International Confirminet Millennium

Comprehensive Management of National and International Payments

Madrid - May 2013

CONFIRMINET MILLENNIUM INTERNATIONAL FILE FORMATS

The standard entry format for the Comprehensive Payment Management Product is exactly the same as the standard format of Booklet 34 of the CSB, except for changes in some fields due to specific product requirements.

COMPREHENSIVE MANAGEMENT OF NATIONAL PAYMENTS

Internal composition

Each file must contain the following records

-. A record with code 03 and data number 001, header record with identifying details of the Remittance.
-. A detailed record, code 06 and data number 010, with data of the Payment orders (Supplier, Amount, Payee Account).
-. A detailed record, code 06 and data number 011, with Supplier Name.
-. A detailed record, code 06 and data number 012, with Supplier Address.
-. A detailed record, code 06 and data number 013, with the Telephone number. (Optional). -. A detailed record, code 06 and data number 014, with Supplier Post Code and Town. -. A detailed record, code 06 and data number 015, with Supplier Region.
-. A detailed record, code 06 and data number 016, with the Supplier Fax Number.
-. A detailed record, code 06 and data number 170, with Supplier e-mail address, if appropriate. (Optional)
-. A Totals record, code 08 .

Description of Records

First Record: Header record with Information on the Remittance

Position	Description	Length	Comments
1-2	Record code	X(2)	'03' Compulsory
3-4	Currency identifier.	X(2)	'06' or '56' depending on the remittance currency.
5-14	Issuer code	X(10)	Client NIF/CIF
15-26	Free	X(12)	The first 7 positions will contain BK internal reference. NEXO dispatch number.
27-29	Data number	X(3)	'001' Compulsory
30-35	Send date	X(6)	YYMMDD Format Compulsory
36-41	Issue date	X(6)	YYMMDD Format Compulsory
42-45	Agency Code where the contract resides	X(4)	This will always be '0128'
46-49	Branch Code where contract is held	X(4)	Compulsory
50-59	Contract number	X(10)	Compulsory. Comprehensive Payment Management Contract number. Compulsory.
60-63	Free	X(4)	Blanco
64-65	Control Digit	X(2)	Digit which completes the CCC (Client Account Code) of the Comprehensive Payment Management account. Compulsory

66-72	Free	X(7)	Blanco

Description of Records

Detailed record

These records will have common initial positions, the same for all of them and some specific areas.
First, below we see the format common to them all:

Position	Description	Length	Comments
1-2	Record code	X(2)	'06' Compulsory
3-4	Transaction code	X(2)	'06' Transfer '07' Cheque '09' Recorded payment. If the currency is the Peseta or '56' Transfer '57' Cheque '59' Recorded payment. If the currency is the Euro. Compulsory. If credit in BK account it would be '06'.
5-14	Issuer code	X(10)	Client NIF/CIF
15-24	Supplier NIF/CIF	X(10)	Supplier NIF/CIF
25-26	Free	X(2)	Blanco
27-29	Data number	X(3)	'010' Compulsory. '011' Compulsory. '012' Compulsory. '013' Optional. '014' Compulsory. '015' Compulsory. '016' Optional. '170' Optional. '018' Compulsory
30-65	Depends on the type of record. Description of specific areas	X(36)	Blanco
66-72	Free	X(7)	Blanco

Description of Records

Detailed Record

Description of specific areas, depending on the Data Number.

Data no.	Position	Description	Length	Comments
010	30-41	Invoice Amount	X(12)	Unpacked amount aligned to the right and filled in with zeros to the left. No decimal points. No sign. If the currency is the Euro the two digits on the right will indicate the decimals.
Blanco	42-45	Payee Account Bank Code	X(4)	Compulsory, whenever the method of Payment selected is not by Cheque.
Blanco	46-49	Payee Account Branch Code	X(4)	Compulsory, whenever the method of Payment selected is

				not by Cheque.
Blanco	50-59	Payee Account Number	X(10)	Compulsory, whenever the method of Payment selected is not by Cheque.
Blanco	60-60	Free	X(1)	Blanco
Blanco	61-61	Amount sign	X(1)	If it is a normal invoice, leave blank. If it is a payment order, to distinguish it from invoices, put '-'. Compulsory
Blanco	62-63	Free	X(2)	Blanco
Blanco	64-65	Payee Account Control Digit	X(2)	Compulsory if the method of Payment selected is not by Cheque.

Description of Records

Detailed Record
Description of specific areas, depending on the Data Number.

Data	Position	Description	Length	Comments no.
011	30-65	Supplier name	X(36)	Compulsory
				Aligned to the left and filled in with blanks to 36 positions.

Description of Records

Detailed Record
Description of specific areas, depending on the Data Number.

Data no.	Position	Description	Length	Comments
012	30-60	Name of street	X(31)	Compulsory
				Aligned to the left and filled in with blanks to the right.
Blanco	61-65	Name of street	X(5)	Compulsory.
				Number given to no decimal points, aligned to the left and filled in with blanks to the right.

This record is optional, i.e. it does not have to appear.

Data no.	Position	Description	Length	Comments
013	30-32	Supplier telephone area code	9(3)	Optional.
Blanco	33-39	Supplier telephone number.	9(7)	Optional.
Blanco	40-65	Free.	X(26)	Blanco

Data no.	Position	Description	Length	Comments
014	30-34	Post Code	X(5)	Compulsory
Blanco	35-65	Town	X(31)	Compulsory
				Aligned to the left and filled in with blanks to the right

Data no.	Position	Description	Length	Comments
015	30-60	Region	X(31)	Compulsory

				Aligned to the left and filled in with blanks to the right
Blanco	61-62	Country	X(2)	Optional. Country Swift Code.
Blanco	63-65	Free	X(3)	Blanco

This record is optional, i.e. it does not have to appear.

Data no.	Position	Description	Length	Comments
016	30-32	Supplier fax area code	9(3)	Optional.
Blanco	33-39	Supplier fax number.	9(7)	Optional.
Blanco	40-65	Free.	X(26)	Blanco

This record is optional, i.e. it does not have to appear, if the Supplier does not have an E-mail address.

Data	Position	Description	Length	Comments no.
170	30-65	E-mail address.	X(36)	Optional. Aligned to the left and
				filled in with blanks to the right

Description of Records

Detailed Record
Description of specific areas, depending on the Data Number.

Data no.	Position	Description	Length	Comments
018	30-35	Invoice due date	X(6)	Compulsory.
Blanco	36-51	Invoice number	X(16)	YYMMDD format. Compulsory
Blanco	52-65	Free.	X(14)	Aligned to the left and filled in with blanks to the right. In this field the value given will
		Left as Client internal reference. value		be observed, for Bankinter it is transparent. It refers to the of the reference field of the order.

Description of Records

Totals record: To carry out a check of the file received.

Position	Description	Length	Comments
1-2	Record code	X(2)	'08' Compulsory
3-4	Currency identifier.	X(2)	'06' or '56' depending on currency of the remittance. Blanco
5-14	Issuer code	X(10)	Client NIF/CIF
15-29	Free	X(15)	Blanco
30-41	Amounts total	X(12)	Total amount of invoices. This is a number given to no decimal points, aligned to the right and filled in with zeros to the left. Although there may be some

			negative Payment Orders the amounts in the corresponding amounts fields will be added as if they were all positive.
42-49	Number of data records 010	X(8)	This is a number given to no decimal points, aligned to the right and filled in with zeros to the left.
50-59	Total number of data records	X(10)	This is a number given to no decimal points, aligned to the right and filled in with zeros to the left
60-72	Free	X(13)	Blanco

COMPREHENSIVE MANAGEMENT OF INTERNATIONAL PAYMENTS

Internal composition

Each file must contain the following records

-. A record with code 03 and data number 001, header with identifying data of the Remittance. -. A detailed record, code 06 and data number 010, with data of the Payment orders (Amount). -. A detailed record, code 06 and data number 011, with Supplier Name.
-. A detailed record, code 06 and data number 012, with Supplier Address.
-. A detailed record, code 06 and data number 014, with Supplier Post code and Town.
-. A detailed record, code 06 and data number 017, with Supplier Telephone and Fax numbers, if the supplier would like to receive information via this medium. (Optional)
-. A detailed record, code 06 and data number 170, with the Supplier e-mail address, if it has one and wishes to receive information via this medium. (Optional)
-. A detailed record, code 06 and data number 171, with the continuation of the Supplier e-mail address, if it has one and wishes to receive information via this medium. (Optional)
-. A data entry, code 06 and data number 172, containing the continuation of the supplier's e-mail address, if available and the supplier wishes to receive information by this means (Optional).
-. A detailed record, code 06 and data number 173, with the Supplier account and Country Swift Code.
-. A detailed record, code 06 and data number 174, with the Swift address and BLZ/CHIP code of the Supplier account.
-. A detailed record, code 06 and data number 175, with the Supplier Language.
-. A data entry, code 06 and data number 176, containing the supplier's second e-mail address, if available and the supplier wishes to receive information by this means (Optional).
-. A data entry, code 06 and data number 177, containing the continuation of the supplier's second e-mail address, if available and the supplier wishes to receive information by this means (Optional).
-. A data entry, code 06 and data number 178, containing the continuation of the supplier's second e-mail address, if available and the supplier wishes to receive information by this means (Optional).
-. A data entry, code 06 and data number 179, containing the supplier's third e-mail address, if available and the supplier wishes to receive information by this means (Optional).
-. A data entry, code 06 and data number 180, containing the continuation of the supplier's third e-mail address, if available and the supplier wishes to receive information by this means (Optional).
-. A data entry, code 06 and data number 181, containing the continuation of the supplier's third e-mail address, if available and the supplier wishes to receive information by this means (Optional).
-. A detailed record, code 06 and data number 018, with invoice identification data (invoice number and due date).
-. A detail record, with code 06 and datum number 182, with its internal supplier reference number.
-. A Totals record, code 08 .

Description of Records

First Record: Header record with information on the Remittance

Position	Description	Length	Comments
1-2	Record code.	X(2)	'03' Compulsory.
3-4	Data code.	X(2)	'60' Compulsory.
5-14	Issuer code.	X(10)	Client NIF/CIF. It should be aligned to the left

			and filled in with blanks to the right. Compulsory.
15-26	Free.	X(12)	The first 7 positions will contain BK internal reference.
27-29	Data number.	X(3)	'001' Compulsory.
30-35	Send date.	X(6)	YYMMDD Format. Compulsory.
36-41	Issue date.	X(6)	YYMMDD Format. Compulsory.
42-45	Agency Code where the contract resides	X(4)	This will always be '0128'. Compulsory.
46-49	Branch Code where contract is held	X(4)	Compulsory.
50-59	Contract no.	X(10)	Comprehensive Payment Management Contract number. Compulsory.
60-63	Free.	X(4)	Blanco
64-65	Control Digit.	X(2)	Digit which completes the CCC of the Comprehensive Payment Management account. Compulsory
66-72	Free.	X(7)	

Detailed Record

These records will have common initial positions, the same for some of them and some specific areas.
First, below we see the format common to them all:

Position	Description	Length	Comments
1-2	Record code.	X(2)	'06' Compulsory.
3-4	Data code.	X(2)	'60' Compulsory.
5-14	Issuer code.	X(10)	Client NIF/CIF. Compulsory.
15-24	International Supplier Reference.	X(10)	Valid Personal or Corporate Tax Identification Number or International Supplier Reference, calculated according to the algorithm described in Annex 1. Obligatory.
25-26	Free.	X(2)	Blanco
27-29	Data number.	X(3)	'010' Compulsory. '011' Compulsory. '012' Compulsory. '014' Compulsory. '017' Optional. '170' Optional. '171' Optional. '172' Optional.

			'173' Compulsory. '174' Compulsory. '175' Compulsory. '176' Optional. '177' Optional. '178' Optional. '179' Optional. '180' Optional. '181' Optional. '018' Compulsory
30-72	Depends on type of record. Description of specific areas.	X(43)	Blanco

Description of specific areas, depending on the Data Number.

Data no.	Position	Description	Length	Comments
010	30-41	Invoice amount.	9(10)V9(2)	Invoice amount with 12 total positions, the two last positions being decimals. No sign. Aligned to the right and filled in with zeros to the left. Compulsory.
Blanco	42-60	Free.	X(19)	Blanco
Blanco	61-61	Sign of Invoice amount.	X(1)	It will allow the following values: ' ', if it is a normal invoice and '-', if its a payment order to settle with invoices. Compulsory.
Blanco	62-72	Free.	X(11)	Blanco

Description of specific areas, depending on the Data Number.

Data no.	Position	Description	Length	Comments
011	30-65	Supplier name.	X(36)	It should be aligned to the left and filled in with blanks to the right. Compulsory.
Blanco	66-72	Free.	X(7)	Blanco

Description of specific areas, depending on the Data Number

Data no.	Position	Description	Length	Comments
012	30-65	Supplier Address.	X(36)	It should be aligned to the left and filled in with blanks to the right. Compulsory.
Blanco	66-72	Free.	X(7)	Blanco

Description of specific areas, depending on the Data Number

Data no.	Position	Description	Length	Comments
014	30-40	Free.	X(11)	Blanco
Blanco	41-72	Supplier Post Code and	X(32)	It should be aligned to the left and

		Town.		filled in with blanks to the right. Compulsory.

Description of specific areas, depending on the Data Number This record is optional. It may or may not exist.

Data no.	Position	Description	Length	Comments
017	30-34	Supplier telephone area code.	X(5)	It refers to the telephone area code of the country the supplier belongs to. It should be aligned to the left and filled in with blanks to the right. Optional (if the telephone area code is entered it is compulsory to enter the telephone number).
Blanco	35-46	Supplier telephone number.	X(12)	Supplier telephone number . It should be aligned to the left and filled in with blanks to the right. Optional (if the telephone area code is entered it is compulsory to enter the telephone number).
Blanco	47-51	Supplier fax area code.	X(5)	It refers to the fax area code of the country the supplier belongs to. It should be aligned to the left and filled in with blanks to the right Optional (if the fax is entered it is compulsory to enter the fax area code).
Blanco	52-63	Supplier Fax number.	X(12)	Supplier fax number. It should be aligned to the left and filled in with blanks to the right. Optional (if the area code is entered it is compulsory to enter the fax number).
Blanco	64-72	Free.	X(9)	Blanco

Description of specific areas, depending on the Data Number This record is optional. It may or may not exist.

Data no.	Position	Description	Length	Comments
170	30-65	Supplier e-mail	X(36)	It refers to the Supplier e-mail address. Aligned to the left and filled in with blanks to the right. Compulsory.
Blanco	66-72	Free.	X(7)	Blanco

Description of specific areas, depending on the Data Number This record is optional. It may or may not exist.

Data no.	Position	Description	Length	Comments
171	30-65	Supplier e-mail	X(36)	It refers to the continuation of the

		(continuation).		supplier e-mail address, if this did not fit in the previous record. Aligned to the left and filled in with blanks to the right. Compulsory.
Blanco	66-72	Free.	X(7)	Blanco

Description of specific areas, according to Data Number
This record is optional. It may or may not exist.

Data No.	Position	Description	Length	Comment
172	**30-65**	**Supplier's E-mail (continuation).**	**X(36)**	**Corresponds to the continuation of the Supplier's e-mail address, in case it does not fit in the previous entry. Must be aligned to the left and filled with blank spaces to the right. Obligatory.**
	66-72	**Free.**	**X(7)**	

Description of specific areas, depending on the Data Number

Data no.	Position	Description	Length	Comments
173	30-63	Supplier account.	X(34)	It refers to the account the transfer will be sent to, if the transfer is to a European Union country it will be in IBAN format, otherwise it will be the account indicated by the supplier bank. If it is IBAN format, it should have the following format: • Country code (ISO), length:2, type: alphanumerical. • IBAN control digit, length: 2, type: alphanumerical. Basic Bank Account Number (BBAN), up to 30 alphanumerical characters, from 0 to 9, from A to Z (only capital letters), without spaces between them. It has a fixed length per country. Compulsory.
Blanco	64-64	Free.	X(1)	Blanco
Blanco	65-66	SWIFT code of the supplier account country.	X(2)	It refers to the SWIFT code of the supplier account. Compulsory.
Blanco	67-72	Free.	X(6)	Blanco

Description of specific areas, depending on the Data Number

Data no.	Position	Description	Length	Comments
174	30-40	Swift Address.	X(11)	It refers to the Swift address of the payee bank. It should be aligned to the left and filled in with blanks to the right. Compulsory.
Blanco	41-56	BLZ/CHIP code.	X(16)	It refers to the BLZ/CHIP code. It should be aligned to the left and filled in with blanks to the right. Optional.
Blanco	57-72	Free.	X(16)	Blanco

Description of specific areas, depending on the Data Number

Data no.	Position	Description	Length	Comments
175	30-30	Free.	X(1)	
Blanco	31-36	Free.	X(6)	
Blanco	37-37	Language.	X(1)	It refers to the language in which the supplier will receive the information sent to it by the bank The following values will be allowed: • 'E', if it wants to receive it in Spanish. • 'I', if it wants to receive it in English. Compulsory.
Blanco	38-72	Free.	X(35)	Blanco

Description of specific areas, according to Data Number

Data No.	Position	Description	Length	Comment
176	**30-65**	**Supplier's E-mail**	**X(36)**	**Corresponds to the Supplier's second e-mail address. Must be aligned to the left and**

				filled with blank spaces to the right. Obligatory.
	66-72	Free.	X(7)	

Description of specific areas, according to Data Number This record is optional. It may or may not exist.

Data No.	Position	Description	Length	Comment
177	30-65	Supplier's E-mail (continuation).	X(36)	Corresponds to the continuation of the Supplier's second e-mail address, in case it does not fit in the previous entry. Must be aligned to the left and filled with blank spaces to the right. Obligatory.
	66-72	Free.	X(7)	

Description of specific areas, according to Data Number This record is optional. It may or may not exist.

Data No.	Position	Description	Length	Comment
178	30-65	Supplier's E-mail (continuation).	X(36)	Corresponds to the continuation of the Supplier's second e-mail address, in case it does not fit in the previous entry. Must be aligned to the left and filled with blank spaces to the right. Obligatory.
	66-72	Free.	X(7)	

Description of specific areas, according to Data Number

Data No.	Position	Description	Length	Comment
179	30-65	Supplier's E-mail	X(36)	Corresponds to the Supplier's third e-mail address. Must be aligned to the left and filled with blank spaces to the right. Obligatory.
	66-72	Free.	X(7)	

Description of specific areas, according to Data Number
This record is optional. It may or may not exist.

Data No.	Position	Description	Length	Comment
180	30-65	Supplier's E-mail (continuation).	X(36)	Corresponds to the continuation of the Supplier's third e-mail address, in case it does not fit in the previous entry. Must be aligned to the left and justified with blank spaces to the right. Obligatory.
	66-72	Free.	X(7)	

Description of specific areas, according to Data Number This record is optional. It may or may not exist.

Data No.	Position	Description	Length	Comment
181	30-65	Supplier's E-mail (continuation).	X(36)	Corresponds to the continuation of the Supplier's third e-mail address, in case it does not fit in the previous entry. Must be aligned to the left and justified with blank spaces to the right. Obligatory.
	66-72	Free.	X(7)	

Description of specific areas, according to Datum Number

Datum No.	Position	Description	Length	Comments
182	30-39	Supplier Reference in local application	X(10)	If the supplier has a valid Corporate/Personal Tax Identification Number (CIF/NIF), it must be indicated, otherwise an identifying supplier reference shall be provided: said reference may be comprised of up to 10 positions. It must be aligned to the left and right-justified with leading blanks. Obligatory.
	40-72	Free.		

Description of specific areas, depending on the Data Number

Data no.	Position	Description	Length	Comments
018	30-35	Invoice Due date.	X(6)	YYMMDD format. Compulsory.
Blanco	36-51	Invoice number.	X(16)	It should be aligned to the left and filled in with blanks to the right. Compulsory.
Blanco	52-65	Free. Left as Client internal reference.	X(14)	In this field the value given will be observed, for Bankinter it is transparent. It refers to the value of the reference field of the order.
Blanco	66-72	Free.	X(7)	Blanco

Description of Records

Totals record: To carry out a check of the file received.

Position	Description	Length	Comments
1-2	Record code.	X(2)	'08' Compulsory.
3-4	Data code.	X(2)	'60' Compulsory.
5-14	Issuer code.	X(10)	Client NIF/CIF Compulsory.
15-29	Free.	X(15)	Blanco
30-41	Amounts total.	9(10)V9(2)	Total amount of invoices. It will be the total in euros of all the invoices (if there are any negative invoices they will be added as if they were positive). Amount given to two decimal points, without showing the decimal point and, aligned to the right and filled in with zeros to the left. Compulsory.
42-49	Number of data records 010	9(8)	This is a number given to no decimal points, aligned to the right and filled in with zeros to the left. Compulsory.
50-59	Total number of data records	X(10)	This is a number given to no decimal points, aligned to the right and filled in with zeros to the left. It contains the total of records contained by the block, including that of the header and totals. Compulsory
60-72	Free	X(13)	Blanco

Annex 1

Supplier Reference

The supplier reference shall be comprised of a valid Corporate Tax Identification Number (CIF) or by a string of 10 alphanumerical digits corresponding to a unique reference that identifies said supplier; that is:

- Valid Corporate Tax Identification Number (CIF)
- Unique / Identifying supplier reference

CODING OF UNIQUE SUPPLIER REFERENCE

The SHA1 algorithm, explained below, was used to achieve a reference that ensures the code's uniqueness:

Algorithm input data:

- Client account 63.
- Non-unique reference used by client to identify supplier, indicated in record 182.

Algorithm Output Data:

- Identifying Supplier Reference comprised of 10 positions.

ALGORITHM:

HASH variable initialisation:
HASH(0) = &H67452301
HASH(1) = &HEFCDAB89
HASH(2) = &H98BADCFE
HASH(3) = &H10325476
HASH(4) = &HC3D2E1F0

Step 1.- We create the input message by concatenating Client Account 63 and the non-unique supplier reference.

Step 2.- ConvertToWordArray Function
We add bit "1" to the input message
We add k "0" bits to the message, where k is the minimum >= 0, so that
Message length (in bits) is congruent to 448 (mod 512)
Complete message length as a whole number comprised of 64 bits

Step 3.- Process the message in 512-bit pieces
For each piece:
-- Divide into 16 32-bit words
-- Extend the 16 32-bit words to 8 32-bit words
for i from 16 to 79
w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) leftrotate 1
-- Initialise variables for this piece
a = HASH(0) b =
HASH(1) c =
HASH(2) d =
HASH(3) e =
HASH(4)

Main loop
for i from 0 to 79
if $0 \leq i \leq 19$ then

```
            f = (b and c) or ((not b) and d)
            k = 0x5A827999
        else if 20 ≤ i ≤ 39
            f = b xor c xor d
            k = 0x6ED9EBA1
        else if 40 ≤ i ≤ 59
            f = (b and c) or (b and d) or (c and d)
            k = 0x8F1BBCDC
        else if 60 ≤ i ≤ 79
            f = b xor c xor d
            k = 0xCA62C1D6

        temp = (a leftrotate 5) + f + e + k + w[i]
        e=d
        d=c
        c = b leftrotate 30
        b=a
        a = temp
    -- We update the HASH values

        HASH(0) = HASH(0) + a
        HASH(1) = HASH(1) + b
        HASH(2) = HASH(2) + c
        HASH(3) = HASH(3) + d
        HASH(4) = HASH(4) + e
```

Step 4.- We create the output message (+ concatenation):

OUTPUT = Last two digits (Hex(HASH(0)) + Last two digits (Hex(HASH(1)) + Last two digits (Hex(HASH(2)) + Last two digits (Hex(HASH(3)) + Last two digits (Hex(HASH(4))

OUTPUT = CAPITAL LETTERS (OUTPUT)

EJEMPLO DE CÓDIGO UTILIZADO EN VISUAL BASIC

En un Modulo Clase(Class1):

```
BEGIN
  MultiUse = -1 'True
  Persistable = 0 'NotPersistable
  DataBindingBehavior = 0 'vbNone
  DataSourceBehavior = 0 'vbNone
  MTSTransactionMode = 0 'NotAnMTSObject
END
Attribute VB_Name = "CSha256"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = True
Attribute VB_PredeclaredId = False
Attribute VB_Exposed = False
Option Explicit

Private m_lOnBits(30)     As Long
Private m_l2Power(30)     As Long
Private K(63)             As Long

Private Const BITS_TO_A_BYTE    As Long = 8
```

```
Private Const BYTES_TO_A_WORD As Long = 4
Private Const BITS_TO_A_WORD As Long = BYTES_TO_A_WORD *
BITS_TO_A_BYTE
Private Const MODULUS_BITS As Long = 512
Private Const CONGRUENT_BITS As Long = 448
Private Sub Class_Initialize()
    m_lOnBits(0) = 1              ' 00000000000000000000000000000001
    m_lOnBits(1) = 3              ' 00000000000000000000000000000011
    m_lOnBits(2) = 7              ' 00000000000000000000000000000111
    m_lOnBits(3) = 15             ' 00000000000000000000000000001111
    m_lOnBits(4) = 31             ' 00000000000000000000000000011111
    m_lOnBits(5) = 63             ' 00000000000000000000000000111111
    m_lOnBits(6) = 127            ' 00000000000000000000000001111111
    m_lOnBits(7) = 255            ' 00000000000000000000000011111111
    m_lOnBits(8) = 511            ' 00000000000000000000000111111111
    m_lOnBits(9) = 1023           ' 00000000000000000000001111111111
    m_lOnBits(10) = 2047          ' 00000000000000000000011111111111
    m_lOnBits(11) = 4095          ' 00000000000000000000111111111111
    m_lOnBits(12) = 8191          ' 00000000000000000001111111111111
    m_lOnBits(13) = 16383         ' 00000000000000000011111111111111
    m_lOnBits(14) = 32767         ' 00000000000000000111111111111111
    m_lOnBits(15) = 65535         ' 00000000000000001111111111111111
    m_lOnBits(16) = 131071        ' 00000000000000011111111111111111
    m_lOnBits(17) = 262143        ' 00000000000000111111111111111111
    m_lOnBits(18) = 524287        ' 00000000000001111111111111111111
    m_lOnBits(19) = 1048575       ' 00000000000011111111111111111111
    m_lOnBits(20) = 2097151       ' 00000000000111111111111111111111
    m_lOnBits(21) = 4194303       ' 00000000001111111111111111111111
    m_lOnBits(22) = 8388607       ' 00000000011111111111111111111111
    m_lOnBits(23) = 16777215      ' 00000000111111111111111111111111
    m_lOnBits(24) = 33554431      ' 00000001111111111111111111111111
    m_lOnBits(25) = 67108863      ' 00000011111111111111111111111111
    m_lOnBits(26) = 134217727     ' 00000111111111111111111111111111
    m_lOnBits(27) = 268435455     ' 00001111111111111111111111111111
    m_lOnBits(28) = 536870911     ' 00011111111111111111111111111111
    m_lOnBits(29) = 1073741823 ' 00111111111111111111111111111111
    m_lOnBits(30) = 2147483647 ' 01111111111111111111111111111111
    m_l2Power(0) = 1              ' 00000000000000000000000000000001
    m_l2Power(1) = 2              ' 00000000000000000000000000000010
    m_l2Power(2) = 4              ' 00000000000000000000000000000100
    m_l2Power(3) = 8              ' 00000000000000000000000000001000
    m_l2Power(4) = 16             ' 00000000000000000000000000010000
    m_l2Power(5) = 32             ' 00000000000000000000000000100000
    m_l2Power(6) = 64             ' 00000000000000000000000001000000
    m_l2Power(7) = 128            ' 00000000000000000000000010000000
    m_l2Power(8) = 256            ' 00000000000000000000000100000000
    m_l2Power(9) = 512            ' 00000000000000000000001000000000
    m_l2Power(10) = 1024          ' 00000000000000000000010000000000
    m_l2Power(11) = 2048          ' 00000000000000000000100000000000
    m_l2Power(12) = 4096          ' 00000000000000000001000000000000
    m_l2Power(13) = 8192          ' 00000000000000000010000000000000
    m_l2Power(14) = 16384         ' 00000000000000000100000000000000
    m_l2Power(15) = 32768         ' 00000000000000001000000000000000
    m_l2Power(16) = 65536         ' 00000000000000010000000000000000
    m_l2Power(17) = 131072        ' 00000000000000100000000000000000
    m_l2Power(18) = 262144        ' 00000000000001000000000000000000
    m_l2Power(19) = 524288        ' 00000000000010000000000000000000
    m_l2Power(20) = 1048576       ' 00000000000100000000000000000000
    m_l2Power(21) = 2097152       ' 00000000001000000000000000000000
    m_l2Power(22) = 4194304       ' 00000000010000000000000000000000
    m_l2Power(23) = 8388608       ' 00000000100000000000000000000000
```

```
m_l2Power(24)   = 16777216      ' 00000001000000000000000000000000
m_l2Power(25)   = 33554432      ' 00000010000000000000000000000000
m_l2Power(26)   = 67108864      ' 00000100000000000000000000000000
m_l2Power(27)   = 134217728     ' 00001000000000000000000000000000
m_l2Power(28)   = 268435456     ' 00010000000000000000000000000000
m_l2Power(29)   = 536870912     ' 00100000000000000000000000000000
m_l2Power(30)   = 1073741824    ' 01000000000000000000000000000000

K(0) = &H428A2F98 K(1)
= &H71374491 K(2) =
&HB5C0FBCF K(3) =
&HE9B5DBA5 K(4) =
&H3956C25B K(5) =
&H59F111F1 K(6) =
&H923F82A4 K(7) =
&HAB1C5ED5 K(8) =
&HD807AA98 K(9) =
&H12835B01
K(10) = &H243185BE K(11)
= &H550C7DC3 K(12) =
&H72BE5D74 K(13) =
&H80DEB1FE K(14) =
&H9BDC06A7 K(15) =
&HC19BF174 K(16) =
&HE49B69C1 K(17) =
&HEFBE4786
K(18) = &HFC19DC6
K(19) = &H240CA1CC K(20)
= &H2DE92C6F K(21) =
&H4A7484AA K(22) =
&H5CB0A9DC K(23) =
&H76F988DA K(24) =
&H983E5152 K(25) =
&HA831C66D K(26) =
&HB00327C8 K(27) =
&HBF597FC7 K(28) =
&HC6E00BF3 K(29) =
&HD5A79147
K(30) = &H6CA6351
K(31) = &H14292967 K(32)
= &H27B70A85 K(33) =
&H2E1B2138 K(34) =
&H4D2C6DFC K(35) =
&H53380D13 K(36) =
&H650A7354 K(37) =
&H766A0ABB K(38) =
&H81C2C92E K(39) =
&H92722C85 K(40) =
&HA2BFE8A1 K(41) =
&HA81A664B K(42) =
&HC24B8B70 K(43) =
&HC76C51A3 K(44) =
&HD192E819 K(45) =
&HD6990624 K(46) =
&HF40E3585 K(47) =
&H106AA070 K(48) =
&H19A4C116 K(49) =
&H1E376C08 K(50) =
&H2748774C K(51) =
&H34B0BCB5 K(52) =
&H391C0CB3
```

```
    K(53)  = &H4ED8AA4A
    K(54)  = &H5B9CCA4F K(55)
           = &H682E6FF3 K(56)
           = &H748F82EE K(57)
           = &H78A5636F K(58)
           = &H84C87814 K(59)
           = &H8CC70208 K(60)
           = &H90BEFFFA K(61)
           = &HA4506CEB K(62)
           = &HBEF9A3F7 K(63)
           = &HC67178F2
End Sub

Private Function LShift(ByVal lValue As Long, ByVal iShiftBits As
Integer) As Long
    If iShiftBits = 0 Then
        LShift = lValue
        Exit Function
    ElseIf iShiftBits = 31 Then
        If lValue And 1 Then LShift = &H80000000 Else LShift = 0
        Exit Function
    ElseIf iShiftBits < 0 Or iShiftBits > 31 Then
        Err.Raise 6
    End If
    If (lValue And m_l2Power(31 - iShiftBits)) Then LShift = ((lValue
And m_lOnBits(31 - (iShiftBits + 1))) * m_l2Power(iShiftBits)) Or
&H80000000 Else LShift = ((lValue And m_lOnBits(31 - iShiftBits)) *
m_l2Power(iShiftBits))
End Function
Private Function RShift(ByVal lValue As Long, ByVal iShiftBits As
Integer) As Long
    If iShiftBits = 0 Then
        RShift = lValue
        Exit Function
    ElseIf iShiftBits = 31 Then
        If lValue And &H80000000 Then RShift = 1 Else RShift = 0
        Exit Function
    ElseIf iShiftBits < 0 Or iShiftBits > 31 Then
        Err.Raise 6
    End If
    RShift = (lValue And &H7FFFFFFE) \ m_l2Power(iShiftBits)
    If (lValue And &H80000000) Then RShift = (RShift Or (&H40000000 \
m_l2Power(iShiftBits - 1)))
End Function

Private Function AddUnsigned(ByVal lX As Long, ByVal lY As Long) As
Long
    Dim lX4 As Long, lY4 As Long, lX8 As Long, lY8 As Long, lResult As
Long
    lX8 = lX And &H80000000 lY8 =
    lY And &H80000000 lX4 = lX
    And &H40000000 lY4 = lY And
    &H40000000
    lResult = (lX And &H3FFFFFFF) + (lY And &H3FFFFFFF)
    If lX4 And lY4 Then
        lResult = lResult Xor &H80000000 Xor lX8 Xor lY8
    ElseIf lX4 Or lY4 Then
        If lResult And &H40000000 Then lResult = lResult Xor
&HC0000000 Xor lX8 Xor lY8 Else lResult = lResult Xor &H40000000 Xor
lX8 Xor lY8
    Else
```

```
            lResult = lResult Xor lX8 Xor lY8
        End If
        AddUnsigned = lResult
End Function
Private Function Ch(ByVal X As Long, ByVal Y As Long, ByVal z As Long)
As Long
        Ch = ((X And Y) Xor ((Not X) And z))
End Function
Private Function Maj(ByVal X As Long, ByVal Y As Long, ByVal z As
Long) As Long
        Maj = ((X And Y) Xor (X And z) Xor (Y And z))
End Function

Private Function S(ByVal X As Long, ByVal n   As Long) As Long
        S = (RShift(X, (n And m_lOnBits(4))) Or   LShift(X, (32 - (n And
m_lOnBits(4)))))
End Function
Private Function R(ByVal X As Long, ByVal n   As Long) As Long
        R = RShift(X, CInt(n And m_lOnBits(4)))
End Function
Private Function Sigma0(ByVal X As Long) As   Long
        Sigma0 = (S(X, 2) Xor S(X, 13) Xor S(X,   22))
End Function

Private Function Sigma1(ByVal X As Long) As Long
        Sigma1 = (S(X, 6) Xor S(X, 11) Xor S(X, 25))
End Function

Private Function Gamma0(ByVal X As Long) As Long
        Gamma0 = (S(X, 7) Xor S(X, 18) Xor R(X, 3))
End Function

Private Function Gamma1(ByVal X As Long) As Long
        Gamma1 = (S(X, 17) Xor S(X, 19) Xor R(X, 10))
End Function

Private Function ConvertToWordArray(sMessage As String, lWordArray()
As Long)
        Dim lMessageLength As Long, lNumberOfWords As Long, lBytePosition
As Long, lByteCount As Long, lWordCount As Long, lByte As Long
        lMessageLength = Len(sMessage)
        lNumberOfWords = (((lMessageLength + ((MODULUS_BITS -
CONGRUENT_BITS) \ BITS_TO_A_BYTE)) \ (MODULUS_BITS \ BITS_TO_A_BYTE))
+ 1) * (MODULUS_BITS \ BITS_TO_A_WORD)
        ReDim lWordArray(lNumberOfWords - 1)
        Do Until lByteCount >= lMessageLength
            lWordCount = lByteCount \ BYTES_TO_A_WORD
            lBytePosition = (3 - (lByteCount Mod BYTES_TO_A_WORD)) *
BITS_TO_A_BYTE

            '*********************************************
            'Modificado
            'lByte = AscB(Mid$(sMessage, lByteCount + 1, 1))
            '*********************************************
            lByte = Asc(Mid$(sMessage, lByteCount + 1, 1))

            lWordArray(lWordCount) = lWordArray(lWordCount) Or
LShift(lByte, lBytePosition)
            lByteCount = lByteCount + 1
        Loop
        lWordCount = lByteCount \ BYTES_TO_A_WORD
```

```
    lBytePosition = (3 - (lByteCount Mod BYTES_TO_A_WORD)) *
BITS_TO_A_BYTE
    lWordArray(lWordCount) = lWordArray(lWordCount) Or LShift(&H80,
lBytePosition)
    lWordArray(lNumberOfWords - 1) = LShift(lMessageLength, 3)
    lWordArray(lNumberOfWords - 2) = RShift(lMessageLength, 29)

        '*********************************************
        'Modificado
        'ConvertToWordArray = lWordArray
        '*********************************************

    ConvertToWordArray = lWordArray

End Function
Public Function SHA256(sMessage As String) As String

   '*********************************************
   'Modificado
   'Dim HASH(7) As Long, M() As Long, w(63) As Long, A As Long, B As
Long
   '*********************************************

    Dim HASH(7) As Long, M(63) As Long, w(63) As Long, A As Long, B As
Long
    Dim C As Long, D As Long, E As Long, F As Long, G As Long, H As
Long
    Dim I As Long, J As Long, T1 As Long, T2 As Long

    HASH(0)  = &H6A09E667
    HASH(1)  = &HBB67AE85
    HASH(2)  = &H3C6EF372
    HASH(3)  = &HA54FF53A
    HASH(4)  = &H510E527F
    HASH(5)  = &H9B05688C
    HASH(6)  = &H1F83D9AB
    HASH(7)  = &H5BE0CD19

   '*********************************************
   'Modificado
   'ConvertToWordArray sMessage, M()
   '*********************************************

    M = ConvertToWordArray(sMessage, M)

    For I  = 0 To UBound(M) Step 16
        A = HASH(0)
        B = HASH(1)
        C = HASH(2)
        D = HASH(3)
        E = HASH(4)
        F = HASH(5)
        G = HASH(6)
        H = HASH(7)

        For J = 0 To 63
            If J < 16 Then w(J) = M(J + I) Else w(J) =
AddUnsigned(AddUnsigned(AddUnsigned(Gamma1(w(J - 2)), w(J - 7)),
Gamma0(w(J - 15))), w(J - 16))
            T1 = AddUnsigned(AddUnsigned(AddUnsigned(AddUnsigned(H,
Sigma1(E)), Ch(E, F, G)), K(J)), w(J))
```

```
            T2 = AddUnsigned(Sigma0(A), Maj(A, B, C))
            H=G
            G=F
            F=E
            E = AddUnsigned(D, T1)
            D=C
            C=B
            B=A
            A = AddUnsigned(T1, T2)
        Next

        HASH(0)  = AddUnsigned(A,  HASH(0))
        HASH(1)  = AddUnsigned(B,  HASH(1))
        HASH(2)  = AddUnsigned(C,  HASH(2))
        HASH(3)  = AddUnsigned(D,  HASH(3))
        HASH(4)  = AddUnsigned(E,  HASH(4))
        HASH(5)  = AddUnsigned(F,  HASH(5))
        HASH(6)  = AddUnsigned(G,  HASH(6))
        HASH(7)  = AddUnsigned(H,  HASH(7))
    Next

   '*********************************************************
   'Incluido
   '
    Dim p0 As Integer, p7 As Integer

    If Len(Trim(Hex(HASH(7)))) > 8 Then p7 = 9 Else p7 = 1 If
    Len(Trim(Hex(HASH(0)))) > 8 Then p0 = 9 Else p0 = 1

   '*********************************************************

   '*********************************************************
   'Modificado
   'SHA256 = LCase$(Left$(Hex(HASH(0)), 1) & Right$(Hex(HASH(0)), 1) &
_
   '               Right$(Hex(HASH(1)), 1) & Right$(Hex(HASH(2)), 1) &
_
   '               Right$(Hex(HASH(3)), 1) & Right$(Hex(HASH(4)), 1) &
_
   '               Right$(Hex(HASH(5)), 1) & Right$(Hex(HASH(6)), 1) &
_
   '               Left$(Hex(HASH(7)), 1) & Right$(Hex(HASH(7)), 1))

    SHA256 = LCase$(Mid$(Hex(HASH(0)), p0, 1) & Right$(Hex(HASH(0)),
1) & _
                    Right$(Hex(HASH(1)), 1) & Right$(Hex(HASH(2)), 1) &
_
                    Right$(Hex(HASH(3)), 1) & Right$(Hex(HASH(4)), 1) &
_
                    Right$(Hex(HASH(5)), 1) & Right$(Hex(HASH(6)), 1) &
_
                    Mid$(Hex(HASH(7)), p7, 1) & Right$(Hex(HASH(7)), 1))

    SHA256 = UCase(SHA256)

End Function
```