GuP Enterprise Keyserver Einleitung & Installation

Einleitung

Der Giegerich & Partner Enterprise Keyserver ist ein Schlüsselserver für OpenPGP-Schlüssel, der für den Einsatz in kleineren Unternehmen konzipiert ist. Der Keyserver implementiert das hkp Protokoll und lässt sich dadurch mit GnuPG ansteuern, hat aber auch ein Webinterface, über das sich Schlüssel auflisten, löschen, herunter- und hochladen lassen. Für alle diese Aktionen gibt es auch eine API für Programme, die auf HTTP aufbaut. Der Keyserver kann mithilfe des MS Active Directory Nutzer Authentifizieren und Rechte verwalten.

Systemvoraussetzungen

- IIS 7 oder IIS 8
- IIS URL Rewrite Module (http://www.iis.net/downloads/microsoft/url-rewrite)
- Die Ports 11371 und 44300 sind nicht von anderen Diensten belegt und die Clients können darauf zugreifen (sind in Firewalls nicht blockiert).
- Asp.Net auf dem IIS
  - Installation mit folgendem Befehl:

    ```
    pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-ApplicationDevelopment;IIS-ASPNET;IIS-NetFxExtensibility;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-Security;IIS-RequestFiltering;IIS-HttpCompressionStatic;IIS-WebServerManagementTools;IIS-ManagementConsole;WAS-WindowsActivationService;WAS-ProcessModel;WAS-NetFxEnvironment;WAS-ConfigurationAPI;IIS-ASPNET45;IIS-WindowsAuthentication
    ```

    Eventuell muss der Rechner danach neu gestartet werden.

Webseite

- Kopieren Sie den Ordner „Keyserver“ in ein Verzeichnis, auf das der IIS Zugriff hat. (Normalerweise C:\inetpub\)
- Fügen Sie die Webseite im IIS hinzu.
  - Im IIS Manager über Sites (Rechtsklick) → Webseite hinzufügen → <Pfad zur Webseite>
- Binden Sie Port 11371 an das Protokoll „http“ und Port 44300 an das Protokoll „https“. Bitte beachten Sie, dass Sie für eine https Verbindung ein Zertifikat benötigen.
- Aktivieren Sie die Windows-Authentifizierung für die Webseite, indem Sie auf die hinzugefügte Webseite klicken → im Bereich IIS auf Authentication → Windows-Authentifizierung, und rechts oben enable klicken.

- Des weiteren benötigt die Webseite Schreibrechte auf das Unterverzeichnis „keyring“ des Keyservers.
  Öffnen Sie dazu im Windows Explorer die Eigenschaften des Ordners und wechseln auf die Registerkarte Berechtigungen. Dort fügen sie den lokalen Benutzer „IIS AppPool\DefaultAppPool“ hinzu und geben ihm Schreibrechte. Stellen Sie sicher, dass bei der Benutzerauswahl der lokale Rechner ausgewählt ist.

Update

Für ein Update muss der Prozess „gpg-agent“ manuell beendet werden. Danach kann einfach der Ordner kopiert werden.

Achtung: Bitte achten Sie darauf, dass die GnuPG Schlüssel im Verzeichnis „keyring“ dabei **nicht** überschrieben werden!

Konfiguration

Vorbereitung

Um den Keyserver konfigurieren zu können, müssen sie Gruppe „KeyServerAdmin“ erstellen, damit sich Mitglieder dieser Gruppe als Administratoren am Keyserver anmelden können. Die Gruppe kann wahlweise lokal auf dem Server erstellt werden, oder im Active Directory, wobei bei einer lokalen Gruppe zu beachten ist, dass eine Anmeldung dann nur vom Server aus möglich ist.

- Bei einer Gruppe im Active Directory muss die Group Scope auf Domain Local stehen.

Konfiguration des Keyservers über das Webinterface

Die Einstellmöglichkeit finden Sie links in der Navigationsleiste als „Settings“, nachdem Sie sich mit Ihrem Zugangsdaten für die Domäne angemeldet haben.

Hier haben Sie die Möglichkeit festzulegen welche Funktionen den Anwendern zur Verfügung steht. Dabei können Sie eine Funktion folgendermaßen einschränken:

Einstellung	**Bedeutung**
Everyone may do this	Diese Funktion steht allen Benutzern zur Verfügung. Dies ist unabhängig davon, ob der Benutzer am Keyserver angemeldet ist, oder nicht.
Only Keyserver Administrators may do this	Diese Funktion steht nur den in der Gruppe „KeyServerAdmin“ befindlichen Benutzern zur Verfügung.
This feature is turned off	Diese Funktionalität steht keinem Benutzer zur Verfügung.

- Mit dem Feld Upload lässt sich einstellen, wer Schlüssel hochladen und aktualisieren (erneut hochladen) kann.
- Mit dem Feld Delete lässt sich einstellen, wer Schlüssel löschen darf. Die Schaltfläche wird später auch nur diesen Benutzern im Webinterface angezeigt.
- Mit dem Feld Download & List lässt sich einstellen, wer Schlüssel in der Liste sieht und/oder herunterladen darf.

> Zugriff mit GnuPG ist immer ohne Anmeldung, d.h. auch Administratoren können Schlüssel nur sehen, wenn die Option auf `Everyone may do this` steht.

Empfohlene Einstellungen

Feld	Einstellung

Upload	`Only Keyserver Administrators may do this`
	oder
	`Everyone may do this`

Delete	`Only Keyserver Administrators may do this`
Download & List	`Everyone may do this`

Verwendung mit gpg4o und GnuPG

GnuPG (Kommandozeile)

Der Keyserver kann mit dem Parameter `--keyserver hkp://NAME_OR_IP:11371` oder in der gpg.conf mit dem Eintrag `keyserver hkp://NAME_OR_IP:11371` als zu verwendender Keyserver festgelegt werden.

gpg4o (Windows + Outlook)

Der Keyserver kann in den Einstellungen von gpg4o im Bereich `Schlüsselserver` als `hkp://NAME_OR_IP:11371` eingetragen werden.

Kleopatra (GPG4Win oder Linux)

`Einstellungen` → `GnuPG-System` → `GPG for OpenPGP`

Im Bereich `Konfiguration der Schlüsselserver` den zu verwendenden Schlüsselserver einstellen:

Protokoll:	`hkp`
Servername:	`NAME_OR_IP`
Server-Port:	`11371`

Verwendung über die Weboberfläche

Links befindet sich eine Navigationsleiste, auf der die derzeitige Seite Orange angezeigt ist.

Rechts oben ist ein Button, mit dem man sich am Keyserver anmelden kann. Diese Anmeldung erfolgt über NTLM oder Kerberos, d.h. der Anmeldedialog variiert von Browser zu Browser.

Angemeldete Nutzer sehen rechts oben statt `Login` `Welcome, <USER>` und können auf der Navigationsleiste die Seite `Settings` sehen. Außerdem haben angemeldete Nutzer möglicherweise zusätzliche Funkionen auf einzelnen Seiten.