ЗАЩИТА ДАННЫХ

СОХРАНИТЬ ВСЁ

Токенизация карточных данных

Ян Коршунов

2023

Немного о себе

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Банки

- Международный промышленный банк
- Банк инноваций и развития
- Адмиралтейский банк
- Сбербанк, БПС-Сбербанк
- ВТБ

Стандарты

PCI DSS
PA DSS (SSF)
P2PE
PIN Security

Автор патента по токенизации карточных данных

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2756576

СПОСОБ ТОКЕНИЗАЦИИ НОМЕРА БАНКОВСКОЙ КАРТЫ И СПОСОБ ДЕТОКЕНИЗАЦИИ НОМЕРА БАНКОВСКОЙ КАРТЫ

Патентообладатель: *Публичное акционерное общество "Сбербанк России" (ПАО Сбербанк) (RU)*

Авторы: *Коршунов Ян Юрьевич (RU), Соколов Дмитрий Юрьевич (RU), Сафронов Юрий Викторович (RU), Никитин Александр Юрьевич (RU)*

Заявка № 2020131500
Приоритет изобретения 24 сентября 2020 г.
Дата государственной регистрации в Государственном реестре изобретений Российской Федерации 01 октября 2021 г.
Срок действия исключительного права на изобретение истекает 24 сентября 2040 г.

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Как защищать карточные данные

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

PAN (номер карты): **4188 6868 8888 6666***

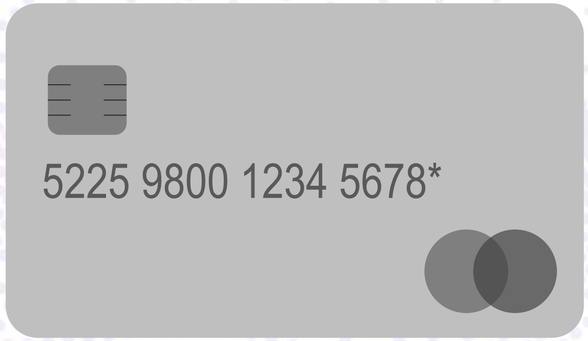
- Маскирование 4188 68** **** 6666
- Усечение 4188 68 6666
- Шифрование U2FsdGVkX19zu7IYe5ZJe … eNSURvH+WNRhoqDFA1
- Хеширование 6464945a4222b76158fb5a1ab9603306
- Токенизация 4188 686C 135A 6666

* совпадения случайны

Токенизация – преимущества

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

PAN
primary account number



ТОКЕНИЗАЦИЯ

DPAN
digitized primary account number

- авторизация
- претензионная работа
- передача по требованиям регуляторов

- идентификация
- внутренние расчеты
- интеграции
- аналитика
- интерфейсы
- все остальное

\+ Является уникальным CardID

\+ Маскированный PAN = Маскированный DPAN

\+ Может быть использован для любой ИС в Банке

\+ DPAN идентифицирует карту так же, как и PAN

\+ Имеет такой же формат записи, но гарантированно отличим от PAN (есть буквы)

* совпадения случайны

Токенизация – требования

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Требования к токенизации номеров карт (PCI Tokenization Guide)

- Токенизация не отменяет требований PCI DSS, но позволяет сократить область аудита
- Решение должно гарантировать невозможность восстановления номера карты вне области аудита
- Решение должно быть со строгими средствами контроля
- Решение должно обладать отсутствием коллизий, устойчивостью, сходимостью, стойкостью

Рекомендованные варианты реализации (список не закрытый)

- Обратимое шифрование стойкими алгоритмами
- Хеширование с секретной солью
- Замена по индексу, по последовательности или на основе случайных чисел

Использование базы данных для хранения значений таблиц замен для токенов

- Сложно масштабировать
- Трудно достичь отказоустойчивости
- Проблемы быстродействия

Прозрачность или секретность алгоритмов

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Почему можно и нужно делать алгоритмы открытыми

- Корпоративная невозможность имплементации секретных алгоритмов
- Принцип Керкгоффса про алгоритмы и ключи
- Иллюзия «безопасности через неизвестность»

Секретные величины в алгоритмах

- Использование HSM
- Принцип разделения ключей
- Хранение секретов в оперативной памяти

Хорошие и плохие примеры

- Хранение ключей шифрования данных в сейфе владельцев бизнеса и открытый алгоритм действий с ними
- Использование секретных «алгоритмов» без секретных ключей при выборе пин-кода платежных карт
- Использование условно секретных «ключей», таких как дат и имен в паролях

Защита алгоритмов и реализаций

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

- Патентование алгоритмов и способов реализации
- Процедура патентования
- Патентообладатель и автор

Сравнение реализаций алгоритмов токенизации

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Реализация Сбербанка *

- Несколько таблиц замен
- FPE (format preserving encryption)

Реализация ВТБ

- Использование простых чисел
- Одна таблица замены
- Самостоятельная реализация криптоалгоритма
- Выигрыш в компактности и скорости

* (взято из публичных источников – патент RU2756576C1)

Процесс внедрения

ЗАЩИТА ДАННЫХ
СОХРАНИТЬ ВСЁ

Коротко про **PCI DSS** в **ВТБ**

Последовательный\параллельный подход, временные интеграции, миграция данных по системам или по диапазонам карт

Архитектурные концепции

Сложности внедрения (особые случаи), конфликт регуляторных требований

Благодарю за внимание!

yan @ korshunoff.com

* совпадения случайны

** все изложенное является вымыслом автора и носит развлекательный характер