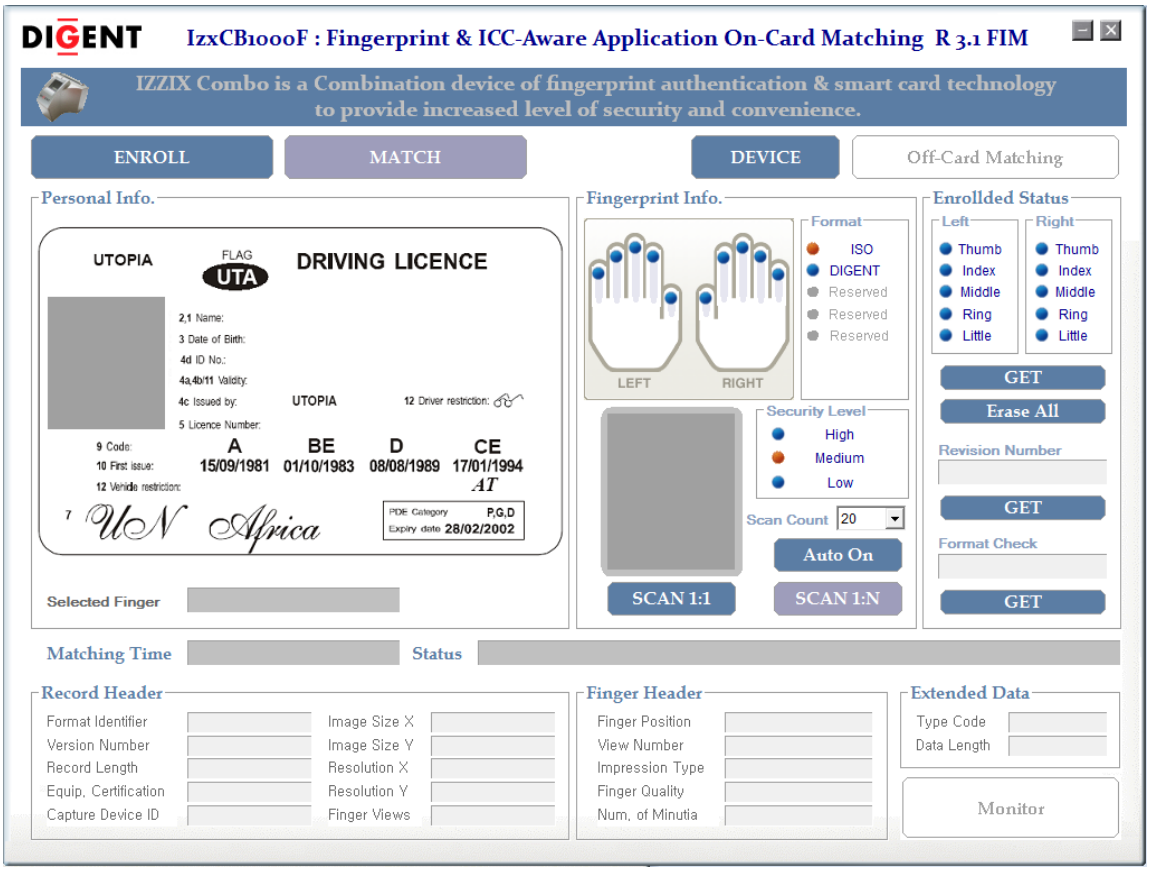
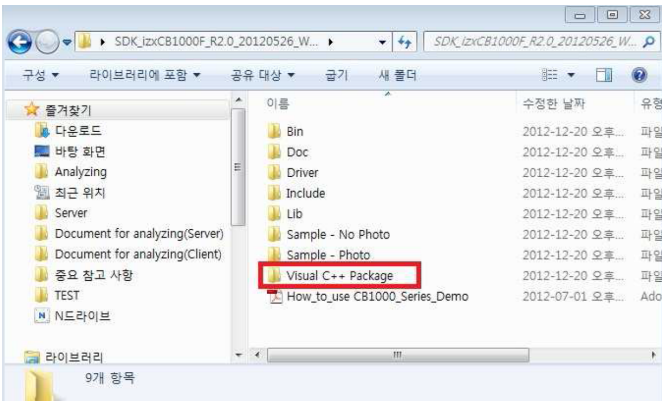
CB1000F Demo



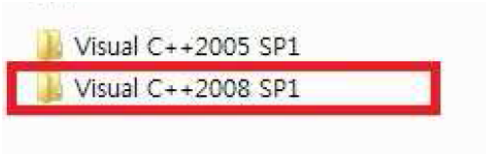
Инсталация

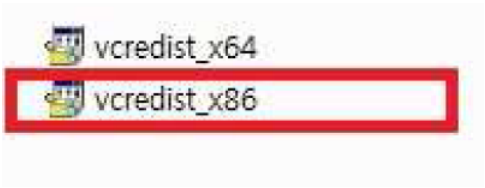
Преди да може да използваме **CB1000F Demo** трябва предварително да инсталираме помощен софтуер и драйвъри.

1. Инсталира **Visual C++ Redistributable Setup.exe** от папката **Visial C++ Package**.



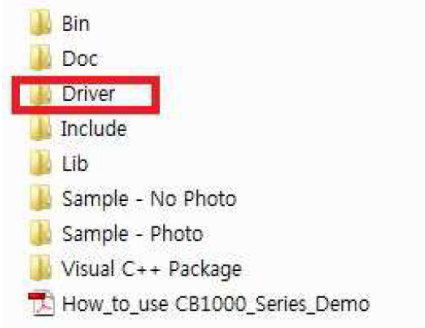
Препоръчителна версия Ver. 2008 SP1 32 bits.

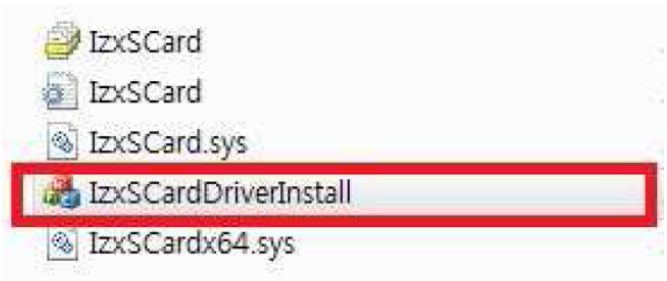




Следвайте стъпките на инсталатора (стандартно - next, next, finish).

2. От папката **Driver** стартирайте **IzxSCardDriverInstall.exe** - инсталатор на драйвъри за демо програмата, която използвам **CB1000F** комбиниран четец.

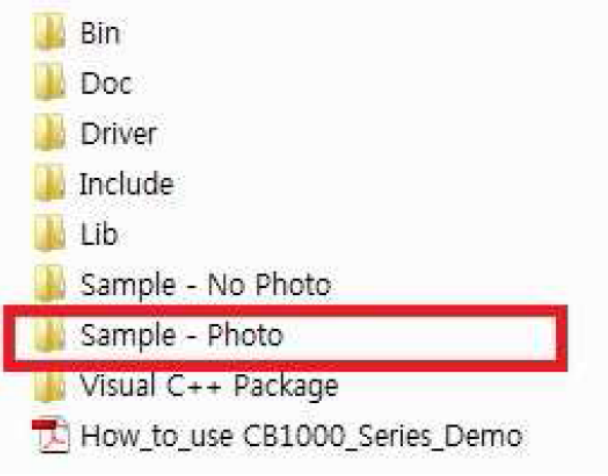






Забележка: Възможно е да се направи комбинация от други четци на смарт карти и пръстови отпечатъци, но тогава трябва да се инсталират драйвърите за съответния четец. За повече информация и драйвъри за други хардуерни устройства за сканиране на пръстови отпечатъци http://www.digent.com/English/.

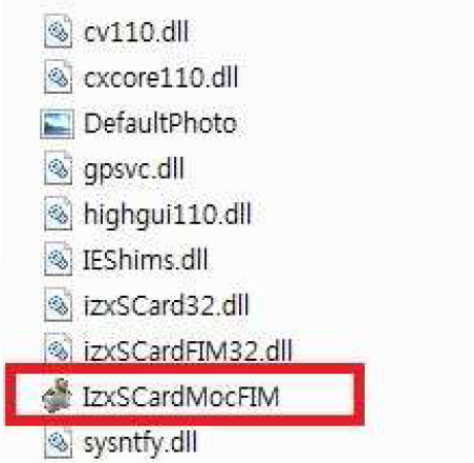
3. Стартирането на демо програмата - вариантите са два “**Sample - Photo**” и “**Sample - No Photo**”. Разликата между двете е, че при единия вариант се записва снимка на картодържателя на самата смарт карта, в другия - не.



След като сме избрали една от папките влизаме в папката **Release**



и стартираме програмата **IzxSCardMocFIM.exe** (да се стартира чрез **“Run as an Administrator”** ако програмата се стартира на операционна система **Windows 7**)



4. След като сме стартирали програмата, отиваме на екрана **DEVICE** (след като сме натиснали бутона **DEVICE**), за да проверим дали всичко е наред и дали закачение устройства към PC са разпознати от програмата.

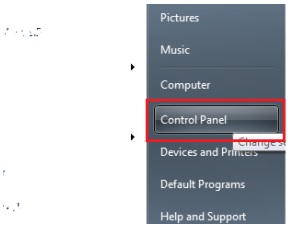


5. Въпреки че инсталацията на драйвърите е протекла успешно, възможно е демо програмата да не успява да разпознае хардуерните устройства (след като натиснем бутона **DEVICE**) и съответно да имаме този изглед:

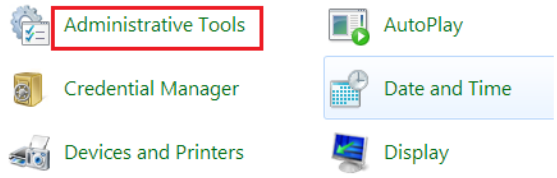


В този случай е необходимо да направим следните стъпки:

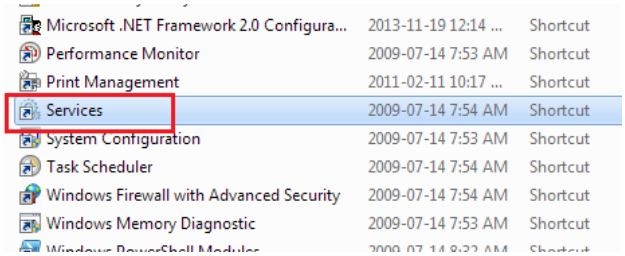
1. *Старт бутон на Window - Control Panel*



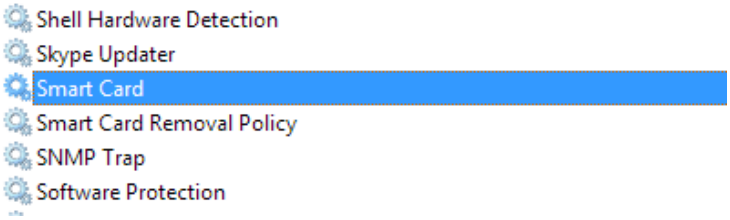
2. *Отворете Administrative Tools*



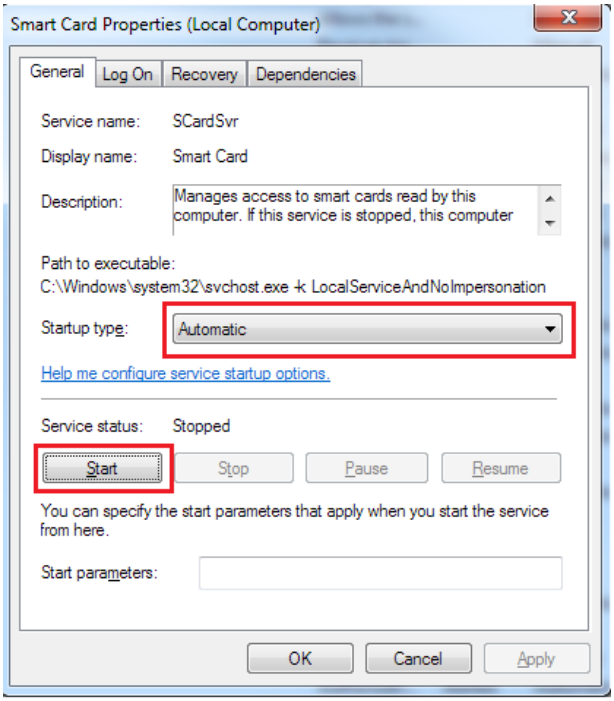
3. *Отворете Services*



4. *Двоен-клинк на Smart Card сервиза*



и го настройваме по следния начин - Startup type as “Automatic”, Service status as “Start”.



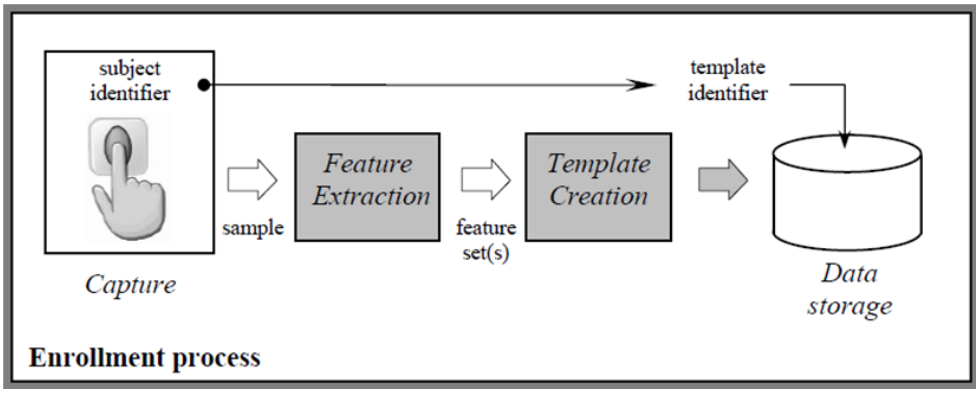
5. *Стартирайте отново демо програмата.*

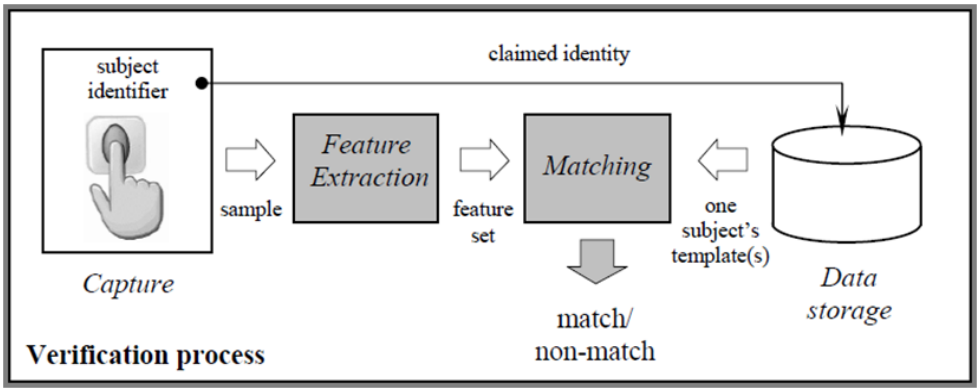
CB1000F Demo

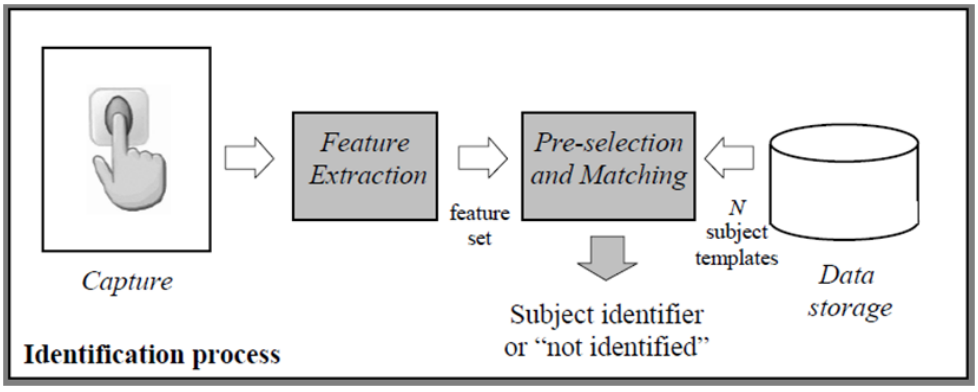
Демо програмата демонстрира основните процеси при функционирането на системи базирани на биометрични (пръстови отпечатъци) данни.

Типовете биометрични системи са индентифициращи и верифициращи. Разликата между двете е комплекта от шаблони за сравнение - при идентифициращите броя шаблони е неопределен (зависи от алгоритъма за търсене), а при верифициращите е точно един.

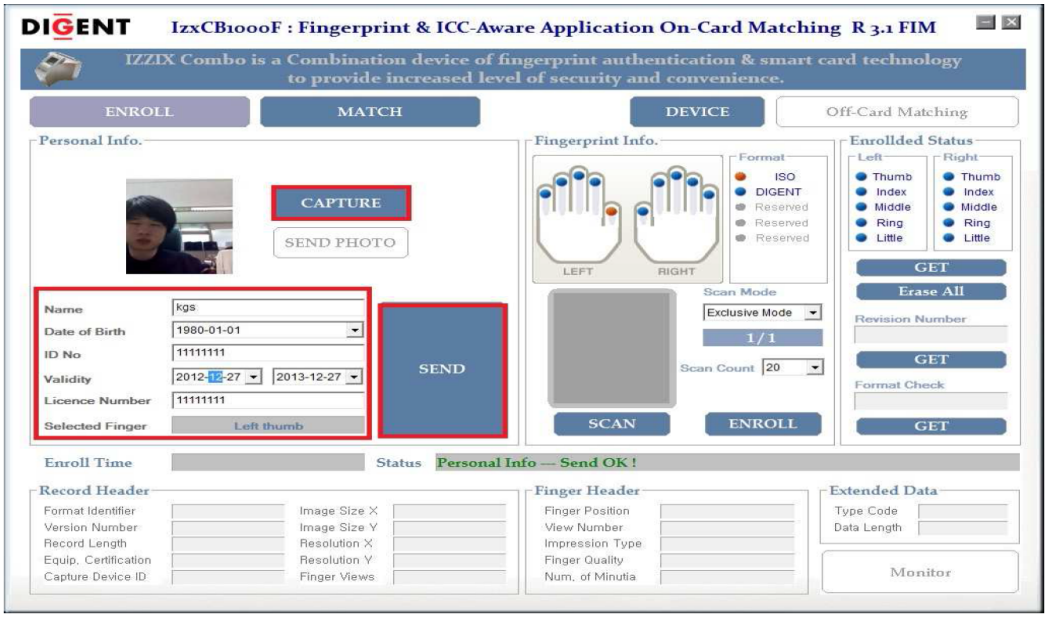
Без значение от типа система основните процеси са два - Enrollment (регистриране) и Matching (сравняване):







Демо програмата показва нагледно тези процеси. За да симулираме например процеса на Enrollment натискаме бутона **Enroll**, за да ни се появи екрана за регистрация



В секцията **Personal Info.** попълваме лична информация (имена, дата на раждане, снимка) и съответно може да се направи и снимка (ако ще се записва на smartcard-тата). След като сме готови с данните е необходимо да поставим smartcard в комбинирания четец и да натиснем бутона **SEND.**

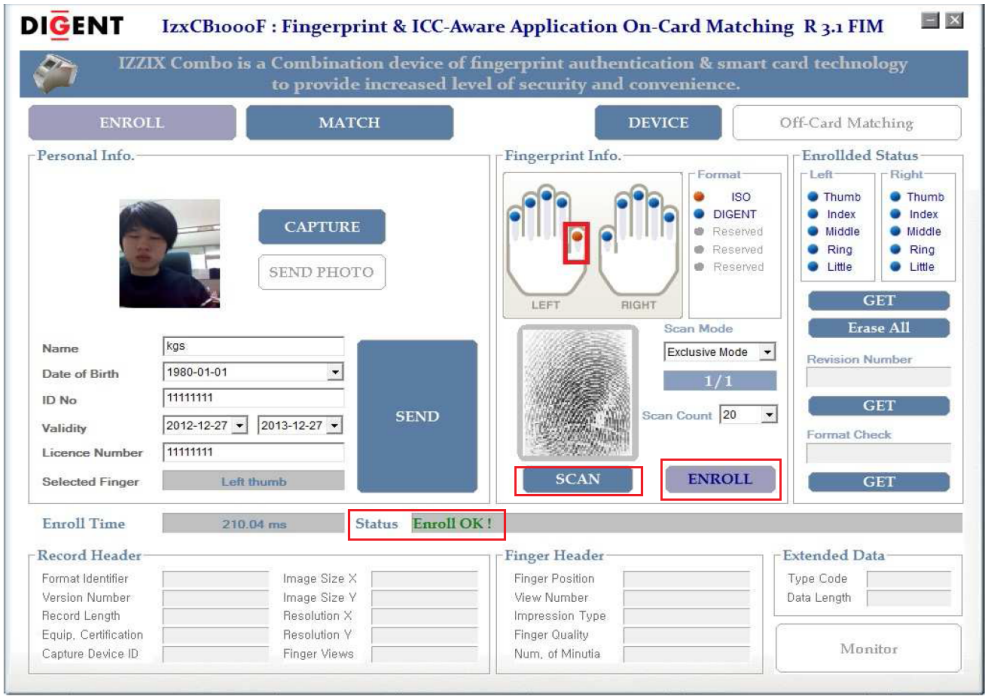


Ако записването е успешно ще получите съобщение в полето статус:



Забелецка: Ако възникне грешка - проверете как е поставена картата, типа карта, проблеми в следствие на некоректно инсталирани драйвъри или хардуерно устройство.

Следващата стъпка от регистрацията е да запишем данните за пръстовите отпечатъци на smartcard-тата.

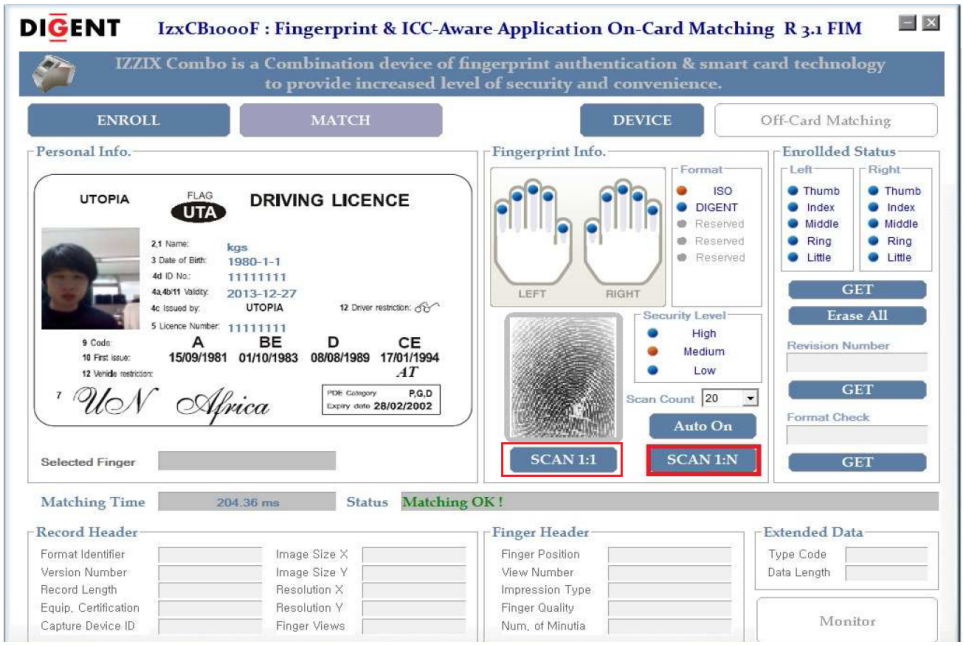


Избираме пръст, формат (ISO, DIGENT), брой последователни сканирания (за по-голяма сигурност при извличане на данни от пръстовия отпечатък) и когато сме готови с това поставяме съответния пръст на четеца и натискаме бутона **SCAN**. Когато приключим със сканирането/сканиранията натискаме бутона **ENROLL**, за да запишем данните на картата.

За проверим дали данните са коректно записани или какво е записано може да използваме секцията **Enrollded Status** и съответните бутони за това**.** В същия панел имаме и възможност да изчистим данните от smartcard-тата чрез бутона **Erase All**.

Панелите **Record Header**, **Finger Header**, **Extended Data** са помоюни за софтуерните разработчици.

След като сме направили регистрацията (Enrollment) и сме записали данните на картата е време да направим обратния процес - верификация/сравнение. За да видим екрана за сравнение, използваме бутона **MATCH.**



Демо програма предлага два варианта за верификация - съответно бутоните **SCAN 1:1** и **SCAN 1:N**. За целта поставяме вече регистрираната карта с данни и избираме един от двата бутона. Ако използваме бутона **SCAN 1:1** е необходимо да изберем точно определен пръст от картинката, защото се очаква верификацията да е 1 към 1. При другия вариант няма нужда изрично да се посочва пръст. В този случай може да кажем че се симулира процеса на идентификация (с тази разлика че не се идентифицира човек, а по-скоро пръст, но процеса е подобен). При успешно сравнение се показва съобщение **Matching OK!** и ако има лична информация запазена в картата се извлича и показва в секцията **Personal Info.**

Duo Pass (Access Control / Time & Attendance)



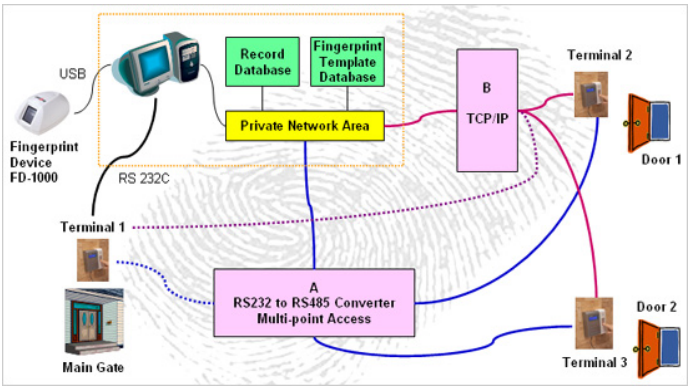


Описание на контролера

Duo PASS е хардуерно устройство, подходящо за контрол на достъпа. То е независимо, но също така предлага и отдалечен достъп до себе си по TCP/IP. Има вградена памет/базаданни на регистрираните потребители, RFID и четец на пръстови отпечатъци. Същото така разполага и вътрешен часовник, на база който може да записва времето на достъп. Чрез комбинация от PIN, RFID карта и пръстов отпечатък може да се постигне много добра сигурност на контрола на достъп - трифакторна автентикация (какво имам - RFID карта; кой съм - пръстов отпечатък, какво знам - password/pin code). Запазва до 8000 записа на достъп + време. RFID четеца е мулти-диапазонен от 125 KHz (RFID) до 13.56 MHz (NFC). Софтуера към устройството предоставя възможност за отдалечено извличане на логове и управление на самото устройство.

Забележка: за по-подробна спецификация на устройството
http://www.gobizkorea.com/catalog/product_view.jsp?blogId=lampustech&listStyle=A&objId=966026

Примерен вариант на конфигуриране



Управление на Duo PASS контролера

TODO Вкъщи ръководството

FM1000 Mouse



Чрез компютърната мишка FM1000, в която има вграден четец на пръстови отпечатъци и софтуера IZZIX Secure SE може да се демонстрира как е възможно да се допълни и подобри сигурността при използването на персонален компютър.

Софтуера в комплект с четеца (който е перфектно позициониран така че палеца да попада винаги върху него) разполага със следните по специфични функционалности:

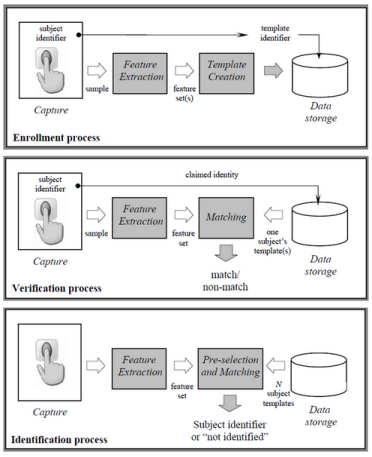
- Автентикиране в системата чрез пръстов отпечатък, отпечатък и парола (възможно е и резервен вариант в случай на инцидент да се автентикираме и стандартно с парола)

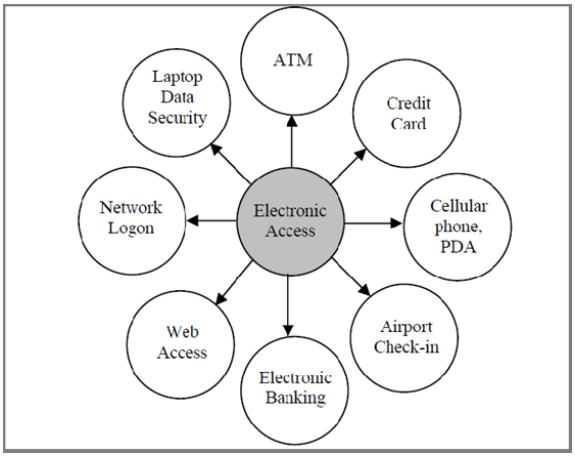
- Допълнителна сигурност при криптиране на файлове и папки като се използват и биометрични данни.

Повече детайли: http://www.digent.com/English/product/secure.htm

Задачи и упражнение за вкъщи

- Да се намери информация за сравнения на различни алгоритми за извличане на данни от пръстовите отпечатъци. Да се опишат предимства и недостатъци.
- Отново анализ на алгоритми, но този път за търсене в база или пък да се разгледат алтернативни начини на съхранение на пръстови отпечатъци. Да се разгледат съответно плюсовете и минусити.
- Анализ/ описание на четци на пръстови отпечатъци. Предимства и недостатъци. Може да се направи и сравнение на ценова база.
- Да се опишат процесите в една биометрична система и да се дадат примери за внедрени такива:





Вариант е тези задачи да се дадат една седмица по-рано, за да може студентите да се запознаят и да направят съответно презентации и да представят на останалите. След като направят теоритичното представяне, на следващите занятия може да се премине към пратическо упражнение и запознаване със устройствата и процесите описани в началото.