Anhang A: Glossar

Abmeldung

Fortzug aus einer Gemeinde ins Ausland unter Auflösung aller Wohnungen in dieser Gemeinde (in eine andere Gemeinde oder ins Ausland). Der Datensatz wird inaktiv.

Alleinige Wohnung

Hat die meldepflichtige Person in der Bundesrepublik eine Wohnung bezogen, so ist diese ihre alleinige Wohnung im Sinne des Melderechts.

Anmeldung

Zuzug in eine Gemeinde. Der Datensatz wird neu angelegt oder aktiviert (Wiederzuzug).

Aufgabe einer Nebenwohnung

Auszug aus der Wohnung

Authentizität

Authentizität ist die Sicherheit darüber, dass eine nachricht auch tatsächlich von dem behaupteten Verfasser oder Sender einer Nachricht stammt. Man sichert Authentizität, um sich vor falschen Absendern zu schützen.

In dem Kontext *"Meldewesen"* muss beispielsweise sichergestellt sein, dass Datenübermittlungen an andere Bhörden nach § 18 MRRG nur dann erfolgen, wenn über die Identität der anderen Behörde kein Zweifel besteht. Es muss also die Authentizität des Absenders einer Bitte um Datenübermittlung gesichert werde um auszuschliessen, dass sich Unberechtigte durch Vorspiegelung falscher Identitäten in den Besitz personenbezogener Daten bringen.

Die Authentizität und die Integrität einer Nachricht können mit Hilfe elektronischer Signaturen bewiesen werden.

Beigeschriebene Person

Als *beigeschriebene Person* (auch gebräuchlich: *"Hinweis-Ehegatte"*, *"Hinweis-Kind"*, *"Pseudo-Einwohner"*) wird im Meldewesen eine Person bezeichnet, die in der örtlichen Meldebehörde nicht gemeldet ist, aber in einer rechtlichen Beziehung zu einem (gemeldeten) Einwohner der örtlichen Meldebehörde steht. Das können zum Beispiel sein:

- ein Ehegatte, der in einer anderen Gemeinde oder im Ausland gemeldet ist (seinen Aufenthalt hat),
- ein Elternteil (oder beide), der in einer anderen Gemeinde oder im Ausland als sein Kind gemeldet ist (den Aufenthalt hat),
- ein Kind, das in einer anderen Gemeinde als die Eltern / ein Elternteil gemeldet ist, oder
- ein gesetzlicher Vertreter zu einer Person, der in einer anderen Gemeinde als sein Mündel gemeldet ist.

Für die Aufgabenerledigung der örtlichen Meldebehörde dürfen über diese Personen Daten in einem gesetzlich normierten Umfang (§ 2 Abs. 1 MRRG) erhoben werden — obwohl sie nicht Einwohner dieser Gemeinde sind.

Einfache Melderegisterauskunft

Vor- und Familienname, Anschriften, Doktorgrad. Siehe §21 Abs. 1 und 1a MRRG.

Erweiterte Melderegisterauskunft

Eine einfache Melderegisterauskunft sowie zusätzliche Daten, deren Anfrageberechtigung nachzuweisen ist (lt. MRRG § 21, Abs. 2).

Gesamtauskunft an den Betroffenen

Vollständige Auskunft über alle zur anfragenden Person gespeicherten Daten, vgl. MRRG § 8.

Hauptwohnung

Hat die meldepflichtige Person in der Bundesrepublik mehrere Wohnungen, so ist eine dieser Wohnungen die Hauptwohnung, und zwar diejenige, die vorwiegend benutzt wird.

MEDIA@Komm

MEDIA@Komm ist eine Initiative der Bundesregierung, um die Entwicklung und Anwendung von Multimedia in Städten und Gemeinden gezielt zu unterstützen. Hierzu wurde 1998 ein Städtewettbewerb ausgelobt, an dem sich 136 Städte und Gemeinden mit ihren Konzepten beteiligt haben. 1999 wurden durch eine Jury die drei Preisträger Bremen, Esslingen und der Städteverbund Nürnberg ermittelt.

In einem integrativen Ansatz sollen im städtischen Raum innovative multimediale Dienste und Anwendungen möglichst unter Nutzung der digitalen Signatur entwickelt und deren Möglichkeiten und wirtschaftlichen Potenziale demonstriert werden. Zwischen öffentlicher Verwaltung, Bürgern und Wirtschaft sollen rechtsverbindliche Dienstleistungen und Transaktionen vollelektronisch ohne Medienbrüche getätigt werden können (*“virtuelles Rathaus”*, *“elektronische Akte”*, *“Bürgerkarte”*), um so Effizienz und Transparenz von Verwaltungs- und Geschäftsvorgängen zu verbessern. Durch die modellhafte Entwicklung und Erforschung der rechtlichen, technischen und ökonomischen Voraussetzungen für die *“virtuelle Stadt”* sollen

- die Arbeits- und Lebensbedingungen der Bevölkerung verbessert,
- die Verwaltungen effizienter und bürgerfreundlicher,
- die Unternehmen flexibler und produktiver werden.

Hierzu bedarf es insbesondere der Nutzung digitaler Signaturen, die auf Chipkarten gespeichert werden. Diese Karten mit den so genannten privaten Schlüsseln ermöglichen einen vertrauenswürdigen und sicheren elektronischen Geschäftsverkehr.

Nebenwohnung

Weitere Wohnungen neben der Hauptwohnung.

OSCI–Transport

Ein Protokollstandard zur vertraulichen und sicheren Übermittlung von Nachrichten in einer auf das deutsche Signaturgesetz abgestimmten Sicherheitsumgebung. Die Entwicklung begann im Rahmen des MEDIA@Komm Städtewettbewerbs. OSCI ist vor allem in Hinblick auf Kommunikationsanforderungen im E–Government zugeschnitten.

OSCI–Transport Nachrichten haben einen zweistufigen *“Sicherheitscontainer”*. Dadurch ist es möglich, Inhalts- und Nutzungsdaten streng voneinander zu trennen und kryptografisch unterschiedlich zu behandeln. Die Inhaltsdaten werden vom Autor einer OSCI–Transport-Nachricht so verschlüsselt, daß nur der berechtigte Leser sie dechiffrieren kann. Die Nutzungsdaten werden vom Intermediär für die Zwecke der Nachrichtenvermittlung und die Erbringung der Mehrwertdienste benötigt, sie werden deshalb für den Intermediär verschlüsselt. Ein Angreifer kann wegen dieser Verschlüsselungen weder die Nutzungs-, noch die Inhaltsdaten abhören.

Jeder Sicherheitscontainer (für Nutzdaten und Inhaltsdaten) erlaubt die digitale Signatur und die Verschlüsselung des jeweiligen Inhalts. Dadurch sind Vertraulichkeit, Integrität und Authentizität der Nachrichten gewährleistet.

Die Public Key Infrastruktur innerhalb der OSCI Kommunikationspartner ist — zumindest für natürliche Personen — in der Regel die durch das deutsche Signaturgesetz definierte. Es gibt somit keine geschlossene Benutzergruppe. Der Besitz einer Signaturkarte mit einem Signaturzertifikat nach SigG und einem Verschlüsselungszertifikat sind für die OSCI-Kommunikation ausreichend. Je nach Sicherheitsanforderung kann auch der Einsatz fortgeschrittener elektronischer Signaturen (ohne Chipkarte) sinnvoll sein, auch dies wird durch OSCI–Transport unterstützt.

Elektronische Signatur

Werden digitale Dokumente elektronisch signiert, so kann bei einer anschliessenden Prüfung zweierlei bewiesen werden:

- das signierte Dokument wurde nicht nachträglich geändert oder manipuliert
- das Dokument wurde tatsächlich vom Inhaber des Signaturzertifikats unterschrieben

Die elektronische Unterschrift dient somit nur der Wahrung der Integrität und der Authentizität. Sofern zusätzlich die Vertraulichkeit gefordert ist, muss dies durch zusätzliche Maßnahmen (zum Beispiel Verschlüsselung des Nachrichteninhalts) bewerkstelligt werden.

Das Anbringen einer elektronischen Signatur läuft im Prinzip wie folgt ab:

1. Über den Nachrichteninhalt wird ein Hashwert berechnet. Dieser ist eindeutig durch den Nachrichteninhalt bestimmt. Jede Veränderung am Nachrichteninhalt hat sofort einen anderen Hashwert zur Folge.
2. Der Signierende verschlüsselt diesen Hashwert mit einem privaten Schlüssel, der nur ihm zugänglich ist.
3. Der Nachrichteninhalt und der verschlüsselte Hashwert werden zusammen an den Empfänger der Nachricht übermittelt.

Anschließend kann die Signatur wie folgt geprüft werden:

4. Der Empfänger nutzt den öffentlichen Schlüssel des Absenders, um den Hashwert zu dechiffrieren. Dieser Schlüssel ist öffentlich verfügbar. In der Public-Key-Infrastruktur des deutschen Signaturgesetzes wird die korrekte Zuordnung eines öffentlichen Schlüssels zu einer Person durch die Zertifikatsherausgeber, zum Beispiel die TeleSec oder Signtrust, gewährleistet. Sofern der Versuch des Dechiffrierens zu einem Erfolg führt, kann sich der Empfänger sicher sein, dass derjenige signiert hat, dessen Namen im Zertifikat des öffentlichen Schlüssels eingetragen ist. Niemand sonst besitzt den privaten Schlüssel, mit dem der Hashwert zuvor chiffriert worden war.
5. Der Empfänger berechnet nach der gleichen Methode wie der Signierende einen Hashwert über den Nachrichteninhalt. Er vergleicht diesen mit dem Hashwert, den ihm der Sender verschlüsselt übermittelt hat. Sind beide Werte gleich, kann sich der Empfänger sicher sein, dass ihm die Nachricht in der gleichen Form vorliegt, wie der Sender sie unterschrieben hat. Jede Veränderung nach Signaturerstellung hätte zu einem anderen Hashwert geführt.

Ummeldung

Umzug innerhalb einer Gemeinde von Adresse A nach Adresse B ohne Veränderung der übrigen Daten.

Wohnungsaufgabe

Im MRRG wird in § 11 nur von dem *“Beziehen einer Wohnung”* bzw. vom *“Ausziehen aus einer Wohnung”* inkl. damit verbundener Abmeldung gesprochen.

Wohnungsbegründung

Beziehen einer Wohnung mit Anmeldung, vgl. MRRG § 11.

Digitales Zertifikat

Ein digitales Zertifikat ist eine Datenstruktur, welche die Zuordnung von Attributen zu einem Objekt bestätigt.

Im Rahmen des Signaturgesetzes bestätigt zum Beispiel eine akkreditierte Zertifizierungsstelle, dass ein bestimmter öffentlicher Signaturschlüssel zu einer Person mit einem bestimmten Vor- und Familiennamen gehört. Durch den Einsatz dieser Zertifikate ist man also nicht auf die Behauptung des Absenders über seinen Namen angewiesen, sondern dieser Name wird vom Zertifikatsherausgeber bestätigt.

Eine sehr wichtige, konkrete Datenstruktur für digitale Zertifikate ist das X.509 Format.
