

Ver 1.3

**TES and Applicable
Standards of Interest**



TABLE OF CONTENTS

Executive Summary	3
Compliance/Coverage Matrix	4
APPENDIX.....	6
Compliance: ISO 19794	6
Relevant Points from Specification	6
TES Compliance Information	6
Data Structure Compliance: ISO 19785	7
Basic Information	7
TES Compliance Information	7
API Compliance: ISO 19784	7
Basic Information	7
TES Compliance Information	8
FIPS 180, 197 and 198	8
FIPS 180: SHS	8
FIPS 198: HMAC	8
FIPS 197: AES	8
TES Compliance Information	9
Compliance with operational security requirements: FIPS 190 and 201	9
FIPS 190: Advanced Authentication Technologies	9
FIPS 201: PIV	10
TES Compliance Information	10

TES and Applicable Standards of Interest

Executive Summary

TES protects your investment by delivering for interoperability and compliance to industry standards in BIometrics, Cryptography, Compression and RFID. By complying with key aspects of relevant standards, TES is achieving Best Practices and establishing an unsurpassed value proposition.

Standards of Interest

TES has been designed to take into consideration the following applicable International Standards Organization (ISO) and USA Federal Information Processing Standard (FIPS) documents.

ISO

- ISO 19784: Biometric Application Programming Interface (API) specifications
- ISO 19785: Common Biometric Exchange Formats Framework (CBEFF), data element specifications
- ISO 19794: Biometric data interchange formats, face image specifications

FIPS

- FIPS 180: Secure Hash Standard (SHS)
- FIPS 190: Advanced authentication technologies
- FIPS 197: Advanced Encryption Standard (AES)
- FIPS 198: Keyed-Hash Message Authentication Code (HMAC)
- FIPS 201: Personal Identity Verification (PIV)

In several critical areas TES exceeds the applicable standards. We cite our DPS (Dual Protection Safeguard), ZK (Zero Knowledge), no necessity for a CENTRAL database, multi-factor testing and machine learning as examples of mature technology infused into TES for superior performance.

Compliance/Coverage Matrix

Standard	General Coverage	Specific TES Coverage	Advantages for TES
ISO 19794	Application-level interoperability for BIOmetric solutions	Face image formats	Capability to process images of various size and resolution. This is an advantage for forward and backward compatibility. Users can regulate this by specifying any criteria necessary for their needs regarding registration images which would comply or exceed a given standard.
ISO 19785		Biometric record formats	<p>TES has two modes of operation. The native mode uses a data schema and record format which provides strong security arising from ZK encoding and small storage footprints as a result of a high degree of compression, in accordance with our proprietary implementation. The optional mode provides compliant registration profiles per the standard but incurs –storage and security penalties as per the Note.</p> <p>Note: CBEFF records will be significantly larger, so storage overheads are correspondingly greater. Since CBEFF is also designed for open readability there is no privacy/security measures associated with the record and photo, leaving them vulnerable.</p>
ISO 19784		API specifications	<p>TES is designed to be a closed user group application with input or output of data. This silo approach ensures that no outside force can “hack” the system. Current design maximizes operational security since no exposure of application-level information is made with external parties.</p> <p>An optional API is offered to comply with the specification based C/C++ language constraints to create compliant function calls per user specified requirements.</p>

Standard	General Coverage	Specific TES Coverage	Advantages for TES
<p>FIPS 180</p> <p>FIPS 197</p> <p>FIPS 198</p>	<p>Cryptographic mechanisms & protocols</p>	<p>Message hashing</p> <p>Data encryption</p> <p>Keyed message hashing</p>	<p>TES incorporates Dual Protection Safeguard (DPS) for maximum cryptographic security. DPS inner protection uses a ZK (zero knowledge) logarithm for a performance advantage. More specifically, this results in cryptographic security that scales exponentially with parameter bit-length ie equivalent to specified hashes & ciphers.</p> <p>DPS outer protection uses AES encryption at a 256 bit level for any information that may be exposed beyond the binary algorithm and/or machine code. Although this approach is technically redundant, it significantly increases the cost and time to penetrate our technology. For example, any data that is exported outside of TES is protected by DPS technology for rigorous formal compliance to the specification.</p>
<p>FIPS 190</p> <p>FIPS 201</p>	<p>Operational & technological deployment issues</p>	<p>Advanced authentication technologies</p> <p>PIV systems, components & processes</p>	<p>TES exceeds the specification due to ZK cryptographic construction, strong security and privacy characteristics and integrated token-biometric methodology.</p> <p>An important area of this specification that we comply with is our facial recognition engine which allows for improvements in operational performance arising from user familiarization. This adaptive and dynamic aspect of our implementation is a major benefit for including machine learning as part of TES.</p>

TES offers an unsurpassed degree of security. It exhibits excellent hardness against brute force attacks which systematically traverse the key space.

APPENDIX

Compliance: ISO 19794

Relevant Points from Specification

Images should facilitate:

- Human examination of facial features ie moles and/or scars useful in identity verification
- Human verification of identify via comparison
- Computerized face verification via one-to-one analysis
- Computerized face identification via one-to-many search

Additional specification of:

- Scene constraints ie pose and expression
- Photographic properties ie lighting, positioning and camera focus
- Digital image attributes ie image resolution and image size

Image formats (JPEG or JPEG-2k) are specified to be embedded in CBEFF-compliant data structures.

Compliant face images conform to the following functional specifications:

- Basic face: complies with image format, but not additional specifications
- Frontal face: adheres to lowest-grade of additional requirements for human examination and/or computerized recognition
- Full frontal face: adheres to highest-grade of additional requirements; inclusive of full head, neck and shoulders. Suitable for permanent storage; applicable for identity documents ie passports, driver licenses and mug shots.
- Token frontal face: adheres to intermediate-grade of additional requirements; inclusive of specific geometric sizes and eye positioning based on image dimensions. Suitable for minimizing storage requirements for human and computerized face verification, but not necessarily human examination or computerized identification.

TES Compliance Information

TES uses its award winning¹ Biomash Engine to implement ZK compressive encoding of biometric data derived from face images, with following system specifications:

- Imaging capture device: VGA (640x480) resolution camera
- Face region of interest (ROI): 63x71 pixels
- Inter-eye separation: 40 pixels and is therefore interoperable with:
 - Full frontal images: with minimum inter-eye separation of 120 pixels, and minimum face width (encompassing ROI) of 240 with permissible aspect ratios of 1:1.25 to 1.33
 - Token frontal images: with minimum inter-eye separation of 60 pixels, with proportional reductions in face width from full frontal dimensions

Biomash does not require the storage of face images captured during registration, which is an advanced protective feature for user privacy and security. A richer set of application scenarios such as single-use verifications with disposable user tokens may now be implemented with the

¹ Best in Show Finalist at RFID Journal Tradeshow, April 2008 Las Vegas USA

Biomash engine. On the other hand, availability of face images in operational biometric information records (BIR) is useful for both human and computerized analysis. The Biomash engine provides an option to modify the registration process to store user profiles. Consequently, we can offer a special version of TES to provide face image storage compliant with the specification.

Data Structure Compliance: ISO 19785

Basic Information

CBEFF is intended to promote interoperability of biometric applications and systems via specification of Standard Biometric Headers (SBH) for vendor-specific BIR. Compliant BIRs would therefore consist of:

- SBH as therein specified by CBEFF
- One or more biometric data blocks (BDB), contents of which is expressly beyond the scope of CBEFF

Standardization process also specifies Biometric Registration Authorities to assign unique identifiers to biometric organizations and vendors.

TES Compliance Information

Incorporation of biometric-hash parameters within a CBEFF-compliant BIR for application data interoperability is available as an option; otherwise for reasons cited in the Matrix table we prefer to use our advanced technology which delivers rigorous security with no necessity for a database or retention of facial records. We believe our solution renders the standard obsolete and cite our productivity in terms of people per hour, false accept and false reject performance as setting the more relevant benchmarks for our class of multi-factor security without the necessity of using CBEFF.

API Compliance: ISO 19784

Basic Information

The Biometric API (Bio-API) specification defines Service Provider Interfaces (SPI) within biometric systems supportive of integration of multiple biometric sub-systems from different vendors. To this end, Bio-API outlines an abstracted biometric system architecture suited for various biometric technologies and solutions. The Bio-API architectural framework allows for integration of multiple Biometric Service Provider (BSP) components provided by different vendors to be dynamically invoked as required by a biometric application system. Interactions among Bio-API compliant BSPs would use CBEFF compliant BIRs.

Bio-API covers the basic biometric functions at a high-level, and provides a database interface to allow BSP components to manage large-scale BIR storage and retrieval. The objective is to enhance performance, especially for computation-expensive tasks ie large population searches.

The standard also specifies biometric component registry providing information regarding biometric components integrated into the biometric system of interest, and furthermore a component registry interface for the management and inspection of that registry.

Bio-API function calls and data structures are specified in the C programming language.

TES Compliance Information

Addition of a Bio-API interface layer to compliment the native TES API for system integration interoperability is available. This can support export of user specified data or integration into custom use cases. Note: The TES API is available in terms of VB/C/C++ function calls to exceed the specification.

FIPS 180, 197 and 198

FIPS 180: SHS

Compressive hash functions in which multiple input message blocks are processed to result in a compact message digest of configurable bit size. To optimize the RFID data container size we have engineered our block size as multiples of 32 bits. ie 160, 256, 384 and 512-bits. Specified algorithms such as the Secure Hash Algorithm (SHA) 1, 256, 384 and 512 are integral components of a basic algorithmic framework to deliver zero knowledge. ZK is an irreversible transformation and therefore protects the data from reverse engineering. By implementing best practices cryptographic security of hash functions, presuming absence of algorithmic defects, we scales exponentially with bit length of message digest.

FIPS 198: HMAC

Extension of compressive hash function to incorporate symmetric key, resulting in message digest which is dependant on both message and key, the latter presumed to be shared between message sender and receiver. It is presumed the Cryptographic security of HMAC (Hash Message Authentication Code) is equivalent to that of underlying hash function.

FIPS 197: AES

Symmetric block cipher in which multiple input plaintext blocks are processed to result in output ciphertext blocks of equivalent size. The approved algorithm is AES which operates on plaintext/ciphertext blocks of 128-bits; and is configurable to operate with keys of 128, 192 and 256-bits. Symmetric encryption is a trapdoor one-way transformation, which means it is irreversible if the trapdoor, ie key presumed to be shared between data sender and receiver, is not known. Best-case cryptographic security of block ciphers, presuming absence of algorithmic defects, scales exponentially with bit length of key and data block.

TES Compliance Information

The Biomash Engine is based on a state machine constructed from various information-theoretic operations, the combination of which is equivalent to construction of hash functions and block ciphers. The substantive difference with respect to conventional cryptographic algorithms stems from its acceptance of floating-point (facial biometric) inputs, which are subject to lossy compressive transformations equivalent to those found in hash functions. The end result is a bit string of configurable size using memory blocks which are optimized for RFID data containers, typically from 96-256 bits and larger. Of course, longer bit-strings result in robust recognition under more varied operational environments such as night time versus day time lighting. The cryptographic security of the Biomash state machine and its DPS technology is equivalent to that of cryptographic hashes and block ciphers, and scales exponentially with the length of the output bit string.

Operationally a Biomash output string would not require additional protective measures, but we apply our DPS technology to exceed compliance objectives.

Compliance with operational security requirements: FIPS 190 and 201

FIPS 190: Advanced Authentication Technologies

Outlines advanced methods surpassing password-only authentication for identity verification of computer users, with physical tokens and user biometrics being specifically mentioned. Standard also recommends combinations of passwords, tokens and biometrics as providing enhanced security in comparison to single-method authentication.

With respect to biometric systems, standard specifies low False Acceptance Rates (FAR) and False Rejection Rates (FRR) as the primary figures-of-merit, but acknowledges user factors. Most important of these is user familiarization with the deployed methods, with two weeks cited as the nominal period after which the FRR can be expected to fall off significantly. Another consideration is possibility that some users may have impairments that prevent biometric capture acceptable to the deployed system, thereby necessitating one or more alternative methods ie token and/or password. Token-side storage of biometric data is specifically mentioned as being desirable from the viewpoints of operational and storage security. Cryptographic protocols are also specifically mentioned as being desirable if present as a central component of the deployed system.

Standard also recommends consideration of user acceptance, with ideal case of biometric being both non-invasive and enabling continuous authentication. In the latter case; users would not need to undertake additional action for authentication purposes, and also prevents access by users other than the individual properly authenticated for access. Face recognition is specifically mentioned as being favorable in this respect.

FIPS 201: PIV

Defines a PIV (Personal Identity Verification) system for use in various applications such as physical, computer and information access control. Acceptable PIV systems enable creation of identification credentials, and subsequent verification of claimed identity. Each PIV card is specified to be of credit-card form, with one or more embedded integrated circuit chips (ICC). Permissible ICC interfaces are:

- ISO 7816: for contact-based cards
- ISO 14443: for contactless cards

With other machine-readable elements being:

- Optical barcode
- Magnetic stripe

The specification is inclusive of both operational and technological considerations such as:

- Issue based on rigorous verification of identity, with various mandatory and optional identity data specified for display on the physical card and for storage on the ICC
- Issue only by parties of officially accredited reliability
- Resistance to identity fraud, tampering, counterfeiting and malicious exploitation; via incorporation of various security features ie etching, engraving, holograms and watermarks
- Straightforward and rapid electronic verification
- Security and privacy requirements are best practices

Biometrics are specifically recommended as providing additional security, with face image required to be:

- Printed on front of PIV card
- Uploaded via ICC interface for display at security checkpoints

With the latter being a CBEFF-compliant token or frontal face image.

TES Compliance Information

TES state of the art Biomash facial recognition and multi-factor algorithms meet or exceed key aspects of the specification as follows:

- Verification method being an integration of token possession and user biometric
- Verification method being reliant on ZK cryptographic encoding
- Storage on the ICC is optimized for rapid electronic verification
- Issuance of RFID Security Credentials is strictly controlled by restricted users to those with authorized token/biometric/password combinations
- Improvement in operational performance after user familiarization period
- Face biometric being regarded as being inherently acceptable
- Face biometric enabling continuous verification in computer workstation scenarios
- Strong protection of user security and privacy
- DPS technology satisfies best practices constraint