

Whitepaper

Funktionen und Leistungen deegree Enterprise Edition

© grit - graphische Informationstechnik Beratungsgesellschaft mbH
© lat / lon Gesellschaft für raumbezogene Informationssysteme mbH

Der Inhalt dieses Dokuments darf ohne vorherige schriftliche Erlaubnis nicht reproduziert oder veröffentlicht werden,
auch nicht in Teilen oder Auszügen.

Inhalt

1	Motivation.....	3
2	deegree Enterprise Edition: Management Summary	4
3	deegree Enterprise Edition: Architektur	4
4	Geodienste	6
4.1	Geodienste der deegree Enterprise Edition	6
4.2	Geodienste aus Räumlichen Datenbanken.....	7
4.3	High Resolution Plot Service	7
4.4	Ergänzende Hinweise zum WMTS	7
5	INSPIRE Services	8
6	Administrationswerkzeuge, Nutzerverwaltung, Zugriffsbeschränkungen	10
6.1	Allgemeines.....	10
6.2	OGC Service Management	11
6.3	Nutzer- und Rechteverwaltung.....	12
6.4	Zugriffsbeschränkungen.....	13
6.4.1	Sicherheitsstandards für die Absicherung von Geodiensten	13
6.4.2	Absicherung der Geodienste.....	14
6.4.3	Einbindung in GIS-Clients	14
6.5	SDI Defender	14
6.6	Upload, Update & ETL.....	14
6.7	Accounting	15
6.8	Monitoring	15
7	xPlanBox.....	16

Aufbau von Geodateninfrastrukturen mit der deegree Enterprise Edition

1 Motivation

Die Konzentration von Fachverfahren in Rechenzentren ist heute beherrschender Trend. Neben der Optimierung von Kosten soll insbesondere die Sicherheit und Verfügbarkeit der Fachverfahren erhöht werden.

Geodateninfrastrukturen machen hier Probleme. Sie fallen aus dem üblichen Rahmen: Sie sind komplex und nutzen eine Vielzahl gegenseitig abhängiger Komponenten. Für ihren Betrieb ist fachspezifisches Wissen erforderlich.

Bislang war das unkritisch, da die Geofachleute ihre IT-Infrastrukturen selbst betrieben haben. Doch mit der Migration ins Rechenzentrum ist das nicht mehr so einfach. In einem Rechenzentrumsbetrieb müssen die unterschiedlichen operativen Ebenen Fachadministration und Systemadministration strikt getrennt werden. Dabei zeigt sich, dass die Architektur von Geodateninfrastrukturen darauf nicht ausgerichtet ist. Die Verschränkung der Aufgaben von Systemverwaltung und Geofachleuten ist oft so erheblich, dass ein reibungsloser Betrieb nicht möglich ist und der Betrieb der Geodateninfrastruktur den Geofachleuten überlassen wird, außerhalb der Rechenzentrums-Strukturen und mit entsprechenden Konsequenzen, z. B. was die Kosten und die Sicherheit der IT-Umgebung angeht.

Ein weiteres Problem ist die eingesetzte Software. Für die Einrichtung von Geodateninfrastrukturen haben sich eine Reihe von Open Source Produkten als Standard manifestiert. Gerade was die IT-Sicherheit angeht, hat Open Source zwar grundsätzlich einen guten Ruf, aber der kommt nur dann zum Tragen, wenn die Software entsprechend gepflegt wird. Die nachhaltige und geordnete Pflege der Software, z.B. wenn es darum geht, neue Datenbankversionen oder Laufzeitumgebungen zu unterstützen, ist jedoch bei Open Source Projekten oft ein großes Problem. Ähnliches gilt beim Komplex „Long Term Support“ – der ist oft nicht vorhanden.

Aus gutem Grund erlauben die Sicherheitsrichtlinien der Rechenzentren ausschließlich den Einsatz professionell unterstützter Software. Mit der Bereitstellung neuer Softwarestände ist es betriebsseitig aber nicht getan. Sie müssen auch installiert und - um die Verfügbarkeit der Geodateninfrastruktur nicht zu gefährden - ausreichend getestet werden. Der Aufwand für einen sicheren Betrieb sollte also nicht unterschätzt werden. Ein professioneller Supportvertrag ist also unabdingbar, jedoch nicht immer verfügbar.

Die deegree Enterprise Edition genügt diesen Anforderungen.

2 deegree Enterprise Edition: Management Summary

Geodateninfrastrukturen (GDI) sind dafür gemacht, Geofachdaten einem breiten Anwenderkreis zur Verfügung zu stellen. Verteilt liegende Daten sollen interoperabel über standardisierte Geodaten-dienste verfügbar gemacht werden.

deegree ist *das* Open Source Framework für die Bereitstellung OGC-konformer Geodatendienste. deegree ist bekannt für die Konformität zu den Standards des Open Geospatial Consortiums (OGC) und wird von einer Vielzahl von Nutzern in ganz Europa eingesetzt.

Die deegree Enterprise Edition ist die Produktversion von deegree. Sie verfügt über eine definierte Betriebsumgebung, ist getestet und Ready-to-Use. Im Zuge der Weiterentwicklung der Software werden Fehlerkorrekturen, Updates und Upgrades bereitgestellt. Sie verfügt über umfangreiche funktionale Erweiterungen, die vor allem für den professionellen Einsatz im Rechenzentrum entworfen wurden. Diese betreffen die Administration der Dienste, Zugriffskontrolle und Nutzerverwaltung sowie die Absicherung der Geodaten-Dienste (WMS, WFS), das Monitoring der Systemverfügbarkeit und der Schutz vor Missbrauch. Darüber hinaus enthält sie weitere Werkzeuge, z. B. Accounting, Plot Service etc.

Nicht zuletzt werden für die deegree Enterprise Edition Professional Services angeboten. Diese umfassen Installation, Konfiguration, Störungsbeseitigung und ETL-Dienstleistungen. Für diese Leistungen stehen konkrete, vertraglich verpflichtete Ansprechpartner zur Verfügung, die dafür sorgen, dass die korrekte Funktionalität der Software langfristig gewährleistet ist.

deegree Enterprise Edition enthält einen vollständigen INSPIRE-Stack. Die Software ist imstande, die von der INSPIRE-Richtlinie geforderte Zuverlässigkeit und Performance zu liefern. Das ist möglich, weil die Software-Architektur auf einen Rechenzentrumsbetrieb hin ausgerichtet ist und alle Komponenten aufeinander abgestimmt sind und fehlerfrei zusammenarbeiten. deegree Enterprise Edition wird umfangreich getestet, um einen fehlerfreien Betrieb zu garantieren.

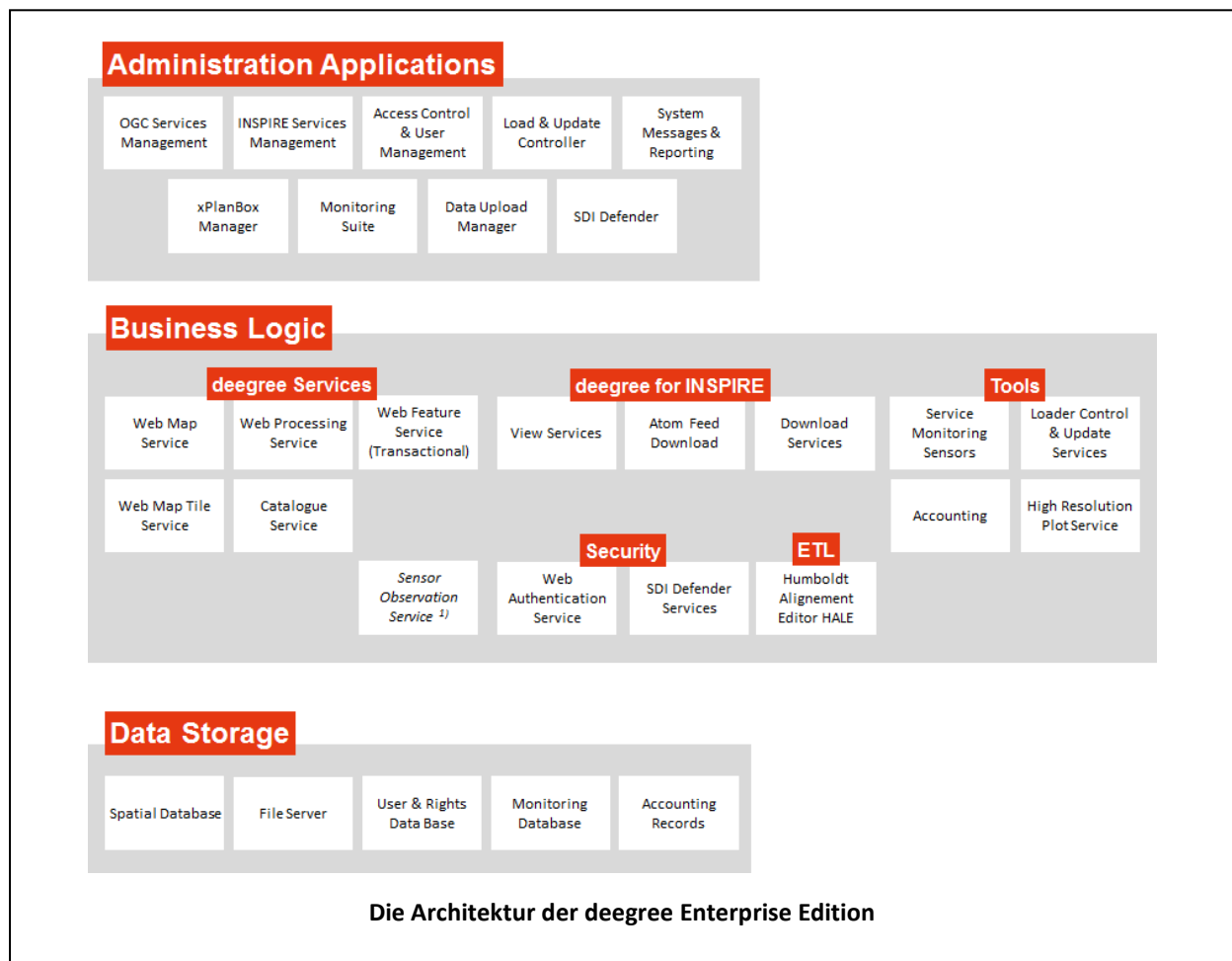
Die deegree Enterprise Edition wird durch das deegree Konsortium entwickelt. Weitere Informationen zur deegree Enterprise Edition finden sich auf www.deegree-enterprise.de.

3 deegree Enterprise Edition: Architektur

Die deegree Enterprise Edition hat eine 3-Schicht-Architektur, in der die einzelnen Schichten logisch voneinander getrennt und somit gut skalierbar sind. Diese moderne Systemarchitektur wird standardmäßig für den Aufbau von Geodateninfrastrukturen verwendet. Sie trägt wesentlich zur Systemstabilität und Systemverfügbarkeit bei und ist für die Umsetzung der INSPIRE-Anforderung unabdingbar.

Die 3 Schichten und ihre Komponenten sind in der Abbildung dargestellt:

1. Administration Applications: Um die Dienste und Funktionen der deegree Enterprise Edition steuern und verwalten zu können, enthält das Framework webbasierte Administrationswerkzeuge. Diese befinden sich in dieser Schicht.
2. Business Logic: Alle funktionalen Komponenten des Systems sind als Services verfügbar. Hier liegen die deegree Services, die INSPIRE-Dienste und weitere System- und Verwaltungsdienste.
3. Data Storage: Diese Schicht enthält alle Daten der Geodateninfrastruktur. Geodaten im Vektorformat werden wahlweise in den räumlichen Datenbanksystemen PostgreSQL / PostGIS oder Oracle / Oracle-Spatial gespeichert. Geodaten in Rasterformaten werden im Dateisystem oder in den räumlichen Datenbanksystemen gespeichert. Dies gilt auch für die vorkonfektionierten Datensätze, die für die INSPIRE-Downloaddienste bereitgestellt werden müssen. Der Data Storage enthält weiterhin alle Daten der Verwaltungskomponenten, wie zum Beispiel der Nutzerverwaltung, des Monitorings und des Accountings.



4 Geodienste

4.1 Geodienste der deegree Enterprise Edition

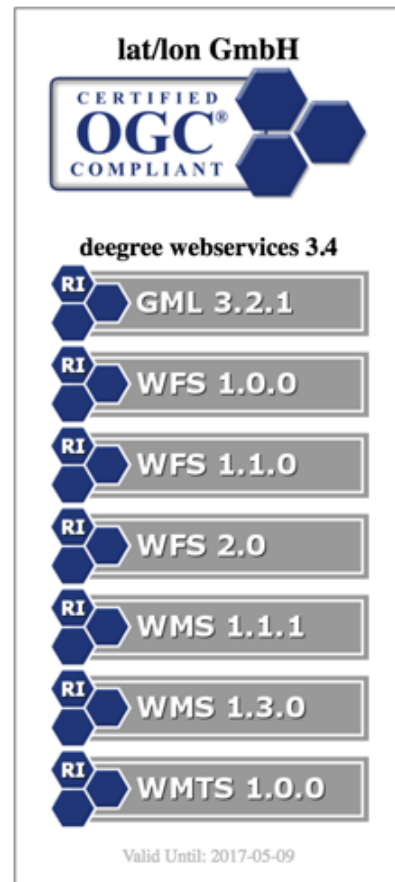
Zentrale Bedingung für die Nutzbarkeit von Geodiensten ist die Einhaltung von Standards und Implementierungsspezifikationen. Die Standards des Open Geospatial Consortiums (OGC) sind hier das Maß der Dinge. OGC definiert einen weiten Bereich von Standards, zentrale Bedeutung kommt allerdings den Darstellungs- und Downloaddiensten zu.

Die Services der deegree Enterprise Edition stellen die umfangreichste Implementierung der OGC Standards im Open Source Sektor dar. Diese sind offizielle Referenzimplementierung des OGC für die Darstellungs- und Download-Dienste WMS 1.3.0 und WFS 2.0, weiterhin Referenzimplementierung für die Standards GML 3.2.1, WFS 1.0.0, WFS 1.1.0, WMS 1.1.1 und seit September 2016 auch für WMTS 1.0.0.

Referenzimplementierungen sind dadurch gekennzeichnet, dass sie funktional vollständig sind, mit der OGC CITE¹ Testsuite erfolgreich überprüft wurden und eine entsprechende Instanz der Software öffentlich zur Verfügung steht. Offizielle OGC Referenzimplementierungen dürfen mit dem Zertifikat "Certified OGC Compliant" gekennzeichnet werden.

Auch die weiteren Dienste der deegree Enterprise Edition sind OGC-konform. So bietet deegree Implementierungen des Filter Encoding Standards in den Versionen 1.1.0 und 2.0, Styled Layer Descriptor 1.1.0 und Symbology Encoding 1.1.0 sowie für die Dienstschnittstellen CSW 2.0.2 und WPS 1.0.0. Damit ist die Erweiterung einer auf deegree Enterprise Edition basierenden Geodateninfrastruktur um weitere Komponenten auf der Basis von OGC Standards gesichert.

Dieses im Open Source Umfeld einzigartige Setup von Implementierungen der Standards des OGC ist besonders geeignet zur Umsetzung konformer Dienste im Rahmen der Europäischen Geodateninfrastruktur INSPIRE. Deren Richtlinien sehen die Erfüllung der Anforderungen genau derjenigen OGC Standards vor, für die deegree die Referenzimplementierung ist, also GML 3.2.1, WFS 2.0 und WMS 1.3.0 sowie WMTS 1.0.0.



¹ Compliance, Interoperability, Testing & Evaluation Program
<http://cite.opengeospatial.org/teamengine/>

Als ergänzende Maßnahme wird die Konformität der Dienste auch gegen die GDI-DE Testsuite² überprüft. Durch diese Maßnahme wird eine besonders hohe funktionale Qualität der Geodienste gewährleistet, weil die Überprüfung mittels zweier unterschiedlicher Qualitätssicherungswerkzeuge dazu führt, dass etwaige Fehlinterpretationen der implementierten Tests direkt erkannt werden können.

4.2 Geodienste aus Räumlichen Datenbanken

Räumliche Datenbanken spielen im Umfeld von Geodateninfrastrukturen eine wichtige Rolle, da diese als Datenhaltungsschicht essentiell zur Performanz und Skalierbarkeit der darauf aufsetzenden Geodienste beitragen. Daher ist die Unterstützung solcher Geodatenbanken als Datenhaltungsschicht für die Umsetzung von standardisierten Geodienstschnittstellen bei der Umsetzung einer GDI unumgänglich.

Im Umfeld der Lösungen von Geodatenbanken sind insbesondere drei Softwarepakete zu beachten. Das Open Source Segment wird durch PostgreSQL/PostGIS abgedeckt. Darüber hinaus ist Oracle mit Locator/Spatial das am weitesten verbreitete Datenbanksystem im Bereich der räumlichen Datenbanken. deegree Enterprise Edition kann mit beiden Datenbanksystemen umgehen. Speziell für PostgreSQL/PostGIS und Oracle Locator bietet deegree verschiedene Strategien zur Datenhaltung an. Zum einen können Geoobjekte (= Features) vollständig relational zerlegt in der Datenbank abgelegt werden. Zum anderen ist es möglich, mittels des sogenannten BLOB-Stores eine besonders auf Performanz optimierte Datenhaltung aufzubauen. Darüber hinaus bietet der sogenannte SimpleSQLFeatureStore die Möglichkeit, die Datenhaltung bezüglich ihres Detailgrads für verschiedene Levels of Detail zu gestalten.

4.3 High Resolution Plot Service

deegree Enterprise Edition enthält einen Plot-Service, mit dem hochauflösende und großformatige PDF-Zeichnungen von jedem OGC-konformen Kartendienst erstellt werden können. Der Dienst kann von jedem Klienten, der die Dienste-Schnittstelle implementiert, angesprochen werden.

4.4 Ergänzende Hinweise zum WMTS

Der WMTS ist als OGC-konformer Dienst des Typs Tiling Service implementiert. Er bietet folgende Möglichkeiten zur Performanceoptimierung:

1. deegree Caching-TileStores: deegree verwendet für das Caching das Open Source Framework Ehcache. Bereits angezeigte Bildkacheln werden deshalb direkt aus dem Speicher nachgeladen, wodurch ein erheblicher Geschwindigkeitszuwachs erzielt werden kann.
2. deegree TileStores: Sie bieten die Möglichkeit, Rasterdaten als Bildpyramiden zu speichern und den Zugriff auf die Bildpyramiden-Ebenen massiv zu beschleunigen. deegree Enterprise Edition

² <http://testsuite.gdi-de.org/gdi/>

hat die Fähigkeiten, auf Bildpyramiden zuzugreifen und enthält Werkzeuge, um diese zu erzeugen.

Der Einsatz der deegree Enterprise Edition gewährleistet insgesamt eine höchstmögliche Konformität zu den geforderten Standards von OGC und INSPIRE.

5 INSPIRE Services

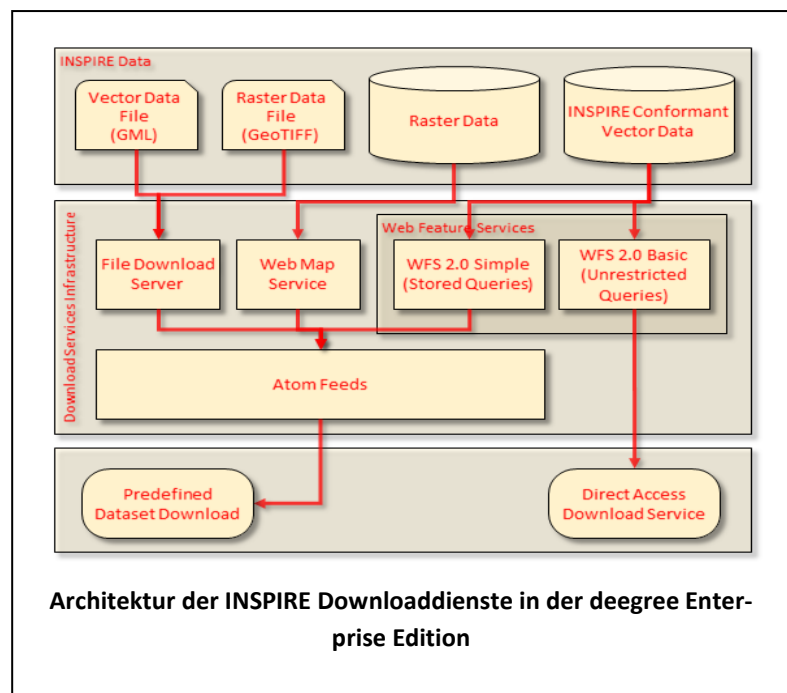
Die deegree Enterprise Edition enthält einen vollständigen INSPIRE Stack zur Bereitstellung von Geodiensten und zur Veröffentlichung von Daten. Die Systemarchitektur und technische Infrastruktur von deegree Enterprise Edition ist so konzipiert, dass die von INSPIRE geforderten Qualitätsmerkmale in Bezug auf Leistung, Kapazität und Verfügbarkeit erreicht werden.

Alle Themen, die im Anhang I bis III der INSPIRE-Richtlinie (2007/2/EG) aufgeführt sind, können mit der deegree Enterprise Edition als INSPIRE Downloaddienste bereitgestellt werden:

1. Einfacher Downloaddienst (Predefined Dataset Download): Bei einem einfachen Downloaddienst können Datensätze im Ganzen heruntergeladen werden.
2. Direktzugriffs-Downloaddienst (Direct Access Download Service): Bei einem Direktzugriffs-Downloaddienst kann selektiv auf die Daten zugegriffen werden.

Die zum Download bereitgestellten INSPIRE Daten haben Vektor- oder Rasterformat und liegen entweder als ein Satz von Dateien vor oder werden in räumlichen Datenbanken gespeichert.

Alle im Vektor-Format vorliegenden Daten müssen INSPIRE-konforme Strukturen aufweisen³. Das gilt sowohl für die im Dateiformat vorliegenden Daten als auch für



³ Die für INSPIRE relevanten Datensätze werden in aller Regel nicht in INSPIRE-konformen Datenmodellen gehalten und fortgeführt. Sie sind deswegen vor jeder Bereitstellung in ein INSPIRE-konformes Format zu überführen. Die deegree Enterprise Edition enthält die für diesen Prozess benötigten Programme.

die in einer räumlichen Datenbank gespeicherten Daten. Innerhalb der Downloaddienste findet keine Transformation statt.

Um den Zugang zu den Daten zu vereinheitlichen, wurde in der deegree Enterprise Edition die in der Abbildung dargestellte Architektur realisiert. Ihr wesentliches Merkmal ist die Realisierung der einfachen Downloaddienste über Atom Feeds und der Direktzugriffs-Downloaddienste über einen Web Feature Service in der Version 2.0.

1. Einfacher Downloaddienst mit Atom-Feeds

Das Atom-Syndication Format ist ein XML-Format, das den plattformunabhängigen Austausch von Informationen erlaubt, zum Beispiel für Web-Feeds. Ein Atom Feed enthält sowohl die Metadaten zu den INSPIRE-Daten als auch einen Downloadlink. Dieser Link verweist entweder auf eine Datei mit INSPIRE-Datensätzen oder er enthält eine vorgefertigte Anfrage an einen OGC-kompatiblen WMS oder WFS. In beiden Fällen hat der Anfragende keinen Einfluss auf Größe und Inhalt des Datensatzes. Die Aufteilung der INSPIRE-Daten in einzelne Datensätze wird durch den Bereitsteller der Daten durchgeführt. Für die Erstellung der Atom-Feeds steht dem Fachadministrator eine Web-Anwendung zur Verfügung. Mit dieser Web-Anwendung ist eine teilautomatische "Daten-Dienste-Kopplung" über die UUID des Datensatzes des Catalog Service for Web (CSW) möglich.

2. Direktzugriffs-Downloaddienst mit WFS 2.0

Hier werden die INSPIRE-Daten über einen Web Feature Service bereitgestellt. Alle im WFS 2.0 Standard verfügbaren Anfrage- bzw. Selektionsmethoden stehen zur Verfügung, so dass aus den bereitgestellten Daten gezielt diejenigen herausgefiltert werden können, die von besonderem Interesse sind (Direct Access Download Service). Darüber hinaus bietet die deegree Enterprise Edition auch die Möglichkeit, die WFS 2.0 Schnittstelle zur Bereitstellung einfacher Downloaddienste zu nutzen (Pre-defined Dataset Download Service).

Sowohl bei den auf Atom-Feed als auch auf WFS-2.0-basierten Downloaddiensten müssen die Metadaten der jeweiligen Datenbestände mit bereitgestellt werden. Die deegree Enterprise Edition verfügt über Methoden, mit denen die im Metadaten-Informationssystem gehaltenen Informationen in die Atom Feeds bzw. die Rückgabewerte der GetCapabilities-Anfrage eingebettet werden können.

Wie die anderen Dienste können auch die INSPIRE-Downloaddienste durch die Sicherheitsfunktionen der deegree Enterprise Edition in Bezug auf die Zugangsrechte kontrolliert und überwacht werden.

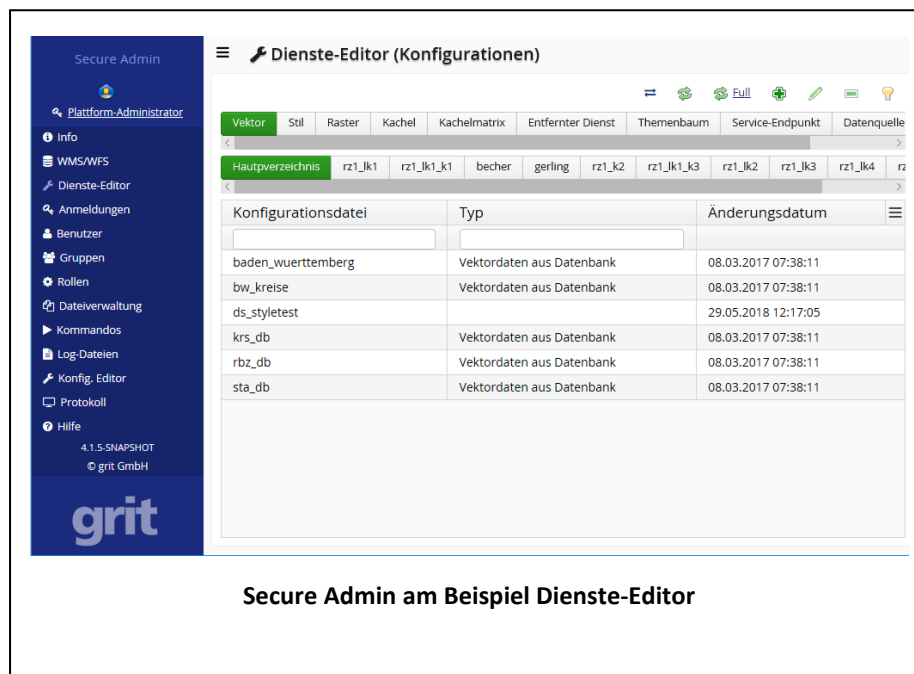
Die Systemarchitektur und technische Infrastruktur ist so konzipiert, dass die von INSPIRE geforderten Qualitätsmerkmale in Bezug auf Leistung, Kapazität und Verfügbarkeit erreicht werden.

6 Administrationswerkzeuge, Nutzerverwaltung, Zugriffsbeschränkungen

6.1 Allgemeines

Die Verwaltungsoberflächen der deegree Enterprise Edition sind der Schlüssel zum Rechenzentrumsbetrieb, weil mit ihrer Hilfe Zugang zu Bereichen und Funktionen gewonnen werden kann, zu denen ansonsten nur die Systemverwaltung Zugriffsrechte hätte.

Die Administration der deegree Enterprise Edition erfolgt über ein integriertes Paket von Web-Anwendungen. Die Webanwendungen sind mandantenfähig und können so konfiguriert werden, dass hierarchische Zugriffsrechte abgebildet werden.



Der Secure Admin stellt eine graphische Benutzeroberfläche für die Bearbeitung der deegree Konfiguration bereit. Dadurch ist die Konfiguration ohne Bearbeitung von XML-Dateien möglich. Ebenfalls ist eine Bearbeitung von SE-Darstellungsregeln mit dem Secure Admin über eine graphische Benutzeroberfläche möglich.

6.2 OGC Service Management

Die Geodienste der deegree Enterprise Edition werden über die Webanwendung „OGC Service Management“ verwaltet. Die Oberfläche ermöglicht es einem Administrator, die deegree Geodienste und Datenquellen wie z. B. WFS, WMS, WMTS oder CSW zu konfigurieren und während des Betriebs zu administrieren. Dabei wird ein einheitliches Konfigurationskonzept für deegree Geodienste eingesetzt, das eine Trennung von Diensten und Datenquellen vorsieht. Das folgende Schaubild zeigt das am Beispiel des WMS und des WFS. Ihre Konfiguration ist unabhängig von der Art, wie die Features im Feature Store gespeichert sind.

Die initiale Konfiguration der Geodienste erfolgt in der Regel prozessgesteuert während der Übernahme von neuen Geodaten in die Datenbank. Die Administrationswerkzeuge erzeugen eine neue Dienstkonfiguration und binden diese automatisch in die Laufzeitumgebung ein.

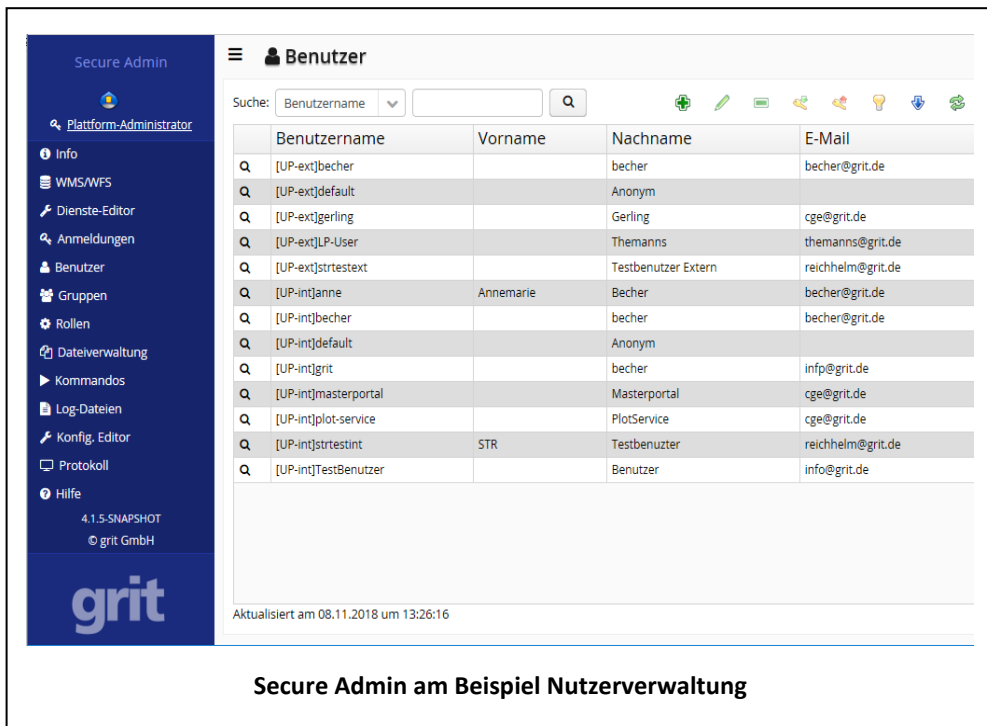
Eine nachträgliche Anpassung der Eigenschaften der Geodienste ist ebenfalls möglich. Dabei kann der Fachadministrator sowohl die Dienste als auch die Datenquellen konfigurieren.

Sofern die Daten über den „Data Upload Manager“ eingespielt werden, erfolgt dies in der Regel prozessgesteuert während der Übernahme der neuen Geodaten in die Datenbank.

6.3 Nutzer- und Rechteverwaltung

Damit das System vor unberechtigtem Zugriff geschützt werden kann, muss es wissen, wer Zugriff verlangt. Deshalb müssen sich die Anwender zunächst authentifizieren. Ihnen werden dann die in ihrem Nutzerprofil eingetragenen Rechte zugewiesen (Autorisierung).

Die deegree Enterprise Edition enthält eine webbasierte Nutzer- und Rechteverwaltung (Access Control & User Management). Diese ist Bestandteil der Komponente „Secure Admin“. Die Rechte der Anwender werden durch Fachadministratoren



Benutzername	Vorname	Nachname	E-Mail
[UP-ext]becher		becher	becher@grit.de
[UP-ext]default		Anonym	
[UP-ext]gerling		Gerling	cge@grit.de
[UP-ext]LP-User		Themanns	themanns@grit.de
[UP-ext]strtestext		Testbenutzer Extern	reichhelm@grit.de
[UP-int]Janne	Annemarie	Becher	becher@grit.de
[UP-int]becher		becher	becher@grit.de
[UP-int]default		Anonym	
[UP-int]grit		becher	inf@grit.de
[UP-int]masterportal		Masterportal	cge@grit.de
[UP-int]plot-service		PlotService	cge@grit.de
[UP-int]strtestint	STR	Testbenutzer	reichhelm@grit.de
[UP-int]TestBenutzer		Benutzer	info@grit.de

Aktualisiert am 08.11.2018 um 13:26:16

Secure Admin am Beispiel Nutzerverwaltung

verwaltet, die Anwender selbst haben keinen Zugriff.

Die Benutzerverwaltung sieht vor, dass jeder Benutzer einer Benutzergruppe zugewiesen wird. Es ist möglich, mehrere Benutzergruppen zu einer weiteren Gruppe zusammenzufügen, sodass ein rekursives Datenmodell umgesetzt werden kann.

Die Benutzer können entweder manuell eingegeben oder durch Anschluss an ein bereits bestehendes Benutzerverzeichnis übernommen werden. Schnittstellen bestehen zu Microsoft Active Directory und Oracle OID.

Den Benutzern und Benutzergruppen stehen auf der Datenseite sog. Rollen gegenüber. In einer Rolle werden Geodienste (WMS, WFS) und Bestandteile dieser Geodienste (Layer, FeatureTypes) zusammengefasst.

Den Benutzergruppen werden über die Benutzeroberfläche Rollen zugewiesen – sie haben dann Zugriff auf die in den Rollen konfigurierten Daten.

Die Nutzerverwaltung enthält noch einen weiteren Funktionsbereich, mit dem die Konfigurationsdateien in der Produktionsumgebung geändert werden können. Dies ist notwendig, da Fachadministratoren aus Sicherheitsgründen im Produktionsbereich keinen Zugang zum Dateisystem des Servers haben. Die Benutzerverwaltung hingegen ist gegenüber dem Produktionsserver authentifiziert und darf bestimmte Dateiverzeichnisse lesen und die dort befindlichen Dateien, die Konfigurationsdateien der Geodienste, ändern. Sie ist weiterhin dazu berechtigt, spezifische Geodienste zu stoppen und neu zu starten, sodass die Änderungen in den Konfigurationsdateien auch tatsächlich in diesen Diensten sichtbar werden. Über Backup-Funktionen ist es möglich, alte Konfigurationsdateien zu rekonstruieren und den ursprünglichen Zustand wiederherzustellen.

Die Nutzerverwaltung ist mandantenfähig: Jedem Administrator werden nur die Funktionen und Konfigurationsdateien zugewiesen, die ihm zustehen. Sie kennt zwei Berechtigungsstufen für Administratoren:

1. Der Hauptadministrator hat Zugriff auf alle Funktionen der Nutzerverwaltung und Konfigurationsdaten.
2. Der Fachadministrator erhält nur einen für seinen Anwendungsfall passenden Funktionsumfang und darf auch nur seine eigenen Konfigurationsdaten anpassen. Einem Fachadministrator werden zum Beispiel nur die Daten einer „Datenverantwortlichen Stelle“ zugewiesen, etwa die Daten eines Landkreises oder einer Kommune.

Sollte ein Administrator in der Weboberfläche Funktionalitäten oder Konfigurationsdateien nicht angeboten bekommen, so liegt dies an der Mandantensteuerung und den entsprechend gesetzten Berechtigungen.

6.4 Zugriffsbeschränkungen

6.4.1 Sicherheitsstandards für die Absicherung von Geodiensten

Um die Geodienste vor unberechtigtem Zugriff zu schützen, enthält die deegree Enterprise-basierte Lösung einen Web Authentication Service (WAS). Der Web Authentication Service greift auf die in der Nutzerverwaltung verwalteten Rechte zurück und sorgt dafür, dass einem Anwender nur die für ihn vorgesehenen Ressourcen freigeschaltet werden.

Es ist jedoch anzumerken, dass zurzeit kein gültiger OGC Standard für die Absicherung von Geodiensten existiert. Die in deegree Enterprise Edition enthaltene Lösung lehnt sich deshalb an die im Architekturkonzept der GDI-DE beschriebene Lösung an. Diese benutzt die Secure Assertion Markup Language (SAML) des Organization for the Advancement of Structured Information Standards Konsortiums (OASIS) und das Basic Services Model des OGC. Der Web Authentication Service ermöglicht die Authentifizierung und Autorisierung von Clients sowie den Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen unterschiedlichen OGC-konformen Diensten. Die deegree Enterprise Edition unterstützt die von der GDI-DE beschriebenen Standards zur Absicherung von Geodiensten.

6.4.2 Absicherung der Geodienste

Die Module der deegree Enterprise Edition für die Zugriffskontrolle ermöglichen die Absicherung von Geodiensten auf der Ebene von Diensten, Operationen und Daten. So können Benutzer über das Rechtemanagement eingeschränkten Zugriff auf spezifische Operationen eines Geodienstes oder auf Daten erhalten.

6.4.3 Einbindung in GIS-Clients

Um gesicherte Geodienste in anderen GIS-Clients nutzen zu können, steht dem Nutzer ein Werkzeug zur Einbindung von abgesicherten Geodiensten zur Verfügung. Mit diesem Werkzeug ist es auch für GIS-Clients möglich, welche nicht über die Möglichkeit der Eingabe von Benutzernamen und Benutzererkennung verfügen, die abgesicherten Geodienste zu nutzen. Dazu werden etablierte Verfahren für die Authentifizierung über HTTP Anfragen genutzt.

Die Nutzerverwaltung der deegree Enterprise Edition verfügt über ein umfassendes Rollen- und Rechte-Management, mit dem die Berechtigungen für die Geodienste verwaltet werden.

6.5 SDI Defender

Diese Funktion schützt die Geodateninfrastruktur vor Missbrauch. Alle Zugriffe auf die Geodateninfrastruktur werden über die sog. SDI Defender Fassade geleitet und von ihr analysiert. Wird ein Missbrauch, beispielsweise ein hochfrequenter Zugriff durch einen Bot beobachtet, wird der weitere Zugriff des Nutzers auf die GDI verhindert. Die betreffende IP-Adresse wird protokolliert, der Nutzer wird auf die missbräuchliche Nutzung hingewiesen und die Sperrung wird dem Administrator mitgeteilt. Für die Konfiguration und die Auswertung der missbräuchlichen Zugriffe hat SDI Defender eine eigene, webbasierte Oberfläche.

6.6 Upload, Update & ETL

deegree Enterprise Edition verfügt über Funktionalitäten, mit denen Geodaten in die GDI hochgeladen, transformiert und publiziert werden können. Über eine Web Applikation kann der Anwender seine Geodaten zunächst in ein Postfach der GDI hochladen. Sofern erforderlich, werden die Daten anschließend transformiert, in die GDI hochgeladen und für die Publikation bereitgestellt. Nach Kontrolle der Richtigkeit erfolgt die Publikation der Daten durch einen Fachadministrator. Die Applikation ist mandantenfähig, die Postfächer sind durch die zentrale Nutzerverwaltung abgesichert.

Die deegree Enterprise Edition selbst enthält keine Werkzeuge für die Transformation von Geodaten, beispielsweise in die INSPIRE Datenmodelle (ETL-Prozess). Für diese Aufgabe sieht deegree Enterprise Edition eine enge Kopplung mit dem Humboldt Alignment Editor (HALE)⁴ vor.

⁴ HALE ist Open Source Software und unter der LGPL 3.0 lizenziert. <https://www.igd.fraunhofer.de/Institut/Abteilungen/GEO/Projekte/HALE-HUMBOLDT-Alignment-Editor>
<http://www.esdi-community.eu/projects/hale>

HALE ist generisch aufgebaut und verarbeitet diverse Datenformate, deren individuelle Datenstrukturen über Transformationsregeln erfasst werden. Der Ablauf der Upload/Update-Prozesse ist damit für alle Datentypen gleich.

HALE kann folgende Datenformate importieren: Shapefile (SHP), XML Schema, GML Application Schema, CSV, XML, GML, CityGML, Database, SQLite and Spatialite, XLS.

6.7 Accounting

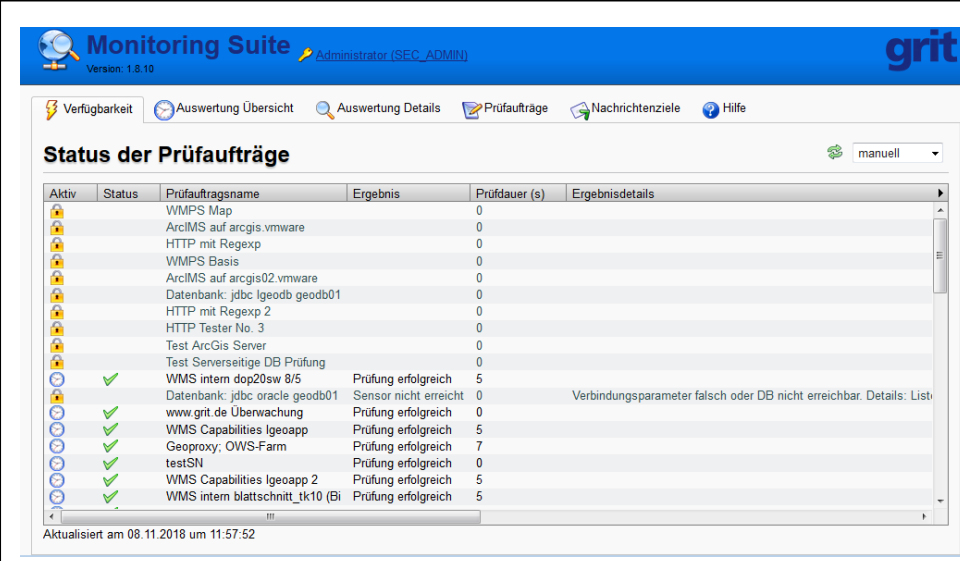
Alle datenbezogenen Aktivitäten des Gesamtsystems werden protokolliert und in einer Datenbank gespeichert. Über eine webbasierte Oberfläche können die Inhalte der sogenannten Abrechnungsdatenbank ausgewertet und gepflegt werden.

Dafür steht die Web-Komponente „System Messages & Reporting“ Manager zur Verfügung, mit der die Einträge abgerufen und ausgewertet werden können. Die Aktivitäten können eingesehen werden, die Protokolle können ausgewertet werden. Vorbereitete Reports können in Form von CSV-Dateien heruntergeladen werden.

Die Modellierung der Protokolldaten und der Datenbank ist offengelegt, d.h. die Datenbank kann als Schnittstelle zu einem bestehenden Abrechnungssystem genutzt werden.

6.8 Monitoring

Die Monitoring-Komponente überwacht die GDI im Hintergrund und setzt dazu spezialisierte Sensoren ein. Diese sind individuell auf die zu überwachenden Dienste angepasst und überprüfen jeweils einzelne Aspekte ihrer Leistung, von der generellen Systemverfügbarkeit bis hin zur Systemleistung (Ant-



Monitoring Suite Administrator (SEC_ADMIN) Version: 1.8.10

Verfügbarkeit | Auswertung Übersicht | Auswertung Details | Prüfaufträge | Nachrichtenziele | Hilfe

Status der Prüfaufträge manuell

Aktiv	Status	Prüfauftragsname	Ergebnis	Prüfdauer (s)	Ergebnisdetails
🔒		WMPS Map		0	
🔒		ArcIMS auf arcgis.vmware		0	
🔒		HTTP mit Regexp		0	
🔒		WMPS Basis		0	
🔒		ArcIMS auf arcgis02.vmware		0	
🔒		Datenbank: jdbc lgeodb geodb01		0	
🔒		HTTP mit Regexp 2		0	
🔒		HTTP Tester No. 3		0	
🔒		Test ArcGis Server		0	
🔒		Test Serverseitige DB Prüfung		0	
🔒	✓	WMS intern dop20sw 8/5	Prüfung erfolgreich	5	
🔒	✗	Datenbank: jdbc oracle geodb01	Sensor nicht erreicht	0	Verbindungsparameter falsch oder DB nicht erreichbar. Details: List
🔒	✓	www.grit.de Überwachung	Prüfung erfolgreich	0	
🔒	✓	WMS Capabilities lgeoapp	Prüfung erfolgreich	5	
🔒	✓	Geoproxy; OWS-Farm	Prüfung erfolgreich	7	
🔒	✓	testSN	Prüfung erfolgreich	0	
🔒	✓	WMS Capabilities lgeoapp 2	Prüfung erfolgreich	5	
🔒	✓	WMS intern blattschnitt_tk10 (Bi	Prüfung erfolgreich	5	

Aktualisiert am 08.11.2018 um 11:57:52

Monitoring Suite

wortzeiten, Effizienz). Die Ergebnisse des Monitorings (Verfügbarkeit, Funktionen und Zugriffe) werden in einer Datenbank protokolliert.

Zur Steuerung des Monitorings werden die vorhandenen Sensoren den zu

kontrollierenden Diensten zugewiesen. Dabei kann eingestellt werden, wie intensiv der jeweilige Dienst überwacht werden soll (Zeitintervalle). Die Informationen über den aktuellen Systemzustand werden über ein Ampelsystem sowie anhand von vordefinierten Reports und Statistiken dargestellt. Etwaige Systemfehler werden den im System eingetragenen Verantwortlichen sofort per E-Mail gemeldet. Die Administration des Monitorings sowie die Auswertung der Systemzustände erfolgt über eine webbasierte Benutzungsoberfläche.

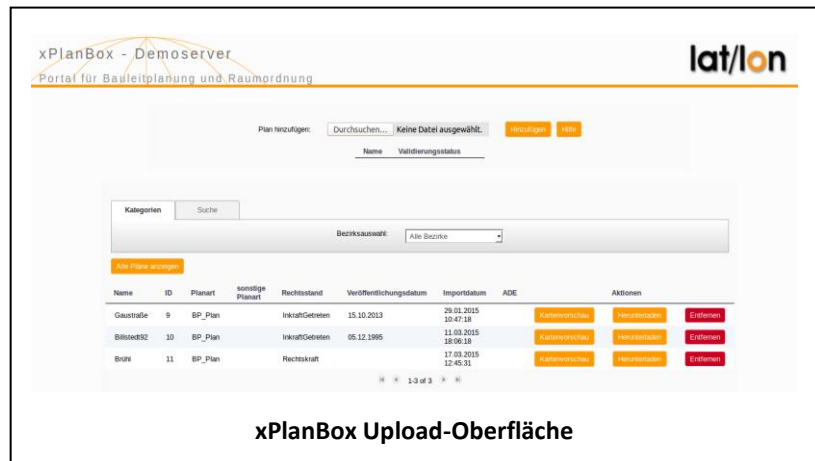
7 xPlanBox



Mit der xPlanBox steht eine integrierte Lösung bereit, die auf Basis des XPlanung-Standards XPlanGML den Austausch raumbezogener Planwerke auf kommunaler, regionaler und Landesebene zwischen verschiedenen IT-Systemen ermöglicht. Die xPlanBox stellt Module für die Verwaltung und Publikation von Geodaten im XPlanGML-Format sowie die Schnittstellen für die Einbettung in Verfahren der Öffentlichkeitsbeteiligung zur Verfügung.

Einige Funktionalitäten der xPlanBox sollen hier besonders hervorgehoben werden. Der XPlanManager ist die Verwaltungskomponente für die Bauleitpläne, die den Import inklusive Validierung der Eingangsdaten ermöglicht. Hinzu kommt eine schlanke Planübersicht, die über Kategorisierungs- und Suchfunktionalitäten verfügt, was insbesondere bei einer großen Anzahl von Bebauungsplänen sehr hilfreich ist. Der XPlanManager besitzt weiterhin eine Kartenvorschau, sowie die Möglichkeit, Pläne zu löschen und zu exportieren. Dadurch wird gewährleistet, dass eine effektive Verwaltung des vorhandenen Planbestandes möglich ist. Optional können Funktionalitäten zur Unterstützung von Planaufstellungsverfahren und zur nutzerbezogenen Absicherung der Anwendung hinzugeschaltet werden, wodurch der Einsatz der xPlanBox zur Unterstützung von vorhanden Prozessen innerhalb der Verwaltung besonders effizient gestaltet werden kann. Die WFS Schnittstellen werden in zwei verschiedenen Formen angeboten. Zum einen verfügt die XPlanBox über einen entsprechend zum XPlanung Standard und der INSPIRE Richtlinie konformen Downloaddienst. Zum anderen existiert ein WFS, der geeignet ist, XPlanGML verschiedener Versionen auf einem flachen GML Schema basierend abzugeben. Dies ist insbesondere in Bezug auf das Einbinden in Geoinformationssysteme und Geoportale wichtig, da diese die komplexen Strukturen von XPlanGML nicht verarbeiten können (äquivalent zu den INSPIRE Datenmodellen). Der Darstellungsdienst der xPlanBox wird durch eine INSPIRE-konforme WMS Schnittstelle bereitgestellt, die einen interoperablen Zugriff auf die Kartendarstellung der Planinhalte ermöglicht.

Dadurch können georeferenzierte Rasterdateien zu den Plänen genauso abgebildet werden, wie die in XPlanGML modellierten Vektordaten. Für die Visualisierung der XPlanGML basierten Planinhalte im XPlanWMS wird auf den OGC Standard Symbology Encoding zurückgegriffen. Dadurch steht eine interoperable Implementierung der



xPlanBox Upload-Oberfläche

Planzeichenverordnung innerhalb der xPlanBox zur Darstellung von Planinhalten bereit. Die WMS Schnittstelle verfügt über eine Sachinformationsabfrage, mit der Plananhänge, bspw. PDF Dateien, referenziert werden können.

Mit den beschriebenen Dienstschnittstellen verfügt die xPlanBox über ein standardkonformes und dadurch interoperables Setup für die erfolgreiche Publikation von Planwerken der Bauleitplanung.

Die xPlanBox integriert neben den bereits beschriebenen Schnittstellen für die Beauskunftung von bereits rechtlich verbindlichen Planwerken umfangreiche Funktionalitäten zur Unterstützung von Planaufstellungsverfahren. Hier werden spezielle, aber dennoch standard-konforme Dienstschnittstellen bereitgestellt, die die zeitlich eingeschränkte und abgesicherte Publikation von Planwerken im Rahmen von Aufstellungsverfahren ermöglicht.