Identitätsbasierte Kryptografie - Hindernisse auf dem Weg von der Theorie in die Praxis

Björn Fay[1], Jörn Schweisgut[1], Christian Tobias[2]

[1] Justus-Liebig-Universität Gießen
E-Mail: crypto@math.uni-giessen.de
[2] Utimaco Safeware AG Oberursel
E-Mail: Christian.Tobias@utimaco.de

Abstract: Identitätsbasierte Kryptografie wird häufig als Lösung angeführt, um den komplexen und aufwändigen Aufbau und Betrieb einer Public Key Infrastruktur (PKI) zu vermeiden. Als öffentliche Schlüssel eines Benutzers dienen bei identitätsbasierter Kryptografie persönliche (aber öffentlich zugängliche) Daten dieses Benutzers, wie beispielsweise seine E-Mail-Adresse oder seine Telefonnummer. Eine überprüfbare Zuordnung einer Identität zu einem öffentlichen Schlüssel, wie sie eine PKI leistet, scheint also auf den ersten Blick nicht nötig. Der vorliegende Artikel vergleicht die Komponenten, die zum Betrieb einer PKI sowie einer Infrastruktur für identitätsbasierte Kryptografie nötig sind. Es wird sich zeigen, dass der Betrieb einer PKI bei einem vergleichbaren Sicherheitsniveau nur unwesentlich aufwändiger ist und der Einsatz identitätsbasierter Kryptografie neue Herausforderungen mit sich bringt und nur in sehr speziellen Strukturen sinnvoll erscheint.

Key words: Identitätsbasierte Verschlüsselung, Identitätsbasierte Kryptografie, Key Escrow, Rückruf, Public-Key-Infrastruktur (PKI).

1 Einleitung

Bei der „identitätsbasierten“ Verschlüsselung (identity-based encryption - IBE) ist der öffentliche Schlüssel eines Nutzers eine eindeutig zu ihm gehörende, öffentlich zugängliche Information, die mit seiner Identität verknüpft ist, z.B. die E-Mail-Adresse. Da damit eine Zuordnung von Identitäten zu öffentlichen Schlüsseln automatisch gegeben ist, entfällt die Notwendigkeit der Zertifizierung öffentlicher Schlüssel und, das System kommt ohne eine Zertifizierungsstelle (certification authority - CA) und die damit verbundene Public-Key-Infrastruktur (PKI) aus. In diesem System gibt es eine vertrauenswürdige dritte Instanz (private key generator - PKG), die mittels ihres geheimen Schlüssels, der die Rolle eines Generalschlüssels im System hat, und dem öffentlichen Schlüssel des Benutzers dessen geheimen Schlüssel berechnet. Außerdem publiziert der PKG noch eine zu seinem geheimen Schlüssel gehörende öffentliche Information.

Der Hauptvorteil von identitätsbasierter Verschlüsselung mit festem Benutzerkreis ist, dass der geheime Schlüssel des PKG nach Ausstellung aller geheimen Schlüssel der Nutzer vernichtet werden kann. Hierbei wird vorausgesetzt, dass die ausgegebenen Schlüssel unbegrenzte Lebensdauer haben. In diesem Basissystem gibt es keine Möglichkeit zur Sperrung von Schlüsseln.

Das ursprüngliche System identitätsbasierter Kryptografie, das 1984 von Adi Shamir [Sha85] veröffentlicht wurde, war nur zur Erstellung digitaler Signaturen gedacht. Um in diesem System eine Nachricht digital zu signieren, wird wie gewöhnlich der geheime Schlüssel verwendet. Zur Verifikation wird aber anders als bei der Public-Key Kryptografie nur die identitätsbasierte öffentliche Information und die öffentliche Information des PKG benötigt.

Im Jahr 2001 wurde die identitätsbasierte Kryptografie durch Dan Boneh und Matthew K. Franklin [BF01] durch Verwendung von Weil-Paarungen auch zur Ver- und Entschlüsselung eingesetzt. Da der geheime Schlüssel eines jeden Teilnehmers bei Kenntnis des geheimen Schlüssels des PKG berechnet werden kann, beinhaltet das System automatisch Key Escrow. Beim Key Escrow gibt es eine zentrale Stelle, die im Bedarfsfall, z.B. nach richterlicher Genehmigung, verschlüsselte Nachrichten der Teilnehmer entschlüsseln kann.

Da Key Escrow nicht immer wünschenswert ist, kann man die identitätsbasierte Verschlüsselung mit der gewöhnlichen Public-Key-Verschlüsselung kombinieren, die auf Zertifikaten basiert. Bei der sogenannten zertifikatsbasierten Verschlüsselung verwendet eine zertifikatsausstellende Instanz (CA) identitätsbasierte Kryptografie bei der Erstellung der Zertifikate.

Eine andere Möglichkeit Key Escrow zu vermeiden bzw. zu erschweren ist, dass man den PKG auf mehrere Instanzen verteilt, so dass nur gemeinschaftlich der geheime Schlüssel eines Benutzers berechnet werden kann.

2 Motivation und Zielsetzung des Artikels

Bis vor einigen Jahren wurde PKI noch als Killer-Applikation für die Absicherung von Computer-Netzwerken gesehen. Es gab zahlreiche Vorhaben, firmenweite oder noch größere Infrastrukturen aufzubauen. Die meisten dieser Vorhaben wurden jedoch nicht im geplanten Umfang umgesetzt. Sie wurden entweder abgebrochen oder zunächst mit einem reduzierten Funktionsumfang oder für einen kleineren Teilnehmerkreis realisiert. Dieses Scheitern liegt daran, dass die Komplexität des Aufbaus einer PKI oft unterschätzt wurde. Identitätsbasierte Kryptografie (identity-based cryptography - IBC) wird häufig als Lösung angeführt, um die Komplexität einer Schlüsselinfrastruktur zu reduzieren.
Bei IBC lassen sich öffentliche Schlüssel direkt aus öffentlichen persönlichen Daten ihrer Besitzer herleiten. Deshalb ist eine Zertifizierung der öffentlichen Schlüssel nicht mehr nötig. Im Folgenden werden wir PKI und IBC gegenüberstellen und sie insbesondere hinsichtlich ihres Implementierungsaufwandes untersuchen. Es wird

sich zeigen, dass zur Erreichung eines vergleichbaren Sicherheitsniveaus die Bausteine, deren Absicherung bei einer PKI einen großen Teil des Aufwandes ausmacht, in ähnlicher Form auch bei IBC vorhanden sein müssen. Wir werden sehen, dass die Einführung einer IBC Infrastruktur nur in sehr speziellen Umgebungen einen Sinn macht.

3 Definitionen

Ein identitätsbasiertes Verschlüsselungsschema besteht aus den folgenden Bausteinen:

Setup: Der PKG (private key generator) ist eine vertrauenswürdige dritte Partei. Sie erstellt ihr Schlüsselpaar, was im Folgenden mit SK_{PKG} und PK_{PKG} bezeichnet wird. Dieses Schlüsselpaar sind Systemparameter, die auf eine lange Laufzeit ausgelegt sind. Der öffentliche Schlüssel PK_{PKG} ist allgemein zugänglich.

Ableitung des geheimen Schlüssels: Der Empfänger der Nachrichten, Bob, authentifiziert sich gegenüber dem PKG. Dieser berechnet mit dem öffentlich zugänglichen Teil von Bobs Identität ID_{Bob} und seinem eigenen geheimen Schlüssel SK_{PKG} den geheimen Schlüssel $sk_{ID_{Bob}}$ von Bob. Der Schlüssel wird über einen sicheren Kanal an Bob übertragen.

Verschlüsselung: Die Absenderin, Alice, verwendet den öffentlichen Schlüssel PK_{PKG} des PKG sowie Bobs öffentlich zugänglichen Teil seiner Identität ID_{Bob} als dessen öffentlichen Schlüssel und verschlüsselt damit die Nachricht für Bob.

Entschlüsselung: Bob kann, nachdem er den Geheimtext von Alice erhalten hat, diesen mit Hilfe des öffentlichen Schlüssels PK_{PKG} des PKG sowie seines geheimen Schlüssels $sk_{ID_{Bob}}$ entschlüsseln.

Das Schlüsselpaar (PK_{PKG}, SK_{PKG}) des PKG ist dabei kein Schlüsselpaar im klassischen Sinne. Der öffentliche Anteil PK_{PKG} besteht aus öffentlichen Parametern, die alle Teilnehmer des Systems benutzen müssen. Beispiele für solche Parameter sind die benutzte mathematische Gruppe, der Nachrichten- und Geheimtextraum sowie eventuell benutzte Hashfunktionen. Der geheime Schlüssel SK_{PKG} ist eine Trapdoor-Information, die es dem PKG ermöglicht, die geheimen Benutzerschlüssel aus den jeweiligen IDs zu berechnen.

Entsprechend kann man ein identitätsbasiertes Signaturschema betrachten, das aus den folgenden Komponenten besteht:

Setup: Wie bei der identitätsbasierten Verschlüsselung erstellt der PKG ein Schlüsselpaar (SK_{PKG}, PK_{PKG}).

Ableitung des geheimen Schlüssels: Die Signierende, Alice, authentifiziert sich gegenüber dem PKG, welcher ähnlich wie bei der Verschlüsselung mittels ID_{Alice} und SK_{PKG} einen geheimen Signaturschlüssel $sk_{ID_{Alice}}$ von Alice berechnet. Der Schlüssel wird über einen sicheren Kanal an Alice übertragen.

Signatur: Die Signiererin, Alice, verwendet den öffentlichen Schlüssel PK_{PKG} des PKG sowie ihren geheimen Schlüssel $sk_{ID_{Alice}}$ zum Signieren der Nachricht.

Verifikation: Bob kann, nachdem er die Signatur von Alice erhalten hat, diese mit Hilfe der öffentlich zugänglichen Information aus Alice' Identität ID_{Alice} und des öffentlichen Schlüssels PK_{PGK} des PKG verifizieren.

4 Frühere Arbeiten

Im Jahr 1984 veröffentlichte Adi Shamir eine Arbeit [Sha85] über identitätsbasierte Kryptografie, die eigentlich ein identitätsbasiertes Signaturschema auf RSA, aber kein Verschlüsselungsschema beinhaltete. Das war lange Zeit ein offenes Problem, bis es 2001 unabhängig durch Boneh und Franklin [BF01] und Cocks [Coc01] gelöst wurde.

Das System wurde in zahlreichen Arbeiten erweitert. Dabei ist das System von Horwitz und Lynn [HL02] zu nennen, das identitätsbasierte Verschlüsselung in hierarchischen PKGs untersucht. Baek und Zheng stellten in [BZ04] den Zusammenhang zwischen identitätsbasierte Verschlüsselung und Schwellenschemata her, indem sie den geheimen Schlüssel aufteilten, der zu einer Identität gehört. Bei der fuzzy-ID-basierten Verschlüsselung von Sahai und Waters [SW04] sind sogar Digitalfotos als öffentliche Information möglich.

Aber auch auf dem Gebiet der identitätsbasierten Signaturschemata sind noch einige Verfahren, wie z.B. [Hes02] und [ZK02] zu nennen. Im identitätsbasierten Chamäleon-Signaturschema [AdM04] von Ateniese und Medeiros werden nichtübertragbare Signaturen erstellt, d.h. nur der designierte Verifizierer ist in der Lage, die Gültigkeit einer Signatur zu überprüfen.

Das System von Cha und Cheon [CC03] ist vergleichbar mit dem Verschlüsselungsschema von Boneh und Franklin, so dass die Kombination beider Verfahren als ein vollständiges identitätsbasiertes Public-Key-Kryptosystem angesehen werden kann, mit dem man sowohl signieren als auch verschlüsseln kann. Weitere Systeme mit Signatur und Verschlüsselung sind z.B. [Boy03], [ML02] und [LQ03].

4.1 Varianten ohne Key Escrow

Wie bereits erwähnt enthält das Basissystem von identitätsbasierten Kryptoverfahren immer auch ein inhärentes Key Escrow. Im folgenden Abschnitt werden wir drei Varianten beschreiben, die dieses Problem teilweise lösen.

4.1.1 Certificate-Based Encryption

Die Idee bei der Certificate-Based Encryption ist, dass man zusätzlich zu der IBE noch eine asymmetrische Verschlüsselung (public-key encryption - PKE) benutzt. Der Benutzer bekommt von dem PKG der IBE einen geheimen Schlüssel und erzeugt aber gleichzeitig auch noch ein Schlüsselpaar für eine PKE, dessen geheimen Schlüssel nur der Benutzer kennt. Die Verschlüsselung wird dann sowohl mit der IBE als auch mit der PKE durchgeführt, so dass man zum Entschlüsseln beide geheimen Schlüssel benötigt. Dem PKG fehlt also der geheime Schlüssel des Benutzers (für die PKE) zum endgültigen Entschlüsseln der Nachrichten und ein Benutzer ohne gültigen geheimen Schlüssel für die IBE (den er von dem PKG erhält) kann ebenfalls nicht entschlüsseln. Der öffentliche Schlüssel der PKE muss also nicht zertifiziert bzw. überprüft werden, wie dies bei einer normalen PKI der Fall ist und die Gefahr des Schlüsselmissbrauchs durch den PKG ist ebenfalls gebannt.

Genauere Angaben hierzu finden sich in [Gen03]. Dort wird auch beschrieben, wie sich das Rückrufproblem bzw. das sich durch dessen Lösung entstehende Performanceproblem lösen lässt.

4.1.2 Certificateless Cryptography

Eine ähnliche Idee wie in [Gen03] wird in [ARP03] verfolgt. Auch hier wird das Schlüsselpaar zum Teil von dem PKG und zum Teil vom Benutzer generiert, so dass der PKG nicht alleine den geheimen Schlüssel des Benutzers berechnen kann. Allerdings kann der Benutzer bereits einen öffentlichen Schlüssel berechnen ohne die „geheime Hälfte“ des PKG zu kennen. Der Unterschied zum System von Gentry [Gen03] liegt vor allem im Sicherheitsmodell, worauf in [ARP03] näher eingegangen wird.

In [CC05] wird eine verbesserte Version vorgestellt, wobei noch einmal ein Überblick mit Definitionen für das neue Modell angegeben wird.

4.1.3 Verteilte PKG

Bei dem in [LBD+04] beschriebenen Verfahren (es wird auch noch ein kleiner Überblick über andere Verfahren gegeben, die das Key Escrow Problem lösen) handelt es sich um eine aufgeteilte Variante eines IBC. Der PKG wird aufgeteilt in ein KGC (key generation center) und mehrere KPAs (key privacy authorities), wobei das KGC für die Authentifikation zuständig ist, also Aufgaben der Registration Authority (RA) in einer PKI übernimmt. Die KPAs sind für die Geheimhaltung des privaten Schlüssels des Benutzers zuständig. Dazu werden sowohl Blendungen als auch Geheimnisteilungsverfahren benutzt.

Diese Trennung der Zuständigkeiten führt aber leider auch zu einer Schwachstelle in dem Verfahren, die in [CJZ05] aufgezeigt wird. Ein unehrliches KGC kann nämlich den KPAs eine falsche Identität vorspiegeln und dadurch an den geheimen Schlüssel des Benutzers gelangen, womit das Problem des Key Escrow leider nicht gelöst wird.

Es werden aber in [BF01] und [CHSS02] weitere Möglichkeiten vorgestellt, wie man den PKG auf mehrere Instanzen aufteilen kann, so dass alle beteiligten Instanzen mitarbeiten müssen, um den geheimen Schlüssel eines Benutzers berechnen zu können.

5 Praktische Anforderungen an Schlüsselinfrastrukturen

Registrierung, Schlüsselerzeugung und Schlüsselausgabe sowie das Bereitstellen von Informationen zum Gültigkeitsstatus von Zertifikaten sind Aufgaben, die in einer PKI typischerweise von einer CA (eventuell mit Unterstützung weiterer RAs) vorgenommen werden und die den größten Teils des Aufwandes und Schutzbedarfs einer CA ausmachen. Sind die Schlüssel ausgegeben und zertifiziert, so muss die CA mittels Widerrufslisten oder Online-Abfrage ständig aktuelle Informationen über gesperrte Zertifikate zur Verfügung stellen. Wir werden in diesem Abschnitt diese typischen CA-Aufgaben in einer PKI daraufhin untersuchen, ob sie auch in einer IBC Infrastruktur gebraucht werden und wie sie eventuell gelöst werden müssen.

5.1 Registrierung und Schlüsselausgabe

Sowohl in einer PKI als auch bei IBC müssen sich neue Benutzer zunächst zweifelsfrei gegenüber einer vertrauenswürdigen Instanz identifizieren. Das kann in beiden Fällen persönlich in einer RA oder bei weniger sicherheitskritischen Anwendungen über das Netz erfolgen[1]. Eine unzureichende Identifizierung führt in beiden Fällen zu vielfältigen Missbrauchsmöglichkeiten. Im Falle einer PKI können Benutzer eigene Schlüssel unter einem fremden Namen zertifizieren lassen. Im Falle einer IBC könnte jemand sich den geheimen Schlüssel für eine fremde E-Mail-Adresse aushändigen lassen. Während es bei einer PKI möglich ist, öffentliche Schlüssel selbst erzeugter Schlüsselpaare zertifizieren zu lassen, so wird bei IBC der geheime Benutzerschlüssel immer von der vertrauenswürdigen Stelle erzeugt[2]. Die Übergabe des geheimen Schlüssels an den Benutzer hat in beiden Fällen persönlich oder über einen gesicherten Kanal zu erfolgen.
Bei Registrierung und Schlüsselübergabe gibt es also allenfalls minimale Unterschiede.

[1] In der Praxis wird dabei lediglich geprüft, ob eine korrekte E-Mail-Adresse angegeben wurde und ob der Antragsteller Zugriff auf diesen E-Mail-Account hat. Dazu werden die zum Abholen des ausgestellten Zertifikats nötigen Credentials an die angegebene E-Mail-Adresse gesendet.

[2] Für die Sicherheit des Benutzers ist es von elementarer Bedeutung, dass sein Schlüsselpaar sachkundig in einer gesicherten Umgebung erzeugt wird. In den meisten Fällen dürfte der Sicherheitsstandard der CA deutlich über dem des Systems liegen, auf dem ein Benutzer seine Schlüsselpaare selbst erzeugt. Von einer Erzeugung beim Benutzer ist deshalb in den meisten Fällen abzuraten.

5.2 Schlüsselwechsel und Schlüsselsperrung

Regelmäßige Schlüsselwechsel werden in PKIs durch eine beschränkte Gültigkeitsdauer der Zertifikate erzwungen. Durch Sperrung eines Zertifikats und anschließende Zertifizierung eines neuen Schlüssels, kann ein Schlüsselwechsel ferner in Ausnahmesituationen (etwa bei Kompromittierung eines Schlüssels) vorgenommen werden. Die Sperrung eines Schlüssels erfolgt bei PKI meist durch Aufzählung der nicht mehr gültigen Schlüssel in so genannten Sperrlisten. Es ist ferner möglich vor der Benutzung eines bestimmten Schlüssels, dessen Status durch eine Online-Anfrage abzufragen. In beiden Fällen muss sichergestellt sein, dass die entsprechende Auskunft authentisch ist. Dies wird in der Regel durch eine digitale Signatur der vertrauenswürdigen Instanz erreicht. Das Problem der Schlüsselsperrung ist bei PKI gelöst. Da Informationen über gesperrte Zertifikate ständig verfügbar sein müssen, ist dies mit hohen Betriebskosten verbunden. Das Problem des Schlüsselwechsels ist hingegen bei IBE derzeit ungelöst. Es ist eines der meistdiskutierten Probleme im Umfeld von IBE. Als Teillösung kann man auch bei IBE die Schlüssel jeweils mit einer Gültigkeitsdauer versehen. Z.B. kann man als öffentlichen Schlüssel eine Kombination der E-Mail-Adresse (oder eines anderen öffentlichen Wertes) und eines Gültigkeitszeitraums benutzen, wobei man sich auf einen Standard einigen muss, damit der Sender jeweils weiß, wie der aktuelle Gültigkeitszeitraum aussieht.

6 Vergleich von IBE mit PKI-basierter Kryptografie

Als erstes Resultat halten wir fest, dass die Aufwände für Registrierung und Schlüsselverteilung in beiden Fällen etwa gleich hoch sind. Sowohl die CA (im Falle einer PKI) als auch der PKG (im Falle einer IBE) müssen ihre geheimen Schlüssel vor unberechtigter Benutzung schützen. Auch hier dürfte der Aufwand zum Schutz in etwa gleich groß sein. Bei Kompromittierung eines Schlüssels einer PKG können alle bis zu diesem Zeitpunkt versandten Nachrichten entschlüsselt und Signaturen für beliebige Teilnehmer erstellt werden (zumindest bei den Varianten mit inhärentem Key Escrow). Wird ein CA-Schlüssel kompromittiert, so kann durch falsche Zertifikate ein erheblicher Schaden angerichtet werden. Alle Geheimtexte und Signaturen, die auf zuvor ausgestellten Zertifikaten beruhen, bleiben allerdings sicher. Der Schutzbedarf des geheimen Schlüssels des PKG ist also eher noch höher anzusetzen als der eines geheimen CA-Schlüssels. Die Benutzung von IBE reduziert also nicht den Aufwand, der zum Aufbau der eigentlichen Infrastruktur nötig ist.
Auf Client-Seite ist der Schutz des geheimen Benutzerschlüssels von zentraler Bedeutung. Hier kommen für PKIs und IBE die gleichen Mechanismen in Betracht. Ab einem gewissen Sicherheitsniveau muss der geheime Benutzerschlüssel auch bei IBE durch Hardware (etwa durch Smart Cards) geschützt werden. Gegenüber einer PKI entfällt lediglich die Komponente zur Verwaltung von Zertifikaten. Alle anderen Komponenten, die bei einer PKI in der CA oder bei den Clients vorhanden sein müssen, werden bei IBE ebenfalls benötigt. Der Vorteil von IBE gegenüber PKIs

besteht lediglich darin, dass öffentliche Schlüssel direkt aus den Benutzerdaten erzeugt werden können und nicht aus einem Verzeichnis bezogen werden müssen. Damit ist das Handling für den Sender der Nachricht leichter. Der Aufwand des Empfängers bleibt aber ungefähr gleich hoch, sofern man vom Key-Revocation absieht.

Diese Vorteile erkauft man sich aber mit einer Reihe von Nachteilen, von denen wir folgende für die gravierendsten halten:

Key Escrow: Die Grundversionen von identitätsbasierter Kryptografie, wie sie in Abschnitt 3 beschrieben sind, enthalten immer die Möglichkeit des Key Escrows durch den PKG. Bei Verschlüsselungsverfahren mag ein solches inhärentes Key Escrow durchaus vertretbar sein, bei Signaturverfahren widerspricht es aber der Non-Repudiation-Eigenschaft und ist nicht akzeptabel.
Es gibt Varianten, bei denen das Problem des Key Escrow auf die eine oder andere Art gelöst ist (siehe hierzu Abschnitt 4.1).

Key Revocation: Bei allen vorgeschlagenen Varianten von identitätsbasierter Kryptografie ist eine Sperrung oder ein Wechsel eines Benutzerschlüssels zu einem beliebigen Zeitpunkt ohne zusätzlichen Einsatz von Sperrlisten oder einer Online-Abfrage derzeit nicht möglich. In beiden Fällen muss sichergestellt sein, dass die Sperrliste bzw. die Antwort der Online-Abfrage authentisch ist. Dies ist ohne den Einsatz zusätzlicher PKI-Komponenten kaum machbar.

Der derzeit beste Lösungsansatz hierfür ist das Beschränken der Gültigkeitsdauer der jeweiligen Schlüssel. Dies kann etwa dadurch realisiert werden, dass der öffentliche Schlüssel eines Teilnehmers neben seiner ID noch die Gültigkeitsdauer enthält. Bobs öffentlicher Schlüssel wäre also von der Form (ID_{Bob}, t_{valid}), wobei t_{valid} eine geeignete Kodierung des Gültigkeitszeitraumes ist. Die Schlüsselwechsel sind dann aufgrund der beschränkten Gültigkeitsdauer häufiger. Daher wird der Aufwand vom Sender einer verschlüsselten Nachricht auf den Empfänger verlagert.

Sicherung der Authentizität der öffentlichen Parameter: Ziel einer PKI ist die authentische Zuordnung von Benutzern zu öffentlichen Schlüsseln. Dadurch werden so genannte Man-in-the-Middle Angriffe verhindert, bei denen ein Angreifer Charly einer anderen Teilnehmerin Alice seinen eigenen öffentlichen Schlüssel als den eines dritten Teilnehmers Bob unterschiebt. Fällt Alice auf diese Täuschung rein, so kann Charly künftig alle Nachrichten lesen, die Alice an Bob senden möchte. Bei IBE sind ähnliche Angriffe möglich, wenn die benutzten systemweiten Parameter PK_{PKG} nicht authentisch sind. Es ergibt sich also das gleiche Problem wie bei einer PKI, dem mit ähnlichen Mitteln und Aufwand begegnet werden kann bzw. muss. Ein solcher Angriff könnte folgendermaßen ablaufen[3]:

Seien PK_{PKG} die systemweiten öffentlichen Parameter. Zunächst erzeugt Angreifer Charly sich mittels des Algorithmus Setup ein eigenes Schlüsselpaar (PK_C, SK_C). Wir nehmen nun an, dass es Charly gelingt, Alice davon zu überzeugen, dass die Werte PK_C die korrekten öffentlichen Systemparameter sind. In diesem

[3]Der Angriff wird am Beispiel der identitätsbasierten Verschlüsselung dargestellt, kann aber in analoger Weise auch auf identitätsbasierte Signaturschemata angewendet werden.

Fall wird Alice PK_C und ID_{Bob} benutzen, um ihre Nachricht zu verschlüsseln. Charly kann dann aus ID_{Bob} und SK_C einen Wert $sk^*_{ID_{Bob}}$ berechnen und mit diesem die versandte Nachricht entschlüsseln. Bei $sk^*_{ID_{Bob}}$ handelt es sich um Bobs geheimen Schlüssel in der von Charly aufgesetzten Infrastruktur (mit Charly als PKG). Charly hat also Alice in eine falsche Infrastruktur gelockt, in der Charly die Rolle des PKG hat. Anschließend hat er die Möglichkeiten des PKG zum Key Escrow genutzt, um die mit den untergeschobenen falschen Parametern verschlüsselte Nachricht zu entschlüsseln.
Dieser Angriff entspricht in der Welt der PKI einer Fälschung des Root-Zertifikats.

Eine teilweise Ausnahme bilden hier die Varianten aus Abschnitt 4.1.
Bei der Aufteilung auf mehrere PKG-Instanzen lässt sich auch weiterhin ein solcher Angriff durchführen. Der auf verschiedene Instanzen aufgeteilte geheime Schlüssel der PKG spielt für den Angriff keine Rolle. Die benutzten öffentlichen Parameter sind für alle (verteilten) Instanzen gleich. Können diese ersetzt werden, so hat der Angriff nach wie vor Erfolg.
Bei den certificate-based und certificateless Varianten müsste der Angreifer C nicht nur die Parameter (inkl. Schlüssel) der CA bzw. PKG durch eigene ersetzen, sondern auch noch die des Teilnehmers B, da man zum Entschlüsseln (bzw. Signieren) beide geheimen Schlüssel braucht, die des PKG und des Benutzers.

Es folgt, dass die benutzten (systemweiten) Parameter unbedingt abgesichert werden müssen. Dies kann beispielsweise dadurch gemacht werden, dass sie fest in die verwendete Benutzersoftware (für Sender und Empfänger) verdrahtet werden. Dieses Vorgehen eignet sich aber nur für eine geschlossene Infrastruktur. Bei großen Infrastrukturen wird es, insbesondere im Hinblick auf die bestehende Problematik des Key Escrow, eine Reihe von PKGs geben. In diesem Fall müssen deren öffentliche Parameter auf andere Weise abgesichert werden. Dies kann wiederum mit Hilfe einer PKI geschehen. In diesem Fall würde man einzelne Zweige einer PKI durch IBE realisieren und könnte mit diesem zusätzlichen Hilfsmittel die PKI für große Benutzerzahlen besser skalieren.

Um die Zuordnung von Personen zu Identitäten eindeutig zu gestalten, können weitere Datenfelder wie z.B. die Position in der Firma, Geburtsdatum etc. in die Identität eingefügt werden. Ferner können weitere Datenfelder für den Einsatzzweck des Schlüssels (Verschlüsselung, Signatur oder Authentifizierung) ergänzt werden. Je mehr zusätzliche Felder man verwendet, desto schwerer ist es für den Sender, einen syntaktisch korrekten Identitätsstrings zu bilden, und desto mehr ähnelt dieser inhaltlich und vom Aufbau her einem Zertifikat in einer PKI.

7 Zusammenfassung und Fazit

Wir haben gezeigt, dass der Aufwand zum Betrieb einer reinen IBE Infrastruktur nur unwesentlich geringer ist als der Aufwand zum Betrieb einer PKI. Für den Sender einer Nachricht entfällt die Notwendigkeit, das Zertifikat des Absenders zu

besorgen und zu prüfen. Für den Empfänger der Nachricht und den PKG sind die Aufwände in beiden Fällen jedoch ähnlich hoch. Bei Verwendung von Schlüsseln mit kurzer Gültigkeitsdauer verlagert sich der Aufwand teilweise vom Sender einer Nachricht auf den Empfänger (vgl. Abschnitt 6 - Key Revocation).

Insbesondere die nur unzureichend gelöste Sperrung von Schlüsseln und die Notwendigkeit, die Authentizität der öffentlichen Parameter PK_{PKG} der PKG sichern zu müssen, wiegen manchen Vorteil von IBE wieder auf. In geschlossenen Systemen können diese Probleme durch eine feste Einbettung der Parameter PK_{PKG} in die eingesetzte Soft- bzw Hardware gelöst werden. In offenen Infrastrukturen, in denen Benutzer miteinander kommunizieren möchten, die verschiedenen PKGs angehören, ist dies jedoch nicht möglich. In solchen Infrastrukturen scheint eine Lösung obiger Probleme ohne zusätzlichen Einsatz einer PKI derzeit kaum möglich.

Für den Betrieb reiner IBE-Infrastrukturen sehen wir sehr enge Grenzen gesetzt:

- Es muss akzeptabel sein, dass Benutzerschlüssel nicht zu beliebigen Zeitpunkten gesperrt werden können. Damit scheidet diese Infrastruktur für den Einsatz in Bereichen mit hohen Sicherheitsanforderungen aus.
- Je nach benutzter Variante (siehe Abschnitt 4) muss ein inhärentes Key Escrow akzeptabel sein. Dies sehen wir nicht als generellen Nachteil des Systems an, da eine solche Funktionalität in einigen Umgebungen durchaus wünschenswert ist. So hat eine Firma ein berechtigtes Interesse daran, auf die verschlüsselten Daten ihrer Mitarbeiter zuzugreifen. Dies gilt insbesondere, wenn der betreffende Mitarbeiter kurzfristig wegen Krankheit oder ähnlichen Umständen nicht verfügbar ist.
- Die Authentizität der öffentlichen Parameter PK_{PKG} der PKG kann durch organisatorische Maßnahmen sichergestellt werden. Dies kann etwa durch feste Einbettung in das benutzte System geschehen oder durch Veröffentlichung der Parameter (oder ihres Hashwerts) über einen alternativen Kommunikationskanal. Die Sicherung der Authentizität von PK_{PKG} durch organisatorische Maßnahmen ist in offenen Systemen deutlich schwieriger und aufwändiger als in geschlossenen.

In Umgebungen, in denen keine Widerrufsmechanismen zur Verfügung stehen, können sowohl bei IBE als auch bei PKI Schlüssel mit kurzer Gültigkeitsdauer verwendet werden. Dies lässt sich bei IBE einfacher umsetzen. Wegen des geringeren Aufwandes auf der Seite des Senders eignet sich IBE auch insbesondere für mobile Geräte. Weitere Anwendungen von IBE werden in [SD03] und [LP05] beschrieben.

Nutzt man IBE als Teilsystem einer PKI, so stellt sich die Situation völlig anders dar. Durch die PKI können die öffentlichen Parameter PK_{PKG} der PKG leicht abgesichert werden. Auch für die Sperrung von Schlüsseln können die Methoden der PKI verwendet werden (etwa Sperrlisten oder Online-Abfragen). Durch den Einsatz von IBE innerhalb einer PKI kann etwa die Anzahl an Zertifikaten in einem Teilbaum drastisch reduziert und damit die Verwaltung der öffentlichen Schlüssel

für diesen Baum stark vereinfacht werden. Allerdings bezahlt man diesen Vorteil mit der Tatsache, dass Benutzer nun sowohl über PKI-Software zur Verwaltung von Zertifikaten als auch über IBE-Software zur eigentlichen Verschlüsselung der Nachrichten verfügen müssen. Auch in diesem Fall darf man durch den Einsatz von IBE keine Verminderung der Komplexität der Infrastruktur erwarten. Vielmehr erreicht man durch Hinzunahme von IBE zu einer PKI ein Abwägen (Trade-Off) einzelner Aufwände, die eine Vereinfachung einzelner Abläufe zur Folge haben kann. Wählt man das eingebettete IBE System so, dass die am häufigsten genutzten Abläufe verbessert werden, so kann sich durchaus eine Effizienzsteigerung für das Gesamtsystem ergeben.

Danksagung: Unser spezieller Dank gilt Thomas Hueske von der SRC GmbH dafür, dass er uns beim Verfassen dieses Artikels als Diskussionspartner zur Verfügung stand und sowohl mit seinen Anmerkungen als auch insbesondere durch seine Fragen sehr zur Verbesserung des Ergebnisses beigetragen hat.

Literatur

[AdM04] Giuseppe Ateniese und Breno de Medeiros. Identity-Based Chameleon Hash and Applications. In *Financial Cryptography '04*, Jgg. 3110 of *Lecture Notes in Computer Science*, Seiten 164–180. Springer, 2004.

[ARP03] Sattam S. Al-Riyami und Kenneth G. Paterson. Certificateless Public Key Cryptography. Cryptology ePrint Archive, Report 2003/126 (`http://eprint.iacr.org/2003/126.pdf`), 2003.

[BF01] Dan Boneh und Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO '01*, Jgg. 2139 of *Lecture Notes in Computer Science*, Seiten 213–229. Springer, 2001.

[Boy03] Xavier Boyen. Multipurpose Identity-Based Signcryption (A Swiss Army Knife for Identity-Based Cryptography). In *CRYPTO '03*, Jgg. 2729 of *Lecture Notes in Computer Science*, Seiten 383–399. Springer, 2003.

[BZ04] Joonsang Baek und Yuliang Zheng. Identity-Based Threshold Decryption. In *Public Key Cryptography '04*, Jgg. 2947 of *Lecture Notes in Computer Science*, Seiten 262–276. Springer, 2004.

[CC03] Jae Choon Cha und Jung Hee Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. In *Public Key Cryptography '03*, Jgg. 2567 of *Lecture Notes in Computer Science*, Seiten 18–30. Springer, 2003.

[CC05] Zhaohui Cheng und Richard Comley. Efficient Certificateless Public Key Encryption. Cryptology ePrint Archive, Report 2005/012 (`http://eprint.iacr.org/2005/012.pdf`), 2005.

[CHSS02] L. Chen, Keith Harrison, David Soldera und Nigel P. Smart. Applications of Multiple Trust Authorities in Pairing Based Cryptosystems. In *InfraSec '02*, Jgg. 2437 of *Lecture Notes in Computer Science*, Seiten 260–275. Springer, 2002.

[CJZ05] XU Chunxiang, ZHOU Junhui und QIN Zhiguang. A Note on Secure Key Issuing in ID-based Cryptography. Cryptology ePrint Archive, Report 2005/180 (`http://eprint.iacr.org/2005/180.pdf`), 2005.

[Coc01] Clifford Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In *IMA Int. Conf. '01*, Jgg. 2260 of *Lecture Notes in Computer Science*, Seiten 360–363. Springer, 2001.

[Gen03] Craig Gentry. Certificate-Based Encryption and the Certificate Revocation Problem. In *EUROCRYPT '03*, Jgg. 2656 of *Lecture Notes in Computer Science*, Seiten 272–293. Springer, 2003.

[Hes02] Florian Hess. Efficient Identity Based Signature Schemes Based on Pairings. In *Selected Areas in Cryptography '02*, Jgg. 2595 of *Lecture Notes in Computer Science*, Seiten 310–324. Springer, 2002.

[HL02] Jeremy Horwitz und Ben Lynn. Toward Hierarchical Identity-Based Encryption. In *EUROCRYPT '02*, Jgg. 2332 of *Lecture Notes in Computer Science*, Seiten 466–481. Springer, 2002.

[LBD+04] Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang und Seungjae Yoo. Secure Key Issuing in ID-based Cryptography. In *Second Australasian Information Security Workshop (AISW2004)*, Jgg. 32 of *CRPIT*, Seiten 69–74. ACS, 2004.

[LP05] Hoon Wei Lim und Kenny G. Paterson. Identity-Based Cryptography for Grid Security. In *IEEE International Conference on e-Science and Grid Computing e-Science*, 2005.

[LQ03] Benoît Libert und Jean-Jacques Quisquater. New identity based signcryption schemes from pairings. Cryptology ePrint Archive, Report 2003/023 (`http://eprint.iacr.org/2003/023.pdf`), 2003.

[ML02] John Malone-Lee. Identity-Based Signcryption. Cryptology ePrint Archive, Report 2002/098 (`http://eprint.iacr.org/2002/098.ps.gz`), 2002.

[SD03] Diana K. Smetters und Glenn Durfee. Domain-Based Administration of Identity-Based Cryptosystems for Secure Email and IPSEC. In *12th USENIX Security Symposium*, Seiten 215–230, 2003.

[Sha85] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO '84*, Jgg. 196 of *Lecture Notes in Computer Science*, Seiten 47–53. Springer, 1985.

[SW04] Amit Sahai und Brent R. Waters. Fuzzy Identity Based Encryption. Cryptology ePrint Archive, Report 2004/086 (`http://eprint.iacr.org/2004/086.pdf`), 2004.

[ZK02] Fangguo Zhang und Kwangjo Kim. ID-Based Blind Signature and Ring Signature from Pairings. In *ASIACRYPT '02*, Jgg. 2501 of *Lecture Notes in Computer Science*, Seiten 533–547. Springer, 2002.