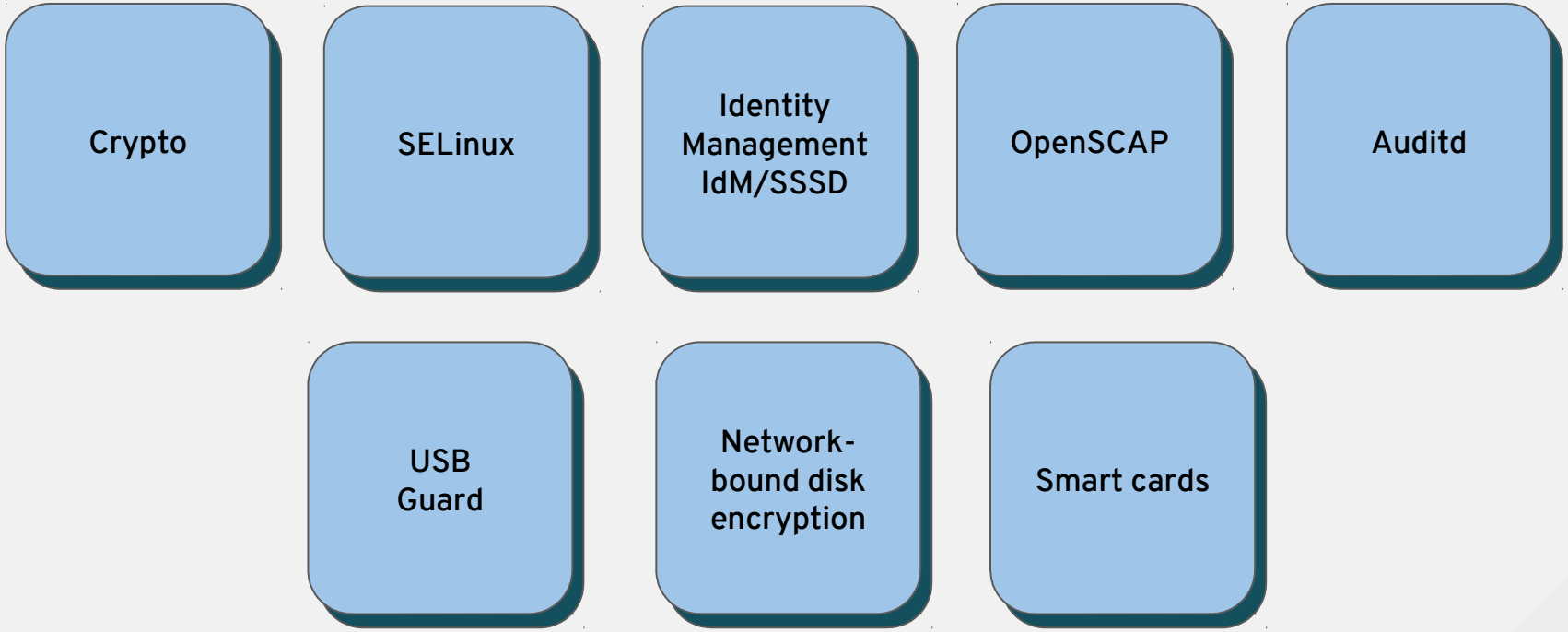
Новости безопасности
Red Hat Enterprise Linux 7.4

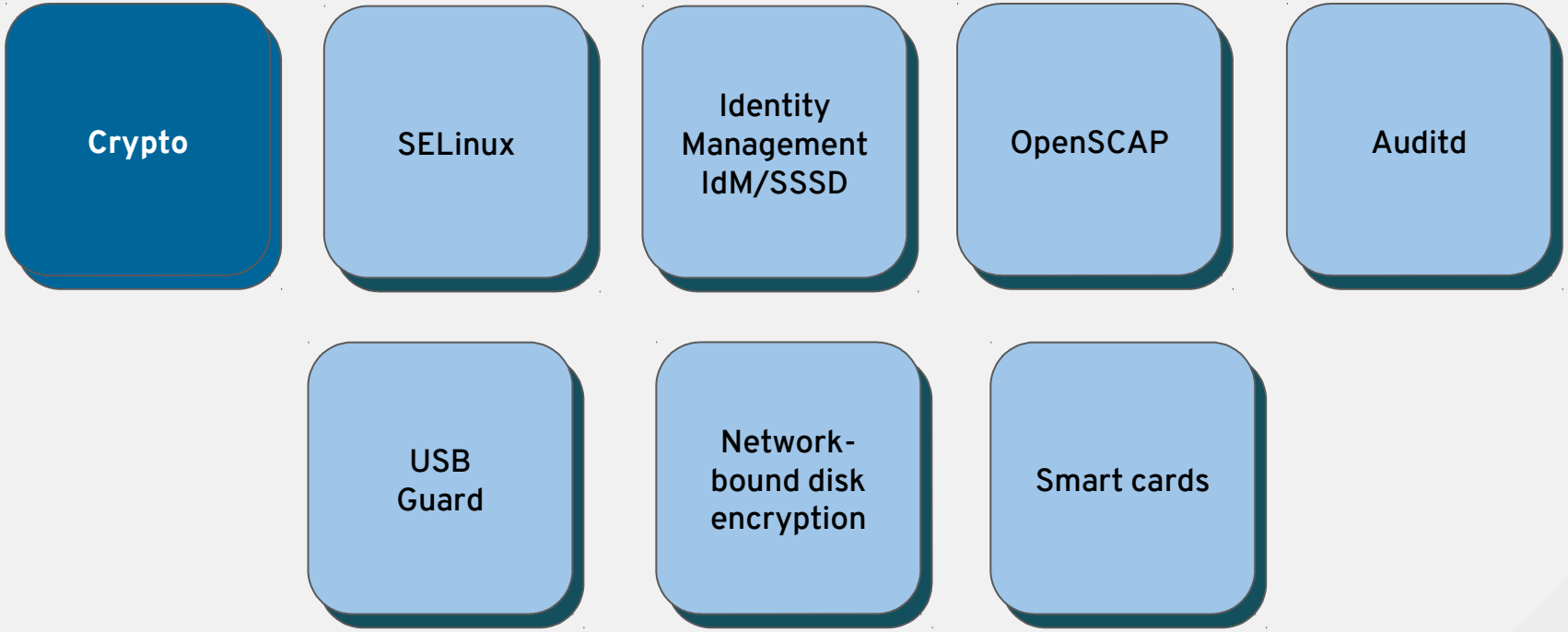
Red Hat Forum Moscow 2017

Alexander Bokovoy
Sr. Principal Software Engineer
22.09.2017

Security Technologies



Security Technologies



Crypto Technologies

Обзор

- Криптоалгоритмы и протоколы
  - Вывод из обращения SSH 1.0, SSL 2.0
  - Поддержка SHA-256
- getrandom()
- Криптоинфраструктура для Python

Crypto Technologies

Криптоалгоритмы и протоколы

- Вывод из обращения
  - Протокол SSH 1.0 убран из сервера OpenSSH
    - Поддержка в клиенте OpenSSH оставлена, но по умолчанию выключена
  - Протокол SSL 2.0 убран из GnuTLS, NSS и OpenSSL
  - Протокол обмена Диффи-Хеллмана в TLS по умолчанию поддерживает только варианты с 1024 бит или больше (вплоть до 8192)
  - Поддержка MD5, MD4 и SHA-0 по умолчанию отключена в OpenSSL
  - Поддержка RC4 по умолчанию отключена в OpenSSH

Crypto Technologies

Криптоалгоритмы и протоколы

- Обновление SHA
  - Все криптоутилиты по умолчанию переведены на использование SHA-256
  - В OpenSSH добавлена поддержка SHA-256
- OpenSSL 1.0.2k
  - Поддержка DTLS (датаграммы TLS 1.2)
  - Автоматический выбор эллиптических кривых в TLS
  - Поддержка application-level protocol negotiation
  - Поддержка Cryptographic Message Syntax: RSA-PSS, RSA-OAEP, ECDH, X9.42 DH

Crypto Technologies

Поддержка системного вызова getrandom

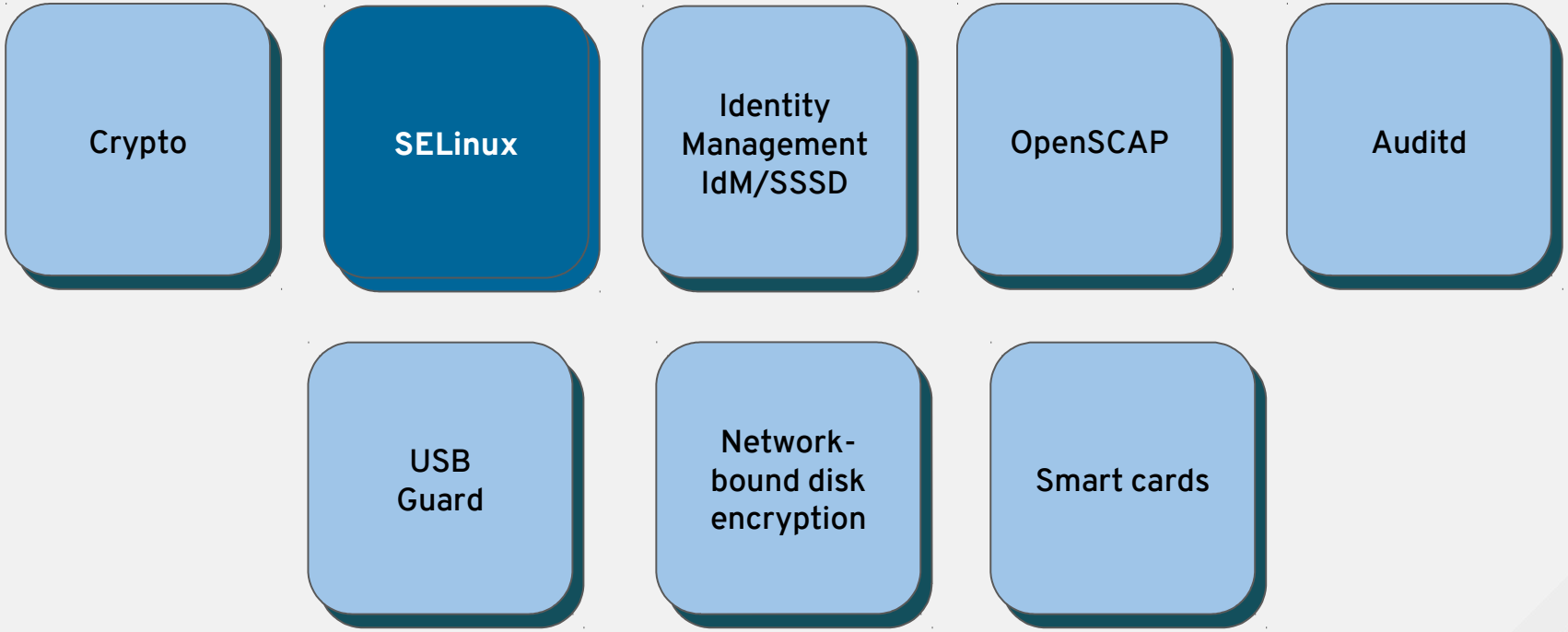
- В ядро RHEL 7.4 добавлена поддержка вызова getrandom(2)
  - Неблокирующий доступ к ядерному CPRNG в обычном режиме
  - В процессе ранней загрузки доступ блокируется до инициализации 128 бит энтропии
  - Лучшая комбинация /dev/random и /dev/urandom для приложений

Crypto Technologies

Криптоинфраструктура для Python

- Автоматическая проверка валидности сертификатов
  - **urllib, httplib, xmlrpclib**
  - Общесистемный источник сертификатов
    - **/etc/pki/ca-trust**

Security Technologies

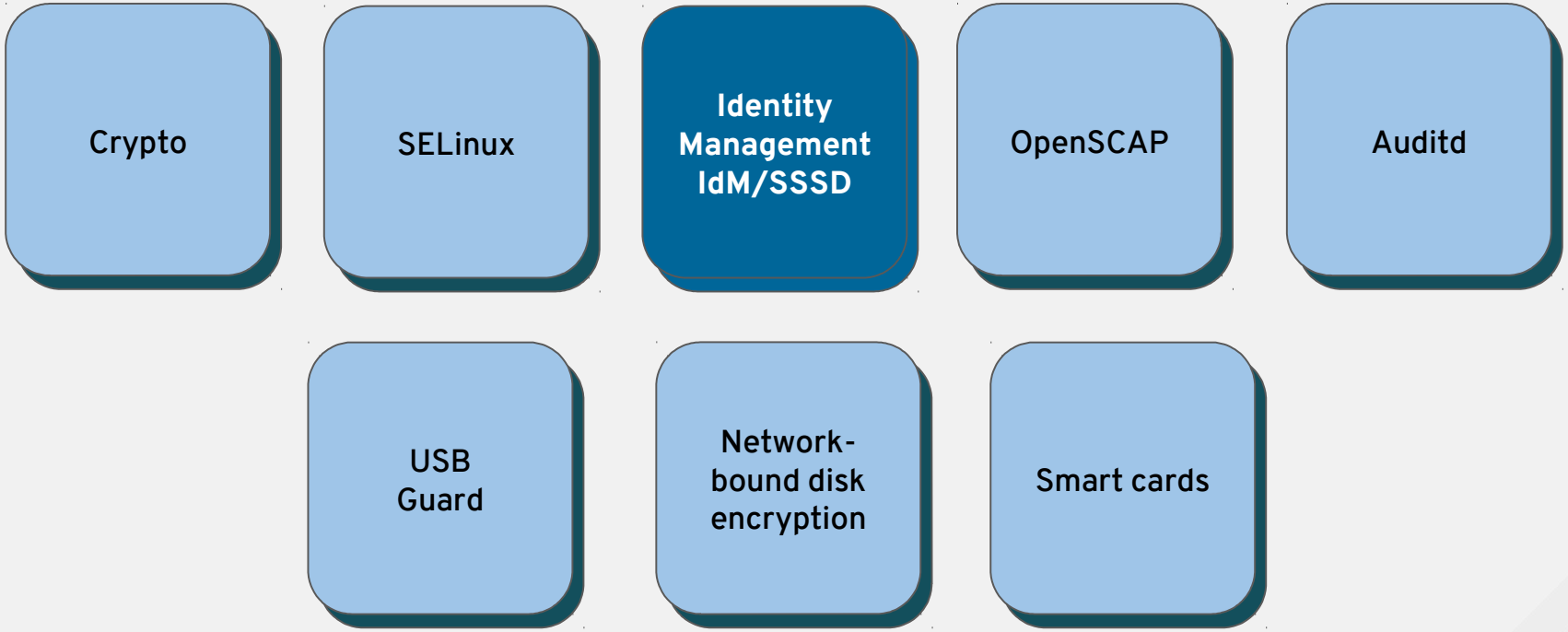


SELinux

Обзор

- Политики SELinux обновлены и поддерживают все новые классы и права, поддерживаемые в ядре RHEL 7.4
- Политики контейнеризации объединены в общий блок правил
  - container.te + docker.if → container.pp
- SELinux теперь поддерживает GFS2
- NFS и SELinux
  - Поддержка индивидуальных меток SELinux в NFS по умолчанию выключена
    - Добавлена и по умолчанию включена в RHEL 7.3

Security Technologies



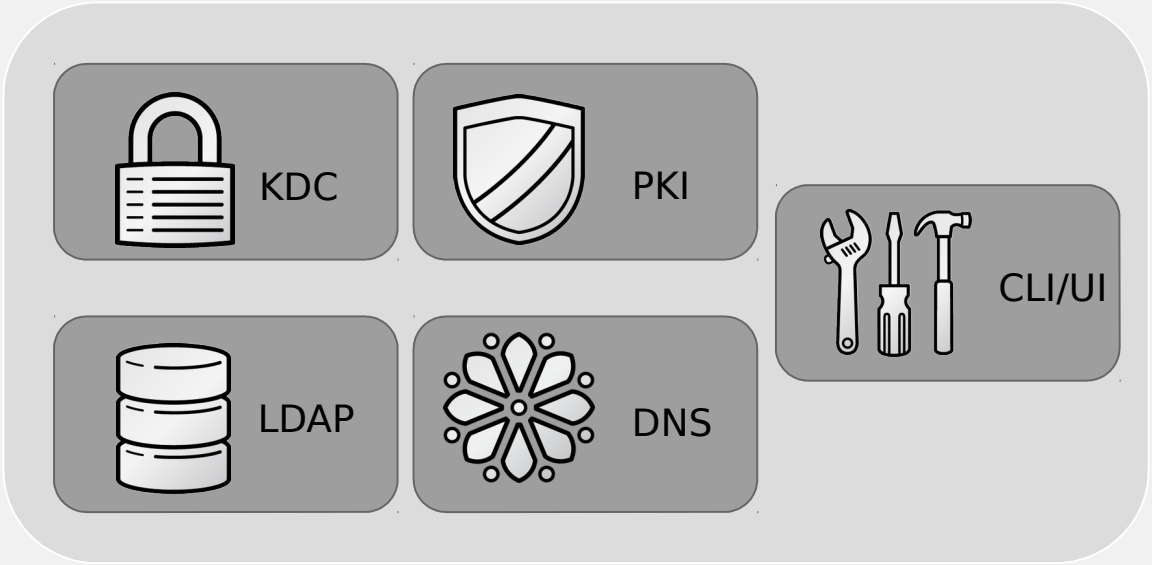
Identity Management

Обзор

- Информация о пользователях и групах
- Аутентификация и система единого входа (single sign-on) на основе Kerberos
- Централизованный контроль доступа к приложениям
- Централизованное управление политиками доступа sudo

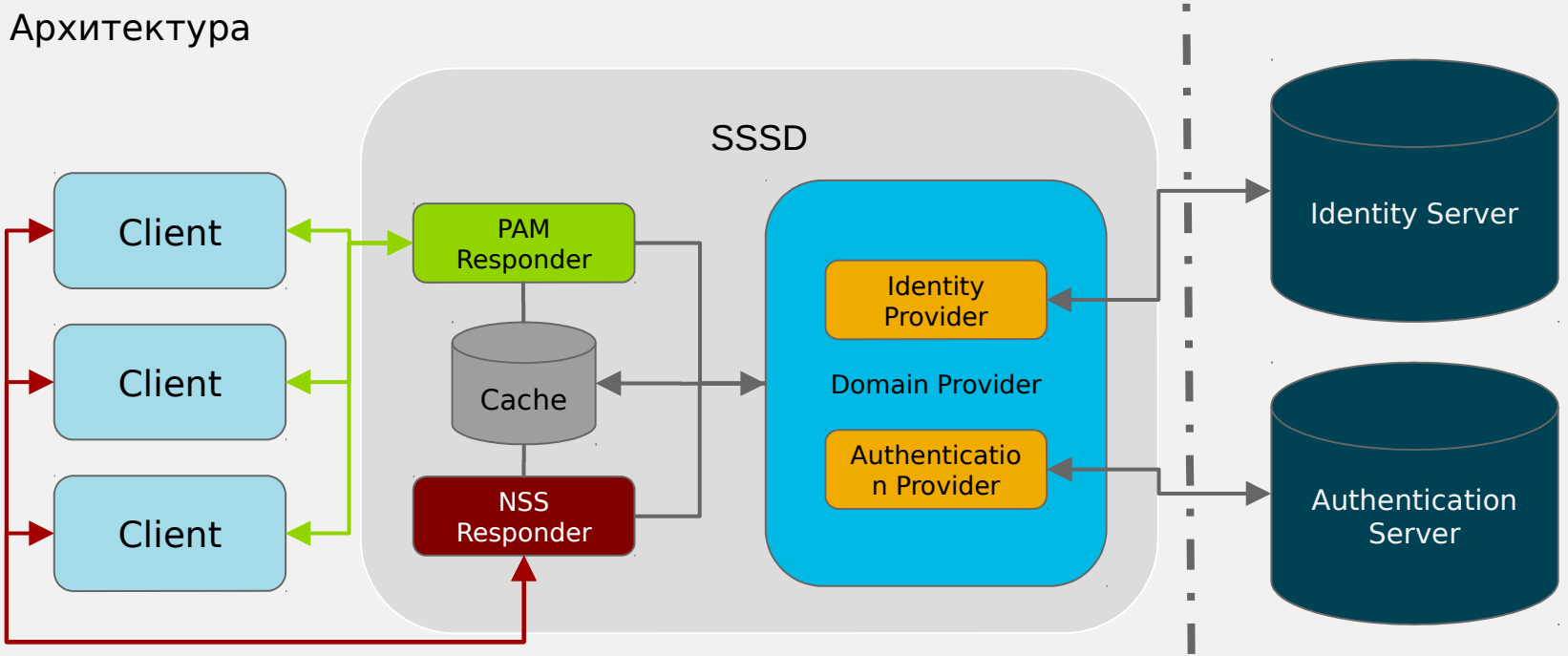
Identity Management - IdM

Architecture



SSSD

Архитектура

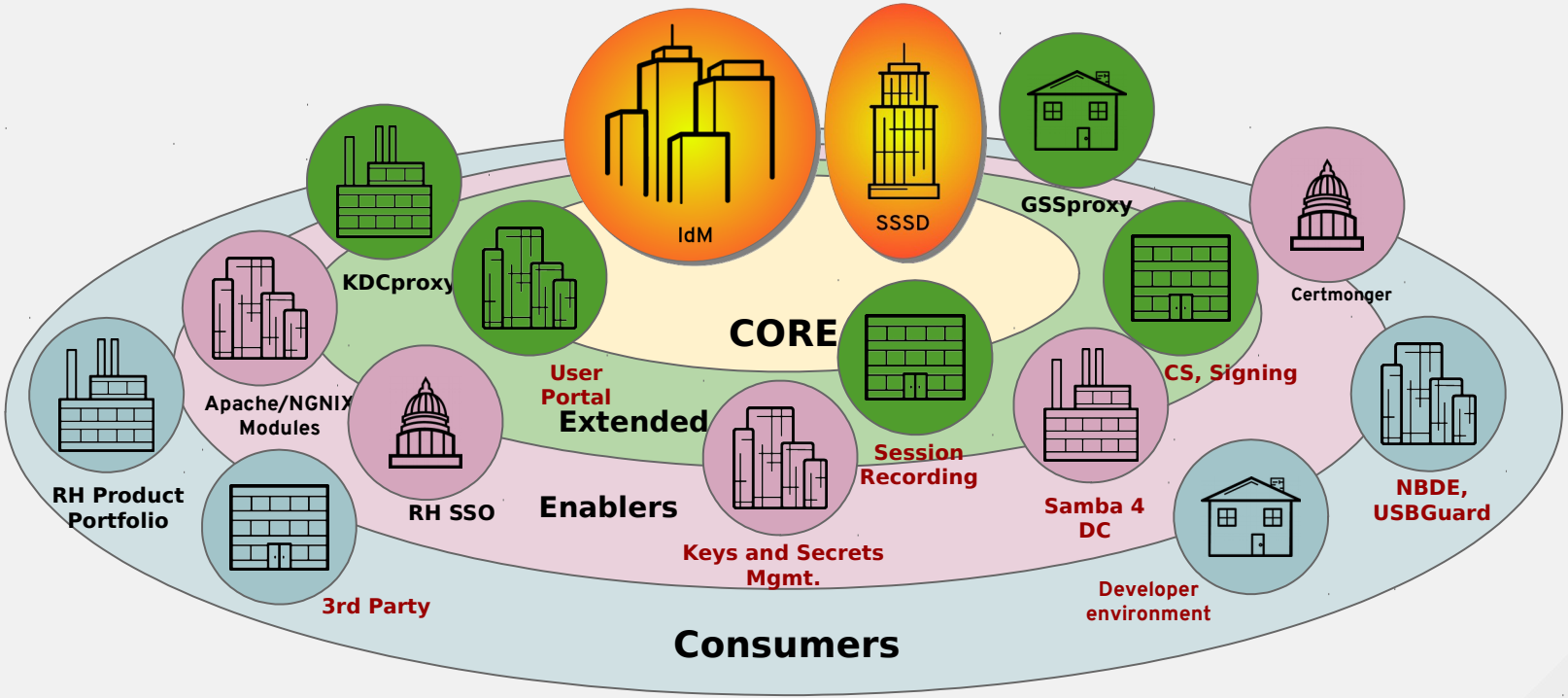


Identity Management

Возможности

- Клиенты RHEL и другие системы на основе POSIX
- Интеграция с Active Directory
- Host based access control, SUDO, Automount, Netgroups, POSIX, SELinux user mappings, SSH keys
- Выпуск сертификатов и депонирование ключей
- Многофакторная аутентификация
- Средства управления ресурсами для всего стека приложений, от системного до прикладного уровней

Identity Management Fabric



Identity Management

Новое в 7.4

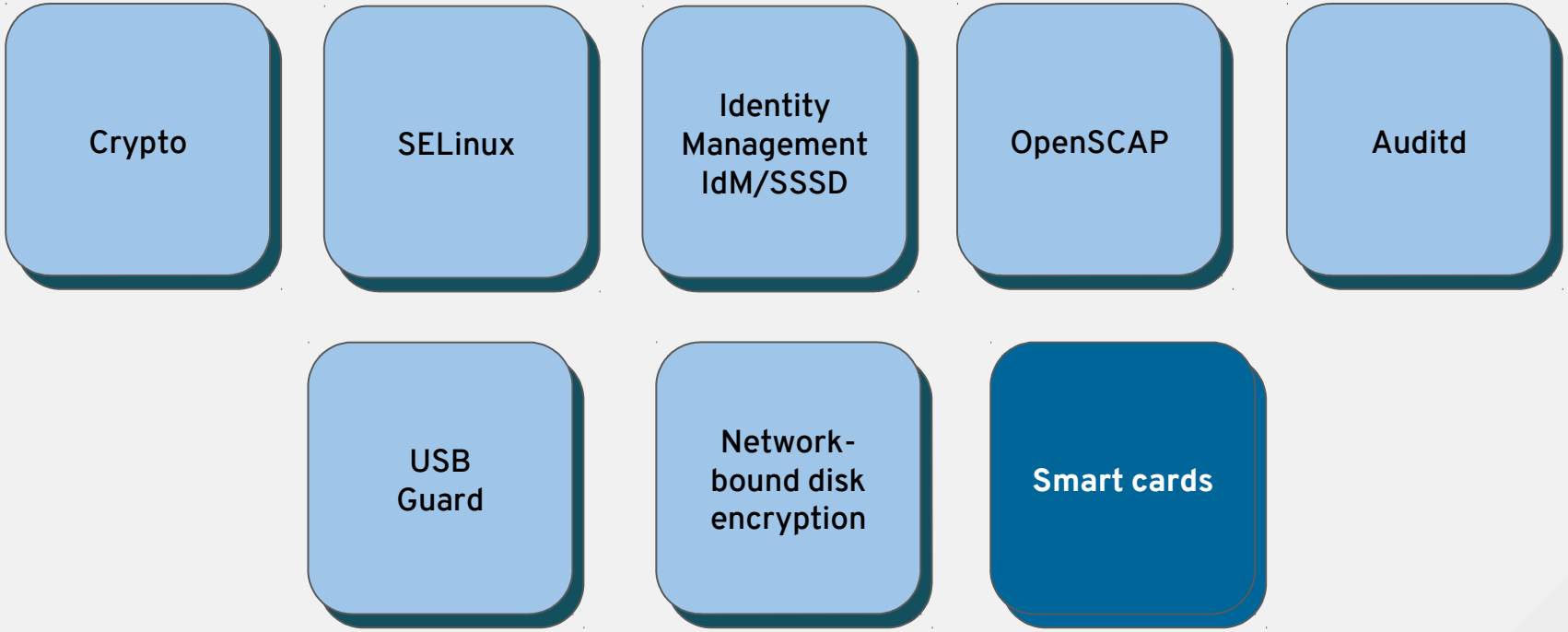
- RHEL Identity Management обновлена до версии FreeIPA 4.5
- Поддержка смарткарт
- Поддержка установки Identity Management в режиме FIPS
- Поддержка контейнерных образов rhel7/ipa-server и rhel7/sssd
- DNSSEC (technology preview)
- Поддержка API FreeIPA (technology preview)

Identity Management

Поддержка смарткарт

- Kerberos PKINIT
- Авторизация по смарткарте в консоли управления Identity Management
- Поддержка авторизации по смарткарте в SSSD
  - Автоматическое получение билетов Kerberos
  - Локальная авторизация
  - Интеграция с GNOME
- Развитые правила авторизации сертификатов при использовании смарткарт
- Поддержка пользовательских ролей с одним и тем же сертификатом

Security Technologies

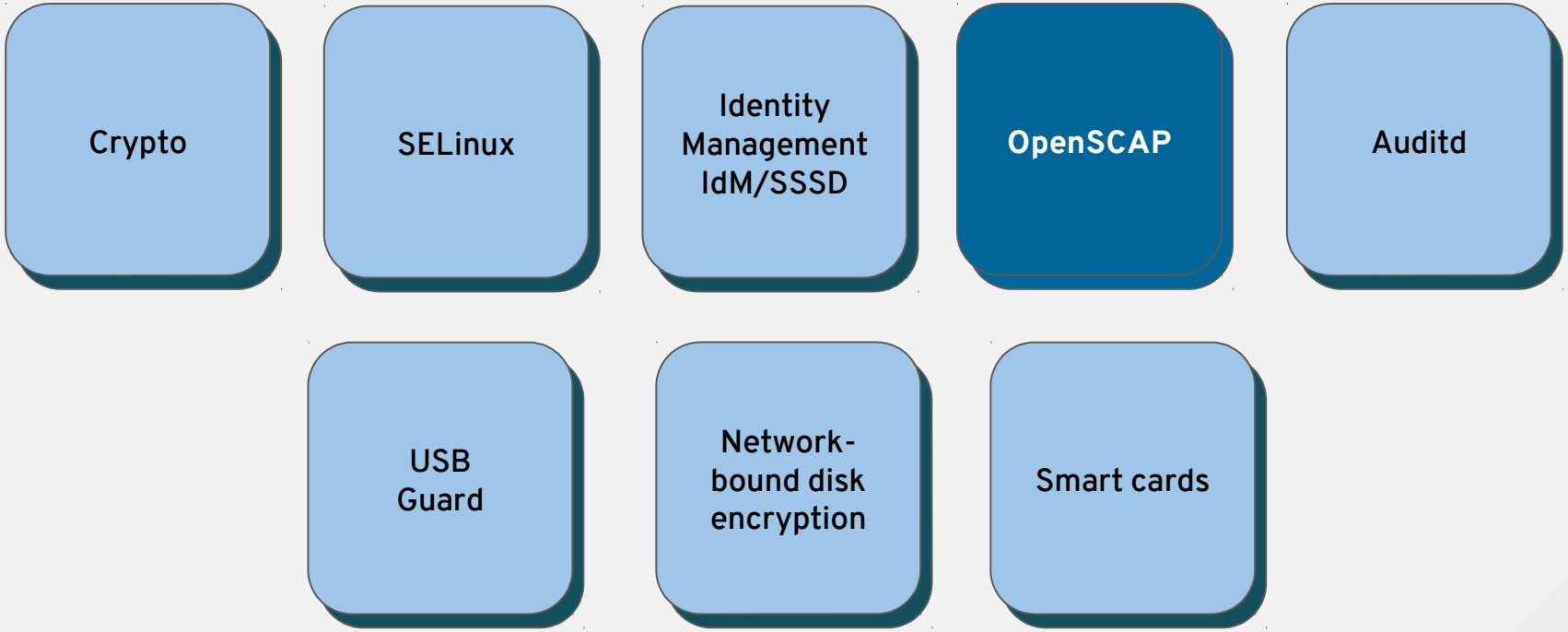


OpenSC

Поддержка смарткарт

- OpenSC обновлена до версии 0.16.0
  - Поддержка Common Access Card (CAC)
  - Реализация PKCS#11 API
  - Апплет Coolkey для замены пакетов coolkey
- Поддержка более широкого спектра оборудования

Security Technologies



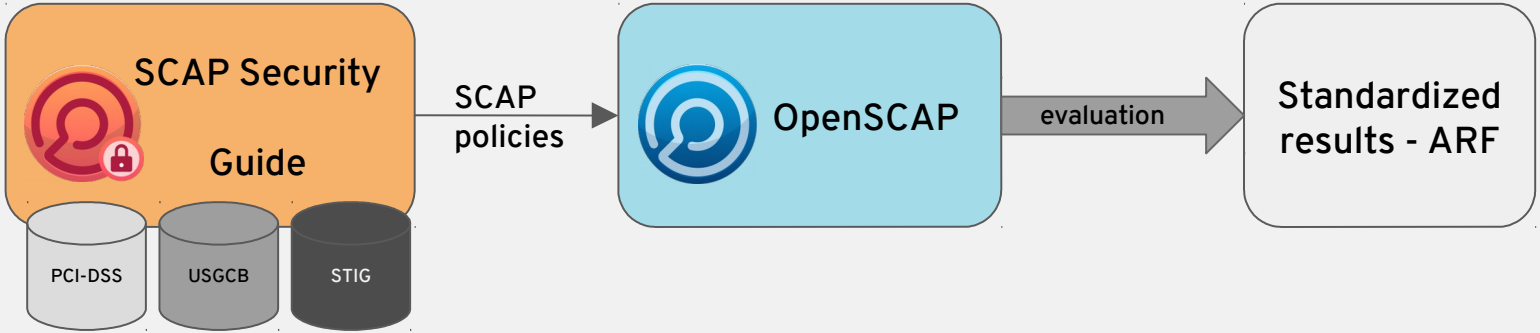
OpenSCAP

Обзор

- Сканирование систем и контейнеров:
  - Поиск известных уязвимостей
  - Соответствие политикам безопасности
- Версия OpenSCAP 1.2 получила сертификат NIST
  - Может применяться для выяснения соответствия политикам безопасности в государственных органах (США)

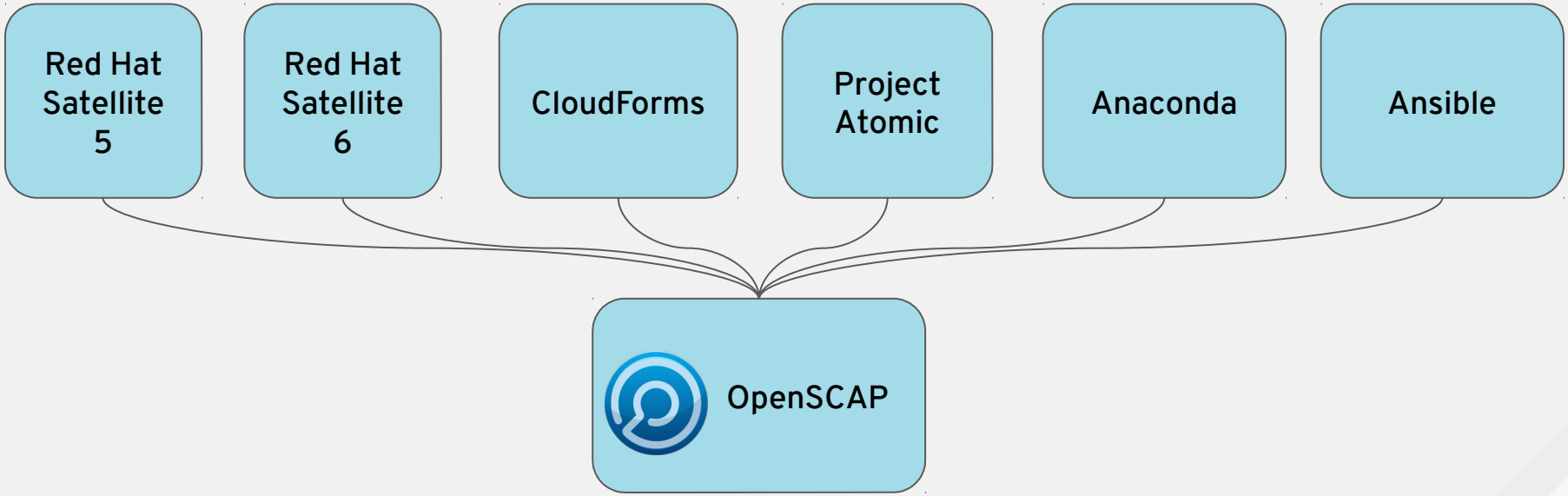
OpenSCAP

Архитектура

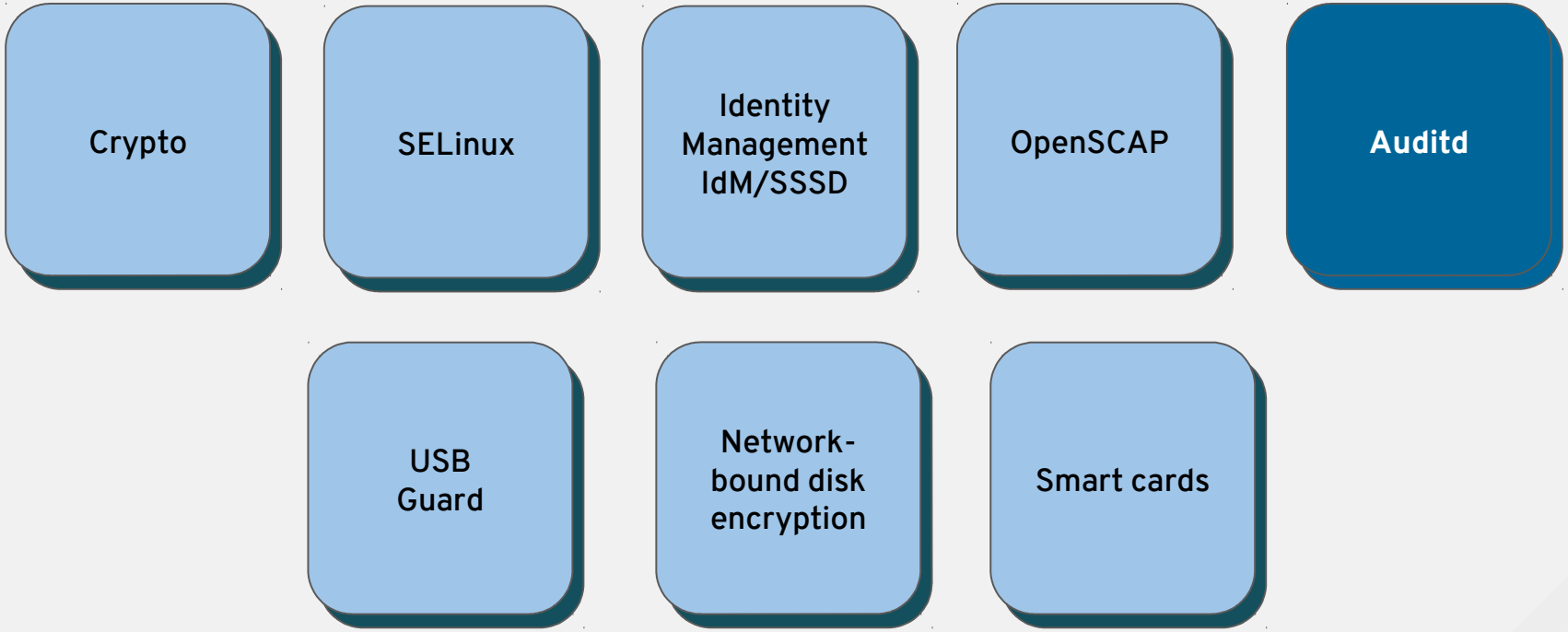


OpenSCAP

Интеграция



Security Technologies

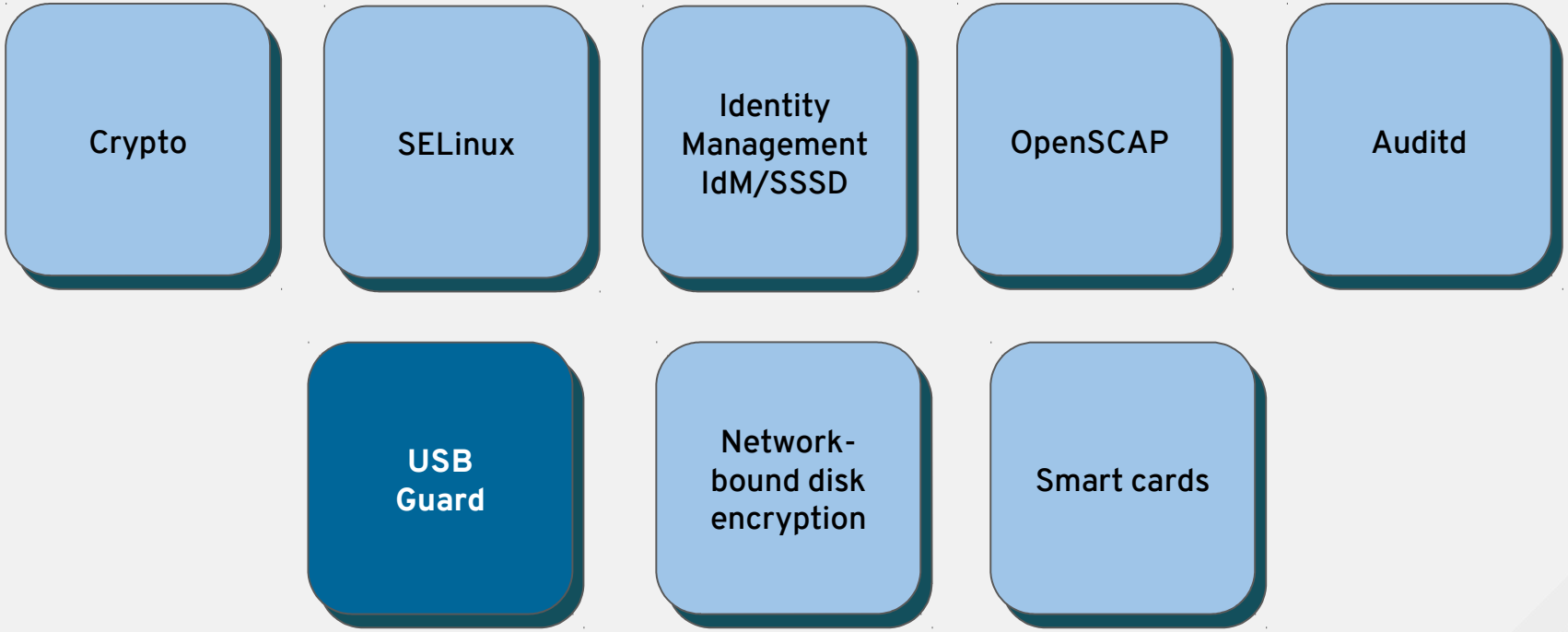


Auditd

Обзор

- Обновление версии 2.7.6
- Аудит низкоуровневых операций ядра и системных служб
  - AUDIT_KERN_MODULE – аудит загрузки и выгрузки модулей ядра
  - AUDIT_NETFILTER_PKT – улучшено представление пакетов в журнале
- Добавлены новые поля для фильтрации журнала аудита
- Экспорт данных из журнала в машиночитаемый формат (CSV)

Security Technologies

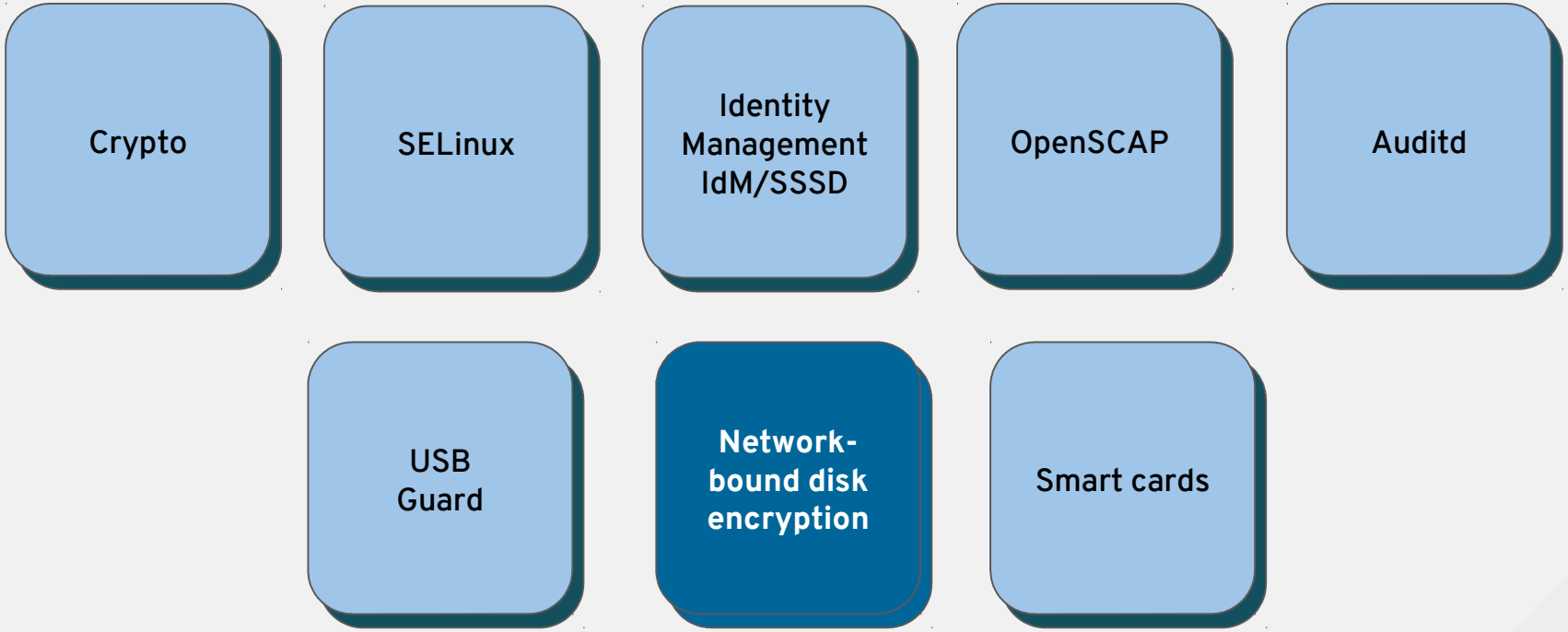


USB Guard

Обзор

- Блокирование USB устройств на основе информации о них
  - Управление классами устройств
  - Автоматическое исполнение сценариев по правилам

Security Technologies



Network-bound disk encryption

Обзор

- Проекты clevis/tang
- Привязка ключей шифрования к сетевому источнику
- Развитая политика условий разблокирования
- Интеграция с LUKS
  - Шифрование root и загрузка
- Интеграция с GNOME
  - Шифрование внешних устройств

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos