

Methodik

Der Standard unterteilt die sichere Systementwicklung in drei voneinander abhängige Hauptprozesse: Risiko, Vertrauenswürdigkeit und System-Lebenszyklus. Es beschreibt generische und Basis-Aktivitäten. Diese Aktivitäten befähigen eine Organisation zur Entwicklung und Einführung eines systematischen, wohl definierten Prozesses, der es ihr ermöglicht, einen bestimmbaren Reifegrad zu erreichen.

Das Prozess-Referenz-Modell hat zwei Dimensionen (domain und capability), die nach Aktivitäten strukturiert sind. Die Basis-Aktivitäten teilen sich in solche, die zur sicheren Entwicklung erforderlich sind und andere, die zur Projektorganisation beitragen. Die 61 auf die sichere Entwicklung bezogenen Basis-Aktivitäten werden in elf Prozess-Bereiche zusammengefasst. Bezogen auf die Projektorganisation werden weitere 68 Basis-Aktivitäten (zusammengefasst in wiederum elf Prozess-Bereiche) dargestellt. Die generischen Aktivitäten, die auf alle Prozesse anwendbar sind, lassen sich fünf Fähigkeitsstufen geordnet nach aufsteigendem Reifegrad zuordnen. Folgende Reifegrade sind in SSE-CMM vorgeschlagen:

Reifegrad	Bezeichung	Erläuterung
0	Nicht umgesetzt	
1	Formlos umgesetzt	Es existieren zwar einzelne Maßnahmen. Ein wirklicher Prozess ist aber kaum organisiert und noch sehr instabil
2	Geplant und weiterverfolgt	Ein stabiler Prozess existiert und wird in Projekten mit einem Projektmanagement gelebt
3	Gut definiert	Ein Prozess ist definiert und es existiert ein Prozessmodell, das eine konsistente Implementierung des Prozesses sicherstellt
4	Quantitativ kontrolliert	Es existieren Prozessmessungen und Prozessdatenanalysen, die für die Weiterentwicklung des Prozesses genutzt werden
5	Kontinuierlich verbessernd	Das Management ist regelmäßig in die Prozessbewertung und die weitergehende Prozessoptimierung einbezogen

Über vordefinierte Prüflisten lässt sich ohne großen Aufwand der eigene Status für die einzelnen Sicherheitsprozesse innerhalb einer sechsstufigen Skala ablesen und somit auch ein Benchmarking und ein Zielbeschreibung durchführen. Somit ist dies ein guter Folgeschritt nach der Etablierung eines ISMS, zum Beispiel nach ISO/IEC 27001 oder IT-Grundschutz.

Aber auch in der Entwicklungs- und Etablierungsphase lohnt sich ein Blick in diesen Standard, da hier Teilprozesse teilweise stärker konkretisiert sind, als dies etwa in BS 7799 der Fall ist.

Weitere Anmerkungen

Das Dokument ist generisch gehalten, um auf alle Organisationen unbeachtet Typ, Größe und Geschäftsfeld anwendbar zu sein. Das Dokument beinhaltet Anforderungen an den Managementprozess, der mittelbar zur Informationssicherheit beiträgt. Die einzelnen Aktivitäten des Managementprozesses werden detailliert beschrieben und begründet. Elemente des Managementsystems werden nicht dargelegt. Der Fokus liegt also eindeutig auf dem »Prozess«.

Bisherige Ausgaben

- ISO/IEC 21827:2002
- ISO/IEC 21827:2008

4.5.5 BSI-TR-03125

Arbeitsgebiet:	Informationstechnik: Technische Richtlinien des BSI
Name des Standards:	Englisch Technische Richtlinie für Beweiswerterhaltung kryptographisch signierter Dokumente

Inhalt und Anwendungsbereich

Für Dokumente, die in elektronischer Form gespeichert werden, gelten die gesetzlichen Aufbewahrungspflichten genauso wie für Papierdokumente, wobei sich in der elektronischen Welt daraus die folgenden Anforderungen ableiten:

Für die gesamte Speicherdauer muss gewährleistet sein:

- die Lesbarkeit,
- die Verfügbarkeit,
- die Integrität und
- die Authentizität der Dokumente.

Lesbarkeit und Verfügbarkeit sind unabhängig von immer kürzer werdenden informationstechnischen Innovationszyklen sicherzustellen. Integrität und Authentizität werden erreicht, indem Dokumente elektronisch signiert werden. Die Beweiskraft digitaler Signaturen ist allerdings zeitlich begrenzt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher einen Leitfaden erarbeitet, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume – bis zum Ende der Aufbewahrungsfristen – im Sinne eines rechtswirksamen Beweiswerterhalts vertrauenswürdig gespeichert werden können. Zu diesem Zweck werden anhand einer hersteller- und produktunabhängigen Referenzarchitektur funktionale und sicherheitstechnische Mindestanforderungen definiert, gemäß denen Systeme, Komponenten, Schnittstellen und deren Zusammenspiel für den Beweiswerterhalt aufgebaut, überprüft und in Betrieb genommen werden können. Diese Referenzarchitektur beschreibt eine Middleware zwischen den Endanwendungen und den Speichermedien für die Langzeitspeicherung und ist somit deutlich von einem Archivsystem abzugrenzen.

Die Technische Richtlinie besteht aus einem Hauptdokument sowie einer Reihe ergänzender Anlagen, die sich an der beschriebenen Referenzarchitektur orientieren, und in denen einzelne Aspekte näher spezifiziert und erläutert werden.

Hauptdokument:

- TR-ESOR als BSI TR-03125, Version 1.1, 2011

Anlagen:

- TR-ESOR-M.1 ArchiSafe-Modul, als BSI TR-03125-M.1
- TR-ESOR-M.2 Krypto-Modul, als BSI TR-03125-M.2
- TR-ESOR-M.3 ArchiSig-Modul, als BSI TR-03125-M.3
- TR-ESOR-B Profilierung für Bundesbehörden, als BSI TR-03125-B
- TR-ESOR-E Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, als BSI TR-03125-E
- TR-ESOR-F Formate und Protokolle, als BSI TR-03125-F
- TR-ESOR-S Schnittstellen, als BSI TR-03125-S

Ergänzt werden diese Technische Richtlinie und Anlagen durch Testspezifikationen. Getestet werden kann Konformität in drei Abstufungen:

- Funktionale Konformität
- Technische Konformität
- Konformität zum Behördenprofil

Die Konformität eines Produktes oder Teilproduktes auf Modulebene der Referenzarchitektur kann durch das BSI zertifiziert werden. Hierzu ist eine erfolgreiche Prüfung durch eine beim BSI anerkannte Prüfstellen Voraussetzung.

Weitere Anmerkungen

Die Technische Richtlinie mit seinen Anlagen wird ergänzt durch ein Common Criteria-Schutzprofil für das ArchiSafe-Modul. Das Schutzprofil (ACM-PP) findet sich als BSI-CC-PP-0049 auf den Webseiten des BSI unter www.bsi.bund.de.

4.5.6 ISO/IEC TR 15443

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	A framework for IT security assurance Rahmenrichtlinien zur Sicherung von IT-Sicherheit

Inhalt und Anwendungsbereich

Der technische Bericht 15443 soll eine Hilfestellung bei der Entscheidung geben, nach welchen Kriterien und mit welchen Methoden man die Vertrauenswürdigkeit in die Sicherheit von IT-Produkten, -Systemen oder -Dienstleistungen bewertet.

Er besteht aus drei Teilen:

Teil 1: Überblick und Rahmenrichtlinie (Overview and framework)

Teil 2: Sicherungsmethoden (Assurance methods)

Teil 3: Analyse der Sicherungsmethoden (Analysis of assurance methods)

Insofern liegt der unmittelbare Nutzen auf der Anwenderseite. Dies betrifft natürlich weniger den Endverbraucher als die Entscheidungsvorbereitung in Firmen und anderen Organisationen. Beispiele für interessierte Leser könnten daher sein: IT-Sicherheitsverantwortliche in Organisationen, insbesondere Einkaufsverantwortliche, Verfasser von Sicherheitskonzepten, IT-Sicherheits-Berater.

Neben diesen Verantwortlichen für die Nutzung von Produkten, Systemen und Dienstleistungen sind die Kriterien natürlich auch für die Anbieter solcher Leistungen von Interesse, da sie anhand des Berichtes entscheiden können, welche Arten von Verfahren sie anwenden, um Vertrauen bei ihren Kunden zu schaffen. Für sie ist also beispielsweise interessant, welche Kombination von Qualitätsnormen, ISMS-Standards und Produktevaluierungen die Vertrauenswürdigkeit ihrer Firma und deren Produkte am besten demonstriert.

Für Leser des vorliegenden Leitfadens könnte der technische Bericht 15443 besonders von Interesse sein, da er – bezogen auf das Gebiet Vertrauenswürdigkeit – ein ähnliches Ziel wie dieser Leitfaden verfolgt. Sein Ziel ist es ja, die Bedeutung und Nutzbarkeit verschiedener Standards und Methoden in diesem Gebiet einzuordnen und damit eine Grundlage für die Entscheidung zur Nutzung eines oder mehrerer dieser Standards und Methoden zu schaffen.

Bisherige Ausgaben

- ISO/IEC TR 15443-1:2005, 2012
- ISO/IEC TR 15443-2:2005, 2012
- ISO/IEC TR 15443-3:2007

4.6 Spezielle Sicherheitsfunktionen: Normen zu kryptographischen und IT-Sicherheitsverfahren

Sichere Kommunikation zwischen Sender und Empfänger beruht auf folgenden Eigenschaften der Verarbeitung und Kommunikation. Die Information:

- ist nicht unbefugt verändert worden (Integrität),
- von keinem unbefugten Dritten gelesen worden (Vertraulichkeit) und wirklich vom Sender an den Empfänger verschickt worden (Authentizität).

Die geforderten sicheren Eigenschaften können technisch durch verschiedene Sicherheitsmechanismen und -dienste realisiert werden, die teilweise miteinander kombiniert werden, z. B. kann der Hashwert eines Dokumentes mit einer digitalen Signatur zur Sicherstellung der Integrität des Dokuments unterschrieben werden. In den folgenden Kapiteln werden die entsprechenden Standards der Informationstechnik erläutert.

Verschlüsselung

Die Standardisierung offen gelegter Verschlüsselungsverfahren war lange umstritten. Einerseits soll sie von einer öffentlich geführten Diskussion über die Qualität der spezifizierten Mechanismen begleitet werden und nicht zuletzt aus diesem Grund zu großer Akzeptanz führen. Andererseits stellen veröffentlichte Algorithmen, die auf breiter Basis zum Einsatz kommen, für potentielle Angreifer natürlich ein besonders lohnendes Ziel dar.

Aufgrund dieser Situation gibt es sowohl offen gelegte (Beispiel: DES und AES) als auch nicht offen gelegte Verschlüsselungsstandards; zu letzteren zählt z. B. die Mehrzahl der von ETSI/SAGE spezifizierten Verfahren für Telekommunikationsanwendungen.

4.6.1 ISO/IEC 18033

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Encryption algorithms Verschlüsselungsalgorithmen

Inhalt und Anwendungsbereich

Das Hauptziel von Verschlüsselung ist der Schutz der Vertraulichkeit von gespeicherten oder übertragenen Daten. Ein Verschlüsselungsalgorithmus wird auf Daten (die häufig als Klartext bezeichnet werden) angewendet, so dass verschlüsselte Daten (Schlüssel- oder Chiffretext) entstehen; dieses Verfahren wird als Verschlüsselung oder Kryptierung beziehungsweise Chiffrierung bezeichnet. Der Standard ISO/IEC 18033 beschreibt die Anwendung von Verschlüsselungsalgorithmen.

Der Standard besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Asymmetrische Schlüssel (Asymmetric ciphers)
- Teil 3: Blockschlüssel (Block ciphers)
- Teil 4: Stromschlüssel (Stream ciphers)

Teil 1 hat allgemeinen Charakter und stellt Definitionen auf, die für die weiteren Teile dieser Normenreihe gelten. Die notwendigen Eigenschaften der Verschlüsselung und bestimmte allgemeine Aspekte ihrer Anwendung werden beschrieben. Die Kriterien zur Auswahl eines in den weiteren Teilen festgelegten Algorithmusses werden definiert und der Bezug dieses Dokuments zum Verzeichnis der Algorithmen dargestellt.

Teil 2 legt eine allgemeine Methode zur Erstellung hybrider Verschlüsselungsschemata fest.

Die beiden Hauptkomponenten sind ein Schlüssel verkapselnder Mechanismus (key encapsulating mechanism, KEM), der asymmetrische kryptographische Techniken zur Erzeugung und Verschlüsselung eines zufälligen symmetrischen Schlüssels benutzt, und ein Daten verkapselnder Mechanismus (data encapsulating mechanism, DEM), um tatsächlich unter Einsatz dieses symmetrischen Schlüssels eine Nachricht zu verschlüsseln. Es werden jeweils mehrere KEM und DEM definiert.

Teil 3 legt Algorithmen und Eigenschaften von Blockchiffren fest, deren Blocklängen 64 Bit oder 128 Bit betragen. Die Algorithmen erfüllen die im ersten Teil dieser Normenreihe aufgestellten Anforderungen.

Teil 4 legt Algorithmen für Stromchiffren fest. Dazu gehören die Verfahren zur Erstellung von Schlüssel-Datenketten für eine Stromchiffre. Des Weiteren werden bestimmte pseudozufällige Erzeuger für die Erstellung von Schlüssel-Datenketten beschrieben.

Weitere Anmerkungen

Ein Verschlüsselungsalgorithmus sollte so beschaffen sein, dass der Chiffretext keine Informationen über den Klartext verrät, außer vielleicht dessen Länge. Jeder Verschlüsselungsalgorithmus muss außerdem für einen Entschlüsselungsprozess vorgesehen sein, der den Chiffretext in den originalen Klartext zurückwandeln muss.

Bisherige Ausgaben

- ISO/IEC 18033-1:2005
- ISO/IEC 18033-1:2005/Amd 1:2011
- ISO/IEC 18033-2:2006
- ISO/IEC 18033-3:2005
- ISO/IEC 18033-3:2010
- ISO/IEC 18033-4:2005
- ISO/IEC 18033-4:2011

4.6.2 ISO/IEC 10116

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Modes of operation for an n-bit block cipher Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus

Inhalt und Anwendungsbereich

Das Dokument legt vier Funktionsweisen eines n-Bit Blockschlüssel-Algorithmusses fest. Dabei handelt es sich um Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) und Cipher Feedback (CFB). Diese unterscheiden sich auch im Hinblick auf die Fortpflanzung von Übertragungsfehlern und die Resistenz gegen bestimmte Angriffe. Um die Auswahl der passenden Funktionsweise zu unterstützen, werden die Eigenschaften der vier Funktionsweisen beschrieben und verglichen.

Weitere Anmerkungen

Blockschlüssel-Algorithmen arbeiten mit Datenblöcken festgelegter Größe, die zu verschlüsselnden Nachrichten können jedoch von beliebiger Länge sein. Hauptsächlich werden vier Funktionsweisen von Blockschlüssel-Algorithmen eingesetzt, die die meisten praktischen Anforderungen an den Einsatz der Verschlüsselung bei Computern und Netzwerken abdecken.

Bei einigen Funktionsweisen kann ein Auffüllen erforderlich werden, um die benötigte Eingabe-länge für den Algorithmus zu gewährleisten. Diese Auffülltechniken gehören nicht zum Anwendungsbereich dieses Dokuments.

Bisherige Ausgaben

- ISO/IEC 10116: 1991
- ISO/IEC 10116: 1997
- ISO/IEC 10116: 2006
- ISO/IEC 10116: 2006/Cor 1:2008

4.6.2 ISO/IEC 19772

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Authenticated encryption authentisierte Verschlüsselung

Inhalt und Anwendungsbereich

Dieses Dokument legt sechs Methoden der authentisierten Verschlüsselung fest, das heißt vorgegebene Wege zur Verarbeitung eines Datenstroms mit den Sicherheitszielen Datenvertraulichkeit, Datenintegrität, Datenursprungsauthentisierung. Für die drei Methoden müssen der Urheber und der Empfänger der geschützten Daten einen geheimen Schlüssel teilen. Das Schlüsselmanagement selbst liegt nicht im Anwendungsbereich dieses Dokuments.

Weitere Anmerkungen

Falls sowohl ein Schutz der Vertraulichkeit als auch der Integrität erforderlich ist, besteht die Möglichkeit, eine Verschlüsselung und einen Message Authentication Code (MAC) beziehungsweise eine Signatur zusammen zu benutzen. Obwohl diese Verfahren in vielen Kombinationen eingesetzt werden können, bieten nicht alle davon den gleichen Sicherheitsgrad. Daher wird beschrieben, wie die Vertraulichkeits- und Integritätsmechanismen miteinander zu kombinieren sind, um einen möglichst optimalen Sicherheitsgrad zu erreichen. Darüber hinaus können in einigen Fällen signifikante Effektivitätssteigerungen erreicht werden, indem eine einzelne Methode zur Verarbeitung der Daten festgelegt wird, die sowohl die Vertraulichkeit als auch die Integrität schützt.

Bisherige Ausgaben

- ISO/IEC 19772:2008
- ISO/IEC 19772:2009

4.6.3 ISO/IEC 29192

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Lightweight cryptography Leichtgewichtige Kryptographie

Inhalt und Anwendungsbereich

Das Gebiet der leichtgewichtigen Kryptographie befasst sich mit kryptographischen Verfahren, die aufgrund ihres geringen Ressourcenbedarfs besonders für den Einsatz in ressourcenbeschränkten Umgebungen (z.B. RFID-Tags, Sensoren) geeignet sind.

Leichtgewichtige Kryptographie heißt nicht unbedingt schwache Kryptographie: die in ISO/IEC 29129 spezifizierten Mechanismen bieten alle zumindest ein Sicherheitsniveau von 80 Bit.

ISO/IEC 29192 besteht aus den Teilen:

Teil 1: Allgemeines Modell (General)

Teil 2: Blockchiffren (Block ciphers)

Teil 3: Stromchiffren (Stream ciphers)

Teil 4: Asymmetrische Mechanismen (Mechanisms using asymmetric techniques)

Teil 1 hat allgemeinen Charakter und beinhaltet Definitionen und Konzepte, die für die weiteren Teile dieser Normenreihe gelten, insbesondere die Kriterien für die Auswahl der in den weiteren Teilen festgelegten Algorithmen.

Teil 2 spezifiziert zwei Algorithmen für Blockchiffren: Present und CLEFIA.

Teil 3 spezifiziert zwei Algorithmen für Stromchiffren: Trivium und Enocoro.

Teil 4 definiert leichtgewichtige asymmetrische kryptographische Mechanismen zur Authentifizierung und zum Schlüsselaustausch. Diese sind cryptoGPS, ALIKE und IBS.

Weitere Anmerkungen

An einem weiteren Teil 5 mit dem Schwerpunkt Hashfunktionen wird gearbeitet. Dieser Teil befindet sich derzeit noch in einem frühen Stadium.

Bisherige Ausgaben

- ISO/IEC 29192-1:2012
- ISO/IEC 29192-2:2012
- ISO/IEC 29192-3:2012
- ISO/IEC 29192-4:2013

Digitale Signaturen

Durch das Verfahren der Digitalen Signaturen soll sichergestellt werden, dass elektronische Dokumente nicht unbemerkt verfälscht und ihre Aussteller nachweisbar identifiziert werden können. Bei Digitalen Signaturen unterscheidet man Schemata, bei denen die unterschriebene Nachricht aus der Unterschrift wiedergewonnen werden kann (Signatures giving message recovery) und solche, bei denen dies nicht der Fall ist, da ein Hashwert gebildet und dieser als eigener Nachrichtenanhang signiert wird (Signatures with appendix). Zu einer besonders attraktiven Alternative zum RSA-Verfahren bzw. dem DSA haben sich in den letzten Jahren Signaturmechanismen auf der Basis elliptischer Kurven entwickelt.

4.6.5 ISO/IEC 9796

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Digital signature schemes giving message recovery Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht

Inhalt und Anwendungsbereich

Das Ziel der Normenreihe ist die Festlegung von Digitalen Unterschriftsmechanismen, die eine teilweise oder vollständige Wiederherstellung von Nachrichten bei verringertem Speicher- und Übertragungsaufwand ermöglichen.

Dieser Standard besteht aus folgenden Teilen:

- Teil 2: Mechanismen auf der Basis der Faktorisierung ganzer Zahlen (Integer factorization based mechanisms)
- Teil 3: Mechanismen auf Basis des diskreten Logarithmus (Discrete logarithm based mechanisms)
- Teil 1 wurde zurückgezogen.

Teil 2 legt drei Digitale Unterschriftenschemata zur Wiederherstellung von Nachrichten fest, deren Sicherheit auf dem Faktorisierungsproblem (großer) ganzer Zahlen beruht. Die Schemata ermöglichen entweder eine teilweise oder die vollständige Wiederherstellung der Nachricht.

Teil 3 legt zwei Digitale Unterschriftenschemata fest, die eine Datenwiederherstellung ermöglichen und auf dem Problem der diskreten Logarithmen beruhen. Beide Schemata beruhen auf der Schwierigkeit des Problems der diskreten Logarithmen. Das erste Schema wird über ein Hauptfeld definiert, das zweite über eine elliptische Kurve in einem endlichen Feld. Des Weiteren definiert das Dokument ein Redundanzschema, das eine Hash-Funktion zur Zerlegung einer kompletten Nachricht benutzt, und legt fest, wie die Grundsignaturschemen mit den Redundanzschemen verbunden werden.

Weitere Anmerkungen

Die Normenreihe beschreibt, auf welchen mathematischen Grundlagen die Digitale Unterschriftenschemata aufbauen, für welche Anwendungsfälle sie jeweils geeignet sind, und stellt Beispiele dar.

Bisherige Ausgaben

- ISO/IEC 9796:1991 (inzwischen zurückgezogen)
- ISO/IEC 9796-2: 1997, 2002, 2010
- ISO/IEC 9796-3:2000, 2006

4.6.6 ISO/IEC 14888

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Digital signatures with appendix Digitale Signaturen mit Anhang

Inhalt und Anwendungsbereich

Eine Digitale Signatur beim elektronischen Austausch von Informationen bietet dieselben Möglichkeiten, die von einer handschriftlichen Signatur bei Postsendungen erwartet werden. Daher kann sie zur Authentisierung, Sicherheit und Nicht-Abstreitbarkeit von Daten eingesetzt werden. Ziel dieser Normenreihe ist die Festlegung von Mechanismen für Digitale Signaturen mit Anhang für Nachrichten beliebiger Länge.

Die internationale Norm ISO/IEC 14888 besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Identitätsbasierte Mechanismen (Identity-based mechanisms)
- Teil 3: Zertifikatsbasierte Mechanismen (Certificate-based mechanisms)

Teil 1 des Standards deckt die Grundprinzipien und Hauptanforderungen an Digitale Signaturen mit Anhang ab und enthält eine allgemeine Beschreibung der Signatur- und Prüfprozesse. Die verschiedenen Anwendungen wie die Authentisierung von Instanzen, Schlüsselmanagement und Nicht-Abstreitbarkeit werden in diesem Dokument nicht behandelt.

Teil 2 legt die Grundstruktur, die mathematischen Funktionen und möglichen Daten fest, die die Signatur- und Prüfprozesse einer Identitäts-basierten Digitalen Signatur mit Anhang für beliebig lange Nachrichten ausmachen.

Dieser Signaturmechanismus erfordert den Dienst einer vertrauenswürdigen Stelle, die den Signaturschlüssel eines Abzeichnenden aus dessen Identität ableitet.

Teil 3 legt Mechanismen der Digitalen Signatur mit Anhang fest, deren Sicherheit auf einer Aufgabe zum diskreten Logarithmus aufbauen. Dieses Dokument enthält eine allgemeine Beschreibung eines Mechanismus für eine Digitale Signatur mit Anhang und eine Anzahl von Mechanismen, die Digitalen Signaturen mit Anhang liefern und legt für jeden dieser Mechanismen die Schlüssel- und Signaturerstellung sowie die Signaturbestätigung fest.

Weitere Anmerkungen

Digitale Signaturen mit Anhang nutzen kollisionsresistente Hash-Funktionen, die sowohl im Signatur- als auch im Prüfprozess eingesetzt werden. Im Prüfprozess ist die Hauptfunktion die Prüffunktion, die durch den Prüfschlüssel festgelegt wird. Andere Hauptfunktionen im Signaturprozess sind das Vor-Abzeichnen und das Abzeichnen. Dabei ist die Vor-Abzeichnen-funktion von der Nachricht unabhängig und die Abzeichnenfunktion wird durch den Signaturschlüssel selbst bestimmt.

Bisherige Ausgaben

- ISO/IEC 14888-1:1998, 2008
- ISO/IEC 14888-2:1999, 2008
- ISO/IEC 14888-3:1998, 2006
- ISO/IEC 14888-3: 2006/Cor 1:2007
- ISO/IEC 14888-3: 2006/Amd 1:2010
- ISO/IEC 14888-3: 2006/Amd 2:2012
- ISO/IEC 14888-3: 2006/Cor 2:2009

4.6.7 ISO/IEC 15946

Arbeitsgebiet:	Informationstechnik – Sicherheitstechnik: IT-Sicherheitsverfahren
Name des Standards:	Cryptographic techniques based on elliptic curves Auf elliptischen Kurven aufbauende kryptographische Verfahren

Inhalt und Anwendungsbereich

ISO/IEC 15946 behandelt auf elliptischen Kurven aufbauende kryptographische Verfahren für öffentliche Schlüssel. Diese schließen die Etablierung von Schlüsseln für Systeme geheimer Schlüssel und Mechanismen für Digitale Signaturen mit ein.

Nach einer Neuzuordnung der jeweiligen Mechanismen zu den einschlägigen Standards, insbesondere für digitale Signaturen und Schlüsselbereitstellung beschränkt sich ISO/IEC 15946 auf eine allgemeine Einführung in elliptische Kurven (Teil 1), sowie die Erzeugung geeigneter elliptischer Kurven (Teil 5). Die Teile 2 bis 4 wurden im Zuge einer Harmonisierung der verschiedenen Normungsreihen anteilig in andere Normen überführt und danach zurückgezogen.

ISO/IEC 15946 besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 5: Erzeugung geeigneter elliptischer Kurven (Elliptic curve generation)

Teil 1 beschreibt die für den Einsatz der in den anderen Teilen beschriebenen Mechanismen notwendigen mathematischen Grundlagen und allgemeinen Techniken und bezieht sich vor allem auf die Kryptographie mit elliptischen Kurven.

Teil 5 behandelt die Erzeugung geeigneter elliptischer Kurven zur Anwendung mit den in den anderen Teilen beschriebenen Verfahren. Das Auffinden geeigneter elliptischer Kurven hat, wie übrigens auch die Parametrisierung anderer Schlüsselverfahren, wesentliche Bedeutung für die Sicherheit einer Anwendung.

Weitere Anmerkungen

Öffentliche Schlüssel (sog. Public-Key)-Verfahren auf Basis elliptischer Kurven sind dem RSA-Algorithmus und anderen Public-Key Verfahren der ersten Generation in Bezug auf Sicherheit und Performance deutlich überlegen; so kann mit elliptischen Kurven der Schlüssellänge 160 Bit bereits ein höheres Sicherheitsniveau erreicht werden als mit 1024-Bit RSA. Die Anwendung dieser Normenreihe beschränkt sich auf kryptographische Techniken, die auf elliptischen Kurven aufbauen, die über endliche Felder mit Potenzen erster Ordnung (inklusive der Sonderfälle der ersten Ordnung und Kennzahl Zwei). Die Darstellung des zugrunde liegenden endlichen Feldes (das heißt dessen Basis genutzt wird) liegt außerhalb des Anwendungsbereichs dieses Dokuments.

Bisherige Ausgaben

- ISO/IEC 15946-1: 2002, 2008
- ISO/IEC 15946-1: 2008/Cor 1:2009
- ISO/IEC 15946-2: 2002 (inzwischen zurückgezogen)
- ISO/IEC 15946-3: 2002 (inzwischen zurückgezogen)
- ISO/IEC 15946-4: 2004 (inzwischen zurückgezogen)
- ISO/IEC 15946-5: 2009
- ISO/IEC 15946-5: 2009/Cor 1:2012

Hash-Funktionen und andere Hilfsfunktionen

Eine kryptographische Streuwertfunktion bzw. Hash-Funktion komprimiert (beliebig lange) Nachrichten zu einem nicht manipulierbaren Prüfwert fester Länge (meist 128 oder 160 Bit).

Hash-Funktionen sind daraufhin optimiert, sog. Kollisionen zu vermeiden.

4.6.8 ISO/IEC 10118

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	hash functions hash-Funktionen

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 10118 beschreibt Aufbau und Anwendung von Hash-Funktionen. Er besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Hash-Funktionen auf Basis eines n-bit-Blockschlüssel- Algorithmus (Hash-functions using an n-bit block cipher)
- Teil 3: Fest zugeordnete Hash-Funktionen (Dedicated hash-functions)
- Teil 4: Hash-Funktionen auf Basis modularer Arithmetik (Hash-functions using modular arithmetic)

Teil 1 beschreibt grundlegende Konzepte von Hash-Funktionen und enthält Definitionen, Abkürzungen und Anforderungen, die gleichermaßen für alle anderen Teile dieser Normenreihe gelten.

Teil 2 legt zwei Hash-Funktionen fest, die einen n-Bit Blockschlüssel-Algorithmus nutzen. Daher sind sie für eine Umgebung geeignet, in der ein solcher Algorithmus schon vorhanden ist. Sie bauen auf einem bestimmten Verkettungsmodus auf, der teilweise als MDC (Manipulation/Modification – Detection Code) bezeichnet wird.

Teil 3 legt fest zugeordnete Hash-Funktionen fest, das heißt für einen speziellen Zweck entwickelte Streuwertfunktionen. Die in diesem Teil benutzten Hash-Funktionen bauen auf der iterierten Anwendung von Kompressionsfunktionen auf. Dieser Teil legt sieben verschiedene Kompressionsfunktionen fest.

Teil 4 legt zwei kollisionsresistente Hash-Funktionen fest, die eine modulare Arithmetik nutzen, um eine Kompressionsfunktion und eine Verringerungsfunktion anzuwenden. Diese Hash-Funktionen kürzen Nachrichten von beliebiger aber begrenzter Länge zu einem Hash-Code, dessen Länge durch die Länge der für die Verringerungsfunktion genutzten Primzahl bestimmt wird.

Weitere Anmerkungen

Hash-Funktionen bilden beliebige Bitfolgen in einem vorgegebenen Bereich ab. Sie können zur Reduktion einer Nachricht zu einem kurzen Abdruck genutzt werden, der als Eingabe in einen Digital Signaturmechanismus dient, oder damit sich der Benutzer auf eine vorgegebene Bitfolge festlegt, ohne dass diese Zeichenfolge verraten wird. Die in eine Hash-Funktion einzugebende Zeichenkette wird Datenfolge, die ausgegebene Zeichenfolge Hash-Code genannt.

Bisherige Ausgaben

- ISO/IEC 10118-1: 1994, 2000
- ISO IEC 10118-2: 1994, 2000
- ISO IEC 10118-2 COR2:2007
- ISO/IEC 10118-2: 2010
- ISO/IEC 10118-2: 2010/Cor 1:2011
- ISO/IEC 10118-3: 2003, 2004
- ISO/IEC 10118-3: 2004/Amd 1:2006
- ISO/IEC 10118-4: 1998

4.6.9 ISO/IEC 18031

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Random bit generation Erzeugung von Zufallszahlen

Inhalt und Anwendungsbereich

Dieses Dokument legt ein konzeptionelles Modell eines Zufallszahlengenerators für kryptographische Zwecke mit seinen Elementen fest. Dazu beschreibt es die für einen nicht-deterministischen Zufallszahlengenerator beziehungsweise einen deterministischen Pseudozufallszahlengenerator notwendigen Hauptelemente sowie deren Eigenschaften und Sicherheitsanforderungen.
Das Dokument bietet umfassende Informationen von der Festlegung eines Begriffsmodells, der Terminologie und der Bausteine eines Zufallsbit-Erzeugers bis hin zu einem Leitfaden für die Entwicklung eines (Pseudo- oder) Zufallszahlengenerators.

Weitere Anmerkungen

Die Erzeugung von zufälligen Bitfolgen für den kryptographischen Einsatz ist anspruchsvoll und für die Wirksamkeit bestimmter kryptographischer Verfahren äußerst wichtig. Falls beispielsweise der Schlüssel eines symmetrischen Algorithmus über seine Vorhersagbarkeit bestimmt werden kann, kann die Sicherheit des Algorithmus gefährdet sein.
Das Dokument bietet neben der Erzeugung binärer Zufallsfolgen ebenso einen Leitfaden für die Umwandlung von Bitfolgen in Zufallszahlen an. Darüber hinaus notwendige Techniken zur statistischen Prüfung von Zufallsgeneratoren und ihr detaillierter Aufbau, werden in diesem Dokument nicht behandelt.

Bisherige Ausgaben

- ISO/IEC 18031:2005
- ISO/IEC 18031:2011

4.6.10 ISO/IEC 18032

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Prime number generation Primzahlerzeugung

Inhalt und Anwendungsbereich

Dieses Dokument behandelt die Erzeugung von Primzahlen, wie sie für kryptographische Protokolle und Algorithmen gebraucht werden. Es legt Methoden fest, mit denen Zahlen darauf getestet werden können, ob sie Primzahlen sind, und zeigt die Anwendung dieser Methoden zur Primzahlenerzeugung und -prüfung. Weiterhin definiert es Varianten der Methoden zur Erzeugung von Primzahlen für die Erfüllung bestimmter kryptographischer Anforderungen.

Weitere Anmerkungen

Die in diesem Dokument festgelegten Methoden zur Erzeugung, Prüfung und Bestätigung von Primzahlen können bei kryptographischen Systemen angewendet werden, die auf den Eigenschaften von Primzahlen aufbauen (zum Beispiel einige asymmetrische Verfahren). Die Festlegungen zu den beschriebenen Tests beschreiben in einfachster Weise, welche Eigenschaften getestet werden müssen.

Bisherige Ausgaben

- ISO/IEC 18032: 2005

Authentifizierung

Informationstechnische Mechanismen zur Authentifizierung von Kommunikationspartnern bestehen aus einer Abfolge von Berechnungs- und Kommunikationsschritten und beinhalten zumindest zwei verschiedene Instanzen d.h. technische Ausprägungen für juristische oder natürliche Personen. Abhängig vom Typ der Berechnungsschritte unterscheidet man Mechanismen auf der Basis symmetrischer Blockschlüssel, digitaler Signaturen, kryptographischer Prüfsummen und von Zero-Knowledge-Protokollen. Letztere ermöglichen die Begrenzung der Informationsmenge, die in einem kryptographischen Protokoll von der beweisenden zur verifizierenden Instanz fließt.

Mechanismen zur Authentifizierung von Daten basieren auf der Berechnung bzw. Verifizierung kryptographischer Prüfsummen und werden häufig als Authentifizierungs-Codes oder MACs (Message Authentication Codes) bezeichnet.

4.6.11 ISO/IEC 9798

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Entity authentication Authentisierung von Instanzen

Inhalt und Anwendungsbereich

Die Normenreihe legt informationstechnische Mechanismen zur Authentisierung von Instanzen fest. Diese werden zur Bestätigung eingesetzt, dass eine Instanz tatsächlich die ist, die sie vorgibt zu sein. Eine zu authentisierende Instanz beweist ihre Identität, indem sie zeigt, dass sie einen geheimen Authentisierungsschlüssel kennt. Die Mechanismen sind für den technischen Austausch von Informationen zwischen Instanzen und, wo notwendig, mit einem vertrauenswürdigen Dritten (Trusted Third Party, TTP) gedacht.

Der Standard besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Mechanismen auf Basis von symmetrischen Verschlüsselungsalgorithmen (Mechanisms using symmetric encipherment algorithms)
- Teil 3: Authentifikation von Instanzen unter Benutzung eines Algorithmus mit öffentlichem Schlüssel (Mechanisms using digital signature techniques)
- Teil 4: Mechanismen auf Basis einer kryptographischen Prüffunktion (Mechanisms using a cryptographic check function)
- Teil 5: Mechanismen auf Basis von Zero-Knowledge-Techniken (Mechanisms using zero-knowledge techniques)
- Teil 6: Mechanismen auf Basis von manuellem Datentransfer (Mechanisms using manual data transfer)

Teil 1 führt in die grundlegenden Konzepte ein und beschreibt ein allgemeines Modell für die Authentifizierung von Instanzen.

Teil 2 legt vier Mechanismen zur Authentisierung von Kommunikationspartnern fest, die symmetrische Verschlüsselungsalgorithmen nutzen. Diese Mechanismen zeichnen sich dadurch aus, dass die zu authentisierenden Kommunikationspartner ihre Identitäten dadurch beweisen, dass sie einen geheimen Authentisierungsschlüssel kennen.

Teil 3 legt fünf Mechanismen zur Authentisierung von Kommunikationspartnern fest, die einen Algorithmus für öffentliche Schlüssel und eine Digitale Signatur zur Bestimmung der Identität einer Instanz nutzen. Die Anwendung dieses Teils ist nicht auf einen bestimmten Algorithmus begrenzt; jeder Algorithmus für öffentliche Schlüssel, der die Anforderungen der Authentisierungsalgorithmen erfüllt, kann eingesetzt werden.

Teil 4 legt vier Mechanismen zur Authentisierung von Kommunikationspartnern fest, die eine kryptographische Prüffunktion nutzen, und beschreibt den geforderten Inhalt von Nachrichten, der zur Aufstellung der Rahmenbedingungen notwendig ist.

Teil 5 legt drei Mechanismen zur Authentisierung von Instanzen fest, die Zero-Knowledge Techniken nutzen. Mit Zero-Knowledge bezeichnet man dabei die Eigenschaft, nur die Gültigkeit einer Authentisierung aber kein darüberhinausgehendes Wissen ableiten zu können. Alle in diesem Teil der Normenreihe festgelegten Mechanismen bieten die einseitige Authentisierung. Diese Mechanismen sind zwar nach den Prinzipien des Zero-Knowledge aufgebaut, können gemäß der genauen (mathematischen) Definition aber keine völlige Zero-Knowledge-Eigenschaft darstellen.

Teil 6 legt vier Mechanismen zur Authentisierung von Instanzen fest, die auf einem manuellen Datentransfer zwischen den authentisierenden Geräten aufbauen. Diese vier Mechanismen sind für unterschiedliche Gerätetypen geeignet.

Bisherige Ausgaben

- ISO/IEC 9798-1:1991; 1997; 2010
- ISO/IEC 9798-2:1994; 1999; 2008
- ISO/IEC 9798-2 COR1:2004
- ISO/IEC 9798-2:2008/Cor 1:2010
- ISO/IEC 9798-2:2008/Cor 2:2012
- ISO/IEC 9798-2:2008/Cor 3:2013
- ISO/IEC 9798-3:1993; 1998
- ISO/IEC 9798-3:1998/Cor 1:2009
- ISO/IEC 9798-3:1998/Amd 1:2010
- ISO/IEC 9798-3:1998/Cor 2:2012
- ISO/IEC 9798-4:1995; 1999
- ISO/IEC 9798-5:1999; 2004; 2009
- ISO/IEC 9798-6:2005; 2010
- ISO/IEC 9798-6:2005/Cor 1:2009

4.6.12 ISO/IEC 9797

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Message Authentication Codes (MACs) Nachrichten-Authentisierungscodes (MACs)

Inhalt und Anwendungsbereich

Die Normenreihe legt Algorithmen für Nachrichten-Authentisierungscodes (Message Authentication Code, MAC) das heißt Datenvollständigkeitsmechanismen fest, die eine kurze Zeichenkette (den MAC) als eine komplexe Funktion aus jedem Datenbit und einem geheimen Schlüssel erzeugen. MAC-Algorithmen werden eingesetzt, um die Integrität von Daten zu gewährleisten. Ihr Zweck ist die Entdeckung jeder unautorisierten Veränderung der Daten wie Löschen, Einfügen oder Transportieren von Objekten innerhalb der Daten.

Der Standard besteht aus den Teilen:

- Teil 1: Mechanismen auf Basis eines Blockschlüssel-Algorithmus (Mechanisms using a block cipher)
- Teil 2: Mechanismen auf Basis einer dedizierten Hash-Funktion (Mechanisms using a dedicated hash-function)
- Teil 3: Mechanismen auf Basis einer universellen Hash-Funktion (Mechanisms using a universal hash-function)

Teil 1 legt sechs MAC-Algorithmen fest, die auf dem CBC-Modus einer Blockchiffre beruhen. Zusätzlich werden drei Auffüllmethoden beschrieben. Das Auffüllen (Padding) wird notwendig, wenn die Länge des Datensatzes nicht ein Vielfaches der Blocklänge n ist.

Teil 2 legt drei MAC-Algorithmen fest, die einen geheimen Schlüssel und eine Hash-Funktion mit einem n-Bit Ergebnis nutzen, um einen m-Bit MAC zu berechnen. Insbesondere werden die Konstruktionsschemata HMAC und MDx-MAC spezifiziert.

Teil 3 legt vier MAC-Algorithmen fest, die einen geheimen Schlüssel und eine universelle Hash-Funktion mit einem n-Bit Ergebnis nutzen, um einen m-Bit MAC zu berechnen. Diese sind UMAC, Badger, Poly1305-AES und GMAC.

Weitere Anmerkungen

MAC-Algorithmen ermöglichen außerdem die Authentifizierung des Datenursprungs. Damit kann sichergestellt werden, dass eine Nachricht tatsächlich von einer Instanz kommt, die in Besitz eines bestimmten geheimen Schlüssels ist.

Bisherige Ausgaben

- ISO/IEC 9797-1: 1999, 2011
- ISO/IEC 9797-2: 2002, 2011
- ISO/IEC 9797-3: 2011
- ISO/IEC 9797:1994 (zurückgezogen)

PKI-Dienste

Unter dem Begriff Public-Key Infrastruktur (PKI) werden die Instanzen zusammengefasst, die für den Einsatz asymmetrischer Kryptographie (insbesondere digitaler Signaturen) in offenen Systemen erforderlich sind. Zu den wichtigsten Aufgaben einer PKI zählen die Registrierung der Nutzer sowie das Ausstellen, Verwalten und ggf. Prüfen von Zertifikaten, welche die Grundlage für die informationstechnische Fälschungssicherung darstellen.

Die Beweiskraft elektronischer Dokumente hängt entscheidend davon ab, ob Urheber und Inhalt, aber auch der Erstellungszeitpunkt zweifelsfrei und fälschungssicher feststellbar sind. Aus diesem Grund spielen neben digitalen Signaturen auch Zeitstempeldienste eine wichtige Rolle für die vertrauenswürdige elektronische Kommunikation.

4.6.13 ISO/IEC 15945

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Specification of TTP services to support the application of digital signatures Spezifikation der Dienste eines vertrauenswürdigen Dritten zur Anwendung auf Digitale Signaturen

Inhalt und Anwendungsbereich

Dieser Standard definiert technische Dienste für einen vertrauenswürdigen Dritten (Trusted Third Parties – TTP, in der Regel Trust Center), die im Zusammenhang mit digitalen Signaturen notwendig sind. Beispiele solcher Dienste sind Registrierung, Zertifizierung, Schlüsselerzeugung und Gegen-Zertifizierung. Erst die damit verbundene Interoperabilität macht auch das kommerzielle Anbieten solcher Dienste lohnend. Die Schwerpunkte des Dokumentes liegen auf der technischen Implementierung, Interoperabilität und technischen Anforderungen dieser Dienste.

Das Dokument richtet sich primär an die Betreiber von Trust-Centern (etwa Zertifizierungs-diensteanbieter), aber auch an die Hersteller von technischen Systemen für die Erbringung oder Nutzung solcher Dienste.

Weitere Anmerkungen

ITU-T publiziert ISO/IEC 15945 textgleich als Recommendation ITU-T X.843.

Bisherige Ausgaben

- ISO/IEC 15945:2002

4.6.14 ISO/IEC TR 14516

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Guidelines for the use and management of Trusted Third Party services Richtlinien für die Nutzung und das Management eines vertrauenswürdigen Dritten

Inhalt und Anwendungsbereich

Dieser Leitfaden behandelt Fragen des Managements und der Nutzung eines vertrauenswürdigen Dritten (in der Regel Trust Center) im Rahmen einer Public-Key Infrastruktur (PKI). Insbesondere spezifiziert er grundlegende Aufgaben und Dienste sowie die Rollen und Verantwortungsbereiche von Trusted Third Parties (TTPs) und deren Nutzern.

Das Dokument legt verschiedene Kategorien wie Zeitstempeldienste, Unleugbarkeit, Schlüsselverwaltung, Zertifikatsverwaltung und elektronische Beurkundung fest, in die Trusted Third Parties (TTP) Dienste eingeteilt werden

können. Innerhalb der einzelnen Kategorien sind logisch zu einander gehörenden Dienste zusammen gefasst.
Es werden Leitlinien für TTP Manager, Entwickler und Bediener sowie zur Unterstützung von Einsatz und Verwaltung von TTPs aufgestellt. Des Weiteren werden die Funktionseinheiten von TTP Diensten sowie die jeweiligen Aufgaben und Verantwortlichkeiten von TTPs und Anwendern festgelegt.

Weitere Anmerkungen

ITU-T publiziert ISO/IEC 14516 textgleich als Recommendation X.842.

Bisherige Ausgaben

- ISO/IEC TR 14516: 2002

Schlüsselmanagement

Aufgabe des Schlüsselmanagements ist die Bereitstellung und Kontrolle von Schlüsselmaterial für kryptographische Mechanismen. Dies umfasst insbesondere die Schlüsselerzeugung, -verteilung, -speicherung und -zerstörung. Eine Hauptaufgabe ergibt sich in den meisten Anwendungen daraus, dass sich die kommunizierenden Instanzen vor einer kryptographisch gesicherten Datenübertragung erst über die dabei zu verwendenden Schlüssel verständigen müssen. Schlüssel für symmetrische Kryptosysteme müssen auf sicherem Wege zwischen den Teilnehmern ausgetauscht und generell geheim gehalten werden. Bei asymmetrischen Systemen dagegen kann (oder muss sogar) je nach Anwendungsfall der öffentliche Schlüssel offen übertragen oder in einem öffentlich zugänglichen Verzeichnis gespeichert werden.

4.6.15 ISO/IEC 11770

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Key management Schlüsselmanagement

Inhalt und Anwendungsbereich

Der Zweck des Schlüsselmanagements ist die Bereitstellung von Verfahren zum Umgang mit kryptographischem Verschlüsselungsmaterial, das nach den gültigen Sicherheitsbestimmungen in symmetrischen oder asymmetrischen kryptographischen Algorithmen eingesetzt wird. Dieser Standard besteht aus den Teilen:

- Teil 1: Rahmenrichtlinien (Framework)
- Teil 2: Mechanismen unter Benutzung von symmetrischen Techniken (Mechanisms using symmetric techniques)
- Teil 3: Mechanismen auf Basis von asymmetrischen Techniken (Mechanisms using asymmetric techniques)

- Teil 4: Mechanismen auf Basis von schwachen Geheimnissen (Mechanisms using weak secrets)
- Teil 5: Gruppenschlüsselmanagement (Group key management)

Teil 1 legt die Ziele des Schlüsselmanagements fest, beschreibt die allgemeinen Modelle auf denen die Mechanismen des Schlüsselmanagements aufbauen, definiert die für alle Teile dieser Reihe gültigen Grundkonzepte der Schlüsselmanagement, bestimmt die Schlüsselmanagementdienste, stellt die Eigenschaften der Schlüsselmanagementmechanismen auf, legt die Anforderungen zur Verwaltung des Verschlüsselungsmaterials über den gesamten Lebenszyklus fest und beschreibt die Rahmenbedingungen für die Verwaltung des Verschlüsselungsmaterials über den gesamten Lebenszyklus.

Teil 2 definiert Mechanismen zur Schlüsselfestlegung unter Verwendung symmetrischer kryptographischer Techniken, genauer: entweder symmetrische Verschlüsselungsalgorithmen oder kryptographische Prüffunktionen. Diese Mechanismen können beispielsweise von den Mechanismen zur Authentisierung von Instanzen nach ISO/IEC 9798-2 abgeleitet werden, indem die Verwendung der Textfelder innerhalb dieser Mechanismen festgelegt wird. Das Dokument beschreibt den geforderten Inhalt von Nachrichten, die kryptographische Schlüssel nutzen oder notwendig sind, um die Bedingungen festzusetzen, bei denen ein geheimer Schlüssel erstellt werden kann.

Teil 3 definiert Mechanismen des Schlüsselmanagements für symmetrische Verfahren, die auf asymmetrischen kryptographischen Techniken basieren. Das Dokument befasst sich dabei vor allem mit der Bereitstellung eines gemeinsamen Geheimnisses für die Schlüsselauswahl und den Schlüsselaustausch zwischen zwei Partnern eines symmetrischen Verfahrens sowie die authentische Verteilung von dazu nötigen öffentlichen Schlüsseln der asymmetrischen Technik. Nicht betrachtet werden die weiteren Aspekte des Schlüsselmanagements wie Lebenszyklusverwaltung und Mechanismen zum Lagern, Archivieren, Löschen, Zerstören usw. von Schlüsseln.

Teil 4 definiert Mechanismen des Schlüsselmanagements, die auf schwachen Geheimnissen basieren. Er legt kryptographische Techniken fest, die für die Erstellung von einem oder mehreren geheimen Schlüsseln entwickelt wurden und auf einem von einem gespeicherten Passwort abgeleiteten schwachen Geheimnis beruhen. Das Dokument befasst sich jedoch nicht mit Aspekten wie Lebenszyklusverwaltung oder Mechanismen zum Lagern, Archivieren, Löschen, Zerstören usw. von schwachen Geheimnissen, starken Geheimnissen und erstellten geheimen Schlüsseln.

Teil 5 definiert Mechanismen zur Schlüsselfestlegung für (größere) Gruppen und behandelt sowohl Mechanismen für Baumstrukturen, als auch kettenbasierte Mechanismen.

Weitere Anmerkungen

Teil 1 behandelt sowohl die automatisierten als auch die manuellen Aspekte des Schlüsselmanagements. Teil 2 beschäftigt sich nicht explizit mit dem Gebiet des Interdomain-Schlüsselmanagements. Teil 3 deckt außerdem nicht die Anwendungen der Veränderungen ab, die von den Mechanismen des Schlüsselmanagements genutzt werden. Teil 4 beschreibt Mechanismen die entwickelt wurden, um ausgeglichene Vereinbarungen über passwortauthentisierte Schlüssel, erweiterte Vereinbarungen über passwortauthentisierte Schlüssel und das Abrufen passwort-authentisierter Schlüssel zu erreichen.

Bisherige Ausgaben

- ISO/IEC 11770-1:1996, 2010
- ISO/IEC 11770-2:1996, 2008
- ISO/IEC 11770-2:2008/Cor 1:2009
- ISO/IEC 11770-3:1999, 2008
- ISO/IEC 11770-3:2008/Cor 1:2009
- ISO/IEC 11770-4:2006
- ISO/IEC 11770-4:2006/Cor 1:2009
- ISO/IEC 11770-5:2011

Kommunikationsnachweise

Kommunikationsnachweise dienen dazu, das nachträgliche Ableugnen einer tatsächlich stattgefundenen Kommunikation technisch zu verhindern. Sicherheitsmechanismen für diesen Bereich werden häufig als eine Domäne asymmetrischer Kryptographie betrachtet, können jedoch auch mit symmetrischen Verfahren realisiert werden.

4.6.16 ISO/IEC 13888

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Non-repudation Nicht-Abstreitbarkeit

Inhalt und Zweck

Der Zweck von Nicht-Abstreitbarkeitsdiensten ist das Erstellen, Sammeln, Erhalten, Verfügbar-machen und Prüfen von technischen Beweisen zu geforderten Ereignissen oder Aktionen um Streitfälle über das Auftreten oder Wegbleiben dieser Ereignisse oder Aktionen lösen zu können.

Dieser Standard besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General model)
- Teil 2: Mechanismen auf Basis von symmetrischen Techniken (Mechanisms using symmetric techniques)
- Teil 3: Mechanismen auf Basis von asymmetrischen Techniken (Mechanisms using asymmetric techniques)

Teil 1 beschreibt ein Model für Nicht-Abstreitbarkeitsmechanismen, bei dem die Beweiserbrin-gung auf kryptographischen Prüfwerten beruht, die mit symmetrischen oder asymmetrischen kryptographischen Techniken erzeugt werden. Darunter fallen generische Beweiserzeugungs- und Prüfmechanismen, die sichere Hüllen und Digitale Signaturen umfassen und auf symmetrischen beziehungsweise asymmetrischen kryptographischen Techniken beruhen.

Teil 2 legt symmetrische Techniken nutzende Mechanismen für die Erzeugung, den Austausch und die Bestätigung von Nicht-Abstreitbarkeitsmerkmalen fest. Er beschreibt fünf Grundmechanismen zur Erstellung der Nicht-Abstreitbarkeit von Ursprung, Versendung, Empfang und Transport sowie für Zeitstempel. Für jeden davon müssen die beteiligten Instanzen in der Lage sein, einzeln mit dem vertrauenswürdigen Dritten (TTP) zu kommunizieren. Die Mechanismen erfordern den Einsatz bestimmter Nicht-Abstreitbarkeitsmerkmale.

Teil 3 legt zwei Mechanismen für die Bereitstellung von Nicht-Abstreitbarkeitsdiensten fest, die asymmetrische kryptographische Techniken nutzen und die Erzeugung von Beweisen für die Nicht-Abstreitbarkeit des Ursprungs (non-repudiation of origin, NRO) und die Nicht-Abstreitbarkeit der Zustellung (non-repudiation of delivery, NRD) ohne die direkte Beteiligung einem vertrauenswürdigen Dritten (TTP) ermöglichen. Darüber hinaus definiert dieser Teil Mechanismen für NRO und NRD unter Beteiligung einer TTP sowie für die Nicht-Abstreitbarkeit der Vorlage und die Nicht-Abstreitbarkeit des Transports.

Weitere Anmerkungen

Diese Normenreihe bietet Nicht-Abstreitbarkeitsmechanismen für die folgenden Phasen der Nicht-Abstreitbarkeit: Beweiserzeugung, Beweistransfer, -lagerung und -abfrage sowie Beweisbestätigung. Die Streitschlichtung liegt außerhalb des Anwendungsbereiches dieses Dokuments.

Bisherige Ausgaben

- ISO/IEC 13888-1:1997; 2004, 2009
- ISO/IEC 13888-2:1998, 2010
- ISO/IEC 13888-2:2010/Cor 1:2012
- ISO/IEC 13888-3:1997, 2009

Zeitstempeldienste

Die Beweiskraft elektronischer Dokumente hängt entscheidend davon ab, ob Urheber und Inhalt, aber auch der Erstellungszeitpunkt zweifelsfrei und fälschungssicher feststellbar sind. Aus diesem Grund spielen neben digitalen Signaturen auch Zeitstempeldienste eine wichtige Rolle für die vertrauenswürdige Kommunikation.

4.6.17 ISO/IEC 18014

Arbeitsgebiet:	Informationstechnik: IT-Sicherheitsverfahren
Name des Standards:	Time-stamping services Zeitstempeldienste

Inhalt und Anwendungsbereich

In der Normenreihe werden Mechanismen und Protokolle für vertrauenswürdige Zeitstempel spezifiziert.

Der Standard besteht aus den Teilen:

- Teil 1: Rahmenangaben (Framework)
- Teil 2: Zeitstempelmechanismen mit dedizierten Zeitstempeln (Mechanisms producing independent tokens)
- Teil 3: Zeitstempelmechanismen mit verknüpften Zeitstempeln (Mechanisms producing linked tokens)

In Teil 1 wird das Ziel einer Zeitstempelstelle bestimmt, ein allgemeines Modell, auf dem Zeit-stempeldienste aufbauen, beschrieben, Zeitstempeldienste und die Grundprotokolle von Zeitstempeln definiert, das allgemeine Protokoll zwischen den beteiligten Instanzen festgelegt und die Vernetzungsprotokolle für eine Zeitstempelstelle bestimmt.

Teil 2 definiert Zeitstempelmechanismen, die unabhängige Merkmale erstellen, damit ein Existenzbeweis nach dem anderen geprüft werden kann. Es werden drei voneinander unabhängige Mechanismen betrachtet: Zeitstempel, die Digitale Signaturen nutzen, Zeitstempel, die Codes zur Authentisierung von Nachrichten (MCA) nutzen und Zeitstempel, die Archivierung nutzen.

Teil 3 beschreibt Zeitstempeldienste, die verknüpfte Merkmale erzeugen. Ein allgemeines Model solcher Zeitstempeldienste wird ebenso vorgestellt wie die Hauptkomponenten zu deren Erstellung. Datenstrukturen und -protokolle für den Austausch mit solchen Zeitstempeldiensten werden definiert und typische Beispiele beschrieben. Dieser Teil definiert die zusätzlichen Datenarten, die die Anwendung von Zeitstempelmechanismen unterstützen, um verknüpfte Merkmale zu erzeugen. Außerdem werden die Verknüpfungs-, Gruppierungs- und Veröffentlichungsabläufe sowie die dazugehörigen Protokolle festgelegt.

Weitere Anmerkungen

Der Einsatz von unabhängigen Merkmalen (Teil 2) setzt Vertrauen in die Zeitstempelstelle (Time stamping authority, TSA) voraus.

Bisherige Ausgaben

- ISO/IEC 18014-1:2002, 2008
- ISO/IEC 18014-2:2002, 2009
- ISO/IEC 18014-3:2004, 2009

5 Anhang

Bezug zu anderen Standards

Standards beziehen sich auch auf andere Standards. In der folgenden Liste sind diese Abhängigkeiten aufgeführt. Die Liste besitzt nicht den Anspruch auf Vollständigkeit.

Informationssicherheits-Managementsysteme (ISMS)

ISO/IEC 27001	ISO/IEC 27001 bezieht sich besonders eng auf ISO/IEC 27002 und hat eine inhaltliche Verbindung zu allen anderen Normen der 2700x-Familie. Im Kontext integrierter Managementsysteme ist auch ISO 9000 als Normenreihe zu nennen.
ISO/IEC 27002	Da hier Sicherheitsmanagement behandelt wird, besteht ein enger Bezug zu ISO/IEC 27001.

Risikomanagement

ISO/IEC 27005	Das Risikomanagement hat wesentliche inhaltliche Bezüge zur ISO/IEC 27001 und zur ISO 9000

Evaluierung von IT-Sicherheit

Common Criteria

ISO/IEC 15408 (CC)	Mehrere andere Dokumente stehen in Bezug zu diesem Standard: ISO/IEC 18045 definiert die Methodologie, mit der Evaluierungen gemäß 15408 durchgeführt werden. Insofern ist hier eine unmittelbare Abhängigkeit vorhanden. ISO/IEC 15446 gibt Hinweise, wie Schutzprofile (Protection Profiles) und Sicherheitsvorgaben (Security Targets) verfasst werden, die im Kontext der Evaluierung nach 15408 relevant sind. ISO/IEC 15292 stellt die Arbeitsweise von Registrierungsstellen für Protection Profiles dar. Der technische Bericht ISO/IEC 19791 stellt eine Möglichkeit dar, die Evaluierung auf IT-Systeme inklusive ihres Betriebs anzuwenden.
ISO/IEC TR 15443	Da es das Ziel dieses Standards ist, einen Weg zur Auswahl von Vertrauenswürdigkeitsmethoden aufzuzeigen, besteht naturgemäß ein Zusammenhang zu allen anderen Standards, die in diesem Abschnitt genannt sind. Fast alle von ihnen gehören zu einer der Vertrauenswürdig-keitsmethoden, die im Standard behandelt werden. Darüber hinaus werden aber auch viele ISO- und Nicht-ISO-Standards in ISO/IEC TR 15443 behandelt, die im vorliegenden Dokument nicht behandelt wurden.
ISO/IEC 18045	Ein Bezug besteht unmittelbar zur ISO/IEC 15408 (Common Criteria), und dadurch indirekt zu weiteren damit zusammenhängenden Standards.

■ ISO/IEC 21827 (SSE-CMM)	SSE-CMM wurde ebenfalls als Fast Track in der ISO/IEC – als International Standard (IS) 21827 – eingereicht. Zu folgenden Standards besteht ein Bezug: ISO/IEC 12207, , ISO/IEC 15288, ISO/IEC TR 1504-2, ISO/IEC TR 1504-4, ISO/IEC 27002.

Schutzprofile

■ ISO/IEC TR 15446	Ein Bezug besteht unmittelbar zur ISO/IEC 15408 (Common Criteria), und dadurch indirekt zu weiteren damit zusammenhängenden Standards

.

Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Verschlüsselung

■ ISO/IEC 18033	ISO/IEC 10116
■ ISO/IEC 10116	ISO/IEC 8372, ANSI X3.106, FIPS Publication 81
■ ISO/IEC 19772	ISO/IEC 9796-2/6, ISO/IEC 9797-1/2, ISO/IEC 11770-1/4, ISO/IEC 14888-1/3, ISO/IEC 18033-1/4

Digitale Signaturen

■ ISO/IEC 9796	ISO/IEC 9797-2, ISO/IEC 10118-1/4, ISO/IEC 9798-1, ISO/IEC 14888-1/3
■ ISO/IEC 14888	ISO/IEC 8825-1, ISO/IEC 10118 (alle Teile), ISO/IEC 15946-1
■ ISO/IEC 15946	ISO/IEC 9796-3, ISO/IEC 11770-3

Hash-Funktionen und andere Hilfsfunktionen

■ ISO/IEC 10118	ISO/IEC 9797
■ ISO/IEC 18031	ISO/IEC 10116, ISO/IEC 10118-3, ISO/IEC 11770-1, ISO/IEC 18032, ISO/IEC 18033-3, ISO/IEC 19790
■ ISO/IEC 18032	ISO/IEC 18031

Authentifizierung

■ ISO/IEC 9798	ISO 7498-2, ISO/IEC 10181-2
■ ISO/IEC 9797	ISO 7498-2, ISO/IEC 10116, ISO/IEC 10118-1, ISO/IEC 10118-3

PKI-Dienste

■ ISO/IEC 15945	ISO/IEC 9594-8, ISO/IEC 9798-1, ISO/IEC 10118-1, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 10118-4, ISO/IEC 11770-1, ISO/IEC 11770-3, ISO/IEC 14888-2, ISO/IEC 14888-3 ISO/IEC 27002, ISO/IEC 13888-1, ISO/IEC 13888-2, ISO/IEC 13888-3 ISO/IEC TR 14516 ergänzt diesen Standard durch Richtlinien zur Nutzung und Management eines vertrauenswürdigen Dritten (in der Regel Trust Center).
■ ISO/IEC TR 14516	ISO/IEC 9594-8, ISO/IEC 10181-1, ISO/IEC 10181-4, ISO 7498-2, ISO/IEC IS 15945 ergänzt diesen TR durch die technische Spezifikation von Protokollen für solche Services.

Schlüsselmanagement

ISO/IEC 11770	ISO/IEC 9796-3, ISO/IEC 9798-2, ISO/IEC 9798-3, ISO/IEC 10118-1, ISO/IEC 10118-3, ISO/IEC 15946-1, ISO/IEC 18031, ISO/IEC 18032, ISO/IEC 18033-1

Kommunikationsnachweise

■ ISO/IEC 13888	ISO/IEC 9796, ISO/IEC 9797, ISO/IEC 10118 (alle Teile), ISO/IEC 14888 (alle Teile)

Zeitstempeldienste

■ ISO/IEC 18014	ISO/IEC 9798-1, ISO/IEC 10118-1, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 10118-4, ISO/IEC 11770-1, ISO/IEC 11770-3, ISO/IEC 14888-2, ISO/IEC 14888-3, ISO/IEC 15946-2

Links

BSI / IT-Grundschutz

Alle Unterlagen zum IT-GSHB findet man auf der Webseite des Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de).
Alle Unterlagen zum IT-Grundschutzhandbuch sind beim BSI unter www.bsi.bund.de/gshb/index.htm zu finden, sowohl der Leitfaden (http://www.bsi.bund.de/gshb/Leitfaden/index.htm) als auch das Grundschutztool (www.bsi.bund.de/gstool/index.htm).

CC

Der internationale Standard ISO/IEC 15408 steht kostenlos zur Verfügung, z. B. unter http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

FIPS 140-2

Der internationale Standard steht kostenlos zur Verfügung, z. B. unter csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

ISO

Informationen zur ISO-Organisation findet man auf der Webseite www.iso.org.

ITTF

Informationen zu ISO/IEC Joint Technical Committee 1 (JTC 1) und dem Arbeitsprogrammen einzelner Unterkomitees des JTC 1 sowie zu prozeduralen Fragen findet man auf der Webseite isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/ITTF.htm.

ISO/IEC JTC 1

Webseite des ISO/IEC Joint Technical Committee 1 (JTC 1): isotc.iso.org (siehe dann: Home, dann: ISO/IEC 001 JTC 1 »Information technology)

ISO/IEC JTC 1/SC 27

Informationen über das ISO/IEC-Unterkomitee ISO/IEC JTC 1/SC27 »IT Security techniques« sind unter www.jtc1sc27.din.de/en verfügbar

SD 6 »Glossary of IT Security Terminology«

Standing Document 6 (SD6) – Glossary of IT Security Terminology ist verfügbar unter www.jtc1sc27.din.de/sce/sd6 (siehe dann: Downloads)

SD 7 »Catalogue of SC27 Projects and Standards«

Standing Document 7 (SD7) – ISO/IEC JTC 1/SC27 Catalogue of Projects and Standards kann heruntergeladen werden unter www.jtc1sc27.din.de/sce/sd7 (siehe dann: Download)

NIST

Das National Institute of Standards and Technology des US Handelsministerium hat eine Webseite unter www.nist.gov.

DIN

Informationen über die Tätigkeiten des Deutschen Institut für Normung findet man auf der Webseite www.din.de.

DIN NI

Informationen über den DIN-Normenausschuss »Informationstechnik« (NI) und seine Arbeitsausschüsse sind unter www.nia.din.de verfügbar

DIN VDE

Das VDE-Vorschriftenwerk umfasst Satzungen und sonstige Grundsatzschriftstücke des VDE, DIN VDE-Normen (VDE-Bestimmungen), VDE-Leitlinien und Beiblätter zu den vorgenannten Schriftstücken (www.vde-verlag.de/normen.html)

ISACA

Information Systems Audit and Control Association – Verband Internationaler Auditoren der Informatik.
Der Cobit Standard kann kostenlos bei www.isaca.de heruntergeladen werden.
(Es existiert nur von der Version 4.0 eine deutschsprachige Fassung)

6 Ausblick – so geht's weiter

Mit dieser Sonderauflage zur CEBIT 2014 betreten wir gewisses Neuland. Verstärkt wurde an uns in der Vergangenheit der Wunsch herangetragen, die Vielfalt der IT-Sicherheitsstandards auf bestimmte Themenbereiche herunter zu brechen. Diesem Wunsch haben wir in dieser Ausgabe im Thema der elektronischen Identitäten entsprochen und wir wollen diesen Ansatz weiterführen. Die nächste Sonderausgabe mit einem Themenschwerpunkt ist zum Herbst 2014 geplant. Die vorliegende Auswahl der Standards beschreibt dabei nur einen Teil der verfügbaren Standards. Weitere Standards finden Sie auf der Kompass-Internetseite.

Mit den Möglichkeiten des Internets verbunden sind ebenfalls eine Reihe von Eigenschaften, die dazu beitragen, den Kompass der IT-Sicherheitsstandards kontinuierlich zu erweitern und für Sie noch nutzbarer zu machen. Neben fortlaufenden Aktualisierungen profitieren Sie online auch von komfortablen Möglichkeiten zur Qualitätsverbesserung des »Kompass der IT-Sicherheitsstandards« beizutragen und sich mit Ihren Anmerkungen und Anregungen aktiv einzubringen. Wir freuen uns auf Ihre Rückmeldungen und wünschen Ihnen abschließend eine gute Lektüre unter:
www.kompass-sicherheitsstandards.de

Auch die Online-Version sowie dieser Sonderdruck des Leitfadens »Kompass der IT-Sicherheitsstandards« entstanden durch die enge Zusammenarbeit zwischen BITKOM und DIN. Allen beteiligten danken wir für die Mitarbeit, die diese Ausgabe ermöglicht hat, sehr herzlich auf unserer Webseite.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 2.100 Unternehmen, davon rund 1.300 Direktmitglieder mit 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. 900 Mittelständler, mehr als 100 Start-ups und nahezu alle Global Player werden durch BITKOM repräsentiert. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Das DIN ist ein eingetragener gemeinnütziger Verein mit Sitz in Berlin (DIN Deutsches Institut für Normung e. V., gegründet 1917). Das DIN ist die für die Normungsarbeit zuständige Institution in Deutschland und vertritt die deutschen Interessen in den weltweiten und europäischen Normungsorganisationen. Dieser Status wurde im Vertrag mit der Bundesrepublik Deutschland am 5. Juni 1975 anerkannt.
Das DIN ist der runde Tisch, an dem sich Hersteller, Handel, Verbraucher, Handwerk, Dienstleistungsunternehmen, Wissenschaft, technische Überwachung, Staat, d. h. jedermann, der ein Interesse an der Normung hat, zusammensetzen, um den Stand der Technik zu ermitteln und unter Berücksichtigung neuer Erkenntnisse in Deutschen Normen niederzuschreiben.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

DIN

Deutsches Institut der Normung e.V.
Normenausschuss Informationstechnik und Anwendung (NIA)

Burggrafenstraße 6
10787 Berlin
Telefon 030/2601-0
Telefax 030/2601-1231
nia@din.de
www.nia.din.de