Utimaco LIMS

Elemente einer modernen Lösung zur gesetzeskonformen Überwachung von Telekommunikationsdiensten

Inhaltsverzeichnis

1 Aufgaben von Lawful Interception 3
2 Lawful Interception im 21. Jahrhundert 5
2.1 Wachsender Bedarf für Lawful Interception 6
2.2 Grundlagen aus der Gesetzgebung 7
2.2.1 Nationale Gesetze 7
2.2.2 Die Europäische Union 8
2.2.3 Das Europäische Institut für Telekommunikationsnormen 8
2.2.4 Die Vereinigten Staaten 9
2.2.5 Das "3rd Generation Partnership Project" 9
2.2.6 Lösungen zur Einhaltung der Gesetze 10
3 Interception Grundlagen 12
3.1 Rollen und Funktionsbereiche 12
3.2 Schlüsselkomponenten für Lawful Interception 13
3.3 Vertrauens- und Ethikstandards bei Lawful Interception 15
4 Annäherung an die Problematik 17
4.1 LIMS Systemarchitektur 17
4.2 Aktive, passive und hybride Interception 18
4.3 Grundfunktionen von LIMS 22
4.4 Vorteile von LIMS 22
4.5 Zusammenfassung 23
5 Weiterführende Informationen 24
5.1 Interception-Gesetze 24
5.2 Interception-Standards 25
6 Glossar und Abkürzungsverzeichnis 26

1 Aufgaben von Lawful Interception

Mit dem weltweiten Popularitätsgewinn immer neuer Formen elektronischer Kommunikation – insbesondere auf Internettechnologien basierender digitaler Kommunikation – hat sich der Bedarf für Lawful Interception (LI) grundlegend verändert. In vielen Ländern geltende behördliche Regelungen stellen für Telekommunikationsfirmen, Netzbetreiber und Serviceanbieter in ihrem Streben nach Erfüllung aktueller Anforderungen eine erhebliche Herausforderung dar. Die in den letzten Jahren für die Befolgung lokaler und nationaler Regeln entwickelten Tools unterscheiden sich beträchtlich von den Lösungen solcher Zeiten, zu denen Lawful Interception vornehmlich das Fernsprechnetz betraf und eine simple Überwachung eines geschlossenen Netzwerks erlaubte. Im jetzigen digitalen Zeitalter bietet das Internet mehrere Mittel für Nachrichtenaustausch und Sprechverbindungen — über ein unbegrenzteres und dynamischeres Telekommunikationsnetzwerk als das Fernsprechnetz. Die Unternehmen geraten in die Pflicht, ihre Netzwerkinfrastrukturen zu verändern und zu erweitern, um die notwendigen Rahmenbedingungen für Lawful Interception zu erfüllen und die Techniken zu unterstützen, die eine Erfassung und Analyse von Kommunikationsdaten zur Beantwortung von Strafverfolgungsanfragen erlauben.

Die Komplexität der heutigen Kommunikationsumgebung erhöht den Bedarf an Lawful Interception-Tools und betrifft den breiten Bereich von drahtgebundenem und drahtlosem Kommunikationsaustausch. Diese Tools benötigen die Interoperabilität, um einfach in vorhandene Netzwerkinfrastrukturen integriert zu werden, außerdem die Funktionssicherheit, um realen Herausforderungen in bewährter und sicherer Weise zu begegnen. Ungeachtet der genutzten Architektur oder Technologie in Lawful Interception-Aktivitäten müssen effektive Lösungen auf Abruf bereitstehen um ermächtigten Behörden auf alle gesetzlich legitimierten Überwachungsanfragen die geforderten Informationen beschaffen zu können.

Dieses Dokument diskutiert die Bestandteile einer erfolgreichen Lawful Interception-Lösung aus der Perspektive der Unternehmen, die eine Umstrukturierung ihres Netzwerks gemäß den aktuellen Anforderungen planen. Die Zielgruppe schließt

Netzbetreiber mit festen und mobilen Installationen, Internetprovider, Telefongesellschaften, Systemintegratoren und Strafverfolgungsbehörden ein.

2 Lawful Interception im 21. Jahrhundert

Die Kommunikationsmedien des 21. Jahrhunderts sind vielseitig, universell einsetzbar und basieren auf einer wachsenden Menge von technischen Möglichkeiten. Moderne Kommunikationsnetze bieten den Zugang über eine große Palette von Technologien, wie z.B. PSTN, ISDN, xDSL, WLAN, WiMax, GSM, GPRS, UMTS, CDMA, Kabel, und andere auf dem Internet Protokoll (IP) basierende Technologien.

Beschränkten sie sich vor wenigen Jahren noch auf ein festes Netzwerkmodell, umfassen Sprechverbindungsdienste heute kabellose Technologien wie Mobiltelefone und internetbasierten Informationsaustausch wie Voice-over-IP (VoIP). Ebenso werden Datendienste wie Videodienste, Faxdienste, Short Message Services (SMS), E-Mail, Bildübertragungen i. Internetbasierte Kommunikation ist mittlerweile allgegenwärtig, neben den Basismöglichkeiten von E-Mail-Kommunikation werden heute auch Instant Messaging, Peer-to-Peer-Netzwerke (P2P), Chatdienste und preiswerte Sprechverbindungen durch eine Vielzahl von Unternehmen angeboten. Hinzu kommen neu entstandene Technologien wie das Session Initiation Protocol (SIP).

Das Wesen des Internet lässt außerdem ahnen, dass in Zukunft neue Anwendungen und innovative Tools entwickelt werden, die unsere Kommunikationsmöglichkeiten in unvorhersagbarer Weise erweitern. Angesichts dieser Überflüsse an Kommunikationsmöglichkeiten benötigen nationale Sicherheitsorganisationen und Exekutivorgane Mechanismen und bewährte Techniken, um kriminelle Aktivitäten und terroristische Operationen aufzuspüren.

Der Bedarf an Lösungen zur Strafverfolgung wächst mit der sich kontinuierlich entfaltenden Dynamik des Marktes und der Entwicklung von gesetzlichen und behördlichen Rahmenbedingungen. Netzbetreiber, ISPs, Telefongesellschaften und andere sind mit der beispiellosen Verpflichtung gegenüber der Allgemeinheit und den Behörden konfrontiert, ihre Arbeitsabläufe und Infrastrukturen anzupassen, um ausgewählte Zieldaten aus dem gewaltigen Informationsfluss ihrer TK-Dienste extrahieren und überwachen zu können. Zum Beispiel kann die Überwachung einer einzigen E-Mail durch die große Menge an IP-Traffic, die durch einen typischen Internet-Knoten wie z.B. DE-CIX geleitet wird, eine große Herausforderung für einen Betreiber bedeuten. Immerhin transportiert das DE-CIX im Mittel 41.3 Gigabits (Gbps) pro

Sekunde[1]. Hier wird deutlich, dass modernste Technologie nötig ist, um gesetzliche Überwachungsaktivitäten für solche breitbandigen Dienste zu bewältigen.

2.1 Wachsender Bedarf für Lawful Interception

Die weltweite Explosion von Kommunikationstechnologien erzeugt beachtliche Herausforderungen für Strafverfolgungsbehörden und nationale Sicherheits-organisationen, die für den Kampf gegen verschiedene Formen der Kriminalität und des Terrorismus verantwortlich zeichnen. Mit zunehmender Popularität der neuen Kommunikationsmedien steigt ebenfalls die Raffinesse mit der Kriminelle diese Medien für ihre eigenen Zwecke missbrauchen. Dies zeigen die Analysen der für die allgemeine Sicherheit zuständigen nationalen und internationalen Organe. Angesichts der breiten Verfügbarkeit und einfachen Nutzung von modernen Kommunikationsmöglichkeiten auch durch kriminelle Vereinigungen sind Überwachungsmöglichkeiten von rechtswidrigen Inhalten und Aktivitäten wichtig und zwingend erforderlich.
Als Antwort auf die wachsende Bedrohung und weltweite terroristische Operationen haben einzelne Länder und internationale Organisationen Regeln entwickelt, die eine gesetzliche Überwachung von Kommunikation über die zuvor in diesem Dokument diskutierten Kanäle ermöglichen. Obwohl Überwachungsrichtlinien für die Kommunikation über traditionelle Kanäle, wie das Telefon, bereits einige Jahre existieren, wurden viele dieser Richtlinien um Regelungen für internetbasierte Kommunikation und damit verbundene Formen von Sprach- und Datenkommunikation ergänzt. Diese Regeln fordern die Befolgung durch Netzbetreiber und Service Provider, die Telekommunikationsdienste für Endverbraucher anbieten. In solchen Fällen werden Lösungen benötigt, die effektiv in die Infrastruktur integriert werden können und – sobald implementiert - Lawful Interception für einen weiten Bereich von Kommunikationstypen unterstützen. Um ethische Ansprüche und Datenschutzerfordernisse zu erfüllen, müssen diese Lösungen alle Aktivitäten von illegaler Überwachung bis zu illegalem Zugriff Telekommunikationsdaten auf jeder Ebene verhindern, einschließlich des Zugriffs von internen Mitarbeitern.

[1] DE-CIX daily graph and weekly graph, www.de-cix.net/stats, 25. Juni 2006.

2.2 Grundlagen aus der Gesetzgebung

Ein sich teilweise überschneidendes Gerüst aus internationalen und nationalen Regeln bildet den Grundstein für die gesetzliche Überwachung von Telekommunikationsdiensten. Es wurde geschaffen, um Strafverfolgungsbehörden zur Überwachung von Nachrichten oder Informationen zu befähigen, die zu illegalen Zwecken ausgetauscht werden. Dieser Abschnitt bietet einen Überblick über den weltweit anerkannten regulatorischen Rahmen.

2.2.1 Nationale Gesetze

Weltweit werden die für Lawful Interception relevanten Richtlinien kontinuierlich aktualisiert und geändert, um mit den Fortschritten in der Telekommunikation und neuen Formen von Sprach- und Datenkommunikation Schritt zu halten. Obwohl die Gesetzgebung und das Wesen der für die Einhaltung nötigen Lösungen von Region zu Region verschieden sind, ist der allgemeine Grundgedanke sehr ähnlich und die der Erfüllung dienenden Tools besitzen ähnliche Eigenschaften. Im Idealfall ist eine erfolgreiche Lawful Interception-Lösung flexibel genug, um sich an variable Regeln anzupassen und kompatibel genug, um problemlos in den unterschiedlichen Netzwerkinfrastrukturen diverser Regionen eingesetzt zu werden.

Länder auf der ganzen Welt haben als Antwort auf terroristische und kriminelle Bedrohungen Gesetzgebungen erlassen, die eine rechtliche Basis für Lawful Interception darstellen. Die Unterschiede von Land zu Land entstehen aus spezifischen, durch die jeweilige Gesetzgebung definierten Regelungen, und betreffen die zu überwachenden Kommunikationsdienste, die abgedeckten verwendbaren Datenformate und die Mechanismen, durch die einzelne Kommunikationstypen an die Strafverfolgungsbehörden (im folgenden auch LEA „Law Enforment Agency“ genannt) übergeben werden.

In Deutschland, als Beispiel, bestimmt die Telekommunikations-Überwachungsverordnung die Telekommunikationsdienste, für welche die Betreiber bei Überwachungsoperationen Unterstützung leisten müssen. Die Anforderungen gelten sowohl für leitungsvermittelnde Netze, paketvermittelnde Netze, Funknetze, Übertragungswege für direkten, teilnehmerbezogenen Internetzugriff und Breitbandkabelnetze. In den Vereinigten Staaten hat der Kongress angeordnet, dass alle

Telekommunikationsbetreiber Überwachungsmöglichkeiten für die Vollzugsbehörden bereitstellen müssen.
Andere Länder haben andere Bestimmungen und eine geeignete Lawful Interception-Lösung sollte nationale und regionale Varianten und ein breites Spektrum von Servicetypen in Einklang bringen können.

2.2.2 Die Europäische Union

In einem Ratsbeschluss[2] vom 17. Januar 1995 spezifiziert die Europäische Union Anforderungen an die nationale Gesetzgebung und für Strafverfolgungsbehörden, die die Basis schaffen für zahlreiche nationale Telekommunikationsüberwachungsgesetze sowie für diverse internationale Überwachungsstandards.

2.2.3 Das Europäische Institut für Telekommunikationsnormen

Das Europäische Institut für Telekommunikationsnormen (ETSI/European Telecommunications Standards Institute) ist ein bedeutender Motor für die Definitionen in Lawful Interception Normen, nicht nur in Europa, sondern weltweit. Vom ETSI entwickelte Normen spezifizieren eine grundlegende Architektur für LI, die eine systematische und erweiterbare Kommunikationsschnittstelle zwischen Netzbetreibern und LEAs ermöglicht. Bezeichnenderweise ist diese Architektur so gestaltet, dass sie auf jede Art von heutigen und zukünftigen leitungs- oder paketvermittelnden Sprach- und Datennetze anwendbar ist.
Eine Erfüllung gemäß den Bedingungen der ETSI-Standards wird erreicht, indem die technischen Anforderungen für Lawful Interception, und insbesondere die Anforderungen für die Übergabeschnittstelle (HI/Handover Interfaces) an die LEA, eingehalten werden.
In einer Vielzahl von Ländern bilden die ETSI-Standards die Grundlage für die technische Regulierung von Lawful Interception. Deren Einhaltung ist zwingend vorgeschrieben ist. Die für LI genutzte Übergabeschnittstelle muss laut Definition des Standards ein fest eingebautes Teil der Netzwerkinfrastruktur des Serviceanbieters oder Netzbetreibers sein und vollständig allen Überwachungsvorschriften entsprechen. Eine Liste der ETSI LI Standards und Spezifikationen befindet sich in Abschnitt 5.

[2] Amtsblatt der Europäischen Gemeinschaften, 96/C 329/01: "Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs."

2.2.4 Die Vereinigten Staaten

Das vom Kongress im Oktober 1994 erlassene amerikanische Gesetz “Communications Assistance for Law Enforcement Act” (CALEA) legt die Bedingungen fest, unter denen Telekommunikationsanbieter einer Strafvollzugsbehörde bei der Überwachung von bestimmten Teilnehmern bzw. bestimmten Gesprächen assistieren müssen, die per gültigem Gerichtsbeschluss beantragt wurde. Der Anbieter ist zudem verpflichtet die Aufzeichnung überwachter Kommunikationen an die ersuchende Behörde liefern. Dieses Gesetz wurde kürzlich durch die “Federal Communications Commission” (FCC) erweitert, so dass auch Firmen, die VoIP-Dienstleistungen anbieten, den Erfüllungskriterien entsprechen müssen.

Um diesen Regelungen nachzukommen, müssen Anbieter von IP-basierten Telefondiensten ihre Netzwerke bis zum Stichtag am 14. Mai 2007 so ausstatten, dass gemäß Gerichtsbeschluss die Kontrolle von VoIP-Kommunikation möglich ist, einschließlich einer Funktion zur Aufzeichnung der Gesprächsinhalte.

Zusätzlich zu CALEA führen einige andere US-Normungsorganisationen Erfüllungskriterien ein, die Netzbetreiber in Bezug auf die US-Gesetze beachten müssen. In diesem Bereich aktive Organisationen sind das “American National Standards Institute” (ANSI), “Telecommunications Industry Association” (TIA), “Alliance for Telecommunications Industry Solutions” (ATIS), PacketCable und andere. Abschnitt 5 bietet einen Überblick über die vorhandenen Standards.

2.2.5 Das “3rd Generation Partnership Project”

Neben den ETSI-Spezifikationen hat ein Zusammenschluss von Technologieunternehmen im Rahmen des “3rd Generation Partnership Project” (3GPP) technische Spezifikationen für Lawful Interception in Mobilfunknetzen definiert. Die technischen Standards ‘3GPP TS 33.106-108’ schaffen die Grundlage für die Umsetzung der gesetzlichen Anforderungen und gewährleisten die Interoperabilität zwischen den ausleitenden Stellen und den Behörden.

Das 3GPP wurde Ende 1998 von den Organisationen ETSI, der “Association of Radio Industries and Businesses/Telecommunication Technology Committee” (ARIB/TTC) in Japan, “China Communications Standards Association” (CCSA) in China, der “Alliance for Telecommunications Industry Solutions” (ATIS) in Nordamerika und der “Telecommunication Technology Association” (TTA) in Südkorea gegründet.

2.2.6 Lösungen zur Einhaltung der Gesetze

Unabhängig von der geltenden Regulierung gibt es in den meisten Staaten Vorschriften, nach denen Lawful Interception auf Anweisung einer Behörde ausgeführt werden dürfen und müssen. Die folgende Liste hebt die wichtigsten Fähigkeiten und Anforderungen einer Lawful Interception-Lösung hervor.

- **Übergreifende Überwachungsmöglichkeiten:** Die LI-Lösung muss alle Gespräche und Nachrichten eines bestimmten Ziels lückenlos abfangen und überwachen können.
- **Zuverlässigkeit und Integrität:** Die LI-Lösung muss die Lieferung von präzisen und akkuraten Ergebnissen bei höchstem Schutz der Datenintegrität sicherstellen. Die LI-Lösung muss ebenso zuverlässig sein wie der zu überwachende Dienst.
- **Separation des Inhalts:** Daten aus überwachter Kommunikation sollten in einzelne Komponenten zerlegbar sein; zum Beispiel sollten die Ereignisinformationen (IRI/Interception Related Information) vom Kommunikationsinhalt (CC/Communication Content) trennbar sein.
- **Transparente Überwachung:** Die durch die Lösung ausgeführten Überwachungsmaßnahmen dürfen für die Teilnehmer nicht erkennbar sein.
- **Sofortige Aktivierung und Übermittlung in Echtzeit:** Beim Befolgen einer Lawful Interception Anfrage muss eine Lösung unverzüglich aktivierbar sein und eine Echtzeit-Reaktion bei der Lieferung überwachter Daten bieten.
- **Ausreichende Kapazität:** Die Lösung muss eine adäquate Kapazität haben, um den Umfang der Überwachungsaktivitäten verarbeiten zu können.
- **Datensicherheit und -schutz:** Sensible private Daten müssen während der vollständigen Übertragung zur autorisierten Behörde geschützt werden. Nur autorisiertes Personal darf in der Lage sein, Überwachungsdaten zu sehen.
- **Entschlüsselung:** Nach vorheriger Entschlüsselung sollen verschlüsselte Daten im Klartextformat gesendet werden, wenn die entsprechenden Schlüssel dem Dienstanbieter oder Netzbetreiber zur Verfügung stehen.

- **Vollständiges Protokollieren von Ereignissen:** Alle Überwachungsaktivitäten müssen als Teil einer zentralen und manipulationssicheren Aufbewahrungsstelle aufgezeichnet und für spätere Sicherheitskontrollen abgelegt werden.

3 Interception Grundlagen

Erfolgreiche Lawful Interception-Maßnahmen erfordern die Kooperation und Interaktion zwischen einer Vielzahl von Parteien. Außerdem sind physikalische Mechanismen in den Infrastrukturen erforderlich, um die Arbeitsprozesse zu unterstützen. Diese Themen werden in den folgenden Abschnitten vorgestellt.

3.1 Rollen und Funktionsbereiche

Lawful Interception erfordert die Kooperation und Interaktion zwischen den folgenden Parteien.

- **Regierungsbehörden und gesetzgebende Körperschaften:** Die Lawful Interception betreffenden Regeln und Anforderungen sind durch gesetzgebende Körperschaften nationaler Regierungen im Gesetz definiert und bestätigt. Sie werden durch die verantwortlichen Regierungsbehörden erlassen und durchgesetzt.
- **Strafverfolgungsbehörden (LEAs):** Aufträge für gesetzliche Überwachungsmaßnahmen stammen typischerweise von Strafverfolgungsbehörden, basierend auf Gerichtsbeschlüssen oder gerichtlichen Anordnungen einer anerkannten Behörde. Diese Aufträge werden dann dem Dienstanbieter oder Netzbetreiber übergeben, der sie innerhalb einer vorgegebenen Zeitspanne und gemäß den auftragsspezifischen Bedingungen ausführen muss.
- **Dienstanbieter oder Netzbetreiber:** Über eine Netzwerkinfrastruktur verteilte Daten- und Sprachkommunikationsdienste unterliegt der Verantwortung des Dienstanbieters oder des Netzbetreibers. Für alle verfügbaren Kommunikationsdienste muss im Rahmen einer gesetzlichen Überwachungsmaßnahme Zugriff auf die Kommunikationsdaten eines zu überwachenden Teilnehmers gewährt werden.
- **Interception Service Provider:** Dienstanbieter und Netzbetreiber können die Fachkenntnis eines Interception Service Providers einsetzen, um Lawful Interception Aufträge zu managen und auszuführen. Diese Dienste können von der

Bereitstellung von Leihausrüstungen und technischem Support bis zum Angebot vollständig auslagerter Überwachungsdienste (Managed Service) reichen.

Abbildung 1 zeigt einen typischen Lawful Interception-Prozess vom Auftragseingang bis zur Datenbereitstellung.

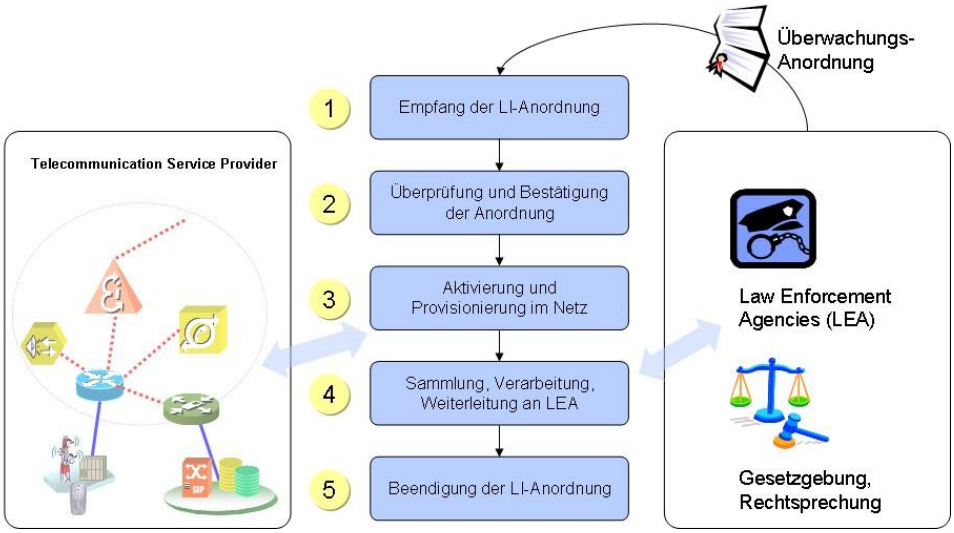

Abbildung 1: Prozessübersicht Lawful Interception

3.2 Schlüsselkomponenten für Lawful Interception

Auf Systemebene umfasst eine typische LI-Lösung die in Abbildung 2 dargestellten Komponenten. Das Monitoring Center kommuniziert mit dem LI System über standardisierte Schnittstellen (z.B. definiert durch ETSI, ANSI), um Überwachungs-maßnahmen einzurichten und um abgefangene Kommunikation zu übermitteln. Wie dargestellt, werden dabei die Metadaten (IRI/Interception Related Information) und der eigentliche Inhalt der Kommunikation (CC/Content of Communication) separat übertragen.

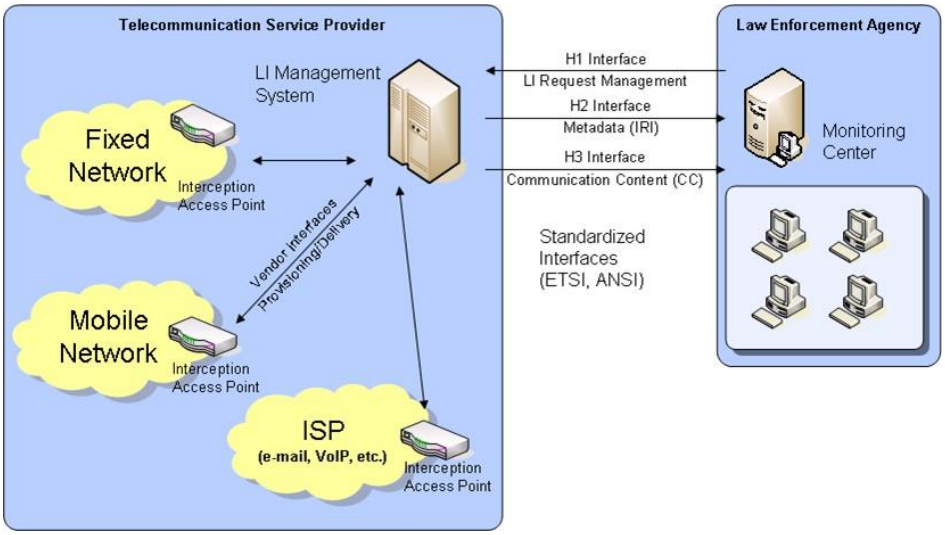

Abbildung 2: Vereinfachte Architektur einer Lawful Interception Lösung

Aus der Perspektive des Netzbetreibers oder Dienstanbieters gibt es folgende primäre Pflichten und allgemeine Anforderungen für die Entwicklung und den Einsatz einer Lawful Interception-Lösung.

- **Wirtschaftlichkeit:** Die Lösung minimiert die Zeit und den Aufwand, durch automatisierte Einrichtung von Überwachungsmaßnahmen im Netz und prompte Bestätigung gegenüber der Behörde.
- **Minimierung des Einflusses auf die Netzwerkinfrastruktur:** Der Betrieb der Lawful- Interception-Lösung sollte die Performance oder das Verhalten des Kommunikationsdienste oder des Netzes in keiner Weise negativ beeinträchtigen.
- **Konformität sicherstellen:** Die Lösung entspricht den Bestimmungen der nationalen Gesetzgebung sowie den internationalen Standards und stellt den reibungslosen Betrieb mit Ausrüstungen von anderen Netzwerk- und Monitoring Center-Herstellern sicher.
- **Unterstützung zukünftige Technologien:** Die Lösung muss flexibel anpassbar sein an neue Standards und technische Spezifikationen. Außerdem muss das System skalierbar sein, um eine Zunahme des Kommunikationsumfangs oder der Anzahl der Überwachungsmaßnahmen zu bewältigen.
- **Zuverlässigkeit:** Die Lösung liefert akkurate Ergebnisse und garantiert Datensicherheit auf jeder Stufe des LI-Prozesses.

- **Sicherheit:** An jeder Stelle des LI-Systems müssen die überwachten Daten vor illegalem oder unerlaubtem Zugriff geschützt sein. Überwachungsaktivitäten dürfen in keiner Weise durch den Benutzer bemerkbar sein.

3.3 Vertrauens- und Ethikstandards bei Lawful Interception

Lawful Interception, d.h. die Überwachung privater Kommunikation, erzeugt ambivalente Ansichten bei staatlichen Behörden und dem Bürger und verlangt nach einer ausgewogenen Balance zwischen nationaler Sicherheit und dem Recht auf Privatsphäre. Einwohner vieler Länder sind berechtigterweise wachsam gegenüber den Regierungen und Strafverfolgungsorganen, die in ihre privaten Aktivitäten eindringen. Deshalb müssen die ethischen Interessen und essentiellen Grundrechte des Einzelnen in jeder Lawful Interception-Lösung strikt beachtet werden.
In den letzten Jahrzehnten hat sich Lawful Interception von einem wenig geregelten und nicht gradlinig interpretiertem Konzept zu einem klar etabliertem Konstrukt aus Gesetzen und Richtlinien entwickelt, das die Grenzen und Rahmenbedingungen festlegt, innerhalb derer die Behörden und Geheimdienste operieren müssen. Dieses Konstrukt erntete Anerkennung als bedeutende Methode zur strafrechtlichen Verfolgung von Kriminalität und zum Aufspüren potentieller terroristischer Handlungen vor deren Ausführung.
Es existiert ein empfindliches Gleichgewicht zwischen den Anwendungsmöglichkeiten der Regierung, Kriminalität und Terrorismus aufzuspüren und zu verhindern, zum einen und andererseits den individuellen Rechten und privaten Belangen der Einwohner des Landes. Eine verantwortungsvolle, ethisch begründete Lawful Interception-Lösung erkennt an, dass diese Ausgeglichenheit nur erreicht werden kann, wenn den Zielen der gesetzlichen Strafverfolgung und den individuellen Rechten der Bürger auch gleiche Wichtigkeit eingeräumt wird. Um in einer Lösung eine solche Ausgeglichenheit anzustreben, müssen sowohl die technologischen Aspekte der Aufgabe als auch die rechtlichen und ethischen Gesichtspunkte beachtet werden, die bei der Überwachung jeder Form von Kommunikation unumgänglich sind.
Gesetzestreue, Verantwortlichkeit und Absicherung sind zum Schutz gegen das unerlaubte Eindringen in die Privatsphäre von höchster Bedeutung in einer seriösen Lawful Interception-Lösung. Kontrollmechanismen zur Einhaltung dieser Ansprüche

sollten integrierte Bestandteile der Lösung sein. Einziger Zweck einer LI-Lösung sollte sein, in einem gültigen und legalen Rahmenwerk Informationen zu gewinnen, mit denen kriminelle Aktivitäten aufgespürt und terroristische Absichten verhindert werden können. Wohldurchdachte Lawful Interception-Lösungen wie das LI Management System von Utimaco besitzen eingebaute Vorrichtungen zur Vorbeugung von Missbrauch, wie z.B. Authentifizierung und Authorisierung des Benutzerpersonals. Integrierte Schutzmechanismen zum Aufzeichnen aller Ereignisse stellen die Verantwortlichkeit sicher und sind ein essentieller Aspekt im LI-Prozess. Ein weiteres Merkmal ist die gesicherte Speicherung und Übermittlung der überwachten Daten vom Ursprung zu den involvierten LEAs. Die Einhaltung der etablierten Standards und die Zertifizierung durch Regulierungsbehörden spielen eine entscheidende Rolle.

4 Annäherung an die Problematik

Das Lawful Interception Management System (LIMS) von Utimaco ist eine LI-Lösung, die in mehr als 40 Ländern weltweit erfolgreich eingesetzt wird und die den Anforderungen der jeweiligen Service Providern und Netzbetreibern entspricht. LIMS ist angepasst an die lokalen gesetzlichen Bedingungen und unterstützt alle überwachungsrelevanten Kommunikationsarten. Dieser Abschnitt gibt einen Überblick der Architektur und Features von LIMS.

4.1 LIMS Systemarchitektur

Die Utimaco LIMS Systemarchitektur bietet maximale Flexibilität und nutzt ein modulares Designkonzept, das beliebig auf zahlreiche Dienste, Technologien und LI-Standards wie auch auf alle zukünftigen Entwicklungen im Lawful Interception Bereich abgestimmt werden kann. LIMS ist entworfen für die Verwendung bei Dienstanbietern oder Netzbetreibern und umfasst die in Abbildung 3 dargestellten Elemente.

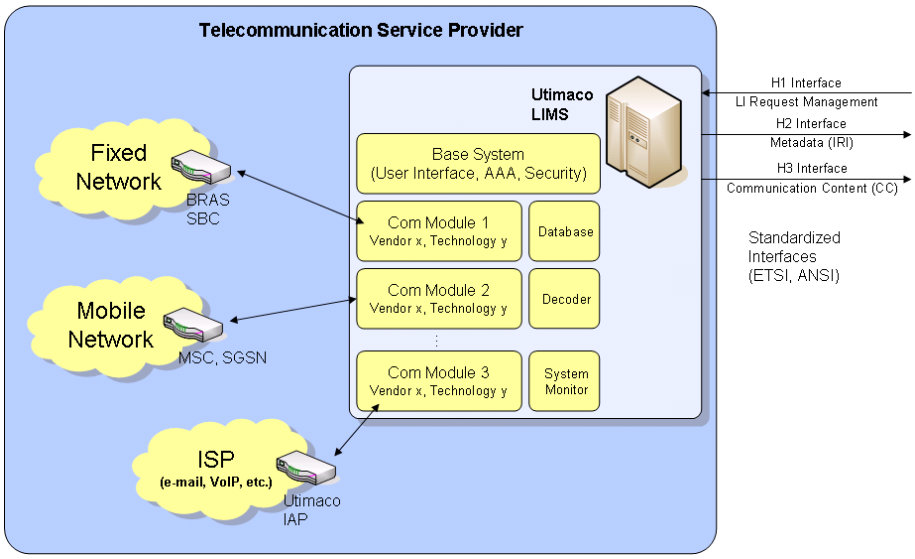

Abbildung 1: Elements von LIMS

Zahlreiche individuelle Kommunikationsmodule, abhängig von der Anzahl an Netzwerkelementen mit Überwachungsfunktionen managen den Datenzufluss von und zu den Interception Access Points (IAP) in den verschiedenen Kommunikationsnetzen. Die Verwaltungswerkzeuge sind in einer zentralen, bedienerfreundlichen grafischen

Schnittstelle zusammengefasst, über die alle Systemaktivitäten gesteuert und überwacht werden können. Die Implementierung unterstützt drei verschiedene Ansätze der Überwachung: aktive, passive und hybride Überwachung.
Für jede Art von Netzwerkelementen existiert mindestens ein Kommunikationsmodul. Dieser modulare architektonische Ansatz ist die Grundlage für die Flexibilität und Skalierbarkeit von LIMS. Zusätzliche Kommunikationsmodule können je nach Größe des Überwachungsnetzwerks und je nach Anzahl der überwachten Netzwerkelemente hinzugefügt werden. Wachsen die Leistungsanforderungen, können die Kommunikationsmodule über mehrere Server verteilt werden um Performance-Engpässe zu vermeiden.
Die modulare Architektur ermöglicht Utimaco eine effizientere Verwaltung der Überwachung von zahlreichen Arten von Netzen und Diensten. Zurzeit unterstützt das Utimaco LIMS über 100 verschiedene Netzwerkelemente und entwickelt kontinuierlich neue Interception Access Points, um mit neuen Kommunikationstechnologien Schritt zu halten.

4.2 Aktive, passive und hybride Interception

Bei aktiver Überwachung repräsentiert der IAP eine physikalische Komponente eines Netzwerkelements, wie z.B. ein Serving GPRS Support Node (SGSN) in einem mobilen Netzwerk oder ein Breitband Remote Access Server (BRAS) in einem festen IP-Netzwerk. LIMS erhält die Überwachungsdaten—bestehend aus Metadaten (IRI) und Inhalt (CC)— direkt von einem oder mehreren Netzwerkelementen, wie in Abbildung 2 gezeigt. In diesem Fall muss das Netzwerkelement zumindest Basisfähigkeiten zur Überwachung und Filterung besitzen. Die Effektivität der aktiven Überwachung hängt insbesondere ab vom modularen Design des LI-Systems und der Interoperabilität mit den Geräten dritter. Utimaco führt umfassende Tests durch, um die Interoperabilität mit anderen Herstellern zu maximieren.

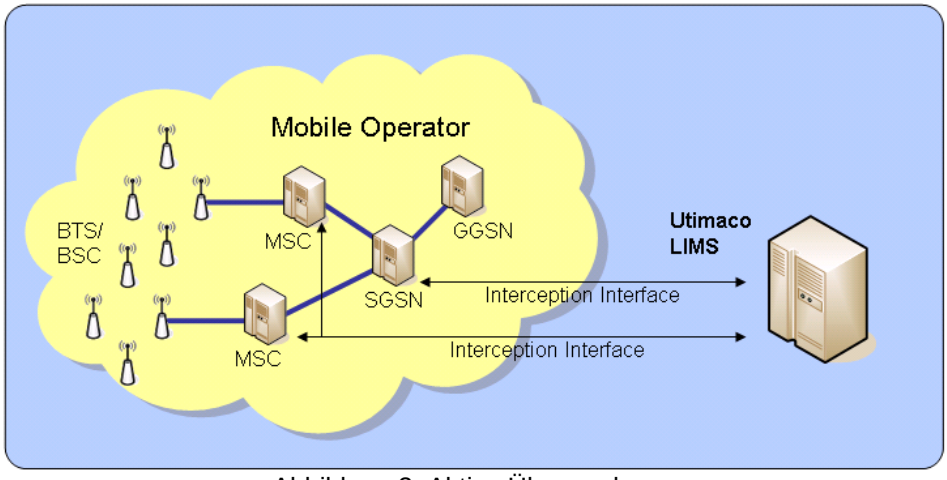

Abbildung 2: Aktive Überwachung

Aktive Überwachung hat folgende Vorteile:

- **Preisgünstige Implementierung:** Wenn die Netzwerkelemente über grundlegende Überwachungs- oder Filterfähigkeiten verfügen, kann dieser Ansatz sehr kosteneffektiv sein.
- **Minimale Hardwarevoraussetzungen:** In den meisten Fällen wird keine zusätzliche Hardware benötigt.
- **Schnelle Bereitstellung:** Aktive Überwachungs-Vorrichtungen können im Allgemeinen sehr schnell eingesetzt werden.
- **Hohe Verfügbarkeit:** Die Verfügbarkeit der aktiven Interception als Komponente des laufenden Netzwerks kann einfach hergestellt werden.

Der größte Nachteil der aktiven Interception ist, dass einige Netzwerkelemente keine Interception-Fähigkeit haben. Weitere Nachteile:

- Aktive Überwachung kann negativen Einfluss auf die Leistung des Netzwerkelements haben, das die Interception-Funktion ausführt.
- Bei hohem Datendurchsatz kann das Netzwerkelement (z. B. Router) Pakete am Interception-Port verlieren.

Bei passiver Interception ist der IAP ein von LIMS verwaltetes und vom Betreibernetzwerk unabhängiges Netzwerkelement. Der passive IAP filtert, dekodiert und

liefert die Metadaten und Inhalte der Überwachung zum LIMS, wie in Abbildung 5 dargestellt. Passive Interception arbeitet auf einer Kopie des Netzwerk-Verkehrs und ist damit vollständig transparent für den Rest des Netzes. Auch für die zu überwachende Person ist dadurch jegliche Interception-Aktivität nicht zu bemerken.

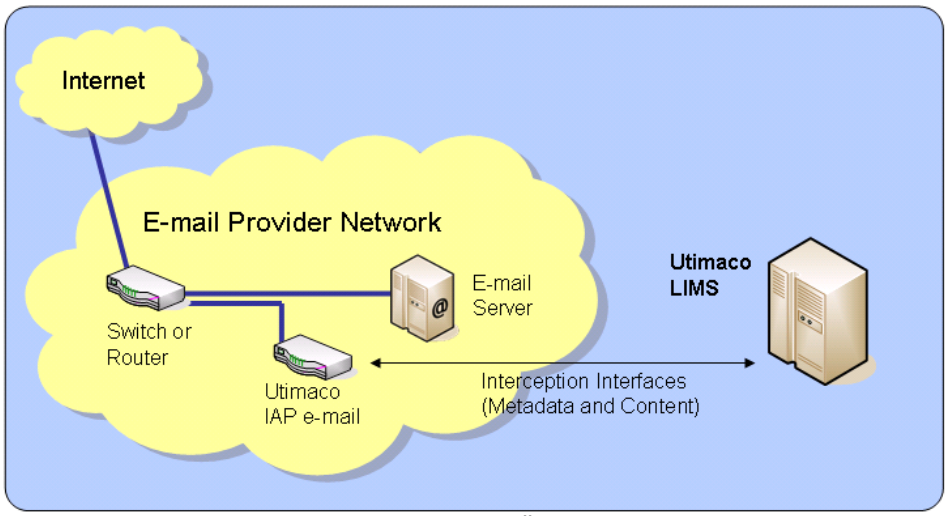

Abbildung 3: Passive Überwachung

Passive Überwachung hat folgende Vorteile:

- **Flexibilität:** Passive Überwachung kann mit nahezu jedem Netzwerk und sehr vielen verschiedenen Diensten genutzt werden.
- **Unabhängiger Betrieb:** Passive Überwachung ist unabhängig vom Betreibernetzwerk.
- **Unsichtbarkeit:** Die Operationen passiver Überwachung sind für den Nutzer und das übrige Netzwerk komplett unsichtbar. Alle Interception- und Filteraktivitäten werden auf einer Kopie des Datenverkehrs ausgeführt.
- **Keine Leistungsbeeinträchtigung:** Das Modell der passiven Interception berührt die Netzwerkleistung in keinster Weise, außerdem beeinträchtigt es weder die Vertrauenswürdigkeit noch die Verfügbarkeit der Netzwerkressourcen.

Passive Überwachung zeigt folgende Nachteile auf:

- **Zusätzliche Kosten:** Durch den zusätzlichen Hardware- und Softwareaufwand erhöhen sich im Allgemeinen die Kosten einer LI-Lösung.

- **Berücksichtigung der Leistung:** Die IAP-Hardware hat feste Leistungsbeschränkungen, die im Design der Lösung berücksichtigt werden müssen.

Hybride Interception kombiniert die Vorzüge und verbindet aktive und passive Überwachung. Der gemischte Ansatz gewinnt in den komplexen Netzwerkarchitekturen und Service-Plattformen der heutigen Zeit immer mehr an Bedeutung. In IP-Netzwerken können zum Beispiel die Anmeldedaten eines bestimmten Benutzers passiv überwacht werden, um die aktuelle IP-Adresse des Teilnehmers aufzuspüren. Ist die IP-Adresse einmal bekannt, kann ein IP-Router den zugehörigen Datenverkehr aktiv zum Interception-System weiterleiten (beziehungsweise kopieren), von wo er dann an die entsprechenden Monitoring Center verteilt wird. Abhängig von der Struktur des Netzwerks und der Art der überwachten Dienste ist hybride Interception häufig die einzig praktikable Lösung. Da Metadaten (IRI) und Kommunikationsinhalt (CC) an verschiedenen Stellen des Netzwerks abgefangen werden können, kennzeichnet LIMS beides mit jeweils eindeutigen Markierungen. Damit kann ein Monitoring-Center die Informationen nach Erhalt unkompliziert zuordnen. Abbildung 6 zeigt das prinzipielle Konzept einer hybriden Überwachung an einem Beispiel für VoIP.

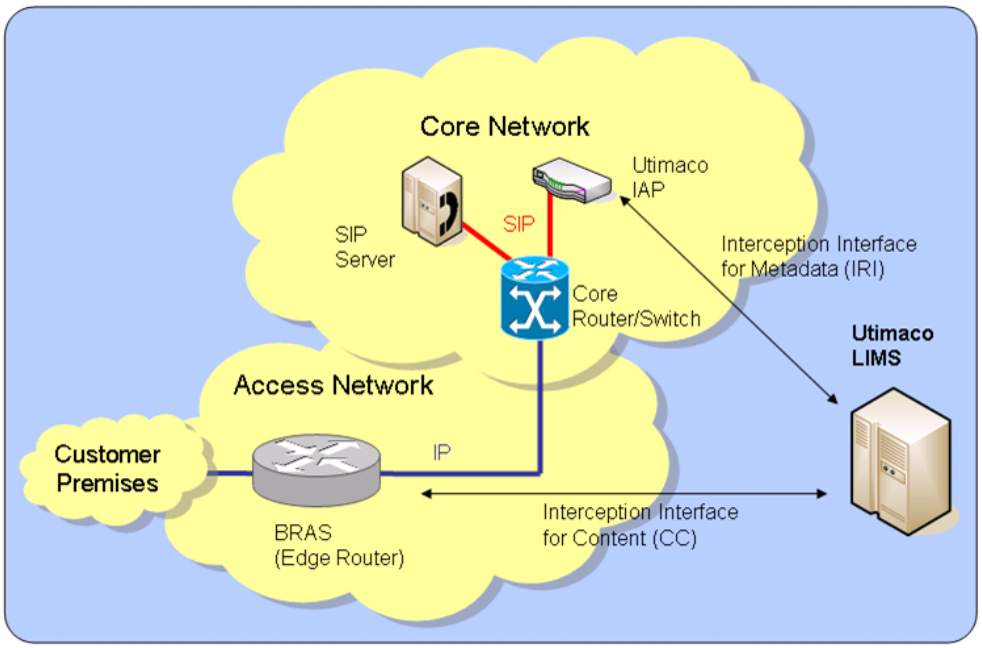

Abbildung 4: Hybride Interception

4.3 Grundfunktionen von LIMS

LIMS trennt die funktionalen Elemente jeder Lösung in drei grundlegende Bereiche:

- Administration
- Provisionierung und Datensammlung
- Mediation und Weiterleitung

Abbildung 7 bietet einen Überblick der jeweiligen Aufgaben, die in den drei Bereichen bearbeitet werden.

Abbildung 5: LIMS Funktionen

4.4 Vorteile von LIMS

LIMS bietet eine kosteneffiziente, umfassende Lawful Interception-Lösung. Diese Lösung vereinfacht die Installation und Wartungsarbeiten für Dienstanbieter und Netzbetreiber und gewährt gleichzeitig die Sicherheit, die Privatsphäre und die Vertrauenswürdigkeit, die Utimaco-Kunden gewohnt sind. LIMS hat folgende entscheidende Vorteile.

- **Bequeme Bedienung:** Ein zentrales Management-System für alle zu überwachenden Dienste mit benutzerfreundlicher Verwaltungsschnittstelle.
- **Konformität und Interoperabilität:** Die Lösung zeichnet sich durch die Vielzahl der unterstützten Herstellerschnittstellen aus und bietet garantierte Einhaltung der nationalen Gesetze und internationalen Standards.

- **Kosteneffizienz und Skalierbarkeit:** Die modulare Architektur von LIMS erlaubt die kosteneffiziente Anpassung der Überwachungslösung an die tatsächlichen Anforderungen für den jeweiligen Dienst und das Netzwerk.
- **Qualifizierter Support:** Alle LIMS-Installationen werden mit kompetentem Fachwissen desCustomer-Support-Teams von Utimaco unterstützt.
- **Hohe Sicherheit und Verlässlichkeit:** LIMS ist für sicherheitskritische Anwendungen geschaffen und basiert auf den Erfahrungen und bewährten Technologien, die Utimaco bereits seit 1983 im IT-Sicherheitsbereich liefert.

4.5 Zusammenfassung

Den Herausforderungen für Netzbetreiber und Dienstanbieter wird im Idealfall mit LI-Lösungen begegnet, die auf Basis der wichtigsten Anforderungen der Industrie entwickelt wurden. Die LIMS-Lösung von Utimaco spricht die vordringlichen Aufgaben in der Industrie aus verschiedenen Blickwinkeln an. Weltweit wächst das Volumen an Datenverkehr, der überwacht und gefiltert werden muss – die skalierbare LIMS-Architektur ist ausreichend gerüstet, zunehmende Bandbreiten zu verarbeiten. Mit Sicht auf die steigende Anzahl an Telekommunikationsdiensten und neu eingeführte Arten von Diensten passt sich das modulare Design von LIMS flexibel an sich ändernde Technologien an. Durch aktive Teilnahme in nationalen und internationalen Standardisierungsgremien und direkte Zusammenarbeit mit den regulierenden Behörden ist Utimaco in der Lage die Änderungen in der Gesetzeslage und in den technischen Standards frühzeitig umzusetzen. Dank der Kooperation mit führenden Infrastrukturherstellern und der kontinuierlichen Weiterentwicklung der Interception-Technologien integriert sich die LIMS-Lösung reibungslos und kosteneffizient in die diversen Kommunikationsnetzstrukturen. Die Erfahrung und Anerkennung von Utimaco im Sicherheits- und LI-Bereich machen es möglich, effektiv zwischen den Interessen von Netzbetreibern und Service Provider und den Anforderungen der LEAs und Regulierungsbehörden zu vermitteln, indem Lösungen geboten werden, die die Einhaltung der Vorschriften gewährleistet und den Schutz der Investitionen der Betreiber berücksichtigen.

5 Weiterführende Informationen

Besuchen Sie www.utimaco.de/lims für weitere Information über Utimaco und Lawful Interception-Lösungen.

Die folgende Tabelle gibt einen Überblick über einige der wichtigsten Überwachungs-Gesetze und -Standards in verschiedenen Ländern.

5.1 Interception-Gesetze

Vereinigte Staaten von Amerika	Omnibus Crime Control and Safe Streets Act of 1968.
	Electronic Communications Privacy Act of 1986 (ECPA).
	USA Patriot Act, 2001.
	Communications Assistance for Law Enforcement Act, 1994 (CALEA).
	Foreign Intelligence Surveillance Act (FISA) of 1978.
Kanada	Criminal Code (R.S. 1985, c. C-46). An Act respecting the Criminal Law (Part VI, Invasion of Privacy; Part XV, Special Procedure and Powers).
Japan	"Law authorizing interceptions of telecommunications in crime investigations" (Law No. 137, 1999) (Communication Interception Act (CI-Act)).
	"Code of Criminal Procedure – CCP."
Frankreich	Loi n° 91-636 du 10 juilliet 1991 relative au secret des correspondances émises par la voie des télécommunications.
	Décret n° 93-119 du 28 janvier 1993, Décret relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646 du 10 juillet 1991.
Italien	Intercettazioni di conversoni o communicazione, Art. 266 – 271, Code di Procedura Penale, 1988.
	Decreto del presidente della repubblica del 19 settembre 1997, n. 318: Regolamento per l'attuazione di direttive comunitarie nel settore delle telecomunicazioni.
Großbritannien	Regulation of Investigatory Powers Act 2000 (RIPA).
	The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.
Russland	SORM I+II (Sistema Operativno-Rozysknykh Meropriyatii), 2000.
Deutschland	Telecommunications Act (TKG), 2004.
	G10 Law, 2001.
	Strafprozessordnung (StPO), 2002.
	Gesetz über das Zollkriminalamt und die Zollfahndungsämter, (Zollfahndungsdienstgesetz - ZFdG), 2002.
	Telekommunikationsüberwachungsverordnung (TKÜV), 2005.
Niederlande	Tijdelijke regeling aftappen openbare telecommunicatienetwerken en –diensten, 1998.
	Telecommunications Act 1998.

5.2 Interception-Standards

ETSI, EU	ETSI TS 101 331, Requirements of Law Enforcement Agencies
	ETSI ES 201 158, Requirements for Network Functions
	ETSI TS 101 671 / ETSI ES 201 671, Handover Interface for the Lawful Interception of Telecommunications Traffic
	ETSI TR 102 053, Notes on ISDN LI functionalities
	ETSI TR 101 943, Concepts of Interception in a Generic Network Architecture
	TS 102-232-1Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 1: Handover specification for IP delivery
	TS 102-232-2Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 2: Service-specific details for E-mail services
	TS 102-232-3Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 3: Service-specific details for internet access services
	TS 102-232-4Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 4: Service-specific details for Layer 2 services
	TS 102-232-5Lawful Interception (LI);Handover Interface and Service-Specific Details (SSD) for IP delivery;Part 5: Service-specific details for IP Multimedia Services
	ETSI TS 101 909-20-1/2 IP Multimedia Time Critical Services; LI for Services related to E.164 Voice Telephony, LI for streamed MM services
	ETSI EN 301 040, Terrestrial Trunked Radio; Lawful Interception interface (TETRA)
ATIS, US ATIS	T1.678
	T1.724, ATIS-1000013.2007 LAES for IAS
ATIS-TIA, US	J-STD-025, J-STD-025-A, J-STD-025-B
PacketCable, US	PacketCable 1.5: Electronic Surveillance, PKT-SP-ESP1.5-I01-050128
	PacketCable 2.0: Electronic Surveillance Intra-Network, Specification, PKT-SP-ES-INF-I01-060406
3GPP	TS 33.106, TS 33.107, TS 33.108
ITU-T	IPCableCom, Project on time-critical interactive services over cable television network using IP-protocol, in particular Voice and Video over IP

Bemerkung: Obwohl die in den Tabellen enthaltenen Angaben sorgfältig ausgewählt und geprüft wurden, wird kein Anspruch auf Vollständigkeit erhoben

6 Glossar und Abkürzungsverzeichnis

3GPP	The 3rd Generation Partnership Project (3GPP) ist ein Zusammenschluss zwischen ETSI (Europe), ARIB/TTC (Japan), CCSA (China), ATIS (North America), und TTA (South Korea). www.3gpp.org
AAA	Authentication, Authorization, Accounting
ANSI	American National Standards Institute. www.ansi.org
BRAS	Broadband Remote Access Server, sammelt den Output von DSLAMs
BSC	Base Station Controller, ein Subsystem in einem GSM-Mobilnetz
BTS	Base Transceiver Station, eine GSM-Basisstation
CALEA	Communications Assistance for Law Enforcement Act (CALEA), U.S. Law
CC	Communication Content, Inhalt der Kommunikation
CDMA	Code division multiple access, gängige Netzwerktechnologie der zweiten Generation (2G) in den Vereinigten Staaten, Australien und anderen Ländern
ETSI	European Telecommunications Standards Institute (ETSI). www.etsi.org
IAP	Interception Access Point, Stelle des Netzwerks, an der die Interception stattfindet
IRI	Interception Related Information, die Metadaten zu einem entsprechenden Kommunikationsdienst, e.g., Anrufdetailaufzeichnungen, Anrufzeit, Anrufer-ID, E-Mail-Adresse
LI	Lawful Interception
LIMS	Lawful Interception Management System
MSC	Mobile Switching Center, Teil eines GSM-Netzwerks
SGSN	Serving GPRS Support Node, Teil eines GSM-Netzwerks
UMTS	Universal Mobile Telecommunications System (UMTS), eine der Mobilfunktechnologien der dritten Generation (3G)

Utimaco Safeware AG
Germanusstr. 4
52080 Aachen
Germany
Telefon: +49 (241) 1696-0
Fax: +49 (241) 1696-199

li-contact@utimaco.com
http://lims.utimaco.com