AACS Key Order Form

ORDER FORM TO AACS KEY GENERATION FACILITY ("KGF")

For all orders, Licensee is advised to confirm eligibility under the applicable Approved License to order the AACS Keys requested via this Key Order Form.

Device Key & Sequence Key ("DKSK") Order

- Eligible Adopter Sub-categories: Player Mfr., Recorder Mfr., Component Mfr.
- Examples of eligible Licensees: manufacturers of devices such as optical media recorders/players, manufacturers of components such as integrated circuits; online service providers.
- Unique Device Key Orders: Maximum two hundred thousand (200,000) keys; minimum one thousand (1,000) keys; increments of one thousand (1,000) keys.
- Shared Device Key Orders: Maximum ten (10) keys; minimum one (1) key. **All Shared Device Keys in a single order must have the same expiration date.**
- Shared Device Key "First Orders" contain both Device Key Sets and Sequence Key Sets. Shared Device Key "Update Orders" contain only Device Key Sets.
- No more than one "First Order" Key Set may be integrated into Licensed Products that utilize the same technology to maintain the secrecy of the Key Sets (*i.e.*, if placing a Shared Device Key order of more than one (1) key, then each of the Key Sets must be used in either different Licensed Products models or in Licensed Products using substantially different key protection technologies).

Drive/Host Authentication Certificate ("DHAC") Order

- Eligible Adopter Sub-categories: Player Mfr., Recorder Mfr., Component Mfr., Drive Mfr.
- Examples of eligible Licensees: manufacturers of devices such as optical media drives (read-only or read/write or players that perform host-drive authentication).
- Host Proactive Renewal Certificate Orders: maximum ten (10) certificates; minimum one (1) certificate.
- Host Enhanced Robustness Certificate Orders: maximum one million (1,000,000) certificates; minimum one thousand (1,000) certificates; increments of one thousand (1,000) certificates.
- Drive Certificate Orders: maximum one million (1,000,000) certificates; minimum one thousand (1,000) certificates; increments of one thousand (1,000) certificates.

MCS Authentication Certificate and MCS Private Key ("DHAC") Order

- Eligible Adopter category: Online Service Provider
- MCS Authentication Certificate Orders (including the MCS Private Key): maximum three (3) certificates; minimum one (1) certificate; increments of one (1) certificate.

Media Key Block /Sequence Key Block ("MSKB") Order

- Eligible Adopter Sub-categories: Licensed Content Producer, Recorder Mfr., Component Mfr, Media Mfr.
- Content Participants/Providers are eligible to order MKBs/SKBs
- Examples of eligible licensees: audio-visual content providers, optical disc media replicators, manufacturers of blank optical disc media.
- MKB orders and Partial MKB orders are not required for recordable media using a format for which MKBs or Partial MKBs are not required to be pre-recorded. Recordable MKB Orders may be placed by the device manufacturer where the latest Type 3 MKB is required to be installed at manufacturing time.

Continued next page

- MKB Orders: maximum MKBs per order five hundred (500); minimum one (1) MKB per order.
- For the case of pre-recorded media each entry also includes the corresponding SKBs and Type 3 and Type 4 MKBs.
- For the case of recordable media each entry only includes one Type 3 MKB.

Content Certificate ("CERT") Order

- Eligible Adopter Sub-categories: Licensed Content Producer
- Content Participants/Providers are eligible to order Content Certificates
- Examples of eligible Licensees: providers of audio-visual content and Licensed Content Producers.
- Content Certificate Orders: maximum number of signings per order to include, when submitted together, one Content Certificate per disc layer and one Prepared Video Certificate.

Content Certificate for CSS ("CSSC") Order

- Eligible Adopter Sub-categories: Licensed Content Producer
- Content Participants/Providers are eligible to order Content Certificates
- Examples of eligible Licensees: providers of audio-visual content and Licensed Content Producers.
- Content Certificate for CSS Orders: maximum number of signings per order -, one Content Certificate

ORDER ID:_____**DKSK**

AACS Device Key & Sequence Key Order

Name of Adopter/Content Participant/Content Provider ("Licensee")

_____

Licensee ID (4 digits): _____ _____ _____ _____

PGP Fingerprint: _____

SELECT ONE

- ☐ **Blu-ray/HD DVD Class I**
- ☐ ~~**Blu-ray/HD DVD Class II**~~
- ☐ **CBHD (China) order**

Bill-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Ship-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Order Type Type (check ONE): ☐ Key Conversion Data (**KCD**) ☐ Non-KCD (**NONKCD**)

Key Order	**Unit(s) Ordered**	**Amount**
Set(s) of Device Key or Sequence Key Pairs (Choose one, Type A or C)		
1. **Unique Device Keys** - "Enhanced Robustness"	**(Max. 200,000)**	x **US$ 0.08/pair** = US$ _____
2. **Shared Device Keys** - "Proactive Renewal" Order Type: _____ First/Initial Order (**FO**) or Reorder (**UO**)		**Check "☑" desired tier (one only):** ☐ **US$ 3,000.00** for up to 100K copies per year ☐ **US$ 10,000.00** for up to 1M copies per year ☐ **US$ 25,000.00** for up to 10M copies per year ☐ **US$ 50,000.00** over 10M per year = US$ _____

Order Fulfillment Fee: US$ 500.00

Acknowledged and agreed by Licensee:

By: _____ Title: _____

Name: _____ Order Date:_____

For AACS LA Use Only:

Completed KOF Received (date/initial**):** _____ **Fee Payment Received (**date/initial**):** _____

Order Sent to KGF (date/initial**):** _____ **Order Sent to Licensee (**date/initial**):** _____

KGF Output Filename: _____

NOTES

ORDER ID:_____DHAC

AACS Drive/Host Authentication Certificate Order

Name of Adopter/Content Participant/Content Provider ("Licensee")

_____ **NOTE: Currently Not Applicable to CBHD**

Licensee ID (4 digits): _____ _____ _____ _____

PGP Fingerprint: _____

Bill-to Address:		**Ship-to Address:**	
Contact Name:	_____	Contact Name:	_____
Address:	_____	Address:	_____
	_____		_____
	_____		_____
Telephone:	_____	Telephone:	_____
Email:	_____	Email:	_____

Certificate Type (check ONE): ☐ Drive (**D**) ☐ Host Proactive Renewal (**HPR**) ☐ Host Enhanced Robustness (**HER**)
☐ **MCS Authentication Certificate**

Bus Encryption (check ONE): ☐ Enabled ☐ NOT Enabled

Certificate Order	**Unit(s) Ordered**	**Amount**
Drive Certificate	**(Max. 1,000,000)**	x US$ 0.02/pair = US$ _____
Host Enhanced RobustnessCertificate ☐ Set "Data Key Settable" (DKS) flag	**(Max. 1,000,000)**	x US$ 0.02/pair = US$ _____
Host Proactive Renewal Certificate ☐ Set "Data Key Settable" (DKS) flag		**Check "☑" desired tier (one only):** ☐ **US$ 500.00** for up to 100K copies per year ☐ **US$ 2,000.00** for up to 1M copies per year ☐ **US$ 5,000.00** for up to 10M copies per year ☐ **US$ 10,000.00** over 10M per year = US$ _____
MCS Authentication Certificate including Private Key		**x US$ 500 per certificate = US$**_____

Order Fulfillment Fee: US$ 500.00

Acknowledged and agreed by Licensee:

By: _____ Title: _____

Name: _____ Order Date:_____

For AACS LA Use Only:

Completed KOF Received (date/initial**):** _____ **Fee Payment Received (**date/initial**):** _____

Order Sent to KGF (date/initial**):** _____ **Order Sent to Licensee (**date/initial**):** _____

KGF Output Filename: _____

NOTES

ORDER ID:_____MSKB

AACS Media Key Block /Sequence Key Block Order

Name of Adopter/Content Participant/Content Provider ("Licensee")

_____

Licensee ID (4 digits): _____ _____ _____ _____

PGP Fingerprint: _____

SELECT ONE

- ☐ **Blu-ray/HD DVD Class I**
- ☐ ~~**Blu-ray/HD DVD Class II**~~
- ☐ **CBHD (China) order**

Bill-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Ship-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Media Type (check ONE): ☐ Pre-recorded (**P**) ☐ Recordable (**R**)

MKB Order	Unit(s) Ordered	Amount
Set(s) of MKB/SKB (*i.e.*, 1 to 500)		
Recordable (estimated usage – devices/discs)		x US$ 0.02/disc or device = US$_____

Note: Please refer to Exhibit B of the AACS license agreement for instructions regarding reporting and payment for usage of MKBs/SKBs.

Order Fulfillment Fee: US$ 500.00

Acknowledged and agreed by Licensee:

By: _____ Title: _____

Name: _____ Order Date:_____

For AACS LA Use Only:

Completed KOF Received (date/initial**):** _____ **Fee Payment Received (**date/initial**):** _____

Order Sent to KGF (date/initial**):** _____ **Order Sent to Licensee (**date/initial**):** _____

KGF Output Filename: _____

NOTES

ORDER ID:_____CERT

AACS Content Certificate Order

Name of Adopter/Content Participant/Content Provider ("Licensee")

_____

Licensee ID (4 digits): _____ _____ _____ _____

PGP Fingerprint: _____

Bill-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Ship-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Note: Order will be shipped via email to this address.

Content Participant/Provider Licensee ID: ___ ___ ___ ___

Content Signing	Disc Type	Number of Disc Layers	Amount
Content Certificate	**Blu-ray HD DVD CBHD** (circle one)	**1 2** (circle one)	**US$ 0.04 per disc, unless volume pricing plan selected**

Certificate 1 filename (or "N/A"): _____

Certificate 2 filename (or "N/A"): _____

Prepared Video Certificate filename (or "N/A") _____

Note: HD DVD and CBHD discs use only one Content Certificate on a multi-layer disc

Note: Please refer to Exhibit B of the AACS license agreement for instructions regarding reporting and payment for usage of Content Certificates.

Order Fulfillment Fee: US$ 500.00

Email shipping is provided at no charge.

Physical shipping: US$ 200.00 additional fee (☐ check here if physical shipping requested)

Acknowledged and agreed by Licensee:

By: _____ Title: _____

Name: _____ Order Date:_____

For AACS LA Use Only:

Completed KOF Received (date/initial**):** _____ **Fee Payment Received (**date/initial**):** _____

Order Sent to KGF (date/initial**):** _____ **Order Sent to Licensee (**date/initial**):** _____

KGF Output Filename: _____

NOTES

ORDER ID:_____**CSSC**

AACS Content Certificate for CSS Order

Name of Adopter/Content Participant/Content Provider ("Licensee")

_____

Licensee ID (4 digits): _____ _____ _____ _____

PGP Fingerprint: _____

Bill-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Ship-to Address:

Contact Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

Note: Order will be shipped via email to this address.

Content Participant/Provider Licensee ID: ___ ___ ___ ___

Content Signing	Amount
Content Certificate for CSS	**US$ 500.00**

Certificate filename: _____

Order Fulfillment Fee: US$ 500.00

Email shipping is provided at no charge.

Physical shipping: US$ 200.00 additional fee (☐ check here if physical shipping requested)

Acknowledged and agreed by Licensee:

By: _____ Title: _____

Name: _____ Order Date: _____

For AACS LA Use Only:

Completed KOF Received (date/initial**):** _____ **Fee Payment Received (**date/initial**):** _____

Order Sent to KGF (date/initial**):** _____ **Order Sent to Licensee (**date/initial**):** _____

KGF Output Filename: _____

NOTES

Terms and Conditions of Key Order

The capitalized terms not herein defined shall have the respective meanings provided in the Interim Adopter Agreement, Interim Content Participant Agreement or Interim Content Provider Agreement, as may be applicable.

1. Order and payment: Order and payment shall be made pursuant to the Adopter Agreement or Content Participant/Provider Agreement, as may be applicable.
2. Delivery: Orders will be processed promptly upon receipt, in the order received, and upon confirmation of order eligibility. No order will be processed for which the Ordering Entity is not an Adopter or Content Participant or Content Provider in good standing with all applicable Annual Administrative Fees paid and no other outstanding fees unpaid. No order is considered to have been received by AACS LA until such time as the Key Order Form is complete and payment of all applicable Key Fees has been received.
3. Shipment: Default shipping varies by key order type. Other shipping options may be available at an extra cost. Please note that shipping time does not change the time required to process and generate an order.
4. Force Majeure: AACS LA shall not be considered in default or be liable for any delay or failure to perform any provisions of this KOF or Adopter Agreement, Content Participant Agreement or Content Provider Agreement if such delay or failure arises directly or indirectly out of an act of nature, an act of public enemy, freight embargoes, electrical outage, strikes, quarantine restrictions, unusually severe weather conditions, insurrection, riot, earthquakes or such other causes beyond the control of AACS LA or its agents (including but not limited to the License Administrator and the KGF Host).

Contact Information

AACS License Administrator

AACS LA, LLC
c/o AACS Administration
3855 SW 153rd Drive
Beaverton, Oregon 97006 USA
Tel.: 503-619-0863
Fax: 503-644-6708
Email: admin@aacsla.com

AACS Bank Account/Wire Transfer Information

Bank of America
12280 S.W. Canyon Road
Beaverton, Oregon 97005 USA

Checking acct. no.	0045 6048 4887
Checking acct. name	Advanced Access Content System (AACS)
ABA routing no.	026 0095 93
ACH/Direct Dep. no.	323 070 380
SWIFT ID	BOFAUS3N

APPENDIX A - Order Delivery Format

1. Order delivery format

Orders are delivered in a binary file. The file comprises a header, an order-type specific header, one or more order entries, and an order signature. Each order file contains data for one order type: device keys and sequence keys, or media key blocks and sequence key blocks, or signed content certificates, or drive/host/MCS authentication certificates. Each entry contains order data and a SHA-1 integrity check value. The order signature authenticates the headers and all of the order entries using the $AACS\_LA_{priv}$ key.

1.1. Header

Each order file begins with a header that identifies the type of order, its size, the licensee it is for, and the characteristics of the data. All numerical values are in big-endian order.

<table>
<tr><th>Field Name</th><th>Size (bits)</th><th colspan="3">Description</th></tr>
<tr><td>Version</td><td>16</td><td>0x0002</td><td colspan="2">If the order is a device order for Class II devices, or
the order is a media order for pre-recorded media and the order includes media key delta values and unified MKBs (MKB Type 10), or
the order is a Content Signing Order containing either a Prepared Video Content Certificate or a CSS Content Certificate, or
the order is a Drive/Host Certificate order with a certificate that has Bus Encryption capable or Data Key Settable set, or
the order is for a Managed Copy Server private keys and public key certificates.</td></tr>
<tr><td></td><td></td><td>0x0001</td><td colspan="2">If the order is not one of the above.</td></tr>
<tr><td>Reserved</td><td>16</td><td colspan="3">Reserved for future use.</td></tr>
<tr><td>Order Generation TimeStamp</td><td>64</td><td colspan="3">Date the order was generated, as an unsigned 64-bit integer representing the number of milliseconds since January 1, 1970, 00:00:00 GMT. This date is unique for each order.

To prevent possible replay attacks, recipient licensee is required to verify the order generation date matches the actual order timeframe.</td></tr>
<tr><td>Licensee_ID</td><td>16</td><td colspan="3">ID of Licensee requesting order.

0x0000 TEST -- Usage is reserved by AACS</td></tr>
<tr><td>Order_Format</td><td>16</td><td colspan="3">The Order_Format field may take the following values:</td></tr>
<tr><td></td><td></td><td>Encoding</td><td colspan="2">Definition</td></tr>
<tr><td></td><td></td><td>0x001*</td><td colspan="2">DKSK – Device Order (Class I – device and sequence key sets)</td></tr>
<tr><td></td><td></td><td></td><td>0x0010</td><td>Type A+KCD [HW ER]</td></tr>
<tr><td></td><td></td><td></td><td>0x0011</td><td>Type A+NONKCD [SW ER]</td></tr>
<tr><td></td><td></td><td></td><td>0x0012</td><td>Type C+KCD First Order [HW PR FO]</td></tr>
<tr><td></td><td></td><td></td><td>0x0013</td><td>Type C+NONKCD, First Order [SW PR FO]</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">DKSK – Device Order (Class I update orders – no sequence keys)</td></tr>
<tr><td></td><td></td><td></td><td>0x0016</td><td>Type C+KCD, update order [HW PR UO]</td></tr>
<tr><td></td><td></td><td></td><td>0x0017</td><td>Type C+NONKCD, update order [SW PR UO]</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">DKSK – Device Order (Class II – no sequence keys)</td></tr>
<tr><td></td><td></td><td></td><td>0x0018</td><td>Type A+KCD Class II [HW ER II]</td></tr>
<tr><td></td><td></td><td></td><td>0x0019</td><td>Type A+NONKCD, Class II [SW ER II]</td></tr>
<tr><td></td><td></td><td></td><td>0x001A</td><td>Type C+KCD, Class II [HW PR II]</td></tr>
</table>

			0x001B	Type C+NONKCD, Class II [SW PR II]
		0x002*	MSKB – Media Order (MKBs and SKBs/uMKBs)	
			0x0020	Pre-recorded media.
			0x0021	Recordable media.
		0x003*	CERT – Content Signing.	
			0x0030	Content Certificate Signing
			0x0031	Prepared Video Content Certificate Signing
			0x0032	CSS Content Certificate Signing
		0x004*	DHAC – Drive/Host Authentication Certificates.	
			0x0040	Drive keys and certificates.
			0x0041	Host keys and certificates, Enhanced Robustness
			0x0042	Host keys and certificates, Proactive Renewal
			0x0048	Drive keys and certificates - Bus Encryption capable
			0x004C	Host keys and certificates, Enhanced Robustness, - Bus Encryption capable
			0x004D	Host keys and certificates, Enhanced Robustness, - Bus Encryption capable, Data Key Settable
			0x004E	Host keys and certificates, Proactive Renewal, - Bus Encryption capable
			0x004F	Host keys and certificates, Proactive Renewal, - Bus Encryption capable, Data Key Settable
		0x0050	N/A – originally Host Revocation List order from Drive/Host KGF	
		0x0060	MCSC – Managed Copy Server keys and certificates	
Order_Size	32	Number of entries contained in the order.		
Order_Entry_Size	32	Size in bytes of a single entry in the order.		

This header is immediately followed by information specific to each type of order.

1.2. Device Order

A Device Order consists of the order header mentioned above, a Device Order header and the data for each order entry (which here represents the data for a particular device), and the end section.

Device Order header

Field Name	Size (bits)	Description
Reserved	16	Fixed to 0x0001
Device_Keys	16	Number of device keys in a device key set. Set to 253.
Sequence_Keys	16	Number of sequence keys in a device key set. This is the number of columns in the sequence keys matrix. Set to 256 for order type 0x0010-0x0013. Set to 0 for order types 0x0016-0x0017 and 0x0018-0x001B
Reserved	16	Reserved for future use

Device Order entry

Field Name	Size (bits)	Description
Device_node	32	Bits [31…1] (where bit[0] is the lsb) represents the path from the root to a leaf in a binary tree. This leaf is the device node.
$Umask_i$, $UVnumber_i$	(8 + 32) * Device_Keys	The $Umask_i$, $UVnumber_i$ identify the subset-difference that the i^{th} device key is associated with. The mask for u is specified in the first byte, as the number of low-order zero bits in the mask. The last 4 bytes are the uv number, most significant byte first.
K_{d_i}	128 * Device_Keys	The device keys are in the same order as their $Umask_i$ and $UVNumber_i$.
$Column_i$, Row_i	(16 + 16) * Sequence_Keys	The column index and row index of the i^{th} Sequence Key: $0 \leq Column_i <$ Sequence_Keys $0 \leq Row_i <$ rows in sequence keys matrix This field is not present if the number of sequence keys is set to zero in the device order header.
K_{s_i}	64 * Sequence_Keys	The sequence keys, in the same order as the row and column indices. This field is not present if the number of sequence keys is set to zero in the device order header.
Seed	160	Random value
Integrity_Hash	160	SHA-1 hash of the preceding fields associated with Order Format 1. Please note that there will be an Integrity_Hash for the keys and other values associated with each device in the package.

1.3. Media Order

A Media Order consists of the order header mentioned above, a media order header, and the data for each order entry (which here represents the data for a particular MKB/SKB/uMKB set), and the end section.

Media Order header – Version 1 order files

Version 1 media order files contain a single MKB type 3 in each entry, if the order is for recordable media. If the order is for pre-recorded media, each entry contains an MKB type 3, an MKB type 4, and a set of SKBs. This header describes the contents.

Field Name	Size (bits)	Description
Reserved	16	Fixed to 0x0001
MKB_size	32	Size (in byes) of the MKBs type 3 and 4 contained in this order. All MKBs of the same type included in an order will always have the same size. This value is valid for all MKBs type 3 and type 4 included in the order.
SKB_size	32	Size (in byes) of the SKB portion of each entry contained in this order. This is the combined size of all the sets of SKB size, SKB data, and Media Key Variant values in each entry. This value is set to zero for recordable media orders.
SKB_rows	16	Number of rows on each SKB Calculate Variant Data and Conditionally Calculate Variant Data record. This is the number of rows in the sequence keys matrix. This value is set to 16384.
SKB_Max_Variants	16	Maximum number of variants associated with an SKB in each title in a prepared title sequence. This value is set to 1024.
SKB_count	8	Number of SKB variants per SKB in each order. If this value is set to zero (i.e. an order with no SKBs), the fields “SKB_size”, “SKB_rows” and “Max_Variants” should be ignored. This value is set to zero for recordable media orders and to 6 for pre-recorded media orders.
Reserved	8	Future use.

The size of an MKB can vary from order to order. For example, if a device(s) has been revoked in the time between orders, the MKB in new order will have a different size. However, at the time of cutting an order, all the MKBs generated for such order will have the same size independent of the MKB type.

Media Order header – Version 2 order files

Version 2 media order files contain entries for pre-recorded media. The entries include a Media Key Delta value and a set of Unified MKBs.

Field Name	Size (bits)	Description
Reserved	16	Fixed to 0x0001
MKB_size	32	Size (in byes) of the MKBs type 3 and 4 contained in this order. All MKBs of the same type included in an order will always have the same size. This value is valid for all MKBs type 3 and type 4 included in the order.
SKB_size	32	Size (in byes) of the SKB portion of each entry contained in this order. This is the combined size of all the sets of SKB size, SKB data, and Media Key Variant values in each entry. This value is set to zero for recordable media orders.
SKB_rows	16	Number of rows on each SKB Calculate Variant Data and Conditionally Calculate Variant Data record. This is the number of rows in the sequence keys matrix. This value is set to 16384.
SKB_Max_Variants	16	Maximum number of variants associated with an SKB in each title in a prepared title sequence. This value is set to 1024.
SKB_count	8	Number of SKB variants per SKB in each order. If this value is set to zero (i.e. an order with no SKBs), the fields "SKB_size", "SKB_rows" and "Max_Variants" should be ignored. This value is set to zero for recordable media orders and to 6 for pre-recorded media orders.
Reserved	8	Future use.
UMKB_size	32	Size (in byes) of the uMKB portion of each entry contained in this order. This is the combined size of all the sets of uMKB size, uMKB data, and Media Key Variant values in each entry. This value is set to zero for recordable media orders.
UMKB_Max_Variants	16	Maximum number of variants associated with a uMKB in each title in a prepared title sequence. This value is set to 1024.
UMKB_count	8	Number of uMKB variants per uMKB in each order. If this value is set to zero (i.e. an order with no uMKBs), the fields "UMKB_size" and "UMKB_Max_Variants" should be ignored. This value is set to zero for recordable media orders and to 6 for pre-recorded media orders.
Reserved	8	Future use.

Pre-recorded media order entry (Version=0x0001)

When the order type is 0x20, and the order version is 0x0001, the format of each order entry is the following:

Field Name	Size (bits)	Description
MKB type 3	32*n* (MKB_size)	Media Key Block type 3. To be placed in pre-recorded disc for recorders to update their default MKB.
MKB type 4	32*n* (MKB_size)	Media Key Block for pre-recorded media.
K_m	128	Media Key encoded in the MKB present in the previous field
K_{CD}	128	The key conversion data. The content preparer places the key conversion value on the media. A zero value means that the MKB does not contain any entries that require the key conversion data.
SKB_0 size	32	Size of SKB_0 in the next field.
SKB_0	32*n* (SKB_0 size)	1st Sequence Key Block associated with the MKB type 4 in this entry
$Media\_Key\_Variant_{0,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the 1st SKB. Media Key Variants are provided in ascending order
SKB_1 size	32	Size of SKB_1 in the next field
SKB_1	32*n* (SKB_1 size)	2nd Sequence Key Block associated with the MKB type 4 in this entry
$Media\_Key\_Variant_{1,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the 2nd SKB. Media Key Variants are provided in ascending order
:		
SKB_n size	32	Size of SKB_n in the next field (n = Num_Variant_Sets - 1).
SKB_n	32*n* (SKB_n size)	Last Sequence Key Block associated with the MKB type 4 in this entry
$Media\_Key\_Variant_{n,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the last SKB. Media Key Variants are provided in ascending order
Integrity_Hash	160	SHA-1 hash of all the preceding fields on this order entry. Please note that there will be an Integrity_Hash for each entry.

Pre-recorded media order entry (Version=0x0002)

When the order type is 0x20, and the order version is 0x0002, the format of each order entry is the following:

Field Name	Size (bits)	Description
MKB type 3	32*n* (MKB_size)	Media Key Block type 3. To be placed in pre-recorded disc for recorders to update their default MKB.
MKB type 4	32*n* (MKB_size)	Media Key Block for pre-recorded media.
K_m	128	Media Key encoded in the MKB present in the previous field
K_{CD}	128	The key conversion data. The content preparer places the key conversion value on the media. A zero value means that the MKB does not contain any entries that require the key conversion data.
K_m Delta	128	Media Key Delta – bit-by-bit difference between the media key encoded in the MKB type 3 and the media key encoded in the MKB type 4. This ones complement difference is the exclusive OR of the two media keys.
SKB_0 size	32	Size of SKB_0 in the next field.
SKB_0	32*n* (SKB_0 size)	1st Sequence Key Block associated with the MKB type 4 in this entry
$Media\_Key\_Variant_{0,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the 1st SKB. Media Key Variants are provided in ascending order
SKB_1 size	32	Size of SKB_1 in the next field
SKB_1	32*n* (SKB_1 size)	2nd Sequence Key Block associated with the MKB type 4 in this entry
MKB_1 size	32	Size of MKB Type 10 in the next field.
MKB_1	32*n* (MKB_1 size)	2nd MKB type 10 associated with the MKB type 4 in this entry.
$Media\_Key\_Variant_{1,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the 2nd SKB. Media Key Variants are provided in ascending order
:	:	:
SKB_n size	32	Size of SKB_n in the next field (n = Num_Variant_Sets - 1).
SKB_n	32*n* (SKB_n size)	Last Sequence Key Block associated with the MKB type 4 in this entry
$Media\_Key\_Variant_{n,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the last SKB. Media Key Variants are provided in ascending order
MKB_0 size	32	Size of MKB Type 10 in the next field.
$MKB\_Type\_10_0$	32*n* (MKB_0 size)	1st MKB type 10 associated with the MKB type 4 in this entry.
$Media\_Key\_Variant_{0,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the 1st SKB. Media Key Variants are provided in ascending order
MKB_1 size	32	Size of MKB Type 10 in the next field.
MKB_1	32*n* (MKB_1 size)	2nd MKB type 10 associated with the MKB type 4 in this entry.
$Media\_Key\_Variant_{1,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the 2nd SKB. Media Key Variants are provided in ascending order
:	:	:
MKB_n size	32	Size of MKB Type 10 in the next field.
$MKB\_Type\_10_n$	32*n* (MKB_n size)	Last MKB type 10 associated with the MKB type 4 in this entry.
$Media\_Key\_Variant_{n,k}$	128 * Max_Variants	Media Key Variant values resulting from processing the last SKB. Media Key Variants are provided in ascending order
Integrity_Hash	160	SHA-1 hash of all the preceding fields on this order entry. Please note that there will be an Integrity_Hash for each entry.

Recordable media order entry

When the order type is 0x21, the format of each order entry is the following:

Field Name	Size (bits)	Description
MKB type 3	32*n* (MKB_size)	Media Key Block for recordable media.
Integrity_Hash	160	SHA-1 hash of all the preceding fields on this order entry. Please note that there will be an Integrity_Hash for each entry.

1.4. Content Signing Order

This order consists of a single entry instead of a sub-header / entry combination. This means that a single certificate can be signed per request.

Content signing order entry (Version 1)

A version 1 order delivery file is only used for orders in which a Content Certificate is signed and no Default MCS PVCC is included. This order format is identical to that produced before CSS and PVCC certificate signing orders were available from the AACS Key Generation Facility.

Field Name	Size (bits)	Description
CRL_size	32	Size of the Content Revocation List included in this order file.
Content_Certificate_Size	32	Size of the Content Certificate field
CRL	16*n*	Content Revocation List.
Content_Certificate	16*n*	Signed Content Certificate (this is the certificate the licensee provided, now signed)
Integrity_Hash	160	SHA-1 hash of all the preceding fields on this order entry. Please note that there will be an Integrity_Hash for each entry

Content signing order entry (Version 2)

A version 2 order delivery file is provided if the order includes a Default MCS PVCC, or if the signed certificate is a PVCC or CSS Content Certificate.

Field Name	Size (bits)	Description
CRL_size	32	Size of the Content Revocation List included in this order file.
Content_Certificate_Size	32	Size of the Content Certificate field
Default_MCS_PVCC_Size	32	Size of the default MCS Prepared Video Content Certificate field. This field is set to zero if no default PVCC is included.
CRL	16*n*	Content Revocation List.
Content_Certificate	16*n*	Signed Content Certificate (a CC, PVCC, or CSS CC) (this is the certificate the licensee provided, now signed)
Default_MCS_PVCC	16*n*	Signed default MCS Prepared Video Content Certificate (PVCC for the default Managed Copy Server - the facility generates this certificate automatically, if requested).
Integrity_Hash	160	SHA-1 hash of all the preceding fields on this order entry. Please note that there will be an Integrity_Hash for each entry

1.5. Drive/Host/MCS Authentication Certificate Order

A Drive/Host/MCS Authentication Key Order consists of the order header mentioned above, a Drive/Host Authentication Certificate Order header (Drive or Host certificate orders), the data for each order entry (which here represents the data for a particular drive, host, or Managed Copy Server), and the end section.

Drive/Host Authentication Certificate Order header

Field Name	Size (bits)	Description
Reserved	16	Set to 0x0001 .
Reserved	16	Reserved for future use.

Note: This header is not present in MCS Authentication Certificate orders.

Drive/Host/MCS Authentication Certificate Order entry

Field Name	Size (bits)	Description
Private Key	160	Private Key used for drive, host, or MCS authentication.
Public Key Certificate	736	Public Key Certificate which includes the Public Key corresponding the Drive, Host, or MCS Private Key above.
Seed	160	Seed that may be used as a constant value for a random or pseudorandom number generator implemented in the corresponding drive, host, or Managed Copy Server.
Integrity_Hash	160	SHA-1 hash of all the preceding fields on this order entry. Please note that there will be an Integrity_Hash for each entry.

1.6. End Section

Each order file ends with the end section which includes a signature using one of the AACS LA Private Keys. The AACS_LA_CC_{priv} key is used to sign Content Certificate Orders. The AACS_LA_{priv} key is used to sign all other orders. The signature is applied to all the entire contents of the order file up to but not including this section. Recipient licensee is required to validate the signature on the order file using the appropriate public key to ensure its authenticity.

Field Name	Size (bits)	Description
Order signature	320	Signature on the entire contents of the order file up to but not including this section, using AACS_LA_{priv} key for Content Certificate orders and AACS_LA_{priv} key for all other orders.