DTLA CVP-2 Volume1 Specification

Hitachi Maxell, Ltd.

Intel Corporation

Panasonic Corporation

Sony Corporation

Toshiba Corporation

Revision 1.1

March 9, 2015

Preface

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Hitachi Maxell, Ltd., Intel, Panasonic, Sony, and Toshiba (collectively, the "5C") disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Some portions of this document, identified as "Draft" are in an intermediate draft form and are subject to change without notice. Adopters and other users of this Specification are cautioned these portions are preliminary, and that products based on it may not be interoperable with the final version or subsequent versions thereof.

Intellectual Property

Implementation of this specification requires a license from the Digital Transmission Licensing Administrator.

Contact Information

Feedback on this specification should be addressed to dtla-comment@dtcp.com.

The Digital Transmission Licensing Administrator can be contacted at dtla-manager@dtcp.com.

The URL for the Digital Transmission Licensing Administrator web site is: http://www.dtcp.com.

Printing History:

July 15, 2014	DTLA CVP-2 Volume 1 Specification Revision 1.0
July 22, 2014	DTLA CVP-2 Volume 1 Specification Revision 1.0

Table of Contents

Figures

Chapter 1 Introduction

1.1 Purpose and Scope

This specification details the keying material components that DTLA provides to support CVP-2 Authentication as defined in the DLNA guidlelines.

1.2 References

This specification shall be used in conjunction with the following publications. When the publications are superseded by an approved revision, the revision shall apply.

[DAUTHG] DLNA Guidelines, Part 7: Authentication, March 2014

[CVP2DPG] DLNA Guidelines Part 5: Device Profiles, March 2014

[RFC3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC5480] ECC Subject Public Key Information

[RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation (CRL) Profile

[X.690] ITU-T Rec. X.690 (11/2008) OSI networking and system aspects – Abstract Syntax notation (ASN.1), Series X: Data Networks, Open System Communications and Security

[X9.62-2005] Public Key Cryptography for the Financial Services Industry The Elliptic Curve Digital Signature Algorithm (ECDSA)

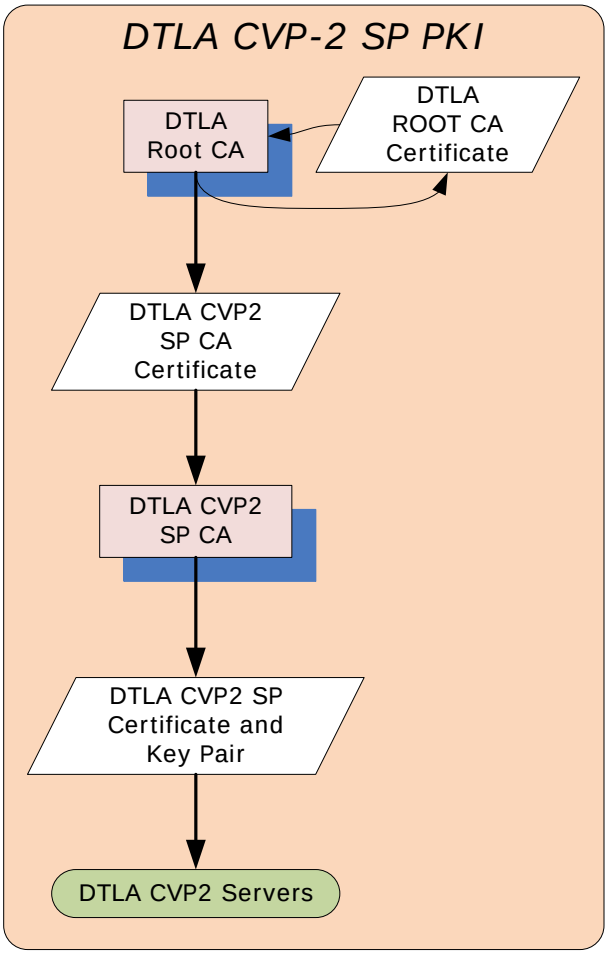
1.3 Abbreviations

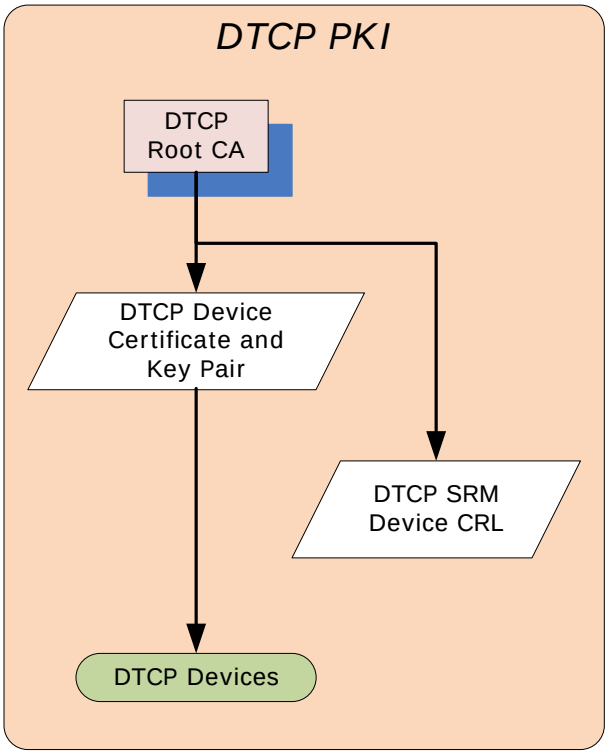
This chapter lists abbreviations and acronyms used throughout this document.

CA	Certificate Authority
CVP-2	Commercial Video Profile 2
PKI	Public Key Infrastructure
SP	Service Provider

1.4 Overview

The current DTCP PKI will be used to generate Device certificates with CVP-2 flag for use in authenticating a CVP-2 compliant client device with CVP-2 Server. The DTLA CVP-2 SP PKI will be used to generate certificates for CVP-2 servers. The DTLA CVP-2 SP PKI consists of DTLA Root CA and a DTLA CVP-2 Service Provider CA. The DTLA CVP-2 Service Provider CA will generate DTLA CVP-2 Service Provider certificates and corresponding private/public key pair.





Chapter 2 DTCP PKI

The section describes those elements of the DTCP specification that are needed to support DLNA CVP-2.

2.1 General

These cryptographic algorithms are based upon cryptographic schemes, primitives, and encoding methods described in IEEE 1363-2000.

An Elliptic Curve Cryptosystem (ECC) is used as the cryptographic basis for DH and DSA.

The definition field classifies ECC implementations. For this system, the definition field used is *GF(p)* where *p* is a large prime number greater than three. An elliptic curve *E* over the field *GF(p)*, where $p > 3$, is defined by the parameters *a* and *b* and the set of solutions (*x, y*) to the elliptic curve equation together with an extra point often called the point at infinity. The point at infinity is the identity element of the Abelian group, (*E,* +). The elliptic curve equation used is

$$y^2 = x^3 + ax + b \text{ where } 4a^3 + 27b^2 \neq 0,$$

Where *a, b, x, y,* are elements of *GF(p).* A point *P* on the elliptic curve consists of the x-coordinate and the y-coordinate of a solution to this equation, or the point at infinity, and is designated $P = (x_p, y_p)$.

For EC-DSA and EC-DH, a basepoint *G* on the elliptic curve is selected. All operations in the elliptic curve domain are calculated on an elliptic curve E defined over *GF(p)*. The public key Y^1 (a point on the elliptic curve) and private key Y^{-1} (a scalar value satisfying $0 < Y^{-1} < r$) for each entity satisfies the equation:

$$Y^1 = Y^{-1} G$$

In specifying the elliptic curve used:

The order of basepoint *G* will have a large prime factor.

E denotes the elliptic curve over the finite field GF(p) of p elements represented as integers modulo p. Elliptic curve points consist of the x-coordinate and y-coordinates, respectively; for an elliptic curve point $P = (x_P, y_P)$ which is not equal to the elliptic curve point at infinity.

	Description	**Size (bits)**
p	A prime number greater than 3 of finite field *GF(p)*	160
a*, *b	The coefficients of elliptic curve polynomial	160 each
G	The basepoint for the elliptic curve *E*	320
r	The order of basepoint *G*	160
L^{-1}	DTLA private key of EC-DSA key pair which is an integer in the range (*1*, *r–1*)	160
L^1	DTLA public key of EC-DSA key pair where $L^1 = L^{-1}G$	320

These parameters, with the exception of L^{-1}, are in Volume 2 of this specification.

2.2 DTCP CVP-2 Device Certificate

A device certificate is given to each compliant device *X* by the DTLA and is referred to as X_{CERT}. This certificate is stored in the compliant device and used during either the DTCP authentication process or the CVP-2 authentication process.

2.2.1 Baseline Format

The following Figure 1 shows the baseline device certificate format:

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Certificate Type				Format				Dev Gen				Reserved (zero)									C2	AL	AP	Device ID							
Device ID continued (Total 40 bits)																															
Device EC-DSA Public Key (320 bits)																															
DTLA EC-DSA signature of all preceeding fields (320 bits for c and followed by d value)																															

Figure 1 Baseline Device Certificate Format

Device certificates are comprised of the following Baseline Format fields:

- **Certificate Type** (4 bits). The only encoding which is currently defined is 0, which indicates the DTCP certificate. All other encodings are currently reserved.
- **Certificate Format** (4 bits). This field specifies the format for a specific type of certificate. Currently the following formats are defined:
    - **Format 1** = the Baseline Full Authentication device certificate format.
    - **Other encodings are currently reserved.**
- **Device Generation** (X_{SRMG}, 4 bits). This field indicates the non-volatile memory capacity and therefore the maximum generation of renewability messages that this device supports. The encoding 0 indicates that the device shall have a non-volatile memory capacity for storing First-Generation SRM. The encoding 1 indicates that the device shall have a non-volatile memory capacity for storing Second-Generation SRM.
- **Reserved** Field (9 bits). These bits are reserved for future definition and are currently defined to have a value of zero. For clarity, devices should not abort AKE if a Reserve bit has a value other than zero.
- **C2 flag** (1bit). The C2 flag is set to a value of one to indicate, when used in the CVP-2 authentication process, that the associated device is DLNA CVP-2 certified. The C2 flag has no meaning when a DTCP CVP-2 Device Certificate is used for the DTCP authentication process.
- **AL flag** (1 bit). Additional Localization flag. The AL flag is set to value of one to indicate that the associated device is capable of performing the additional localization test, otherwise shall be set to value of zero.
- **AP flag** (1 bit). Authentication Proxy flag. A device certificate with an AP flag value of one is used by a DTCP bus bridge device, which receives a content stream using a sink function and retransmits that stream to another bus using a source function[1]. The procedures for processing this field are specified in Appendix C of the DTCP Volume 1 Specification.
- The **device's ID** number (X_{ID}, 40 bits) assigned by the DTLA.
- The **EC-DSA public key** of the device (X^1, 320 bits)
- An **EC-DSA signature** from the DTLA of the components listed above (320 bits)

The overall size of a Baseline Format device certificate is 88 bytes.

[1] To maintain consistency with the previous version of this specification, the value of AP flag for a device with a common device certificate is set to one regardless of the DTCP bus bridge capability.

2.3 Elliptic Curve Digital Signature Algorithm (EC-DSA)

2.3.1 Signature

The following signature algorithm is based on the ECSSA digital signature scheme using the DLSP-DSA signature primitive and EMSA-SHA-1 encoding method defined in of IEEE 1363-2000.

Input:

- M = the data to be signed
- X^{-1} = the private key of the signing device (must be kept secret)
- p, a, b, G, and r = the elliptic curve parameters associated with X^{-1}

Output:

- $S_{X^{-1}}[M]$ = a 320-bit signature of the data, M, based on the private key, X^{-1}

Algorithm:

Step 1, Generate a random value, u, satisfying $0 < u < r$, using RNG_F. A new value for u is generated for every signature and shall be unpredictable to an adversary for every signature computation. Also, calculate the elliptic curve point, $V = uG$.

Step 2, Calculate $c = x_V \bmod r$ (the x-coordinate of V reduced modulo r). If $c = 0$, then go to **Step 1**.

Step 3, Calculate $f = [SHA\text{-}1(M)]_{msb\_bits\_in\_r}$. That is, calculate the SHA-1 hash of M and then take the most significant bits of the message digest that is the same number of bits as the size of r.

Step 4, Calculate $d = [u^{-1}(f + cX^{-1})] \bmod r$ (note that u^{-1} is the modular inverse of u mod r while X^{-1} is the private key of the signing device). If $d = 0$, then go to **Step 1**.

Step 5, Set first 160 bits of $S_{X^{-1}}[M]$ equal to the big endian representation of c, and the second 160 bits of $S_{X^{-1}}[M]$ equal to the big endian representation of d. ($S_{X^{-1}}[M] = c \,||\, d$)

2.3.2 Verification

The following verification algorithm is based on the ECSSA digital signature scheme using the DLVP-DSA signature primitive and EMSA-SHA-1 encoding method defined in of IEEE 1363-2000.

Input:

- $S_{X^{-1}}[M]$ = an alleged 320-bit signature (c || d) of the data, M, based on the private key, X^{-1}
- M = the data associated with the signature
- X^1 = the public key of the signing device
- p, a, b, G, and r = the elliptic curve parameters associated with X^{-1}

Output:

- "valid" or "invalid", indicating whether the alleged signature is determined to be valid or invalid, respectively

Algorithm:

Step 1, Set c equal to the first 160 bits of $S_{X^{-1}}[M]$ interpreted as in big endian representation, and d equal to the second 160 bits of $S_{X^{-1}}[M]$ interpreted as in big endian representation. If c is not in the range [1, r – 1] or d is not in the range [1, r – 1], then output "invalid" and stop.

Step 2, Calculate $f = [SHA\text{-}1(M)]_{msb\_bits\_in\_r}$. That is, calculate the SHA-1 hash of M and then take the most significant bits of the message digest that is the same number of bits as the size of r.

Step 3, Calculate $h = d^{-1} \bmod r$, $h_1 = (fh) \bmod r$, and $h_2 = (ch) \bmod r$.

Step 4, Calculate the elliptic curve point $P = (x_P, y_P) = h_1G + h_2X^1$. If P equals the elliptic curve point at infinity, then output "invalid" and stop.

Step 5, Calculate $c' = x_P \bmod r$. If $c' = c$, then output "valid"; otherwise, output "invalid."

Chapter 3 DTLA CVP-2 SP PKI

3.1 General X.509 Format

The structure of certificates is based on [RFC5280]. All Certificates SHALL be DER encoded [X.690]. All attributes of the issuer and subject fields SHALL be encoded as type UTF8String.

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  EXPLICIT Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3
     extensions      [3]  EXPLICIT Extensions OPTIONAL
                          -- If present, version MUST be v3
     }
```

Implementer notes:

As stated in [5280]; For signature calculation, the data that is to be signed is encoded using the ASN.1 distinguished encoding rules (DER) [X.690]. ASN.1 DER encoding is a tag, length, value encoding system for each element.

Excerpt of section 4.1.2.5 Validity of [RFC5280], CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.

3.2 DTLA Root CA Certificate format

Certificate field name	Value
Version	*v3* (integer value 2)
SerialNumber	Conforms to [RFC5280]
Signature	ecdsa-with-SHA256 (OID-1.2.840.10045.4.3.2) [RFC5480]
Issuer	Contains attributes: -countryName “US” -organizationName “Digital Transmission License Administrator ” -commonName “DTLA Root CA”
Validity	Expires 2045-12-31 (December 31, 2045)
Subject	Contains attributes: -countryName “US” -organizationName “Digital Transmission License Administrator ” -commonName “DTLA Root CA”
SubjectPublicKeyInfo	[RFC5480] algorithmIdentifier is id-ecPublicKey OID 1.2.840.10045.2.1 namedCurve NIST P-256 EC object identifier 1.2.840.10045.3.1.7 (RFC5480 secp256r1) subjectPublicKey carries DTLA Public EC256 ECPoint
IssuerUniqueID	Not used
SubjectUniqueID	Not used
BasicConstraints extension	Mandatory, critical. The Boolean cA field is set to TRUE. The pathLengthConstraint field is not used. [RFC5280]
CRLDistributionPoints extension	Not used
KeyUsage extension	Mandatory, critical. Only key usage bit *keyCertSign and cRLsign* is set.
AuthorityKeyIdentifier extension	Not used; Note that there is one exception;where a CA distributes its public key in the form of a "self-signed"certificate, the authority key identifier MAY be omitted.(4.2.1.1 of RFC5280)
SubjectKeyIdentifier extension	Mandatory, non-critical. The key identifier method (1) is used as defined in [RFC5480] (160-bit SHA-1 hash of the subjectPublicKey field, excluding the tag, length, and number of unused bits).
CertificatePolicies extension	Not used
ExtKeyUsage extension	Not used
Id-pkix-ocsp-nocheck extension	Not used
SignatureAlgorithmId	ecdsa-with-SHA256 (OID-1.2.840.10045.4.3.2) [RFC5480]
SignatureValue	Conforms to [RFC5280]

3.3 DTLA CVP-2 Service Provider CA Certificate format

Certificate field name	Value
Version	*v3* (integer value 2)
SerialNumber	Conforms to [RFC5280]
Signature	ecdsa-with-SHA256 (OID-1.2.840.10045.4.3.2) [RFC5480]
Issuer	Contains attributes: -countryName “US” -organizationName “Digital Transmission License Administrator ” -commonName “DTLA Root CA”
Validity	Expires 2045-12-31 (December 31, 2045) but no later than the DTLA Root CA certificate
Subject	Contains attributes: -countryName “US” -organizationName “Digital Transmission License Administrator ” -commonName “DTLA CVP-2 SP CA”
SubjectPublicKeyInfo	[RFC5480] algorithmIdentifier is id-ecPublicKey OID 1.2.840.10045.2.1 namedCurve NIST P-256 EC object identifier 1.2.840.10045.3.1.7 (RFC5480 secp256r1) subjectPublicKey carries DTLA Public EC256 ECPoint
IssuerUniqueID	Not used
SubjectUniqueID	Not used
BasicConstraints extension	Mandatory, critical. The Boolean cA field is set to TRUE. The pathLengthConstraint field is not used. [RFC5280]
CRLDistributionPoints extension	Not used
KeyUsage extension	Mandatory, critical. Only key usage bit *keyCertSign and cRLsign* is set.
AuthorityKeyIdentifier extension	Mandatory, non-critical. This extension contains only the *keyIdentifier* field that has the same value as the corresponding DTLA Root CA Certificate’s subjectKeyIdentiffier extension value.
SubjectKeyIdentifier extension	Mandatory, non-critical. The key identifier method (1) is used as defined in [RFC5280] (160-bit SHA-1 hash of the subjectPublicKey field, excluding the tag, length, and number of unused bits).
CertificatePolicies extension	Not used
ExtKeyUsage extension	Not used
Id-pkix-ocsp-nocheck extension	Not used
SignatureAlgorithmId	ecdsa-with-SHA256 (OID-1.2.840.10045.4.3.2) [RFC5480]
SignatureValue	Conforms to [RFC5280]

3.4 DTLA CVP-2 Service Provider certificate Format

The CVP-2 Service Provider certificate is given to each DLNA CVP-2 compliant server. This certificate is stored in the compliant device and used during the CVP-2 authentication process. DTLA CVP-2 SP CA will generate the private/public key pair and corresponding DTLA CVP-2 Service Provider certificate.

Certificate field name	Value
Version	*v3* (integer value 2)
SerialNumber	Conforms to [RFC5280]
Signature	ecdsa-with-SHA256 (OID-1.2.840.10045.4.3.2) [RFC5480]
Issuer	Contains attributes: -countryName “US” -organizationName “Digital Transmission License Administrator ” -commonName “DTLA CVP-2 SP CA”
Validity	Expires five (5) years from the issuance date, but no later than the DTLA CVP-2 Service Provider CA certificate
Subject	Contains attributes: -countryName “XX” (2 characters, in accordance with ISO 3166) -organizationName (e.g. “Company Name”) DTLA confirm uniqueness -organizationalUnit (provided by requestor) -commonName (provided by requestor FullyQualifiedDomainName FQDN) Max length is 64 characters for fields except countryName
SubjectPublicKeyInfo	[RFC5480] algorithmIdentifier is id-ecPublicKey OID 1.2.840.10045.2.1 namedCurve NIST P-256 EC object identifier 1.2.840.10045.3.1.7 (RFC5480 secp256r1) subjectPublicKey carries DTLA Public EC256 ECPoint
IssuerUniqueID	Not used
SubjectUniqueID	Not used
BasicConstraints extension	Not used
CRLDistributionPoints extension	Not used
KeyUsage extension	Mandatory, critical. Only key usage bit *digitalSignature and keyEncipherment* are set.
AuthorityKeyIdentifier extension	Mandatory, non-critical. The extension contains only the keyIdentifier field that has the same value as the DTLA CVP-2 SP CA Certificate’s subjectKeyIdentifier extension value.
SubjectKeyIdentifier extension	Not used
CertificatePolicies extension	Not used
ExtKeyUsage extension	Mandatory, non-critical. The extension contains only the CVP-2-kp-server object identifier 2.16.840.1.114508.2
SubjectAltName extension	Mandatory, non-critical. Same value as CommonName field contains FQDN
Id-pkix-ocsp-nocheck extension	Not used
SignatureAlgorithmId	ecdsa-with-SHA256 (OID-1.2.840.10045.4.3.2) [RFC5480]
SignatureValue	Conforms to [RFC5280]