

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

СИСТЕМА СКАНИРОВАНИЯ

- Инфракрасное сканирование
- Источник ИК-подсветки, CCD сенсор в нижней части устройства

ТОЧНОСТЬ СЧИТЫВАНИЯ

- False Acceptance Rate (FAR): 0.00001%
- False Rejection Rate (FRR): 0.01%
- Failure to Enroll Rate (FTE): (ISO/IEC 19795-1 алгоритм сканирования, банковский уровень защиты данных)

СКОРОСТЬ ВЕРИФИКАЦИИ

- Около 1 секунды

ХАРАКТЕРИСТИКИ

- Зеленые и красные светодиодные индикаторы (опционально со звуковыми сигналами)

ИНТЕРФЕЙС

- USB 2.0
- Длина кабеля 1.8 м
- Шифрование данных биометрического венозного паттерна

СЕРТИФИКАТЫ И СТАНДАРТЫ

- ISO 19092, BIO API – поколения 2.0 соответствует требованиям ISO/IEC 19784-1. Язык безопасности – С, AES 256 шифрование, CE, система адаптирована в корпоративные решения 1С, сканеры имеют нотификацию ФСБ РФ

ГЕОМЕТРИЯ УСТРОЙСТВА И ВЕС

- 59(W) x 82(D) x 74(H) мм
- 96g



HITACHI H1

РЕШАЕМЫЕ ЗАДАЧИ

-  Защита систем от несанкционированного доступа к ПК и утечки информации, защита финансовых и управленческих процессов.
-  Аутентификация, учет, а также управление рабочими процессами сотрудников (WFM), включая контроль рабочего времени.
-  Ускорение процесса обслуживания клиентов на POS-точках продаж розничной сети, в банках и других структурах рынка ссудного капитала, а также в рамках государственных служб.
-  Контроль рабочего времени сотрудников.
-  Сегментированный интеллектуальный доступ в рамках рабочих систем. Программная аналитика по рабочим процессам и оптимизация их. ROI (Return of Investment) = 160% при рамках клиентской базы - 20 000 пользователей за период 3 года.
-  Обеспечение цифрового документооборота. Цифровая биометрическая подпись и авторизация электронных контрактов, платежей и сервисов.
-  Прямые платежи клиентов в формате B2C посредством HITACHI H1 «оплата пальцем» без использования банковских SMART карт или наличных денег в магазинах, ресторанах, на объектах социальной инфраструктуры в соответствии со всеми стандартами безопасности Visa, Master Card.
-  Формирование рабочих алгоритмов и процессов на основе статистики, полученной посредством биометрии. Построение «самообучающихся» интеллектуальных систем» внутри корпоративных управленческих форматов.

МОДИФИКАЦИИ HITACHI H1

ОПИСАНИЕ HITACHI B1 и B1F

- Тип сканера: настольные;
- Коннект: USB;
- B1: Windows, Mac, Citrix / B1F: Windows;
- Формирование образа: в устройстве;
- PKI и Finger vein pattern: on-SIM;
- Геометрия: 74 x 59 x 82 mm;
- Вес: 102 g.;
- Характеристики: LED, звуковой сигнал, B1: SIM слот / B1F: слот Smart карт

ФУНКЦИИ

- Хранение приватных ключей;
- Хранение PKI сертификатов;
- Хранение биометрических паттернов;
- Биометрическая сверка данных;
- Цифровая подпись

СПЕЦИФИКАЦИИ

- Java Card 2.2.2 или поздняя версия;
- Global Platform 2.1.1 более поздняя версия;
- AES256 и RSA2048 алгоритмы;
- Память EEPROM для установки CAP (40KB)

ПОДДЕРЖИВАЕТ

- Gemalto/IDCore 40
- G&D/SmartCafeExpert 7.0 и др.

ОПИСАНИЕ HITACHI B2

- Тип сканера: карманные / переносные;
- Коннект: USB + Bluetooth Smart;
- B2: Windows, Mac, Citrix, iOS, Android (переносной сканер B2 можно подключить к переносному мобильному устройству);
- Формирование образа: в устройстве;
- PKI и Finger vein pattern: on-SIM;
- Геометрия: 18 x 55 x 91 mm;
- Вес: 65 g.;
- Характеристики: LED, звуковой сигнал, SIM слот, дисплей, контрольные кнопки, батарея;

HITACHI B1 и B1F

Настольные биометрические сканеры рисунка вен пальцев на базе HITACHI H1, совмещенные со SMART SIM картой для банковской сферы (рынка ссудного капитала) и рынка Телеком.



ПЕРЕНОСНОЙ СКАНЕР-КОЛЛЕКТОР HITACHI B2

Переносные автономные биометрические сканеры рисунка вен пальцев на базе хэша кода HITACHI H1 для банковской сферы (рынка ссудного капитала), сферы прямых розничных продаж, курьерских служб, интернет-сервисов и возможности мобильного сбора биометрических паттернов.



ADVENT 75H1

Настенный процессорный терминал-контроллер с встроенным сканером рисунка вен HITACHI H1 и интерактивным экраном Touch Screen 7,5» для решения задач безопасности, СКУД (в рамках Систем контроля управления доступом), учёта рабочего времени и интерактивного интеллектуального управления организацией работы персонала.



РЕШАЕМЫЕ ЗАДАЧИ



Защита банков, объектов инфраструктуры, офисов, производственных предприятий. Защита хранилищ, складов, помещений с особым доступом.



Аутентификация, учет, а также управление рабочими процессами сотрудников (WFM) посредством интерактивного интерфейса и экрана Touch, включая планирование собраний, передачи целевых указаний сотрудникам посредством экрана управления устройства, учет материальных ценностей со складов и формирование рабочих алгоритмов и финансовых бюджетов на основе реальных действий пользователей.



Ускорение процесса обслуживания сотрудников, верифицированных клиентов или подрядчиков компании или банка посредством ускоренного оформления документов и упрощения рабочих процедур посредством цифрового документооборота.



Контроль рабочего времени сотрудников.



Сегментированный интеллектуальный доступ в рамках рабочих систем и непосредственно на объектах инфраструктуры. Программная аналитика по рабочим процессам и оптимизация их.



Обеспечение цифрового документооборота. Цифровая биометрическая подпись и авторизация электронных контрактов, платежей и сервисов прямо на территории отделений банков, в офисах на предприятиях и складах посредством формата «электронного интеллектуального интерфейса с биометрической верификацией».



Прямые платежи клиентов в формате B2C посредством HITACHI H1 «оплата пальцем» без использования банковских SMART карт или наличных денег в магазинах, ресторанах, на объектах социальной инфраструктуры в соответствии со всеми стандартами безопасности Visa, Master Card. Терминал позволяет предложить широкий спектр интерактивных опций посредством полноценного Windows 10 и удобного Touch screen экрана.



Формирование рабочих алгоритмов и процессов на основе статистики, полученной посредством биометрии. Построение «самообучающихся интеллектуальных систем» внутри корпоративных управленческих форматов.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

СИСТЕМА СКАНИРОВАНИЯ

- Инфракрасное сканирование посредством устройства HITACHI H1
- Источник ИК-подсветки, CCD сенсор в нижней части устройства

ТОЧНОСТЬ СЧИТЫВАНИЯ

- False Acceptance Rate (FAR): 0.00001%
- False Rejection Rate (FRR): 0.01%
- Failure to Enroll Rate (FTER): (ISO/IEC 19795-1 алгоритм сканирования, банковский уровень защиты данных)

СКОРОСТЬ ВЕРИФИКАЦИИ

- Около 1 секунды

ИНТЕРФЕЙС

- TCP/IP, RS232, USB3.0, USB2.0, HDMI type A, RS485 опционально
- Шифрование данных AES256 + разные алгоритмы криптографии и шифрования данных биометрического паттерна при заведении пользователей, а также при считывании.

СЕРТИФИКАТЫ И СТАНДАРТЫ

- ISO 19092, BIO API – поколения 2.0 соответствует требованиям ISO/IEC 19784-1. Язык безопасности – C, AES 256 шифрование, CE, система адаптирована в корпоративные решения 1C SAP, сканеры имеют нотификацию ФСБ РФ

ГЕОМЕТРИЯ УСТРОЙСТВА

- 150(W) x 70(D) x 320(H) мм

ХАРАКТЕРИСТИКИ

- Зеленые и красные светодиодные индикаторы (опционально со звуковыми сигналами) на сканере HITACHI H1
- LCD монитор 7,5 дюймов, либо 10 дюймов с Touch screen и защитным антивандальным покрытием из стекла или поликарбоната
- Корпус - Сталь авиационная. Антивандальный - IP65
- Ethernet / WiFi опционально 802.11b/g/n+BT 4.0 (2.4GHz/5G)
- OS: Windows 10 лицензированный Mini PC 2GB/32GB, Flash hardware decode, Html5
- Процессор Intel Cherry Trail Z8350 Quad Core 1.8GHz
- Ram: 2GB DDR3L
- Память: 32GB
- GPU: Intel HD Graphics, 12 EUs @200-500 Mhz
- Питание 2A / 5 Вольт, желательно 3A, использование PoE нежелательно
- Резервное питание (батарея) опционально - 12000 mAh
- Опционально - считыватели карт Mifare, Em Marine, HID



HITACHI UBR

Альтернативное средство аутентификации для банкоматов, предлагающее улучшенную безопасность и защиту от использования подсмотренных, подобранных, украденных или переданных другому лицу PIN-кодов.



РЕШАЕМЫЕ ЗАДАЧИ

-  Криптография и шифрование биометрических паттернов в соответствии с наивысшими требованиями банков.
-  Защита от подделок аутентификационных данных — полное соответствие нормам ISO 19092 и требованиям к защите биометрических паттернов во время операций с банкоматом, нормам по безопасности программных банковских решений
-  Быстрое решение любых задач банковский деятельности на высочайшем уровне в различных сферах
-  Обеспечение высочайшего уровня защиты на программном и аппаратном уровне
-  Создание надежной и скоростной связи между считывателем и блоком управления (РС АТМ), между считывателем и сотрудником банка (ЕТН)
-  Блокировка от проникновения злоумышленников в систему управления
-  Организация системы электронной подписи
-  Управление процессом аутентификации пользователей
-  Надежное хранение и регистрация биометрических данных
-  Настройка индивидуальных сервисов с привязкой к биометрической верификации, возможность автоматизации процесса подписания договоров с банками в автономном режиме посредством терминалов и банкоматов. Как итог - уменьшение инфраструктуры отделений банков и экономия.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

СИСТЕМА СКАНИРОВАНИЯ

- Инфракрасное сканирование
- Источник ИК-подсветки, CCD сенсор в нижней части устройства

ТОЧНОСТЬ СЧИТЫВАНИЯ

- False Acceptance Rate (FAR): 0.00001%
- False Rejection Rate (FRR): 0.01%
- Failure to Enroll Rate (FTER): (ISO/IEC 19795-1 алгоритм сканирования, банковский уровень защиты данных)

СКОРОСТЬ ВЕРИФИКАЦИИ

- Минимальное время считывания в формате 1:1 примерно 0,3-0,5 сек.

ИНТЕРФЕЙС

- USB 2.0
- Шифрование данных биометрического венозного паттерна.

OS

- Windows Vista Business SP2, Windows 7 Professional SP1 (32bit), Windows 7 Professional SP1 (64bit)

СТАНДАРТЫ

- CE, FCC (Class A), RoHS, SO 19092, BIO API – поколения 2.0 соответствует требованиям ISO/IEC 19784-1. Язык безопасности – C, AES 256 шифрование, CE, система адаптирована в корпоративные решения 1С, сканеры имеют нотификацию ФСБ РФ

ГЕОМЕТРИЯ УСТРОЙСТВА

- 69,0 x 46,5 x 80,5mm

ПРЕИМУЩЕСТВА:

Значительное повышение безопасности операций с банкоматами и терминалами. Рисунок вен, в отличие от PIN-кода нельзя записать, или как пластиковую карту передать другому, украсть или потерять.

Наивысшие характеристики в рамках требований безопасности **ISO 19092, BIO API** – поколения **2.0** соответствует требованиям **ISO/IEC 19784-1**. Язык безопасности – C, **AES 256** шифрование.

Биометрическая идентификация наряду с чип-картами гарантирует, что личность владельца карты соответствует уникальному рисунку вен его пальцев. Модели верификации: 1) Биометрия, 2) Биометрия + **PIN**, 3) Биометрия + **PIN** + **Online Bank**.

Невозможно получить биометрический образ рисунка вен, в отличие от технологий «распознавания лиц» или сканирования отпечатков пальцев.

Возможность встраивания в банкоматы: **Diebold, NCR, Wincor Nixdorf**.

Высокая скорость считывания при высокой многосложности биометрического паттерна.

Уникальная технология сквозного инфракрасного сканирования с различным вектором расположения подсветки и сенсора.

Сочетание сетевого и автономного режимов работы в одном устройстве. Компактный размер, не требует много места. P

Возможность интеграции в банкоматы или терминалы с интерактивным интерфейсом, позволяющие не только верифицировать транзакции или снимать/вносить на счет наличные деньги, но и верифицировать конкретные сервисы, «подписывать» посредством венозных сканеров соглашения и договора на предоставление клиентских услуг, что является уникальным инструментом для создания «Умных виртуальных банков» с уменьшенным числом сотрудников в отделениях. Реализация полноценного принципа цифрового или онлайн банка.