КРАТКОЕ РУКОВОДСТВО

[**1. Настройки Континент TLS для работы с ПК «Бюджет-Смарт Про» (республиканская база) 1**](#_Toc187305432)

[**1.1. Установка личного сертификата 1**](#_Toc187305433)

[**1.2. Настройка списка ресурсов 1**](#_Toc187305434)

[**1.3. Установка серверного сертификата 2**](#_Toc187305435)

[**1.4. Установка корневого сертификата CAP root CA и корневого сертификата Удостоверяющего центра АУ «ЦИТ» 3**](#_Toc187305436)

[**1.5. Обновление CRL 5**](#_Toc187305437)

[**1.6. Наличие лицензии КриптоПро CSP 5**](#_Toc187305438)

# Настройки Континент TLS для работы с ПК «Бюджет-Смарт Про» (республиканская база)

# Установка личного сертификата

Необходимо установить личный сертификат, выданный АУ «ЦИТ», через программу Крипто Про CSP по инструкции, записанной на USB-носитель (Инструкция по установке сертификата и настройке рабочего места.pdf).

# Настройка списка ресурсов

В основном меню Континент TLS-клиента выберите пункт "Главная". В области отображения информации откроется список имеющихся защищенных ресурсов и TLS-серверов (соединений). Выберите закладку "Добавить" на панели инструментов, а затем "Ресурс" в раскрывшемся списке. В правой части области отображения информации основного окна появится поля настроек, их нужно заполнить как на скриншоте, указав имя ресурса **budg.cap.ru** и **smartod.cap.ru**





# Установка серверного сертификата

Необходимо установить серверный сертификат АУ «ЦИТ», записанный ЦИТом на USB-носитель пользователя (**АУ \_ЦИТ\_ Минцифры Чувашии (серверный).cer**) или скачать по ссылке <https://cit.cap.ru/doc/laws/2024/11/25/prochee>.

Для установки серверного сертификата запустите Континент TLS**.** Выберите в главном меню TLS-клиента пункт "Управление сертификатами".

В области отображения информации появится список установленных сертификатов. На панели инструментов выберите категорию Серверные сертификаты и нажмите кнопку "Импортировать".

На экране появится стандартное окно открытия файла. Укажите серверный сертификат, записанный ЦИТом на USB-носитель пользователя (**АУ \_ЦИТ\_ Минцифры Чувашии (серверный).cer**) и нажмите кнопку "Открыть". Начнется загрузка и установка сертификата. После успешного завершения операции на экране появится соответствующее информационное сообщение.

Нажмите кнопку "ОК".

После установки серверного сертификата в главном меню TLS-клиента пункт "Управление сертификатами" добавленный серверный сертификат должен выглядеть так:



# Установка корневого сертификата CAP root CA и корневого сертификата Удостоверяющего центра АУ «ЦИТ»

Необходимо скачать корневой сертификат CAP root CA по ссылке [Скачать сертификат](https://fs.cap.ru/file/ALioimUnMNOlVM3VImczQ97jiu5zYS8G)

Двойным щелчком мыши открыть скачанный файл **CAP-root-CA\_new.cer**. Нажать кнопку «Установить сертификат»



Выбираем «Текущий пользователь»



Выбираем пункт «Поместить все сертификаты в следующее хранилище» и нажимаем «Обзор»



**Выбираем «Доверенные корневые центры сертификации»**



 





**Аналогично установить Корневой сертификат Удостоверяющего центра АУ «ЦИТ» Минцифры Чувашии (uc-au-cit2023.cer), который записан на USB-носитель пользователя или по ссылке** <https://cit.cap.ru/news/2023/12/05/tls-cert-2023>

# Обновление CRL

Выберите в главном меню TLS-клиента пункт "Управление сертификатами", вкладка «CDP» и нажать на кнопку «Скачать CRL».

****

# Наличие лицензии КриптоПро CSP

Необходимо проверить наличие постоянной лицензии КриптоПро CSP

