Certificate Expiration FAQ

1. **What has happened, and what is the background information?**

    a. On Dec 31, 2023, 00:00:00:00 GMT, the certificate chain (tdc-bur-user01) that Deluxe was using to sign CPLs within their global mastering toolset Cipher (v1) expired.
        i. This is not an abnormal situation, as certificates for Mastering systems expire anywhere from 5-15 years, depending on the system manufacturer's business requirements (there are no standards or requirements on certificate validity length).
        ii. Deluxe had already been prepping for this date by the creation of another certificate chain with their Cipher (v2) environment, which was deployed globally over the month of December 2023 to replace the original Mastering system and soon to be expiring signer certificate. During the month of December, many titles had CPLs created in both systems.

    b. Some playback servers deployed in exhibition validated this certificate at time of starting playback (after Dec 31, 2023, 00:00:00:00 GMT), and then failed due to the certificate within the CPL's signature being expired.
        i. This was based on a calculation of the `Not After` date/time stamp with the CPL's signature certificate chain when compared to `Current Date/Time` on the server (see 7 below for more details why this occurred).

    c. Deluxe re-created CPLs within Cipher (v2) with the new cert to get through the holiday week for first run content and limited repertory content, based on customer and exhibitor feedback as needed (see 11.a below for more details).
        i. This is not sustainable long term as per the amount of CPLs this could potential affect (see 2.b.ii below).

2. **What content was/is affected?**

    a. This ONLY affected SMPTE encrypted CPL content.
    b. This particular instance was limited to Deluxe created content.
        i. Deluxe has been using this specific certificate globally since late 2015 on all CPLs created in house in Cipher (v1).
        ii. It is estimated that approximately 450,000 CPLs have been created that match this certificate and the SMPTE format.
    c. *ALSO - Any other SMPTE encrypted content that was created and signed by an "expired" certificate, created by ANYONE*.

3. **Is there content created that is NOT affected?**

    a. It has been determined that this does not affect (on any certificate):
        i. IOP content.
        ii. Unencrypted content (regardless of IOP/SMPTE format).
    b. Other SMPTE content:
        i. Created by Deluxe on currently "non-expired" certificates.
        ii. Created by other vendors on currently "non-expired" certificates.

4. **Why is IOP and Unencrypted content not affected (as noted in 3.a above)?**

    a. Signature (and thereby signature certificates) is optional on both IOP and unencrypted CPLs and therefore ignored by validation steps (see 7 below) at playback time on servers.

5. What systems are affected?

a. The following playback systems determined to fail on playback due to this validation:
    i. Christie
        a. IMB-S2
        b. IMB-S3
        c. Dolby E3LH
        d. NOTE: This was only on the above systems that were not updated as per 6.a.ii below
    ii. GDC
        a. All GDC Digital Cinema server models updated with a DCI compliant firmware were affected.
    iii. Sony
        a. Media Block XCT-M10 (SRX-R515 and SRX-R815 projectors)
        b. LMT-300 (SRX-R320 projectors)
        c. LMT-200 (SRX-R220 projectors)
    iv. Dolby CP850 ONLY in dual KDM auditorium (used with IAB/ATMOS content)
        a. IMS3000
        b. This does not affect:
            i. Dolby CP850s in single KDM auditorium for IAB/ATMOS content
            ii. Dolby CP850s for non-IAB/ATMOS content
        c. Note: This only affects the playback of the IAB/ATMOS track. The rest of the content still plays as normal, with MainSound playing, if available, in some cases.

6. Wouldn't this have happened before?

a. Actually… This did recently occur in June of 2023 when another certificate used by both Deluxe and Disney expired.
    i. At that time, reports of issues were limited to only occurring on Christie servers (as noted in 5.a.i above), and there were no further reports of incidents.
    ii. As such, Christie issued a fix that was widely deployed around Oct 2023 (see 10.a below).
b. This has potentially occurred many times over the past years when other certificates for other Mastering systems have expired. It's assumed that this was not as widely noticed in prior instances, perhaps due to the prevalence of IOP content.

7. Are there more details on this validation step(s) that was failing?

a. At the time of playback, servers are required to validate the signature (which is required for SMPTE encrypted content).
    i. The rules for validation of the certificate within the CPL signature are defined as per SMPTE ST 430-2, section 6.2.
        a. Step (9) of this section states:
        If the validation context includes a desired time, check that the desired time is within the validity dates. Informative Note: In most cases the desired time is the current time, but a different time might be used to examine historical or future information. Implementations that do not need to know the current time in order to otherwise comply with their requirements typically will not include a desired time in the validation context and therefore will skip this step.
    ii. DCI DCSS version 1.4.3 (published version as of Dec 31, 2023) also stated in section 9.4.3.5 functions of the Security Manager:

        a. Step (4.c) stated:
           The CPL meets the two validation requirements defined in Section 5.2.1. of SMPTE 430-5 D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema.
    b. The ambiguity of mentioning `current time` in SMPTE ST 430-2 as "in most cases" was interpreted as the desired time to validate against, according to the affected server manufacturers. There is often room for interpretation in the standards and specifications such as this, but this was effectively invalidating any SMPTE encrypted CPLs with an expired certificate within the signature, which was not widely expected by the industry.

8. Is there a way to clarify this validation, and/or do we need to update standards?

a. DCI has issued a revision of the DCSS (version 1.4.4 published Jan 3, 2024) that updates step (4.c) of section 9.4.3.5 to:
   The CPL meets the two validation requirements defined in Section 5.2.1. of SMPTE 430-5 "D-Cinema Operations – Security Log Event Class and Constraints for D-Cinema" with the following caveat: When performing Step 9 of Section 6.2 in SMPTE ST 430-2, the desired time of the validation context shall be equal to the IssueDate field of the target CPL (and not the current time). This behavior permits the continued playback of a CPL after the expiration of its signing certificate, but ensures that the signing took place during the certificate's validity period.
b. SMPTE ST 430-2 should not need an update with the clarification added by DCI.
    i. This will likely be discussed more within SMPTE 27C Document Maintenance group at the next revision of ST 430-2.
c. This will likely be good enough clarification for both current and future implementations.

9. Why is this an issue, shouldn't CPLs "expire"?

a. Technical reasons aside, many content owners and vendors have never expected to have to recreate CPLs after a certain amount of time, and certainly never expected CPLs to "expire". There is little desire to recreate CPLs every 5-15 years for the same content. Most title databases within vendors and studios track versions by CPL UUID/CTT, as a fixed non-changing element.
    i. This is aside from usual CPL migration for standards updates, such as moving from IOP to SMPTE, and/or adding additional SMPTE CPL metadata, and/or new validation on the mastering side due to implementation issues.
b. Every DCP vendor has CPL signer certificates that will eventually expire. Some sooner than others, and many have already expired.
c. There are quite of number repertory titles that are constantly and frequently in the field, even more so since the pandemic. Much of that content has been mastered on mastering systems which have had certs expire *many years ago*.
d. No one disagrees that a CPL's certificate shouldn't be validated based on the time of creation (`IssueDate`), as clarified by DCI (as per 8.a above), but this would not "invalidate" a CPL. This would allow all repertory content already mastered to continue to play without incident in the future, as long as the certificate was valid at the time of the creation of the CPL.
e. The footprint of CPLs and affected systems has the potential to (and appears to have already) reach all territories and markets, this will only increase with time.

10. Are there fixes by the server manufacturers? What can exhibition do?

a. Christie
    i. There is already an update available (as per 6.a.ii above). All help desks should be aware of this.
        a. Download at: https://myftp.christiedigital.com/?u=YQpr&p=3PqT
        b. Software versions that resolve the issue:

i. IMB-S2: v1.8.11(4)
ii. IMB-S3: CineLife 2.7.1-12
iii. Dolby E3LH: CineLife 2.3.60-3

b. GDC
   i. Software versions that resolve the issue:
      - 8.01-build312
      - 9.0-build521
      - 10.0-build135
      - 17.3-build45
      - 17.5-build40
      - 19.0-build34
   ii. It is suggested to reach out to your integrator and/or the manufacturer as needed.
c. Sony
   i. Sony is aware and has been working on a potential software update for its servers
   ii. XCT-M10 media block software and release notes can be downloaded at: https://app.cimediacloud.com/r/xDNWuhwjMENB
   iii. LMT-300 media block software and release notes can be downloaded at: https://app.cimediacloud.com/r/dBkJwg4LCAhI
   iv. It is suggested to reach out to your integrator and/or the manufacturer as needed.
d. Dolby
   i. It is suggested to reach out to your integrator and/or the manufacturer as needed.
   ii. There is a software version available to address the issue:
      - CP850 SW v2.3.2.5 release notes: https://dolby.box.com/s/g7o3pczxg3zsxanjn0ymbbmy99b8iai7
      - CP850 SW v2.3.2.5 software: Contact Dolby for access to the software by emailing CinemaSupport@dolby.com

11. Are there any workarounds?

a. A new CPL may be generated with a currently valid certificate in the signature.
   i. This may either be done as Version File (VF) package of just CPL/PKL/AssetMap or full OV package with original MXF track files.
   ii. This DOES NOT require new MXF track files or a re-encode of the essence files (no "re-packaging" or "re-mastering").
   iii. This works on all systems currently affected.
   iv. This is not expected to be a long-term "fix", only to be done in some cases as needed until future software updates are published by server manufacturers.
b. FOR GDC ONLY:
   i. A new SMPTE KDM may be generated without `ContentAuthenticator`
      a. This will bypass the stoppage of playback during the additional signature certificate validation as noted in the ISDCF Doc 5 - Guideline for SMPTE KDMs and Certificates Behaviors (available at: https://files.isdcf.com/papers/ISDCF-Doc5-kdm-certs.pdf), item "CPL Signature" in section (3.2):
      - In the case of a KDM with the ContentAuthenticator element present, a failed CPL Signature failure shall always result in playback rejection. In such case, the certificates used in the CPL signing chain shall successfully pass the applicable validation rules identified in Annex A. Failure to pass identified certificate validation rules shall result in playback rejection as well.
      - In the case of a KDM without ContentAuthenticator, a CPL signature shall NOT result in playback rejection. It is recommended that a CPL signature failure be logged in such cases, while the playback shall NOT be forbidden because of this failure. In such case, the certificates used in the CPL signing chain do not have to

pass the applicable validation rules identified in Annex A. Failure to pass identified certificate validation rules shall NOT result in playback rejection.

ii. This has been vetted by GDC and verified by Deluxe. Special attention should be paid to the security concerns when using this option.
iii. This option *does not work* on Sony systems, presently.
iv. This option does not work with the Dolby CP850 using system software v2.3.2.3 or earlier. Instead, the software version referenced in 10.d.ii above should be installed.
v. This option has not been tested on Christie, as there is currently a fix available (see 10.a above), and this workaround is not needed.

c. FOR Sony:
    i. As an interim measure to support cinema operations, Sony is working with Deluxe and the studios to provide support for updating CPLs for certain content as necessary to enable playback on Sony projectors (as per 11.a.i above).

12. All this mentioning of certificates, are KDMs affected?

a. NO - All current validation of certificates within KDMs is *working as intended and expected*.
b. KDMs are meant to expire, as well as their certificates.
    i. Deluxe migrated their KDM certificate globally mid-2023, and recently migrated all KDMs that were on the “old” Cipher (v1) certificate, as per normal planning.
    ii. This is not the first mastering or KDM certificate that has expired, this is a common experience as most (if not all) vendors have had bulk KDM certificate migrations in the past.