ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА - БАЗОВАЯ ОСНОВА СЗИ В ОС ASTRA LINUX SPECIAL EDITION

Аксенова Мария

Аналитик Департамента системного анализа и управления требованиями
Дирекции базовой операционной системы

Часть комплекса защиты ОС

- Мандатный контроль целостности
- Замкнутая программная среда
- Мандатное управление доступом
- Защита СУБД и средств виртуализации
- Киоск

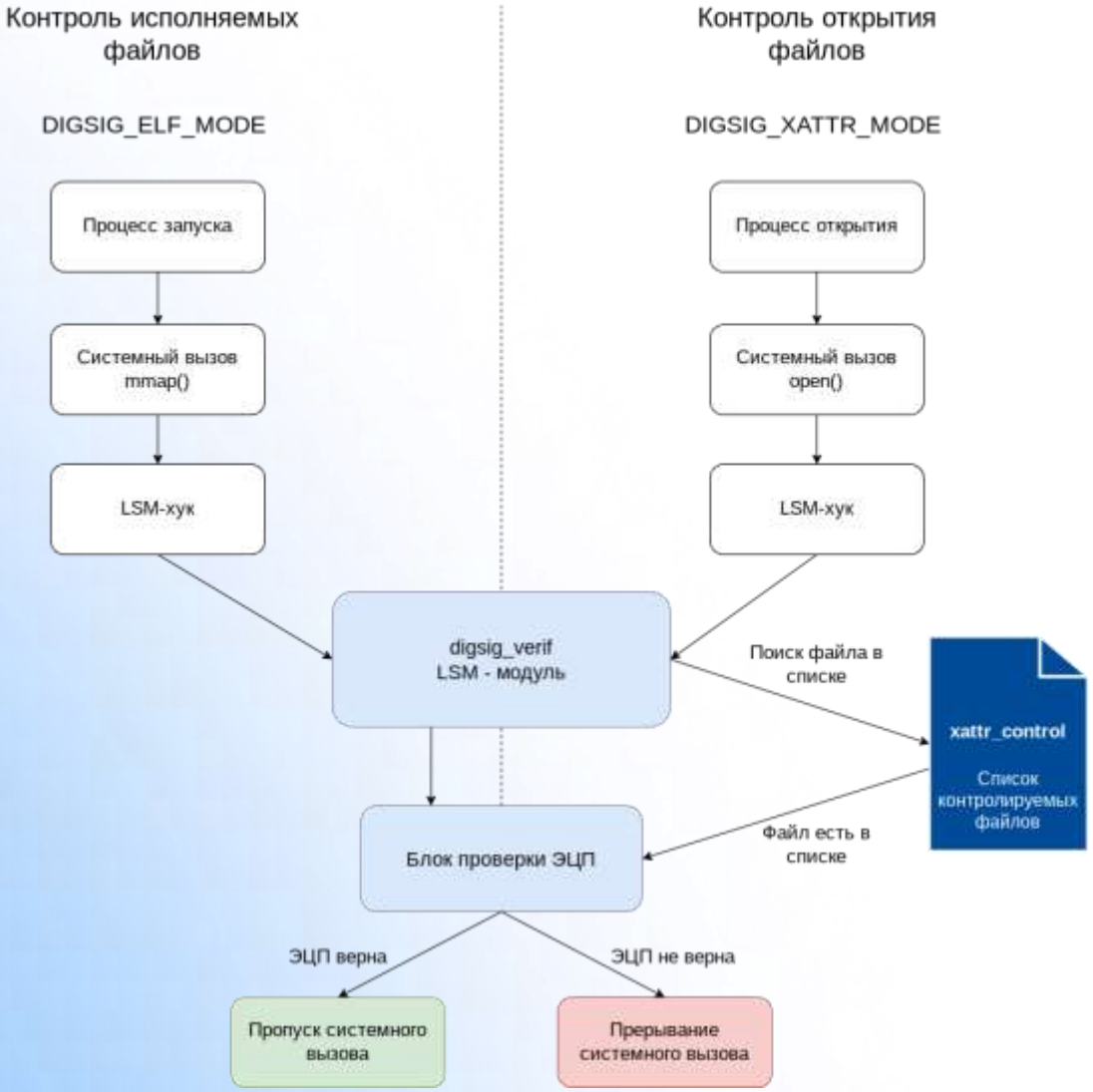
Для чего это нужно?

Замкнутая программная среда

- Гарантировать подлинность программного обеспечения. Все бинарные файлы и библиотеки типа ELF проходят процедуру подписания при сборке дистрибутива, которую выполняет как сам производитель ОС, так и вендоры ПО.

- Выполнять динамический контроль целостности файлов в процессе эксплуатации. Это минимизирует время реакции на изменения, так как запуск (или открытие) измененного файла будет запрещён сразу же.

Как это работает?



Уведомление 20:05

Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG) /home/astra/Desktops/ Desktops1/helloworld

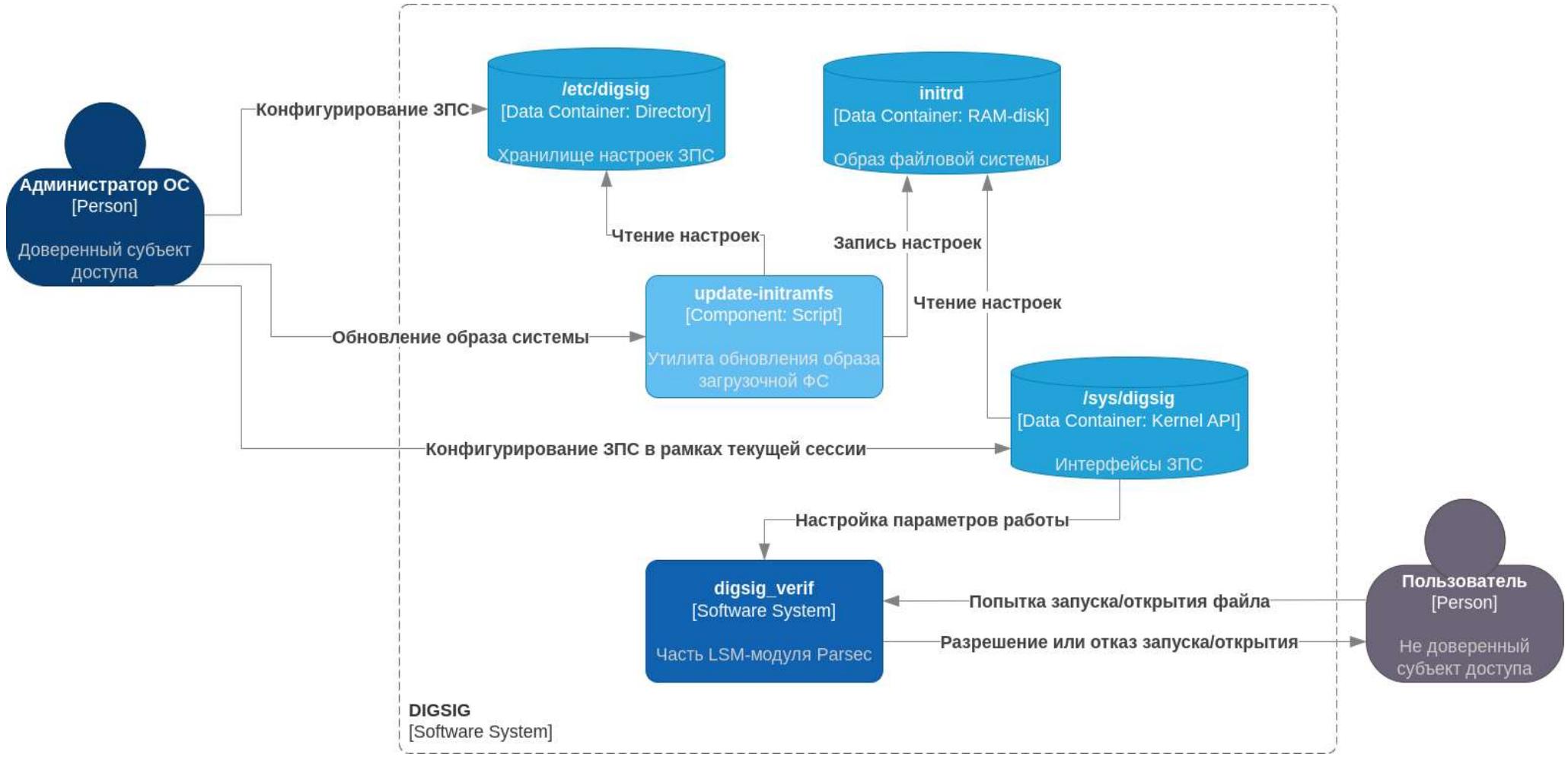
Уведомление 20:05

Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG) /home/astra/Desktops/ Desktops1/OSDAY2024.txt

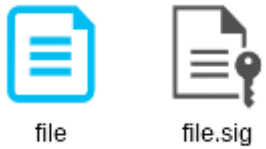
Уведомление 20:05

Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG) /opt/VBoxGuestAdditions-6.1.46/bin/VBoxClient

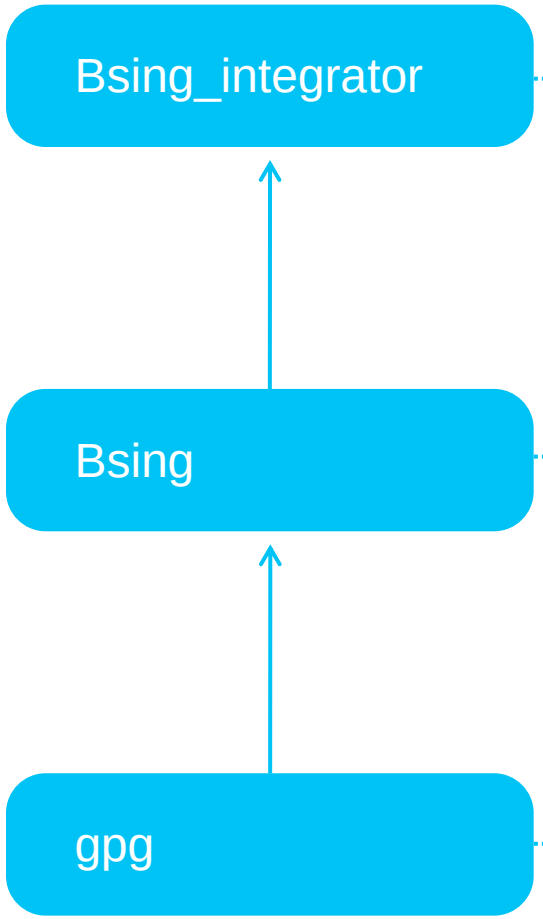
Настройка модуля



Способы создания подписи

Вид подписи		Сценарий использования
	elf	Используется для создания подписи внутри бинарного файла или разделяемой библиотеки типа ELF.
	attached	Используется для организации доверия к PE-файлам, в том числе DLL. Предназначен для контролируемого запуска Windows-программ в среде Wine.
	xattr	Используется на местах эксплуатации ОС для организации доверия, например, к конфигурационным файлам отдельных программ.
	dettached	Предназначен для файлов произвольного типа, в том числе для модулей ядра. Он не нарушает структуру исходного файла, что может играть важную роль в системах, использующий периодический контроль целостности по эталонным значениям контрольных сумм.

Инструменты для работы с подписями



Утилита верхнего уровня. Является надстройкой над bsing и поддерживает функции:

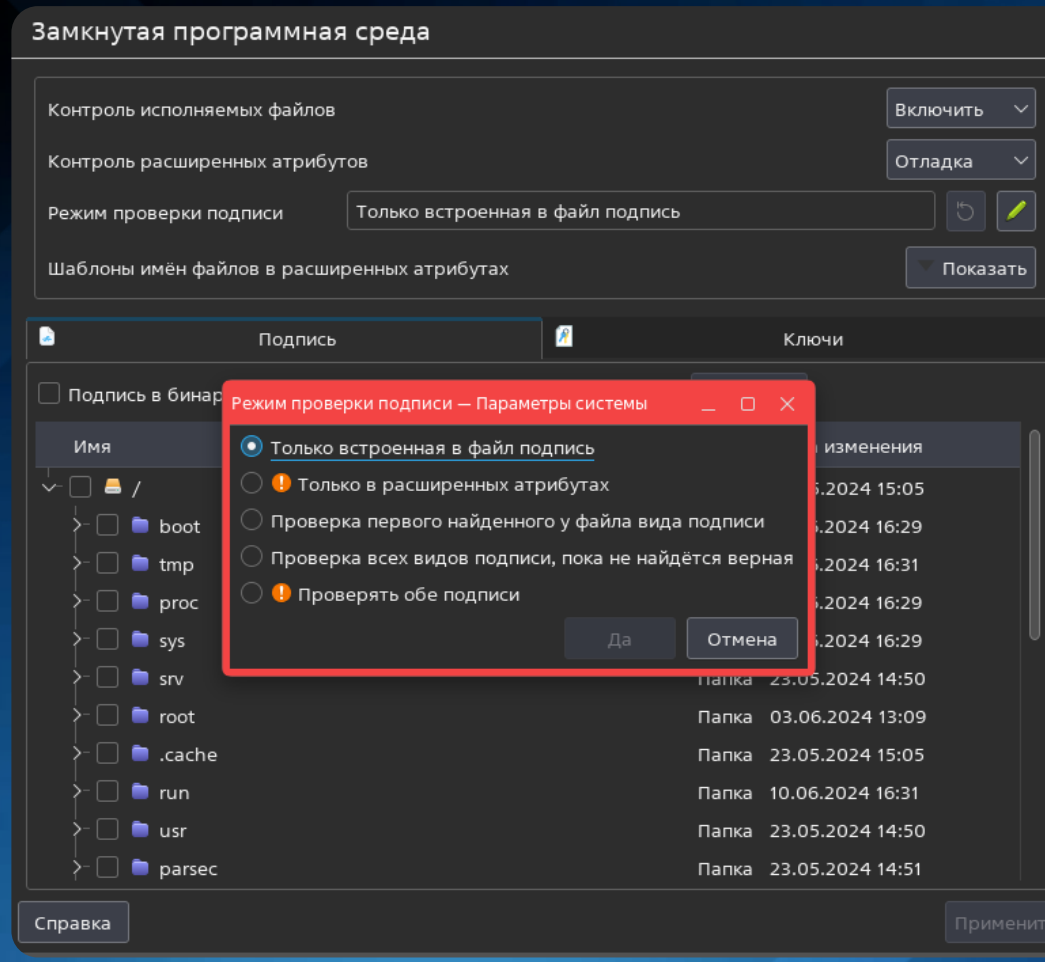
- Автоматического определения типа файла и создания соответствующей ему вида подписи
- Создание подписей для набора файлов по спискам или директориям
- Анализа файловой системы и формирования списка файлов, соответствующих заданному идентификатору сертификата ключа цифровой подписи

Утилита базируется на gpg и используется для создания заданного вида подписи файлов

Утилита нижнего уровня. Используются для генерации ключевых пар в соответствии с отечественными стандартами.

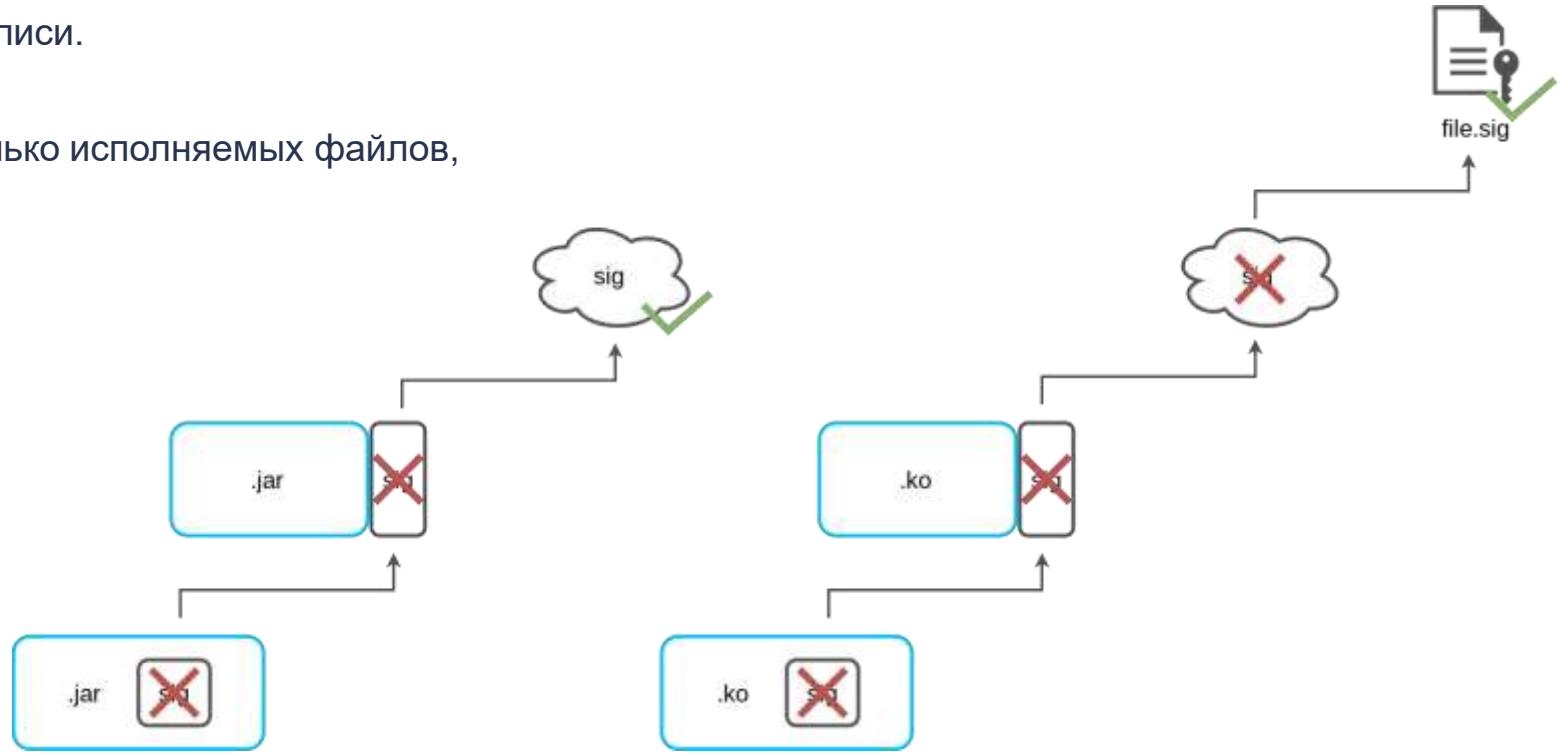
Режимы проверки подписи

- Режим проверки только встроенной подписи. Базовый режим контроля запуска файлов, актуален только для исполняемых файлов и разделяемых библиотек типа ELF.
- Режим проверки первого найденного вида подписи. Поиск подписи выполняется в следующем порядке: встроенная подпись, подпись в расширенных атрибутах, отсоединенная подпись.
- Режим поиска верной ЭЦП. В данном режиме выполняется проверка всех видов подписей до тех пор, пока не найдётся верная. Режим обеспечивает отказоустойчивость ПО в случае отзыва сертификата проверки его встроенной подписи.
- Режим проверки подписей только в расширенных атрибутах. Режим, обеспечивающий полный переход к цепочке доверия, сформированной на уровне эксплуатирующей ОС организации.
- Режим проверки как встроенной подписи, так и подписи в расширенных атрибутах. Усиленный режим двухфакторной проверки подписей файлов как на сертификате производителя ПО, так и на собственном сертификате организации.

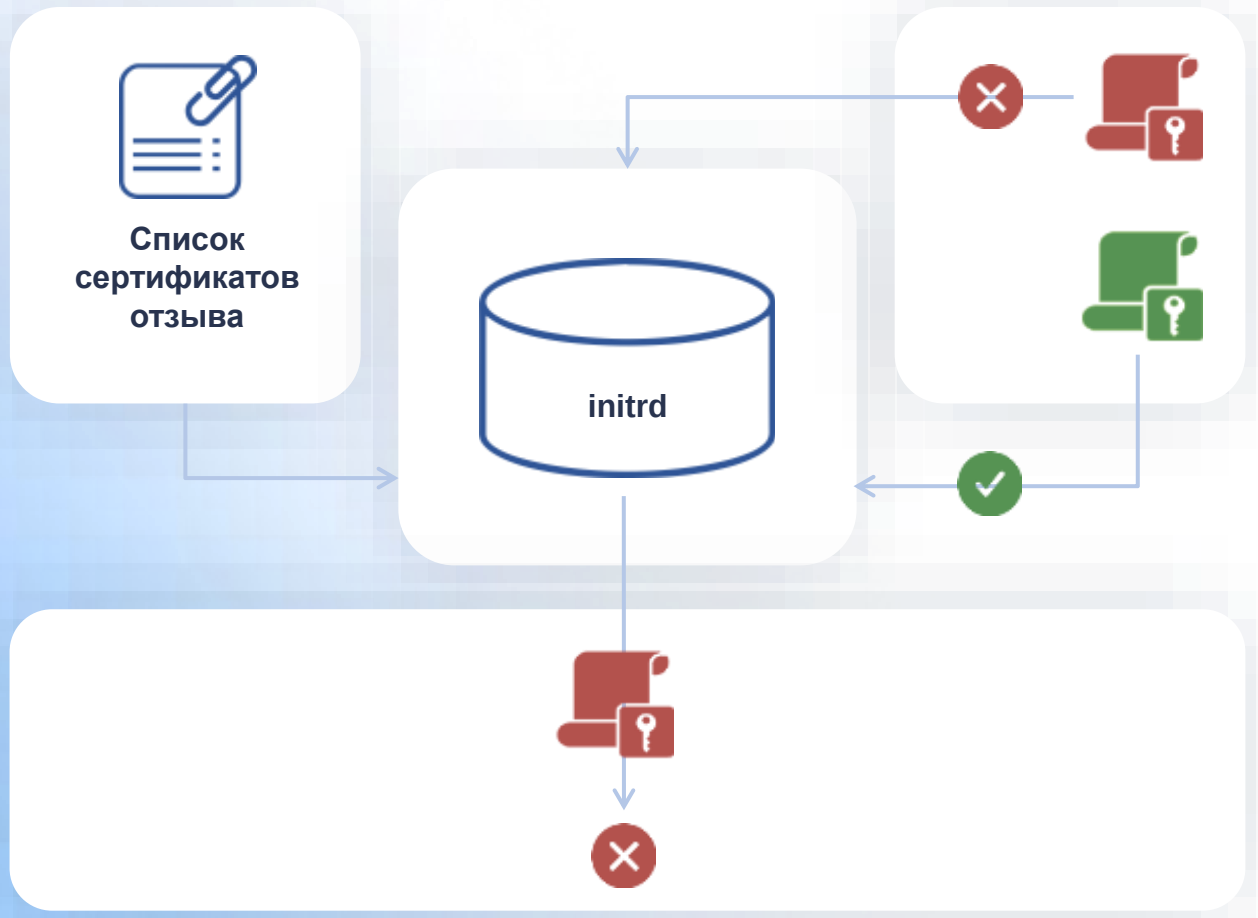


Универсальный режим проверки подписи

- Проверка первого найденного вида подписи.
- Открывает перспективу контроля не только исполняемых файлов, но и интерпретируемого кода.
- Для этого на стороне интерпретатора должен быть реализован системный вызов mmap() в момент запуска интерпретируемого файла.
- Уже есть успешный кейс с Axiom JDK. Планируем развиваться в этом направлении.



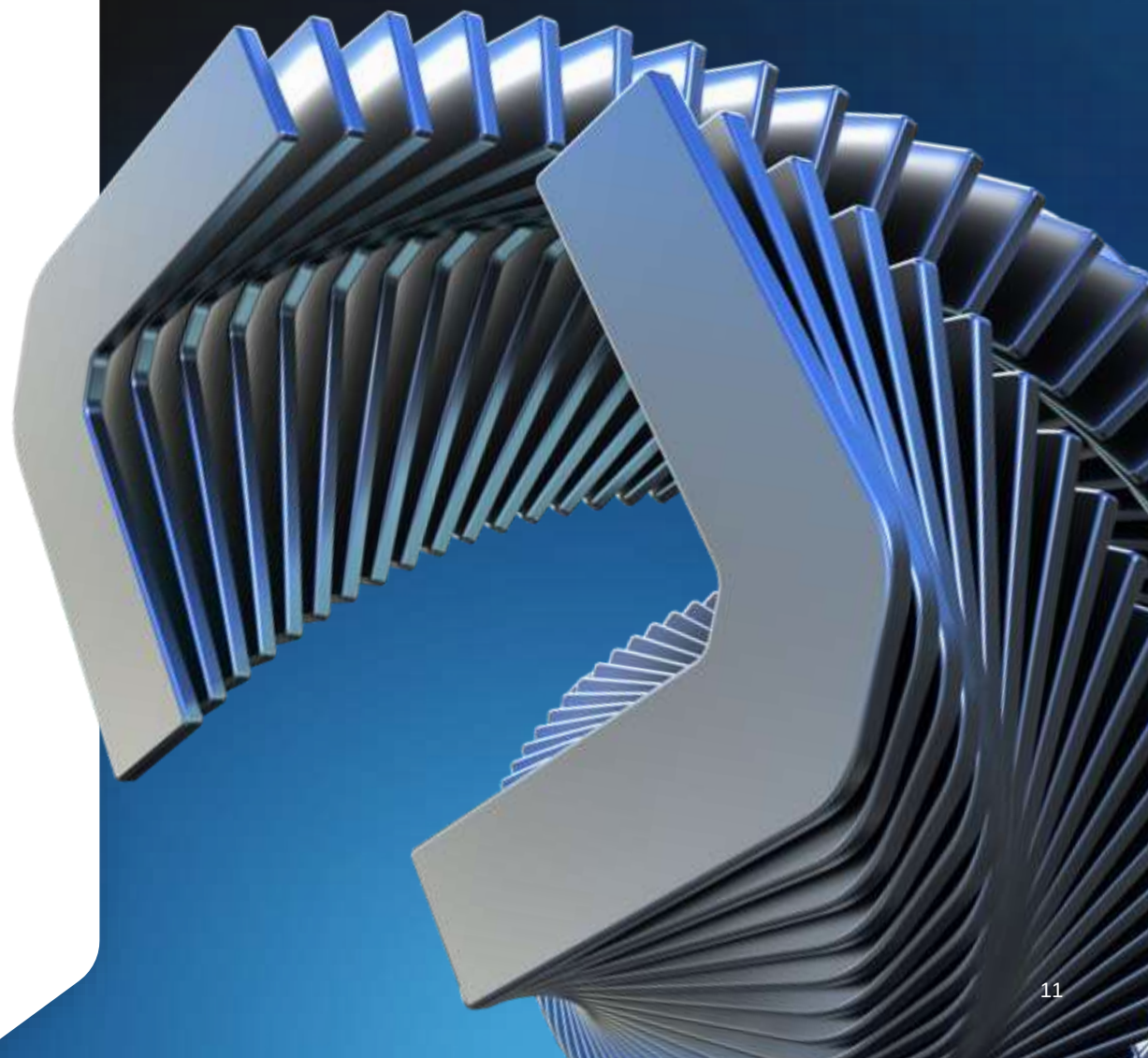
Механизм отзыва сертификатов



- Механизм реализует возможность исключения скомпрометированных сертификатов из проверок всех видов подписей в замкнутой программной среде.
- В user-space, при этом, организуется "чёрный список", запрещающий последующую загрузку любого из сертификатов, расположенных в данном списке.
- Список представляет собой набор значений SHA1, рассчитанных от gpg-сертификатов ключей проверки цифровой подписи.

Что дальше?

- Расширение границ контролируемых в замкнутой программной среде объектов доступа.
- Готовы к интеграциям с криптографическими провайдерами для организации взаимодействия с удостоверяющими центрами и последующего использования квалифицированных сертификатов цифровой подписи в замкнутой программной среде.
- Всегда открыты к тестированию наших компонентов защиты. Принимаем и будем принимать активное участие на площадках по поиску уязвимостей и независимому исследованию безопасности.



АСТРА

Спасибо!

Так же подписывайтесь на наши обновления:

ASTRA LINUX®