INSTITUTE VLATACOM

vKDS

Система распределения ключей Vlatacom vKDS (Vlatacom Key Distribution System)

Описание системы

Система распределения ключей компании Vlatacom близко взаимодействует со структурой открытых ключей (PKI) и системой создания симметричных ключей. Результатом является финальный инкапсулированный ключ, который кроме содержимого ключа содержит сертификаты, и его может использовать только уполномоченное лицо только на устройстве, для которого он был создан. Поскольку процесс шифрования заснован на использованных ключах, предложенное ключевое решение по обеспечению безопасности ИКТ-системы создает фундамент для правильного использования устройств шифрования текста и файлов, устройств шифрования голоса, устройств телеконференцсвязи, устройств шифрования линий передачи и интегральной безопасности всей информационной системы.

Основные характеристики

- Централизованная система управления ключами.
- Совместимость с системой сертифицирующих органов Vlatacom vCA (Vlatacom Certification Authorities system) и системой создания симметричных ключей Vlatacom vSKP (Vlatacom Symmetrical Key Production System).
- Связь с vCA и vSKP через оптические волокна с протоколами TLS и SSL обеспечивает максимальный уровень безопасности коммуникации.
- Сильная трехфакторная проверка подлинности и авторизация всех участвующих лиц, заснованная на системе vCA, подразумевает три принципа: «то, что я есть», «то, что у меня есть» и «то, что я знаю».
- Подлинность всех устройств в цепи управления ключами проверяется vCA.
- Обеспечивает безопасную коммуникацию между машинами.
- Устройство распределения ключей, защищенное от постороннего вмешательства, с трехфакторной проверкой подлинности.
- База данных об использовании ключей.

Поддерживаемые стандарты

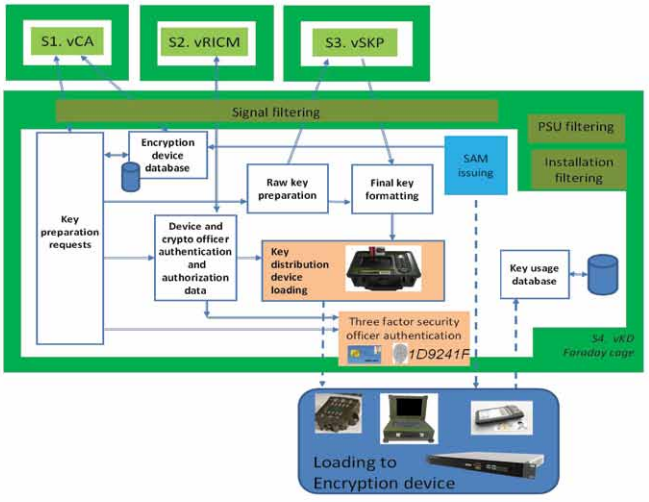
- Управление ключами в соответствии с X.509, PKIX (RFC5280) и PKCS#12.
- Поддерживаемые протоколы для коммуникации с CA: OCSP (RFC2560, RFC5019), CRLS (RFC4387), CMP (RFC4210 and RFC 4211). Список отзыва сертификатов в соответствии с RFC5280.
- Распределенные ключи создаются на основе чисто случайных последовательностей, которые соответствуют NIST SP 800-22A.
- Ключи хэшируются в соответствии с NIST SHS PUB 180-4.
- Пользовательские коммуникационные протоколы, хэш-функция и схемы управления ключами доступны по требованию.

Архитектура системы и интерфейсы

Вся система установлена в электромагнитной, защищенной от подслушивания среде. Уполномоченный сотрудник по вопросам безопасности, подлинность которого проверят vCA,
отправляет запрос на подготовку ключа на определенное устройство шифрования, который на устройствах загружают специальные сотрудники по вопросам безопасности. В соответствии с этими запросами, система создания симметричных ключей создает ключ в «сыром» формате. Ключ запаковывается в финальном формате и становится готовым для загрузки на защищенное от постороннего вмешательства устройство распределения ключей. Ключи загружаются на устройства шифрования на отдаленном терминале в электромагнитных «палатках» или клетках Фарадея. Информация об успешной загрузке ключей на устройство шифрования сохраняется на устройстве распределения ключей, а загруженные ключи удаляются навсегда, чем снижается до минимума возможность несанкционированного доступа и обеспечивается максимальный уровень безопасности. База данных распределения ключей возвращается в клетку, и информация о загрузке ключей на устройстве шифрования сохраняется в базе данных об использовании ключей.

Главные преимущества

- Одна централизованная система распределения ключей для всех устройств шифрования.
- Централизованное создание ключей и база данных об использовании ключей обеспечивают максимальный уровень безопасности и контроля над всем процессом шифрования.
- Обеспечивает долгосрочную безопасную коммуникацию между машинами.



INSTITUTE VLATACOM

Address:
Vlatacom d.o.o.
Milutina Milankovića 5
11070 Belgrade, Serbia

tel: +381 11 377 11 00
fax: +381 11 377 11 99
info@vlatacom.com
www.vlatacom.com