ATSC Recommended Practice: Security and Content Protection

Doc. A/361:2019
10 December 2019

Advanced Television Systems Committee
1776 K Street, N.W.
Washington, D.C. 20006
202-872-9160

The Advanced Television Systems Committee, Inc., is an international, non-profit organization developing voluntary standards and recommended practices for digital television. ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries. ATSC also develops digital television implementation strategies and supports educational activities on ATSC standards. ATSC was formed in 1983 by the member organizations of the Joint Committee on Inter-society Coordination (JCIC): the Electronic Industries Association (EIA), the Institute of Electrical and Electronic Engineers (IEEE), the National Association of Broadcasters (NAB), the National Cable Telecommunications Association (NCTA), and the Society of Motion Picture and Television Engineers (SMPTE). For more information visit www.atsc.org.

Note: The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. One or more patent holders have, however, filed a statement regarding the terms on which such patent holder(s) may be willing to grant a license under these rights to individuals or entities desiring to obtain such a license. Details may be obtained from the ATSC Secretary and the patent holder.

Implementers with feedback, comments, or potential bug reports relating to this document may contact ATSC at https://www.atsc.org/feedback/.

Revision History

Version	Date
Recommended Practice approved	10 December 2019

Table of Contents

ATSC Recommended Practice: Security and Content Protection

1. SCOPE

This Recommended Practice describes recommended operational modes and parameters for implementation of the security features (excluding DRM) described in ATSC A/360:2019 [1].

1.1 Organization

This document is organized as follows:

- Section 1 – Outlines the scope of this document and provides a general introduction.
- Section 2 – Lists references and applicable documents.
- Section 3 – Provides a definition of terms, acronyms, and abbreviations for this document.
- Section 4 – Recommended Practice
- Section 5 – Key management
- Section 6 – Certificate management
- Section 7 – Security System Design Recommendations

2. REFERENCES

All referenced documents are subject to revision. Users of this Recommended Practice are cautioned that newer editions might or might not be compatible.

2.1 Informative References

The following documents contain information that may be helpful in applying this Standard.

[1] ATSC: "ATSC 3.0 Security and Service Protection," Doc. A/360:2019, Advanced Television System Committee, Washington, D.C., 20 August 2019.

[2] IEEE: "Use of the International Systems of Units (SI): The Modern Metric System," Doc. SI 10, Institute of Electrical and Electronics Engineers, New York, N.Y.

[3] National Institute of Standards and Technology, U.S. Department of Commerce: "Recommendations for Key Management, Part 1: General," NIST Special Pub. 800-57 Part 1, Rev. 4, January 2016, available at http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4.

3. DEFINITION OF TERMS

With respect to definition of terms, abbreviations, and units, the practice of the Institute of Electrical and Electronics Engineers (IEEE) as outlined in the Institute's published standards [2] should be used. Where an abbreviation is not covered by IEEE practice or industry practice differs from IEEE practice, the abbreviation in question will be described in Section 3.3 of this document.

3.1 Compliance Notation

This section defines compliance terms for use by this document:

should – This word indicates that a certain course of action is preferred but not necessarily required.

should not – This phrase means a certain possibility or course of action is undesirable but not prohibited.

3.2 Treatment of Syntactic Elements

This document contains symbolic references to syntactic elements used in the audio, video, and transport coding subsystems. These references are typographically distinguished by the use of a different font (e.g., restricted), may contain the underscore character (e.g., sequence_end_code) and may consist of character strings that are not English words (e.g., dynrng).

3.2.1 Reserved Elements

One or more reserved bits, symbols, fields, or ranges of values (i.e., elements) may be present in this document. These are used primarily to enable adding new values to a syntactical structure without altering its syntax or causing a problem with backwards compatibility, but they also can be used for other reasons.

The ATSC default value for reserved bits is '1'. There is no default value for other reserved elements. Use of reserved elements except as defined in ATSC Standards or by an industry standards-setting body is not permitted. See individual element semantics for mandatory settings and any additional use constraints. As currently-reserved elements may be assigned values and meanings in future versions of this Standard, receiving devices built to this version are expected to ignore all values appearing in currently-reserved elements to avoid possible future failure to function as intended.

3.3 Acronyms and Abbreviations

The following acronyms and abbreviations are used within this document.

AES Advanced Encryption Standard
ATSC Advanced Television Systems Committee
CSR Certificate Signing Request
DRM Digital Rights Management
ECC Elliptic Curve Cryptography
MAC Media Access Control
NIST National Institute of Standards and Technology
OSCP Online Certificate Status Protocol
PKCS Public Key Cryptography Standards
RSA A public-private key encryption algorithm
SHA Secure Hash Algorithm
SP Scattered Pilot
TLS Transport Layer Security

3.4 Terms

The following terms are used within this document.

reserved – Set aside for future use by a Standard.

4. RECOMMENDED PRACTICE

This document provides a set of recommended practices for implementors of ATSC A/360 [1].

4.1 Key Size Selection

NIST Recommendation SP 800-57 [3] provides useful information relating to the comparative cryptographic strength of symmetric and asymmetric key sizes. The choice of algorithms and key

sizes should be aligned to a security strength of at least 128 as described in SP 800-57, Section 5.6. Keys with a security strength of 128 are considered acceptable when applying cryptographic protection and when processing cryptographically protected data through 2031 and beyond. When choosing algorithms and key sizes, the most up-to-date version of SP 800-57 should be consulted.

A security strength of 128 is equivalent to the following key sizes specified in A/360:

AES Symmetric Key	128 bit
RSA Asymmetric Key	3072 bit modulus
ECC Curve	secp256r1
Message Digest and Hash	256 bit SHA-2
Hashed MAC	160 bit SHA-1

A security strength of 192 is equivalent to the following key sizes specified in A/360:

AES Symmetric Key	192 bit
RSA Asymmetric Key	7680 bit modulus
ECC Curve	secp384r1
Message Digest and Hash	384 bit SHA-2
Hashed MAC	256 bit SHA-2

A security strength of 256 is equivalent to the following key sizes specified in A/360:

AES Symmetric Key	256 bit
RSA Asymmetric Key	15360 bit modulus
ECC Curve	secp521r1
Message Digest and Hash	512 bit SHA-2 or SHA-3
Hashed MAC	256 bit SHA-2

Note: NIST SP 800-57 Part 1 Revision 4 disallows the use of RSA Key sizes of 1024 bit modulus and does not consider a RSA Key size of 2048 bit modulus to be suitable or applying cryptographic protection beyond 2030.

4.2 Choice of Cryptographic Algorithms for Signatures

The choice of cryptographic algorithms used in asymmetric keys can have a significant effect on both the time taken to sign or encrypt data and the size of the signature block. Currently keys that conform to RSA-3072 or to the secp256r1 curve parameters are considered to be sufficiently secure to be used in an ATSC 3.0 broadcast environment.

The recommendation for the choice of the signature algorithm and message digest algorithm for use with a cryptographic key is, in order of preference, as follows:

1) rsa-pkcs1, SHA-256
2) ecdsa, secp256r1, SHA-256
3) ecdsa, secp384r1, SHA-384
4) ecdsa, secp521r1, SHA-512

Note: RSA Key sizes are larger than ecdsa keys (but the described ecdsa methods are more secure and more computationally-intensive than RSA with shorter key sizes).

As of the date of this Recommended Practice, NIST [3] has determined that rsa-pkcs1 (with RSA-3072 key size), SHA-256 is sufficiently secure for digital signatures until beyond 2031. Additionally, implementors of the ATSC 3.0 system should be aware that RSA-4096 calculations

are approximately as secure and computationally intensive as secp256r1, but that secp256r1 key sizes are smaller (4096 vs. 256 bits). Therefore, broadcasters should use rsa-pkcs1 (with RSA-3072 key size), SHA-256 for signing signaling and applications.

The certificate authority used by the broadcaster should advise broadcasters in the case that a change to a different set of signature and message digest algorithms is considered advisable.

4.3 Transport Layer Security (TLS)

Broadcaster servers that respond to TLS Client interaction channel requests should establish a connection under the TLS 1.3 protocol using one of the TLS 1.3 Cipher Suite combinations defined in A/360. In the case that the broadcaster server does not support TLS 1.3 and requests the TLS Client to downgrade to TLS 1.2 the server will use one of the TLS 1.2 Cipher Suites defined in A/360 [1], because only TLS 1.2 and TLS 1.3 are allowed.

When making these TLS connections, the server should choose to negotiate the connection using the first Cipher Suite that the Client supports from the corresponding list below for the TLS protocol version being negotiated, and should choose the first combination appropriate.

For TLS 1.3 the order of preference is:

1) TLS_AES_128_GCM_SHA256 with secp256r1 and ecdsa_secp256r1_sha256
2) TLS_AES_128_GCM_SHA384 with secp384r1 and ecdsa_secp384r1_sha384
3) TLS_AES_128_GCM_SHA384 with secp521r1 and ecdsa_secp521r1_sha512

For TLS 1.2 the order of preference is:

1) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
2) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
3) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
4) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

5. KEY MANAGEMENT

The use of good key management practices is critical for the security of the broadcaster's service and the following recommendations are provided to limit the opportunities for key compromise.

1) Where keys need to be accessed on a regular basis, for example in signing signaling tables, keys should be generated within the confines of a hardware-based security module, and all cryptographic calculations using the key should occur within the confines of that security module.
2) Keys should not be stored on either a fixed or removable media device, even where that file has been encrypted, unless the media device itself is safely stored in a secure location (like a safe) that requires multi-person access.
3) Keys should be protected using a key wrapping system that uses M-of-N encryption tokens to access the key when keys are stored on a fixed or removable media device. The M-of-N tokens should use a minimum M value of 2 and a minimum N value of 3.
4) An encrypted version of the key, as per (3) above, should be stored in a secure location that requires multi-person access. This escrowed version of the key can be used to install a key onto another hardware token for use in a redundant pair (see below).
5) All key storage devices (including hardware security modules) and computer systems used to create application and signaling signing messages defined in A/360 which are not in regular use should be safely stored in a secure location that requires multi-person access (like a safe).

6) Passwords used to manage hardware security devices such as M-of-N encryption tokens should be randomly generated and securely stored in tamper-evident envelopes. These passwords are expected to be used irregularly and changes in broadcaster personnel may result in a different person performing a particular role in place of the person who originally created the password.

5.1 Redundant Systems

Where two or more systems are used to provide failover redundancy and each of these systems needs to have access to the same application or signaling signing key, the key should be created on one hardware-based security module and then escrowed (as described above). Copies of the escrowed key can be made to other hardware-based security modules to enable access to the same key from multiple systems.

Note that some hardware security modules may not provide a system that allows a key to be extracted even under the control of M-of-N encryption tokens, such devices will not be suitable for use in an environment that needs to implement failover redundancy.

5.2 Key Replacement and Spares

The broadcaster should maintain sufficient spare hardware security modules to ensure compatibility with the currently installed systems whenever a new key is generated for use in A/360 security signaling and application signing. All spare devices should be initialized and verified as working replacements at the time of purchase.

Where a storage device contains key materials that are no longer used by the broadcaster, these key materials should be securely destroyed in accordance with the device manufacturer's procedures. Once the destruction of legacy keys has been verified, the broadcaster can reuse the device to generate and store future keys.

6. CERTIFICATE MANAGEMENT

6.1 Trusted Certificates

Where a broadcaster receives a trusted certificate (for example, a Root Certificate) from a third party, the broadcaster should independently verify the authenticity of that certificate with the issuer. The check may involve calculating a message digest (hash or fingerprint) of the certificate contents and verifying this with a designated representative of the certificate issuer, preferably using a verification mechanism that does not involve electronic mail or internet message exchange.

Trusted certificates should only be installed into broadcaster systems once their validity has been independently established.

6.2 Subsidiary Certificate Installation

The trust path for any certificate that a broadcaster installs into its equipment should be verified to a previously installed trusted certificate. Where the certificate is authenticating a key that is owned by the broadcaster, the broadcaster should also verify that the public key authenticated by the certificate matches the key that it owns.

6.3 OCSP Responder Identities

The OCSP Responder identity for each of the ATSC issued certificates is contained in the Authority Information Access extension for that certificate. The identities used are likely to be

common across all certificates issued for broadcaster use and the content of this extension should be verified against a certificate authority's published list before the certificate is installed into a broadcaster system. Where necessary, an unknown OCSP Responder Identity should be verified with the certificate issuer in order to establish trust in the new identity.

6.4 Certificate Content

The broadcaster needs to supply naming information to the certificate authority in its certificate request. The form of this naming information will be controlled by the certification policies defined by the certificate authority. The certification procedures established by the certificate authority can require the broadcaster to provide evidence of ownership or rights to use for information that will be authenticated by the certificate; the broadcaster should be prepared to provide the evidence requested by the certificate authority before the certificate can be issued. This can include the provisioning of an electronic certificate request file in PKCS#10 (CSR) format.

Note: The specific certification practices and procedures used by the certification authority are beyond the scope of this document. However, the broadcaster will need to comply with those practices and procedures that determine the certificate authority's requirements for issuing subscriber certificates.

6.5 Certificate Revocation

Where the broadcaster becomes aware or believes that one or more of its keys have been compromised, it is important to follow the revocation procedures established by the certification authority. These procedures should be followed at the earliest possible opportunity. The broadcaster should interact with the certificate authority, including where considered necessary an audit of the broadcaster's security procedures, to re-establish a secure operating environment for its systems.

In the case that the revoked certificate authenticates a certificate authority or an OCSP Responder (rather than a broadcaster certificate), the broadcaster should follow the guidance issued by the certificate authority in order to re-establish secure operation of its systems.

6.6 Certificate Expiration and Renewal

The broadcaster is responsible for managing requests to issue a replacement certificate before the expiration of any currently active certificates is reached, and should apply for a replacement certificate early enough to ensure a replacement can be delivered before expiration. The certificate authority procedures should indicate the process for renewing a certificate; this may involve the generation of a new key depending on the certificate authority policies and procedures.

7. SECURITY SYSTEM DESIGN RECOMMENDATIONS

7.1 Managing the Certification Data Table

The Certification Data Table structure has been designed to allow the table to be signed off-line and only the OCSP Responses to be added to the table during regular operation. Broadcasters should adhere to this design principle by using a separate process to create and sign those components of the Certification Data Table other than the OCSP Responses. The signed components can then be moved to a service that includes the up-to-date OCSP Responses prior to transmission.

7.2 Application Signing

Where application content does not change dynamically (for example, in response to feedback from the current user or other external activity), the application signing for both author and distributor should be managed in an off-line environment.

7.3 OCSP Request Consolidation

The application and signaling signing processes include OCSP Responses for each of the certificates included in the message structures. For efficiency reasons, all of the OCSP Requests sent to a single OCSP Responder should be consolidated into a single request. This not only reduces the number of requests sent to a single OCSP Responder, but also limits the number of OCSP Responder certificate and signature instances that are included in the signed application and signaling message.

– End of Document –