Schlüsselfragen

Zur Umsetzung der Vertraulichkeit und Integrität von Daten in IT-Anwendungen sind meist Verschlüsselung und Signaturen die Mittel der Wahl. Bei ihrem Einsatz sind allerdings neben der Qualität des genutzten kryptographischen Verfahrens weitere -in vielen Fällen ebenfalls sehr sicherheitsrelevante- Aspekte zu berücksichtigen.

Obwohl zentrale Voraussetzung aller Systeme, die auf der Sicherheit von Schlüsseln beruhen, zeigt sich häufig, dass das Thema Key Management zu wenig Aufmerksamkeit bekommt. Dies erstaunt umso mehr, da doch gerade durch ein fehlerhaftes Key Management schwere Sicherheitsprobleme auf der einen Seite, aber auch eine Verletzung datenschutzrechtlicher Anforderungen auf der anderen Seite resultieren können.

Dieses Schwerpunktheft befasst sich daher mit den Fragen rund um das Thema Sicherheit und Datenschutz beim Key Management. Aufbauend auf den generellen Fragen zum Thema stellen die einzelnen Autoren dabei anhand von Praxisbeispielen konkrete Lösungsansätze, aber auch mögliche Problemfelder vor.

- Im ersten Beitrag **Konzept und Nutzen von Certificate Policy und Certification Practice Statement** gehen Jürgen Brauckmann und Ralf Gröper der Frage nach, ob CP und CPS überhaupt dazu geeignet sind, die Sicherheit einer PKI zu beurteilen.
- Der anschließende Beitrag **Key Management - Fundamentals** von John Babbidge beschäftigt sich dann mit den wesentlichen Grundanforderungen an ein sinnvolles und vor allem sicheres Key Management.
- Kim Nguyen und Carsten Schwarz eröffnen mit ihrem Beitrag **Innovatives Key Management für die Qualifizierte Elektronische Signatur mit dem neuen Personalausweis** den Themenblock zum *Key Management mit dem nPA*. Sie stellen die Verfahren zur „Signature as a Service“ und „Verification as a Service“, sowie die Nutzungsmöglichkeiten der Webapplikation „sign-me“ vor.
- Im Beitrag **Authentisierung mit der Open eCard App** widmet sich das Autorenteam um Detlef Hühnlein im Anschluss den unterschiedlichen Mechanismen zur Authentisierung mit dem nPA, bspw. durch die Open eCard App.
- **Sichere Nutzung von Cloud-Speicherdiensten** titelt der erste von zwei Beiträgen zum Themenblock *Key Management bei Daten in der Cloud*. Lukas Kalabis, Thomas Kunz und Ruben Wolf adressieren hierbei das Thema aus Richtung der Nutzung von Cloud-Speicherdiensten.
- Michael Kranawetter geht im Beitrag **Identität in der Cloud und On-premise** dann auf „Windows Azure“ ein und zeigt dabei die speziellen Möglichkeiten auf.

Ergänzt wird der Schwerpunkt des Heftes diesmal durch insgesamt fünf Aufsätze:

- Thomas Kunz, Peter Niehues und Ulrich Waldmann stellen eine mögliche **Technische Unterstützung von Audits bei Cloud-Betreibern** dar.
- Der Beitrag **Datensicherheit: Was leisten externe verschlüsselte Festplatten?** von Leonid Gimbut beschäftigt sich mit Verschlüsselung mobiler Datenträger und wird durch eine Stellungnahme des ULD ergänzt, das die Datenschutzzertifizierung durchgeführt hat.
- Martin Schröder und Frank Morgner stellen dann in ihrem Beitrag das Thema der **eID mit abgeleiteten Identitäten** vor.
- Im Beitrag **Zur Problematik der Identifikation ausländischer Teilnehmer im Vollzug des deutschen Emissionshandels** geht Renée Hinz auf die Aspekte ein, die einer internationalen Organisation, bspw. bei der Umsetzung der Anforderungen nach dem Signaturgesetz, begegnen können.
- Abschließend stellen dann Björn Schreinermacher und Benedikt Buchner ihre Überlegungen zum Thema **Interviews online stellen** vor.

Zusammen mit dem gesamten Herausgeberteam wünsche ich Ihnen als Gastherausgeber eine informative und spannende Lektüre. Wir hoffen, dass auch diese Ausgabe Ihnen, verehrte Leserinnen und Leser, viele Anregungen für Ihre Projekte gibt.

Christoph Wegener