

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.

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.
- 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.

AACCS 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 “<input checked="" type="checkbox"/>” desired tier (one only): <input type="checkbox"/> US\$ 3,000.00 for up to 100K copies per year <input type="checkbox"/> US\$ 10,000.00 for up to 1M copies per year <input type="checkbox"/> US\$ 25,000.00 for up to 10M copies per year <input type="checkbox"/> 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 AACCS 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

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**)

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 Robustness Certificate <input type="checkbox"/> Set “Data Key Settable” (DKS) flag	(Max. 1,000,000)	x US\$ 0.02/pair = US\$ _____
Host Proactive Renewal Certificate <input type="checkbox"/> Set “Data Key Settable” (DKS) flag		Check “<input checked="" type="checkbox"/>” desired tier (one only): <input type="checkbox"/> US\$ 500.00 for up to 100K copies per year <input type="checkbox"/> US\$ 2,000.00 for up to 1M copies per year <input type="checkbox"/> US\$ 5,000.00 for up to 10M copies per year <input type="checkbox"/> US\$ 10,000.00 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

AACS Media Key Block /Sequence Key Block Order

Name of Adopter/Content Participant/Content Provider (“Licensee”)

Licensee ID (4 digits): _____

PGP Fingerprint: _____

<p><u>SELECT ONE</u></p> <p><input type="checkbox"/> Blu-ray/HD DVD Class I</p> <p><input checked="" type="checkbox"/> Blu-ray/HD DVD Class II</p> <p><input type="checkbox"/> CBHD (China) order</p>

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
Set(s) of MKB/SKB (<i>i.e.</i> , 1 to 500)	

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

AACCS 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 AACCS 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 AACCS 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 AACCS 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: AACCS 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 AACCS 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 AACCS 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 (AACCS)
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 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.

Field Name	Size (bits)	Description																								
Version	16	0x0001																								
Reserved	16	Reserved for future use																								
Order Generation TimeStamp	64	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.																								
Licensee_ID	16	ID of Licensee requesting order 0x0000 TEST -- Usage is reserved by AACS																								
Order_Format	16	The Order_Format field may take the following values:																								
		<table border="1"> <thead> <tr> <th>Encoding</th> <th>Definition</th> </tr> </thead> <tbody> <tr> <td>0x001*</td> <td>Device Order (device and sequence key sets)</td> </tr> <tr> <td>0x0010</td> <td>Type A, Enhanced Robustness</td> </tr> <tr> <td>0x0011</td> <td>N/A</td> </tr> <tr> <td>0x0012</td> <td>N/A</td> </tr> <tr> <td>0x0013</td> <td>Type C, proactive renewal First Order</td> </tr> <tr> <td>0x0016</td> <td>N/A</td> </tr> <tr> <td>0x0017</td> <td>Type C, Proactive Renewal Update Order</td> </tr> <tr> <td>0x002*</td> <td>MediaKey Block Order (MKBs and SKBs)</td> </tr> <tr> <td>0x0020</td> <td>Pre-recorded media</td> </tr> <tr> <td>0x0021</td> <td>Recordable media</td> </tr> <tr> <td>0x0030</td> <td>Content Signing</td> </tr> </tbody> </table>	Encoding	Definition	0x001*	Device Order (device and sequence key sets)	0x0010	Type A, Enhanced Robustness	0x0011	N/A	0x0012	N/A	0x0013	Type C, proactive renewal First Order	0x0016	N/A	0x0017	Type C, Proactive Renewal Update Order	0x002*	MediaKey Block Order (MKBs and SKBs)	0x0020	Pre-recorded media	0x0021	Recordable media	0x0030	Content Signing
Encoding	Definition																									
0x001*	Device Order (device and sequence key sets)																									
0x0010	Type A, Enhanced Robustness																									
0x0011	N/A																									
0x0012	N/A																									
0x0013	Type C, proactive renewal First Order																									
0x0016	N/A																									
0x0017	Type C, Proactive Renewal Update Order																									
0x002*	MediaKey Block Order (MKBs and SKBs)																									
0x0020	Pre-recorded media																									
0x0021	Recordable media																									
0x0030	Content Signing																									

		0x004*	Drive/Host Authentication Certificates
		0x0040	Drive keys and certificates
		0x0041	Host keys and certificates, Enhanced Robustness
		0x0042	Host keys and certificates, Proactive Renewal
		0x0050	N/A
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. Hardcoded 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. Hardcoded to 256 Set to 0 for order types 0x0017
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 ≤ Column _i < Sequence_Keys 0 ≤ Row _i < rows in sequence keys matrix
K _{s_i}	64 * Sequence_Keys	The sequence keys, in the same order as the row and column indices.
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 Key Block Order

A Media Key Block 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 set), and the end section.

Field Name	Size (bits)	Description
Reserved	16	Fixed to 0x0001
MKB_size	32	Size (in bytes) of the MKBs contained in this order. Since all MKBs 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. This value is fixed to 12628.
SKB_size	32	Size (in bytes) of the SKB portion of each entry contained in this order. This includes the SKB size, the SKB data and the Media Key Variant values for all of the SKBs corresponding to each entry.
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 fixed to 16384.
Max_Variants	16	Maximum number of variants of each title in a prepared title sequence. This value is fixed to 1024
Num_SKBs	8	Number of SKBs per SKB in each order. If this value is set to 0 (i.e. an order with no SKBs), the fields “SKB_size”, “SKB_rows” and “Max_Variants” should be ignored. This value is fixed to 0 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.

Pre-recorded media order entry

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

Field Name	Size (bits)	Description
MKB type 3	32n (MKB_size)	Media Key Block type 3. To be placed in pre-recorded disc for recorders to update their default MKB.
MKB type 4	32n (MKB_size)	Media Key Block for pre-recorded media
K _m	128	Media Key encoded on the MKB present on 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	32n (SKB_size)	1 st 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 1 st SKB. Media Key Variants are provided in ascending order
SKB ₁ size	32	Size of SKB ₁ in the next field
SKB ₁	32n (SKB_size)	2 nd 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 2 nd SKB. Media Key Variants are provided in ascending order
		⋮
SKB _n size	32	Size of SKB _n in the next field
SKB _n (n = Num_SKBs - 1)	32n (SKB_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.

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	32n (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.

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	16n	Content Revocation List.
Content_Certificate	16n	Signed content certificate
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 Authentication Certificate Order

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

Drive/Host Authentication Certificate Order header

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

Drive/Host Authentication Certificate Order entry

Field Name	Size (bits)	Description
Drive (Host) Private Key	160	Drive (Host) Private Key used for drive authentication
Drive (Host) Certificate	736	Drive (Host) Certificate which includes the Drive (Host) Public Key corresponding the Drive (Host) Private Key above
Seed	160	Seed may be used as constant value for random/pseudorandom number generator implemented in corresponding drive (host).
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

APPENDIX B - Content Certificate Filename Convention

Input File: AACCS Content Certificates are required to be submitted with a filename that conforms to the following convention:

LicenseeID_CompanyName_Title

Where

- **LicenseeID**
 - is the 4-digit Licensee ID, i.e. LLLL
 - Examples:
 - 0009
 - 0075
 - 0362
 - 4279

- **CompanyName**
 - is the Licensee company/replicator name
 - to maximize the ability of the Key Generation Facility to track the filename, the CompanyName should also include the email address (not including domain or punctuation) of the person submitting the order
 - Examples:
 - Toshiba_HYamada
 - SonyOsawa4
 - Microsoft_GatesB
 - IBMDulce

- **Title**
 - is a content identifier which will be recognizable by the Licensee. It is not necessary for it to be recognizable by the KGF, so either a real title or a project code name/number is appropriate
 - the title can optionally include Layer information
 - Examples
 - MovieTitle
 - MovieTitle_DualLayer1
 - MovieTitleSingleLayer
 - ProjectCode_Layer2
 - ProjectCode

Examples of complete input filenames

- 0009_Toshiba_HYamada_MovieTitle
- 0009_Toshiba_HYamada_MovieTitle_DualLayer1
- 0075_Microsoft_GatesB_ProjectCode_Layer2
- 4279_IBMDulce_MovieTitleSingleLayer

The input file name should be “LicenseeID_CompanyName_Title” with no extension. There is a limitation on the length of the **filename of the output file**, hence it is necessary to impose a maximum length of 99 characters to the input file name.

Allowable characters in the input filename include the following:

Uppercase letters	A-Z
Lowercase letters	a-z
Numbers	0-9
Dot/period	.
Dash	-
Underscore	_

Output File: The filename of the signed content certificate, i.e. the output file produced by the KGF, shall follow the following convention:

<input_file_name>_MM.DD.YYYY_HH.MM.SS.sss.PGP

where

- <input_file_name>** is the first 99 character of the input filename.
- MM.DD.YYYY** is the month, day, year of the successfully signed Content Certificate
- HH.MM.SS.SSS** is hours, minutes, sec, and fractions of the successfully signed Content Certificate.

The Key Generation Facility will not parse or otherwise interpret the input filename. Instead it merely copies up to 99 characters of the input filename, and then appends the timestamp and the ".PGP" file extension to construct the output filename. Note that, even in the case where two input filenames get truncated to the same string, the time stamp will make the output filename unique. However, care should be taken to avoid this outcome, as it introduces the potential for confusion between two Content Certificate orders.