

# программный комплекс «CMETA – CMAPT»

# Руководство по работе с

электронной подписью (ЭП)



# СОДЕРЖАНИЕ

1.		НАСТРОЙКА СЕРВЕРА ПРОВЕРКИ СЕРТИФИКАТОВ	
	1.1.	Установка CertServer	3
	1.2.	Установка корневого сертификата	3
	1.3.	Настройка «Сервер ключей»	6
2.		ЭЛЕКТРОННАЯ ПОДПИСЬ	7
	2.1.	Настройка ЭП в программном комплексе «Смета-Смарт»	7
	2.2.	Справочник уровней ЭП	8



## 1. НАСТРОЙКА СЕРВЕРА ПРОВЕРКИ СЕРТИФИКАТОВ

#### 1.1. Установка CertServer

CertServer - это служба, предназначенная для проверки валидности ЭП документов базы и первичных документов, а также отозванных сертификатов. CertServer осуществляет непосредственное взаимодействие SQL сервера и средства криптографической защиты информации CryptoPro.

На сервере, помимо самой Службы, должно быть установлено средство защиты Crypto Pro CSP и Корневой сертификат УЦ. Порт для обмена информацией с SQL Server - 3847 TCP.

При установке CertServer создает Службу, которая будет запускаться автоматически. Доверенные корневые сертификаты и сертификаты доверенных пользователей устанавливаются выбором соответствующей строки контекстного меню ярлыка службы. Так как служба запускается от имени системной учетной записи администратора, корневые доверенные сертификаты, которые были установлены в хранилище пользователя, необходимо перенести в папку сертификатов локального компьютера (*Рисунок 10шибка! Источник ссылки не найден.*).



Рисунок 11. CertServer

#### 1.2. Установка корневого сертификата

Для установки сертификата Удостоверяющего центра ООО «Кейсистемс» откройте файл сертификата и нажмите кнопку [Установить сертификат] (*Рисунок 2Ошибка! Источник ссылки не найден.*).



Сертификат ? 🔀					
Общие Состав Путь сертификации					
Сведения о сертификате					
 Целостность этого сертификата не гарантирована. Возможно, он поврежден или изменен.					
Кому выдан: СА КЕҮЅҮЅТЕМЅ					
<b>Кем выдан:</b> СА КЕҮSYSTEMS					
<b>Действителен с</b> 09.04.2012 по 10.04.2018					
<u>Установить сертификат</u> Заявление поставщик	ia				
O	<				

Рисунок 2. Сертификат

В открывшемся окне «Мастер импорта сертификатов» нажмите кнопку [Далее] (*Рисунок 3Ошибка! Источник ссылки не найден.*).



Рисунок 3. Мастер импорта сертификатов

В процессе установки выберите пункт **Поместить все сертификаты в следующее хранилище**. Для выбора хранилища сертификатов нажмите кнопку **[Обзор...]** (*Рисунок* **40шибка! Источник ссылки не найден.**).

![](_page_4_Picture_1.jpeg)

	_
Хранилище сертификатов	
Хранилища сертификатов - это области системы в которых производится хранение сертификатов.	_
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.	
С двтоматически выбрать хранилище на основе типа сертификата	
Поместить все сертификаты в следующее хранилище	
Хранилище сертификатов:	
<u>О</u> бзор	
	_
< Назад Далее > Отмена	1

Рисунок 42. Хранилице сертификатов

В открывшемся окне «Выбор хранилища сертификата» выберите папку «Доверенные корневые центры сертификации» и нажмите кнопку [OK] (*Рисунок 5*).

;		<b>_</b>				
нные корн	евые центры	ы сертифика				
тельные с	тношения в	предприяти				
(уточные і	центры серти	ификации				
нные изда	атели					
икаты, кі	которым нет	ловедия 🚬				
показать физические хранилища						
	анные корн птельные с суточные изда амкаты, ко ть физичес	нные корневые центрі ітельные отношения в (уточные центры серті інные издатели інкаты, к котопым нет ть физические хранили				

Рисунок 5. Выбор хранилища сертификатов

Для установки сертификата Удостоверяющего центра нажмите кнопку [Готово] (*Рисунок 6Ошибка! Источник ссылки не найден.*).

Мастер импорта сертификат	08	×
	Завершение работы мастера импорта сертификатов Работа мастера импорта сертификатов успешно завершена. Были указаны следующие параметры:	
	данилице сертификатов, выоранное пользователем Содержание	
	Назад Готово Отмена	

Рисунок 6. Завершение импорта сертификатов

![](_page_5_Picture_1.jpeg)

#### 1.3. Настройка «Сервер ключей»

Утилита проверки ЭП является необходимым компонентом для работы с ЭП в программном комплексе. Файл установки CertServerSetup.msi программы проверки ЭП размещен на сайте разработчика по адресу: http://keysystems.ru/files/misc/cert/CertServerNew/.

Установите службу сервера ключей, используя дистрибутив, на общедоступный компьютер, который и будет сервером ключей. На этом же компьютере должно быть установлено средство криптографической защиты информации CryptoPro. Укажите сервер ключей в соответствующей настройке программного комплекса (*Рисунок 7Ошибка! Источник ссылки не найден.*).

ДЕРЕВО НАСТРОЕК = > НАСТРОЙКИ = > ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ = > СЕРВЕР КЛЮЧЕЙ

![](_page_5_Picture_6.jpeg)

Рисунок 7. Сервер ключей

На сервере ключей также должны быть установлены сертификаты открытых ключей пользователей, ЭП которых будет накладываться на документы, либо корневой сертификат удостоверяющего центра, выдавшего сертификаты пользователям.

Служба проверки ЭП (сервер ключей) должна быть запущена. В ПК «Смета-Смарт» при нажатии кнопки **Просмотр/установка ЭЦП** на документе, имеющем подпись, SQL сервер обращается к серверу ключей, который проверяет корректность ЭП документа в соответствии с установленным на сервере ключей сертификатом открытого ключа.

Если настройка сервера указана неверно, либо на сервере ключей не запущена программа проверки ЭП CertServer.exe, при нажатии кнопки **Просмотр/установка ЭЦП** в графе **Статус** будет выдано сообщение об ошибке. При получении сообщения «Cannot connect» необходимо проверить корректность значения настройки *Сервер ключей* (значение отсутствует). Сообщение «Cannot resolve IP address» означает, что настройка задана, но к указанному серверу невозможно подключится.

![](_page_6_Picture_1.jpeg)

## 2. ЭЛЕКТРОННАЯ ПОДПИСЬ

#### 2.1. Настройка ЭП в программном комплексе «Смета-Смарт»

В программном комплексе (ПК) «Смета-Смарт» реализован механизм использования электронной подписи (ЭП). ЭП представляет собой реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭП и проверить принадлежность подписи владельцу сертификата ключа ЭП. Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭП.

Для работы с ЭП в ПК «Смета-Смарт» необходимо выполнить основные настройки (Рисунок 8).

Hac	тройки Сорв	Mc 2avaar	ии Окир Сп		70 n	
	Настройки	ine Salaraz			жинастройки объектов	x
	Настройки документов Параметры				Са т 88 Пользователь: <Общее значение>	-
	Изменение пароля Реквизиты пользователя Заявка администрирования пользователя Пользователи Группы пользователей Шаблоны создания пользователей АРМы		ателя	<ul> <li>Удаленный доступ</li> <li>Электронная подпись</li> <li>Ж Адрес службы штампов времени</li> <li>Ж Документы для подписания ЭЦП, соот</li> <li>Ж Идентификатор ключа</li> <li>Ж Искать сертификаты в локальном хран</li> <li>Ж Использовать алгоритм подписывания</li> <li>Ж Использовать Автомат ЭЦП</li> </ul>		
2	Пул соединений пользователей Сбросить состояние окон приложения Работать в автономном режиме 07.05.2017 09.05.201			ия 09.05.201	<ul> <li>- № Использовать ЭЦП</li> <li>- № Назначение сертификатов (OID)</li> <li>- № Контроль ФИО сертификата с ФИО в р</li> <li>- № Настройка уровней пользователей</li> <li>- № Пополемии с водпистичники вокология</li> </ul>	
и нави ации			07.03.2017	13.03.201	При зачислении проверять ЭЦП прикг     Ж Проверять сертификаты в списке отоз     М     Поведение с подписанными докупени     Кастройка общая для всех]	
Ганы	14.03.2017				ОК Отмена Примен	ИТЬ

Меню Настройки: НАСТРОЙКИ \ Электронная подпись

Рисунок 8. Настройка ЭП

Настройка ЭП в ПК «Смета-Смарт» производится по следующим параметрам:

• Использовать ЭП(Да\Нет) – данная настройка включает/выключает использование ЭП.

• Сервер Ключей - указывается сервер сертификации, который служит для проверки подлинности подписи.

• Назначение сертификата(OID) – указываются числовые значения соответствующие конкретному назначению сертификата (OID). Например, если указать в поле 1.3.6.1.4.1.311.10.3.12, то подписывать смогут только пользователи с назначением подписи Подписывание документа; если поле оставить пустым, то подписывать смогут пользователи с любым назначением сертификата.

Для того чтобы посмотреть назначение сертификата нужно нажать на кнопку **(Пуск)** и в поисковой строке ввести **Certmgr.msc**. В открывшемся окне раскрыть папку «Личное» → «Сертификаты» в правой части окна выбрать сертификат и открыть его двойным щелчком

#### <u>Подсистема «Смета – СМАРТ»</u>

![](_page_7_Picture_1.jpeg)

мыши. В открывшемся сертификате перейти на вкладку «Состав» и выбрать поле «Улучшенный ключ». В поле «Улучшенный ключ» отображается назначение сертификата (*Рисунок 9*).

ПУСК => ВЫПОЛНИТЬ => CERTMGR.MSC => ЛИЧНОЕ => СЕРТИФИКАТЫ => СОСТАВ => УЛУЧШЕННЫЙ КЛЮЧ

	Сертификат			
Программы (1)	Общие Состав Путь сертификации			
🚡 Certmgr				
Файлы (1)	Показать: <Все>			
Installation_Certificate_Windows_7	Поле Значение			
1	Действителен с       15 апреля 2014 г. 11:38:05         Действителен по       15 апреля 2016 г. 11:48:05         Субъект       ermolaeva@keysystems.ru, Д         Открытый ключ       RSA (1024 Bits)         Сседения о шаблоне серт       Шаблон=DomainUser(1.3.6.1         Улучшенный ключ       Защищенная электронная п         Использование ключа       Цифровая подпись, Шифров         Подписывание сертимисата       11Политиса сертимисата:И         Защищенная электронная почта (1.3.6.1.5.5.7.3.2)       то подписывание колоча         Подписывание кода (1.3.6.1.5.5.7.3.3)       Поравка отметки времени (1.3.6.1.5.5.7.3.2)         Установка отметки времени (1.3.6.1.5.5.7.3.8)       Установка отметки времени (1.3.6.1.5.5.7.3.3)			
Ознакомиться с другими результатами Certmgr.msc	Свойства Копировать в файл Подробнее о <u>составе сертификата</u>			
	OK			
🖀 Certmgr - [Сертификаты - текущии пользовате	ль\Личное\Сертификаты]			
Файл Действие Вид Справка				
🗢 🔿 🖄 📰 🤞 💺 🕅 🗟 🛛 🖬	1 (2)			
🗊 Сертификаты - текущий пользователь	Кому выдан Кем выдан			
⊿Личное	🗧 🗣 Дмитриева Кристина Дмитриевна 🛛 KSCA2			
Сертификаты				
<ul> <li>Доверительные отношения в предприяти</li> </ul>	и			
Промежуточные центры сертификации				
Хранилище Личное содержит 1 сертификат.				

Рисунок 9. Назначение сертификата

• Срок действия закрытого ключа (дни) – допустимый период для закрытого ключа, в который можно использовать ЭП для подписи отчета, после истечения этого периода необходимо переполучить сертификат.

#### 2.2. Справочник уровней ЭП

Справочник уровней ЭП несет в себе информацию, к какому типу и уровню относится пользователь. Уровни позволяют выстраивать порядок подписания отчетов.

#### НАВИГАТОР\СПРАВОЧНИКИ \ ПРОЧИЕ СПРАВОЧНИКИ \ УРОВНИ ЭЦП

![](_page_8_Picture_0.jpeg)

»	🖹 Уровни З	эцп	x				
		Кол-во пользователей Σ	Номер	Наименование			
	*						
		16	1	эцп			

Рисунок 10. Справочник уровней ЭП

Окно состоит из панели инструментов и списка пользователей, входящих в уровни (Рисунок 10).

С помощью кнопок на панели инструментов можно выполнять следующие операции:

**Создать** (Ctrl + N) – добавить уровень в справочник уровней ЭП;

Редактировать (Ctrl + E) − отредактировать уже имеющийся уровень в справочнике уровней ЭП;

🗙 Удалить – удалить уровень из справочника уровней ЭП;

ڬ Печать (Ctrl + P) – вывести на печать список уровней ЭП;

<sup>1</sup> Передать (Ctrl + R) – Выгрузить в файл список уровней ЭП;

**Принять** (Ctrl + R) – Загрузить из файла список уровней ЭП;

Solution (Ctrl + R) – обновить список уровней ЭП;

Окно уровней ЭП включает в себя:

• Кол-во пользователей – отображается количество пользователей включенных в данный уровень ЭП;

• Номер – отображается уровень, в который входит пользователь;

• Наименование – отображается наименование уровеня ЭП;

Чтобы создать новый уровень необходимо на панели инструментов нажать на кнопку [Создать], чтобы изменить существующий уровень необходимо на панели инструментов нажать на кнопку [Редактировать]. Затем в окне редактирования уровня (*Рисунок 11*) необходимо ввести в поле «Номер» уровень ЭП и в поле «Наименование» ввести имя уровня. В таблице необходимо заполнить список пользователей включенных в уровень ЭП. После нажать на кнопку Сохранить.

![](_page_9_Picture_1.jpeg)

Номер:				1		
Наименование:				ЭЦП 1 уровня		
· · · · · ·		4IIF				I <b>v</b>
-2	⊞		Пол	ьзователь	Примечание	Идентификатор ключа
3-	×					
			boc	h		
7			pnn			
• M		мац	ца			

Рисунок 11. Редактирование уровней ЭП

Для того чтобы добавить нового пользователя в справочник уровней ЭП необходимо нажать на кнопку [Добавить строку]. В поле «Пользователь» указать логин, под которым пользователь работает в программе, логин выбирается из справочника. В поле «Идентификатор ключа» выбрать из справочника сертификат.

Поле «Идентификатор ключа» можно оставить пустым, тогда при подписании отчета пользователю будут предложены все доступные сертификаты на компьютере.

#### 2.3. Подписание отчета ЭП в документах

Подписание отчетов происходит в списке документов нужного режима, например «Заявка на кассовый расход».

#### НАВИГАТОР \ ДОКУМЕНТЫ \ БЕЗНАЛИЧНЫЕ РАСЧЕТЫ \ ЗАявка на кассовый расход

В меню кнопки [Электронная подпись] на панели инструментов расположены следующие кнопки:

• Электронная подпись - вывести список, который содержит информацию о подписях документа и авторах;

- **Печать информации об ЭЦП** (Ctrl+P) –вывести информацию об ЭП для печати;
- **Подписать документ** позволяет поставить ЭП на выбранный документ;

При подписании отчета у пользователей, у которых в справочнике «Уровни ЭП» в поле Сертификат ничего не указано, появляется всплывающее окно со всеми доступными сертификатами на компьютере (*Рисунок 12*).

![](_page_10_Picture_1.jpeg)

![](_page_10_Picture_2.jpeg)

Рисунок 12. Выбор сертификата пользователя при подписание отчета

• После выбора нужного сертификата и нажатии на кнопку [OK] будет выдан протокол подписания отчета.

• Снять подпись – снимает ЭП с подписанного документа.

После подписания, у документа добавляется статус 🥒 Документ подписан ЭЦП.