Zeitschrift für Datenrecht und Informationssicherheit

digma

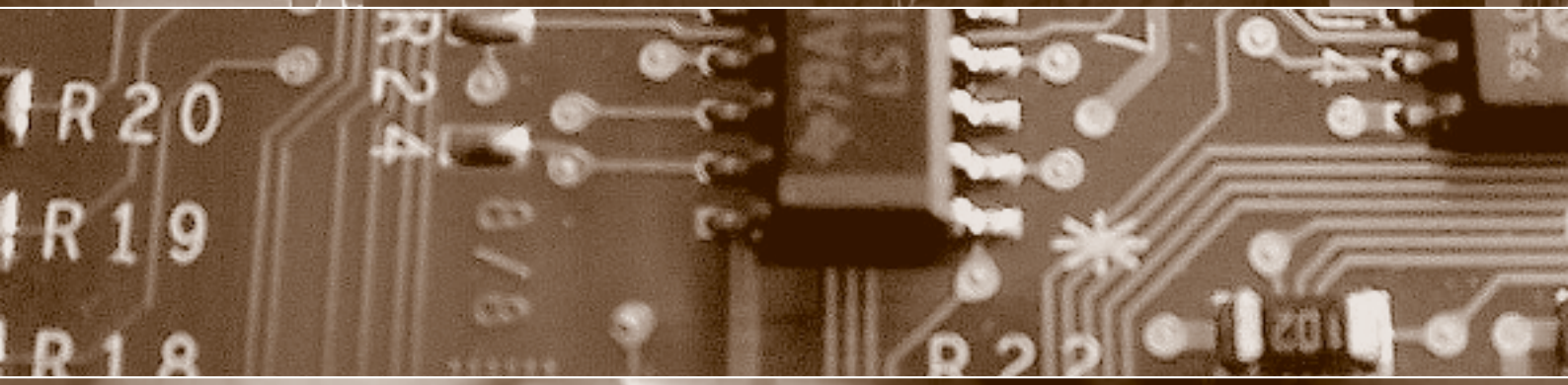
www.digma.info 17. Jahrgang, Heft 1, März 2017

digma-Tagung zum Datenschutz 2017
Infos zum Programm im Heft

Schwerpunkt:

Datenschutzreform

fokus: Souveräner Datenschutz ist notwendig
fokus: Mehr Datenschutz durch Technik?
report: Einsetzbare Kryptographie für die Cloud



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Datenschutzreform

Extraterritoriale Wirkung der DSGVO

Wann gelten die Bestimmungen der DSGVO auch für Schweizer Unternehmen? Und inwiefern findet das schweizerische Datenschutzrecht auf internationale Verhältnisse Anwendung? In der Praxis schwieriger wird die Vollstreckung von datenschutzrechtlichen Massnahmen und Sanktionen im internationalen Verhältnis sein.

Mehr Datenschutz durch Technik?

Vieles, was in der neuen Datenschutzgrundverordnung gefordert wird, scheint «technisch möglich», doch noch kaum in der Praxis erprobt. Nutzer werden die umfangreichen Informations- und Partizipationsrechte der DSGVO wohl erst nutzen können, wenn Software- und Onlineserviceindustrie erste mit technischem Datenschutz integrierte Produkte anbieten können.

Souveräner Datenschutz ist notwendig

Das DSG hat angesichts der rasanten technologischen Entwicklungen an Wirkung verloren. Mit der Totalrevision des DSG bietet sich nun die Gelegenheit, das DSG wieder richtig zu justieren. Dabei ist aber bei allen Bestimmungen deren Wirksamkeit kritisch zu hinterfragen: Wo wäre weniger mehr?

Anpassungsbedarf in den Kantonen

Auch die Kantone müssen ihre Datenschutzgesetze den neuen Anforderungen anpassen. Dabei sind die Regelungen nicht eins zu eins zu übernehmen – es muss im Resultat ein gleichwertiger Schutz gewährleistet werden. Der Leitfaden der Konferenz der Kantonsregierungen leistet den Kantonen wertvolle Unterstützung für eine Umsetzung mit Augenmass.

In eigener Sache

Wie auf Seite 113 in digma 2016.3 angekündigt, erscheinen die beiden Nummern 2016.4 und 2017.1 als Doppelnummer erst Ende des ersten Quartals 2017. Der Grund ist die Tatsache, dass die Vernehmlassungsunterlagen des Bundes für die Totalrevision des Datenschutzgesetzes statt, wie ursprünglich angekündigt, im August erst im Dezember 2016 veröffentlicht wurden. Damit war es den Autorinnen und Autoren nicht möglich, ihre Manuskripte rechtzeitig für die Nummer 2016.4 fertigzustellen. Die vorliegende Nummer ist dafür umso umfangreicher ausgefallen und vereint Beiträge sowohl zur Bedeutung der EU-Datenschutzreform für die Schweiz als auch zum Vorschlag des Bundesrates für die Schweizer Datenschutzreform inklusive der Umsetzung der internationalen Vorgaben in den Kantonen. Wir danken für Ihr Verständnis und wünschen eine erhellende Lektüre!

Einsetzbare Kryptografie für die Cloud

Es gibt geeignete kryptografische Mechanismen, die dem Cloud-Nutzer anstelle lediglich reiner Zusagen in Service Level Agreements technische Sicherheit und erhöhten Datenschutz bieten. Was braucht es zur korrekten Anwendung? Daran arbeitet das Horizon-2020-Projekt PRISMACLOUD.

Chance zur Stärkung des Datenschutzes

privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, nimmt Stellung zum Vorentwurf zum totalrevidierten DSG. Er ist eine Chance, das DSG den aktuellen Herausforderungen anzupassen, auch wenn es noch Verbesserungsbedarf gibt.

Wirksames Datenschutzgesetz

Was sich unser Cartoonist denkt, wenn er von bestimmten Wirtschaftsverbänden hört, das alte Datenschutzgesetz tue es eigentlich schon …

report

forum

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, lic. iur. Marco Fey

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Inland: CHF 174.00, Jahresabo Ausland: CHF 199.00, Einzelheft: CHF 48.00
PrintPlus: Jahresabo Inland: CHF 195.00, Jahresabo Ausland CHF 220.00

PrintPlus: Das PrintPlu§-Abonnement bietet die Möglichkeit, bequem und zeitgleich zur Printausgabe jeweils das PDF der ganzen Ausgabe herunterzuladen. Detaillierte Informationen finden Sie unter www.schulthess.com/printplus.

Anzeigenmarketing: Zürichsee Werbe AG, Herr Pietro Stuck, Seestrasse 86, 8712 Stäfa
Tel. +41 (0)44 928 56 11, pietro.stuck@zs-werbeag.ch

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, www.schulthess.com, zeitschriften@schulthess.com

Forschung

Einsetzbare Kryptografie für die Cloud

Henrich C. Pöhls, Dipl.Inform. M.Sc. Info.-Sec., wissenschaftlicher Mitarbeiter, Universität Passau, Deutschland hp@sec.uni-passau.de

Thomas Länger, Dipl.-Ing. Dr., Premier Assistant, Université de Lausanne, Schweiz thomas.laenger@unil.ch

Cloud-Computing erobert seit mehreren Jahren immer weitere Anwendungsfelder. Bedeutende technische Fortschritte wurden gemacht, die eine On-Demand-Bereitstellung von Ressourcen zu einem vertretbar günstigen Preis ermöglichen. In der Kryptografie existieren gute und durchaus performante Mechanismen, um viele Sicherheits- oder Datenschutzprobleme, die beim Cloud-Computing entstehen, zu lösen. Um diese verfügbar zu machen, werden neben den geeigneten Krypto-Verfahren, welche für den Anwendungskontext die passende kryptografische Sicherheit aufweisen müssen, aber auch einsetzbare Softwarekomponenten benötigt – oder am besten gleich fertige Cloud-Services. Es braucht zusätzlich noch anwenderverständliche Beschreibungen der Sicherheitsprobleme und -lösungen. In diesem Beitrag werden mögliche interdisziplinäre Hemmnisse identifiziert und die dafür im Forschungsprojekt EU H2020 PRISMACLOUD[1] bereits erarbeiteten Lösungsvorschläge dargelegt.

Einsetzbares Cloud-Computing

Cloud-Computing ist inzwischen einfach benutzbar geworden. Dies ermöglicht den Cloud-Nutzern, Dienstleitungen von Cloud-Anbietern zu beziehen, die ein weites Spektrum abdecken: von ganzen Infrastrukturen (also virtuellen Rechnern; Infrastructure-as-a-Service), über Datenspeicherung (Storage-as-a-Service), bis hin zu reiner Rechenleistung (Computing-as-a-Service). Erst der fortgeschrittene Abbau der technischen Komplexität für die Endnutzer hat Cloud-Computing zu einem Massenmarkt wachsen lassen. Während die Einstiegshürden für Nutzer immer weiter sinken, sind die Risiken, welche solch ein technisches «Outsourcing» mit sich bringt, nicht gesunken.

Bedrohungen

Der Verlust der Privatsphäre von Individuen, oder die Kompromittierung der Vertraulichkeit von Geschäftsgeheimnissen sind die offensichtlichen Bedrohungen; aber auch der Verlust der Integrität von gespeicherten Daten oder fehlerhafte Berechnungen müssen als Bedrohungen auf Seiten der Cloud-Nutzer berücksichtigt werden. Die mit diesen Bedrohungen verbundenen Risiken umfassen technische Risiken, aber insbesondere eine Anzahl von ernstzunehmenden Datenschutz- und Privatsphärerisiken. Diesen Risiken wird heutzutage überwiegend mit organisatorischen Massnahmen begegnet, wie zum Beispiel mit «Best Practices» und rechtlichen «Service Level Agreements». Zu häufig hängt die Wirksamkeit dieser Instrumente vom «guten Willen» des Datenbearbeiters ab. Bei Verstössen greifen nur Rechtsmittel, wünschenswert wäre eine präventive, technische Lösung.

Lösungen

Bekannte und bereits weitverbreitete kryptografische Verfahren bringen häufig keine Lösung. Die existierenden und etablierten Lösungen, wie Verschlüsselung und Digitale Signaturen kommen häufig bereits bei den Anforderungen der meisten Cloud-Anwendungsszenarien an ihre Grenzen. Will man beispielsweise eine kryptografische Standardverschlüsselung für eine Shared-Storage-Anwendung einsetzen, dann verwandelt eine client-seitige Verschlüsselung zwar die Daten in nicht mehr lesbare Chiffrate und sichert so deren Vertraulichkeit in der Cloud. Allerdings bedarf ein Teilen der Daten mit Dritten nun einer sicheren Verteilung des Schlüssels.

Spezielle Kryptografie

Wir geben im Folgenden drei Beispiele[2] für kryptografische Verfahren zur Lösung spezieller Probleme des Cloud-Computings, welche in PRISMACLOUD von der mathematischen Kryptografie bis hin zur einsetzbaren cloud-basierten Anwendung gebracht werden sollen:

- *Secret Sharing Schemes* für die verteilte Speicherung von Daten,
- *Malleable Signatures* zur Datenreduktionen unter Beibehaltung der Authentizität,
- *Verifiable Computing* zur Überprüfbarkeit von an die

Cloud delegierten Berechnungen.

Diese Methoden gelten als kryptografisch sicher und können heute mit überschaubaren Overhead eingesetzt werden.

Secret Sharing

Für die verteilte Datenspeicherung in der Cloud bieten sich Secret Sharing-Technologien an. Diese wurden 1979 von Adi Shamir beschrieben[3]. Sie sichern die Vertraulichkeit der Daten bei der Übermittlung und Speicherung von Daten in der «Public Cloud», aber es reicht ein einfacheres Zugriffsmanagement, um Daten mit autorisierten Dritten zu teilen. Dazu werden die Daten zunächst beim End-Nutzer in mehrere verschiedene sog. «Shares» umgerechnet. Ein Share allein ergibt keinen Sinn und wird daher, wie verschlüsselte Daten auch, bei einem Cloud-Anbieter gespeichert. Anders als bei verschlüsselten Daten bedarf es für die Entschlüsselung keines Schlüssels, sondern es wird eine vorher festgelegte Anzahl der Shares benötigt, um die Daten wiederherzustellen. Daher verteilt man die Shares auf mehrere verschiedene Anbieter, so kann keiner allein die Originaldaten wiederherstellen. Um Daten mit anderen zu teilen, gibt man autorisierten Nutzern Zugriff auf die notwendige Anzahl von Shares. Es reicht also aus, wenn der Anwender den Zugriff für Dritte autorisiert, es müssen ihnen keine Schlüssel übermittelt werden; auch müssen die Daten im Vorfeld nicht für bestimmte Empfänger vorbereitet worden sein.

Malleable Signatures

Malleable Signature Schemes (dt. «editierbare Signaturen») sind spezielle digitale Signaturen, die Anfang der Zweitausender-Jahre erstmals beschrieben wurden[4]. Sie können gleichzeitig die Authentizität von Daten bewahren, erlauben aber auch, dass die Daten nach Massgabe der Dateneigentümer verarbeitet werden. So ermöglicht diese Technologie konsequent die Umsetzung der «data minimisation», welche der Datenschutz häufig fordert: Teile der signierten Daten können vor der Weitergabe an Dritte «entfernt» werden, wobei die Authentizitätseigenschaft der zurückbleibenden Daten erhalten bleibt. Mit anderen Worten: Die digitale Signatur verifiziert korrekt, selbst wenn Teile entfernt wurden. Welche Teile entfernt oder geändert werden dürfen[5], kann mittels einer Sicherheitsrichtlinie geregelt werden.

Verifiable Computing

Weiter als editierbare Signaturen geht Verifiable Computing. «Functional Signatures Schemes» ermöglichen die Überprüfung der Ergebnisse von Berechnungen, ohne die Berechnungen zur Kontrolle selbst durchführen zu müssen. Fehlerhafte Berechnungen der Cloud werden damit erkennbar.

Anwendungshemmnisse

Obgleich schon längere Zeit bekannt, finden sich die genannten Verfahren heute kaum in der Breite der Cloud-Anwendungen. Wir haben folgende sechs Hinderungsgründe identifiziert:

- unzureichende Softwareunterstützung,
- unzureichendes Verständnis der kryptografischen Methoden,
- keine verständliche Beschreibung der Sicherheitszugewinne für Anwender,
- unzureichende Standardisierung,
- kryptografische Optimierungen mit geringen Anwendungsnutzen und
- rechtliche Unklarheiten.

Die obige Liste ist nicht priorisiert und erhebt auch nicht den Anspruch auf Vollständigkeit. Insbesondere durch die Abhängigkeiten zwischen den obigen Gründen

Kurz&bündig

Die gute Nachricht: Es gibt geeignete kryptografische Mechanismen, die dem Cloud-Nutzer anstelle lediglich reiner Zusagen in Service Level Agreements (SLA) technische Sicherheit und erhöhten Datenschutz bieten. Die schlechte Nachricht: Sie benötigen kryptografische Expertise zur korrekten Anwendung. Die Lösung sind benutzbare Softwarebibliotheken, welche die kryptografischen Funktionalitäten vollständig einkapseln, und zusätzlich Standards. Dies erfordert eine interdisziplinäre Zusammenarbeit von Kryptografen mit Software- und Cloud-Service-Entwicklern.

Literatur

- Shamir Adi, How to Share a Secret, Communications of the ACM, Nov. 1979, Vol. 22 No.11.
- Steinfeld R./Bull L./Zheng Y., Content extraction signatures, ICISC 200, vol. 2288, 163–205, Springer, 2002.
- Johnson R./Molnar D./Song D./Wagner D., Homomorphic signature schemes, CT-RSA, 244–262, Springer, 2002.
- Ateniese G./Chou D.H./de Medeiros B./Tsudik G., Sanitizable signatures. ESORICS 2005, LNCS 3679, 159–177. Springer, 2005.
- Länger T./Pöhls H.C./Ghernaouti S., Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds, ENISA Annual Privacy Forum, 2016, Springer.
- Lorünser T./Slamanig D./Länger T./Pöhls H.C., PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services, 11th ARES Conference, 2016, IEEE.
- von Geelkerken F.W.J./Pöhls H.C./Fischer-Hübner S., The legal status of malleable- and functional signatures in light of Regulation (EU) No 910/2014, 3rd Int. Academic Conference of Young Scientists on Law & Psychology, 2015.
- Höhne F./Pöhls H.C./Samelin K., Rechtsfolgen editierbarer Signaturen, Datenschutz und Datenrecht (DuD), 36 (6) 485-491, 2012.

(z.B. braucht es Referenzimplementierungen für die meisten Standardisierungsprozesse), befinden sich eine Reihe der oben genannten kryptografischen Verfahren noch «in der Warteschleife». Diese zu beenden ist eines der Hauptziele des EU-geförderten Forschungsprojekts PRISMACLOUD. Wir werden im letzten Abschnitt des Artikels nun die Probleme und Lösungswege beschreiben, die zu einer grösseren Verbreitung führen sollen.

Softwareunterstützung

Unzureichender Softwareunterstützung wird durch konsequente Implementierung der Algorithmen und deren Umsetzung als Software-Bibliotheken begegnet. Ausgehend von den in Bibliotheken gekapselten Algorithmen werden prototypische Cloud Services entwickelt, welche die korrekte Verwendung der kryptografischen Methoden zeigen. Diese Cloud Services können in der Public Cloud bereitgestellt werden und bieten den Top-Level-Anwendungen Schnittstellen und Funktionen wie jeder andere Cloud Service.

Dieser Softwareentwurf muss in enger Zusammenarbeit zwischen Softwareentwicklern und Kryptografen ablaufen, denn nur dann können potenzielle Fehlerquellen vermieden werden. PRISMACLOUD hat dazu einen eigenen Crypto-Development-Life-Cycle beschrieben[6].

Verständnis der kryptografischen Methoden

Ein unzureichendes Verständnis der kryptografischen Methoden und deren Sicherheitszugewinne verhindert, dass diese Methoden überhaupt von Cloud-Anwendungs- und Softwareentwicklern in Erwägung gezogen werden. Aber auch wenn ein Cloud-Dienst entsprechende Funktionalitäten zur Verfügung stellt: Die Vorteile der Kryptografie müssen dem zahlenden Kunden kommuniziert werden, zumal durch sie zusätzliche Kosten (z.B. höherer Speicherverbrauch, längere Rechenzeit, zusätzliche Kommunikation) verursacht werden.

PRISMACLOUD arbeitet in der interdisziplinären Kommunikation zwischen Anwendungsentwicklern, Nutzern und Kryptografen über sog. Cloud Security Patterns[7]. Patterns beschreiben zunächst typische Anwendungsfälle, also z.B. «Speicherung von Daten in der Cloud, um diese später verschiedenen Dritten zum Zugriff bereitzustellen». Dies geschieht in natürlicher, für die Anwendungsentwickler verständlicher Sprache. Ebenso werden auch Bedrohungen beschrieben (z.B. «Verlust der Vertraulichkeit durch Mitlesen des Anbieters»), um dann konkrete kryptografische Lösungen vorzuschlagen (z.B. «Secret Sharing»). Dies hilft dem Anwendungsentwickler, gezielt nach Cloud-Anbietern zu suchen, die gesuchte Funktionalitäten unterstützen bzw. den Softwareentwicklern entsprechende Bibliotheken in den Workflow einzubinden. Denn erst dann, wenn Endnutzer eine Funktion[8] fordern und Entwickler diese auch korrekt implementieren können, wird die Cloud sicherer werden.

Schlussendlich lässt sich mithilfe der Patterns die gesteigerte Funktionalität besser anpreisen. Denn nur wenn auch für Cloud-Nutzer der Vorteil klar wird, können kryptografisch gesicherte Cloud-Dienste am Markt punkten.

Standardisierung

Die unzureichende Standardisierung führt dazu, dass neuere Verfahren im praktischen Einsatz benachteiligt werden. So kann die Interoperabilität leiden, wenn es zum Beispiel verschiedene Implementierungen desselben Krypto-Algorithmus gibt, diese aber nicht miteinander kompatibel sind. Dann reicht schon die Möglichkeit drohender Inkompatibilitäten aus, um eine Entscheidung gegen einen neueren, passenderen Algorithmus zu fällen.

Der grosse und stark wachsende Cloud-Computing-Markt hat zu einer heterogenen, unüberschaubaren Menge von Standards geführt, während gleichzeitig die Marktführer und des Weiteren Open-Source-Projekte auf proprietäre Defacto-Standards setzen. Die EU selbst hat in ihrer Cloud-Computing-Strategie (2012) die Aktion «Cutting through the Jungle of Standards» als «Key Action 1» definiert. PRISMACLOUD verfolgt hier eine dezidierte Strategie bei der International Organisation for Standardisation (ISO) und bei weiteren Konsortien und Interessens-Gruppierungen, um Sicherheitseigenschaften und Konfigurations-Optionen der entwickelten kryptografischen Konzepte und Methoden in Standards einfliessen zu lassen.

Kryptografische Optimierung

Kryptografische Optimierungen mit geringem Anwendungsnutzen führen nur zu stärkeren Sicherheitseigenschaften, aber nicht zu einer breiteren Anwendbarkeit. Ein Beispiel ist die kryptografische Eigenschaft «Transparenz» für editierbare Signaturen: Sie versteckt autorisierte, nachträgliche Änderungen bei der Signaturprüfung. Dies ist zweifelsohne eine Stärkung der Datenschutzeigenschaften, selbst der Vorgang des

Entfernens von personenbezogenen Daten wird verborgen, nicht nur das Datum selber. Allerdings widerspricht dies den rechtlichen Vorgaben an elektronische Signaturen nach deutschem und europäischem Recht. Damit mindert eine transparente editierbare Signatur sofort den Beweiswert, was sich negativ auf die potenzielle Anwendung auswirkt[9].

Recht

Rechtliche Unklarheiten entstehen durch nur im Detail unterschiedliche Sicherheitseigenschaften. So offerieren editierbare Signaturen nur eine abgeschwächte Form des Integritätsschutzes: Nicht alle nachträglichen Änderungen führen zu einer invaliden Signatur, wie dies bei Standard-Signaturen der Fall ist. Wählt man die kryptografischen Eigenschaften geschickter und verzichtet auf kryptografische Transparenz, dann lassen auch editierbare Signaturen jedwede nachträgliche Änderung erkennen – genau wie das rechtssichere Vorbild[10].

Zusätzlich geben Standards auch Rechtssicherheit. «Non-standard» und nicht einmal «Best-Practices»-Lösungen werden häufig erst dann erwogen, wenn ein Wettbewerbsvorteil winkt.

Fazit

Die Hinderungsgründe für praktisch verwendbare und anwendungsnahe kryptografische Lösungen für die Cloud sind nicht nur vielfältig, sie sind auch interdisziplinär und miteinander verwoben. Es fehlt zuallererst das Bewusstsein der Nutzer, dass es kryptografische Lösungen für die Probleme in der Cloud überhaupt gibt. Es mangelt zurzeit also schlicht auch an der Nachfrage. Daher entwickelt das Horizon-2020-Projekt PRISMACLOUD[11] anwendungsgetrieben kryptografische Methoden, welche in Software und Hardware implementiert werden. Die qualifizierte Integration wird anhand von drei Szenarien aus den Bereichen E-Government, E-Health und Smart-Cities gezeigt werden. PRISMACLOUD zeigt: Benutzbare Kryptografie bedarf einer einfachen und transparenten Integrationsmöglichkeit in existierende Geschäftsprozesse, welche bereits heute in der Cloud stattfinden. ■

Fussnoten

1 EU Horizon 2020 Projekt PRISMACLOUD (No. 644962), Laufzeit: Feb. 2016 – Aug. 2018, www.prismacloud.eu.

2 PRISMACLOUD beschäftigt sich zusätzlich zu Secret Sharing Schemes, Malleable-, Functional- und Group Signature Schemes auch noch mit Remote Data Checking, Attribute-Based Credentials, Private Information Retrieval, Graph Signature Schemes, Format- und Order-Preserving Encryption, Zero-Knowledge Proofs, sowie k-Anonymity. Vgl. auch Lorünser/Slamanig/Länger/Pöhls, 2016.

3 Siehe Shamir, 1979.

4 Siehe (Steinfeld/Bull/Zheng, 2002, und unabhängig auch Johnson/Molnar/Song/Wagner, 2002.

5 Editierbare Signaturen können auch Änderungen erlauben, siehe (Ateniese/Chou/de Medeiros/Tsudik, 2005.

6 Siehe Lorünser/Slamanig/Länger/Pöhls, 2016.

7 Siehe Länger/Pöhls/Ghernaouti, 2016.

8 Sicherheit und Datenschutz sind «Funktionen», welche Nutzer gezielt verlangen sollten.

9 Siehe Geelkerken/Pöhls/Fischer-Hübner, 2014, und Höhne/Pöhls/Samelin, 2012.

10 Johnson/Molnar/Song/Wagner, 2002, Ateniese/Chou/de Medeiros/Tsudik, 2005.

11 EU Horizon 2020 Projekt PRISMACLOUD (No. 644962), Laufzeit: Feb. 2016 – Aug. 2018, www.prismacloud.eu.

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement **digma** (4 Hefte des laufenden Jahrgangs) à **CHF 174.00**
(Versandkosten: Schweiz inklusive)

Name Vorname

Firma

E-Mail

Strasse/Nr.

PLZ Ort

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8001 Zürich
Telefon +41 44 200 29 29
Telefax +41 44 200 29 28
E-Mail: zeitschriften@schulthess.com
Homepage: www.schulthess.com

Schulthess §