Автоматическое подписание SignTool в Windows 10

Для работы SignTool необходимо установить пакет разработчика Windows SDK: https://developer.microsoft.com/ru-ru/windows/downloads/sdk-archive/

Данная инструкция описывает сценарий автоматического подписания файлов с помощью SignTool и Рутокен ЭЦП. При настройке кэширования PIN кода, можно настроить автоматическое подписания без входа в сеанс пользователя Windows 10.

Проверка данного сценария проводилась на виртуальной машине Windows 10 с использованием Рутокен ЭЦП 3.0 3220. Проброс Рутокена на виртуальную машину не привёл к каким-либо ошибкам и трудностям.

- Импорт сертификата на Рутокен
- Изменение Криптопровайдера
- Регистрация сертификатов
- Настройка кеширования PIN кода
- Создание скрипта для подписания документов
- Добавление Скрипта в Службы Windows
- Настройка службы
- Подключение по SSH
- Итог

Импорт сертификата на Рутокен

Для импорта сертификата на Рутокен необходимо выполнить следующие действия

1. Нажмите кнопку Пуск и введите Командная строка и выберите пункт Запуск от имени администратора.



- 2. Если необходимо введите имя и пароль администратора компьютера.
- 3. Подключите Рутокен к компьютеру.
- В командной строке наберите следующую команду: certutil -csp "Microsoft Base Smart Card Crypto Provider" -importpfx C:\sign_code.pfx и нажмите Enter.

5. Введите пароль PFX и нажмите Enter.



6. Введите PIN-код от Рутокена и нажмите OK.

Безопасн	Безопасность Windows						
Смарт	Смарт-карта						
Введите	Введите ПИН-код.						
	•••••	୕					
	Щелкните здесь для п дополнительных свед	олучения ений					
	ОК	Отмена					

7. Дождитесь сообщения что команда успешно выполнена.



Изменение Криптопровайдера

Для корректной работы SignTool при закешированном PIN коде от Рутокена, необходимо изменить параметры криптопровайдера.

1. Зайти в Панель Управления Рутокен и перейти в раздел Настройки.

- В разделе Настройки криптопровайдера необходимо нажать на "Настроить криптопровайдер".
 В пункте "Семейство Рутокен ЭЦП", необходимо выбрать Aktiv ruToken CSP v1.0.
- 4. После этого потребуется отключить токен, перезагрузить компьютер и подключить его обратно для применения настроек.

🐒 Панель управления Рутокен 🛛 🕹		
Администрирование Сертификаты Настройки О программе		
Считыватели Рутокен S		
Количество считывателей Рутокен S: 3 V Изменить		
Максимальное количество устройств Рутокен S, с которыми возможно работать одновременно.		
Настройки PIN-кода		
Администраторы могут настраивать параметры РІN-кодов: кзиирование, напоминание о смене РІN-кода по умолчанию, Настройка кодирование в UTF-8.		
Политики качества PIN-кодов		
Политики качества PIN-кодов позволяют повысить уровень Настройка Безопасности. При смене PIN-кода будет выполняться его проверка на стойкость согласно заданным критериям.		
Настройки криптопровайдера	Настройки криптопровайдера	×
Просмотр и изменение настроек криптопровайдера для различных моделей Настроить криптопровайдер	Модель Рутокен	Криптопровайдер по умолчанию
Фитрутокен.	Рутокен S и Рутокен Lite	Aktiv ruToken CSP v1.0 $$
	Семейство Рутокен ЭЦП	Aktiv ruToken CSP v1.0 🗸
	Настройки криптопровайдера А Способ генерации ключевых па для семейства устройств Рутокен	ktiv ruToken CSP v1.0 р RSA-2048 (и RSA-4096, если поддерживается) ЭЦП
Закрыть		ОК Отмена Применить

Регистрация сертификатов

Для корректной работы SignTool, необходимо зарегистрировать сертификат.

Для этого в Панеле Управления Рутокен, в разделе Сертификаты необходимо поставить галочку напротив нужного сертификата для подписи. Так же, необходимо проверить, что на нужном вами сертификате указан криптопровайдер Aktiv ruToken CSP v1.0.

👔 Панель управления Рутокен			Х
Администрирование Сертификаты Настрой	ки О програми	ме	
Подключенные Рутокены			
🖋 Рутокен ЭЦП 3.0 0	~	Ввести PIN	-код
Aktiv ruToken CSP v1.0	ернету: сертифи ой парой	кат действителен	
Имя	Истекает	Зарегистриров	ан
Сертификаты с ключами(3) user1, Users user1-9b9f96f5-2295-4168-858e-527-45	17.11.2025		
user1, Users user1-7ac82060-c970-4697-8222-7f9-35	03.11.2025		
user1, Users user1-230e1faf-756e-4708-88bb-1a9-3	14.09.2025		
Выписать сертификат	ать Удалить	По умолчанию	1 Свойства
			Закрыть

Подробнее с работой в Панели Управления Рутокен можно ознакомиться в статье Начало работы с устройствами Рутокен.

Настройка кеширования PIN кода

Для включения кеширования пин-кода необходимо обратиться в службу нашей технической поддержки.

Создание скрипта для подписания документов

Ниже приведён пример скрипта Power Shell для подписания файлов помещённых в заранее созданную папку через SignTool. Скрипт автоматически перемещает файл C:\test.exe в папку C:\sign и подписывает его. После чего, скрипт переходит в статус ожидания. Далее можно вручную переносить файлы в папку sign, скрипт автоматически их подпишет. Можно переносить и несколько файлов одновременно, скрипт подпишет их все по очереди. **Главное, чтобы в названии файла не было пробелов.**

Обратите внимание, что путь к signtool может отличаться в зависимости от версии установленного Windows SDK (в примере ниже, этот путь - signed light = "C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x64\signtool.exe").

Так же, в самой команде подписания sign, необходимо указывать отпечаток вашего сертификата (в примере ниже, это - sign /debug /sha1 f90be6d

6ba25c388a384189ba5cd7975a3a04389 /v /td SHA256 \$filePath).

Более подробно о том, как узнать отпечаток сертификата, можно прочитать в статье "Подпись файлов в Windows с помощью сертификата на Рутокен".

```
# Path and filter settings
$path = "C:\sign"
$filter = "*.*"
# Ensure the path exists
if (!(Test-Path $path)) {
  Write-Host "Path '$path' does not exist!"
  return
}
# The script block called when files are created
$action = {
  $signtoolPath = "C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x64\signtool.exe"
  $filePath = $Event.SourceEventArgs.FullPath
  $arguments = "sign /debug /sha1 f90be6d6ba25c388a384189ba5cd7975a3a04389 /v /td SHA256 $filePath"
  Write-Host "Signing file '$filePath'"
  #Start-Process -FilePath $signtoolPath -ArgumentList $arguments -NoNewWindow
  Invoke-Expression "& '$signtoolPath' $arguments"
}
$sourceldentifier = "FileCreated"
# Unregister the event if it is already registered
try {
  $existingEvent = Get-EventSubscriber -SourceIdentifier $sourceIdentifier -ErrorAction Stop
  if ($null -ne $existingEvent) {
     Unregister-Event -SourceIdentifier $sourceIdentifier
  }
}
catch {
  Write-Host "Event not found. Registering the event."
}
# Create the FileSystemWatcher
$fsw = New-Object IO.FileSystemWatcher $path, $filter
$fsw.EnableRaisingEvents = $true
$job = Register-ObjectEvent $fsw Created -SourceIdentifier $sourceIdentifier -Action $action
# Validate if the event is actually registered
if (Get-EventSubscriber | Where-Object { $_.SourceIdentifier -eq $sourceIdentifier })
{
  Write-Host "Event has been registered successfully."
}
else
{
  Write-Host "Failed to register event."
}
```

Write-Host "Script is now monitoring \$path."
<pre># Copy test.exe to the sign folder \$testExePath = "C:\test.exe" if (Test-Path \$testExePath) { Copy-Item \$testExePath -Destination \$path Write-Host "test.exe copied to \$path." } else { Write-Host "Could not find \$testExePath." }</pre>
Prevent the console from closing immediately do { Start-Sleep -Seconds 1 } while (\$true)

Добавление Скрипта в Службы Windows

Для того, чтобы скрипт работал при старте ОС и подписывал файл до входа в учётную запись пользователя, необходимо запустить скрипт как службу Windows.

Для этого используем NSSM (Non-Sucking Service Manager) — это утилита, позволяющая устанавливать исполняемые файлы приложений в качестве служб в ОС семейства Microsoft Windows.

1. Для установки NSSM, необходимо запустить PowerShell. Для этого, откроем поиск и наберём PowerShell ISE. Запустить его нужно от имени администратора.



2. Создаём новый файл и запускаем команды для установки NSSM:

Set-ExecutionPolicy Bypass -Scope Process -Force; iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.psl')) choco install nssm

🤮 Администратор: Windows PowerShell ISE	
Файл Правка Вид Сервис Отладка Дополнительскомпоненты Справка	
Fersingeneild not* X	
1 Set-ExecutionPolicy Bypass -Scope Process -Force:	^
2 iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))	
	~
PS_C+\Windows\ssc+wm32s	A
ro t. (windows) systemsza	\sim

3. Создаём новый сценарий в PowerShell ISE, прописываем наш скрипт для подписания файлов (из раздела Создание скрипта для подписи документов) и сохраняем в удобном месте (в нашем примере, скрипт сохранён по пути C:\script.ps1)



4. Далее, прописываем и запускаем команду для добавления нашего скрипта в службы Windows. В данном примере, служба будет называться "script".



5. Если необходимо удалить службу, можно в командной строке использовать команду sc delete "Имя Службы"

Настройка службы

1. Для начала, необходимо проверить, создалась ли наша служба. Для этого, в поиске прописываем и запускаем Службы.



2. В списке служб, находим нашу (в данном примере, называется script). Кликаем по ней правой кнопкой мыши и переходим в Свойства.

🌼 Службы						>	×
Файл Действие	Вид Справка						
(= =) 📰 🖾	à 📑 🛛 📰 🕨 🔲 🖬 🕨						
🔍 Службы (локалы	О. Службы (локальные)						
	script	^ Лия	Описание	Состояние	Тип запуска	Вход от имени	,
		McpManagementService	<Не удает		Вручную	Локальная сис	
	Остановить службу	MessagingService_83944	Служба, о		Вручную (ак.	Локальная сис	. 1
	Перезапустить службу	Alicrosoft App-V Client	Manages A		Отключена	Локальная сис	. I
		Microsoft Edge Elevation Se	Обеспечи		Вручную	Локальная сис	
		🌼 Microsoft Edge Update Serv	Обеспечи		Автоматиче	. Локальная сис	
		🆏 Microsoft Edge Update Serv	Обеспечи		Вручную (ак.	Локальная сис	
		🆏 Microsoft Update Health Se	Maintains		Отключена	Локальная сис	
		🥋 OpenSSH Authentication A	Agent to h	ent to h		Локальная сис	сис
		🆏 Plug and Play	Позволяет	Выполняется	Вручную	Локальная сис	
		🆏 PrintWorkflow_83944	Обеспечи		Вручную (ак.	Локальная сис	
		Quality Windows Audio Vid	Quality Wi		Вручную	Локальная слу	
		🔯 script		Запустить	иче	\User	
		Shared PC Account Manager	Manage	Остановить	ена	Локальная сис	
		🥋 SMP дисковых пространст	Служба		Þ	Сетевая служба	
		SysMain SysMain	Поддер	Приостановить	иче	. Локальная сис	
		WMware Alias Manager and	Alias M	Продолжить	иче	. Локальная сис	•
		WMware Snapshot Provider	VMware	Перезапустить	P	Локальная сис	•
		WMware SVGA Helper Service	Helps V	Все задачи	> иче	. Локальная сис	•
		WMware Tools	Provide		иче	. Локальная сис	•
		WarpJITSvc	Provide	Обновить	b (ак.	Локальная слу	•
		Windows Audio	Управл	Свойства	иче	. Локальная слу	٠,
		SR Windows Mixed Reality On	Enshler		_	Покальная сис	
< >	Расширенный / Стандартный /			Справка			_

3. В свойствах переходим во вкладку Вход в систему и указываем имя и пароль пользователя, от имени которого будет запускаться служба. Применяем и перезагружаем компьютер.

Свойства: script (Локал	ьный компьютер)		×
Общие Вход в систему	Восстановление	Зависимости	1
Вход в систему:	_		
О С системной учетно	й записью		
Разрешить взаи	модействие с рабоч	им столом	
О учетной записью:	.\User		Обзор
Пароль:	•••••	•	
Подтверждение:	•••••	•	
	ОК	Отмена	Применить

4. После настройки, службу необходимо перезапустить.

Подключение по SSH

Подписание файлов работает даже при переносе файлов в папку sign удалённо, через ssh.

Для подключения по ssh необходимо установить компонент OpenSSH Server на одну из клиентских машин (данный компонент доступен к установке при версии Windows 10 старше 1809). 1. Переходим в меню Пуск - Настройки - Приложения.

	R Use Docane Bixog	ная учет	ная запись					OneDrive Bxog	С Центр обновлен Windows Последняя проверка: 2 назад	ия 10 ч	Просмотр веб- страниц Рекомендуемые параметры
⊒	Система Экран, звук, уведомления, питание		Устройства Bluetooth, принтеры, мышь	Найти п	араме	тр Телефон Связата устройство с Android, iPhone	م (Сеть и Интернет Wi-Fi, режим "в самолет VPN	e",	¥	Персонализация Фон, экран блокировки, цвета
E	Приложения Удаление, значения по умолчанию, доп. компоненты	8	Учетные записи Учетные записи, зл. почта, синхронизация, работа, семья		∩ À字	Время и язык Распознавание голоса, регион, дата	8	Игры Xbox Game Bar, снимки, режим игры		ው	Специальные возможности Экранный диктор, контрастность
Q	Поиск Найти мои файлы, разрешения	A	Конфиденциальность Расположение, камера, микрофон	:	С	Обновление и безопасность Обновления Windows					

2. Зайти в раздел Дополнительные компоненты.

🔶 Параметры							
ሰ Главная		Приложения и возможности					
Найти параметр	٩	Выбор расположения для получения					
Придожения		приложений					
		Установка приложений исключительно из Microsoft Sto защитить ваше устройство.	ore поможет				
🗵 Приложения и	возможности	Из любого места					
і⊒т Приложения по	о умолчанию						
-							
Ші Автономные ка	ірты	Приложения и возможности					
🗈 Приложения ди	ія веб-сайтов	Дополнительные компоненты					
П Воспроизвелен		Псевдонимы выполнения приложения					
	ие видео	Поиск, сортировка и фильтрация по дискам. Чтобы удалить или переместить приложение, выберите его в списке.					
† Автозагрузка		Искать в этом списке					
		Сортировка: Имя У Фильтровать по: Все диски	/				
		Найдено приложений: 46					
		Cortana Microsoft Corporation	8,00 K5 22,04,2024				
			20.2 M				
		MICrosoft .NET Framework 4.8.1 SDK	20,3 Mb 22.04.2024				
		Microsoft .NET Framework 4.8.1 Targeting Pack	42,3 МБ 22.04.2024				

3. Нажать **Добавить компонент** и ввести в поиске **Сервер OpenSSH**. Также убедитесь, что на обеих машинах установлен компонент **Клиент OpenSSH**.



4. Для подключения к серверу OpenSSH, необходимо в командной строке ввести команду:

ssh username@IPaddress

Где username - это имя пользователя сервера, a IPaddress - это IP адрес сервера OpenSSH.

Так как OpenSSH по умолчанию работает через порт 22, необходимо убедиться, что у клиента и у сервера есть разрешения на использование этого порта.

Итог

Если вы настроили кеширование PIN-кода и создали службу как указано в инструкции, то при подключенном Рутокене к машине, у вас будет подписываться указанный вами в скрипте файл до логина в учётную запись пользователя. Далее, служба будет ожидать следующие файлы для подписи в папке sign.