Certification Practice Statement

ATSC 3.0 Certificate Authority (ATSC3CA)

Silicondust USA, Inc.

Version 20251201-1
December 1, 2025
www.silicondust.com
www.atsc3ca.com

1 Introduction

Launched in 2025, the ATSC 3.0 Certificate Authority (ATSC3CA) is a service owned and operated by Silicondust USA, Inc.

Silicondust issues trusted digital certificates compliant with ATSC 3.0 standards to television stations and entities working with ATSC 3.0 technology, doing so in accordance with this Certification Practice Statement.

In its role as a Certificate Authority, Silicondust performs functions associated with public key operations that include:

1. Receiving requests, issuing, revoking, and renewing digital certificates.
2. Providing and maintaining a high reliability Online Certificate Status Protocol (OCSP) responder service.
3. Publication, maintenance, and hosting of Certificate Revocation Lists (CRLs).
4. Maintaining compliance with the ATSC 3.0 Security and Service Protection A/360 Standard.

Certificates and the OCSP service conform to the current version of the ATSC 3.0 Security and Service Protection A/360 Standard published by ATSC at https://www.atsc.org/atsc-documents/type/3-0-standards/.

2 Certificates Requests

2.1 Requester / Entity validation

The requester/entity validation is performed by Silicondust or by a Broadcast System Integrator qualified by Silicondust. The current list of Broadcast System Integrators qualified by Silicondust is as follows:

- Heartland Video Systems (HVS)

When the requester/entity is a television station requesting FullTrust certificates for broadcast use the requester/entity validation includes the following:

- Verify the accuracy and authenticity of the information provided.
- Verify the requester is an authorized representative of the station.
- Verify the Callsign, BSID, and station ownership information against the public FCC database.

When the requester/entity requests AskTrust certificates for use in a private RF environment the requester/entity validation includes the following:

- Verify the accuracy and authenticity of the information provided.
- Verify the entity name against the DUNS database or government issued paperwork provided.

2.2 CSR Validation

The CSR validation is performed by Silicondust. This validation includes the following:

- Verify the key referenced in the CSR is 3072-bit RSA.
- Verify the Subject field in the CSR includes sufficient and identifying information matching the paperwork.

Note that the Subject Common Name (CN) and BSID values in the certificate are set by the certificate generation process, not sourced from the CSR.

3 Certificate Usage

3.1 FullTrust Certificates

- Only available to licensed television stations.
- For use in public broadcasts.
- Certificates are locked to the station BSID.
- Certificates cannot be shared across multiple stations or sites.
- Certificates may be shared among multiple pieces of equipment within a single station-site, for example broadcast equipment in a failover configuration.

3.2 AskTrust Certificates

- Only for use in private RF environments. Must not be used in a public broadcast.
- Certificates cannot be on sold or transferred.
- Certificates cannot be shared across multiple sites.
- Certificates may be shared among multiple pieces of equipment within a single site, for example equipment in a failover configuration.

3.3 Prohibited Certificate Uses

Certificates are prohibited from being used to the extent that the use is inconsistent with applicable law.

Certificates are prohibited from being used as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe damage to persons or property.

Certificates are not for use as a means of providing transmitter identity assurance. There is no guarantee that any given transmitter is the original source of a signed broadcast.

4 Certificate Revocation

4.1 Reporting

A certificate holder is required to report theft, exposure, or loss of control of a private key. This includes data breaches where the private key may have been exposed, theft of equipment where the equipment contains a private key, etc.

Abuse reporting, prohibited use reporting, loss of control reporting, etc must be made to:

atsc3ca@silicondust.com

or

Silicondust USA Inc.
Attn: ATSC3CA
2150 Portola Ave, Suite D #143
Livermore, CA 94551, USA

4.2 Evaluation

Silicondust will examine each received report within five business days, excluding USPS holidays.

Revocation is triggered in cases of:

- Request to revoke a certificate by the entity the certificate was issued to.
- Theft, exposure, or loss of control of a private key.
- Demonstrated use of the private key such as signing, not by the entity the certificate was issued to.
- Use of a certificate **by the holder** in a way not allowed by applicable law, not allowed by published ATSC standards, or not allowed by ATSC3CA policy.

Note that a pirate broadcast that replays signed signaling received from a licensed and compliant broadcast does not constitute “use of a certificate by the holder” and is not a basis for revocation.

Silicondust understands that care must be taken as false reports could be filed in an attempt to disrupt television stations similar to calling in a fake bomb threat.

For FullTrust certificates used by a licensed television station for public broadcast, Silicondust or an approved Broadcast System Integrator will attempt to reach the station engineer prior to a certificate being revoked. Silicondust or the Broadcast System Integrator will attempt to work with the station to resolve the underlying problem and to help with the Certificate Request process in order to obtain new certificates with new private keys.

AskTrust certificates may be revoked without delay and without notice when any of the above trigger conditions are met.

4.3 Revocation Delay

Silicondust may, at its discretion, delay publishing the revocation of FullTrust certificates used by a licensed television station for the sole purpose of smoothing a station's transition to new certificates.

When a certificate revocation is published it may take some number of hours to reflect in OCSP responses and the CRL download due to normal update cycles and web caching.

Note that a bad actor may be able to continue to broadcast using an old OCSP response up until the end date of that old response, typically 7 days after the OCSP response was generated.

5 Certificate Validation

To verify the validity of a digital certificate the equipment must verify against a current Online Certificate Status Protocol (OCSP) response to ensure the certificate has not been revoked.

Certificate Revocation List (CRL) files are maintained and published following PKI norms. There is no requirement for equipment to download and check a CRL due to the above OCSP requirement.

5.1 Receivers

The ATSC 3.0 standard requires a current OCSP response be sent in the broadcast. This negates the need for a receiver to issue an OCSP request and receive an OCSP response via the Internet.

The receiver is required to complete OCSP verification of the certificate before using the certificate. If the OCSP response in the broadcast is missing or fails validation the OCSP verification of the certificate has failed and the certificate must not be used by the receiver.

6 Broadcast Equipment

Sending a current OCSP response in the broadcast is critical to the broadcast. In the event that a new OCSP response cannot be obtained the last known OCSP response must be sent in the broadcast, and only discarded once the end time is reached (typically 7 days from issuance). This ensures that an internet outage or OCSP service outage cannot result in the broadcast failing receiver validation unless the outage lasts more than 7 days.

To meet this requirement, when an OCSP response is received it must be stored in non-volatile storage such that it can be retrieved and sent in the broadcast after a reboot or power cycle without Internet access.

It is recommended that a new OCSP request be attempted approximately every hour. Equipment should avoid scheduling this request at a fixed time such as on the hour, but rather use a randomized delay between each request. For example, a random delay in the range of 45 to 75 minutes.

The OCSP URL is included in each certificate. The protocol is HTTP.

The Content-Type of the OCSP request must be "application/ocsp-request".

7 At-Station OCSP

A licensed television station meeting physical security requirements may purchase At-Station OCSP hardware to ensure ongoing compliant operation throughout an Internet outage lasting more than 7 days.

The hardware is in the form of a secure USB token that acts as a OCSP server. The CPU onboard uses a secure boot process, encrypted storage, and is epoxy potted. No private keys are stored in the token.

The token is paired with the station's broadcast equipment to ensure it cannot operate if intercepted before installation or if misplaced after initial installation.

The token can only provide OCSP responses matching the certificates issued to the specific station.

Patent Pending.

8 Silicondust as a Customer

Silicondust operates ATSC3CA isolated from other business interests. In the event that other aspects of Silicondust business require and fully qualify for ATSC 3.0 certificates, the same certificate request process, validation process, and certificate issuing rules in this certification statement will be applied. Likewise Silicondust (the customer) is bound by the

same requirements for safeguarding private keys and allowed use of certificates. In the event of a compliant the same investigation process and actions will be applied.

To ensure complete transparency, ATSC3CA will publish a list of all certificates issued to Silicondust on the ATSC3CA website. No certificates have been issued to Silicondust as of the date of this publication.

9 Special cases

It is expected that equipment vendors, test suite vendors, and/or interop event operators will have use cases that cannot be fulfilled under normal policies.

Special cases are not available for FullTrust certificates.

Special cases must not be used outside of a private RF environment.

To apply for special handling the requester must be an equipment vendor, test suite vendor, or interop event operator. The requester must have a valid use case that cannot be addressed through normal policies.

The use case will be evaluated by Silicondust, the security implications considered and documented, and a proposed solution (if any) discussed with the requester.

If a solution is finalized the special case will be added to this section of the certification statement and published within 7 days of the special case being delivered.

9.1 OCSP token for broadcast equipment vendors

Problem: Broadcast equipment vendors supplying television stations need to be able to develop and test with OCSP tokens similar to the tokens available to television stations, however policy does not allow for an OCSP token to be issued to an entity that is not a licensed television station.

Solution: Issue AskTrust certificates to the broadcast equipment vendor as per normal policy. Issue a test OCSP token that does not contain OCSP responses, rather it returns a 307 Temporary Redirect when queried with a valid request such that the OCSP request is redirected to the normal Internet based OCSP responder service.

Available to: Broadcast equipment vendors supplying television stations. Requester must meet normal AskTrust requirements.

Security implications: None. The OCSP response is obtained via the Internet as normal for an AskTrust certificate. If used in a public broadcast it offers no advantage or purpose.

9.2 Expired or near-expiry certificates for testing

Problem: it is necessary to test with expired certificates or certificates that are about to expire.

Solution: Issue AskTrust certificates with an end date set earlier than normal policy.

Available to: Equipment vendors, test suite vendors, and interop event operators. Requester must meet normal AskTrust requirements.

Security implications: None.

Appendix A: Acronyms

Acronym	Full Name
ATSC	Advanced Television Systems Committee
ATSC3CA	ATSC 3.0 Certificate Authority [by Silicondust]
CA	Certificate Authority
CN	Common Name
CRL	Certificate Revocation List
CSR	Certificate Signing Request
HVS	Heartland Video Systems [Inc]
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure

Appendix B: Types of Certificates

Leaf Certificate Types:

- FullTrust Application Author Certificate
- FullTrust Application Distributor Certificate
- FullTrust Signaling Signing CDT Certificate
- FullTrust Signaling Signing SMT Certificate
- AskTrust Application Author Certificate
- AskTrust Application Distributor Certificate
- AskTrust Signaling Signing CDT Certificate
- AskTrust Signaling Signing SMT Certificate

Intermediate Certificate Types:

- FullTrust Intermediate Certificate
- AskTrust Intermediate Certificate
- Root OCSP Responder Certificate

Root Certificate Types:

- Root Certificate

Appendix C: Certificate Profiles

FullTrust / AskTrust Leaf Certificates:

Version	3	
Serial Number	160 bit	
Signature Algorithm	sha256WithRSAEncryption	
Issuer (CN one of)	CN	**FullTrust**: ATSC3 FullTrust CA G<n> **AskTrust**: ATSC3 AskTrust CA G<n>
	O	Silicondust USA, Inc.
	C	US
Validity	1-2 years + 1 month	
Subject (CN one of)	CN	**App Author**: <callsign> Application Author **App Distributor**: <callsign> Application Distributor **CDT**: <callsign> Signaling Signing CDT **SMT**: <callsign> Signaling Signing SMT
	O	Organization
	OU	Organization Unit, optional
	L	Locality, required in USA
	ST	State or Province, required in USA
	C	Country
Subject Public Key	3072 bit RSA	
Subject Key Identifier	160 bit	
Authority Key Identifier	160 bit	
Basic Constraints	Critical, CA:FALSE	
Certificate Policies (one of)	**FullTrust**: Critical, 1.3.6.1.4.1.64225.1.1 **AskTrust**: Critical, 1.3.6.1.4.1.64225.1.2	
Key Usage	Critical, Digital Signature	
Extended Key Usage (one of)	**App Author**: Critical, 1.3.6.1.4.1.51552.37.1 **App Distributor**: Critical, 1.3.6.1.4.1.51552.37.2 **CDT**: Critical, 1.3.6.1.4.1.51552.37.3 **SMT**: Critical, 1.3.6.1.4.1.51552.37.3	
CRL Distribution Points	URI:http://pki.atsc3ca.com/<filename>.crl	
Authority Information Access	OCSP - URI:http://pki.atsc3ca.com/ocsp	
Subject Directory Attributes	1.3.6.1.4.1.51552.9.1 = BSID set containing 1 or more BSID values	
Signature Algorithm	sha256WithRSAEncryption	

FullTrust / AskTrust Intermediate Certificates:

Version	3	
Serial Number	160 bit	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	CN	ATSC3 Root-CA Silicondust
	O	Silicondust USA, Inc.
	C	US
Validity	10 years	
Subject (CN one of)	CN	**FullTrust**: ATSC3 FullTrust CA G<n> **AskTrust**: ATSC3 AskTrust CA G<n>
	O	Silicondust USA, Inc.
	C	US
Subject Public Key	3072 bit RSA	
Subject Key Identifier	160 bit	
Authority Key Identifier	160 bit	
Basic Constraints	Critical, CA:TRUE, pathlen:0	
Certificate Policies (one of)	**FullTrust**: Critical, 1.3.6.1.4.1.64225.1.1 **AskTrust**: Critical, 1.3.6.1.4.1.64225.1.2	
Key Usage	Critical, Digital Signature, Non Repudiation, Certificate Sign, CRL Sign	
CRL Distribution Points	URI:http://pki.atsc3ca.com/atsc3_root_ca_silicondust.crl	
Authority Information Access	OCSP - URI:http://pki.atsc3ca.com/ocsp	
Signature Algorithm	sha256WithRSAEncryption	

Root-signed OCSP Responder Certificate:

Version	3	
Serial Number	160 bit	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	CN	ATSC3 Root-CA Silicondust
	O	Silicondust USA, Inc.
	C	US
Validity	10 years	
Subject	CN	ATSC3 Root-CA OCSP Responder G<n>
	O	Silicondust USA, Inc.
	C	US
Subject Public Key	4096 bit RSA	
Subject Key Identifier	160 bit	
Authority Key Identifier	160 bit	
Basic Constraints	Critical, CA:FALSE	
Key Usage	Critical, Digital Signature	
Extended Key Usage	OCSP Signing	
OCSP No Check		
Signature Algorithm	sha256WithRSAEncryption	

Root Certificate:

Version	3	
Serial Number	160 bit	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	CN	ATSC3 Root-CA Silicondust
	O	Silicondust USA, Inc.
	C	US
Validity	100 years	
Subject	CN	ATSC3 Root-CA Silicondust
	O	Silicondust USA, Inc.
	C	US
Subject Public Key	4096 bit RSA	
Subject Key Identifier	160 bit	
Basic Constraints	Critical, CA:TRUE	
Key Usage	Critical, Certificate Sign, CRL Sign	
Signature Algorithm	sha256WithRSAEncryption	

Trademarks & Copyright