# Sicherheitsaspekte in NEXUS – einer Plattform für ortsbezogene Anwendungen

## Security Aspects of NEXUS – A Platform for Spatially Aware Applications

Christian Hauser, Alexander Leonhardi, Paul J. Kühn, Universität Stuttgart

Die Verbreitung ortsbezogener Dienste bedroht die Privatsphäre der Benutzer in einer neuen Weise. Das Bilden eines hochgenauen Profils der Ortsinformation lässt häufig Rückschlüsse auf aktuelle Tätigkeit und Vorlieben eines Benutzers zu. Da die entsprechenden Dienste zur Erbringung ihrer Funktionalität auf die Verfügbarkeit genauer Ortsinformation angewiesen sind, muss der Benutzer in der Lage sein, den Zugriff auf diese Information nach seinen Bedürfnissen zu erlauben bzw. einzuschränken. Darüber hinaus darf es nicht möglich sein, ohne seine Zustimmung die Ortsinformation mit seiner Identität zu verknüpfen. In diesem Artikel wird nach einer kurzen Einführung auf die Datenhaltung hochgenauer Ortsinformation sowie die damit verbundene Sicherheitsproblematik eingegangen. Danach werden Möglichkeiten zum Schutz sowohl der Ortsinformation als auch der Identitätsinformation aufgezeigt und abschließend diskutiert.

Deployment of location-based services constitutes a new threat to a user's privacy. Creating an exact location profile often permits inference of the user's activity and preferences. As these services need exact location information to provide their functionality, a user has to be able to allow or restrict the access to his location information. Furthermore, correlation of his location information with his identity must not be possible without his explicit consent. After an introduction to data management of exact location information, security problems of location-based services will be outlined in this article. Finally, possibilities for protecting location information as well as identity information will be described and discussed.

## 1 Einleitung

Für die Benutzer mobiler Datendienste entstehen zur Zeit eine Reihe interessanter neuartiger Anwendungen durch die Einbeziehung der aktuellen Position ihrer mobilen Endgeräte (Mobiltelefone, PDAs). Diese so genannten ortsbezogenen Dienste (engl. *Location Based Services*, LBS) bieten ihre Informationen abhängig von der aktuellen geografischen Position ihrer Benutzer an; in [3] ist beispielsweise ein Stadtführer mit Ortsbezug beschrieben. Diese Dienste können einen Benutzer beispielsweise auf eine günstige Busverbindung an einer nahegelegenen Haltestelle aufmerksam machen oder ihn nach dem nächsten Restaurant suchen lassen, das ein bestimmtes Gericht auf der Speisekarte hat. Gerade für die aufkommende dritte Mobilfunkgeneration wird für solche ortsbezogenen Datendienste ein großes Potenzial vorhergesagt.

Bei den Ortsinformationen, die ein solches System verarbeiten muss, handelt es sich um äußerst sensitive Informationen. So kann beispielsweise über die Ortsinformation auf die aktuelle Tätigkeit eines Benutzers geschlossen werden (z. B. vor welchen Schaufenstern er bei einem Stadtbummel stehen bleibt). Durch die Beobachtung der Ortsinformationen über einen längeren Zeitraum hinweg kann somit ein sehr detailliertes Profil seiner Gewohnheiten erstellt werden. Ein Beispiel für einen entsprechenden Angriff ist, dass aus dem Aufenthaltsort von Spitzenmanagern auf den Stand wichtiger Fusionsgespräche geschlossen werden kann.

Die Sicherheitsproblematik von Ortsinformationen wird sich mit der zukünftig zu erwartenden höheren Genauigkeit der gespeicherten Ortsinformationen und der weiteren Verbreitung solcher Dienste noch deutlich verschärfen. Es ist zu erwarten, dass die Ak-

 

zeptanz von LBS stark davon abhängen wird, ob die vertrauliche Behandlung der Ortsinformationen garantiert ist. Es muss also von Seiten der LBS aus ein schlüssiges Konzept für eine Zugriffskontrolle und die Garantie des Datenschutzes erbracht werden.

Das fakultätsübergreifende Forschungsprojekt NEXUS an der Universität Stuttgart hat zum Ziel, Basiskonzepte und eine verteilte Systeminfrastruktur für ortsbezogene Dienste zu schaffen. Es stellt diesen dazu ein erweitertes Modell (engl. *Augmented World Model,* AWM) ihrer Umgebung zur Verfügung, das Repräsentanten für reale statische (z. B. Häuser oder Bäume) und mobile Objekte (z. B. Personen oder Fahrzeuge) beinhaltet. Daneben enthält es auch virtuelle Objekte, wie beispielsweise virtuelle Litfasssäulen [13], die Orte und Objekte der realen Welt mit Informationen oder Diensten auch aus externen Informationsräumen wie dem WWW verknüpfen.

Innerhalb der NEXUS-Plattform sind die statischen Daten verteilt auf so genannten *Spatial Model Servern* gespeichert, die jeweils einen räumlichen und thematischen Ausschnitt des Umgebungsmodells verwalten. Die dynamischen Ortsinformationen mobiler Objekte, die durch entsprechende Positionierungssensoren – wie einen GPS-Empfänger – oder aus der Mobilkommunikationsinfrastruktur bestimmt werden, werden hingegen mit hoher Genauigkeit separat in einem verteilten Lokationsdienst gespeichert (siehe unten). Eine Föderationsschicht stellt ortsbezogenen Diensten eine einheitliche Schnittstelle und Beschreibungssprache für den Zugriff auf das AWM zur Verfügung, indem sie entsprechende Anfragen an die zuständigen Server weiterleitet und die zurückgelieferten Teilergebnisse integriert (siehe [16] für Details). Mit der speziellen Problematik der Verwaltung von Straßendaten im AWM beschäftigt sich ein weiterer Artikel dieser Ausgabe [19].

In diesem Artikel werden ausgehend vom NEXUS-Lokationsdienst (LS) die Sicherheitsproblematiken behandelt, die bei einer zentralen Speicherung von Ortsinformationen auftreten. Es werden darauf folgend Mechanismen vorgestellt, die eine flexible und effektive Zugriffskontrolle für die im LS gespeicherten Ortsinformationen ermöglichen. Zusätzlich können die zu einem mobilen Objekt gespeicherten Ortsinformationen unter verschiedenen Pseudonymen bekannt gemacht werden, was verhindert, dass die von verschiedenen Klienten abgefragten Ortsinformationen durch einen Angreifer aggregiert werden. Insgesamt zeigen diese Mechanismen, dass ein effektiver und praktikabler Schutz von Ortsinformationen möglich ist.

Der Artikel ist im Weiteren folgendermaßen aufgebaut: Abschnitt 2 beschreibt die Funktionalität des NEXUS-Lokationsdienstes. Mit der daraus resultierenden Sicherheitsproblematik befasst sich Abschnitt 3 und Abschnitt 4 diskutiert verwandte Arbeiten. Abschnitt 5 schlägt eine flexible Zugriffskontrolle für den Lokationsdienst vor und Abschnitt 6 einen Mechanismus, mit dem ein Benutzer seine Ortsinformationen unter verschiedenen Pseudonymen bekannt machen kann. Kapitel 7 beschließt diesen Artikel mit einer Zusammenfassung und einem Ausblick.

## 2 Funktionalität des NEXUS-Lokationsdiensts

Vor der Diskussion der Sicherheitsproblematiken, die sich aus der zentralen Speicherung der Ortsinformationen ergeben, soll hier zuerst kurz die Funktionalität und Architektur des NEXUS-Lokationsdienstes beschrieben werden, der diesen Betrachtungen zugrunde liegt.

Das Anwendungsprogramm eines mobilen Benutzers, mit dem dieser auf ortsbezogene Dienste zugreift, registriert seine Ortsinformation zu diesem Zweck mit einer vom Benutzer vorgegebenen Genauigkeit unter Verwendung der Operation *register* beim LS. Danach aktualisiert es die Ortsinformationen gemäß der eingestellten Genauigkeit mittels der Operation *update* (für eine Betrachtung geeigneter Aktualisierungsprotokolle siehe [14]). Durch die Operation *deregister* kann es ein Objekt wieder beim LS abmelden (siehe Bild 1).

Ortsbezogene Dienste (z. B. ein Navigationsdienst) können daraufhin die Ortsinformationen der mobilen Objekte beim LS auf verschiedene Arten abrufen. Mit einer Positionsanfrage wird die aktuelle Position eines bestimmten mobilen Objekts abgefragt (*positionQuery*). Dabei könnte es sich beispielsweise um die aktuelle Positionen eines Mitglieds der Reisegruppe des Benutzers handeln. Anstatt von einem bestimmten mobilen Objekt gehen Gebiets- und Nachbarschaftsanfragen von einem geografischen Gebiet oder Ort aus. Eine Gebietsanfrage (*rangeQuery*)

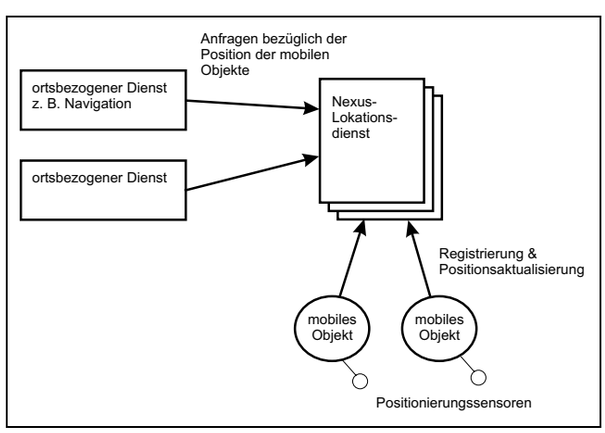


**Bild 1:** Funktion des NEXUS-Lokationsdienstes.

liefert alle mobilen Objekte zurück, die sich innerhalb eines angefragten Gebiets befinden und kann beispielsweise dazu verwendet werden, um die Ortsinformationen für alle mobilen Objekte zu erhalten, die auf einer Karte angezeigt werden sollen. Eine Nachbarschaftsanfrage (*neighborQuery*) gibt schließlich das nächste mobile Objekt zu einer bestimmten Position zurück, zum Beispiel das nächstgelegene (freie) Taxi.

Um die letzten zwei Operationen bearbeiten zu können, ist eine zentrale Datenhaltung der Ortsinformationen, wie sie durch den LS realisiert ist, unbedingt notwendig. Dies wird noch verschärft, wenn – wie geplant – der LS einen Ereignismechanismus beinhalten soll, mit dem der LS einen Klienten über das Eintreten eines bestimmten Ereignisses (z. B. wenn ein mobiles Objekt ein bestimmtes Gebiet betreten hat) benachrichtigt, wenn dieser vorher sein Interesse für dieses Ereignis angemeldet hat.

Da der NEXUS-Lokationsdienst innerhalb der NEXUS-Plattform einerseits die Ortsinformationen einer großen Zahl von mobilen Objekten verwalten muss und andererseits die gespeicherten Ortsinformationen mit hoher Genauigkeit vorliegen sollen, ist eine effiziente und verteilte Realisierung des LS von großer Bedeutung. In [15] ist die Architektur des verteilten LS im Detail beschrieben. Innerhalb dieser Architektur ist jeweils immer ein bestimmter Server für die Verwaltung der Registrierungs- und Ortsinformationen eines mobilen Objekts zuständig, der damit auch die Zugriffskontrolle auf die Ortsinformationen durchführt.

## 3 Sicherheitsprobleme ortsbezogener Systeme

Im Bereich der GSM-Mobiltelefonie werden heute bereits erste ortsbezogene Dienste angeboten. In diesem Bereich wird seit längerem bereits eine Diskussion über die Gefahr gespeicherter Ortsinformation geführt, siehe u. a. [7].

Das im Forschungsprojekt NEXUS diskutierte Szenario weist allerdings einige Unterschiede zu den Location-Based Services der GSM-Anbieter auf, die darauf schließen lassen, dass derartige Konzepte ohne weitergehende Sicherheitsmechanismen deutliche Akzeptanzprobleme erleiden würden. So ist die Ortsinformation in GSM weitgehend zum Auffinden der mobilen Benutzer und zur Steuerung des Verbindungsaufbaus notwendig. Sie steht daher primär nur dem Mobilfunkbetreiber zur Verfügung, dem die Benutzer bezüglich korrekter Handhabung vertrauen müssen. Diese Ortsinformation wird jetzt teilweise auch für LBS benutzt, weist allerdings eine niedrige Genauigkeit auf.

In NEXUS ändern sich diese Randbedingungen. Es liegt Ortsinformation von verschiedenen Sensoren vor, welche im Lokationsdienst zur genauest möglichen Ortsinformation aggregiert wird. Darüber hinaus ist es in NEXUS explizit erwünscht, dass viele verschiedene Parteien die Ortsinformation der Benutzer abfragen dürfen. Neben den Diensten können auch Endanwender auf die eigene Ortsinformation oder die anderer Benutzer zugreifen. Der Aufenthaltsort eines Benutzers kann dabei unmittelbar über eine Anfrage direkt nach dessen Ort ermittelt werden, oder gegebenenfalls mittelbar über Anfragen nach dem Ort seines mobilen Geräts oder seines Autos geschlossen werden, da diese Objekte ebenfalls im NEXUS-LS erfasst sein können.

Der Benutzer, der die Hoheit über diese Objekte hat, wird Autorität der Objekte genannt. Im weiteren Verlauf dieses Artikels werden Anfragende, die Ortsinformation von Objekten abfragen, allgemein als Subjekte bezeichnet. Objekte können sowohl Benutzer als auch Dinge sein.

Jeder, der zeitlich unbeschränkten Zugang zu der hochgenauen Ortsinformation hat, kann prinzipiell ein genaues Ortsprofil einzelner Benutzer aufstellen. Dieses Ortsprofil kann darüber hinaus mit weiteren Daten angereichert werden, um ein differenziertes Persönlichkeitsprofil eines Benutzers zu erhalten. Im Zusammenhang mit LBS werden meist nicht nur die Ortsinformation kommuniziert, sondern auch andere Daten teils persönlicher Art. Damit wird die Ortsinformation in einen Kontext gesetzt und lässt genauere Schlüsse auf den jeweiligen Benutzer zu.

Aus dieser Darstellung wird ersichtlich, dass eine Ortsinformation alleine nicht gefährlich ist. Es muss zusätzliche Information mit dieser Ortsinformation verbunden werden, damit sie, im positiven wie im negativen Sinne, nutzbar wird. Dabei muss allerdings nicht unbedingt der Name des Benutzers bekannt sein. Oftmals genügt es, sonstiges auf den Benutzer bezogenes Wissen mit dem Ortsprofil in Verbindung zu bringen. Ein Beispiel hierfür ist die Korrelation des Bewegungsprofils eines unbekannten Kunden mit seinem Kaufverhalten in einem Kaufhaus.

Die Schutzanforderung an NEXUS bezieht sich daher auf die Kombination der Ortsinformation mit der Identität eines Benutzers. Um diese Kombination vor unautorisierter Aufdeckung zu schützen, gibt es prinzipiell zwei Möglichkeiten. Entweder kann die Aussagekraft der Ortsinformation reduziert werden oder die der Identitätsinformation.

Ortsinformation ist hierbei einfacher zu behandeln. Durch Reduktion der Genauigkeit wird die Aussagekraft geringer. Einfache Ansätze hierfür sind zum Beispiel die Angabe eines Rasterquadrates, in welchem sich der Benutzer aufhält, anstatt der ge-

nauen Information oder ein zufälliger Fehler, welcher der genauen Ortsinformation aufaddiert wird.

Ausgehend von diesen Mechanismen gibt es bezüglich des NEXUS-LS zwei Schutzmöglichkeiten. Der Benutzer kann entscheiden, dass er dem System nicht vertraut und daher von vornherein nur ungenaue Information in den LS geben. Diese Möglichkeit ist allerdings unflexibel, da beispielsweise ein vertrauenswürdiger Dienst keine genaue Ortsinformation vom LS beziehen kann und auf diese Weise die Funktionalität des gesamten Systems stark eingeschränkt ist. Daher ist es wünschenswert, dass die Benutzer ihre Ortsinformation mit maximaler Genauigkeit in den LS geben. Dieser muss im Folgenden die Aufdeckung der Genauigkeit regeln und hierzu eine Zugriffskontrolle (engl. *Access Control*, AC) implementieren. Dort wird je nach Berechtigung des Anfragenden die Genauigkeit der herausgegebenen Ortsinformation geregelt. Die Berechtigungen Dritter zum Zugriff auf Ortsinformation eines Benutzers müssen dabei jeweils durch diesen kontrollierbar sein.

Bei der zweiten Möglichkeit muss der Benutzer der Zugriffskontrolle bezüglich korrekter Funktion vertrauen. In besonders sensitiven Fällen kann er jedoch die beiden Schutzmöglichkeiten miteinander kombinieren, indem er dem LS zeitweise nur ungenaue oder keine Ortsinformation bereitstellt.

Die Reduktion der Aussagekraft einer Identitätsinformation birgt mehr Schwierigkeiten, da es keine mathematischen Verfahren gibt, diese Information mehr oder weniger zu verschleiern. Es kann jedoch einem Benutzer ermöglicht werden, mehrere Pseudonyme zu benutzen, über die jeweils nur ein Teil seines persönlichen Profils bekannt ist [8]. Es ist beispielsweise denkbar, dass im Kontext eines Pseudonyms eine temporäre IP-Adresse bekannt ist, im Kontext eines zweiten eine Email-Adresse und im Kontext eines dritten nur ein Liquiditätsnachweis für ein anonymes Zahlungssystem. Durch die Auswahl eines der drei Pseudonyme kann der Benutzer in gewisser Weise den Grad an Anonymität wählen. Insbesondere ist es wünschenswert, dass der LS über die sehr genaue Ortsinformation hinaus wenige Informationen über den Benutzer erfährt, um Missbrauchsmöglichkeiten einzuschränken.

Aus den aufgeführten Schutzmöglichkeiten lassen sich die Anforderungen an NEXUS bezüglich des Schutzes der Ortsinformationen ableiten. Der LS benötigt eine flexible Zugriffskontrolle, welche die Genauigkeit der aufgedeckten Ortsinformationen abhängig von der Berechtigung des authentifizierten Anfragenden regelt. Die Benutzer müssen hierbei jederzeit in der Lage sein, die Berechtigungen bezüglich ihrer Ortsinformation zu kontrollieren. Zum Schutz der Benutzeridentität muss nicht nur eine generelle pseudonyme Nutzung von NEXUS und insbesondere des LS ermöglicht werden, sondern es muss den Benutzern darüber hinaus die Möglichkeit eingeräumt werden, mehrere Pseudonyme zu benutzen. Ferner muss bei allen Betrachtungen zur Sicherheit immer auch die Benutzbarkeit des Systems beachtet werden. Im Hinblick auf den LS bedeutet dies vor allem die Wahrung der Leistungsfähigkeit trotz Zugriffskontrolle und evtl. Genauigkeitsreduktion. Eine Betrachtung dessen ist jedoch nicht Thema dieses Artikels.

## 4 Verwandte Arbeiten

In der Literatur finden sich Lösungsvorschläge sowohl für Zugriffskontrollen bezüglich Ortsinformation als auch für kontrollierte Aufdeckung persönlicher Information durch die Verwendung von Pseudonymen. Spreitzer und Theimer schlagen in [18] vor, einen Benutzeragenten, der unter Kontrolle des Benutzers ist, alle Anfragen nach dessen Ortsinformation bearbeiten zu lassen. Dies wäre für Positionsanfragen möglich, würde allerdings Gebietsanfragen und Nachbarschaftsanfragen erschweren, die elementare Bestandteile des NEXUS-LS sind. Leonhardt beschreibt in [12] eine Zugriffskontrolle für einen globalen LS mit flexibler Definition der Berechtigungen und statischer Zugriffskontrollliste (engl. *Access Control List*, ACL). Er kombiniert hierfür Konzepte einer mandatorischen und einer diskreten Zugriffskontrolle.

Gerd tom Markotten, Jendricke, Köhntopp und Pfitzmann haben u. a. mehrfache Untersuchungen bezüglich der Benutzung verschiedener Pseudonyme durchgeführt. In [8] und [10] wird ein Identitätsmanager vorgeschlagen, welcher den Benutzer anwendungsübergreifend bei der Wahl des jeweils verwendeten Pseudonyms unterstützt. Der Fokus in [8] liegt auf E-Commerce-Anwendungen, wobei der Benutzbarkeit des Systems eine große Bedeutung zugemessen wird.

Für NEXUS mit unterschiedlichst gearteten Diensten ist diese Lösung nicht ohne Weiteres möglich. Es würde über alle Anwendungen hinweg ein sehr detailliertes Profil des Benutzers entstehen, da unterschiedliche Anwendungen verschiedenste Informationen zu dem jeweiligen Pseudonym benötigen. In [11] werden Anonymität, Pseudonyme und Identitätsmanagement allgemein beleuchtet und diskutiert.

Der in der Literatur beschriebene Einsatz von Pseudonymen wird von uns mit den Prinzipien der *Simple Public Key Infrastructure* (SPKI/SDSI) [5], welche in folgendem Abschnitt am Beispiel des LS vorgestellt werden, kombiniert, um den Schutz der Kombination von Identitätsinformation und Ortsinformation sicherzustellen.

## 5 Zugriffskontrolle zur Regelung der Ortsinformation

Die Authentisierung der Anfragenden durch die Zugriffskontrolle im LS basiert auf asymmetrischer Kryptografie. Ein anfragendes Subjekt unterschreibt die Anfrage mit einer digitalen Signatur, welche es mit seinem privaten Schlüssel erzeugt. Anhand dieser Signatur kann die Zugriffskontrolle des LS die Korrektheit der Kennung des Anfragenden überprüfen und entscheiden, ob und in welcher Genauigkeit Zugriff auf die gewünschten Daten gewährt wird.

In diesem Abschnitt werden die wichtigsten Prinzipien von SPKI/SDSI vorgestellt und anhand der Zugriffskontrolle des NEXUS-LS erläutert. Im Einzelnen handelt es sich hierbei um Berechtigungszertifikate und die Verwendung von asymmetrischen Schlüsseln als Kennung der Beteiligten.

### 5.1 Berechtigungszertifikate

Berechtigungen der einzelnen Subjekte können der Zugriffskontrolle beispielsweise zentral durch einen Administrator bekannt gemacht werden, der eine Zugriffskontrollliste verwaltet. Durch die große Anzahl potenziell anfragender Subjekte und potenziell abzufragender Objekte in einem global angelegten System wie NEXUS wird diese Zugriffskontrollliste sehr groß, wodurch sich u. a. die Bearbeitungszeit verlängert. Bei jeder Änderung einer Berechtigung muss der Administrator zur Aktualisierung der Zugriffskontrollliste kontaktiert werden.

Zur Erleichterung der Verwaltung großer, zentraler Listen können Teile in eigene, dezentrale Dokumente ausgelagert werden. Für die Zugriffskontrollliste des LS bedeutet dies, dass die Autorität des betreffenden Objekts einem Subjekt ein digital unterschriebenes Zertifikat ausstellt, in welchem dessen genaue Berechtigung zertifiziert wird. Bei einer Anfrage muss dieses Zertifikat vom Subjekt vorgelegt werden. Die Zugriffskontrolle entscheidet auf dieser Basis, ob die Anfrage des Subjekts beantwortet werden darf. Die Berechtigung kann dort zwischengespeichert werden, wodurch neue Anfragen des berechtigten Subjekts schneller bearbeitet werden können, da eine erneute Überprüfung des Zertifikats entfallen bzw. vereinfacht werden kann. Bild 2 zeigt das Prinzip einer Anfrage mit angefügtem Berechtigungszertifikat.

Diese dezentrale Realisierung hat mehrere Vorteile. Die statischen Zugriffskontrolllisten können um einiges kleiner ausfallen, da in ihnen nur noch die Autoritäten stehen müssen, welche Berechtigungszertifikate ausstellen dürfen. In den meisten Fällen wird dies nur ein Benutzer sein, der die Berechtigung für die Ortsinformation seines Endgeräts verwaltet. Ferner vergrößern Berechtigungen, die nie benutzt werden,


**Bild 2:** Anfrage mit Berechtigungszertifikat.

die Zugriffskontrollliste nicht unnötigerweise. Darüber hinaus muss für Änderungen der Berechtigung kein zentraler Administrator kontaktiert werden. Der Weg der Berechtigung über das Zertifikat in die Zugriffskontrolle ist flexibel und kann sogar über unvertraute Parteien führen, da die Integrität des Zertifikats durch eine digitale Unterschrift gesichert ist und der Inhalt bei Bedarf verschlüsselt werden kann.

Auf diese Weise können neue Subjekte (z. B. Dienste) sehr schnell in das Szenario eingebunden werden. Die Autorität des Objekts stellt dem neuen Subjekt ein Berechtigungszertifikat aus und schon ist dieses prinzipiell in der Lage, die Ortsinformation des Objekts beim LS abzufragen.

### 5.2 Asymmetrische Schlüssel als Kennung

Um ein bestimmtes Subjekt unmissverständlich zu berechtigen, ist es notwendig, dieses in der Zugriffskontrollliste oder dem Zertifikat zu benennen. Hierzu muss eine global eindeutige Kennung verwendet werden, die dem Subjekt fest zugeordnet ist. Das am weitesten verbreitete Beispiel hierfür ist der Name des Subjekts, welcher durch Erweitern mit zusätzlicher Information global eindeutig gemacht werden kann, wie dies bei Email-Adressen realisiert ist.

Da die Zugriffskontrolle die Signatur der Anfrage mit dem öffentlichen Schlüssel des Subjekts prüft, muss dieser fest an das Subjekt gebunden sein. Auch diese Bindung wird meist über den Namen des Subjekts erreicht, welcher von einer globalen, unabhängigen Zertifizierungsinstanz (engl. *Certification Authority*, CA) überprüft und dessen Korrespondenz zu dem entsprechenden Schlüssel von ihr zertifiziert wird. Die Zugriffskontrolle des LS muss dabei der unabhängigen Zertifizierungsinstanz vertrauen und kann nach der Prüfung des Zertifikats die Berechtigung des zum Schlüssel gehörigen Namens im angehängten Berechtigungszertifikat oder der Zugriffskontrollliste nachsehen. Bild 3 zeigt den Fluss der Berechtigung von der Autorität des Objekts über den Namen zum Subjekt.

Die Verwendung des Namens als Kennung birgt allerdings mehrere Probleme. So ist es einerseits schwierig, global eindeutige Namen, welche für Benutzer noch aussagekräftig sind, festzulegen und zu zertifizieren. Andererseits sind Namen identifizierend und eine anonyme Nutzung daher nicht möglich. Da-

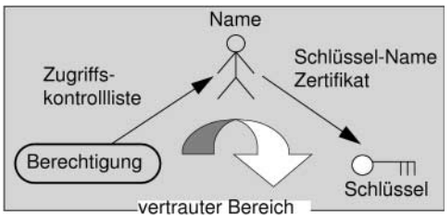


**Bild 3:** Autorisierung über Name.

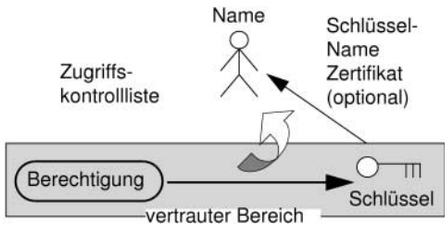


**Bild 4:** Autorisierung über Schlüssel.

rüber hinaus hängt die Entscheidung, ob einem Subjekt Zugriff gewährt werden soll, meist nicht von dessen Namen ab, sondern, gerade in einem globalen System wie NEXUS, in dem sich Benutzer häufig nicht persönlich kennen, von anderen Attributen des Subjekts. Beispiele hierfür sind die Attribute *Zahlungsfähigkeit* oder *Berechtigung des Zugriffs* auf Ortsinformation, die durch Zertifikate fest an das Subjekt gebunden werden können.

Um diese Probleme zu vereinfachen, liegt es nahe, direkt die asymmetrischen Schlüssel der Subjekte und Objekte als Kennung zu benutzen [4]. Der öffentliche Schlüssel kann als global eindeutig betrachtet werden und erfüllt damit die erste Bedingung einer geeigneten Kennung. Durch die direkte Kopplung zum zugehörigen privaten Schlüssel ist er darüber hinaus eng an den Inhaber dieses Schlüssels gebunden und erfüllt damit auch die zweite Bedingung.

Die Zugriffskontrolle des LS kann in diesem Fall direkt prüfen, ob mit dem berechtigten öffentlichen Schlüssel die Signatur der Anfrage überprüft werden kann – also ob das Berechtigungszertifikat tatsächlich den Anfragenden autorisiert – und ob gegebenenfalls die Unterschrift des Berechtigungszertifikats von einer Autorität stammt, die Berechtigungen für das betreffende Objekt ausstellen darf. Diese Autoritäten sind in der Zugriffskontrollliste aufgeführt und benutzen als Kennung ebenfalls öffentliche Schlüssel, so dass die Signatur des Berechtigungszertifikats wiederum direkt mit der Kennung der Autorität aus der Zugriffskontrollliste überprüft werden kann.

Im Entscheidungsprozess der Zugriffskontrolle kommt auf diese Weise nie der Name eines Benutzers ins Spiel. Das bedeutet einerseits, dass die Zugriffskontrolle pseudonym benutzbar wird – der öffentliche Schlüssel dient als Pseudonym – andererseits muss die Zugriffskontrolle keiner unabhängigen Namenszertifizierungsinstanz vertrauen. Die Vergabe der Berechtigungen kann ferner flexibel und dezentral ohne Einbindung eines zentralen Administrators erfolgen. Darüber hinaus ermöglichen die kleineren Zugriffskontrolllisten sowie das Entfallen der Kontaktierung der Zertifizierungsstelle eine schnellere Bearbeitung von Anfragen an den LS gegenüber einer Lösung mit Namenszertifikaten und statischen Zugriffskontrolllisten. Bild 4 zeigt den Fluss der Berechtigung in diesem Szenario. Aus Platzgründen muss für weitere Details auf die Literatur verwiesen werden [1; 2; 4; 5].

## 5.3 Skalierbarkeit

Gebietsanfragen an den LS werden durch die Verwendung von Berechtigungszertifikaten komplexer, da Berechtigungen für Objekte und nicht für Gebiete ausgestellt werden. Es genügt daher nicht, der Anfrage ein einzelnes Berechtigungszertifikat anzuhängen, sondern es müssten Zugriffsberechtigungen auf Ortsinformationen aller Objekte angehängt werden, die sich potenziell in diesem Gebiet befinden. Die große Anzahl anzuhängender Zertifikate wird von uns dadurch verringert, dass die Autorität eines Objekts bei der Registrierung im LS eine Standardgenauigkeit und eine Standardkennung für unberechtigte Anfragen angibt. Hierbei ist es möglich, die Sichtbarkeit komplett auszuschließen. Über diese Standardrechte hinaus kann ein anfragendes Subjekt gegebenenfalls Berechtigungen bezüglich Objekten angeben, an denen es speziell interessiert ist. Dadurch ist es möglich, von diesen Objekten genauere Information zu bekommen, siehe auch [9]. Um die Anzahl anzuhängender Zertifikate weiter zu verringern, bietet es sich an, benutzte Berechtigungen im LS teilweise zwischenzuspeichern. Werden sie zusammen mit dem Objektdatensatz im LS gespeichert, so sind sie bei jedem Anfragetyp sofort verfügbar, da der Objektdatensatz bei jeder Anfrage aufgefunden wird.

Dezentrale Infrastrukturen wie SPKI/SDSI bringen durch das Fehlen der zentralen Zertifizierungsinstanz grundsätzlich Schwierigkeiten bezüglich der Skalierbarkeit bei Rückruf (engl. *revocation*) von Berechtigungen mit sich. [5] nennt einige Verfahren zur Abhilfe. In unserem Szenario ist der Rückruf irrtümlich ausgestellter Berechtigungen allerdings kein Problem, da die Zugriffskontrolle des LS gewissermassen als zentrale Instanz wirkt. Will eine Autorität eine Berechtigung zurückziehen, so kann sie dem LS ein Rückrufzertifikat senden, das in die Zugriffskontrollliste bezüglich des entsprechenden Objekts eingetragen wird. Dieser Eintrag überschreibt evtl. bereits vorhandene oder während einer Anfrage neu eingereichte Berechtigungen. Rückrufzertifikate müssen

daher in der Zugriffskontrollliste während ihrer gesamten Gültigkeitsdauer gespeichert werden.

Eine Regelung der Aussagekraft der Identität ist allerdings durch Verwendung von Berechtigungszertifikaten noch nicht gut möglich. Die Benutzer können zwar mehr oder weniger persönliche Information an den öffentlichen Schlüssel binden, allerdings ist dies ein monotoner Vorgang. Einmal bekannt gewordene Information kann nicht mehr verborgen werden. Durch die dauernde Verwendung eines einzigen Pseudonyms (des Schlüssels) ist es daher für Angreifer möglich, das Profil stetig zu vergrößern. Deckt der Benutzer im Folgenden einmal seinen Namen oder eine sonstige identifizierende Information auf, so ist prinzipiell die komplette Datenspur des Pseudonyms verraten und mit ihm in Verbindung zu bringen. Im folgenden Abschnitt wird darauf eingegangen, wie es Benutzern ermöglicht wird, mehrere Pseudonyme zu verwenden und damit die Aufdeckung ihrer personenbezogenen Daten zu kontrollieren.

## 6 Unterschiedliche Pseudonyme zur Regelung der Identitätsinformation

Die Verwendung mehrerer Pseudonyme erbringt neben der oben angesprochenen Möglichkeit zur Regelung der Identitätsinformation auch die Grundlage zur Steuerung, welche Aktionen eines Benutzers verkettet werden dürfen und welche nicht. Will dieser beispielsweise die Verkettung einer neuen Aktion mit seinem bisherigen Nutzungsprofil durch einen Dienst vermeiden, so wählt er ein neues Pseudonym und meldet sich gegebenenfalls unter diesem zweiten Pseudonym als neuer Benutzer an. Bei geschickter Wahl des Pseudonyms weiß der Dienst nicht, dass beide Pseudonyme zu ein und derselben Person gehören.

Direkt nach der Erzeugung kann ein Pseudonym als anonyme Information angesehen werden, da es nichts anderes als eine Zeichenkette ist. Davon ausgehend kann es, zum Beispiel über Attributszertifikate, mit mehr oder weniger personenbezogener Information angereichert werden. Auf diese Weise kann ein Benutzer die Aufdeckung seiner Identitätsinformation regeln, wobei er allerdings vorsichtig mit der Herausgabe global eindeutiger oder gar seine Person identifizierender Daten sein muss. Wird beispielsweise im Kontext beider Pseudonyme die gleiche Mail-Adresse angegeben, so ist der Dienst in der Lage zu erschließen, dass beide Pseudonyme zu einer Person gehören. Ein anderes, weit verbreitetes Beispiel für diesen Mechanismus sind die so genannten „Cookies“ im WWW. Dies sind eindeutige Textketten, über die u. a. verschiedene Transaktionen eines Benutzers miteinander verkettet werden, selbst wenn sich dessen IP-Adresse jeweils ändert.

Ist ein Benutzer bei verschiedenen Subjekten unter verschiedenen Pseudonymen bekannt, so können auch diese nicht ohne weiteres die Daten, die sie über den Benutzer gesammelt haben, korrelieren, da ihnen der Zusammenhang zwischen den Pseudonymen verborgen ist. Eine Verkettung über global eindeutige Attribute der Pseudonyme ist hier allerdings ebenfalls möglich.

Der Lokationsdienst muss jedoch zu jedem Pseudonym die passende Ortsinformation finden können. Eine Möglichkeit wäre, jedes Pseudonym im LS zu registrieren und gesondert zu aktualisieren. Dies würde jedoch Nachteile bzgl. der Skalierbarkeit bringen, da die gleiche Information mehrfach zwischen Objekt und LS übertragen werden muss. Darüber hinaus wäre diese Duplizierung der sensitiven Ortsinformation prinzipiell eine Verletzung des Datensparsamkeitsprinzips. Der LS könnte durch die genaue Übereinstimmung der Spuren der verschiedenen Pseudonyme diese miteinander verketten.

Wir sehen daher vor, dass die Autorität eines Objekts eine oder mehrere verschiedene Referenzen auf die Ortsinformation eines Objektes erzeugen kann. Diese Referenz gibt sie Subjekten zur Abfrage beim LS. Die Subjekte sehen die vom LS gelieferte Ortsinformation somit unter der jeweiligen Referenz und können diese dem ihnen bekannten, lokalen Pseudonym des Objekts zuordnen. Die Referenzen sind dabei so realisiert, dass nur der LS diese aufeinander und auf die entsprechende Ortsinformation abbilden kann. Die Referenzen können nicht durch kollaborierende Subjekte miteinander korreliert werden. Der LS wiederum kann aus den Referenzen keine Rückschlüsse auf die lokale Sicht eines Subjektes auf ein Objekt (Pseudonym, weitere Informationen) ableiten.

Eine Realisierungsmöglichkeit für die Referenzen ist, dass die Autorität des Objekts das dem LS bekannte Pseudonym des Objekts zusammen mit einer zufälligen Information unter Zuhilfenahme des öffentlichen Schlüssels des LS verschlüsselt. Die zufällige Information muss für jede Referenz unterschiedlich sein, damit das Chiffrat ein eigenes Erscheinungsbild hat. Der LS kann die Referenz entschlüsseln und findet darin das Pseudonym, unter dem er die gewünschte Information in seiner Datenbank gespeichert hat. Die zufällige Information wird von ihm verworfen.

Bild 5 zeigt das prinzipielle Szenario mit einem Navigationsdienst „N“ und einem Ereignisdienst „E“, welche beide die Ortsinformation des Objekts mit der Identität „O“ abfragen dürfen. $\{xy\}_{LS}$ bedeutet hierbei, dass die Daten „xy“ mit dem öffentlichen

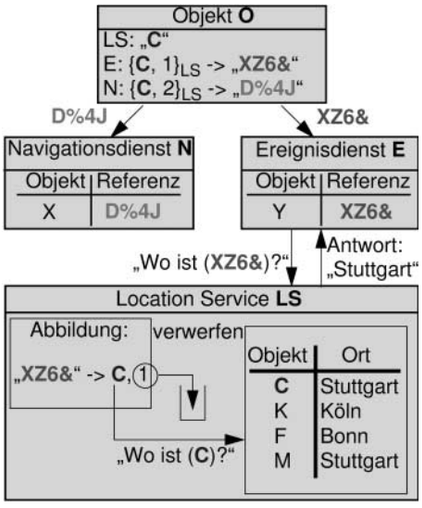


**Bild 5:** Ortsabfrage mit Referenzen.

Schlüssel des LS verschlüsselt werden. Die Berechtigungszertifikate bleiben der Übersichtlichkeit wegen unberücksichtigt.

Das Objekt „O“ ist dem Navigationsdienst unter dem Pseudonym „X“, dem Ereignisdienst als „Y“ und dem LS als „C“ bekannt. Es erzeugt zwei Referenzen, indem es das dem LS bekannte Pseudonym „C“ zusammen mit einer jeweils unterschiedlichen, zufälligen Information (hier: „1“ bzw. „2“) mit dem öffentlichen Schlüssel des LS chiffriert. Dies ergibt im Beispiel die beiden Chiffrate „D%4J“ und „XZ6&“ Der Navigationsdienst bekommt die Referenz „D%4J“ und der Ereignisdienst die Referenz „XZ6&“. Die beiden Dienste haben keine Möglichkeit, die zwei Referenzen als zu dem gleichen Objekt gehörig zu erkennen oder gar auf dessen Identität „O“ abzubilden. Der LS dagegen kann die Referenzen durch Entschlüsseln mit seinem privaten Schlüssel auf „C“ und damit auf die betreffende Ortsinformation abbilden. Er kann allerdings keine Rückschlüsse auf die anderen Pseudonyme des Objekts („X“ und „Y“) ziehen, welche nur den jeweiligen Subjekten „N“ bzw. „E“ bekannt sind. Wenn Anforderungen an Nichtrückweisbarkeit der Antwort bestehen, kann gefordert werden, dass der LS diese unterschreibt. Falls er die Echtheit der Ortsinformation belegen muss, kann er die Unterschrift des Sensors speichern und ggf. in die Antwort integrieren.

Zu der hier beschriebenen Realisierung der Referenzen sind einige Dinge anzumerken. So bremst das Entschlüsseln einer Referenz während einer Anfrage an den LS dessen Leistungsfähigkeit zu einem gewissen Grad. Es ist allerdings generell so, dass Sicherheit einen Mehraufwand bedeutet und zusätzliche Kosten verursacht. Wir sind der Meinung, dass der Nutzen für die Privatsphäre den Mehraufwand an dieser Stelle rechtfertigt. Erste Untersuchungen zeigen, dass die Skalierbarkeit der Anfragen an den LS zumindest bei wiederholter Verwendung einer Referenz gewahrt bleiben kann. Weitergehende Untersuchungen sind für die Zukunft geplant.

Das Subjekt muss außerdem in der Lage sein, eine Referenz als zu dem gewünschten Objekt gehörig zu verifizieren. Es muss an dieser Stelle allerdings klargestellt werden, dass ein Benutzer generell die Möglichkeit hat, seine Ortsinformation zu fälschen, zum Beispiel, indem er sein Endgerät zu Hause lässt, damit dieses nicht seine aktuelle Position an den LS gibt. Es ist aber möglich zu verhindern, dass ein Benutzer die Referenz eines anderen ohne dessen Wissen benutzt. Ein genaues Verfahren zur Prüfung der Referenzen ist neben den im nächsten Abschnitt angesprochenen Punkten Gegenstand unserer derzeitigen Arbeit. Darüber hinaus stellt die zufällige Information einen verdeckten Kanal dar, über den Information an den LS übermittelt werden kann, die vom transportierenden Subjekt nicht gesehen wird.

## 7 Diskussion und Ausblick

Die oben beschriebenen Mechanismen ermöglichen die Regelung sowohl der über einen Benutzer bekannten Orts- als auch Identitätsinformation in NEXUS sowie deren Verkettung. Dabei ist im LS eine flexible Zugriffskontrolle vorgesehen, so dass Benutzer verschiedenen Subjekten unterschiedliche Zugriffsrechte einräumen können. Dadurch können beispielsweise Dienste, denen der Benutzer vertraut, auf sehr genauer, personenbezogener Ortsinformation operieren, während Dienste, denen nicht vertraut wird, die Ortsinformation nur ungenau oder pseudonymisiert bekommen. Durch die Verwendung von Berechtigungszertifikaten wird diese Flexibilität erhöht. Sie ermöglichen u. a. Delegation von Rechten an andere Subjekte, verschiedene Wege der Übertragung von Autorisierungsinformation in die Zugriffskontrolle des LS, und sie tragen zur Dezentralisierung der Zugriffskontrollentscheidung bei. Darüber hinaus verkleinert sich die Zugriffskontrollliste im LS und kann daher effizienter bearbeitet werden.

Wie oben gezeigt wurde, sind die hauptsächlichen Skalierbarkeitsprobleme von Berechtigungszertifikaten bei uns durch die zentrale Einbindung des Lokationsdienstes abgeschwächt.

Durch die pseudonyme Verwendung des LS wird verhindert, dass der Zusammenhang der sehr genauen Ortsinformation zu einem konkreten Benutzer bekannt ist. Dieser müsste sonst dem LS ein extrem hohes Vertrauen entgegenbringen. Die Verwendung von asymmetrischen Schlüsseln als Pseudonyme für Benutzer beschleunigt und vereinfacht nicht nur die Zugriffskontrollentscheidung, da kein Umweg über den Namen des Benutzers notwendig ist, sondern

macht zumindest aus Sicht der Zugriffskontrolle eine globale Namenszertifizierungsstelle überflüssig. An anderer Stelle außerhalb des LS, zum Beispiel für die richterliche Verfolgung von regelwidrigem Verhalten, kann nach wie vor der Bedarf an eine solche Zertifizierungsstelle bestehen. Die Garantie auf Rückverfolgbarkeit eines Pseudonyms kann allerdings auch ohne Namenszertifikate durch so genannte *Identity Escrow Zertifikate* erreicht werden [2]. Eine genaue Untersuchung der Zurechenbarkeitsaspekte ist Gegenstand unserer zukünftigen Arbeit.

Maskierungsangriffe, wodurch z. B. ein falsches Subjekt berechtigt werden oder der LS gefälscht werden könnte, sind auf allgemeine Authentisierungsprobleme zurückzuführen und nicht Bestandteil der Betrachtungen dieses Artikels. Ebenso werden keine Angriffe auf die Verfügbarkeit (*Denial of Service*) betrachtet.

Die Verwendung mehrerer Pseudonyme wird von der kostengünstigen Methode der Pseudonymerzeugung unterstützt, wobei lediglich ein neues Schlüsselpaar generiert werden muss. Die Verkettung der Pseudonyme wird durch die Verwendung von Referenzen verhindert. Wird das Pseudonym bezüglich eines bestimmten Kommunikationspartners gewechselt, so kann dieser das Profil über den Benutzer nicht weiterführen. Darüber hinaus kann es auf diese Weise verschiedenen Subjekten erschwert werden, durch Kollaboration das ihnen bekannte Benutzerprofil zu vergrößern. Aus diesen Gründen ist es ratsam, mit unterschiedlichen Kommunikationspartnern mindestens je ein eigenes Pseudonym zu benutzen. Dies stellt einen gewissen Widerspruch zu [10] dar, worin die Pseudonyme anwendungsübergreifend benutzt werden, um die Bedienbarkeit des Systems sicherzustellen. Für die Benutzung des Systems ist daher eine sehr differenzierte Tool-Unterstützung notwendig, durch welche die Benutzer in der Erzeugung und Auswahl ihrer verwendeten Pseudonyme und Referenzen unterstützt werden. Dies könnte eine Art *Identitätsmanager* sein, ähnlich dem in [8; 10] beschriebenen. Abgesehen davon, muss der Vorteil der Unverkettbarkeit einzelner Aktionen jeweils gegen den Nachteil fehlender Benutzeranpassung der Anwendungen abgewogen werden.

Dem LS muss mindestens dahingehend vertraut werden, dass er den Zusammenhang mehrerer Referenzen nicht an andere Subjekte verrät, da diese sonst die ihnen bekannten Pseudonyme des Benutzers darüber verketten könnten. Auf keinen Fall darf der LS die Abbildungsfunktion der Referenzen aufeinander verraten. Da hierzu die Aufdeckung seines privaten Schlüssels notwendig wäre, ist dies allerdings keine Anforderung, die durch Verwendung der Referenzen neu hinzukommt. Einen Angriff durch den LS betrachtend ist es diesem ohne Hilfe anderer Subjekte nicht möglich, aus verschiedenen Referenzen unterschiedliche Pseudonyme eines Objekts abzuleiten und damit Daten dieser Pseudonyme zu dem von ihm aufgestellten Profil hinzuzufügen.

Verglichen mit der Verwaltung der Ortsinformation in heutigen Mobilfunksystemen ist das notwendige Vertrauen in den NEXUS-LS erheblich verringert. Die Mobilfunkbetreiber wissen den genauen Zusammenhang der Ortsinformation zur Mobilfunknummer, welche eine globale Kennung ist, die sich nie ändert. Im Kontext dieser Telefonnummer sind in Deutschland neben dem Ortsprofil mindestens ein Name und eine Adresse bekannt, oftmals auch eine Bankverbindung und weitere teils personenbezogene Daten.

Um die oben ausgeführten Ziele zu erreichen, ist es für den LS notwendig, ein Verfahren zu besitzen, um genaue Ortsinformation derart ungenau zu rechnen, dass es einem Angreifer unmöglich ist, daraus wieder genaue Ortsinformation abzuleiten. Eine einfache Rasterung der Ortsinformation oder die zufällige Addition eines Fehlers genügt hierzu nicht. Beide Verfahren geben in gewissen Situationen mehr Information heraus, als gewünscht. Die Entwicklung von Verfahren für diesen Zweck sind Gegenstand weiterer Forschung.

Ein ganz anderes Problem bringt die Betrachtung der Kommunikation über die verwendeten Endgeräte mit sich. Diese deckt derzeit meist die Geräteadresse, zum Beispiel die IP-Adresse, auf. Wird die Geräteadresse im Kontext aller Pseudonyme sichtbar, so sind diese mit sehr wenig Aufwand miteinander verkettbar. Es wird daher eine anonyme Kommunikationsinfrastruktur benötigt, welche die echten Adressen der Endgeräte, beispielsweise durch Verwendung eines Stellvertreters im Netz, verschleiert und die Adressierung über Pseudonyme ermöglicht. Ansätze hierfür existieren in der Literatur bereits, siehe z. B. [17; 6].

**Danksagung**

Wir danken Matthias Kabatnik für die fruchtbaren Diskussionen, die viel zu der hier vorgestellten Arbeit beigetragen haben.

**Literatur**

[1] *Aura, T.:* Distributed access-rights management with delegation certificates. Secure Internet Programming: Security Issues For Distributed and Mobile Objects, J. Vitek, C. Jensen (Eds.), Springer, 1999, pp. 211–235.

[2] *Aura, T.; Ellison, C.:* Privacy and accountability in certificate systems, Research Report A61, Helsinki University of Technology, 2000.

[3] *Cheverst, K.; Davies, N.; Mitchell, K.; Friday, A.:* Experiences of Developing and Deploying a Context-Aware Tourist Guide: The GUIDE Project, Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, USA, 2000, pp. 20–31.

[4] *Ellison, C. M.:* "The nature of a useable PKI", Computer Networks, Vol. 31, No. 8, April 1999, pp. 823–830.

[5] *Ellison, C. M.; Frantz, B.; Lampson, B.; Rivest, R.; Thomas, B.; Ylonen, T.:* SPKI certificate theory, IETF, RFC 2693, September 1999.

[6] *Fasbender, A.; Kesdogan, D.; Kubitz, O.:* Variable and scalable security: protection of location information in Mobile IP, Proceedings of the 46th IEEE Vehicular Technology Conference (VTC '96), IEEE (Ed.), IEEE, Atlanta, USA, April 1996.

[7] *Federrath, H.; Jerichow, A.; Kesdogan, D.; Pfitzmann, A.; Spaniol, O.:* „Mobilkommunikation ohne Bewegungsprofile", Informationstechnik und Technische Informatik (it+ti), Vol. 38, No. 4, August 1996, pp. 24–29.

[8] *Gerd tom Markotten, D.; Jendricke, U.:* „Identitätsmanagement im E-Commerce", Informationstechnik und Technische Informatik (it+ti), Bd. 43, Nr. 5, September 2001.

[9] *Hauser, C.; Kabatnik, M.:* Towards privacy support in a global location service, Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001), pp. 81–89, Paris, September 2001.

[10] *Jendricke, U.; Gerd tom Markotten, D.:* Usability meets security – the Identity-Manager as your personal security assistant for the Internet, Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC 2000), pp. 344–353, New Orleans, USA, December 2000.

[11] *Köhntopp, M.; Pfitzmann, A.:* „Informationelle Selbstbestimmung durch Identitätsmanagement", Informationstechnik und Technische Informatik (it+ti), Bd. 43, Nr. 5, September 2001, S. 227–235.

[12] *Leonhardt, U.; Magee, J.:* "Security considerations for a distributed location service", Journal of Network and Systems Management, Vol. 6, No. 1, September 1998.

[13] *Leonhardi, A.; Kubach, U.; Rothermel, K.; Fritz, A.:* Virtual Information Towers – A Metaphor for Intuitive, Location-Aware Information Access in a Mobile Environment, Proceedings of the 3rd IEEE International Symposium on Wearable Computers (ISWC '99), San Fransisco, USA, 1999, pp. 15–20.

[14] *Leonhardi, A.; Rothermel, K.:* A Comparison of Protocols for Updating Location Information, Baltzer Cluster Computing Journal, Vol. 4, No. 4, 2002, pp. 355–367.

[15] *Leonhardi, A.; Rothermel, K.:* Architecture of a Large-scale Location Service, Technischer Bericht Nr. 2001/01, Fakultät Informatik, Universität Stuttgart, 2001.

[16] *Nicklas, D.; Grossmann, M.; Schwarz, T.; Volz, S.; Mitschang, B.:* A Model-Based Open Architecture for Mobile, Spatially-Aware Applications, in Proceedings of the 7th International Symposium on Spatial and Temporal Databases (SSTD 2001), Redondo Beach, USA, pp. 117–135.

[17] *Reed, M. G.; Syversion, P. F.; Goldschlag, D. M.:* "Anonymous connections and Onion Routing", IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, August 1998, pp. 482–494.

[18] *Spreitzer, M.; Theimer, M.:* "Scalable, secure, mobile computing with location information", Communications of the ACM, Vol. 36, No. 7, July 1993, pp. 27–27.

[19] *Volz, S.; Grossmann, M.; Hönle, N.; Nicklas, D.; Schwarz, T.:* „Integration mehrfach repräsentierter Straßenverkehrsdaten für eine föderierte Navigation", Informationstechnik und Technische Informatik (it+ti), Bd. 44, Nr. 5, Oktober 2002, S. 260–267.

**Dipl.-Inf. Alexander Leonhardi** ist wissenschaftlicher Mitarbeiter am Institut für Parallele und Verteilte Höchstleistungsrechner.

Adresse: Institut für Parallele und Verteilte Höchstleistungsrechner, Universität Stuttgart, Breitwiesenstr. 20–22, D-70565 Stuttgart,
E-Mail: leonhardi@informatik.uni-stuttgart.de

**Dipl.-Ing. Christian Hauser** ist wissenschaftlicher Mitarbeiter am Institut für Nachrichtenvermittlung und Datenverarbeitung (IND) der Universität Stuttgart.

**Prof. Dr.-Ing. Dr. h.c. mult. P. J. Kühn** ist Leiter des Instituts für Nachrichtenvermittlung und Datenverarbeitung (IND) der Universität Stuttgart.

Adresse: Institut für Nachrichtenvermittlung und Datenverarbeitung, Universität Stuttgart, Pfaffenwaldring 47, D-70569 Stuttgart,
E-Mail: {kuehn, hauser}@ind.uni-stuttgart.de