



©
INSTITUT
FÜR SYSTEM -
MANAGEMENT
GmbH

Ein Mitglied der
Secu-Sys Gruppe

Oldendorfer Str. 12
D-18147 Rostock

Tel. +49 (0)381 37573-0
Fax +49 (0)381 37573-29

info@secu-sys.de
www.secu-sys.de

Geschäftsführer
Prof. Dr. Dr. Gerd Rossa
Dipl. Kfm. Lars Hansen
Dipl. Ing. Holger Görz

Sitz der Gesellschaft
Rostock

Handelsregister
HRB 7547

Weitere Mitglieder
der Secu-Sys Gruppe

Secu-Sys Mitte GmbH
Oldendorfer Str. 12
D-18147 Rostock

Secu-Sys
Consulting GmbH
Gregor-Mendel-Str. 58
A-1190 Wien

bi-Cube®

IDENTITY
MANAGEMENT

PROVISIONING

PROZESS
MANAGEMENT

SINGLE SIGN-ON

ENTRANCE
CONTROL

IDENTITY
SERVER

USB-BLOCKER

Erklärung des iSM zum Datenschutz biometrischer Daten

Aufgrund der allgemeinen Datenschutz-Bedenken, die im Zusammenhang mit der biometrischen Erkennung von Personen immer wieder genannt werden, möchte das Institut für System-Management folgende Stellungnahme in Bezug zum Umgang mit biometrischen Daten abgeben:

- Bei der Speicherung der biometrischen Daten des Fingerabdruckes werden lediglich einzelne Merkmale (Minuzien) eines Abdruckes gespeichert. Es werden keine vollständigen Abbilder der biometrischen Merkmale gespeichert.
- Die Biometriedaten (Fingerabdruck) werden in Form eines Templates, d.h. ein mathematischer Extract bestehend aus Punkten und Abständen, abgespeichert.
- Es ist nicht möglich, aus diesem Template ein Bild des Fingerabdruckes wiederherzustellen.
- Alle gespeicherten Daten werden aus Gründen des Datenschutzes und zur Vorbeugung eines evtl. Datenmissbrauchs mit Triple DES (3DES) verschlüsselt.
- Die sowohl personen-bezogenen als auch die biometrischen Daten eines Nutzers obliegen beim iSM einer besonders hohen Sicherheitseinstellung in der Datenbank.
- Der Zugang zur Datenbank ist nur mit Nutzung der iSM-Tools möglich, die wiederum einer sehr dezidierten Berechtigungsstruktur unterliegen.
- Es ist nicht möglich, einen Fingerabdruck einer fremden Quelle „einzuschleusen“ und auf diesen dann die Identifikation des fremden Nutzers aufzubauen, da:
 - es keine Schnittstelle zur Übergabe eines Bildes gibt und
 - das Image des Sensors einen sog. Formfaktor hat, der ganz genau einzuhalten ist und mit der dazu gehörenden Software verarbeitbar ist.
- Je nach Anwendungszweck werden bei der Verifikation eines Nutzers, der Name des Users bzw. dessen Verwaltungs-Nummer, Datum und Uhrzeit der Erkennung sowie der Ort der Erkennung (welcher Sensor) ermittelt und gespeichert. (z.B. für eine Zeiterfassung). Es wird nicht versucht Daten zu ermitteln, die Rückschlüsse auf den Gesundheitszustand oder ethnische Herkunft zulassen.
- Die gespeicherten Daten dienen ausschließlich der Verwendung in der iSM-Software bzw. der Anwendungsumgebung
- Eine Weitergabe der biometrischen Daten an Dritte erfolgt nicht

Mit diesen Grundsätzen hält sich das iSM an die Empfehlung des Bundesbeauftragten für den Datenschutz und die Informationssicherheit (bfdi)
<http://www.bfdi.bund.de/>