StarSign® Bio Token 3.0 M

USB Token

Reference Manual
Edition 10.2005

Giesecke & Devrient

ID No. 30017639

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

This hardware key is in compliance with the following test specification:

CEI EN 61000-4-2; CEI EN 61000-4-3; CISPR22

as required by:

CEI EN 61000-6-1, CEI EN 61000-6-2, CEI EN 61000-6-3, CEI EN 61000-6-4

which are specified for the following test:

- "ESD Immunity test"
- "Radiated radio-frequency and electromagnetic field immunity test"
- "Radiated Emission Verification"

In compliance with the "Essential Requisites" for the EMC Directive 89/336/EEC.

FCC ID: TIJ-BIOTOKEN-M

Giesecke & Devrient GmbH
StarSign® Bio Token 3.0 M
Supply: 5V DC
Absorption: 250 mA

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT REMARKS

Due to the limited space on the product shell, all FCC certification references are on this technical manual.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Contents

About StarSign Bio Token 3.0 M

Characteristics

StarSign Bio Token 3.0 M is a USB-PKI token based on the STARCOS 3.0 operating system. The token comprises a fingerprint sensor and on-token fingerprint verification functionality. The biometric data never leaves the token.

StarSign Bio Token 3.0 M is supported by StarSign middleware and can therefore be used for all public key applications supporting MS CAPI (CSP) or PKCS#11.

Fingerprint verification can be used instead of – or in addition to – PIN verification, granting a higher user convenience and a real tie between user and token. This is particularly of interest in applications that require non-repudiation.

StarSign Bio Token 3.0 M also comprises an independent flash drive.

Features

Features of StarSign Bio Token 3.0 M include:

- Based on STARCOS 3.0 operating system
- On-token sensor, image processing and biometric verification (on-card matching)
- Supported by StarSign middleware; use with all public key applications supporting MS CAPI (CSP) or PKCS#11
- Security system according to 7816-4; secure writing and messaging
- Cryptographic authentication and key management
- Encryption
  - Symmetric encryption: DES, 3DES
  - Asymmetric encryption: RSA-CRT with up to 2048 bits
- Support of up to 4 logical channels
- Biometric enrollment and verification functionality
- LED status indication
- additional flash memory drive

Related Standards

StarSign Bio Token 3.0 M adheres to the following standards:

- ISO/IEC 7816-3
- ISO/IEC 7816-4
- ISO/IEC 19794-2

More information on the relevant standards may be found in the appendix (see ‘C Reference Literature’ on page 19).

About the Document

Target Group

This manual addresses developers and specialists of smart card applications.

Required Knowledge

In order to use StarSign Bio Token 3.0 M, you should be familiar with:

- Smart card hardware/software
- Related ISO/IEC standards
- Experience in biometric user authentication and cryptographic services

This document assumes that you have a basic understanding of Microsoft Windows terminology and actions. Should you feel that this is not the case, it is suggested that you refer to your Windows manuals first.

Notation

In order to facilitate access to required information and to provide quick orientation, the following graphical aids and notations have been used:

This convention	Indicates
Italic	Operating system command or mode

Notes comprise hints and recommendations useful when working with StarSign Bio Token 3.0 M.

Please read warnings carefully - they are specified to prevent severe malfunctions and loss of data!

The header page of each chapter features an overview of the topics covered in the chapter. All technical terms and abbreviations used are explained in a glossary at the end of the manual.

1 Basics

This chapter provides you with background information on StarSign Bio Token 3.0 M.

Contents

1.1 General Introduction to Biometrics

Scope

Biometrics is the science of measuring physical or behavioral characteristics unique to an individual such as face, voice or fingerprint to verify a person's identity. Biometric characteristics can be described as something we are.

Biometrics and other Types of User Authentication

Unlike user authentication based on something the user knows, such as a PIN or password, or something he or she has, e.g. a smart card or other token, biometric systems work by relying on a biometric characteristic - something that is both unique and inseparably tied to the person. While PINs, passwords and keys can be forgotten, lost, lent or stolen, biometrics cannot. The user himself becomes the means of identification, the biological password.

Biometric user authentication can elevate overall system security and enhance ease of use, as users no longer have to remember PINs and passwords.

Enrollment and Verification

Before biometric authentication can be used to verify the identity of a user, a biometric enrollment has to be performed beforehand. This means that the characteristic data of the biometric trait has to be captured and saved as a reference in a separate process in advance to verification. During verification, the characteristic data of the biometric trait is captured again and compared to the previously stored reference data. If both data sets coincide to a sufficient level, access is granted.

Biometric Error Rates

In contrast to a PIN or password comparison, two different photos or characteristic data sets captured of the same biometric trait will always differ a bit due to positioning, background lighting, etc. Thus, biometric comparison returns a figure which represents a level of coincidence, i.e. the probability that two presented data sets belong to the same person. Depending on a threshold value, access is granted or denied. As a consequence, a slight possibility remains that an unauthorized user be granted access to a protected system or that a legitimate user will be denied access. The threshold value responsible for the error rates can be set by the system administrator. These error rates are characteristic for all biometric systems and are called false acceptance rates (FAR) and false rejection rates (FRR).

Fingerprint Verification

Fingerprint verification is not only the most prominent but also one of the most secure and well-understood biometric measures. Software converts the image of a fingerprint into digital form and extracts a set of characteristics, i.e. a template, unique to the user's fingerprint. The characteristic information from one fingerprint contains up to 60 key points. Crucial key points where finger-ridges end or split up are local features called minutiae. They provide unique, identifiable information.

1.2 Biometrics, Smart Cards and Tokens

On-Card Matching

In on-card matching biometric templates, i.e. data sets, are compared with a previously stored biometric reference template in the smart card processor itself. This happens in full analogy to the PIN verification where the entered PIN is sent to the smart card processor and compared on-card with a previously stored PIN. The advantage of this method is that the reference template is stored exclusively in the secure smart card processor environment, reliably protecting sensitive personal data against unauthorized access.

Access Rules

An individual access rule is assigned to each elementary file on the smart card processor. As a consequence, elementary files can be accessed (read/write/update) by cryptographic authentication, PIN verification, biometric authentication or a combination of all three.

Applications

The paramount application for biometrics in combination with cards and tokens is the use in public key infrastructures, where biometric user authentication can be used to enable the cryptographic functions or services offered by the smart card processor. Thus, for example, StarSign Bio Token can be used as a secure signature creating device, that can be legally tied to the token holder with on-card fingerprint verification.

1.3 LED Status

LED Arrangement

StarSign Bio Token 3.0 M contains two bicolor LEDs on the top side for visually signalizing its current status and operation to the user:

- Left LED
  Illuminates in either green or yellow
- Right LED
  Illuminates in either red or yellow

Fig. 1 Arrangement of the LEDs

LED Status/Mode

The LED states listed in the table signalize the current status and operation to the user:

Status/Mode	LED indication	Description
Idle	Green and red LEDs flash	Waiting for command
Place finger	Left yellow LED blinks	Wait for finger
Busy	Red LED blinks quickly	StarSign Bio Token 3.0 M is busy
Success	Green LED illuminated	Enrollment/verification successful
Reject	Red LED illuminated	Enrollment/verification failed
Boot	Green and red LED illuminated	Booting device
TEST mode	Both yellow LEDs flash	Allow diagnostic commands
ADMIN mode	Left yellow LED flashes, red LED illuminated	Allows parameter configuration and firmware update
Firmware update	Both yellow LEDs illuminated	Signal firmware update status

Fig. 2 LED status/mode

2 Command Reference

This chapter describes the StarSign Bio Token 3.0 M command set. The commands are listed in alphabetical order.

Contents

2.1 ENROLL FINGERPRINT

Scope

ENROLL FINGERPRINT is used to collect a reference data set from the user and store it in the smart card processor.

The command performs the following:

- Scans an image
- Generates a template
- Transmits the template to the smart card processor, where it is stored via the *UPDATE BINARY* command

In order to enhance the quality of the reference template, two or more templates can be merged to one large template.

Before carrying out this command you must create a file for the reference data on the smart card operating system. For details see STARCOS 3.0 reference manual edition 06/2005 or later.

Command

CLA	INS	P1	P2
'A0'	'10'	'00'	

P2 Specifies the merge parameter. Several templates can be merged into one large template before sending the master template to the smart card processor.

'00'
Final enroll command

'01'
Non-final enroll command

Non-final enroll commands grab images, but extracted characteristic features are stored in the internal RAM of StarSign Bio Token 3.0 M and not on the smart card processor.

The final enroll command grabs a final image, extracts features, assembles or merges these features with the features in the internal RAM of StarSign Bio Token 3.0 M and finally stores them on the smart card processor.

Response

SW1	SW2
'90'	'00'

Status Bytes

This command may return one of the following status bytes.

Code	Description
'65 81'	Memory failure
'69 82'	Security status not satisfied
'69 86'	Command not allowed (no current EF)
'6A 84'	Not enough memory space
'90 00'	Successful operation
'A7 00'	General ARM7 error
'A7 01'	Unknown instruction
'A7 02'	Length error
'A7 11'	Timeout error
'A7 12'	Sweep too slow
'A7 13'	Sweep too fast
'A7 14'	Sweep not straight
'A7 15'	Sweep too short
'A7 16'	Too many defect lines on sensor
'A7 17'	Image quality too bad
'A7 18'	Too few features
'A7 19'	Merge failed
'A7 1A'	Try again error
'A7 1B'	Resync error
'A7 1C'	Maximum number of merges exceeded
'A7 81'	Invalid parameter

2.2 VERIFY FINGERPRINT

Scope

VERIFY FINGERPRINT is used to verify a user's fingerprint. It initiates fingerprint image acquisition, processing and feature extraction.

The features are sent to the smart card processor for on-card verification and the outcome is reported in the response APDU to the host.

The command performs the following:

– Scans an image
– Generates a template and transmits it to the smart card processor, where it is compared with the reference template (see '2.1 ENROLL FINGERPRINT' on page 10) via the *VERIFY* command.

Biometric threshold, retry counter and access rules have to be configured in the file system of STARCOS. For details see STARCOS 3.0 reference manual edition 06/2005 or later.

Command

CLA	INS	P1	P2
'A0'	'20'	'00'	

P2 Specifies the Key Identifier (KID) used to reference the biometric data stored in the smart card processor during the enrollment phase (see '2.1 ENROLL FINGERPRINT' on page 10).

Response

SW1	SW2
'90'	'00'

Status Bytes

This command may return one of the following status bytes.

Code	Description
'63 Cx'	Verification failed (x represents the number of remaining retries)
'64 00'	File or data missing; enrollment file corrupt
'69 82'	Security status not satisfied
'69 83'	Authentication method blocked
'69 85'	Conditions of use not satisfied
'6A 82'	File not found
'6A 88'	Referenced data not found
'90 00'	Successful operation
'A7 00'	General ARM7 error
'A7 01'	Unknown instruction

Code	Description
'A7 02'	Length error
'A7 11'	Timeout error
'A7 12'	Sweep too slow
'A7 13'	Sweep too fast
'A7 14'	Sweep not straight
'A7 15'	Sweep too short
'A7 16'	Too many defect lines on sensor
'A7 17'	Image quality too bad
'A7 18'	Too few features
'A7 19'	Merge failed
'A7 1A'	Try again error
'A7 1B'	Resync error
'A7 20'	General verify fingerprint error
'A7 81'	Invalid parameter

2.3 VERSION INFO

Scope

VERSION INFO is used to request public information on StarSign Bio Token 3.0 M from the host.

Parameter P2 of the command APDU specifies the item tag of the version information to be retrieved. The response data returns the requested version information.

Command

CLA	INS	P1	P2	L_e
'A0'	'8A'	'00'		

P2 Specifies the item tag of the version information

'01'
StarSign Bio Token 3.0 M firmware version, build date and time

'02'
Key info: CRC of currently valid authentication key

L_e Specifies the expected length: '00' <= length <= '80'

'00'
Returns the maximum available data

Response

DATA	SW1	SW2
Response string	'90'	'00'

Status Bytes

This command may return one of the following status bytes.

Code	Description
'90 00'	Successful operation
'A7 00'	General ARM7 error
'A7 01'	Unknown instruction
'A7 02'	Length error
'A7 81'	Invalid parameter
'A7 8A'	General version info error

Appendix

The appendix contains additional information on StarSign Bio Token 3.0 M.

Contents

A Overview of Status Bytes

Return Codes

For error codes not defined in the following see the STARCOS 3.0 reference manual.

The following error codes are defined.

Status Bytes	Error code	Description
'63 Cx'		Counter provided by 'X' (valued from 0 to 15); exact meaning depending on the command
'64 00'		State of non-volatile memory unchanged (SW2 = '00', other values are RFU)
'65 81'		Memory failure
'69 82'		Security status not satisfied
'69 85'		Conditions of use not satisfied
'69 86'		Command not allowed (no current EF)
'6A 84'		Not enough memory space in the file
'A7 00'	SW_ARM7	General error
'A7 01'	SW_UNKNOWN_INSTRUCTION	Unknown instruction
'A7 02'	SW_LENGTH_ERROR	Length error
'A7 11'	SW_TIMEOUT	Timeout error
'A7 12'	SW_SWEEP_TOO_SLOW	Sweep too slow
'A7 13'	SW_SWEEP_TOO_FAST	Sweep too fast
'A7 14'	SW_SWEEP_NOT_STRAIGHT	Sweep not straight
'A7 15'	SW_SWEEP_TOO_SHORT	Sweep too short
'A7 16'	SW_SENSOR_DEFECT	Too many defect lines on sensor
'A7 17'	SW_IMG_QUALITY_TOO_BAD	Image quality too bad
'A7 18'	SW_TOO_FEW_FEATURES	Too few features
'A7 19'	SW_MERGE_FAILED	Merge failed
'A7 1A'	SW_TRY_AGAIN	Try again error

Status Bytes	Error code	Description
'A7 1B'	SW_IO_ERROR	Resync error
'A7 1C'	SW_MAX_MERGE	Maximum number of merges exceeded
'A7 20'	SW_VERIFY_FP	General verify fingerprint error
'A7 81'	SW_INVALID_PARAMETER	Invalid parameter
'A7 84'	SW_GET_CHALLENGE_FAILED	General get challenge error

B Technical Specifications

Scope

This section lists the technical specifications of StarSign Bio Token 3.0 M

Token Housing

StarSign Bio Token 3.0 M housing has the following characteristics.

- dimensions closed: 80 x 33 x 17 mm
- dimensions open: 107 x 33 x 17 mm
- mechanism to protect sensor and USB interface from wear

Power Consumption

250 mA

Interfaces

StarSign Bio Token 3.0 M supports the following interfaces:

- USB 1.1
- PKCS#11 (with middleware)
- MS CAPI 1.0 (CSP) (with middleware)

Sensor

Atmel swipe sensor

Operating System

StarSign Bio Token 3.0 M uses the following operating system with listed characteristics.

- STARCOS 3.0
- 72 kB EEPROM
- symmetric encryption: DES, 3DES
- asymmetric encryption: RSA-CRT with up to 2048 bits
- security system in accordance with ISO 7816-4
- up to 8 DF levels
- up to 4 logical channels
- secure write
- secure messaging
- memory management
- several authentication options

System Requirements

StarSign Bio Token 3.0 M has the following system requirements.

- IBM PC with Pentium 90 MHz processor or higher
- 32 MB RAM for Windows 2000, 2003 and XP
- free USB port

C Reference Literature

ISO

ISO/IEC 7816-3
Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols
ISO/IEC, 1997 (http://www.iso.org)

ISO/IEC 7816-4
Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange
ISO/IEC, 1995 (http://www.iso.org)

ISO/IEC FDIS 19794-2
Information technology - Biometric data interchange formats - Part 2: Finger minutiae data
ISO/IEC, 2005 (http://www.iso.org)

D Glossary

3DES
: The Triple-DES algorithm is a modified DES encryption. It consists of calling the DES algorithm three times in succession, with alternating encryption and decryption. If the same key is used for all three DES calls, the Triple-DES encryption corresponds to a normal DES encryption. However, if two or three different keys are used, Triple-DES encryption is significantly stronger than a single DES encryption.

CAPI
: Crypto Application Programming Inteface

CRC
: Cyclic Redundancy Check
A simple and widely used form of EDC (Error Detection Code) for the protection of data. The CRC must be computed using an initial value and a divider polynomial before it can be used.

CSP
: Cryptographic Service Provider
Cryptographic support for Microsoft and other CryptoAPI products.

DES
: Data Encryption Standard
A standard cryptographic algorithm specified as DEA in ISO 873-1. An algorithm for symmetric cryptography. Now used as 'triple DES' in EMV operations (e.g., ARQC generation) where data is encrypted using the first half of a double length key, is decrypted using the second half, then re-encrypted using the first half again.

EF
: Elementary File
EFs represent the actual data storage in the file tree of a smart card. EFs contain one of the following internal file structures: Transparent, Linear Fixed, Linear Variable or Cyclic.

FAR
: False Acceptance Rate
Due to the nature of biometrics there is a slight possibility that an unauthorized user is granted access to a system protected by biometrics.

FRR
: False Rejection Rate
Due to the nature of biometrics there is a slight possibility that a legitimate user is denied access to a system protected by biometrics.

KID
: Key and algorithm identifier for authentication (C/CC/DS).
)

PKCS
: Public Key Cryptography Standards

PKI
: Public Key Infrastructure
A series of procedures established by a Certification Authority for the generation, signing, distribution and revocation of the keys used in an asymmetric cryptography scheme.

RFU
: Reserved for Future Use

RSA-CRT
: RSA - Chinese Remainder Theorem
Special parameter setting for asymmetric crypto algorithm.

STARCOS
: Smart Card Chip Card Operating System
Forms the basis of multifunctional smart card applications. STARCOS enables the implementation of various applications (e.g., electronic purse, access control to data networks, and digital signatures).Smart card operating systems control the data transfer, the storage areas, and process information; they manage the resources and supply all necessary functions for the operation and administration of a random number of applications.

USB
: Universal Serial Bus
Port not only for connecting external peripheral devices such as keyboard, mouse, scanner, etc., but also USB hubs. These devices can be added during active operation.

Index