



Technical Specification

Tamper protection with BGC HMAC
(HMAC-SHA256-128)

April 2009

Ver. 1.2

Contents

Contents.....	2
1 General.....	3
2 Tamper protection with HMAC-SHA256-128.....	3
2.1 Calculation.....	3
2.2 File data format.....	4
2.2.1 General.....	4
2.2.2 Normalised character set.....	4
2.2.3 Example normalisation of Swedish special characters.....	4
2.3 File’s fundamental appearance.....	5
2.3.1 Seal Opening record (TK 00).....	5
2.3.2 Tamper Protection record (TK 99).....	5
3 Key Management.....	6
3.1 Principle.....	6
3.2 Responsibility for keys.....	6
3.3 Key verification value.....	6
4 Definition of characters used.....	7
4.1 EBCDIC – ASCII Conversion Table.....	9
5 Contact.....	9

Versions

Date	Version	Description	Responsible for change
Feb 2008	1.0	New Document	Fredrik Eriksson
June 2008	1.0	Swedish special characters added to character table in 4	Fredrik Eriksson
Jan 2009	1.1	Document restructured Clarification on normalisation of Swedish special characters.	Fredrik Eriksson
Apr 2009	1.2	Section 3c in 2.1 removed. Note on seal verification of 00-record added in 2.1 New example 2.2.3, normalisation of special characters Changes in conversion table (4.1), 0xBE converts to 0xC3 Control characters 0x00-0x3F converts to 0xC3,	Fredrik Eriksson

1 General

BGC accept files with HMAC-SHA256-128 tamper protection. To send files, the sender must have an agreement with their bank and must have been assigned a customer number and a seal key upon signing the agreement. Additionally, the rules stipulated in this document must be followed.

In principle, BGCs method of tamper protection with HMAC-SHA256-128 means that a file to be sent to BGC is run through an algorithm (256-bit secure hash algorithm, SHA256) that calculates a cryptographic checksum on the file, a hash-based message authentication code (MAC). The BGC HMAC standard uses a secret key that is 128 bits long to generate a MAC that is also 128 bits long. (Note that the MAC should be truncated to 128 bits since SH256 normally generates a 256-bit value. It is the first 128 bits that should be used as the MAC.)

More information on HMAC-SHA256-128 can be found in the following documents:

FIPS-180-3 (Describes HMAC)

FIPS-198-1 (Describes SHA256)

RFC4868 (Describes HMAC-SHA256-128 and how the hash value is truncated)

This Doc (Describes BGC HMAC, specifics regarding BGC implementation of the standard.)

2 Tamper protection with HMAC-SHA256-128

2.1 Calculation

When a data file with payment information is created, the MAC is calculated with HMAC-SHA256-128 as per the following:

1. **Create Seal Opening record.** This record contains the seal date and type (always HMAC).
2. Initiate the algorithm with the current key, provided by BGC.
3. **Calculate MAC**
 - a. Read the file and **normalise** the contents.
 - b. Send the normalised file data to the algorithm to calculate the MAC.
4. **Calculate** a Key Verification Value, **KVV**.
5. **Create Tamper Protection record** containing the KVV and MAC.
6. **Complete the file** with Tamper Protection record and **send** it to BGC for processing.

When calculating the MAC;

- The entire file including the Seal Opening record (TK 00), must be processed in the algorithm. The Tamper Protection record (TK 99) however, is used to store the calculated MAC and, therefore, should not be included in the calculation.
- If end-of-line characters are used in the file (LF, CRLF, Carriage Return Line Feed), these characters should not be included in the calculation.
- Note that the file data should be normalised before the calculation of the MAC.
- Note that only the first 80 characters of the Seal Opening record should be included in the seal calculation, regardless of actual size. Particularly important when validating seal on received files.

2.2 File data format

2.2.1 General

Because the algorithm is binary, great weight must be placed on the data format of the file, to prevent problems with potential character conversions, as keyboard characters are not represented in the same way in different environments. If the file looks different at BGC than it did at the sender, the calculated MAC will also differ. Consequently, the file's contents may need to be converted to a type of normalised standard character set so that the file always looks the same at the time of calculation regardless of where it was created. This means that a normalisation of file data must take place before the MAC is calculated.

2.2.2 Normalised character set

For the method pertaining to this document (HMAC-SHA256-128), all characters in the 7-bit ASCII table (see the table at the end of this document), excluding the control character, are included, i.e. all characters from hex 20 (space) to hex 7E (~), inclusive. Bit patterns to be used in the calculation of the MAC are defined for each character, in the table at the end of this document.

Swedish special characters, åäöéüÅÄÖÉÜ, must also be included in the calculation. This means that these characters have to be interpreted as if they were part of the 7-bit ASCII character set. (For instance, the character “Ö” should be replaced with hex 5C during MAC calculation) Hex- and binary codes for these characters are also listed in the table at the end of this document.

All characters not listed in the table are replaced by hex C3 (dec 195) before seal calculation.

2.2.3 Example normalisation of Swedish special characters

If using ISO 8859-1 on client side, this table is an example on how normalisation of Swedish special characters into 7-bit ASCII sealing data, as described in section 2.2.2 above can be performed.

Character	ISO 8859-1		-->	7-Bit ASCII	
	Hex	Dec		Dec	Hex
É	C9	201	-->	64	40
Ä	C4	196	-->	91	5B
Ö	D6	214	-->	92	5C
Å	C5	197	-->	93	5D
Ü	DC	220	-->	94	5E
é	E9	233	-->	96	60
ä	E4	228	-->	123	7B
ö	F6	246	-->	124	7C
å	E5	229	-->	125	7D
ü	FC	252	-->	126	7E

2.3 File's fundamental appearance

The file must have the format and the character set that the applicable applications presuppose. Important records for tamper protection are the Seal Opening record (TK 00) and the Tamper Protection record (TK 99).

2.3.1 Seal Opening record (TK 00)

The Seal Opening record (TK 00) contains information about the method (HMAC) and the date the file was signed (key date). The Seal Opening record must always be 80 characters long, regardless of the length of following records, and must be structured as indicated in the table below.

Positions	Field description
1-2	Transaction code, always "00"
3-8	Key date YYMMDD – date that the file's seal was created.
9-12	Type of condensate, always "HMAC" for this type of algorithm.
13-80	Blank/reserve

2.3.2 Tamper Protection record (TK 99)

In the Tamper Protection record (TK 99), information is stored regarding the date the file was signed (key date), the checksum (KVV) for the key used, and the MAC obtained from the calculation. The Tamper protection record must be structured as indicated in the table below.

Positions	Field description
1-2	Transaction code, always "99"
3-8	Key date YYMMDD – date that the file's seal was created.
9-40	KVV for key used, 128 bits, presented as 32 hexadecimal digits.
41-72	MAC for the file, 128 bits, presented as 32 hexadecimal digits.
73-80	Blank/reserve

3 Key Management

3.1 Principle

HMAC-SHA256-128 requires a 128-bit key for the calculation of a MAC on the data. This is normally represented as 32 hexadecimal digits in manual processing. A key is valid, until a new key is requested, which is then delivered in a sealed key envelope. The key is secret to all outsiders and only those assigned, and consequently entrusted, to handle the key shall have knowledge of it.

3.2 Responsibility for keys

Within BGC, keys are handled with a high level of secrecy. Therefore, great responsibility rests with the customer to manage keys and introduce program support for this in such a way that keys cannot be disclosed to or used by unauthorised parties.

The objective of key management is to achieve a situation in which the key is stored securely and cannot be revealed or abused. The following requirements must be set for secure key management:

- Keys are locked away when not in use.
- Keys are retrieved and entered in manually at each use, unless encryption is available in the environment in which tamper protection is used.
- Processing should take place in an environment such that it can be reasonably ensured that the key values are not disclosed to unauthorised parties.

3.3 Key verification value

A Key Verification Value (KVV) shall be calculated each time a key is used to protect a file. The KVV is calculated as a MAC for a “standard file” with the current key. (The “Standard file” for calculation of KVV has the contents: “00000000”, i.e. 8 zeros in ASCII-format, hex 30.) The KVV value shall be placed in the indicated location in the Tamper Protection record (TK 99) and is used in the seal verification process at BGC.

Each key has a different Key Verification Value (KVV) and hence, by verifying the KVV before calculation of MAC, the risk that erroneous key values are used can be reduced. To check the entry, the KVV can be stored in the system for comparison with the KVV obtained for the entered key.

4 Definition of characters used

This table shows the data to be used in the calculation of a MAC in accordance with BGCs method HMAC-SHA256-128. The characters that are not in the table are replaced, as previously mentioned, with hex C3 (dec 195) before seal calculation.

Hexadecimal	Binary	Char. as per 7-bit ASCII ISO/IEC 646
20	0010 0000	SP
21	0010 0001	!
22	0010 0010	" (double quote)
23	0010 0011	#
24	0010 0100	\$
25	0010 0101	%
26	0010 0110	&
27	0010 0111	' (single quote)
28	0010 1000	(
29	0010 1001)
2A	0010 1010	*
2B	0010 1011	+
2C	0010 1100	,
2D	0010 1101	- (minus sign)
2E	0010 1110	.
2F	0010 1111	/
30	0011 0000	0
31	0011 0001	1
32	0011 0010	2
33	0011 0011	3
34	0011 0100	4
35	0011 0101	5
36	0011 0110	6
37	0011 0111	7
38	0011 1000	8
39	0011 1001	9
3A	0011 1010	:
3B	0011 1011	;
3C	0011 1100	<
3D	0011 1101	=
3E	0011 1110	>
3F	0011 1111	?
40	0100 0000	@, É
41	0100 0001	A
42	0100 0010	B
43	0100 0011	C
44	0100 0100	D
45	0100 0101	E
46	0100 0110	F
47	0100 0111	G
48	0100 1000	H
49	0100 1001	I
4A	0100 1010	J

4B	0100 1011	K
4C	0100 1100	L
4D	0100 1101	M
4E	0100 1110	N
4F	0100 1111	O
50	0101 0000	P
51	0101 0001	Q
52	0101 0010	R
53	0101 0011	S
54	0101 0100	T
55	0101 0101	U
56	0101 0110	V
57	0101 0111	W
58	0101 1000	X
59	0101 1001	Y
5A	0101 1010	Z
5B	0101 1011	[, Å
5C	0101 1100	\, Ö
5D	0101 1101], Ä
5E	0101 1110	^, Ü
5F	0101 1111	_ (underscore)
60	0110 0000	` , é
61	0110 0000	a
62	0110 0001	b
63	0110 0010	c
64	0110 0100	d
65	0110 0101	e
66	0110 0110	f
67	0110 0111	g
68	0110 1000	h
69	0110 1001	i
6A	0110 1010	j
6B	0110 1011	k
6C	0110 1100	l
6D	0110 1101	m
6E	0110 1110	n
6F	0110 1111	o
70	0111 0000	p
71	0111 0001	q
72	0111 0010	r
73	0111 0011	s
74	0111 0100	t
75	0111 0101	u
76	0111 0110	v
77	0111 0111	w
78	0111 1000	x
79	0111 1001	y
7A	0111 1010	z
7B	0111 1011	{ , ä
7C	0111 1100	, ö
7D	0111 1101	} , å
7E	0111 1110	~ , ü

4.1 EBCDIC – ASCII Conversion Table

When calculating a MAC, ASCII shall always be used. Consequently, if the customer’s platform uses EBCDIC, a character conversion must be applied before the MAC calculation.

The following conversion table shall be used in these cases.

The outer frame represents the hexadecimal EBCDIC value. To translate SPACE (x’40’) in EBCDIC to ASCII, the following is done:

1. Find 4x in the left-hand column.
2. On the 4x row, find the value below the x0 column.
3. The value found is 20, which corresponds to SPACE (x’40’) in EBCDIC.

	x0	x1	x2	X3	X4	X5	X6	X7	X8	X9	xA	xB	xC	xD	xE	xF
0x	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3
1x	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3
2x	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3
3x	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3
4x	20	C3	C3	7B	C3	C3	C3	7D	C3	C3	C3	2E	3C	28	2B	21
5x	26	60	C3	C3	C3	C3	C3	C3	C3	C3	C3	5D	2A	29	3B	5E
6x	2D	2F	C3	23	C3	C3	C3	24	C3	C3	7C	2C	25	5F	3E	3F
7x	C3	5C	C3	C3	C3	C3	C3	C3	C3	60	3A	5B	5C	27	3D	22
8x	C3	61	62	63	64	65	66	67	68	69	C3	C3	C3	C3	C3	C3
9x	C3	6A	6B	6C	6D	6E	6F	70	71	72	C3	C3	C3	C3	C3	5D
Ax	C3	7E	73	74	75	76	77	78	79	7A	C3	C3	C3	C3	C3	C3
Bx	C3	C3	C3	C3	C3	5B	C3	C3	C3	C3	C3	7C	C3	C3	C3	C3
Cx	7B	41	42	43	44	45	46	47	48	49	C3	C3	C3	C3	C3	C3
Dx	7D	4A	4B	4C	4D	4E	4F	50	51	52	C3	C3	7E	C3	C3	C3
Ex	40	C3	53	54	55	56	57	58	59	5A	C3	C3	40	C3	C3	C3
Fx	30	31	32	33	34	35	36	37	38	39	C3	C3	5E	C3	C3	C3

5 Contact

For more information about BGC HMAC, visit our website www.bgc.se/hmac or contact us at: hmac-sigill@bgc.se.