

Information

Statement of iSM to the Data Privacy Protection of Biometric Data

Technologies Solutions Trends Experience

Following the general concerns of data privacy protection in connection with the biometric identification of individuals, the Institute for Systems Management would like to comment on this subject:

- Only a single criterion (minutiae) of a fingerprint impression is saved and not the entire images of the biometrical sign.
- The biometrical signs (fingerprint) are converted into a mathematical model (Template). A Template equals a large amount of numbers.
- It is not possible to recover an image of the fingerprint of this template.
- To protect the data and prevent possible data misuse all saved data are encrypted with triple DES (3DES).
- Person-related data as well biometric information of a user oblige a particular high security level in the iSM database.
- It is not possible to lock in a fingerprint of a foreign source to identify the foreign user, since:
 - no interface for the transfer of a fingerprint picture is available and
 - the image of the sensor applies to a so called form factor which must be followed closely and is processed with the associated software.
- To identify the user according to application purpose, his name, administration number, date and time, place and time of the identification as well a the location (what sensor) is determined and saved (e.g., for a time registration). It is not attended to record a state of health or ethnic origin.
- The saved data is exclusively used in the iSM software or application environment.
- A passing on to third parties does not occur.

With these principles iSM abides to the recommendation of the federal representative for the data privacy protection and the information security (bfdi).

<http://www.bfdi.bund.de/>