

# ID-software (based on version 25.10.23.8403)

Administrator view

## ID-SOFTWARE ADMINISTRATOR VIEW

Based on ver. 25.10.23.8403

Document information	
Date of creation	21/01/2019
Receivers	Information System Authority
Author	Urmas Vanem, OctoX
Version	25.10/1

Version information		
Date	Version	Changes/Notices
21/01/2019	19.01/1	Public version, based on the 18.12 software.
24/07/2019	19.7/1	Added the .exe installation key for automatic activation of the Chrome signing support and updated to software version 19.7. Changed by Kristel Merilain
20/11/2019	19.10/1	Changed the default installation of the AWP component OTCertSynchronizer and updated to software version 19.10. Changed by Kristjan Vaikla
31/01/2020	20.01/1	Added the print summary registry location for the default view in DigiDoc4 client and updated to software version 20.01. Changed by Kristjan Vaikla
02/07/2020	20.05/1	Added the AWP 5.3.4 SR1 component parameter for the registration key, which includes translation for Windows servers, and updated to software version 20.05. Changed by Kristjan Vaikla
11/10/2020	20.10/1	Removed the TeRa timestamping application and updated to software version 20.10. Changed by Kristjan Vaikla
28/02/2022	22.02/1	Added the Web eID update, removed outdated information, added information about new installation options, described the central

# ID-software (based on version 25.10.23.8403)



Administrator view

		deployment of browser extensions. Updated to software version 22.02/1. Changed by Urmas Vanem
29/03/2022	22.03/1	Fixed the Chrome Web eID extension value in the chapter on the central deployment of extensions. Changed by Urmas Vanem
13/04/2022	22.04/1	Changed the default location for adding Web eID extensions. Changed by Tarmo Nurmela
21/04/2022	22.04/2	Added the possibility to install the Idemia minidriver automatically with the MSI package (without card/reader, RDP case). Changed by Urmas Vanem
13/06/2022	22.06/1	Added a chapter about the software update logic and a description of Chrome policies 'Configure native messaging blocklist/allowlist'. Changed by Urmas Vanem
29/07/2022	22.07/1	The base version of the software described in the document has now been updated to 22.06.0.1930, changes related to the new version have been described and outdated information has been removed. Added information about the central policies of Firefox. Changed by Kristel Merilain, Urmas Vanem
11/08/2022	22.08/1	Added a description of the ID-software update process. Changed by Urmas Vanem
31/08/2022	22.08/2	Corrected the information in the tables in the chapter 'The behaviour of browser extensions by extension during installation'. Changed by Kristel Merilain
14/12/2022	22.12/1	Changed the description of the behaviour of Edge and Chrome web browsers during installation and updated to software version 22.11. Changed by Kristjan Vaikla
29/12/2022	22.12/1	Updated the information in the transform files of the 'AWP', Digidoc ShellExt, and Web eID chapters. Changed by Märt Hirtentreu
24/10/2024	24.10/1	Removed Gemalto minidriver, updated installation logic, changed how web browsers install extensions, etc. Changed by Urmas Vanem
16/06/2025	25.06/1	Replaced AWP with IDPlug. Changed by Raul Metsma
31/10/2025	25.10/1	Added ClassicClient



		Changed by Raul Kaidro
--	--	------------------------

## Introduction

In the new version of the ID-software, there are some new things from an IT administrator perspective, which this document will focus on. The images in the manual are illustrative and based mostly on version 25.10.23.8403.

The ID-software supports the following operating systems and browsers:

- Operating systems: Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Windows Server 2025.
- Browsers: versions of Mozilla Firefox, Google Chrome and Microsoft Edge Chromium supported by the aforementioned operating systems.

More detailed information about the changes in the latest ID-software version can be found at <https://www.id.ee/en/article/id-software-versions-info-release-notes/>.

## ID-software overview

The new ID-software now consists of only one EXE file, Open-EID-25.10.23.8403.exe, which can no longer be unpacked into MSI components. Everything needed for installation is included in this one EXE file. In advance, however, I note that MSI files can still be downloaded separately from <https://installer.id.ee/media/win/Open-EID.zip>.

An easy way to install ID-software interactively is to run an EXE file that installs the software in a default configuration. If desired, it is possible to install only certain components, for this you have to select Customize from the welcome window that opened at the beginning of the installation:

# ID-software (based on version 25.10.23.8403)

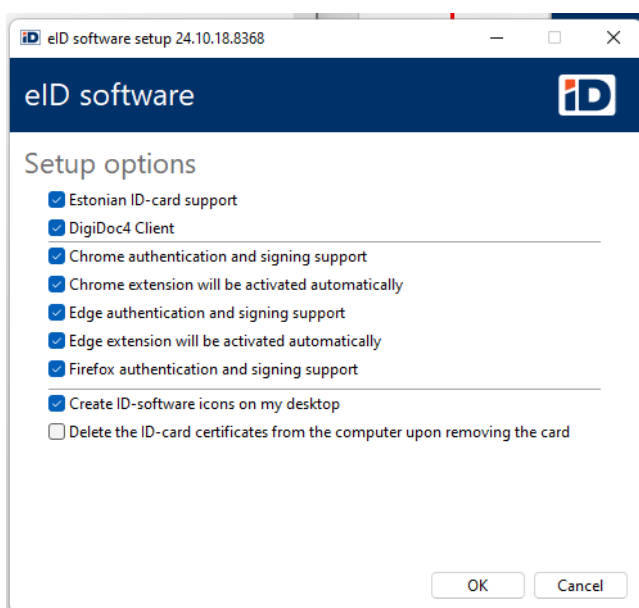


Administrator view



Picture 1 – customize the installation

The customization options are:



Picture 2 – default options

## Brief overview of the components

I note here again that the components are available separately as MSI packages from the address <https://installer.id.ee/media/win/Open-EID.zip>.



## IDPlug

IDPlug is the software for the Idemia card, which also installs the minidriver for Idemia cards.

The component IDPlug Services is also part of the IDPlug. When it is installed and the smart card is removed from the card reader, SK ID-card certificates are deleted from the Windows user certificate store. By default, the exe installation will not install IDPlug Services and ID-card certificates are not removed from the certificate store when removing the card from the reader. To install this component, the exe installation must start with the command line parameter `InstallCertSynchronizer=1`.

## SmartCard Client

SmartCard Client is the software for the Thales card, which also installs the minidriver for Thales cards.

## CertDelApp

When it is installed and the smart card is removed from the card reader, Zetes ID-card certificates are deleted from the Windows user certificate store. By default, the exe installation will not install CertDelApp and ID-card certificates are not removed from the certificate store when removing the card from the reader. To install this component, the exe installation must start with the command line parameter `InstallCertSynchronizer=1`.

## Digidoc\_ShellExt

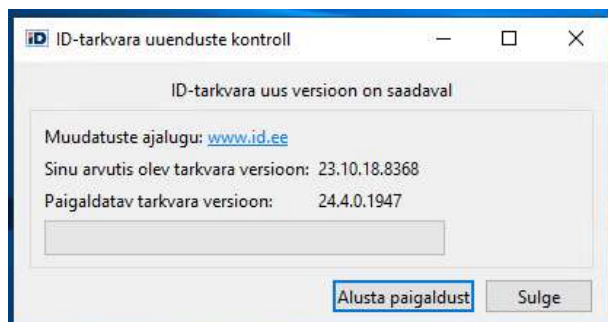
This component allows to start signing and encryption in DigiDoc4 by right-clicking on the file.

## DigiDoc4

DigiDoc4 is a piece of software that enables the signing, validation, encryption, and decryption of documents as well as managing the PINs and PUKs of ID-cards.

## ID-updater

ID-updater is a mandatory component that contains a collection of system files. During installation, the task scheduler task 'id updater task' is created, which checks the availability of new software once per week and suggests any identified updates to the user.



Picture 3 – example: ID-updater found a newer version of the software (EST)

## Web eID

Web eID allows Estonian ID-cards to be used for online authentication and signing. The Web eID component consists of a native app and extensions for the well-known web browsers Google Chrome, Mozilla Firefox and Microsoft Edge.

## In enterprises

In big and medium enterprises, the ID-software is usually installed and controlled centrally by a central management solution. SCCM<sup>1</sup> and AD/GP<sup>2</sup> are most common.

### SCCM

In addition to the configuration options available in GUI, collections of keys for EXE installations can be used for automatic installations:

1. ChromeSupport=0 – the Chrome extension is not added, 1 by default.
2. EdgeSupport=0 – the Edge extension is not added, 1 by default.
3. ForceChromeExtensionActivation2=1 – the Chrome extension is activated automatically, 1 by default.
4. ForceEdgeExtensionActivation2=1 – the Edge extension is activated automatically, 1 by default.
5. FirefoxSupport=0 – the Firefox extension is not added, 1 by default.
6. InstallCertSynchronizer=1 – installs the component OTCertSynchronizer, 0 by default<sup>3</sup>.
7. MinidriverInstall=0 – the minidriver is not installed, 1 by default.
8. Qdigidoc4Install=0 – the DigiDoc software is not installed, 1 by default.

<sup>1</sup> System Center Configuration Manager

<sup>2</sup> Active Directory / Group Policy

<sup>3</sup> If this setting is enabled, the user's certificates are removed from the Windows certificate store when the EID card is removed.

# ID-software (based on version 25.10.23.8403)



Administrator view

9. IconsDesktop=0 – the DigiDoc icon is not put on the desktop, 1 by default.
10. AutoUpdate=0 – 'id updater task' is not added to the task scheduler, 1 by default.

**Please note! The installation keys shown above are case sensitive!**

For example, the command line 'OpenEID.\_???.exe /quiet AutoUpdate=0 IconsDesktop=0' installs the ID-software in unattended mode, does not activate automatic updates, and does not add the ID-software icons to the desktop.

By default, it is enough to run the EXE for the software installation – the correct language version is downloaded according to the computer's configuration.

When using SCCM for ID-software installation, the simplest way is to create an installation package and install it into the computer with the default command line 'OpenEID....exe /quiet AutoUpdate=0'.

As a result of this normal installation, we see the ID-software as usual in the software list:



Picture 4 – ID-software in list

## AD/GPO

If you do not have a central software management system in the enterprise, but you can use the *Group Policy* functionality, you can also use MSI-based installations. We recommend making GPO installations computer-based!

**Please note! By default, MSI installations are intended only for new installations. MSI components do not remove any previous (or current) versions of EXE installations.**

You can find the overview of different MSI components used from the chapter above 'Brief overview of the components'.










As mentioned before, MSI packages are not automatically included with the new ID-software version and cannot be unpacked from EXE. However, they can be downloaded separately from <https://installer.id.ee/media/win/Open-EID.zip>.

# ID-software (based on version 25.10.23.8403)



Administrator view

The following files are available as MSI packages:

Name	Date modified	Type	Size
 CertDelApp_64_Setup.msi	10/30/2025 9:57 AM	Windows Installer Pa...	1,096 KB
 CertDelApp_arm64_Setup.msi	10/30/2025 9:57 AM	Windows Installer Pa...	1,084 KB
 Digidoc_ShellExt-3.13.9.16.x64.msi	10/30/2025 9:57 AM	Windows Installer Pa...	720 KB
 Digidoc4-4.9.0.5378.x64.msi	10/30/2025 9:59 AM	Windows Installer Pa...	4,616 KB
 idplug-classic-4.4.0-Estonia_64bit.msi	10/30/2025 9:58 AM	Windows Installer Pa...	44,024 KB
 ID-Updater-3.18.0.5475.x64.msi	10/30/2025 9:59 AM	Windows Installer Pa...	20,248 KB
 SmartCard_Client_64_User_setup.msi	10/30/2025 9:58 AM	Windows Installer Pa...	8,167 KB
 SmartCard_Client_arm64_User_setup.msi	10/30/2025 9:58 AM	Windows Installer Pa...	13,477 KB
 web-eid_2.8.0.913.x64.msi	10/30/2025 9:59 AM	Windows Installer Pa...	6,432 KB

*Picture 5 – zipped MSI file*

The MST files described below in the manual can be downloaded from the location <https://www.id.ee/en/article/administrators-guide-for-administration-and-installation-of-open-eid/>.

Please also note that a number of MST files have also been updated with the new MSI versions and be sure to use the new ones as the old ones won't work!

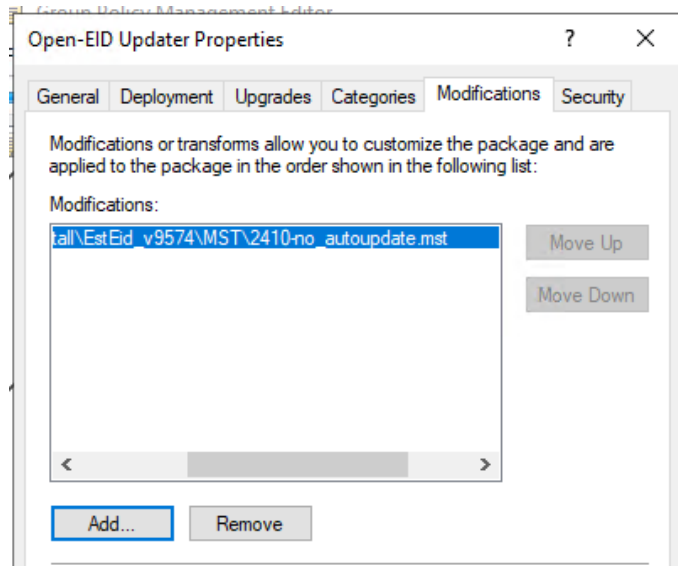
Below is a brief overview about how to configure GPO-MSI installations.

## *ID-Updater*

ID-Updater is a mandatory component. We recommend installing it first!

Options:

- If you do not want to activate the automatic software update functionality (deferred 'id updater task'), we must use transform file No\_AutoUpdate.mst with this MSI installation. And it probably makes sense to disable it, since MSI installations today don't support software update checking in this way.



Picture 6 – sample about adding a transform file to the MSI installation

## IDPlug

IDPlug is the minidriver and basic software for Idemia cards.

Differently from EXE installation (check the IDPlug component description), MSI install adds the component IDPlug Services by default. If you do not want to enable this component, you must use a transform file.

Options:

- To disable the component IDPlug Services:
  - Add the transform file DisableIDPlugServices.mst.

## SmartCard Client

SmartCard Client is the minidriver and basic software for Thales cards.

## CertDelApp

CertDelApp is the tool for cleaning old certificates for Thales cards.

## DigiDoc4

The DigiDoc4 is a necessary component if you want to sign and encrypt documents as well as manage the PINs and PUKs of ID-cards.

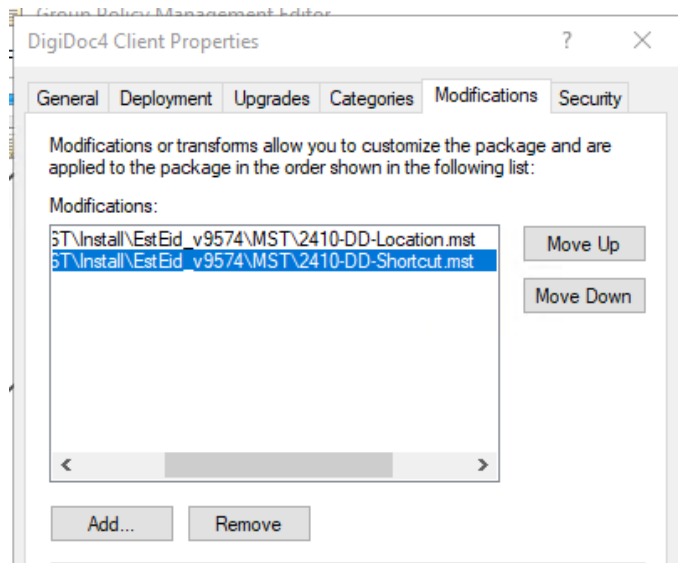
Options:

# ID-software (based on version 25.10.23.8403)



Administrator view

- For GPO-MSI installations, it is necessary to use the transform file 2410-DD-Location.mst. In this case, the software is installed in the same folder "PROGRAM FILES\Open-EID" as the necessary drivers!
- The default MSI installation does not install the necessary icons on the desktop. However, if we want to do this, the transform file 2410-DD-Shortcut must also be added to the installation!



Picture 7 – adding transform files for MSI installation

## Adding right-click signing and encryption to Windows

Enables signing and encrypting files with the right click on Windows.

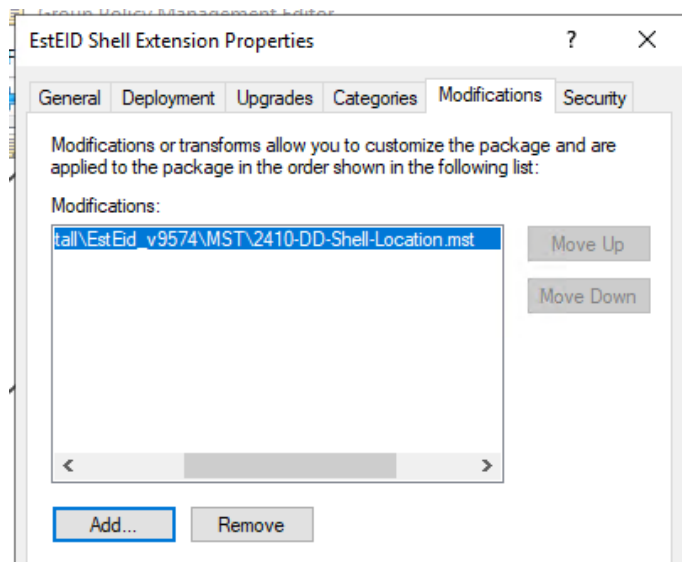
Options:

- For GPO-MSI installations, it is necessary to use the transform file 2410-DD-Shell-Location.mst. In this case, the software is installed in the same folder "PROGRAM FILES\Open-EID" as the necessary drivers!

# ID-software (based on version 25.10.23.8403)



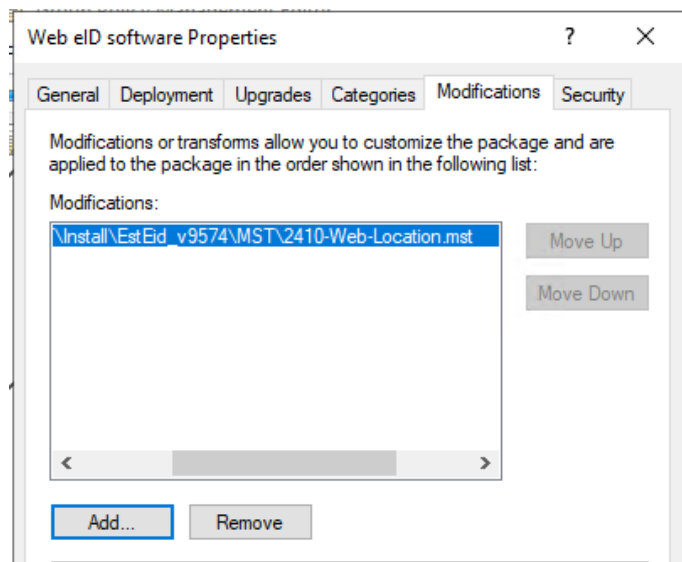
Administrator view



Picture 8 – sample of adding a transform file to a GPO-MSI installation

## Web eID

Browser extensions and native app. For GPO-MSI installations, it is necessary to use the transform file 2410-Web-Location.mst. In this case, the software is installed in the same folder "PROGRAM FILES\Open-EID" as the necessary drivers!



Picture 9 – sample of adding a transform file to a GPO-MSI installation.

# ID-software (based on version 25.10.23.8403)



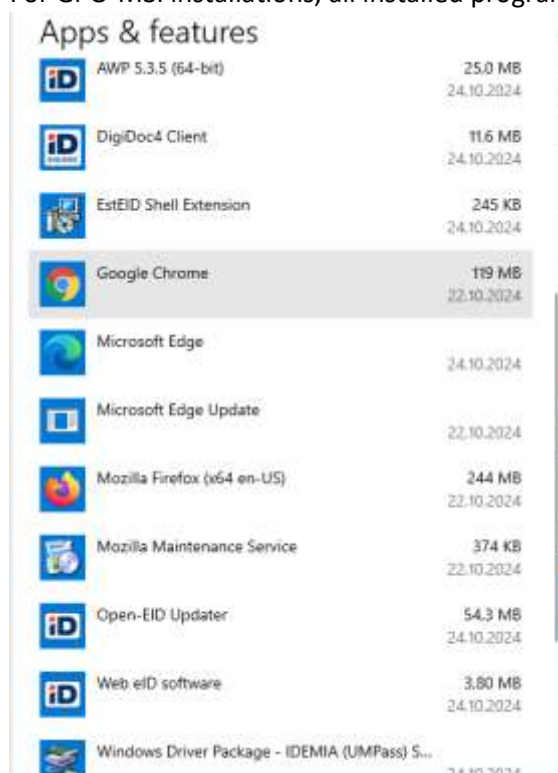
Administrator view

The list of MSI custom packages in the GPMC management console looks like this:

Name	Version	Deployment state	Source
DigiDoc4 Client	4.9	Assigned	\\novaator2\pub\INSTALL\Digidoc4-4.9.0.5378.x64.msi
EstEID Shell Extension	3.13	Assigned	\\novaator2\pub\INSTALL\Digidoc_ShellExt-3.13.9.16.x64...
IDEMIA IDplug Classic 4...	4.4	Assigned	\\novaator2\pub\INSTALL\idplug-classic-4.4.0-Estonia_64bi...
Open-EID Updater	3.18	Assigned	\\novaator2\pub\INSTALL\ID-Updater-3.18.0.5475.x64.msi
SmartCard Client 64 bit...	8.0	Assigned	\\novaator2\pub\INSTALL\SmartCard_Client_64_User_setu...
Web eID software	2.8	Assigned	\\novaator2\pub\INSTALL\web-eid_2.8.0.913.x64.msi

Picture 10 – sample of en-US MSI GPO installation

For GPO-MSI installations, all installed programs also appear in the software list:



Picture 11 – MSI installations in the program list of the Control Panel

Notes:

- Use the correct language for the MSI package if available!
- The order of MSI installation components is not important, but all components depend on the MSI 'Open-EID updater'. The minidriver is also important, as other components depend on it.
- MST files can be downloaded from <https://www.id.ee/en/article/administrators-guide-for-administration-and-installation-of-open-eid/>.
- It is also recommended to publish the related root and intermediate certificates in the domain to all servers and workstations automatically through the group policies.



## Deploying extensions centrally

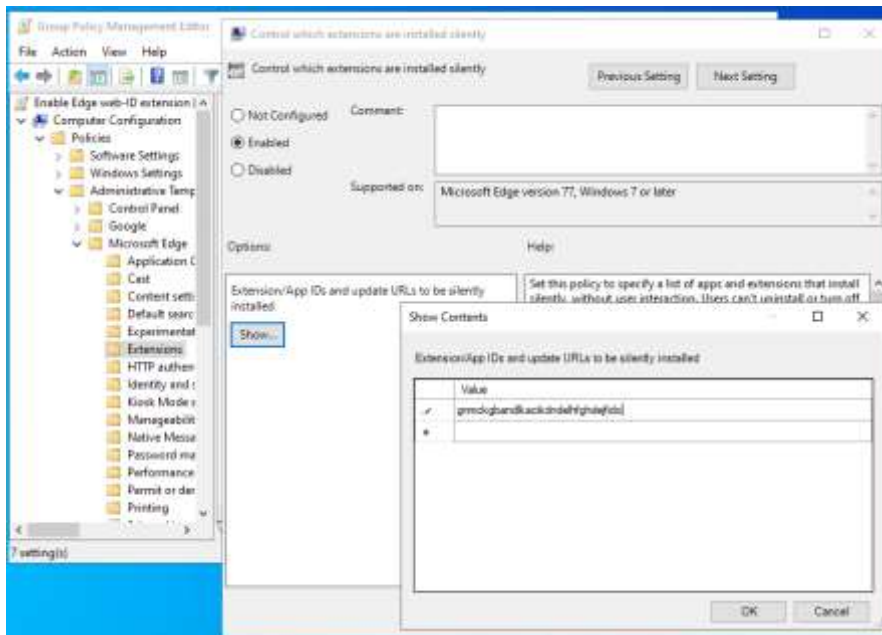
Browser extensions can also be deployed centrally via Group Policy.

Please test configurations described below in your specific environment(s) before deployment!

### Chromium Edge

For Edge, you need to download the newest Edge policy framework from <https://www.microsoft.com/en-us/edge/business/download> and integrate it into your environment.

After enabling policies, you can create a new policy that makes the use of the Web eID extension automatic in the domain. For that, set the value of the field 'CC/Administrative Templates/Microsoft Edge/Extensions - 'Control which extensions are installed silently'' to 'gnmckgbandlkacikndelhfghdejfido'.



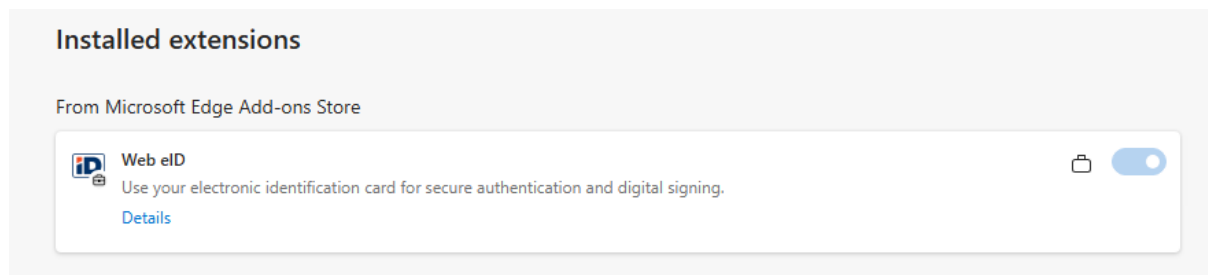
Picture 12 – the Edge extension ID is gnmckgbandlkacikndelhfghdejfido

When opening the Edge extensions window after applying this policy, we will see the following picture:

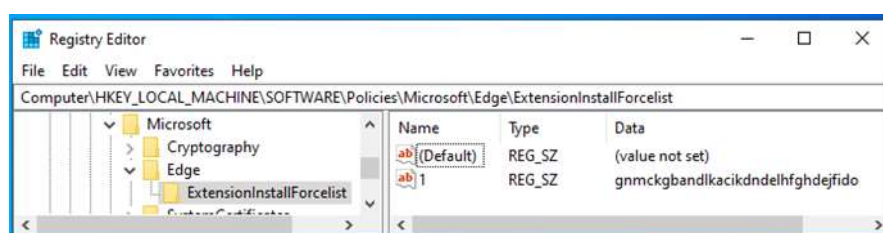
# ID-software (based on version 25.10.23.8403)



Administrator view



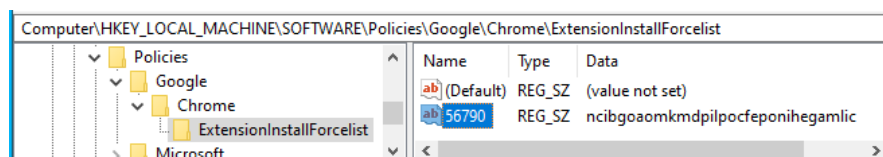
Picture 13 – the Edge Web eID extension is enabled centrally



Picture 14 – policy information in the registry

## Google Chrome

The Chrome policy is set during the installation of the ID-software. The following information written to the registry enables the Web eID extension in Chrome automatically:



Picture 15 – Chrome policy in the registry after installation

However, if you want to centrally manage policies in Chrome, the following instructions may help.

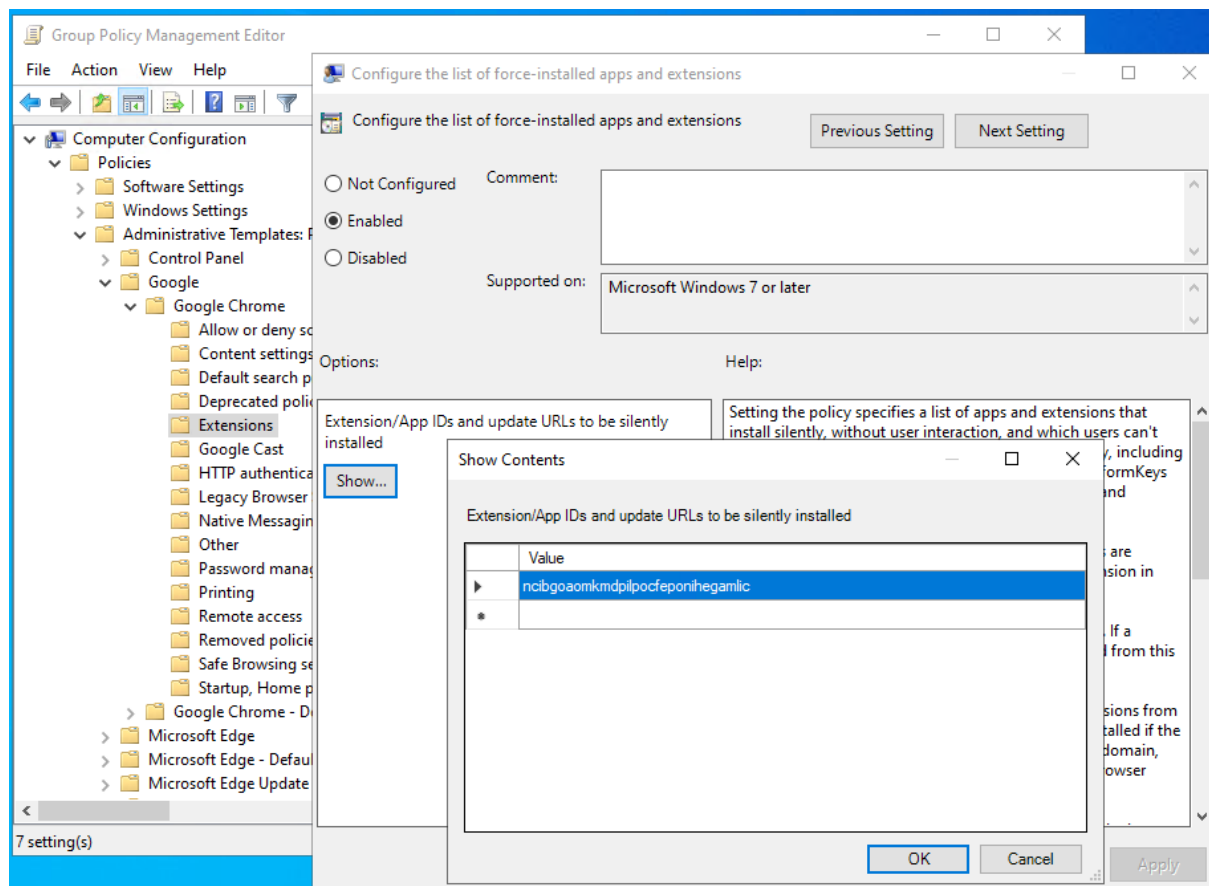
To enable the Chrome extensions policies centrally, you need to download the newest template files from <https://chromeenterprise.google/browser/download/#windows-tab> and integrate those into the domain solution.

After enabling policies, you can create a new policy that makes the use of the Web eID extension automatic in the domain. or that, set the value of the field 'CC/Administrative Templates/Google/Google Chrome/Extensions – 'Configure the list of force-installed apps and extensions'' to 'ncibgoaomkmdpilpocfeponihagamlic'.

# ID-software (based on version 25.10.23.8403)

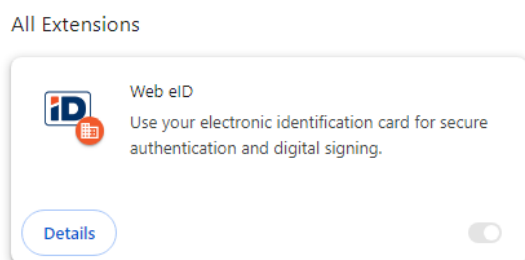


Administrator view



Picture 16 – Chrome Web eID extension ID is *ncibgoaomkmdpilpocfeponihgamlc*

When opening Chrome extensions window after applying this policy, we will see the following picture:

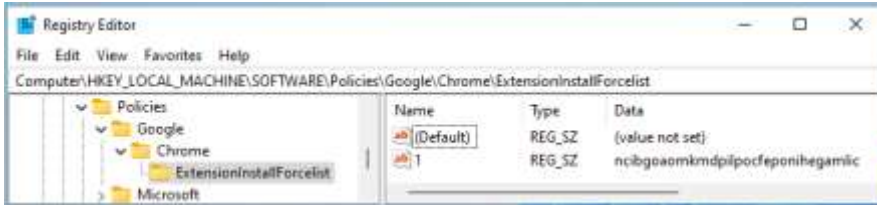


Picture 17 – the Chrome Web eID extension is enabled centrally

# ID-software (based on version 25.10.23.8403)



Administrator view



Picture 18 – policy information in the registry

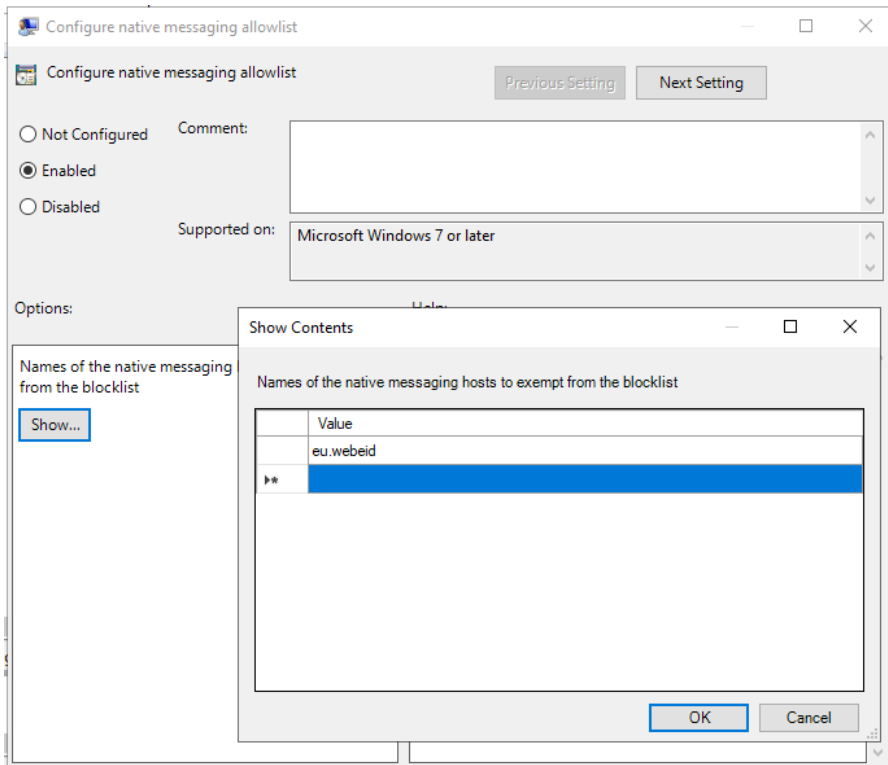
## Additional possible configuration in the ‘native messaging’ view

If the ‘Configure native messaging blacklist’ property is set to ‘\*’ with Chrome policies, signing using the Chrome extension described above will not work. For example, on the test page <https://hwcrypto.github.io/hwcrypto.js/sign.html>, we will get the error ‘getCertificate () failed: Error: technical\_error’ when attempting to sign.

```
Debug: hwcrypto.js 0.0.13 with failing backend Chrome native messaging extension  
getCertificate() failed: Error: technical_error
```

Picture 19 – error while attempting to sign

To overcome this problem, we need to allow the host eu.webeid in the Chrome policy ‘Configure native messaging allowlist’:



Picture 20 – enabling eu.webeid in the Chrome policy

# ID-software (based on version 25.10.23.8403)



Administrator view

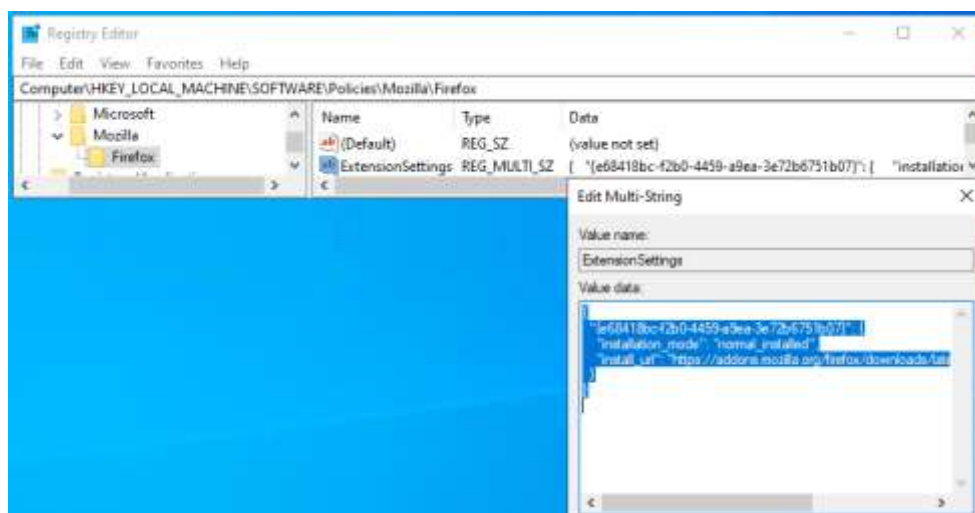
After applying the policy, signing on the webpage succeeds.

```
Debug: hwcrypto.js 0.0.13 with Chrome native messaging extension 2.0.1/2.0.0.552
Using certificate:
-----BEGIN CERTIFICATE-----
MIIFwDCCA6igAwIBAgIQAeWx9HwMfgtaOMgg00+EnjANBgkqhkiG9w0BAQsFADBi
MQswGQYJKoZIhvcNAQkEQAQwDQYJKoZIhvcNAQkEQAQwDQYJKoZIhvcNAQkEQAQw
-----END CERTIFICATE-----
```

Picture 21 – signing on the page <https://hwcrypto.github.io/hwcrypto.js/sign.html> succeeds

## Mozilla Firefox

The Firefox policy is already set during the installation of the ID-software; the information reflected in the following image is written into the Windows registry. Using the aforementioned policy, the Web eID extension is automatically installed on Firefox:



Picture 22 – Firefox policy in the registry after ID-software installation

However, if you want to centrally manage policies for Firefox, the information below can be helpful.

To use central policies for Firefox, you need to download the newest Firefox administrative templates from <https://github.com/mozilla/policy-templates/releases> and integrate them to the domain solution.

After introducing the policies to the domain environment, you can create a new policy that makes the use of the Web eID extension for Firefox automatic in the domain. There are several options for this, but it is perhaps advisable to overwrite the policy already described during the installation. To do this, set the value of the field 'CC/Administrative Templates/Mozilla/Firefox/Extensions:Extension Management' to the following text:

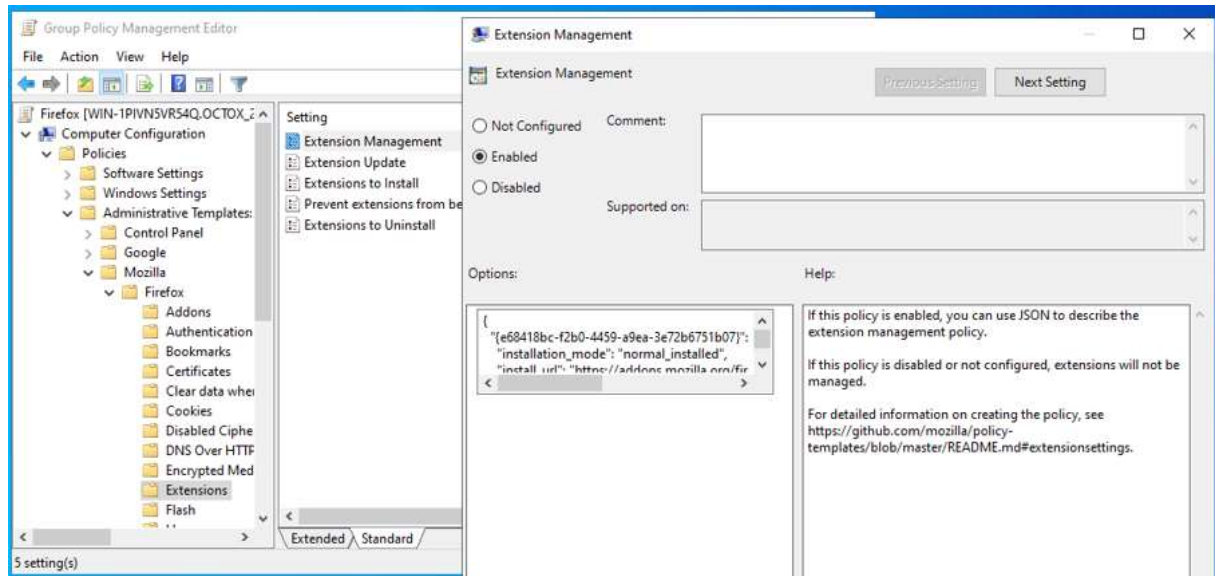
```
{
  "{e68418bc-f2b0-4459-a9ea-3e72b6751b07}": {
    "installation_mode": "normal_installed",
```

# ID-software (based on version 25.10.23.8403)



Administrator view

```
"install_url": "https://addons.mozilla.org/firefox/downloads/latest/web-eid-  
webextension/latest.xpi"  
}  
}
```



Picture 23 – central Firefox policy to enable Web eID functionality

When opening the Firefox extensions management window after applying the policy described above (or also after installing the ID-software), we see the following image:



Picture 24 – the Firefox Web eID extension is installed and enabled

The corresponding information is written into registry into the same place as during the installation of ID-software, see 'Picture 22 – Firefox policy in the registry after ID-software installation'.

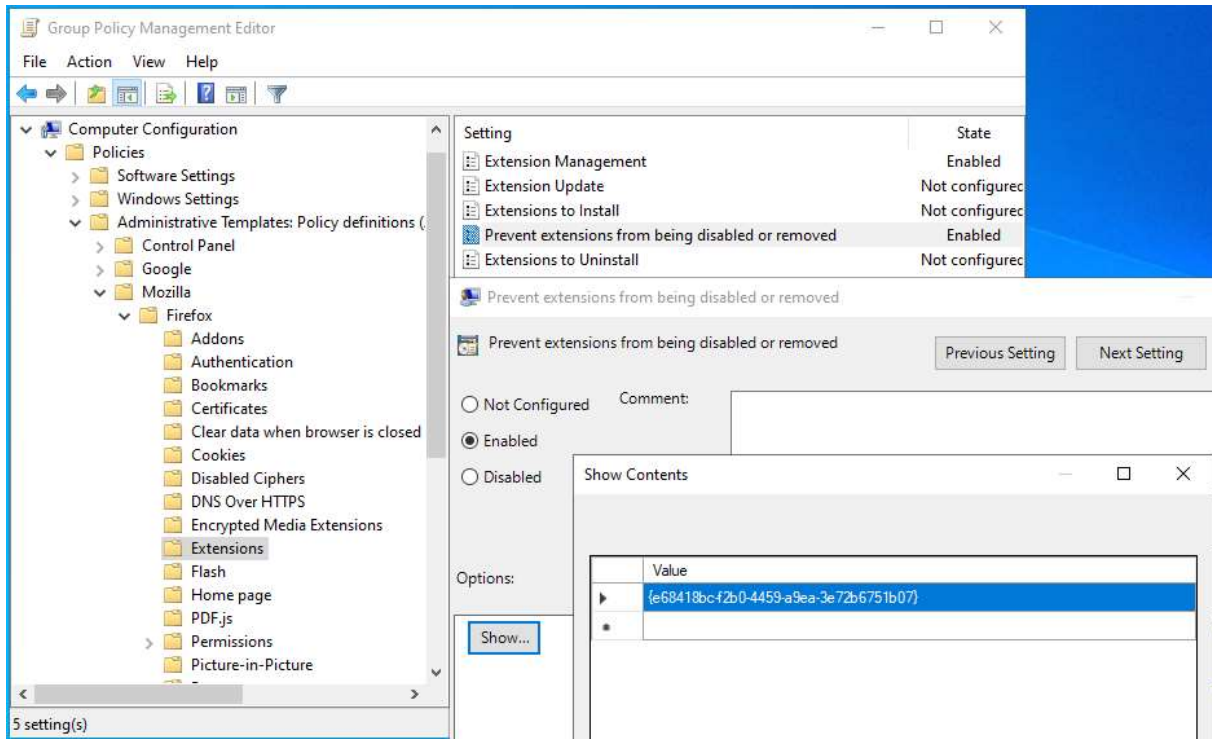
If you want the user to not be able to turn off the Web eID extension independently, one of the actions from the following list must be performed:

# ID-software (based on version 25.10.23.8403)



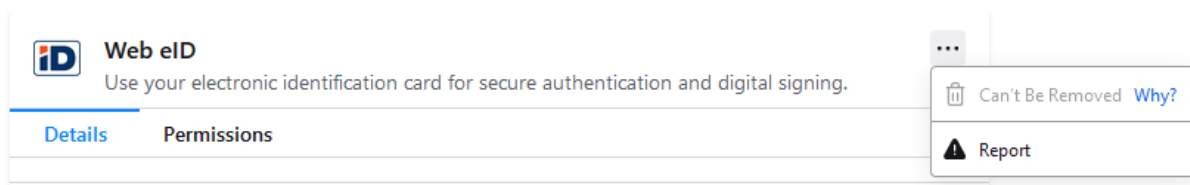
## Administrator view

- 1) Replace the text 'normal\_installed' with the text 'force\_installed' in the value of the field described above;
- 2) Add the line {e68418bc-f2b0-4459-a9ea-3e72b6751b07} to the list 'CC/Administrative Templates/Mozilla/Firefox/Extensions:Prevent extensions from being disabled or removed'.



Picture 25 – disable disabling the Firefox Web eID policy

After applying one or another policy, the user can no longer disable Firefox Web eID extension:



Picture 26 – the Web eID extension is always on

In addition, you can install the extension using the list 'CC/Administrative Templates/Mozilla/Firefox/Extensions:Extensions to install', but for the current configuration, it is preferred to overwrite the existing value.



## Updating the software

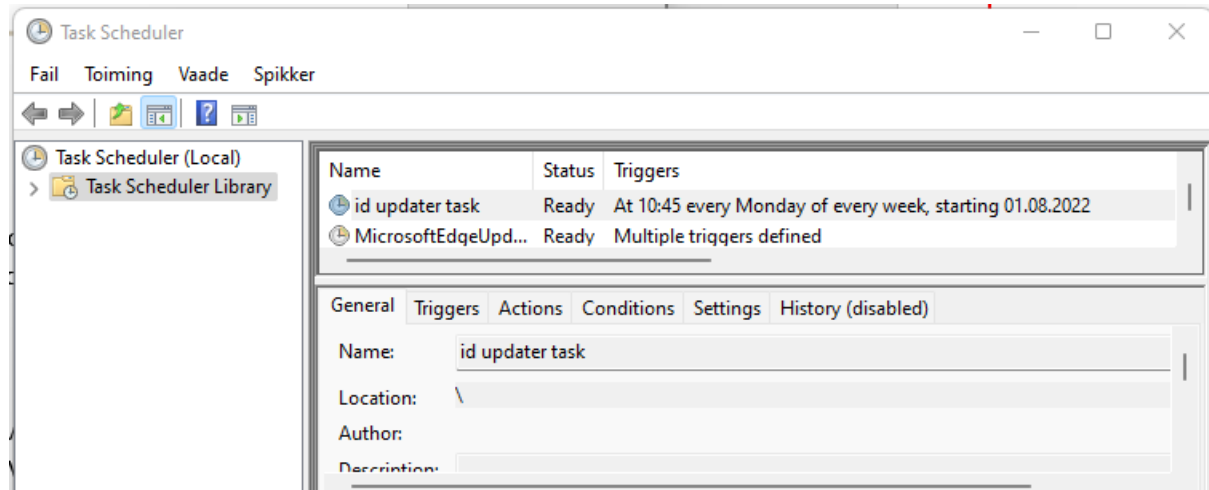
Central configuration is used for checking ID-software updates. The process compares the software version in use with the latest version available and, in the case of DigiDoc4, also with the latest supported software version. The central configuration can be found at <https://id.eesti.ee/config.json>. There are three different ways to start checking for software updates:

1. Using the scheduled task 'id updater task';
2. Starting the DigiDoc4 program;
3. Running a manual search for software updates when launching the DigiDoc4 application.

### Scheduled task 'id updater task'

I note at the very beginning that this method of updating only works with EXE installations, since the registry values described below are not created with an MSI installation.

As written above, by default, during the installations, the scheduled task 'id updater task' is created, which checks the availability of a newer software version. If a newer version of the software is available, it will be offered to the user.



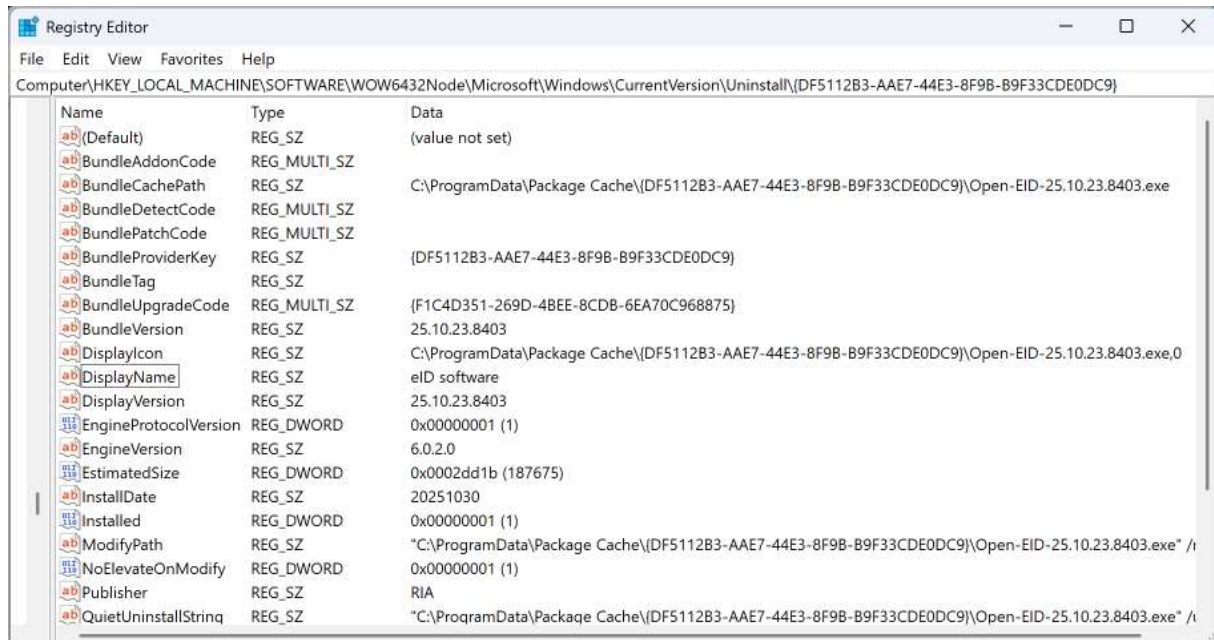
Picture 27 – 'id updater task'

For ID-software version 25.10.23.8403, the version on the software can be found in the registry in the DisplayVersion field under the key  
HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{5FBF3885-332F-4E02-B7C8-589775D00818}

# ID-software (based on version 25.10.23.8403)



Administrator view



Picture 28 – ID-software version 25.10.23.8403 in the registry

The generated unique key (here: {DF5112B3-AAE7-44E3-8F9B-B9F33CDE0DC9}) is different for each ID-software version. When the scheduled task 'id updater task' is started, the central configuration is loaded into the computer's memory, the WIN-LATEST parameter is read from there and compared with the DisplayVersion parameter in the registry. If the WIN-LATEST is greater than the value of the DisplayVersion field in the registry, the user is offered a software update.

See also '

Picture 3 – example: ID-updater found a newer version of the software'.

## Starting DigiDoc4

Also when starting the DigiDoc4 program, the software version is checked and compared with the version in the central configuration. The first time the DigiDoc4 program is started, the central configuration file config.json is downloaded to the folder %APPDATA%\RIA\qdigidoc4. At the first start, the LastCheck field is also written to the user's registry, which, as expected, describes the time when the last request for a new version of the central configuration file was successful.

# ID-software (based on version 25.10.23.8403)



Administrator view



Picture 29 – user-based information on DigiDoc4

At each subsequent start of the DigiDoc4 application, the current date is compared with the *LastCheck* value mentioned above, and if this difference is greater than 4 days, the availability of new software is automatically checked. In the case of a successful check, the *LastCheck* field is also updated.

## Outdated software

If the DigiDoc4 version in the *LastVersion* field in the user's registry section is smaller than the one described in the QDIGIDOC4-SUPPORTED line in the central configuration file, the user will be informed of this every time the DigiDoc4 program is started: 'Your ID-software has expired. To download the latest software version, go to ...'.

## Newer version of software

If the DigiDoc4 version in the *LastVersion* field of the user's registry section is smaller than the one described in the QDIGIDOC4-LATEST line of the central configuration file, the user will be informed of this after starting the DigiDoc4 program: 'An ID-software update has been found. To download the update, go to ...'. The user is notified of the update the first time a version difference is found, and subsequent notifications are only sent when changes have been made to the central configuration file.<sup>4</sup>

## Manual update search

To manually search for ID-software updates, open the settings in the DigiDoc4 program and then click the 'Refresh configuration' text at the bottom. As a result, the process always checks for a new configuration file, downloads it if necessary, and then compares the version there with the software version on the computer. The computer version is read analogously to the scheduled task 'id updater task', from the DisplayVersion registry field under the key

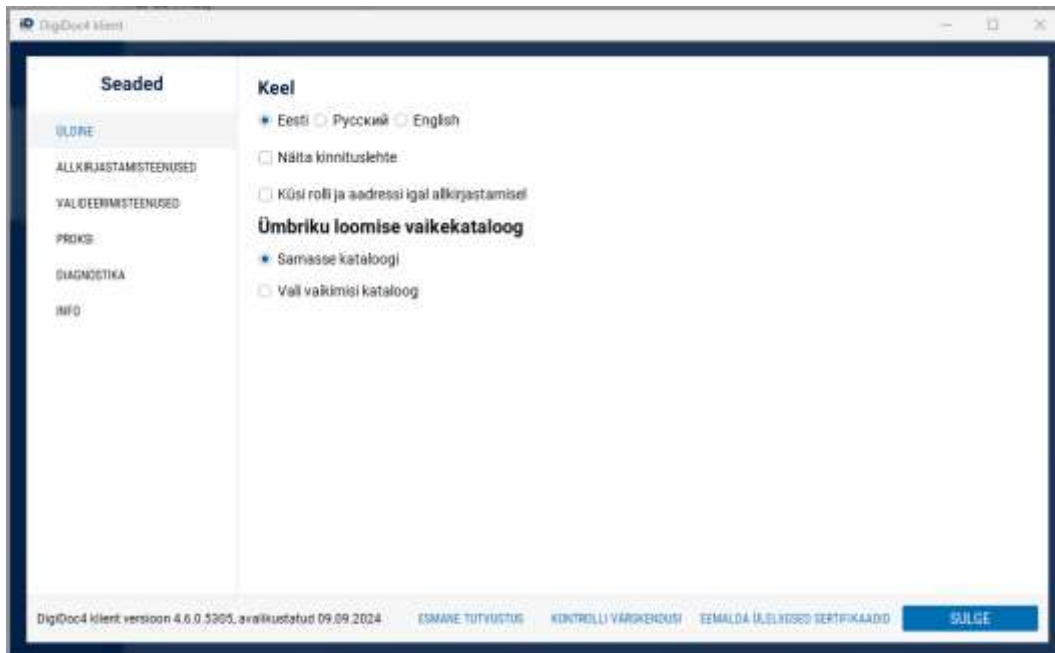
<sup>4</sup> Usually, changes are made to the central configuration file once a month.

# ID-software (based on version 25.10.23.8403)



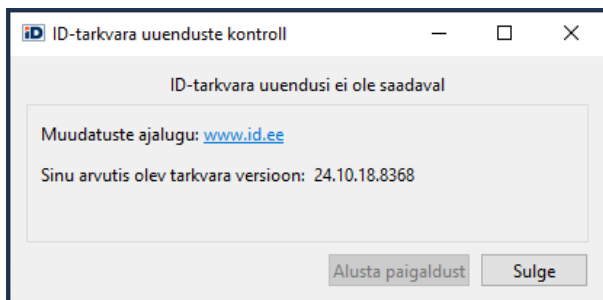
Administrator view

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{5FBF3885-332F-4E02-B7C8-589775D00818}.



Picture 30 – refresh configuration under DigiDoc4 settings (EST)

If a software update is available, it will be offered to the user. User will also be notified if no ID-software updates are available:



Picture 31 – the latest version is already installed

I note here that this method also works correctly only for EXE installations.