

Vernetzung von Informationen zur Darstellung der Landeslage (VIDaL)

AP3: Vorgaben für die Lageplattform

Veröffentlichung des Expertenforums VIDaL

Stand: 25.03.2020

Inhalt

1	Einführung	4
2	Aufbau des vorliegenden Dokuments	5
3	Festlegungen zur Lageplattform	6
3.1.	Standards	6
3.2.	Architektur der Lageplattform	6
3.3.	Eigenschaften der Lageplattform	8
3.3.1.	Servicestrukturen der Plattform	8
3.3.2.	Kommunikationskonzept	9
3.3.3.	Adaptermodell der Lageplattform	9
3.4.	Kommunikation in den Netzebenen	9
3.4.1.	Accessebene	9
3.4.2.	Backendnetz	10
3.5.	Funktionale Anforderungen (Use Cases)	10
3.5.1.	Prinzipielle Aufgabe der Plattform	10
3.5.2.	Anspruch auf syntaktische und semantische Interoperabilität	11
3.5.3.	Weitere fachliche Ansprüche an die Plattform	11
3.6.	Funktionale Anforderungen – Metaebene	12
3.6.1.	Plattform Authentifizierung und Autorisierung	13
3.6.2.	Nachrichtenstruktur und -sicherung	13
3.6.3.	Systemzugang	14
3.6.4.	Sicherer Transport	14
3.6.5.	Trennung der Technologiekomponenten	15
3.7.	Authentifizierung	15
3.7.1.	Authentifizierungsmethoden	15
3.7.2.	Vorteile und Nachteile der Methoden	16
3.7.3.	Betriebsaspekte bei der Authentifizierung	17
3.8.	Adressierungskonzept	18
3.8.1.	Ausgangssituation und Anforderungen	18
3.8.2.	Verwendung von OIDs	19
3.8.3.	Netzwerkzugang und Nachrichtenübermittlung	21
3.8.4.	Adressierungsverfahren und Informationsordnung	22
3.8.5.	Adressierung und Geo-Verteilung	23
3.8.6.	Adressierung und Autorisierung	25

3.8.7.	Föderale Adressierung	26
3.8.8.	Dienstprimitive – Master Use Cases.....	27
3.8.9.	Anbindung Endpunkt zum Accesspoint mit REST	28
3.8.10.	Erstregistration (Onboarding) und Löschung (Kill)	29
3.8.11.	Registrierung und Deregistrierung.....	29
3.8.12.	Metadaten set von Nutznachrichten.....	30
3.8.13.	Nachrichten senden.....	30
3.8.14.	Nachrichten empfangen	31
3.8.15.	Administrative Nachrichten	31
3.9.	Übersetzungsdienst (Translational Service).....	32
3.9.1.	Übersetzungsdienst in Anlehnung an EPISECC	32
3.9.2.	Aufgaben des Translational Services.....	32
3.10.	Archivierungsservices	35
3.11.	Nichtfunktionale Anforderungen	36
3.11.1.	Nicht-funktionale Aspekte (Sammlung).....	36
3.11.2.	Sicherheit und Rechteverwaltung	36
3.11.3.	Verfügbarkeit	38
3.11.4.	Schutzklasse	38
3.11.5.	Zukunftsfähigkeit.....	38
4	Betrieb der Lageplattform	38
4.1.	Fachlicher Betrieb.....	40
4.2.	Technische Betriebsumgebung	40
5	Abkürzungsverzeichnis / Glossar.....	42

1 Einführung

Das Expertenforum VIDaL (Vernetzung von Informationen zur Darstellung der Landeslage) des PMeV (Bundesverband Professioneller Mobilfunk e.V.) hat sich die Aufgabe gegeben, den Aufbau von soliden und zukunfts-fähigen Strukturen für den Informationsaustausch zwischen den Institutionen des Krisenmanagements eines Bundeslandes durch die Definition von Vorgaben für ihren Aufbau zu unterstützen.

Die Ergebnisse der Arbeit werden in vier Dokumenten zusammengefasst und allen interessierten Parteien lizenz- und diskriminierungsfrei über die Internetseiten des PMeV zur Verfügung gestellt.

Das führende Dokument

- Ergebnisse des Expertenforums VIDaL

stellt das Expertenforum, seine Arbeitsweise und im Überblick die vereinbarten Empfehlungen für den Auf- und Ausbau eines Systems zum Informationsaustausch zwischen den Akteuren des Krisenmanagements im Land am Beispiel Nordrhein-Westfalens dar.

Detaillierte Vorgaben für die konkrete Umsetzung eines solchen Systems wurden in drei Arbeitspaketen zusammengetragen und liegen in weiteren Dokumenten vor:

- AP1: Inhalte der Informationspakete
- AP2: Medien und Strecken
- AP3: Vorgaben für die Lageplattform

Das vorliegende Dokument dient der Darstellung der Ergebnisse des Arbeitspakets 3, dem vereinbarten technischen Aufbau für die zukünftige VIDaL-Lageplattform.

2 Aufbau des vorliegenden Dokuments

Das vorliegende Dokument ist wie folgt gegliedert:

- Standards und Standardisierungsbestrebungen
- Festlegungen zur Architektur der Plattform
- Festlegungen zu den Plattformeigenschaften
- Festlegungen zu den Betriebsaspekten

Zu jedem der Themen wird in einem spezifischen Kapitel der jeweils verfolgte Ansatz erläutert und mit Abbildungen versehen.

Am Ende des Dokuments befindet sich ein Abkürzungsverzeichnis / Glossar.

3 Festlegungen zur Lageplattform

Die in den Arbeitspaketen 1 und 2 festgelegten Dateninhalte, Übertragungsstrecken und Protokolle sollen durch die Lageplattform übertragen/vermittelt werden. Dabei sollen zur Übertragung der Daten die dort festgelegten Standards und Protokolle verwendet werden.

Die Lageplattform ist so aufzubauen, dass zukünftige Funktionalitäten und Kommunikationsbedarfe der beteiligten Landesstellen (Lagezentren, Leitstellen usw.) beachtet werden und somit die Kommunikationsplattform jederzeit erweitert werden kann.

3.1. Standards

Folgende Standards bzw. Protokolle sind durch die Lageplattform zu unterstützen:

Transportnetz: IP

Verschlüsselung: HTTPS / TLS

Datenaustauschprotokoll: REST / RESTful API

Adressierung: OID

3.2. Architektur der Lageplattform

Die Lageplattform wird in Form eines Hubs (Verteilknoten) aufgebaut.

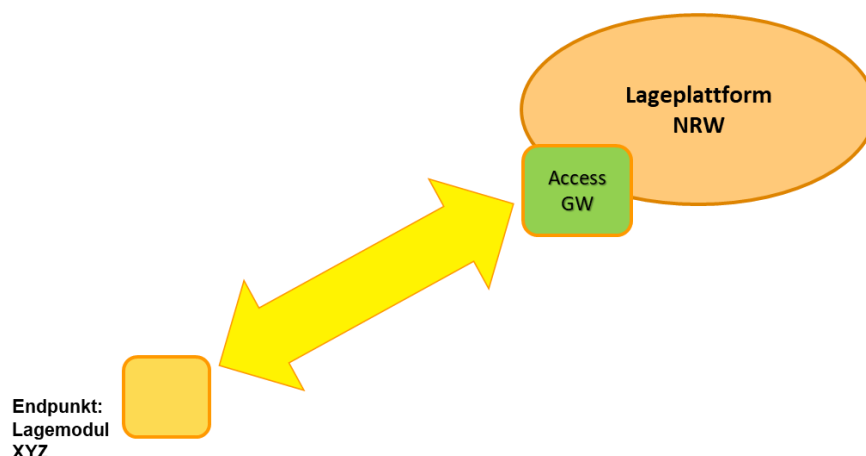
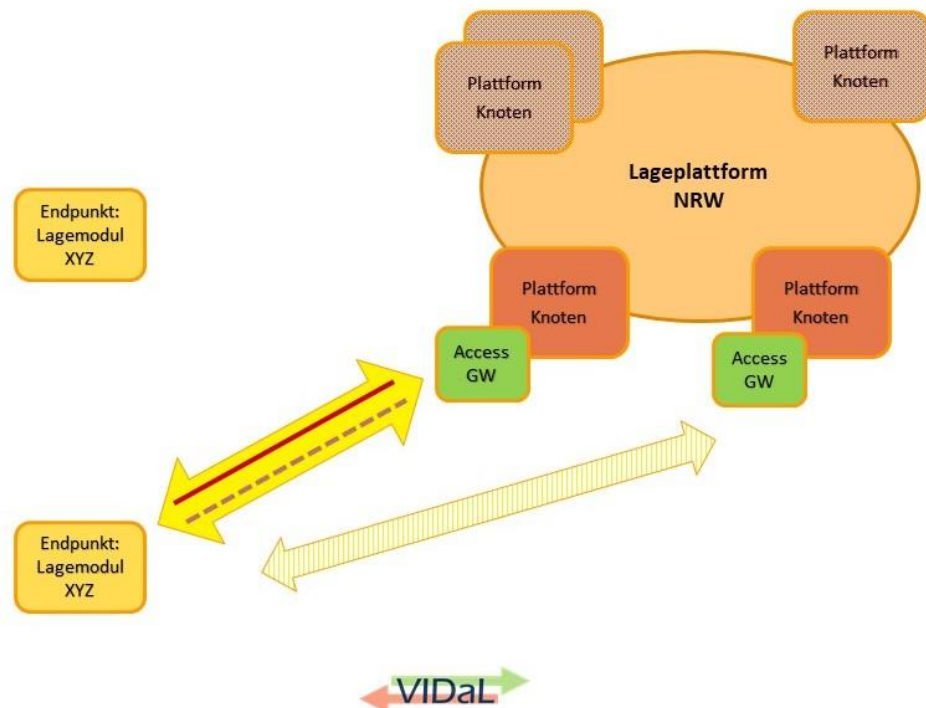


Abbildung 1: Prinzipielle Architektur der Lageplattform

Um eine hohe Ausfallsicherheit zu gewährleisten, wird dieser Hub in Form eines verteilten, vermaschten Hub-Netzes mit dezentralem Access aufgebaut. Diese Hubs werden georedundant im Land NRW verteilt und

können die Nachrichten ebenfalls verteilt vermitteln/verarbeiten (Lastverteilung). In einfachster Form besteht dieses Hubnetzwerk aus zwei vernetzten Hub-Knoten, die gegebenenfalls autark operieren können. Diese Hubs werden nachfolgend als Plattform-Knoten bezeichnet.

Damit werden die hohen Forderungen nach Dienstqualität, Redundanz und Erreichbarkeit erreicht.



5

Abbildung 2: Architektur der Lageplattform als Hub-Netzwerk

Die Summe der Plattform-Knoten stellt die eigentliche Lageplattform dar. Es gibt keine superzentralistische Anordnung. Ausnahmen stellen lediglich die Datenarchivierung und ähnliche Funktionen dar, die revisionssicher und außerhalb der Lageplattform (als Endpunkt der Lageplattform) gespeichert bzw. verarbeitet werden.

Jeder Endpunkt besitzt mindestens einen primären Access zu einem Access Gateway. Dieses Access Gateway ist ein Prozess auf dem Plattformknoten zur Realisierung jeglichen Kommunikationsanspruchs über REST aus Richtung Konsument. Zur Realisierung eines Zweitweges wird dem Konsumenten bei der Registration mindestens ein sekundärer Weg zur Plattform mitgeteilt, um im Fall des Nichterreichens des primären Access über den sekundären Access Zugang zur Lageplattform zu ermöglichen.

Sämtliche Endpunkte haben nur Verbindungen (ggf. redundant) zur Lageplattform. Es besteht keine Interkonnektivität der Endpunkte zueinander.

3.3. Eigenschaften der Lageplattform

3.3.1. Servicestrukturen der Plattform

Ein Zugangstyp, ein Schnittstellentyp: Es soll nur ein Typ von Zugang zur Lageplattform erfolgen. Dieser Access erfolgt für alle Konsumenten und fachlichen Provider in gleicher Systematik.

Endpunkte als Autoritäten (unter Berücksichtigung derzeitiger Kompetenzverteilungen und föderaler Governance-Strukturen): Fachlich-technische Systeme als Konsumenten oder Datenquellen für die Lageplattform NRW sind eigenständige Endpunkte (die sich als Autoritäten verhalten), die mit der Plattform verbunden sind und sich im Nachrichtenaustausch (an der Schnittstelle zwischen dem Endpunkt und der Lageplattform) angepasst an die Schnittstellen, Strukturen und Governance der Lageplattform NRW befinden. Alle Endpunkte verhalten sich als dessen Autorität in gleicher Weise und dienen zum Senden und Empfangen von Nachrichten. Jeder dieser Endpunkte ist in der Landeshierarchie eindeutig verortet und repräsentiert diesen Knoten. Zentrale Aspekte, wie die Adressierung oder die revisionssichere Archivierung von Informationen, werden über eine zentrale Governance des Bundeslandes NRW geregelt. Alle anderen Aspekte folgen den fachlich-strukturellen Governance-Anforderungen, die lokaler geprägt sind. Die Verantwortung für authentische Inhalte liegt bei den Endpunkten und nicht bei der Lageplattform. Folgende spezielle Endpunkte werden festgehalten, die der beschriebenen Endpunkt-Systematik folgen:

- **Zentrales Gateway zu externen Systemen:** Insbesondere beim interstaatlichen Nachrichtenaustausch ist von sich substantiell unterscheidenden Governance-Strukturen auszugehen. Der Übergang zu diesen externen Systemen (und Beteiligten) muss kontrolliert, sicher und systematisch erfolgen, wozu sichere Access-Gateways verwendet werden. Das Gateway folgt innerhalb der Lageplattform NRW den gemeinsamen Prinzipien hinsichtlich Nachrichtenaustausch, Adressierung, etc., wird jedoch nach außen entsprechend „übersetzt“. Dies können Beteiligte einer fremden Plattform oder z.B. Sensornetze von landeseigenen Sensorverbunden sein.
- **Syntaktische oder syntaktisch-semantische Übersetzung (Translations-Endpunkt):** Ein typischer Endpunkt ist auch ein plattformnaher fachlicher Provider zur z.B. fachlichen Translation von Nachrichten für VIDaL

3.3.2. Kommunikationskonzept

Das Kommunikationskonzept umfasst folgende Funktionen:

- Daten Ein-/ Ausgabe: manuell, teilautomatisiert, vollautomatisiert
- Automatische Überprüfung versendeter Nachrichten auf Gültigkeit bei Antrag zur Validierung
- Gesicherte Zustellung der Nachrichten zum Empfänger oder Empfängergruppe
- Datenhoheit liegt ausschließlich beim Sender
- Generierung von anlassbezogenen Gruppen (besonderes Ereignis) als Adressierungsziel
- Unterstützung von Referenzen/Links zu externen Streams von Bewegungsdaten, Audio, Video
- Transport von Nachrichten mit Metadaten zu Bildern, Videos, Karten, Audio (keine Übertragung von Massendaten)
- Unterstützung von Aliasadressen und Gruppenadressen (Verteiler)

3.3.3. Adaptermodell der Lageplattform

Die Lageplattform besitzt Adapter in Form von Access-Gateways. Diese Adapter haben folgende Funktionen:

- Verschlüsselte Kommunikation zum Access Gateway
- Kommunikation auf Basis von REST
- Registration, Deregistration, Authentifizierung, Autorisierung
- „Heart-beat“ zum Access (Lebenszeichengabe)
- Message-Validierung (optional)

Im Sinne aller fachlichen Nachrichten soll die Lageplattform Umschläge („Envelopes“) zum Transport aller gegenwärtigen und zukünftigen Nachrichtentypen unterstützen. Der Nachrichteninhalt („Payload“) soll von Anwendungsfall zu Anwendungsfall unterschiedliche Formate, bevorzugt standardisierte und kontextangepasste Formate wie CAP, EMSI, usw. unterstützen.

Über die Lageplattform werden dann innerhalb eines solchen Umschlages die Daten zwischen den einzelnen Endpunkten transportiert.

3.4. Kommunikation in den Netzebenen

3.4.1. Accessebene

Im Access der Konsumenten wird ein Host über Layer-3 Netze zugänglich gemacht. Dabei gibt es nur Verkehr über eine lokale Firewall des Konsumenten zum Dienstanbieter (dem Access Gateway). Es wird optional

ein zweiter Weg zum sekundären Access gewährt. Eine Interkommunikation (Adressierung, Routing, Fehlerfallbearbeitung, etc.) über die Plattform zu fachlichen Providern oder Konsumenten erfolgt auf Applikationsebene und nicht auf Layer3.

Zur Absicherung des Access wird typischerweise eine Firewall pro Knoten erforderlich sein. Dies ist begründet durch den Zugriff (Access), der über das Internet zu erwarten ist. Außerdem sind mögliche Infrastruktur-Deployments zu ermöglichen, die eine Positionierung der Knoten im Internet vorsehen (d.h. außerhalb eines sicheren Landesnetzes mit sicherem Übergang zwischen diesem und jedem externen Netzwerk, sowie dem Internet).

3.4.2. Backendnetz

Die Plattform-Knoten sind in Form eines Layer3 Verbundes miteinander vernetzt. Es wird auch in Hinblick auf die administrativen Aufgaben an den Knotenrechnern ein gesichertes verschlüsseltes IP-Netz verwendet.

3.5. Funktionale Anforderungen (Use Cases)

3.5.1. Prinzipielle Aufgabe der Plattform

Im Folgenden werden die fachbezogenen Anwendungen aufgeführt, welche sich derzeit in Bearbeitung durch Expertenforen des PMeV befinden:

- BAO – Austausch von Lageinformationen (VIDaL)
- AAO – Austausch von Einsatzinformationen (EFUL)

Die nachfolgenden fachbezogenen Anwendungen sind als mögliche, zukünftige Anwendungen zu verstehen, für welche teilweise heute schon konkrete Bedarfe in Deutschland bestehen, diese jedoch aufgrund derzeit fehlender Übertragungssysteme noch nicht realisiert wurden:

- AAO – Austausch von tagesaktuellen Informationen
- BAO – Echtzeit-Streaming* von Videos für eine gemeinsame Lagebeurteilung aller beteiligten Stäbe, ggf. auch beteiligter Leitstellen zur Steuerung der Einsatzkräfte
- AAO, BAO – Transport von Messenger-Chats unterschiedlicher Hersteller für einen lageabhängigen, organisationsübergreifenden Austausch von Chats, Bilder, Videos

3.5.2. Anspruch auf syntaktische und semantische Interoperabilität

Der Anspruch auf syntaktische und semantische Interoperabilität soll folgende Themen abdecken:

- Inanspruchnahme Adapterprinzip: Quellsysteme können selbsttätig in Trägerformate übersetzen (Entlastung der Translationsprovider)
- Semantik-Prozess als verteilter Provider: Dienste zur sowohl semantischen als auch syntaktischen Translation der Information in einheitliches Format und Bedeutung
- Service zur Übersetzung von Informationen unterschiedlicher Organisationen und Sprachen anhand der Referenz-Datenbank
- Semantische Konzepte der Organisationen (Teilnehmer) werden anhand der Plattform-Systematik „klassifiziert“

Erweiterungen zur gesicherten Übertragung „binärer Objekte“ wie Bildern, Dokumente, und Referenzen zu Videos / Streams etc. sollen möglich sein.

3.5.3. Weitere fachliche Ansprüche an die Plattform

- Aufgabenverteilung
 - Trennung der Aufgaben innerhalb des Systems durch Separierung und Austauschbarkeit funktionaler Einheiten, u.a. Übertragungswegsicherung, Authentifizierung, Autorisierung, Zugriffskontrolle, Routing, Adressierung, Datenhaltung, Verarbeitung, Resilienz-Mechanismen
- Nachrichten-Verarbeitung:
 - Sende- und Empfangsspeicher von Nachrichten
 - Die Default-Einstellung sieht vor, dass nur die empfangenen Daten gespeichert werden, zusätzlich können auch die versendeten Daten gespeichert werden. Bei Bedarf können andere Konfigurationen vorgenommen werden.
 - Bereitstellung einer gesonderten Übertragungskategorie zur transienten Nachrichtenübermittlung (ohne diese persistent zu halten, z.B. Lebensdauer = 0)
 - Bestimmung der Lebensdauer der gespeicherten Kopie einer Nachricht
 - Möglichkeit der Versendung von Referenzierungen großer Datenobjekte in einer Nachricht
 - Die Daten werden lokal (georeferenziert) gespeichert, die logische Aufteilung kann beliebig erfolgen (z.B. jede Gemeinde hat ihren eigenen Speicher vom externen Provider)

- Frei definierbare Netzwerktopologie innerhalb des Applikationsnetzwerkes
- Unterstützung von föderalen Strukturen bezüglich fremder Endanwender
- Entkoppelung von logischer und physischer Topologie des Systems bei frei definierbarer Abstraktion der Beziehungen im Applikationsnetz
- Adressierungssystem OID
 - Verlässlichkeit: Global unverwechselbar und konsistent, persistent (lange Lebensdauer), mit hierarchischer Namensstruktur, selbstverantwortliche Vergabe innerhalb der eigenen Organisation bei gleichzeitigem Einbinden in den global standardisierten Namensraum. Möglichkeit zur strukturierten Adressbezeichnervergabe entsprechend des bestehenden Meldungswegs, bzw. diesen abbildend.
 - Funktionalität, Flexibilität: Einfache Adressierung ist gegeben durch einen strukturierten Bezeichner. Gruppenadressierung kann stattfinden über (1) Bezeichner mit Wildcards, (2) Listen kombinierbar aus einfachen Adressen (Multicast) und solchen mit Adressmustern (siehe (1)), sowie (3) durch das Definieren von gespeicherten Verteilerlisten (Gruppenziele)
- Semantische Zuordnung und Interpretation von Inhalten
 - Bereitstellung eines Thesaurus zur Zusicherung eines gemeinsamen Verständnisses von Nachrichten, an den Übergängen innerhalb der strategisch-taktisch-operativen Kommandostruktur über einen externen Provider
 - Anpassung des Datenmodells und dessen Repräsentation bei gleichbleibender semantischer Gültigkeit
- Nicht-Abstreitbarkeit der Kommunikationsaktivitäten
 - Inhaltliche Bestätigung und Verifizierbarkeit auf dem Meldeweg (z.B. digitales Signieren durch die vorgesetzte Behörde)
 - Option einer dezentralen Beweisführung über verschickte Nachrichten
- Allgemeine Unabhängigkeit von Dritten bezüglich der Authentifizierung, Autorisierung und Gewährleistung/ Nicht-Abstreitbarkeit

3.6. Funktionale Anforderungen – Metaebene

Folgende fachunabhängige Eigenschaften/Fähigkeiten soll die Lageplattform ebenfalls besitzen. Hierbei stehen administrative Fähigkeiten im Vordergrund

3.6.1. Plattform Authentifizierung und Autorisierung

Aufgrund der sicherheitskritischen Natur eines VIDaL-Datenaustausches bzw. zukünftiger Datenaustauschvorhaben, sowie den Erfahrungen aus anderen Projekten, empfiehlt sich eine Schichtentrennung (siehe Abbildung 3:) wichtiger Funktionen.

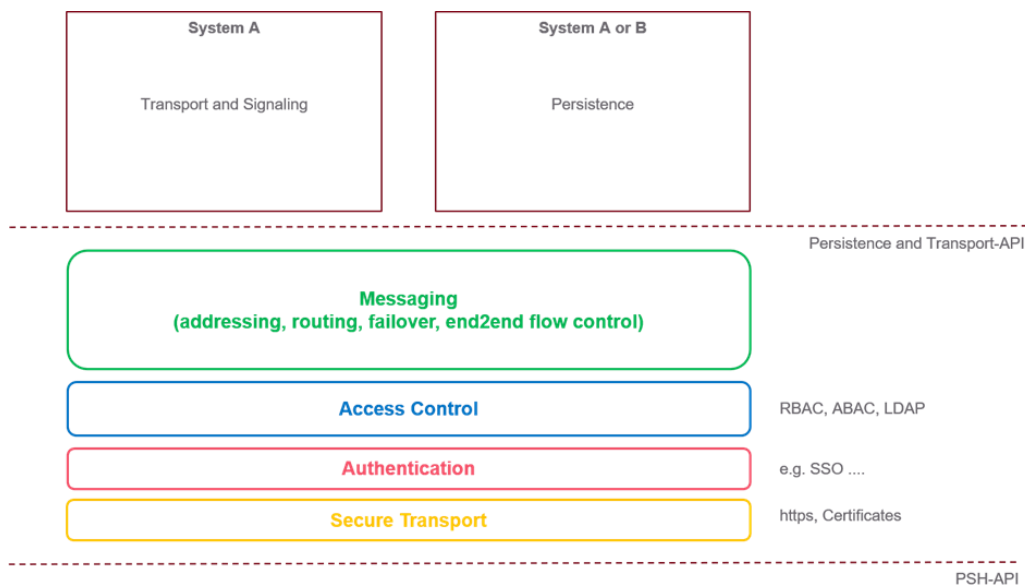


Abbildung 3: Schichtentrennung der Lageplattform

Sicherer Transport (z.B. über TLS), wird mit Zugangskontrolle (Authentication) und Berechtigungskontrolle (Access Control / Authentication) von dem eigentlichen Nachrichtenaustausch (Adressierung, Routing, Failover-Mechanismen, Flusskontrolle, ...) abgegrenzt.

Aus diesen Überlegungen leiten sich folgende Umsetzungsempfehlungen hinsichtlich der Schaffung einer geeigneten Schichtentrennung und Nachrichtenstruktur ab, um eine mehrstufige Sicherheitsstrategie zu gewährleisten (MUSS-Anforderungsempfehlung) und die oberhalb angeführte Schichtentrennung umzusetzen.

3.6.2. Nachrichtenstruktur und -sicherung

- Nachrichtenumschlag („Envelope“) zur Kapselung und Adressierung von Nachrichten und ggf. Erfassung weiterer Metainformationen werden Formate empfohlen, die einen geringen Overhead erzeugen und offengelegt sind. Diese Formate sollten zumindest folgende Felder/Attribute enthalten:

- Destination (OID-Adresse, siehe Abschnitt zu Adressierung)
 - Tags (optional für Nachrichten): Liste an Zeichenketten, die eine inhaltliche Zusammenführung von Nachrichten zu einem Thema erlauben.
 - Content type („ctype“): Zeichenkette, die das transportierte Nachrichtenformat der Payload beschreibt
 - Payload (siehe unterhalb) in einer textuellen Repräsentation gemäß zu unterstützenden Formaten.
- Innerhalb des Umschlags wird die eigentliche Nachricht („Payload“) transportiert, wobei folgende Payload-Struktur empfohlen wird:
 - Unabhängigkeit der Payload vom Umschlag, um keine Abhängigkeit zwischen Inhalt und Metadaten zu erzeugen.
 - Die Payload kann verschiedenste standardisierte (z.B. EMSI, CAP) als auch proprietäre Nachrichtenformate transportieren, die nicht über die gleichen Metainformationfelder verfügen, ohne den Standard aufweichen zu müssen
 - Standardisierte Datenformate EMSI und CAP sind als Payload inhärent zu unterstützen
 - Die Payload kann über eine weitere Verschlüsselung abgesichert werden (End-to-end-Encryption), um auch ggf. Informationen vor dem „Transporteur“ (i.e. die Nachrichteninfrastruktur und dessen Betreiber) zusätzlich zu schützen. Eine Verschlüsselung kann negative Auswirkungen auf die Übersetzungen von Nachrichten erzeugen oder eine Entschlüsselung erfordern (optionale Empfehlung für spätere Ausbaustufen).

3.6.3. Systemzugang

Authentifizierung (Authentication): Das System muss die „Identität“ (Pseudo-Identität, Nutzerbezeichnung, Node-Bezeichnung, etc.) des Absenders und Empfängers feststellen und den Zugang zum VIDaL-Nachrichtenaustausch von außen und von innen limitieren können.

Autorisierung (Authorization): Das System muss Möglichkeiten zur Steuerung der Zugriffsberechtigungen bieten und Nutzer entsprechend berechtigen.

3.6.4. Sicherer Transport

Transportverschlüsselung: Der Nachrichtenaustausch zwischen VIDaL-Hubs (Knoten) oder Endgeräten muss über eine Transportverschlüsselung verfügen, sofern dies technisch herstellbar ist. Durch Anwendung von HTTPS und TLS in der REST-Kommunikation ist eine gute Transportverschlüsselung implizit realisiert. Technisch ist dies unter

Umständen für extern eingebundene Lösungen nicht möglich, die jedoch nach Anforderung des Bedarfsträgers angebunden werden müssen.

3.6.5. Trennung der Technologiekomponenten

Die aufgelisteten Sicherheitsebenen sind funktional getrennt in der Lageplattform umzusetzen, um längerfristig den Austausch von Einzeltechnologien und somit Vorteile im Betrieb und der Erweiterbarkeit der Lageplattform zu ermöglichen.

3.7. Authentifizierung

3.7.1. Authentifizierungsmethoden

Basic Authentication: ist ein Authentifizierungsmechanismus bei dem der Server den Client/Benutzer auffordert seinen Benutzernamen und Passwort zu schicken. Bevor der Client dem Server die Daten übermittelt, werden diese aneinandergehängt und in einer Base64 Zeichenkette kodiert. Sobald die Zeichenkette am Server ankommt, werden die Daten vom Client mit den am Server vorhandenen Daten verglichen. Erst nachdem eine Übereinstimmung ermittelt werden kann, gilt der Client als erfolgreich identifiziert. Wie erwähnt, werden die Anmeldedaten nicht verschlüsselt, sondern nur kodiert. Um dieser Schwachstelle entgegen zu wirken, wird empfohlen, die Anmeldedaten nur über einen gesicherten Übermittlungskanal zu übertragen. Solch ein Übermittlungskanal wird mittels HTTPS ermöglicht.

Die erfolgreiche Authentifizierung des Clients/Benutzers ist eine notwendige aber nicht hinreichende Bedingung, um die Vertraulichkeit und Integrität der zu übertragenden Nachricht über den gewünschten Meldeweg zu gewährleisten. Erst wenn der Server sich gegenüber dem Client authentifiziert, wird der Kreis geschlossen und dadurch eine lückenlose Übertragung ermöglicht.

Digitale Zertifikate: mit Hilfe von digitalen Zertifikaten kann sich der Server identifizieren. Diese Zertifikate sind gleichzeitig auch für die Herstellung des HTTPS Kanals notwendig. Diese Vorgehensweise befähigt den Client/Benutzer rechtzeitig (bevor Anmeldeinformationen, Nachrichten übertragen werden) zu erkennen, ob sein Kommunikationspartner auch derjenige ist, der er vorgibt zu sein. Ein digitales Zertifikat enthält Informationen, die mit einer bestimmten Entität verknüpft sind, die von einer vertrauenswürdigen und anerkannten Zertifizierungsinstanz/Zertifizierungsstelle validiert und signiert worden sind. Die wichtigsten Informationen in einem digitalen Zertifikat sind: der Aussteller

des Zertifikats, der Gültigkeitszeitraum, die Signatur, das Subjekt (z.B. Domänenname des Servers), der öffentliche Schlüssel des Subjekts. Diese Informationen ermöglichen den Aufbau einer sicheren HTTPS Verbindung sowie die Authentifizierung des Servers gegenüber dem Client/Benutzer. Es gibt Situationen, in denen die Gültigkeit eines Zertifikats aufgehoben werden muss, bevor das im Zertifikat befindliche Ablaufdatum erreicht wird. Es gibt zwei Ansätze, die es ermöglichen, frühzeitig ein Zertifikat als nichtig zu erklären: Certificate Revocation List (CRL) und Online Certificate Status Protocol (OCSP). Bei CRL handelt es sich um eine Liste, die periodisch (von einmal bis mehrmals am Tag) aktualisiert wird, und die als nichtig erklärte Zertifikate enthält. Dies bedeutet, dass ein Server, der mittels Zertifikate seine Clients authentifiziert, jeden Tag die Liste herunterladen muss, um zu überprüfen, ob die Client-Zertifikate immer noch gültig sind. Als Alternative zu CRL wurde OCSP entwickelt, das aktuellere Informationen bezüglich eines Zertifikats liefern kann. Das Protokoll sieht vor, dass immer, wenn ein Server den Zustand eines Zertifikats prüfen will, er eine Anfrage an den OCSP-Server schicken muss, der als Antwort den ihm bekannten Zustand (gültig, nichtig, unbekannt) des Zertifikats übermittelt. Die Zertifikate können von einer international anerkannten Zertifizierungsstelle oder auch selbst signiert sein. Die Entscheidung welche Art von Zertifikat auszuwählen ist, ist vom Anwendungsfall abhängig wie z.B.: innerhalb eines abgeschotteten Netzwerkes können selbst signierte Zertifikate zum Einsatz kommen, während bei der Kommunikation über öffentliche Netzwerke selbst signierte Zertifikate im Normalfall nicht akzeptiert werden.

3.7.2. Vorteile und Nachteile der Methoden

Basic Authentication (BA)

Vorteile:

- Das Aufsetzen / die Bereitstellung der Authentifizierung mittels Benutzername und Passwort kann schnell ausgeführt werden, sowohl auf der Server- als auch auf der Benutzer-/Client-Seite.
- Sichere Passwörter können rasch erzeugt werden.

Nachteile:

- Der Benutzername und Password können während der Übermittlung (z.B. während des Authentifizierungsprozesses, des Zurücksetzens des Passworts) über das Internet abgehört und dadurch unwissend kompromittiert werden.
- Lange, starke, sichere Passwörter können schwer oder gar nicht von Menschen im Gedächtnis gespeichert werden. Dies führt dazu, dass leichter zu merkende Passwörter bevorzugt werden, die aber gleichzeitig unsicherer sind.

- Die Datenbank, in der die Passwörter gespeichert werden, kann als eine potenzielle Schwachstelle angesehen werden. Falls ein Angreifer Zugang zu der Datenbank erlangt, sind alle darin enthaltene Datensätze kompromittiert.

Digitale Zertifikate

Vorteile:

- Bei der Übermittlung eines Zertifikats werden keine geheimen Daten (z.B. Passwörter) mitgeschickt. Dies bedeutet, dass die Übertragung auch über unsichere Kommunikationskanäle stattfinden kann.
- Die Verwaltung der Zertifikate wird von einer zentralen Stelle gewährleistet, was dazu führt, dass der Prozess leichter zu verwalten ist.
- Digitale Zertifikate können auch für die Erstellung von verschlüsselten Meldewegen benutzt werden, die die Integrität und Vertraulichkeit der übermittelten Informationen gewährleisten.

Nachteile:

- Das Aufsetzen / die Bereitstellung als auch die Wartung der benötigten Infrastruktur ist ein komplexes Unterfangen.
- Falls die Zertifizierungsstelle kompromittiert wird, müssen alle sich im Umlauf befindlichen Zertifikate als kompromittiert eingestuft werden.
- Beim Widerruf eines Zertifikats muss mit einer Zeitverzögerung gerechnet werden, die von der benutzten Zertifizierungsstelle eingeführt wird.

3.7.3. Betriebsaspekte bei der Authentifizierung

Unabhängig von der ausgewählten Lösung müssen mehrere Aspekte im Vorfeld abgesprochen werden, die einen reibungslosen und sicheren Datenaustauschprozess ermöglichen können. Im Falle der Basic Authentication Lösung müssen folgende Punkte vereinbart werden:

- Muss sich eine Person das Passwort merken können?
- Wie soll das Passwort dem Benutzer übermittelt werden? Potenzielle Optionen wären: über das Internet, den Postweg usw.
- Falls es dem Benutzer bewusstgeworden ist, dass sein Passwort kompromittiert worden ist, wie sieht das weitere Vorgehen aus? Wer wird benachrichtigt? Wie wird dem Benutzer ein neues Passwort zugewiesen? Wird dem Benutzer der Zugang zu allen Dienstleistungen verweigert?
- Soll ein uneingeschränktes Zurücksetzen des Passworts möglich sein?
- Wie sieht der Ablauf aus, falls die Passwörter auf der Server-Seite kompromittiert werden?

- Welche Zertifizierungsstellen sollen akzeptiert werden?
- Falls ein Zertifikat kürzlich abgelaufen ist, soll dies während des Authentifizierungsprozesses toleriert werden?
- Wie sieht der Rückfallplan bei der Kompromittierung einer Zertifizierungsstelle aus?
- Bei der Kompromittierung eines einzelnen Zertifikats: sollte man nur auf CRLs und OCSP setzen oder vielleicht auch andere schnellere Lösungen in Betracht ziehen?
- Wie soll sich das System verhalten falls ein Zertifikat nicht validiert werden kann, weil z.B. die Zertifizierungsstelle nicht erreichbar ist?

3.8.1. Ausgangssituation und Anforderungen

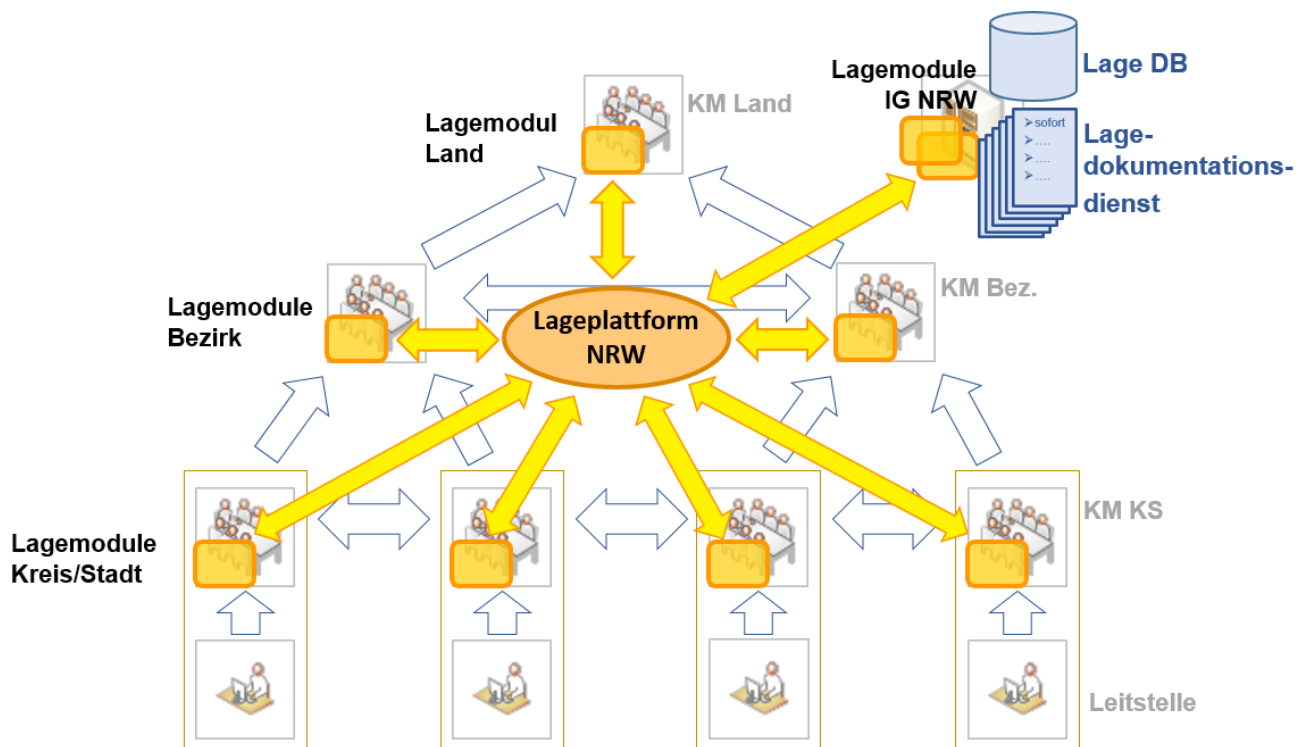


Abbildung 4: Architektur von VIDaL

Wie in Abbildung 4 dargestellt, erfordert VIDaL einen innerhalb der Landesgrenzen föderativ kollaborativen Ansatz bei gleichzeitigem Bedarf an Abgrenzung von Verwaltungs- und Datenhoheit.

Wichtige vorhersehbare Parameter zur Beschreibung der Anforderungen an ein Adressierungsschema für die Systemarchitektur sind: Das Nachrichtenaufkommen, die Anzahl zu adressierender Endpunkte, die Dynamik in der Kommunikationsstrukturveränderung und die Agilität von Verfahrensweisen und Problemlösungswerkzeugen, um einen in allen Situationen optimalen Betrieb aufrecht erhalten zu können.

Anforderungen im Einzelnen:

- Zu unterstützende Protokolle, protokollmultipler Nachrichtentransport
- Einzeladressierung aller Entitäten im Netzwerk
- Themenbezogene Zuordnung von Nachrichten auf Ereignisse
- Statische Gruppenadressierung, zusammenfassen von Adressen (Verteiler)
- Autarke Administration und Datenhoheit im eigenen Adressraum
- Ein föderiertes Zusammenspiel von Sub-Systemen
- Ein privates Overlay-Netzwerk von Applikationen im Internet
- Zugriffs- und Übertragungskontrolle

3.8.2. Verwendung von OIDs

Die unter Abbildung 4 dargestellte Hierarchie und Bereichsebenen sollen logisch auf das VIDaL Kommunikationssystem abgebildet werden. Dazu werden Object Identifier (im Weiteren als OID bezeichnet) verwendet

Ein Object Identifier ist:

„ [...] ein weltweit eindeutiger Bezeichner, der benutzt wird um ein Informationsobjekt zu benennen [...]. Ein OID stellt einen Knoten in einem hierarchisch zugewiesenen Namensraum dar, [...]. Jeder Knoten ist durch eine Folge von Nummern eindeutig gekennzeichnet, die seine Position beginnend an der Wurzel des Baumes angibt. Neue Knoten zur eigenen Verwendung können bei den entsprechenden Autoritäten des übergeordneten Knotens beantragt werden. Die Regeln für die Vergabe und Registrierung von OIDs sind festgelegt in den Normen ISO/IEC 9834 und DIN 66334. Die Verwaltung des OID-Baumes und die Sicherstellung der Eindeutigkeit von OIDs beruhen auf der Übertragung der Zuständigkeit für die untergeordneten Knoten an den Besitzer einer OID.“

Im Vergleich zu einem proprietären Adressierungsschema für die am VIDaL Kommunikationssystem teilnehmenden Organisationen und Behörden bietet die Adressierung über den standardisierten Identifikationsmechanismus mittels OID eine Reihe von Vorteilen:

- OIDs gewährleisten eine weltweit eindeutige Kennzahl zur Identifizierung von Objekten, wodurch der Austausch von Daten auch auf eine internationale Ebene ausgeweitet werden kann.
- Mittels OID können Objekte aller Art eindeutig identifiziert werden, also z.B. Organisationen und ihre untergeordneten Einheiten ebenso wie IT-Systeme, Dokumente, Nachrichten etc.
- Erweiterbarkeit und Skalierbarkeit: Durch den hierarchischen Aufbau ist das OID Identifizierungsschema nahezu unendlich erweiterbar, jeder „Ast“ kann so tief wie notwendig aufgeschlüsselt werden.
- Das kompakte Format der OIDs aus durch Punkte getrennte Zahlenkombinationen erlaubt eine effiziente Verarbeitung beim Austausch von Daten.
- Die Vergabe von OIDs ist im Standard explizit dezentral geregelt. Das bedeutet, dass jeder Knoten in der OID-Hierarchie selbst für die Vergabe von untergeordneten OIDs zuständig ist. Dadurch ergibt sich eine sehr flexible Gestaltung je nach Anwendungsbereich des jeweiligen Unterbaumes.

Aufgrund der hierarchischen Struktur und ihrer globalen Signifikanz bei gleichzeitiger freier Definierbarkeit im eigenen Geltungsbereich eignet sich das OID Schema somit gut für die logische Abbildung einer hierarchisch föderativen Systemstruktur wie jener von VIDaL.

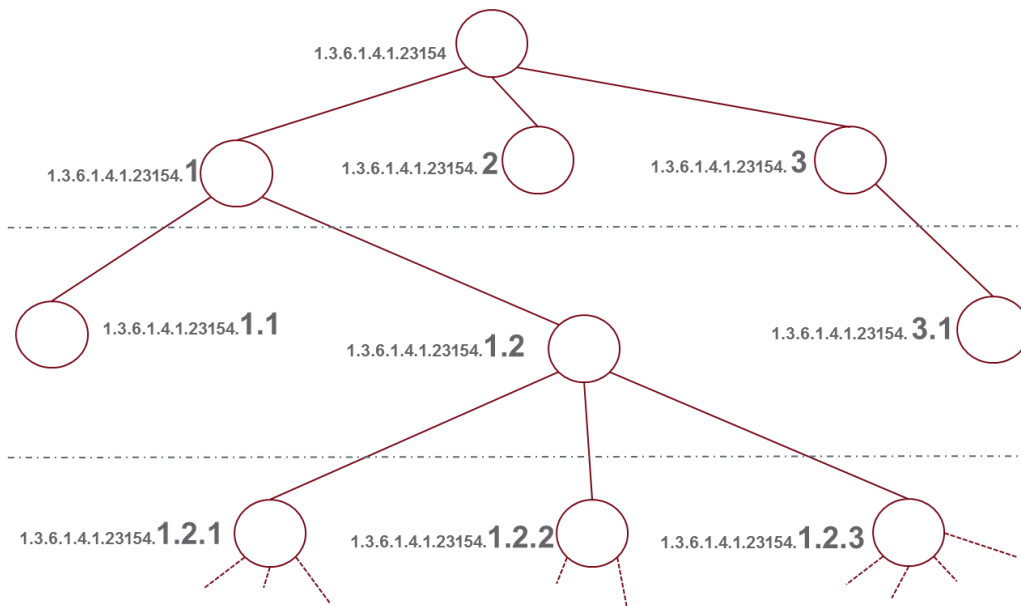


Abbildung 5: Beispiel für eine OID Hierarchie

In Abbildung 5 wird beispielhaft eine von mehreren möglichen Umsetzungen zur Adressierung von hierarchisch aufgebauten Organisationseinheiten dargestellt. Als Ausgangspunkt für den

Hierarchiebaum in internationalem Kontext dient hier die Enterprise OID der AIT Austrian Institution of Technology. Der Identifier in seinen drei verschiedenen Darstellungs-möglichkeiten:

DOT: 1.3.6.1.4.1.23154

IRI: /ISO/Identified-Organization/6/1/4/1/23154

ASN.1: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 23154}

Die oberste Hierarchieebene hat die OID: 1.3.6.1.4.1.23154 und deren untergeordneten OIDs mit der Endung .1, .2 und .3. Die mittlere Ebene wird über .1.1, .1.2 und .3.1 adressiert. Das gleiche Verfahren wird dann auf die darunterliegende Ebene angewendet.

3.8.3. Netzwerkzugang und Nachrichtenübermittlung

Zwei unterschiedliche Arten von Nachrichtensender und -empfänger können identifiziert werden: (1) Endpunkte als Nachrichtenquellen und -senken, sowie (2) Zugangsknoten welche den Endpunkten Zugang zum Netzwerk gewähren und deren Nachrichten weiterleiten. Siehe dazu auch folgende Abbildung 6

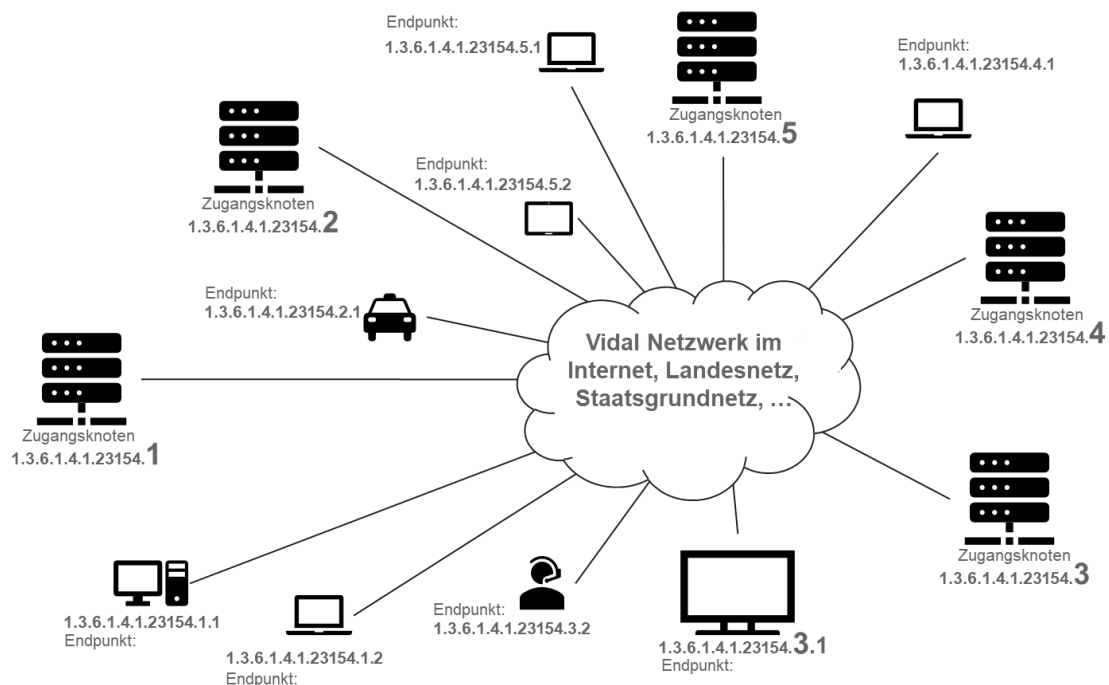


Abbildung 6: Verteilungsagnostischer Zugriff

Die Zulieferung der Nachrichten erfolgt indirekt über zwei Ebenen: 1. Im Zugriff auf die Zugriffsknoten über URLs und 2. durch Auslieferung der Nachrichten über OIDs innerhalb des Applikationsnetzwerkes.

Die Vergabe von OIDs sollte durch das System erfolgen, und deren Zuordnung an Endpunkte, die sich mit dem System verbinden, durch die Zugangsknoten via Authentifizierung zugewiesen werden.

Im ersten Schritt vertrauen alle Zugriffsknoten und Endpunkte auf die physische Übermittlung ihrer Nachrichten über das Internet. Hier erfolgt die Adressierung über URLs und die Zustellung via sog. REST-Services. Darüber liegend werden im zweiten Schritt, innerhalb eines Netzwerkes aus Applikationen, die Metadaten der Nachrichten überprüft, um diese an den entsprechenden Endpunkt weiterzuleiten. Zusätzlich zu anderen Steuerfunktionen bestimmen die Sender und Empfänger OIDs, an wen die Nachricht weitergeleitet oder übergeben werden soll und ob die jeweiligen Sender und Empfänger über die entsprechenden Rechte verfügen.

Die gesamte vom unterliegenden Netzwerk zu übertragende Nachricht besteht aus der aktuell zu übertragenden Information sowie zusätzlicher Metainformation zur Übertragung. Der aktuelle Inhalt einer zu versendenden Nachricht wird in einen Umschlag gepackt, so dass Datenpakete von beliebiger Protokollstruktur vermittelt werden können.

3.8.4. Adressierungsverfahren und Informationsordnung

Über die Beschreibung der Adressierungssyntax, der Nomenklatur der Adressbezeichner hinaus, gilt es auch die darüber liegende Semantik des Verfahrens zu beschreiben. Zwei Basisverfahren der Adressierung können unterstützt werden: (1) Einzel-Adressierung von Endpunkt zu Endpunkt und (2) Adressierung von Endpunkt zu einer Gruppe von Endpunkten. Zusätzlich dazu kann noch die additive Funktionalität des Nachrichten-Taggings beschrieben werden, um einzelne Nachrichten zu Konversationen zusammenzufassen, um Konversationen Ereignissen und Themen zuzuordnen, oder um verfahrensspezifische Metainformationen wie Security Tags anfügen zu können.

Jede Nachricht enthält die Quell- (src) und Zieladresse (dest) der zu übertragenen Information. Bei der Einzel-Adressierung (1) enthalten beide Adressen konkrete OID Bezeichner, z.B. von OID=1.2.3.45 an OID=1.2.5.86. Bei der Gruppen-Adressierung kann ein bestimmter Ast in der OID Hierarchie angesprochen werden, so dass mit der Nachricht von OID=1.2.5.9 an 1.2.7.6.* alle registrierten Endpunkte in einem Adressraum unterhalb der OID Hierarchie von 1.2.7.6 adressiert würden. Alle Endpunkte, deren Adressen mit 1.2.7.6 beginnen, würden die

Nachricht erhalten, nicht aber jene mit dem Beginn ihrer Adresse als:
1.2.7.5 oder 1.2.7 ...

Zusätzlich und optional könnte jeder Nachricht eine Liste von Tags zur thematischen, organisatorischen oder funktionalen Zuordnung angefügt werden. Abgesehen von sicherheitstechnischen Funktionen, wie die Auswertung von Security-Tags, könnten sich Interessenten zum Zwecke einer umfassenden Lageübersicht über bestimmte Ereignisse oder Themen und deren Gesamtkontext mit allen zugehörigen Konversationen informieren lassen.

Beispiele zur Nomenklatur der eben beschriebenen Funktionalitäten:

- 1) Einzel-Adressierung: src=1.3.6.1.4.1.23154.3,
dest=1.3.6.1.4.1.23154.1.2.3
- 2) Gruppen-Adressierung: src=1.3.6.1.4.1.23154.3,
dest=1.3.6.1.4.1.23154.1.2.*
- 3) Tagging:
 - a) src=1.3.6.1.4.1.23154.3, dest=1.3.6.1.4.1.23154.1.2.1,
tags=[hafen-feuer, rettungseinsatz, sec:56ad6483dc40a, ...],
 - b) src=1.3.6.1.4.1.23154.1, dest=1.3.6.1.4.1.99999.*, tags=[hafen-feuer, presse]

Einführung von Alias(s) als Tags für Endpunkte sind zulässig und fachlich hilfreich.

3.8.5. Adressierung und Geo-Verteilung

Die Funktionalitäten zur Replikation von Zugriffsknoten und deren Geo-Verteilung sollten unterschieden werden von jener der Nachrichten-übermittlung. Zusätzlich sollte die logische Unterteilung des Adressraumes mittels hierarchischer Gliederung durch OIDs auch eine nicht nur logische, sondern auch physische Trennung der Endpunkte ermöglichen. Letzteres ist vor allem dann wichtig, wenn unterschiedliche Institutionen im Netz die Hoheit über ihre Daten und über die Nachrichtenvermittlung behalten und Verantwortlichkeiten zu Datenschutz und -sicherheit entsprechend zugeordnet werden müssen.

So ergeben sich zwei unterschiedliche, ggf. ineinandergreifende Verteilungsmechanismen:

1. Eine Geo-Verteilung basierend auf flacher, knotenorientierter Replikation, so dass physisch und lokal getrennte Knoten logisch wie ein einziger Knoten operieren können. Hierbei werden die Zugangsknoten über ihre URLs verbunden und applikationsnetzwerksintern über eine eindeutige ID

angesprochen. Miteinander verbundene Zugangsknoten tauschen dann alle Nachrichten, die sie von den Endpunkten zur Weiterleitung erhalten, untereinander aus. Darüber hinaus dient dieses Übertragungsschema dazu, Administrationsbefehle und Verwaltungsdaten zu replizieren.

2. Eine Geo-Verteilung basierend auf Adressraumaufteilung wird, im Gegensatz zu Punkt 1, dazu verwendet, um in Unterbäumen der Gesamthierarchie des OID Schemas logisch und physisch separiert operieren zu können.

Die Kombination beider Methoden wird in Abbildung 7 beispielhaft dargestellt. Unterschieden werden kann zwischen „Replikation vs. Adressraumverwaltung“ und „Nachrichten vs. Administrationsevents“. Replikation kann breitflächig über das Zusammenschalten von Zugangsknoten für verteilte Administration und Nachrichtenweiterleitung oder selektiert via Gruppen-Adressierung als getrennte Adressraumverwaltung innerhalb der OID Hierarchie durchgeführt werden.

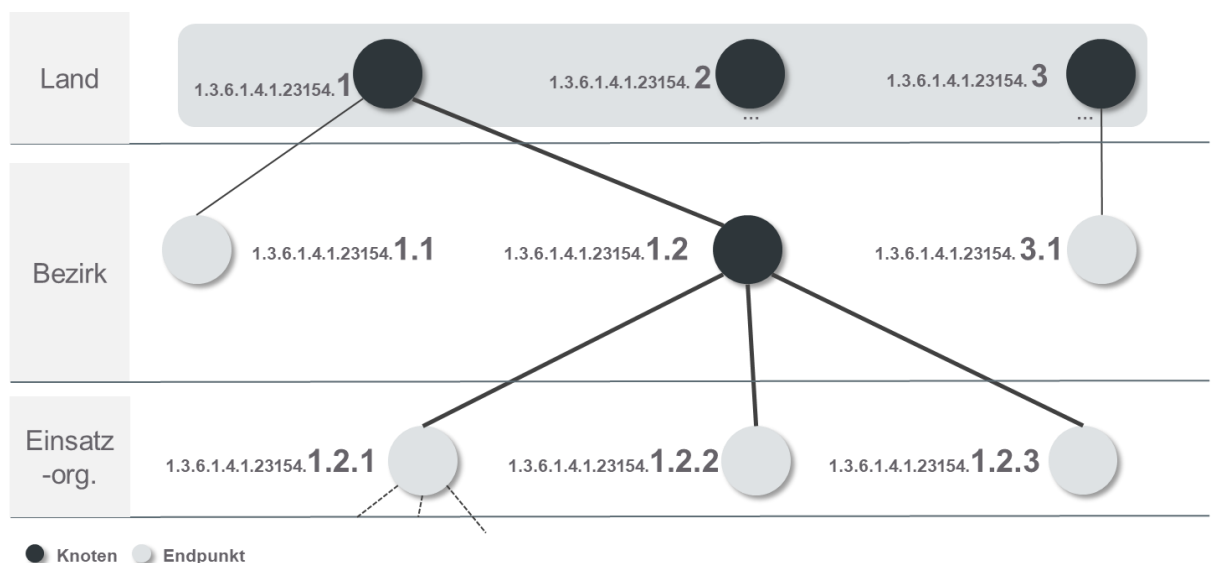


Abbildung 7: Adressierung vs. Geo-Verteilung der Knoten

Das Beispiel in Abbildung 7 zeigt mehrere Knoten der Lageplattform VIDaL, die über eigene Adressbereiche verfügen. Logisch untergeordnet sind Endpunkte oder weitere Knoten zugeordnet, denen einen Sub-Adressbereich zugeordnet ist. Mit dieser Logik sind flache als auch hierarchische Topologien zu jedem Zeitpunkt herstellbar, d.h. eine iterative Ausrollbarkeit sowie ein iteratives Wachstum der Plattform ist sichergestellt. Weiteres sind über diesen Mechanismen „lokale“ Datenverteilungen über den nächstgelegenen Knoten möglich, die bei

Netzausfällen einen Partitionsbetrieb ermöglichen. Einzelne Knoten können weiteres gespiegelt werden, um ohne logische Trennung eine Redundanz oder sogar Georedundanz zu ermöglichen.

3.8.6. Adressierung und Autorisierung

Für die Autorisierung zur Nachrichtenübermittlung, d.h. die Kontrolle darüber, wer an wen Nachrichten senden und wer von wem Nachrichten empfangen darf, kann der gleiche Mechanismus, wie er zuvor für die Nachrichtenweiterleitung und Gruppenadressierung mit OIDs beschrieben wurde, verwendet werden.

Auch hier wird die Aufgabe in zwei Schritten abgewickelt: (1) Authentifizierung und Autorisierung bei der Verbindung zu den Zugriffsknoten über REST Schnittstellen und dann (2) innerhalb des Applikationsnetzwerkes basierend auf der Sender- und Empfängerinformation in den Metadaten der Nachricht.

Im ersten Schritt kommen die üblichen Mechanismen und Industriestandards beim Zugriff auf Internet Ressourcen zu tragen, im zweiten Schritt wird die Berechtigung zum Senden bzw. Empfangen einer Nachricht aufgrund von Adresslisten und Platzhaltermustern von OIDs beschrieben.

Der vorgeschlagene Mechanismus zum Taggen von Nachrichten kann auch für Security Tags verwendet werden. Außerdem können benutzte oder benutzbare Tags im System verwaltet und deren Zugriffsrechte administriert werden.

Beispielhafte Skizzierung zur Definition von Zugriffsrechten:

- user-01: send=[1.2.3.4, 1.2.3.5.1, 1.9.*] receive=[1.2.3.4.*, 1.9.*]
- user-02: send=[] receive=[1.8.3.*]
- user-03: send=[1.2.4.6.*, 1.2.9.5] receive=[]

und für Tags:

- hafen_feuer: send=[1.2, 1.9] receive=[1.2.3.*, 1.9.*]
- presse: send=[1.2.1] receive=[1.*]

Im obigen Beispiel kann "user-01" an die Adressen 1.2.3.4, 1.2.3.5.1 und an alle Endpunkte unter der OID 1.9 senden, sowie von allen unter den OIDs 1.2.3.4 und 1.9 registrierten Sendern empfangen. Der User „user-02“ kann an niemanden versenden, aber von bestimmten OIDs und OID Gruppen empfangen, während User „user-03“ an die Adresse 1.2.1 Nachrichten verschicken, aber von niemandem Nachrichten empfangen kann.

Ähnlich könnte eine Zugriffskontrolle für Tags definiert werden. In gegebenem Beispiel könnten die User mit den OIDs 1.2 und 1.9 Nachrichten mit dem Tag „hafen_feuer“ versenden und User unter den OID Adressgruppen 1.2.3 und 1.9 Nachrichten, die dieses Tag enthalten, bei Bedarf abrufen.

3.8.7. Föderale Adressierung

Die Lageplattform NRW soll für einen zukünftigen Datenverbund über föderale Grenzen und Systeme mit anderen Adressierungsparadigmen hinweg vorbereitet sein. Dazu wird ein Konzept entwickelt, das eine Adressumsetzung an der Systemgrenze vorsieht. Für die Abbildung von OID in externe Adressen wird ein Gateway erforderlich sein, das die Ziel- und Quelladressen der Nachrichten durch die im jeweiligen System bekannte Adresse ersetzt. Um die Adressen von externen Knoten auf OID abzubilden, wird ein OID-Range reserviert, der zur Adressierung der externen Systeme und Clients verwendet wird. Durch dieses Mapping ist es möglich, die externen Systeme auf die gleiche Art und Weise wie plattform-interne Knoten in das Autorisierungs- und Authentifizierungskonzept zu integrieren.

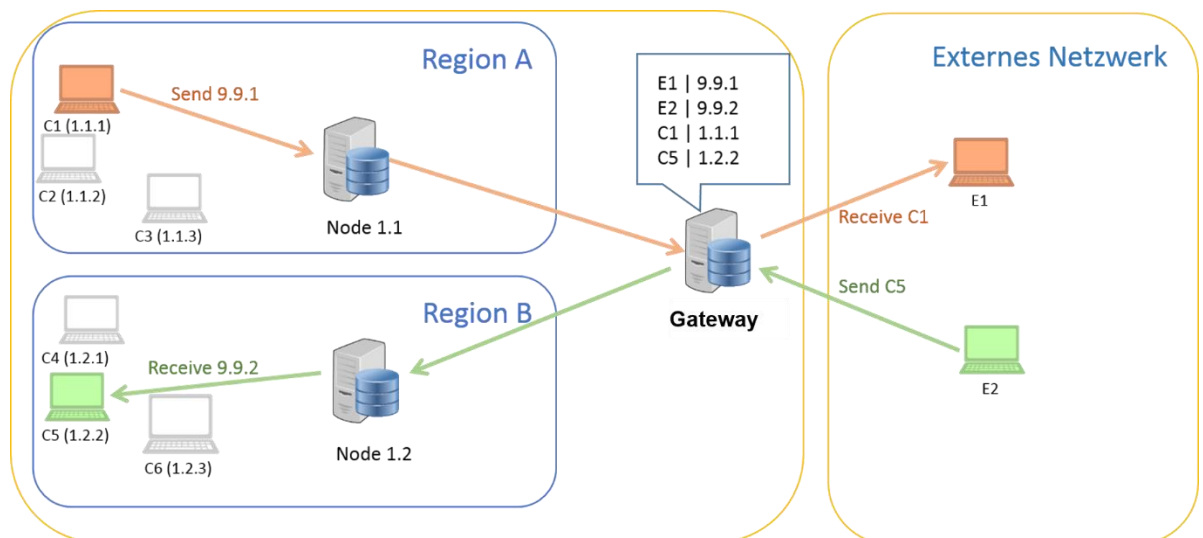


Abbildung 8: Föderale Adressierung

In Abbildung 8 ist die Kommunikation über Systemgrenzen hinweg beispielhaft dargestellt. Der OID-Range für externe Systeme ist hier mit 9.9.* definiert. Ein Knoten C1 innerhalb der Lageplattform NRW adressiert Nachrichten an einen Knoten E1 in einem externen Netzwerk mit der OID 9.9.1. Durch das OID-Routing werden diese Nachrichten an das Gateway geleitet. Dort erfolgt die Umsetzung in die tatsächliche externe Adresse E1. Im umgekehrten Fall sendet ein externer Knoten E2 Nachrichten an den für ihn als C5 zu adressierenden Knoten in der Lageplattform NRW.

Dazu muss er die Nachricht IP-technisch an das Gateway senden. Dort wird die Zieladresse durch die OID des Zielsystems (1.2.2) ersetzt, die Absenderadresse wird durch die dem externen Knoten E2 zugeordnete OID 9.9.2 ausgetauscht und an den plattform-internen Knoten C5 geroutet.

Voraussetzung für die Anbindung von externen Systemen ist – analog zur Anbindung der plattform-internen Knoten – die Registrierung jedes neu zu integrierenden Teilnehmersystems an der Lageplattform NRW wie es im Abschnitt „Sicherheit und Rechteverwaltung“ dieses Dokumentes beschrieben ist.

3.8.8. Dienstprimitive – Master Use Cases

Das funktionale Set von Metafunktionalität und Endpunkt zentrierten administrativen Funktionen wird in Dienstprimitive zusammengefasst und in diesem Kapitel zusammen dargestellt.

Der Endpunkt Teilnehmer / das Lagemodul besitzt eine P2P Verbindung zum zugehörigen Access (logischer Zugangspunkt) der Lageplattform und hat auch nur dorthin eine Verbindung (IP basiert). Eine ersetzende Verbindung kann eingenommen werden zu einem vertretenden Access der Lageplattform (Redundanzfall). Es besteht keine Interkonnektivität der Endpunkte zueinander.

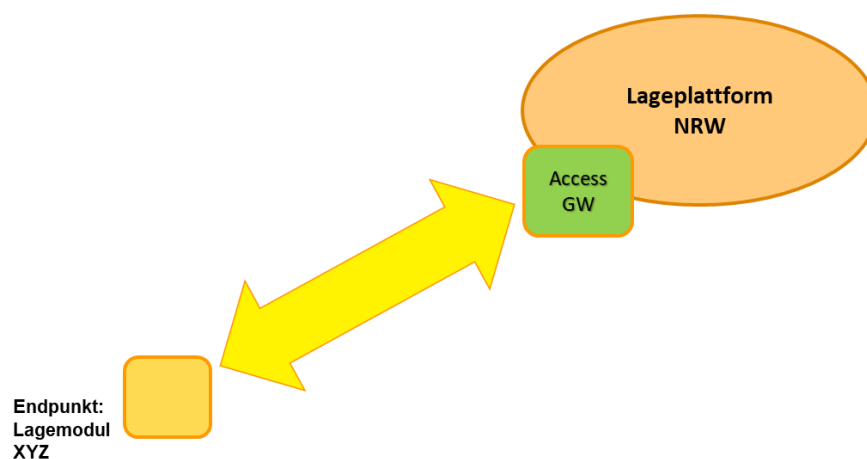


Abbildung 9: Zugang zur Lageplattform über logischen Access eines Knoten

Die Services umfassen folgende Funktionen:

- Erst-Registrierung eines Endpunktes / Teilnehmers (Anlage eines Teilnehmers / Endpunktes)
- Löschen eines Endpunktes (administrativer Kill eines Teilnehmers / Endpunktes)
- Registrierung eines Endpunktes / Teilnehmer zum Verkehrsantritt (Anmelden von der Plattform)

- Deregistrierung eines Endpunktes / Teilnehmer zum Verkehrsaustritt (Abmelden von der Plattform)
- Funktionen zum Nutzverkehr – Nachrichten senden
- Funktionen zum Nutzverkehr – Nachrichten empfangen
- Lebenszeichen (Nullfunktion) des Endpunktes
- Lebenszeichen (Indikation optional) des entfernten Endpunktes
- Lebenszeichen des Access Gateways zur Plattform
- Redundanz und Vertretungsnachrichten des VIDaL Access Gateways
- Administrative Funktionen aus Richtung Endpunkt

3.8.9. Anbindung Endpunkt zum Accesspoint mit REST

Representational State Transfer [7] (REST), das vom Browser genutzt wird, ist ein Programmierparadigma des Internets. Da die Nutzung der Cloud mittlerweile verbreitet ist, tauchen eine Vielzahl von Programmierschnittstellen (APIs) auf, um Webdienste verfügbar zu machen. Die logische Wahl ist REST, um APIs zu erstellen, die es Endbenutzern erlauben, sich mit Cloud-Diensten zu verbinden und mit ihnen zu interagieren. [8]

Eine RESTful API schlüsselt eine Transaktion auf, um eine Reihe von kleinen Modulen zu erstellen. Jedes von ihnen ist zuständig für einen bestimmten, der Transaktion zugrundeliegenden Teil. Diese Modularität bietet Entwicklern eine erhebliche Flexibilität. Es kann für sie aber auch eine Herausforderung sein, dies von Anfang an zu berücksichtigen.

RESTful APIs machen sich explizit die in RFC 2616 definierten HTTP-Anfragemethoden zunutze. Sie verwenden PUT, um den Zustand einer Ressource (das kann ein Objekt, eine Datei oder ein Block sein) zu ändern oder sie zu aktualisieren. Mit GET wird eine Ressource abgerufen, mit POST wird sie erstellt und mit DELETE gelöscht.

Vorteile:

Bei REST handelt es sich um einen offenen Quasistandard, welcher eine große Verbreitung erlebt und zudem einen gesicherten Datenaustausch zwischen Applikationen über TCP/IP realisiert. REST hat sich auch wegen der http(s) konformen Kommunikationsweise rasant verbreitet, da Sicherheitsmechanismen zur Verkehrskontrolle aus der Browsernutzung bekannt und etabliert war. Somit sind Netzübergänge aus unterschiedlichen Sicherheitsniveau der unterschiedlichen Netze gut betreibbar. Die Anwendbarkeit von REST in einer bestehenden Web-Infrastruktur macht die Verwendung besonders modern zukunftssicher.

In den letzten Jahren wurde z.B. die Verwendung von SOAP sukzessive von REST-Services im Internet abgelöst.

REST dient, wie SOAP (oder WSDL und RPC) also vor allem der Kommunikation zwischen Maschinen. REST hat sich hier als besonders hilfreich erwiesen, da es anders als SOAP keine Methodeninformationen kodiert.

REST eignet sich vor allem dann, wenn es darum geht, Daten zu erhalten und gegebenenfalls anzuzeigen. Zudem kann man REST sehr einfach implementieren.

Die Anwendung der RESTful API ist seit Jahren die geforderte Kommunikationsmethodik zur Datenaustausch in der zivilen Gefahrenabwehr laut DIN Spec 91287 [6].

Nachteile:

Da es bei REST, im Gegensatz zu SOAP, an Standardisierung fehlt, ist die Gefahr von Missverständnisse bei der Service Deklaration gegeben. Es ist daher zwingend erforderlich Trägerformate (d.h. gemeinsame Datenformate) zu vereinbaren, die innerhalb des REST-Methoden-Korsetts transportiert werden. Die Lageplattform VIDaL benötigt daher definierte Schnittstellen (insb. ein definierter Nachrichtenumschlag sowie anerkannte Payload-Formate).

Abgeleitete Anforderung:

Aus diesen Überlegungen wird die Anforderung zur Verwendung von REST-Services zwischen Lageplattform VIDaL und ihren assoziierten Endpunkten abgeleitet. Weitere zusätzliche Schnittstellenparadigmen können optional bereitgestellt werden.

3.8.10. Erstregistration (Onboarding) und Löschung (Kill)

Die Erstregistrierung (Onboarding) dient zur Initialisierung eines Endpunktes gegenüber der Plattform. Hierbei werden der logische Name, die OID des Endpunkts, auf Basis eines Initialisierungsdatensets mit einem offline (Zweitweg) erlangten Zertifikat geprägt und der Plattform über eine Initialsession bekannt gemacht. Diese Initialisierung erfolgt einmalig.

Eine administrativ erzwungene Löschung eines Endpunktes deaktiviert alle Caches und die Autorität des Endpunktes in der Plattform (Kill).

3.8.11. Registrierung und Deregistrierung

Die Registrierung und Deregistrierung eines Endpunkts sind Aktivitäten zur planmäßigen Betriebsaufnahme und -trennung von der Plattform.

Bei der Registration erfolgt eine vollständige Identifikation des Endpunktes gegenüber der Plattform. Als Ergebnis der Registration erfolgt eine Übergabe eines Vektors zur Autorität des Endpunktes und Reserveadressen zum Backup-Access. Der reguläre Betrieb tritt ein und die Nachrichten Queue wird symmetrisch verarbeitet.

3.8.12. Metadatenset von Nutznachrichten

Das Metadatenset des Nachrichtenumschlages umfasst folgende Attribute:

- Nachrichten_ID (Quell-OID + Zähler)
- Zieladresse (OID) + Adresszusatz + Ziel Name (Alias)
- Priorität
- Absenderadresse (OID) + Adresszusatz + Absendername
- Nachrichtentype + Version der Nachricht (7a), Version (7b – fachliche Version)
- Ident-Vektor (separierte Indikatoren)
- Timestamp
- Secure (Flag für sichere Nachricht)
- Tags (Symbol auf fachlichem Anlass)
- Timeout (Lagedauer in Warteschlangen)
- Signatur (optional)

3.8.13. Nachrichten senden

Derzeit sind folgende Nachrichten spezifiziert, welche Anforderungen aus dem AP1 abdecken. Diese Nachrichtentypen werden in standardisierten Umschlägen (Envelope) transportiert:

- LageInformation (enthält Erstmeldung, Folgemeldung und Schlussmeldung)
- RessourceInformation (von einem ELS an die Lagedatenbank)
- StatistikInformation (von einer Leitstelle an die Lagedatenbank)
- BestätigungLageInformation
- BestätigungRessourceInformation
- BestätigungStatistikInformation

Weitere Nachrichten können nach dem gleichen Schema (Header, Key-Value-Paare) spezifiziert und versendet werden.

Nachrichtenziele sind einerseits Einzelziele, welche mit der OID des Endpunkts adressiert werden. Hierbei sind auch Adressen hinter Endpunkten zur gerichteten Kommunikation mit einem Subsystem des Konsumenten, Gateways oder Providers zulässig. Ein Versand von Nachrichten an den Adressaten ist nützlich und muss erlaubt sein. Damit sind Kommunikation von Subsystemen eines Konsumenten und

Redundanzen am Endpunkt realisierbar. Eine Mehrfachinstanziierung des Endpunkts mit gleicher Adresse (und Autorität) ist zulässig.

Nachrichtenziele sind andererseits Gruppenziele, welche mit der OID der Gruppe adressiert werden. Hierbei sind voreingerichtete Gruppenziele (Verteiler), wie auch spontane Gruppen zu fachlichen Ereignissen realisiert.

Endpunkt- und Gruppenadressen können mit einem privaten Alias versorgt werden. Gruppen können zur Laufzeit Änderungen der Adressziele erfahren und vom Eigner gelöscht werden.

3.8.14. Nachrichten empfangen

Die gesendeten Nachrichten müssen von den adressierten Empfängern ausgewertet werden. Lagemodule müssen nur jene Nachrichten auswerten können, welche sie auch betreffen. Bei Empfang einer „unbekannten“ Nachricht kann das Lagemodul mit einer Fehlermeldung antworten.

Ein Beispiel betreffend die derzeit spezifizierten Nachrichten: Die Lagedatenbank ist zur Aufnahme der aktuellen Lage-Statistik bestimmt. Das Lagemodul der Lagedatenbank muss die Nachricht „Statistikinformation“ verarbeiten können, kann aber beim Empfang von „LageInformation“-Nachrichten mit einem Fehlercode antworten.

3.8.15. Administrative Nachrichten

Administrative Nachrichten dienen der Lebenszeichengabe der beteiligten Kommunikationspartner Endpunkt, Access, und der symmetrischen Ermittlung und Darlegung/Dokumentation der fachlichen und technischen Gesundheit der Beteiligten.

Diese Nachrichten können auch eine Nichtbereitschaft angrenzender Systeme signalisieren. Die Lebenszeichen werden direkt von den Endpunkten und Gateways beantwortet. Die Ping-Nachricht dient dazu, (optional) an die Applikation weitergegeben zu werden und von dieser beantwortet zu werden. Damit ist auch eine Überwachung auf Layer 7 gegeben. Falls die Applikation keine Ping-Nachrichten unterstützt, sollte das jeweilige Lagemodul diese beantworten.

Die Ping-Nachricht enthält als Parameter ein Token und Zusatzinformation. Der Token muss zurückgesendet werden, die Antwort kann ebenfalls Zusatzinformation enthalten.

- Lebenszeichen (Nullfunktion) des Endpunktes
- Lebenszeichen (Indikation optional) des entfernten Endpunktes
- Lebenszeichen des Access Gateways zur Plattform

3.9. Übersetzungsdienst (Translational Service)

Übersetzungsdienste sind über spezialisierte Endpunkte nutzbar. Die Übersetzungsdienste sind keine Plattform-integrierten Dienste. Sie werden von Translationsprovidern als klassische Endpunkte abgebildet. Redundanzen dieser Provider werden durch Vertretungsendpunkte realisiert. Im ersten Schritt werden Thesaurus basierte Semantik-Translationen eingeführt, um Normierungen von Begrifflichkeiten über taktische und sprachliche Bedeutungsräume zu erreichen.

3.9.1. Übersetzungsdienst in Anlehnung an EPISECC

Die nachfolgend skizzierte Nachrichtenübersetzung folgt den Ansätzen des EPISECC-Projekts, bringt diese Ansätze jedoch in die Architektur eines förderierbaren Systems, weshalb die Vermeidung von Deadlock-Zuständen zu berücksichtigen ist.

Die Nachrichtenübermittlung wird von der Nachrichtenübersetzung entkoppelt. Diese Entkoppelung zieht die Verantwortung für das Auslösen der Übersetzung an jene Stelle, die die Verantwortung am besten tragen und den „State“ am besten verwalten kann – dem Adapter für die Client-Software, z.B. einem Lageinformationssystem, oder die Client-Software selbst.

3.9.2. Aufgaben des Translational Services

Das Translational Service zur semantischen Übersetzung von übermittelten Nachrichten benötigt folgende Funktionen:

- Semantische Übersetzung einer Originalnachricht oder von Auszügen einer Originalnachricht (ggf. wird durch eine Übersetzung die Validität eines Nachrichtenformats gebrochen)
- Rückübermittlung der übersetzten Nachricht mit Referenz auf das Original zur anfragenden Stelle (unter Beibehaltung aller durch VIDaL angewandten Sicherheitsmechanismen)

Technisch zu berücksichtigende Aspekte:

- Vermeidung von Deadlocks erfordert eine klare Abhängigkeitssteuerung: Die Übersetzung wird durch den Empfänger auf Basis der Originalnachricht unter Nutzung eines spezialisierten und bekannten Translationsproviders asynchron

angefordert, wodurch der empfangende Endpunkt die volle Kontrolle bei der Weiterleitung und Steuerung des Prozesses behält

- Übermittlung der übersetzten Nachricht als auch der Originalnachricht (d.h. Nachvollziehbarkeit der Übersetzungstätigkeit)

Erweiterbare Aufgaben, die später berücksichtigt werden sollten:

- Formatübersetzungen, z.B. EMSI in weitere Formate

Folgende Aspekte sind beim Translational Service sicherzustellen:

- Aktualität der Informationen (Übersetzungstabellen etc.) ist sicherzustellen
- Redundanzen der Translationsservices (z.B. durch Bereitstellung an mehreren Orten in der Nähe von VIDaL-Knoten), um Nicht-Verfügbarkeitszeiten und Abhängigkeiten zu minimieren
- Verschlüsselte geheime Informationen können durch ein Service in der Netzwerkinfrastruktur nicht übersetzt werden, weshalb die Übersetzung von unverschlüsselten Teilinformationen ausgewählt durch den Client empfohlen wird; E2E verschlüsselte Objekte an Nachrichten werden durch die Systeme am Endpunkt eigenverantwortlich behandelt
- Alternativ ist die Replikation oder Caches der Übersetzungsdienstinhalte in den Client zu prüfen, wobei die Synchronisation der Informationen der Thesauri über Hash zu lösen ist.

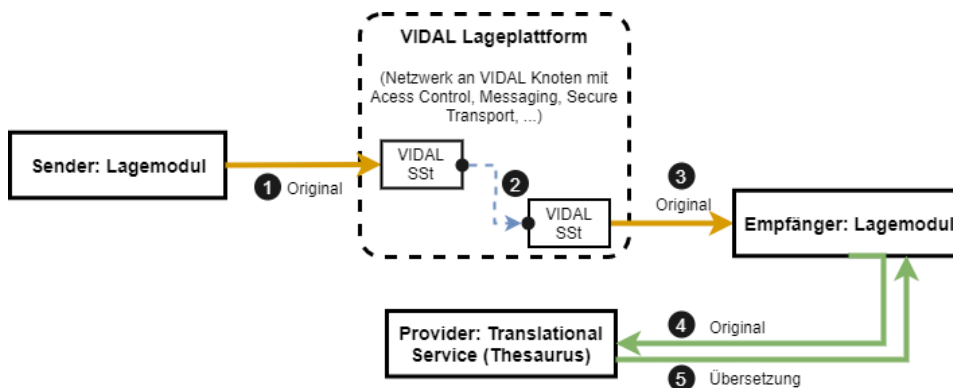


Abbildung 10: Architekturübersicht zu Integration eines semantischen Übersetzungsdienstes in eine förderierbare Gesamtarchitektur

Die Übersetzung folgt dementsprechend folgendem Prozess (Abbildung 10):

1. Übermittlung der Nachricht an einen Translationsendpunkt über den VIDaL-Knoten (primärer Knoten oder derzeit verfügbare Alternative)

2. Innerhalb des VIDaL-Netzwerks an Knoten wird die Nachricht geroutet, verarbeitet, übermittelt zugestellt (über eine VIDaL typische Endpunkt Schnittstelle nach außen)
3. Die Nachricht wird vom Empfänger mit Originalinhalt erhalten und entweder durch den Adapter oder die Client-Software zwischenzeitlich verarbeitet
4. Bei Bedarf wird eine Übersetzung angestoßen und der Status über den Erhalt der Übersetzung verwaltet
5. Die Übersetzung wird von einem „Translational Service“ durchgeführt und über den Adapter an das Lagesystem zugestellt. Sofern keine Übersetzung im Adapter erhalten wird – beziehungsweise sofern seitens des Übersetzungsdienstes eine Fehlermeldung geliefert wird, kann der Adapter oder der Übersetzungsdienst einige Maßnahmen ergreifen:
 - Wiederholung der Übersetzungsanfrage, ggf. unter Abänderung der Anfrageinhalte
 - Weiterleitung der Anfrage durch den Übersetzungsdienst an ein weiteres Übersetzungsservice (z.B. sofern der Übersetzungsdienst überlastet ist), der die Anfrage bearbeitet, und über den ursprünglichen Übersetzungsdienst oder direkt die Antwortnachricht ausfolgt (Empfohlen als Ausbaustufe, da Sicherheitsdetails mit Bedarfsträgern exakt zu erarbeiten sind)
 - Der Übersetzungsdienst meldet dem VIDaL-Adapter einen Knoten / Übersetzungsdienst mit, der die Anfrage bearbeiten kann (z.B. bei Überlastsituationen oder inhaltliche Trennung der Knoten hinsichtlich unterstützter Formate; Empfohlen als Ausbaustufe, da Sicherheitsdetails mit Bedarfsträgern exakt zu erarbeiten sind)

Dieser Vorgang ermöglicht ein förderierbares Vorgehen bei der Nachrichtenzustellung, bildet also jegliches Skalierungsszenario der Zukunft ab, kann dabei jedoch Deadlock-Situationen verhindern, in denen der Empfänger auf Nachrichten wartet, die zu keiner Ausfertigung folgen.

Die Aufgabenteilung folgt im Wesentlichen dem Prinzip moderner Web-Services und Mikroservices:

- Verteilung der Fehlerfälle an exakt jene Stellen, die am einfachsten den State halten können und somit anforderungsspezifisch reagieren können;
- Etablierung einer „Fail early“-Mentalität mit direkten Fehlerbereinigungsinteraktionen (selbstkorrigierende Systematik), die eine möglichst direkte Fehlerrückmeldung zwischen exakt den betroffenen Diensten und den angesprochenen Adaptoren / Client-Lösungen erzeugt.
- Der „Translational Service“ ist als externer Dienst zu etablieren, welcher somit konform eines Endpunktes an der Kante der Plattform agiert. Es können mehrere fachlich spezifische Übersetzungsdienste

existieren. Diese systemische Standardisierung vereinfacht das Kommunikationsmodell, da keine spezifischen Zugangsmethoden etabliert werden müssen.

3.10. Archivierungsservices

Archivierungsservices von Nachrichten zum fachlichen Logging sind spezifische Endpunkte. Diese Provider zum Metadatenlogging und zur Archivierung von Nachrichten sind nicht Teil der Plattform. Diese werden an Orten der rechtlichen Zulässigkeit etabliert, um die Lageplattform von Datenansammlungen freizuhalten.

Im Fachverfahrenskontext wird z.B. IG NRW Lage DB oder der Lagedokumentationsdienst als Provider etabliert. Hierbei werden auch Fach-Funktionen wie das „Late Entry“ realisierbar.

3.11. Nichtfunktionale Anforderungen

3.11.1. Nicht-funktionale Aspekte (Sammlung)

- Separation von Übertragungssicherheitsmaßnahmen und Authentifizierung
- Separieren der Entscheidung über einen Zugriff vom Ort der Zugriffskontrolle
- Die Zugriffskontrolle soll externalisierbar, zentralisierbar und dynamisch verwaltbar sein, basierend auf Userattributen oder rollenbasierten Regeln
- Unterstützung einer Funktionalität zur Einmalanmeldung (SSO) für die Clients
- Unter anderem zum Zwecke einer zentralisierbaren, bzw. Einbindung einer bestehenden Userverwaltung.
- Dezentralisierung und Replikation
- Datensicherheit durch transparente Replizierbarkeit, Austauschbarkeit und einfach realisierbarer Migration verschiedener funktionaler Komponenten
- Ausfallsicherheit durch Dezentralisierung, Replizierung und Skalierbarkeit der Systemkomponenten
- Geo-Verteilung der Hauptverteilerknoten im Applikationsnetz
- Dezentrale Ausführung der Nachrichtenübermittlung bei zentraler Administration und kaskadierender Verwaltung der Zugriffskontrolle
- Orchestrierung/Choreographie der einzelnen Systemkomponenten
- Automatisierter Fallback auf Backup Systemkomponenten
- Weitere Anforderungen:
- Plattform muss zwingend Prioritäten bei der Übermittlung berücksichtigen.
- Lagemodule und Einsatzleitsysteme müssen weiterhin auch autark funktionieren, es darf keine Abhängigkeiten geben.

3.11.2. Sicherheit und Rechteverwaltung

Security:

- Prinzip der mehrstufigen Datensicherheit
 - Transportverschlüsselung im Access und im Backbone
 - Option auf Verschlüsselung des Umschlaginhaltes
 - Option auf Ende zu Ende Verschlüsselung am Objekt (Attributebene)
- Schutzmechanismen gegen unautorisierten Zugriff, insb.
 - Anmeldeprozess: Registrierung, Authentifizierung (Anwendung von Zertifikat)
 - Absicherung gegenüber Zugriffen aus dem Internet (z.B. Firewall)
- Bewusste und datensparsame Verteilung von Daten:

- Verteilung der Daten (Nachrichten) an registrierte und ausgewählte Teilnehmer
- Verteilung der Daten (Nachrichten) nur an adressierte Datenempfänger (d.h. zielgerichtete Kommunikation gemäß Verteilungsintention des Senders)
- Datenhoheit liegt ausschließlich beim Sender
- Keine Datenspeicherung (transiente Verarbeitung der Daten zum Zweck der technischen Zustellung von Nachrichten)

Rechte an Gruppen (Implizite Mitgliedschaften):

- Gruppen im Sinne von Kommunikationsräumen können dauerhaft und temporär eingerichtet, und mit Namen und Zweck gekennzeichnet werden.
- die Einrichtung ist ein verantwortliches Tun des Senders und somit Eigentümers der Gruppe
- das Zurückziehen/Löschen einer Gruppe ist ein optionales Tun des Eigentümers
- Gruppen können quasi statisch (dauerhaft) bestehen und die Aufgabe eines Nachrichtenverteilers annehmen
- es können mehrere Gruppen parallel bestehen
- die Kenntnis über die Gruppe impliziert das Recht der Nutzung dieser
- Einladung der Teilnehmer in eine Benutzergruppe mit Schreib-/Leseberechtigung durch den Eigentümer
- Teilnehmer können Einladungen jederzeit annehmen und widerrufen
- Innerhalb einer Gruppe sind alle eingespeisten Nachrichten für alle Teilnehmer sichtbar

Datenschutz:

- keine persistente Datenspeicherung im System (in den Knoten der Lageplattform); nach erfolgreicher Zustellung oder Timeout werden Daten verworfen, lediglich zwischenzeitlich technisch zum Zweck der Zustellung gespeichert
- Sicherstellung einer Injektion eines Nachrichtentyps spezifischen oder quellendefinierten Parameters für Aufbewahrungsfristen der Nachrichten auf der Plattform (Queuing Time)
- Speicherung von Metadaten (Adressköpfe der Umschläge) in Log-Dateien oder Diensten muss ermöglicht werden
- Speicherung von Daten zur Beweissicherung in Form einer Nachrichtenkopie an einen Dienstleister (als Konsumenten der Plattform / Log Provider) ist sicherzustellen

3.11.3. Verfügbarkeit

Anwendung / Dienste Verfügbarkeit:

Bei den Diensten handelt es sich um sicherheitskritische Anwendungen, welche eine für Leitstellen und Lagezentren übliche Verfügbarkeit von mind. 99,5% benötigen, was beim Design der Systemarchitektur zu berücksichtigen ist.

Redundanzen:

- Geo-Redundanz bei den Plattform-Knoten
- Access zur Plattform ist über einen zweiten Weg möglich (optionaler sekundärer Access)
- Es könne verschiedenste Provider als Endpunkt zu jeglichem Serviceanlass etabliert werden
- Translationsprovider können mehrfach als Endpunkt etabliert werden
- Backbone der Plattform muss tolerant agieren (unbedingte Asynchronität)

3.11.4. Schutzklasse

Bei dem Austausch von Daten zwischen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) handelt es sich in der Regel um sicherheitskritische Daten und sind daher mit Vorsorge zur Sicherung der Daten vor Dritten zu leisten. Daten mit vertraulichem Inhalt müssen einer strikten „Ende-zu-Ende“ Verschlüsselung unterliegen, bevor diese die Plattform betreten. Die Plattform erfährt keine besondere Einstufung bezüglich der Schutzbedürftigkeit.

3.11.5. Zukunftsfähigkeit

Die Zukunftsfähigkeit der Lageplattform VIDaL ist gegeben durch

- Ihre Erweiterbarkeit durch ihr föderales Konzept. Dadurch kann die Plattform bei Bedarf auf andere Bundesländer, Länder oder Organisationen skaliert werden.
- Ihre Erweiterbarkeit der Meldungsklassen. Damit kann der Austausch von zusätzlichen Informationen realisiert werden.

Die kontinuierliche Weiterentwicklung des Systems (Fachlichkeit, Funktionalität) muss durch Verwendung entsprechender Tools und Software sichergestellt sein.

Die Plattform muss alle im Rahmen des Projekts VIDaL definierten Inhalte und zukünftige Erweiterungen „vermitteln“ können.

Idealerweise kann die Lageplattform auch für den Austausch von Einsätzen zwischen Leitstellen genutzt werden.

Weitere Inhalte wie der Austausch von Informationen zu Objekten (KRITIS) sollten ebenfalls abgebildet werden können

- Stadt / Kreis -> Bezirksregierung -> Land

Eine Nachrichtenexpansion (Erweiterung / Änderung) darf keine Implikation auf die Lageplattform haben. Alle Nutznachrichtentypen müssen eine strikte Trennung von Metaobjektbeschreibung und Objekthalt erfahren.

Die Expansion von Teilnehmern (Endpunkte) muss gewährleistet werden.

4 Betrieb der Lageplattform

4.1. Fachlicher Betrieb

Der fachliche Betrieb einer Lageplattform NRW ist verantwortlich für die Administration sämtlicher Systemelemente die für einen ordnungs- und bestimmungsgemäßen Betrieb von Relevanz sind. Aufgrund der Vielzahl unterschiedlicher Nutzergruppen von BOS – und perspektivisch von KRITIS – kommt dem fachlichen Betrieb einer Lageplattform eine hohe Bedeutung zu.

Der fachliche Betrieb umfasst u. a.:

- Domäne-Verwaltung (Option Domäne je Lageplattforminstanz)
- Teilnehmer-Verwaltung (Mandantenorientierung in der Org.-Hierarchie)
- Konfiguration, Rollen, Rechte, Routing-Rules
- Security
- weitere

Betrieb & Service:

- Koordination Erweiterung der Semantik-DB im speziellen durch den Translations-provider (auch Option auf zukünftiges Expertenforum)

Mandanten-Fähigkeit ist erforderlich:

- Städte / Kreise, Bezirksregierungen, Land... Ausbaustufe npol / pol
- Daten von A nach B und von A an Gruppen von Mandanten

Die Mandantenfähigkeit wird im fachlichen Betrieb dadurch unterstützt, dass im Adressierungsschema OID fachlich jeweils sichergestellt wird, dass alle Zweige unterhalb eines mandanten-relevanten OID-Knotens nur an einen dedizierten Mandanten vergeben werden. Damit kann nicht nur eine vollständige OID-Adresse angegeben (Daten von A nach B), sondern auch – mandantenfähig – der gesamte Teilbaum unterhalb des mandanten-relevanten Knotens adressiert werden (Daten von A an Gruppen von Mandanten).

4.2. Technische Betriebsumgebung

Der technische Betrieb der Lageplattform entspricht im Wesentlichen dem eines Standard-IT-Systems. Dies umfasst u. a.:

- Verfügbarkeit eines Test- & Referenzsystems für
 - o Test neuer Programmstände
 - o Nachbildung von Fehlerzuständen
 - o Testumgebung für neue Benutzer der Plattform (Clients)
- Verfügbarkeit eines Helpdesk 24/7 für
 - o fachlichen Betrieb (Betreuung neuer Anwender)

- o technischen Betrieb (Wartung)
- Betrieb gem. ITIL

Für Betrieb & Service der Plattform sind folgende Eigenschaften der Plattform unabdingbar:

- Unterstützung eines Rechenzentrums-Betriebs / Betriebs in einer Cloud Umgebung
- Skalierbarkeit im laufenden Betrieb
- Software-Aktualisierung im laufenden Betrieb ohne Systemstillstand

5 Abkürzungsverzeichnis / Glossar

Abkürzung	Erläuterung
AG	Arbeitsgruppe
AAO	Allgemeine Aufbau-Organisation
API	Application Programming Interface, Programmierschnittstelle
BAO	Besondere Aufbau-Organisation
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
CAP	Common Alerting Protocol
CIS	Common Information Space
CRL	Certificate Revocation List
E2E	Ende-zu-Ende
EDXL	Emergency Data Exchange Language
EFUL	Expertengruppe für universelle Leitstellenschnittstelle
EMSI	Emergency Management Shared Information
Envelope	Umschlag der Nachricht, der Metainformationen enthält
EPISECC	Establish a Pan-European Information Space to Enhance seCurity of Citizens
GDI NRW	Geodateninfrastruktur Nordrhein-Westfalen
HTTPS	Hypertext Transfer Protocol Secure
IG NRW	Informationssystem Gefahrenabwehr Nordrhein-Westfalen
IP	Internet Protocol
Konsument	System bzw. Software das an die Lageplattform VIDaL angebunden ist
KRITIS	Kritische Infrastrukturen
Lage DB	Alias für eine externe Applikation zur Speicherung der Lage Daten
Lagemodul	Software zur Anbindung eines Systems an die Lageplattform VIDaL
Lagesystem	System bzw. Software für Krisenstäbe zur Dokumentation und Bewältigung von Lagen und Großeinsätzen
MLP	Mobile Location Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier

P2P	Peer-To-Peer
Payload	Inhalt einer Nachricht
PSH	Public Safety Hub
Queueing	Warteschlangentechnik
REST	Representational State Transfer (Programmierparadigma)
RPC	Remote Procedure Call
SOAP	Simple Object Access Protocol
SSO	SingleSignOn
Tag	Markierung einer Nachricht zur Zuordnung zu einem Thema
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
VIDaL	Vernetzung von Informationen zur Darstellung der Landeslage
WSDL	Web Services Description Language