

# NTFS-Berechtigungen

---

## 1. Authentifizierung (Wer greift zu?)

### Access Token

Beim Einloggen eines Benutzers wird ein Access-Token erstellt.

Jeder vom Benutzer gestartete Prozess erhält eine Kopie dieses Access-Tokens.

### Inhalt des Access-Tokens

- SID des Benutzers
- SIDs der Gruppen, in denen der Benutzer Mitglied ist
- logon SID der Session
- Liste von Privilegien des Benutzers und der Gruppen
- SID des Besitzers
- SID der primary group
- ...

### Windows Befehl

```
whoami /all
```

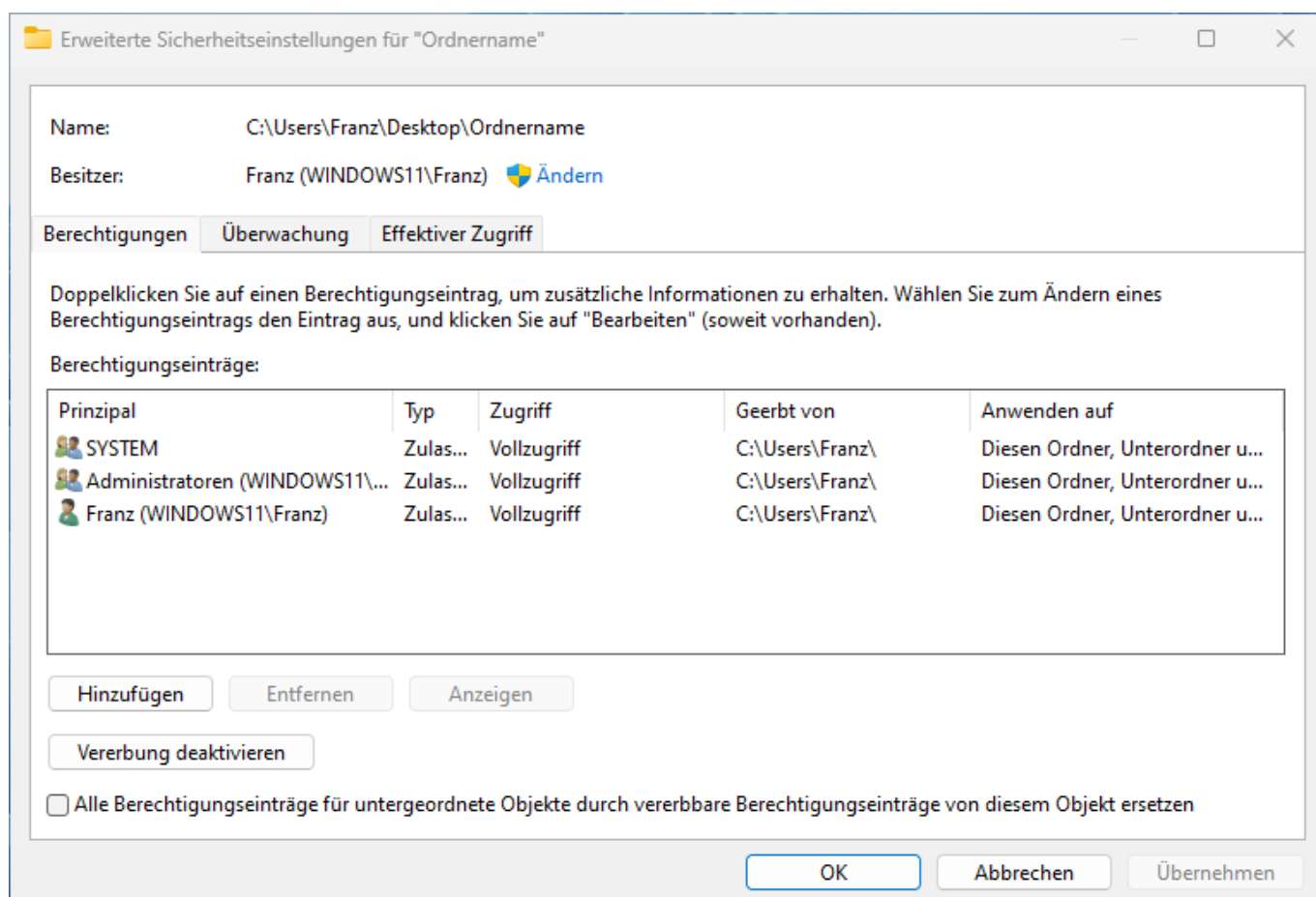
## 2. Autorisierung (Zuweisung von Zugriffsrechten)

### Security Descriptor

Jedes sicherungsfähige Objekt (Laufwerk, Ordner, Datei, ...) kann einen Security-Descriptor haben, der festlegt, wer wie auf dieses Objekt zugreifen darf.

### Inhalt des SD (Security Descriptor)

- SID des Besitzers
- DACL (Discretionary Access Control List)
  - ACE1
  - ACE2
  - ACE3
- DACL\_PROTECTED (erben von oben?)
- SACL (System Access Control List)
  - ACE4
  - ACE5
  - ACE6
- SACL\_PROTECTED (erben von oben?)
- ...



## ACE (Access Control Entry)

- Trustee (Benutzer oder Gruppe)
- ACEType (Allow / Deny)
- ACEFlags (vererben an)
  - Diesen Ordner
  - Unterordner
  - Dateien
- ACEMask (Rechte)
  - lesen
  - schreiben
  - ...

Berechtigungseintrag für "Ordnername"

Prinzipal: Franz (WINDOWS11\Franz) [Prinzipal auswählen](#)

Typ: Zulassen

Anwenden auf: Diesen Ordner, Unterordner und Dateien

Erweiterte Berechtigungen: [Grundlegende Berechtigungen anzeigen](#)

<input checked="" type="checkbox"/> Vollzugriff	<input checked="" type="checkbox"/> Attribute schreiben
<input checked="" type="checkbox"/> Ordner durchsuchen / Datei ausführen	<input checked="" type="checkbox"/> Erweiterte Attribute schreiben
<input checked="" type="checkbox"/> Ordner auflisten / Daten lesen	<input checked="" type="checkbox"/> Unterordner und Dateien löschen
<input checked="" type="checkbox"/> Attribute lesen	<input checked="" type="checkbox"/> Löschen
<input checked="" type="checkbox"/> Erweiterte Attribute lesen	<input checked="" type="checkbox"/> Berechtigungen lesen
<input checked="" type="checkbox"/> Dateien erstellen / Daten schreiben	<input checked="" type="checkbox"/> Berechtigungen ändern
<input checked="" type="checkbox"/> Ordner erstellen / Daten anhängen	<input checked="" type="checkbox"/> Besitz übernehmen

Berechtigungen nur für Objekte und/oder Container in diesem Container übernehmen [Alle löschen](#)

OK Abbrechen