



SmartDataCenter

Подготовка данных для персонализации приложений на смарт-картах

Краткое описание

SmartDataCenter – программный продукт, выполняющий подготовку данных для персонализации приложений на смарт-картах.

SmartDataCenter дополняет исходные данные из системы Back Office или системы генерации данных для магнитной полосы значениями необходимых параметров EMV-приложения (включая параметры риск-процедур), управляет выполнением необходимых криптографических процедур и формирует персонализационный файл в требуемом формате (в том числе *EMV Common Personalization*). **SmartDataCenter** позволяет готовить данные для персонализации как EMV-приложений, так и нефинансовых приложений: транспортных, социальных, лояльности и т.д. **SmartDataCenter** обеспечивает гибкую интеграцию с другими программными системами и криптографическими устройствами.

Функции

- Дополнение данных из входного потока постоянными и вычисляемыми значениями в соответствии с конфигурацией подготавливаемых данных;
- Группировка входных данных в соответствии с требованиями приложений для смарт-карт;
- Вычисление значений тегов по формулам с использованием значений других тегов и полей данных;
- Генерация и преобразование секретных величин в соответствии с отраслевыми стандартами *EMV 4.1*, *EMV* и *Visa Common Personalization* и требованиями приложений *VSDC 1.3.2/1.4.0*, *M/Chip 2.1/4.0*:
 - Генерация UDK-ключей для EMV-приложений;
 - Использование RSA-ключей эмитента для вычисления сертификата данных (формирование данных SDA);
 - Генерация RSA-ключей карты и формирование сертификатов карты (поддержка DDA/CDA и шифрованного ПИН-кода);
 - Перешифрование ПИН-блока и изменение его формата;
 - Перекодирование DES-ключей с проверкой контрольного значения;
 - Изменение формата представления RSA-ключей из CRT в двухкомпонентное с возможностью изменения транспортного ключа.
- Формирование данных, управляющих процедурами загрузки и инсталляции приложений на картах *GlobalPlatform*;
- Ассоциация криптограмм MDK-ключей EMV-приложения, RSA-ключей эмитента и их сертификатов, а также описаний набора приложений для того или иного типа карт с BINами карточных продуктов;
- Возможность выбора тех или иных карточных ключей на основе правил, анализирующих входные данные (может быть использована для изменения транспортных ключей в зависимости от того, в какой персонализационный центр направляются данные);
- Формирование выходного файла в различных форматах:
 - XML;
 - *Visa Common Personalization v 1.5*;
 - *EMV Common Personalization v 1.0*.

Возможности и особенности

Ввод данных

Для ввода данных из внешних источников используется скрипт-языки, поддерживающие технологию Active Scripting™, что позволяет:

- адаптироваться к формату входных данных;
- взаимодействовать с несколькими источниками данных одновременно;
- получать данные из любой промышленной СУБД;
- предварительно обрабатывать данные на этапе ввода.

Стандартные случаи взаимодействия с системами Back Office, наиболее часто встречающиеся в России и СНГ, описаны в разделе «[SmartDataCenter в действии](#)» далее в этом документе.

Режимы работы

SmartDataCenter позволяет работать в двух режимах: интерактивном и пакетном.

В интерактивном режиме пользователь имеет возможность описать конфигурацию подготавливаемых данных и запустить обработку входных данных с помощью понятного графического пользовательского интерфейса.

Пакетный режим обеспечивает обработку входных данных при запуске программы из командной строки с необходимым набором параметров. Это позволяет легко интегрировать в **SmartDataCenter** технологическую цепочку обработки информации.

Вывод данных

Выходной файл с персонализационными данными может формироваться в одном из форматов, названных выше, что позволяет просто обеспечивать взаимодействие системы подготовки данных с произвольной системой персонализации.

Архитектура

В общем случае система подготовки данных для персонализации приложений на смарт-картах имеет следующую архитектуру: входные данные из системы Back Office обрабатываются скрипт-программой ввода данных и попадают в **SmartDataCenter**, где на их основе происходит генерация и обработка требуемых величин. Криптографические процедуры выполняются в криптоустройстве SafeNet (*Eracom*) или *Thales e-Security*; подготовленные персонализационные данные выводятся в файл в требуемом формате.



Рис. 1. Система подготовки данных для персонализации приложений на смарт-картах.

Поддержка и сопровождение

Специалисты компании ПРОНИТ помогают клиенту в построении системы:

- устанавливают программное обеспечение;
- адаптируют конфигурации, обеспечивающие подготовку данных для EMV-приложений, реализованных на картах различных производителей;
- обучают персонал работе с программным обеспечением;
- предоставляют сопутствующую документацию,
- помогают в решении вопросов в офисе клиента, по электронной почте или телефону.

SmartDataCenter в действии

В данном разделе приведены примеры, в каких конфигурациях **SmartDataCenter** готовит персонализационные данные во взаимодействии с наиболее популярными в России и СНГ системами Back Office.

Если Back Office предоставляет только PAN, Expiry Date и Cardholder Name, то для получения персонализационных данных в Систему подготовки персонализационных данных включаются программа **MSDP Manager**, которая осуществляет генерацию данных для магнитной полосы и ПИН, а также **SmartDataCenter**.

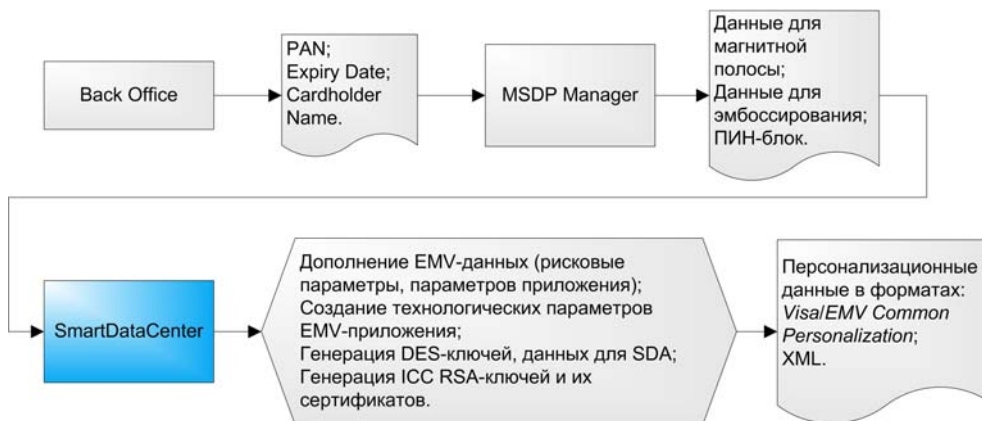


Рис. 2. Система подготовки данных для персонализации микросхемы при минимальной функциональности Back Office

Если Back Office предоставляет готовые данные для магнитной полосы и эмбоссирования, а также зашифрованный ПИН-блок, то Система подготовки EMV-данных будет содержать только **SmartDataCenter** и будет выглядеть так:

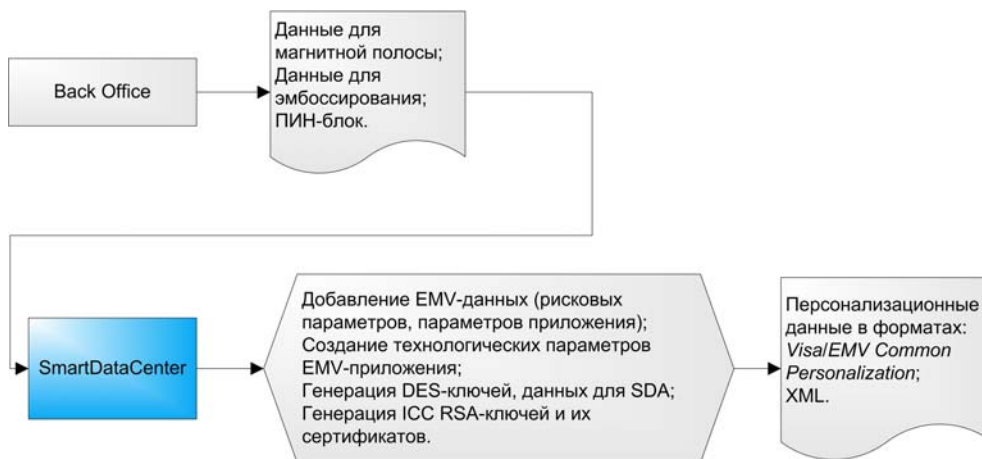


Рис. 3. Система подготовки данных для персонализации микросхемы с системой Back Office, экспортирующей зашифрованный ПИН-блок

Возможна ситуация, когда система Back Office подготавливает и часть EMV-данных.

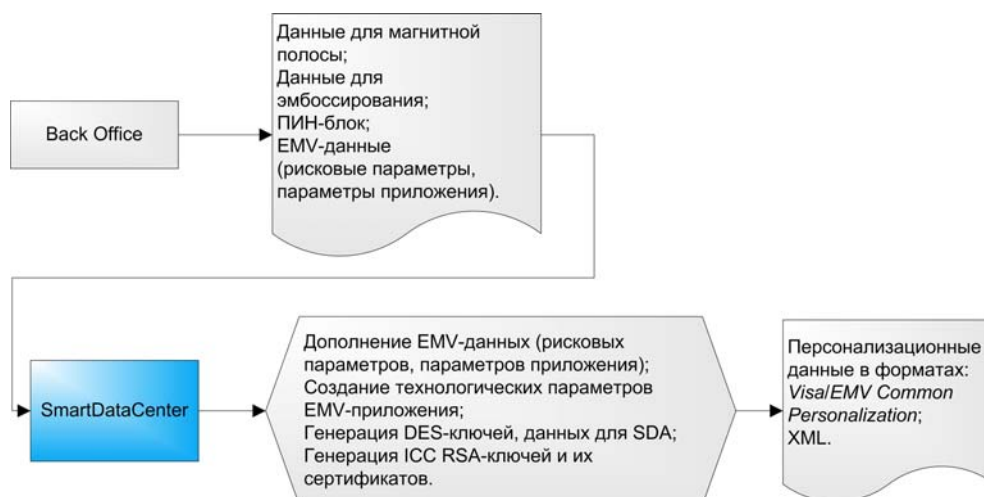


Рис. 4. Система подготовки персонализационных данных с Back Office, экспортирующей часть EMV – данных

Это наиболее распространенные в России и СНГ конфигурации. В каждом случае гибкость продуктов для подготовки персонализационных данных позволила провести адаптацию к системам Back Office и в результате получить один и тот же требуемый результат – файл с персонализационными данными в формате отраслевых стандартов *Visa/EMV Common Personalization* или XML.

Платформа

Рабочая станция SmartDataCenter	<i>Windows 2000, XP</i>
Криптоустройство	<i>SafeNet (Eracom); Thales e-Security.</i>