ATTRIBUTBASIERTE KRYPTOGRAPHIE FÜR DIE JUSTIZ

Aljoscha Dietrich / Christoph Sorge

Wissenschaftlicher Mitarbeiter
juris-Stiftungsprofessur für Rechtsinformatik an der Universität des Saarlandes und CISPA, 66123 Saarbrücken, DE
aljoscha.dietrich@uni-saarland.de; http://www.legalinf.de

Universitätsprofessor
juris-Stiftungsprofessur für Rechtsinformatik an der Universität des Saarlandes und CISPA, 66123 Saarbrücken, DE
christoph.sorge@uni-saarland.de; http://www.legalinf.de

***Schlagworte:** Vertraulichkeit, Verschlüsselung, attributbasierte Kryptographie, elektronische Akte*

1. Einleitung

Bei der Einführung elektronischer Akten stellt sich für die Justiz als Hauptanforderung die Gewährleistung der Datensicherheit und des Datenschutzes bzw. konkreter der Schutzziele Vertraulichkeit, Integrität und Authentizität. Der – ggf. sogar weltweit mögliche – elektronische Zugriff kann das Gefährdungspotential enorm erhöhen, da dieser nun massenhaft und unter Umständen sogar unbemerkt erfolgen kann. Neben klassischen Zugriffskontrollverfahren wie Zugriffskontrolllisten ist der Königsweg zum Schutz der Vertraulichkeit elektronischer Daten die Verwendung starker Kryptographie.

Etablierte kryptographische Verfahren arbeiten i.d.R. mit Schlüsseln, die an Personen gebunden sind; somit können etwa Probleme entstehen, wenn der exakte Empfänger noch gar nicht bekannt ist oder aufgrund von Urlaub oder Krankheit vertreten wird.

Ein Lösungsansatz liegt in der attributbasierten Kryptographie. Hier werden Daten nicht für eine Person, sondern für definierte Attribute bzw. Rollen verschlüsselt. Bei der Verschlüsselung wird also nicht angegeben, welche Person die Daten entschlüsseln soll, sondern welche Attribute bzw. Merkmale diese haben muss.

Im Folgenden soll dargestellt werden, wie ein exemplarischer Prozess in der Justiz ablaufen könnte, wer beteiligte Akteure sind und wer Zugriff auf die Akten benötigt. Darauf aufbauend soll untersucht werden, welche Lösungen attributbasierte Kryptographie hier bieten kann. Die Einbeziehung attributbasierter Kryptographie in praktische Sicherheitsinfrastrukturen ist bislang noch Forschungsgegenstand, so dass die hier vorgestellten Überlegungen nicht auf eine kurzfristige Umsetzung abzielen, sondern lediglich Ausgangspunkt für weitere Forschungsanstrengungen sein können. Auch gehen wir in diesem Beitrag davon aus, dass Zugriffsrechte stets möglichst restriktiv gewählt werden sollten – dieser Ansatz ist aus Sicht der IT-Sicherheit wünschenswert, was aber nicht garantiert, dass seine Umsetzung gewünscht wird.

2. Beschreibung der Aktenregistrierung in der Justiz

Es soll von folgendem Szenario ausgegangen werden: bei einem ordentlichen Gericht tritt ein verfahrenseinleitender Geschäftsvorfall auf. Dieser und die folgenden Vorgänge sollen verallgemeinert beschrieben werden, so dass sie möglichst in ähnlicher Form auf verschiedenste Gerichte angewandt werden können. Nach einem allgemeinen Überblick gehen wir auf die Geschäftsverteilung und schließlich die beteiligten Akteure ein.

2.1. Vorgang

Die wesentlichen Schritte der Aktenregistrierung sind wie folgt:

1. Eingang eines verfahrenseinleitenden Geschäftsvorfalls bei der Eingangsgeschäftsstelle Die Feststellung der Zuständigkeit erfolgt nach dem Geschäftsverteilungsplan (GVP). Nach § 21e GVG wird der GVP bei jedem Gericht vom Präsidium für ein Geschäftsjahr im Voraus beschlossen. Hierbei muss gewährleistet werden, dass das Gebot des gesetzlichen Richters gemäß Art. 101 Abs. 1 S. 2 GG und § 16 GVG nicht verletzt wird. Einzelne Sachen müssen also auf Grund allgemeiner und vorab festgelegter Merkmale an den berufenen Richter gelangen.[1] Es soll so die Einflussnahme auf die Zuweisung des zuständigen Richters verhindert werden.
2. Weitergabe des Geschäftsvorfalls zu der zuständigen Geschäftsstelle des berufenen Richters und Bildung der Akte Verfahrenseinleitende Geschäftsvorfälle sind grundsätzlich unter einer Nummer nach einer gegebenen Systematik zu registrieren. Schriftstücke, die die gleiche Angelegenheit betreffen, sind zu Akten zu vereinigen[2]. Die Geschäftsstelle hat die Verantwortung über den Verbleib der Akten, da sie diesen nachzuweisen hat und jederzeit feststellen können muss.[3]
3. Weitergabe der Akte an den zuständigen Richter.

2.2. Gestaltungsfreiheit der Geschäftsverteilung

Solange der Bestimmtheitsgrundsatz, welcher aus dem Gebot des gesetzliches Richters folgt, nicht verletzt wird, nach welchem die Kriterien zur Zuweisung so eindeutig und präzise wie möglich sein müssen[4], liegt die Geschäftsverteilung und personelle Zuweisung der Richter im Ermessen des Präsidiums.[5] Mögliche Kriterien zur Verteilung sind beispielsweise

- die Anfangsbuchstaben des Beklagten bzw. Angeklagten,
- die Sachgebiete,
- der räumliche Bereich (Wohnsitz der Parteien)
- Eingangsnummern

Auch ein Mischsystem ist möglich.[6]

2.3. Beteiligte Akteure mit Aktenzugriff

Aus der Geschäftsverteilung kann geschlossen werden, welche Personen üblicherweise Zugriff auf eine Akte zu einem Geschäftsvorfall bei Gericht benötigen:

---

1 Selder, Das Bundesverfassungsgericht und der gesetzliche Richter, 2011, ZRP, S. 165; BVerfG, Verfassungswidrigkeit des Ausschluss des Umgangsrechts eines nichtehelichen Vaters, 2005, NJW, S. 2689.

2 Für das Beispiel des Saarlandes siehe § 3 Abs. 1. S. 1 der Saarländischen Aktenordnung (AktO-Saarland).

3 § 5 Abs. 1 S. 1 AktO-Saarland.

4 Zimmermann, GVG § 21e. In Rauscher, Thomas/Krüger, Wolfgang (Hrsg.), Münchener Kommentar zur ZPO, 4. Auflage, München 2013, Rn. 15.

5 Zimmermann, GVG § 21e. In Rauscher, Thomas/Krüger, Wolfgang (Hrsg.), Münchener Kommentar zur ZPO, 4. Auflage, München 2013, Rn. 11.

6 Zimmermann, GVG § 21e. In Rauscher, Thomas/Krüger, Wolfgang (Hrsg.), Münchener Kommentar zur ZPO, 4. Auflage, München 2013, Rn. 11.

– Zuständiger Richter

– Bei Nichtverfügbarkeit des zuständigen Richters dessen Vertreter gemäß der festgelegten Vertretungskette nach GVP

– Urkundsbeamte der zuständigen Geschäftsstelle

Nach Darstellung der Abläufe vor Gericht soll im Folgenden näher auf die attributbasierte Kryptographie eingegangen werden

3. Attributbasierte Kryptographie

Aktuelle Verschlüsselungsverfahren lassen sich grob in zwei Klassen unterteilen: Bei *symmetrischen* Verfahren wird der gleiche Schlüssel zur Ver- und Entschlüsselung von Daten verwendet. Sollen Daten verschlüsselt übertragen werden, müssen sich die Kommunikationspartner zunächst auf einen gemeinsamen Schlüssel einigen. Bei *asymmetrischen* Verfahren (auch: Public-Key-Verfahren) unterscheiden sich die Schlüssel für die Ver- und Entschlüsselung. Bei den bislang gängigen Umsetzungen hat jeder Nutzer ein Schlüsselpaar mit je einem öffentlichen und einem oder mehreren dazu passenden privaten Schlüsseln. Dieses Schlüsselpaar kann vom jeweiligen Nutzer individuell generiert werden.

Der öffentliche Schlüssel – der dem Namen entsprechend tatsächlich veröffentlicht werden kann – wird verwendet, um Daten zu verschlüsseln, der private Schlüssel, um sie wieder zu entschlüsseln. Will Nutzerin *Alice* dem Nutzer *Bob* eine verschlüsselte Nachricht schicken, benötigt sie also zum Zeitpunkt der Verschlüsselung Bobs öffentlichen Schlüssel.

Auch die Attributbasierte Verschlüsselung[7] (Attribute-Based Encryption, ABE) lässt sich den asymmetrischen Verfahren zuordnen. Im Gegensatz zu vielen etablierten asymmetrischen Verfahren ist es bei attributbasierter Kryptographie allerdings nicht erforderlich, im Vorhinein ein Schlüsselpaar aus einem öffentlichen und einem privaten Schlüssel zu erzeugen. Ob ein Nutzer eine Datei entschlüsseln kann, entscheidet sich stattdessen abhängig davon, ob Attribute (des Nutzers oder der Datei) zu einer vorgegebenen Datenstruktur passen, die die Zugriffsberechtigungen (des Nutzers oder auf die Datei) beschreibt – die sogenannte *Policy*. Sie ähnelt der Policy in klassischen Zugriffskontrollverfahren (wie etwa Zugriffskontrolllisten) – allerdings gibt es keine Instanz, die zum Zeitpunkt des Zugriffs auf die Daten einen Abgleich vornimmt, sondern dieser Abgleich erfolgt implizit beim Versuch, die Daten zu entschlüsseln.

Aus den Eigenschaften der ABE folgt ein wesentlicher Unterschied zu den bislang etablierten asymmetrischen Verfahren. Nutzer können ihre Schlüssel nicht mehr selbst generieren, da ihre Zugriffsberechtigungen davon abhängen. Vielmehr muss diese Aufgabe von einer zentralen Instanz (oder ggf. mehreren kooperierenden Instanzen), dem Schlüsselerzeuger, übernommen werden.

ABE-Verfahren lassen sich – je nachdem, ob die Policy dem Schlüssel oder den verschlüsselten Daten zugeordnet wird – in die beiden Klassen Key-Policy-ABE und Ciphertext-Policy-ABE unterteilen.

[7] Attrapadung, Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More. In Nguyen/Oswald (Hrsg.), Advances in Cryptology – EUROCRYPT 2014, Proceedings, Band 8441 der Reihe Lecture Notes in Computer Science, Springer, Berlin/Heidelberg 2014, S. 557–577.

3.1. KP-ABE

Key-Policy-ABE[8] (KP-ABE) bedeutet, dass Attribute verwendet werden, um die verschlüsselten Daten zu beschreiben – etwa Datum, Ort, Dateityp, Kategorie, Klassifikation des Inhalts oder Autor. Jeder Teilnehmer des Systems erhält einen Schlüssel, der die *Policy* für den Zugriff enthält; der Schlüssel beschreibt also, welche Attribute den Daten zugeordnet sein müssen, damit der Schlüsselinhaber diese entschlüsseln kann. So ließe sich beispielsweise festlegen, dass ein Nutzer alle im Januar 2016 verfassten Dokumente entschlüsseln kann (wenn der Monat der Erstellung eines Textes als Attribut verwendet wird).

Folge dieses Vorgehens ist, dass der Schlüsselerzeuger die Aufgabe hat, über die Zugriffsrechte der Nutzer zu entscheiden, denn die generierten Schlüssel hängen von den Zugriffsrechten ab. Wer Daten verschlüsselt, muss lediglich die zugehörigen Attribute auswählen.

3.2. CP-ABE

Bei Ciphertext-Policy-ABE[9] (CP-ABE) beschreiben die Attribute Eigenschaften oder Rollen der beteiligten Teilnehmer des Verfahrens. Attribute könnten sich beispielsweise auf die Behörde, Abteilung, Region, Funktion, Dienstgrad, Qualifikation, Wohnort usw. der beteiligten Personen beziehen. Die Policy ist den Daten zugeordnet. Der Schlüsselerzeuger hat hier also die Aufgabe, diese Attribute durch Ausstellung eines entsprechenden Schlüssels zu bestätigen. Wer Daten verschlüsselt, muss beschreiben, welche Attribute oder Attributkombinationen zum Zugriff auf die Daten berechtigen.

3.3. Policy

Mit der Policy wird die Berechtigungsstruktur definiert und beschrieben, diese kann als boolesche Formel bzw. Baum (bei ABE in der Regel mit UND- oder ODER-Operatoren) dargestellt werden. Aus der Policy kann also abgeleitet werden, wer Zugriff auf die Daten erhält. Abbildungen 1 und 2 zeigen Beispiele solcher Policies. In Abbildung 1 sind die Attribute «Mietrecht» und «Saarbrücken» mit dem «Und»-Symbol verknüpft. Gehen wir von einem KP-ABE-Verfahren aus, wird Zugriff also den Teilnehmern gewährt, deren Schlüssel gleichzeitig die beiden genannten Attribute enthalten. Abbildung 2 zeigt eine mögliche Policy bei CP-ABE-Verfahren mit Oder-Verknüpfung, bei der Richter Meyer, die für ihn zuständige Geschäftsstelle oder Mitglieder seiner Vertretungskette zugreifen dürfen.

[8] Rouselakis/Waters, Practical constructions and new proof methods for large universe attribute-based encryption, ACM Conference on Computer and Communications Security 2013, S. 463–474.

[9] Bethencourt/Sahait/Waters, Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, Proceedings, Band 2848, IEEE, Berkley 2007, S. 321–334; Rouselakis/Waters, Practical constructions and new proof methods for large universe attribute-based encryption, ACM Conference on Computer and Communications Security 2013, S. 463–474.

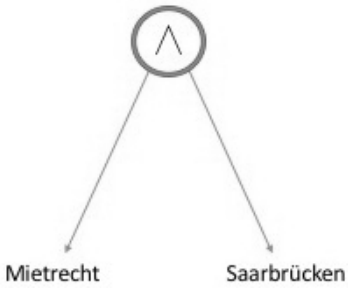

Abbildung 1: Policy für Mietrecht UND Saarbrücken (KP-ABE)

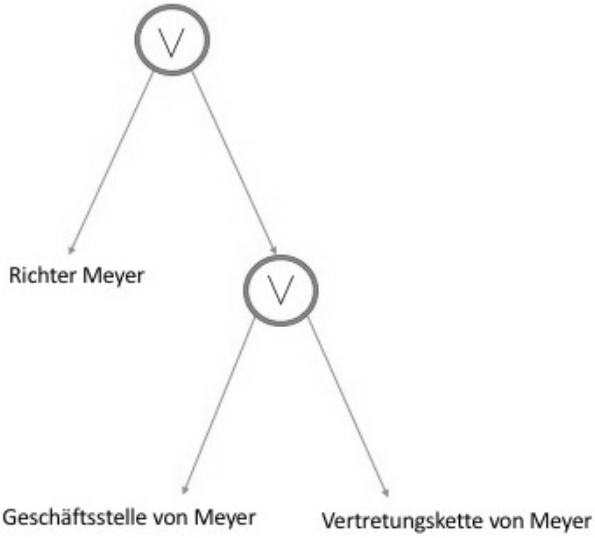

Abbildung 2: Policy für Richter Meyer, seine Geschäftsstelle oder seine Vertretungskette (CP-ABE)

4. Einsatzmöglichkeiten attributbasierter Kryptographie in der Justiz

In diesem Abschnitt soll untersucht werden, welche Lösungen attributbasierte Kryptographie für die Justiz bieten kann. Im Zuge der Digitalisierung der Justiz wird es absehbar auch zu der Digitalisierung der Gerichtsakten, der sogenannten E-Akte, kommen. Für diese E-Akten dürfte ein hoher bis sehr hoher Schutzbedarf gelten, insbesondere unter den Gesichtspunkten der Vertraulichkeit und Integrität. Attributbasierte Kryptographie kann für das Schutzziel Vertraulichkeit eingesetzt werden, d.h. sie dient dem Schutz vor unbefugter Preisgabe von Informationen, indem nur der berechtigte Personenkreis die Daten entschlüsseln kann. Um die Vorteile zu verstehen, vergleichen wir ABE-Verfahren mit dem heute üblichen Vorgehen.

Bei der Verwendung traditioneller Public-Key-Verfahren, bei denen jeder Beteiligte ein eigenes Schlüsselpaar hat, bietet sich für den Schutz der Vertraulichkeit einer Akte folgender Ablauf an. Das Public-Key-Verfahren wird hierbei mit einem symmetrischen Kryptographiesystem kombiniert[10]:

1. Bei der Anlage einer Akte wird diese unter Verwendung eines symmetrischen Verschlüsselungsverfahrens mit einem zufällig gewählten Schlüssel verschlüsselt. Bei späteren Ergänzungen der Akte wird dieser Vorgang wiederholt.
2. Der Schlüssel aus Schritt 1 wird mittels des Public-Key-Verfahrens – jeweils einzeln – mit den öffentlichen Schlüsseln aller Zugriffsberechtigten verschlüsselt. Das Ergebnis der Operation wird der elektronischen Akte hinzugefügt.
3. Um die Akte zu lesen, entschlüsselt der Zugriffsberechtigte zunächst mit seinem privaten Schlüssel den Schlüssel aus Schritt 1 und mit diesem die Akte.
4. Soll später eine weitere Person die Zugriffsberechtigung erhalten, muss ebenfalls ein Zugriffsberechtigter – denkbar wäre hier etwa die Geschäftsstelle des Gerichts – den Schlüssel aus Schritt 1 entschlüsseln und mit dem öffentlichen Schlüssel des neu Zugriffsberechtigten neu verschlüsseln.

Der Vorteil attributbasierter Verfahren liegt nun darin, dass der vierte Schritt in der Regel entfallen kann: Zum Zeitpunkt der Verschlüsselung muss lediglich feststehen, welche Attribute zum Zugriff berechtigen. Der Personenkreis, der sich daraus ergibt, kann sich aber im Nachhinein ändern. Daten müssen also insgesamt nur einmal verschlüsselt werden und können von allen Teilnehmern entschlüsselt werden, welche einen privaten Schlüssel mit den entsprechenden Attributen bzw. der entsprechenden Policy erhalten.

Auf diesem Weg können auch Vertreter, Nachfolger u.ä. erfasst werden. Im Vertretungsfall könnte der vertretende Richter ohne Mitwirkung der Geschäftsstelle oder einer sonstigen Instanz direkt auf die Akte zugreifen. Dieser Vorteil ist beiden Verfahrensklassen (KP-ABE und CP-ABE) gemein, doch unterscheidet sich die konkrete Umsetzung.

4.1. Schlüsselgenerierung

Die Schlüsselerzeugung kann bei einer attributbasierten Verschlüsselung nur von einer zentralen Instanz durchgeführt werden. Da diese Instanz Zugriff auf alle privaten Schlüssel und daher potentiell auch auf alle verschlüsselten Dokumente erhält, muss sie ein sehr großes Vertrauen genießen. Es würde sich daher anbieten, die Schlüsselgenerierung intern bei dem zuständigen Gericht zu belassen. Würde beispielsweise die Verteilgeschäftsstelle die Schlüsselgenerierung übernehmen, wäre zugleich sichergestellt, dass diese jederzeit Zugriff auf die Akten hätte. Der potentielle Zugriff könnte hier also u.a. auch einen Vorteil darstellen. Denkbar wäre jedoch auch eine zentrale Stelle, beispielsweise auf Landesebene, welche die Schlüssel für alle zuständigen Gerichte generiert. Da die Effizienz der attributbasierten Verschlüsselung jedoch stark von der Anzahl der vorgesehenen Attribute abhängt, bietet es sich in jedem Fall an, für jedes Gericht eine eigene Menge an Schlüsseln zu erzeugen.

4.2. Wahl des Verfahrens der attributbasierten Kryptographie

Grundsätzlich können bei attributbasierter Kryptographie in der Justiz beide beschriebenen Verfahrensklassen (KP-ABE und CP-ABE) zur Anwendung kommen. Sie unterscheiden sich aber darin, wie ein GVP modelliert werden kann.

[10] Sorge/Gruschka/Lo Iacono, Sicherheit in Kommunikationsnetzen, Oldenbourg, München 2013, S. 50 f.

4.2.1. Attribute der Akte (KP-ABE)

Im Fall der KP-ABE muss der Schlüsselerzeuger über die Policy entscheiden, die dem Nutzerschlüssel zugeordnet ist, während bei der Anlage einer Akte deren Attribute festzuhalten sind. Ein Attribut könnte beispielsweise lauten «Mietrechtsfall» und eine Policy könnte beinhalten «darf auf Mietrechtsfälle und auf Wohnungseigentumsrechtsfälle zugreifen». Ein GVP, der Fälle aufgrund von Kriterien zuteilt, die sich als Attribut einer Akte ausdrücken lassen, kann intuitiv auf KP-ABE-Verfahren abgebildet werden. Neben dem Sachgebiet könnten hier etwa geographische Kriterien oder Personennamen herangezogen werden. Auch komplexe GVP, bei denen mehrere Kriterien kombiniert werden und ein Richter etwa die Zuständigkeit für Mietrechtsfälle im Stadtgebiet Saarbrücken hat, bei denen der Nachname des Beklagten im Bereich «A bis K» liegt, können abgebildet werden. Mit der Verabschiedung eines neuen GVP wäre die Erzeugung neuer Schlüssel mit den zugehörigen Policies verbunden.

4.2.2. Attribute des Teilnehmers (Richters) (CP-ABE)

Im Fall der CP-ABE muss der Schlüsselerzeuger die Attribute des jeweiligen Nutzers festlegen, während bei der Anlage einer Akte die Policy festzulegen ist, welche Attribute bzw. Attributkombinationen zum Zugriff berechtigen. Ein Attribut könnte hier beispielsweise lauten «ist zuständig für Mietrechtsfälle» und eine Policy könnte beinhalten «Zugriff ist erlaubt für Personen, die für Mietrechtsfälle zuständig sind». Wie das Beispiel zeigt, lassen sich prinzipiell Zugriffsrechte sehr ähnlich zu KP-ABE-Verfahren abbilden. Die Komplexität der Modellierung unterscheidet sich jedoch: Das obige Beispiel eines Richters mit Zuständigkeit für Mietrechtsfälle im Stadtgebiet Saarbrücken, bei denen der Nachname des Beklagten im Bereich «A bis K» liegt, lässt sich nicht einfach dadurch abbilden, dass der Richter Attribute bezogen auf «Mietrecht», «Stadtgebiet Saarbrücken» und «A bis K» erhält. Der Policy würde hier die Grundlage fehlen, um den Zusammenhang der Attribute zu berücksichtigen; es wären also zusammengesetzte Attribute (Zuständigkeit für «Mietrechtsfälle aus dem Stadtgebiet Saarbrücken mit Anfangsbuchstaben A bis K» als *ein* Attribut) nötig. Solche Zusammensetzungen wären allerdings vermutlich eindeutig für einen Richter, so dass der konzeptionelle Vorteil von ABE-Verfahren – der ja gerade in der Abkehr von der Verschlüsselung für einzelne Personen besteht – erst im nächsten Schritt deutlich wird. Da dieser Vorteil für KP-ABE-Verfahren in ähnlicher Weise gilt, diskutieren wir ihn im nächsten Abschnitt separat.

4.2.3. Gemeinsame Eigenschaften

Beiden Verfahrensklassen gemein ist die Möglichkeit, Aspekte der Gerichtsorganisation zu modellieren: Zu den Zugriffsrechten eines Richters gehören stets entsprechende Rechte seiner Geschäftsstelle sowie seiner Vertreter. Die Modellierung erfolgt in gleicher Weise wie für die Zugriffsrechte des Richters selbst. Hier spielen ABE-Verfahren ihre Stärken besonders aus, denn während die Zuständigkeit eines Richters während der Geltungsdauer eines GVP festgelegt ist, können Geschäftsstellenzuständigkeiten sich ändern. Auch ohne Änderungen an der Verschlüsselung der Akte selbst vorzunehmen, kann etwa durch Generierung neuer Schlüssel neu hinzukommenden Mitarbeitern Zugriff gewährt werden.

4.3. Änderungen des GVP

Ein gänzlich neuer GVP mit einer neuen Verteilungssystematik oder neuer Attributmenge dürfte eher die Ausnahme als die Regel darstellen – schon allein, um eingeübte Geschäftsabläufe nicht jedes Jahr völlig verwerfen zu müssen. Trifft nun doch einer der beiden Fälle ein, müssen neue Schlüssel erstellt werden. Hier kann davon ausgegangen werden, dass diese nicht mit den bereits erstellten Altdokumenten kompatibel sind. Um den weiteren Zugriff zu ermöglichen, müssen entweder die alten Schlüssel weiter aufgehoben werden, oder die Altdokumente erneut verschlüsselt werden.

Wird ein bestehendes System behalten, kann es dennoch zu Verschiebungen von Zuständigkeiten kommen. So müssen beispielsweise einzelne Personen aufgrund neuer Zuständigkeiten auch neue Schlüssel erhalten, die jedoch nur für die neuen Fälle und nicht alte Akten gelten. Dies könnte durch zeitlich terminierte Attribute behoben werden, wie «Mietsache 2016». Um das bestmögliche Vorgehen zum Umgang mit dieser Dynamik herauszuarbeiten, besteht aber noch weiterer Forschungsbedarf.

4.4. Außerplanmäßiger und externer Zugriff

Außerplanmäßige oder seltene Fälle, die Zugriffsmöglichkeiten von weiteren Personen erfordern, würden bei der Modellierung in einem Verfahren der attributbasierten Kryptographie unverhältnismäßigen Aufwand erfordern. So könnte beispielsweise im Falle einer dienstlichen Beurteilung eines Richters die Einsicht in von ihm bearbeitete Akten nötig werden. Sollten solche Fälle auftreten, können sie auch gut von der Geschäftsstelle bearbeitet werden. Die entsprechenden Dokumente könnten dann u.a. mit klassischen kryptographischen Verfahren den außerplanmäßig Zugriff nehmenden Personen zur Verfügung gestellt werden.

Gleiches gilt allgemein für den Zugriff Gerichtsexterner, beispielsweise zur Aktensicht. Der Zugriff kann entweder durch gesicherte Terminals im Gericht angeboten oder auch hier durch die zuständige Geschäftsstelle mit klassischen Verschlüsselungsverfahren ermöglicht werden.

5. Fazit

Attributbasierte Kryptographie kann bei dem zukünftigen Einsatz der E-Akte innerhalb von Gerichten einige Vorteile ausspielen. So müssen die Akten nicht mehr für jede berechtigte Person verschlüsselt werden und je nach Verfahren müssen die Personen bei der Verschlüsselung auch noch gar nicht bekannt sein. Des Weiteren lassen sich Vertretungsfälle sehr leicht abbilden. Von Nachteil könnte sein, dass vor der Schlüsselgenerierung die möglichen Attribute sehr genau erfasst werden müssen, da sie im Nachhinein nicht mehr verändert werden können. Auch darf die Attributmenge nicht zu groß sein, da das Verfahren andernfalls ineffizient wird.

Beim Einsatz der ABE in der Justiz dürften die Vorteile jedoch überwiegen und den Zugriff auf verschlüsselte Daten vereinfachen und effizienter gestalten. ABE kann jedoch nur zusätzlich zu etablierten Verfahren eingesetzt werden, welche insbesondere bei außerplanmäßigen und externen Zugriffen weiterhin nötig sein werden.

6. Danksagung

Wir danken Herrn Gennadij Liske für wertvolle Anregungen.

7. Literatur

Attrapadung, Nuttapong, Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More. In Nguyen, Phong Q./Oswald, Elisabeth (Hrsg.), Advances in Cryptology – EUROCRYPT 2014, Proceedings, Band 8441 der Reihe Lecture Notes in Computer Science, Springer, Berlin/Heidelberg 2014, S. 557–577.

Bethencourt, John/Sahai, Amit/Waters, Brent, Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, Proceedings, Band 2848, IEEE, Berkley 2007, S. 321–334.

BVerfG, Verfassungswidrigkeit des Ausschluss des Umgangsrechts eines nichtehelichen Vaters, 2005, NJW, S. 2689.

Rouselakis, Yannis/Waters, Brent, Practical constructions and new proof methods for large universe attribute-based encryption, ACM Conference on Computer and Communications Security 2013, S. 463–474.

Selder, Johannes, Das Bundesverfassungsgericht und der gesetzliche Richter, 2011, ZRP, S. 164–166.

Sorge, Christoph/Gruschka, Nils/Lo Iacono, Luigi, Sicherheit in Kommunikationsnetzen, Oldenbourg, München 2013.

Zimmermann, Walter, GVG § 21e. In Rauscher, Thomas/Krüger, Wolfgang (Hrsg.), Münchener Kommentar zur ZPO, 4. Auflage, München 2013, Rn. 11–15.