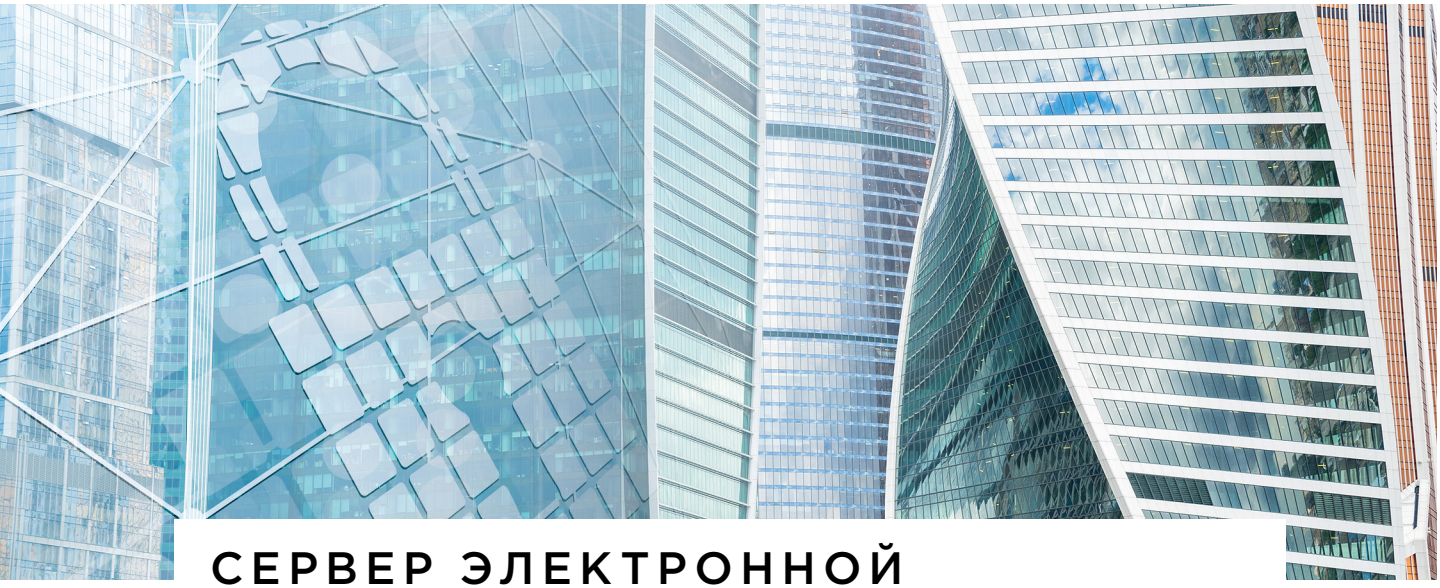
КРИПТОПРО

СЕРВЕР ЭЛЕКТРОННОЙ ПОДПИСИ

КРИПТОПРО DSS


КРИПТОПРО



СЕРВЕР ЭЛЕКТРОННОЙ ПОДПИСИ **КРИПТОПРО DSS**

КриптоПро DSS — это сервер облачной электронной подписи, позволяющий различным организациям предоставлять удобный способ подписания документов своим пользователям. Электронная подпись становится по-настоящему легкой с КриптоПро DSS.

КриптоПро DSS предоставляет веб-интерфейс, который может использоваться как сам по себе, так и в составе других веб-порталов. Для интеграции с системами дистанционного банковского обслуживания, электронного документооборота, торговыми площадками, приложениями для настольных компьютеров, мобильными устройствами и т. д. предоставляются различные API. На выбор доступны интерфейсы SOAP, REST и HTTP API (HTTP Redirect). Облачные ключи также можно использовать через стандартный интерфейс CryptoAPI.

Ключи пользователей создаются и хранятся в защищенном криптографическом модуле КриптоПро HSM, оставаясь неизвлекаемыми. КриптоПро HSM обеспечивает класс защиты КВ2, благодаря чему ключи надежно защищены даже от администратора.

КриптоПро DSS поддерживает различные способы аутентификации, начиная от обычных паролей до наиболее строгих криптографических методов. Для создания квалифицированной ЭП могут использоваться:

- Мобильное приложение myDSS (доступно для iOS и Android);
- Специальная SIM-карта с криптографическим апплетом;
- Аутентификация с использованием средств протокола TLS, смарт-карт или USB-токенов с криптографией.

Также поддерживаются и другие методы аутентификации:

- Одноразовые пароли по SMS (OTP-via-SMS);
- OATH-совместимые генераторы одноразовых паролей (OTP-токены);
- Внешние Центры Идентификации с поддержкой стандартных протоколов федеративной аутентификации WS-Federation и OpenID Connect.

С использованием внешних Центров Идентификации можно обеспечить прозрачный вход (single sign-on) пользователей внешних систем в КриптоПро DSS.

ПРЕИМУЩЕСТВА **КРИПТОПРО DSS**

НАИВЫСШАЯ СТЕПЕНЬ ЗАЩИТЫ КЛЮЧЕЙ ОТ КОМПРОМЕТАЦИИ

Ваши ключи создаются и хранятся в защищенном криптографическом модуле HSM, оставаясь неизвлекаемыми. HSM снабжен датчиками вскрытия, контролем портов, механизмами доверенной генерации и уничтожения ключей, защитой от утечек по побочным каналам – и это далеко не все. Ключи надежно защищены даже от внутреннего нарушителя, являющегося администратором. Схемы аутентификации пользователей имеют уровень безопасности не ниже, чем у самих хранимых ключей. Ключи становятся не просто неизвлекаемыми, но и некомпрометируемыми.

ПОДДЕРЖИВАЕМЫЕ ФОРМАТЫ ПОДПИСИ:

- CMS/PKCS#7;
- CAdES-BES, CAdES-T и CAdES-X Long Type 1;
- XML Digital Signature, XMLDSig;
- Подпись PDF (Open Document Format -.pdf);
- Подпись документов Microsoft Office (Open Office XML -.docx, xlsx);
- Необработанная подпись ГОСТ Р 34.10 (для создания на её основе других форматов).

ПОДЛИННАЯ МОБИЛЬНОСТЬ ПОДПИСИ

Забудьте про связку из токенов, USB-хаб и установку драйверов. Вы больше не будете привязаны к одному рабочему месту – к вашему ключу в облаке вы можете получить доступ из любого места и с любого устройства: с настольного компьютера, ноутбука, планшета, смартфона и простого «телефона-звонилки» даже без Интернета. Не отчаивайтесь, если в день торгов вы забыли ключевой носитель дома – альтернативный способ аутентификации позволит даже в таких ситуациях все подписать в срок.

ПОДДЕРЖИВАЕМЫЕ ОПЕРАЦИИ

- Подписание документа
- Проверка подписи документа
- Проверка сертификата
- Дополнение подписи до усовершенствованного формата
- Шифрование и расшифрование документов
- Создание запросов на сертификат для передачи в удостоверяющий центр
- Автоматическая отправка запросов в ПАК КриптоПро УЦ для управления сертификатами пользователей

1. Пользователь, система или кто-то за пользователя создает документ в сервисе, интегрированном с КриптоПро DSS.
2. Документ отправляется на сервер КриптоПро DSS на подписание данному пользователю.
3. КриптоПро DSS запрашивает разрешение на подпись документа в мобильном приложении myDSS.
4. Пользователь видит в приложении подписываемый документ, подтверждает операцию, вводит пароль или проходит аутентификацию Touch ID/Face ID
5. На сервер КриптоПро DSS отправляется криптографический код подтверждения, привязанный к пользователю, к содержимому документа, времени операции и отпечатку устройства.
6. После проверки кода подтверждения КриптоПро DSS отправляет запрос на подписание документа ключом пользователя в КриптоПро HSM и получает подписанный документ.
7. Подписанный документ отправляется обратно в систему.

УСТАНОВКА СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ НЕ ТРЕБУЕТСЯ

На рабочее место, которым может быть и мобильное устройство, нужно установить лишь простое в использовании легковесное средство аутентификации. Работу по настройке всех криптографических механизмов и форматов, а также по управлению ключами возьмут на себя наши серверные компоненты. Отсутствие средств электронной подписи на рабочем месте позволяет обеспечить централизованное управление ключами в корпоративной сети.

ПРОИЗВОДИТЕЛЬНОСТЬ, НАДЕЖНОСТЬ И ОТКАЗОУСТОЙЧИВОСТЬ

Вычисление электронной подписи в КриптоПро DSS происходит со скоростью, сравнимой со скоростью работы «фермы» из тысяч USB-токенов. Простым увеличением аппаратных ресурсов можно масштабировать производительность до любого необходимого уровня. В отличие от физического, облачный токен никогда не сломается, не утонет в кофе и не потеряется. Вы наконец-то можете забыть о страхе в критический момент оказаться один на один с отказавшим устройством, у которого попросту исчерпан ресурс. Аппаратное резервирование серверных компонент позволит пережить любой сбой незаметно для пользователей.

СОХРАНЕНИЕ ИНВЕСТИЦИЙ

Вам не придется менять или дорабатывать систему документооборота. Не нужно отказываться от привычного ПО для работы с электронной подписью. Все, что умеет работать со стандартом де-факто российского рынка средств ЭП – КриптоПро CSP, при установке облачного криптопровайдера Cloud CSP бесшовно сможет использовать ключи в КриптоПро DSS. Не спешите выбрасывать и аппаратные токены, они смогут послужить в качестве средств аутентификации к ключам пользователей в облаке. Для перехода на алгоритм ГОСТ Р 34.10-2012 не нужно покупать ни новые токены, ни новое ПО – переход не потребует дополнительных вложений*.

**В рамках расширенной технической поддержки*

СНИЖЕНИЕ СТОИМОСТИ ВЛАДЕНИЯ

По сравнению с локальными средствами ЭП, аппаратными токенами и смарт-картами, при использовании КриптоПро DSS существенно упрощаются процедуры передачи СКЗИ пользователям и установки средств ЭП на рабочие места. Централизованное хранение ключей с аппаратным резервированием, высокая производительность и возможность обслуживания множества пользователей одним сервером значительно уменьшают стоимость владения данным решением.

Первое и единственное сертифицированное ФСБ России средство облачной электронной подписи.*

**на 1 сентября 2018 г.*

ДЛЯ
ЗАМЕТОК


КРИПТОПРО

INFO@CRYPTOPRO.RU