

Positive Probenidentifikation

Patrick Gleichmann (532508) und Peter Krausgrill (232504)
Laborautomation WS 2002/2003

1. KOMPONENTEN	2
<i>Hardware</i>	2
<i>Software</i>	2
<i>Delphi Komponenten</i>	2
2. SIMULATION.....	3
2.1 <i>Hinweis</i>	3
2.2. <i>Das Hauptfenster</i>	3
2.3. <i>Der Simulationsablauf</i>	4
2.4. <i>Chaining von Informationen</i>	6
2.5 <i>Manipulation</i>	7
3. DATENBANK	8
3.1. <i>ERM</i>	8
3.2. <i>Files</i>	8
3.3. <i>Erläuterung von erklärungsbedürftigen Attributen</i>	9
<i>Messages</i>	9
4. DONGLE DLL	10
4.1. <i>Übersicht</i>	10
4.2. <i>Die exportierten Funktionen</i>	10
5. VERSCHIEDENES	11
5.1. <i>Barcode Scanner</i>	11
5.2. <i>CMS</i>	11

1. Komponenten

Hardware

- Rainbow iKey 1000
[<http://www.rainbow.com/ikey/ikey1000.html>]
- HHP IMAGETEAM 4410 Barcode Scanner
[<http://www.hhp.com/hhp/products/product.tpl?prodsku=67863248676413>]

Software

- Microsoft Windows XP
[<http://www.microsoft.com/windowsxp>]
- Apple Mac OS X 10.2
[<http://www.apple.com/downloads/macosx>]
- Borland Delphi 6/7
[<http://www.borland.com/delphi/index.html>]
- Borland C Compiler 5.5
[<http://info.borland.com/techpubs/borlandcpp>]
- iKey SDK (inkl. Treiber)
[Nur auf CDR erhältlich]
- Apache HTTP Server 1.3
[<http://httpd.apache.org>]
- PHP 4
[<http://www.php.net>]
- MySQL 3.2
[<http://www.mysql.com>]
- Apple September 2002 Devkit (gcc 3.1, ProjectBuilder, InterfaceBuilder)
[<http://www.apple.com/developer/>]

Delphi Komponenten

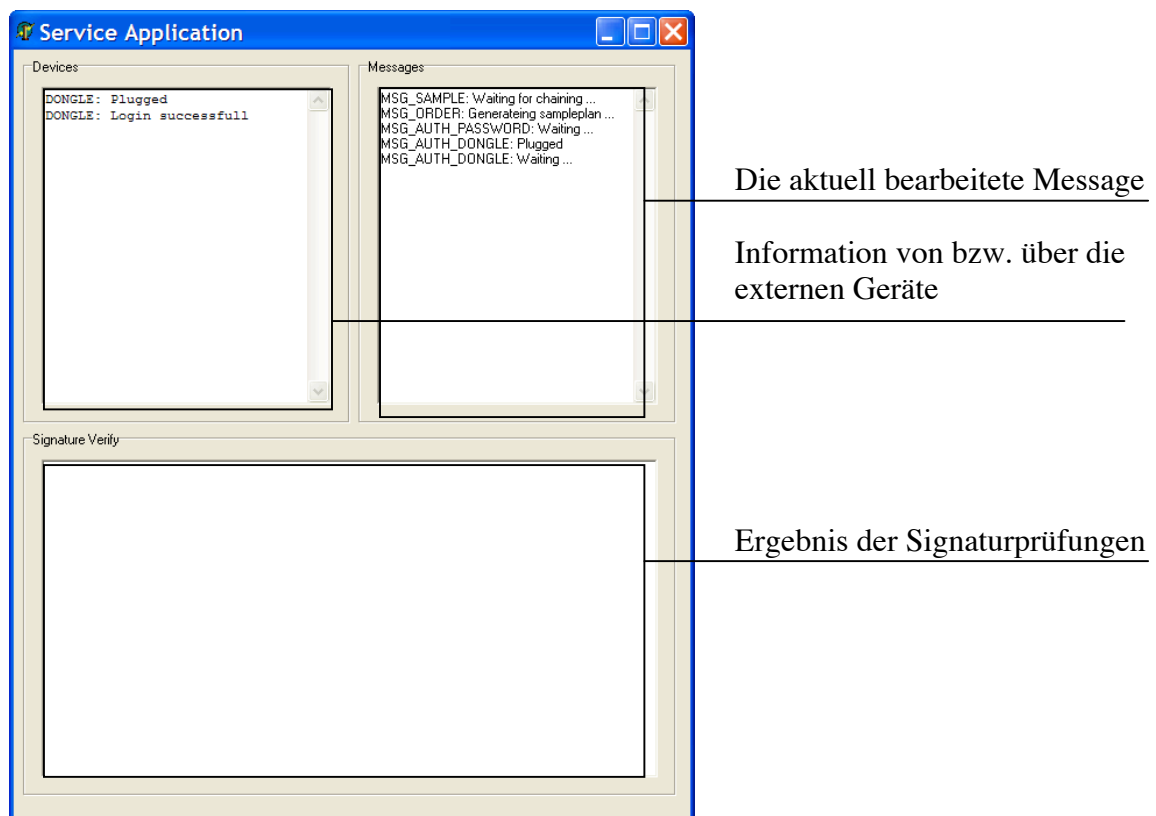
- CiaComPort
[<http://www.mestdagh.biz/>]
- RDataMatrix
[http://www.java4less.com/delphi_barcodes.html]

2. Simulation

2.1 Hinweis

Die Applikation ist als reine Simulation ausgelegt, d.h. sie folgt immer einen linearen Verlauf. Es können also nicht gleichzeitig mehrere Order aufgegeben werden. Eine weitere Beschränkung ist, das es nur einmal läuft, was aber zur Demonstration ausreicht.

2.2. Das Hauptfenster



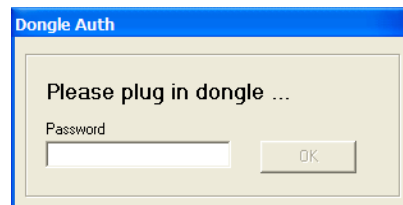
Im Hauptfenster wird der interne Ablauf sichtbar gemacht. Bei einer realen Anwendung bliebe dies dem Benutzer versteckt.

2.3. Der Simulationsablauf

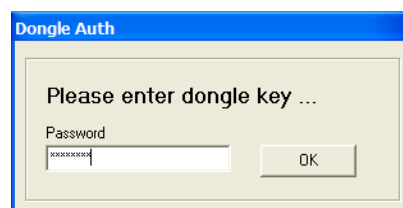
SAP/MM, SAP/QM bzw. Prozeßplan

- 1.) Der Dongle muß eingesteckt werden um sich zu authentifizieren.

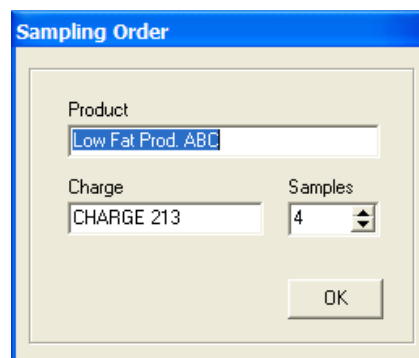
Hinweis: Zieht man zu einem späteren den Dongle ab, so beginnt man wieder bei diesem Schritt.



2. Um auf den private Key und die Software zugreifen zu können, muß nun der Dongle Schlüssel („Passwort“) eingegeben werden.
In unserem Fall die „12345678“.



3. Es wird eine Order festgelegt.
Dazu spezifiziert man ein Produkt, eine Chargenbezeichnung und die Anzahl der Proben („Samples“), die gezogen werden sollen.



Probennehmer

4. Aus einem Container, z.B. gefüllt mit TG-Ware, werden Proben genommen. Es wird also die ID des Containers mit denen der Probengefäße verknüpft.

Nun muß der Ablauf im Abschnitt

→ Chaining von Informationen (2.4)

durchgeführt werden.

Die Parameter sind:

Elternknoten = Container
Kinderknoten = Probengefäße

5. Wenn man nun ein beliebiges (Sub-) Sample scannt ...

The screenshot shows a software dialog box titled "Laboratory". It is divided into three main sections: "Label", "Sample Information", and "Sample splitting". In the "Label" section, there is a square placeholder for a QR code, an "ID" label next to an empty text input field, and a "Title" label next to another empty text input field. The "Sample Information" section is currently empty. The "Sample splitting" section features a dropdown menu with the value "0" and a button labeled "split".

6. ... bekommt man die gesamte verfügbare Information, inkl. der Hierarchie, angezeigt.

In diesem Dialog hat man auch die Möglichkeit das akt. Sample zu teilen. Man legt einfach die Anzahl der Sub-Samples fest und sendet den Auftrag mittels "split".

Der darauf folgende Ablauf ist analog zum Probennehmen und ist wieder in

→ Chaining von Informationen (2.4)

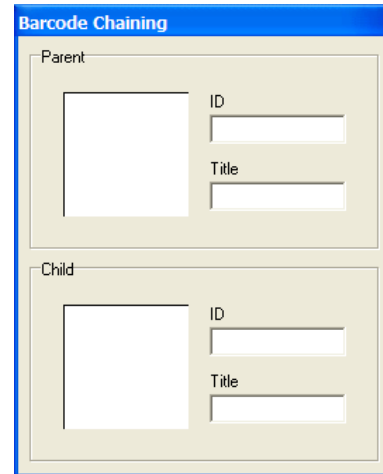
beschrieben.
Parameter:

Elternknoten = Sample
Kinderknoten = Sub-Sample

This screenshot shows the same "Laboratory" dialog box after a scan. The "Label" section now contains a QR code, the "ID" field is populated with "00020501", and the "Title" field is populated with "SAMPLE 1". The "Sample Information" section displays a hierarchical tree structure with the following items: "Low Fat Prod. ABC" (with a minus sign), "CHARGE 213 - A1000001" (with a minus sign), and "SAMPLE 1 - 00020501" (with a minus sign). The "Sample splitting" section now has a dropdown menu set to "2" and the "split" button.

2.4. Chaining von Informationen

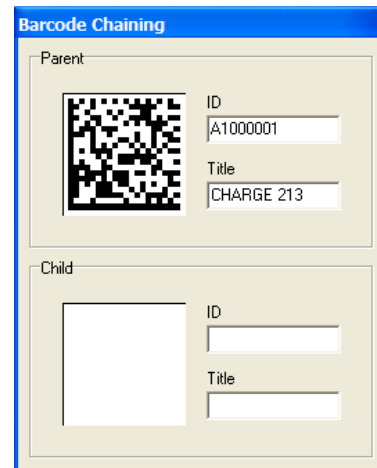
1. Zunächst muß der Elternknoten, d.h. (Sub-) Sample bzw. Container vor der Teilung, gescannt werden.



The screenshot shows a software window titled "Barcode Chaining". It is divided into two sections: "Parent" and "Child". Each section contains a square area for a barcode and two input fields labeled "ID" and "Title". In this step, all fields are empty.

2. Der gescannte Knoten erscheint im oberen Bereich. Es wird der Barcode, die ID und der Titel („Title“) angezeigt.

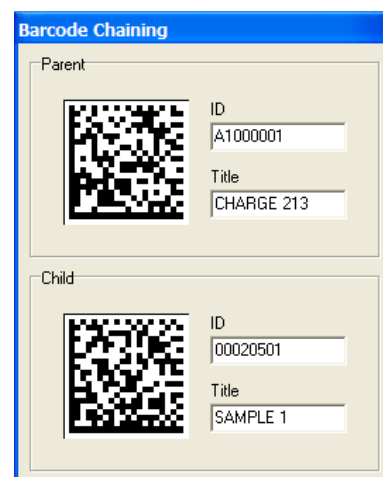
Jetzt muß der Barcode eines der Kinderknoten, d.h. (Sub-)Sample, gescannt werden.



The screenshot shows the "Barcode Chaining" window. The "Parent" section now contains a QR code, the ID field is filled with "A1000001", and the Title field is filled with "CHARGE 213". The "Child" section remains empty.

3. Beide IDs sind nun miteinander verknüpft. Die Informationen des Kindknoten werden unter der des Elternknotens angezeigt.

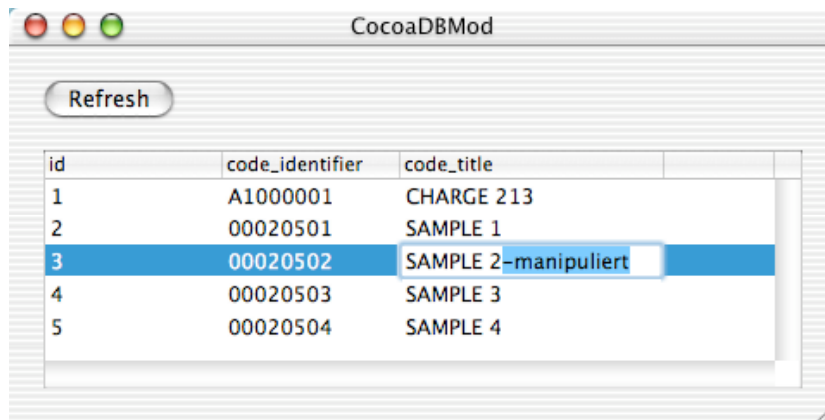
Soll mehr als ein Kindknoten mit dem Elternknoten verknüpft werden, so ist Schritt 2. zu wiederholen.



The screenshot shows the "Barcode Chaining" window. Both the "Parent" and "Child" sections now contain QR codes and filled-in fields. The "Parent" section has ID "A1000001" and Title "CHARGE 213". The "Child" section has ID "00020501" and Title "SAMPLE 1".

2.5 Manipulation

Externe Manipulationen:



The screenshot shows a window titled "CocoaDBMod" with a "Refresh" button and a table with the following data:

id	code_identifier	code_title
1	A1000001	CHARGE 213
2	00020501	SAMPLE 1
3	00020502	SAMPLE 2-manipuliert
4	00020503	SAMPLE 3
5	00020504	SAMPLE 4

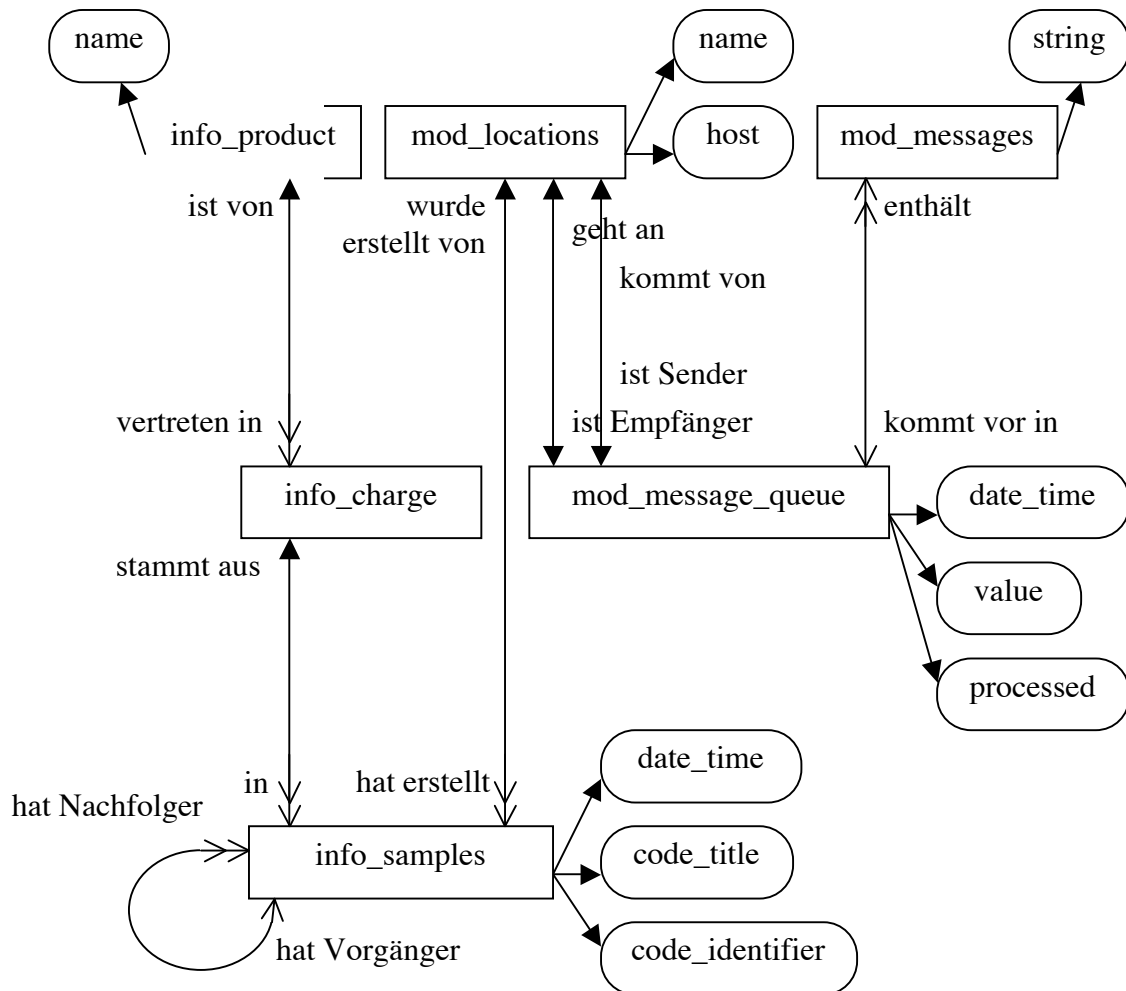
werden sofort erkannt:



Zusätzlich könnte die Überprüfung durch ein separates Programm erfolgen. Es müßte nur von der zuständigen Organisation (z.B. FDA) gestartet werden und würde alle verfälschten Datensätze zurückliefern.

3. Datenbank

3.1. ERM



3.2. Files

info_product (product_id, name, signature)
 mod_locations (location_id, host, name, description, signature)
 mod_messages (message_id, string, description, signature)
 info_charge (charge_id, product_id, sample_id, signature)
 mod_message_queue (queue_id, sender_id, receiver_id, message_id, date_time, value, processed, signature)
 info_samples (sample_id, parent_id, location_id, date_time, code_identifier, code_title, signature)

3.3. Erläuterung von erklärungsbedürftigen Attributen

mod_locations:

host = Host auf dem das Modul läuft
name = Allgemeiner Name

mod_messages:

string = Die Nachricht in Textformat

mod_message_queue:

date_time = Zeitstempel
value = Messageparameter
processed = Boolean (1=Ja, 0=Nein), ob die Message schon abgearbeitet wurde

mod_samples:

date_time = Zeitstempel, d.h. wann das Sample erstellt wurde
code_identifizier = Barcode
code_title = Beschreibung des Samples

Messages

String	Beschreibung
MSG_AUTH_DONGLE	Auf das Anstecken des Dongles warten
MSG_AUTH_PASSWORD	Dongle Schlüssel abfragen
MSG_ORDER	Probenplan generieren
MSG_SAMPLE	Verknüpfen der einzelnen IDs
MSG_LAB	Anzeige der Laborfensters, d.h. Informationshierarchie und Möglichkeit zu Splitten

4. Dongle DLL

4.1. Übersicht

Das Erstellen und Verifizieren der digitalen Signaturen findet mit Hilfe eines externen Dongles – dem Rainbow iKey 1000 – statt. Zusätzlich wird die Zugriffskontrolle demonstriert. Der Benutzer muß sich erst durch Anstecken des Dongles und Eingabe einer PIN authentifizieren, bevor er auf die Software und Daten zugreifen kann.

Der Zugriff auf den Dongle findet mittels der dem SDK beiliegenden PKCS #11 (Public Key Cryptography Standard) Library statt. Diese genorme Library übernimmt die direkte Kommunikation mit dem Dongle („Token“). Weiterführende Informationen findet man in Kapitel 5 „Developing for a PKI Environment“ des iKey Owner’s Manual.

Als Schlüsselalgorithmus haben wir RSA („RSA_PKCS“) mit einer Schlüssellänge von 512 bit gewählt, weil er der einzige – von PKCS unterstützte - Algorithmus ist, der sowohl für Signaturen als auch für Verschlüsselung verwendet werden kann. Für den realen Einsatz sollte man eine größere Schlüssellänge benutzen.

Um das Hauptprogramm möglichst übersichtlich zu halten, wurde die Dongle Funktionalität in eine DLL ausgelagert.

4.2. Die exportierten Funktionen

Funktion	Beschreibung
Init	Initialisieren der DLL. Muß einmal nach dem Laden der DLL aufgerufen werden.
NewSession	Starten einer neuen Session. Hier wird u.a. geprüft, ob ein Dongle angesteckt ist.
Die nachfolgenden Funktionen benötigen eine gültige Session:	
LastError	Liefert die letzte Fehlermeldung – falls vorhanden – zurück.
EndSession	Beenden einer Session.
TokenPresent	Prüft, ob der Dongle noch angesteckt ist. Ist dies nicht der Fall, so wird „EndSession“ aufgerufen.
UserLogin	Übergabe des Certificate-PINs. Erst nach erfolgreichem Login kann man auf den Private Key zugreifen.
UserLogout	Sperrt den Zugriff auf den Private Key wieder.
SignData	Erstellt die Signatur über einen Datenpuffer.
VerifyData	Überprüft, ob eine mittels „SignData“

5. Verschiedenes

5.1. Barcode Scanner

Nach dem Einschalten des Gerätes, muß vor jeder Kommunikation eine Konfiguration geladen werden. Dies geschieht durch Scannen eines spezifischen „Setting-Barcodes“. Dabei werden verschiedene Parameter wie Baudrate gesetzt.

Die Kommunikation mit dem Scanner findet über die serielle Schnittstelle statt. Sobald etwas gescannt wurde, steht es als Klartext bereit.

5.2. CMS

Information	Sender	Receiver	Message	Processed	Timestamp		
Listing	SAP	SAP	MSG_AUTH_DONGLE	yes	20030213210348	edit	delete
Product	SAP	SAP	MSG_AUTH_PASSWORD	yes	20030213210400	edit	delete
Charge	SAP	SAP	MSG_ORDER	yes	20030213210404	edit	delete
Samples	SAP	SAP	MSG_SAMPLE	yes	20030213210528	edit	delete
Sequence	SAP	SAP	MSG_LAB	no	20030213210528	edit	delete
New Entries							
Product							
Charge							
Samples							
Sequence							

[Show all] [Previous page] [1] [Next page]

Um während der Entwicklung die Datenbank gut im Blick zu haben, haben wir unser bestehendes CMS an die neue Datenbank angepasst. Grundsätzlich kann man mit ihm Einträge anlegen, auflisten und bearbeiten.