UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Informatik

FB 4
Informatik

Konzept einer Public Key Infrastruktur in iCity

Sebastian Magnus
Markus Maron

Nr. 12/2009

Arbeitsberichte aus dem Fachbereich Informatik

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Zöbel

Kontaktdaten der Verfasser

Sebastian Magnus, Markus Maron
Institut für Informatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: smagnus@uni-koblenz.de, maron@uni-koblenz.de

Inhaltsverzeichnis

Zusammenfassung

Dieses Dokument schlägt ein Konzept für eine Personal Key Infrastruktur in iCity vor. Über ein Trust Center (TC) ausgestellte Zertifikate gewährleisten einen sicheren Schlüsselaustausch mit nachweisbarer Authentisierung des Kommunikationspartners, Abhörsicherheit sowie Unverfälschtheit und Nachweisbarkeit der Nachrichten. Das gemeinsam vertrauenswürdige TC muss während der Kommunikation nicht erreichbar sein. Es erhält lediglich öffentliche Informationen. Das Konzept stellt mehrere Sicherheitsstufen vor, die sichere Identifikation und Anonymität unterschiedlich gewichten.

1 Motivation

iCity ist ein vom Europäischen Fond für Regionale Entwicklung gefördertes, wirtschaftsnahes Forschungsprojekt. Es untersucht kostenlose, orts- und kontextabhängige personalisierte Informations- und Transaktionssysteme. Nutzer können mit einem mobilen Endgerät, wie zum Beispiel einem Mobiltelefon, über Bluetooth auf Dienste in ihrer direkten Umgebung zugreifen. Beim Umgang mit personalisierten Daten spielt Übertragungssicherheit auf dem letzten Meter eine zentrale Rolle: Die Verbindung muss vor unberechtigtem Zugriff, Manipulation und Angriffen gegen die Privatsphäre geschützt werden. Erst durch ausreichende Sicherheit werden Transaktionen wie mobile Zahlvorgänge oder der Kauf von Wertobjekten, z.B. Eintrittskarten und Fahrkarten, ermöglicht.
Dieses Dokument beschreibt eine Sicherheitsinfrastruktur für iCity. Zu einem beliebigen Zeitpunkt vor der Kommunikation muss ein Zertifikat von einem Trust Center (TC) erstellt werden, dieses kann von jedem Teilnehmer auch offline geprüft werden. Für den Verbindungsaufbau ist kein Zugriff auf die zentrale, vertrauenswürdige Stelle nötig. Die verschiedenen Anwendungsgebiete in iCity erfordern unterschiedliche Sicherheitsstufen. Jede Kommunikation wird durch asymmetrische Verschlüsselung vor Abhören geschützt. Bei reinen Informationsdiensten steht das gesetzlich geschützte Recht auf Anonymität des Teilnehmers im Vordergrund [1, 2], bei Kauf- oder Bezahlvorgängen hingegen muss die Unverfälschtheit und Beweisbarkeit der Transaktion gewährleistet sein [3, 4].
Das nachfolgende Konzept ist flexibel genug, um in unterschiedlichen Szenarien eingesetzt zu werden. Hierfür werden drei unterschiedliche Nutzer-Zertifikate (AHC, AC, PC) und ein Trust-Center-Zertifikat (TCC) definiert. Diese ermöglichen den Aufbau einer abhörsicheren Verbindung, die Authentifizierung des Kommunikationspartners oder seines Zertifikates, die Prüfung auf Unverfälschtheit und Herkunft von Nachrichten sowie die auch nachträgliche Beweisbarkeit der Kommunikation in Bezug auf Inhalt und Teilnehmer.
Aufbau und Funktion der Trust Center bzw. der Signaturen orientieren sich am FIPS 186-2 Digital Signature Standard [5] und Veröffentlichungen der Bundesnetzagentur (BNetzA) [6, 7, 8, 9]. Das Konzept weicht aber von gesetzlichen Definitionen [10, 11] der BNetzA ab. Insbesondere die Zertifikatsstufen mit höherer Anonymität implementieren nicht alle von der BNetzA spezifizierten Sicherheitsanforderungen [6].

1.1 Das iCity Projekt

iCity ist ein wirtschaftsnahes Forschungsprojekt, das als ein ambientes System den mobilen Zugriff auf in die Umgebung integrierte Access Points über Nahfunktechnik ermöglicht. Anwender benötigen lediglich ein handelsübliches Bluetooth-Mobiltelefon, um die Dienste zu nutzen. Es entstehen keine zusätzlichen Kosten auf dem letzten Meter. iCity baut auf Ergebnissen der Projekte IASON [12], Campus News [13, 14, 15] und City on Foot [16] auf. Gemeinsam mit unseren Projektpartnern wird es in den Bereichen Aussenwerbung, öffentlicher Nahverkehr und im Gesundheitswesen getestet.

1.1.1 Mobile Ticketing

In Zusammenarbeit mit der Koblenzer Elektrizitäts und Verkehrs AG unterstützt iCity im öffentlichen Nahverkehr Fahrgäste durch zusätzliche Fahrplanauskünfte. Der Kunde bekommt den aktuellen Fahrplan, Planänderungen und seine Umstiege gemeldet. Die aktuelle Fahrt und Favoriten werden automatisch gesendet, so dass umständliche Eingaben auf dem Mobilgerät minimiert werden. Busfahrten sind durch die Bindung an Aufenthalt und Bewegung an persönliche Daten geknüpft. Werden zugleich mobile Handy-Fahrkarten angeboten, kommt eine Finanztransaktion und der Austausch eines digitalen Wertobjektes hinzu. Dann muss die Kommunikation nachweisbar und vor Manipulation oder Abhören geschützt sein.

1.1.2 Mobile Marketing

In Kooperation mit awk Aussenwerbung GmbH wird das ambiente System als Medium zur Vermittlung von Werbung, Gutscheinen und Produktinformation verwendet. Einerseits können herkömmliche Inhalte digital übermittelt werden, andererseits können diese aber auch durch zusätzliche Medien wie Videos und interaktive Inhalte angereichert werden.
In der Marktforschung hat die Erfassung von Nutzerdaten eine zentrale Bedeutung. iCity bietet neue Möglichkeiten, die Häufigkeit, Dauer und Wiederholung von Kontakt zu Passanten automatisch zu messen. Im Gegensatz zu herkömmlichen Methoden, die manuell zählen, können Kosten eingespart und genauere Daten erfasst werden.
Datenerfassung steht im Konflikt mit der Privatsphäre des Kunden. Hier bietet iCity Werkzeuge zur unumkehrbaren Pseudonymisierung [17], die datenschutzkonforme Marktforschung ermöglichen.

1.1.3 Mobile Healthcare

Neue Medikamente erfordern eine plötzliche Umstellung der Lebensgewohnheiten: Die Arznei muss zur richtigen Zeit eingenommen werden und Nebenwirkungen müssen beachtet werden. Hier soll iCity helfen, indem der Arzt einen digitalen Beipackzettel mit allen notwendigen Informationen direkt auf das Handy

schickt: So kann man auch unterwegs problemlos nachsehen. Zusätzlich empfängt der Patient einen Kalendereintrag, der zur Einnahmezeit durch einen Alarm erinnert.
Gesundheit ist eines der persönlichsten, vertraulichsten Gebiete: Zwar hat der Patient im Allgemeinen hohes Vertrauen in den Arzt, aber keine dritte Person darf die Kommunikation mithören. Die Verbindung muss vor unberechtigtem Zugriff geschützt werden. Auch dürfen die Nachrichten auf dem Übertragungsweg nicht verfälscht werden: Ein Beweis über den korrekten und vollständigen Empfang ist nötig.

1.2 Anwendungsbeispiele

Bevor die iCity-PKI detailliert beschrieben wird, geht dieser Abschnitt auf Anwendungestypen und ihre Sicherheitsbedürftnisse ein.

Anonyme Informationsdienste: Bei Fahrplaninformationen, Aussenwerbung, Touristeninformation und Produktinformation handelt es sich prinzipiell um öffentliche Informationen. Bei solchen anonymen Informationsdiensten ist für den Serviceanbieter die Identität des Empfängers nicht relevant. Während die Identität des Diensteanbieters öffentlich ist, muss das Recht des Kunden auf Privatsphäre beachtet werden: Dieser soll eine Kommunikation ohne preisgabe persönlicher Daten aufbauen können. Dritte dürfen die Kommunikation nicht belauschen, z.B. um Interessenprofile zu erstellen. Der Kunde muss vor Phishing oder anderen Social Engineering Angriffen geschützt werden: Der Dienstanbieter muss eindeutig erkennbar sein.

Registrierte und kontextabhängige Dienste: Dienste können von einer vorherigen Kommunikation abhängig sein. Darunter zählen Prepaid-Zahlungen oder personalisierte Dienste. Diese Dienste können anonym sein oder mit einer während der Registrierung bekanntgegebenen Identität verbunden sein. Für die Nutzung des Dienstes muss der Kunde seine Identität nicht (respektive nicht erneut) preisgeben, er muss aber als Gesprächspartner wiedererkannt werden, z.B. über eine Identifikationsnummer. Im Beispiel einer Prepaid-Zahlung würde der Kunde eine Kennung bei seiner ersten Einzahlung zugewiesen bekommen, anhand der spätere Transaktionen zugeordnet werden.
Während die Identität des Dienstanbieters öffentlich ist und als Schutz vor Betrug nachgewiesen werden muss, muss der Kunde nur seine Kennung beweisen können. Erneut ist Schutz vor Abhörung nötig. Typischerweise benötigen diese Dienste Wege, die Echtheit und den Inhalt von Transaktionen während der Kommunikation und auch im Nachhinein nachweisen zu können.

Personenbezogene Dienste: Insbesondere, wenn rechtliche Handlungen oder Finanztransaktionen ausgeführt werden, müssen die Kommunikationspartner als natürliche oder juristische Personen nachweisbar sein. Derartige Dienste sind nur möglich, wenn die Kommunikationspartner sich als vertrauenswürdig anerkennen in Bezug auf den Umgang mit den empfangenen Daten. Eine ausdrückliche

Zustimmung der Partner wird also vorausgesetzt.
Wie zuvor muss die Kommunikation vor Angriffen Dritter geschützt werden. Beide Partner müssen ihre Identität nachweisen. Die Kommunikation muss bezüglich Teilnehmer und Inhalt nachweisbar sein.

Anonyme Peer-to-Peer Dienste: Im Internet erfreuen sich Peer-to-Peer Dienste wie Chatprogramme, Multiplayer Spiele oder Dienste im Bereich Social Networking immer höherer Beliebtheit. Derartige Dienste sind auch in iCity denkbar. Typischerweise wird ein hoher Grad an Anonymität gefordert: Benutzer wollen unter einem Pseudonym agieren und Kontrolle darüber haben, welche Daten von ihnen mitgeteilt werden. Es wird Schutz vor Abhören durch Dritte und ein Mittel zur Pseudonymisierung benötigt. Andererseits ist Nachweisbarkeit und Authentisierung nicht relevant: Die Nutzer sind sich darüber bewusst, dass die Teilnehmer nicht immer die Wahrheit sagen.

1.3 Wiedererkennung und persönliche Identifikation

Wiedererkennung bezeichnet die Erkennung eines Kommunikationspartners, mit dem bereits eine Kommunikation stattgefunden hat. Eine persönliche Identifikation bezeichnet die Erkennung des Kommunikationspartners als Person, Unternehmen oder sonstigen Akteur der physischen Welt.
Persönliche Identifikation steht in starkem Widerspruch zur Anonymität, Wiedererkennung ermöglicht während der Kommunikation eine Anonymität unter Preisgabe des Kontext.
Das beschriebene Konzept stellt drei Stufen der Erkennung bereit. Kommunikationspartner können durch personalisierte Zertifikate ihre natürliche Identität nachweisen, wodurch z.B. ein Unternehmen seine Kunden vor Phishing schützen kann oder B2B-Anwendungen denkbar werden. Sie können stattdessen auch in anonymen Zertifikaten Pseudonyme oder eine Zertifikats-ID austauschen. Erneuter Kontakt zum Pseudonym bzw. dem Zertifikat wird erkannt. Diese Stufe ist insbesondere zur Wahrung der Privatsphäre von Privatpersonen geeignet. Als dritte Stufe können vollständig anonyme Zertifikate von den Kommunikationspartnern für Ad-Hoc-Verbindungen selbst erzeugt werden. Diese ermöglichen vollständige Anonymität ohne Erkennung des Partners, sind aber für Fälschung und Man-in-the-Middle (MITM)-Angriffe während des Verbindungsaufbaus anfällig. Sie tauschen lediglich kryptographische Informationen zur Verschlüsselung der Verbindung aus.

1.4 Unterstützte Sicherheitsmerkmale

Sicherheit umfasst eine Vielzahl an Merkmalen. Diese können einander widersprechen (z.B. Identifikation eines Teilnehmers und Anonymität) oder mit anderen Zielsetzungen kollidieren (z.B. Usability, Transparenz). Das nachfolgende Konzept soll mehrere, für unterschiedliche Szenarien geeignete Maßnahmen in einer gemeinsamen Private Key Infrastructure (PKI) vereinen. Je nach Szenario werden die Merkmale Wiedererkennung und Identifikation, Abhörsicherheit,

Unverfälschtheit und Beweisbarkeit unterschiedlich berücksichtigt.
Abhörsicherheit schützt vor Mitlauschen durch Dritte. Hierfür nutzt iCity in die PKI integrierte kryptographische Verfahren. Der in asymmetrischen Verfahren prinzipiell problematische Schlüsselaustausch wird durch von einem Trust Center ausgestellte Zertifikate gelöst.
Nachdem die Kommunikationspartner über Zertifikate ihre öffentlichen Schlüssel ausgetauscht haben, können Nachrichten signiert werden[18]. Dies ist mit allen Sicherheitsstufen möglich. Wird eine Nachricht verfälscht, so wird die Signatur ungültig. Die Echtheit und Korrektheit ist durch die Signatur sowohl beim Empfang als auch nachträglich gegenüber Dritten nachweisbar. Dabei handelt es sich um eine technische Beweisbarkeit, ob diese eine juristische Beweisbarkeit impliziert müsste zunächst geprüft werden.
Zugleich kann der Empfänger nachweisen, dass die Nachricht vom Besitzer des zum Zertifikat passenden geheimen Schlüssel stammt. Wurde das Zertifikat vom TC signiert und hat der Besitzer seinen geheimen Schlüssel nicht weitergegeben, so ist dies der angenommene Kommunikationspartner.

2 Globales Schema

Dieser Abschnitt stellt die Teilnehmer der PKI und die von ihnen ausgetauschten Nachrichten vor. Eine detaillierte Beschreibung folgt in den späteren Abschnitten.

2.1 Definition der Teilnehmer und Objekte

Die nachfolgend definierten Teilnehmer und PKI-Objekte sind zur Übersicht in Tabelle 1 aufgelistet.
An der PKI nehmen ein Trust Center T, der Absender A und der Empfänger B teil. Ziel der PKI ist eine Kommunikation zwischen A und B, ohne dass ein unberechtigter Dritter manipulieren oder mithören kann. Hochgestellte Indizes bezeichnen im Folgenden den Inhaber eines Objektes, z.B. ist K^T_{Pub} der öffentliche Schlüssel des Trust Centers.
Jeder der Teilnehmer verfügt über einen öffentlichen Schlüssen K_{Pub} und einen privaten Schlüssel K_{Priv}. Es sollen Nachrichten M_d ausgetauscht werden. Eine kryptographische Hashfunktion $h(M)$ ist eine Einwegfunktion, die zu einer Nachricht M einen repräsentativen Wert konstanter Länge berechnet [8, 7]. Zu ihnen zählt zum Beispiel die SHA-Familie [19]. Zu einem Hash-Wert kann keine diesen Wert erzeugende Nachricht effizient konstruiert werden. Kleine Änderungen der Nachricht verändern ihren Hash-Wert erheblich. Die Funktion wird Kollisionsfrei genannt, wenn Kollisionen mit an Sicherheit grenzender Wahrscheinlichkeit nicht auftreten [8].
Eine Verschlüsselungsfunktion

$$c(M_d, K_{Pub}) = M^{K_{Pub}} \tag{1}$$

bzw.

$$c(M_d, K_{Priv}) = M^{K_{priv}} \tag{2}$$

ist nach [18] eine Einweg-Falltürfunktion. Aus der verschlüsselten Nachricht kann ohne Wissen über den korrespondierenden Schlüssel die ursprüngliche Nachricht M_d nicht rekonstruiert werden. Durch erneute Anwendung mit dem korrespondierenden Schlüssel wird die ursprüngliche Nachricht wiederhergestellt:

$$c(M^{K_{priv}}, K_{Pub}) = M_d \tag{3}$$

bzw.

$$c(M^{K_{Pub}}, K_{Priv}) = M_d \tag{4}$$

Das TC kann den Inhaber $I \in \{A, B, T\}$ eines Schlüsselpaares durch ein Zertifikat Z^I bescheinigen. Zertifikate enthalten kryptographische Informationen, darunter der öffentliche Schlüssel des Inhabers K^I_{Priv} sowie eine Kennnummer und optionale Informationen über den Inhaber. Sie werden genauer in Abschnitt 3 beschrieben.
Die Signatur einer Nachricht ist ihr mit dem privaten Schlüssel des Erzeugers I (i.A. der Absender) chiffrierter Hash-Wert [5, 7]:

$$S(M, I) = S(M, K^I_{Priv}) = c(h(M), K^I_{Priv}) \tag{5}$$

Die Nachricht darf verschlüsselt oder auch unverschlüsselt sein. Über den öffentlichen Schlüssel kann der ursprüngliche Hash-Wert rekonstruiert werden:

$$h(M) = c(S(M, I), K^I_{Pub}) \tag{6}$$

Signaturen dienen zum Nachweis der Herkunft und Echtheit einer Nachricht.

2.2 PKI-Verbindungsschema

Abbildung 1 zeigt, welche Interaktionen in der PKI vorgesehen sind. Dieser Abschnitt wird die Schritte allgemein beschreiben, detaillierte Erklärungen folgen in Abschnitt 5.
Zwischen A und B sollen Nachrichten ausgetauscht werden. Absender und Empfänger können ihre Rollen Tauschen, auch das TC kann Absender oder Empfänger sein, z.B. bei der Zertifikatserstellung oder der Aktualisierung von Sperrlisten.
Neue Zertifikate werden beim TC erzeugt und stellen ihre Echtheit über eine Signatur $S(Z^I, T)$ sicher werden.
Zwischen A und B kann eine Kommunikation zur Identifikation (vgl. 5.3) oder zum Nachrichtenaustausch (vgl. 5.5) stattfinden. Hierfür werden Zertifikate beim Verbindungsaufbau übergeben. Sowohl Nachrichtenaustausch als auch Identifikation werden über die kryptographischen Informationen aus dem Zertifikat gesichert.
Korrumpierte Zertifikate können über eine Sperrliste ungültig gemacht werden. Diese Sperrliste wird durch das TC oder durch andere Teilnehmer aktualisiert.

Bezeichner	Beschreibung
A	Sender einer Nachricht
B	Empfänger einer Nachricht
T	Trust Center
$I \in \{A, B, T\}$	Inhaber eines Zertifikats oder Schlüssels
K^I_{Pub}	Öffentlicher Schlüssel von Teilnehmer I
K^I_{Priv}	Geheimer Schlüssel von Teilnehmer I
M	Nachricht
M_d	Klartext Nachricht
M_K	Mit Schlüssel K chiffrierte Nachricht
Z^I	Zertifikat des Teilnehmers I
$c(M, K)$	(De-)Chiffre-Funktion, die Nachricht M mit Schlüssel K (de-)chiffriert.
$h(M)$	Kryptographische Hash-Funktion
$S(M, I)$	Signatur des Teilnehmers I

Tabelle 1: Objekte und Teilnehmer der PKI

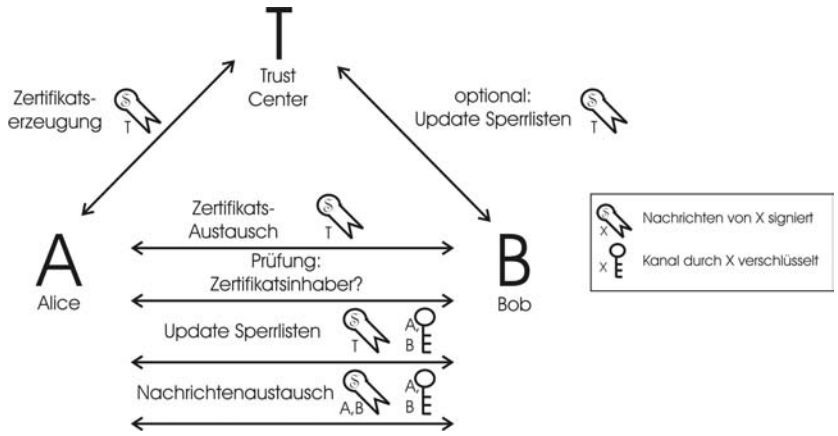

Abbildung 1: Interaktion der Teilnehmer

3 Das Trust Center

Der nachfolgende Abschnitt wird zunächst in 3.1 das Trust Center als die Zertifikate verwaltende und herausgebende Stelle vorstellen. Bei mehreren TCs können Zertifikate in einer Vertrauenshierarchie anerkannt werden. Diese Hierarchie wird in 3.2 beschrieben. Dieser Abschnitt behandelt nur die Aufgaben und den Aufbau des TC. Die von ihm herausgegebenen Zertifikate werden in Abschnitt 4 beschrieben.

3.1 Aufgaben des Trust Centers

Ein Trust Center ist eine für alle Kommunikationspartner vertrauenswürdige Stelle. Dabei genügt es, dass ein TC in Bezug auf die korrekte Signierung der Zertifikate und die Prüfung der Zertifikatsdaten vertrauenswürdig ist.
Das Trust Center bestätigt mit seiner Signatur die Echtheit und Zusammengehörigkeit von Daten. Daten und Signatur ergeben zusammen ein Zertifikat. Zertifikate einer PKI müssen zumindest ein Identifikationsmerkmal und den öffentlichen Schlüssel des Besitzers enthalten, des weiteren können sie zusätzliche Daten bescheinigen wie z.B. die Identität des Inhabers oder eine Gültigkeitsdauer. Solche zusätzlichen Daten müssen vom TC auf Korrektheit geprüft werden. Zertifikate sind durch die Signatur fälschungssicher. Sie werden dem Besitzer übergeben und können von diesem direkt weitergereicht werden. Das TC verwaltet Sperrlisten für Zertifikate, deren geheime Schlüssel korrumpiert sind.

3.2 Initiale und Hierarchische Trust Centers

In größeren Systemen könnte es mehr als ein Trust Center geben. Ähnlich wie im Internet könnten diese ihre Zertifikate gegenseitig anerkennen. Hierfür ist aus Sicht eines Kommunikationsteilnehmers eine Unterscheidung nach initialen TCs und hierarchisch anerkannten TCs nötig.
Initiale TCs werden von den Kunden ohne automatisierbare Verifizierung akzeptiert. Dies ist für mindestens ein ursprüngliches TC notwendig, da für dieses noch keine vertrauenswürdige Stelle in der PKI bekannt ist. Das initiale TC kann gemeinsam mit der kryptographischen Applikation übertragen werden, oder es muss über einen externen Kanal wie z.B. die Eingabe einer optisch übertragenen PIN bestätigt werden.
TC können andere TCs als vertrauenswürdig anerkennen. Hierzu stellen sie ein Zertifikat aus, das die kryptographischen Daten des anerkannten TC signiert. Am Zertifikat ist erkennbar, von welchem TC die Anerkennung stammt. Falls ein TC seine Vertrauenswürdigkeit verliert, können hierüber auch alle hierarchisch abstammenden Zertifikate gesperrt werden. Ein abstammendes TC bleibt nur vertrauenswürdig, falls es zugleich von einem alternativen, weiterhin vertrauenswürdigen Zweig anerkannt wird.
Abbildung 2 zeigt eine beispielhafte Vertrauenshierarchie mit TC9 als einzigem initialen TC des Teilnehmers. In gestrichelten Linien ist ein Vertrauensdigraph der TCs dargestellt. Ein TC bescheinigt die von ihm aus direkt erreichbaren

TCs als vertrauenswürdig, alle im Digraphen erreichbaren TCs können vom Teilnehmer als vertrauenswürdig eingestuft werden. Die durchgezogenen Linien beschreiben, auf welchem Weg die Vertrauenswürdigkeit entsprechend der Informationen aus dem Zertifikat anerkannt wurde. Offensichtlich unterliegt den tatsächlich anerkannten TCs ein Wald (hier sogar Baum) mit den initialen TCs (hier TC9) als Wurzeln.
Trotz komplexer Hierarchie ist anzunehmen, dass der Aufwand zur Verwaltung der TCs nicht groß ist. Die PKI-Page [20] schätzt die Anzahl der Internet- Zertifikatsstellen weltweit auf 150 Stellen, die Bundesnetzagentur erwähnt auf ihrer Homepage 10 akkreditierte CAs [21]. Innerhalb iCity ist eine wesentlich kleinere Anzahl ausreichend. Neue Trust Center oder Vertrauensbeziehungen sind eher selten zu erwarten.

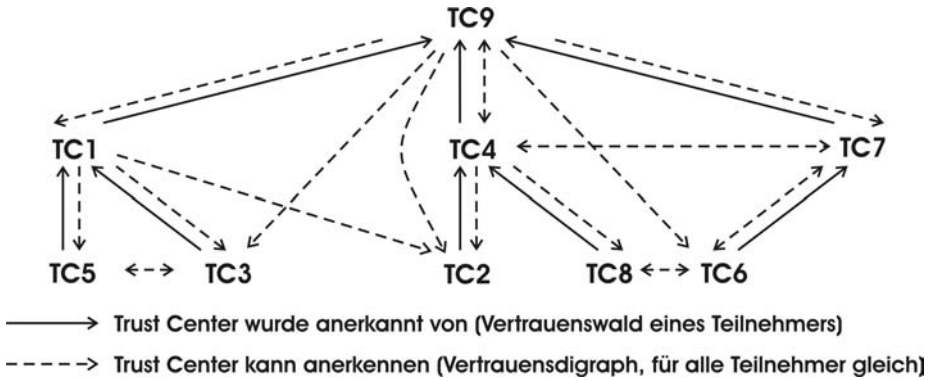

Abbildung 2: Trust Center Hierarchie mit neun TCs

4 Aufbau der Zertifikate

Dieser Abschnitt beschreibt die verschiedenen Zertifikatstypen. Diese enthalten unterschiedliche Daten: Zertifikate mit höherer Sicherheit enthalten zum Einen die Daten der weniger sicheren Zertifikate, aber auch zusätzliche Informationen. Es stehen vier Zertifikatstypen zur Verfügung (Abschnitt 4.1 bis 4.4), deren Beziehung in Abbildung 3 illustriert ist.
Die ersten drei Zertifikatstypen (AHC, AC und PC) unterscheiden sich in den enthaltenen Daten und den damit erreichten Sicherheitsmerkmalen. Sie enthalten Daten über einen Teilnehmer. Der vierte Typ (TCC) ist vom Aufbau zum PC identisch, enthält jedoch Informationen über ein TC und wird zum Prüfen anderer Zertifikate verwendet.
Es wird nach kryptographischen Daten, administrativen Daten, Benutzerdaten und der Signatur unterschieden. Welche Daten in diesen Kategorien vermerkt sind, beschreibt Abschnitt 4.5.

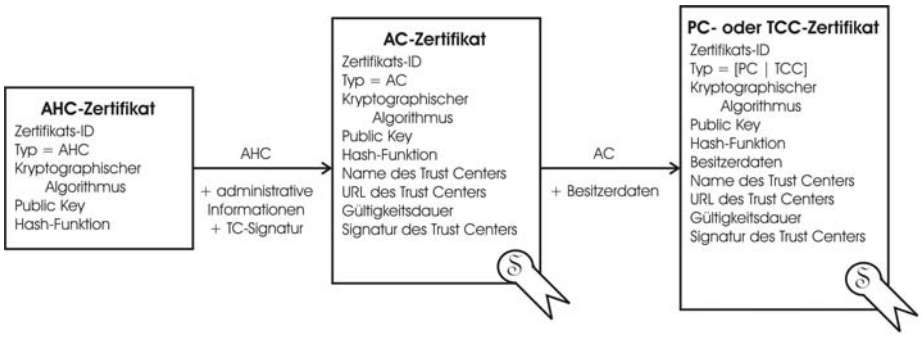

Abbildung 3: Zertifikatstypen

4.1 Ad-Hoc Zertifikat (AHC)

Ad-Hoc Zertifikate (AHC) sind vollständig anonyme, vom Inhaber selbst erzeugte Zertifikate. Sie bieten keinen Schutz vor falschen Identitäten und erlauben damit MITM-Angriffe. Sie können genutzt werden, damit zwei Kommunikationspartner eine abhörsichere Verbindung ohne gemeinsames TC aufbauen. AHC enthalten lediglich die kryptographischen Informationen und bieten keine weiteren Sicherheitsmerkmale, insbesondere könnte ein Angreifer während des Zertifikatsaustausch den öffentlichen Schlüssel durch seinen eigenen austauschen.
Die Zertifikate können genutzt werden, wenn aus Sicht des Senders nicht relevant ist, mit wem die Kommunikation geführt wird, der Inhalt der Nachricht aber vor unbefugtem Mithören Dritter geschützt werden soll. So kann z.B. ein Verkehrsunternehmen Fahrplaninformationen an einen Kunden mit AHC senden, ohne dass Dritte Kenntnis über das Reisevorhaben erlangen.

4.2 Anonymes Zertifikat (AC)

Anonyme Zertifikate (AC) enthalten kryptographische und administrativen Informationen. Ihre Unverfälschtheit wird durch eine TC-Signatur nachgewiesen. Der Kommunikationspartner erkennt, dass er mit dem Inhaber des Zertifikates und des damit verbundenen Schlüsselpaares kommuniziert. Er kann diesen bei mehrmaligem Kontakt an der Zertifikats-ID wiedererkennen und so einen Kontext zu vorherigen Kommunikationen herstellen. Die natürliche Person bleibt anonym. Der Inhaber kann mehrere solcher Zertifikate besitzen und in unterschiedlichem Kontext verwenden.
Ein AC ist ein erweitertes AHC, welches die Zusammengehörigkeit einer eindeutigen Zertifikatsnummer und der kryptographischen Informationen bescheinigt. Über die Signatur des TC kann die Gültigkeit und Korrektheit nachgewiesen werden.

4.3 Personalisiertes Zertifikat (PC)

Über personalisierte Zertifikate kann die natürliche Identität eines Teilnehmers gemeinsam mit kryptographischen Informationen durch ein Trust Center signiert werden. Diese Information kann anschließend nicht gefälscht werden, die Identität des Inhabers ist also nachweisbar. Dieses Zertifikat kann z.B. von Unternehmen genutzt werden, um Kunden vor Phishing-Angriffen zu schützen, oder es kann durch eine geprüfte Adresse das Zahlungsrisiko größerer mobile Payment-Transaktionen mindern.

4.4 Trust Center Zertifikat (TCC)

Das Trust Center Zertifikat (TCC) ist wie das PC aufgebaut, dient jedoch nicht der Erkennung des Kommunikationspartners, sondern der Erkennung eines Trust Centers und dadurch der Prüfung von Signaturen auf Zertifikaten.
Die TCC für initiale Trust Center müssen auf einem externen Kanal gewonnen werden, beispielsweise können sie gemeinsam mit der verschlüsselnden Applikation ausgeliefert werden. Da für initiale TC keine vertrauenswürdige Stelle existiert, die diese signieren kann, bleibt ihre Signatur leer. Ihre Vertrauenswürdigkeit wird durch den externen Kanal gewährleistet.
Bei mehr als einem TC kann ein Kunde auch den Zertifikaten der von seinem TC für vertrauenswürdig anerkannten TCs vertrauen. Hierfür erstellt ein bereits bekanntes TC für ein anderes TC ein Zertifikat und signiert dieses. Dies kann iterativ wiederholt werden. Offensichtlich entsteht so eine hierarchische Abstammung der Zertifikate mit Baumstruktur. Verliert ein TC seine Vertrauenswürdigkeit, so können über die Aussteller-Einträge alle davon abstammenden TC erkannt und ebenfalls entfernt werden. Falls ein so abgeschnittenes TC zugleich von einem weiterhin vertrauenswürdigen TC abstammt, kann es durch ein auf dem anderen Zweig signierten Zertifikat erneut aufgenommen werden.

4.5 Datenfelder der Zertifikate

Je nach Zertifikatstyp werden unterschiedliche Daten benötigt. Diese lassen sich in die Gruppen kryptographischer, administrativer und persönlicher Daten aufteilen, hinzu kann eine Signatur des TC kommen. Alle Zertifikate enthalten nur öffentliche Daten und können unverschlüsselt übertragen werden. Tabelle 2 listet die Informationsblöcke mit einer Kurzbeschreibung auf und gibt die Zertifikatstypen an, in denen sie enthalten sind.
Kryptographische Informationen: Als kryptographische Information wird im Zertifikat der verwendete Verschlüsselungsalgorithmus des Inhabers, sein öffentlicher Schlüssel und die verwendete Hash-Funktion eingetragen. Der private Schlüssel wird niemals weitergegeben, auch nicht ans TC.
Die kryptographische Information ermöglicht einem Kommunikationspartner einerseits, eine abhörsichere Verbindung zum Zertifikatsinhaber aufzubauen, andererseits kann der Inhaber eigene Nachrichten mit der Funktion

$$S(M, I) = c(h(M), K^I_{Priv}) \tag{7}$$

Kryptographische Informationen (AHC, AC, PC, TCC)	
Krypt. Algorithmus	Name des kryptographischen Algorithmus $c()$, i.A. RSA.
K_{Pub}	Öffentlicher Schlüssel des Inhabers.
Hash-Funktion	Name der Hash-Funktion $h()$.
Administrative Informationen (AC, PC, TCC, teilweise AHC)	
Typ	Zertifikatstyp [AHC | AC | PC | TCC]
Zertifikats-ID	Innerhalb eines Herausgebers eindeutige Zertifikatsnummer (bei AC, PC und TCC). In AHC enthalten, aber nicht eindeutig.
Gültigkeitsdauer	Zertifikat ist nach Ablauf ungültig. Nicht in AHC.
Aussteller	Name des ausstellenden Trust Centers. Nicht in AHC.
URL des Ausstellers	URL des ausstellenden Trust Centers. Nicht in AHC.
Besitzerdaten (PC, TCC)	
Registriert von	TC-internes Kürzel, wer die Daten geprüft hatte.
ID-Typ	Art des Identifikationsmerkmales (z.B. Personalausweis).
ID-Wert	Wert des Identifikationsmerkmales (z.B. Ausweisnummer).
Vorname	Vorname des Antragstellers.
Nachname	Nachname des Antragstellers.
Unternehmen	Optionaler Name des Unternehmens.
Adresse	Adresse der Person oder des Unternehmens: Land, Stadt, Postleitzahl, Straße, Hausnummer. Optional E-Mail, Telefon, URL.
Signatur des Trust Centers (AC, PC, TCC)	
Signatur $c(h(Z^I), K^T_{Priv})$	Signatur des Zertifikates durch das ausstellende TC, beweist Korrektheit.

Tabelle 2: Datenfelder der Zertifikate

signieren. Der Empfänger kann die Echtheit über den Test auf $c(S(M,I),K^I_{Pub}) = h(M)$ nachweisen. Die kryptographischen Informationen können für Signatur und Abhörschutz jeweils nur in eine Richtung genutzt werden, für bidirektionale Sicherheit müssen beide Teilnehmer ihre Zertifikate austauschen.

Administrative Informationen: Ein weiterer Informationsblock enthält den Namen des ausstellenden TC, dessen URL und eine Gültigkeitsdauer. Diese Informationen tragen nicht zur kryptographischen Sicherheit bei, sondern liefern Informationen zur Prüfung von Vertrauenswürdigkeit und Gültigkeit. Für die Zuordnung zu einem Teilnehmer enthält der Block eine Zertifikats-ID und den Zertifikatstypen.

Anhand des TC-Namens erkennt der Empfänger, wie die Signatur des TC zu prüfen ist. Die URL wird zur Prüfung des Zertifikates nicht benötigt, allerdings kann der Empfänger hierüber zusätzliche Informationen wie aktuelle Sperrlisten anfordern. Ist das Gültigkeitsdatum des Zertifikates überschritten, so darf es nicht weiter verwendet werden und kann gelöscht werden.

Besitzerdaten: In einigen Szenarien ist die Erkennung des Kommunikationspartners als natürliche oder juristische Person wichtig. Dies ist nötig, wenn ein Unternehmen von seinen Kunden identifiziert werden sollte (z.B. als Schutz vor Phishing) oder wenn Transaktionen zum Austausch von Geld oder Gütern ansonsten mit einem unangemessenen Risiko verbunden wären.

Besitzerdaten enthalten den natürlichen Namen und die Adresse des Beantragenden sowie mindestens ein Erkennungsmerkmal (z.B. die Personalausweisnummer). Zusätzlich können der Unternehmensname und Informationen zur Erreichbarkeit, wie E-Mail, URL oder Telefon, eingetragen werden.

Diese Daten müssen vor der Zertifizierung auf Korrektheit geprüft werden. Zur späteren Nachvollziehbarkeit trägt das TC ein Kürzel des Prüfers ein.

Signatur des Trust Centers: Das ausstellende TC bestätigt die Korrektheit der Daten, indem es diese mit seinem privaten Schlüssel signiert. Zuvor müssen diese daher vom TC auf Korrektheit geprüft werden. Die Signatur kann durch den öffentlichen Schlüssel des TC von jedem geprüft werden. Alle enthaltenen Datenblöcke werden gemeinsam signiert.

5 Verbindungsaufbau und Verifizierung

5.1 Zertifikatsaustausch

Zertifikate enthalten nur öffentliche Daten und brauchen im Allgemeinen nicht als Schutz vor Abhörung verschlüsselt werden. Im Gegensatz zum Internet werden Zertifikate in ambienten Systemen wie iCity jedoch dort eingesetzt, wo sich der Inhaber befindet. Beobachter könnten also einen Zusammenhang zwischen Zertifikat, gesehener Person und Situation herstellen. Es empfielt sich darum, ACs und PCs auf einer bereits durch ein AHC gesicherten Verbindung zu übertragen, so dass nur der Kommunikationspartner die Besitzerdaten und die Zertifikats-ID lesen kann.

Da ihre Echtheit durch die Signatur des TC nachgewiesen wird, brauchen sie

nicht von Vertrauenswürdigen Stellen übermittelt werden.
Jeder Teilnehmer ist im Besitz seiner eigenen Zertifikate, deshalb bietet es sich an, Zertifikate zu Beginn einer Kommunikation auszutauschen. Wurde ein Zertifikat bereits in einer früheren Sitzung übertragen und ist die Gültigkeitsdauer noch nicht abgelaufen, so braucht es nicht erneut übertragen werden. Der Kommunikationspartner kann Zertifikate speichern, um die Echtheit von Nachrichten auch später noch nachweisen zu können.

5.2 Prüfung der Echtheit des Zertifikates

Dem Zertifikat wurde vom ausstellenden Trust Center eine Signatur

$$S(Z,T) = c(h(Z), K^T_{Priv}) \tag{8}$$

angehängt. Diese Signatur kann durch den öffentlichen Schlüssel des TC entschlüsselt und mit dem Hash-Wert der Nachricht verglichen werden [5]:

$$c(S(Z,T), K^T_{Pub}) = h(Z) \tag{9}$$

Hierfür muss der prüfende Kommunikationspartner, also i.A. nicht der Inhaber, dem ausstellenden TC vertrauen und über dessen Zertifikat verfügen. Dies ist offensichtlich nicht bei Ad-Hoc Zertifikaten und nicht bei initialen Trust Center Zertifikaten möglich. Initiale TCC müssen deshalb vor unbefugtem Zugriff auf das mobile Endgerät geschützt werden. Insbesondere nach Hacker-Angriffen auf das Betriebssystem oder Diebstahl könnten diese manipuliert werden.

5.3 Verifizierung des Inhabers

Die Echtheit eines Zertifikates kann zwar sofort geprüft werden, trotzdem sollte der Inhaber den Besitz des geheimen Schlüssels vor der Kommunikation nachweisen. Ansonsten könnte ein Angreifer zuvor mitgezeichnete Datenpakete, die korrekt mit dem geheimen Schlüssel signiert wurden, als Repeater-Angriff erneut senden.
Zur Prüfung des Inhabers I erzeugt der Kommunikationspartner A eine Zufallszahl M_{Rand}. Diese verschlüsselt er mit dem öffentlichen Schlüssel des Zertifikatinhabers:

$$M^{K^I_{Pub}}_{Rand} = c(M_{Rand}, K^I_{Pub}) \tag{10}$$

Das Ergebnis sendet er an den Zertifikatsinhaber. Dieser entschlüsselt die Nachricht mit seinem geheimen Schlüssel und sendet sie als Klartext an den Absender zurück:

$$M'_{Rand} = c(M^{K^I_{Pub}}_{Rand}, K^I_{Priv}) \tag{11}$$

Ist die Zahl gleich der ursprünglichen Zufallszahl, so handelt es sich um den Inhaber.

Alternativ könnte das Zertifikat geprüft werden, indem eine Zufallszahl in Klartext übertragen wird und vom Zertifikatsinhaber mit K^I_{Priv} chiffriert wird. Diese muss mit K^I_{Pub} entschlüsselt die ursprüngliche Zahl ergeben. Im Gegensatz zur oben vorgeschlagenen Abfolge könnte ein Angreifer hierdurch aber auch gezielt Inhalte verschlüsseln lassen, um an die zugehörige mit K^I_{Priv} chiffrierte Nachricht zu gelangen.

5.4 Sperrung Korrumpierter Zertifikate

Trotz kryptographischer Sicherheit sind Angriffe auf die PKI denkbar. Ein Teilnehmer könnte durch nicht-technische Angriffe (z.B. Diebstahl) oder durch äußere Sicherheitsmängel (Trojaner, Mängel des Betriebssystems) seinen geheimen Schlüssel einem Angreifer preisgeben. Später abgesendete oder zuvor mitgezeichnete Nachrichten können vom Angreifer gelesen werden, oder er kann sich als Inhaber des Zertifikates ausgeben. Während das TC die Korrektheit eines Zertifikates beweisen kann, ohne dass zu diesem während der Verbindung ein Kontakt nötig ist, können Zertifikate nicht offline entzogen werden.
Nachfolgend wird die Sperrung von Zertifikaten über eine Newsgroup-ähnliche Aktualisierung von Sperrlisten beschrieben. Dieser Ansatz kann jedoch nicht garantieren, ob und wann ein Teilnehmer von der Sperrung erfährt.
PC und AC können gesperrt werden, falls der Inhaber selbst noch über den geheimen Schlüssel verfügt und sich somit als Besitzer identifizieren kann. PC können auch über Prüfung des Identifikationsmerkmales ohne den geheimen Schlüssel gesperrt werden. Verfügt der Inhaber eines AC (z.B. nach Diebstahl des Gerätes) nicht mehr über den Schlüssel, kann das Zertifikat nicht gesperrt werden; Eventuell wäre ein für Menschen verständliches, selbst gewähltes Sperrkennwort denkbar.
Gesperrte Zertifikate werden in einer Blacklist bei den TCs verwaltet. Dazu erzeugt das zuständige TC einen Sperrauftrag, der die ID des korrumpierten Zertifikates, die Gültigkeitsdauer und die Signatur des TC enthält. Dieser wird an alle TC weitergereicht.
Tritt ein PKI-Teilnehmer mit einem TC in Kontakt, werden alle aktuellen Sperreinträge übertragen. Liegt die Gültigkeitsdauer eines Eintrags in der Vergangenheit, so ist das zugehörige Zertifikat bereits abgelaufen und der Eintrag kann gelöscht werden.
Falls überwiegend mit Access Points kommuniziert wird, die über eine Online-Anbindung auf das TC zugreifen können, erhalten Teilnehmer sehr schnell die neuesten Listen. Allerdings kann der Zeitpunkt nicht garantiert werden. Der Ansatz geht von kurzen Blacklists aus, deren Aktualisierung keine Probleme hinsichtlich Speicherbedarf und Bandbreite verursachen.

5.5 Kommunikation und Echtheit von Nachrichten

Über die vorherigen Schritte können die Kommunikationspartner öffentliche Schlüssel austauschen und verifizieren, dass keine falsche Identität vorgetäuscht wird. Ein Angreifer wäre aber noch immer in der Lage, zuvor mitgeschriebene,

bereits signierte Nachrichten in das Gespräch einzustreuen oder Nachrichten zufällig zu verändern. Folgendes Kommunikationsprotokoll soll einen bidirektionalen, sicheren Kommunikationskanal mit Garantie für die Nachrichtenintegrität realisieren:

1. Die Teilnehmer tauschen ihre Zertifikate aus. Jeder erhält somit den öffentlichen Schlüssel des Partners.

2. Die Zertifikate werden wie in 5.2 beschrieben gegenseitig geprüft. Dabei erhält jeder von seinem Partner eine Zufallszahl M_{Rand}. Nun ist bekannt, ob der Partner tatsächlich Inhaber des Zertifikates ist.

3. Die Teilnehmer tauschen Updates der Blacklist aus. Nur Einträge, die dem Gegenüber unbekannt sind und deren Ablaufsdatum in der Zukunft liegt, werden übertragen.

4. Alle weiteren Nachrichten werden mit dem öffentlichen Schlüssel des Kommunikationspartners verschlüsselt, der Absender A sendet dem Empfänger B zu einer Nachricht M_d also nur die chiffrierte Nachricht:

$$M^{K^B_{Pub}} = c(M_d, K^B_{Pub}) \tag{12}$$

5. Jeder Nachricht wird eine Zufallszahl angehängt. Der ersten Nachricht wird M_{Rand} vorangestellt, jede weitere Nachricht bekommt die Zufallszahl ihres Vorgängers vorangestellt. Eine zuvor mitgeschriebene und wiederholte Nachricht eines Angreifers würde mit der falschen Zahl beginnen und wäre somit ungültig. Die Prüfzahlen können zugleich verwendet werden, um die korrekte Reihenfolge der Zahlen zu überprüfen.

6. Jede Nachrichten wird vom Absender signiert:

$$S(M^{K^B_{Pub}}, A) = c(h(M^{K^B_{Pub}}), K^A_{Priv}) \tag{13}$$

7. Der Empfänger überprüft die Signatur der Nachricht auf Korrektheit:

$$h(M^{K^B_{Pub}}) = c(S(M^{K^B_{Pub}}, A), K^A_{Pub}) \tag{14}$$

8. Der Empfänger entschlüsselt die Nachricht:

$$M_d = c(M^{K^B_{Pub}}, K^B_{Priv}) \tag{15}$$

9. Der Empfänger überprüft, ob die Prüfziffer am Beginn der Nachricht mit der Ziffer am Ende der vorherigen Nachricht übereinstimmt.

10. Schritt 3 bis 8 werden für alle weiteren Nachrichten wiederholt. Der Rückkanal wird analog gesichert.

Es ist möglich, das Zertifikat während der Kommunikation zu wechseln. Dazu müssen auf der bereits gesicherten Verbindung die ersten beiden Schritte mit dem neuen Zertifikat wiederholt werden, die weiteren Schritte erfolgen mit neuem Schlüssel. Hierdurch könnte sich ein Teilnehmer zunächst durch ein AHC verbinden und dann abhörsicher ein PC übertragen. Die Sicherheitsstufe einer Verbindung kann dadurch situationsabhängig zunehmen (z.B. Produktinformation mit AC, Kauf- und Zahlvorgang mit PC).

6 Anwendung der PKI in Beispielszenarien

Dieser Abschnitt zeigt, wie die in Abschnitt 1.2 vorgestellten Szenarien mit der iCity-PKI umgesetzt werden können.

Anonyme Informationsdienste: Der Dienstanbieter sendet dem Kunden ein PC zu. Dieser kann das Unternehmen dadurch eindeutig identifizieren, Betrugsversuche werden bei der Prüfung der Signatur sofort erkannt. Der Kunde antwortet mit einem AHC. Von nun an sind die öffentlichen Schlüssel der Kommunikationspartner bekannt, Nachrichten können nur vom echten Partner gelesen werden.

Registrierte und Kontextabhängige Dienste: Der Dienstanbieter identifiziert sich gegenüber dem Kunden mit einem PC, der Kunde mit einem AC. Da die Daten des Dienstanbieters öffentlich sind, gibt er zuerst sein Zertifikat aus. Durch die öffentlichen Schlüssel wird ein abhörsicherer Kanal aufgebaut. Die Kommunikation ist durch Signaturen beweisbar.

Personenbezogene Dienste: Beide Teilnehmer identifizieren sich mit einem PC. Der Dienstanbieter, dessen Identität öffentlich ist, beginnt mit der Übertragung seines Zertifikates. Das Zertifikat des Kunden, das persönliche Daten enthält, wird auf der geprüften, abhörsicheren Verbindung übertragen. Falls beide Teilnehmer natürliche Personen sind, kann die Übertragung der Zertifikate auf Anwendungsebene z.B. durch Übertragung einer von den Teilnehmern vereinbarten Kennummer autorisiert werden. Die Verbindung ist abhörsicher und in Bezug auf Teilnehmer und Inhalt beweisbar.

Anonyme Peer-to-Peer Dienste: Beide Teilnehmer verwenden ein für die Kommunikation erzeugtes AHC zur Verschlüsselung der Verbindung. Dieses ist während des Austauschs für MITM-Angriffe anfällig: Gelingt es einem Angreifer, während des Zertifikatsaustauschs beiden Teilnehmern sein eigenes Zertifikat zu übertragen und den echten Partner vom Empfang abzuhalten, so kann er Nachrichten mithören und manipulieren. Die Nutzer müssen sich darüber bewusst sein, in einem vollkommen anonymen Szenario auch keine Garantien über die Sicherheit zu bekommen. Ein Angriff ist erschwert, da sich beide Teilnehmer bewegen, im Allgemeinen Sichtkontakt haben und eine Störung der Funkverbindung ohne Verlust der eigenen Verbindung für einen Angreifer schwierig ist.

7 Fazit

Die vorgestellte PKI ermöglicht abhörsichere, beweisbare, fälschungssichere Ende-zu-Ende oder sogar Person-zu-Person Verbindungen. Vor Absicherung des Kanals werden lediglich öffentliche Informationen ausgetauscht. Unterschiedliche Sicherheitsstufen lassen verschiedene Abwägungen zwischen Sicherheit und Anonymität zu. Die Teilnehmer benötigen zu einem beliebigen Zeitpunkt vor ihrem Nachrichtenaustausch eine Verbindung zu einem gemeinsam vertrauenswürdigen Trust Center. Während des Verbindungsaufbaus und der Kommunikation ist keine Verbindung zum TC nötig. Ausgetauschte Nachrichten lassen sich auch im Nachhinein anhand eines Zertifikates prüfen. Auch hierfür ist keine Verbindung zum TC nötig.

Literatur

[1] Bundesministerium der Justiz: Bundesdatenschutzgesetz (BDSG). (August 2006)

[2] Becher, S., Laue, P., Maidl, M., Modsching, M.: Die Datenschutz- und sicherheitskonforme Ausgestaltung von Location Based Services am Beispiel eines mobilen Touristenführers. Mobilität und mobile Informationssysteme 2007 (MMS) (March 2007) 86–96

[3] Phan, T.T.H., Dang, T.K.: An Extended Payment Model with Fair Non-Repudiation Protocols for M-Commerce. In: MoMM'2007 - The Fifth International Conference on Advances in Mobile Computing and Multimedia. (2007) 227–232

[4] Hiltgen, A., Kramp, T., Weigold, T.: Secure Internet Banking Authentication. IEEE Security & Privacy **4**(2) (March 2006) 21–29

[5] U.S. Department of Commerce, National Institute of Standards and Technology: Digital Signature Standard (DSS). Federal Information Processing Standards Publication (186-2) (January 2000)

[6] Bundesnetzagentur: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten. (July 2005)

[7] Bundesnetzagentur: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen). Bundesanzeiger (13) (January 2009) 346 – 257

[8] Bundesnetzagentur: Elektronische Signatur (Online; Stand 2009-04-06 18:25:00 +0200)
http://www.bundesnetzagentur.de/media/archive/4565.ppt

[9] Giessmann, E., Lippert, M., Bundesnetzagentur, T-Systems: Trustcenter Bundesnetzagentur – Realisierung Übersignaturkomponente. **2** (March 2008)

[10] Bundesministerium der Justiz: Gesetz über Rahmenbedingungen für elektronische Signaturen (SiG). (Oktober 2007)

[11] Bundesministerium der Justiz: Verordnung zur elektronischen Signatur (Signaturverordnung – SigV). (November 2007)

[12] Furbach, U., Maron, M., Read, K.: Location Based Informationsystems. KI - Künstliche Intelligenz (3/2007) (Juli 2007) 64–67

[13] Maron, M., Read, K.: CAMPUS NEWS - an Intelligent Bluetooth-based Mobile Information Network. (September 2007)

[14] Maron, M., Read, K., Schulze, M.: CAMPUS NEWS - Artificial Intelligence Methods Combined for an Intelligent Information Network. Constructing Ambient Intelligence **11** (2008) 44–52

[15] University of Koblenz, Artificial Intelligence Research Group: Campus News - an Intelligent Bluetooth-based Mobile Information System (Online; Stand 2009-02-26 17:15:17 +0100)
`http://campusnews.uni-koblenz.de`

[16] U. Furbach, Maron, M., Read, K.: Information Systems for Spatial Metro. Street-Level Desires – Discovering the City on Foot. Delft University of Technology, Department of Urbanism (2008)

[17] Maron, M., Magnus, S., Read, K.: An empirical study to evaluate the location of advertisement panels by using a mobile marketing tool. Mobile Business, International Conference on **0** (2009) 196–202

[18] Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM **21** (1978) 120–126

[19] National Institute of Standards and Technology: Announcing the Secure Hash Standard. Federal Information Processing Standards Publication **180–2** (August 2002)

[20] Kelm, S.: PKI-Page: Auflistung der Certification Authorities (Online; Stand 2009-01-26 14:43:00 +0200)
`http://www.pki-page.org/`

[21] Bundesnetzagentur: Certification-Service Providers (CSP) (Online; Stand 2009-03-12 17:20:00 +0200)
`http://www.bundesnetzagentur.de/enid/`
`5246b9ffeea3c837a0d5808acc329fc5,0/Electronic_Signature/`
`Certification-Service_Providers_2u2.html`

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik

(http://www.uni-koblenz.de/fb4/publikationen/arbeitsberichte)

Sebastian Magnus, Markus Maron, Konzept einer Public Key Infrastruktur in iCity, Arbeitsberichte aus dem Fachbereich Informatik 12/2009

Sebastian Magnus, Markus Maron, A Public Key Infrastructure in Ambient Information and Transaction Systems, Arbeitsberichte aus dem Fachbereich Informatik 11/2009

Ammar Mohammed, Ulrich Furbach, Multi-agent systems: Modeling and Virification using Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 10/2009

Andreas Sprotte, Performance Measurement auf der Basis von Kennzahlen aus betrieblichen Anwendungssystemen: Entwurf eines kennzahlengestützten Informationssystems für einen Logistikdienstleister, Arbeitsberichte aus dem Fachbereich Informatik 9/2009

Gwendolin Garbe, Tobias Hausen, Process Commodities: Entwicklung eines Reifegradmodells als Basis für Outsourcingentscheidungen, Arbeitsberichte aus dem Fachbereich Informatik 8/2009

Petra Schubert et. al., Open-Source-Software für das Enterprise Resource Planning, Arbeitsberichte aus dem Fachbereich Informatik 7/2009

Ammar Mohammed, Frieder Stolzenburg, Using Constraint Logic Programming for Modeling and Verifying Hierarchical Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 6/2009

Tobias Kippert, Anastasia Meletiadou, Rüdiger Grimm, Entwurf eines Common Criteria-Schutzprofils für Router zur Abwehr von Online-Überwachung, Arbeitsberichte aus dem Fachbereich Informatik 5/2009

Hannes Schwarz, Jürgen Ebert, Andreas Winter, Graph-based Traceability – A Comprehensive Approach. Arbeitsberichte aus dem Fachbereich Informatik 4/2009

Anastasia Meletiadou, Simone Müller, Rüdiger Grimm, Anforderungsanalyse für Risk-Management-Informationssysteme (RMIS), Arbeitsberichte aus dem Fachbereich Informatik 3/2009

Ansgar Scherp, Thomas Franz, Carsten Saathoff, Steffen Staab, A Model of Events based on a Foundational Ontology, Arbeitsberichte aus dem Fachbereich Informatik 2/2009

Frank Bohdanovicz, Harald Dickel, Christoph Steigner, Avoidance of Routing Loops, Arbeitsberichte aus dem Fachbereich Informatik 1/2009

Stefan Ameling, Stephan Wirth, Dietrich Paulus, Methods for Polyp Detection in Colonoscopy Videos: A Review, Arbeitsberichte aus dem Fachbereich Informatik 14/2008

Tassilo Horn, Jürgen Ebert, Ein Referenzschema für die Sprachen der IEC 61131-3, Arbeitsberichte aus dem Fachbereich Informatik 13/2008

Thomas Franz, Ansgar Scherp, Steffen Staab, Does a Semantic Web Facilitate Your Daily Tasks?, Arbeitsberichte aus dem Fachbereich Informatik 12/2008

Norbert Frick, Künftige Anfordeungen an ERP-Systeme: Deutsche Anbieter im Fokus, Arbeitsberichte aus dem Fachbereicht Informatik 11/2008

Jürgen Ebert, Rüdiger Grimm, Alexander Hug, Lehramtsbezogene Bachelor- und Masterstudiengänge im Fach Informatik an der Universität Koblenz-Landau, Campus Koblenz, Arbeitsberichte aus dem Fachbereich Informatik 10/2008

Mario Schaarschmidt, Harald von Kortzfleisch, Social Networking Platforms as Creativity Fostering Systems: Research Model and Exploratory Study, Arbeitsberichte aus dem Fachbereich Informatik 9/2008

Bernhard Schueler, Sergej Sizov, Steffen Staab, Querying for Meta Knowledge, Arbeitsberichte aus dem Fachbereich Informatik 8/2008

Stefan Stein, Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld, Arbeitsberichte aus dem Fachbereich Informatik 7/2008

Matthias Bohnen, Lina Brühl, Sebastian Bzdak, RoboCup 2008 Mixed Reality League Team Description, Arbeitsberichte aus dem Fachbereich Informatik 6/2008

Bernhard Beckert, Reiner Hähnle, Tests and Proofs: Papers Presented at the Second International Conference, TAP 2008, Prato, Italy, April 2008, Arbeitsberichte aus dem Fachbereich Informatik 5/2008

Klaas Dellschaft, Steffen Staab, Unterstützung und Dokumentation kollaborativer Entwurfs- und Entscheidungsprozesse, Arbeitsberichte aus dem Fachbereich Informatik 4/2008

Rüdiger Grimm: IT-Sicherheitsmodelle, Arbeitsberichte aus dem Fachbereich Informatik 3/2008

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik 2/2008

Markus Maron, Kevin Read, Michael Schulze: CAMPUS NEWS – Artificial Intelligence Methods Combined for an Intelligent Information Network, Arbeitsberichte aus dem Fachbereich Informatik 1/2008

Lutz Priese,Frank Schmitt, Patrick Sturm, Haojun Wang: BMBF-Verbundprojekt 3D-RETISEG Abschlussbericht des Labors Bilderkennen der Universität Koblenz-Landau, Arbeitsberichte aus dem Fachbereich Informatik 26/2007

Stephan Philippi, Alexander Pinl: Proceedings 14. Workshop 20.-21. September 2007 Algorithmen und Werkzeuge für Petrinetze, Arbeitsberichte aus dem Fachbereich Informatik 25/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS – an Intelligent Bluetooth-based Mobile Information Network, Arbeitsberichte aus dem Fachbereich Informatik 24/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS - an Information Network for Pervasive Universities, Arbeitsberichte aus dem Fachbereich Informatik 23/2007

Lutz Priese: Finite Automata on Unranked and Unordered DAGs Extented Version, Arbeitsberichte aus dem Fachbereich Informatik 22/2007

Mario Schaarschmidt, Harald F.O. von Kortzfleisch: Modularität als alternative Technologie- und Innovationsstrategie, Arbeitsberichte aus dem Fachbereich Informatik 21/2007

Kurt Lautenbach, Alexander Pinl: Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 20/2007

Rüdiger Grimm, Farid Mehr, Anastasia Meletiadou, Daniel Pähler, Ilka Uerz: SOA-Security, Arbeitsberichte aus dem Fachbereich Informatik 19/2007

Christoph Wernhard: Tableaux Between Proving, Projection and Compilation, Arbeitsberichte aus dem Fachbereich Informatik 18/2007

Ulrich Furbach, Claudia Obermaier: Knowledge Compilation for Description Logics, Arbeitsberichte aus dem Fachbereich Informatik 17/2007

Fernando Silva Parreiras, Steffen Staab, Andreas Winter: TwoUse: Integrating UML Models and OWL Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 16/2007

Rüdiger Grimm, Anastasia Meletiadou: Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen, Arbeitsberichte aud dem Fachbereich Informatik 15/2007

Ulrich Furbach, Jan Murray, Falk Schmidsberger, Frieder Stolzenburg: Hybrid Multiagent Systems with Timed Synchronization-Specification and Model Checking, Arbeitsberichte aus dem Fachbereich Informatik 14/2007

Björn Pelzer, Christoph Wernhard: System Description:"E-KRHyper", Arbeitsberichte aus dem Fachbereich Informatik, 13/2007

Ulrich Furbach, Peter Baumgartner, Björn Pelzer: Hyper Tableaux with Equality, Arbeitsberichte aus dem Fachbereich Informatik, 12/2007

Ulrich Furbach, Markus Maron, Kevin Read: Location based Informationsystems, Arbeitsberichte aus dem Fachbereich Informatik, 11/2007

Philipp Schaer, Marco Thum: State-of-the-Art: Interaktion in erweiterten Realitäten, Arbeitsberichte aus dem Fachbereich Informatik, 10/2007

Ulrich Furbach, Claudia Obermaier: Applications of Automated Reasoning, Arbeitsberichte aus dem Fachbereich Informatik, 9/2007

Jürgen Ebert, Kerstin Falkowski: A First Proposal for an Overall Structure of an Enhanced Reality Framework, Arbeitsberichte aus dem Fachbereich Informatik, 8/2007

Lutz Priese, Frank Schmitt, Paul Lemke: Automatische See-Through Kalibrierung, Arbeitsberichte aus dem Fachbereich Informatik, 7/2007

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 6/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß, „grUML – Eine UML-basierte Modellierungssprache für T-Graphen", Arbeitsberichte aus dem Fachbereich Informatik, 5/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 4/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik, 3/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik, 2/2007

Anastasia Meletiadou, J. Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe"
(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005