TeleID
by Encotone Ltd.
popularizing digital signatures

Tele-ID v.6.2

FIPS 140-2 Non-Proprietary Security Policy

Level 2 validation

Version 2.4 - March 26, 2004

Encotone Ltd. **TECN-004**

www.encotone.com

Email: info@encotone.com

Scope of Document

The following document is designed to describe the security rules of the Tele-ID v6.2:

- A clear and concise specification of the principles to be used to guide the design decisions.
- Addresses all of the applicable requirements of FIPS 140-2.
- Includes an overview of the cryptographic module.
- Lists roles and services of the module and how they are related, the different types of Critical Security Parameters (CSPs) (keys, key components), capabilities and protections.
- Addresses any additional security requirements imposed by the manufacturer to achieve the goals of their design.

I/ Product Overview

The cryptographic boundary is the outer case of the Tele-ID device.

Encotone's **Tele-ID** is an acoustic end user personal and portable device, which allows fully PKI compliant digital signatures not only via the Internet but also via the ubiquitous telephone and cellular networks.

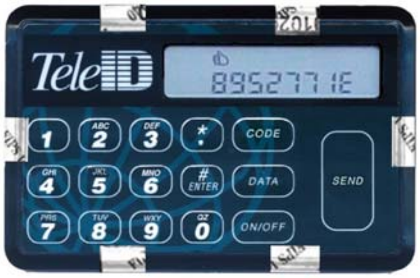

Figure 1: The Tele-ID

Tele-ID is a two-factor authentication (PIN-secured) device that resembles a small calculator. It houses a small keyboard, display and acoustic tone generator. It generates and safely stores the user's Private Key while its Public Key is sent to the Certification Authority in order to receive a standard (X.509) PKI certificate. The device includes an optical data input interface and a loudspeaker used as the acoustic output interface. For user convenience in office applications the Tele-ID is located on a simple stand connected to the PC and allowing fully hands free operation.

A small software package installed on the user's PC (can be downloaded from a website) performs conversion of the acoustic signals into standard PKCS#7 message that can be checked by standard PKI vendor tools as any PKI signature.

I.1/ Tele-ID as Signing Device

Three technologies exist to store private keys and sign electronic documents; they include chip cards, USB tokens and Encotone Tele ID. The Tele-ID is the third and most advanced device; to store a private key and to sign electronically documents. The main differences between the Tele-ID and the other two other existing devices (chip card and USB token) are:

- Active against passive device - the Tele-ID has internal battery providing it operational independence. Unlike chip cards and USB tokens which need external power source (a reader or PC) the Tele-ID operates everywhere and anytime.
- User interface – the Tele-ID has internal keyboard and display for user interface while chip cards and USB tokens use the PC keyboard as interface to user. In the world of Trojan horses, viruses, cookies, etc. this is a serious security advantage, especially when keying in private information like PIN.
- Acoustic and optical interfaces – the Tele-ID is equipped with two 'one-way' interfaces: optical input interface and acoustic output interface. Unlike these two contact-less interfaces, chip cards and USB tokens need direct galvanic contact to the PC, which again compromises the device security.
- The Tele-ID has an internal real time clock (possible due to internal battery) unlike the other two devices that take the time from the PC. The difference is huge: have a reliable internal time source (used to "time stamp" each digital signature) compared to the user settable PC originated time.

I.2/ Digitally Signing with Tele-ID

The Tele-ID is a complex, outstanding device that allows few types of digital signatures as follows:

- Signing documents in office environment – this usage is common to all three types of devices (chip card, USB tokens and Tele-ID) and is supported equally well with some slight differences between them.
  For this application the Tele-ID shall be located on its office Tele-ID stand, which is connected to the PC. The Hash value of the document to be signed (part of the PKI digital signing process and identical for all devices) are sent to the Tele-ID via its optical interface, are signed by the chip located inside the Tele-ID and returned to the PC via the device's acoustic interface directly to the PC microphone input. In continuation, using Encotone's Tele-ID driver software module, the digital message is detected, decoded and converted into a standard PKCS#7 message. One important advantage of the Tele-ID is the capability to digitally sign documents while your computer is off-line (not connected to Internet) due to its reliable time stamping (internal clock) capability.
- Signing documents using any PC – not everybody has his own PC or not always has it next to him when requested to sign a document. People can sign agreements with other people or institutions (banks, companies, government, etc.) while using their office PC, a computer in the university, in an Internet café or hotel room. The common characteristic of these computers is that they do not have any support for digital signatures: no chip card reader attached, maybe no USB interface and definitely no special software preinstalled. In such case, the Tele-ID can still provide a solution based on the standard browser and the almost ubiquitous microphone of the computer. In the rare case such a microphone is not available, a wired or cellular telephone can be used as reader, requesting an IVR (Interactive Voice Response) on the service provider side to support the application.

Using the standard browser the user can get on the screen the document to be signed. Once the user is ready to sign he/she clicks on a special icon and in response the website will calculate and display the FIPS standard SHA-1 hash of the document. This website is not part of this validation. In continuation the user introduces the hash into the Tele-ID using the device's keyboard and upon pressing a button the digitally signed hash shall be acoustically transmitted into the microphone of the PC or telephone.

- Signing on bank transactions – bank transactions are mostly numerical and concise messages, which can be expressed usually as a series of few numbers (one or two account numbers, amount, etc.). The Tele-ID has the "short message" signing capability specially designed to handle such bank transactions.
  Bank customers can access their personal account using the browser of any PC connected via Internet to the bank's website. By the way, the OTP (One-Time Password) capability of the Tele-ID helps securely access the personal account while user not requested to remember any complicated username and password. This OTP is used to access another product that is not part of this validation. In continuation, in order to perform transactions, the user is instructed which data relevant to the specific transaction to enter into its Tele-ID. Now, by simply depressing a button the digitally signed data (and intrinsically the transaction) is transmitted acoustically to a microphone.
  In very similar way bank transactions can be performed via the telephone. In such case the website shall be replaced by an IVR and/or phone operator. The user introduces the data received via the telephone into his Tele-ID and by pressing a button digitally signs on it and sends the signed document acoustically to the telephone's microphone.
- Digital signature as strong authentication – the Tele-ID provides this additional outstanding capability, namely to use a digital signature as an authentication message. The Tele-ID has an internal real time clock used to time stamp all messages generated by the device. By digitally signing on the time function a very strong coded (PKI) message can be acoustically sent to a recipient side including: the identity of the sender (identified by the use of its private key) and the precise time when the message was created. The recipient can easily check the message using standard PKI tools available today as part of any browser. The beauty of this solution is that works equally well via Internet or telephone. Bank customers using both Internet and telephone to get remote service can safely access their account using the Tele-ID without need to remember any complicated usernames and passwords.

The Tele-ID when compared with chip cards and USB tokens is not only the safest digital signature device but also provides outstanding unique solutions appropriate especially for commuters who are not caring a laptop with them or simply any people who are not mandatory owners of a PC. These special features are provided as add-on to supporting, in a very similar way, all signing characteristics and functionalities chip cards and USB tokens provide. The Tele-ID offers the capability to sign data over any telephone.

II/ Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2 as a multi-chip stand-alone module.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports & Interfaces	2
Roles, Services, & Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Test	2
Design Assurance	2
Mitigation of Other Attacks	N/A

III/ Roles and Services

The cryptographic module supports two roles:

1. User: The operator of the Tele-ID.
2. Cryptographic Officer: The operator of the Tele-ID.

Concurrent users are not allowed.

The cryptographic module enforces identity-based authentication. The purpose of the Tele-ID is to be a cryptographic identifier for one unique individual. When the module is initialized it is assigned with a unique identifier, which has an associated register to store a PIN. The operator must enter the correct PIN to authenticate him/herself to the module. The module requires re-authentication after the <ON/OFF> button is pressed. The module automatically switches off after the module pre-configured time-out.

The services provided to the User or Cryptographic Officer after successfully authenticating to the module are as follows:

- Output Public Key:
  The Tele-ID displays on the LCD the key, the data and the thumbs-up icons simultaneously. The Tele-ID must receive the command <SEND> (through the keypad or through optical connection) for outputting the public key acoustically in order to allow the User to enroll to the Registration Authority. Then, in order to confirm to the device the correct reception of the public key, a three-digit confirmation number must be inputted into the device (through the keypad or through optical connection). If the correct confirmation number is inputted, the device passes to the service Proof of Possession (if it has been required during the device initialization).

- Proof of Possession (PoP):
  This service can be required by the Registration Authority for the User enrollment and can be addressed only immediately after successful public key confirmation number input, not only after PIN authentication.
  The device displays on the LCD the key, the PoP and the thumbs-up icons simultaneously. The Tele-ID is ready to receive through optical connection the PKCS#10 certificate request's hash value, to sign it and to output the PoP signature acoustically. Than, the Tele-ID should receive a three digits confirmation (through the keypad or through optical connection) to make sure that the PoP signature has been received correctly. Usually, this process is made automatically with the public key registration, without requiring anything from the user, using the optical connection input and the acoustical connection output. If the correct confirmation number is inputted, the device passes to the service signature.

- ECDSA Signature on Data Entered Locally:
  The Tele-ID receives up to 20 digits of data introduced through its keypad or through its optical connection. The command <SEND> makes the Tele-ID calculating and outputting the data ECDSA signature.

- ECDSA Signature on Hash Value:
  The Tele-ID receives through its optical connection a SHA-1 hash value of a document. The command <SEND> makes the Tele-ID calculate and output an ECDSA signature of the SHA-1 hash value.

- ECDSA Signature on Auto-computed Identification Message:
  If the command <SEND> is activated through its keypad or through its optical connection when no data is entered in the Tele-ID, the device calculates an identification message, signs it according to ECDSA and outputs the signature acoustically.

- One Time Password (OTP):
  If the command <CODE> is activated through the device keypad or through optical connection, the device calculates and displays during 30 seconds a new OTP and, if the 'acoustic output of OTP' option is selected during initialization the OTP is also outputted acoustically.

- Change PIN:
  After entering the initial PIN the device can request automatically from the user to enter a new PIN and to confirm it, this is an initialization option. Also, anytime, the user can change his PIN. The new PIN should be chosen in a 'secure' fashion that rejects trivial PIN.

- Stress PIN:
  Instead of entering his PIN, the User can enter a Stress PIN that prevents damages and PIN disclosure during a criminal offence: it can be '*PIN', i.e: *365784 instead of 365784 or 'inverse PIN', i.e.: 454463 instead of 364454. When it is activated with a stress PIN, the Tele-ID seems to operate normally but in fact it warns the server by producing systematically stress signature and stress OTP.

- DTMF Generation:
  After using the <SEND> key once, the User can operate his Tele-ID as a DTMF generator. The input keys (digits 0 to 9, <*/.> and <#/ENTER> keys) generate DTMF tones for transmission down a telephone line.

- Re-Synchronization:
  The Tele-ID can receive through optical protocol a string for correcting the synchronization of its GMT clock. This service can correct a maximum drift of 68 minutes.

- Re-Enrollment:
  The Tele-ID can receive through optical protocol a string that makes the device calculating a new key pair and proceeding to a new enrollment.

- Device Initialization

  Initializes the Tele-ID with proper parameters and generates an ECDSA key pair. This process is procedurally controlled.

These services can be performed without authentication:

- Power Up Self Tests
  The power up self tests are invoked pressing the on/off switch to an active mode.

- Auto Test:
  When the Tele-ID device is in state 'not initialized', if pressing on <SEND> and <ON/OFF> keys, the device start an eleven stage auto-test where the following systems are checked: MCU RAM, LCD with all LED segments and icons, keypad, timekeeper, halt mode, MCU in Run-32kHz mode, MCU in Run-4 MHz mode, DTMF's 8 frequencies acoustic generation, 4 DTMF signals (1, 5, 9, D) acoustic generation, supply voltage detection (SVD) and optical interface.

- Get Serial Number:
  When the Tele-ID is initialized, by pressing <ON/OFF> key and than <#/Enter> the Tele-ID displays the device serial number entered during the initialization process.

- Device Lock:
  The device is programmed to limit the number of PIN attempts should it fall into the wrong hands. When that limit is reached, the device is locked and cannot be operated because the internal data is zeroized.

IV/ List of all Security Functions

This section lists the different algorithms implemented into the cryptographic module:

Approved Security Functions:

- ECDSA: FIPS approved algorithm for generating digital signature per FIPS 186-2 Appendix 6 Curve K 163 described also in ANSI X.9.62
- SHA-1: FIPS approved secure hashing per FIPS 180-2
- DRNG: FIPS approved DRNG per FIPS 186-2, Appendix 3

Non-Approved Security Functions:

- NDRNG

V/ Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC rules. Thus the module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for Home use (Class B). As required by FIPS 140-2 level 3 requirements, the module was tested and then verified in the test report as meeting these FCC requirements. The module and its accompanying documentation is labeled in accordance with FCC requirements with the appropriate FCC warnings.

VI/ Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module provides two distinct operators, the User and the Cryptographic Officer.
2. The cryptographic module provides identity-based authentication, rejecting any non-authorized user.
3. The cryptographic module operates in the FIPS mode when the Tele-ID is initialized with a maximum number of incorrect PINs of nine. The cryptographic module operates in the non-FIPS mode when the Tele-ID is initialized with a maximum number of incorrect PINs of ten - fifteen. Notice that the initialization software does not offer the possibility to initialize the Tele-ID with a value superior to nine incorrect PINs.

4. If the cryptographic module remains inactive for a pre-configured period of 'T' seconds, the module automatically switches off.
5. After 'X' consecutive unsuccessful PIN code validation attempts occur, the cryptographic module automatically zeroizes all contents of RAM. 'X' is a pre-configured value during initialization.
6. After pressing the <ON/OFF> button, the cryptographic module performs the following tests:
    - ECDSA KAT
    - SHA-1 KAT (this is incorporated as part of the ECDSA KAT)
    - DRNG KAT
    - Private key integrity test
7. The module performs the following conditional tests:
    - Continuous DRNG and NDRNG test
    - ECDSA Key Pair Consistency
8. The module uses a FIPS approved DRNG per FIPS 186-2, Appendix 3.
9. The module does not have services to input/output the Tele-ID private key.
10. Authentication data can only be input through the module's keypad.
11. The zeroization service is performed by the Device Lock service, which writes two times over the contents of memory.
12. The module provides status information through the display.
13. Procedural controls are in place to control access to the module before initialization.
14. The minimum PIN length is 6 digits and the maximum PIN length is 8 digits. These are controlled by the module. This meets the probability requirement that is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur.
15. In FIPS mode, the module only allows up to a maximum of 9 wrong PIN attempts before the module zeroizes all data stored in RAM. The probability 9/10^6 is less than the required 1/10^5 that a random attempt will succeed or a false acceptance will occur in a one minute period.
    The Tele-ID supports a non-FIPS approved mode of operation if the parameter that specifies the number of incorrect PIN attempts allowed is greater than 9.
16. The only feedback the module provides is three dash lines during the entry of authentication data.
17. The feedback does not provide information that weakens the strength of the authentication data.

18. The module employs the following physical security mechanisms:

    The tamper evidence equipment of the module consists of 6 ‘FIPS 140-2 approved’ tamper evidence stickers placed on the module. The Tele-ID should be inspected periodically to ensure the six tamper evident seals are in place and not broken.

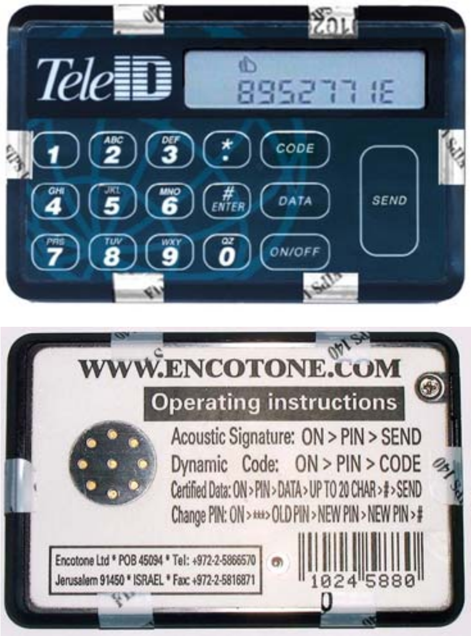
TeleID
895277 IE
1
ABC 2
DEF 3
*
CODE
GHI 4
JKL 5
MNO 6
# ENTER
DATA
SEND
PRS 7
TUV 8
WXY 9
QZ 0
ON/OFF
WWW.ENCOTONE.COM
Operating instructions
Acoustic Signature: ON > PIN > SEND
Dynamic Code: ON > PIN > CODE
Certified Data: ON > PIN > DATA > UP TO 20 CHAR > # > SEND
Change PIN: ON > *** > OLD PIN > NEW PIN > NEW PIN > #
Encotone Ltd * POB 45094 * Tel: +972-2-5866570
Jerusalem 91450 * ISRAEL * Fax: +972-2-5816871
1024 5880

Figure 2: The Tele-ID tamper evidence equipment

19. The module does not utilize an operating system that falls under the definition of a modifiable operational environment per FIPS 140-2.
20. The private ECDSA key component is stored in plaintext form in RAM.

VII/ Definition of Cryptographic Security Parameters

The following are Critical Security Parameters contained in the module:

- ECDSA Private Key: 163-bit ECDSA private key used for signature.
- PIN: Used for authenticating the owner of the card.
- RAND: An initialization vector (RAND) is sent to the module during initialization and is used as part of the NDRNG that then seeds FIPS approved DRNG.

The following is a public key parameter:

- ECDSA Public Key: ECDSA public key that is generated along with the private key component. After keypair generation, the public key component is output and deleted from memory.

VIII/ Definition of CSP Modes of Access

Table 2 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Generate (G): ECDSA public/private key generation.
- Destroy (D): Write over the contents.
- Sign (S): Signature processes using the ECDSA private key.
- Input (I): Input of authentication data.
- Output (O): Output of signature or the public key.
- Compare (C): User PIN verification.

IX/ Service to CSP Access Operation Relationship

Table 2 Services Versus CSP Access

	CSP Access Operation			Applicable Role		
Services	ECDSA Private Key	PIN	RAND	User	Crypto Officer	Unauthenticated
Device Lock	D	D	D	X	X	X
Get Serial Number				X	X	X
Auto Test				X	X	X
Power-Up Self Tests				X	X	X
Re-Synchronization		I C		X	X	
Re-Enrollment	D	I C		X	X	
DTMF Generation		I C		X	X	
OTP Generation				X	X	
ECDSA Signature on Auto-computed Identification Message	S	I C		X	X	
Change PIN		I C		X	X	
Stress PIN		I C		X	X	
ECDSA Signature on Hash Value	S	I C		X	X	
ECDSA Signature on Data Entered Locally	S	I C		X	X	
PoP	S	I C		X	X	
Output Public Key		I C		X	X	
Device Initialization	G		I	X	X	

X/ Mitigation of Other Attacks

No claims of mitigation of other attacks are made.