

Architektur eGRIS / Terravis extern

Version: 0.6
Datum: 8.07.2011
Autoren: Claude Eisenhut

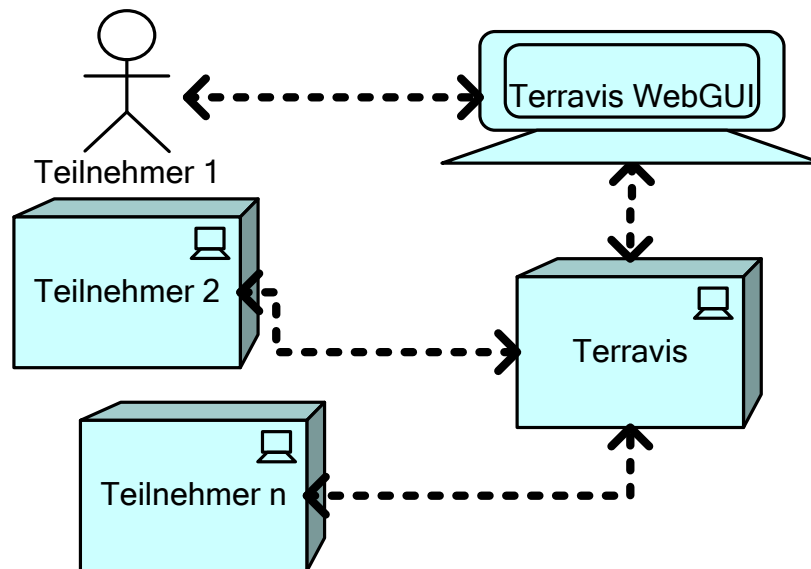
Einführung

Das folgende Dokument wurde erstellt, um die gemeinsame Vorstellung der Funktionsweise des eGRIS-Systems (Terravis-System inkl. Teilnehmer-Systeme) zu dokumentieren. Es beschreibt aber nicht die Architektur des Terravis-Systems. Bestehende Standards (z.B. eCH) werden dann berücksichtigt, wenn sie auch in der Banken-IT-Welt verbreitet sind und unverändert 1:1 nutzbar (auch keine Spezialisierung notwendig) sind.

Systemarchitektur

Im Rahmen des eGVT kommunizieren die Teilnehmer-Systeme technisch (unterhalb des Applikationsniveau) nicht direkt miteinander, sondern immer via Terravis. Damit eine detaillierte Prozesskontrolle/-Steuerung und auch eine Verrechnung realisiert werden kann.

Der eGVT ist technisch ein geschlossenes System.



Systemarchitektur

Die technische Schnittstelle zwischen Teilnehmersystem und Terravis wird mit SOAP (mit HTTP-Binding) und über Twoway-SSL realisiert.

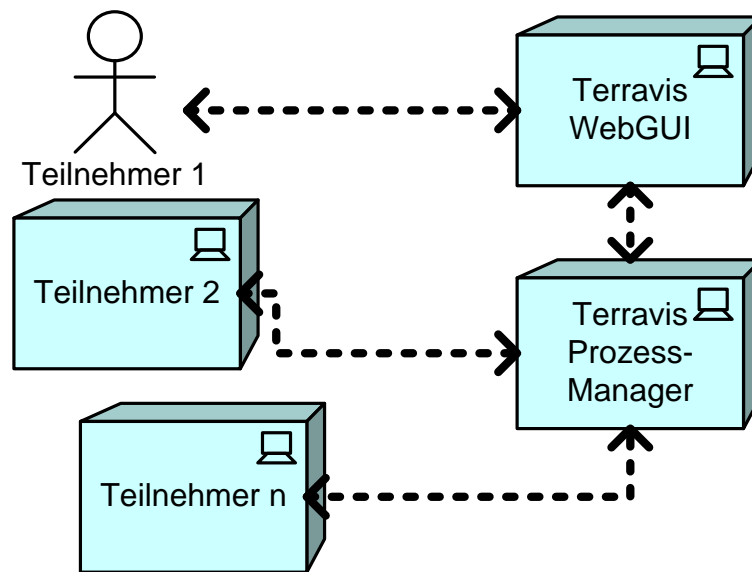
Es gibt auch Teilnehmer (z.B. Notare), die kein eigenes System betreiben. Für diese stellt Terravis ein WebGUI zur Verfügung.

Je nach Prozessschritt handelt es sich um eine synchrone oder asynchrone Kommunikation. Eine synchrone Kommunikation findet normalerweise dann statt, wenn die Ausführung des Prozessschritts automatisiert ist. Eine asynchrone Kommunikation findet dann statt, wenn der Prozessschritt nicht automatisierbar ist. Auch bei den Teilnehmern müssen Web-Services bereitgestellt werden (für die zum Teilnehmer hin gerichtet Kommunikation).

Andere technische Kommunikationsschnittstellen sind nicht vorgesehen.

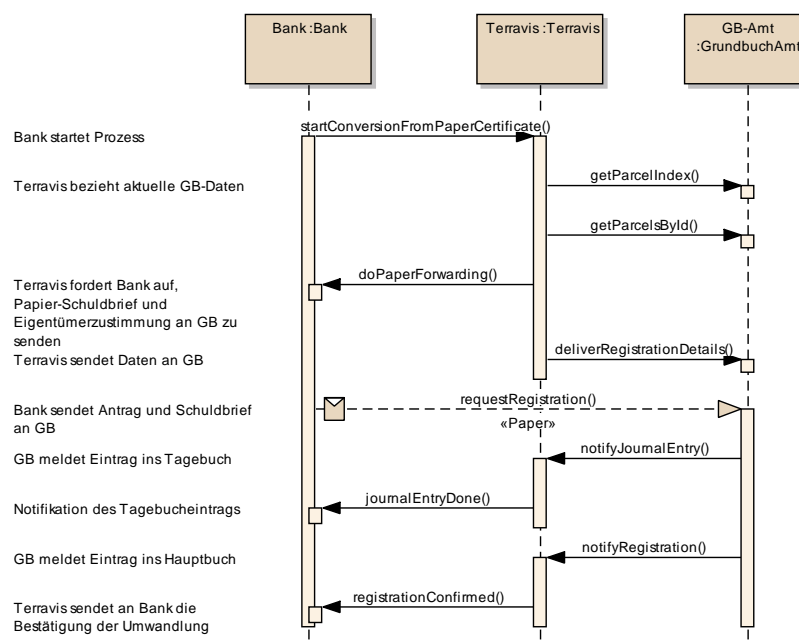
Meldungs- und Protokollarchitektur

Auch auf dem Applikationsniveau (fachliche Stufe) kommunizieren die Teilnehmer mit Terravis.



Kommunikation auf fachlicher Stufe

Ein Prozess wird normalerweise durch einen Teilnehmer gestartet. Ein Prozess besteht aus einzelnen Schritten. Die einzelnen Schritte werden, typischerweise, durch die Teilnehmer ausgeführt. Es gibt automatisierbare und nicht automatisierbare Schritte. Der Meldefluss (wann Terravis mit welchem Teilnehmer kommuniziert) ergibt sich aus der Prozessdefinition (die Abfolge der Schritte).



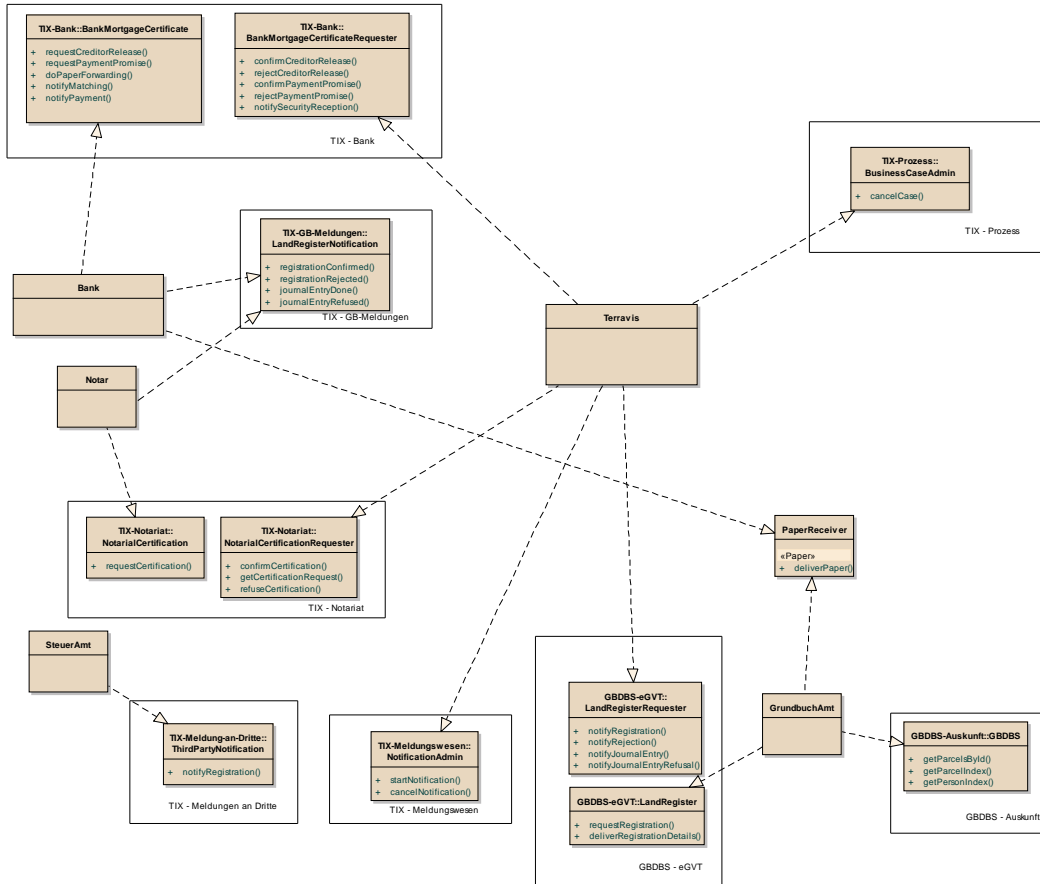
Beispiel eines Meldeflusses

Einbindung Terravis-WebGUI

Das Terravis WebGUI wird vom Terravis Prozess-Manager wie ein normales Teilnehmer-System angesprochen (mit denselben Web-Services-Definitionen). Somit ist in den Prozessdefinitionen keine Unterscheidung notwendig, nur der Service-Endpoint referenziert einen Terravis internen Web-Service.

Übersicht der Web-Services

Die Web-Services werden in einzelnen Spezifikationen beschrieben. Die Aufteilung in einzelne Spezifikationen hat zum Ziel, dass Änderungen nur auf eine begrenzte Anzahl Teilnehmer (bzw. deren Service-Instanzen) Auswirkungen haben.

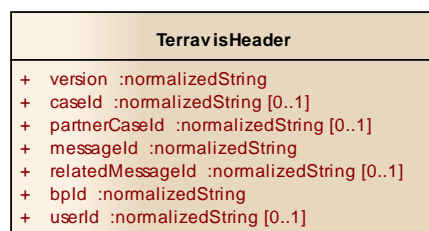


Übersicht der Web-Service Spezifikationen

Die GBDBS-Spezifikation beschreibt die Schnittstellen von und zum Grundbuch Amt.

Header

Eine Meldung enthält als fachlichen Inhalt typischerweise alle Informationen, die der Empfänger (Mensch und Maschine) für die Abarbeitung des Prozessschrittes benötigt. Für die Adressierung und Prozesssteuerung werden weitere Informationen benötigt. Für diese wird eine Headerstruktur definiert, die in allen Meldungen vorhanden ist.



Headerstruktur

Quittierung

Alle Meldungen, unabhängig ob der Request vom Teilnehmer-System oder vom Terravis-System ausgeht, werden technisch synchron quittiert. Diese sofortige, technische Quittung ist in der Regel nicht signiert.

Meldungstypen

Es braucht eine *konkrete fachliche* Typisierung der Meldungen (z.B. GB-Anmeldung oder GB-Abweisung), damit die Prozesssteuerung automatisch durchgeführt werden kann. Es braucht aber (auf der fachlichen Stufe der Kommunikation) keine abstrakte Typisierung (z.B. Auftrag, Auftragsbestätigung, Notifikation, Fehler, Test, ...).

Dossier

Es gibt kein explizites Dossier zum einzelnen Geschäftsfall. In den einzelnen Meldungen sind nicht alle Daten zu einem Geschäftsfall enthalten, sondern nur diejenigen die für den aktuell auszuführenden Prozessschritt erforderlich sind. Jeder Teilnehmer kann für sich ein oder mehrere Dossiers führen, die Zuordnung zum Terravis-Geschäftsfall ist aber Sache des einzelnen Teilnehmers.

Signaturen

Einzelne Meldungstypen müssen signiert sein. Es gibt die folgenden Anforderungsklassen:

- unverbindlicher Informationsaustausch
- Willensäußerung ohne Formvorschrift
- Willensäußerung mit gesetzlich geforderter Schriftlichkeit
- Beglaubigung durch Notar
- Beglaubigung durch Grundbuchverwalter (z.B. Bescheinigung über Einschreibung im Hauptbuch)

Für die ersten beiden werden keine digitalen Signaturen eingesetzt. Nur für die letzten drei werden qualifizierte digitale Signaturen gem. ZertES eingesetzt.

Die Zuordnung eines Meldungstypen zu einer Signatur-Anforderungsklasse erfolgt im Rahmen der Prozessdefinition.

Alle im Rahmen von Terravis eingesetzten qualifizierten Signaturen sind aber so gestaltet, dass eine Signaturvalidierung ohne Zugriff auf externe Services erfolgen kann.

Alle notwendigen Rolleninformationen (Claim Assertions; z.B. ob jemand vertretungsbefugt, Notar oder Grundbuchverwalter ist) sind als qualifizierende Signaturattribute Teil der Signatur. Die folgenden Rollen müssen unterscheidbar sein:

- Vertretungsbefugt (für ein Amt, Unternehmen, natürliche Person)
- Notar
- Grundbuchverwalter

Alle Signaturen enthalten auch als qualifizierendes Attribut einen Zeitstempel.

Für die qualifizierenden Attribute wird ETSI TS 101 903 verwendet. Der exakte Signaturaufbau, die genauen Attributnamen, der Ablauf der Signaturerstellung und Signaturvalidierung werden in einem getrennten Dokument beschrieben.

Terravis definiert welcher Timestamp Dienst verwendet werden kann.

Terravis definiert, welche Ausgangszertifikate für die Signatur der Attribute gültig sind.

Adressierung

Die Kommunikation erfolgt zwischen dem Teilnehmer-System (z.B. eine GB-Instanz) und Terravis, aber nicht zwischen Personen. Eine genauere Adressierung (einer bestimmten Person, Funktion, Organisationseinheit oder Applikationsfunktion) ist Sache des Teilnehmer-Systems. Es müssen in der Meldung genügend Informationen vorhanden sein, damit das Teilnehmer-System eine solche, feinere Adressierung, vornehmen kann.

Prozesskontrolle

Auch die Teilnehmer setzen evtl. Prozesskontrolltools ein. Die Schnittstellen müssen das zulassen.

Terravis ist der Prozess-Eigentümer. Terravis ist für die Prozessdefinition verantwortlich und für die korrekte Ausführung der Prozesse (Abfolge der Schritte). Terravis ist nicht für die korrekte Ausführung der Schritte durch die Teilnehmer verantwortlich. Bei asynchroner Kommunikation muss technische sichergestellt sein, dass der richtige Teilnehmer die Antwort-Meldung sendet (header:relatedMessageld ist identisch mit der vorgehenden header:messageld).

Die Prozessdefinition regelt, was bei technischen Fehlern (z.B. Meldung validiert nicht) passiert (die möglichen Folgeschritte sind).

Die Prozessdefinition regelt, was bei fachlichen Fehlern (z.B. Kaufvertrag (PDF) ohne Kaufpreis) passiert (die möglichen Folgeschritte sind).

Mögliche Fehlerbehandlungsstrategien sind:

- ignorieren ohne Eintrag im Log
- ignorieren mit Eintrag im Log
- Schritt wiederholen ohne Frist
- Schritt wiederholen mit Frist
- Fehler an den Vorgänger weitergeben (=zurück in der Prozessschrittabfolge)
- Prozess sofort abbrechen.

Notifikation

Es gibt auch Teilnehmer (z.B. Steueramt), die nicht an den eigentlichen Geschäftsprozessen teilnehmen, aber bei bestimmten Vorgängen (z.B. Änderung des Eigentümers) eine Mitteilung erhalten möchten. Diese Art von Meldungen wird als Notifikation bezeichnet.

Als Teil der Prozessdefinition wird definiert, an welchen Stellen und/oder für welche Datenelemente welche Notifikationen durch Terravis generiert werden.

Ein Teilnehmer kann sich bei Terravis für solche Notifikationen "abonnieren", ohne an den konkreten Prozessen beteiligt zu sein.

Es gibt auch Geschäfte im Grundbuch, die nicht über Terravis laufen. Diese müssen auch notifiziert werden können.

Verrechnung

Der Meldungsverkehr wird durch die Teilnehmer am jeweiligen Prozess bezahlt. Die Aufteilung der Kosten erfolgt aufgrund der Rolle die ein Teilnehmer innerhalb des Prozesses hat.

In den Meldungsstrukturen braucht e somit keine extra Informationen für die Verrechnung.

Die Verrechnung ist nicht Bestandteil dieses Dokumentes.

Infrastrukturservices

Es braucht auch Services die nicht direkt einer Fachfunktion im Geschäftsverkehr entsprechen. Es braucht z.B.:

- einen Service, der eine EGRID in einen Service-Endpoint des Grundbuch-Amtes abbildet
- Empfänger für Notifikationen an/abmelden

Basisspezifikationen

Extensible Markup Language (XML) 1.0 (Fifth Edition)

XML Schema Part 1: Structures Second Edition

XML Schema Part 2: Datatypes Second Edition

Simple Object Access Protocol (SOAP) 1.1

Web Services Description Language (WSDL) Version 1.1

XML Signature Syntax and Processing (Second Edition)

SuisseID Specification Version 1.3

ETSI TS 101 903 (v 1.4.2): XML Advanced Electronic Signatures (XAdES)

RFC3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

Gestaltungsrichtlinien für die Webservices

Die Web-Services und/oder Meldungsstrukturen dürfen sich nicht ändern, wenn der Prozessablauf sich ändert.

Die Schemas der Schnittstellen werden soweit möglich stark typisiert.

Die Service-Beschreibungen werden in einzelne Namespaces unterteilt, so dass sich Änderungen auf den jeweiligen Namespace beschränken (und die Service-Instanzen die diesen Namespace implementieren, statt auf alle Service-Instanzen).

Die Web-Services wissen nicht, dass sie von einer BPEL-Engine aufgerufen werden, und sind entsprechend auch nicht so gestaltet.

Die Granularität der einzelnen Operationen wird so gewählt, dass möglichst genau eine bestimmte Fachfunktion (aus Sicht Senderorganisation) in der Empfängerorganisation mit einem einzelnen Aufruf ausgelöst werden kann.

Jeder Service unterstützt dynamische Versionsverhandlung, so dass eine Instanz (Server und/oder Client) gleichzeitig mehrere Versionen unterstützen kann, und der Client feststellen kann, welche Versionen der Server unterstützt.

Versionierung

Ändert sich ein Schema oder die Semantik, wird der entsprechende Schema Namespace-Name geändert.

Ausnahmen¹:

- Die Änderung ist nur für Terravis nicht rückwärtskompatibel.
- Die Änderung ist klein, findet in einem nicht produktiv im Einsatz stehenden Schema statt, und ist unter den betroffenen Entwicklungsteams abgesprochen.

SOAP

Der technische Inhalt wird nicht im soap:header kommuniziert, sondern eingebettet in den fachlichen Inhalt im soap:body². Ist technischer Inhalt bei einem Prozessschritt

¹ Die Ausnahmen sollen helfen, den Gesamtaufwand zu optimieren

² Weil nicht alle SOAP-Tools eine Ergänzung des soap:header unterstützen.

auch fachlich relevant, wird die entsprechende Information doppelt kommuniziert, einmal im technischen Header und einmal im eigentlichen fachlichen Inhalt (z.B. die caseld beim Eröffnen eines neuen Geschäftsfalles).

Es wird der sogenannte document/literal wrapped Stil verwendet:

- pro Operation höchstens ein In-WSDL:Part
- Der WSDL:Part referenziert eine XML-Element Definition
- Das referenzierte Element hat keine XML-Attribute
- Das referenzierte Element hat den selben Namen wie die Operation

Es wird ein HTTP-Binding verwendet.

Für binäre Dateien wird xsd:base64binary verwendet ^{3,4}.

WSDL

Schema-Typen werden immer in einem eigenen XML-Schema definiert. Es werden keine Schema-Typen im WSDL definiert.

XML-Schema

Auf den Einsatz von all, union, choice wird aus Kompatibilitätsgründen verzichtet. Auf den Einsatz von restriction bei complexType wird aus Kompatibilitätsgründen verzichtet.

XML

Alle XML-Elemente die ein Objekt repräsentieren, haben ein optionales XML-Attribut id (für system-interne Verwendung), dass transient ist und durch Terravis ignoriert und nicht weitergereicht wird.

Namensrichtlinien für die Webservices

Für die Namen im WSDL und XSD der Webservices wird Englisch verwendet. Die Schemas der Fachdaten bleiben Deutsch.

Namen die Objekte bezeichnen beginnen mit einem Grossbuchstaben.

Namen die Objekteigenschaften bezeichnen beginnen mit einem Kleinbuchstaben.

Bei Namen die sich aus mehreren Wörtern zusammensetzen, beginnen die Folgewörter mit einem Grossbuchstaben.

³ "SOAP Messages with Attachments" wird nicht von allen Tools unterstützt (<http://www.w3.org/TR/SOAP-attachments>), und bietet zusätzliche Schwierigkeiten bei der Signaturerstellung/validierung

⁴ MTOM ist für SOAP 1.1 nicht verbreitet realisiert (<http://www.w3.org/Submission/soap11mtom10/>)