

Интеграция защищённой операционной системы QR ОС в доменную инфраструктуру

Докладчик: Баринов А. Д.



Преимущества доменной инфраструктуры

- Централизованное управление учетными записями
- Единая точка аутентификации
- Единая точка управления политиками
- Повышенный уровень информационной безопасности

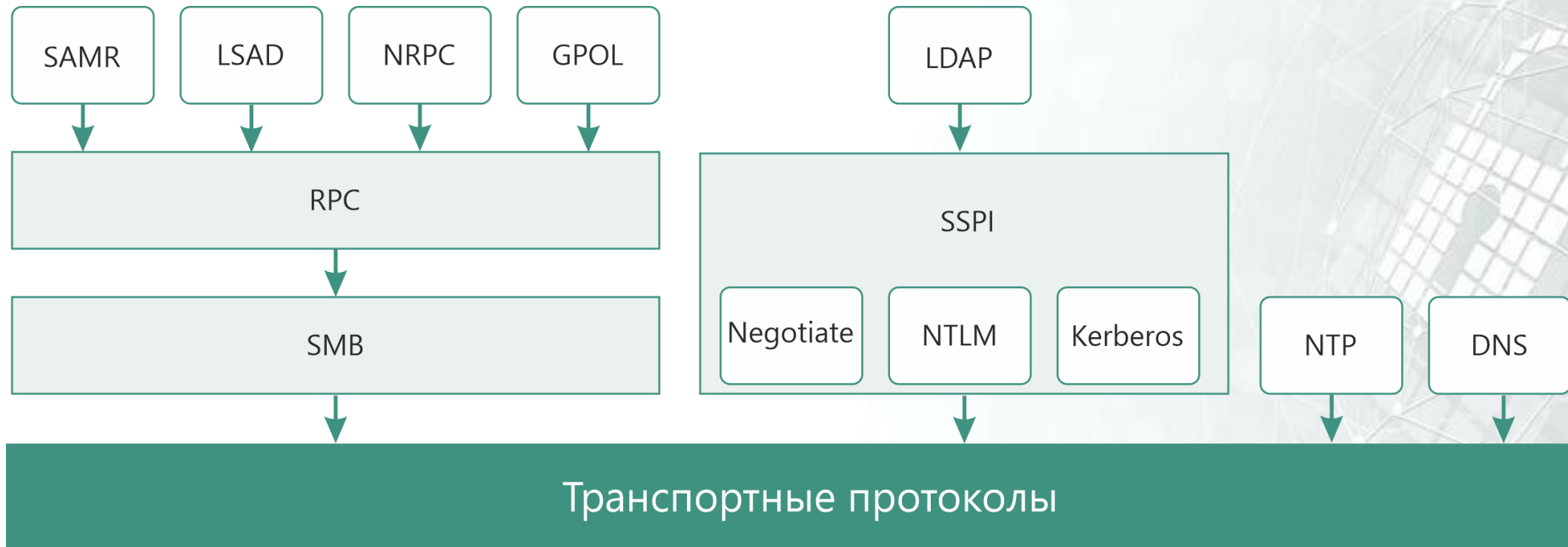


Требования для интеграции в домен

- В операционной системе рабочей станции должны быть установлены соответствующие **компоненты**
- У машины должен быть сконфигурирован **сетевой интерфейс**, через который будет выполняться доступ к КД
- **Межсетевой экран** должен быть настроен таким образом, чтобы сетевые пакеты протоколов, используемых для работы в домене не блокировались
- Время рабочей станции должно быть **синхронизировано** с КД



Протоколы взаимодействия с доменом



Протоколы аутентификации

Kerberos и NTLM:

- Интерактивный вход доменным пользователем
- Сетевой вход доменным пользователем
- Смена пароля доменного пользователя
- Обеспечение целостности и конфиденциальности
- Поддержка SSPИ



Реализация протокола Kerberos в QP ОС

Статическая библиотека:

- Разбор и построение пакетов протокола (AS, TGS, AP, PRIV, CRED, ERROR)
- Шифрование и подсчёт контрольных сумм

Динамическая библиотека:

- » Интерактивный вход доменного пользователя в систему
- » Генерация запроса аутентификации к серверу приложения с предварительной аутентификацией на КД и получением служебного билета
- » Смена пароля доменного пользователя

Динамическая библиотека поставщика поддержки безопасности:

- Согласование контекста безопасности
- Шифрование, дешифрование, подпись и проверка подписи сообщений



Облегчённый протокол доступа к каталогам LDAP

Прототипы функций, экспортируемых динамической библиотекой реализации протокола LDAP в QP ОС, идентичны прототипам функций библиотеки Wldap32.dll

Сценарии использования протокола в QP ОС:

- Создание на КД аккаунта компьютера
- Изменение атрибутов доменных учётных записей
- Получение списка доменных групп и пользователей
- Получение места расположения групповых политик

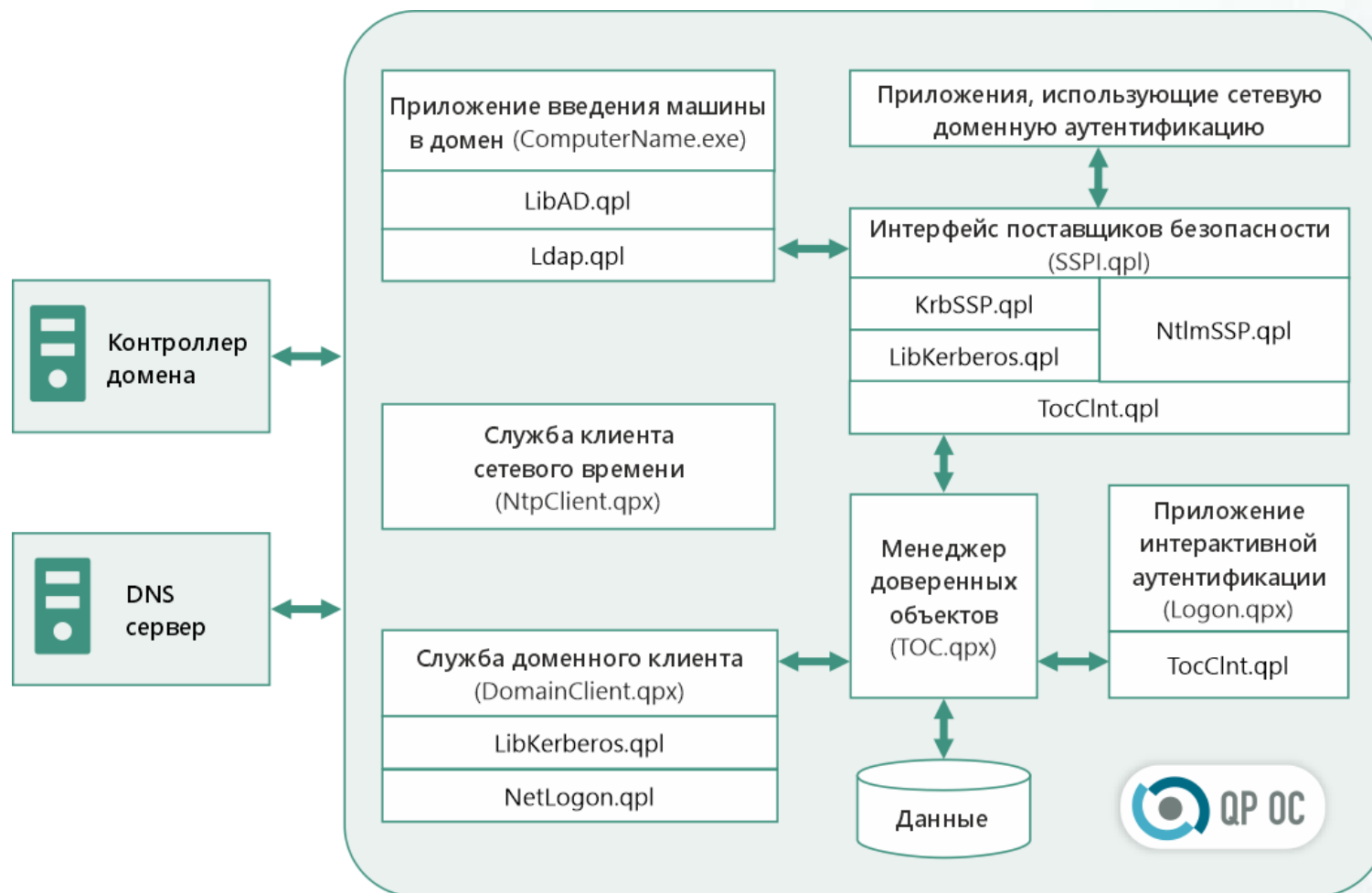


Другие протоколы

- Протокол дистанционного **диспетчера учётных записей безопасности SAMR**
- Дистанционный протокол **локального органа безопасности LSAR**
- Протокол сетевой **аутентификации Netlogon**
- Основной протокол **групповой политики GPO**
- Протокол **сетевого времени NTP**



Схема компонентов доменного взаимодействия QR ОС



Информационные потоки между узлами домена

- Потоки управления доменом
- Файловый обмен
- Web-трафик
- Трафик СУБД
- Потоки дистанционного управления доступом
- Почтовый обмен

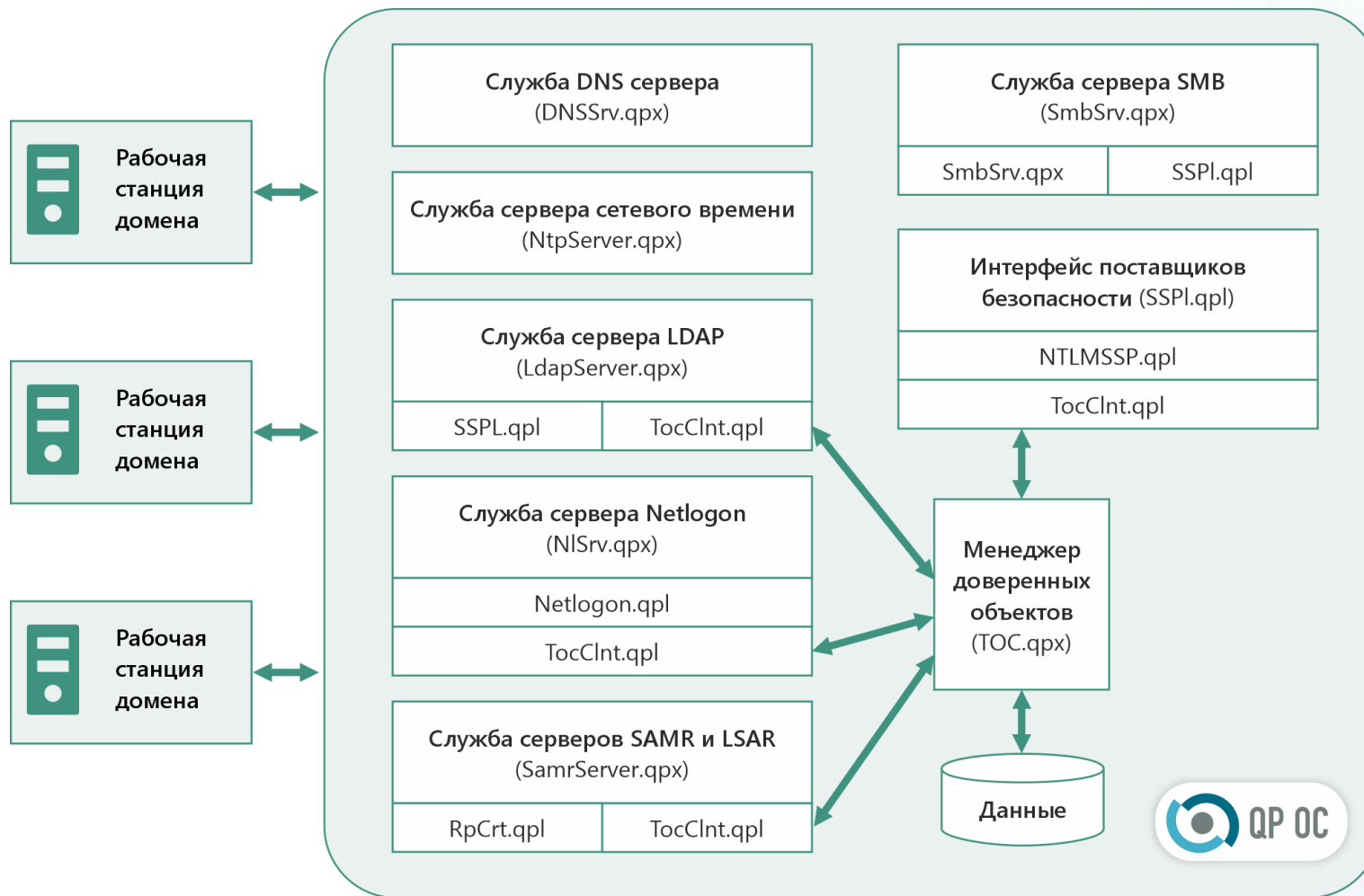


Роли контроллера домена под управлением QP ОС

- Роль сервера **облегчённого протокола доступа к каталогам LDAP**
- Роль сервера **службы доменных имён DNS**
- Роль сервера **сетевое времени NTP**
- Роль сервера **аутентификации Netlogon**
- Роль сервера дистанционного **диспетчера учётных записей безопасности SAMR**
- Роль сервера дистанционного протокола **локального органа безопасности LSAR**
- Роль сервера **дистанционного доступа к файлам SMB**



Схема модулей КД QR ОС



Процесс разработки

Сетевой монитор

Файл | Навигация | Захват | Инструменты

Фильтр отображаемых сетевых пакетов

Номер	Время	Источник	Получатель	Протокол	Размер	Информация
45	7.007751206	3.1.253.197	3.1.253.97	KRB5	1486	TGS-REP
46	7.007751274	3.1.253.97	3.1.253.197	TCP	54	1052 > 88 [ACK] Seq=1346 Ack=1433 Win=260608 ...
47	7.007751403	3.1.253.97	3.1.253.197	TCP	54	1052 > 88 [FIN, ACK] Seq=1346 Ack=1433 Win=262...
48	7.007751487	3.1.253.197	3.1.253.97	KRB5	60	
49	7.007751529	3.1.253.197	3.1.253.97	TCP	60	88 > 1052 [RST, ACK] Seq=1433 Ack=1347 Win=0 L...
50	7.007751804	3.1.253.97	3.1.253.197	SMB	1498	Session Setup AndX Request
51	7.007752316	3.1.253.197	3.1.253.97	SMB	441	Session Setup AndX Response

Security Blob: 6082054a06062b0601050502a082053e3082053aa00d300b06092a864886f712

GSS-API Generic Security Service Application Program Interface
OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)

Simple Protected Negotiation

negTokenInit:

- mechTypes: 1 item
- Padding: 1
- reqFlags: 16 (sequenceFlag, confFlag, integFlag)
- mechToken: 60840000051706092a864886f71201020201006e82050630820502a003020105
- krb5_blob: 60840000051706092a864886f71201020201006e82050630820502a003020105
 - KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
 - krb5_tok_id: KRB5_AP_REQ (0x1)
- Kerberos AP-REQ

Native OS: QpOS

000000560 03 1F 41 79 3E 3C 85 FC B7 2E A8 36 4F 15 E0 4F ..Ay><???.?60.?0
000000570 3F 94 3B 73 AC AD 90 90 42 4A 1B 90 69 34 E7 C9 ?.;s???.BJ..i4??
000000580 C7 22 88 6F 70 F8 FF 4D 3C 91 69 48 C1 19 8B 37 ?".op??M<.iH?..7
000000590 21 CF 37 F4 DE 12 6D 7C 35 55 7C C4 C3 AA DD C9 !????.m|5U|?????
0000005A0 1B 48 95 F7 A9 27 A3 2A A2 B8 4D 32 E8 51 FF BF .H.???'*??M2?Q??

Управление пользователями

Управление

Пользователи

- Admin
- InitialInstaller
- Группы
 - Администраторы
 - Гости
 - Опытные пользователи
 - Пользователи
 - Читатели журнала событий
- Доменные пользователи
 - ad
 - Admin
 - Dima
 - krbtgt
 - TestUser1
 - TestUser10
 - TestUser11
 - TestUser12
 - TestUser13
 - TestUser14
 - TestUser15
 - TestUser16
 - TestUser17
 - TestUser18

Членство в группах

Группа	SID
i0u	S-1-5-21-1190752932-98976074-3591906684-2129
i2u	S-1-5-21-1190752932-98976074-3591906684-2130
Администраторы	S-1-5-32-544
Администраторы домена	S-1-5-21-1190752932-98976074-3591906684-512
Администраторы предприятия	S-1-5-21-1190752932-98976074-3591906684-519
Администраторы схемы	S-1-5-21-1190752932-98976074-3591906684-518
Без ВКС	S-1-5-21-1190752932-98976074-3591906684-3257
ВКС	S-1-5-21-1190752932-98976074-3591906684-3256
Владельцы-создатели групповой п...	S-1-5-21-1190752932-98976074-3591906684-520
Все	S-1-1-0
Подготовка контента	S-1-5-21-1190752932-98976074-3591906684-3258
Пользователи	S-1-5-32-545
Пользователи домена	S-1-5-21-1190752932-98976074-3591906684-513

Удалить | Добавить | Привилегии

Процесс тестирования

- Разработка нагрузочных и функциональных **тестов**
- Использование **статических анализаторов**
- Использование **опций компилятора** (RunTimeCheck /RTCsu, Buffer Security Check /GS)
- Профилирование использования **памяти**

Дальнейшее развитие

- Реализация **серверной службы билетов Kerberos**
- Реализация **доверительных отношений в доменах**
- Интеграция с **сервером обновлений** операционной системы QR ОС
- Автоматическое обновление **антивирусных баз** в рамках домена
- Интеграция с **СХД (системы хранения данных)**





Спасибо за внимание!

