TOBY-L2 / MPCI-L2 series

Enforced security

Application Note

Abstract

This document describes the implementation of security based on password protected storage. The password protected storage is used to protect customer certificates and private keys.

www.u-blox.com

UBX-19022699 - R01

Document Information

Title	**TOBY-L2 / MPCI-L2 series**	
Subtitle	Enforced security	
Document type	Application Note	
Document number	UBX-19022699	
Revision and date	R01	19-Jul-2019
Disclosure Restriction		

Product status	**Corresponding content status**	
Functional Sample	Draft	For functional testing. Revised and supplementary data will be published later.
In Development / Prototype	Objective Specification	Target values. Revised and supplementary data will be published later.
Engineering Sample	Advance Information	Data based on early testing. Revised and supplementary data will be published later.
Initial Production	Early Production Information	Data from product verification. Revised and supplementary data may be published later.
Mass Production / End of Life	Production Information	Document contains the final product specification.

This document applies to the following products:

Product name	
MPCI-L201-02S	Except for MPCI-L201-02S-00 type number
TOBY-L200-03S	Except for TOBY-L200-03S-00 type number
TOBY-L201-02S	Except for TOBY-L201-02S-00 type number
TOBY-L210-03S	Except for TOBY-L210-03S-00 type number
TOBY-L280-03S	Except for TOBY-L280-03S-00 type number

Contents

1 Introduction

1.1 Scope

The “enforced security” mechanism requires a secure “sanitized” environment, where the initial security personalized data are stored and where the module enforced security is initialized. The initial security personalized data are used to retrieve the master encryption key, which is used to encrypt +USECMNG managed certificates and private keys.

⚠ Once the enforced security is initialized, the security features cannot be disabled and the module is sealed in enforced security mode.

☞ The enforced security mode provides encryption of stored certificates and private keys and only allows an update to the module by means of a firmware update with encrypted signature and signature verification certificate.

2 Enforced security initialization

2.1 Overview

To provide the enforced security feature, the enforced security initialization needs to be executed. The enforced security initialization should be executed in a controlled/sanitized environment.

A sanitized environment is an environment where the customer has complete control of the module and the risk of initial security personalization data exposure is minimal. This environment is usually available in the production/integration stage of the module or in the stage of the initial module personalization.

⚠ The enforced security initialization can be executed only once in a module's lifetime.

The initial security personalization data are stored in the module and used for further encryption/decryption operations.

2.2 Enforced security personalization data

The provided enforced security personalization data are in a form of a string password. This string password is stored in a special storage within the module and is obfuscated using module specific information. The obfuscation provides a minimal/first level of flash exposure protection and a first level of anti-cloning protection.

2.3 Enforced security initialization commands

The +USECCFG AT command shall be used to initialize the enforced security. With this command it is possible to check the status of the enforced security and to initialize it with the password. The command configures and enables the password encryption for +USECMNG managed certificates and private keys.

☞ Once the enforced security is initialized, all the previously certificates and private keys imported with +USECMNG AT command will not be usable anymore.

☞ The +USECCFG AT command enables also the use of encrypted signature for firmware update via +UFWSINSTALL and disables the MD5 based firmware update via +UFWINSTALL and +UFWUPD AT commands.

2.3.1 How to enable the enforced security

Command	Response	Description
`AT+USECCFG=0,1,"my_pwd"`	`OK`	'my_pwd' is the password string. The maximum accepted length for <password> parameter is 128 characters

2.3.2 How to check if enforced security is enabled

Command	Response	Description
`AT+USECCFG=0`	`+USECCFG: 0,1` `OK`	The encryption is enabled and the enforced security is initialized. The parameter <encryption_status> values are: • 0: encryption disabled • 1: encryption enabled

3 Password protected +USECMNG storage

The +USECMNG AT command manages and imports certificates and private keys. This data are used to secure the communication channel, to authenticate the communicating parties and to provide confidentiality of the communication.

The imported certificates and private keys are stored in the module file system in a raw binary format. To provide the best possible security, this data needs to be protected against unauthorized use and copy. The use of enforced security provides a password based encryption mechanism which encrypts the +USECMNG imported certificates and private keys and protects them against unauthorized use.

To enable the +USECMNG encryption, the enforced security needs to be initialized by providing the enforced security password.

☞ The +USECMNG AT command cannot manage at the same time both encrypted and unencrypted data: if the +USECMNG encryption is enabled then all the data that was imported without the encryption cannot be used anymore. All the imported certificates in the non-encryption mode need to be deleted before the +USECMNG encryption is enabled and then re-imported in the encrypted mode.

The +USECMNG AT command does not return any information about the encrypted and non-encrypted modes, but these modes can be retrieved by using the enforced security initialization configuration command +USECCFG (see section 2.3).

4 Enforced Firmware Update security

4.1 Secure Firmware Update package transfer

On TOBY-L2 module series the firmware update package, to be used with +UFWINSTALL, shall be stored in the module file system via FTP protocol.

The FTP protocol uses two distinct connections, one as control connection (used to send FTP commands) and one as data connection (used to send and receive the data bytes). Currently in all TOBY-L2 product versions to which this document does not apply, the FTP client (+UFTP) supports only the encryption of the control connection and therefore it does not satisfy the enhanced firmware update security requirements.

To satisfy the enhanced firmware update security requirements, the products to which this document is applicable shall use the HTTP(S) protocol, which allows the customer to use SSL/TLS to securely transfer the update package.

Be aware that the following examples may be missing other settings related to configuration of the HTTP profile; see the u-blox AT Commands Manual [1].

The transfer of the firmware update package via HTTP(S) is achieved by means of +HTTPC command with <http_command>=100, together with +UHTTP command with <HTTP_secure>=1.

Command	Response	Description
`AT+UHTTP=<profile_id>,6,1[,<USECMNG_profile>]`	`OK`	Enable HTTPS.
`AT+UHTTPC=<profile_id>,100,<path>`	`OK` `+UUHTTPCR: <profile_id>,100,<http_result>,<http_status_code>,<md5_sum>`	Start the transfer of the firmware update package via HTTPS.

To provide an even higher level of security, additional security features are also available via +USECMNG and +USECPRF (for more details see the u-blox AT Commands Manual [1]):

- Usage of certificate pinning
- Usage of advanced cipher-suites:
  - ECDHE-ECDSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-ECDSA-AES128-SHA256

The use of certificate pinning is available by the means of

- extended +USECPRF AT command:
  `AT+USECPRF=<prf_d>,12,<param_val>,<pinning_level>`
- extended import type +USECMNG AT command:
  `AT+USECMNG=<op_code>,3,<…>`

To use of advanced chipper-suites is available by the means of

- extended +USECPRF AT command:
  `AT+USECPRF=<prf_id>,2,255,<iana_ciphersuite_first_byte>,<iana_ciphersuite_second_byte>`

4.2 Encrypted signature firmware update

TOBY-L2 series modules provide the ability to verify the integrity of the update package. The integrity is verified by using an MD5 hash algorithm prior to the start of the installation process.

For all TOBY-L2 product versions to which this document applies, the enhanced firmware update security concept requires the update package authenticity/origin verification in addition to the integrity verification.

The authenticity/origin can be verified with the use of an encrypted signature. The signature is an asymmetrically encrypted hash of the update package. The verification of the signature provides the authenticity/origin as well as the integrity verification.

The process of signature verification is executed by the update feature, which creates the fingerprint of the update package and compares it with the decrypted signature provided by the update command.

The signature decryption uses the public part of the customer provided X.509 certificate. The signature in this case is encrypted using the private part of the same certificate. The generation of the private key, certificate and signature as well as the encryption of the signature is under the customer responsibility.

The firmware update process is started with +UFWINSTALL AT command with the md5 hash passed as parameter. With the enhanced security enabled the firmware update process must be invoked with +UFWSINSTALL AT command, which needs of the <signature> and <usecmng_iname> additional parameters:

- the parameter <signature> is a 64 byte hexadecimal value representing an encrypted SHA-256 fingerprint of the file
- the parameter <usecmng_iname> specifies the internal name of the FW signature verification certificate to be used to decrypt the <signature> and retrieve the SHA-256 file fingerprint, which will be afterwards compared to the actual file retrieved SHA-256 fingerprint.

To provide the ability to upload a FW signature verification certificate, the security data management command (+USECMNG) allows an import of security data with <type>=4, which is a “signature verification certificate”. The +USECMNG list command will display this certificate with a tag “VC”.

The encrypted signature FOTA update is available through:

- extended import type +USECMNG AT command: `AT+USECMNG=<op_code>,4,<…>`
- additional AT command: `AT+UFWSINSTALL=<signature>,<usecmng_iname>`

Example:

- `AT+USECMNG=0,4,"CustomerFWVerificationCert",204`
- `AT+UFWSINSTALL="f5bc0b28d…","CustomerFWVerificationCert"`

4.3 Firmware update package encrypted signature generation

To create a valid firmware update package signature, a customer needs to generate a certificate with the digital signature private key usage option.

The customer must have access to the certificate public and private keys.

The customer retrieves an official firmware update package and generates a SHA256 HASH signature, which is then encrypted using RSA with the private key. The retrieved binary signature must be BASE64 encoded. The customer must import the certificate by using the +USECMNG AT command and use the <internal_name> and BASE64 signature within the +UFWSINSTALL command.

4.3.1 Example of signature generation using openssl and standard linux tools

```
#!/bin/sh
n=$1
basedir=/data/$n
keyfile=$basedir/priv.key
certfile=$basedir/cert.pem
pubpemfile=$basedir/pubkey.pem
keyfile=$basedir/priv.key
outfile=$basedir/signature.bin
outfileb64=$basedir/signature.b64
datafile=$basedir/update.zip
subj=$n

mkdir -p $basedir
openssl req -newkey rsa:2048 -nodes -keyout $keyfile -x509 -days 365 -out $certfile -
nodes -subj '/CN=$subj'
openssl x509 -pubkey -noout -in $certfile  > $pubpemfile
openssl dgst -sha256 -sign $keyfile -out $outfile $datafile
base64 $outfile > $outfileb64
```

Appendix

A Glossary

Abbreviation	Definition
FOTA	Firmware Over The Air
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
MD5	Message-Digest Algorithm
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Table 1: Explanation of the abbreviations and terms used

Related documents

[1] u-blox AT Commands Manual, Doc. No. UBX-13002752
[2] u-blox AT Commands Examples Application Note, Doc. No. UBX-13001820
[3] u-blox Cellular Module Firmware Update Application Note, Doc. No. UBX-13001845

☞ For regular updates to u-blox documentation and to receive product change notifications, register on our homepage (www.u-blox.com).

Revision history

Revision	Date	Name	Comments
R01	19-Jul-2019	amat	Initial release

Contact

For complete contact information, visit us at www.u-blox.com.

u-blox Offices

North, Central and South America

u-blox America, Inc.

Phone: +1 703 483 3180
E-mail: info_us@u-blox.com

Regional Office West Coast:

Phone: +1 408 573 3640
E-mail: info_us@u-blox.com

Technical Support:

Phone: +1 703 483 3185
E-mail: support@u-blox.com

Headquarters
Europe, Middle East, Africa

u-blox AG

Phone: +41 44 722 74 44
E-mail: info@u-blox.com
Support: support@u-blox.com

Asia, Australia, Pacific

u-blox Singapore Pte. Ltd.

Phone: +65 6734 3811
E-mail: info_ap@u-blox.com
Support: support_ap@u-blox.com

Regional Office Australia:

Phone: +61 2 8448 2016
E-mail: info_anz@u-blox.com
Support: support_ap@u-blox.com

Regional Office China (Beijing):

Phone: +86 10 68 133 545
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Chongqing):

Phone: +86 23 6815 1588
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shanghai):

Phone: +86 21 6090 4832
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office China (Shenzhen):

Phone: +86 755 8627 1083
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

Regional Office India:

Phone: +91 80 405 092 00
E-mail: info_in@u-blox.com
Support: support_in@u-blox.com

Regional Office Japan (Osaka):

Phone: +81 6 6941 3660
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Japan (Tokyo):

Phone: +81 3 5775 3850
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

Regional Office Korea:

Phone: +82 2 542 0861
E-mail: info_kr@u-blox.com
Support: support_kr@u-blox.com

Regional Office Taiwan:

Phone: +886 2 2657 1090
E-mail: info_tw@u-blox.com
Support: support_tw@u-blox.com