



BLIKSUND

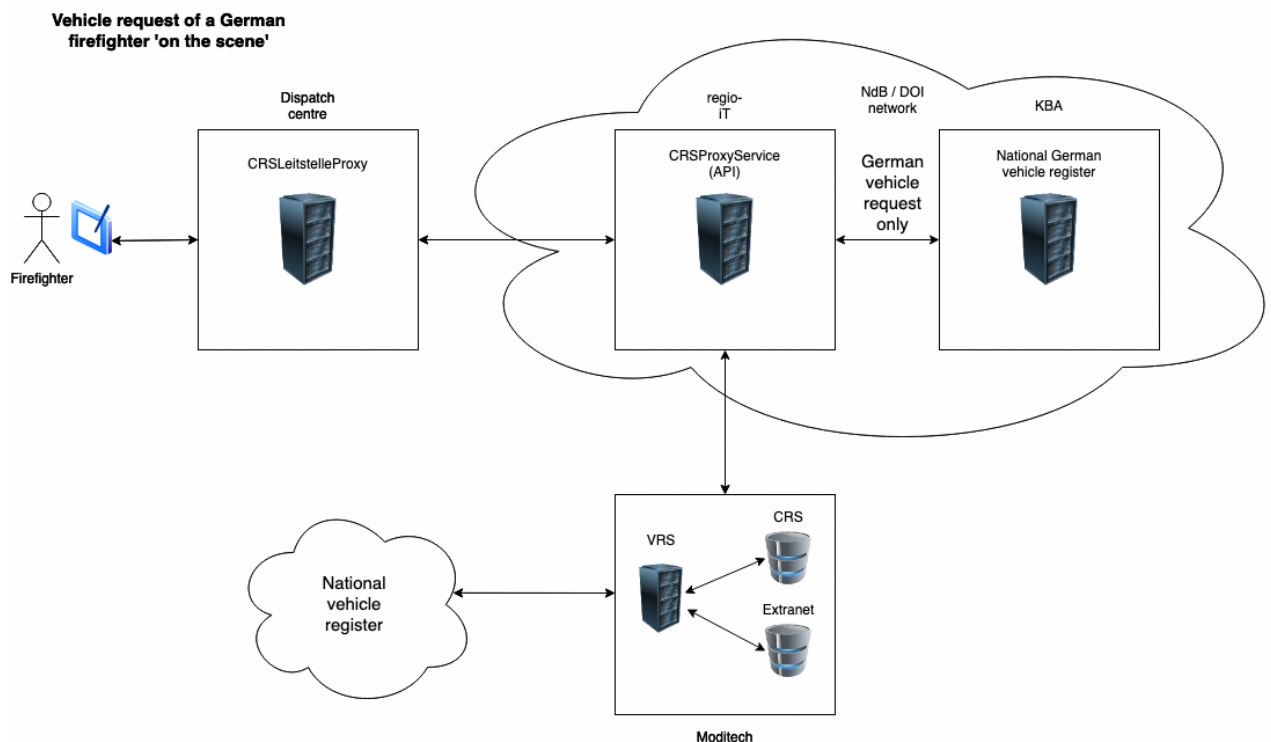
Leitstelle Proxy Installation Crash Recovery System (CRS)

Versie: July 2025

Introduction

In Germany only German number plates can be requested from a dispatch centres (Leistelle) premise to the KBA (national vehicle register of Germany). A fire fighter on the scene of an accident is not allowed to make a direct number plate request. To by-pass this restriction, the dispatch centre can install the CRSLeitstelleProxy WebApi in it's premise. Because the proxy is hosted in the premise of the dispatch centre and number plate request is sent from this location, it is allowed to make connection to the KBA. The device of the fire fighter has to be configured to make connection to this proxy. The proxy has to be public accessible for the fire fighter of the dispatch centre.

Schematic diagram



In the preferences of the application, the address of the Dispatch Centre Portal is set to the public URL of the CRSLeitstelleProxy, e.g. <https://crs.beispiel-leitstelle.de/>. The CRSLeitstelleProxy is hosted at the Dispatch Centre.

As soon as the firefighter request for vehicle data by numberplate or VIN, the request is sent to the CRSLeitstelleProxy API. The vehicle request will be forwarded to the CRSProxyService hosted in the secured and private network 'NdB / DOI' network. The dispatch centre is responsible for making a connection between their own network and the 'NdB / DOI' network. If the CRSProxyService receives a request, it will check the country of the vehicle request. A German vehicle request, will be directly forwarded to the KBA (national vehicle register of Germany). Requests for all other countries will be sent to the VRS (VehicleRegistrationService) directly hosted at Bliksund. The VRS will request for vehicle data in the national vehicle register of the specific country and for matching data in the CRS-database.

The reply of the KBA will be forwarded to the VRS hosted at Bliksund for matching the vehicle data in the CRS-database. The result of this request will be returned to the CRSProxyService which will send back the reply to the CRSLeitstelleProxy. The CRSLeitstelleProxy will then send the reply back to the device of the firefighter.

Requirements

The proxy is an ASP.NET Core WebApi. The server on which the interface is hosted, should meet the following requirements:

- Windows Server 2012 – 2019.
- IIS with ASP.Net Core 3.0 installed.
- Access to the secured NdB / DOI network from this server (our server in the NdB/DOI network should be reachable at <https://moditech.regioit.testa-de.net>).
- The webserver should be public available via an URL, e.g. <https://crs.beispiel-leitstelle.de/>.
- A secured HTTPS connection / certificate, as this is requirement by the apps.

Installation

IIS

To install and configure IIS on the server, follow the steps as described by this article of Microsoft:

<https://docs.microsoft.com/en-us/iis/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2>

ASP.Net Core 3.0

After the installation and configuration of IIS, install the ASP.Net Core 3.0. It is recommended to install the Hosting Bundle which includes the .NET Runtime and IIS support. The installer can be downloaded from the following location:

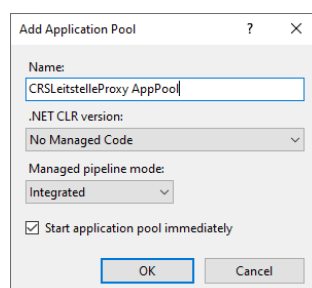
<https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-aspnetcore-3.0.3-windows-hosting-bundle-installer>

After downloading the installer, click on it to start the installation. Click on Install button and follow the wizard to install the required files.



IIS Application Pool

.Net Core apps in IIS needs a new application pool to work with the '**No managed code**' option. To create the application, open the IIS Manager and then navigate to '**Application Pools**'. Next click on '**Add Application Pool**'. In the dialog enter a name for the application, e.g. 'CRSLeitstelleProxy AppPool'. For the .NET Framework Version, choose '**No Managed Code**'. The other options can be left as-is.

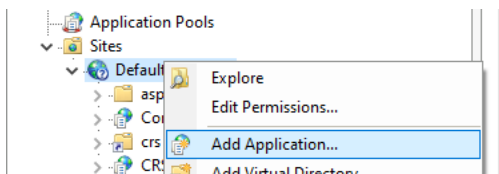


The created application pool should be listed in the Application Pool panel.

IIS WebApi

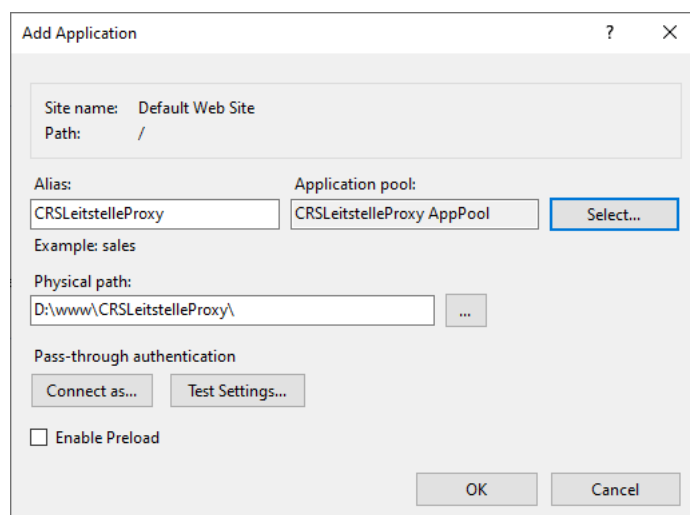
After the application pool is created and is ready to use, the WebApi has to be added as an application to IIS.

To add the application, open the IIS Manager, from the left menu unfold 'Sites' and right-click on 'Default Web Site'. In the context-menu, select 'Add Application...'.



In the 'Add Application' dialog, enter the name for the application '**CRSLeitstelleProxy**' and assign the created application pool '**CRSLeitstelleProxy AppPool**' to it. Beware the name of the application is related to the URL on which the WebApi can be reached. For example, if the base address of the server is <https://crs.beispiel-leitstelle.de>, the application is reachable at <https://crs.beispiel-leitstelle.de/CRSLeitstelleProxy/>

Next, select the physical path of the WebApi's folder. Make sure that this folder is created anywhere within the server's drive.



SSL Certificate

For security and because the (mobile) CRS apps requires HTTPS connections, a SSL certificate must be installed on the IIS server. The dispatch centre is responsible for creating and maintaining the SSL certificate. The most important information of the SSL certificate is the common name in the certificate. The common name must be the fully-qualified domain name (FQDN) (e.g. crs.beispiel-leitstelle.de). A wildcard certificate is also possible, in that case the common name will be e.g. *.beispiel-leitstelle.de

To request and install an SSL certificate in IIS, follow the steps as described by this article of Digicert: <https://www.digicert.com/kb/csr-creation-ssl-installation-iis-10.htm>

Basic authentication (optional)

It is not required to add Basic Authentication to the CRSLeitstelleProxy Service. However for safety reasons it is recommend to do so. To install and configure Basic Authentication in IIS, follow the steps as described by this article of Microsoft:

<https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/basicauthentication>

After the basic authentication is installed and configured, a user has to be added. The credentials of this user must be entered in the apps for authentication purposes.

To add a user, right click on **'Computer'** if available on the desktop. Otherwise go to **'Control Panel'**, navigate to **'Administrative Tools'** and click on **'Computer Management'**. Next, choose **'Manage'** and under **'Local Users and Groups'** a new user can be added. Edit the user and remove all the roles. Untick the option 'User must change password at next logon' and tick the option 'User cannot change password'. After the user is created, give that user permission to read the directory where the application is hosted.

WhiteList

To prevent other firefighters from other dispatch centre making use of this specific instance of the CRSLeitstelleProxy, only licence codes registered in the whitelist can access the CRSLeitstelleProxy. Administrators of the dispatch centre can add or remove the licence code(s) in the list. Normally this will be a site licence code.

Currently the whitelist is administered in a text-file. Each licence code is entered on a separate line. The whitelist should be kept out of the Webroot of the application. The text-file can be stored anywhere on the local drive of the server. However, make sure the user on which the API runs have enough user rights to read the file.

The path to this file can be administered in the appsettings.json file of the CRSLeitstelleProxy with the following setting:

```
"CRSPProxyLicenceCodeWhiteListOptions": {  
  "FilePath": "D:\\whitelist\\whitelist.txt"  
}
```



Caching (Experimental)

This is an experimental setting. The CRSLeitstelleProxy can cache the vehicle request for 5 days. With caching enabled it will not forward every request to national vehicle request, but return the result of the cache if the vehicle is request earlier. The result from the cache will be returned immediately to the user.

Enabling or disabling return vehicle request can be administered in the appsettings.json file:

```
"CRSPProxyVehicleRequestServiceOptions": {  
    "EnableCache": false  
}
```

CRSPProxy options

The connection settings for the CRSPProxy service hosted in the NdB / DOI can be administered in the CRSPProxyVehicleRegistrationOptions section of the appsettings.json file. However, normally it is not needed to change these settings. Keep them as is unless instructed to change them.

```
"CRSPProxyVehicleRegistrationOptions": {  
    "URL": "https://moditech.regioit.testa-de.net/CRSPProxyService/",  
    "Port": 443,  
    "Username": "moditechapi",  
    "Password": "1XK0hN0kA/nizCEuU9yH8w=="  
}
```

Default Appsettings.json

```
{  
    "Logging": {  
        "LogLevel": {  
            "Default": "Information",  
            "Microsoft": "Warning",  
            "Microsoft.Hosting.Lifetime": "Information"  
        }  
    },  
    "CRSPProxyVehicleRegistrationOptions": {  
        "URL": "https://moditech.regioit.testa-de.net/CRSPProxyService/",  
        "Port": 443,  
        "Username": "moditechapi",  
        "Password": "1XK0hN0kA/nizCEuU9yH8w=="  
    },  
    "CRSPProxyLicenceCodeWhiteListOptions": {  
        "FilePath": "D:\\whitelist\\whitelist.txt"  
    },  
}
```



```
"CRSPProxyVehicleRequestServiceOptions": {  
    "EnableCache": false  
},  
"AllowedHosts": "*" }  
}
```