Terravis

Elektronisches Auskunftsportal
Elektronischer Geschäftsverkehr eGV

Sicherheitsleitfaden für die Integration in Terravis

Änderungsverzeichnis

Version	Status	Name	Datum	Beschreibung
1.3	Final	René Eberhard	28. Januar 2013	Präzisierungen und kleinere textuelle Anpassungen

Inhaltsverzeichnis

1 Einleitung

Terravis ermöglicht den elektronischen Geschäftsverkehr zwischen Grundbuchämtern, Notariaten und Banken. Damit können erstmals zwischen diesen Parteien Grundstück- und Hypothekargeschäfte über eine einzige Schnittstelle abgewickelt werden. Die Kommunikation erfolgt sicher, standardisiert und medienbruchfrei. Zusammen mit dem papierlosen Schuldbrief wird Terravis Wirtschaft, Notare und Verwaltung von Administration entlasten und die Prozesse beschleunigen.

Dieses Dokument richtet sich an die Partner (Finanzinstitute, Grundbuchämter, Swisstopo) von Terravis. Es gibt eine beispielhafte Übersicht über die grundlegenden Integrationsschnittstellen und beschreibt die wichtigsten, Terravis bezogenen technischen und organisatorischen Schutzobjekte, welche im Verantwortungsbereich der jeweiligen Teilnehmer liegen und entsprechend sicher gehandhabt werden müssen.

Hinweis
Die Liste der Schutzobjekte ist beispielhaft und nicht abschliessend. Die jeweiligen Parteien sind alleinig dafür verantwortlich, ihre eigenen Schutzobjekte sowie deren Abhängigkeiten zu identifizieren und diese entsprechend zu bewerten. Es liegt auch in der alleinigen Verantwortung der jeweiligen Parteien, den Schutz der entsprechenden Objekte über geeignete Massnahmen sicherzustellen.

1.1 Begriffe

1.1.1 Definitionen

Bezeichnung	Beschreibung
A || B	Lückenloses Aneinanderfügen von A und B -> AB.
Auditeinträge	Alle wichtigen Zugriffe, Abfragen und Transaktionen werden in Terravis protokolliert. Diese Auditeinträge können durch einen Benutzer, der auf die Funktion „Audit“[1] berechtigt ist, abgerufen werden. Untenstehend sind die wichtigsten Auditeinträge aufgeführt: ▪ Zeitpunkt der Transaktion ▪ Eindeutige Transaktions-ID ▪ Typ der Transaktion / Abfrage ▪ Partner ID ▪ User ID ▪ Betroffene Kantone einer Transaktion ▪ Typ der Antwort auf eine Anfrage (z.B. Übersicht, Index, Dokument, Datenlieferung, etc.) ▪ Status der Transaktion (Erfolgreich, Fehler, etc.) ▪ Suchkriterien im Falle einer Suchabfrage

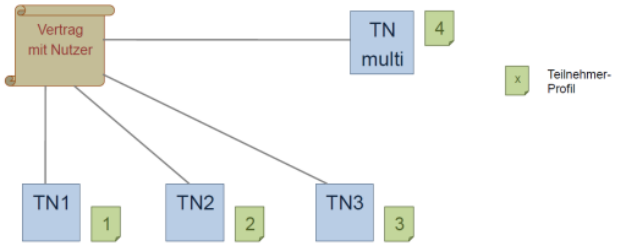
[1] Gemäss [RollenProfil]

Bezeichnung	Beschreibung
Benutzer Natürliche Person	Berechtigte, natürliche Person, die von einem Teilnehmer für die Nutzung von Terravis registriert wurde. Der Benutzer verwendet die von Terravis bereitgestellte Businessfunktionalität. Es liegt in der Verantwortung des Teilnehmers, dem Nutzer die richtigen Zugriffsberechtigungen gemäss [RollenProfil] zu vergeben.
CA	Certification Autority (Zertifizierungsdiensteanbieter)
Datenabfrage	Siehe „Elektronisches Auskunftsportal“.
Datenbezug (Webservice)	a) Synchroner Datenbezug Der Benutzer (Client) bezieht die Grundbuchinformationen als Antwort auf seine Anfrage vom Webservice von Terravis. b) Asynchroner Datenbezug Pull Der Benutzer prüft periodisch über einen Webservice von Terravis, ob die Grundbuchinformationen bereitstehen, und bezieht diese. Der Benutzer (Client) baut eine Verbindung zu Terravis (Server) auf. c) Asynchroner Datenbezug Push Terravis sendet die angeforderten Daten an einen Webservice des Benutzers. Terravis (Client) baut eine Verbindung zum Webservice des Benutzers (Server) auf.
Elektronischer Geschäftsverkehr (eGV) (Webapplikation)	Im Rahmen des elektronischen Geschäftsverkehrs stellt Terravis eine zentrale Prozessplattform in Form einer Webapplikation für die Abwicklung der domänenübergreifenden Geschäftsprozesse bereit.
Elektronisches Auskunftsportal (Webapplikation)	Ein Benutzer bezieht nicht rechtsgültige Grundbuchinformationen[2] als PDF Datei über das Web-GUI von Terravis.

[2] Beispiel [GBA-Arosa56]

<table>
<tr><th>Bezeichnung</th><th>Beschreibung</th></tr>
<tr><td>Grundbuchinformationen</td><td>Grundbuchdaten ohne rechtsgültige Wirkung (mit zusätzlich angereicherten Daten).
Aktuell gelten die folgenden Berechtigungen im Zusammenhang mit der Einsichtnahme in die Grundbuchinformationen-PDF. Die diesbezüglichen Rollen sind weitgehend im [RollenProfil] beschrieben und richtigen sich nach den Vorgaben der [GBV].
<table>
<tr><th>#</th><th>Beschreibung gemäss [GBA-Arosa56]</th><th>[RollenProfil]</th><th>Status</th></tr>
<tr><td>1.</td><td>Grundstückbeschreibung</td><td>☑</td><td>Öffentlich</td></tr>
<tr><td>2.</td><td>Dominierte Grundstücke</td><td>In 1. enthalten</td><td>Öffentlich</td></tr>
<tr><td>3.</td><td>Eigentum</td><td>☑</td><td>Öffentlich</td></tr>
<tr><td>4.</td><td>Anmerkungen</td><td>☑</td><td>Öffentlich</td></tr>
<tr><td>5.</td><td>Dienstbarkeiten</td><td>☑</td><td>Öffentlich</td></tr>
<tr><td>6.</td><td>Grundlasten</td><td>In 5. enthalten</td><td>Öffentlich</td></tr>
<tr><td>7.</td><td>Vormerkungen</td><td>☑</td><td>Eingeschränkte Einsicht</td></tr>
<tr><td>8.</td><td>Grundpfandrechte</td><td>☑</td><td>Eingeschränkte Einsicht</td></tr>
<tr><td>9.</td><td>Rangverschiebungen</td><td>In 8. enthalten</td><td>Eingeschränkte Einsicht</td></tr>
<tr><td>10.</td><td>Hängige Geschäfte</td><td>Immer aktiviert</td><td>Öffentlich</td></tr>
<tr><td>11.</td><td>Plan für das Grundbuch</td><td>☑</td><td>Öffentlich</td></tr>
<tr><td>12.</td><td>Amtliche Bewertung[3] (Steuerwerte)</td><td>☑</td><td>Eingeschränkte Einsicht</td></tr>
<tr><td>13.</td><td>Korrespondenzadresse Eigentümer</td><td>☑</td><td>Öffentlich</td></tr>
<tr><td>14.</td><td>Bezugsoptionen</td><td>Immer aktiviert</td><td>Öffentlich</td></tr>
</table>
</td></tr>
<tr><td>Grundbuchinformationen-PDF</td><td>Grundbuchinformationen als PDF</td></tr>
<tr><td>Grundbuchinformationen-XML</td><td>Grundbuchinformationen als XML mit angefügten Grundbuchinformationen-PDF.</td></tr>
</table>

[3] Die Einsicht in Steuerwerte ist in Terravis nicht aktiviert. Diese Informationen sind nicht Bestandteil des Grundbuches

Bezeichnung	Beschreibung
Multi-Teilnehmer Organisationseinheit	Ein dem Teilnehmer übergeordneter Teilnehmer. Der Multi-Teilnehmer kann potentiell alle Funktionen der unterliegenden Teilnehmer ausführen. Der Multi-Teilnehmer kann jedoch keine Teilnehmer erfassen.  **Abbildung 1**
Nutzer Organisation	Kunde/Lieferant (juristische Person, Behörde, Urkundsperson und Geometer etc.), der das Terravis System nutzen möchte. Der Nutzer schliesst mit Terravis einen schriftlichen Vertrag über die Nutzung von Terravis ab.
RA	Registration Authority (Registrierstelle einer CA)
SuisseID IAC	SuisseID Identification and Authentication Certificate (kein qualifiziertes Signaturzertifikat nach ZertES)
Teilnehmer Organisationseinheit, Mandant	Eine Organisationseinheit der Organisation (z.B. Kanton, Gemeinden etc.). Ein Teilnehmer hat ein spezifisches [RollenProfil], das den jeweiligen Benutzern vererbt wird. Teilnehmer werden immer durch Terravis erfasst.
Urkundsperson	Träger eines öffentlichen Amtes (Notar).

1.1.2 Referenzen

Referenz	Beschreibung
[GBA-Arosa56]	Grundbuchinformationen Arosa / 56 / CH327777651750 `Arosa, 56.pdf`
[GBV]	Grundbuchverordnung, vom 23. September 2011 (Stand am 1. Januar 2012), SR 211.432.1
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RollenProfil]	Rollenprofile Pilot Auskunftsportal Terravis `101019 Rollenprofile Terravis.pdf`
[SuisseID Spezifikation]	eCH-0113: SuisseID specification, Version 1.5, Stand 30. November 2011
[VZertES]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur, 943.032 Stand 1. August 2011
[ZertES]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, 943.03 Stand 1. August 2008

1.2 Über dieses Dokument

Die Kapitel in diesem Dokument wurden nutzerspezifisch gegliedert. Die spezifischen Informationen für die jeweilig unten aufgeführten Nutzer sind in den entsprechenden Kapiteln aufgeführt.

1.2.1 Urkundspersonen

Die untenstehenden Kapitel richten sich an Urkundspersonen, welche Terravis im Rahmen ihrer Geschäftstätigkeiten nutzen.

#	Überschrift	Kapitel
a.	Systembeschreibung	Kapitel 2
b.	Urkundspersonen und für Urkundspersonen zuständige kantonale Stelle	Kapitel 3
c.	Terravis	Kapitel 6
d.	Verschiedenes	Kapitel 7

1.2.2 Institutionelle Kunden

Die untenstehenden Kapitel richten sich an institutionelle Kunden, welche Terravis im Rahmen ihrer Geschäftstätigkeiten nutzen.

#	Überschrift	Kapitel
a.	Systembeschreibung	Kapitel 2
b.	Institutionelle Kunden	Kapitel 4
c.	Terravis	Kapitel 6
d.	Verschiedenes	Kapitel 7

1.2.3 Grundbuchämter

Die untenstehenden Kapitel richten sich an Grundbuchämter, die Daten im Rahmen von Terravis bereitstellen resp. die Terravis im Rahmen ihrer Geschäftstätigkeiten nutzen.

#	Überschrift	Kapitel
a.	Systembeschreibung	Kapitel 2
b.	Grundbuchämter	Kapitel 5
c.	Terravis	Kapitel 6
d.	Verschiedenes	Kapitel 7

1.2.4 Swisstopo

Swisstopo stellt im Rahmen von Terravis raumbezogene Geodaten in Form von visualisierten Parzellenplänen bereit. Auf die integrationsspezifischen Abhängigkeiten zu Swisstopo wird in diesem Dokument nicht eingegangen.

2 Systembeschreibung

Die Nutzung von Terravis unterliegt übergeordneten Vertrags- und Nutzungsbestimmungen und erfolgt über gegenseitig authentisierte SSL Verbindungen zwischen den Client- und Serverkomponenten.

2.1 Organisatorische / Vertragliche Übersicht

Folgend sind die wichtigsten Teilnehmer mit ihren Vertragsbeziehungen und Interaktionen im Zusammenhang mit organisatorischen Prozessen aufgeführt.

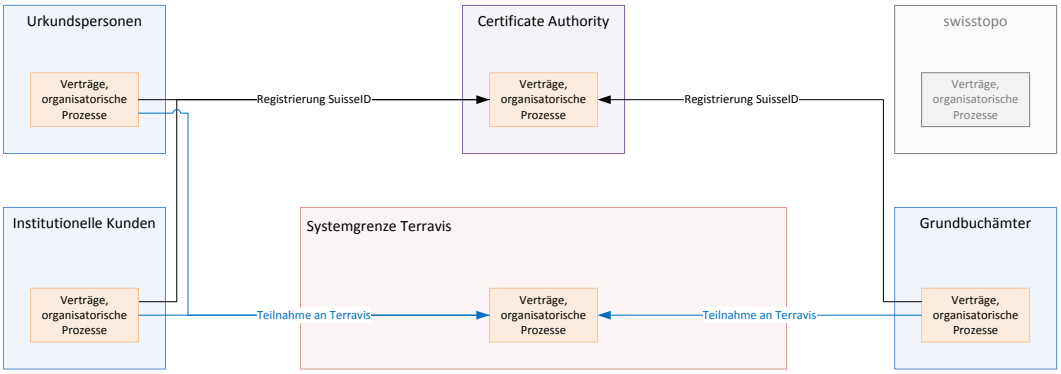


Abbildung 2

2.2 Technische Systemübersicht

Folgend sind die wichtigsten Teilnehmer und Systemkomponenten aufgeführt.

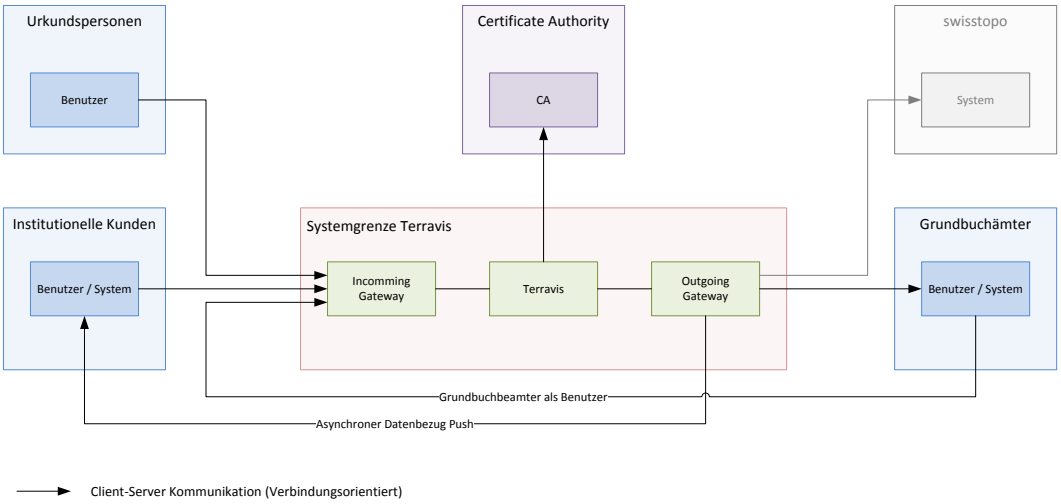


Abbildung 3

2.3 Technische Schnittstellen und Zuständigkeiten

2.3.1 Systemgrenze Terravis - Zuständigkeiten

Alle Komponenten, die sich ausserhalb der Systemgrenze[4] von Terravis befinden, unterliegen dem Verantwortungsbereich der jeweiligen Teilnehmer.

Die jeweiligen Parteien sind eigenständig verantwortlich für alle technischen und organisatorischen Prozesse sowie für alle Systemkomponenten, die sich innerhalb ihrer eigenen Systemgrenzen befinden.

Die Verantwortlichkeiten hinsichtlich der Qualität oder der Verfügbarkeit gemeinsam genutzter Komponenten, insbesondere der Netzwerkverbindungen zwischen den Parteien, müssen zwischen den entsprechenden Parteien abgesprochen werden. Es gibt diesbezüglich keine garantierten Qualitätsmerkmale bezüglich der End-to-End Verbindungen. Diese erfolgen nach „best effort“ der jeweiligen Parteien.

2.3.2 Authentisierung gegenüber SIX Terravis

Die Authentisierung der Benutzer gegenüber SIX Terravis erfolgt entweder mit Username / Passwort oder mit einem zertifikatsbasierten Authentisierungsmerkmal. Die Anforderungen an die zertifikatsbasierten Authentisierungsmerkmale werden von SIX Terravis vorgegeben und unter Kapitel 7.1 beschrieben. Folgend ist eine Übersicht über die vorgegebenen Authentisierungsmerkmale in Abhängigkeit der SIX Terravis Services gegeben:

SIX Terravis Service	Zugelassene Authentisierungsmerkmale
Datenabfrage (Webapplikation)	▪ Username / Passwort ▪ Zertifikatsbasierte Authentisierungsmerkmale (benutzerbezogener Hardware Token)
Datenbezug (Webservice)	▪ Zertifikatsbasierte Authentisierungsmerkmale (serverbezogener Hardware- oder Software Token)
eGV (Webapplikation)	▪ Zertifikatsbasierte Authentisierungsmerkmale (benutzerbezogener Hardware Token)
Administration (Webapplikation)	Falls die administrativen Tätigkeiten über die Webapplikation erfolgen: ▪ Zertifikatsbasierte Authentisierungsmerkmale (benutzerbezogener Hardware Token)
Administration (Webservice)	Falls die administrativen Tätigkeiten über Webservices erfolgen: ▪ Zertifikatsbasierte Authentisierungsmerkmale (serverbezogener Hardware- oder Software Token)

[4] Siehe Abbildung 3

2.4 Administrative Prozesse

Folgend ist eine Übersicht über die wichtigsten administrativen Prozesse aufgeführt. Die detaillierte Beschreibung der einzelnen Prozesse wird durch Terravis bereitgestellt.

2.4.1 Technische Integration in Terravis

Nach Abschluss der vertraglichen Vereinbarungen erfolgt die technische Integration in Terravis. Es gibt grundsätzlich zwei Phasen:

#	Beschreibung
1.	Technische Integration der Schnittstellen, Protokolle und Meldungen in die jeweiligen Applikationen.
2.	Formelle Integration der Parteien. Im Zusammenhang mit der gegenseitigen Authentisierung der Systeme müssen die entsprechenden Authentisierungsmerkmale[5] formell zwischen den Parteien ausgetauscht werden.

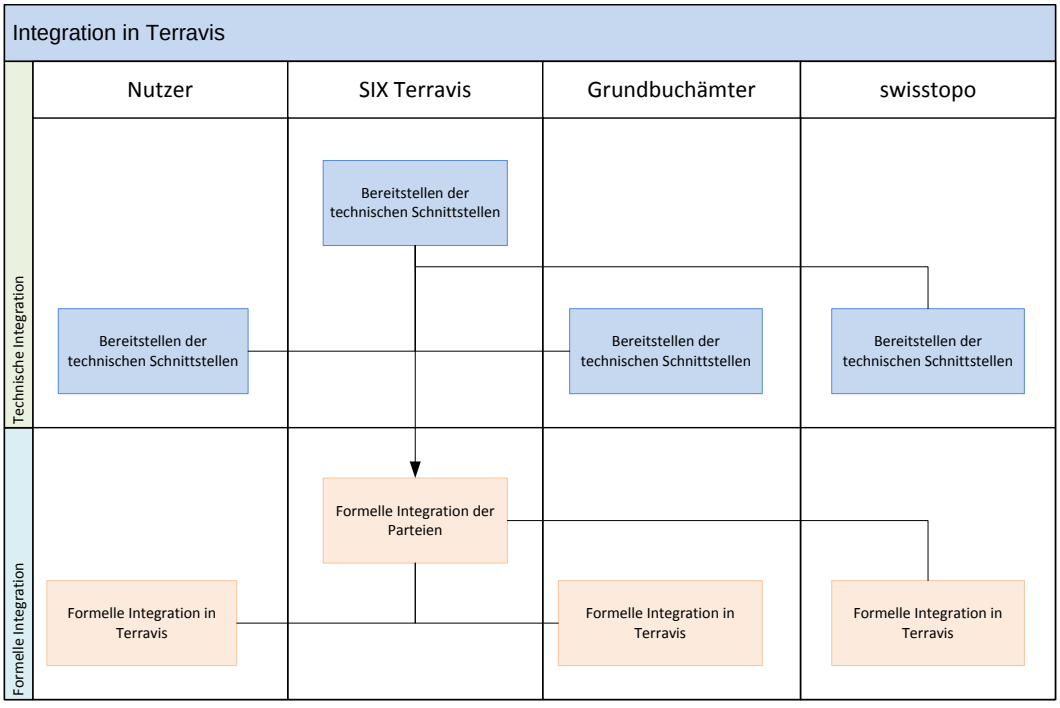


Abbildung 4

[5] Z.B. Benennung des Hostnamens, wie er im X.509 Zertifikat steht und Benennung der ausstellenden CA.

2.4.2 Registrieren von Administratoren und Benutzern

Die Teilnehmer sind selber verantwortlich für die Registrierung und Verwaltung der eigenen Administratoren und Benutzer. Initial wird ein „initialer Administrator“ pro Nutzer formell erfasst und bei Terravis technisch aufgeschaltet. Danach kann der initiale Administrator eigenständig weitere Administratoren oder Benutzer über die Webapplikation oder den Webservice von Terravis registrieren und verwalten.

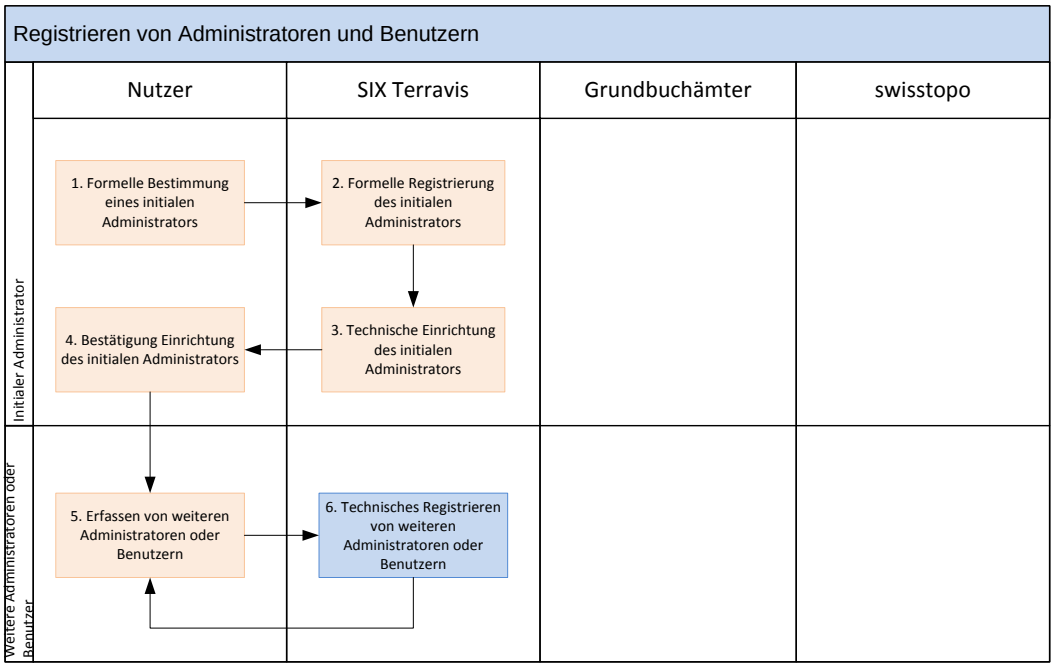


Abbildung 5

2.4.3 Vergabe von Initialpasswörtern durch Terravis

Der Registrierprozess von Benutzern wurde so gestaltet, dass Passwörter nie vollständig im Klartext über das Netzwerk übermittelt werden. Alle von Terravis vergebenen Passwörter sind sogenannte Initialpasswörter, die von den Benutzern nach dem ersten Login geändert werden müssen. Von Terravis generierte Initialpasswörter, die per Email an den Benutzer versendet werden, müssen vom Benutzer mit einem teilnehmerspezifischen Prefix[6] ergänzt werden. Dieser wird bei der formellen Erfassung des initialen Administrators über einen separaten Kanal[7] von Terravis an den Nutzer übermittelt (siehe Kapitel 2.4.2).

Der Benutzer muss nach seinem ersten Login in Terravis sein persönliches Passwort ändern.

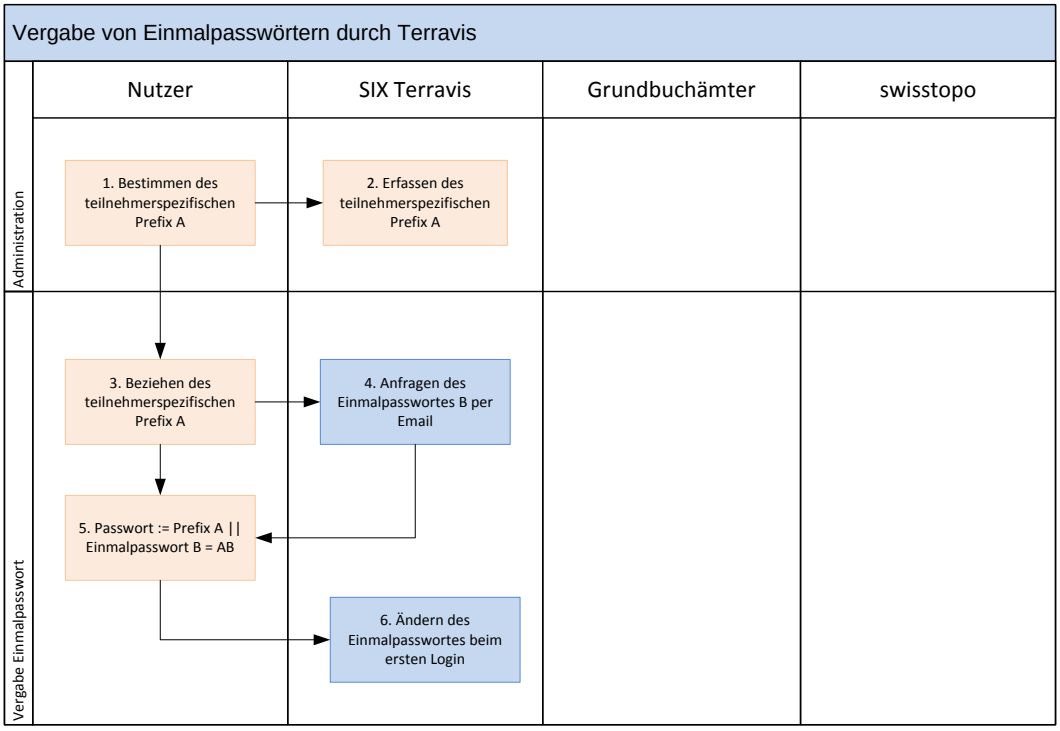


Abbildung 6

[6] Passwort = Teilnehmerspezifischer Prefix „A“ || Einmalpasswort von Terravis „B“ = AB

[7] Z.B. per Post oder Fax

2.5 Technischer Meldungsfluss

Folgend ist eine Übersicht über die prozessspezifischen Meldungsflüsse gegeben.

2.5.1 Datenabfrage

Im Folgenden ist der technische Meldungsfluss im Zusammenhang mit der Datenabfrage beschrieben.

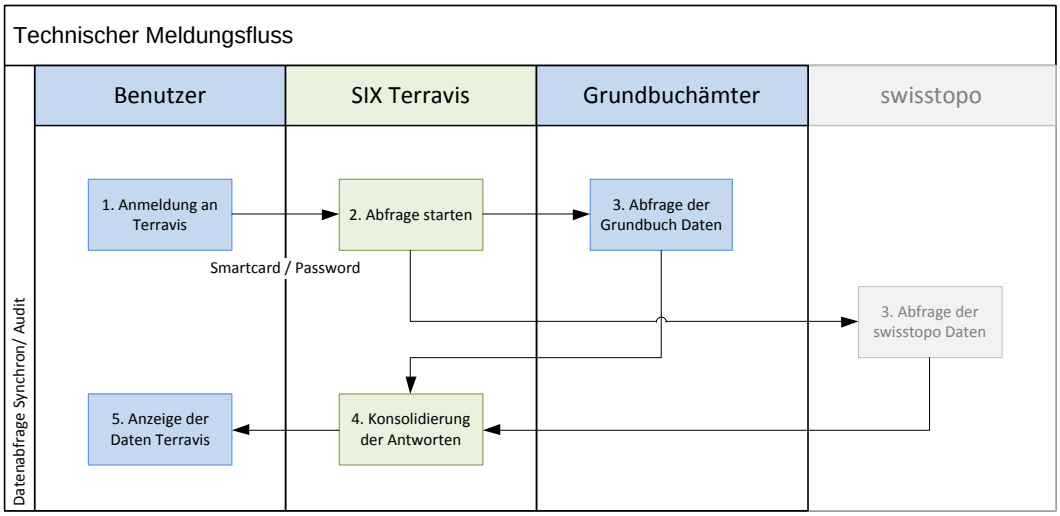


Abbildung 7

#	Beschreibung
1.	Ein Benutzer meldet sich bei Terravis an und übermittelt die Abfragekriterien, über welche er weitere Grundbuchinformationen wünscht.
2.	Terravis authentifiziert den Benutzer und verarbeitet die Anfrage.
3.	Terravis bezieht die gewünschten Informationen von den entsprechenden angebundenen Datenlieferanten.
4.	Die bezogenen Daten werden durch Terravis konsolidiert.
5.	Die Daten werden aufbereitet an den Benutzer geliefert.

2.5.2 Datenbezug

Im Folgenden ist der technische Meldungsfluss im Zusammenhang mit dem Datenbezug beschrieben.

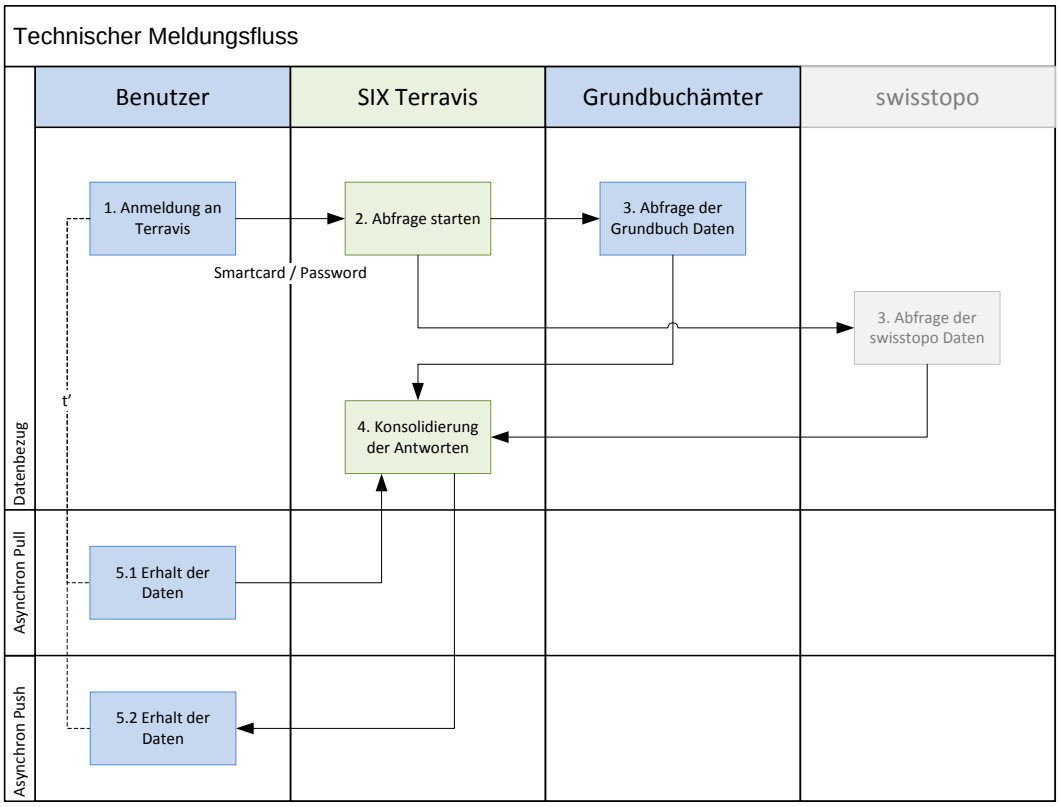


Abbildung 8

#	Beschreibung
1.	Ein Benutzer meldet sich bei Terravis an und übermittelt die Kriterien, über welche er weitere Grundbuchinformationen wünscht.
2.	Terravis authentifiziert den Benutzer und verarbeitet die Anfrage.
3.	Terravis bezieht die gewünschten Informationen von den entsprechenden angebundenen Datenlieferanten.
4.	Die bezogenen Daten werden durch Terravis konsolidiert.
5.	Die Daten werden von Terravis aufbereitet. Die Daten können wahlweise wie folgt asynchron bezogen werden. 1. Die Daten werden vom Benutzer über einen Webbrowser asynchron bei Terravis abgerufen (asynchron Pull). 2. Die Daten werden über einen Webservice von Terravis asynchron an den Benutzer geliefert (asynchron Push).

Das Grundbuch und Swisstopo vertrauen darauf, dass Terravis den Benutzer korrekt authentifiziert und autorisiert hat, bevor die Anfragen an sie weitergeleitet werden.

2.5.3 Terravis eGV Workflow

Im Folgenden ist der technische Meldungsfluss im Zusammenhang mit dem eGV und der elektronischen Signatur beschrieben.

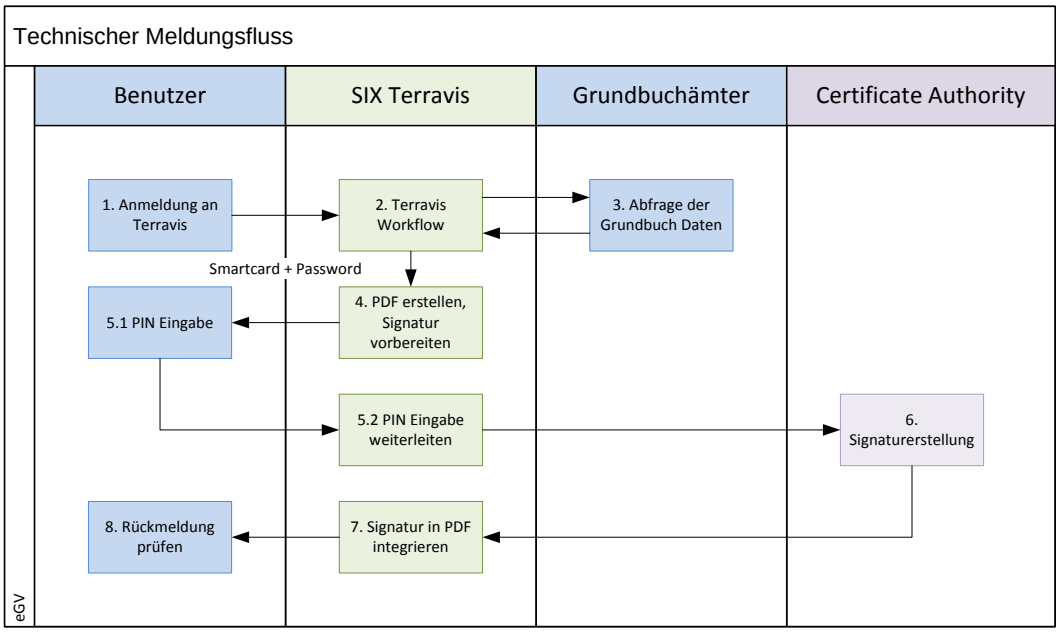


Abbildung 9

#	Beschreibung
1.	Ein Benutzer meldet sich bei Terravis an.
2.	Terravis authentifiziert den Benutzer. Anschliessend kann dieser entsprechend dem Workflow innerhalb Terravis agieren.
3.	Falls innerhalb des Workflows Informationen von Datenlieferanten benötigt werden, werden diese durch Terravis bezogen.
4.	Durch Terravis können PDF Dokumente elektronisch signiert werden. Der Signaturvorgang wird gestartet, indem der Benutzer das zu signierende Dokument innerhalb des Workflows selektiert. Vorgängig kann der Benutzer das PDF Dokumente optional öffnen und visualisieren.
5.	1. Damit der Signaturprozess ausgeführt werden kann, muss der Benutzer seinen persönlichen SuisseID PIN innerhalb des Workflows eingeben. 2. Der PIN wird innerhalb von Terravis an das Signaturmodul weitergeleitet. Der PIN wird nicht zwischengespeichert.
6.	Der bei der CA sicher gespeicherte Signaturschlüssel wird unter Verwendung des PINs des Benutzers für die Signaturerstellung freigeschaltet.

#	Beschreibung
7.	Die Signatur wird durch Terravis in das zuvor ausgewählte PDF Dokument integriert.
8.	Dem Benutzer wird der Status des Signaturvorgangs angezeigt. Er kann optional das signierte PDF Dokument öffnen und prüfen.

3 Urkundspersonen und für Urkundspersonen zuständige kantonale Stelle

Im Folgenden sind die wichtigsten organisatorischen und technischen Prozesse sowie die entsprechenden Schutzobjekte im Zusammenhang mit Urkundspersonen und für Urkundspersonen zuständige kantonale Stellen beschrieben.

3.1 Administrative Prozesse

3.1.1 Bezug einer SuisseID und eines für den zentralen Signaturserver für eGV

Bei eGV Prozessen kann ein Benutzer einzelne elektronische Dokumente über den zentralen Signaturserver von Terravis qualifiziert elektronisch signieren. Hierzu muss der Benutzer ein qualifiziertes Zertifikat nach ZertES (SuisseID) bei einer anerkannten CA beziehen. Nach Erhalt des qualifizierten Zertifikats muss dieses durch den Administrator dem jeweiligen Benutzerkonto bei Terravis zugeordnet werden.

Hinweis
Die Urkundspersonen haben auch die Möglichkeit, die Dokumente lokal auf ihrem PC unter Verwendung eines Signaturprogramms in Verbindung mit einer SuisseID Smartcard zu signieren. Die organisatorischen und technischen Prozesse im Zusammenhang mit der Verwendung einer SuisseID Smartcard sind in diesem Dokument nicht beschrieben.

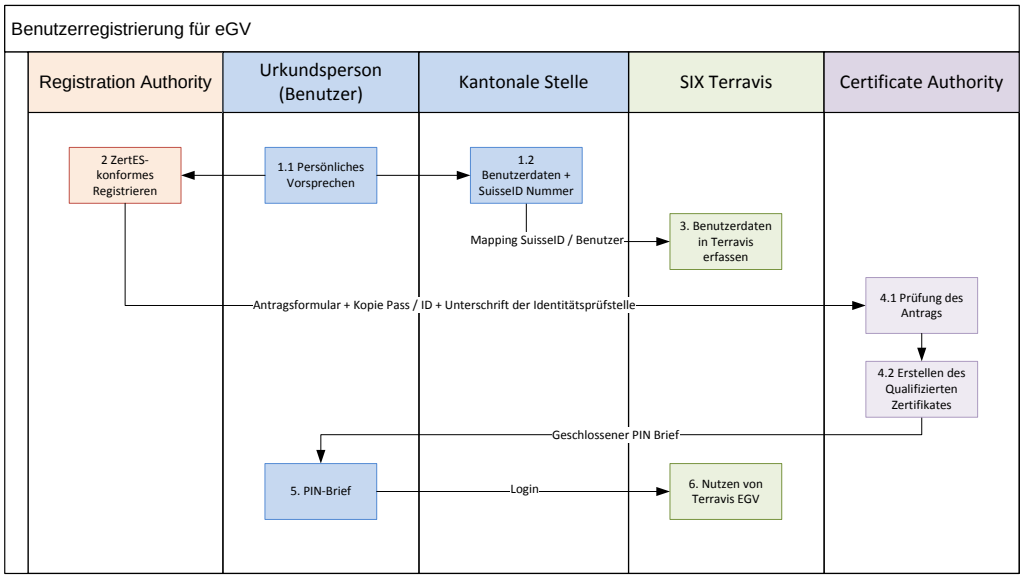


Abbildung 10

#	Beschreibung
1.	1. Damit die Urkundsperson eine SuisseID beziehen kann, muss sie bei einer Registrierstelle, unter Vorweisung eines amtlichen, gültigen Lichtbildausweises, persönlich vorsprechen. 2. Nach dem Ausfüllen des Antragformulars erhält die Urkundsperson ihre persönliche SuisseID Nummer. Diese leitet sie der für Urkundspersonen zuständige kantonale Stelle für die spätere Erfassung in Terravis weiter (siehe Schritt 3.)
3.	Die Registrierstelle prüft den Antrag der Urkundsperson und leitet die Angaben an die CA weiter.
4.	Die für Urkundspersonen zuständige kantonale Stelle erstellt in Terravis ein Benutzerkonto für die entsprechende Urkundsperson und ordnet dieser ihre SuisseID Nummer zu.
5.	1. Die CA prüft den Antrag der Urkundsperson. 2. Nach erfolgreicher Prüfung generiert die CA die Signaturschlüssel sowie das korrespondierende SuisseID Zertifikat.
6.	Die Urkundsperson erhält von der CA den PIN-Brief für die Freischaltung des zentral gespeicherten Signaturschlüssels. Falls die Urkundsperson kein organisationseigenes Authentisierungszertifikat besitzt, erhält sie zusätzlich eine Smartcard zur Authentisierung gegenüber Terravis
7.	Die Urkundsperson kann die Workflowprozesse und den zentralen Signaturserver des eGV nutzen.

3.1.2 Bezug eines Authentisierungsmerkmals

Ein Benutzer muss sich gegenüber eGV mit einem Benutzerzertifikat anmelden. Hierzu kann er ein organisationseigenes Benutzerzertifikat verwenden, das von einer internen CA ausgegeben wurde und die Anforderungen gem. Kapitel 7.1.1 erfüllt. Alternativ hierzu kann er im Rahmen des Registrierprozesses der SuisseID ein Benutzerzertifikat[8] von einer öffentlichen CA beziehen.

[8] SuisseID IAC oder ein dediziertes Benutzerzertifikat zur Authentisierung

3.2 Technische Schnittstellen

Im Folgenden sind die für Urkundspersonen und für Urkundspersonen zuständigen kantonalen Stellen relevanten technischen Schnittstellen beschrieben.

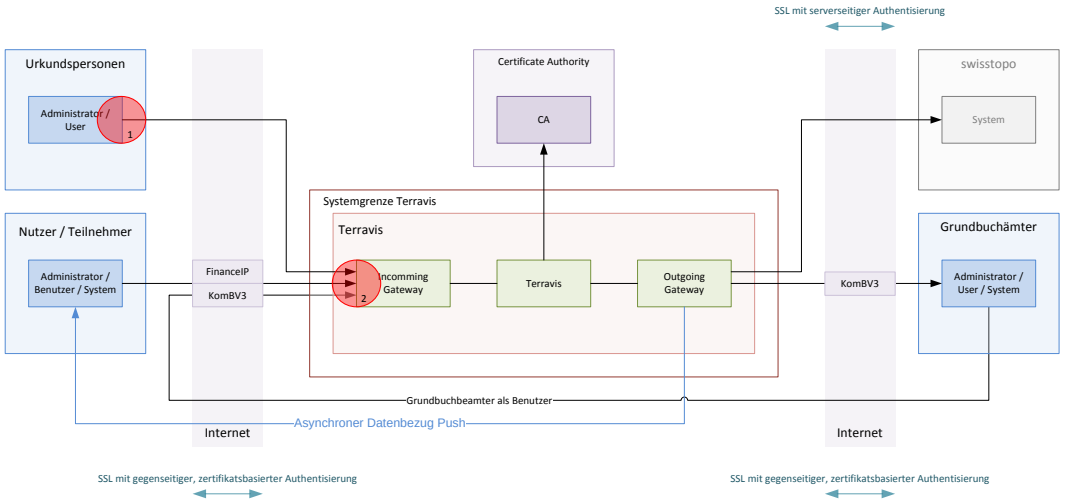


Abbildung 11

3.2.1 Ausgehende Verbindungen

Folgend sind die ausgehenden Verbindungen von Urkundspersonen und für Urkundspersonen zuständigen kantonalen Stellen beschrieben.

#	Beschreibung
1.	Webapplikation für die Administration der Administratoren, Benutzer und Auditoren. Diese Webapplikation wird von den für Urkundspersonen zuständigen kantonalen Stellen genutzt.

Schnittstellen	1, 2
Protokoll	HTML über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Browser des Administrators gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Browser des Administrators. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

#	Beschreibung
2.	Webapplikation für den eGV. Diese Webapplikation wird von den Urkundspersonen genutzt.

Schnittstellen	1, 2
Protokoll	HTML über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Browser des Benutzers gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Browser des Benutzers. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

3.3 Verantwortlichkeiten

Die Urkundspersonen haben Zugriff auf Grundbuchinformationen und können elektronische Dokumente innerhalb oder ausserhalb des Terravis Workflows signieren. Die für Urkundspersonen zuständigen kantonalen Stellen erfassen und administrieren die Benutzerkonten der Urkundspersonen in Terravis. Die folgenden Punkte liegen diesbezüglich in der Verantwortung der Urkundspersonen resp. der für Urkundspersonen zuständigen kantonalen Stellen:

a) Abschliessen von Verträgen und Nutzungsbestimmungen im Zusammenhang mit der Nutzung von Terravis. Die Vertragsparteien sind Terravis und Urkundspersonen resp. die für Urkundspersonen zuständigen kantonalen Stellen.

b) Verwaltung der eigenen Stammdaten in Terravis.

c) Verwaltung der Administratoren und Benutzer inkl. der jeweiligen Rechte in Terravis.

d) Sicheres Handhaben und Verwalten der von Terravis bezogenen Informationen (Grundbuchinformationen, Kundeninformationen, Belege, Formulare, Anträge, Benutzerinformationen, Auditeinträge, etc.)

e) Entsprechend den jeweiligen Nutzungsvorschriften sichere Handhabung und Verwaltung des SuisseID PIN und der SuisseID (siehe Schutzobjekt S1, S2).

f) Entsprechend den jeweiligen Nutzungsvorschriften sichere Handhabung und Verwaltung des Authentisierungsmerkmals im Zusammenhang mit der Authentisierung gegenüber Terravis (siehe Schutzobjekt S4, S5).

g) Erstellen von Arbeitsanweisungen im Zusammenhang mit der Nutzung von Terravis. Die Einhaltung der Arbeitsanweisungen ist zu überwachen.

h) Sicherer Betrieb der eigenen IT-Infrastruktur und Applikationen.

Weitere Verantwortlichkeiten sind bei den untenstehenden Schutzobjekten beschrieben.

3.4 Leitlinien zur Identifizierung von Schutzobjekten

Die jeweiligen Parteien sind eigenständig verantwortlich für alle technischen und organisatorischen Prozesse sowie für alle Systemkomponenten, die sich innerhalb ihrer jeweiligen Systemgrenze befinden (siehe Kapitel 2.1 und 2.2).

Im Folgenden sind beispielhaft die wichtigsten, Terravis spezifischen Schutzobjekte aus Sicht der einzelnen Parteien beschrieben. Es handelt sich hierbei um Vorschläge zur Identifizierung und Bewertung der jeweiligen Schutzobjekte.

Hinweis
Die Liste der Schutzobjekte ist beispielhaft und nicht abschliessend. Die jeweiligen Parteien sind alleinig dafür verantwortlich, ihre eigenen Schutzobjekte sowie deren Abhängigkeiten zu identifizieren und diese entsprechend zu bewerten. Es liegt auch in der alleinigen Verantwortung der jeweiligen Parteien, den Schutz der entsprechenden Objekte über geeignete Massnahmen sicherzustellen.

Die Schutzobjekte sind kategorisiert nach ihrem Schutzbedarf[9].

Schutzbedarf	Beschreibung
Normaler Schutzbedarf	Die Schadensauswirkungen sind begrenzt und überschaubar
Hoher Schutzbedarf	Die Schadensauswirkungen können beträchtlich sein
Sehr hoher Schutzbedarf	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmass erreichen

[9] BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5

3.4.1 Signaturerstellung und Signaturprüfung mit der SuisseID

Die SuisseID wird verwendet, um Daten nach den Vorgaben des Schweizerischen Signaturgesetztes elektronisch zu signieren. Sie muss entsprechend im Rahmen der Bestimmungen des ZertES[10] verwendet werden. Folgend sind nicht abschliessend wichtige Schutzobjekte und Verantwortlichkeiten aus Sicht der Urkundspersonen resp. der für Urkundspersonen zuständigen kantonalen Stellen aufgeführt.

S1.	PIN-Brief und PIN für die SuisseID			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen			
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang des PIN-Briefs und dem PIN für die SuisseID beschrieben: a) Der PIN für die Freischaltung des Signaturschlüssels muss unter alleiniger Kontrolle des jeweiligen Benutzers sein. Somit muss der Benutzer den PIN-Brief der CA in ungeöffnetem Zustand erhalten haben. b) Der initiale PIN sollte bei der ersten Verwendung der SuisseID geändert werden. c) Bei Verlust oder Diebstahl des SuisseID PINs muss der Benutzer so rasch wie möglich die Ungültigerklärung der jeweiligen SuisseID Zertifikate bei der entsprechenden CA beantragen. Falls der entsprechende Benutzer den zentralen Signaturserver von Terravis nutzt, sollte er zusätzlich so rasch wie möglich veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird (für den Fall, dass die Sperrung seitens CA doch was länger dauert).		
S2.	Verwendung der SuisseID			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	1, 2		
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang mit der SuisseID beschrieben: a) Beim Signiervorgang ist darauf zu achten, dass vorgängig der Inhalt der zu unterzeichneten Daten auf Richtigkeit und Vollständigkeit hin überprüft wird. b) Beim Signaturprüfungsvorgang ist darauf zu achten, dass die Signatur zuverlässig überprüft und das Ergebnis der Prüfung korrekt angezeigt wird. Zudem soll der Benutzer, bei Bedarf, den Inhalt der unterzeichneten Daten zuverlässig feststellen können. c) Das mit der SuisseID signierte elektronische Dokument entspricht dem rechtsgültigen Dokument mit Rechtswirkung. Ein Papierausdruck des Dokumentes kann erstellt werden, dieser hat jedoch keine Rechtswirkung. d) Bei Verlust oder Diebstahl der SuisseID oder des zugehörigen PIN, muss der Benutzer so rasch wie möglich dessen Ungültigerklärung bei der CA beantragen. Falls der entsprechende Benutzer den zentralen Signaturserver von Terravis nutzt, sollte er zusätzlich so rasch wie möglich veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird. e) Falls ein auf den Benutzer bezogenes Attribut im SuisseID Zertifikat nicht mehr zutreffend ist, muss er die Ungültigerklärung des entsprechenden Zertifikats bei der CA beantragen.		

[10] [ZertES], [VZertES]

		f) Die für Urkundspersonen zuständige kantonale Stelle, welche berufsbezogene Attribute oder sonstige Angaben zum Benutzer bestätigt hat, ist verpflichtet, ein SuisseID Zertifikat beim jeweiligen Zertifizierungsdiensteanbieter (CA) sperren lassen, falls das entsprechende Attribut nicht mehr zutreffend ist oder der Benutzer nicht weiter im Rahmen von Terravis aktiv sein soll.

3.4.2 Authentisierungsmerkmale

Über die Authentisierungsmerkmale authentisieren sich Benutzer oder Systeme gegenüber Terravis. Sie sind persönlich oder systemspezifisch und dürfen nicht an Dritte weitergegeben werden.

Die Authentisierungsmerkmale sind die Basis für die Authentizität der Kommunikationsteilnehmer sowie für die Integrität und Vertraulichkeit der Daten über das Internet.

Hinweis
Das Eingangsportal von Terravis authentifiziert die Teilnehmer alleinig durch das Authentisierungsmerkmal. Standortbezogene Informationen wie beispielsweise der Zugang über FinanceIP wird nicht in die Authentifizierung der Benutzer miteinbezogen. Sofern die Benutzer die Authentisierungsmerkmale auf sich tragen[11], können sie sich auch ausserhalb der Organisation in Terravis einloggen. Der jeweilige Nutzer ist verantwortlich für seine Benutzer und muss entsprechende Weisungen im Umgang mit den Authentisierungsmerkmalen und der Nutzung von Terravis erlassen.

3.4.2.1 Administration von Administratoren und Benutzern

Die für Urkundspersonen zuständige kantonale Stelle verwaltet die Konten für Administratoren und Benutzer in Terravis. Die jeweiligen Administratoren authentisieren sich mit ihrem persönlichen Authentifizierungszertifikat gegenüber Terravis.

#	Beschreibung		
S3.	Benutzerspezifisches X.509 Zertifikat für die Administration		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen	1, 8	
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang mit dem Authentisierungsmerkmal beschrieben: a) Das Authentisierungsmerkmal ist ein SuisseID IAC oder ein organisationseigenes X.509 Zertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). b) Bei Verlust oder Diebstahl des Authentisierungsmerkmals oder des zugehörigen PINs, muss der Benutzer so rasch wie möglich veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird. Zusätzlich muss der Benutzer die Ungültigerklärung seines Authentifizierungszertifikats bei seiner CA beantragen.	

[11] Beispielsweise SuisseID Smartcard

3.4.2.2 Datenabfrage und eGV

Um die Prozesse im Zusammenhang mit der Datenabfrage oder eGV zu nutzen, muss sich die Urkundsperson über Benutzername / Passwort oder mit ihrem persönlichen Authentifizierungszertifikat gegenüber Terravis authentisieren.

#	Beschreibung		
S4.	Username / Passwort für die Datenabfrage		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen	1, 2	
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang mit Username / Passwort beschrieben: a) Das Passwort ist persönlich und darf nicht an Dritte weitergegeben werden. b) Das Initiale Passwort muss nach dem ersten Login geändert werden. c) Der Benutzer muss sein Passwort ändern, falls er den begründeten Verdacht hat, dass ein Dritter Kenntnis davon erlangt hat. Alternativ hierzu kann er so rasch wie möglich über seinen jeweiligen Administrator veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird.	
S5.	Benutzerspezifisches X.509 Zertifikat für die Datenabfrage und eGV		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen	1, 2	
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang mit dem Authentisierungsmerkmal beschrieben: a) Das Authentisierungsmerkmal ist ein SuisseID IAC oder ein organisationseigenes X.509 Zertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). b) Bei Verlust oder Diebstahl des Authentisierungsmerkmals oder des zugehörigen PINs, muss der Benutzer so rasch wie möglich veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird. Zusätzlich muss der Benutzer die Ungültigerklärung seines Authentifizierungszertifikats bei seiner CA beantragen.	

3.4.3 Terravis bezogene Informationen

Terravis bezogene Informationen enthalten öffentliche und eingeschränkt öffentliche Informationen. Der Benutzer trägt nach Empfang der Informationen die Verantwortung über deren weiteren Verwendung. Die Terravis bezogenen Informationen sind vertraulich im Rahmen des jeweiligen Geschäftsfalles zu verwenden.

#	Beschreibung		
S6.	Grundbuchinformationen		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen		
	Bemerkung	Terravis bezogene Informationen sind u.a. Grundbuchinformationen, Kundeninformationen, Belege, Formulare, Anträge, Benutzerinformationen, Auditeinträge, etc.	

3.4.4 IT-Systeme

Der Datenaustausch erfolgt über Webapplikationen und Webservices. Der Nutzer trägt die Verantwortung über alle seine IT-Systeme, die im Zusammenhang mit Terravis genutzt werden.

#	Beschreibung			
S7.	Verfügbarkeit			
	Kategorie	Normaler Schutzbedarf		
	Schnittstellen			
	Bemerkung	Die Verfügbarkeit der IT-Systeme liegt im Interesse des jeweiligen Nutzers.		
S8.	Schutz vor Schadsoftware			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	1		
	Bemerkung	Der Nutzer ist eigenständig dafür verantwortlich, dass die von Terravis bezogenen Informationen sowie die an Terravis übermittelten Informationen auf Schadsoftware hin untersucht und bei Bedarf entfernt werden.		
S9.	Schutz vor unbefugtem Zugriff			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	1		
	Bemerkung	Der Nutzer ist eigenständig dafür verantwortlich, nur berechtigten Personen oder Systemen den Zugriff auf seine Infrastruktur zu gewähren[12]. Im Weiteren ist der Nutzer eigenständig dafür verantwortlich, seine Systeme vor jeglichen Angriffen aus dem Internet zu schützen. Dies beinhaltet u.a. auch die strukturelle Prüfung der maschinell auswertbaren Informationen auf Protokoll- und Datenebene. **Hinweis:** Wer sich gegenüber Terravis mit einem gültigen Authentisierungsmerkmal authentisiert, gilt Terravis gegenüber als Berechtigter zur Benützung der entsprechenden Dienstleistung. Terravis wird ohne weitere Überprüfung seiner Berechtigung die jeweiligen Abfragen und Aufträge tätigen, auch wenn es sich bei der Person oder dem System nicht um den tatsächlich berechtigten Benutzer oder Nutzer handelt.		

[12] Beispielsweise durch korrekte Prüfung des SSL Server- resp. Clientzertifikats von Terravis

4 Institutionelle Kunden

Im Folgenden sind die wichtigsten organisatorischen und technischen Prozesse sowie die entsprechenden Schutzobjekte im Zusammenhang mit den institutionellen Kunden beschrieben.

4.1 Administrative Prozesse

4.1.1 Bezug einer SuisseID für den zentralen Signaturserver für eGV

Bei eGV Prozessen kann ein Benutzer einzelne elektronische Dokumente über den zentralen Signaturserver von Terravis qualifiziert elektronisch signieren. Hierzu muss der Benutzer ein qualifiziertes Zertifikat nach ZertES (SuisseID) bei einer anerkannten CA beziehen. Nach Erhalt des qualifizierten Zertifikats muss dieses durch den Administrator dem jeweiligen Benutzerkonto bei Terravis zugeordnet werden.

Hinweis
Das im Signaturzertifikat enthaltene O Feld[13] muss den Name der Organisation beinhalten. Diese muss durch die Organisation entsprechend bestätigt werden.

Der Benutzer muss sich gegenüber eGV mit einem Benutzerzertifikat anmelden. Hierzu kann er ein organisationseigenes Benutzerzertifikat verwenden, das von einer internen CA ausgegeben wurde und die Anforderungen gem. Kapitel 7.1.1 erfüllt. Alternativ hierzu kann er im Rahmen des Registrierprozesses der SuisseID ein Benutzerzertifikat[14] von einer öffentlichen CA beziehen.

[13] Subject RDN O

[14] SuisseID IAC oder ein dediziertes Benutzerzertifikat zur Authentisierung

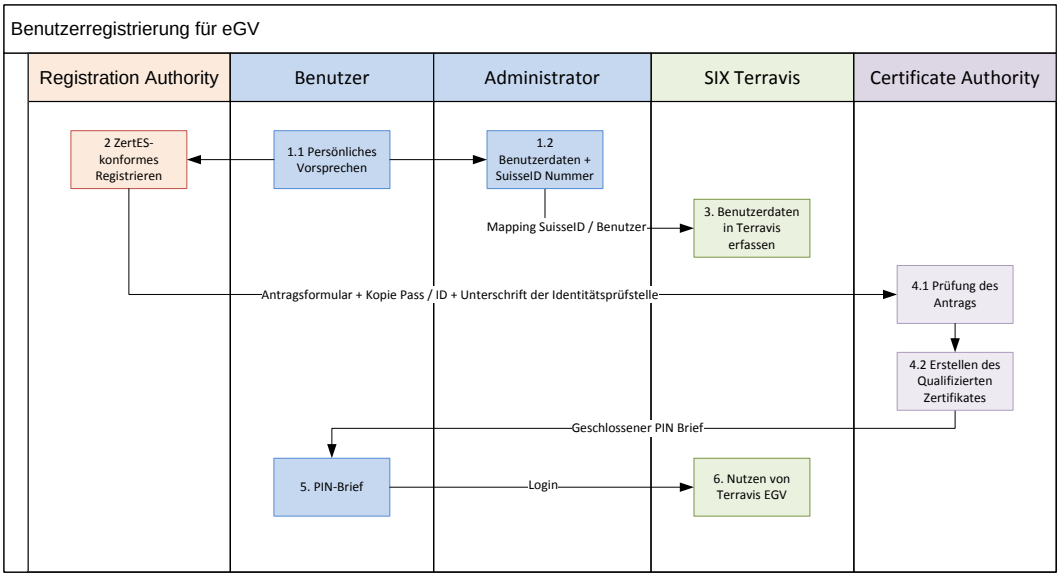


Abbildung 12

#	Beschreibung
1.	1. Damit der Benutzer eine SuisseID beziehen kann, muss er bei einer Registrierstelle, unter Vorweisung eines amtlichen, gültigen Lichtbildausweises, persönlich vorsprechen. 2. Nach dem Ausfüllen des Antragformulars erhält der Benutzer seine persönliche SuisseID Nummer. Diese leitet er dem Administrator für die spätere Erfassung in Terravis weiter (siehe Schritt 3.)
2.	Die Registrierstelle prüft den Antrag des Benutzers und leitet die Angaben an die CA weiter.
3.	Der Administrator erstellt in Terravis ein Benutzerkonto für den entsprechenden Benutzer und ordnet diesem seine SuisseID Nummer zu.
4.	1. Die CA prüft den Antrag des Benutzers. 2. Nach erfolgreicher Prüfung generiert die CA die Signaturschlüssel sowie das korrespondierende SuisseID Zertifikat.
5.	Der Benutzer erhält von der CA den PIN-Brief für die Freischaltung des zentral gespeicherten Signaturschlüssels. Falls der Benutzer kein organisationseigenes Authentisierungszertifikat besitzt, erhält er zusätzlich eine Smartcard zur Authentisierung gegenüber Terravis.
6.	Der Benutzer kann die Workflowprozesse und den zentralen Signaturserver des eGV nutzen.

4.1.2 Bezug eines Authentisierungsmerkmals

Zur Authentisierung gegenüber dem Terravis eGV muss ein Authentifizierungszertifikat verwendet werden. Dieses kann optional im Rahmen des Registrierprozesses der SuisseID ebenfalls bei der entsprechenden CA bezogen werden. Alternativ, unter Berücksichtigung der Anforderungen gem. Kapitel 7.1, kann der Administrator oder der Benutzer das Authentifizierungszertifikat bei einer öffentlichen oder internen CA beziehen.

4.2 Technische Schnittstellen

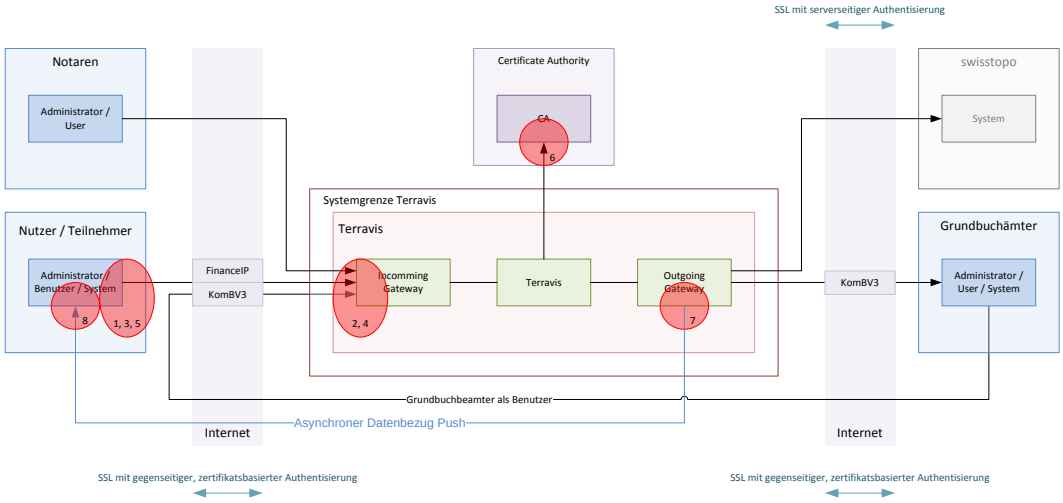


Abbildung 13

4.2.1 Ausgehende Verbindungen von den Nutzern

Folgend sind die ausgehenden Verbindungen von den Nutzern beschrieben.

#	Beschreibung
1.	Webapplikation für die Administration der Administratoren, Benutzer und Auditoren.

Schnittstellen	1, 2
Protokoll	HTML über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Browser des Benutzers gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Browser des Benutzers. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

#	Beschreibung
2.	Webservice für die Administration der Administratoren, Benutzer und Auditoren

Schnittstellen	3, 4
Protokoll	SOAP über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Server des Nutzers gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Server des Nutzers. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

3.	Webapplikation für die Abfrage von Grundbuchinformationen

Schnittstellen	1, 2
Protokoll	HTML über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Browser des Benutzers gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). ▪ Passwortbasierte Authentisierung vom Browser des Benutzers gegenüber dem Terravis Server. **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Browser des Benutzers. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

4.	Webservice für die Abfrage von Grundbuchinformationen

Schnittstellen	3, 4
Protokoll	SOAP über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Server des Nutzers gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Server des Nutzers. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

#	Beschreibung
5.	Webapplikation für den eGV

Schnittstellen	1, 2
Protokoll	HTML über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Browser des Benutzers gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Browser des Benutzers. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

#	Beschreibung
6.	Signieren von Dokumenten mit der SuisseID innerhalb des eGV

Schnittstellen	5, 6
Protokoll	HTML über https vom Benutzer zu Terravis[15].
Authentisierung	Das Signieren von Dokumenten erfolgt im Rahmen eines Workflows innerhalb des eGV. Die hierfür notwendige vorgängige Authentisierung erfolgt gemäss oben beschriebenen Schritt 5. **Nutzer (Client)** ▪ Benutzer PIN Eingabe zur Freischaltung des Signaturschlüssels.

4.2.2 Eingehende Verbindungen zu den Nutzern

Folgend sind die eingehenden Verbindungen zu den Nutzern beschrieben.

#	Beschreibung
1.	Webservice für das Hochladen von Grundbuchinformationen (asynchroner Datenbezug Push)

Schnittstellen	7, 8
Protokoll	SOAP über https
Authentisierung	**Terravis (Client)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Server des Nutzers. Die Authentisierung erfolgt über ein SSL Clientzertifikat gemäss Kapitel 7.1.1. **Nutzer (Server)** ▪ Zertifikatsbasierte Authentisierung vom Server des Nutzers gegenüber Terravis. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

[15] Schnittstelle 1, 2

4.3 Verantwortlichkeiten

Die institutionellen Kunden verwalten entsprechend den jeweiligen Nutzungsvorschriften ihre Benutzer und Administratoren, haben Zugriff auf Grundbuchinformationen und können elektronische Dokumente innerhalb des Terravis Workflows signieren. Die folgenden Punkte liegen diesbezüglich in der Verantwortung der institutionellen Kunden:

a) Abschliessen von vertraglichen Vereinbarungen und Nutzungsbestimmungen im Zusammenhang mit der Nutzung von Terravis. Die Vertragsparteien sind die institutionellen Kunden und Terravis.

b) Verwaltung der eigenen Stammdaten in Terravis.

c) Verwaltung (inkl. allfälliger Sperrung) der Administratoren und Benutzer inkl. der jeweiligen Rechte in Terravis.

d) Sicheres Handhaben, Verwalten und Kontrollieren der von Terravis bezogenen Informationen (Grundbuchinformationen, Kundeninformationen, Belege, Formulare, Anträge, Benutzerinformationen, Auditeinträge, etc.)

e) Sichere Handhabung und Verwaltung des SuisseID PINs und der SuisseID.

f) Sichere Handhabung und Verwaltung des Authentisierungsmerkmals im Zusammenhang mit der Authentisierung gegenüber Terravis.

g) Erstellen von Arbeitsanweisungen im Zusammenhang mit der Nutzung von Terravis. Die Einhaltung der Arbeitsanweisungen ist zu überwachen.

h) Sichere Integration und Betrieb der eigenen IT-Infrastrukturen und Applikationen.

Weitere Verantwortlichkeiten sind bei den untenstehenden Schutzobjekten beschrieben.

4.4 Leitlinien zur Identifizierung von Schutzobjekten

Die jeweiligen Parteien sind eigenständig verantwortlich für alle technischen und organisatorischen Prozesse sowie für alle Systemkomponenten, die sich innerhalb ihrer jeweiligen Systemgrenze befinden (siehe Kapitel 2.1).

Im Folgenden sind beispielhaft die wichtigsten Schutzobjekte aus Sicht der einzelnen Parteien beschrieben. Es handelt sich hierbei um Vorschläge zur Identifizierung und Bewertung der jeweiligen Schutzobjekte.

Hinweis
Die Liste der Schutzobjekte ist beispielhaft und nicht abschliessend. Die jeweiligen Parteien sind alleinig dafür verantwortlich, ihre eigenen Schutzobjekte sowie deren Abhängigkeiten zu identifizieren und diese entsprechend zu bewerten. Es liegt auch in der alleinigen Verantwortung der jeweiligen Parteien, den Schutz der entsprechenden Objekte über geeignete Massnahmen sicherzustellen.

Die Schutzobjekte sind kategorisiert nach ihrem Schutzbedarf[16].

Schutzbedarf	Beschreibung
Normaler Schutzbedarf	Die Schadensauswirkungen sind begrenzt und überschaubar
Hoher Schutzbedarf	Die Schadensauswirkungen können beträchtlich sein
Sehr hoher Schutzbedarf	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmass erreichen

[16] BSI-Standard 100-1: Managementsysteme für Informationssicherhei (ISMS), Version 1.5

4.4.1 Signaturerstellung und Signaturprüfung mit der SuisseID

Die SuisseID wird verwendet, um Daten nach den Vorgaben des Schweizerischen Signaturgesetztes elektronisch zu signieren. Sie muss entsprechend im Rahmen der Bestimmungen des ZertES[17] verwendet werden. Folgend sind nicht abschliessend wichtige Schutzobjekte und Verantwortlichkeiten aus Sicht der Nutzer und Benutzer aufgeführt.

S1.	PIN-Brief und PIN für die SuisseID	
	Kategorie	Hoher Schutzbedarf
	Schnittstellen	
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang des PIN-Briefs und dem PIN für die SuisseID beschrieben: a) Der PIN für die Freischaltung des Signaturschlüssels muss unter alleiniger Kontrolle des jeweiligen Benutzers sein. Somit muss der Benutzer den PIN-Brief der CA in ungeöffnetem Zustand erhalten haben. b) Der initiale PIN sollte bei der ersten Verwendung der SuisseID geändert werden. c) Bei Verlust oder Diebstahl des SuisseID PINs muss der Benutzer so rasch wie möglich die Ungültigerklärung der jeweiligen SuisseID Zetifikate bei der entsprechenden CA beantragen. Falls der entsprechende Benutzer den zentralen Signaturserver von Terravis nutzt, sollte er zusätzlich so rasch wie möglich veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird.
S2.	Verwendung der SuisseID	
	Kategorie	Hoher Schutzbedarf
	Schnittstellen	1, 2
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang mit der SuisseID beschrieben: a) Beim Signiervorgang ist darauf zu achten, dass vorgängig der Inhalt der zu unterzeichneten Daten auf Richtigkeit und Vollständigkeit hin überprüft wird. b) Beim Signaturprüfungsvorgang ist darauf zu achten, dass die Signatur zuverlässig überprüft und das Ergebnis der Prüfung korrekt angezeigt wird. Zudem soll der Benutzer, bei Bedarf, den Inhalt der unterzeichneten Daten zuverlässig feststellen können. c) Das mit der SuisseID signierte elektronische Dokument entspricht dem rechtsgültigen Dokument mit Rechtswirkung. Ein Papierausdruck des Dokumentes kann erstellt werden, dieser hat jedoch keine Rechtswirkung. d) Bei Verlust oder Diebstahl der SuisseID oder des zugehörigen PINs, muss der Benutzer so rasch wie möglich dessen Ungültigerklärung bei der CA beantragen. Falls der entsprechende Benutzer den zentralen Signaturserver von Terravis nutzt, sollte er zusätzlich so rasch wie möglich veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird. e) Falls ein auf den Benutzer bezogenes Attribut im SuisseID Zertifikat nicht mehr zutreffend ist, muss er die Ungültigerklärung des entsprechenden Zertifikats bei der CA beantragen. f) Die für zuständige Stelle, welche berufsbezogene Attribute oder sonstige

[17] [ZertES], [VZertES]

		Angaben zum Benutzer bestätigt hat, ist verpflichtet, ein SuisseID Zertifikat beim jeweiligen Zertifizierungsdiensteanbieter (CA) sperren lassen, falls das entsprechende Attribut nicht mehr zutreffend ist oder der Benutzer nicht weiter im Rahmen von Terravis aktiv sein soll.

4.4.2 Authentisierungsmerkmale

Über die Authentisierungsmerkmale authentisieren sich Benutzer oder Systeme gegenüber Terravis. Sie sind persönlich oder systemspezifisch und dürfen nicht an Dritte weitergegeben werden.

Die Authentisierungsmerkmale sind die Basis für die Authentizität der Kommunikationsteilnehmer sowie für die Integrität und Vertraulichkeit der Daten über das Internet.

Hinweis
Das Eingangsportal von Terravis authentifiziert die Teilnehmer alleinig durch das Authentisierungsmerkmal. Standortbezogene Informationen wie beispielsweise der Zugang über FinanceIP wird nicht in die Authentifizierung der Benutzer miteinbezogen. Sofern die Benutzer die Authentisierungsmerkmale auf sich tragen[18], können sie sich auch ausserhalb der Organisation in Terravis einloggen. Der jeweilige Nutzer ist verantwortlich für seine Benutzer und muss entsprechende Weisungen im Umgang mit den Authentisierungsmerkmalen und der Nutzung von Terravis erlassen.

4.4.2.1 Administration von Administratoren und Benutzern

Die institutionellen Kunden verwalten ihre Konten für Administratoren und Benutzer eigenständig in Terravis. Die jeweiligen Administratoren authentisieren sich mit ihrem Authentifizierungszertifikat gegenüber Terravis.

#	Beschreibung	
S3.	Benutzerspezifisches X.509 Zertifikat für die Administration	
	Kategorie	Hoher Schutzbedarf
	Schnittstellen	1, 2
	Bemerkung	SuisseID IAC oder ein organisationseigenes X.509 Zertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1).
S4.	Systemspezifisches X.509 Zertifikat für die Administration	
	Kategorie	Hoher Schutzbedarf
	Schnittstellen	3, 4
	Bemerkung	Organisationseigenes X.509 Zertifikat für Server (siehe Kapitel 7.1.1)

[18] Beispielsweise SuisseID Smartcard

4.4.2.2 Datenabfrage und eGV

Um die Prozesse im Zusammenhang mit der Datenabfrage oder eGV zu nutzen, muss sich der Benutzer über Benutzername / Passwort oder mit seinem persönlichen Authentifizierungszertifikat gegenüber Terravis authentisieren.

#	Beschreibung		
S5.	Username / Passwort für die Datenabfrage		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen	1, 2	
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang mit Username / Passwort beschrieben: a) Das Passwort ist persönlich und darf nicht an Dritte weitergegeben werden. b) Das Initiale Passwort muss nach dem ersten Login geändert werden. c) Der Benutzer muss sein Passwort ändern, falls er den begründeten Verdacht hat, dass ein Dritter Kenntnis davon erlangt hat. Alternativ hierzu kann er so rasch wie möglich über seinen jeweiligen Administrator veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird.	
S6.	Benutzerspezifisches X.509 Zertifikat für die Datenabfrage und eGV		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen	1, 2	
	Bemerkung	Folgend sind die wichtigsten Punkte im Umgang mit dem Authentisierungsmerkmal beschrieben: a) Das Authentisierungsmerkmal ist ein SuisseID IAC oder ein organisationseigenes X.509 Zertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). b) Bei Verlust oder Diebstahl des Authentisierungsmerkmals oder des zugehörigen PINs, muss der Benutzer so rasch wie möglich veranlassen, dass sein Benutzerkonto bei Terravis gesperrt wird. Zusätzlich muss der Benutzer die Ungültigerklärung seines Authentifizierungszertifikats bei seiner CA beantragen.	

4.4.2.3 Webservice asynchroner Datenbezug Push

Für den asynchronen Datenbezug müssen sich die Systeme gegenseitig über ein systemspezifisches Zertifikat authentisieren.

#	Beschreibung		
S7.	Systemspezifisches X.509 Serverzertifikat		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen	7, 8	
	Bemerkung	Organisationseigenes X.509 Zertifikat (siehe Kapitel 7.1.1)	

4.4.3 Terravis bezogene Informationen

Terravis bezogene Informationen enthalten öffentliche und eingeschränkt öffentliche Informationen. Der Benutzer trägt nach Empfang der Informationen die Verantwortung über deren weiteren Verwendung. Die Terravis bezogenen Informationen sind vertraulich im Rahmen des jeweiligen Geschäftsfalles zu verwenden.

#	Beschreibung		
S8.	Grundbuchinformationen		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen		
	Bemerkung	Terravis bezogene Informationen sind u.a. Grundbuchinformationen, Kundeninformationen, Belege, Formulare, Anträge, Benutzerinformationen, Auditeinträge, etc.	

4.4.4 IT-Systeme

Der Datenaustausch erfolgt über Webapplikationen und Webservices. Der Nutzer trägt die Verantwortung über die IT-Systeme, die im Zusammenhang mit Terravis genutzt werden.

#	Beschreibung			
S9.	Verfügbarkeit der IT-Systeme			
	Kategorie	Normaler Schutzbedarf		
	Schnittstellen			
	Bemerkung	Die Verfügbarkeit der IT-Systeme liegt im Interesse des jeweiligen Nutzers.		
S10.	Schutz vor Schadsoftware			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	1, 3, 5, 8		
	Bemerkung	Der Nutzer ist eigenständig dafür verantwortlich, dass die von Terravis bezogenen Informationen sowie die an Terravis übermittelten Informationen auf Schadsoftware hin untersucht und bei Bedarf entfernt werden.		
S11.	Schutz vor unbefugtem Zugriff			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	1, 3, 5, 8		
	Bemerkung	Der Nutzer ist eigenständig dafür verantwortlich, nur berechtigten Personen oder Systemen den Zugriff auf seine Infrastruktur zu gewähren[19]. Im Weiteren ist der Nutzer eigenständig dafür verantwortlich, seine Systeme vor jeglichen Angriffen aus dem Internet zu schützen. Dies beinhaltet u.a. auch die strukturelle Prüfung der maschinell auswertbaren Informationen auf Protokoll- und Datenebene. **Hinweis:** Wer sich gegenüber Terravis mit einem gültigen Authentisierungsmerkmal authentisiert, gilt Terravis gegenüber als Berechtigter zur Benützung der entsprechenden Dienstleistung. Terravis wird ohne weitere Überprüfung seiner Berechtigung die jeweiligen Abfragen und Aufträge tätigen, auch wenn es sich bei der Person oder dem System nicht um den tatsächlich berechtigten Benutzer oder Nutzer handelt.		

[19] Beispielsweise durch korrekte Prüfung des SSL Server- resp. Clientzertifikats von Terravis

5 Grundbuchämter

Im Folgenden sind die wichtigsten organisatorischen und technischen Prozesse sowie die entsprechenden Schutzobjekte im Zusammenhang mit den Grundbuchämtern beschrieben.

5.1 Administrative Prozesse

5.1.1 Bezug eines Authentisierungsmerkmals

Zur Authentisierung gegenüber dem Terravis eGV muss ein Authentifizierungszertifikat verwendet werden. Dieses kann optional im Rahmen des Registrierprozesses der SuisseID ebenfalls bei der entsprechenden CA bezogen werden. Alternativ, unter Berücksichtigung der Anforderungen gem. Kapitel 7.1, kann der Administrator oder der Benutzer das Authentifizierungszertifikat bei einer öffentlichen oder internen CA beziehen.

5.2 Technische Schnittstellen

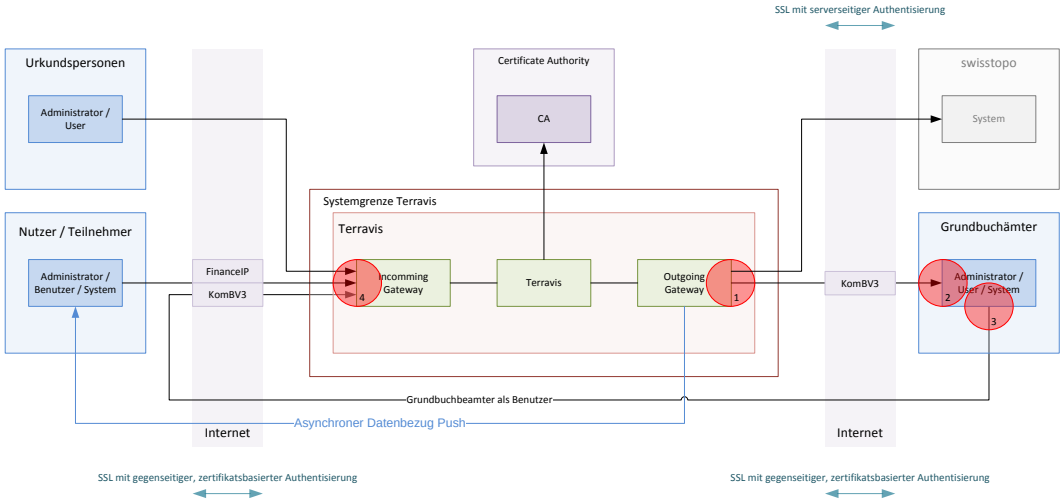


Abbildung 14

5.2.1 Eingehende Verbindungen

Folgend sind die eingehenden Verbindungen zu einem Grundbuchamt beschrieben.

#	Beschreibung
1.	Webservice für den Bezug von Daten beim Grundbuchamt

Schnittstellen	1, 2
Protokoll	SOAP über https
Authentisierung	**Grundbuchamt (Server)** ▪ Zertifikatsbasierte Authentisierung vom Grundbuchamt gegenüber dem Terravis Server. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.1. **Terravis (Client)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Server des jeweiligen Grundbuches. Die Authentisierung erfolgt über ein SSL Clientzertifikat gemäss Kapitel 7.1.2.

5.2.2 Ausgehende Verbindungen

Folgend sind die ausgehenden Verbindungen von Grundbuchämtern beschrieben.

#	Beschreibung
1.	Webapplikation für die Administration der Administratoren, Benutzer und Auditoren.

Schnittstellen	3, 4
Protokoll	HTML über https
Authentisierung	**Nutzer (Client)** ▪ Zertifikatsbasierte Authentisierung vom Browser des Administrators gegenüber dem Terravis Server. Die Authentisierung erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1). **Terravis (Server)** ▪ Zertifikatsbasierte Authentisierung vom Terravis Server gegenüber dem Browser des Administrators. Die Authentisierung erfolgt über ein SSL Serverzertifikat gemäss Kapitel 7.1.2.

5.3 Verantwortlichkeiten

Die Grundbuchämter[20] haben entsprechend den jeweiligen Nutzungsvorschriften Zugriff auf Auditlogs, die Transaktionen im Zusammenhang mit dem jeweiligen Grundbuchamt aufzeichnen. Die folgenden Punkte liegen diesbezüglich in der Verantwortung der Grundbuchämter:

a) Abschliessen von vertraglichen Vereinbarungen und Nutzungsbestimmungen im Zusammenhang mit der Bereitstellung von Grundbuchinformationen. Die Vertragsparteien sind jeweils die Grundbuchämter und Terravis.

b) Verwaltung der eigenen Stammdaten in Terravis.

c) Verwaltung (inkl. allfälliger Sperrung) der Administratoren und Benutzer inkl. der jeweiligen Rechte in Terravis.

d) Sicheres Handhaben, Verwalten und Kontrollieren der von Terravis bezogenen Informationen (Grundbuchinformationen, Kundeninformationen, Belege, Formulare, Anträge, Benutzerinformationen, Auditeinträge, etc.)

e) Sichere Handhabung und Verwaltung des Authentisierungsmerkmals im Zusammenhang mit der Authentisierung gegenüber Terravis.

f) Erstellen von Arbeitsanweisungen im Zusammenhang mit der Nutzung von Terravis. Die Einhaltung der Arbeitsanweisungen ist zu überwachen.

g) Sichere Integration und Betrieb der eigenen IT-Infrastrukturen und Applikationen.

Weitere Verantwortlichkeiten sind bei den untenstehenden Schutzobjekten beschrieben.

[20] Hinweis: Grundbuchbeamte, die Grundbuchinformationen oder Auditeinträge über Terravis beziehen, handeln in der Rolle „Benutzer“.

5.4 Leitlinien zur Identifizierung von Schutzobjekten

Die jeweiligen Parteien sind eigenständig verantwortlich für alle technischen und organisatorischen Prozesse sowie für alle Systemkomponenten, die sich innerhalb ihrer jeweiligen Systemgrenze befinden (siehe Kapitel 2.1).

Im Folgenden sind beispielhaft die wichtigsten Schutzobjekte aus Sicht der einzelnen Parteien beschrieben. Es handelt sich hierbei um Vorschläge zur Identifizierung und Bewertung der jeweiligen Schutzobjekte.

Hinweis
Die Liste der Schutzobjekte ist beispielhaft und nicht abschliessend. Die jeweiligen Parteien sind alleinig dafür verantwortlich, ihre eigenen Schutzobjekte sowie deren Abhängigkeiten zu identifizieren und diese entsprechend zu bewerten. Es liegt auch in der alleinigen Verantwortung der jeweiligen Parteien, den Schutz der entsprechenden Objekte über geeignete Massnahmen sicherzustellen.

Die Schutzobjekte sind kategorisiert nach ihrem Schutzbedarf[21].

Schutzbedarf	Beschreibung
Normaler Schutzbedarf	Die Schadensauswirkungen sind begrenzt und überschaubar
Hoher Schutzbedarf	Die Schadensauswirkungen können beträchtlich sein
Sehr hoher Schutzbedarf	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmass erreichen

[21] BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5

5.4.1 Authentisierungsmerkmale

Über die Authentisierungsmerkmale authentisieren sich Benutzer oder Systeme gegenüber Terravis. Sie sind persönlich oder systemspezifisch und dürfen nicht an Dritte weitergegeben werden.

Die Authentisierungsmerkmale sind die Basis für die Authentizität der Kommunikationsteilnehmer sowie für die Integrität und Vertraulichkeit der Daten über das Internet.

Hinweis
Das Eingangsportal von Terravis authentifiziert die Teilnehmer alleinig durch das Authentisierungsmerkmal. Standortbezogene Informationen wie beispielsweise der Zugang über FinanceIP wird nicht in die Authentifizierung der Benutzer miteinbezogen. Sofern die Benutzer die Authentisierungsmerkmale auf sich tragen[22], können sie sich auch ausserhalb der Organisation in Terravis einloggen. Der jeweilige Nutzer ist verantwortlich für seine Benutzer und muss entsprechende Weisungen im Umgang mit den Authentisierungsmerkmalen und der Nutzung von Terravis erlassen.

5.4.1.1 Administration von Administratoren und Benutzern

Die Grundbuchämter verwalten ihre Konten für Administratoren und Benutzer eigenständig in Terravis. Die jeweiligen Administratoren authentisieren sich mit ihrem Authentifizierungszertifikat gegenüber Terravis.

#	Beschreibung		
S1.	Benutzerspezifisches X.509 Zertifikat für die Administration		
	Kategorie	Hoher Schutzbedarf	
	Schnittstellen	3, 4	
	Bemerkung	SuisseID IAC oder ein organisationseigenes X.509 Zertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC (siehe Kapitel 7.1.1).	

[22] Beispielsweise SuisseID Smartcard

5.4.1.2 Webservice für Datenbezug

Für den Datenbezug müssen sich die Systeme gegenseitig über ein systemspezifisches Zertifikat Authentisieren.

#	Beschreibung			
S2.	Systemspezifisches X.509 Serverzertifikat			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	1, 2		
	Bemerkung	Organisationseigenes X.509 Zertifikat (siehe Kapitel 7.1.1)		

5.4.2 IT-Systeme

Der Datenaustausch erfolgt über Webservices. Das Grundbuchamt trägt die Verantwortung über die eigenen IT-Systeme, die im Zusammenhang mit Terravis genutzt werden.

#	Beschreibung			
S3.	Verfügbarkeit			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen			
	Bemerkung	Die Verfügbarkeit der IT-Systeme der Grundbuchämter liegt im Interesse aller Nutzer.		
S4.	Schutz vor Schadsoftware			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	2, 3		
	Bemerkung	Das Grundbuchamt ist eigenständig dafür verantwortlich, dass die von Terravis bezogenen Informationen sowie die an Terravis übermittelten Informationen auf Schadsoftware hin untersucht und bei Bedarf entfernt werden.		
S5.	Schutz vor unbefugtem Zugriff			
	Kategorie	Hoher Schutzbedarf		
	Schnittstellen	1, 2		

#	Beschreibung	
	Bemerkung	Das Grundbuchamt ist eigenständig dafür verantwortlich, nur berechtigten Personen oder Systemen den Zugriff auf ihre Infrastruktur zu gewähren[23]. Im Weiteren ist das Grundbuchamt eigenständig dafür verantwortlich, seine Systeme vor jeglichen Angriffen aus dem Internet zu schützen. Dies beinhaltet u.a. auch die strukturelle Prüfung der maschinell auswertbaren Informationen auf Protokoll- und Datenebene. **Hinweis:** Wer sich gegenüber Terravis mit einem gültigen Authentisierungsmerkmal authentisiert, gilt Terravis gegenüber als Berechtigter zur Benützung der entsprechenden Dienstleistung. Terravis wird ohne weitere Überprüfung seiner Berechtigung die jeweiligen Abfragen und Aufträge tätigen, auch wenn es sich bei der Person oder dem System nicht um den tatsächlich berechtigten Benutzer oder Nutzer handelt.

[23] Beispielsweise durch korrekte Prüfung des SSL Server- resp. Clientzertifikats von Terravis

6 Terravis

6.1 Verantwortlichkeiten

Terravis ermöglicht den elektronischen Geschäftsverkehr zwischen Grundbuchämtern, Notariaten und Banken. Die folgenden Punkte liegen in der Verantwortung von Terravis:

a) Vertraglichen Vereinbarungen und Nutzungsbestimmungen im Zusammenhang mit der Bereitstellung von Terravis bezogenen Leistungen. Die Vertragsparteien sind Terravis und die jeweiligen Nutzer.

b) Vertraglichen Vereinbarungen und Nutzungsbestimmungen im Zusammenhang mit dem Bezug von Grundbuchinformationen. Die Vertragsparteien sind Terravis und die jeweiligen Grundbuchämter.

c) Vertraglichen Vereinbarungen und Nutzungsbestimmungen im Zusammenhang mit dem Bezug von Geoinformation. Die Vertragsparteien sind Terravis und Swisstopo.

d) Sicheres Handhaben, Verwalten und Kontrollieren der von Terravis bezogenen Informationen (Grundbuchinformationen, Kundeninformationen, Belege, Formulare, Anträge, Benutzerinformationen, Auditeinträge, etc.)

e) Verwaltung (inkl. allfälliger Sperrung) von Administratoren und Benutzern sowie deren Rechte. Die Verwaltung wird primär durch die Teilnehmer selber gemacht. Terravis registriert einzig den „initialen Administrator“ mit seinen entsprechenden Rechten.

f) Bereitstellen von Terravis bezogenen Leistungen im Rahmen der vertraglichen Vereinbarungen und Nutzungsbestimmungen.

g) Sichere Integration und Betrieb der eigenen IT-Infrastrukturen und Applikationen.

7 Verschiedenes

7.1 Zertifikatsbasierte Authentisierungsmerkmale

Die zertifikatsbasierten Authentisierungsmerkmale basieren auf dem X.509 Standard und folgen den Vorgaben von [RFC 5280].

7.1.1 Benutzerzertifikate für die Authentisierung

Die zertifikatsbasierte Authentisierung der Benutzer gegenüber dem Terravis Server erfolgt über das SuisseID IAC oder über ein organisationseigenes Clientzertifikat, das vergleichbare Sicherheitseigenschaften aufweist wie das SuisseID IAC. Die organisationsspezifischen Clientzertifikate werden typischerweise von einer Unternehmens PKI[24] oder von einer öffentlichen PKI ausgestellt.

Falls ein organisationseigenes Clientzertifikat eingesetzt wird, muss der Teilnehmer sicherstellen, dass die folgenden Anforderungen im Zusammenhang mit dem zertifikatsbasierten Authentisierungsmerkmal erfüllt sind:

a) Die Identität der Zertifikatsinhaberin, des Zertifikatsinhabers oder eines Systems muss zweifelsfrei erfasst werden. Ein spezifisches Zertifikat muss eindeutig einer spezifischen Entität zugeordnet werden können.
b) Die Zertifikatsinhaberin, der Zertifikatsinhaber oder der verantwortliche Betreiber eines Systems muss den Nutzungsbestimmungen im Zusammenhang mit der Verwendung des zertifikatsbasierten Authentisierungsmerkmals zustimmen. Die Nutzungsbestimmungen müssen durch die Teilnehmer erstellt werden.

Der private Schlüssel, der im Zusammenhang mit der Authentisierung verwendet wird, muss[25]

c) praktisch nur einmal auftreten können und seine Geheimhaltung muss hinreichend gewährleistet sein;
d) mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur, die im Zusammenhang mit der Authentisierung erstellt wird, bei Verwendung der jeweils verfügbaren Technologie vor Fälschungen geschützt ist;
e) von der rechtmässigen Inhaberin oder vom rechtmässigen Inhaber vor der missbräuchlichen Verwendung durch andere verlässlich geschützt werden können.

[24] Im Falle einer Unternehmens PKI muss, im Rahmen der Registrierung des initialen Administrators, das entsprechende CA Zertifikat sicher an Terravis übermittelt werden.

[25] Sinngemäss zu [SuisseID Spezifikation], Kapitel 3.5.2 (Technical and Administrative Guidelines for the SuisseID IAC)

Es liegt in der alleinigen Verantwortung der SIX Terravis darüber zu entscheiden, ob und unter welchen Umständen organisationseigene Zertifikate eingesetzt werden können.

7.1.2 Systemzertifikate

Die zertifikatsbasierte Authentisierung von Systemkomponenten gegenüber Benutzern oder anderen Systemkomponenten erfolgt über Systemzertifikate. Diese werden typischerweise von einer Unternehmens PKI[26] oder von einer öffentlichen PKI ausgestellt.

Im Zusammenhang mit Systemzertifikaten muss der Teilnehmer sicherstellen, dass die folgenden Anforderungen erfüllt sind:

a) Die Identität der jeweiligen Systemkomponenten muss zweifelsfrei erfasst werden. Ein spezifisches Zertifikat muss eindeutig einer spezifischen Systemkomponente zugeordnet werden können.
   Typischerweise wird der FQDN[27] des jeweiligen Servers im RDN[28] CN des Subject DN eingetragen[29].

Der private Schlüssel, der im Zusammenhang mit der Authentisierung verwendet wird, muss

b) nur einmal auftreten können und seine Geheimhaltung muss hinreichend gewährleistet sein;
c) mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur, die im Zusammenhang mit der Authentisierung erstellt wird, bei Verwendung der jeweils verfügbaren Technologie vor Fälschungen geschützt ist;
d) vor der missbräuchlichen Verwendung durch unberechtigte verlässlich geschützt werden können.

Es liegt in der alleinigen Verantwortung der SIX Terravis darüber zu entscheiden, ob und unter welchen Umständen organisationseigene Zertifikate eingesetzt werden können.

[26] Im Falle einer Unternehmens PKI muss, im Rahmen der Registrierung des initialen Administrators, der Fingerprint des jeweiligen CA Zertifikats, formell an Terravis übermittelt werden.

[27] Fully qualified domain name

[28] Relative Distinguished Name

[29] Beispiel: `CN=www.terravis.ch`

7.1.3 Zertifikatsvalidierung

Die Zertifikatsvalidierung muss den Vorgaben von [RFC 5280] Abschnitt 6 folgen. Im Minimum sollten die folgenden Validierungsschritte durchgeführt werden:

a) Die digitale Signatur des jeweiligen Zertifikats kann mit dem öffentlichen Schlüssel des übergeordneten Zertifikats überprüft werden[30].

b) Alle Zertifikate in der Kette sind zum Zeitpunkt der Signaturprüfung[31] gültig[32].

c) Alle Zertifikate in der Kette sind nicht gesperrt oder suspendiert, das heisst die Seriennummern der entsprechenden Zertifikate sind in der jeweils aktuellen Sperrliste (CRL) nicht eingetragen. Die digitale Signatur der jeweiligen Sperrliste muss erfolgreich mit dem korrespondierenden CA Zertifikat überprüft werden.

Erst nach erfolgreicher Validierung kann, auf der Basis von Attributen oder anderen Zertifikatseigenschaften, eine Zuordnung zu einem Benutzer oder zu einem System gemacht werden.

[30] Das übergeordnete Zertifikat ist typischerweise ein vertrauenswürdiges CA Zertifikat, das auf dem System vorinstalliert ist.

[31] als Bestandteil des Authentisierungsprotokolls

[32] Validierung der Zertifikate basiert auf dem sogenannten „Schalenmodell“