भारत सरकार
संचारमंत्रालय
दूर संचार विभाग
राष्ट्रीय संचार सुरक्षा केंद्र

सत्यमेव जयते

Government of India
Ministry of Communications
Department of Telecommunications
National Centre for Communication Security

NCCS/SAS/ITSAR/STB/2021-22/ Date 18/03/2022

Subject: Notice for stakeholders consultation meeting on the draft ITSAR of Set Top Box (STB) devices.

Dear Stake holders,

On the directions of DoT Hq, National Centre for Communication Security (NCCS), a subordinate office of Department of Telecommunications headquartered at Bengaluru has taken up the work of development of ITSAR for Set Top Box (STB).

2. Security Assurance Standards (SAS) division under NCCS is responsible for drafting and finalising Indian Telecom Security Assurance Requirements (ITSAR) for communication equipment. In this regard, SAS division will be conducting the stakeholders consultation meeting on the draft ITSAR for STB, vide this meeting inputs will be sought from the industry and subject experts for the finalisation of the ITSAR of STB. The proposed consultation meeting will be conducted in online mode only. The details of the online meeting are as below:

- **Date of meeting: 12/04/2022 at 14:30 Hrs**
- **Registration link:** https://nccs-dot.webex.com/nccs-dot/j.php?RGID=rd8070e50e9197ded1de59bd994fde00f

3. Stakeholders are kindly requested to register and participate in the above meeting. The inputs on the draft ITSAR for Set Top Box (STB) devices may please be mailed to the following Email addresses on or before 05/04/2022. The inputs received will be discussed during the above meeting.

1) Shri M N Pavan Kumar, ADG(SAS-1), NCCS – adg3ttscbg-dot@gov.in
2) Shri P Pani Prasad, Dir(SAS-1), NCCS – dirttsc3.bg-dot@nic.in

4. The draft ITSAR for STB can be downloaded from the websites https://nccs.gov.in, www.tec.gov.in and www.dot.gov.in.

5. This issues with the approval of Sr DDG, NCCS Bengaluru

M. N. Pavan Kumar

ADG(SAS-1)

सत्यमेव जयते

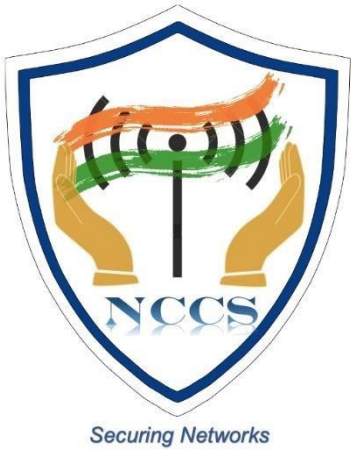
Indian Telecom Security Assurance Requirements

Draft for consultation (DFC)

For

Set Top Box (STB)

NCCS / ITSAR / Broadcasting / STB



National Centre for Communications Security, Bengaluru

Department of Telecom, Ministry of Communications

Government of India

Abstract

This standard specifies the security requirements for digital set top box (STB) used by subscriber to view multichannel television programmes. A Set-top box is a device that receives digital signal, decodes and displays it on television.

Contents

A. Scope

The present document specifies high-level security and data protection provisions for Set Top Box (STB) devices. The security requirements specified through this ITSAR is applicable to following types of Set Top Box (STB) used in the TV services that are delivered through Cable TV, Direct to Home (DTH) systems, Internet Protocol TV (IPTV) & Head-end In the Sky (HITS),

1) **STB one way device:** STB without a return path/(ip) Network interface
2) **STB connectable device:** STB with a return path/(ip) Network interface
3) **FTA STB one way device:** Free to Air (FTA) STB without a return path/(ip) Network interface
4) **FTA STB connectable device:** Free to Air (FTA) STB with a return path/(ip) Network interface

B References

1. ETSI EN 303 645 V2.1.0 (2020-04) - Cyber Security for Consumer Internet of Things: Baseline Requirements

2. ETSI TS 103.701 V.1.1 - Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements

3. ETSI GS ECI 001-5-2 V 1.1.1 - Embedded Common Interface (ECI) for exchangeable CA/DRM solutions;

4. ETSI T3 103.162 V1.1.1 - Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification

C. Definitions

administrator: user who has the highest-privilege level possible for a user of the device, which can mean they are able to change any configuration related to the intended functionality

associated services: digital services that, together with the device, are part of the overall consumer IoT product and that are typically required to provide the product's intended functionality.

EXAMPLE 1: Associated services can include mobile applications, cloud computing/storage and third party Application Programming Interfaces (APIs).

EXAMPLE 2: A device transmits telemetry data to a third-party service chosen by the device manufacturer. This service is an associated service.

authentication mechanism: method used to prove the authenticity of an entity

NOTE: An "entity" can be either a user or machine.

EXAMPLE: An authentication mechanism can be the requesting of a password, scanning a QR code, or use of a
biometric fingerprint scanner.

authentication value: individual value of an attribute used by an authentication mechanism

EXAMPLE: When the authentication mechanism is to request a password, the authentication value can be a character string. When the authentication mechanism is a biometric fingerprint recognition, the authentication value can be the index fingerprint of the left hand.

best practice cryptography: cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques

NOTE 1: This does not refer only to the cryptographic primitives used, but also implementation, key generation and handling of keys.

NOTE 2: Multiple organizations, such as SDOs and public authorities, maintain guides and catalogues of cryptographic methods that can be used.

consumer: natural person who is acting for purposes that are outside her/his trade, business, craft or profession

conditional access system/content protection system: system that uses cryptographic techniques to manage access to digital content

NOTE: Typically, a **content protection system** is either a conditional access system or a digital rights management system.

content provider: party that distributes digital content to a **content receiver**

content receiver: device that is used to access digital content

NOTE: A **content receiver** may contains a chipset with a **content descrambler**.

content descrambler: component in the chipset that is capable of decrypting content

Control Word: Secret key used to encrypt and decrypt content

critical security parameter: security-related secret information whose disclosure or modification can compromise the security of a security module

EXAMPLE: Secret cryptographic keys, authentication values such as passwords, PINs, private components of certificates.

cryptographic hash function: unkeyed cryptographic function that takes data of arbitrary size, referred to as the message, as input and produces an output data block of fixed size, referred to as the message digest

digital signature scheme: keyed asymmetric cryptographic scheme that is used to protect the authenticity of data

NOTE: A **digital signature scheme** consists of a key generation algorithm, a signature generation operation and a signature verification operation. Keys are generated as (secret/private key, public key) pairs. The data is signed using a secret/private key and the corresponding public key is used to verify the signature.

message authentication code algorithm: keyed symmetric cryptographic algorithm that is used to protect the authenticity of data

NOTE: A **message authentication code algorithm** takes a message and a secret key as inputs, and produces an output data block referred to as the MAC. The **message authentication code algorithm** as specified in the present document is used to cryptographically bind a ciphertext message to its associated data; in particular, the algorithm is not used to provide source authentication in the present document.

public-key encryption scheme: keyed asymmetric cryptographic scheme that is used to protect the confidentiality of data

NOTE: A **public-key encryption scheme** consists of a key generation algorithm, an encryption operation and a decryption operation. Keys are generated as (public key, secret/private key) pairs. Data is encrypted using a public key and the data is recovered from the ciphertext using the corresponding secret/private key.

symmetric encryption scheme: keyed symmetric cryptographic scheme that is used to protect the confidentiality of data

NOTE: A **symmetric encryption scheme** consists of a key generation algorithm, an encryption operation and a decryption operation. The encryption and decryption operations of a **symmetric encryption scheme** use the same secret key as input.

debug interface: physical interface used by the manufacturer to communicate with the device during development or to perform triage of issues with the device and that is not used as part of the consumer-facing functionality

EXAMPLE: Test points, UART, SWD, JTAG.

defined support period: minimum length of time, expressed as a period or by an end-date, for which a manufacturer will provide security updates

NOTE: This definition focuses on security aspects and not other aspects related to product support such as warranty.

device manufacturer: entity that creates an assembled final Set Top Box (STB) product, which is likely to contain the products and components of many other suppliers

factory default: state of the device after factory reset or after final production/assembly

NOTE: This includes the physical device and software (including firmware) that is present on it after assembly.

initialization: process that activates the network connectivity of the device for operation and optionally sets authentication features for a user or for network access

initialized state: state of the device after initialization

isolable: able to be removed from the network it is connected to, where any functionality loss caused is related only to that connectivity and not to its main function; alternatively, able to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured

Key Ladder Root Key, or Root Key : Private key (typically 16-byte) used by each compliant chipset at the root of the key ladder.

logical interface: software implementation that utilizes a network interface to communicate over the network via channels or ports

manufacturer: relevant economic operator in the supply chain (including the device manufacturer)

NOTE: This definition acknowledges the variety of actors involved in the STB ecosystem and the complex ways by which they can share responsibilities. Beyond the

device manufacturer, such entities can also be, for example and depending on a specific case at hand: importers, distributors, integrators, component and platform providers, software providers, IT and telecommunications service providers, managed service providers and providers of associated services.

ip network: An IP network is a communication network that uses Internet Protocol (IP) to send and receive messages between one or more machines.

(ip) network interface: physical interface that can be used to access the functionality of STB via a (ip) network

owner: user who owns or who purchased the device

personal data: any information (e.g., details of subscriber, payment related information, viewing history) relating to an identified or identifiable natural person

NOTE: This term is used to align with well-known terminology but has no legal meaning within the present document.

physical interface: physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer

EXAMPLE: Radios, ethernet ports, serial interfaces such as USB, and those used for debugging.

public security parameter: security related public information whose modification can compromise the security of a security module

EXAMPLE 1: A public key to verify the authenticity/integrity of software updates.

EXAMPLE 2: Public components of certificates.

remotely accessible: intended to be accessible from outside the local network

security module: set of hardware, software, and/or firmware that implements security functions

EXAMPLE: A device contains a hardware root of trust, a cryptographic software library that operates within a trusted execution environment, and software within the operating system that enforces security such as user separation and the update mechanism. These all make up the security module.

security update: software update that addresses security vulnerabilities either discovered by or reported to the manufacturer

NOTE: Software updates can be purely security updates if the severity of the vulnerability requires a higher priority fix.

Sensitive-personal data: any information relating to privacy of an identified or identifiable natural person e.g., video stream of a home security camera, payment information, content of communication data and timestamped location data.

sensitive security parameters: critical security parameters and public security parameters

Set Top Box (STB): A Set-top box is a device that receives digital signal, decodes and displays it on television.

Note: This document covers the following 4 different types of STBs,

1) STB one way device: STB without a return path/(ip) Network interface
2) STB connectable device: STB with a return path/(ip) Network interface
3) FTA STB one way device: Free to Air (FTA) STB without a return path/(ip) Network interface
4) FTA STB connectable device: Free to Air (FTA) STB with a return path/(ip) Network interface

Return Path: For interactive applications, the STB may have the provision of processing signal on return path, if the service for return path is provided.

software service: software component of a device that is used to support functionality

EXAMPLE: A runtime for the programming language used within the device software or a daemon that exposes an API used by the device software, e.g. a cryptographic module's API.

telemetry: data from a device that can provide information to help the manufacturer identify issues or information related to device usage

EXAMPLE: A STB device reports software malfunctions to the manufacturer enabling them to identify and remedy the cause.

unique per device: unique for each individual device of a given product class or type

user: natural person or organization

D. Security provisions for Set Top Box (STB)

1.1 No universal default passwords

Provision 1.1-1

Where authentication attributes (e.g., passwords like factory reset password, lock sreen password & parental control pins etc.,) are used and in any state other than the factory default, all STB devices authentication attributes shall be unique per device or as defined by the user.

Device shall not allow any configuration changes without the authentication. Authentication mechanism shall be either through password/pin or through any other mechanism.

Access to OAM interface, debugging or tracing interfaces, such as JTAG, Serial Wire Debug, or MIPI etc., shall be protected with an authentication mechanism.

Provision 1.1-2

Where pre-installed unique per device authentication attributes are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.

Note: This clause is applicable as the uniqueness of authentication attributes is required to minimise risk of automated attacks

Provision 1.1-3

Authentication mechanisms used to authenticate an OAM user in STB device shall use best practice cryptography/strong password.

Access to OAM interface, debugging or tracing interfaces, such as JTAG, Serial Wire Debug, or MIPI etc., shall be protected with an authentication mechanism.

Provision 1.1-4

Where a user can authenticate against a STB device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.

Provision 1.1-5

Device shall have a mechanism available which makes bruteforce attacks on authentication mechanisms via network interfaces impracticable.

Note: OEM to provide mechanisms implemented.

1.2 Implement a means to manage reports of vulnerabilities

Provision 1.2-1

It shall be ensured that no known critical/ high/medium (as per CVE-IDs of NIST- NVD) vulnerabilities(as on date of offer of STB device to designated lab for testing) shall exist in the STB device. For low/uncategorised (as per CVE-IDs of NIST- NVD) category vulnerabilities remediation plan is to be provided.

1.3 Keep software updated

Provision 1.3-1

All updateable software components in STB devices should be securely updateable.

Updatable components: Applications, Operating system and firmware & Bootloader components shall be updatable.

Provision 1.3-2

STB device shall have an update mechanism for the secure installation of updates.

Provision 1.3-3

Automatic mechanisms should be used for software updates.

Note: OEM to provide mechanisms implemented.

Provision 1.3-4

The device should check after initialization, and then periodically, whether security updates are available.

Note: OEM to provide mechanisms implemented.

Provision 1.3-5

STB device shall support automatic updates and/or update notifications. Updates shall be mandatorily applied on to the STB device once it is made available for the device to update.

Note: OEM to provide mechanisms implemented.

Provision 1.3-6

The device shall use best practice cryptography to facilitate secure update mechanisms.

Provision 1.3-7

STB device should verify the authenticity and integrity of software updates.

Provision 1.3-8

Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.

Provision 1.3-9

The device shall display the upgrade/update status of the STB device to the user.

Provision 1.3-10

The model designation of the STB device shall be clearly recognizable, either by labelling on the device or via a physical interface or via a GUI.

1.4 Securely store sensitive security parameters

Provision 1.4-1

Sensitive security parameters (e.g., passwords, pins, secrets etc.,) in persistent storage shall be stored securely by the STB device.

Provision 1.4-2

Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.

Note: OEM to provide mechanisms implemented.

Provision 1.4-3

Hard-coded critical security parameters in device software source code preferably not to be used. if critical security parameters are embedded in the STB SW, these parts of code should be protected against reverse engineering e.g. by using strong obfuscation

Note: OEM to provide mechanisms implemented.

Provision 1.4-4

Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per class of devices and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.

1.5 Communicate securely

Provision 1.5-1

The STB device shall use best practice cryptography to communicate securely

Provision 1.5-2

The STB device should use reviewed or evaluated implementations to deliver network (if IP interface is supported) and security functionalities, particularly in the field of cryptography.

Provision 1.5-3

Cryptographic algorithms parameters should be updateable.

For devices that cannot be updated, it is important that the intended lifetime of the device does not exceed the recommended usage lifetime of cryptographic algorithms used by the device (including key sizes).

Note: Algorithm parameters (e.g., key sizes, hash sizes)

Provision 1.5-4

STBs shall restrict the access to the device functionality including security relevant changes in configuration over the network (via IP interface). If permitted, access to device functionality via a network interface (IP interface) in the initialized state should only be possible after authentication on that interface.

Provision 1.5-5

Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.

Critical security parameters (e.g., intermediate keys, control word, crypto algorithm parameters like initialisation vector in case of AES)

Provision 1.5-6

The STB device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.

Critical security parameters (e.g., intermediate keys, control word, crypto algorithm parameters like initialisation vector in case of AES) remotely accessible network

Provision 1.5-7

The manufacturer shall follow secure management processes for critical security parameters that relate to the device.

1.6 Minimize exposed attack surfaces

Provision 1.6-1

All unused network and logical interfaces shall be disabled.

Provision 1.6-2

Device hardware should not unnecessarily expose physical interfaces to attack.

Provision 1.6-3

Where a debug interface is physically accessible, it shall be disabled in software.

Provision 1.6-4

The manufacturer should only enable software services that are used or required for the intended use or operation of the device.

Provision 1.6-5

Code should be minimized to the functionality necessary for the service/device to operate.

Provision 1.6-6

Software should run with least necessary privileges, taking account of both security and functionality.

Provision 1.6-7

The device should include a hardware-level access control mechanism for memory.

Provision 1.6-8

The manufacturer should follow secure development processes for software deployed on the device.

Undertaking is to be provided

1.7 Ensure software integrity

Provision 1.7-1

The STB device should verify its software using secure boot mechanisms.

Provision 1.7-2

STB device shall check periodically for detection of any unauthorized change to/installation of the software.

In case of detection of any such unauthorized changes, STB shall display the error code in the gui to the end user

Provision 1.7-3

Installation of apps from untrusted sources should be disabled.

If installation of apps is not supported the same may be declared.

1.8 Ensure that personal data is secure

Provision 1.8-1

The confidentiality of personal data (if collected by STB device) transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.

Note: personal data (e.g., details of subscriber, payment related information, viewing history) associated services (provided by the oem/operator)

Provision 1.8-2

The confidentiality of sensitive personal data (if collected by STB device) communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.

Sensitive-personal data examples are: video stream of a home security camera, payment information, content of communication data and timestamped location data.

Provision 1.8-3

All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.

If device doesn't offer such capabilities the same may be declared.

1.9 Examine system telemetry data

Provision 1.9-1

If telemetry data is collected from STB device and services, such as usage and measurement data, it should be examined for security anomalies.

1.10 Make it easy for users to delete user data

Provision 1.10-1

The user shall be provided with functionality such that user data (if collected by STB device) can be erased from the device in a simple manner.

User data such as Personal data, Sensitive-personal data, user configuration and cryptographic material such as user passwords or keys.

Provision 1.10-2

Users should be given clear instructions on how to delete their personal data (if collected by STB device)

1.11 Validate input data

Provision 1.11-1

The STB device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

2. Data protection provisions for STB

Provision 2.1-1

If telemetry data/ personal data is collected from STB devices, consumers shall be provided with information on what telemetry data/ personal data/sensitive-personal data is collected, how it is being used, by whom, and for what purposes.

3. CAS Specific requirements

Provision 3.1-1

Interface between key ladder and descrambling/decryption module shall be secured. Output of CW Keyladder should always goto descrambler/decryption module only (without any option "to change the destination"/ "for intermediate tapping")

Provision 3.1-2

STB device shall not expose CWs/Intermediate keys in plain text form in RAM/NVM.

Provision 3.1-3

Root key/Master key shall be securely stored with read/write lock. Root Key/Master key is to be shared only via a secured path (without any option "to change the destination"/ "for intermediate tapping") to authorised services/components (as specified by OEM) of STB device.

Provision 3.1-4

Cryptographic practices used in CAS implementation & CW security shall follow secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

In case of proprietary cryptographic controls are implemented then the key length shall be matched to the equivalent secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)”.

Provision 3.1-5

Fingerprinting/watermarking of the content shall follow industry best practices.

E. Table: Implementation of provisions for different types of Set top box (STB)

Requirement	Connected device	One way device	FTA - connected device	FTA - one way device
D. Cyber security provisions for Set Top Box (STB)				
1.1 No universal default passwords				
Provision 1.1-1	Applicable	Applicable	Applicable	Applicable
Provision 1.1-2	Applicable	Applicable	Applicable	Applicable
Provision 1.1-3	Applicable	Applicable	Applicable	Applicable
Provision 1.1-4	Applicable	Applicable	Applicable	Applicable

Provision 1.1-5	Applicable	Not Applicable	Applicable	Not Applicable
1.2 Implement a means to manage reports of vulnerabilities				
Provision 1.2-1	Applicable	Applicable	Applicable	Applicable
1.3 Keep software updated				
Provision 1.3-1	Applicable	Applicable	Applicable	Applicable
Provision 1.3-2	Applicable	Applicable	Applicable	Applicable
Provision 1.3-3	Applicable	Applicable	Applicable	Applicable
Provision 1.3-4	Applicable	Applicable	Applicable	Applicable
Provision 1.3-5	Applicable	Applicable	Applicable	Applicable
Provision 1.3-6	Applicable	Applicable	Applicable	Applicable
Provision 1.3-7	Applicable	Applicable	Applicable	Applicable
Provision 1.3-8	Applicable	Applicable	Applicable	Applicable
Provision 1.3-9	Applicable	Applicable	Applicable	Applicable
Provision 1.3-10	Applicable	Applicable	Applicable	Applicable
1.4 Securely store sensitive security parameters				
Provision 1.4-1	Applicable	Applicable	Applicable	Applicable
Provision 1.4-2	Applicable	Applicable	Applicable	Applicable
Provision 1.4-3	Applicable	Applicable	Applicable	Applicable
Provision 1.4-4	Applicable	Applicable	Applicable	Applicable
1.5 Communicate securely				
Provision 1.5-1	Applicable	Not applicable	Applicable	Not applicable
Provision 1.5-2	Applicable	Not applicable	Applicable	Not applicable
Provision 1.5-3	Applicable	Applicable	Applicable	Applicable
Provision 1.5-4	Applicable	Not applicable	Applicable	Not applicable
Provision 1.5-5	Applicable	Applicable	Not applicable	Not applicable
Provision 1.5-6	Applicable	Applicable	Applicable	Applicable
Provision 1.5-7	Applicable	Not applicable	Applicable	Not applicable
1.6 Minimize exposed attack surfaces				
Provision 1.6-1	Applicable	Applicable	Applicable	Applicable
Provision 1.6-2	Applicable	Applicable	Applicable	Applicable
Provision 1.6-3	Applicable	Applicable	Applicable	Applicable
Provision 1.6-4	Applicable	Applicable	Applicable	Applicable
Provision 1.6-5	Applicable	Applicable	Applicable	Applicable
Provision 1.6-6	Applicable	Applicable	Applicable	Applicable

Provision 1.6-7	Applicable	Applicable	Applicable	Applicable
Provision 1.6-8	Applicable	Applicable	Applicable	Applicable
1.7 Ensure software integrity				
Provision 1.7-1	Applicable	Applicable	Applicable	Applicable
Provision 1.7-2	Applicable	Applicable	Applicable	Applicable
Provision 1.7-3	Applicable	Applicable	Applicable	Applicable
1.8 Ensure that personal data is secure				
Provision 1.8-1	Applicable	Applicable	Applicable	Applicable
Provision 1.8-2	Applicable	Applicable	Applicable	Applicable
Provision 1.8-3	Applicable	Applicable	Applicable	Applicable
1.9 Examine system telemetry data				
Provision 1.9-1	Applicable	Applicable	Applicable	Applicable
1.10 Make it easy for users to delete user data				
Provision 1.10-1	Applicable	Applicable	Applicable	Applicable
Provision 1.10-2	Applicable	Applicable	Applicable	Applicable
1.11 Validate input data				
Provision 1.11-1	Applicable	Applicable	Applicable	Applicable
2 Data protection provisions for consumer IoT				
Provision 2.1-1	Applicable	Applicable	Applicable	Applicable
3. CAS Specific requirements				
Provision 3.1-1	Applicable	Applicable	Not Applicable	Not Applicable
Provision 3.1-2	Applicable	Applicable	Not Applicable	Not Applicable
Provision 3.1-3	Applicable	Applicable	Not Applicable	Not Applicable
Provision 3.1-4	Applicable	Applicable	Not Applicable	Not Applicable
Provision 3.1-5	Applicable	Applicable	Not Applicable	Not Applicable