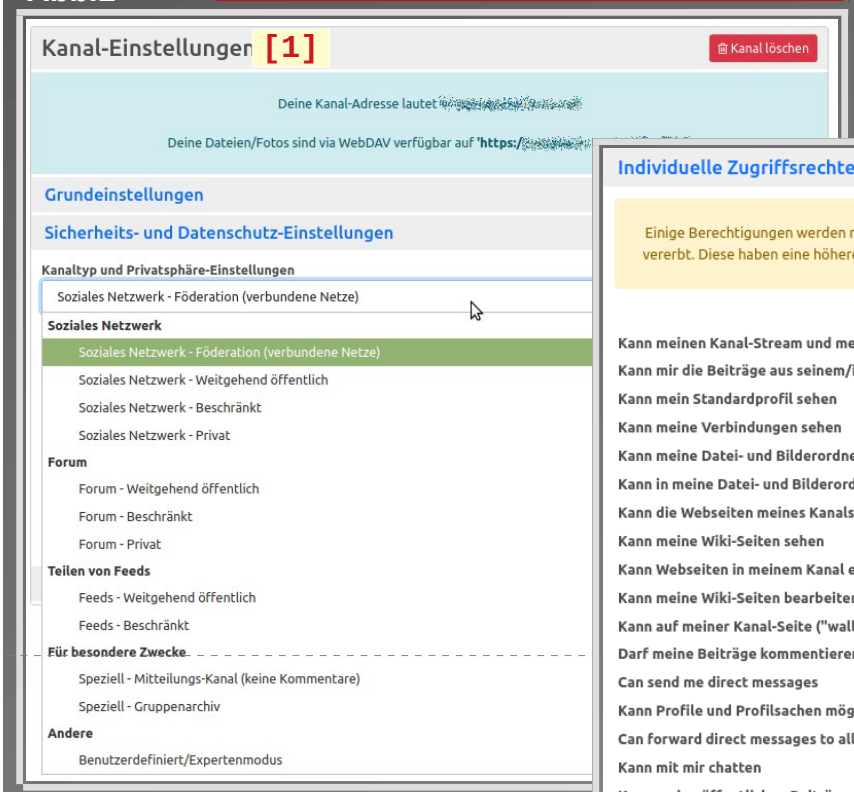
Hubzilla -007

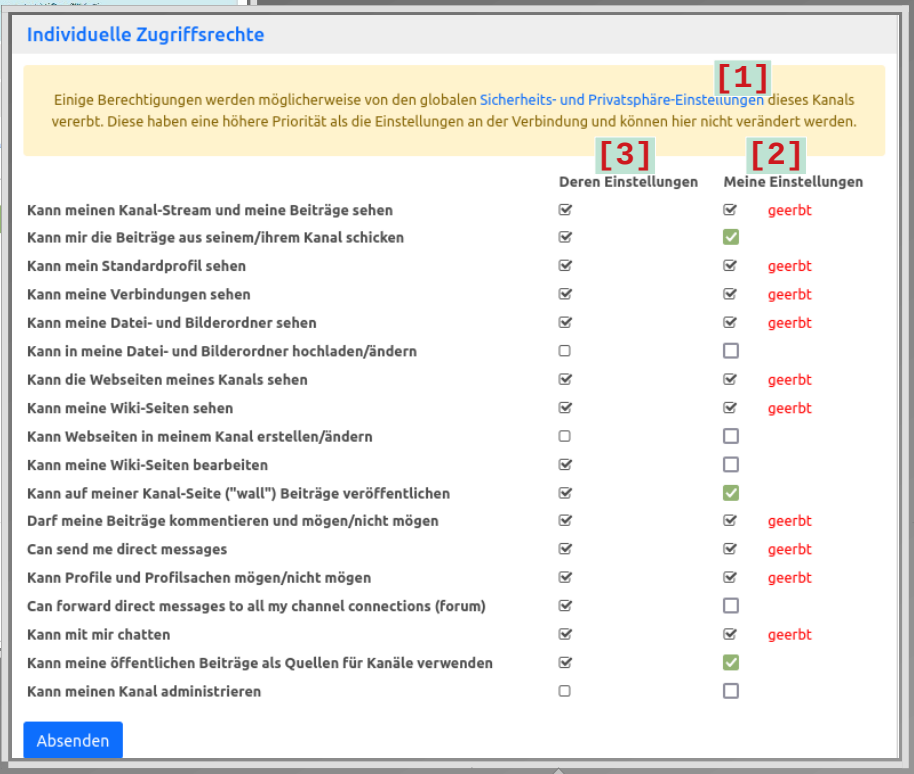
Topologie der Berechtigungen (Permissions)

[1] Mein Kanal ...
hat eine Zuordnung zu einem Kanaltyp, hinter dem Einstellungen zur Sicherheit (zur Privatsphäre) stecken. Die Einstellungen variieren zwischen den einzelnen Kanaltypen. Die detaillierten Einstellungen sind visuell am besten bei den Verbindungen [2] zu erkennen.

Verbindungen (Connections) ...
werden zwischen zwei Kanälen hergestellt, und zwar zwischen meinem Kanal [2] und einem anderen [3]. Da jeder der beteiligten Kanäle eigene Einstellungen zur Sicherheit hat, ist es wichtig, erkennen zu können, wie die beiden miteinander zusammen passen. Das wird im Dialog der **Individuellen Zugriffsrechte** bei einer Verbindung angezeigt.

Abb.1





Was ich bei Anderen und Andere bei mir dürfen ...

Ein Beitrag kann sensible Inhalte enthalten und soll deshalb nicht für weltweit alle sichtbar werden. Das läßt sich in den Berechtigungs-Einstellungen zum Beitrag regeln. Vielleicht füge ich dem Beitrag auch noch ein Bild hinzu und vielleicht ist auch das gleichermaßen schützenswert.

Und so, wie ich meine zu veröffentlichen Informationen schütze, indem ich eingeschränkte Zugriffsberechtigungen einstelle, so werden das auch Andere mit ihren Veröffentlichungen tun.

Und wer bin ich? Und wer sind die Anderen?
Es sind immer die an der Kommunikation im Netz beteiligten Kanäle, hinter denen die Digitalen Identitäten stehen, und durch Namenskonstrukte wie *max.mustermann@irgendwo.www* repräsentiert sind. Solch ein Namenskonstrukt nennt sich übrigens „Webbie“.
Zum Kanal gehören nicht nur Beiträge, sondern auch Dateien, BlogArtikel, Wikis, Chaträume,Profile uvm. Alles Dinge, die schützenswert sein können.

Abb.2.2

Abb.2.1

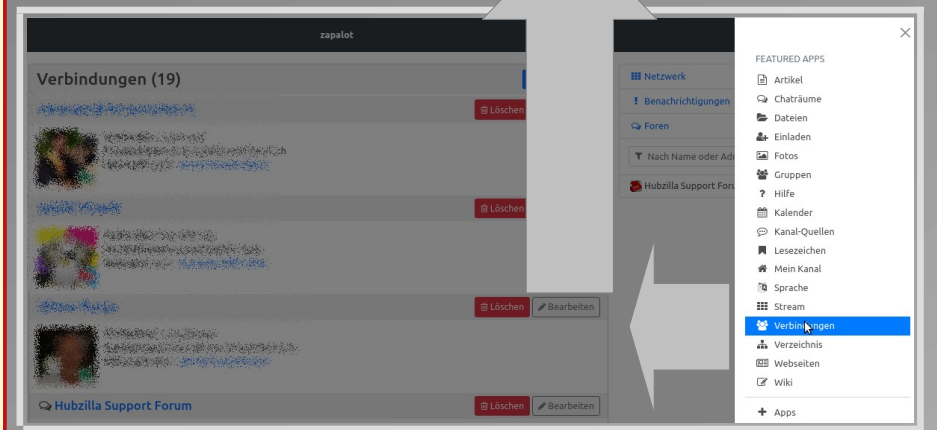


Abb.1 Die Kanaleinstellungen sind aufrufbar über die Menuleiste (oben links) auf der Ikone meines Profils (Menupunkt **Einstellungen**).
Abb.2 Verbindungen sind mit der gleichnamigen App aufrufbar (**Abb.2.1**). Durch Klick auf eine Verbindung werden die Individuellen Zugriffrechte dargestellt (**Abb.2.2**), und zwar die meines Kanals [2] als „Meine Einstellungen“ und die des verbundenen Kanals [3] als „Deren Einstellungen“.

OAU: Zum Verständnis der Topologie eines geschützen Systems ist eine Abstraktion hilfreich, in der drei Dinge aufeinander treffen:

- [**O**] das schützbare Objekt: „WAS?“
- [**A**] der Zugriff darauf (Access): „WIE?“
- [**U**] der Benutzer (User): „WER?“

[O] WAS kann geschützt werden?

- Hub, Site (die Server Instanz mit Hubzilla)
- Channel (jeder Kanal in einem Hub)
- Connection (Verbindungen zu Kanälen)
- Blog article (Artikel im Blog)
- Post (Beiträge)
- Chatrooms (Chat-Räume)
- Cloud (Dateispeicher). Hierbei gibt es drei Ebenen (Level):
  - Cloud, L1
  - Folder (Ordner), L2
  - Files (Dateien), L3
- Profil
- Webpage (Webseite)
- Wiki
- Comment (Kommentar)
- Like/Dislike (Emotionalität, Mag ich, Mag ich nicht)

WIE kann geschützt werden?

Zugriffsarten [A] gibt es in Hubzilla sehr vielfältige und die geeignet einzustellen ist erfahrungsgemäß eine größere Herausforderung bei der anfänglichen Verwendung von Hubzilla. Noch leicht verständlich ist der Wunsch, eine Datei [O] der Cloud [O] lesen [A] zu dürfen. Und auch nicht sehr schwer einzuordnen ist die Absicht, eine Datei in die Cloud hochzuladen [A]. Da gibt es in der Cloud auch Fotos. Die sind in der obigen Liste der Objekte gar nicht aufgeführt. Das ist sogar richtig, denn Fotos gehören nicht zu den schützbaren Objekten. Nanu? Nun, Fotos sind Dateien (sind bestimmte Dateitypen) und Dateien gehören nun doch zu den schützbaren Objekten. Diese scheinbare Spielerei mit den Begriffen ist in den Dialogen (im UI) der Cloud erkennbar: Photos bieten keine Schutzeinstellungen, Dateien dagegen sehr wohl. Und weil Fotos auch Dateien sind und die Bilder auch bei den Dateien wieder zu finden sind, können Fotos effektiv (und zwar dort) geschützt werden. Das geht nicht in der App der Fotos (Photo App), sondern in der der Dateien (Files App).

Als eine obere Ebene in einer Hierarchie der Objekte kann der **Kanal** gesehen werden. Der Kanal hat durch die Festlegung einer Kanalart (Soziales Netzwerk, Forum ...) bereits Vorgaben zum Datenschutz erhalten, die sich auf die darunterliegenden Ebenen auswirken. Ist eine obere Ebene bereits restriktiv, sind es die untergeordneten Objekte mindestens gleichermaßen, können aber auch restriktiver eingestellt sein. Habe ich auf den Kanal (Ebene 1) keinen Zugriff, sehe ich die Ordner der Cloud (Ebene 2) nicht. Kann ich die Ordner sehen, weil ich zum Kanal Zugang habe, kann mir der Zugang zum Foto verwehrt sein. Habe ich von den Berechtigungen die Zugriffserlaubnis zur Betrachtung des Fotos (Ebene 3), jedoch keine Berechtigung zum Ordner (Ebene 2), kann ich das Bild nicht sehen, weil ich bereits ab Ebene 2 ausgesperrt bin. Ein beliebtes Mißgeschick in Hubzilla ist, einen öffentlichen [A] Beitrag [O] zu schreiben (den jeder lesen können soll), in dem Beitrag ein Foto einzufügen, bei dem vergessen wird, das von der Berechtigung gleichermaßen freizügig einzustellen. Aber gehört das Bild nicht zum Beitrag? Inhaltlich sicher ja, strukturell in der Hierarchie aber nicht. Das klingt und ist etwas kompliziert, hat aber den Sinn, eine schützbare Datenquelle (wie das Foto) auch anderswo als in dem Beitrag verwenden zu können, wo dann die Restriktionen, warum auch immer, enger gesetzt sind.

[U] WER darf und wer nicht?

Es gibt impliziet immer mindestens einen Berechtigten, der visuell gar nicht überall als solcher erkennbar ist: der Eigentümer eines geschützten Objekts. Wenn ich einen Beitrag schreibe, habe ich auch automatisch die Berechtigung, den zu lesen und bei Bedarf zu ändern. Im Beitragsstrom wird auch visuell auf den Eigner hingewiesen: *HIlmar hat heute geschrieben…*
Eine Aufzählung der „Benutzer“ (denjenigen, denen Berechtigungen erteilt oder entzogen werden können) ist übersichtlich:

- Jeder
- Nur ich
- Implizite Gruppierungen (z.B. MeineVerbindungen)
- Gruppen (Mitglieder einer (mit der Group App) explizit definierten Gruppe)
- Bestimmte (spezifizierte) Benutzer

In fast allen Fällen ist ein „Benutzer“ im Sinne der Zugriffsberechtigung die Person als Eigentümer eines Kanals, und beide - Benutzer [U] und Kanal [O] - werden visuell durch ein Konstrukt wie ***ichbins@meinhub*** repräsentiert. Solch ein Konstrukt wird auch ***Webbie*** genannt und ist nur syntaktisch anders als die Spezifikation ***meinhub/channel/ichbins***. Ein Kanal ist Objekt und User, und zwar je nach Bezugspunkt: Zur Verbindung [A] mit meinen Kanal [O] ist ein anderer Kanal [U] berechtigt worden.

WAS ist erlaubt und was nicht?

Es gibt ein Schreibrecht [A] für Beiträge [O]. Damit kann ich aber nicht beliebige Beiträge inhaltlich ändern, sondern vielmehr werde ich damit berechtigt, in der Ebene oberhalb des Beitrags (das ist der Kanal) Beiträge zu erstellen und (nur) meine (eigenen) Beiträge zu ändern. Ähnlich verhält es sich bei Dateien. Ein Dokument kann ich betrachten, wenn ich Leserechte für die Datei (Ebene 3), den übergeordneten Ordner (Ebene 2) und den Kanal (Ebene 1) habe. Ein Schreibrecht auf Ebene 2 gewährt mir nicht zwingend, das Dokument (Ebene 3) zu ändern. Es erlaubt mir, in dem Ordner ein Dokument hochzuladen, wenn mir der auf der Kanalebene (Ebene 1) auch zugänglich ist.

Berechtigungsrollen (PERMISSION CATEGORIES) sind Kombinationen aus Objekten [O] und Zugriffsarten [A]. Die Objekte gehören zu meinem, in der Hierarchie übergeordneten Kanal.

Can view my channel stream and posts
- Kann meinen Kanal-Stream und meine Beiträge sehen

Can send me their channel stream and posts
- Kann mir die Beiträge aus seinem/ihrem Kanal schicken

Can view my default channel profile
- Kann mein Standardprofil sehen

Can view my connections
- Kann meine Verbindungen sehen

Can view my file storage and photos
- Kann meine Datei- und Bilderordner sehen

Can view my channel webpages
- Kann die Webseiten meines Kanals sehen

Can view my wiki pages
- Kann meine Wiki-Seiten sehen

Can like/dislike profiles and profile things:
- Kann Profile und Profilsachen mögen/nicht mögen

Can comment on or like my posts
- Darf meine Beiträge kommentieren und mögen/nicht mögen

Can chat with me *(in a chatroom)*
- Kann mit mir *(im Chatraum)* chatten

Can send me private mail messages
- Kann mir private Nachrichten schicken

Can post on my channel (wall) page
- Kann auf meiner Kanal-Seite ("wall") Beiträge veröffentlichen

Can forward to all my channel connections via ! mentions in posts
- Kann über ! Erwähnungen in Beiträgen an alle Verbindungen des Kanals weiterleiten

Can send me private mail messages
- Kann mir private Mitteilungen senden.

Can create/edit my channel webpages
- Kann Webseiten in meinem Kanal erstellen/ändern

Can write to my wiki page
- Kann meine Wiki-Seiten bearbeiten

Can upload/modify my file storage and photos
- Kann in meine Datei- und Bilderordner hochladen/ändern

Can source my public posts in derived channels
- Kann meine öffentlichen Beiträge als Quellen für Kanäle verwenden

Can administer my channel
- Kann meinen Kanal administrieren

WER [U] kann berechtigt werden (mit der Einschränkung **von wo aus)**

Anybody authenticated (could include visitors from other networks)
- Jeder, der angemeldet ist (kann Besucher anderer Netzwerke beinhalten)

Anybody in the Hubzilla network
- Jeder innerhalb des Hubzilla Netzwerks

Any account on {Hub}
- Jedes Nutzerkonto auf {Hub}

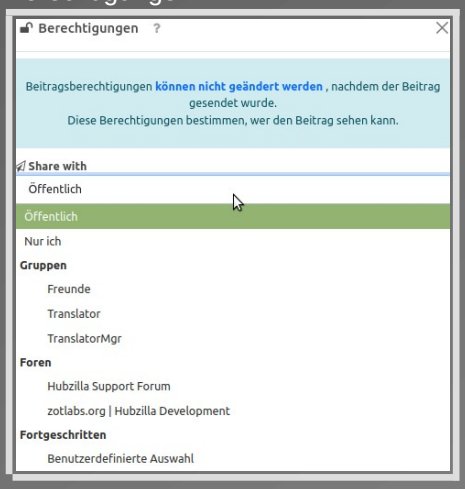
Any of my connections
- Alle meine Verbindungen

Any connections including those who haven't yet been approved
- Alle Verbindungen einschließlich der noch nicht bestätigten

Only connections I specifically allow
- Nur Verbindungen, denen ich es explizit erlaube

Anmerkung: Die verbalen Hinweise können leicht mißverstanden werden. In allen Fällen handelt es sich um die Digitale Identität eines Kanals (formuliert als Webbie). Beispielsweise „jedes Nutzerkonto“ meint eben nicht das Konto, sondern einen Kanal (ein Konto kann mehrere Kanäle haben).

Abb.: Beispieldialog zur Erteilung von Berechtigungen



Imaginäre Objekt Hierarchien in Hubzilla

```
Hub-Instanz (Site)
:...Kanal (channel)
:   :..Artikel (blog)
:   :..Beiträge (post)
:   :..Chaträume (chatroom)
:   :..Dateien (cloud)
:   :  :..Ordner (folder) ...
:   :     :..Datei (file) ...
:   :..Profile
:   :..Verbindungen (connection)
:   :..Webseiten (webpage)
:   :..Wikis (wiki)
:...Kanal (channel) ...
```

MiniGlossar

PERMISSION CATEGORIES – BERECHTIGUNGSROLLEN (O,A). Viele sind vorgegeben. Eigene können (mit der App „Berechtigungsrollen“) definiert werden.

PRIVACY GROUPS [U] – Beliebig benennbare Gruppen, in die Benutzer (Webbies) (mit der „Gruppen“ App) eingeordnet werden. Standardmäßig gibt es die Gruppe „Freunde“.

PERMISSIONS – BERECHTIGUNGEN [U]
- Public - Öffentlich
- Only me - Nur ich
- (Privacy groups - Gruppen)
- (Custom selection - Benutzerdefiniert)