

Informationssicherheit

ID Device

Software Development Kit (SDK)

mit ActiveX Controls (optional)

Version 1.9

Kurzbeschreibung

Hinweis: Für weitergehende Informationen zum Einsatz des SDK's wenden Sie sich bitte an nachfolgende Adresse:

SIEMENS ICM RDC IS BIO

E-Mail: fingertip@mch.siemens.de

Internet: <http://www.fingertip.de/produkte/idmousesdk.asp>

Veröffentlicht von SIEMENS ICM RDC IS BIO PM

Hofmannstr. 51, D - 81379 München

Einleitung

Die vorliegende Beschreibung des ID Device SDK ist an alle Benutzer, Entwickler und Integratoren von biometrischen Systemen gerichtet, welche die Siemens/Cherry/ST ID Produkte als Fingerprint-Device in ihre Anwendungen integrieren möchten. Für die Nutzung des ID Device SDK wird die Handhabung der Betriebssysteme Windows 98, Windows 2000, Windows NT 4.0 (nicht für das ST Device !) oder Windows XP vorausgesetzt. Zusätzliches biometrisches Wissen ist nicht erforderlich.

Das ID Device SDK 1.9 ist deviceunabhängig und unterstützt über Gerätekennung ausschließlich nachfolgende ID Produkte (Devices):

- Siemens ID Mouse A10
- Siemens ID Mouse professional
- Cherry ID Keyboard
- ST Microelectronics TouchChip® Fingerprint Reader

Durch Vorselektion bei der Installation werden deviceabhängig entweder die Treiber für die USB ID Mouse, die Treiber für die USB Cherry Tastatur oder die Treiber für den ST TouchChip® Fingerprint Reader geladen.

Kurzbeschreibung

Das ID Device SDK ist gedacht, um die biometrischen Erkennungsmechanismen der Siemens ID Technologie in verschiedenste SW-Anwendungen zu integrieren.

Es enthält die Siemens Fingerprint-Erkennungsfunktionen zur Erweiterung von Kundenapplikationen unter dem Aspekt „Erhöhung der Sicherheit“ wie auch unter dem Aspekt „easy to use“.

Im einfachsten Fall können herkömmliche Paßwörter und PINs über Fingerreferenzdaten adressiert und zurückgewonnen werden, um dann entsprechende Freischaltungen durchzuführen.

Das ID Device SDK umfaßt Funktionen für den Einlernvorgang einer Person ins System (Enrollment), zur Aktualisierung und Verbesserung von Referenzdaten im Archiv, Funktionen zur Verwaltung von Archiv und personenspezifischen Daten und die Basisfunktionen die zur Identifikation bzw. Verifikation einer Person notwendig sind.

Aufgrund der Modularität des ID Device SDK ergeben sich unterschiedlichste Möglichkeiten die vorhandenen Funktionen zu verwenden. Man unterscheidet zwischen 2 Gruppen von Benutzern. Eine Gruppe davon sind die Systemintegratoren, die das ID Device SDK in ihr eigenes System einbinden und eine eigene Applikation erstellen. Diese Gruppe sind typische Windows Programmierer, die kein biometrisches Spezialwissen benötigen. Die zweite Gruppe ist die der biometrischen Integratoren, die das ID Device SDK und deren biometrischen Funktionen zur Ergänzung/Erweiterung ihrer Sicherheitsapplikationen integrieren wollen.

Die Programmbibliothek des ID Device SDK kann von mehreren Applikationen gleichzeitig benutzt werden; die Funktionen werden über Standard C Funktionsschnittstellen aufgerufen.

Ein Integrator kann die ID Devices über das SDK als reines Bildaufnahmeggerät für Fingerabdrücke verwenden. Diese Bitmap-Fingerbilder können über andere biometrische Fingerprint-Verfahren zur Authentisierung benutzt werden, sofern solche dem Integrator zur Verfügung stehen. In diesem Fall besteht nach der Bildaufnahme keine weitere Unterstützung durch das ID Device SDK, weder für Enrollment und Verifikation noch für die

Archivierung der Fingerdaten. Bei Verwendung von Algorithmen außerhalb des ID Device SDK übernimmt der Integrator die Verantwortung für die Funktion und Qualität des biometrischen Systems.

Zusammenhang Biometrie und biometrische Algorithmen des ID Device SDK's

Das Siemens ID Device SDK ermöglicht es auf einfache Weise vorhandene Applikationen um biometrische Sicherheit zu erweitern. Biometrie allgemein bedeutet die Prüfung der Personenidentität mit Hilfe von eindeutigen personenspezifischen Merkmalen. Diese Merkmale können von physiologischen Verfahren wie Gesichts- und Fingerbildererkennung oder von verhaltensgesteuerten Verfahren wie dynamischer Unterschriftenerkennung oder Sprecherverifikation stammen. Im Gegensatz zu Identifikationsmerkmalen wie Schlüssel oder Smartcards können biometrische Merkmale nicht verloren, gestohlen oder durch unbefugte Personen benutzt werden.

Es gibt grundsätzlich 3 Prozesse in jedem biometrischen System:

1. Enrollment

In diesem Prozeß werden die Referenzdaten einer Person erzeugt. Diese Referenzdaten enthalten die grundlegendsten Informationen über die biometrischen Merkmale einer Person. Das sind im Falle des ID Device SDK die fingerspezifischen Merkmale. Während der nachfolgenden Identifikations- und Verifikationsvorgänge im biometrischen System werden diese Referenzdaten zum Vergleich mit aktuellen Merkmalen herangezogen. Für den Einlernvorgang wird die jeweilige Person aufgefordert, den ausgewählten Finger 3 mal aufzulegen.

2. Verifikation

Verifikation bedeutet die Überprüfung der Person mit der vorgegebenen Identität d.h. es wird die Aussage „Ich bin “ überprüft. Das bedeutet, dass die Identität der zu vergleichenden Person vor dem Start des Verifikationsprozesses angegeben werden muß. Dies kann als Beispiel durch die Angabe des Personennamens oder einer User ID oder durch die Verwendung einer Chipkarte durchgeführt werden.

3. Identifikation

Identifikation bedeutet, das biometrische System überprüft die Identität der Person durch Vergleichen mit allen Personen, die dem System bekannt sind. D.h. es wird nicht die Identität der zu überprüfenden Person vor dem Start der Identifikation angegeben, sondern als Ergebnis bei erfolgreicher Identifikation geliefert.

Das nachfolgende sehr vereinfachte Diagramm stellt den sequentiellen Ablauf der Fingerabdruck-Erkennungsalgorithmen dar. Die Hauptkomponenten sind dabei Encoder und Matcher. Der Encoder ist zuständig für die Extraktion der fingerspezifischen Merkmale, der Matcher vergleicht die aktuellen fingerspezifischen Merkmale (Anfrage) mit denen der gespeicherten Referenz.

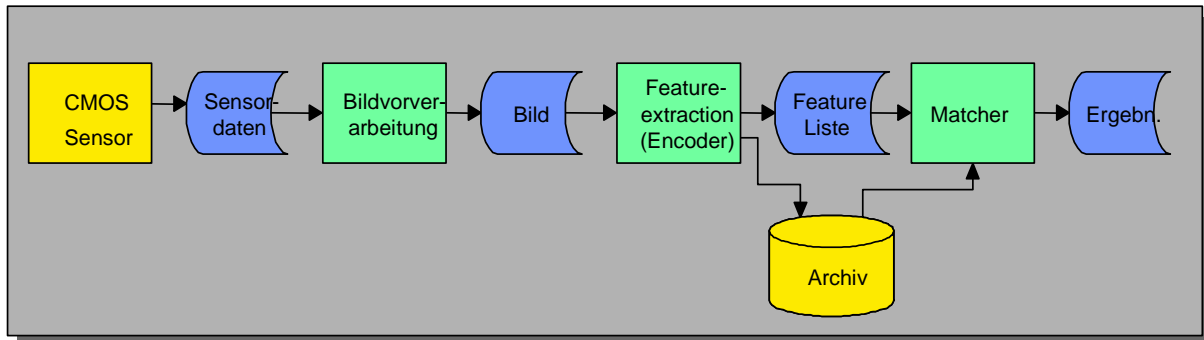


Abbildung 1: Prozeßablauf im ID Device SDK

Umfang des ID Device SDK

Das ID Device SDK besteht aus den folgenden 3 Komponenten:

1. CD ROM ID Device SDK mit:
 - Siemens Demonstration Suite
 - Beispielcode
 - Installationsprogramm
 - Benutzerdokumentation
2. Siemens ID Mouse oder Cherry ID Keyboard
3. CD-ROM ID Device SW 4.0 (optional) mit:
 - Installationsprogramm
 - Benutzerdokumentation

Das ID Device SDK ist eine statisch ladbare Dynamic Link Library (DLL) mit definierten C-Schnittstellen. Das Demoprogramm vermittelt dem Benutzer in graphischer Form einen ersten Eindruck über den Funktionsumfang des ID Device SDK. Das Demoprogramm ist einfach zu benutzen und selbsterklärend. Der Beispielcode enthält typische Aufrufe aller notwendigen ID Device SDK Funktionen.

Zur Nutzung des ID Device SDK werden dem SW-Integrator ein Benutzerhandbuch und ein Programmierhandbuch zur Verfügung gestellt.

Aufbauend auf dem ID Device SDK kann der Anwender eigene Applikationen entwickeln und vertreiben.

Inbetriebnahme des ID Device SDK 1.9

Systemanforderungen

Für die Nutzung des ID Device SDKs und für die Entwicklung von biometrischen Anwendungen mit dem ID Device SDK sowie für den Aufruf des Demoprogrammes sind folgende Voraussetzungen notwendig:

Hardwareanforderungen

- PC mit INTEL Pentium Prozessor ab 233 MHz, Monitor mit minimaler Auflösung von 800x600 Pixel, mindestens 64MB Hauptspeicher
- USB Anschluß
- Siemens ID Mouse, Cherry ID Keyboard oder ST TouchChip® Fingerprint Reader wahlweise

Softwareanforderungen

- Betriebssystem Windows 98, Windows 2000, Windows NT 4.0 ab SP3 (ST Device nicht möglich !), Windows XP
- ID Device SDK Softwarepaket installiert
- Microsoft Visual Studio 6.0 (oder andere kompatible Tools) als Entwicklungstool

Installationsprozeß

1. Siemens ID Mouse, Cherry ID Keyboard oder ST TouchChip® Fingerprint Reader an den USB Anschluß des PC's anstecken.
2. Farbauflösung des Bildschirmes auf mehr als 256 Farben und Bildschirmauflösung auf mindestens 600 x 800 einstellen.
3. ID Device SDK Installations - CD ins CD ROM Laufwerk einlegen und „Setup.exe“ starten und den Installationshinweisen folgen. Das Setup installiert das ID Device SDK in das ausgewählte Zielverzeichnis. Falls notwendig, Rechner neu starten.

Architektur des ID Device SDK

Die nachfolgende Architekturdarstellung stellt den Zusammenhang des ID Device SDK mit Kundenapplikationen und der Siemens ID Mouse dar. Weiter wird in einer einfachen Form die interne Komponentenstruktur dargestellt. Als biometrisches Eingabedevise kann ebenfalls das Cherry ID Keyboard angeschlossen sein.

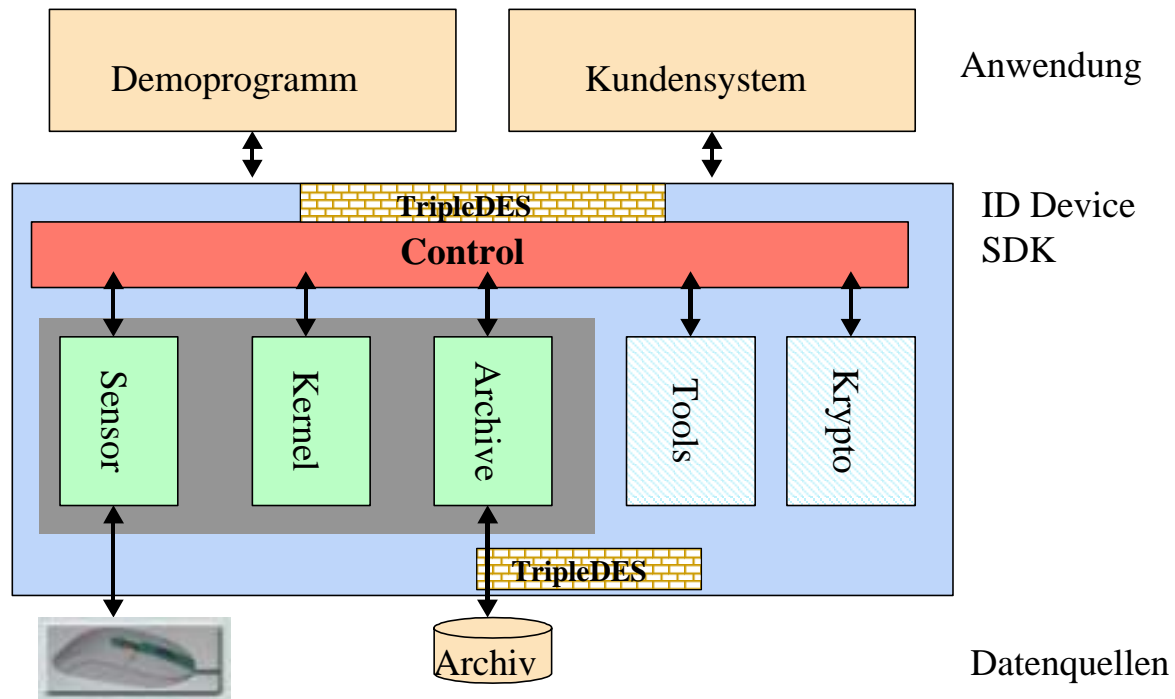


Abbildung 2: Architektur des ID Device SDK

- Komponente "Control"**
 Diese Komponente enthält die Steuerung sämtlicher Funktionen des ID Device SDK und stellt die funktionalen Schnittstellen für die Kommunikation nach außen zur Gesamtanwendung zur Verfügung.
- Komponente „Kernel“**
 Diese Komponente enthält alle Basisfunktionen zur Verarbeitung von Fingerabdrücken.
- Komponente "Sensor"**
 Diese Komponente dient zur Steuerung der Fingertip-Sensorik in den Hardwareeinheiten ID Mouse und Cherry ID Keyboard und liefert ein vollständig gelesenes Bild mit Korrekturen vom FingerTIP™ Sensorchip.
- Komponente "Archive"**
 Diese Komponente enthält Funktionen zum Speichern, Löschen und Lesen von Benutzerdaten bzw. biometrischen Daten aus einem Archiv.
- Komponente "Tools"**
 Diese Komponente stellt Hilfs- und Verwaltungsfunktionen zur Verfügung, die von den übrigen Komponenten verwendet werden können.

- **Komponente "Krypto"**

Diese Komponente stellt Funktionen zur Verschlüsselung bzw. Entschlüsselung und zur Erzeugung von Signaturen für die im ID Device SDK Archiv gespeicherten Referenzdaten zur Verfügung.

Funktionsumfang des ID Device SDK

Sensor Management Funktionen

Diese Gruppe von Funktionen dient zur Aktivierung und zum Test des FingerTip™ Sensors, der in die ID Devices integriert ist. Sie steuern die Kommunikation zum Sensor und ermöglichen das Einlesen von Fingerprint-Rohbildern, die zur Anzeige bzw. zur Erzeugung von Referenzdaten verwendet werden. Diese Funktionen können unabhängig von den Biometrischen Funktionen verwendet werden.

Biometrische Funktionen

Diese Gruppe von Funktionen bilden den Kern des ID Device SDKs und enthalten die Mechanismen zur Erzeugung von biometrischen Daten aus Fingerprint Rohbildern (Encoder) und die Algorithmen für den Vergleich dieser biometrischen Daten mit Referenzeinträgen im Archiv (Matcher). Diese Grundfunktionen sind die Basis für die Identifikation bzw. für die Verifikation einer Person.

Die Erzeugung und Verbesserung von Fingerreferenzdaten kann einerseits durch Encodierung des vom Sensor eingelesenen Rohbildes erfolgen oder durch Übergabe von Bitmap. Dateien aus externen Datenbanken und anschließender Verarbeitung im SDK stattfinden.

Die Verifikation einer Person wird in 2 Ausprägungen unterstützt. Einerseits erfolgt die Verifikation (1:1 Vergleich) durch Korrelation der aktuell aufliegenden Fingerreferenz mit einem Referenzeintrag im SDK-Archiv, der über eine Finger ID aus einer Vielzahl von Archiveinträgen eindeutig adressiert ist. Andererseits werden beim Aufruf des Verifikationsprozesses die zu vergleichenden Referenzdaten durch die Applikation mit übergeben (z.B. ausgelesen aus einer Smartcard) und mit dem aktuell aufliegenden Fingerbild verglichen, dabei muß kein internes SDK-Archiv existieren, die Referenzdaten werden durch die Applikation verwaltet und bei Bedarf durch entsprechende Funktionsaufrufe dem SDK zur Verfügung gestellt. Aufgrund der Modularität des SDKs können Referenzdaten von Fingern auf Smartcards und innerhalb von Client- und Serverplattformen beliebig gespeichert und von dort durch die Applikation zurückgewonnen werden, so daß eine Vielzahl von Smartcard Anwendungen bzw. Client- /Server-Anwendungen kundenspezifisch realisiert werden können.

Archiv Management Funktionen

Diese Gruppe enthält alle notwendigen Funktionsaufrufe zur Verwaltung des Archivs wie z.B. das Löschen von Fingereinträgen, das gezielte bzw. sequentielle Lesen von Personendaten und das Ändern von spezifischen Nutzerdaten (Paßwörter, etc.).

Anmerkung:

Im ID Device SDK wird keine Personenverwaltung angeboten. Referenzdaten, die im ID Device SDK Archiv verwaltet werden sind Finger orientiert, d.h. bei entsprechender Erkennung wird eine Finger ID zurückgemeldet. Der Zusammenhang zwischen gespeicherten Referenzdaten (Finger) und zugehöriger Person muß durch die Applikation hergestellt werden.

Hilfs- und Verwaltungsfunktionen

Diese Gruppe von Funktionen stellt Hilfsfunktionen für das Lesen bzw. Speichern von Bitmap-Dateien und Funktionen zur Umwandlung von Referenzdaten (Biodaten) in vordefinierte Datenformate zur Verfügung.

Über weitere Funktionen werden beispielsweise Speicherfreigaben angefordert bzw. Fehlerklartexte durch Angabe von Fehlernummern zurückgeliefert.

Verschlüsselung

Die im Archiv gespeicherten Referenzdaten und Daten zwischen Funktionsaufrufen werden mit TripleDES mit 128 Bit Schlüssellänge verschlüsselt und signiert. Damit können diese Daten von keiner anderen Anwendung ausspioniert, verändert oder vorgetäuscht werden, selbst wenn diese Daten auf einem externen Server oder auf einer Smartcard abgelegt werden. Die Kundenapplikationen sind für die Übertragung der biometrischen Daten zwischen Client und Server, als auch für die Speicherung auf einem Server oder einer Smartcard, verantwortlich.

Zusammenhang mit biometrischen Standards

Das ID Device SDK orientiert sich an den biometrischen Standards Human Authentication API (HA-API) V2.0 und Biometric API (BAPI) V1.1.

Kompatibilität zu früheren Versionen

Applikationen, welche mit früheren ID Device SDK Versionen entwickelt wurden, benötigen nur geringe oder keine Anpassungen. Bisher bereits bekannte Funktionen bleiben im Aufruf gleich, so daß keine Sourceänderungen in der Applikation notwendig sind. Neue hinzugekommene SDK Funktionen können durch Implementierung in der Applikation genutzt werden.

Alte Fingerprintarchive (SDK 1.6) sind wegen der Devicebindung, Verschlüsselung und Algorithmen-Upgrade nicht mehr nutzbar, d.h. neues Einlernen (Enrollment) der Personen ist notwendig.

Wurde auf Registry-Einträge lesend oder schreibend zugegriffen, muß der Pfad von „...\ ID Device SDK\1.50/1.60/1.80...“ zu„...\ID Device SDK\1.90...“ geändert werden.

Neuerungen/Verbesserungen des ID Device SDK 1.90 gegenüber den Vorgängerversionen (1.6/1.8)

- Treiber für Siemens ID Mouse A10/Professional, Cherry ID Keyboard und ST Micro-electronics TouchChip® Fingerprint Reader (ST TCRS1 Smart Card Reader)
- ID Converter als Extratool zur Umsetzung von Templates /Bio-Daten zwischen ID Devices (Mouse, Keyboard, ST), TopSec ID Modulen (embedded Siemens-Lösung) und Siemens Matching on Card (Smart Card Technologie) in allen Richtungen
- Live Matching Funktionalität für bessere Benutzerführung während der Bildaufnahme (Capture), damit ist eine flexible Steuerung der Authentisierung möglich, was zur weiteren Erhöhung der Erkennungs-Performanz führt.
- Multiple Sensor Device Unterstützung, d.h. es können verschiedene Geräte (Mouse, Cherry, ST) an einem PC benutzt werden.

- Verbesserung der Sicherheitsarchitektur innerhalb des SDK's
- Unterstützung von Windows XP
- Freie Einstellbarkeit der biometrischen Schwellenwerte für fortgeschrittene biometrische Anwendungen.
- Unterstützung der Siemens „Matching on Card“ Technologie
- Integration der Siemens FT Technologie Version 11.0 mit verbesserten Algorithmen für erhöhte biometrische Performanz.
- Verbesserung des Feedbacks beim Enrolment-Prozess
- Prematching Funktion für kürzere Matchzeiten

Zusätzliche Software für das ID Device SDK 1.90 (optional)

ActiveX Controls für einfache Integration in die Applikation und anspruchsvolles „Look and Feel“

Die ActiveX Komponenten, aufbauend auf dem SDK 1.9, ermöglichen die einfache Integration in eine Applikation und Übernahme des „Look and Feel“ der ID Mouse Professional Software. Es werden englische und deutsche Sprachversionen unterstützt.

Die ActiveX DLL beinhaltet die komplette Funktionalität der FAPI.DLL. Die Komponenten werden während des Setup registriert.

Die Abbildung 3 zeigt die grundlegende Architektur des ActiveX.

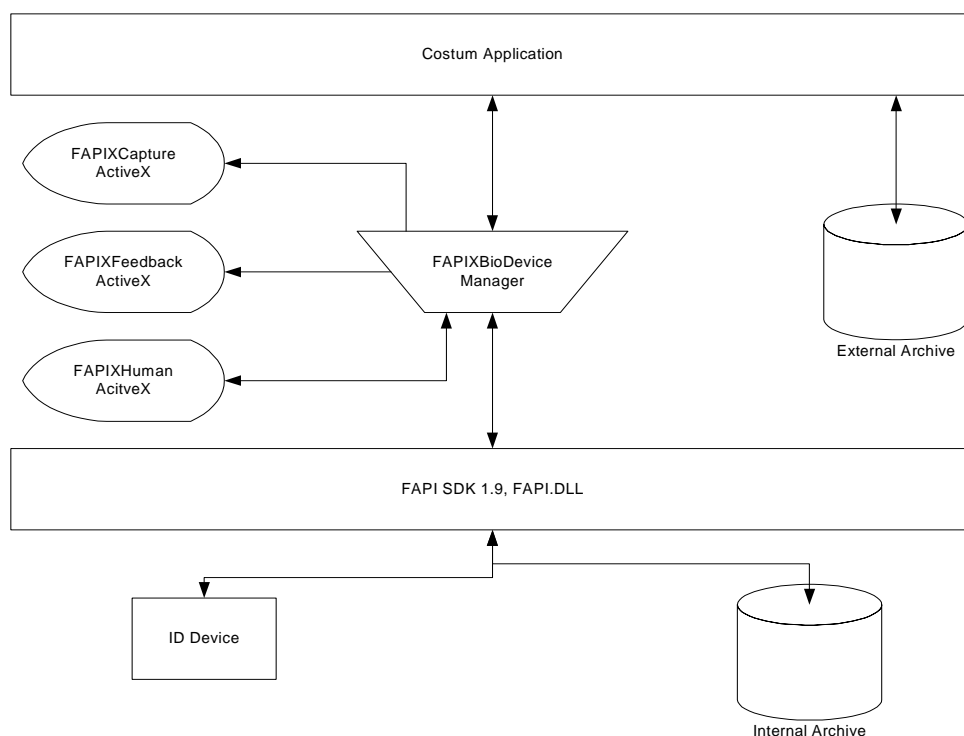


Abbildung 3: Architektur des ID Device SDK 1.9/ ActiveX

ActiveX Komponente - FAPIXCapture

Die Komponente FAPIXCapture erhält die Daten vom FapiXBioDeviceManager und stellt das Sensorbild des ID Sensors dar. Sowohl das Hintergrundbild (z.B. Firmenlogo), als auch die Bildgröße sind veränderbar. Zusätzlich kann eine Textbox unterhalb des Bildes verwendet werden, um Bildinformationen anzuzeigen. Es besteht auch die Möglichkeit, das Sensorbild als Bitmap – Datei abzuspeichern.



Abbildung 4: FAPIXCapture Control

ActiveX Komponente – FAPIXFeedback

Dieses ActiveX Control evaluiert die Feedback Information vom SDK 1.9 während des Enrolment/Capture Prozess und zeigt die Animationen (wie z.B. "Bitte legen Sie den Finger auf den Sensor", ...) oder andere Bilder (siehe Siemens Biometrics Demonstation Suite).



Abbildung 5: FAPIXFeedback

ActiveX Komponente – FAPIXHuman

Diese Komponente dient zur Auswahl der Finger für den Enrolment – Vorgang. Die Daten werden zum FAPIXBioDeviceManager gesendet bzw. notwendige Information vom FAPIXBioDeviceManager erhalten. Enrollte Finger werden mit grüne Knöpfe gekennzeichnet, ausgewählte Finger mit einem blauen Pfeil markiert. Optional können die Finger auch mit rote Knöpfe versehen werden (“manipulierte Finger”).

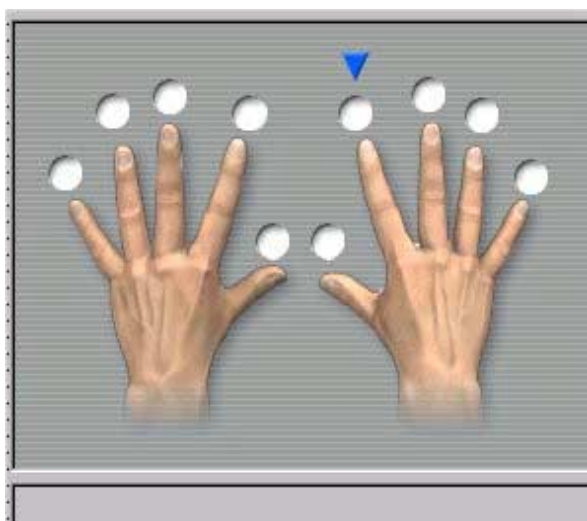


Abbildung 6: FAPIXHuman Control

Beispiel Code: Verify - Identify - Enrolment

Der Beispiel – Code zeigt, wie die Verifikation/Identifikation/Enrolment zu programmieren ist und kann für die Applikation verwendet werden. Zusätzlich sind Beispiele für die restlichen Controls enthalten.

Hardware und Software Anforderungen

Hardware Anforderungen

- min. PC Pentium II 233 Mhz
- min. 64 MB RAM
- USB port
- CD Rom

Windows NT, 2000, XP:

- Siemens ID Mouse inclusive FingerTIP I sensor
- Siemens ID Mouse Professional inclusive FingerTIP I sensor
- Cherry FingerTIP ID Board inclusive FingerTIP I sensor,

Windows 2000, XP:

- ST Microelectronics TCRS1A Touch Chip Device

Hinweis: Windows NT wird vom ST Device nicht unterstützt.

Software Anforderungen

- Betriebssystem
 - Windows 2000 SP2 oder höher
 - Windows NT 4.0 SP6 oder höher (ST Device nicht unterstützt !)
 - Windows XP
- Adobe Acrobat Reader 4.0 oder höher (für Dokumentation)
- ID Device SDK 1.90

Literaturverweis:

[1] ID Device SDK User's Guide

[2] ID Device SDK Programmer's Guide

[3] ID Device SDK / ActiveX Programmer's Guide

[4] Data Book FingerTIP™ CMOS Chip and System, Infineon Technologies AG

Support:

Im Kaufpreis des ID Device SDK sind 4 Stunden Integration-/SDK-Support mit enthalten.