



TV White Space Databases

Motorola
October 13, 2009

Topics



TV White Space Database

- **The Commission should not in any way artificially limit the number of TVWS Database providers**
 - Limiting providers stunts competition & innovation – drives up costs for consumers, and harms greater public interest
 - Multiple TVWS Databases can provide safe, consistent protection
- **There are multiple viable TVWS database architectures and configurations**
 - There are many opportunities for value-added database services (that do not alter incumbent protection)
 - An option should allow computations to be done by the devices

Security

- **Security should be focused on reliability of protection data, not on TVBD authentication**

Unified TVWS Database Architecture

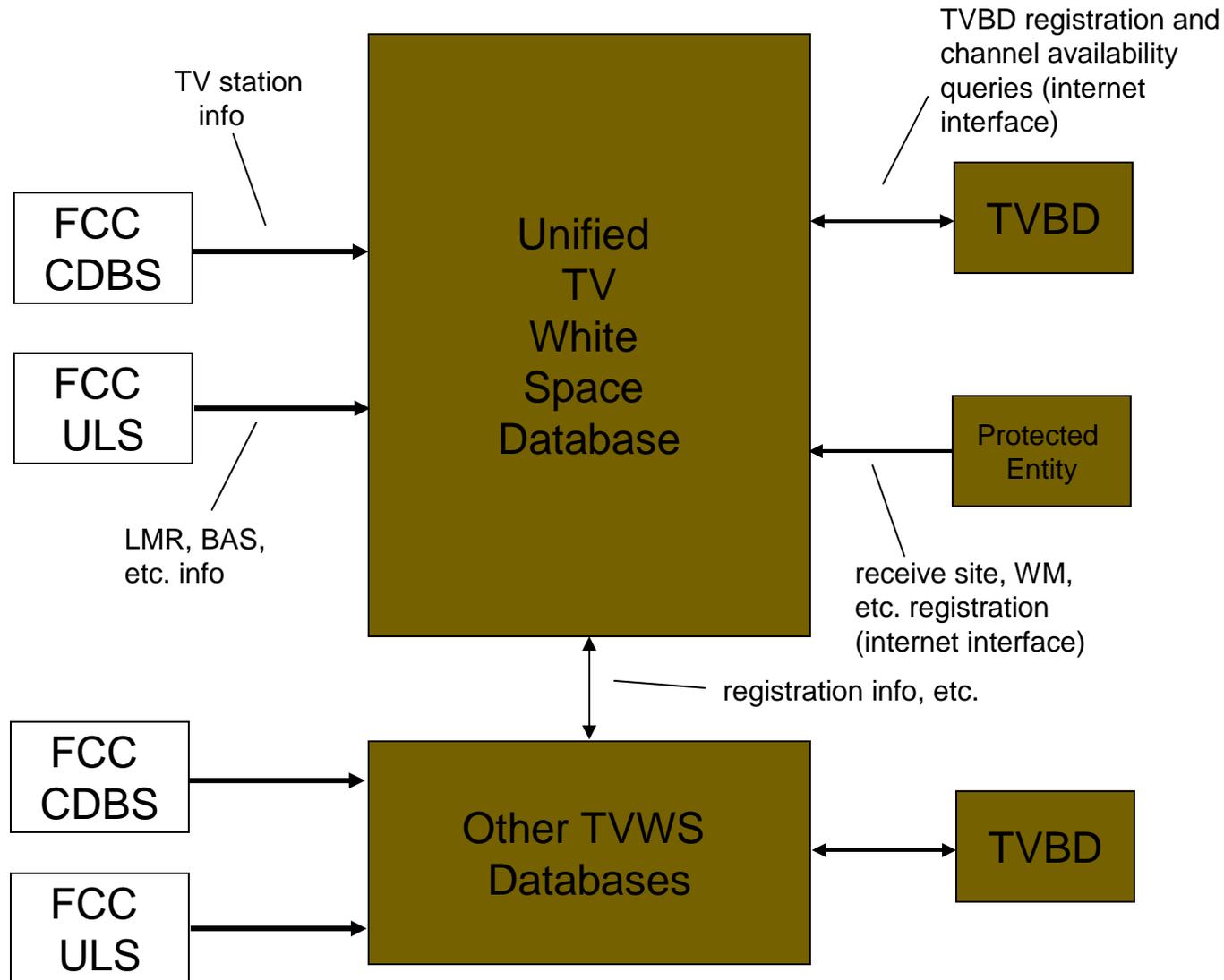


Fig.1 Basic Unified TVWS Database Architecture

One Possible Split Database Architecture

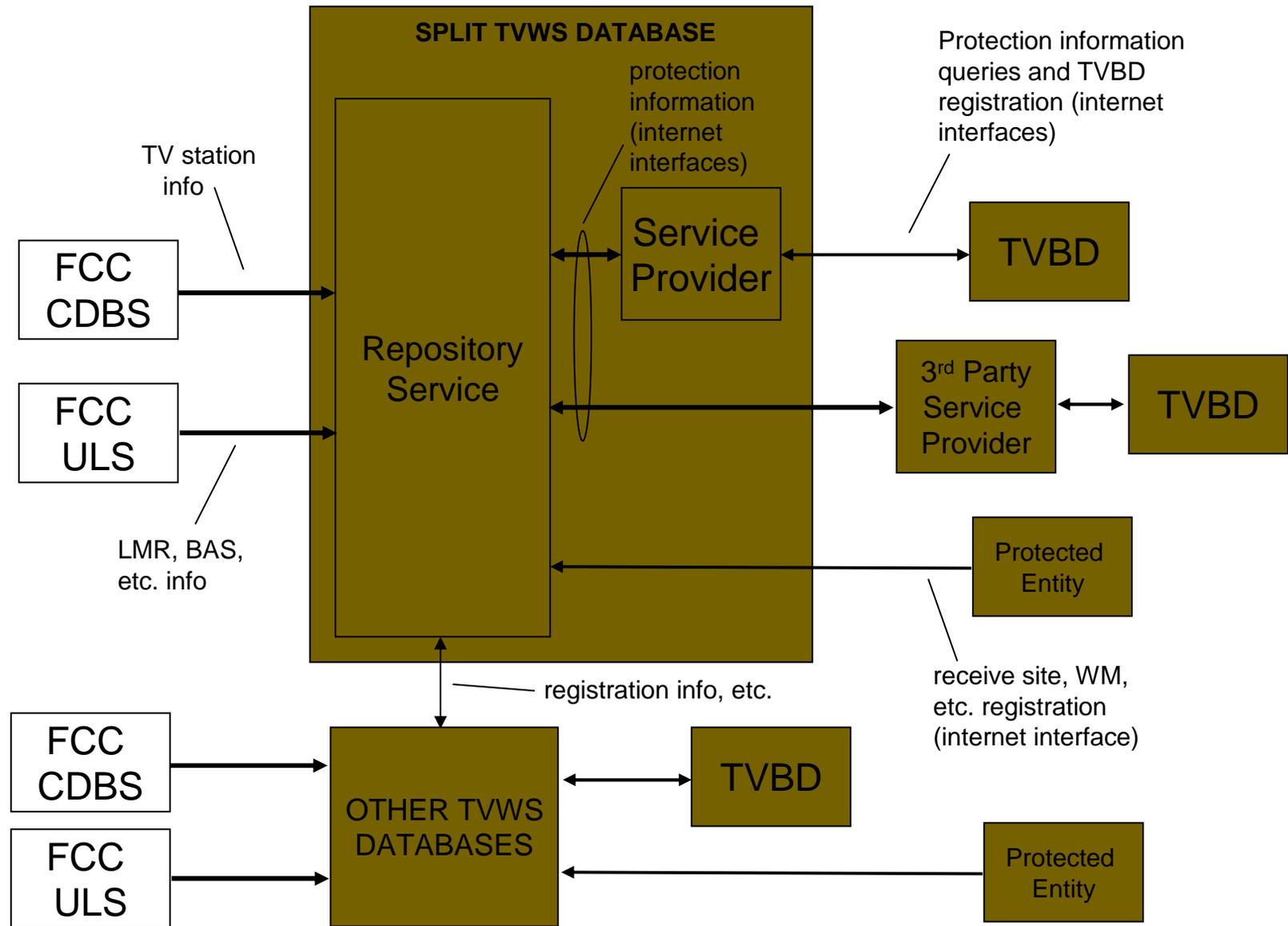


Fig. 2 Split TVWS Database Architecture

Unified Incumbent Data Architecture

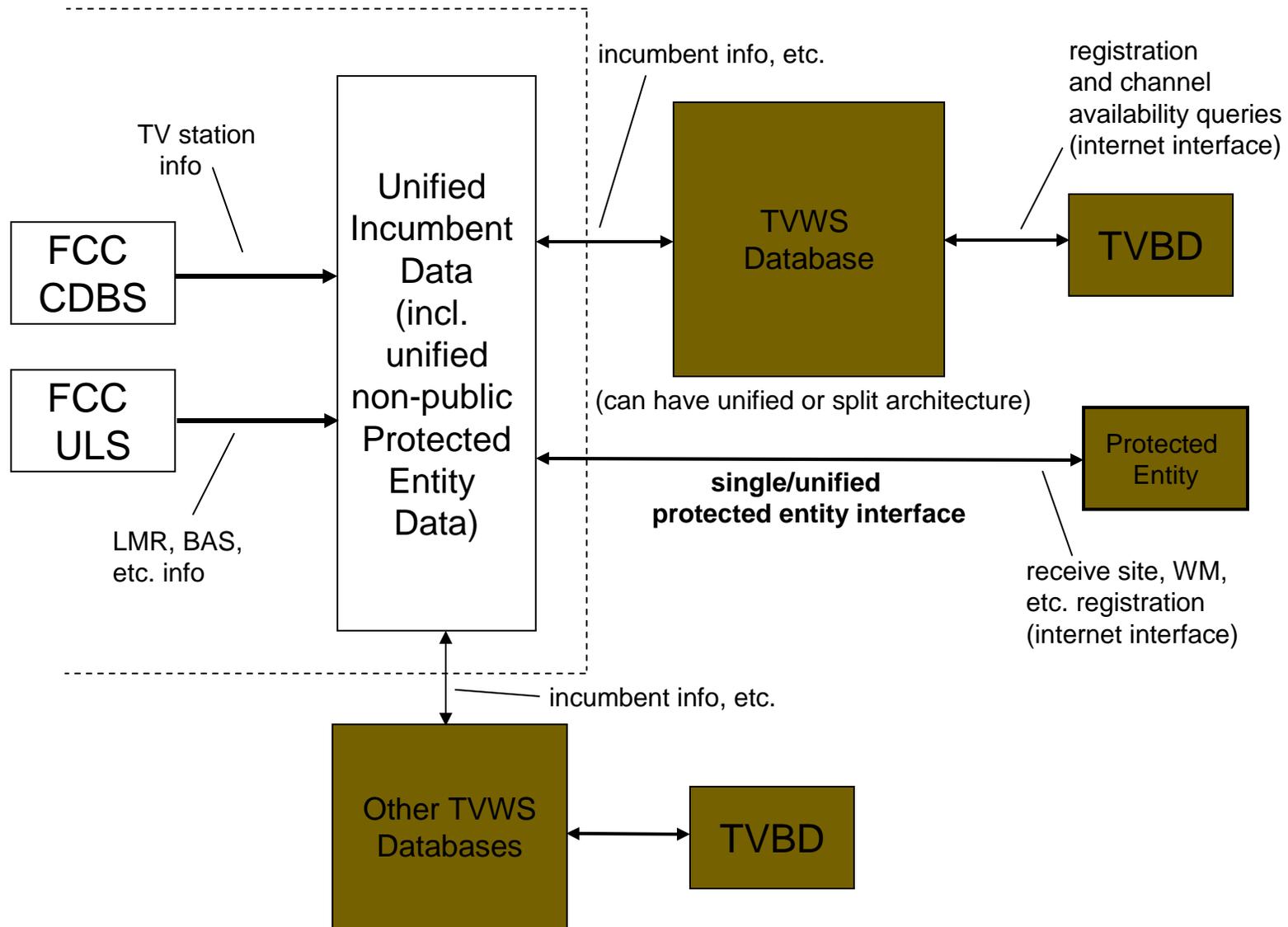


Fig. 3 Unified Incumbent Data Architecture

Unified Incumbent Data Architecture w/TVBD Computation

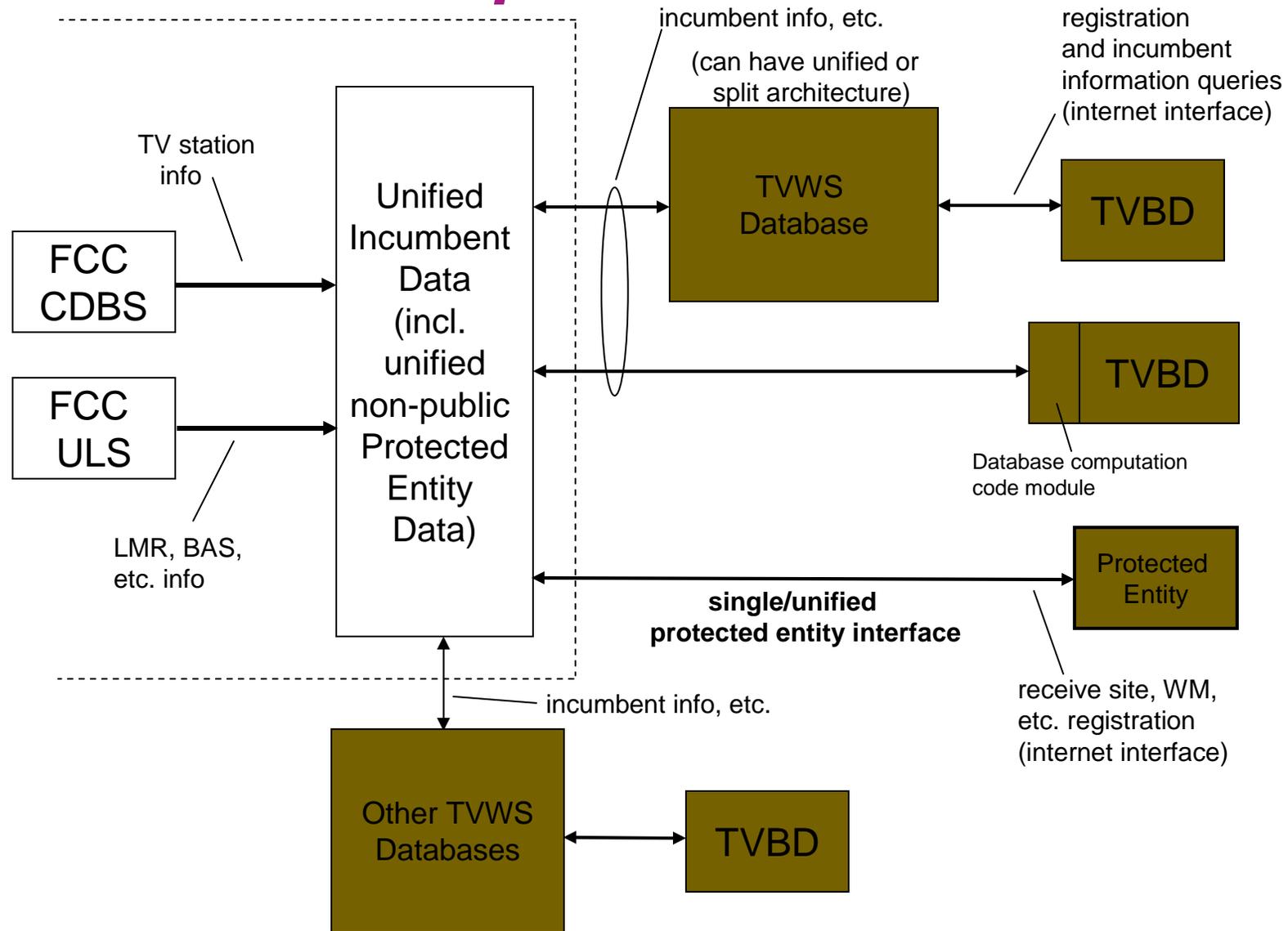


Fig. 4 Unified Incumbent Data Architecture w/TVBD Computation

Database Selection - Summary



Motorola urges the Commission to select multiple database provider

- **Can be safely accomplished by implementing simple automated consistency checking mechanisms (approach would also be required for multiple Service Providers)**
- **Consistency can be further assured by enabling unified incumbent data and protection computations**

Motorola urges the Commission not to mandate a specific TVWS Database architecture

- **Numerous companies have expressed an interest in providing services, each with differing TVWS database architectures**
 - **Commission can still enact other means to assure consistency in protection**
- **The Commission should not artificially limit the number of entities that can provide repository or database services**

These approaches support a healthy, competitive eco-system for TVWS database implementations

- **Multiple databases will drive equipment and service prices down for all consumers**

Assuring Consistency in Protection w/Multiple Databases



Automated database results consistency-checking mechanisms can be implemented to continuously “police” multiple databases for proper operation

- Can quickly identify any protection discrepancies (e.g., due to hacking, etc.)
- Same protection data consistency issues exist with multiple Service Providers

Alternatively (or additionally), two other items can virtually guarantee consistency between different database implementations:

- Using common protected entity information among all TVWS databases (for all incumbents: TV, Wireless Mics, Receive sites, etc.)
- Using the same basic channel availability computational protection algorithms for all TVWS databases (e.g., F-curves, terrain databases, interpolation methods, etc.)

One way to achieve these two goals (while preserving competition) is to:

- Enable open and non-exclusive access to unified protected entity data
 - This also eases protected entity (PE) registration concerns – protected entities only need to go to single source to register all device operation
- Implement open and non-exclusive computational protection code
 - Motorola has offered to significantly aid this effort, based on past implementation experience

These approaches benefit all protected entities, as well as consumers

- Competition will drive equipment and service prices down for all consumers

Dubious Benefit of Strict Device Security



A malicious (e.g., unauthorized) TVBD has one of the following 3 options:

1. Do not check any TVWS databases

- Most likely scenario
- Avoids the TVBD implementation complexity of verifying/authenticating an authorized database

2. Check an unauthorized database

- Unauthorized database would not include Commission required incumbent information or verification
- Avoids the TVBD implementation complexity of verifying/authenticating an authorized database

3. Check an authorized database

- **This is the least likely...**
 - Much easier for device to avoid checking an authorized database
 - Especially if TVBD knows that an authorized database will not serve it (e.g., if it sends a “no-channels available” message)

Devices can contain shared secret that can verify TVBD identity

- **Similar to online banking schemes (billions of dollars of online commerce trusted to this method)**
- **Useful for verifying commercial business relationship with database**

Requiring excessive device security will not reduce potential interference from malicious devices

- **FCC has enforcement mechanisms for unlicensed devices**

Database Provider Security



Claimed TVWS Database Provider threats:

1. **Unauthorized party could offer database service (e.g., spoofing, etc.)**
 - Can be reasonably countered with database authentication mechanisms
2. **Previously authorized database becomes corrupt (e.g., hacked, etc.)**
 - Can also be countered with timely authentication mechanisms
 - Corrupt data can also be quickly identified through automated data integrity checking methods
 - Argument for lightly or moderately restricted access to database results

Security Recommendations



Motorola urges the Commission to not require strict device security

- **Strict device security provides no additional protection benefits**
 - Malicious devices unlikely to check authorized database
 - Drives up cost for devices, and presents key-management problems

Motorola suggests reasonable security measures

- **The use of database authentication (e.g., shared secret methods)**
- **The use of password-based accounts with the database to assure device identity**
 - **Can be used to reasonably assure device identity without significant additional costs to consumers**

Summary



TV White Space Database

- **The Commission should not in any way artificially limit the number of TVWS Database providers**
 - Limiting providers stunts competition & innovation – drives up costs for consumers, and harms greater public interest
- **There are multiple viable database architectures and configurations possible**
 - Multiple TVWS Databases can provide safe, consistent protection
 - There are many opportunities for value-added database services (that do not alter incumbent protection)
 - An option should allow computations to be done by the devices

Security

- **Security should be focused on reliability of protection data, not on TVBD authentication**
- **Database authentication (e.g., shared secret methods)**
- **Password-based accounts with the database to assure device identity**