2015 CEE-SEC(R) Разработка ПО

СБЕРБАНК ТЕХНОЛОГИИ

Шлюзы безопасности в банковской отрасли: сценарии из жизни

Густомясов Игорь
Заместитель директора ЦК по стратегическим разработкам, Сбербанк Технологии
Литвинов Антон
Главный Архитектор, Сбербанк Технологии

22.10.2015

Вступление

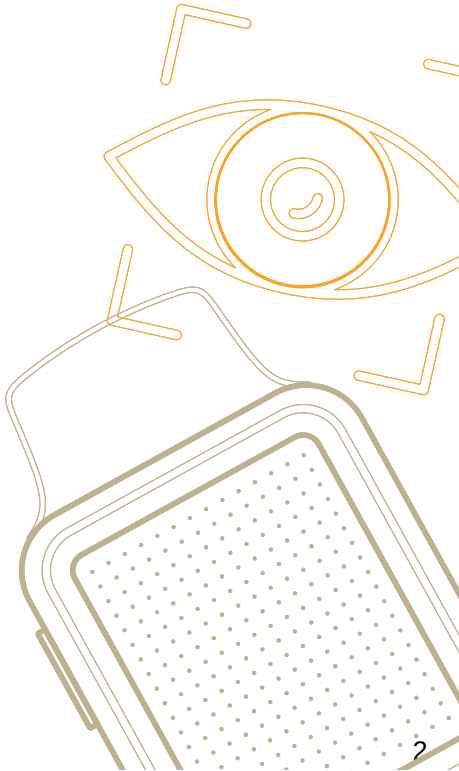
СБЕРБАНК ТЕХНОЛОГИИ

Опыт?

- Более **25** шлюзовых решений для организации внешних взаимодействий с **100+** внешних контрагентов, в том числе для узкоспециализированных задач

О чем пойдет речь?

- Шлюзы, программно-аппаратный комплексы обеспечивающие взаимодействие банковских систем, размещенных в защищенной внутренней сети с контрагентами (организациями или лицами) или собственными агентами (сотрудники, внешние устройства), размещенными во внешней сети



Банковская ИТ-платформа в качестве хаба

СБЕРБАНК ТЕХНОЛОГИИ

Интернет-банк

Мобильный банк

Банкоматы и терминалы

POS-терминалы

Единый фронт-офис

Сервисный хаб

Внутренние финансовые сервисы

Сервисы филиалов и дочерних банков

Внешние финансовые сервисы

Внутренние АС

Интеграционные шлюзы

Денежные переводы

Кредитные бюро

Платежи

Гос.услуги

WESTERN UNION

MoneyGram.

Яндекс деньги

Разделенные решения vs. гибкость бизнеса

СБЕРБАНК ТЕХНОЛОГИИ

	B2B	SOA	APIS	MOBILE	WEB
Бизнес-каналы					
Пользователи	Партнеры	Партнеры Контрагенты	Разработчики	Потребители Сотрудники	Потребители Сотрудники
Решения безопасности	Шлюз B2B	Шлюз SOA	Управление API	Шлюз мобильных решений	Веб-прокси

КСШ, Автоматизированные системы, Приложения

Унифицированный шлюз

СБЕРБАНК ТЕХНОЛОГИИ

Основные принципы построения интеграционных шлюзов

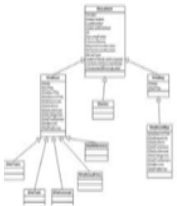
СБЕРБАНК ТЕХНОЛОГИИ

Унификация шлюзовой функциональности

- Фиксированный набор типовой функциональности, общей для всех взаимодействий
- Унифицированная платформа для реализации функциональности шлюза
- Функциональность на основе унифицированных шлюзов
- Управление решением при помощи единой системы управления и мониторинга

Уровень информационной защиты соответствует решаемой задаче

- Комплекс мер защиты выбирается но основе уровня критичности информации и доверенности контрагента
- Для аналогичных по уровню критичности взаимодействий используется одинаковый набор средств защиты на основе утвержденных шаблонов
- Утвержденный комплекс защитных инструментов



Вынесение шлюзовой логики по взаимодействию с контрагентами из АС Банка в шлюз

- Вынесение из АС типовые функции интеграции – преобразование форматов, преобразование протоколов, маршрутизация, контроль SLA, гарантия доставки
- Вынесение из АС функции безопасности – проверка контента на уязвимости, шифрование трафика, работа с ЭЦП

Максимальное повторное использование функциональности

- Однотипная функциональность используется без изменений на различных проектах
- Одинаковые требования по взаимодействию с контрагентом/ АС Банка реализуются один раз и используются впоследствии в разных решениях

Типы шлюзов

СБЕРБАНК ТЕХНОЛОГИИ

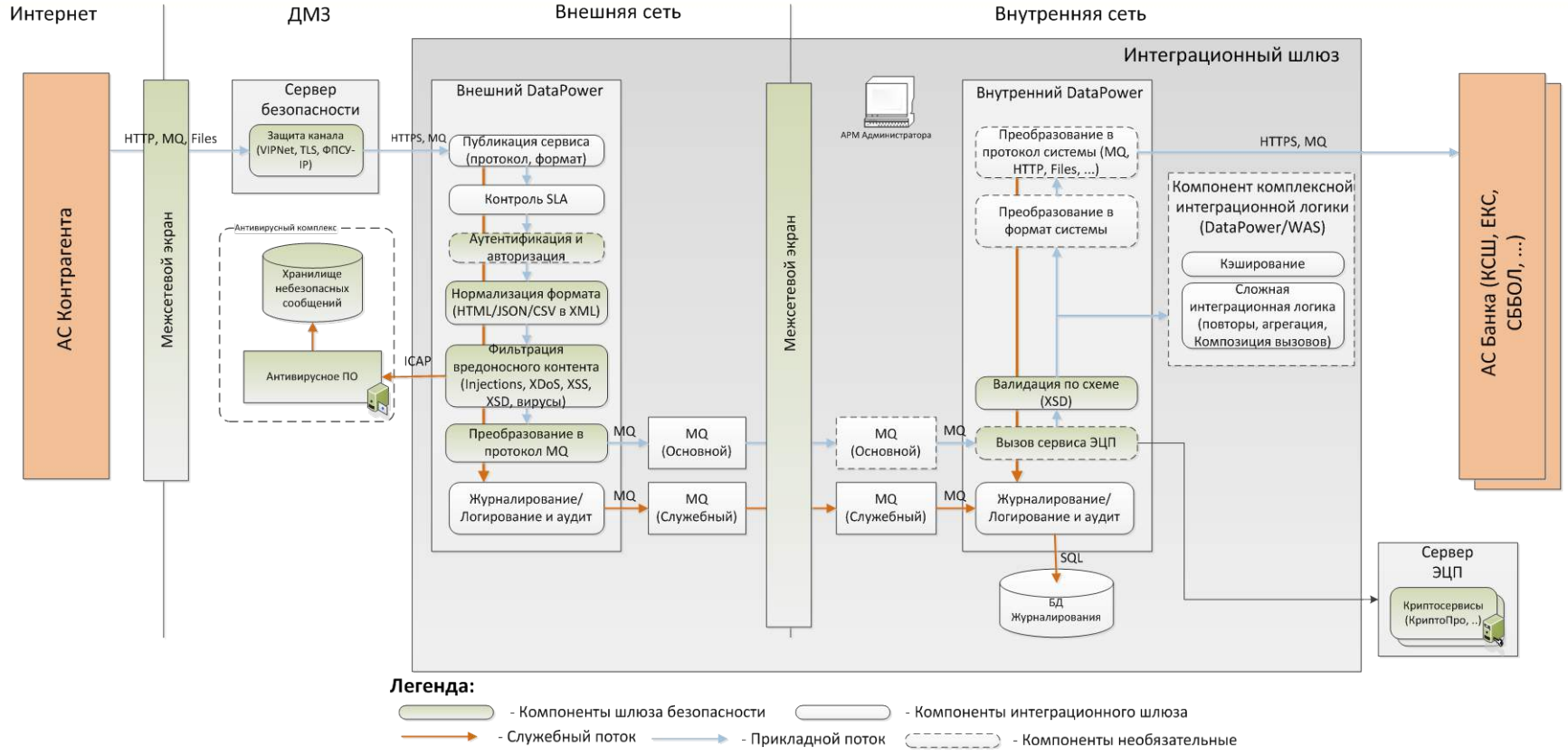
Интеграционный шлюз

- Обеспечивает взаимодействие уровня система – система с произвольным контрагентом и должен поддерживать максимальное количество форматов внешнего взаимодействия наиболее безопасным способом.

Шлюз безопасности

- Обеспечивает взаимодействие модулей одной системы Банка, размещенных во внешней и внутренней сети
- Как правило используется для организации клиентского доступа (сотрудник, клиент) к функциональности конкретной системы Банка.

Компонентный состав интеграционного шлюза



Что дает IBM DataPower?

СБЕРБАНК ТЕХНОЛОГИИ

Сертифицированная безопасность
- FIPS 140-2 Level 3
- Защита от внешних атак (DoS, XML-вирусы, SQL-вставки)
- Аутентификация, авторизация контрагентов
- Валидация данных

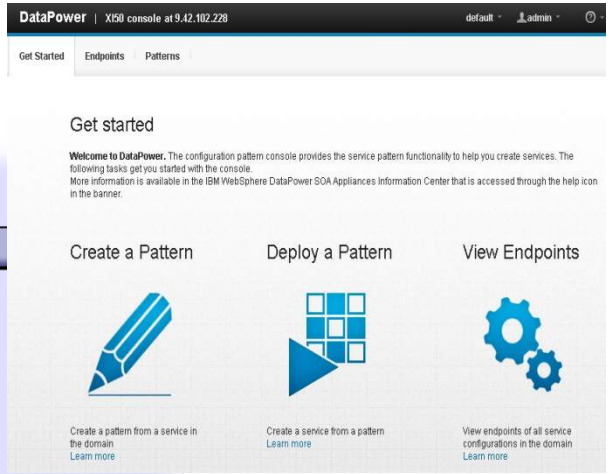
Высокая производительность

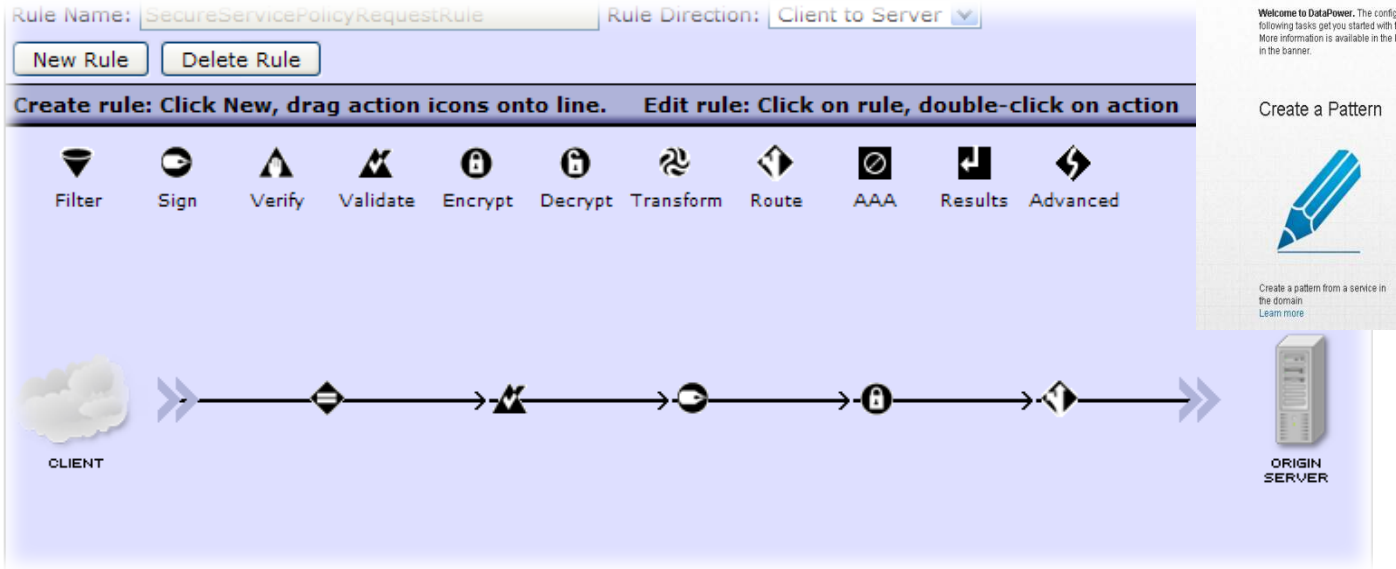
Множество функций в одном устройстве
- Управление сервисным контрактом
- Динамическая маршрутизация и балансировка
- Безопасность на границе сетевых сегментов
- Применение политик безопасности
- Смена транспорта и трансформация сообщений

Легкость настройки
- Простая настройка, обновление и администрирование
- Простое встраивание в шину ESB

Простота конфигурирования

- Применение стандартов безопасности без необходимости писать код
- Интуитивно понятное представление процесса обмена сообщениями
- Импорт/Экспорт конфигураций между средами
- Возможность просматривать содержимое сообщений между действиями для поиска ошибок



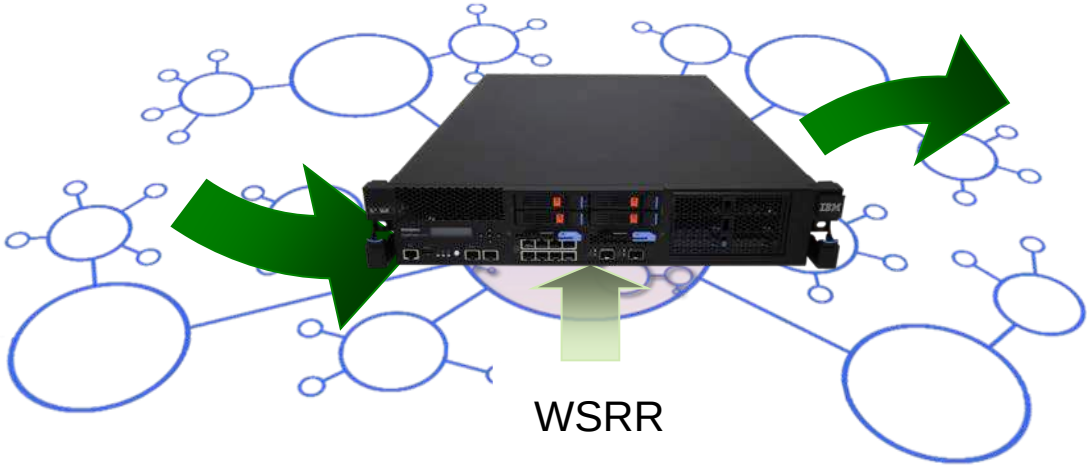


Аутентификация, авторизация и аудит

Централизованное управление сервисами

СБЕРБАНК ТЕХНОЛОГИИ

- Использование IBM WebSphere Service Registry & Repository (WSRR) для хранения, публикации и управления web-сервисами
- Автоматическое выставление сервисов в DataPower через WSRR подписку
- Динамическое извлечение информации для маршрутизации из WSRR



Бизнес-кейс: мобильные и карточные платежи

СБЕРБАНК ТЕХНОЛОГИИ

Цели и достижения:
- Увеличение каналов оплаты
- Улучшение качества предоставления сервиса
- Сокращение времени разработки

Реализация:
Для мобильных платежей, шлюз выполняет следующие действия:
- Аутентификация
- Авторизация
- Валидация запросов по WSDL

Для карточных платежей, шлюз выполняет следующие действия :
- Фильтрация сообщений
- Создание нескольких выходных сообщений из одного входного
- Трансформация из внешнего формата во внутренний
- Маршрутизация на основе значения заголовка
- Обогащение данных

Бизнес-кейс: выдача кредита

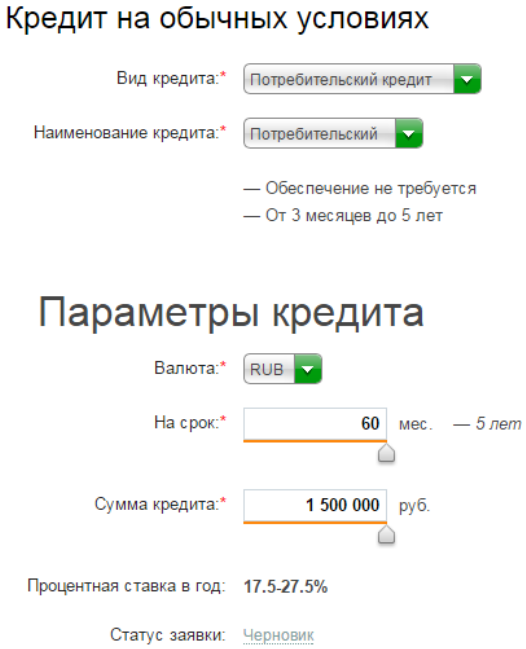
Цели и достижения:

- Предоставление механизмов, позволяющих клиентам быстро оформлять кредиты
- Соответствие внутренним стандартам безопасности и требованиям внешнего регулирующего агентства
- Быстрая интеграция с внешними кредитными рейтинговыми агентствами

Реализация:

Интеграционный шлюз выполняет следующие действия:

- Конструкция сообщения для отправки внешнему агентству для проверки кредитной истории клиента
- Вызов необходимых сервисов, основываясь на результате ответа от внешнего агентства
- Маршрутизация на основе контента
- Выставление сервисов для потребления в корпоративной шине

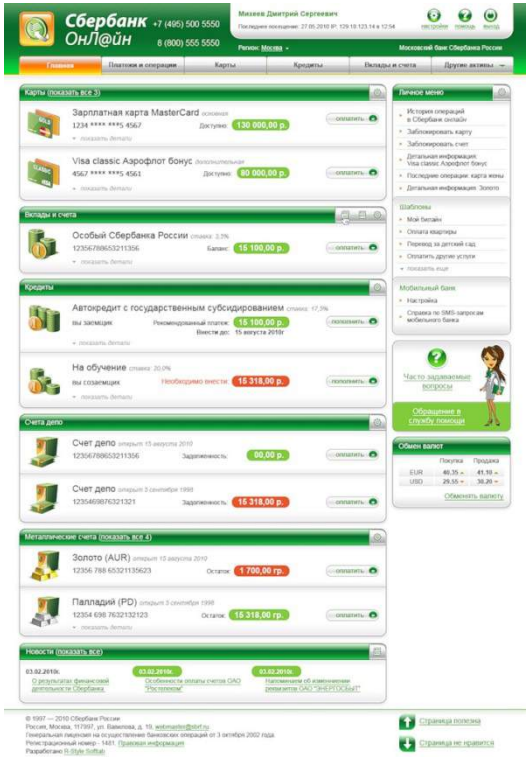


Бизнес-кейс: Сбербанк Онлайн

СБЕРБАНК ТЕХНОЛОГИИ

Цели и достижения:
- Предоставление клиентам безопасной платформы онлайн-банкинга
- Безопасность при взаимодействии с внешними пользователями
- Платформа обслуживает более 30 млн клиентов онлайн-банкинга и имеет до 2000 конкурентных транзакций в секунду

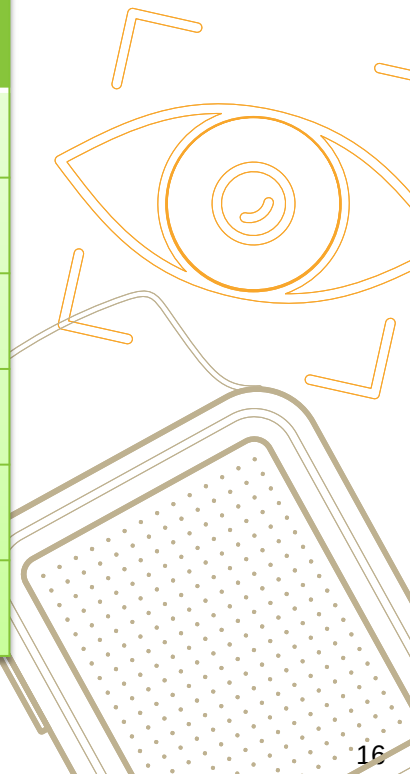
Реализация:
Шлюз АС выполняет следующие действия:
- Защита от атак, фильтрация
- Валидация по схеме
- Смена протоколов HTTP-MQ
- Трансформация
- Управление сервисным контрактом



Сокращение времени разработки

СБЕРБАНК ТЕХНОЛОГИИ

Функционал	Время разработки, часы (кастомное решение)	Время разработки, часы (DataPower)
Безопасность: аутентификация, авторизация, аудит	360	18
Защита от угроз: невозможность отказа, целостность, конфиденциальность	1080	51
Маршрутизация: виртуализация сервиса, динамическая маршрутизацию по контенту	140	20
Смена протокола (HTTP-MQ\MQ-HTTP)	140	20
Трансформация сообщений (в/из XML)	120	40
Управление сервисным контрактом (SLA, пороговые значения)	280	40



СБЕРБАНК
ТЕХНОЛОГИИ

Спасибо!
Вопросы?