Giegerich & Partner

Enterprise KeyServer

Giepa EKS

Administrator Manual

GiepaEKS AdminManual

Revision: 2016/April/28

Content

1 Introduction

The purpose of this manual is to describe to administrators the installation steps, capabilities and configuration of the *Giegerich & Partner Enterprise KeyServer*, abbreviated **EKS**.

The EKS is a keyserver for OpenPGP-Keys designed for small and medium enterprises.

EKS can be used with GnuPG and compatible PGP-software either via the OpenPGP HTTP Keyserver Protocol (HKP) or a web interface. Standard keyserver functions include search, download and upload of keys.

EKS will support all functions when used in combination with a current version of gpg4o, also available from Giegerich & Partner GmbH.

If EKS is running with Windows NTLM (Active Directory) authentication enabled, it also allows authorized users to delete keys through the web interface.

For the purposes of this document the example URL http://localhost:11371 is used. Please use a valid IP address or DNS host name as configured in your network instead of "localhost" where applicable.

2 System requirements

Supported operating systems (64-bit versions only):

- Windows 7 with Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2012 R2

Windows update KB3005628 is required to be installed on all systems (except Windows 7). Please visit the following website for details:

https://support.microsoft.com/en-us/kb/3005628

It is highly recommended to enable Windows Update for automatic updates of the operating system and to apply all security patches when available.

Newer versions of Windows (e.g. Windows Server 2016) will be supported officially after final release versions of an OS have become available.

The setup program requires administrative privileges on the OS.

The following system software will be installed by the EKS setup program when necessary:

- .NET Framework 3.5
- .NET Framework 4
- .NET Framework 4.6.1
- Microsoft SQL Server 2014 Express with Advanced Services
- Internet Information Server (version 7.5, 8 or 10 corresponding with the OS version)
- ASP.NET and required features
- IIS URL Rewrite Module

2.1 Internet connection

An Internet connection is required for operating a publically reachable keyserver.

TCP ports used by the Keyserver:

- 11371 Keyserver website default port
- 443 Optional: website SSL/TLS port, SSL/TLS needs to be configured in IIS.
- 80 Optional: for redirection to the website on port 11371

EKS offers in the Maintenance Tool commands to create firewall rules to allow inbound traffic to TCP port 11371 and to ICMPv4 (Echo protocol for Ping reachability).

For external connectivity these ports need to be forwarded / opened in your network's configuration, i.e. on the router, proxy server or dedicated firewall.

The setup program will check the Internet connection by attempting to connect to URLs at microsoft.com and giepa.de.

3 Installation

The keyserver will be installed with the GiepaEKS_Setup.exe program. The setup program is available via download from the Giegerich & Partner GmbH website or on an installation DVD.

3.1 Components

EKS encompasses a number of different components:

- KeyServer website (using ASP.NET 4.5 on IIS)
- KeySyncService
- Maintenance Tool
- SQL Database and ODBC DSN

The EKS setup program will install and configure all components and system software automatically.

EKS components and system software packages exist as MSI and executable files in subdirectories below the Redist folder of the setup program.

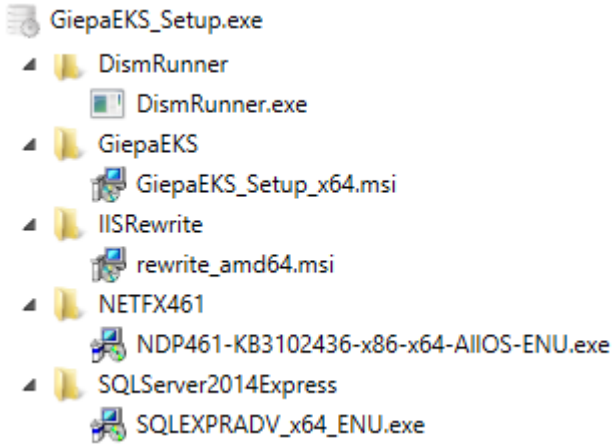

Figure 1: Setup components

3.2 .NET Framework 3.5 and 4

Default installations of current Windows operating systems (Windows 8 or later) do not automatically include the Microsoft .NET Framework in version 3.5. This component is required by Microsoft SQL Server 2014 Express.

The setup program will attempt to install this component automatically if it is detected as missing but requires an Internet connection to download necessary files from the Microsoft Windows Updates website. If no connection to that website could be opened, the setup program will show a corresponding error message.

It is possible to install the .NET Framework 3.5 manually offline (with the Windows installation DVD or image) by using the Windows Control Panel, Programs, "Turn Windows features on or off" and selecting the ".NET Framework 3.5 (includes .NET 2.0 and 3.0)".

Detailed instructions for offline installation of the .NET Framework 3.5 are available on the following websites:

https://msdn.microsoft.com/en-us/library/hh506443%28v=vs.110%29.aspx

https://support.microsoft.com/en-us/kb/2785188

On Windows 7 systems where .NET Framework 4 is not present already, the setup program will install it as the first step before the welcome page is displayed.

3.3 Setup steps

The setup program will guide you through the various steps to install the necessary components and packages. After starting the setup the welcome page will be displayed.

When necessary, warning and error messages will be shown to notify of possible issues like version conflicts, executables still running or a missing Internet connection.

3.3.1 Setup welcome page

On the welcome page the installation folder for the EKS Maintenance Tool application (and the KeySyncService program) can be selected.

The setup program's language can be selected (English or German/Deutsch) by clicking the language box in the title bar.

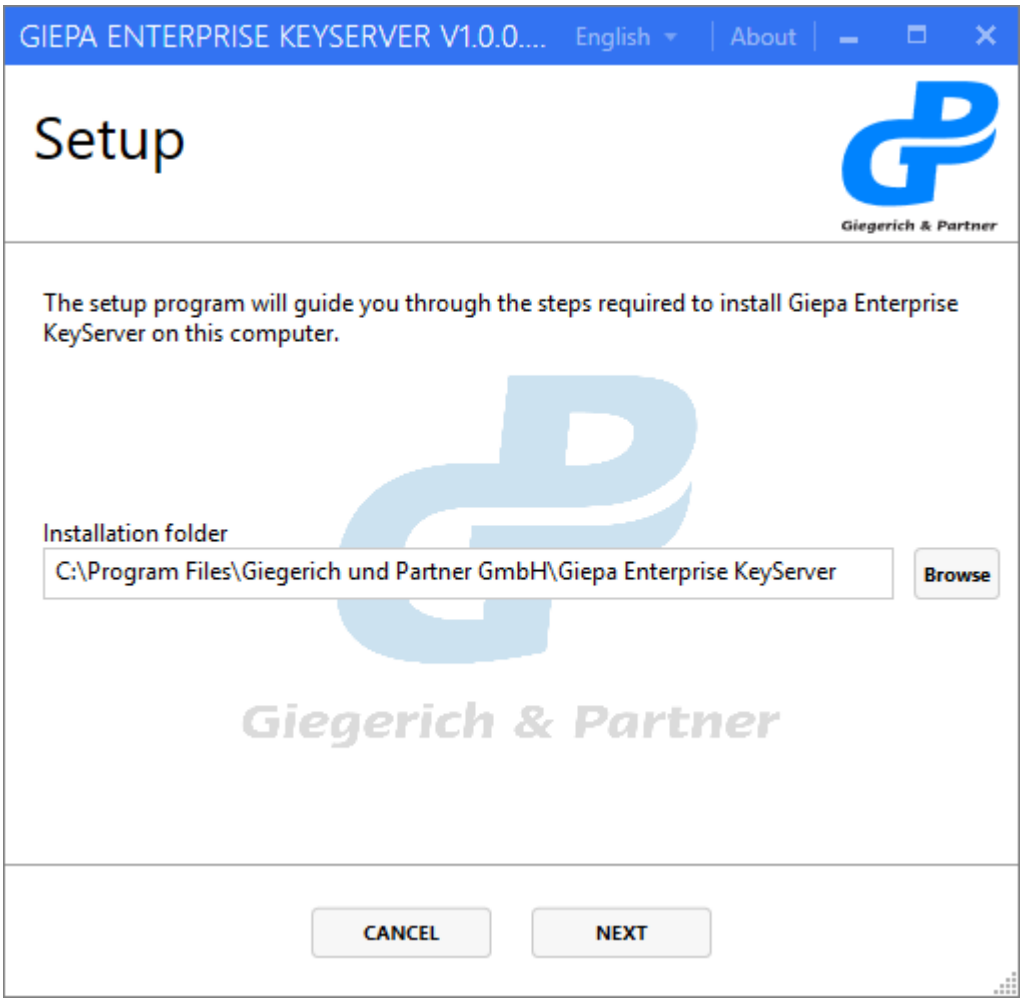

Figure 2: Setup welcome page

The EKS website will be automatically installed into a subfolder of the default IIS Inetpub folder, usually into C:\Inetpub\KeyServer.

In case the setup program detects a general problem a warning or error message will be shown.

After clicking on the „Next" button the EULA page will be displayed.

3.3.2 Setup EULA page

To continue to the next page acceptance of the EULA needs to be confirmed by clicking the checkbox.

Figure 3: Setup EULA page

After confirming the EULA and clicking on "Next" the feature selection page will be displayed. Most features are vital and cannot be deselected.

3.3.3 Setup feature selection page

Most features shown in the feature list are vital to EKS and cannot be deselected.

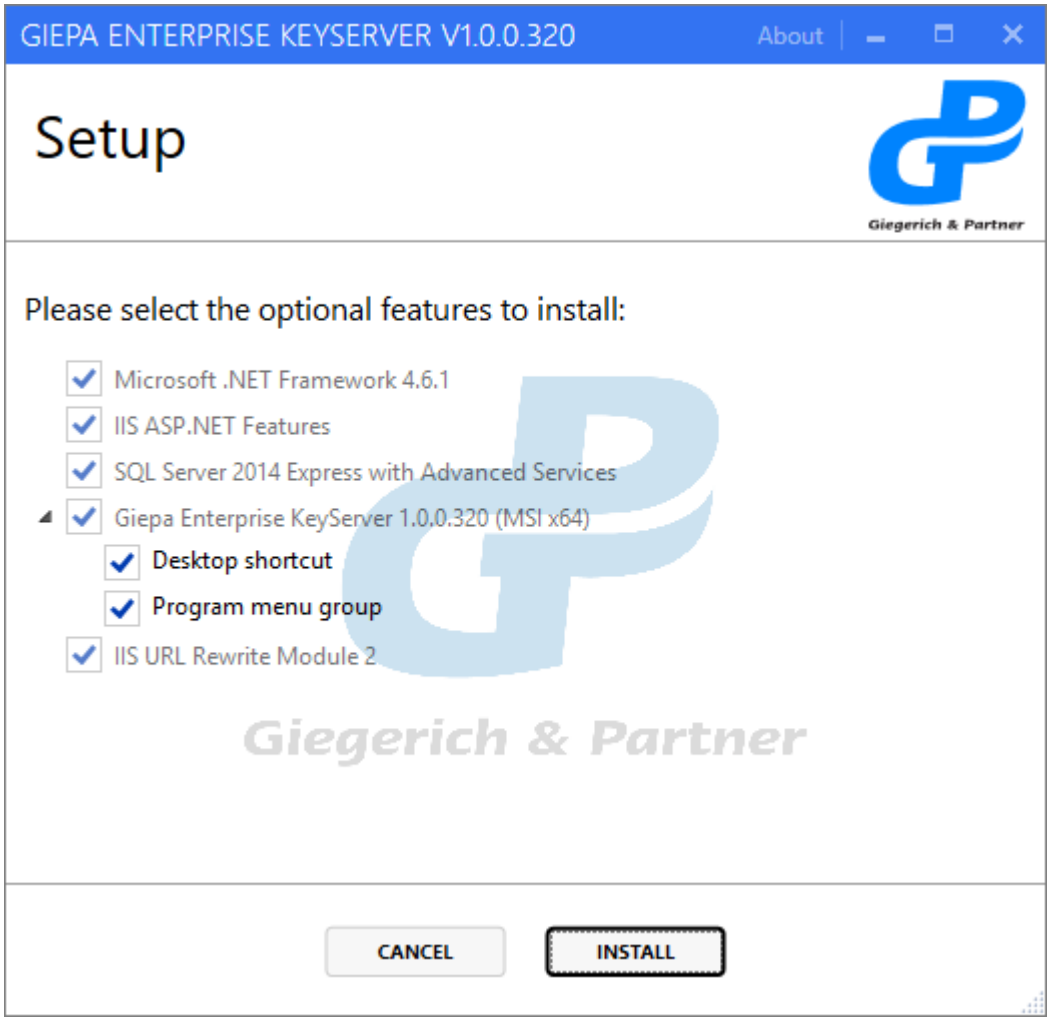

Figure 4: Setup feature selection page

The feature list might show already installed components. The status of the components will be detected during the setup process and only be reinstalled when required.

3.3.4 Setup progress page

After clicking the “Install” button the actual installation of EKS will commence.

The setup process may take up to 15 minutes depending on the number of components that need to be installed.

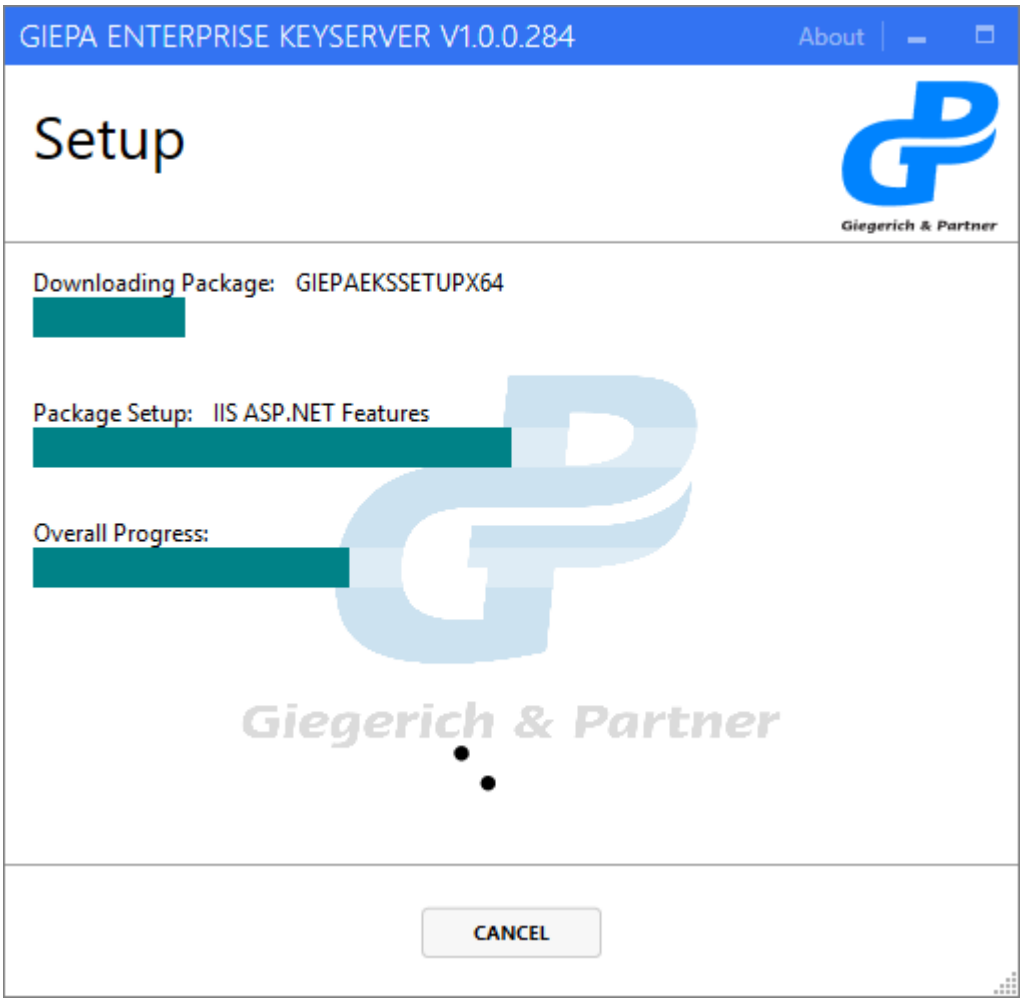

Figure 5: Setup progress page

3.3.5 System restart during setup

To install the system software components .NET Framework 3.5 and .NET Framework 4.6.1 the setup program might require an intermediary system restart.

A corresponding result page will be displayed by the setup program when applicable:

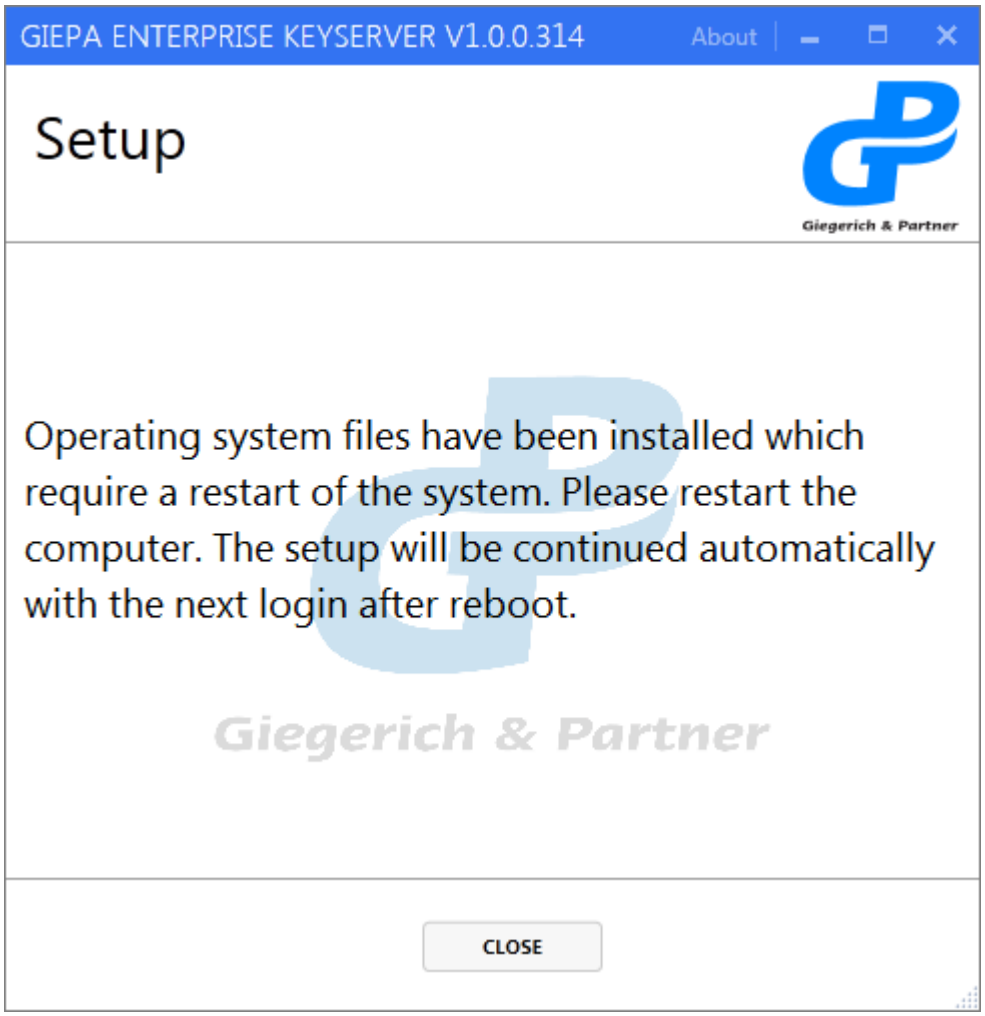

Figure 6: Setup result requiring system restart

The setup program will automatically be executed afresh after the restart.

3.3.6 Setup result page

When the setup process has finished the result page will be displayed. In case of any errors during the setup process an error code and an explanation for errors that occurred will be given.

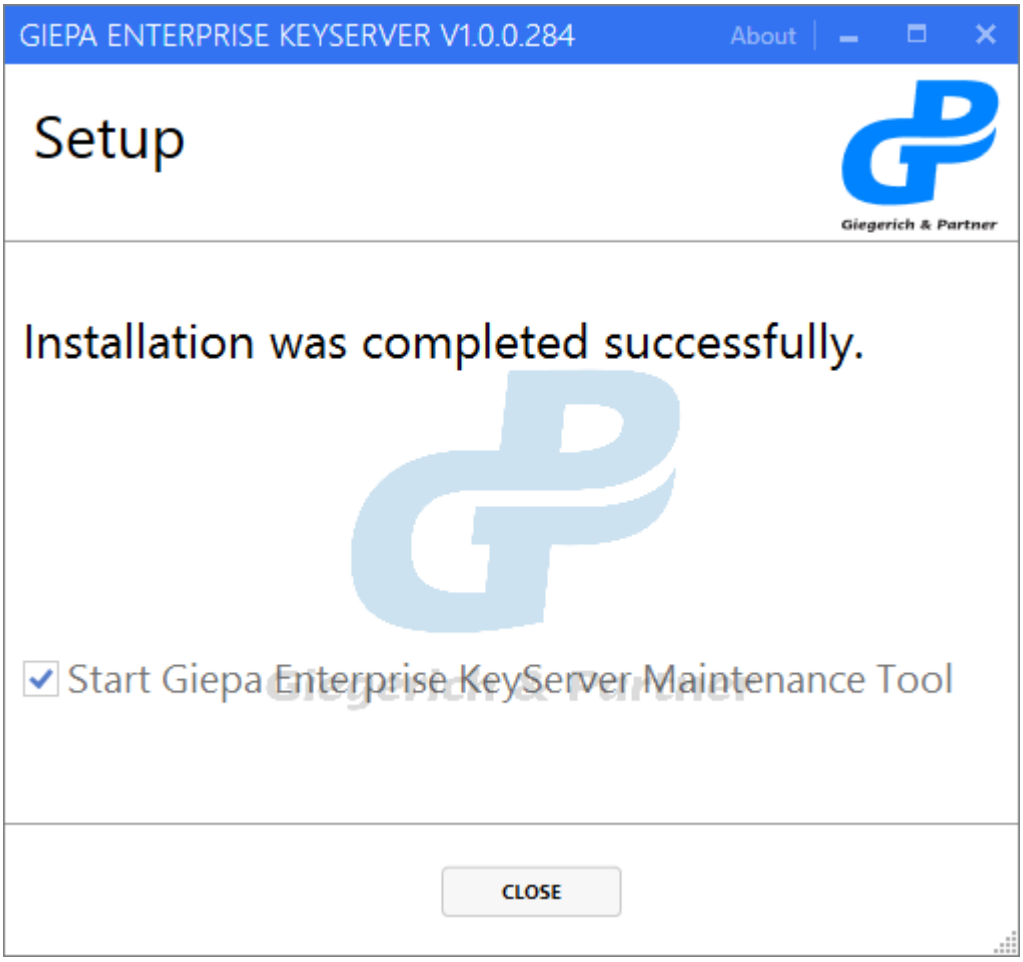

Figure 7: Setup result page

The EKS Maintenance Tool will be started automatically after the setup program is closed. This cannot optionally be deselected because an initial configuration needs to be set by the Maintenance Tool application.

The setup program will create shortcuts to the Maintenance Tool and to a PDF file of this manual.

3.3.7 Initial Maintenance Tool execution

After a successful installation the EKS Maintenance Tool will be started automatically to initialize the necessary EKS configuration settings including the setup of the SQL Server database, IIS website settings and the ODBC DSN item.

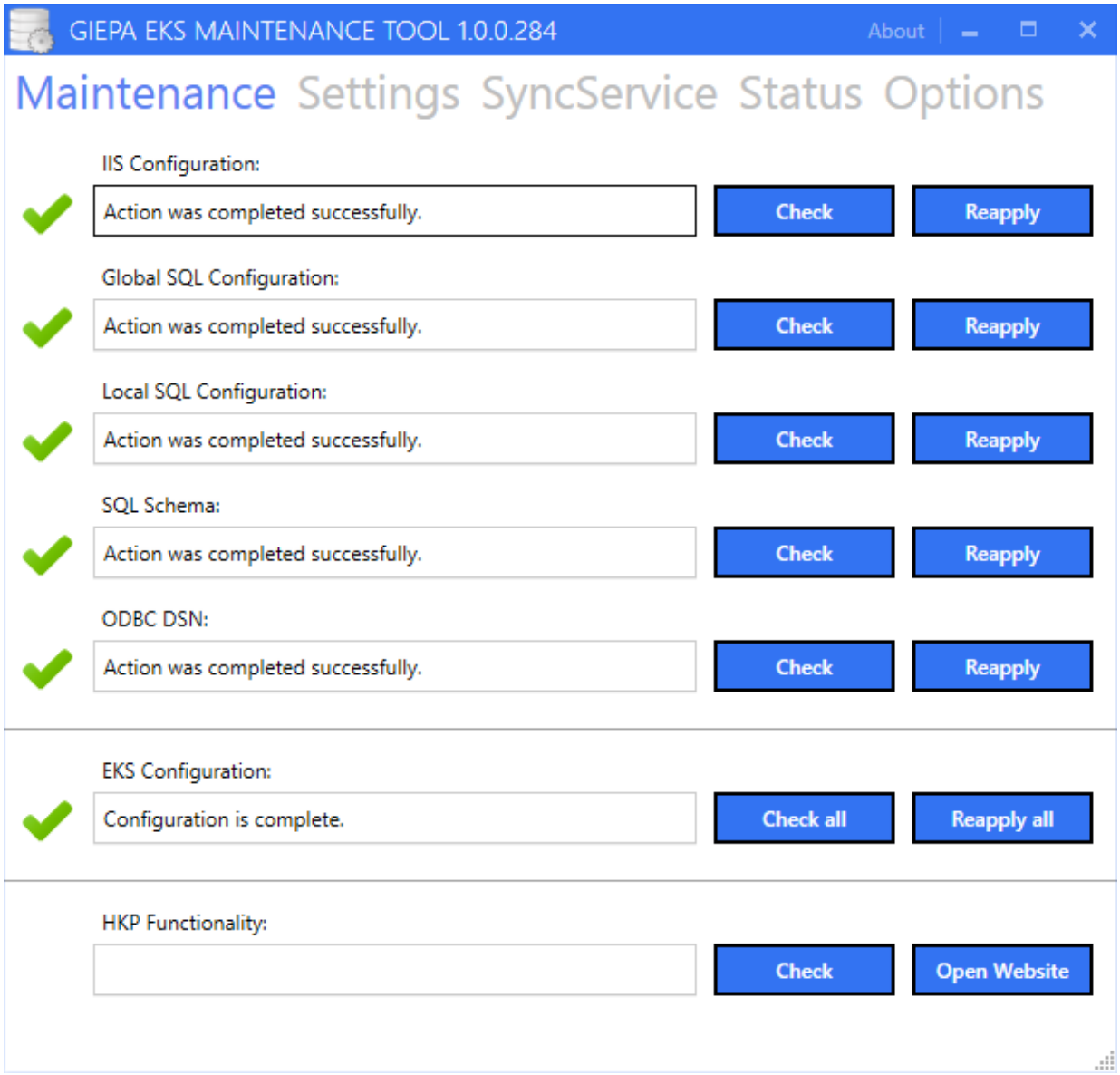

Figure 8: Setup initial execution of Maintenance Tool

The EKS configuration needs to be complete for the EKS to function correctly. Basic functionality of the EKS can be verified by clicking the HKP "Check" button. This will upload and download a Giegerich & Partner support key to the localhost server. Clicking on "Open Website" will open the EKS website at http://localhost:11371

3.4 Update or migration from another keyserver

Data from a different keyserver (EKS or SKS) can be migrated or copied to a new EKS installation.

Updates of existing EKS installations between same major versions (e.g. from version 1.0.0.x to 1.1.0.x) do not require any changes or preparations as only the EKS software components will be updated, leaving the SQL database in place.

It is still recommended to create backups before any software installation.

3.4.1 Using EKS Maintenance Tool backups

Keyserver backups created with the Maintenance Tool can be restored on a fresh installation of EKS.

3.4.2 Using a Web browser

You can use a web browser to download all keys matching a search from a keyserver (both EKS and SKS) by replacing the “index” or “vindex” operation keyword with a “get”.

Example of search URL to search for all keys containing the text “gpg4o”:

http://localhost:11371/pks/lookup?op=index&search=gpg4o

Replace “index“ with “get“ to export the search results:

http://localhost:11371/pks/lookup?op=get&search=gpg4o

You can then simply copy the ASCII-armored key block from the downloaded .asc file and paste it into the upload page of the EKS website.

4 Server configuration and Maintenance Tool

The EKS Maintenance Tool (abbreviated MT) is an application that allows system administrators to maintain and change keyserver settings, add firewall rules, to modify the KeySyncService configuration, to create and restore backups and to collect log files for support purposes.

4.1 Maintenance tab

The setup program will automatically execute the EKS Maintenance Tool as the last step to apply the initial configuration settings on the system.

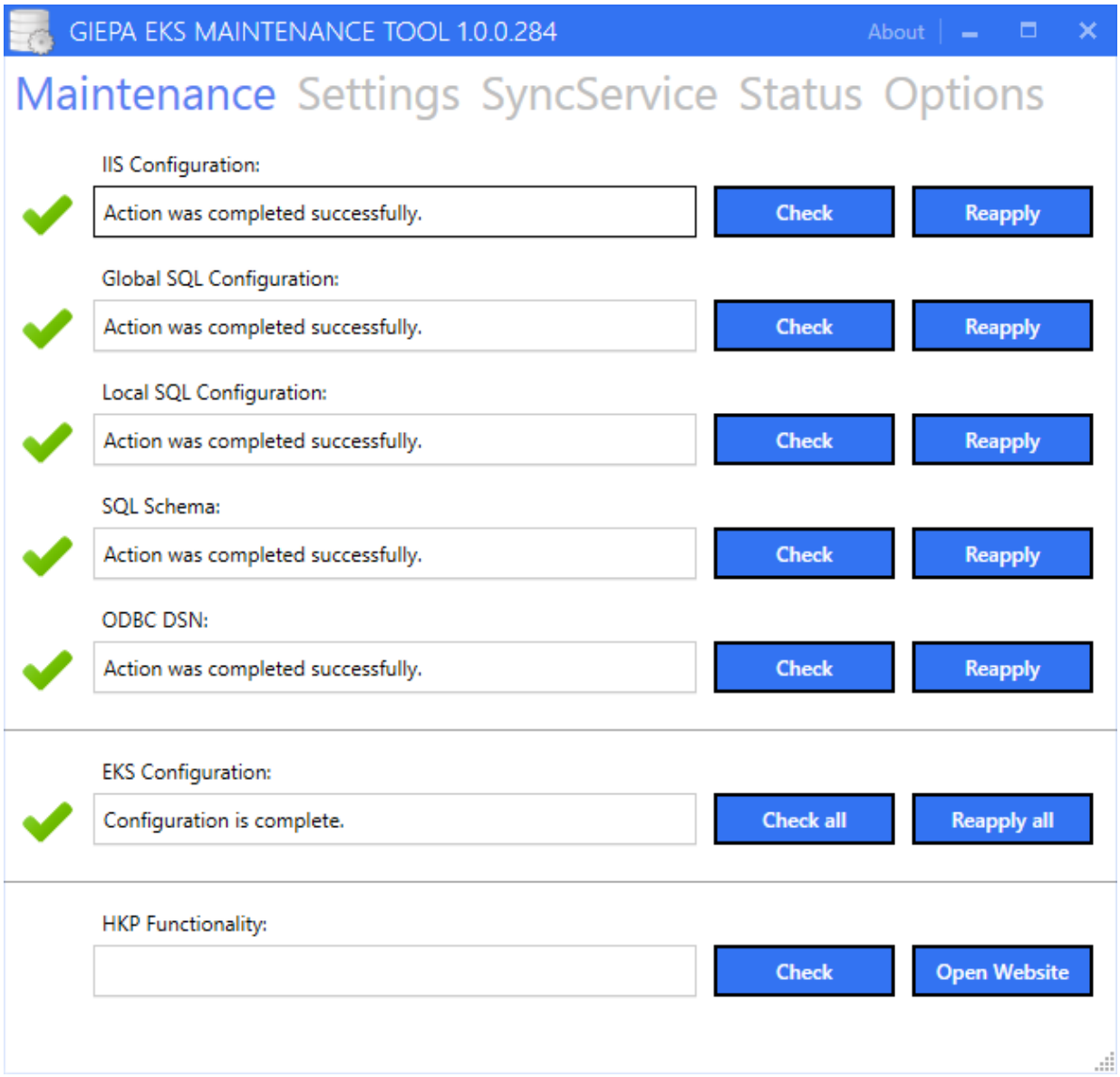

Figure 9: MT maintenance tab after setup

The maintenance tab shows the status for the required system components. All of the configuration items on this tab need to show a working status (as indicated by the green checkmark) for the EKS to function.

An incorrect configuration, an error as a result of an action or a disabled setting will be indicated by a white-on-red cross icon:

4.1.1 HKP functionality

HKP functionality of the keyserver can be checked manually. Clicking the “Check” button will upload and download a Giegerich & Partner GmbH support PGP-key to the local EKS.

4.1.2 Open website

Clicking on *Open Website* will open the local EKS website at address http://localhost:11371

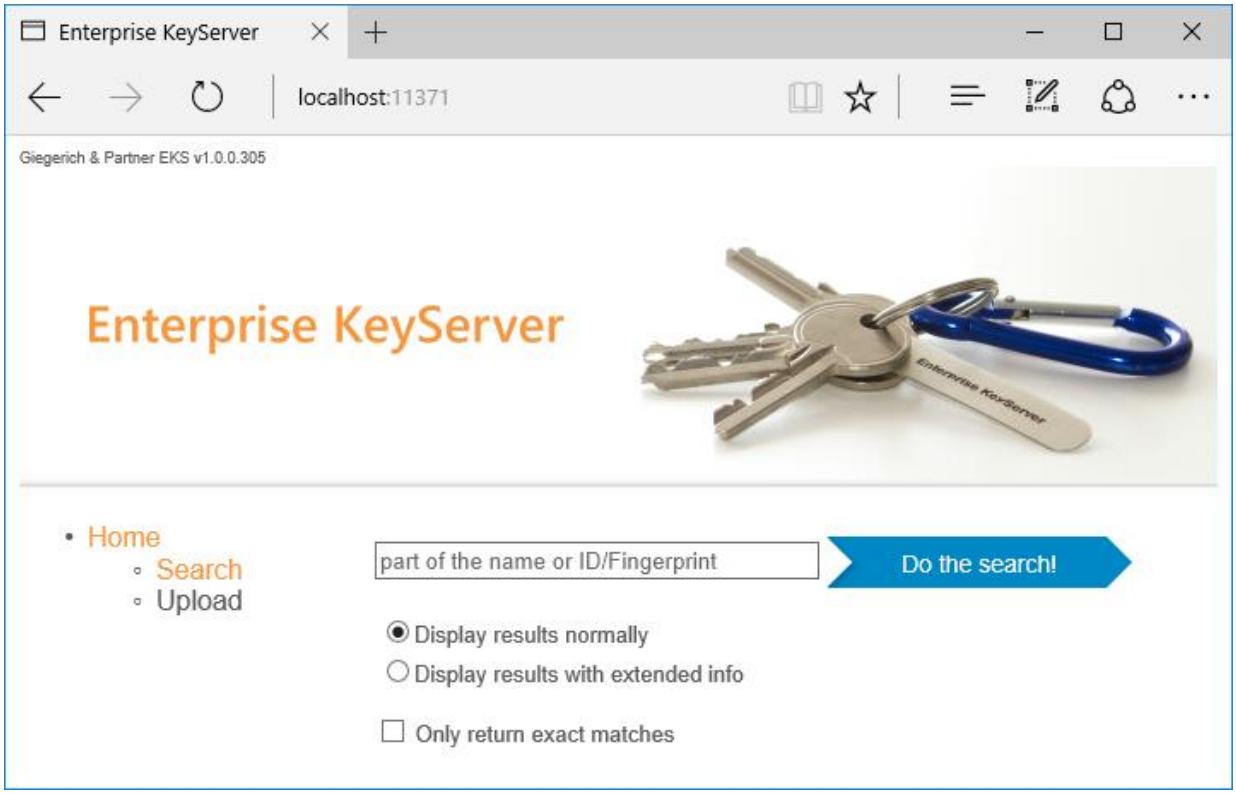

Figure 10: EKS default website, login button disabled

4.2 Settings tab

The settings screen in the Maintenance Tool allows administrators to optionally add or configure various system settings.

4.2.1 Keys database Backup and Restore

You can create and restore backups of the keys database stored by the SQL server. A default folder for backups can be selected; it will initially show the standard folder at:

c:\Program Files\Microsoft SQL Server\MSSQL12.GIEPAEKS\MSSQL\Backup

When changing that folder please ascertain that the SQL service account has write permission for that directory (i.e. only publically writable folders).

With the "Add date" checkbox you can select if filenames of backups should contain the date and time. Filenames will always start with GiepaEKSDatabase and use the .bak extension. Typically backup files will be named like this:

GiepaEKSDatabase_20160630111405.bak

It is recommended to periodically create backups of the keys database, specifically before applying any changes to the system like installing updates.

4.2.2 Log files zip

EKS will create various log files during its operation. For support purposes you can automatically collect and create a Zip of the log files from the previous 14 days. By default the Zip file will be saved on the user's desktop.

When contacting the Giegerich & Partner GmbH support (see section 6.2) by E-mail please attach the Zip of the log files for diagnosis and analysis by our engineers.

4.2.3 Firewall rules

By default the Windows Firewall will only allow inbound traffic for IIS on standard TCP ports 80 and 443. The Maintenance Tool can be used to add a rule to allow inbound traffic on the default keyserver website TCP port 11371.

Additionally a rule can be added to allow inbound traffic for ICMP (Echo only) to enable reachability of the system via *ping*.

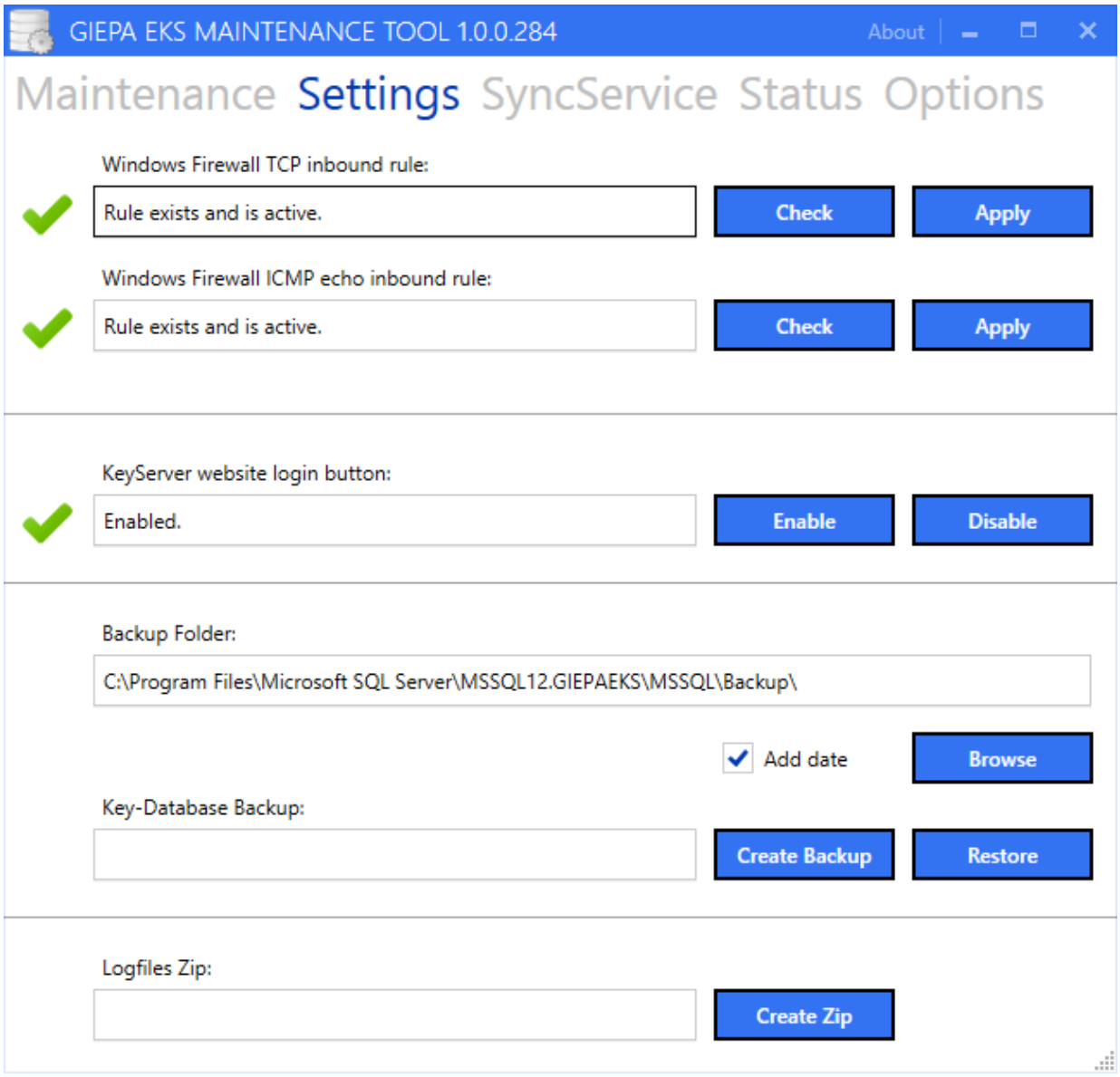

Figure 11: MT settings tab

Advanced firewall settings should be configured by administrators in the Windows Firewall options.

4.2.4 KeyServer website login button

To allow administration of the EKS and deletion of keys via the website a "Login" button can be enabled with the Maintenance Tool.

Enabling the website login button will enable Windows Authentication (NTLM) on the EKS website. When enabled, the website will show a Login button:

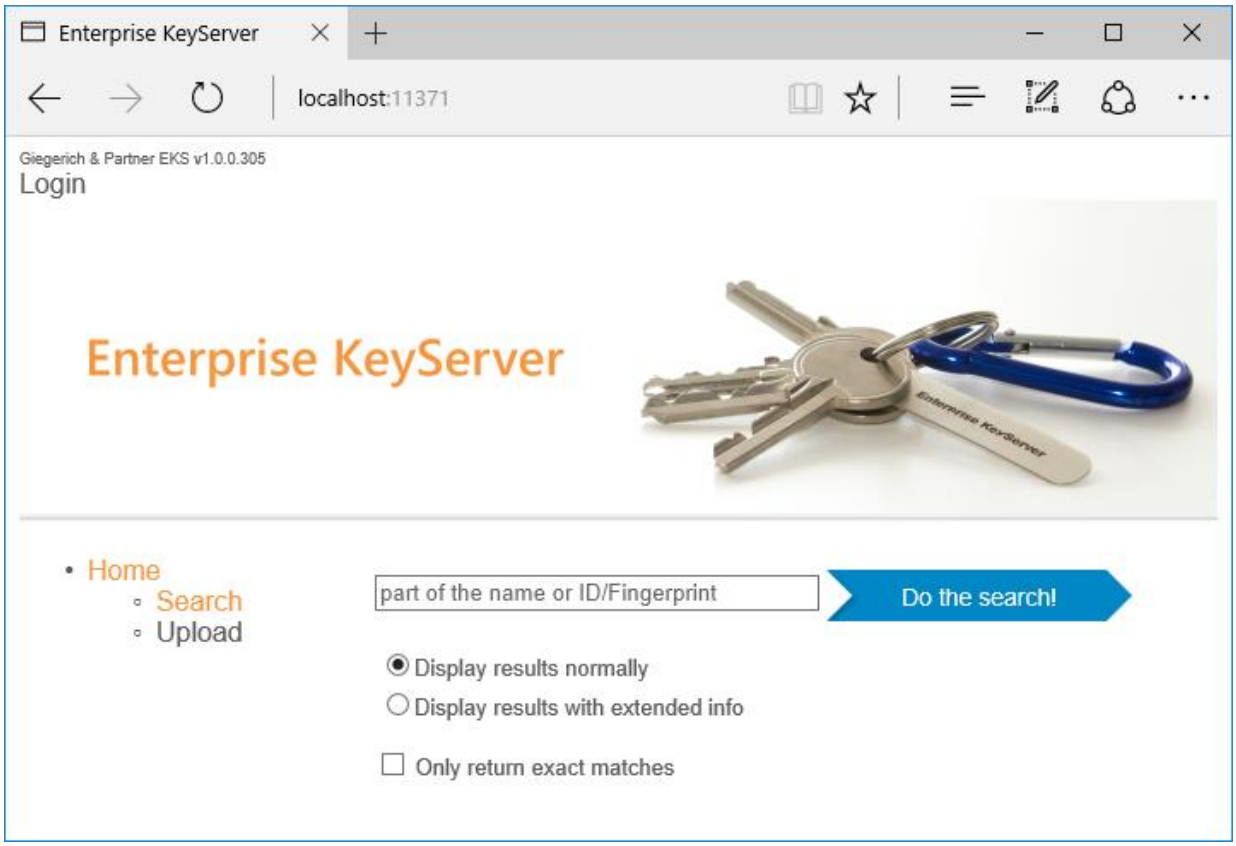

Figure 12: EKS website with login button enabled

4.2.5 EKS website authentication requirements

EKS uses Windows Authentication (NTLM) to verify login users.

Permission to edit EKS settings via the website is validated against membership in the local system user group “KeyServerAdmin”.

You can create this group in the Windows “Computer Management” panel, under “Local Users and Groups”. Add a “New Group” and use as group name “KeyServerAdmin”.

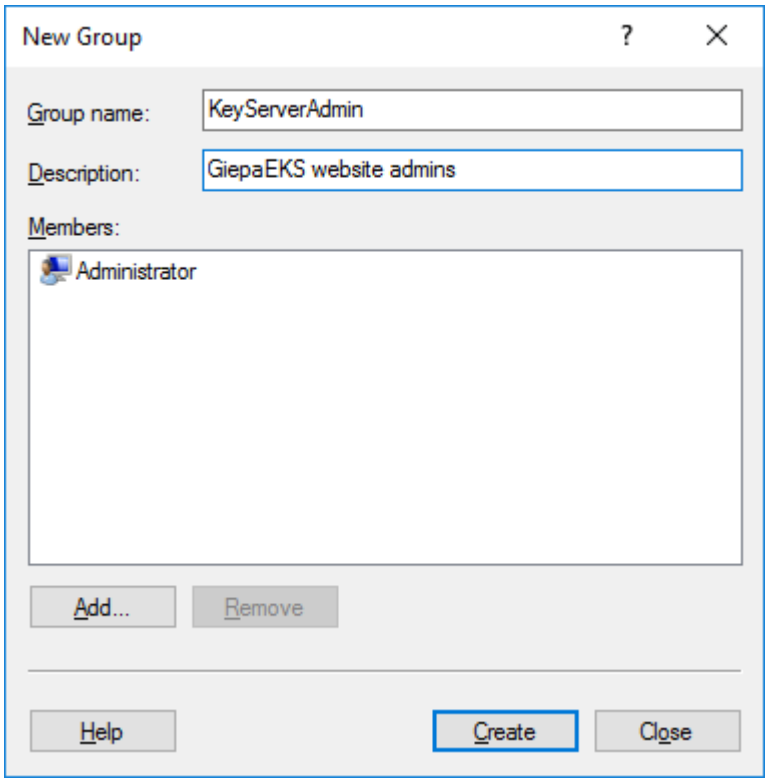

Figure 13: Creating KeyServerAdmin group

All users that should have permission to see and use EKS website settings and to delete keys need to be added to the local “KeyServerAdmin” user group.

4.3 SyncService tab

The SyncService tab allows administrators to control the KeySyncService settings. Sync tasks are defined in the file:

c:\Program Files\Giegerich und Partner GmbH\Giepa Enterprise KeyServer\KeySyncService\synctask.ini

Currently Sync Tasks need to be edited in the synctask.ini file. Explanations and a few sample tasks for uploading and downloading keys with and without search options are listed in that file.

You can chose one of the defined Sync Tasks and start it manually. The status image will show a green check icon when the task has been successfully started by the SyncService. The prerequisite to start a Sync Task is that the SyncService is installed and started.

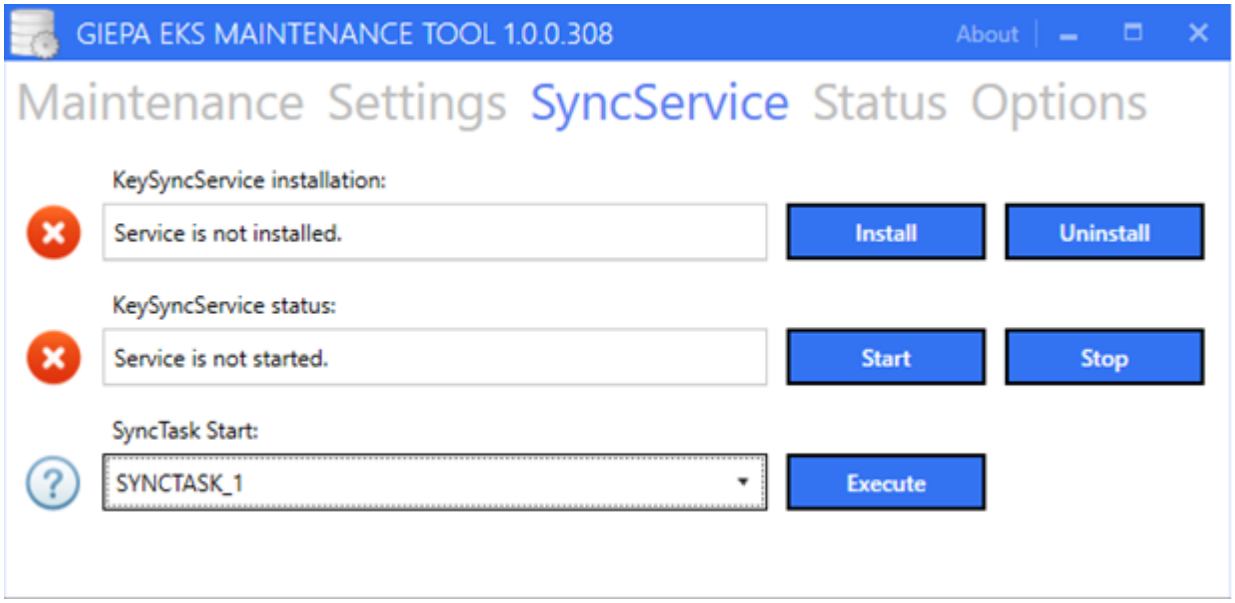

Figure 14: MT SyncService tab

4.4 Status tab

The status tab shows general information about the system environment, OS and component versions.

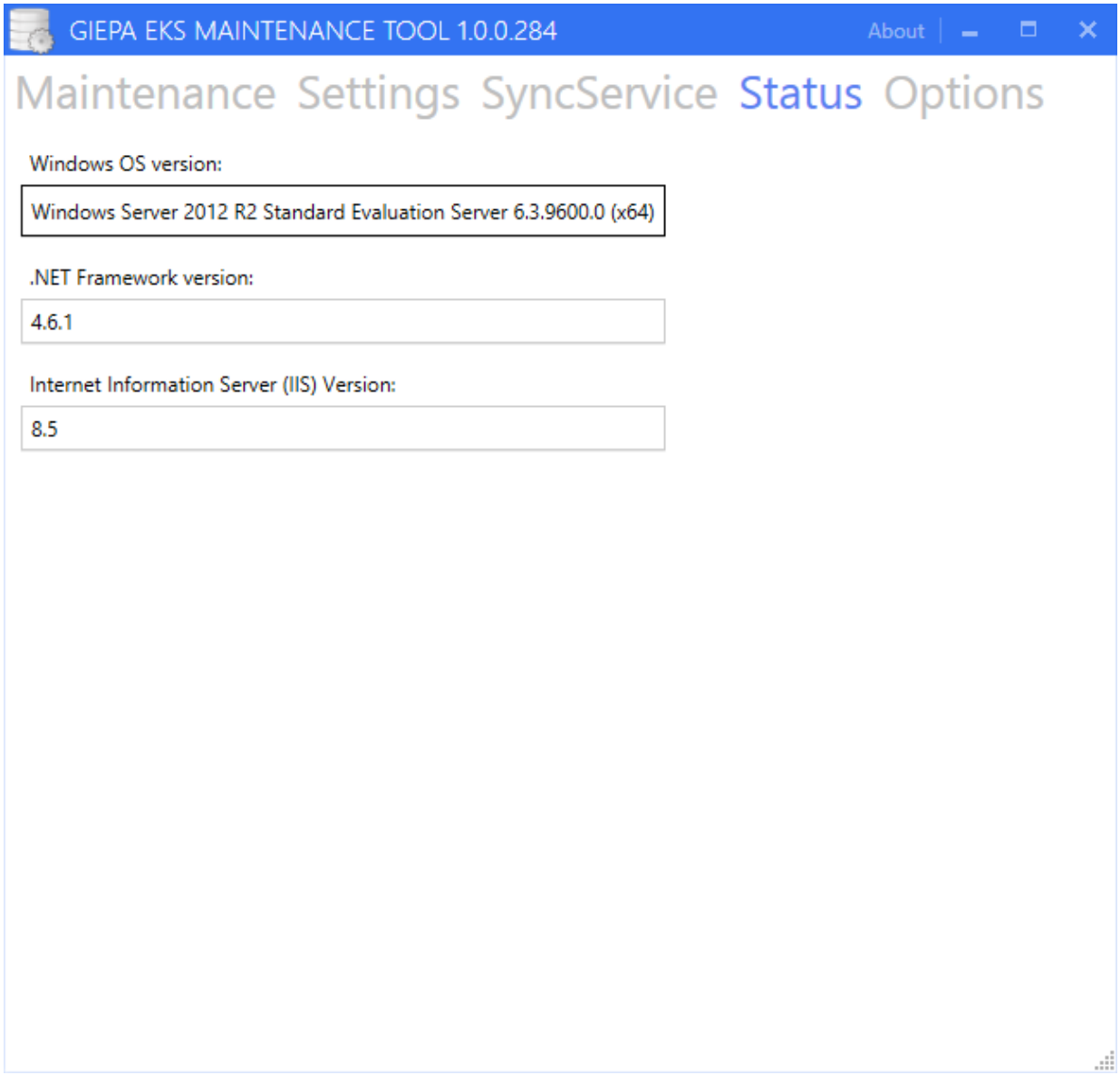

Figure 15: MT Status tab

4.5 Options tab

In the options tab MT application settings can be modified including the display language and themes.

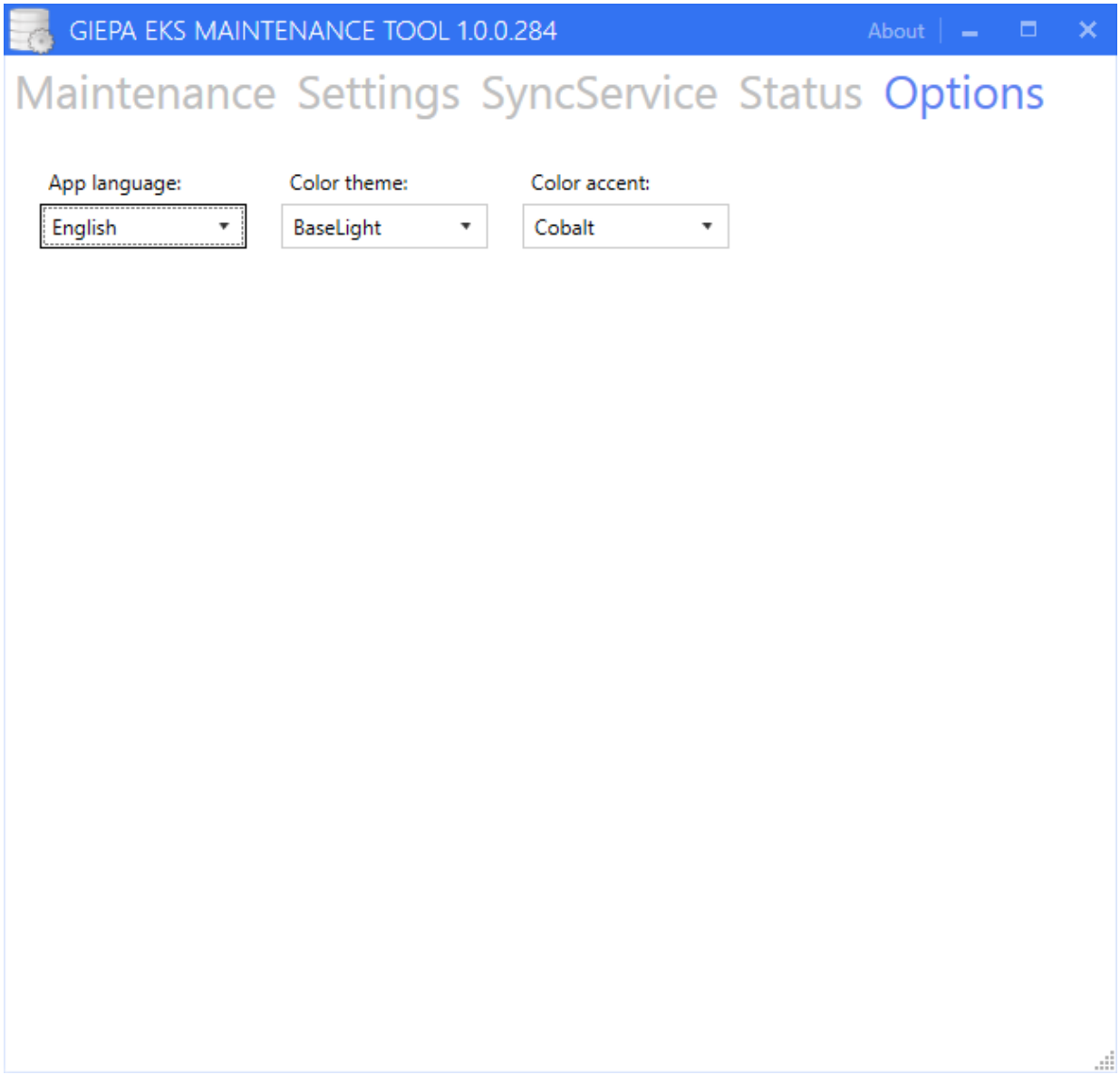

Figure 16: MT Options tab

4.6 Configuring other settings

It is possible to replace the banner image displayed by the EKS website. To do this overwrite the file banner.png located in C:\inetpub\keyserver\static_data with your own image file in PNG format.

5 Using EKS

Keyservers offer two different interfaces / protocols for communication:

- Via a Website (HTTP), by default on TCP port 11371
- Via the OpenPGP HTTP Keyserver Protocol (HKP), by default also using TCP port 11371

Basic keyserver functions like search, download and upload of keys are available with both methods.

5.1 EKS website home page

The EKS website will welcome a user on the keyserver home page, offering a form to search for keys.

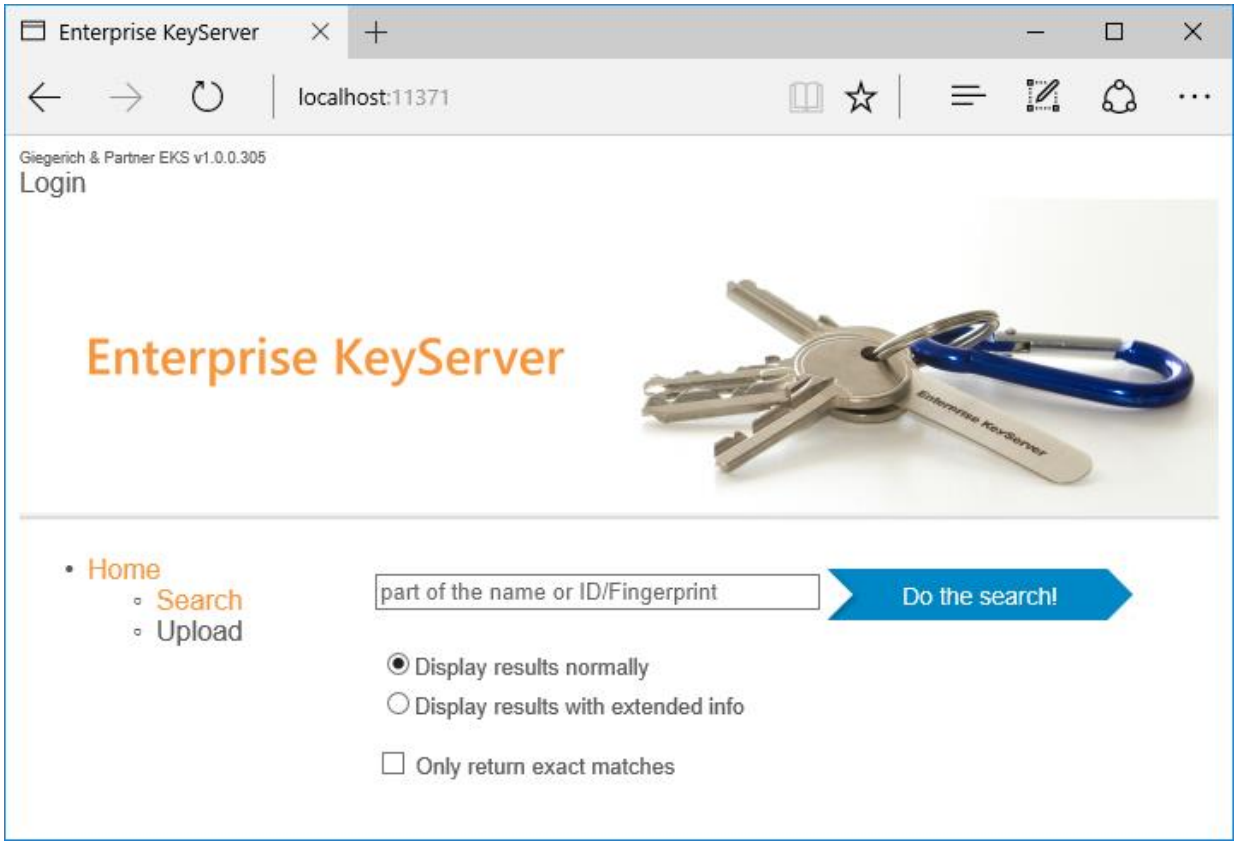

Figure 17: EKS website home page

The "Login" button will only be displayed if it was activated with the Maintenance Tool. Logging in is validated against NTLM / Kerberos authentication.

Users that are logged in will see a "User: <Domain\UserName>" instead of the Login button.

5.1.1 Searching and dowloading keys

You can search the available Keys on the server by a User ID or a fingerprint. Click the “Home” or “Search” buttons in the navigation panel on the left hand side to show the seach page.

Enter part of a key User ID or of the key fingerprint you want to search, then click on the “Do the search!” button.

In case you wish to get additional information e.g. the used encryption algorithm select “Display results with extended info”. The screenshot below shows a sample result set.

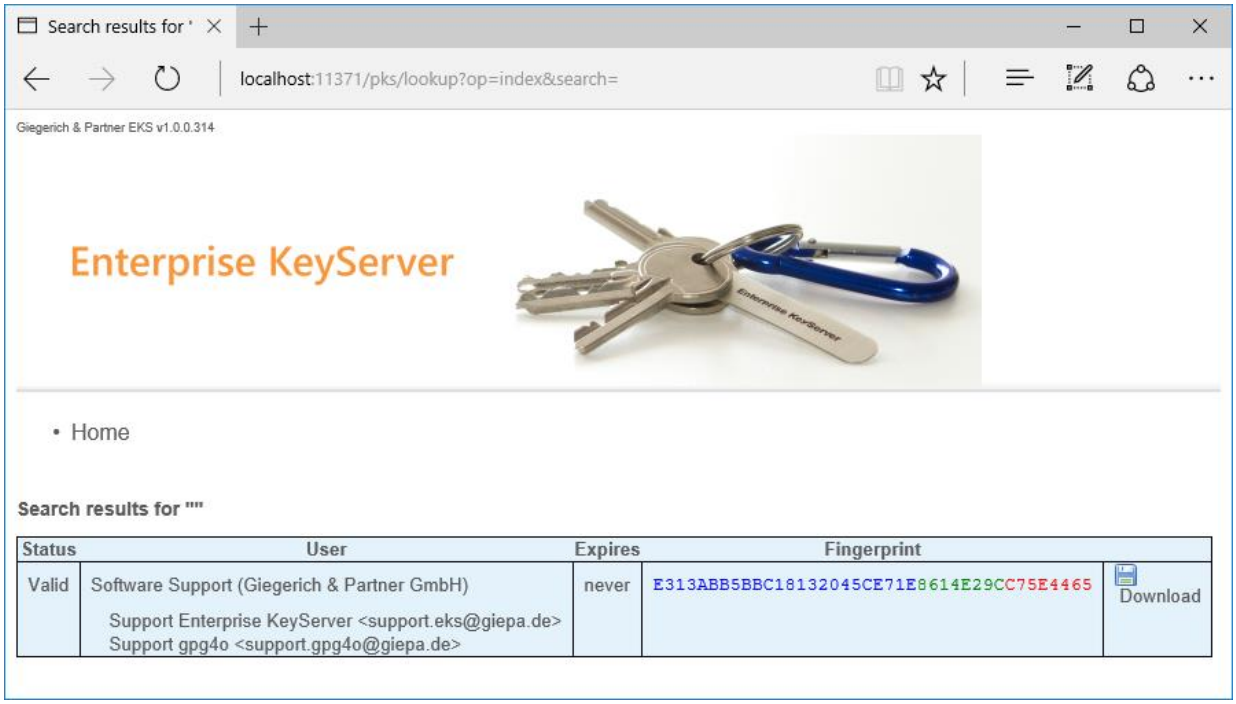

Figure 18: EKS website search result

Clicking on a fingerprint item will display further information about a certain key. To save a ASCII-armored key file (with .asc extension), click on the “Download” link.

5.1.2 Uploading keys

To upload a OpenPGP key click on “Upload” in the navigation panel on the home page.

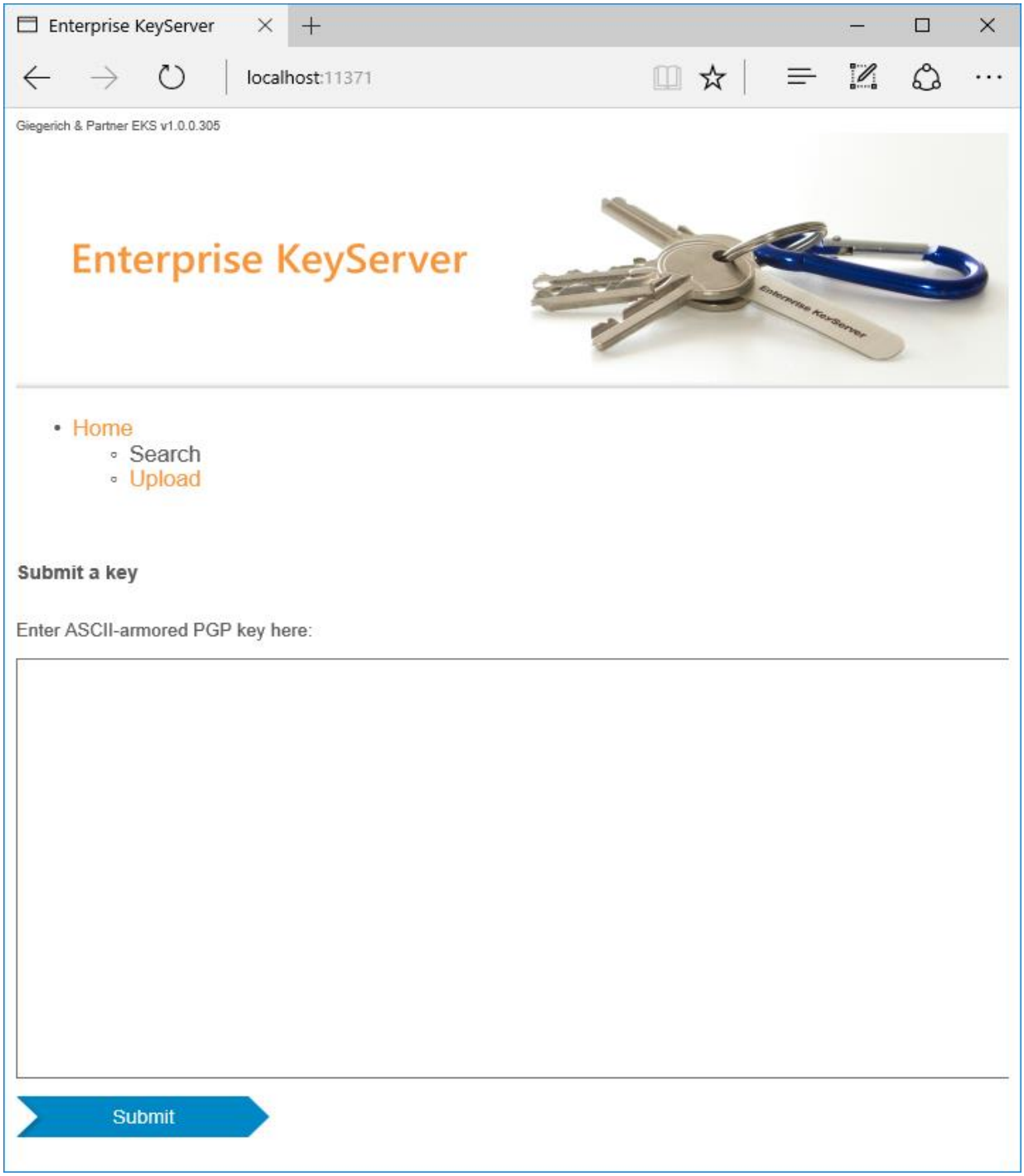

Figure 19: EKS website upload page

You can copy any number of ASCII-armored OpenPGP keys into the form. ASCII-armored keys can be exported from the gpg4o KeyManagement tool, copied from .asc files (e.g. in E-mail attachments) or from other keyservers.

The text of ASCII-armored key(s) always begins with the following line:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

Paste the ASCII-armored OpenPGP key(s) into the submit form, then click on submit to upload the key. If the upload succeeds, a details view will be displayed, similar to this:

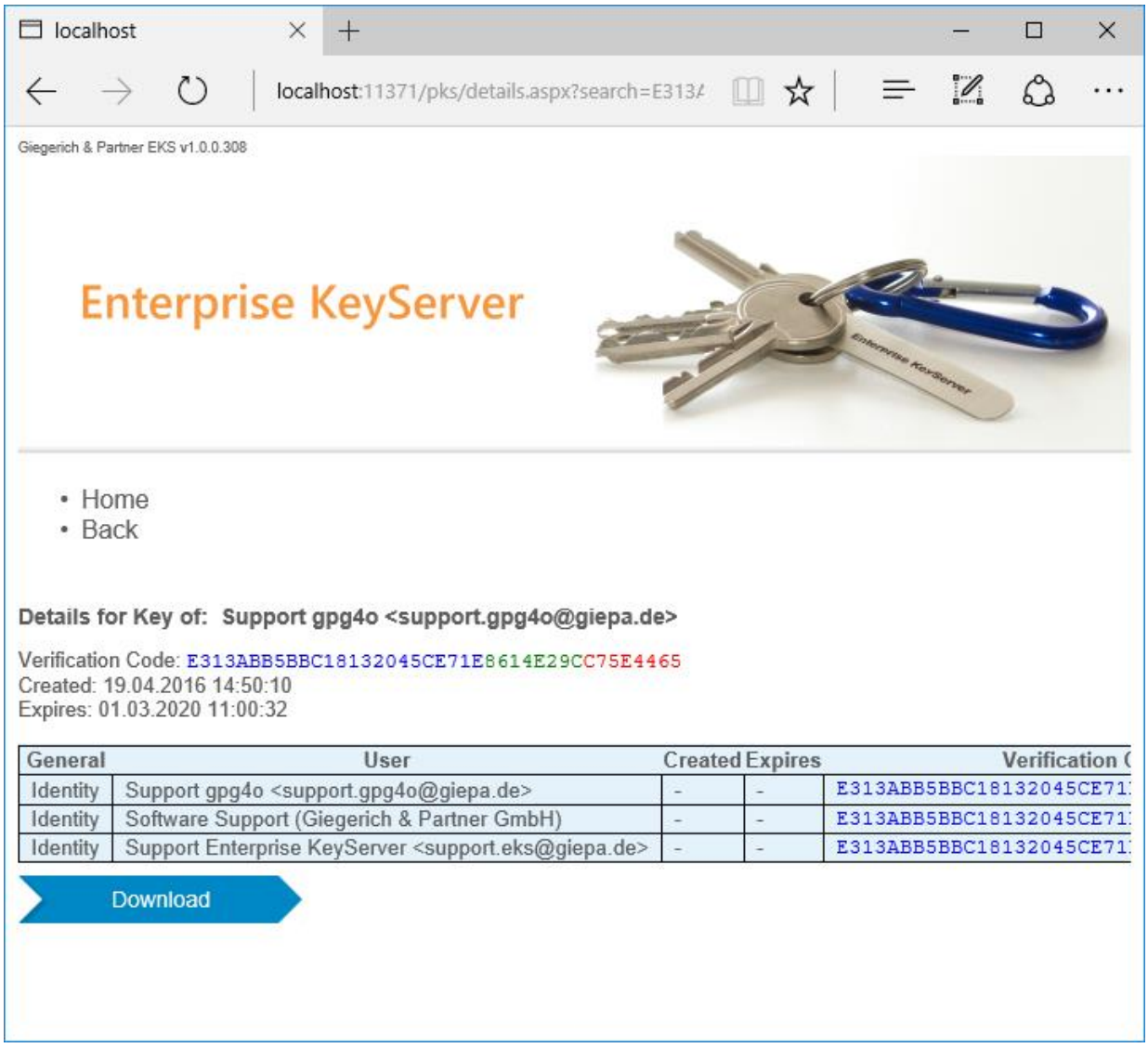

Figure 20: EKS website upload result page

5.1.3 Advanced functions and settings

Advanced keyserver functions (like the ability to delete keys) and settings (control over upload, delete and download & list functions) are available only to authorized logged in users on the website. Clicking on the "Settings" button will display the different "Authorization Settings" that can be modified.

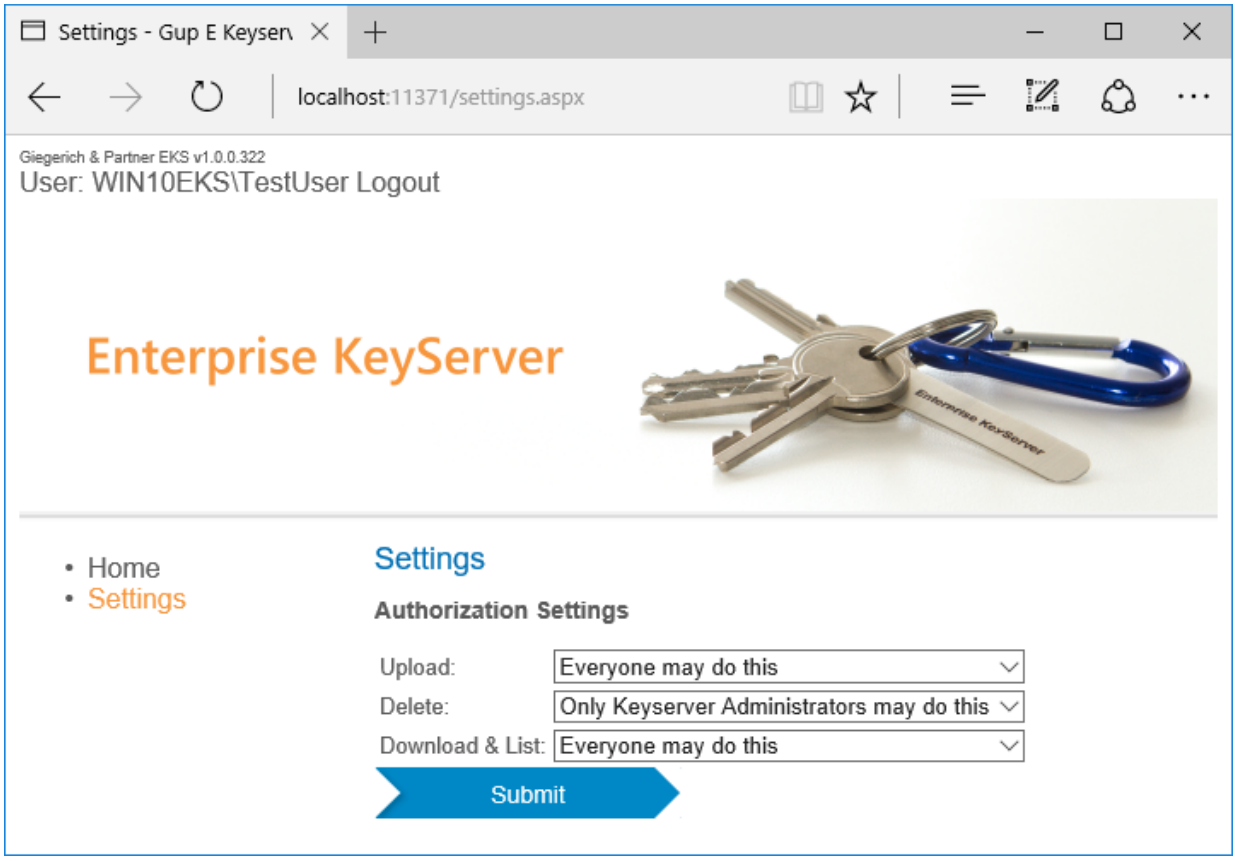

Figure 21: EKS website admin settings page

5.1.4 Deleting keys

In order to be able to remove keys from the keyserver, the EKS website login button needs to be enabled and a member of the KeyServerAdmin local user group needs to be logged in.

To delete a key, search and open the details view of the desired key and click on the delete button.

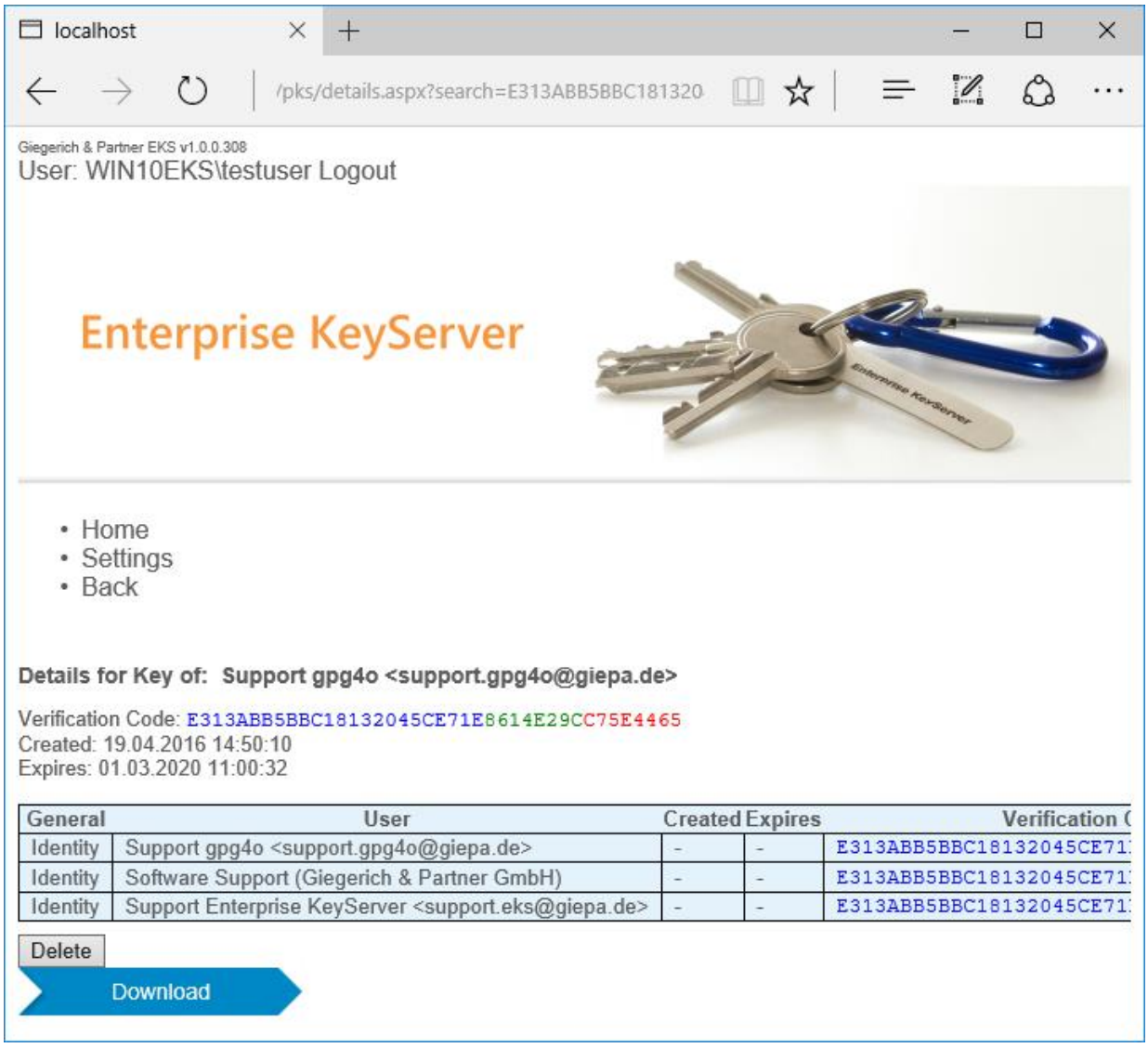

Figure 22: EKS website details with Delete button

5.2 With gpg4o

The EKS host address can be added for usage with gpg4o in the Keyserver settings.

Here as an example the keyserver hkp://localhost:11371 is added (please use a valid host address for your server configuration instead of localhost).

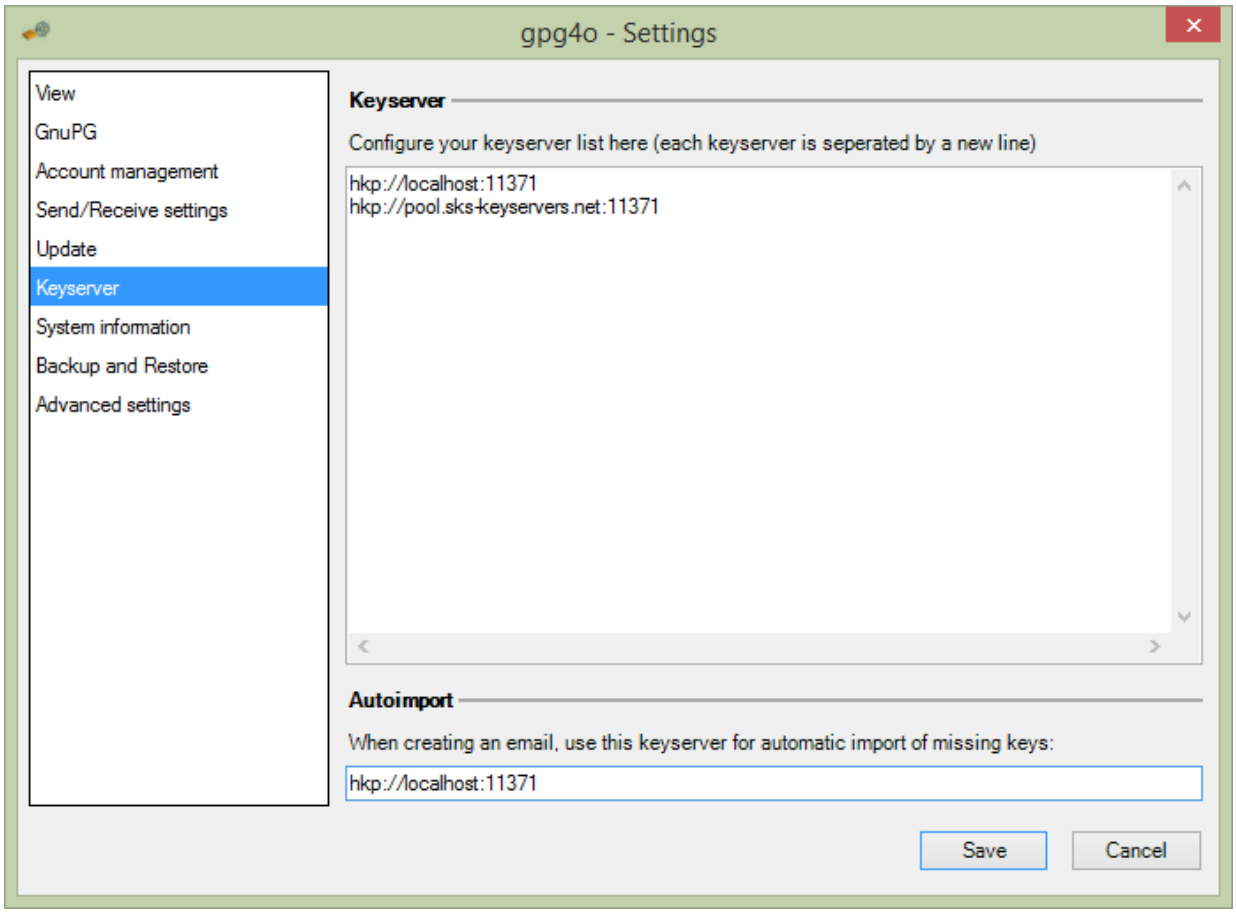

Figure 23: gpg4o Keyserver settings

You can use EKS with the gpg4o KeyManagement tool and as the Autoimport keyserver in gpg4o. Please read the gpg4o manual for details.

5.3 With GnuPG

The Enterprise Keyserver that will be used can be passed with the parameter

--keyserver hkp://localhost:11371

or you can set the default keyserver in gpg.conf in your GnuPG Home directory by adding the following line:

keyserver hkp://localhost:11371

5.4 With Kleopatra

In the Settings go to GnuPG-System, the tab GPG for OpenPGP, there you can enter the keyserver GnuPG should use.

The settings for the Enterprise Keyserver are:

Scheme: HKP; Server Name: localhost; Server Port: 11371

6 Company and support contact information

6.1 About Giegerich & Partner GmbH

Company Profile

Giegerich & Partner is your reliable solution developer. We create efficient IT Infrastructures, care for your IT Security, develop high quality software solutions and refine standard solutions. Your individual needs as a customer set the pace for our work which does not end with the delivery of any solution. We are well known for accompanying the whole solution lifecycle beginning with the very first idea until rollout of the last implementation. And we do that with competent people, not with anonymous call centers.

Who and Where

With over 40 employees near Frankfurt/Main – Germany we support over 1300 customers worldwide in now over 50 countries when it comes to IT Security, software development and email encryption. As a member of the TeleTrust federation in Germany we have obligated ourselves to provide secure IT Security solutions without backdoors. This allows us to be a member of the group "IT Security made in Germany".

Our Mission

We deliver reliable and Tailor-made IT Solutions. Filled with energy, passion and a high skill level, we work for your success with our solution. With us as a partner, you can concentrate on your core business. We care about the (IT) rest. That's what we do: Tailor-made IT.

Values

Highly competent people are important, but not enough. Since we are an owner driven company, we know that reliability, sustainability, personality and partnership are fundamental values for a working relationship with customers, suppliers and employees.

Real people are in the center of our companies universe, not machines. You will experience this by having your personal way of support, long term contact persons and competence. They help you with the technology we provide that helps you run your business as reliable as possible.

Please visit our website at https://www.giepa.de

6.2 Support contact information

Please use the following E-mail address to contact the Giegerich & Partner GmbH support for issues relating to EKS:

support.eks@giepa.de

You can also use the web contact form at:

https://www.giepa.de/contact/?lang=en

General contact information:

Giegerich & Partner GmbH

Robert-Bosch-Str. 18

D-63303 Dreieich

Germany

Phone: +49 (0)6103-5881-0

Web: **https://www.giepa.de/?lang=en**