in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 207-217.

Persönliches Erreichbarkeitsmanagement♣

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

[1]Universität Freiburg, Institut für Informatik und Gesellschaft, Telematik, Friedrichstr. 50, 79098 Freiburg

[2]TU Dresden, Institut für Theoretische Informatik, 01062 Dresden

[3]IBM, European Networking Center, Vangerowstr. 18, 69115 Heidelberg

Zusammenfassung

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

1 Problembeschreibung

Erhöhte technische Erreichbarkeit, z.B. durch Mobilkommunikation, gefährdet die kommunikative Selbstbestimmung der Nutzer von Telekommunikationsnetzen. Besonders betroffen sind Personen, die aus beruflichen Gründen ständig erreichbar sein müssen. Diese erhöhte Erreichbarkeit erfordert neue Möglichkeiten, steuern zu können, wann und von wem man erreicht werden will und ob auch eine Störung akzeptiert wird.

1.1 Was ist persönliches Erreichbarkeitsmanagement?

Persönliches Erreichbarkeitsmanagement kann zwar kein Sekretariat ersetzen, aber es hilft Anrufern und Angerufenen, eine geeignete Situation für ein gemeinsames Telefonat zu finden. Bevor Angerufene tatsächlich (etwa durch ein Klingeln) alarmiert und gestört werden, wird ermittelt, ob der Anruf dafür dringend und wichtig genug ist. Anrufer haben dabei eine Vielfalt von Möglichkeiten, Thema und Dringlichkeit ihres Anrufes zu übermitteln. Umgekehrt können sie erfahren, ob ihr Anruf gelegen kommt oder wann eine günstigere Zeit wäre, und ggfs. Nachrichten hinterlassen. Besitzer eines *Erreichbarkeitsmanagementsystems* (EMS) können ihre Erreichbarkeit für verschiedene Tages- und Arbeitssituationen flexibel konfigurieren.

1.2 Erreichbarkeitsmanagement und mehrseitige Sicherheit

Der Konflikt zwischen Anrufern und Angerufenen ist ein prägnantes Beispiel für die Anforderungen an mehrseitige Sicherheit. Angerufene wünschen im allgemeinen eine hohe Erreichbarkeit bei gleichzeitigem Schutz vor Störungen. Darum sind sie interessiert, vor den Gesprächen möglichst viele Informationen über die Anrufer zu bekommen. Andererseits ist es den Anrufern nicht zuzumuten, schon vor einem Gespräch ihre Identität und weitere persönliche Informationen preisgeben zu müssen.

Die im folgenden angeführten Beispiele verdeutlichen diese Aspekte und zeigen, welche Sicherheitseigenschaften in verschiedenen Situationen bedeutsam werden können:

- Um unnötige Störungen zu vermeiden, ist etwa eine Ärztin im Nachtdienst nicht daran interessiert, jeden beliebigen Anruf entgegenzunehmen. Sie will für Notrufe und eventuell für nahe Verwandte oder gute Freunde erreichbar sein, für die sie sogar nachts aufstehen würde. Grundsätzlich möchte sie sich vor belästigenden Anrufen schützen. Deshalb wird ihr Erreichbarkeitsmanagementsystem bei anonymen Anrufen vom Anrufer zuerst Angaben zur Identität oder zum Anlaß des Anrufes erfragen, bevor es bei ihr klingeln und damit ihren

♣ Aktualisierte und erweiterte Fassung eines in it+ti 38. Jg. Heft 4 (1996) S. 20-23 erschienenen Artikels.

Schlaf stören würde. Der Schutz vor Übertragungsfehlern und vor Anrufern, die eine falsche Identität vortäuschen, erfordert Maßnahmen zur Sicherung der Übertragungsintegrität der Gesprächsinformation und zur Zurechenbarkeit des Anrufes.

- Die Mitarbeiter eines telefonischen Beratungsdienstes sowie Sozialarbeiter können das Erreichbarkeitsmanagementsystem dazu nutzen, sich die Arbeit in Phasen großen Arbeitsandranges zu erleichtern. Menschen, die zu solch heiklen Themen wie AIDS, Alkoholismus, Geschlechtskrankheiten oder Überschuldung Rat suchen, wollen im allgemeinen anonym bleiben. Diese Anonymität ist häufig die Voraussetzung für ein offenes und wirklich hilfreiches Beratungsgespräch. Diese Benutzer eines telefonischen Beratungsdienstes sollten deshalb in der Lage sein, ohne Preisgabe ihrer (wahren) Identität anrufen zu können.

  Sollte die Beratung zwar anonym, jedoch nicht kostenlos erhältlich sein, so sollte der Anruf unter Angabe eines Pseudonymes möglich sein.

Sowohl die Vertraulichkeit als auch die Zurechenbarkeit des Anrufes in ausreichendem Maße zu gewährleisen, ist keine einfache Aufgabe. Die gegenwärtig verfügbaren Mechanismen zur Identifizierung eines Anrufers schützen entweder den Angerufenen, indem der Anrufer seine Identität durch die Übermittlung seiner Telefonnummer preisgeben muß (Zurechenbarkeit des Anrufes) oder den Anrufer, indem sie es ihm erlauben, anonym anzurufen (Schutz der Vertraulichkeit).

Einige Systeme lassen dem Anrufer die Wahl, ob er seine Telefonnummer zeigen möchte oder nicht. In diesem Fall haben die Angerufenen jedoch keine Chance, die Anrufe in ihrer Dringlichkeit zu unterscheiden, bevor sie gestört werden. Der Blick auf die angezeigte Telefonnummer gibt ihnen lediglich einen Hinweis darauf, wer sie gerade erreichen möchte. In diesem Fall sind die Anrufer also gezwungen, ihre Identität preiszugeben (und damit ihre Anonymität zu verlieren), auch wenn theoretisch andere Möglichkeiten zur Repräsentation der Dringlichkeit zur Verfügung stünden (vgl. Abbildung 1).

Persönliches Erreichbarkeitsmanagement ist ein Ansatz, der es den Kommunikationsteilnehmern erlaubt, nur die Informationen auszutauschen, die wirklich für die Anbahnung der Kommunikation gebraucht werden. Dieser sparsame Umgang mit Daten bedeutet somit auch, daß weniger persönliche Information zu schützen ist.

Die im Zusammenhang mit dem persönlichen Erreichbarkeitsmanagement anfallenden Daten sind äußerst sensibel: Einige von ihnen beschreiben die aktuelle Situation der Kommunikationsteilnehmer, einige (z.B. die vorgegebene Reaktion auf eingehende Kommunikationswünsche) enthalten Hinweise auf die persönliche Einstellung des Benutzers anderen Personen gegenüber. Sie müssen deshalb in einer vertrauenswürdigen, persönlichen Umgebung gespeichert und verarbeitet werden (vgl. 2.2).

Persönliches Erreichbarkeitsmanagement hilft, zwischen den widerstreitenden Schutzinteressen von Kommunikationsteilnehmern zu vermitteln, und ist so ein Beispiel für mehrseitig sichere Kommunikationstechnik.

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 er 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 Auswahl und Aushandlung der Erreichbarkeit

2.1 Kommunikationskontext und 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. Abbildung 1 nennt weitere Optionen.

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. Beispielsweise kann von Anrufern, die sich nicht identifiziert haben, eine Identifizierung oder eine Kaution angefordert werden.

2.2 Sichere Speicherung und Kommunikation

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.

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].

Abbildung 1: Repräsentation von Dringlichkeit

- 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 [RaPM_96] 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.

2.3 Benutzungsschnittstelle

Werden einem System persönliche Daten anvertraut, sind Usability und Likeability von entscheidender Bedeutung für die subjektiv empfundene Sicherheit. Deshalb wurde großer Wert auf die Gestaltung der Benutzungsschnittstelle des EMS gelegt. In Zusammenarbeit mit Psychologen der Universitäten Bonn und Tübingen wurde die Benutzungsschnittstelle so gestaltet, daß die Bedienung des EMS für „normale“ Anrufe gegenüber der des klassischen Telefons nicht aufwendiger wird. Die Benutzungsschnittstelle wurde in mehreren Schritten getestet und verbessert.

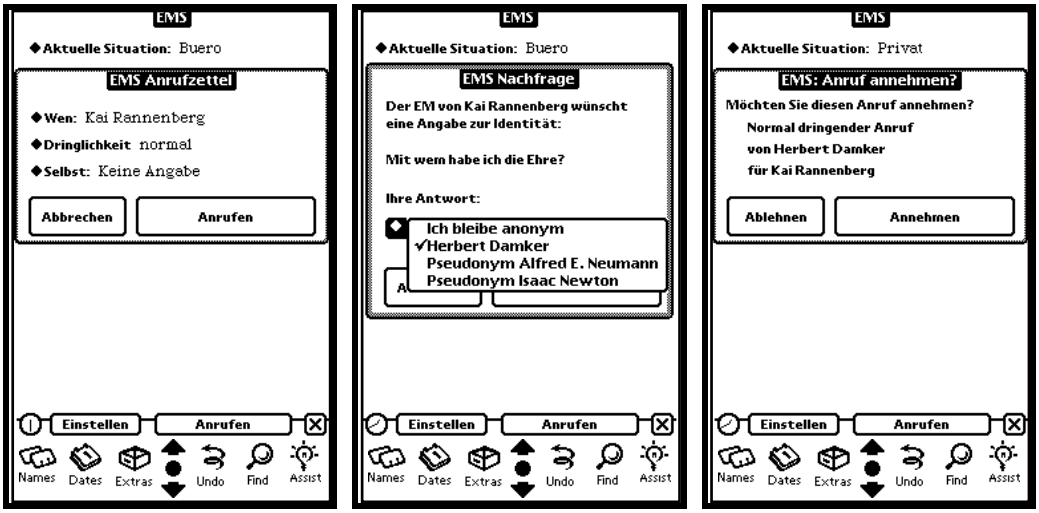

Abbildung 2: Erreichbarkeitsdialoge auf dem Newton MessagePad™

Abbildung 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.

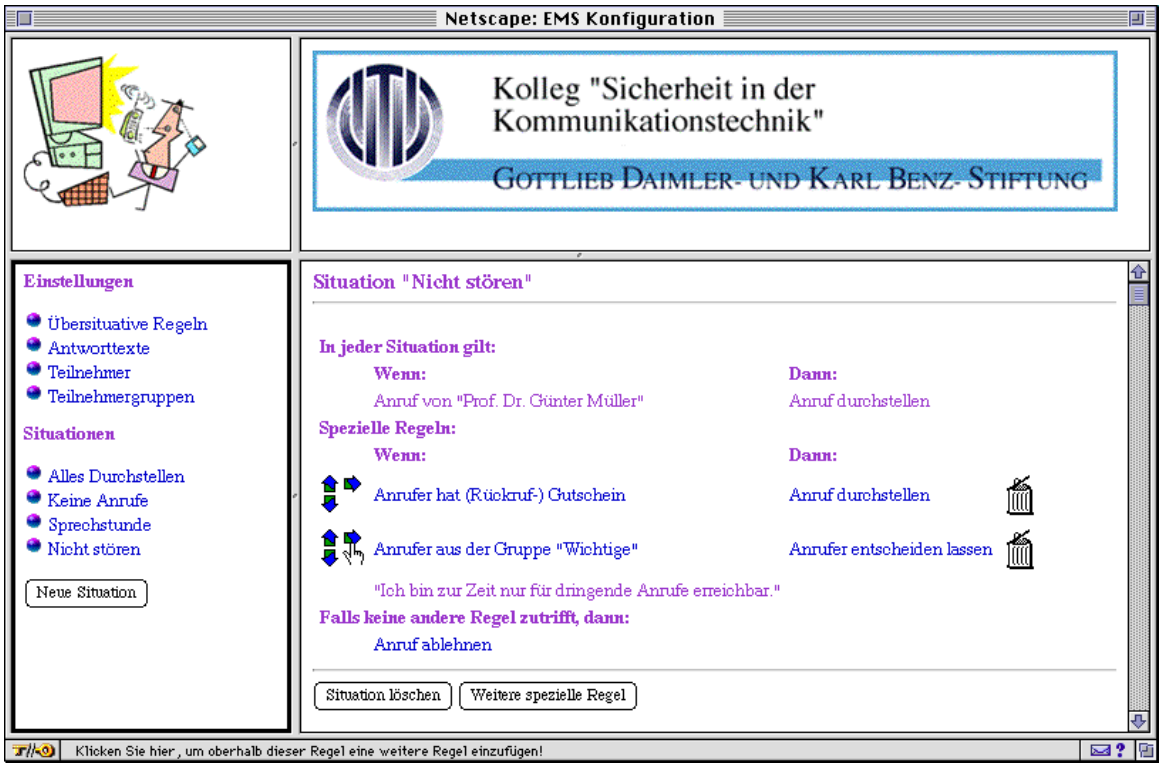

Abbildung 3: Beispiel der Konfigurationsdialoge

Die Konfigurationsdialoge des EMS wurden plattformunabhängig als HTML-Formulare implementiert (Abbildung 3). Sie erlauben es, die Reaktionen des EMS für verschiedene Situationen festzulegen. Über selbstdefinierte Erreichbarkeitsregeln bestimmen die Benutzer, wie ihr EMS auf die verschiedenen Angaben der Anrufer reagiert.

3 Technische Realisierung des Demonstrators

3.1 Komponenten des EMS

Als vertrauenswürdige, persönliche Umgebung dient ein mobiler *Persönlicher Kommunikationsassistent (PKA).* Er unterstützt den Anrufer bei der Formulierung eigener Kommunikationswünsche 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 zu Hause oder an der 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 (vgl. hierzu [Pfitz_93, FJKP_95, Hets_93]).

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).

3.2 Funktionaler Aufbau

Abbildung 4 zeigt den funktionalen Aufbau des Erreichbarkeitsmanagers. Der EM besteht aus den drei Funktionsblöcken Benutzungsschnittstelle, „Kernmaschine“ und Kommunikationsdienste.

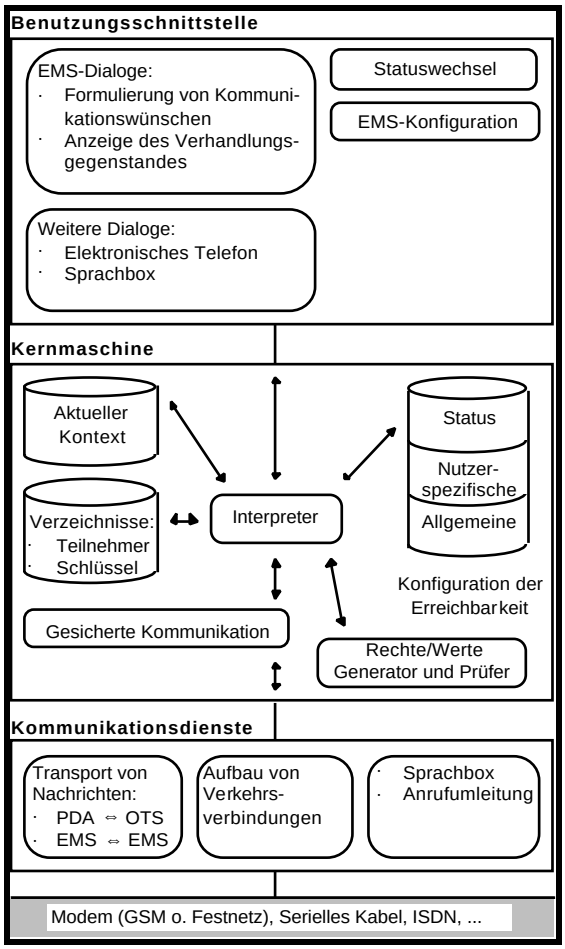

Abbildung 4: Funktionale Gliederung des Erreichbarkeitsmanagementsystems

3.3 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.

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 Teilnehmer zu gewährleisten ist.

5 Literatur

[Pfitz_93] A. Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

[FJKP_95] 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.

[Hets_93] T. Hetschold: Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformation im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes. GMD-Studien Nr. 222, Oktober 1993.

[RaPM_96] K. Rannenberg, A. Pfitzmann, G. Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit. it+ti – Informationstechnik und Technische Informatik 38/4 (1996) 7-10 (auch in diesem Band).