Vision und Realisierung einer sicheren mobilen Informations-Verteilung, Verwaltung und Abfrage

Jens Heider
Fraunhofer Institut für Sichere Telekooperation

Zusammenfassung: In der heutigen Zeit, in der Informationen und deren elektronische Verarbeitung überaus wichtige Wirtschaftsgüter darstellen, kommt zunehmend auch der schnellen und effizienten Verteilung eine Schlüsselrolle zu. Allerdings adressieren aktuelle Lösungsansätze, trotz der fortschreitenden, umfassenden Vernetzung, nur Teilbereiche dieses Problems. Dieser Beitrag stellt daher die Vision einer sicheren mobilen Informationsverteilung vor, die darüber hinaus auch eine mobile Verwaltung verteilter Informationen sowie ihre Abfrage unterstützt. Im Anschluss wird das Konzept einer, auf verfügbaren mobilen Endgeräten, Protokollen und Netzinfrastrukturen basierenden, Plattform beschrieben und deren Anforderungen an die Infrastruktur und die Sicherheit analysiert. Abschließend wird die Realisierung der Architektur und das Sicherheitskonzept vorgesellt.

Schlüsselworte: mobil, Information, Verwaltung, Distribution, Plattform, SOAP

1 Einleitung

In der heutigen Zeit muss eine große Menge an Informationen sehr schnell verteilt werden, um mit der technischen und wirtschaftlichen Entwicklung mithalten zu können. Im Falle von öffentlichen Informationen, die für eine große Anzahl von Empfängern bestimmt sind, z.B. eine im Voraus bekannte, statische Empfängergruppe, kann eine zentralisierte Datenquelle (z.B. mittels Hyper Text Transfer Protocol (http) oder File Transfer Protocol (FTP)) verwendet werden. Ebenso existieren dezentralisierte Ansätze die eine Peer-to-Peer-Lösung verfolgen. Allerdings ist der Fall, in dem wichtige vertrauliche Informationen nur einem einzelnen Empfänger zur Verfügung gestellt werden soll, schwieriger zu bewerkstelligen. Heutzutage wird diese Aufgabe hauptsächlich durch den Einsatz von eMails mit Anhängen gelöst. Doch hierbei ergeben sich die bekannten Probleme und Einschränkungen für die Sicherheit, die Vertraulichkeit und nicht zu Letzt auch für die Benutzerfreundlichkeit durch den fehlenden flächendeckenden Einsatz von Kryptografie und die im eMail-Konzept fehlenden Verwaltungsfunktionen umfangreicher Dateikommunikation. Darüber hinaus fehlt diesem Ansatz ein verteiltes Informations- und Zugriffs-Management über unterschiedliche Quellen, dass dem mobilen Einsatz gerecht wird. Dieses ist notwendig, um alle wichtigen Informationen auf Sender und

Empfängerseite stets aktuell und abrufbar zu halten und dies auch in neuen, verteilten Arbeitsumgebungen und mobilen Anwendungsszenarien zu gewährleisten. Gerade dort ist die Nutzung von eMails für die Verteilung von Dokumenten durch die Beschränkung der Bandbreite und den hohen Übertragungskosten, die in diesem Szenario sowohl beim Sender als auch beim Empfänger anfallen, wenig einladend. Für die verschlüsselte Verteilung von Informationen, die nicht bereits auf dem mobilen Endgerät gespeichert sind, muss dafür zunächst die gesamte Information auf das Endgerät übertragen werden, bevor sie gesendet werden kann, was die Übertragungskosten verdoppelt. Darüber hinaus bieten PDAs und Smartphones zwar einen guten Kompromiss zwischen Größe, Funktionalität und Ubiquität, der es ermöglicht einen Computer mit Verbindung zum Internet immer bei sich zu tragen, aber der eingeschränkte Bedienkomfort bei der Informationssuche und -Verarbeitung führt bei konventioneller Nutzung zu unbefriedigenden Ergebnissen.

Ein anderes Problem der Informationsverwaltung besteht häufig in den über mehrere Systeme verteilten Datenquellen. Bei der Nutzung solcher Datenquellen, wie etwa Datenbanken, eMails und anderen Dateien die lokal auf Arbeits-PCs und Notebooks gespeichert sind, entstehen sehr heterogene Zugriffsprozesse, die zu einer Vielzahl von verschiedenen Protokollen, Sichten und Datei-Versionen führen.

Zusammenfassend lässt sich daher sagen, dass im Informationszeitalter Informationen sicher verwaltet und verteilt werden müssen, auch wenn der eigene Desktop PC oder das Notebook nicht verfügbar sind. In dieser Situation bietet die mobile Kommunikation den Schlüssel zu einem immer verfügbaren Informationsmanagement-Konzept. In dem nächsten Kapitel wird daher zunächst die Vision der mobilen Informationsverwaltung vorgestellt, gefolgt von dem Konzept und einer ersten Realisierung.

2 Die Vision

Die Vision basiert auf der Verwendung von mobilen Endgeräten als Verwaltungs- und Verteilungswerkzeug für alle gespeicherten Informationen, wie z.B. Dokumente, eMails und Projektdaten. Dazu verwendet das Endgerät die verfügbaren kabellosen Kommunikationsverbindungen, um die Übermittlung der gewünschten Information vom Ort der Speicherung zum Ort der Nachfrage, also z.B. vom eigenen Server zu einem über das Internet erreichbare Server eines Projekt-Partners, zu veranlassen. Alle beliebig über verschiedene Datenquellen verteilten Informationen, die einer Identität zugeordnet sind, können auf diese Weise mit mobilen Geräten wie Smartphones, PDAs und Notebooks verwaltet werden. Ebenso ist natürlich eine Nutzung von stationären Geräten möglich, bei der der Benutzer als mobile Komponente betrachtet wird, wie es bei der Nutzung von öffentlichen Internet-PCs der Fall ist. So ist der mobile Benutzer, unabhängig vom Speicherort der Information, jederzeit in der Lage die gewünschten Informationen dorthin zu übermitteln, wo der Empfänger sie speichern und öffnen kann. Ein entscheidender Punkt

dabei ist der Austausch der Empfängerinformationen auf den mobilen Geräten, da durch die limitierten Eingabemöglichkeiten die Benutzerakzeptanz schnell verloren geht. Ohne einen einfachen Austausch von Empfängerinformationen gehen die neuen mobilen Möglichkeiten im Umgang mit Informationen durch die komplexe oder unbequeme Handhabung verloren.

Das Ziel der Vision ist somit, dem Benutzer die einfache mobile Verwaltung der Informationen zu ermöglichen, um den Nutzen sowohl für die eigene Informationssuche, als auch für den Empfänger zu erhöhen. Dazu gehört auch die Übermittlung von Kontextinformationen (vgl. [Sch03]) zu jeder Informationsübertragung, die den Clients hilft die gesendeten Informationen automatisch und effizient zu speichern. Auf diese Weise steigt auch die Effizienz einer späteren Informationssuche.

Der dritte Aspekt ist der Informationszugriff, der unabhängig von den Möglichkeiten des momentanen Geräts erfolgen können soll. Durch Nutzung des Endgeräts als Verwaltungswerkzeug kann nun die Information auch an andere Ausgabegeräte wie etwa Fax-Geräte, Drucker oder Internet-PCs weitergeleitet werden.

Will man die Vision kurz zusammenfassen, so kann man sagen, dass sich das mobile Endgerät durch die ökonomische Nutzung von drahtloser Kommunikation zur mobilen Informationsverwaltung auf der einen Seite und die Nutzung von Internetverbindungen zur eigentlichen Informationsübertragung und Synchronisation auf der anderen Seite, zu einem täglichen Werkzeug für die sichere Verwaltung und Verteilung von Informationen entwickeln wird.

3 Konzept und Realisierung

Das MIDMAY Konzept (Mobile Information Distribution, Management and Access for You!) kombiniert die beschriebene Vision mit der Technik aktueller, verfügbarer Endgerätemöglichkeiten und Systemen zur Informationsspeicherung und -abfrage. Darüber hinaus werden speziell die Sicherheitsaspekte, beginnend bei dem ID-Management, über die Absicherung der Übertragung zwischen den verteilten mobilen und stationären Komponenten, bis hin zur Sicherstellung der Eindeutigkeit der Informationsadressierung zur sicheren Verteilung und Synchronisation berücksichtigt.

3.1 Szenario

Angenommen S trifft auf einer Konferenz einen interessierten potentiellen Geschäftspartner R zu dem bisher keine Kommunikationsbeziehung existierte. Um die Anfangsphase einer Projektanbahnung zu vereinfachen und zu beschleunigen will S an R möglichst schnell relevante Informationen, z.B. Veröffentlichungen, Geschäftsberichte oder Beispielverträge übermitteln. Dazu tauschen nun S und R drahtlos (z.B. per Bluetooth- oder Infrarotschnittstelle) mit ihren mobilen Endgeräten die MIDMAY-Identitäten aus,

die neben den öffentlichen Schlüsseln und der Policy für die weitere Kommunikationsabsicherung auch die Adresse der Homebase enthält. Nun wählt S die Dokumente für R auf seinem Endgerät aus. Zum einfachen und effizienten Auffinden der gesuchten Informationen, bietet das Benutzerinterface S einen Baum aus beschreibenden Schlüsselwörtern an. Die Dokumente befinden sich dabei an den Enden der Pfade von der Wurzel zu den Blättern, wobei sich dasselbe Dokument auch in verschiedenen Pfaden wieder finden kann, was das Auffinden über verschiedene Kontextpfade ermöglicht. Diese Sicht auf die Informationen wurde zuvor von der Homebase von S mit Hilfe von Kontextinformationen, die zu den gespeicherten Informationen vorliegen, erzeugt und auf seinem Endgerät zwischengespeichert. Dazu gehört in welchem Kontext die Information erstellt wurde (z.B. Datum, Ort, Meeting, Projekt, Form, etc.) und in welchem Kontext sie zu anderen Informationen steht. Die Daten über die ausgewählten Informationen werden dann zusammen mit den Kontaktinformationen von R über die drahtlose Internetverbindung an die Homebase von S gesendet. Dort werden die Informationen aus den verschiedenen Datenquellen abgefragt und über einen sicheren Kanal zur Homebase von R übertragen. Die Absicherung des Kanals erfolgt über die Schlüsselinformationen, die der Client von R bei der Kontaktaufnahme mitgeteilt hat.

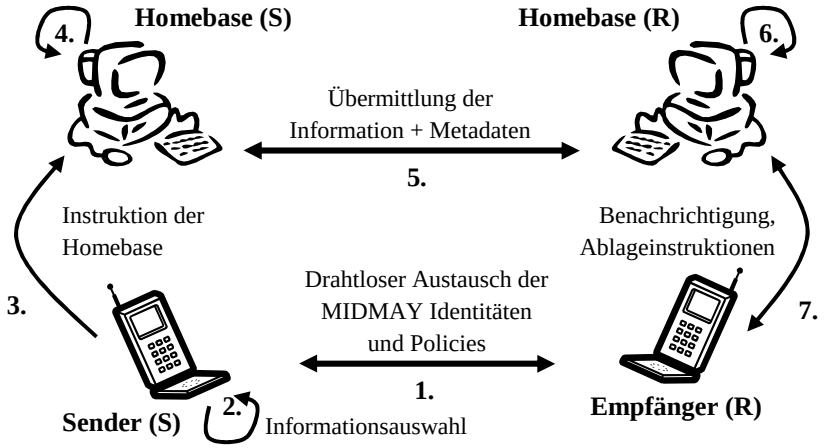

Abbildung 1: Ablauf der Informationsübermittlung im Szenario

Die Homebase von R speichert nun vorläufig die empfangene Information mit Hilfe der übermittelten Kontextinformationen. Nun wird R über die eingegangene Information auf seinem Endgerät informiert. Er hat dann die Möglichkeit den Kontext zu editieren, die Information abzurufen oder sie auf ein anderes Ausgabegerät zu leiten. Späteren Übertragungen zwischen S und R geht zunächst eine Prüfphase der beim ersten Kontakt übermittelten Policy voraus, wenn die Übermittlung nicht auf einer gegenseitigen Aktion beruht. So kann der Empfang von unerwünschten Informationen verhindert werden.

3.2 Komponenten

Der mobile Client dient der übersichtlichen Präsentation der verfügbaren verteilten Informationen und der Interaktion mit dem Benutzer für die Suche und Auswahl sowie der Interaktion mit der Plattform. Zur einfachen Anpassung an die unterschiedlichen Geräteeigenschaften wird das Benutzerinterface der Clients von den darzustellenden Informationen und dem Übertragungsprotokoll entkoppelt. Für diesen Zweck wird zur Kommunikation das Simple Object Access Protokoll (SOAP) eingesetzt, welches einen leichtgewichtigen, entfernten Methodenaufruf ermöglicht und durch die Verwendung von XML die Übermittlung von plattformunabhängigen Informationen unterstützt. Daneben können auch WAP und HTML Browser zur Steuerung der MIDMAY Plattform eingesetzt werden, was die Verfügbarkeit der Plattform auf nahezu jedes vernetzte Gerät ausweitet. Die Verwendung von Browsern hat aber auch für das MIDMAY Konzept den Nachteil, dass keine Aktionen offline durchgeführt werden können. Spezialisierte Clients ermöglichen dagegen die Kontrolle der Zwischenspeicherung bereits übertragener Informationen. Ebenso kann die Darstellung der Oberfläche und der bereits vorhandener Daten offline erfolgen. Dies steigert die Effizienz der MIDMAY Nutzung durch geringere Wartezeiten und die reduzierten Übertragungskosten.

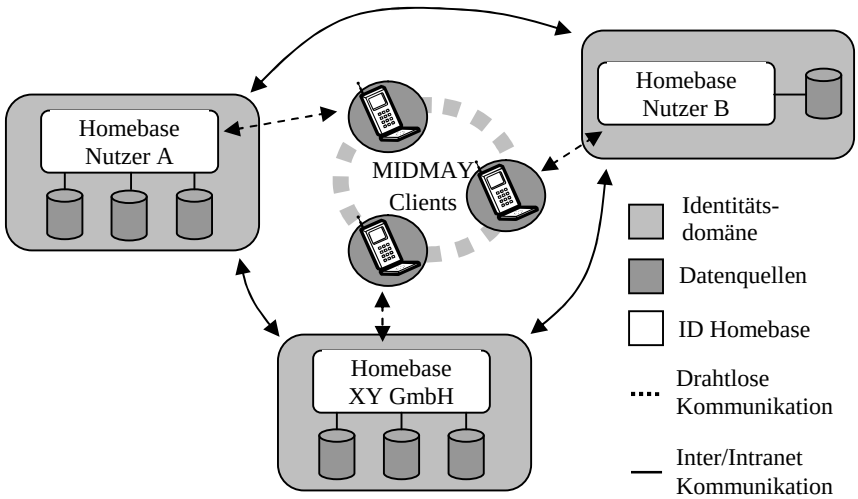

Abbildung 2: Topologie der MIDMAY Komponenten

Im MIDMAY Konzept (siehe Abbildung 2) ist die Homebase die Basis für eine oder mehrere MIDMAY Identitäten. Sie führt die Zugriffe auf die verteilten Datenquellen aus und erzeugt für die Clients eine einheitliche Sicht auf alle eingetragenen Datenquellen, um den Benutzer von der Komplexität der verschiedenen Protokolle, Darstellungen und physischen Speicherorten zu entlasten. Die durch die Homebase generierte Abstraktions-

schicht kann von verschiedenen Frontends genutzt werden, um die Darstellung und die Nutzung an die Möglichkeiten der verschiedenen mobilen Endgeräte anzupassen. Gesteuert durch die Clients, sendet die Homebase Informationen entweder direkt zu einer oder mehreren Homebases oder sie verwendet andere Protokolle wie SMTP oder FTP, wenn der Empfänger über keine MIDMAY Infrastruktur verfügt.

Die Identitätsdomänen fassen die lokal adressierbaren Identitäten, Homebases und Datenquellen zusammen und bilden von außen gesehen die logischen Konten in einem dezentral organisierten Netz. Dabei ist die Identitätsdomäne unabhängig von der physischen Netzstruktur, sodass sich die einzelnen Komponenten in beliebigen Netzen befinden können. Innerhalb der Domänen können beliebige Datenquellen adressiert werden. Diese stellen die Basis der in der Domäne verfügbaren Informationen dar. Die Funktionalität der Homebase wird von logischen Einheiten erbracht, die sich über beliebige physikalische Server verteilen lassen. Die Verwendung von Modulen ermöglicht dabei einen strukturiert erweiterbaren Funktionsumfang der Plattform.

3.3 Homebase Module

Das Data Retrieval Module (DRM) dient der Kommunikation mit den verteilten Datenquellen. Es bietet eine dateiorientierte Schnittstelle, die die Unterschiede der verschiedenen nötigen Ein- und Ausgabefilter der Datenquellen verbirgt. Des Weiteren werden hier die Such- und Navigationsanfragen anhand der ebenfalls in diesem Modul verwalteten Indexierung auf die verschiedenen Datenquellen umgesetzt und die Antworten über die Dateischnittstelle zurückgegeben. Darauf setzt das Unified Representation Module (URM) auf und bildet die indizierten Informationen in eine einheitliche Darstellung ab. Auf diese Weise wird es möglich auf der Clientseite innerhalb einer homogenen Struktur auf beliebige Datenquellen zuzugreifen. Dazu bietet das URM sowohl eine baumorientierte Schnittstelle zur schnellen Navigation innerhalb des Datenbestandes, als auch eine Metadaten-Schnittstelle an, über die auch unscharfes Suchen innerhalb der Metadaten und der Dokumente ermöglicht wird.

Die Übertragung der Dokumente zu anderen Homebase-Modulen übernimmt das Data Transfer Module (DTM), das sich dazu sowohl des ID Management Moduls zur Auflösung der Zieladresse, als auch des Security Assertion Moduls bedient, um eine sichere Übertragung zu gewährleisten. Dazu wird zunächst zwischen den Homebase-Modulen ein sicherer Kanal aufgebaut, über den in der Folge die weiteren Daten ausgetauscht werden. Ebenfalls auf das DTM greift das Data Synchronisation Module zurück (DSM). Es ermöglicht den Abgleich verteilter Daten, wie es beispielsweise bei der lokalen Bearbeitung von Dokumenten an verschiedenen Orten benötigt wird, um eine aktuelle und konsistente Dokumentenverwaltung zu ermöglichen. Das Context Awareness Module (CAM) bietet der Plattform eine Schnittstelle zur kontextsensitiven und ereignisbasierten Steuerung von Funktionen. Dazu können auf der einen Seite Informationen über den aktuellen Kontext des Benutzers anderen Modulen zur Verfügung gestellt werden. Auf der

anderen Seite können sich Module auch für eine Benachrichtigung bei neu eintretenden Ereignissen und Kontextwechseln anmelden. Dies ermöglicht allen Modulen, auf Ereignisse zu reagieren, den aktuellen Kontext zu berücksichtigen und automatisch Aktionen auszulösen. Die Kontextinformationen gewinnt das CAM zum einen direkt über den Client, zum anderen besitzt es auch eine Schnittstelle zur Eingabe von Kontextinformationen durch andere Module. So können z.B. Kontextinformationen über den aktuellen Aufenthaltsort des Benutzers sowohl durch die, vom Client übermittelten Positionsdaten (z.B. mittels GPS-Receiver), als auch durch die Verknüpfung mit Einträgen im elektronischen Terminkalender verarbeitet, aufbereitet und weitergegeben werden.

Die Identitäten der Benutzer werden durch das ID Management Module (IDM) verwaltet. Diese werden über eindeutige Bezeichner abgerufen, die sich aus dem DNS-Namen des Homebase-Servers und einer von diesem vergebenen lokalen ID für jeden dort assoziierten Benutzer zusammensetzen (vgl. IETF RFC2396 Server-based Naming Authority [RFC2396]). Die elektronische Identität besteht neben Kontaktinformationen auch aus Profilen zur Sicherung des Datenverkehrs und Informationen über persönliche Präferenzen im Umgang mit MIDMAY. Darüber hinaus werden auch Accountdaten internetbasierter Dienste verwaltet, sodass die Homebase über das External Service Module (ESM) Informationen dieser Dienste abrufen und mit Hilfe der anderen Module verarbeiten kann. Die Sicherung der Kommunikation wird durch das Security Assertion Module (SAM) gewährleistet. Das Sicherheitskonzept und die Aufgaben werden im nächsten Kapitel erläutert.

4 Sicherheitskonzept der Plattform

Die wesentliche Anforderung an die Sicherheit der Plattform, liegt in einer praxistauglichen Realisierung einer sicheren Informationsübermittlung zwischen, sich bis dato unbekannten, mobilen Personen. Diese Anforderung lässt sich auf die drei, im Konzept dargelegten, Verbindungen zwischen den Parteien anwenden. Explizit sind dies die Verbindungen zwischen den Homebase-Modulen organisatorisch getrennter Benutzer, die Verbindungen zwischen der Homebase und dem mobilen Client und die Verbindungen zwischen den mobilen Clients untereinander.

Da diese Parteien zunächst über keine gemeinsamen Schlüssel verfügen, kann keine authentische und vertrauliche Kommunikation über öffentliche Netze gewährleistet werden. Abhilfe könnte der Aufbau einer Infrastruktur für öffentliche Schlüssel (Public Key Infrastructure, PKI, siehe [Eck01]) ermöglicht, dies hat aber im vorliegenden Fall einige Einschränkungen in der Praxis zur Folge. So erscheint es kaum realisierbar, dass für alle beliebigen Kombinationen zweier, nicht organisatorisch oder geografisch verbundene, Benutzer des Systems eine gemeinsame dritte, vertrauenswürdige Partei existiert, mit der beide Benutzer über einen sicheren Kanal im Vorfeld Informationen über ihre Schlüssel ausgetauscht haben. Die sich aus diesem Spannungsfeld zwischen Sicherheitsanforde-

rungen und Praxistauglichkeit und dem sich durch die Plattform realisierten Umfeld ergebenden Probleme und Möglichkeiten, werden daher in den nächsten Abschnitten betrachtet.

4.1 Identitätsmanagement

Die Nutzung einer verteilten Plattform mit vielen Benutzern erfordert eine sichere Verwaltung der Benutzerdaten. Dies wird in der MIDMAY-Homebase durch ein ID-Management realisiert, das eine Reihe von Aufgaben erfüllt. Die Hauptaufgaben bestehen in der Authentifizierung und Autorisierung der Benutzer. Diese Aufgaben müssen allerdings auf den Client und die Homebase verteilt werden, da beide Komponenten sowohl autark als auch interaktiv agieren. Auf Client-Seite muss der Benutzer z.B. auch authentifiziert werden können, wenn keine Verbindung zur Homebase besteht. Auch soll es möglich sein, durch das einmalige Anmelden auch andere externe Dienste nutzen zu können (Single-Sign-On). Auf der Homebase-Seite finden neben der Kommunikation mit den eigenen Clients – was ebenfalls einer Authentifizierung, Autorisierung und eines User-Managements bedarf hier auf Seiten der Hombase – auch Kommunikation zwischen verschiedenen anderen Homebases oder externen Diensten statt. Bei dieser, vom Benutzer autarken, Interaktion wird das ID-Management verwendet, um sowohl die Identität der Homebase als auch die des beauftragenden Benutzers gegenüber dem Kommunikationspartner auszuweisen. Daher wird ein verteiltes, eng zwischen Hombase und Client verzahntes ID-Management realisiert. Die Verteilung ist aber auch global zu sehen, da keine zentrale Infrastruktur für die lose vernetzten Homebases existiert (und aufgrund der angestrebten Verteilung und Organisation auch nicht existieren kann). Jede Homebase ist daher selbst für ihre Benutzer verantwortlich und somit auch für die Organisation des lokalen Namensraums der Identitäten zuständig.

Auf dem mobilen Endgerät sind hingegen nur kleine Teile der persönlichen Identität abgelegt, um den Schaden im Verlustfall des Gerätes zu minimieren. Aus demselben Grund ist auch der lokale Cache verschlüsselt, sodass bei dem Verlust eines Clients eventuell noch vorhandene Daten auf dem Endgerät nur mit großem Aufwand von unberechtigten Personen eingesehen werden können. Zusätzlich wird im Verlustfall der Identität ein neues Schlüsselpaar zugewiesen, um eine Identitätsübernahme (siehe auch [HHL03]) nach einer Überwindung der Verschlüsselung der lokalen Daten zu verhindern.

Ein dem Datenschutz zugehöriges Ziel des ID-Managements ist die Abwendung einer Preisgabe von Informationen, die eine Profil-Bildung über einen MIDMAY Benutzer ermöglichen. Dies wird durch die Möglichkeit, beliebige Bezeichner gegenüber fremden Benutzern anzugeben, realisiert. Da lediglich die eigene Homebase die Zuordnung zu den Identitäten durchführt, muss bei einem Wechsel lediglich ein neuer Zuordnungseintrag erzeugt werden, was auch automatisch geschehen kann. Gegenüber Benutzern, mit denen Informationen ausgetauscht werden, führt allerdings der öffentliche Schlüssel zu

einer eindeutigen Identifizierbarkeit, unabhängig von dem verwendeten Bezeichner. Soll auch dies verhindert werden, muss der öffentliche Schlüssel parametrisiert werden, ohne den privaten Schlüssel zu ändern.

4.2 Absicherung der Homebase Kommunikation

Die Kommunikation der Homebase mit den Clients wird über asymmetrische Schlüssel realisiert, die beim Prozess der einmaligen Assoziierung des Clients zu einer Homebase von dieser erzeugt werden und offline, zusammen mit dem Server-Zertifikat der Hombase, in das mobile Clientgerät gelangen. Auf diese Weise wird ein Kanal für eine sichere Ende-zu-Ende Verbindung zu den mobilen Clients realisiert. Die Kommunikation zwischen Homebases, die bisher über keine gemeinsamen Schlüsselpaare verfügen, benötigen weitere Informationen von dem Client, der diese Aktion angestoßen hat. Beim Austausch der Identitäten zwischen den mobilen Clients wird daher sowohl der öffentliche Schlüssel des Clients, als auch der der Homebase innerhalb der Ziel-Identität übermittelt. Somit kann der Client in diesem Fall den öffentlichen Schlüssel sicher an die eigene Homebase weitergeben.

4.3 Absicherung der mobilen Endgeräte

Der Absicherung der mobilen Endgeräte kommt eine Schlüsselrolle in der MIDMAY-Plattform zu. Durch die dezentrale Verwaltung der Identitäten, bedarf es einer sicheren Möglichkeit Empfänger-Identitäten und Schlüssel auszutauschen. Im MIDMAY-Konzept geschieht dies drahtlos zwischen den mobilen Endgeräten. Da sich diese in einer lokalen Umgebung befinden, besteht für die Nutzer die Möglichkeit, Informationen auf den Displays der Endgeräte zu vergleichen. Somit ergibt sich aus kryptografischer Sicht ein weiterer Übertragungskanal, der für die Sicherung der Authentizität der Information genutzt werden kann. Im konkreten Fall wird er genutzt, um nach der Übermittlung einer neuen Empfänger-Identität eine Manipulation auf dem Übertragungsweg auszuschließen. Dazu wird auf beiden Seiten ein kollisionsresistenter Hash-Wert (siehe [Eck01]) der übermittelten Daten gebildet und auf den Displays angezeigt, wodurch nun leicht von beiden Teilnehmern die Echtheit der Daten verifiziert werden kann. Nach dieser initialen Übermittlung der Identität besitzen die Kommunikationspartner jeweils den authentischen öffentlichen Schlüssel des anderen (sowohl des Clients als auch der Homebase), den sie an ihre Homebase weitergeben. Diese ist somit in der Lage, eine sichere Verbindung zu dem neuen Kommunikationspartner aufzubauen.

Da die Interaktion zwischen Client und Homebase eine sicherheitskritische Schnittstelle darstellt, erfolgt bei der Initiierung einer Verbindung zunächst eine beidseitige Authentifikation zwischen Client und Homebase auf Basis der in Abschnitt 4.2 beschriebenen ausgetauschten Schlüssel und Zertifikate. Des Weiteren muss die Client Software auch gegen unberechtigte Nutzung geschützt werden. Dieser Benutzerauthentifizierungspro-

zess, der der Nutzung des Clients vorgeschaltet ist, dient auch der Freigabe sicherheitskritischer Funktionen, wie Cachezugriff, Profilübermittlung und Authentisierung gegenüber der Homebase.

5 Ausblick

Die vorgestellte Vision einer sicheren mobilen Informations-Verteilung, Verwaltung und Abfrage bietet eine neue Methode im Umgang mit Informationen. Für einen ersten Prototyp bedarf es der weiteren Untersuchung und Spezifizierung der beschriebenen Homebase Module, sowie der Beobachtung der Hardwareentwicklung bei den mobilen Endgeräten. Hier sind vor allem die Trends zur Integration von GPS-Empfängern für die Positionsbestimmung und die steigende Hardwareperformanz wichtige Faktoren für die Kontextbestimmung und die Funktionalität der mobilen Clients, die eine weitere Vereinfachung des Bedienkonzepts ermöglichen. Darüber hinaus bieten die Betriebssysteme für mobile Endgeräte immer mehr Funktionen zur Unterstützung von drahtloser Kommunikation sowie steigende Zugriffsmöglichkeiten auf ehemals getrennte Ressourcen der Endgeräte. Im Smartphone-Bereich wird damit die Integration der Software in die einheitliche Benutzeroberfläche möglich, sowie die direkte Nutzung von Daten aus den Telefon-Anwendungen wie z.B. Adressbuch, Kurzmitteilung oder Terminplaner. Eine konsequente Nutzung dieser Möglichkeiten, unter Abschätzung und Berücksichtigung der Sicherheit, bietet weiteres Potential für die effiziente Nutzung der mobilen Endgeräte als nützliches Alltags-Werkzeug für den mobilen Umgang mit Informationen.

Literatur

[Eck01] Eckert, C.: IT-Sicherheit, Konzepte, Verfahren, Protokolle. Oldenbourg Vlg.: 2001

[HHL03] Hoffmann, M.; Heider, J.; Larsson, M.: Modernes Identitäts- und Profildatenmanagement. In: Dittrich, K.; König, W.; Oberweis, A.; Rannenberg, K.; Wahlster, W. (Hrsg.), Lecture Notes in Informatics - Proceedings, Informatik 2003, Band 2, Köl-len Druck & Verlag GmbH, ISBN 3-88579-364-4

[Sch03] Schulz, S.: Kontext als Beziehung: Ein Kontextmodell für Mobiles Wissensmanagement. In: Dittrich, K.; König, W.; Oberweis, A.; Rannenberg, K.; Wahlster, W. (Hrsg.), Lecture Notes in Informatics - Proceedings, Informatik 2003, Band 2, Köllen Druck & Verlag GmbH, ISBN 3-88579-364-4

[RFC2396] IETF Network Working Group, RFC 2396 - Uniform Resource Identifiers (URI): Generic Syntax, http://www.ietf.org/rfc/rfc2396.txt, Abruf am 2003-09-30