

## **EDI SCHNITTSTELLE – TECHNISCHE BESCHREIBUNG**

Dokumentation für Einrichtungen gem. HeimAufG

### **BESCHREIBUNG**

Die EDI Schnittstelle wurde mit einem Webservice umgesetzt. Um die EDI Schnittstelle in Ihrem Programm nutzen zu können, muss ein http-Web-Request gesendet werden.

Die Authentifizierung wird durch den Austausch von Zertifikaten gewährleistet. Um die Freiheitsbeschränkungsmeldungen einer Einrichtung korrekt im Dokumentationssystem der Bewohnervertretung erfassen zu können, benötigt jede Einrichtung ein eindeutig zugeordnetes Client-Zertifikat.

Die Übermittlung des Zertifikats erfolgt über die WEB-Applikation der Bewohnervertretung. Sofern die Einrichtung noch über keinen registrierten User verfügt, ist dieser entweder beim örtlich zuständigen Standort der Bewohnervertretung, oder unter [support-edi@bewohnervertretung.at](mailto:support-edi@bewohnervertretung.at) anzufordern.

Sämtliche Informationen zur WEB-Applikation sowie das Anforderungsformular für die Login-Daten stehen unter

<http://www.vertretungsnetz.at/bewohnervertretung/meldung-einer-freiheitsbeschraenkenden-massnahme/> zur Verfügung.

Verfügt die Einrichtung über einen aktivierten WEB-User, fordert die Einrichtung die Ausstellung eines Zertifikats unter [support-edi@bewohnervertretung.at](mailto:support-edi@bewohnervertretung.at) an.

Nach Ausstellung des Zertifikats und entsprechender Rückmeldung durch die Bewohnervertretung, stehen auf der Startseite der WEB-Applikation sowohl das Passwort als auch das Zertifikat für 14 Tage zum Download bereit.

Ab Ausstellung ist das Zertifikat 3 Jahre gültig.

Das Zertifikat muss dem WebRequest hinzugefügt werden, damit die Einrichtung erkannt und authentifiziert wird. Bitte berücksichtigen Sie, dass die Nutzerin/der Nutzer rechtzeitig über einen nahenden Ablauf der Gültigkeit des Zertifikats informiert wird, um sich rechtzeitig bei der Bewohnervertretung bzgl. eines neuen Zertifikats melden zu können.

Die Daten der Freiheitsbeschränkung werden in Form eines XML String dem Body des WebRequest übergeben. Der XML String muss dem EDI XML-Schema entsprechen. Als Ergebnis werden HttpStatusCode zurückgeliefert, welche über Erfolg oder Misserfolg der Authentifizierung und Meldung berichten.

Bei Erfolg wird zusätzlich im Body des WebResponses ein Referenzwert zurückgegeben. Dies ist eine einfache, eindeutige Zahl.

## UMSETZUNG DES VERBINDUNGS-AUFBAUS AUF CLIENT-SEITE (BEISPIEL-CODE IN C#)

In den Beispielen werden folgende Werte verwendet:

- Adresse der EDI Schnittstelle:  
<https://edi.bewohnervertretung.at/api/xmlmapper>
- Dateiname des Institutions-/Einrichtung-Zertifikats: **BIDS EDI Certificate - IK=ER - Id=24.pfx**
- Dateiname des exportierten Zertifikats ohne privaten Schlüssel (Wichtig: Hierbei muss das Zertifikat mit privatem Schlüssel installiert sein): **BIDS EDI Certificate - IK=ER - Id=24.cer**
- Passwort des privaten Schlüssels: **bM\$6}e7Z4\***
- Subject des Zertifikats: **CN=BIDS EDI Certificate – IK:ER – Id:24**

Diese Beispielwerte müssen in der eigenen Applikation dann durch die endgültigen und eigenen Werte ersetzt werden!

### .Net Framework 4.5 und höher

```
public async void SendMeldung()
{
    string url = "https://edi2.bewohnervertretung.at/api/xmlmapper";
    string pfxFile = "BIDS EDI Certificate - IK=ER - Id=24.pfx";
    string cerFile = "BIDS EDI Certificate - IK=ER - Id=24.pfx";
    string cerSubject = "BIDS EDI Certificate - IK:ER - Id:24";
    string cerPassword = "bM$6}e7Z4*";

    string meldung = @"<?xml version=""1.0"" encoding=""utf-8"" ?><Vornahme .....
</Vornahme>";

    // Es gibt mehrere Varianten wie ein Zertifikat geladen werden kann:
    // Variante 1: Lade Zertifikat mittels pfx Datei
    var certificate = new X509Certificate2(pfxFile, cerPassword);

    // Variante 2: Lade Zertifikat mittels cer Datei.
    // Hierbei muss jedoch das Zertifikat mittels der pfx Datei und Passwort
    // im Zertifikatsspeicher des Rechners installiert werden und anschließend
    // das Zertifikat ohne Schlüssel (cer) exportiert werden.
    certificate = new X509Certificate2(cerFile);

    // Variante 3: Zertifikat aus dem Zertifikatsspeicher laden (empfohlen)
    // Hierbei muss jedoch das Zertifikat mittels der pfx Datei und Passwort
    // im Zertifikatsspeicher des Rechners installiert werden.
    certificate = FindCertificateFromStore(cerSubject, StoreLocation.CurrentUser,
StoreName.My);

    // WebRequestHandler:
    // Namespace: System.Net.Http
    // Assembly: System.Net.Http.WebRequest (in System.Net.Http.WebRequest.dll)
    WebRequestHandler handler = new WebRequestHandler();
    handler.ClientCertificates.Add(certificate);

    using (HttpClient client = new HttpClient(handler))
    {
```

```

        var result = await client.PostAsync(url, new StringContent(meldung,
Encoding.UTF8, "application/json"));

        if (result.IsSuccessStatusCode)
        {
            // Meldung wurde erfolgreich übermittelt
        }

        // für weitere informationen
        string returnValue = await result.Content.ReadAsStringAsync();
        // bei erfolg z.B.: returnValue = "123"
    }
}

private static X509Certificate2 FindCertificateFromStore(string cerSubject,
StoreLocation storeLocation, StoreName storeName)
{
    X509Certificate2 cert = null;

    var certStore = new X509Store(storeName, storeLocation);
    certStore.Open(OpenFlags.ReadOnly);

    foreach (var item in certStore.Certificates)
    {
        if (item.Subject.Equals("CN=" + cerSubject,
StringComparison.InvariantCultureIgnoreCase))
        {
            cert = item;
            break;
        }
    }

    certStore.Close();

    return cert;
}

```

## XML – SCHEMA

Für eine genaue Definition sowie eine Beschreibung aller Knoten sehen Sie bitte die mitgelieferte zip-Datei (ebenfalls auf der Website <http://www.vertretungsnetz.at/bewohnervertretung> abrufbar) durch. Sie enthält Definitionen, Dokumentationen und Beispielen zu den XML Elementen. Der Aufruf der Übersicht erfolgt durch die im Stammverzeichnis gelegene **index.html**

## XML Elemente „Einrichtung“, „Abteilung“, „Unterabteilung“

Es muss zweifelsfrei erkennbar sein, woher eine Meldung kommt, wenn die Einrichtung aus mehreren Organisationseinheiten besteht. Verfügt eine Einrichtung beispielsweise über zwei Stationen, so bildet die Bewohnervertretung diese Struktur der Einrichtung in ihrer Datenbank ebenfalls ab. Anhand des XML müssen über die mitgesandte Struktur Einrichtung, Abteilung, ggf. Unterabteilung erkennbar sein bzw. stammt die Meldung von Station 1 oder Station 2.

Sollte es sich bei der Einrichtung um einen dislozierten Organisationsverbund (Organisationseinheiten verteilt auf mehrere Adressen) handeln, muss vor Beginn der Entwicklungsarbeit Kontakt mit der Bewohnervertretung unter [support-edi@bewohnervertretung.at](mailto:support-edi@bewohnervertretung.at) aufgenommen werden.

Die genauen Bezeichnungen der absendenden Organisationseinheiten müssen vor Übermittlung der ersten Echtdaten (Meldung) an die Bewohnervertretung unter [support-edi@bewohnervertretung.at](mailto:support-edi@bewohnervertretung.at) übermittelt werden, damit die Struktur entsprechend angepasst werden kann.

### **Interpretation von mehrfach vorkommenden gleichen Maßnahmen**

Es sollten keine gleichen Maßnahmen in einer Meldung angegeben werden. Das kann vom Schema selbst aber nicht verhindert werden.

Sollten dennoch gleiche Maßnahmen angegeben werden, interpretiert das System diese wie folgt:

- Mehrere gleiche Maßnahmen werden als eine Maßnahme interpretiert.
- Mehrere gleiche Maßnahmen mit unterschiedlichen Enumerationswerten werden als eine Maßnahme interpretiert. Werden z.B. Hand-Arm-Gurte einmal mit "1" und einmal mit "2" angegeben, wird nur die "2" weiterverarbeitet.
- Mehrere gleiche Maßnahmen mit Freitext werden als eine Maßnahme interpretiert.  
z.B. mehrfache Nennung von Einzelfallmedikation, Dauermedikation oder Andere Maßnahme. Die einzelnen Texte werden in einer Maßnahme zusammengefasst.

### **Allgemeines zur Meldung bzw. Aufhebung freiheitsbeschränkender Maßnahmen:**

Es muss möglich sein, einzelne Maßnahmen einer Meldung aufzuheben und (nur im Fall einer vom Gericht ausgesprochenen Zulässigkeit!) zu verlängern.

Unabhängig vom Bestehen einer Meldung, muss es möglich sein, weitere Vornahmemeldungen zu erstellen. Das Übermitteln einer bereits gemeldeten Freiheitsbeschränkung in einer zweiten Meldung ist möglich und würde als separate, zusätzliche Beschränkung/Maßnahme gelten.

Folgende Aufhebungsgründe im Formular heben - **zusätzlich** zu den in der Aufhebung angegebenen Maßnahmen - allfällig noch aufrecht gemeldete Maßnahmen auf:

- entlassen/verzogen (ZUG) bzw. verstorben (TOT)  
führt zur Beendigung sämtlicher aufrecht gemeldeter Maßnahmen der betroffenen Person in der gesamten Einrichtung, da diese in der Einrichtung nicht mehr anwesend ist und somit nicht mehr beschränkt werden kann.

Beispiel:

Station 1 meldet die Maßnahmen Bett: „Seitenteile“ und „Bauchgurt“, Station 2 meldet die Maßnahme „Sitzhose“.

Station 1 markiert in der Aufhebungsmeldung nun mit ZUG oder TOT nur die Maßnahme „Seitenteile“. Automatisch werden damit auch die Maßnahmen „Bauchgurt“ von Station 1 und „Sitzhose“ von Station 2 aufgehoben.

- innerhalb der ER verlegt (UEB)  
führt zur Beendigung sämtlicher aufrecht gemeldeter Maßnahmen der absendenden Station (Organisationseinheit), da die betroffene Person dort nicht mehr beschränkt werden kann, weil sie nicht mehr auf der Station ist. Sehr wohl kann die betroffene Person aber noch in anderen Organisationseinheiten der Einrichtung aufhältig sein und beschränkt werden.

Beispiel:

Station 1 meldet die Maßnahmen Bett: „Seitenteile“ und „Bauchgurt“, Station 2 meldet die Maßnahme „Sitzhose“.

Station 1 markiert in der Aufhebungsmeldung nun mit UEB nur die Maßnahme „Seitenteile“. Automatisch wird damit auch die zweite Maßnahme „Bauchgurt“ von Station 1 aufgehoben. Die Maßnahme „Sitzhose“ von Station 2 ist davon nicht betroffen.

Es empfiehlt sich, den NutzInnen vor dem Schließen eines PatientInnen-/BewohnerInnen-/KlientInnen-Aktes im Fall aufrecht gemeldeter Freiheitsbeschränkungen einen entsprechenden Hinweis zu geben, diese Maßnahmen der Bewohnervertretung als beendet mitzuteilen.

## **RÜCKGABE DES SERVICES**

Das Service berichtet mittels HttpStatusCodes über den Erfolg bzw. Misserfolg der gemeldeten Daten.

### **HttpStatusCodes**

- 200 (OK): Meldung erfolgreich gespeichert
  - Zusätzlich wird eine ID zurückgegeben. Diese dient als Referenzwert und sollte in der Software im entsprechenden Akt hinterlegt werden, um die zukünftige Kommunikation mit der Bewohnervertretung zu vereinfachen.
- 400 (Bad Request):
  - Es konnte keine Einrichtung zu dem Zertifikat gefunden werden.
  - Es wurde kein gültiges XML übermittelt.
  - Das XML enthält Fehler.
- 403 (Forbidden): Ungültiges Zertifikat oder kein Zertifikat vorhanden