it+ti 38/4 (1996) 20-23

Persönliches Erreichbarkeitsmanagement

Andreas Bertsch[1], Herbert Damker[2], Hannes Federrath[3]

[1]IBM, European Networking Center, Vangerowstr. 18, 69115 Heidelberg
[2]Universität Freiburg, Institut für Informatik und Gesellschaft, Telematik, Friedrichstr. 50, 79098 Freiburg
[3]TU Dresden, Institut für Theoretische Informatik, 01062 Dresden

Zusammenfassung

Der Beitrag beschreibt ein datenschutzfreundliches Konzept zur Steuerung der persönlichen Erreichbarkeit. Erreichbarkeitswünsche werden so ausgehandelt, daß die kommunikative Selbstbestimmung des Teilnehmers gefördert wird, ohne dabei seine Datenschutzinteressen zu verletzen.

1 Problembeschreibung

Erhöhte technische Erreichbarkeit, unter anderem durch Mobilkommunikation, gefährdet die kommunikative Selbstbestimmung der Nutzer von Telekommunikationsnetzen. Besonders betroffen sind hier Menschen, die aus beruflichen Gründen ständig erreichbar sein müssen. Erhöhte Erreichbarkeit erfordert also neue Dienste zur selektiven Steuerung der persönlichen Erreichbarkeit.

1.1 Was ist persönliches Erreichbarkeitsmanagement?

Persönliches Erreichbarkeitsmanagement bezeichnet die technisch unterstützte Steuerung der persönlichen Erreichbarkeit eines angerufenen Teilnehmers in Abhängigkeit von übermittelten Informationen über Charakter und Inhalt des gewünschten Kommunikationswunsches durch den anrufenden Teilnehmer vor Zustandekommen der (Gesprächs)verbindung.

Der Angerufene soll für verschiedene Lebens-, Arbeits-, Tagessituationen, also Erreichbarkeitssituationen, seinen *Erreichbarkeitsmanager (EM)* schnell und unkompliziert konfigurieren können.

1.2 Erreichbarkeitsmanagement und Datenschutz

Alle Daten, die einen Personenbezug aufweisen, sind schützenswert. Im EM sind dies Daten über die eigene derzeitige Situation sowie andere Teilnehmer betreffende Daten, beispielsweise wie auf eingehende Kommunikationswünsche reagiert werden soll. Sie sind schützenswert gegenüber allen potentiellen Kommunikationspartnern, aber auch gegenüber dritten Instanzen (wie den Dienstanbietern und Netzbetreibern).

1.3 Demonstrator für mehrseitige Sicherheit

Im Kolleg „Sicherheit in der Kommunikationstechnik“ der Gottlieb Daimler- und Karl Benz-Stiftung dient eine prototypische Implementierung des *Erreichbarkeitsmanagementsystems (EMS)* als Demonstrator für mehrseitige Sicherheit. Einerseits ist dieser ein Beispiel für die Umsetzung mehrseitiger Sicherheit in zukünftiger Technik, andererseits soll der Demonstrator in Laborversuchen und einer Simulationsstudie eingesetzt werden. Dabei sollen die Anforderungen von Benutzern an die Sicherheit und Vertrauenswürdigkeit von Telekommunikationsendgeräten und -netzen untersucht werden. Für diesen Zweck wird der

Demonstrator auch Träger weiterer Sicherheitsmechanismen (Authentikation, qualifizierende Zertifikate, Verschlüsselung), die dem Benutzer zumindest in ihrer Bedienung demonstriert werden.

2 Umsetzung des Erreichbarkeitsmanagements

2.1 Repräsentation von Dringlichkeit

Der *Kommunikationskontext* beschreibt einen Kommunikationswunsch oder eine aktuell bestehende Kommunikation. Er wird als Vorschlag oder Wunsch während der Signalisierung übermittelt und ist Gegenstand der Aushandlung zwischen den Erreichbarkeitsmanagern der Kommunikationsteilnehmer. Erst wenn der ausgehandelte Kommunikationskontext bestimmte Bedingungen erfüllt, kommt eine Verbindung mit der angerufenen Person zustande. Ansonsten kann der Erreichbarkeitsmanager andere Reaktionsweisen, beispielsweise die Aufnahme einer Sprachnachricht oder die Umleitung des Anrufes an eine andere Person, anbieten. Ein Kommunikationskontext enthält:

- in welcher Weise die Kommunikationspartner einander gegenseitig bekannt sind (anonym, per Pseudonym, mit realer Identität),
- welche Dringlichkeit oder welchen Zweck die Kommunikation für die Kommunikationspartner hat,
- auf welche Art und Weise kommuniziert werden soll (Dienstart) und
- welche Sicherheitsanforderungen bestehen und durch welche Mechanismen die aktuelle Kommunikation gesichert wird.

Der Repräsentation der Dringlichkeit eines Kommunikationswunsches kommt besondere Bedeutung zu. In Anlehnung an die zwischenmenschliche Aushandlung von Erreichbarkeit muß ein technisches System hier eine Vielzahl von Optionen bereitstellen. Möglich sind unter anderem Angaben einer subjektiven Dringlichkeit oder einer Referenz. Mögliche Optionen sind:

- *Behauptung von Dringlichkeit:* Der Anrufer gibt seinem Kommunikationswunsch selbst eine bestimmte Dringlichkeit. Diese Einschätzung ist eventuell sehr subjektiv.
- *Angabe einer Funktion:* Hier kann der Anrufer angeben, daß er in einer bestimmten Funktion (oder auch Qualifikation) anruft, beispielsweise als Mitarbeiter eines bestimmten Projektes oder einer Firma. Diese Angabe kann über digitale Zertifikate gesichert werden.
- *Angabe eines Anlasses oder Themas:* Diese Angabe ist durch den Erreichbarkeitsmanager nur dann maschinell auswertbar, wenn es eine vereinbarte Liste von Themen und Anlässen zwischen den Kommunikationspartnern gibt.
- *Angabe einer Referenz:* Dies bedeutet, daß der Anrufer sich bei seiner Kontaktaufnahme auf die Empfehlung einer dritten Person beruft (beispielsweise durch ein von dieser Person ausgestelltes Zertifikat). Wenn die dritte Person dem Angerufenen bekannt ist, kann er die Empfehlung als ein Kriterium für die Annahme von Kommunikationswünschen benutzen.
- *Präsentation eines Gutscheins:* Ein Gutschein unterscheidet sich von einer Referenz dadurch, daß er vom Angerufenen selbst ausgestellt sein muß, etwa weil er einen Rückruf erbeten hat, der ihn sicher erreichen soll.
- *Aussetzen einer Kaution:* Der Anrufer kann, um die Ernsthaftigkeit seines Kommunikationswunsches und die Angabe seiner Dringlichkeit zu unterstützen, einen (evtl. ausgehandelten) Geldbetrag als Kaution an den Angerufenen überweisen. Fühlt der Angerufene sich durch den Anrufer getäuscht, so kann er diesen Betrag einbehalten, an eine gemeinnützige Einrichtung überweisen oder ähnliches [1].

Welche Angaben das EMS des angerufenen Teilnehmers vom Anrufer anfordert und für die Entscheidung über den Kommunikationswunsch auswertet, hat der Angerufene in der persönlichen Konfiguration seines EMS festgelegt. Realistisch ist beispielsweise, daß von Anrufern, die sich nicht identifiziert haben, die Identifizierung oder eine Kaution angefordert wird.

2.2 Sicherheitsaspekte

Bei der Konfiguration des EMS muß der Benutzer sehr sensible persönliche Daten einem technischen System anvertrauen, beispielsweise zu welchen Zeiten er erreichbar ist und mit welchen Personen er kommunizieren oder nicht kommunizieren will. Dies erfordert:

- die Speicherung und Verarbeitung in einer *vertrauenswürdigen, persönlichen* Umgebung: Da die Daten auch gegenüber einem Dienstanbieter oder Netzbetreiber zu schützen sind, ist die Realisierung des Erreichbarkeitsmanagements als reiner Netzdienst nicht möglich.
- den Schutz gegen *Ausforschung*: Der Aushandlungsdialog zwischen Erreichbarkeitsmanagern muß so gestaltet werden, daß durch wiederholte Anfragen keine Informationen über die persönliche Konfiguration der Erreichbarkeit eines Teilnehmers gewonnen werden können. Ausforschungsversuche sollten außerdem erkannt werden können.
- den Schutz des Teilnehmers vor *ungewollter Preisgabe* von persönlichen Angaben oder Werten (Kaution): Dies ist eine Anforderung, die besonders bei der Gestaltung der Benutzungsschnittstelle berücksichtigt werden muß.
- die *Revisionsfähigkeit* des Systems durch den Benutzer: Der Benutzer muß jederzeit die Möglichkeit haben, alle in seinem EM gespeicherten Informationen zu überprüfen, zu ändern und zu löschen. Insbesondere dürfen keine Daten vorhanden sein, die es Dritten erlauben, sein Kommunikationsverhalten bei einem Verlust des EM zu rekonstruieren.

Die Kommunikation und Aushandlung zwischen den Erreichbarkeitsmanagern muß gemäß den Schutzzielen mehrseitiger Sicherheit [4] geschützt werden. Vertraulichkeit von übermittelten Daten kann durch Ende-zu-Ende-Verschlüsselung gewährleistet werden. Anonymität und Unbeobachtbarkeit können nur durch entsprechende Gestaltung der zugrundeliegenden Netzinfrastruktur erreicht werden.

Um das Funktionieren des EM auch bei Mißbrauchsversuchen und Angriffen zu gewährleisten, muß die Integrität und gegebenenfalls die Unabstreitbarkeit der mit einem Kommunikationswunsch übermittelten Angaben sichergestellt werden. So müssen Identitätsangaben durch digitale Signaturen und Zertifikate gesichert werden. Die Unabstreitbarkeit kann gesichert werden, indem die relevanten Kommunikationsaktionen durch einen von den Kommunikationspartnern akzeptierten, unbeteiligten Dritten (Notariatsdienst) protokolliert werden.

Es ergeben sich inhaltliche Verbindungen zu Zugriffskontrollsystemen (der „Zugang“ zur Privatsphäre des Angerufenen wird geschützt) und zu Wertetransfersystemen: „Erreichbarkeitsrechte“, wie Referenzen und Gutscheine, müssen auf sichere Weise weitergegeben werden können. Auch zur Bekräftigung einer Dringlichkeitsangabe mittels „Kaution“ ist ein Wertetransfer nötig.

3 Technische Realisierung

Die Realisierung des Erreichbarkeitsmanagementsystems erfolgt in zwei Komponenten:

Als vertrauenswürdige, persönliche Umgebung dient ein mobiler *Persönlicher Kommunikationsassistent (PKA).* Er unterstützt den Anrufer bei der Formulierung eigener Kommunikati-

onswünsche durch ein Teilnehmerverzeichnis und signalisiert dem Gerufenen eingehende Anrufe und Nachrichten. Im PKA sind die sensiblen Erreichbarkeitsinformationen abgelegt.

Der mobile Teil des Erreichbarkeitsmanagers wird durch eine *ortsfeste Teilnehmerstation (OTS)* ergänzt, die im Festnetz lokalisiert ist, beispielsweise beim Teilnehmer oder an seiner Arbeitsstelle. Sie nimmt alle Kommunikationswünsche für den Benutzer entgegen und leitet sie gegebenenfalls an den PKA weiter. Außerdem nimmt die OTS Funktionen des Erreichbarkeitsmanagers wahr, die (noch) nicht in einem mobilen Gerät realisiert werden können, etwa die Aufzeichnung von Sprachnachrichten. Neben den Aufgaben des Erreichbarkeitsmanagements kann die OTS noch weitere Sicherheitsfunktionen erfüllen, wie die Verwaltung des Aufenthaltsortes des Teilnehmers im Mobilfunknetz (siehe hierzu [1, 2, 3]).

Im Rahmen des Kollegs wird der PKA als Demonstrator auf der Basis eines Newton MessagePad™ implementiert. Die OTS wird auf der Basis eines PC, der über ISDN mit dem Festnetz verbunden ist, realisiert. Die Kommunikation zwischen PKA und OTS erfolgt über das zellulare Mobilfunknetz GSM (Global System for Mobile Communication).

3.1 Funktionaler Aufbau

Bild 1 zeigt den funktionalen Aufbau des Erreichbarkeitsmanagers (PKA *oder* OTS). Der EM besteht aus den drei Funktionsblöcken „Benutzungsschnittstelle“, „Kernmaschine“ und „Kommunikationsdienste“.

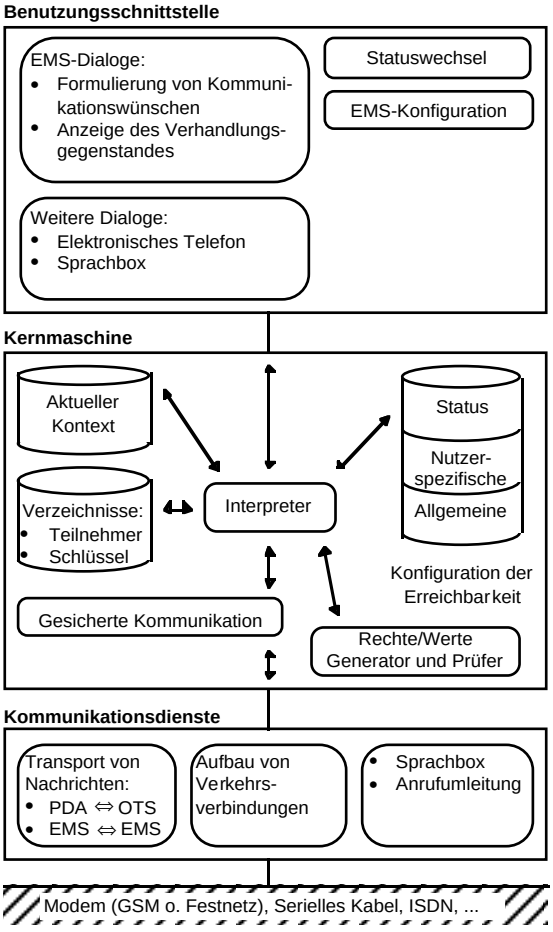

Bild 1: Funktionale Gliederung des Erreichbarkeitsmanagementsystems

3.2 Kernmaschine

Die Kernmaschine des EM wertet den aktuellen Kommunikationskontext aus. Er wird aus den Angaben des Benutzers und den vom Kommunikationspartner übermittelten Daten gebildet. Die Regeln für die Auswertung, die Erreichbarkeitskonfiguration, stammen aus drei verschiedenen Bereichen:

- Der *Status* gibt die aktuelle Situation wieder, in der sich der Benutzer gerade befindet („privat“, „am Arbeitsplatz“, „Besprechung“ etc.). Dieses Datum ändert sich häufig und bestimmt, welche Teilmenge der übrigen Regeln anzuwenden ist.
- Die nutzerspezifische Konfiguration bestimmt der Benutzer über den Konfigurationsdialog des EM. Hier legt er über *individuelle Auswertungsregeln* fest, wie sein EM in den verschiedenen Situationen auf Kommunikationswünsche reagieren soll.
- Ergänzt werden die Auswertungsregeln durch *allgemeine Erreichbarkeitsregeln*, die durch die Kommunikationsteilnehmer nicht verändert werden können (etwa die Festlegung, daß Notrufe immer durchgestellt werden).

Als Ergebnis der Auswertung aktualisiert der Interpreter den Kommunikationskontext und entscheidet, ob der Kommunikationswunsch akzeptiert oder abgelehnt wird oder ob weitere Informationen für eine endgültige Entscheidung (vom eigenen Benutzer oder vom Kommunikationspartner) einzuholen sind. Daraufhin werden entsprechende Nachrichten an den Benutzer des jeweiligen EM (genauer an die Benutzungsschnittstelle), andere Komponenten des eigenen EM oder den EM des Kommunikationspartners versandt.

3.3 Benutzungsschnittstelle

Erreichbarkeitsmanagement stellt gegenüber dem normalen Telefon eine Erweiterung dar, die vom Benutzer zusätzlichen Bedienaufwand erfordert, da er neben der Angabe des gewünschten Kommunikationspartners nun weitere Angaben zur Dringlichkeit seines Gespräches machen soll. Für ein Standardgespräch mit „normaler“ Dringlichkeit wird dieser Mehraufwand durch die Vorgabe von Standardwerten reduziert . Mittels Zugriff auf ein globales Teilnehmer- verzeichnis kann der Aufwand im Einzelfall sogar reduziert werden. Außerdem ist ein Teilnehmer genau unter *einer* Adresse erreichbar, egal wo und in welcher Situation er sich gerade befindet.

Die Benutzungsschnittstelle muß den Benutzer auf einfache Weise bei der Formulierung von Kommunikationswünschen unterstützen, den aktuellen Kommunikationskontext präsentieren und die Konfiguration der Erreichbarkeit sowie den Statuswechsel erlauben.

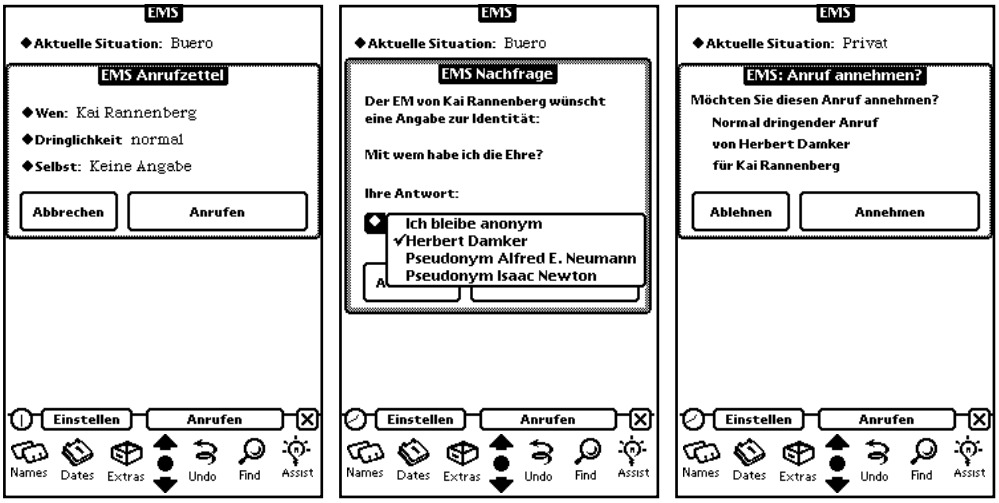

Bild 2: Erreichbarkeitsdialoge auf dem Newton MessagePad™

Bild 2 zeigt drei dieser Dialoge (Formulierung eines Kommunikationswunsches, Rückfrage des EMS des Gerufenen und die Anzeige eines eingehenden Anrufes) für den Fall, daß nur die Angabe (oder Nichtangabe) der eigenen Identität und einer subjektiven Dringlichkeit möglich sind.

4 Erreichbarkeitsmanagement in zukünftigen Netzinfrastrukturen

Wenn mehrseitig sicheres Erreichbarkeitsmanagement in künftige Netzinfrastrukturen integriert werden soll, müssen durch die Netze Bedingungen geschaffen werden, die den Mehrseitigkeitsaspekt von Sicherheit unterstützen.

Für anonyme und pseudonyme, oder besser unbeobachtbare Kommunikationsformen ist die Unterstützung des Netzes erforderlich. Dazu gehören die Signalisierung über Verteilung (Broadcast) und implizite Adressierung. Was heute wegen zu knapper Bandbreite in den Netzen unrealistisch erscheint, ist in Zukunft bei Verfügbarkeit breitbandiger Netze durchaus realisierbar. Dann könnte der Erreichbarkeitsmanager über temporär gültige implizite Adressen angesprochen werden, die an einen vom Teilnehmer ausgesuchten Personenkreis ausgegeben werden.

Ein weiteres Problem stellen die begrenzten Möglichkeiten der heutigen Signalisiernetze dar, die nur die Übermittlung der „nötigsten“ Signalisierinformationen erlauben. Eventuell muß deshalb in Zukunft von der strikten Teilung in (gebührenfreie) Signalisierung und (gebührenpflichtige) Datenkommunikation abgewichen werden. Ein breitbandigerer Ausbau der Signalisiernetze wird ohnehin erforderlich werden, wenn weltweit verfügbare Dienste wie Universal Personal Communication (UPT) aufgebaut werden.

Teillösungen wie „Aussetzen einer Kaution“ erfordern zwangsläufig die Integration von Wertetransfer- oder Zahlungssystemen, bei denen die Anonymität und Unbeobachtbarkeit des Teilnehmers zu gewährleisten ist.

Literatur

[1] A. Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

[2] H. Federrath, A. Jerichow, D. Kesdogan, A. Pfitzmann: Security in Public Mobile Communication Networks. Proc. of the IFIP TC 6 International Workshop on Personal Wireless Communications, Verlag der Augustinus Buchhandlung Aachen, 1995, 105-116.

[3] T. Hetschold: Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformation im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes. GMD-Studien Nr. 222, Oktober 1993.

[4] K. Rannenberg, A. Pfitzmann, G. Müller: Kai Rannenberg, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit. it+ti 38/4 (1996) 7-10.