# Einsatz von IPv6 zur Gewährleistung von Sicherheit beim Smarter Wohnen[1]

Lothar Schöpe, Jochen Meis*

*Fraunhofer Institut für Software- und Systemtechnik (FhG-ISST), Dortmund
{lothar.schoepe | jochen.meis}@do.isst.fraunhofer.de

## Zusammenfassung

Für Wohnungsunternehmen ist es das Ziel, ihren festen Bestand an Mietern zu sichern und zu erweitern. Dieses wirtschaftliche Ziel resultiert aus dem demographischen Faktor - die Bevölkerungszahl ist rückläufig und das Alter von Mietern steigt - und führt auch dazu, dass sich die Wohnungsunternehmen zunehmend in einem Wettbewerb zueinander befinden. Dieses Ziel kann durch die Bereitstellung von it-gestützten Mehrwertdienstleistungen, die für jeden Mieter spezifisch und individuell sind, erreicht werden. Mehrwertdienstleistungen werden in den Bereichen Gesundheit, Komfort und Sicherheit angeboten und führen dazu, dass ältere Mieter zu Hause betreut werden können – und dadurch länger in den eigenen vier Wänden verbleiben – oder das technikaffine Mieter problemlos breitbandige Internetverbindungen zum Telefonieren, zur Audio- und Videoübertragung oder nur zum Surfen nutzen können. It-gestützte Mehrwertdienstleistungen, die Wohnungsunternehmen angeboten werden, entstehen durch die Integration von Mikrosystemtechnik, Hausvernetzung und externen Dienstleistungen. Durch diese Mehrwertdienstleistungen werden die lokalen Komponenten (Steckdosensysteme, Lichtanlagen, Schließanlagen, Rauchmeldersysteme, Bewegungsmelder, Ortungssysteme, Kameras, mobile Endgeräte) integriert genutzt. Hierfür wird in einer Wohnung, einem Gebäude oder einem Campus eine Hard- und Softwareinfrastruktur sowie eine Netzwerkinfrastruktur voraus gesetzt. Die lokalen Komponenten müssen jedoch eindeutig adressierbar sein, um einerseits eine Steuerung zu ermöglichen und andererseits mutwillige oder ungewollte Fehlfunktionen vermeiden zu können.

Zur Adressierung der lokalen Komponenten kann IPv6 genutzt werden. Durch den größeren Adressraum können die lokalen Komponenten innerhalb einer Wohnung, die Wohnungen auf einer Etage, die Etagen innerhalb eines Gebäudes und die Gebäude auf einem Campus eindeutig adressiert werden. Des Weiteren können Möglichkeiten wie IPSec – hardwaretechnisch unterstützt – genutzt werden, um Vertraulichkeit, Authentizität und Integrität zu gewährleisten und Mobile IP um auch Mehrwertdienstleistungen außerhalb einer Wohnung durch mobile Endgeräte zu aktivieren, zu konfigurieren oder zu nutzen.

# 1 Einleitung

Ein neues Einsatzfeld der Softwaretechnologie ist das Anwendungsgebiet Smarter Wohnen. In diesem Anwendungsgebiet werden Dienstleistungsplattformen konzipiert und realisiert, wodurch die Ausführung von Mehrwertdienstleistungen softwaretechnisch unterstützt werden. Durch Mehrwertdienstleistungen i.d.S. erfolgt die Integration von Mikrosystemtechnik, Hausvernetzung und Dienstleistungen, mit dem Ziel die Attraktivität von Wohnungen zu er-

[1] Gefördert durch das Land NRW im Zukunftswettbewerb NRW unter dem Kennzeichen 005-0407-0039.

höhen, um so den Bestand an Mietern zu sichern und zu erweitern. It-gestützte Mehrwertdienstleistungen werden von Wohnungsunternehmen bereitgestellt und Mietern zur Nutzung angeboten (vgl. Abb. 1). Diese Mehrwertdienstleistungen für Mieter ergeben sich aus den drei Bereichen Gesundheit, Komfort und Sicherheit [Trän01].

Zu dem Bereich Gesundheit zählen neben den it-gestützten Mehrwertdienstleistungen zur Unterstützung des betreuten Wohnens (Senior Care, e-HealthCare) auch Dienstleistungen zur Medikamentenversorgung, Medikamenteninformation oder medizinischen Gesundheitsprophylaxe. Zu dem Bereich Komfort zählen adaptierbare und individuelle Dienstleistungen zur Audio- und Videoübertragung oder zur Nutzung von Contentprovidern (öffentliche oder geschlossene Benutzergruppen). Zum Bereich Sicherheit zählen Dienstleistungen zur Einbruchsvorbeugung und –meldung, zur Vandalismusprävention oder Brand- und Leckagemeldung (Brauchwasser, Abwasser, Gas).

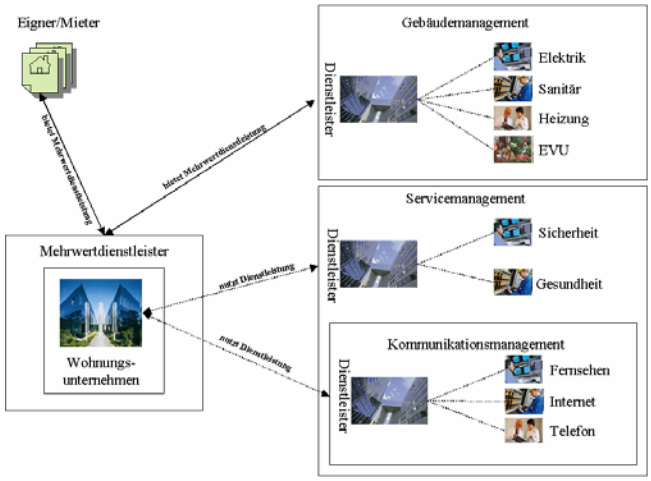


**Abbildung 1:** Mehrwertdienstleistung beim Smarter Wohnen

Zur Unterstützung des Gebäudemanagements bietet das Wohnungsunternehmen it-gestützte Mehrwertdienstleistungen für Handwerksbetriebe (Sanitär, Heizung, Elektrik, etc.) oder Energieversorgungsunternehmen an. Diese Mehrwertdienstleistungen führen bei diesen zu einer Kostenreduzierung durch Vermeidung von Anfahrten, durch zielgerichtete Ersatzteilbeschaffung oder durch optimierte Einsatzplanung.

Notwendige Voraussetzungen für die Bereitstellung von it-gestützten Mehrwertdienstleistungen sind einerseits der Einbau von lokalen Komponenten in eine Wohnung, ein Gebäude oder einen Campus und anderseits die Integration von externen Dienstleistern.

Unter lokalen Komponenten werden Steckdosensysteme, Lichtanlagen, Schließanlagen, Rauchmeldersysteme, Bewegungsmelder, Ortungssysteme, Kameras ebenso verstanden wie Geräte der weißen Ware (Kühlschränke, Waschmaschinen, etc.) oder der braunen Ware (Audio-, Videogeräte) oder Geräte zur Energieversorgung (Thermostaten, Ablesegeräte, Heizungsanlagen, Verbrauchsmessgeräte). Die Vernetzung diese lokalen Komponenten erfolgt durch unterschiedliche Techniken (EIB, LON, IR, Bluetooth, LAN/WLAN [Broy02]), die auch gemeinsam verwendet werden können. Die Steuerung der lokalen Komponenten kann durch verschiedene mobile Endgeräte (Handy, Smartphone, PDA, Tablet-PC) über ein Resi-

dential Gateway erfolgen, durch das auch bei Bedarf eine Transformation von Protokollen erfolgt, wenn verschiedenen Techniken zur Vernetzung von lokalen Komponenten verwendet werden. Die Steuerung kann auch außerhalb einer Wohnung erfolgen, wenn durch das mobile Endgerät Techniken wie GSM, HSCSD, GPRS oder UMTS unterstützt wird und durch das Residential Gateway entsprechende Schnittstellen bereitgestellt werden.

Zu externen Dienstleistern zählen Unternehmen, die in den Bereichen Gesundheit, Komfort und Sicherheit bereits isolierte Dienstleistungen am Markt anbieten (z.B. Notruftaster für ältere Personen, Gebäudeüberwachung für Unternehmen, AV-Übertragung für das Distance Learning).

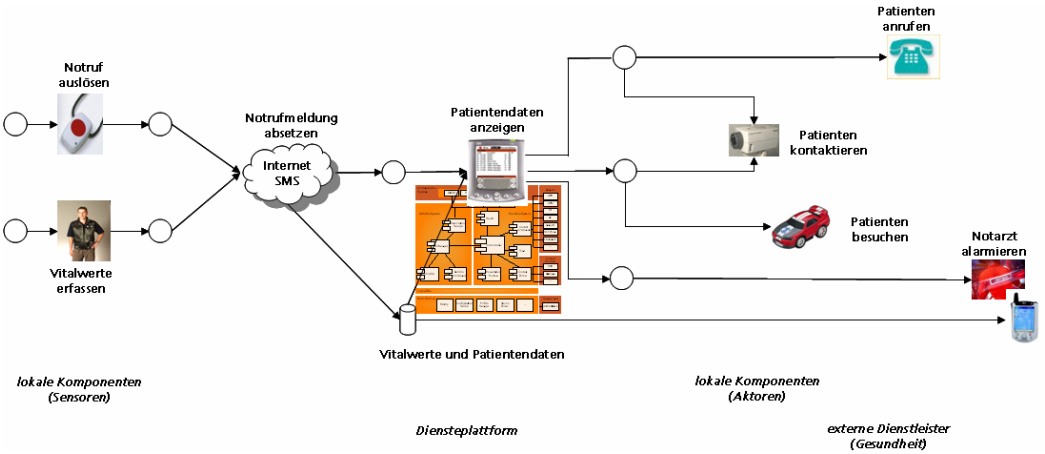


**Abbildung 2:** Mehrwertdienstleistung im Bereich Senior Care

Durch eine it-gestützte Mehrwertdienstleistung werden verschiedene isolierte Dienstleistungen integriert, die Informationen von lokalen Komponenten (Sensoren) ausgewertet und im Bedarfsfall lokale Komponenten zielgerichtet und kontextabhängig gesteuert (vgl. Abb. 2).

# 2 State of the Art

Der Einsatz von lokalen Komponenten und deren Vernetzung wird bereits seit einigen Jahren in nationalen und internationalen Projekten – teilweise mit nationaler oder europäischer Förderung – erprobt, wobei diese Projekte oft durch Universität und Institute wissenschaftlich begleitet werden (vgl. [Voss04]):

- „inhaus“, Duisburg, Deutschland,
- „FutureLife“, Hünenberg, Schweiz,
- „Das intelligente Haus“, Gifhorn, Deutschland,
- „VisionWohnen“, München, Deutschland,
- „AwareHome“, Atlanta, USA,
- “Trunified Haus”, Ahaus, Deutschland,
- „Internet Home“, London, GB,
- „HomeLab“, Eindhoven, Niederlande,

- „Smart Home“, Edinburgh, GB,
- “IT Neighborhood”, Stockholm, Schweden,
- “Wohnen für die Online-Generation”, Dornbirn, Österreich.

Da die Projekte allesamt eigenständig sind, ist die jeweilige Zielsetzung auch hochgradig individuell. Allen Projekten gemeinsam ist jedoch, dass jeweils ein Wohnhaus gebaut und ausgerüstet wurde, um an und in diesem Wohnhaus zielgerichtet spezielle Aspekte des Einsatzes von lokalen Komponenten und deren Vernetzung zu zeigen und zu erproben (vgl. Abb. 3).

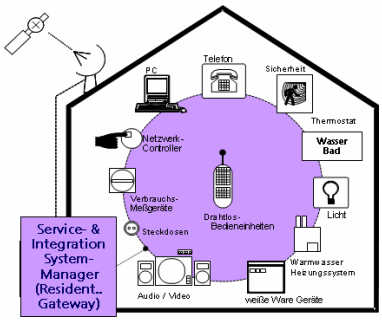


**Abbildung 3:** Steuerung von lokalen Komponenten

Unter anderem wurde in dem Projekt „Internet Home“ erprobt, wie die lokalen Komponenten eines einzigen Herstellers (Honywell) zur Steuerung einer Hauses genutzt und welche Netzwerkkomponenten eines weiteren Herstellers (Cicso) zur Vernetzung verwendet werden können. In dem Projekt „FutureLife“ werden ausgehend von einer Vernetzung von lokalen Komponenten im Küchenbereich des Wohnhauses insgesamt verschiedene Vernetzungstechniken (EIB, Powerline, AMX, TCP/IP, GSM) integriert genutzt, um die lokalen Komponenten zu steuern. In dem Projekt „Smart Home“ wurde erprobt, welche lokalen Komponenten erforderlich sind, um eine optimale Unterstützung des betreuten Wohnens zu erreichen. Die Erhöhung der sozialen Verantwortung und Kompetenz von Mietern eines Stadtteils, im wesentlichen durch die Vernetzung von lokalen Komponenten, wird in dem Projekt „IT Neighborhood“ verfolgt. Der Einsatz eines speziellen Bussystems (EIB) [Eber98] zur Vernetzung wurde in dem Projekt „Wohnen für die Online-Generation“ zusammen mit der Nutzung von beliebigen mobilen Endgeräten zur Steuerung von lokalen Komponenten gezeigt. Das primäre Ziel des Projekts „Das intelligente Haus“ war die Vernetzung von lokalen Komponenten zur Erhöhung der passiven Sicherheit eines Wohnhauses (Einbruchs-, Brand- und Leckagemeldungen), während sekundär durch lokale Komponenten die Verbrauchswerte für Strom, Wasser und Gas erfasst werden, um den sinnvolleren Umgang mit Energieressourcen zu erhöhen. Über verschiedene mobile und stationäre Endgeräte ist einerseits die Steuerung der lokalen Komponenten möglich und andererseits wird die Darstellung der Verbrauchswerte ermöglicht. Die Erprobung von lokalen Komponenten eines Herstellers (Philips) ist Gegenstand des Projekts „HomeLab“. Diese lokalen Komponenten sind in alltägliche Haushaltsgegenstände eingebettet (Badezimmerspiegel, etc.) und werden durch Nutzung von Methoden aus der künstlichen Intelligenz kontextabhängig und bedürfnisorientiert vom Benutzer durch die natürliche Sprache gesteuert. Eine Vernetzung der lokalen Komponenten steht hierbei aber nicht im Fokus. Die Nutzung von verschiedenen Vernetzungstechniken (EIB, LON, GSM) für lokale Komponenten verschiedener Hersteller wird in dem Projekt „Trunified Haus“ erprobt. Die Steuerung dieser lokalen Komponenten erfolgt durch einen zentralen Server, der in der Lage ist Daten

von lokalen Komponenten, die als Sensoren agieren, entgegen zu nehmen, entsprechend eines Regelwerks zu verarbeiten und wiederum Daten an lokale Komponenten (Aktoren) weiter zu leiten. In dem Projekt „VisionWohnen“ werden die primären lokalen Komponenten durch Einsatz des Bussystems EIB vernetzt, wodurch Maßnahmen zur Optimierung des Energieverbrauchs unterstützt werden können. Die Entwicklung einer intelligenten Umgebung zur Unterstützung des betreuten Wohnens speziell für ältere Menschen ist Gegenstand des Projekts „Aware Home“. Durch lokale Komponenten sollen in individuellen Lebensumständen Situationen erkannt werden, in denen eine Erinnerung, eine Warnung oder eine Hilfe für einen älteren Menschen erfolgen muss. Sofern mit lokalen Komponenten interagiert werden muss (Nachrichten vorlesen und bestätigen, Einstellungen vornehmen) erfolgt diese Interaktion über Gestiken, die von visuellen Hilfesystemen erkannt werden.

Bei diesen Projekten stand immer die Vernetzung von lokalen Komponenten und deren Steuerung durch mobile Endgeräte im Fokus, um dadurch eine Steigerung des Komforts für einen Bewohner eines Hauses zu erreichen. Die Realisierung einer Diensteplattform und die Entwicklung von it-gestützten Mehrwertdienstleistungen durch die Einbeziehung von Dienstleistern war bei diesen Projekten – mit Ausnahme des Projekts „FutureLife“, in dem Waren bestellt und von Partnern in die SkyBox geliefert werden – kein wesentlicher Forschungsgegenstand.

# 3 Smarter Wohnen

Die Erarbeitung einer Konzeption zur Ausstattung von Wohnungen, Gebäuden mit lokalen Komponenten und deren Vernetzung, die Konzeption und Realisierung einer Diensteplattform und die Entwicklung von it-gestützten Mehrwertdiensten sind Gegenstand des Fördervorhabens Smarter Wohnen NRW. Partner in diesem Vorhaben sind die Fraunhofer Institute IMS und ISST, das Zentrum für Telematik im Gesundheitswesen und die Hattinger Wohnstätten eG. Die Besonderheit dieses Fördervorhabens ist, dass in einem Modellprojekt durch die Hattinger Wohnstätten eG in einem ausgewiesenen Wohngebiet ca. 200 Wohnungen renoviert, modernisiert und aus-/umgebaut werden sollen. An diesem Modellprojekt wird einerseits die Praxisrelevanz der Konzepte validiert und andererseits deren Skalierbarkeit und Übertragbarkeit. Im Rahmen dieser Maßnahmen werden die neuen Wohnungen mit lokalen Komponenten ausgestattet und mit der erforderlichen Netzwerkinfrastruktur ausgerüstet. Hierdurch wird es möglich it-gestützte Mehrwertdienstleistungen sowohl in den Bereichen Gesundheit, Komfort und Sicherheit für Mieter als auch im Bereich Gebäudemanagement für EVU’s, etc. anzubieten.

Während durch ein Residential Gateway die Integration und die Kommunikation der lokalen Komponenten realisiert wird, wird durch eine Diensteplattform die Integration von einzelnen Diensten und deren Kommunikation untereinander realisiert (vgl. Abb. 4). Um zu gewährleisten, dass durch it-gestützte Mehrwertdienste lokale Komponenten gesteuert werden können, kommuniziert die Diensteplattform mit dem Residential Gateway.

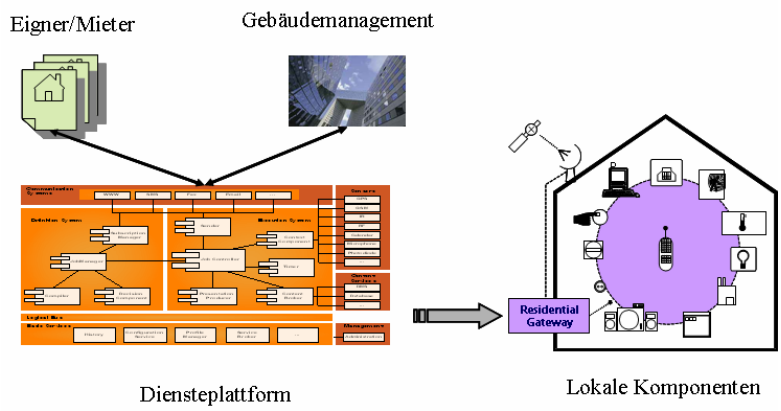


**Abbildung 4:** Diensteplattform für Mehrwertdienstleistungen

Neben der Tatsache, dass jede Wohnung spezifisch mit einer Menge von lokalen Komponenten ausgestattet ist, können lokale Komponenten sowohl etagen-, gebäude- oder campusspezifisch sein. Diese lokalen Komponenten müssen eindeutig identifizierbar und adressierbar sein, damit sie durch it-gestützte Mehrwertdienste als auch über mobile Endgeräte gesteuert werden können. Die eindeutige Adressierung erfolgt über ein Residential Gateway, welches entweder wohnungsspezifisch oder etagen-, gebäude- oder campusspezifisch ist.

Die eindeutige Adressierung soll mit dazu beitragen, dass Sicherheitsanforderungen gewährleistet werden können (vgl. [Rann00]):

- Vertraulichkeit (*Confidentiality*),
  Daten sollen unbefugten Personen nicht zur Kenntnis gelangen. Unbefugte Personen sind nicht nur Mieter anderer Wohnungen, Mitarbeitern des Wohnungsunternehmens, des Netzbetreibers und auch externen Personen (Hacker). Es muss gewährleistet werden, dass kein Dritter die übermittelten Daten verarbeiten kann.
- Integrität (*Integrity*),
  während einer Übermittlung sollen Daten nicht von unbefugten Personen verändert werden können.
- Verfügbarkeit (*Availability*),
  die Verfügbarkeit von Daten und die Erreichbarkeit von Personen kann nicht durch Dritte verhindert werden.

Neben diesen Sicherheitsanforderungen welche die Daten betreffen, die von Mehrwertdiensten benötigt und ausgetauscht werden, müssen Sicherheitsanforderungen gewährleistet werden, die die Partner beim Austausch von Daten betreffen.

- Authentizität (*Authentication*),
  es wird die Identität der Kommunikationspartner gewährleistet.
- Unwiderrufbarkeit (*Non-Repudiation*),
  es wird gewährleistet, das der Empfang von Informationen durch Kommunikationspartner nicht abgestritten werden kann (*NRO, NRR)*.

Diese Sicherheitsanforderungen können sowohl durch hard- und softwaretechnische als auch durch netzwerktechnische Maßnahmen erfüllt werden. Diese Maßnahmen können durch Verwendung von IPv6 zur Adressierung von lokalen Komponenten zusätzlich unterstützt werden.

# 4 IPv6

In die Konzeption von IPv6 wurden von der Internet Engineering Task Force (IETF) viele Erfahrungen im Umgang mit IPv4 integriert (vgl. Abb. 5). IPv6 bietet eine Adressierung von Netzwerkkomponenten durch eine 128Bit Adressierung, eine Vereinfachung des Headers und der Headerstruktur, integrierte Berücksichtigung von mobilen Endgeräten durch Mobile IP und Sicherheitsverfahren durch IPSec [Hind96].

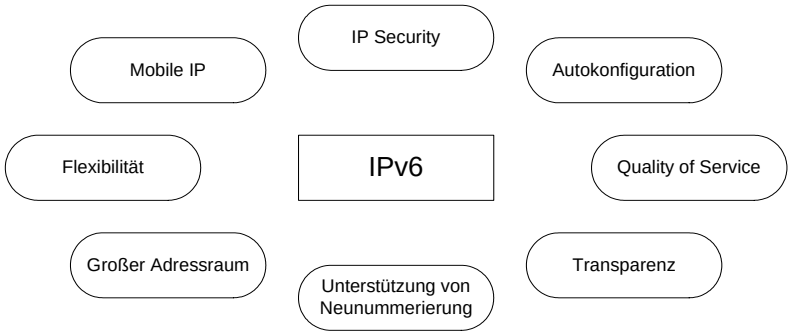


**Abbildung 5:** Komponentenübersicht von IPv6

Gelöscht: (Teil-)

Der Einsatz von IPSec und Mobile IP zur Gewährleistung der Sicherheit beim Smarter Wohnen werden hier skizziert. IPSec ist ein Protokoll, welches für den sicheren Austausch von Paketen auf der IP-Schicht entwickelt worden ist. Es können somit die wesentlichen Sicherheitsanforderungen (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Unwiderrufbarkeit) sowohl im Tunnel als auch im Transport Modus berücksichtigt werden.

Gerade mobile Endgeräte (z.B. PDA, Smartphone, ...) müssen einen einfachen Wechsel und einfache Integration in unterschiedliche Netze ermöglichen. Im Zusammenhang vom Smarter Wohnen werden mobile Geräte sowohl zur Steuerung der lokalen Komponenten einer Wohnung eingesetzt, als auch zur Kommunikation des Systems mit dem Bewohner. Der Bewohner kann über mobile Endgeräte seine Wohnung steuern, konfigurieren und it-gestützte Mehrwertdienste nutzen. Um Informationen aus der Wohnung (Warnmeldungen, usw.) oder Informationen von Dienstleistern (Dienstangebote, usw.) an die mobilen Endgeräte des Bewohners zu übermitteln, wird Mobile IP eingesetzt. Der Einsatz von Mobile IP ermöglicht die Adressierung eines mobilen Endgeräts, welches sich derzeit in einem öffentlichen Netz und nicht in seinem Smarter Wohnen Netz befindet. Für den Informationssender (Wohnung, Diensteplattform, Serviceanbieter) ist somit die Kommunikation mit dem Endgerät vollkommen transparent. Dies wird durch einen eingesetzten Agenten (Router) im Smarter Wohnen Netz sichergestellt.

Angesiedelt ist IPv6 auf der Netzwerkschicht des TCP/IP-Schichtenmodells. Somit besteht die Möglichkeit IPv6 in Netzwerkkomponenten (z.B. Router) zu integrieren ohne auf umfangreichere Applikationen aufbauen zu müssen. Diese direkte Integration des Paketroutings op-

timiert die Verarbeitung der IP-Pakete, so dass ein wesentlich besseres und sichereres weiterleiten der Pakete bis zu den lokalen Komponenten unterstützt werden kann [GaAF03].

## 4.1 IPSec

IPSec erweitert das IP-Protokoll um Sicherheitsfunktionen, kryptischen Algorithmen und Verschlüsselungsverfahren. Zusätzlich kann IPSec flexibel zum Aufbau einer End-zu-End als auch einer Virtual-Privat-Network (VPN) Verbindung eingesetzt werden.

Damit die einzelnen IPSec-Datagramme verarbeitet werden können, werden Informationen über die zur Verfügung stehenden Verschlüsselungsverfahren sowie über deren Parameter benötigt. Hierzu wird für IPSec so genannte Security Assoziation (SA), welche die Kommunikationsbasis einer IPSec-Verbindung darstellt, definiert. Je Header (Authentication Header (AH) und Encapsulation Securtity Payload (ESP) Header) wird eine eigene SA benötigt. Das Konstrukt der SA setzt sich aus dem Security Parameter Index (SPI) und der Zieladresse zur eindeutigen Identifizierung einer SA zusammen. In der Security Association Database (SADB) werden die SA persistent gespeichert.

Die wesentlichen Funktionen zur Gewährleistung der Sicherheit werden von den folgenden drei Komponenten unterstützt und ausgeführt (vgl. Abb. 6):

- Key Managment (KM)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

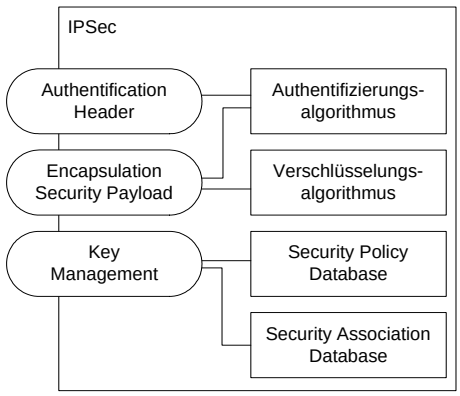


**Abbildung 6:** Komponenten von IPSec

**Gelöscht:** (skizziert)

### 4.1.1 Key Managment (KM)

Die Schlüsselverwaltung kann zum einen manuell geschehen (heute nicht mehr gebräuchlich) und zum anderen kann das Internet Key Exchange (IKE) Protokoll eingesetzt werden. IKE ist ein weltweit anerkannter Standard zum sicheren und automatischen Schlüsselaustausch. Eingesetzt wird IKE beispielsweise bei Virtuell Privaten Netzwerken (z.B. für Telearbeit). Hierzu werden von den beteiligten Kommunikationspartnern viele Parameter, wie zum Beispiel Verschlüsselungsalgorithmus, Schlüssel und Gültigkeitsdauer des Schlüssels, ausgetauscht. Diese Parameter werden in der SA erfasst, wodurch eine SA bei jeder gesicherten Verbindung

benötigt wird. Nachteilig ist derzeit, dass keine adäquate Authentifizierung von dynamisch vergebenen Adressen zum Besitzer möglich ist [Nika01].

### 4.1.2 Authentication Header (AH)

Der Authentication Header wird zur Wahrung der Paketintegrität, Paketauthentizität und zum Schutz vor Wiedereinspielung eingesetzt. Dieses wird durch Hashing-Verfahren wie zum Beispiel MD5 oder SHA-1 sichergestellt. Der AH kann im Transport- und Tunnelmodus eingesetzt werden und Unterstützt somit sowohl eine End-zu-End als auch eine VPN Verbindung. Zu jedem AH gehört ein Security Parameter Index (SPI) und eine Sequence Number (SN) (vgl. Abb. 7). Während der SPI im Rahmen der SA verwendet wird, stellt die SN den Schutz vor Wiedereinspielung sicher. Durch die SN kann somit ein Denial of Service (DoS) unterbunden werden.

| 8 Bit | 8 Bit | 8 Bit | 8 Bit |
|---|---|---|---|
| Next Header | Hdr. Ext. Leng | Reserved | |
| Security Parameters Index (SPI) | | | |
| Sequence Number (SN) | | | |
| Authentication Data (variable) | | | |

**Abbildung 7:** Authentication Header

### 4.1.3 Encapsulating Security Payload (ESP)

Zusätzlich zu den Möglichkeiten welche vom AH unterstützt werden, bietet der ESP Header Vertraulichkeit. Um die Vertraulichkeit zu unterstützen wird nach dem IP-Header ein ESP-Header und nach dem Datenpaket ESP-Trailer eingefügt (siehe Abb. 8). In Analogie zum AH besitzt auch das ESP ein SPI und eine SN zur Identifizierung der SA.

Da vom ESP sowohl Vertraulichkeit als auch Authentizität sichergestellt werden kann, müssen in der SA zwei Verfahren definiert werden. Ein Verfahren zur Verschlüsselung der Daten und ein Verfahren für die Authentifizierung. Im ESP kann auf ein Verfahren (Verschlüsselung oder Authentifizierung) verzichtet werden, keinesfalls auf beide. Zur Verschlüsselung muss mindestens Data Encryption Standard (DES) unterstützt werden. Weitere Verfügbare Verschlüsselungsalgorithmen können eingesetzt werden, solange diese von beiden Verbindungspartnern unterstützt werden.

| 8 Bit | 8 Bit | 8 Bit | 8 Bit |
|---|---|---|---|
| Next Header | Hdr. Ext. Leng | Reserved | |
| Security Parameters Index (SPI) | | | |
| Sequence Number (SN) | | | |
| Payload Data (variable) | | | |
| | Padding | | |
| | | Pad Length | Next Header |
| Authentication Data (variable) | | | |

**Abbildung 8:** ESP-Header

### 4.1.4 Headerkombination für erhöhte Sicherheit

Eine verschachtelte Verwendung der beiden Optionen AH und ESP ist denkbar (vgl. Abb. 9). Zu erst wird mit Hilfe des AH die Sicherung der Integrität, der Authentizität und der Schutz

**Gelöscht:** ¶

**Formatiert:** Nummerierung und Aufzählungszeichen

vor Wiedereinspielung unterstützt. Im Anschluss stellt ESP-Header die Vertraulichkeit durch Verschlüsselung der Daten (inklusive AH) sicher. Bei Verwendung eines Tunnelmodus sowohl zwischen der Wohneinheit und der Diensteplattform als auch zwischen der Diensteplattform und dem Serviceanbieter, wird die (Abhör-)Sicherheit der Daten erhöht.

Der Kombinierte Einsatz von AH und ESP Header stellt ein erhöhtes Maß an Sicherheit dar, so dass ein direkter Zugriff auf die lokalen Komponenten einer Wohnung unterbunden werden kann. Nach außen ist lediglich die Adresse des Gateways des Smarter Wohnen Netz sichtbar. Die Adresse der lokalen Komponenten ist hinter der AH geschützt und durch den ESP Header verschlüsselt.

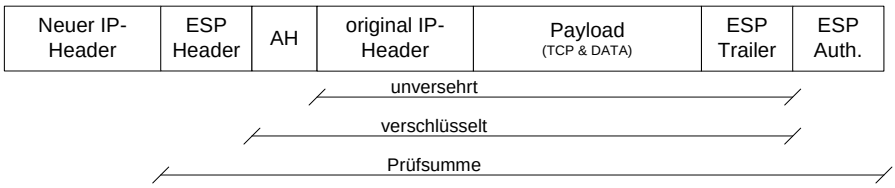


**Abbildung 9:** IP-Paket mit verschachteltem AH und ESP Header (Tunnelmodus)

## 4.2 Mobil IP

Mobilen Endgeräten muss es ermöglicht werden, einen einfachen Netzwechsel zu vollziehen. Bei einem Netzwechsel bekommt das mobile Endgerät eine neue IP vom DHCP des neuen Netzes zugewiesen. Bei einer anderen Möglichkeit bestimmt das mobile Endgerät seine IP selbst und verbreitet sie im Subnetz. Wenn keine Rückmeldung erfolgt, dass die Adresse bereits von einem anderen Gerät in diesem Subnetz verwendet wird, dann behält das mobile Endgerät seine ausgewählte IP. Ansonsten beginnt der Vorgang mit einer neu ausgewählten IP von neuem. Das einzusetzende Verfahren ist abhängig von der jeweiligen Netzstruktur. Folglich hat ein mobiles Endgerät in jedem Netzwerk eine eigene Adresse. Beim IPv6 wird dieses durch die Autokonfiguration [ThNa98, IPv604a] unterstützt und realisiert die Eigenschaft zum „Plug and Play“ der einzelnen Komponenten. Die Autokonfiguration bildet folglich die essentielle Bedingung für mobile Geräte, ohne die ein Netzwechsel nur schwer möglich wäre.

Nachdem für mobile Geräte die Autokonfiguration genutzt wird, ist noch zu klären, wie die Identität des mobilen Gerätes trotz öffentlichen Netzes gewährleistet werden kann. Hierzu muss eine sichere Verbindung zwischen der alten Adresse (im Smarter Wohnen Netz) und der neuen Adresse (im öffentlichen Netz) hergestellt werden [ShRo01]. Die Verbindung wird unterhalb der Vermittlungsschicht aufgebaut, so dass Transparenz für Protokolle auf einer höheren Schicht erreicht wird. Realisiert wird dieses durch Agenten im Smarter Wohnen Netz des mobilen Endgeräts.

Der Einsatz von Mobile IP ermöglicht die transparente Nutzung von mobilen Endgeräten mit einer definierten „care-of address“ [PeJo96]. Über diese „care-of address“ kann somit das mobile Geräte über seine Adresse im Smarter Wohnen Netz erreicht werden. Ein im Smarter Wohnen Netz angesiedelter Agent, fängt Pakete im Smarter Wohnen Netz ab, welche an das mobile Endgerät geschickt werden sollten. Der Agent hält die neuen Adressinformationen des mobilen Endgeräts aus dem öffentlichen Netz in der „care-of address“ vor. Je mobilen Endgeräts kann nur eine primär gültige „care-of address“ vorgehalten werden.

Zum Kommunikationsaufbau zwischen dem Informationssender und dem mobilen Endgerät werden verschiedene Optionen eingesetzt (vgl. Abb. 10). Verfügt ein mobiles Endgerät über eine Internetverbindung ist aber nicht im Smarter Wohnen Netz, dann wird ein Binding-Update (1) an den Agenten im Smarter Wohnen Netz gesendet. Zur Bestätigung des Binding-Update wird ein Binding-Acknowledge (2) übermittelt. Die Binding-Update und Binding-Acknowledgement Optionen sind ebenso wie die Binding-Request Option und die Home-Address Option eine von Mobil IP ausgeprägte „Destination Option“. Das Binding-Update enthält die „care-of address“ zum mobilen Geräte. Binding-Update und Binding-Acknowledgment können zusätzlich von anderen Netzknoten abgefangen und im Binding-Cache zwischengespeichert werden. Somit kann bei einem gültigen Binding im Cache ein Paket direkt an das mobile Endgerät gesendet werden. Bei dieser Optimierung Bedarfs es keiner weiteren Verbindung zum Agenten im Smarter Wohnen Netz. Eine genauere Auseinandersetzung bezüglich Binding ist in [JoPA04] zu finden.

Werden nun IP-Pakete an die Adresse des mobilen Gerätes im Smarter Wohnen Netz gesendet (3), dann kann das Paket direkt an die primäre „care-of address“ weitergeleitet (4) werden. Somit ist für den Absender die Erreichbarkeit des mobilen Endgerätes vollkommen transparent, da es vom Smarter Wohnen Netz sichergestellt wird. Kommt nun eine Verbindung zwischen Informationssender und mobilen Endgerät zustande (5+6), dann kann die weitere Kommunikation direkt zwischen den Kommunikationspartnern (6) stattfinden, da die „care-of addresse“ und die Absenderadresse bekannt sind.

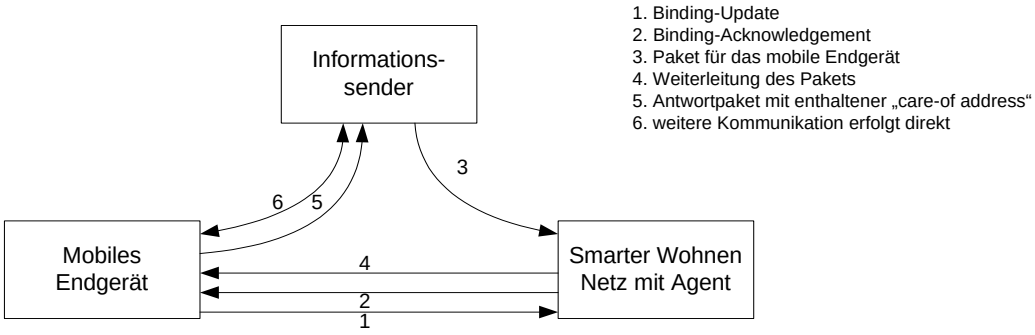


**Abbildung 10:** Kommunikationsaufbau von mobilem Endgerät und Informationssender [IPv604b]

Bezüglich der Skalierbarkeit und der Auslastung des Netzes ist es wichtig, dass die Knotenpunkte lernfähig bezüglich der „care-of address“ eines mobilen Gerätes sind. Ein optimales routen der Pakete zwischen dem Absender und dem mobilen Endgerät kann durch das cachen von Adressen sichergestellt werden. Folglich können Pakete bereits vor dem Agenten im Smarter Wohnen Netz abgefangen und an das mobile Endgeräte zugestellt werden.

# 5 Schluss

Durch eine informationslogistische Diensteplattform zur Realisierung von it-gestützten Mehrwertdienstleistungen einfache Wohnungen zu smarten Wohnungen erweitert. Die lokalen Komponenten werden somit nicht nur direkt durch die Bewohner einer Wohnung genutzt, sondern liefern zusätzliche Informationen für externe Dienstleistungsanbieter. Gerade diese Kopplung wird derzeit in keiner weiteren (Pilot-)Anwendung umfassend unterstützt. Die

**Gelöscht:** E

**Gelöscht:** r

**Gelöscht:** erweitert den Horizont von smarten Wohnungen

**Gelöscht:** für die eigenen Bedürfnisse

Angst, das persönliche Daten anderweitig genutzt werden können und somit der Bewohner zum gläsernen Mensch wird, muss abgebaut und reduziert werden, damit die Mehrwertdienstleistungen in den Bereichen Gesundheit, Komfort und Sicherheit akzeptiert werden.

Mit dem Fokus auf IPv6 lassen sich die zukünftigen lokalen Komponenten einzelnen adressieren und ansprechen, ohne aufwendige Softwarekomponenten, welche die Sicherheit der Kommunikation gewährleisten, zu implementieren. Lokale Komponenten in der smarten Wohnung lassen sich beispielsweise regelbasiert für mehrere it-gestützte Mehrwertdienstleistung nutzen, so dass der Nutzen einer lokalen Komponente gesteigert werden kann. Ebenfalls können die lokalen Komponenten einfacher an die jeweilige Lebenssituation angepasst werden, um als Informationslieferant zu dienen. Folglich werden die it-gestützten Mehrwertdienstleistungen bei einfacher Bedienbarkeit und guten Geschäftsmodellen eine zukünftige Marktakzeptanz aufbauen und dazu beitragen, das Wohnungsunternehmen ihren Mieterbestand sichern können.

Gelöscht: Haushaltsgeräte

Gelöscht: regelbasieren

Die Sicherheit mit IPSec ab der Netzwerkschicht zu realisieren, ermöglicht eine unabhängige Nutzung von it-gestützten Mehrwertdiensten. Diese Unabhängigkeit wird dadurch erreicht, dass nicht für jede Anwendung das Sicherheitskonzept neu implementiert werden muss. Darüber hinaus ist IPSec sowohl zu IPv4 als auch zu IPv6 kompatibel und ermöglicht den Einsatz im Transport- und Tunnelmodus. Zukünftig wird das IPv4 Netz sukzessive abgebaut und durch ein umfassenderes IPv6 Netz ersetzt. Dieser Schritt wird langsam von statten gehen, allerdings muss dieses bei zukünftigen und langfristigen Investitionen, wie hier der Wohnungsmarkt, berücksichtigt werden.

Gelöscht: Anwendungen

Trotz der realisierbaren Vorteile aufbauend auf die it-gestützten Mehrwertdienstleistungen muss die Akzeptanz bei den Bewohnern für jede Mehrwertdienstleistung geprüft werden. Der Nutzen einer Mehrwertdienstleistung ist für jeden Bewohner, jede Bewohnergruppe (Single und Familien, Jung und Alt) unterschiedlich und kann daher nicht allgemeingültig getroffen werden.

Gelöscht: ¶

## Literatur


[Voss04] Vossen, G.; et. al.: Vernetzung und Netzwerk in privaten Haushalten. Informationssysteme Report, Leonardo Computing GmbH, 2004

[Rann00] Ranneberg, K.: Mehrseitige Sicherheit – Schutz für Unternehmen und ihre Partner im Internet. In: Wirtschaftsinformatik, Band 42, Heft 6, Vieweg Verlag Wiesbaden, 2000, pp. 489-499

[Broy02] Broy, M.; et. al.: Integrierte Gebäudesysteme – Technologien, Sicherheit und Märkte. SecuMedia Verlag, Ingelheim, 2002

[Trän01] Tränkler, H.-R.; Schneider, F. (Hrsg.): Das intelligente Haus Wohnen und Arbeiten mit zukunftsweisender Technik. Pflaum Verlag, 2001

[ThNa98] Thomson S.; Narten T.: IPv6 Stateless Address Autoconfiguration. IETF Network Working Group, RFC2462, http://www.ietf.org/rfc/rfc2462.txt, zuletzt besucht am 01.10.2004.

[ShRo01] O'Shea G., Roe M.: Child-proof authentication for MIPv6 (CAM). In: ACM SIGCOMM Computer Communications Review, Vol. 31, Issue 2, April 2001, pp 4-8.

[Eber98] Eberl, U.; Vernetzte Helfer im mitdenkenden Haus. In: Spektrum der Wissenschaft, Spektrum Verlag, Mai 1998, pp. 87 – 92.

[PeJo96] Perkins Ch. E., Johnson D.B.: Mobility Support in IPv6. In: International Conference on Mobile Computing and Networking, ACM Press, New York 1996, pp. 27-37.

[Hind96] Hinden R.M.: IP-Next Generation Overview. In: Communications of the ACM, Vol. 39, Nr 6, New York 1996, pp. 61-71.

[GaAF03] Garyfalos A., Almeroth K., Finney J.: A comparison of network and application layer multicast for mobile IPv6 networks. In: International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, ACM Press, New York 2003, pp. 58-65.

[Nika01] P. Nikander: Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World. In: Cambridge Security Protocols Workshop 2001, April 25-27, Cambridge University, 2001.

[JoPA04] D. Johnson, C. Perkins, J. Arkko: Mobility Support in IPv6. IETF Network Working Group, RFC 3775, http://www.ietf.org/rfc/rfc3775.txt, zuletzt besucht am: 01.10.2004.

[IPv604a] IPv6Net: IPv6 – Eine Übersicht – Mobile IPv6.
http://www.ipv6-net.org/themen/uebe/page10.php#5_1
zuletzt besucht am: 06.10.2004.

[IPv604b] IPv6Net: IPv6 – Eine Übersicht – Mobile IPv6.
http://www.ipv6-net.org/themen/uebe/page11.php#6_1
zuletzt besucht am: 06.10.2004.