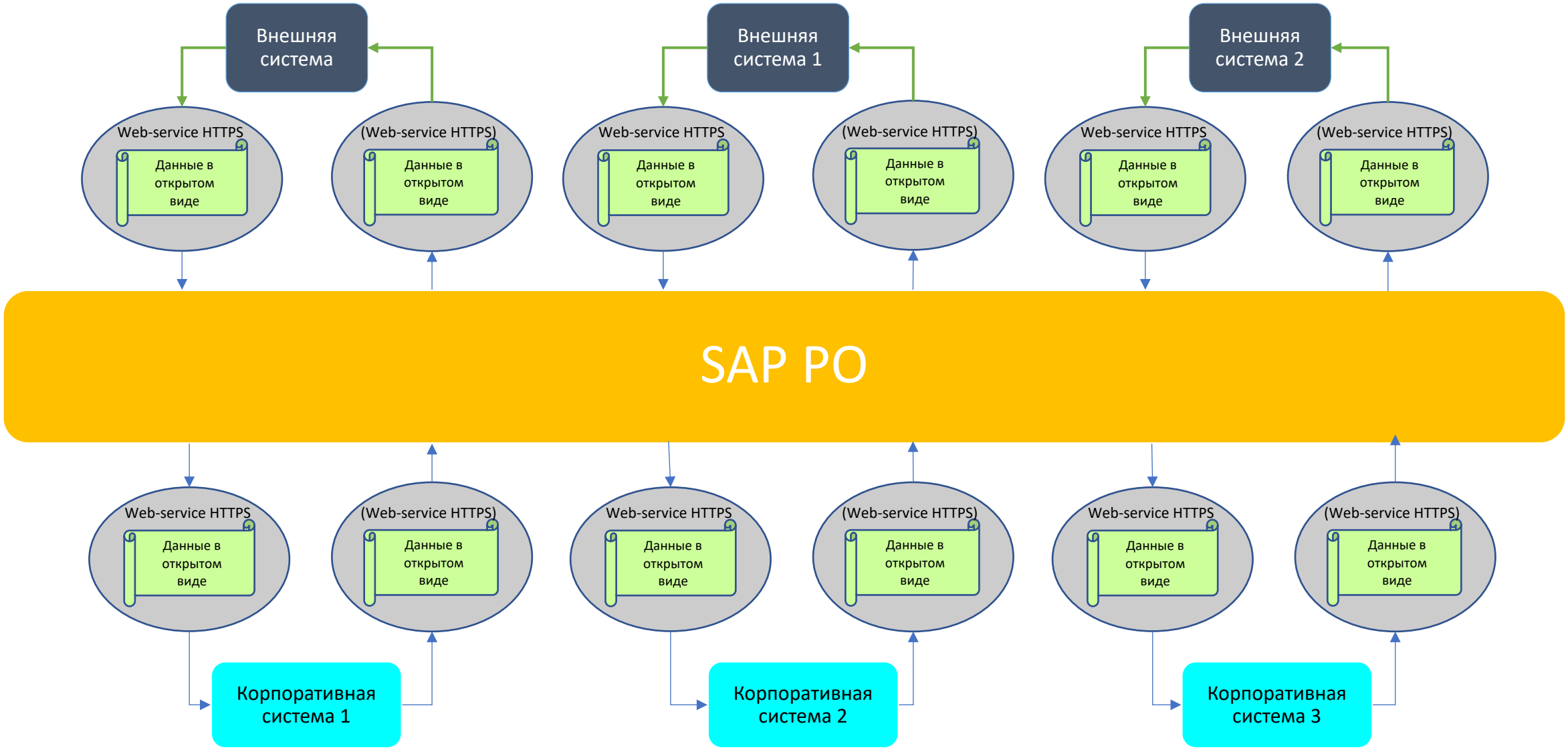
Разработка модуля работы с ГОСТ шифрованием на стороне интеграционной шины SAP PO

Текущая Архитектура решения



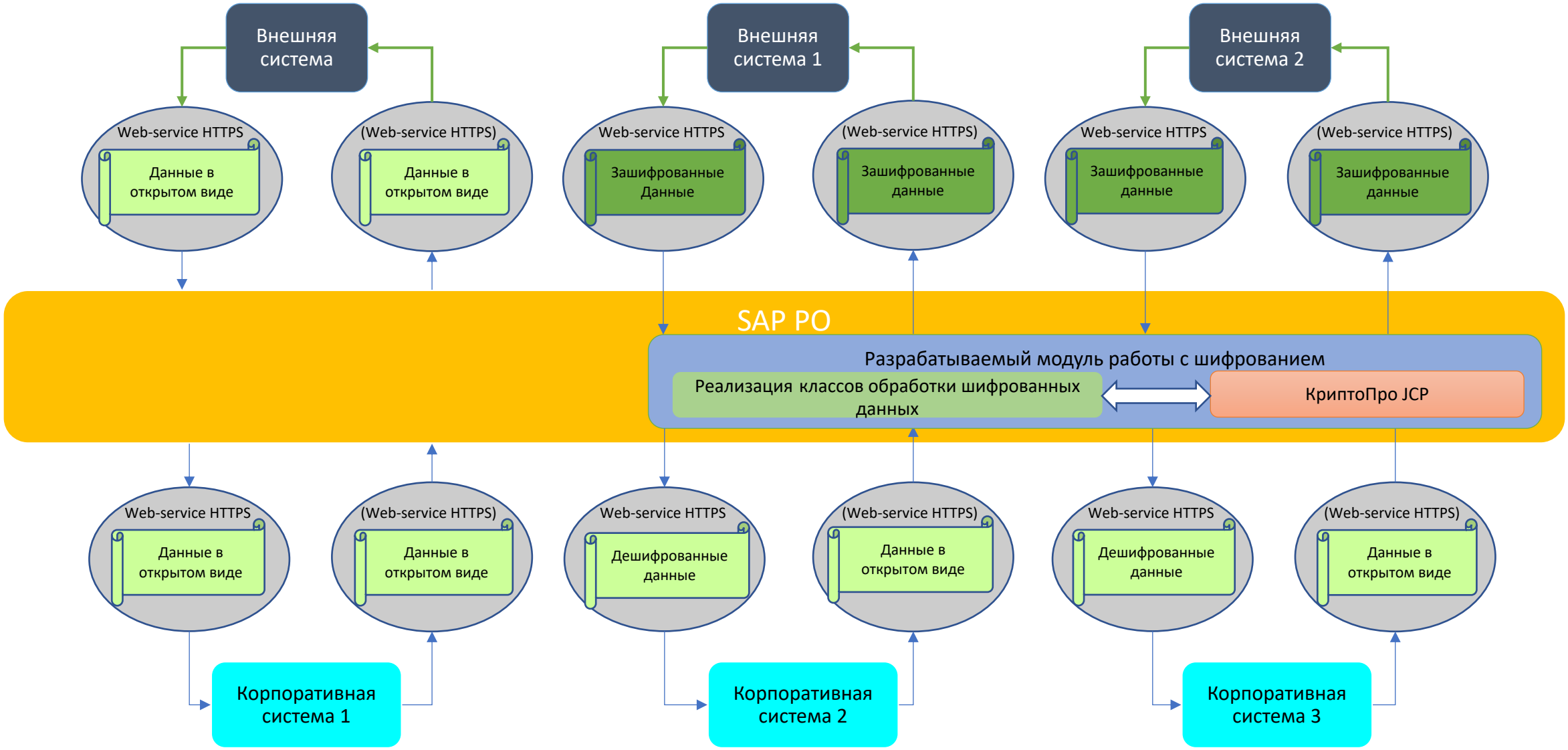
Постановка задач

- Выбор места применения модуля работы с шифрованием по ГОСТ в текущей архитектуре
- Проработка компонентов интеграции с шиной
- Реализация модуля работы с шифрованием с последующим встраиванием в workflow обработки данных

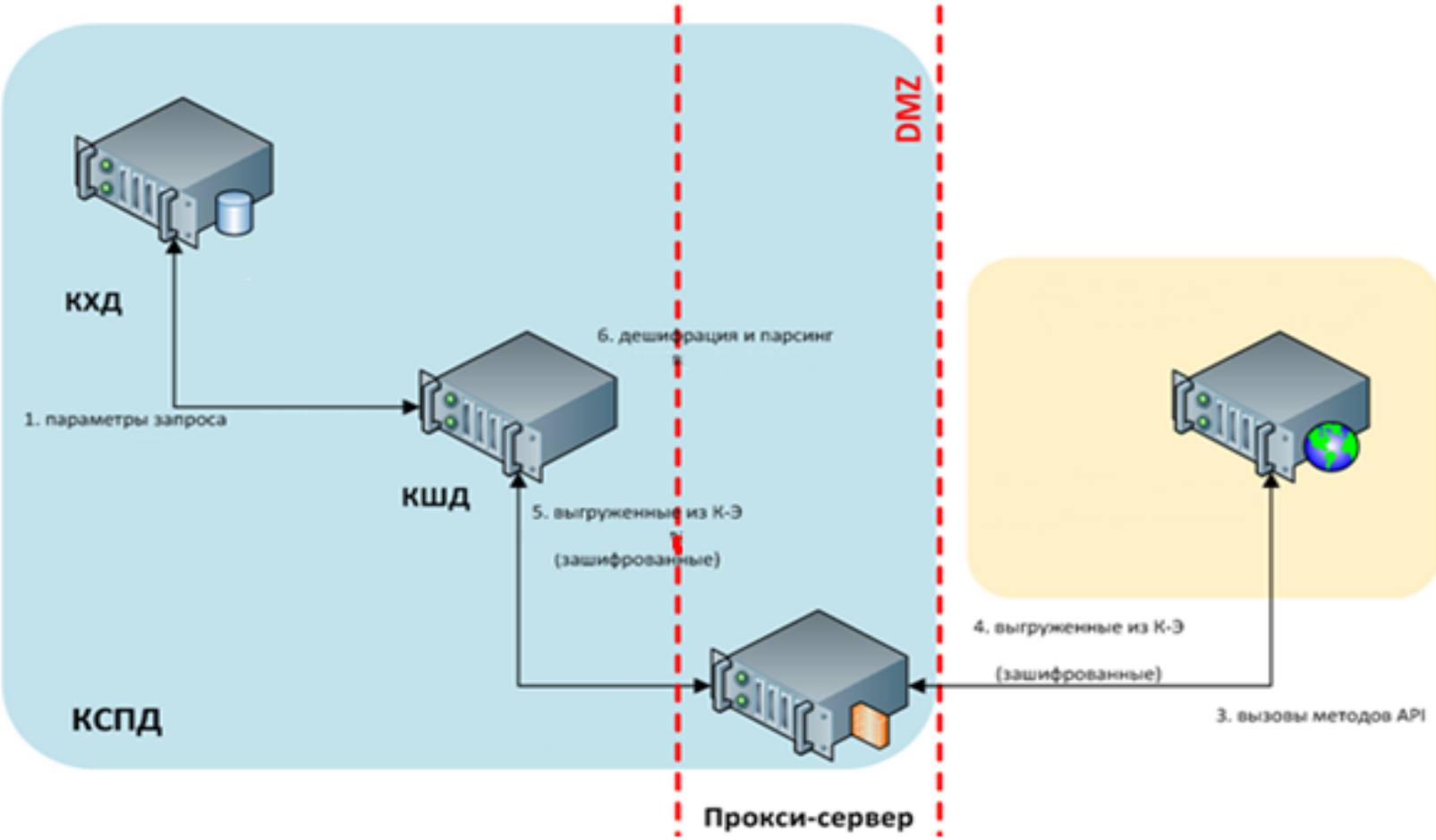
Предъявляемые требования

- В ходе работы требуется использовать существующую инфраструктуру/архитектуру интеграционной шины
- Необходимые компоненты должны инсталлироваться на интеграционную шину
- Для работы с ГОСТ криптографией требуется использовать сертифицированное Российское ПО (предпочтительно Крипто ПРО)
- Работа с шифрованными по ГОСТ 28147-89 данными, а так же с ЭЦП по ГОСТ 34.10-2001

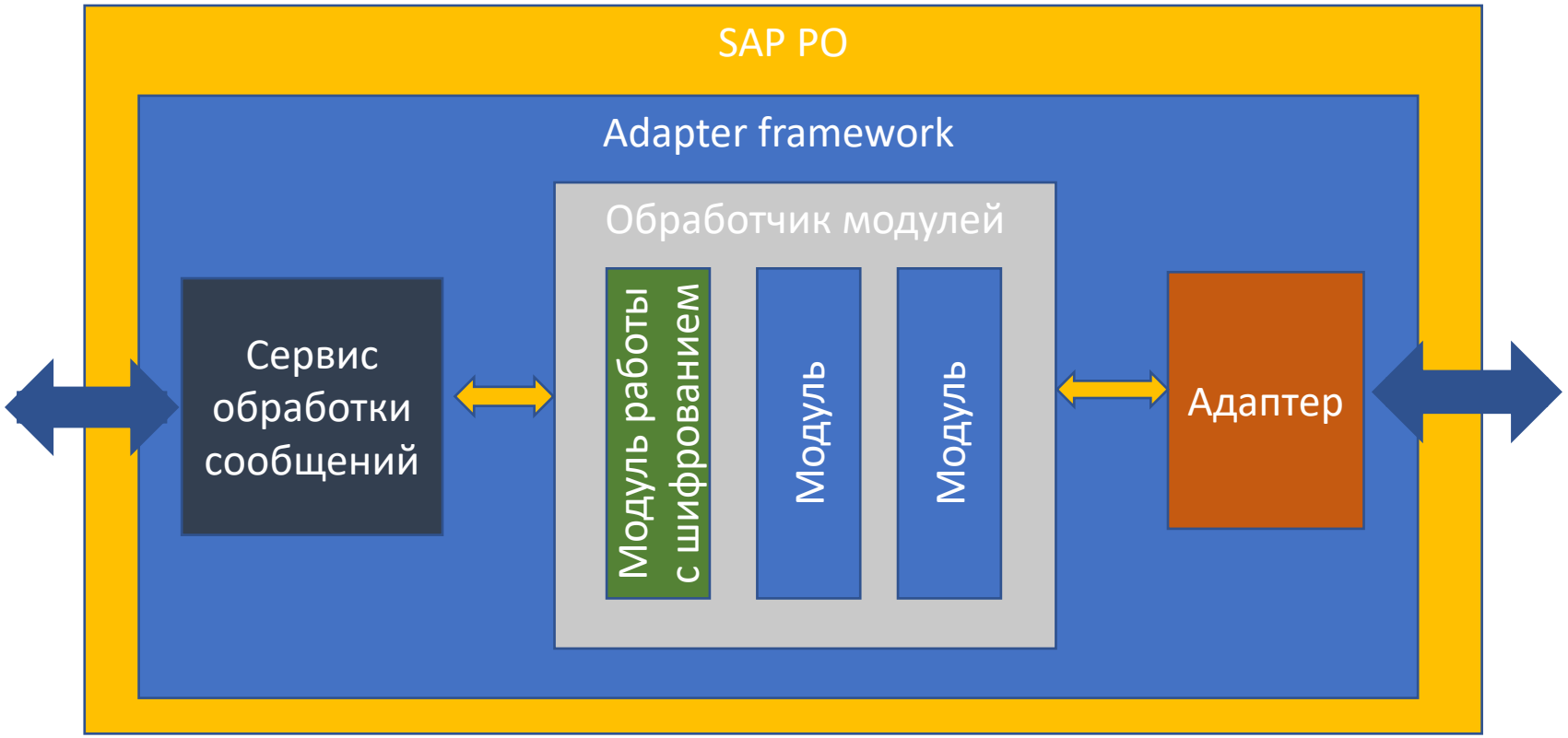
Целевая Архитектура решения



Целевая Архитектура решения



Место интеграции модуля



Платформа Adapter framework основана на **Java runtime environment** и архитектуре **JCA** (Java EE Connector Architecture).

Сервис обработки сообщений занимается обменом сообщениями с центральной системой обработки сообщений

Обработчик модулей позволяет расширять адаптеры дополнительными Java-модулями, что позволяет производить действия над сообщением непосредственно до или сразу после работы адаптера

Адаптеры выполняют прием/передачу сообщений в формате внешней системы с использованием необходимого технического протокола передачи; перевод сообщений между форматом внешней системы и внутренним форматом SAP PO.

Решение для работы с ГОСТ криптографией

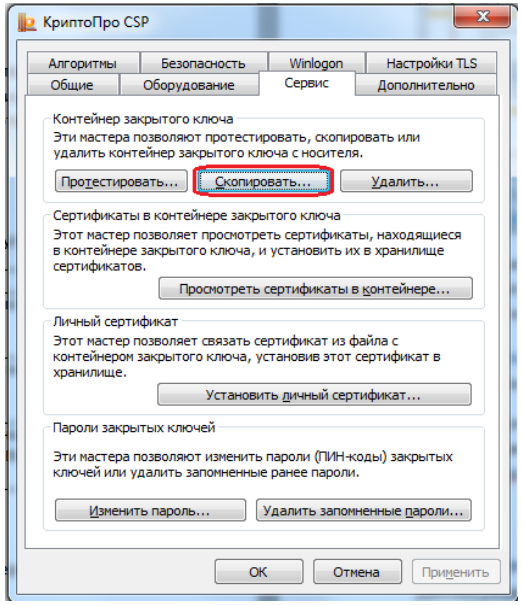
SAP PO в стандартной поставке содержит библиотеку Sapcryptolib которая не поддерживает российское ГОСТ шифрование.

КриптоПро JSP - средство криптографической защиты информации, реализующее российские криптографические стандарты, разработанное в соответствии со спецификацией JCA (Java Cryptography Architecture).

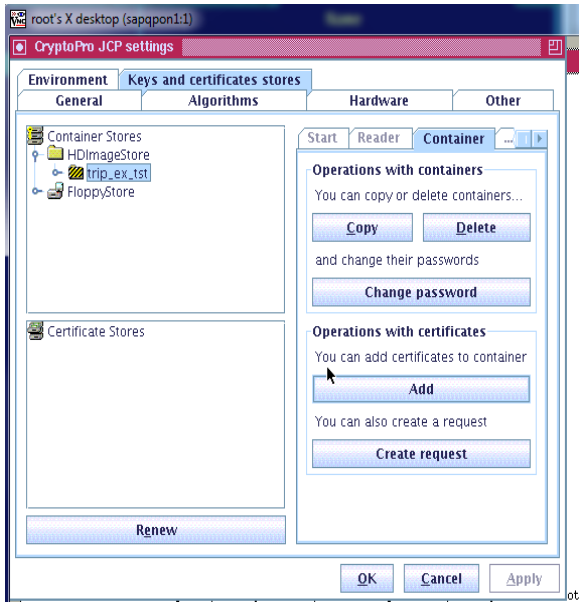
КриптоПро JSP представляет собой Java модуль который выполняет все криптографические операции используя КриптоПро CSP. Данный криптопровайдер сочетает в себе высокую скорость нативного кода с удобством разработки и использования JCE интерфейсов в Java приложениях.

Хранение закрытых ключей в Крипто Про

Экспорт ключа с носителя



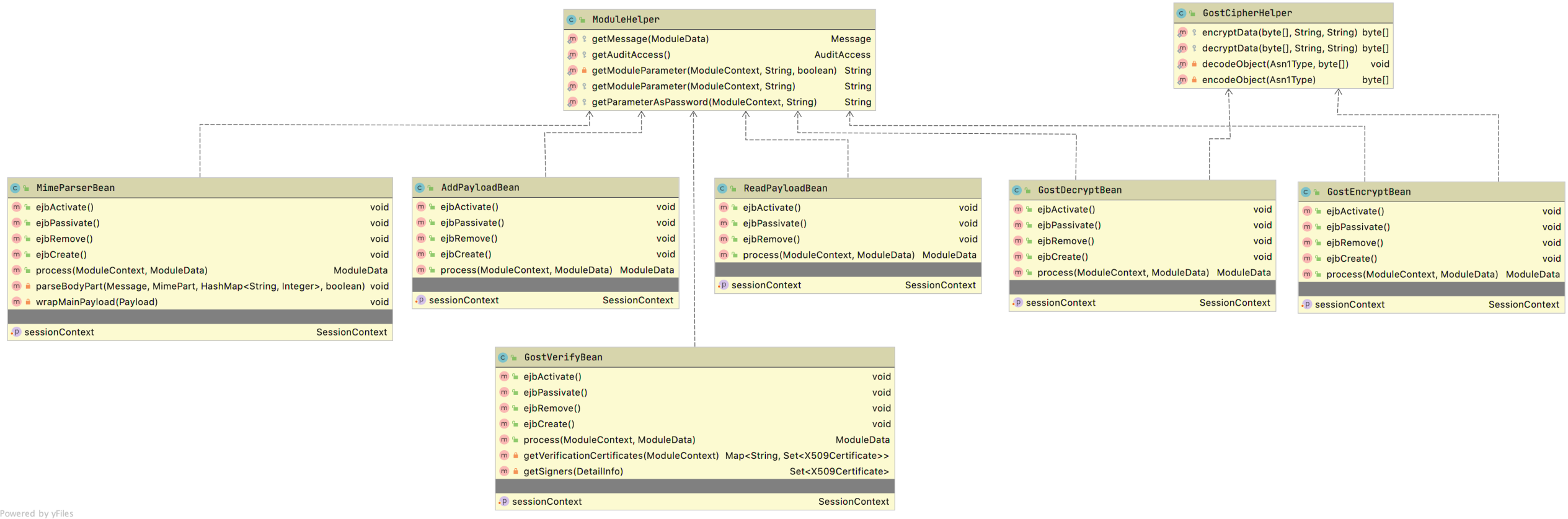
Импорт ключа на сервер в контейнер JCP



Процесс импорта сертификата с закрытым ключём:

1. Получить сертификат с ключом на совместимом с КриптоПро носителе;
2. С помощью ПО КриптоПро CSP на локальном ПК выполнить копирование контейнера на флэш накопитель
3. Скопировать полученный на флэш накопителе контейнер (папка вида <Имя_Контейнера>.000) в хранилище на сервере SAP PO (по умолчанию находится в /var/opt/cprocsp/keys/<sid>adm/)
4. Убедиться в консоли КриптоПро JCP на сервере в видимости контейнера

Перечень разрабатываемых классов



Перечень разрабатываемых классов

Модуль	Описание
AddPayloadBean.java	Модуль считывает значение переменной контекста, и создает из нее дополнительное содержимое сообщения. Значение должно быть строковым. При необходимости значение может быть в Base64 кодировке, в таком случае содержимое декодируется.
ReadPayloadBean.java	Модуль считывает главное содержимое сообщения в переменную контекста. При необходимости содержимое может быть закодировано в Base64 кодировку.
GostDecryptBean.java	Модуль дешифрования данных по ГОСТ 28147-89
GostEncryptBean.java	Модуль шифрования данных по ГОСТ 28147-89
GostVerifyBean.java	Модуль верификации ЭЦП по ГОСТ 34.10-2001
MimeParserBean.java	Модуль выполняет разбор MIME данных главного содержимого переданного ему сообщения. Полученный блок данных или блоки данных (в случае MIME Multipart данных) добавляются как вложения к сообщению.
GostCipherHelper.java	Модуль декодирования
ModuleHelper.java	Helper модуль

Заключение

Спасибо за внимание.