



Key Bridge Global LLC
1600 Tysons Blvd., Suite 450
McLean, VA 22102
Tel: 703 414 3500
Fax: 703 414 3501

TV Bands Database

Registration, Authentication and Security

--

Rules, Interpretations and Implementation

Printed: Monday, August 17, 2009

Document Information

Document Purpose	To capture and document industry consensus relating information assurance, counter-party authentication and transaction security for a TV bands database.
Document Status	Live document / Working Draft
Author/Editor	Jesse Caulfield <jesse.caulfield@keybridgeglobal.com>
Copyright	© 2009 Key Bridge Global LLC

Document History

Date	Author/Editor	Edit Summary	Doc Version
05/15	Jesse Caulfield	First draft – high level architecture and data model	0.1
06/19	Jesse Caulfield	Extensive rewrite for expected public release. Limit scope to security related matters. Interface transactions moved and consolidated in to Architecture doc.	0.2
07/30	Jesse Caulfield	Added device state discussion	0.3
08/08	Jesse Caulfield	Updated risk scenarios, added TLS transport security option	0.4
08/10	Jesse Caulfield	Incorporated industry comments and requested edits Added Mode-I security concerns	0.5
08/13	Jesse Caulfield	Incorporated industry comments and requested edits	0.6
08/17	Jesse Caulfield	Incorporated industry comments and requested edits	0.7

Document Notes

Because the proceeding remains under consideration the requirements may change. Where we believe this may occur we have tried to accommodate by adding flexibility and options to the interface and session design.

Where explicitly stated in the current Rules (as published in the Federal Register) the terms MUST, SHALL and WILL are used. Where there may be room for interpretation or discretion is explicitly granted, this document attempts to enumerate possible options and weigh their cost/benefit to advise commercial policy.

Executive Summary

Registration and Commercial Accounts

- Only valid devices may register with the Database using proper FCC ID and serial number
- Fixed & Mode-II devices must establish a commercial account with the Database administrator prior to receiving channel lists
- Flexible account structures may be required to ensure consumer convenience and adoption
- Devices should report their transmitting channel to the Database

Security Concerns

- The principle concern is interference, either purposeful or by accident
- Unauthorized Databases and purposefully mis-configured Mode-I devices are a significant concern
- Most security risks can be addressed by assuring the identity of and communication path between TVBDs and the Database

Security Procedures

- Only authorized TVBDs may connect to a Database
- All TVBDs must only connect to and receive channel lists from an authorized Database

Security Technologies

- TVBDs and the Database must support and employ mutual authentication
- Fixed and Mode-II TVBDs should connect to the Database with an IPSEC tunnel
- If IPSEC is not possible, TVBDs may connect to the Database using TLS
- Unencrypted communications are not allowed between TVBDs and the Database

Table of Contents

Document History	2
Document Notes	2
Executive Summary	2
Table of Contents	3
Summary of Database Principles and Services	4
Requirements	4
Interpretation	4
Discussion of Device Status and Operational Lifecycle.....	6
Requirements	6
Interpretation	7
TVBD Registration	9
Commercial Accounts with the Database Administrator	10
Discussion of System Risks and Concerns.....	12
Commission Statement.....	12
Interpretation	12
Unauthorized Devices.....	13
Valid but Mis-configured Devices	15
Database Reflectors.....	16
Unauthorized Database Operators.....	18
Mode-I Long-Distance Links.....	20
Multi-homed Mode-I Devices.....	21
Discussion of Security Technologies and Recommendations	22
IPSEC Transport Security.....	23
Transport Layer Security.....	23
Discussion of Authentication versus Authorization.....	24
Summary of Commercial Database Requirements and Recommendations.....	26
Appendix: Questions & To Do List	27

Summary of Database Principles and Services

Requirements

Title 47: Telecommunication

PART 15—RADIO FREQUENCY DEVICES

Subpart H—Television Band Devices

§ 15.713 TV bands database.

- (f) *Fixed TVBD registration. (1) Prior to operating for the first time or after changing location, a fixed TVBD must register with the TV bands database by providing the information listed in paragraph (f)(3) of this section.*
- (g) *A personal/portable device operating in Mode II shall provide the database its FCC Identifier (as required by §2.926 of this chapter), serial number as assigned by the manufacturer, and the device's geographic coordinates (latitude and longitude (NAD 83) accurate to ±50 m)*

§ 15.714 TV bands database administration fees.

- (a) *A TV bands database administrator may charge a fee for provision of lists of available channels to fixed and personal/portable TVBDs and for registering fixed TVBDs and temporary BAS links.*

Interpretation

While security is not generally addressed in the Rules, the following principles are clearly spelled out:

- 1) All Fixed TVBDs must register their identifying information with the Database prior to Initialization.¹
- 2) Mode-II TVBDs are NOT required to register with the Database. Rather, they must present their uniquely identifying credentials (FCC ID and device serial number) when initializing a connection to the Database.²
- 3) Fixed and Mode-II devices must ensure they receive channel lists directly from an authorized Database.
- 4) Mode-I devices are NOT required to register or otherwise communicate with the Database in any way.
- 5) The Database may not impose a fee on the operation of Mode-I devices in any way.
- 6) The Database is authorized to charge fees for the following commercial services:³
 - a. Registering Fixed TVBDs
 - b. Registering temporary BAS links⁴
 - c. Provision of channel lists (to Fixed *and* Mode-II devices)

¹ See 15.713 (f)(3). Also see *Registration* and *Initialization* in this document.

² See 15.713 (g)

³ See 15.714(a)

⁴ Broadcast Auxiliary Services

Required Database Services

It is further required in the Rules that certain information services will be provided by the Database administrator at no cost for the benefit of certain end-users.⁵

For the FCC:

- The administrator will develop and maintain a system whereby the Commission may take enforcement action against a specific TVBD or model of TVBD

For other Database administrators:

- The administrator will develop and maintain a system to exchange and synchronize database content

For the community of incumbent, protected broadcast service providers:

- The administrator will develop and maintain a system for end-users to verify, correct and remove inaccurate records

For the community of low power auxiliary device (microphone) users:

- The administrator will develop and maintain a system for protecting facilities and channel usage during defined events

Paid Services

The following services are provided by the Database administrator for a fee.⁶

For temporary BAS Links

- The administrator will develop and maintain a system to create, maintain and remove registration information for temporary BAS links

For Fixed and Mode-II TVBDs

- The administrator will develop and maintain a system to create, maintain and remove registration information for Fixed TV band devices
- The administrator will develop and maintain a system to calculate and provide, in near real-time, lists of available channels on a non-discriminatory basis

⁵ See 15.715

⁶ See 15.714 (a)

Discussion of Device Status and Operational Lifecycle

Requirements

Title 47: Telecommunication

PART 15—RADIO FREQUENCY DEVICES

Subpart H—Television Band Devices

§ 15.711 Interference avoidance mechanisms.

(c) Spectrum sensing

- (6) *Personal/portable devices operating in the client mode shall identify to the fixed or Mode II personal/portable device those television channels on which it senses any signals above the detection threshold. The fixed or Mode II device shall respond in accordance with the provisions of this paragraph as if it had detected the signal itself.*

(g) *A personal/portable TVBD operating in Mode I may only transmit upon receiving the transmissions of fixed or Mode II TVBD. A personal/portable device operating in Mode I may transmit on either an operating channel of the fixed or Mode II TVBD or on a channel the fixed or Mode II TVBD indicates is available for use.*

§ 15.713 TV bands database.

(e) TVBD initialization.

- (1) *Fixed and Mode II TVBDs must provide their location and required identifying information to the TV bands database in accordance with the provisions of paragraph (b) of this section.*
- (2) *Fixed and Mode II TVBDs shall not transmit unless they receive, from the TV bands database, a list of available channels.*
- (3) *Fixed TVBDs register and receive a list of available channels from the database by connecting to the Internet, either directly or through another fixed TVBD.*
- (4) *Mode II TVBDs register and receive a list of available channels from the database by connecting to the Internet, either directly or through a fixed TVBD.*

(f) Fixed TVBD registration.

- 1) *Prior to operating for the first time or after changing location, a fixed TVBD must register with the TV bands database by providing the information listed in paragraph (f)(3) of this section.*

(g) *A personal/portable device operating in Mode II shall provide the database its FCC Identifier (as required by §2.926 of this chapter), serial number as assigned by the manufacturer, and the device's geographic coordinates (latitude and longitude (NAD 83) accurate to ± 50 m)*

§ 15.714 TV bands database administration fees.

(a) *A TV bands database administrator may charge a fee for provision of lists of available channels to fixed and personal/portable TVBDs and for registering fixed TVBDs and temporary BAS links.*

Interpretation

Only Fixed and Mode-II devices may request channel lists from the Database. There are four possible states for Fixed and Mode-II TV band devices with regard to their operation:

State	Device Status	Database Status	Transmit Status
1	Unregistered and inactive	No database record	Not able to transmit
2	Registered and inactive	Database record but no valid channel list	Not able to transmit
3	Registered and active	Database record plus valid channel list	Able to transmit
4	In Service	Not connected	Able to transmit

The registration of devices and protected services is addressed several times and in several contexts within the Rules that may lead to confusion. We therefore define the following terms for semantic clarity:

Registration is the creation of an active, valid and complete record in the Database. In the context of this document we focus on device registration which is a prerequisite for unlicensed operation of Fixed TV band devices. Device registration is a separate and distinct process from commercial account creation.

Protected services registration is a similar but independent procedure to create active, valid and complete records in the Database describing services entitled to protection but not already in one of the FCC's databases.^{7,8} Protected services registration is outside the scope of this document, which focuses on device registration.

Initialization is a process through which a IP host, which includes TV band devices and possibly other third-party applications, establishes a network communications link (connection) with the Database. Successful initialization indicates that the connecting IP host is properly registered and/or authenticated with the Database.

Function describes a transactional process by which applications on both sides of a connection may exchange useful information. A common, well-known example is the 'HTTP GET' function, through which a web browser requests and receives a specific web object (page, image, etc.).⁹ Similarly, 'CHANNEL QUERY' is a function within the context of TV band devices through which a TVBD may query the Database for a list of available channels at its location.

Once a connection is initialized the connecting party may create any number of sessions. A session may support any number of allowed transactions. In the context of TV bands, the most common function will be a query for channel lists.

Fixed and Mode-II devices are very similar in their operation with the exception that that Mode-II devices must transmit at lower power and expected to move more often. They share a similar state diagram but Mode-II devices should experience more frequent transitions from 'In Service' to 'Channel Query'.

⁷ See 15.713 (b)(2)

⁸ Fixed device Registration requires both a record of the device's identifying information as defined in 15.713 (f)(3) in the Database and a commercial account with the Database administrator. Mode-II TVBDs are not required to maintain a record in Database but may be required to establish a commercial account with the Database administrator for the settlement of fees.

⁹ See RFC 1945: Hypertext Transfer Protocol -- HTTP/1.0 Section 8.1 for the original definition

Prior to beginning transmission (“In Service”), all devices must sense, or ‘listen’, for 30 seconds to ensure their selected channel is not occupied by a protected service the Database may be unaware of.¹⁰ Once in service, devices must continue to sense once every 60 seconds. If a protected service is detected, the device must cease transmitting on that channel. Mode-I devices differ only in that they must also notify their Master TVBD of any in-service sensing violation. In practice, such notifications will likely be made over an existing TV bands data link and immediately prior the cessation of transmission.

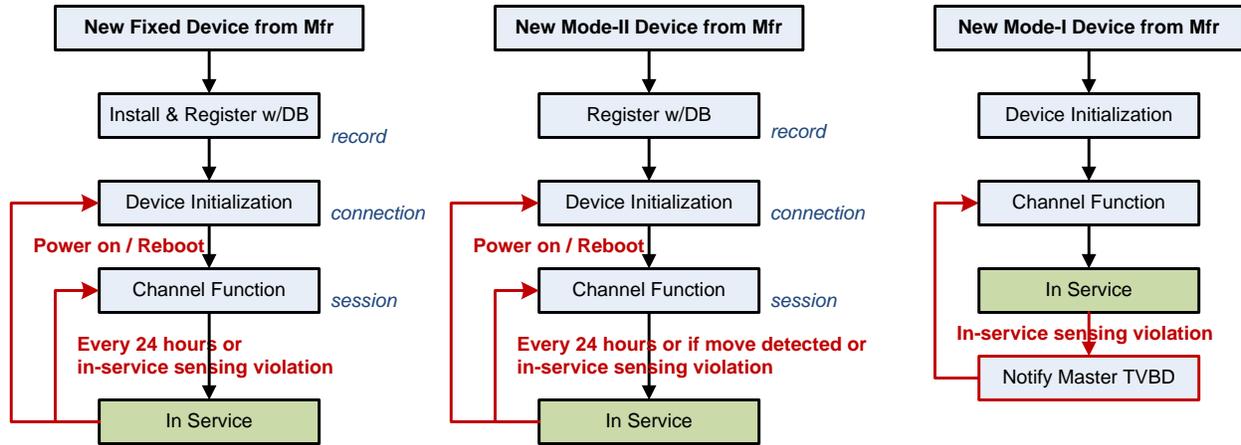


Figure 1: State diagrams for Fixed, Mode-II and Mode-I TVBDs indicating device state plus when fixed or Mode-II devices may establish connections and sessions with the Database. Note that the Mode-I state diagram applies to any TV band device operating in client mode.

Lastly, the Database must provide a method and practice for the Commission to deny service to any individual or class of TV band device (Fixed, Mode-II and Mode-I). In practice, enforcement against Mode-I devices is implemented by the Database via proxy through Fixed and Mode-II devices.

¹⁰ TVBD ‘listen’ or ‘sense’ is not technically defined. See Appendix for a brief discussion.

TVBD Registration

The Commission's published commentary anticipates two general modes of operation for TV band devices: Fixed and Personal / Portable.¹¹ The Personal / Portable category is further subdivided by capability: Mode-II (Master) devices able to initiate and manage a wireless network and Mode-I (Client) devices that join and access those TV band networks.

Registration, as defined earlier, is the creation of an active, valid and complete record in the Database. Registration is a prerequisite for unlicensed operation of Fixed TV band devices.

It should be noted that device registration is not coupled in any way with the creation of a commercial account with the Database administrator. Device registration and commercial accounts are neither prerequisites or requirements of one another; they may be established and maintained separately by independent parties.

Fixed and Mode-II devices have individual and unique registration requirements, which are detailed below.

Registration of Fixed Devices

Commission Statement

21. Overview of Rules for Unlicensed TV Band Devices. The new rules provide for operation of two types of unlicensed TVBDs that may provide broadband data and other types of communications services:

- 1) Fixed devices, which will operate from a fixed location with relatively higher power and could be used to provide a variety of services including wireless broadband access in urban and rural areas, and*

Interpretation

The Commission expects that Fixed devices will be just that: installed in or on a fixed, non-moving structure and intended to act as infrastructure for the delivery of wireless services. More often than not, a service professional is expected to be involved in the installation and possibly the commissioning of Fixed TVBDs. A Fixed device registration process should be designed to accommodate these expectations.

The Database administrator will therefore provide, at minimum, a secure web portal for the registration of Fixed TVBDs. Professional installers and/or end-users of Fixed TVBDs may create, review, update and delete, if desired, their own registration information through the web portal.

Registration of Mode-II Devices

Commission Statement

- 2) personal/portable devices, which will use lower power and could, for example, take the form of devices such as Wi-Fi-like cards in laptop computers or wireless in-home local area networks (LANs)...*

Interpretation

Mode-II TVBDs are anticipated to take the form of various consumer products. The Rules attempt to provide maximum flexibility for Mode-II device operation while preserving the basic requirement that they must always directly access the Database for channel lists.

Mode-II devices are currently not required to register with the Database.

¹¹ Federal Register / Vol. 74, No. 30 / Tuesday, February 17, 2009 / Rules and Regulations

Commercial Accounts with the Database Administrator

Only the TVBD and BAS link operators are required to establish a commercial relationship with a Database administrator and to pay for services. Registration and channel list fees are expected to cover the costs to support TVBD operation plus various supporting administrative information services that must be provided.

Registration of temporary BAS links and Fixed TVBDs is a relatively straightforward commercial transaction and is expected to be principally business-to-business.

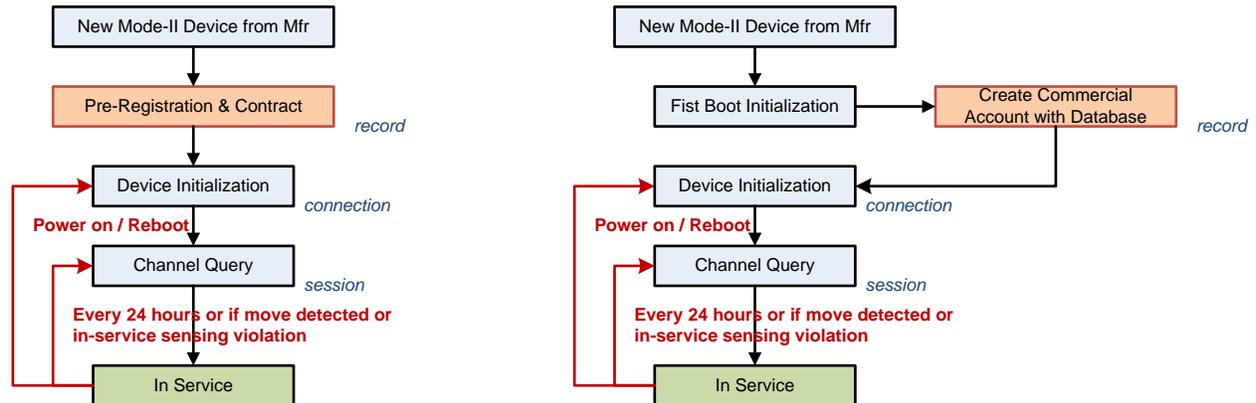


Figure 2: Alternate state diagrams for Mode-II devices. Any valid device may be Registered, and registered devices are authenticated to connect with the Database. A valid commercial account or contract authorizes the creation of sessions, allowing TVBDs to query the Database for an available channel list.

The day-to-day operation of Fixed and Mode-II TVBDs is more involved and will require a standing commercial account between the TVBD owners and the Database administrator with credits, debits and transaction detail reporting.

This is particularly important for Mode-II consumer products intended to be sold at retail, like home gateway routers and wireless access points. The Database must charge for channel lists to cover the cost of operation and present Rules may obligate potentially millions of Mode-II consumers to establish a commercial account with the Database administrator prior to the operation of their TV bands device.

Industry very much wishes to minimize any burden on consumers and barriers to successful, widespread commercial adoption. Below we discuss some options currently under consideration to enable Database access for Mode-II devices.

Pre-paid Contracts

One method to simplify the end-user experience is to bundle a pre-paid channel-query license with Type-II devices prior to consumer activation. Payments could occur at the device point of sale or at the time of manufacturer and be structured as a device activation fee.

A pre-paid license fee would remove any continuing financial obligation on end-users for operation of Mode-II devices and is generally regarded as the best possible solution for consumers.

Structurally, this process would include a pre-paid services contract and Mode-II device registration procedure. The device's identifying information would be marked by the Database as not requiring an associated user account.

Agency Accounts

Another option to minimize the impact on consumers would be for their network service provider to either directly absorb channel inquiry costs or to act as Database billing agent; collecting channel list fees as a surcharge on behalf of the Database administrator.

This option would hide but not eliminate account management requirements from the consumers. However, it does not accommodate un-tethered users not associated with a participating service provider.

Retail Accounts

As a catch-all, and preferably last resort, the Database must provide retail account management capability to support Mode-II consumers who cannot be accommodated by either of the above options.

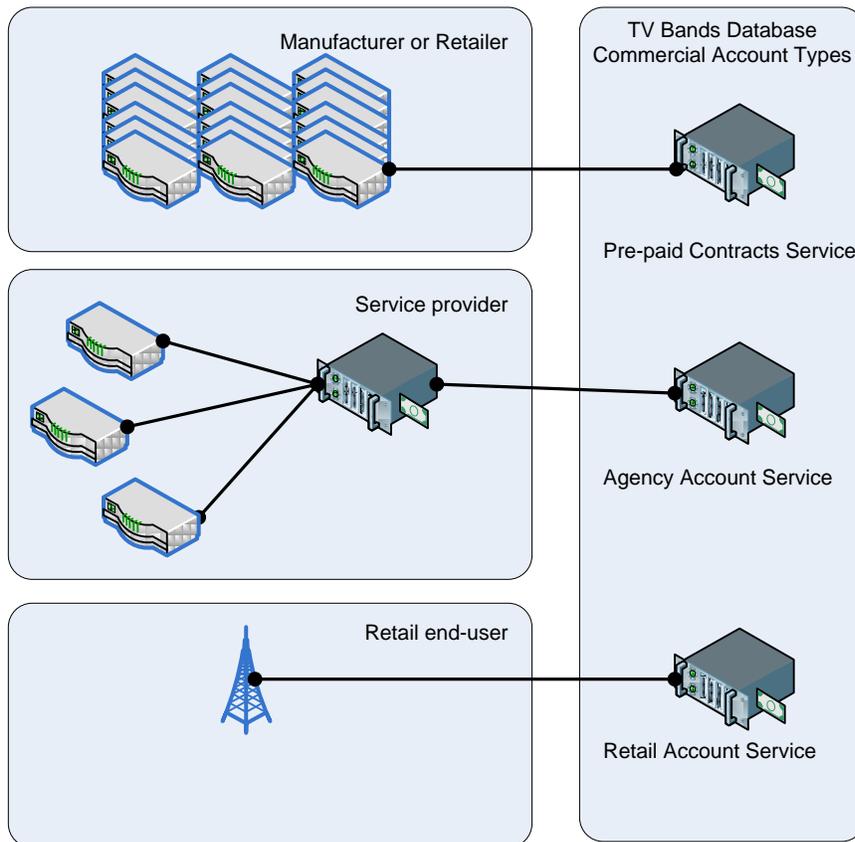


Figure 3: Three concepts for the convenient structuring of Database administrator commercial accounts. Flexible accounts and payment options will be necessary to accommodate unforeseen end-user business models and to minimize the inconvenience for adoption by consumers and service providers.

Discussion of System Risks and Concerns

Commission Statement

...The Commission recognizes the importance of protecting licensed services from harmful interference and the novel challenges involved in reliably identifying unused TV channels. Therefore, it is taking a cautious and conservative approach in this plan, balancing the need to provide sufficient opportunities for proponents to develop viable unlicensed TV band devices (TVBDs) with measures to ensure that such devices fully protect the important licensed services that operate in the TV bands.....¹²

Interpretation

The TV bands database (“Database”) exists primarily to assure proper geographic separation of unlicensed devices from licensed TV transmitters. The Commission goes so far as to anticipate a future where spectrum sensing technology has matured enough that the Database may not be necessary. Until that time however, the Database is the primary method, with sensing as a backup, for identification of unoccupied TV band channels and interference protection.

While the Rules generally do not discuss system security or information assurance, one can read throughout the Report and Order an understood trust and expectation that each component of the system is truly what it represents, is properly configured and will act in a prescribed and predictable manner.

The Database serves as the core of the TV bands system, and must provide a verifiable, secure and authenticated Internet service available to all parties. Accordingly, only valid clients may access the database, and then only for prescribed and well defined purposes.

Database system reliability, authenticity and availability are critically important to all interested parties for the successful operation of unlicensed devices in the TV bands. Incumbent operators will rely upon the Database to ensure their continued and uninterrupted business operation, while new wireless service providers will be operationally dependent upon accurate channel lists.

Until sensing technology is sufficiently mature an assured, verifiable and robust end-to-end Database service is mandatory for successful unlicensed operation in the TV bands.

The Rules expose several important gaps and risks that must be addressed prior to wide commercial acceptance and implementation. The good news is that few are unique to TV bands but rather represent variations of threats already encountered by other Internet-based information systems and services.

¹² See Federal Register / Vol. 74, No. 30 / Tuesday, February 17, 2009 / Rules and Regulations, para. 4

Unauthorized Devices

The Commission currently does not make equipment authorization data available in machine-readable format. It is therefore impossible for the Database to implement automated summary verification of TVBD identification at the time of registration or initialization against an authenticated source. As a consequence, it will be very difficult if not impossible to deny registration to devices (certified or otherwise) that present any properly formatted FCC ID and serial number.

In practice the TV bands database represents a closed information system accessible only by authorized clients and not to the general Internet public. However, Commission policy regarding the EA database precludes the Database from automating the verification of a TVBDs identifying information (FCC ID and Serial Number). This raises three important risks:

- Valid devices may register with the Database with improper FCC ID or serial numbers
- Valid devices may also register with the Database with bogus FCC ID and serial numbers
- Invalid devices may register with the Database using either bogus or cloned FCC ID and serial numbers

“Improper” credentials are identifying information purposefully malformed to circumvent the authentication process entirely, whereas “bogus” credentials are forged or fraudulent identifying information intended to pass as a valid or otherwise authorized and which may have previously been authenticated.

The differences are important. Access attempts with improper identification could indicate malicious intent but would be denied access. For example, improper identification could be used in brute force denial of service (DoS) attacks against the Database.

In contrast, bogus identification could indicate malicious intent to gain access to the Database and information systems. Once granted access to the system a malicious user could attempt further intrusion.

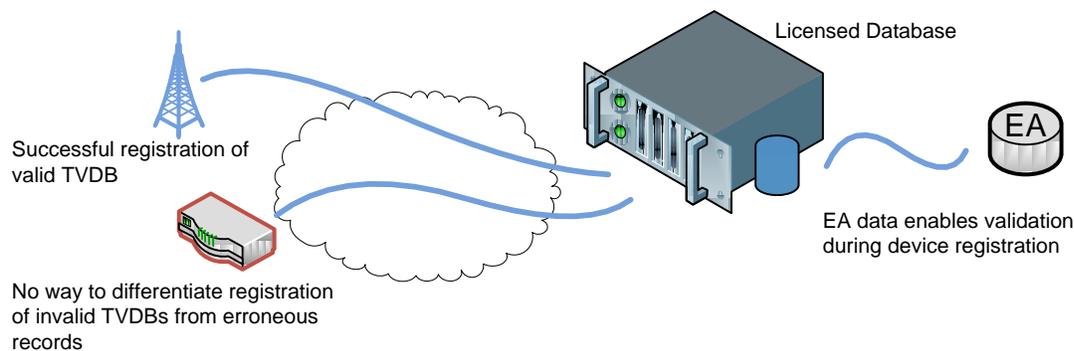


Figure 4: Without the ability to verify TVBD identification the Database cannot differentiate honest registration mistakes from invalid or bogus registration or malicious attack.

Another concern is that devices might present valid identification (i.e. a valid FCC ID and Serial Number) but not be the actual device to which that identification was assigned. This scenario is similar to a hacked or cloned cell-phone, where the hardware device is perfectly valid but presents a false identity.

Bogus, improper and cloned identification scenarios constitute real concerns that unknown systems and uncertified devices may register and access Database services. The Commission’s enforcement capability against specific or groups of TVBDs could also be compromised. Without a check during registration or initiation the Database will have no way to positively confirm TVBD identifying information or relay Commission enforcement messages that do not match the device’s invalid or bogus identification details.

Suggested Resolutions

Access to Equipment Authorization Data

Providing machine-readable access to TV bands-relevant records from the Commission's Equipment Authorization (EA) system will enable the Database to confirm a registering TVBD's identifying information is valid and may help to prevent invalid or uncertified devices from registering.

Database access to EA contents will also facilitate the Commission's own enforcement capability, as registered device information can be assured to match the Commission's known identifying information which may be used in an enforcement action (i.e. product FCC ID and or Serial number.)

Mutual Authentication

The Database must be able to positively identify TVBDs individually and by type.

Mutual authentication through the exchange of public/private keys is one method to suppress cloning. Registrations may be tightly coupled with actual physical devices if keys are incorporated into hardware. When keys are managed in software the linkage is less robust but registration remains strongly linked to a specific end-point.

Query Analysis

The timing and location of channel list inquiries from TVBDs can be analyzed to identify unusual events or behavior. For example, a device should not describe physically impossible movements, like identifying its locations to be in many cities within a very short period of time. Another example is channel hopping, where a TVBD makes many repeated channel list inquiries from the same location.

Suspect device behavior can be filtered against a historic baseline and flagged for additional attention.

Valid but Mis-configured Devices

It is difficult for the Database to prevent all device specific errors, mis-configurations or user-caused mischief. However, some basic checks are possible and may help to catch or suppress the most obvious problems.

- A properly registered device may report incorrect location information
- A properly registered device may not honor valid channel lists

For devices that report incorrect location information due to a temporary error, channel list timing describe earlier may serve to catch or flag spurious errors. Additionally, checks against the type of device and an understanding of its inherent mobility could serve to flag potentially erroneous channel list inquiries.

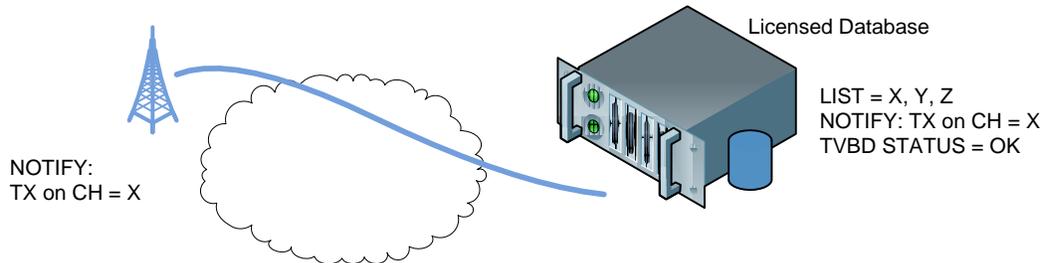


Figure 5: TVBD status reporting could serve to catch common, unintentional operating errors.

Suggested Resolutions

Status Notifications

One possible check is for the TVBD to notify the Database of its transmitting channel and for the Database to confirm notification against the just-issued channel list. For this method to be reliable the TVBD notification routine must be independent of its channel-query function. However, this can be easily defeated by devices that purposefully report a false channel.

Absent third party verification it will be very difficult to identify devices that receive but do not honor valid channel lists.

Database Reflectors

As described in 15.711(f), it is possible for a Fixed or Mode-II device to connect other Fixed or Mode-II devices so that they may inquire for a channel list. All Fixed or Mode-II devices must query the Database directly and may not act as a message proxy.¹³

It's conceivable that this rule could be circumvented by a reconfigured Fixed or Mode-II device to avoid Database fees or for malicious reasons. Such a scenario purposely violates the Rules and creates an increased risk of unintentional but significant and un-enforceable interference.

- A TV band device may act as a reflector and provide channel lists to unknown Mode-I devices
- A TV band device may act as a proxy to help other devices avoid Database fees

Reflecting or proxy message service could enable unauthorized end-users to hide the identity of their TVBD behind a presumably known good device. Under such circumstances, the Database will not know of the existence of the hidden TVBD.

This scenario poses two risks: first for the protection of the Database franchise and second to the Commission's enforcement capability against the unknown devices.

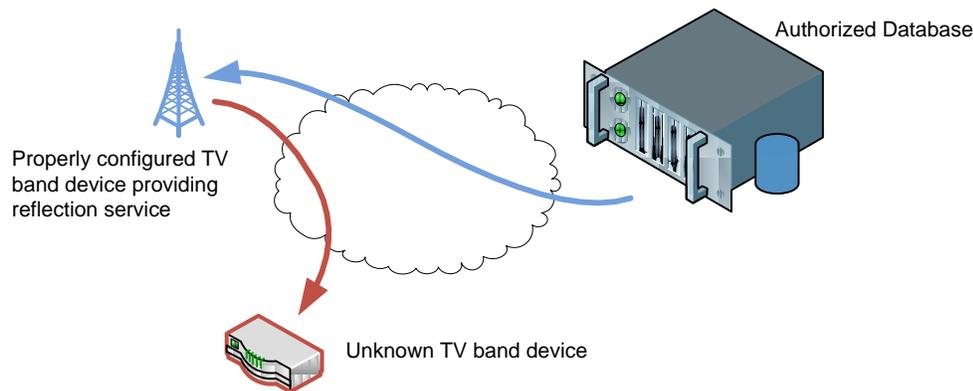


Figure 6: A reflector could enable invalid or otherwise unauthorized TVBDs to operate without the knowledge of the Database

If the 'good' device acts as a proxy, representing the 'bad' TVBD's location as its own, otherwise prohibited devices or those without commercial accounts could receive valid channel lists while negating device authentication or authorization procedures.

If the 'good' device instead acts as a reflector it forwards unmodified copies of its location-specific channel list. In this case the 'bad' device would be both unknown to the Database, operating on an invalid channel list, and likely to cause interference.

Both scenarios potentially undermine the financial integrity of the Database and serve to negate Commission enforcement capability against the unknown TVBD.

¹³ See 15.711(f) "A fixed device may not operate as a client of another fixed device."

Suggested Resolutions

Database reflectors and proxies represent themselves to the Database as legitimate, properly registered devices. They are potentially very difficult to identify and enforce against first identifying their downstream client devices. Several security measures can serve to suppress and discourage them however.

Query Analysis

Using the similar methods described for identifying unauthorized devices, query analysis may be used to identify proxy reflectors.

Mutual Authentication

Similar to the suppression of unauthorized devices, mutual authentication in this context can help to suppress valid but mis-behaving devices once they are detected. A credential that is tightly coupled to the hardware would be more effective than software-based identifying information.

Mutual authentication will require a Database operated certificate authority responsible for issuing, verifying and revoking public/private keys.

Unauthorized Database Operators

It is an unfortunate fact that malicious individuals and parties actively exploit security holes to deface web services, delete private information and damage or otherwise disrupt network services. Information service providers must adopt the position that if it a security risk is present, sooner or later someone will attempt to exploit it to maximum effect.

While the Rules require that TVBDs must directly access a Database, there exists a real risk that an unauthorized Database could provide Internet-based channel list services to unsuspecting or intentionally mis-configured TV band devices. Unauthorized databases cannot have a complete or current set of protected service records and the devices they serve would be very likely to cause harmful interference with incumbent protected services.

Furthermore, unauthorized Databases undermine the FCC's device certification requirement and negate the Commission's TV band enforcement capability. Because they disable network management and interference protection, unauthorized databases represent a significant operational and commercial risk for protected broadcast operations and valid unlicensed TV band services alike. Unauthorized databases are a serious and fundamental risk to successful unlicensed operation in the TV bands.

- A party could set up and operate an unauthorized but technically valid Database service
- A party could intercept connections and represents itself as a Database (man-in-the-middle)
- End users could purposefully mis-configure their devices to access an unauthorized Database

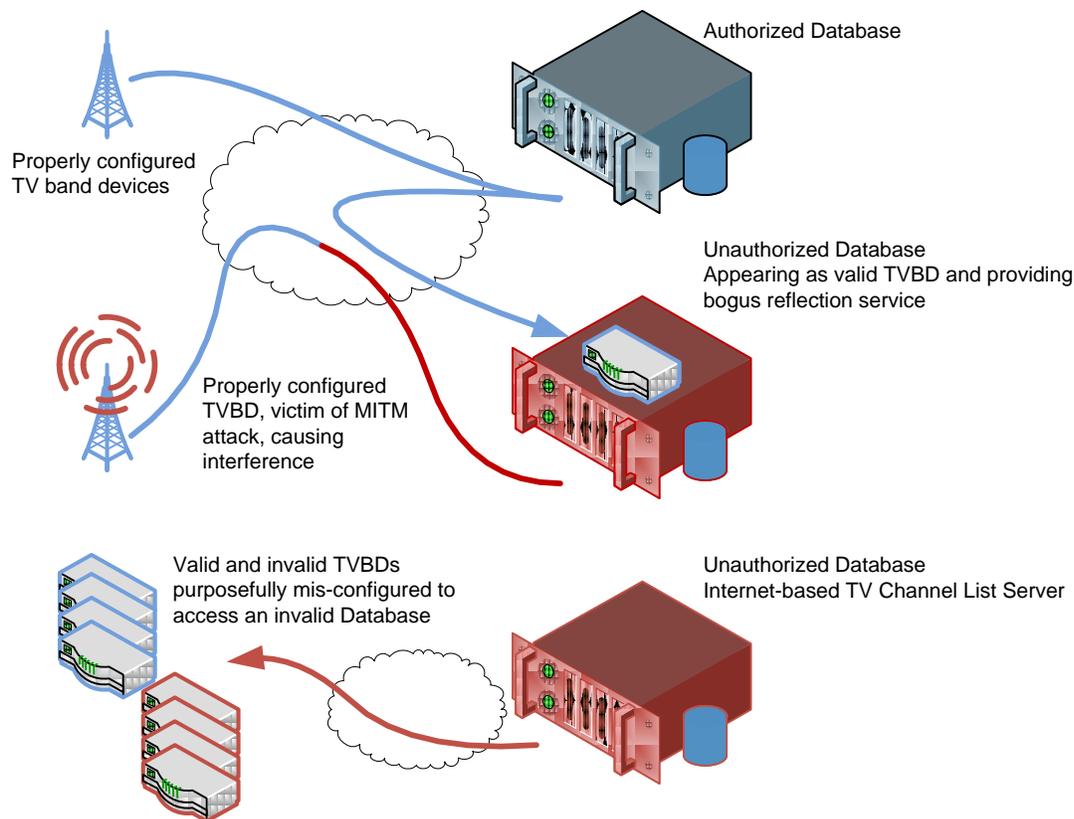


Figure 7: Unauthorized Databases present a more serious set of risks as they enable mis-configured TVBDs to evade FCC certification and enforcement. At best such devices could disrupt section 15.713(b)(2) protected services and at worst cause widespread purposeful TV band interference.

A man-in-the-middle (MITM) attack is when a third party attempts to emulate the Database's characteristics by intercepting an exchange with TVBDs. MITM attacks are typically used to acquire credentials and private data, but in this scenario could also be used to distribute invalid channel lists.

"Phishing" is when a malicious party fools a victim to share their credentials for later exploitation. This is only one of the scenarios that could be used to attack a Type II/Fixed device.

There is little to prevent a technically competent rogue party from setting up an otherwise compliant database using publicly available methods and data to offer channel list services. It is easy to envision an unlicensed TV bands database, located offshore and outside FCC jurisdiction, that provides channel list services without regard to voluntary, section 15.713(b)(2) protected services.

At best unauthorized databases deny the licensed Database of channel-list revenues and create a significant probability of interference to section 15.713(b)(2) services (Cable head ends, microphones, etc.)

In a worst-case scenario, large numbers of TV band devices could be commanded to by a malicious Database operator to attempt purposeful interference.

Suggested Resolutions

Mutual Authentication with Transport Encryption

Most unauthorized Database risks can be addressed by enforcing the requirement TV band devices only connect and accept channel lists from a licensed Database. In short, TVBDs must authenticate the Database credentials and only connect if the credentials are valid.

Mutual authentication addresses the requirement of counter-party identification, where both the Database and the TVBD authenticate themselves in such a way that both parties are assured of the other's proper credentials.

Transport encryption addresses the risk of interception, only allowing connections to be established between IP hosts that present valid credentials. Unless the intercepting party has stolen the licensed Database private keys without the Database's awareness (an exceedingly difficult task), a hijacked or intercepted connection would be immediately recognized by the TVBD.

Automation of Mode-I Device Configuration

Mode-I devices, by sheer force of number, present a potentially large source of interference if compromised or allowed to be mis-configured en-mass.

Similar to WiFi clients and Cable Modems, reasonable constraints on user configuration could be imposed to suppress opportunities for mischief. The purpose would not be to handicap devices but rather to automate the assignment of important transmission parameters with authenticated values.

Many concerns about Mode-I devices can be addressed by limiting opportunities for end-user mischief and ensuring 15.707(c) and (d) are strictly enforced.

Mode-I Long-Distance Links

Section 15.709 (a)(2) places limits on the transmit power of Fixed and Mode-II plus Mode-I devices.

The Rules place no restriction however on receive gain antennas. Because of the excellent transmission and propagation properties of the TV bands frequencies there is a concern that a pair of stations with high receive gain antennas could effectively operate at distances far enough to require a new and unique channel list assignment.

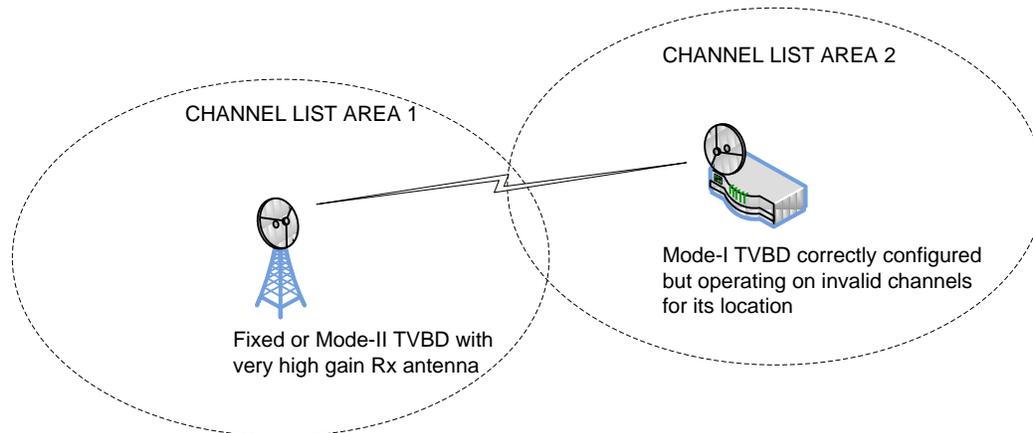


Figure 8: TVBDs configured with high gain receive antennas could create a very long Mode-I link. The Mode-I device, which has no geo-location capability, may receive an invalid channel list for its location.

Mode-I devices are not required to include geo-location capability, but must instead rely upon their Fixed or Mode-II Master devices to retrieve an area appropriate channel list from the Database. It is currently not possible for Mode-I (Client) devices to determine the separation distance to its Fixed or Mode-II (Master) device or to alert the user to a possible geographic boundary violation.

Suggested Resolutions

Fixed / Mode-II Device Registration for Extended Area Channel Lists

Significantly long distance radio paths typically require professional link engineering and installation. For scenarios like the one described here, the geographic location of both devices is likely to be known and fixed.

The Database could accommodate such special cases with a special Fixed and Mode-II device registration that caused two or more area-specific channel list assignments to be returned to the inquiring Master TVBD.

Multi-homed Mode-I Devices

Certain Mode-I devices may seek to connect to more than one base station for access to additional capacity, path redundancy, least-cost or direct traffic routing. In a multi-homed scenario the Mode-I device will have received potentially different channel lists from each Master device.

The concern is that the Mode-I device could be located in between two geographic areas and transmit on a channel that is not valid for its own location. This is illustrated in Figure 9.

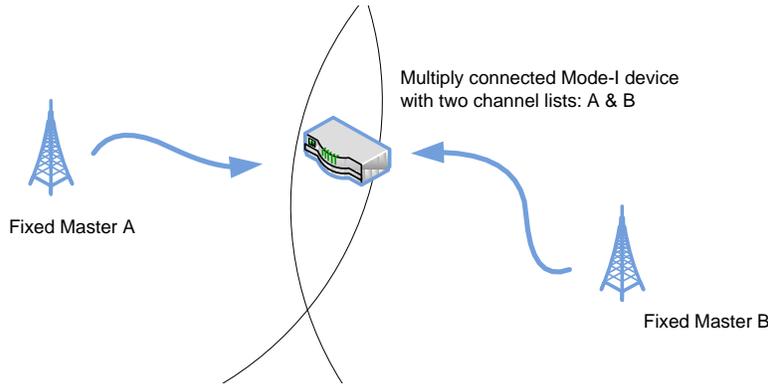


Figure 9: Multi-homed Mode-I (client) devices could have more than one channel list which might not match.

There are two concepts offered to accommodate multi-homed Mode-I devices. Both attempt to ensure the careful management of Mode-I TVBD channel lists.

Suggested Resolutions

Only One Active Connection

The simplest solution is to prohibit more than one active connection at a time for Mode-I TVBDs.

Transmit on Channels Common to All Lists

A more accommodative solution is to allow Mode-I devices to establish as many connections as they wish but with the restriction that the Mode-I device may only transmit on channels common to all the channel lists it receives from the Master devices it has connected to.

Take for example the scenario illustrated in Figure 9, where the Mode-I device is connected to Master device A and B. Assuming the Master devices provide channel lists 'A' and 'B', the Mode-I device would only be allowed to transmit on the channels common to both lists (5 and 6).

List A	2	3	4	5	6				
List B				5	6	7	8	9	10

Discussion of Security Technologies and Recommendations

As discussed earlier, the Rules contain significant security gaps but also task the Database administrator to make commercial services available on a non-discriminatory basis. The administrator should be expected to apply industry best practices and a security model appropriate to the scale of operation and potential economic risks should a system failure or compromise occur. It will be necessary to impose strict guidelines on the system to ensure a commercially successful ecosystem of licensed broadcasters, unlicensed TV band service providers, TVBD manufacturers and microphone users.

To be commercially viable the Database must employ, at minimum, a set of security policies that provide mutual authentication of Database and TVBD and transport security.

There are two principal options for securing the connection between the TVBD (protected endpoint) and Database security gateway (tunnel endpoint): IPSEC and TLS. Both technologies have their respective advantages and appropriate application. The database will support both to accommodate the following Database commercial requirements.

- Fixed and Mode-II TVBDs should connect to the Database with an IPSEC tunnel
- If IPSEC is not possible, TVBDs may connect to the Database using TLS
- Both IP endpoints must authenticate the other (mutual) using shared keys or PKI
- Unencrypted communications are not allowed

In its simplest form, secure connection configurations can be modeled from two basic device modes: a tunnel or an endpoint and three connection types. These are illustrated in Figure 10.

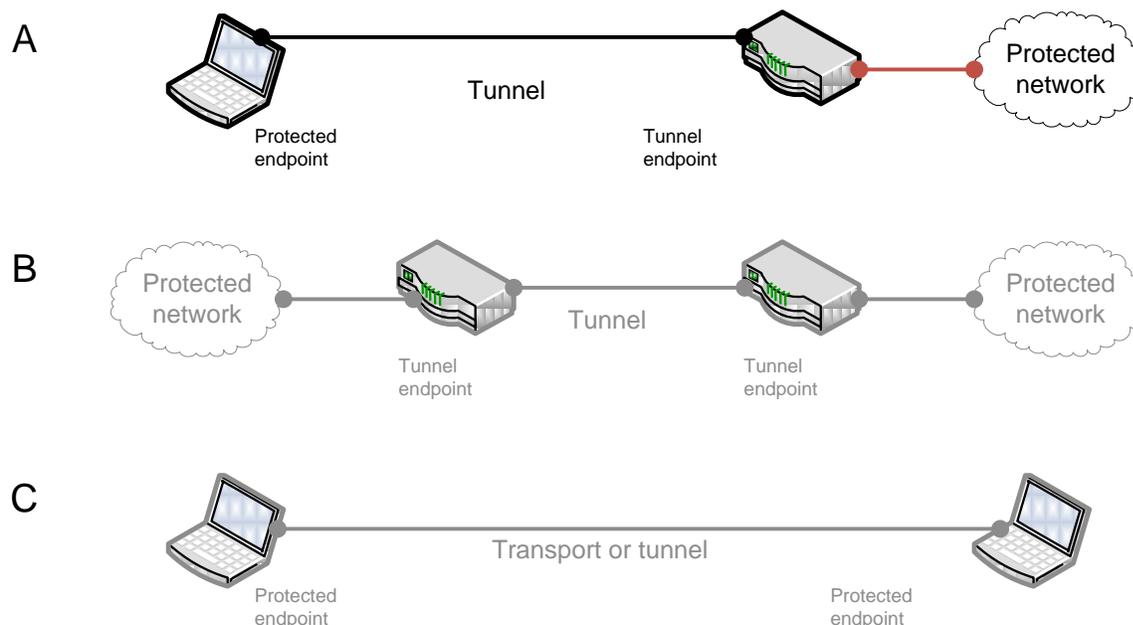


Figure 10: Three basic connection types are possible with secure gateways and endpoints. The Database will support the first (Mode A) by default and may support others if necessary.

The Database will support connection mode 'A', where a TVBD (protected endpoint) only connect to the Database with an IPSEC tunnel, which establishes a secure, authenticated, encrypted connection.

The Database administrator will provide public key infrastructure for IPSEC and a certificate authority for TLS.

IPSEC Transport Security

Communication between the Database and TVBDs occurs across a Connection, which is defined as a point-to-point TCP/IP link between two IP hosts. Connections supporting the exchange of channel lists constitute a commercial transaction and must be secured, authenticated, and encrypted .

IPSEC is a security technology that enables mutual authentication during the establishment of connections between hosts and provides for strong encryption and source authentication of each IP packet exchanged between the connected hosts. Because IPSEC operates at the Network layer of the OSI stack it has a number of important advantages for application development and system operations and scale.

As any tele-worker who uses a VPN connection knows, IPSEC connections are completely transparent to applications. This transparency is potentially a very important feature to the Database. Employing IPSEC will allow Database administrators to adopt off-the-shelf Internet security systems.

The Database will support IPSEC tunnels to provide a standard authentication and encryption layer between Database and TVBDs. This will enable device manufacturers to leverage proven, widely available technology and the Database administrator to deploy a standards compliant security framework using commercial, off-the-shelf security systems.

Transport Layer Security

IPSEC is a robust security technology that has many benefits for TV Band connections over other technologies. Nevertheless, it could impose a burden on particularly lightweight or otherwise CPU-starved TVBDs. Where IPSEC implementation is not possible device manufacturers may instead use transport layer security (TLS) with mutual authentication to establish connections with the Database.

TLS is the successor to Secure Sockets Layer (SSL) and provides for security and data integrity over IP networks. TLS has the disadvantage of being incorporated into applications, which creates an additional layer of software management complexity.

The Database will support TLS connections through a TLS-enabled VPN concentrator, which connect authenticated external web clients to specific internal resources for the creation of sessions.

The Database will not support SSL because of recently discovered security flaws in that technology.

Discussion of Authentication versus Authorization

Authentication is the act of verifying a party's identification is properly formatted, valid, and matches the identification on record by the validating party. Authorization is the act of verifying access by an authenticated party to various functions of a system and to information in the system. The two processes are distinct.

To further illustrate the concept consider a properly configured device that may have valid authentication credentials but has been denied service by the FCC ("black listed"). In such a scenario the device will have positive authentication but negative authorization. In contrast, consider a device that may have a correct Database registration but incorrect or invalid credentials. Were it able to connect to the Database this device would be authorized but it is prevented from receiving services because it cannot be authenticated.

Authentication and authorization rely upon well defined and carefully managed cryptographically secure and verifiable credentials.

TV band system authentication credentials are a valid public/private key combination, issued by the Database during device registration for Fixed devices or during commercial account creation for Mode-II devices.

As presently defined a valid FCC ID and serial number are enough to establish a connection with the Database. Combined with a public/private cryptographic key, the FCC ID and serial number constitute a complete set of credentials that enable a device to both connect with and authenticate itself to the Database.

Once authenticated with the system, TVBDs may attempt to access any Database service and data to which they are authorized.

Mutual Authentication is a security procedure wherein a TVBD must prove its identity to a Database and the Database must prove its identity to the TVBD before a connection is established between the two. Mutual authentication requires that the TVBD and Database prove their respective identities to each other before connecting or accepting information from each other. Identity can be proved using cryptographic means like public key infrastructure and the exchange of public keys.

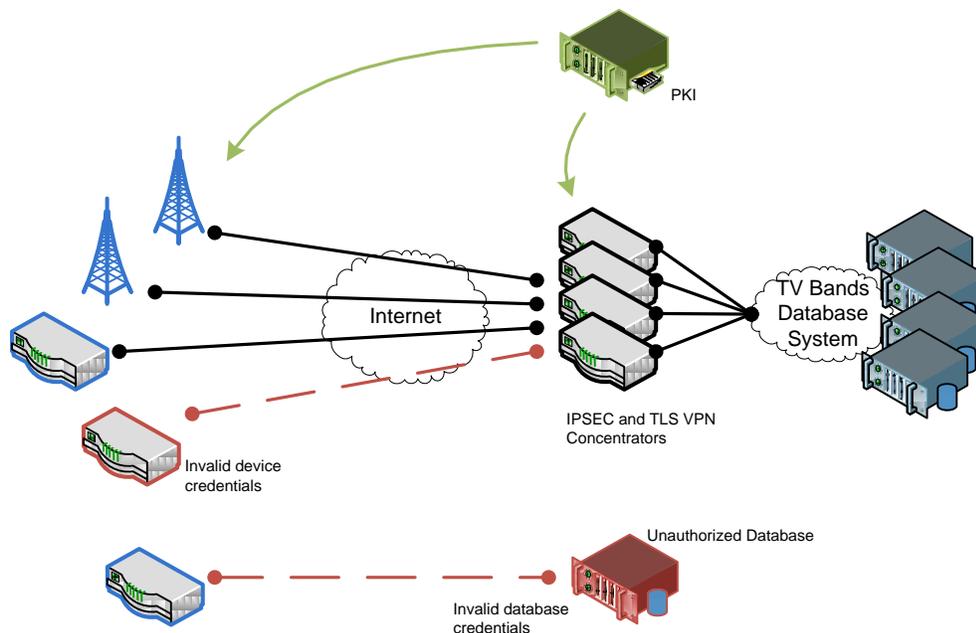


Figure 11: Illustration of three mutual authentication scenarios for assured connections between TVBD and Database. At the top, three valid devices (blue) successfully connect to the Database VPN concentrator, while the fourth device (red) is not allowed to connect due to invalid device credentials. At the bottom a valid device terminates a connection to an unauthorized database (red), again due to invalid authenticating credentials.

Public keys are distributed on demand by a Database administrator provided public key infrastructure (PKI) service (green).

With mutual authentication TVBDs and the Database may establish a connection only after authenticating each other. Both systems may then be reasonably (but not absolutely) assured of the other's identity. Mutual Authentication helps to address two important operational requirements for successful unlicensed TV band operation:

- Only authorized devices may connect to a Database
- All devices must only connect to and receive channel lists from an authorized Database

An important concept in mutual authentication is that neither party should "trust" the other until their identity has been proven. Using public key infrastructure this means that the Database must establish the identity of TVBDs without asking the TVBD and that TVBDs must authenticate the Database is without asking the Database.

With mutual authentication it is very difficult to compromise security through impersonation.

Summary of Commercial Database Requirements and Recommendations

Successful commercial operation requires a security model that is proportional to the economic risk. Accordingly, the Database administrator should be expected to employ Industry best practice to meet the Commission's objectives for unlicensed operation and robust incumbent protection.

In this document we analyze the device operational life cycle and options for fee recovery by the Database administrator. We discuss several concerns and risk scenarios with their suggested resolution. Finally, we review best practice security technologies and some procedures that could be adopted as a security model for the TV bands Database.

This document reaches the following conclusions:

Registration and Commercial Accounts

- Only valid devices may register with the Database using proper FCC ID and serial number
- Fixed & Mode-II devices must establish a commercial account with the Database administrator prior to receiving channel lists
- Flexible account structures may be required to ensure consumer convenience and adoption
- Devices should report their transmitting channel to the Database

Security Concerns

- The principle concern is interference, either purposeful or by accident
- Unauthorized Databases and purposefully mis-configured Mode-I devices are a significant concern
- Most security risks can be addressed by assuring the identity of and communication path between TVBDs and the Database

Security Procedures

- Only authorized TVBDs may connect to a Database
- All TVBDs must only connect to and receive channel lists from an authorized Database

Security Technologies

- TVBDs and the Database must support and employ mutual authentication
- Fixed and Mode-II TVBDs should connect to the Database with an IPSEC tunnel
- If IPSEC is not possible, TVBDs may connect to the Database using TLS
- Unencrypted communications are not allowed between TVBDs and the Database

Appendix: Questions & To Do List

- **Technical definition of 'Spectrum sensing' for TVBDs to accommodate 15.711 (c)(1 through 4)**

What is the actual process by which devices will 'listen' or 'sense' for incumbent services?

For example, does this mean to take X samples per second and average them for 30 seconds? Or would just one sample showing sign of life during the 30 second window qualify as a detection event?

- **How to protect the transmission of FCC ID and serial number when establishing a connection?**

Possibly use FIPS-180-1 (SHA-1) message digest?