Advances in ATSC 3.0 Datacasting Security

Evolving ATSC 3.0 Datacasting Security and Content Access Control

PEAK3

CYBRELLA
CYBERSECURITY EXPERTS

Introduction

The focus of this paper is to propose and promote an approach to evolve the security and content access control for delivering Critical Data to Edge Devices leveraging ATSC 3.0 Datacasting.

The existing ATSC 3.0 Security approach, as defined by A/360, focuses primarily on managing an ATSC3.0 receiver (signaling, application authentication, etc.) rather than defining a mechanism to secure the shared Datacasting broadcast data. Furthermore, the current security specification requires an ongoing IP return path.

The proposed approach discussed in this paper provides the following improvements:

- Secure transmission over a shared broadcast channel
- Secure sharing of a broadcast channel by multiple customers/groups
- Access control of shared broadcast content
- Billing management and enforcement for shared broadcast elements

Furthermore, an ongoing IP return path will not be required to support the capabilities proposed.

Finally, we will also discuss how this approach can be expanded to support post-quantum algorithms.

Datacasting Security: Today

As a starting point for the analysis of the Datacasting security, we will provide a brief overview of the existing ATSC 3.0 Datacasting Security with a discussion on the problems it solves along with the limitations.

The ATSC 3.0 security is defined as in A/360, "ATSC 3.0 Security and Service Protection" and can be downloaded from https://www.atsc.org/atsc-documents/type/3-0-standards/

The ATSC 3.0 Security Authority (A3SA) is in place to develop protocols for securing ATSC 3.0 broadcast services by leveraging the same type of tools now commonplace with web-based delivery – including IP-based encryption protocols, device certificates and rights management technology.

From ATSC 3.0 A/360: *This specification defines a set of methods designed to secure the following content and data flows described in other ATSC 3.0 specifications:*

1. *Content protection*	High-level point to common encryption techniques such as MPEG Common Encryption (CNEC) and DRM.
2. *Authentication of ATSC 3.0 applications*	Ensures that only valid and signed applications are loaded on a Receiver

3. *Authentication of ATSC 3.0 Broadcast Signaling*	Specifies Certificate and Certificate Management using PKI with X.509
4. *Interactive data exchanged over an internet connection between an ATSC 3.0 application and a web content server, including the use of DNS Security*	This allows applications running on Receiver to securely access resources over an Internet connection.
5. *Data flows between an ATSC 3.0 primary device and a companion device*	Specifies Pre-Shared Key Encrypted Connection. We propose to use this mechanism to establish session keys between the Key Manager and the Receivers.

The ATSC 3.0 A/360 Security flow high-level summary:

- Based on standard TLS 1.2 and 1.3 which requires the typical bi-directional handshake to establish a secure connection which are widely used for HTTPS
- Broadcasters create their own private key and register to get a certificate from an agreed upon Certificate Authority (CA).
- Receiver manufacturers create their own private key and register and get a certificate from an agreed upon Certificate Authority (CA)
- The TLS messaging flow is over an Internet connection established for the Receiver and the ATSC 3.0 as appropriate.
- Eonti has been selected by Pearl TV to provide the PKI infrastructure.
- A3SA has selected Widevine to provide DRM (Digital Rights Management)

The problems that the current ATSC 3.0 A/360 security solves include:

- Receiver endpoint security
    - Secure messages to and from the receiver to a server or web server
    - Secure Receiver web page access
    - Receiver application assurance i.e. it's the application you think it is
    - Secure Receiver firmware update i.e. the firmware hasn't been tampered with
- Non-Datacasting shared content security

Limitations of current ATSC 3.0 security as per the specification:

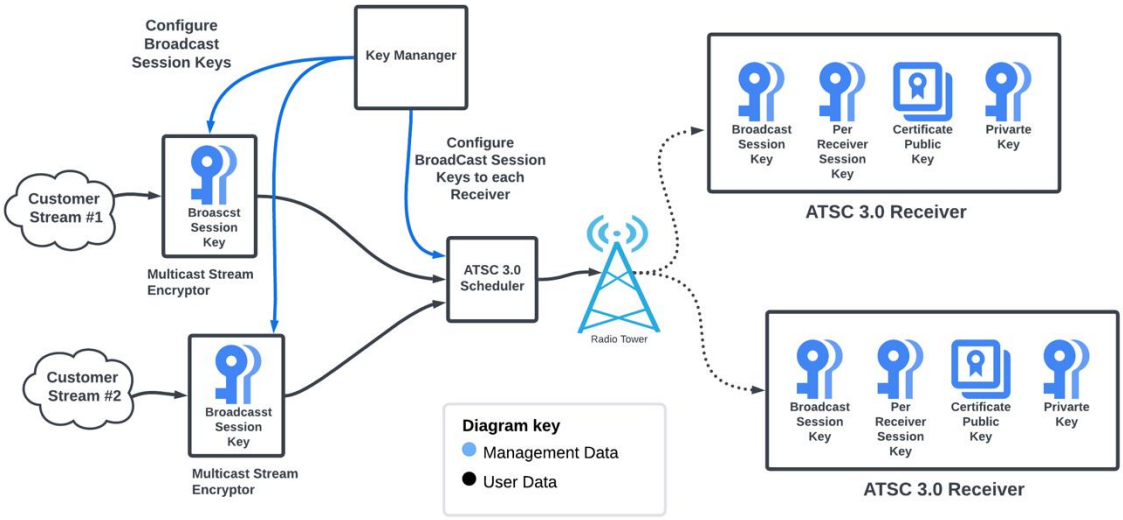
- Focused on endpoint security and requires a broadband return path from the client to the server.
- There are no provisions for encrypting the shared Datacasting content.
- As shared content is not provided, it should also be noted that way to disable a group of a single remote from the shared content is not supported.

Secure Datacasting over Broadcasting Capacity

The following section describes a proposed approach which leverages the existing ATSC 3.0 security specification and addresses the identified limitations.

Broadcast Security Infrastructure

In order support a secure broadcast domain, key security elements are first defined.



Key Manager – software component hosted as a network wide shared instance, likely cloud native, which manages all aspects of broadcast chain, customer and user key creation, management, and distribution.

The Key Manager Security Elements includes a public certificate (public key) for each remote element and a Broadcast Session key for each broadcast security group.

Multicast Stream Encryptor – software component which encrypts user data based upon the Broadcast Session Key for a given user data stream provided by the Key Manager on a per multicast stream basis. This component can be hosted as a centralized cloud service or on-prem as dictated by economic, networking, and security requirements.

ATSC 3.0 Scheduler – The existing ATSC3.0 Scheduler is located at each station and is not expected to change for this proposed security extension. More information on how Peak3 sees the future of Spectrum Resource Management can be found here Advanced ATSC 3.0 Spectrum Resources Techniques.

ATSC 3.0 Receiver – Includes the ATSC 3.0 receiver and Receiver Security App Software which receives the signal, decrypts the data stream using the Broadcast Session Key and passes the user data to the local network.

Each receiver includes a Secure Enclave, such as an eSIM, a PSK/private key and a NIST/FIPS approved crypto module.

Security Elements

The key Security Elements are defined as follows:

Broadcast Session Key (BSK) – shared symmetric key used to encrypt and decrypt user data for a given group of Receivers.

Broadcast Session Group (BSG) – Group of Receivers which have the same Broadcast Session Key. This could be any combination of Receivers as defined by an operator – All, per broadcast chain, per Application, per Customer or per Receiver would all be supported.

Receiver certificate/public key – a PKI certificate and public key which is pre-configured per receiver using the agreed upon CA as per ATSC 3.0 A/360.

For receivers **without** operational return paths, when the customer registers the Receiver with the Key Manager, the CA is contacted to validate the signed certificate and create a Per Receiver Session Key.

Per Receiver Session Key – a symmetric session key per discrete receiver which is agreed upon with the Key Manager when the receiver is registered with the Key Manager. Note that the entire algorithm works based upon the idea that each Receiver has a unique private key.

Connectivity with the Key Manager is assumed to exist only during commissioning/registration of the Receiver.

Receiver Private key – calculated by either the user (if desired) or by the Key Manager when the device is registered. Loaded into each Receiver independently as stored into the local security enclave i.e. the eSIM.

Receiver Registration before Deployment

To commission a Receiver, the following concept of operation is considered:

1. A User with Internet access scans a per device specific QR code which includes the UUID of the remote element.
2. The signed certificate is first validated with the CA.
3. User enters in customer/subscription specific information.
4. User connects to the Receiver via Bluetooth or Ethernet and the Receiver Security App on the Receiver programs the security elements (Per Receiver Session Key) in the Receiver's Secure Enclave, likely an eSIM.
5. The Key Manager registers the UUID, customer, signed certificate and Per Receiver Session Key of the Receiver.
6. The User registers the Zip code of where the unit will be deployed.
    - Note that a mobile Remote Element will need a return communications path to update the location as the Receiver moves.
7. The Receiver is now ready to be deployed.

Datacasting Key Manager CONOPs

The following section describes a notional architecture for an ATSC 3.0 Key Manager Concept of Operation.

Broadcast Session Key Distribution

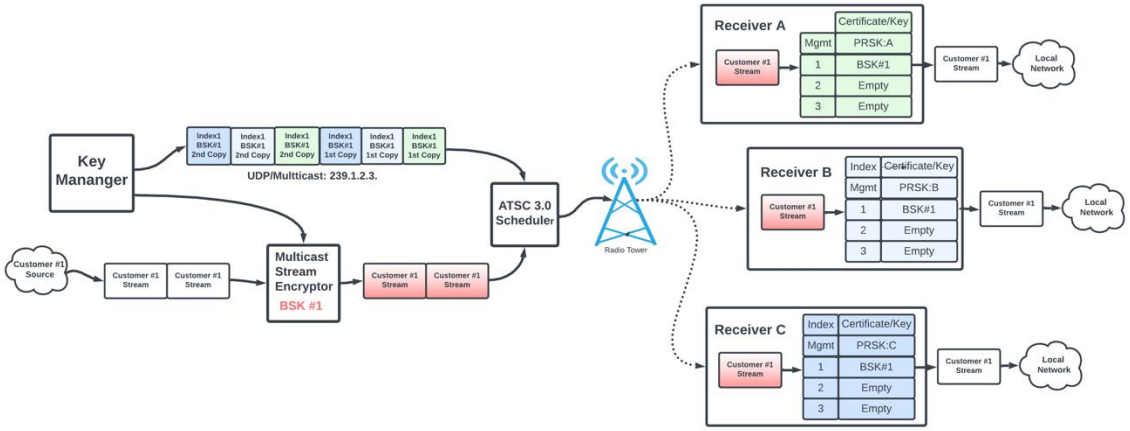
For Broadcast Session Key Distribution, it is assumed that the deployed Receivers already have been registered with the Key Manager. This means the Key Manager and Receiver pair have the agreed upon Per Receiver Session Key.

The Key Manager continuously sends out the current Broadcast Session Key to each remote one at a time in each of the broadcast domains under management.

The Broadcast Session Key is sent to each Receiver by the Key Manager using each Receiver's Per Receiver Session Key. While the message is sent over the shared broadcast channel and all receivers attempt to process it, only the Receiver with the corresponding private key will be able to decrypt the message and update the Broadcast Session Key.

Sending the key individually to each Received element allows for fine grain control, discussed below, over which Receiver will receive content for a given Broadcast Security Group. In addition, this level of control allows the Key Manager to control if a given Receiver continues to have access or is removed from service for lack of payment for example.

By continuously sending out the Broadcast Session Key, any Receiver which has not been available (powered off, bad reception, not installed yet, etc.) will eventually receive and update the Broadcast Session Key.



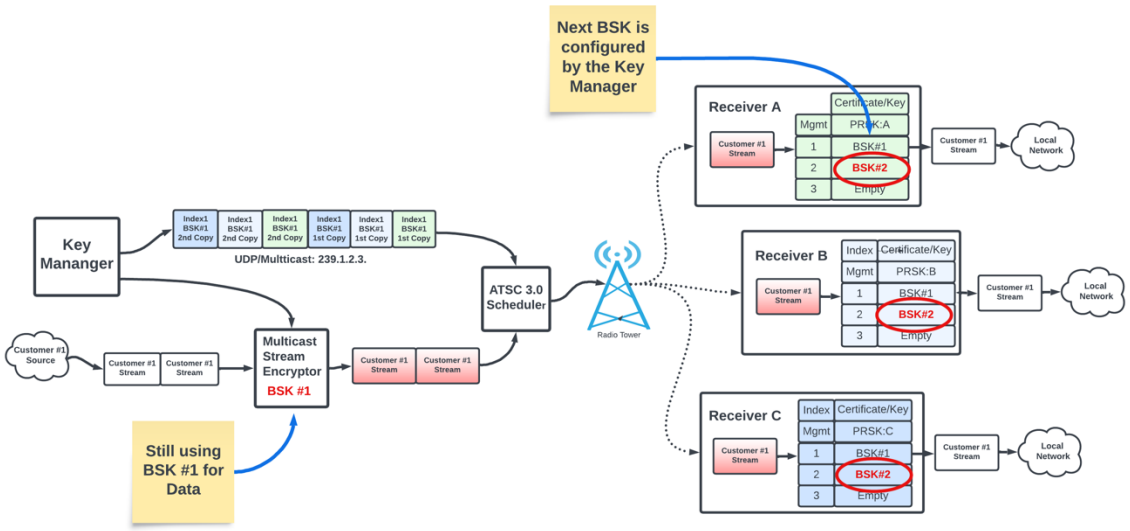
The Multicast Stream Encryptor uses the Broadcast Session Key and Index as directed by the Key Manager for the customer's multicast stream.

Re-keying with the Next Broadcast Session Key

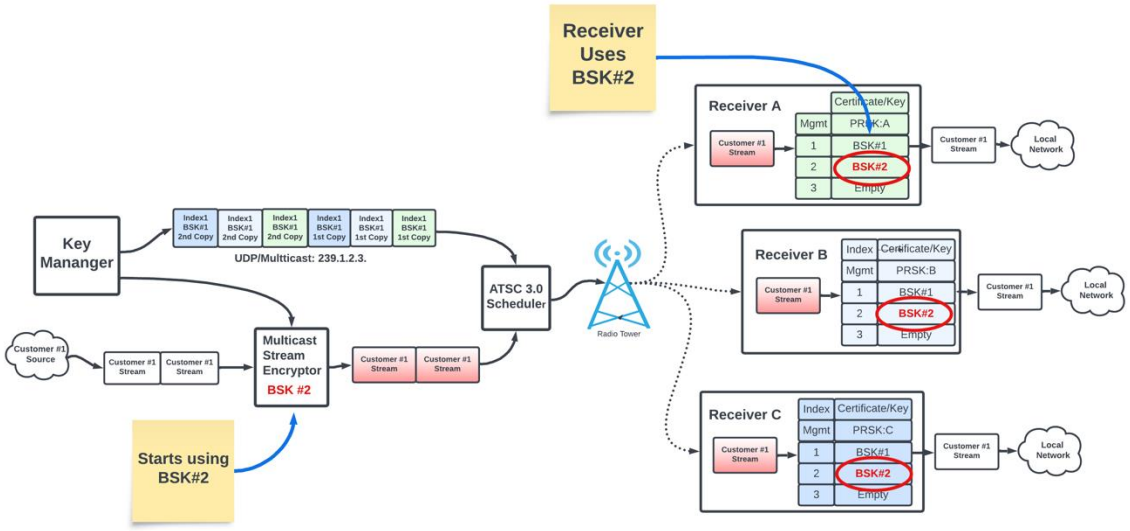
Moving Broadcast Session Keys is the foundational concept that allows the proposed approach to support granting and revoking access to individuals and groups of Receivers.

The primary idea is that Receivers which are being revoked will not receive the new Broadcast Session Key and once the encrypted stream is moved to the new key, the Receiver will no longer be able to decrypt the stream and thus its access is revoked.

First, the next Broadcast Session Key is sent individually only to the Receivers which will continue to have access using the Per Receiver Session Key for that Receiver. The Key Manager manages a concept of Key Index which allows each Receiver to store multiple Broadcast Session Keys simultaneously.



After a configurable number of transmissions, at least 2, of the new Broadcast Session Key, the Key Manager configures the Multicast Stream Encryptor with the next Broadcast Session Key/Index and directs it to start encrypting the customer stream with the next Broadcast Session Key.



The Receiver inspects the Index in the encrypted packet header to know which Broadcast Session Key to use to decrypt the packet. As each Receiver has both the old and the new Broadcast Session Key, the stream cut over happens seamlessly without interrupt or packet drop.

Time to Re-key a Broadcast Session Key

To ensure availability at each Receiver, the next Broadcast Session Key is continuously sent to every Receiver.

The operator will have the option of trading off network management overhead with the how quickly a Receiver returns to service (after powering on, loss of signal, etc.).

Time to re-key a Broadcast Group = Broadcast Session Key Message Size * Number unique Receivers

For example, with a 2Mbp channel with 5% used for management overhead, and 1000 Receivers with a Per Receiver Session Key size of 256 Bytes, this would take:

(2Mb*5% overhead) = 100,000 bits/8 Bytes = 12,500B of Management traffic per sec
12,500B/256 Bytes per message = ~50 Receivers per second
1000 Receivers / 50 Receivers/s = 20 seconds to re-key all the Receivers

This means that a remote device would notionally start decrypting data on average in 10 seconds and worst case of 20s within powering on if there are 1000 Receivers in the same broadcast channel.

Using Security for Access control and Billing

As the Key Manager contains a list of all Receivers, the ability to control access to content is inherent in the architecture.

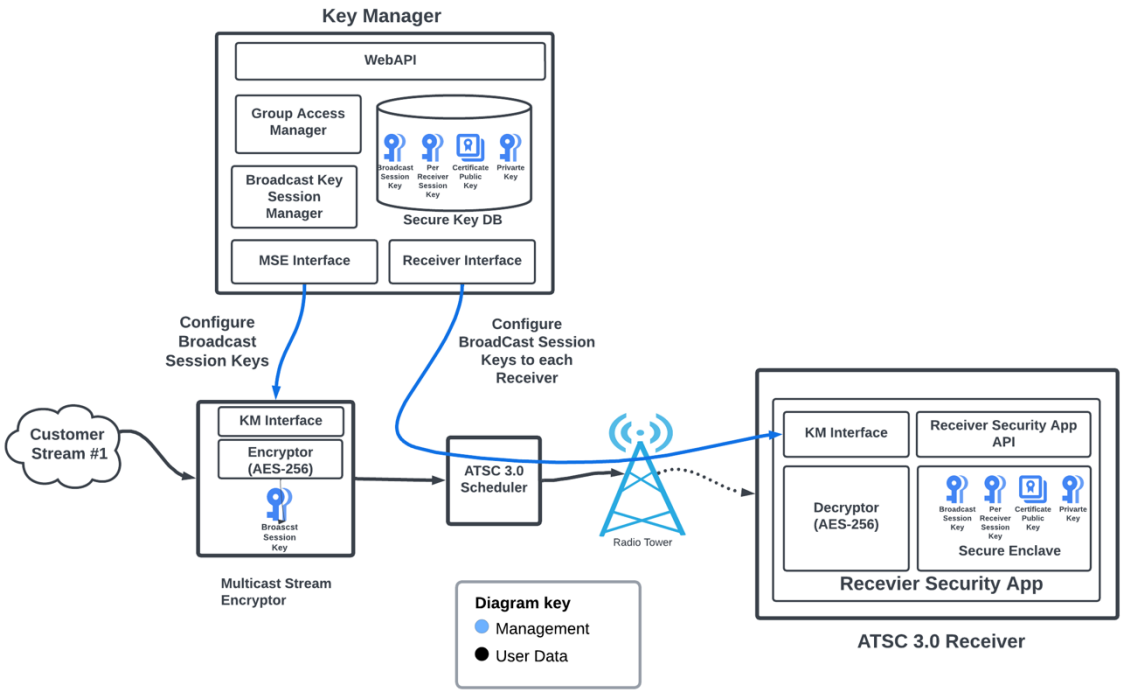
The Key Manager controls which Receiver does and does not get updated with the next Broadcast Session Key.

To limit access to a stream to a single or group of Receivers, the Key Manager will send the next Broadcast Session Key only to approved Receivers. Receivers which do not receive the Next Broadcast Session Key will no longer be able to correctly decrypt received content after the Multicast stream moves to the “Next” Broadcast Session Key.

For example, if a customer is no longer in good standing, the Key Manager will exclude the customer’s associated receivers when it updates to the next Broadcast key. When the customer comes back into good standing, the Receivers will get the appropriate Broadcast Session Key and their Receivers will come back online as they will be able to decrypt incoming data.

ATSC 3.0 Security and Access Control Notional Design

To help evolve the concept, additional detail on high-level functional decomposition as well as roles and responsibilities are provided.



Components

The proposed architecture includes the following components: Key Manager, Multicast Stream Encryptor, Receiver Security App, Receiver Registration App

Key Manager	• Broadcast Session Key Management • Validation of signed Receiver certificates with Certification Authority

	• Per Receiver Session Key X.509 negotiation with Receiver • Management of Broadcast Group • Access and billing control for Broadcast Groups and Receivers • Database with encrypted/secure storage • Infrastructure: Containers managed by Kubernetes • Deployment: Cloud or on-prem
Certificate Authority	• As per A/3.60
Multicast Stream Encryptor	• Receives streams of multicast user data and uses Broadcast Session Key to encrypt the data stream. • 1 per traffic stream • Managed by Key Manager • Infrastructure: Container managed by Kubernetes • Deployment: Cloud or on-prem
Receiver Security App	• Decrypts User streams • Connects with Key Manager to create Per Receiver Session Key • Deployment: Embedded application or container based on Receiver local network. • Stores keying material in a local Secure Enclave such as eSIM as available.

Datacasting Security Future: Quantum Key Distribution

As we look to the future of encryption, Quantum computing is becoming more and more relevant as it is one of the most significant threats to public key cryptography.

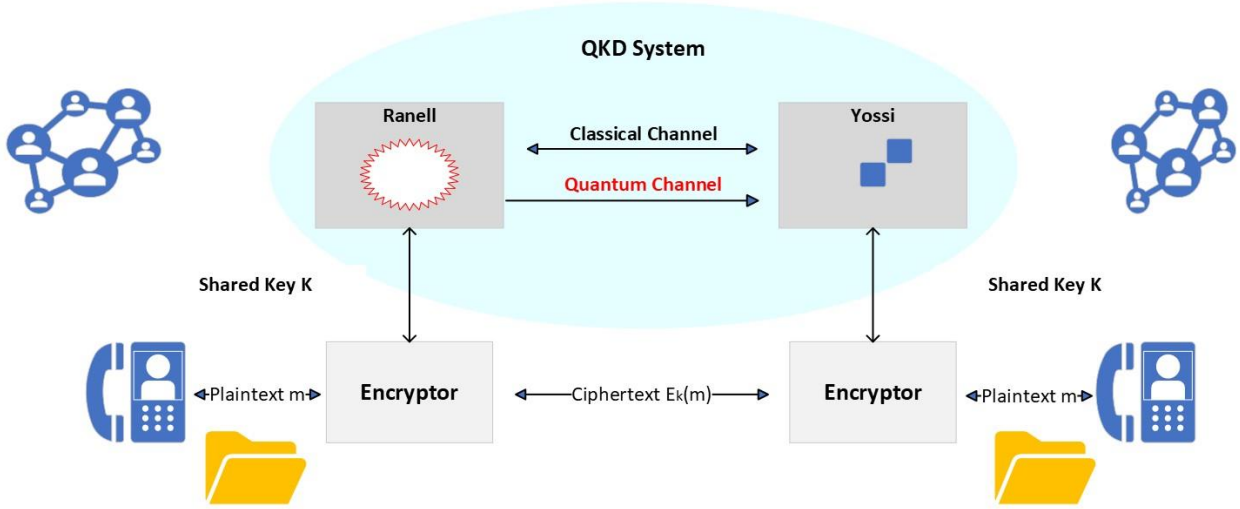
Public key cryptography relies on the factoring of prime numbers which makes it vulnerable to attacks by quantum computing. Cracking 256-bit encryption using a quantum computer is estimated to take a relatively short amount of time, potentially just a few hours. This is due to the computational power and capabilities of quantum computers, which can perform certain types of calculations much faster than classical computers. Once this threat is realized, AES 256 and the PKI infrastructure must be deprecated, and a replacement found.

Furthermore, the urgency of this threat is amplified by “store now and decrypt later” which involves the long-term storage of encrypted data that is currently unreadable in the hopes that future advances in decryption technology will make it readable.

With the advent of quantum computing came quantum cryptography or Quantum key distribution (QKD). As Quantum encryption is based on physics, not prime numbers or complicated mathematical formulas, it is thought to be unbreakable and un-hackable. Quantum key distribution, which is a cryptographic method, uses the principles of quantum mechanics to transmit information securely. QKD also allows two parties to exchange cryptographic keys in such a way that listening is impossible and ensures the security of communication.

How does quantum cryptography work? In plain language, a qubit or quantum bit is a basic unit of quantum information. The qubit is the quantum version of the classic binary bit which can either

represent a 0 or a 1 at the same time. This is called superposition, an important concept of quantum mechanics, as the concept states that a particle can exist in several states simultaneously until it is measured, at which point it collapses into a single state.



Superposition creates a secure communication channel, thereby insuring that eavesdropping attempts will disrupt the quantum state, alerting the parties involved.

Assume that you have a smiley face and a frowning face, each one representing a qubit and assume that a matching pair of them create your key. If the transmission of the qubit (your matching smiley/frowning faces) is interrupted, there will be no access on the receiving end. This in turn sends a prompt to the sender that there was an issue on the other end and to resend the transmission. Since there is a receiver at both ends, the transmission cannot be intercepted without changing the dynamics of the qubit. There are circumstances where there can been degradation, but superposition in most instances ensures that the qubit is always in several states and, at any given time, impossible to intercept.

Conclusion

Evolving the currently specified ATSC 3.0 security infrastructure will be key to enabling growth and scalability across a heterogenous set of customers and applications that must share the broadcast capacity to support the needed economic and monetization model to offset the decline of advertising from linear content.

Groups of users with NRT (Non-Real Time) and non-linear applications will use the capacity intermittently and without the ability to limit access, inefficient static broadcast capacity must be commissioned. The proposed architecture enables this growth through secure multiplexing of shared capacity with significantly more granularly. An operator will create a static PLP and allow multiple users and applications to statistically multiplex the broadcast capacity safely without concern that unapproved receivers will have access to a user's content.

Many of the potential use cases will not be able to have a return path, or the requirement of a return path, will add adoption friction and cost. The proposed solution only requires an Internet connection

during the initial registration. Afterwards, full transmission security and access control can be achieved reliability without requiring a return path.

With the current security specification, there is no defined way to enforce access control for billing on a per receiver or per customer basis. Without the ability to track and revoke access, a subscription-based model is difficult to manage and enforce without relying on a customer to operate and report in good faith. How many units have been deployed? What does the service provider do when a customer fails to pay? Furthermore, most customers won't want to track this information even if they are operating in good faith. The proposed solution solves these very real monetization problems by providing a mechanism to seamlessly track deployed receivers and revoke access with a high degree of granularity without requiring an operational return path.

The ATSC 3.0 community must evolve the existing Datacasting security specification and available capabilities to address these concerns as well as the impending future obsolescence of AES-256 and PKI infrastructure to protect, grow and monetize the ATSC 3.0 Datacasting spectrum.

Please reach out to our team to learn more.

About PEAK3 (www.peakthree.io)

PEAK3 has a long-term engagement with the spectrum owners to offer this alternative data highway to its many technology partners, its enterprise clients, and to its engineering teams to further develop novel applications where the ATSC 3.0 value proposition can enable the edge-device community. From hardware architecture through the application layer, the PEAK3 team has a rich history of successful enterprise edge deployments and IT system designs and operations.
We recognize the unique value proposition ATSC 3.0 provides in delivering secure, efficient, data-delivery methods to the edge. The foundation of our business model is Data-Streaming as a Service for organizations wanting to efficiently get data from one point to many.
PEAK3 provides a standards-based, open, end-to-end, nationwide, wireless, IP, multicast network. In simple terms, we provide a cost-effective datacasting pipe for Internet Service Providers, public and private cloud providers, and any organizations operating large edge device architecture.

About Alp Sezen (Author)

A highly reputable, 30+ year Executive with multiple disciplines on the global technology stage. Positions range from Global Sales Leadership and Business Development to Global Design and Strategy for Product Deployment and Support. Strong track record of start-up implementation and scale in segments ranging from VOIP to Long-range Communication solutions for the Railroad Industry.
His efforts and solutions have positively impacted a wide range of industries from; Military applications, Medical, Telco, parallel computing, Industrial, Retail, Oil& Gas, Enterprise IT, storage solutions and currently AI, 5G and distributed edge computing technology implementations.

About Cybrella (https:.//www.cybrella.io)

Cybrella is a leading Cyber Security consulting service provider based in the US, providing exceptional advisory services worldwide. Cybrella Inc was founded as a US incorporation delivering leading-edge solutions and high-end consultancy to various customers in Cyber Security.
Our unique expertise in cyber security allows us to be the best in what we do, from our employees' expertise that includes a broad range of professional experience and a credible and proven record of accomplishment of certification in the fields of communications, applications, databases, and cloud platforms.

About Franklin A Jackson (Co-Author)

Franklin is the current Chief Operating Office of Cybrella, Inc. He is a recognized industry Cyber Security authority and leader in digital transformation, with substantial experience in steering multiplatform enterprise security solutions. His background includes developing and managing Cyber Security as an enterprise-wide strategic issue in government, medical and financial sectors. He is an expert in cloud and security technologies, providing governance and risk-based security. He has an entrepreneurial approach to developing fast-paced advisory services programs, under extreme budget and time constraints and holds a Department of Defense Active Secret Clearance.