Delphi Encryption Compendium 6.0

This is the official documentation for the Delphi Encryption Compendium 6.0 (or short DEC 6.0) library.
Document version: 1.0 as of 1st January 2019

Disclaimer: while we try to keep this document updated and correct, we cannot guarantee that the content is 100% error free and/or 100% complete. If you find any issues with it please tell us so we can improve it.

Contents

1 What is DEC 6.0 and what not?

DEC is a collection of cryptographic hash functions, cipher algorithms and CRC checksum routines written in Delphi. A short description of each of those algorithm categories can be found in the next chapter. It is a careful redesign of DEC 5.2 with the aim to be better maintainable, mostly interface compatible with DEC 5.2, but also to get rid of various things hindering the use on other platforms than Win32. In short, it is an internally improved version of DEC 5.2. Since the changes were so many and big and because they do influence the interface to your code they warrant a 6.0 version number. By adding XMLDOC comments to quite a lot of the methods etc. and by writing this documentation we also wanted to make this library more accessible to the casual developer.

The minimum supported Delphi version is Delphi 2009 now for the Win32 platform and XE2 for Win64 and OS/X. Support for the Android and iOS platforms requires at least Delphi 10.1 Berlin, as in this release some previously omitted data types were added to the mobile compilers. While it might be Free Pascal (FPC) compatible in some parts, support for this compiler is still being considered experimental. If you have knowledge in FPC and want to help out making DEC more compatible then please contact us!

While DEC contains sample programs and this documentation includes a little bit of cryptography background it is not a beginner's tutorial for properly using cryptography! The authors of this library cannot and will not take any responsibility in any way for what you do with DEC.

Additionally DEC is not written with maximum possible speed in mind. It currently cannot use any hardware units of modern CPUs providing special commands for speeding up encryption and on platforms other than Win32 it doesn't use assembler. While the aim should of course be to provide decent speed, the portability and maintainability of the library is at least equally important. But if volunteers want to help with coding and improving the library who knows where it can get to?

A basic set of DUnit based unit tests is being provided as well to ensure that modifications of DEC do not break anything. While not covering 100% of all possible test cases it helped us quite a lot during development as they uncovered many failures which we could fix before releasing it.

2 A short explanation of cryptography

Cryptography in general is a way of encrypting a message in such a way that only a person with the correct key can decrypt and read it. The message thus can be transferred over some insecure communication channel without enabling an unauthorized reader to read its contents.

But cryptography is more than that and DEC not only provides algorithms for encryption and decryption of text and data.

Besides some helper routines and some formatting classes DEC provides three types of algorithms which will be explained in the next subchapters.

2.1 CRC – Cyclic Redundancy Check

CRC algorithms are usually used to calculate a checksum over some data in order to be able to find out later on whether that data has been transferred correctly or stored properly on disc. Depending on the exact CRC algorithm used it can detect one or more randomly changed bits in a data stream, but the algorithm cannot correct those. Algorithms additionally being able to correct failures up to a certain degree are called error correction codes (ECC) but those are not subject of DEC.

Since it is comparatively easy to produce two messages with different contents (called a collision in the context of cryptography) but the same CRC checksum, they are not suited for cryptographic means like storing a password in a non-reversible way or guarding against malicious alternation of the data transferred. The number range of most CRC variants is simply way too small for this.

CRCs are mostly used because they can be computed quite fast. That is even more beneficial in embedded hardware where the CPU is comparatively slower than even entry level Smartphone CPUs. Many commonly used but not all CRC polynomials are initialized in such a way that calculating the CRC over the data and the appended CRC checksum leads to a result of 0. This makes checking the CRC checksum somewhat easier.

DEC contains a variety of CRC algorithms sharing the very same call interface, which makes it really easy if it should be necessary to switch the algorithm during development of an application.

2.2 Hash functions

Hash functions are a bit like CRC algorithms as far as they are mathematical one way functions, which generate a non-reversible number from data or text given to the hash-function. The resulting number has always the same length, no matter what size the data has over which the hash has been calculated.

Since the resulting number is a quite big number, mostly 64 bit or more, the probability of collisions is significantly smaller than for CRC algorithms. Because of this hash functions are often used to prove that some text or data has not been modified or they are used to store passwords in a way

which makes it impossible to recover the original clear text of the password without brute force calculation.

If hash functions are to be used for password purposes the user would enter his password, the system would calculate the hash over it and compare that to the stored hash value of that user's password. If both match the user has entered his correct password.

The brute force password breaking approach means, that one has to calculate the hash value of all permutations of allowed password characters and compare those to the stored hash value. If the hash algorithm has been properly selected and is being properly used this should be some quite time consuming task.

Some words of caution:

1. Before using a hash function for use as one way password storage check whether there are already known attacks or collisions for that algorithm. Do not use it when there are known collisions, as this enables to enter your system with a different password than the original one as well.
2. Do not simply hash the entered password with the algorithm and store that hash. An attacker with a precomputed table of hash values for any given input will get into your system in no time. Such tables are called rainbow tables, need quite a lot of disc space, but are readily available for most well-known hash algorithms. Now what to do? Simple: add something to the password entered and which is covered by the hash as well. Best would be a value which is different for each password record you create. You can store that value along with your hash value, as it will be needed by your password check function. Another thing to do is to calculate the hash of the hash of the hash. You get it: calculate the hash over the data several times always feeding the result of the last hash calculation as input to the new one. This also defeats the direct use of rainbow tables.
3. Pick a hash algorithm which is slow to be calculated. A brute force attack will be slowed down then, especially if combined with the methods of 2.

2.3 Cipher functions

Cipher functions are algorithms which take clear text or some binary data and encrypt it, so that somebody getting hold of that encrypted data can only make sense out of it if he has the right key to decrypt it.

There are different cipher algorithms available which have different key lengths and different cryptographic strength. Of course they also differ in complexity and calculation time and block based algorithms can differ in block size.

Some of them work on blocks of data with a fixed length. They are generally called *block ciphers*. For those different padding modes are available to fill up blocks when the size of the data to be encrypted is smaller than block size or not an exact multiple of it. Some of these padding modes additionally enhance security by basing the key for the next block on the encrypted output of the

previous block. Other algorithms work with streams and are thus independent on block size. They are generally called *stream ciphers*.

DEC provides different padding algorithms, which can be used for all block based cipher algorithm implementations as they are implemented in a base class. For the sake of completeness the insecure and not recommended ECB (*E*lectronic *C*ode *B*ook) padding mode is being provided as well. DEC also provides useful wrappers which will e.g. allow working with TStream descendants even for block ciphers.

Before using any of the ciphers provided check whether they are suitable for your intended purpose:

1. Do you need compatibility to some other software?
2. Which security level is needed?
3. Check whether the algorithm you want to select is already known as broken! We cannot guarantee that a given algorithm is not yet broken. If we should already know about it we will document this of course.
4. If your software is to be used in different countries, check whether an algorithm of the selected strength is allowed in your target countries, as some forbid strong cryptography. I do not mean the old and luckily dead 40 bit US export cryptography limit.

2.4 Random number generator

For various cryptographic related functions good random numbers are required. Computer can only generate pseudo random numbers in software (Pseudo Random Number Generator, PNRG). A good PNRG needs to have an even distribution of the output values.

Delphi itself includes a PNRG in the system unit, which is automatically included into all your units. This PNRG can be used by calling the `Random(x)` method. Be aware that you need to initialize this by calling `Randomize` first! Otherwise it might always produce the same sequence of random numbers.

DEC also contains a PNRG for a certain class of algorithms. The main purpose of that is to stay independent of any changes made to Delphi's `Random` function.

3 DEC explained in detail

3.1 Installation

If you fetch your copy of DEC via *Tools/GetIt* the following instructions do not apply to you.

Since DEC does not provide any components installing it is quite simple. Just unzip your downloaded DEC distribution into some empty folder. Make sure to keep the directory structure intact.

Afterwards open *Tools/Options* in the Delphi IDE. Navigate to *Delphi options*. Click on *Library* and add the directory you just unzipped DEC into as new library path.

Now you should be able to add any of the DEC units to your uses clause and start to use it in your project.

We recommend using a separate directory for each Delphi version you have installed on your computer, so Delphi cannot mess up any dcus created etc.

3.2 Structure

DEC 6.0 contains the following parts/directories:

\Docs
Contains all the documentation, including the one you are currently reading. If you need help using DEC please look at the provided docs first.

\Source
This directory contains the units of DEC in source code form. So everything is transparent to you.

<einzelne Units [= Zweck] grob erklären? Oder eigenes Kapitel dafür?>

\UnitTests

In order to ensure that DEC properly works and that any change we should make to its source code still produces a properly working version of DEC we created a bunch of DUnit unit tests. Additionally we try to be DUnitX compatible with our tests. We currently simply prefer DUnit because DUnit is included with older Delphi versions already and it has a nice and helpful GUI runner, which DUnit X so far still lacks if we're not mistaken. It also hast a test case skeleton generator built into an IDE wizard.

You should be able to load the UnitTest Project group, compile and run it. You can select between `DUnit` and `DUnitX` by enabling or disabling the `DUnitX` define. In order to enable it remove the . in front of the $ sign. To disable it, add the . again.

With this unit test project you should be able to verify that the version of DEC you are using passes all tests. The tests mostly cover the basics only so these are not a 100% guarantee that DEC is bug free, but those tests already helped us quite a lot while reshaping DEC!

Those users knowing the old distribution might know the old test application using the test vectors (test data) from a text file. We not only converted this hard to read application into unit tests, we also added tests for areas not covered yet, e.g. for the CRC routines.

\Demos

This directory contains some simple demo projects aimed to help you getting started with DEC.

The following demos are currently available:

Demo	Purpose
Format_Conmsole	Simple demo of how to use the DEC formatting classes. In the example TFormat_Hex is used.
Hash_Console	Simple demo of how to use the DEC hash classes. In the demo the RipeMD160 algorithm is used showing that our implementation produces the same hash output as the official website.
Cipher_Console	Simple demo of encrypting a string with the DES algorithm and successfully decrypting it.
Hash_FMX	Simple cross platform demo for the hash classes. Allows any of the available hash classes to be used, thus showing the class list mechanism and allows for the selection of the input and output encoding to be used.
Cipher_FMX	Simple cross platform demo for the cipher classes. Allows any of the available cipher classes to be used, thus showing the class list mechanism and allows for the selection of the input and output encoding to be used.
Crypto Workbench	A quite extensive workbench containing lots of useful functions for dealing with cryptography, like encrypting/decrypting a file, generation of hashes via various sources like files or strings and much more. Serves as a full featured but comparatively big VCL based demo.

3.3 Using DEC

3.3.1 The DEC base class

All classes of DEC derive from a common base class *TDECObject*. This class is implemented in *DECBaseClass.pas*. Most of its methods are class methods, so they can be directly called on a class reference without requiring an object reference. But of course they can be called on a proper object reference as well. Most deal with DECs class registration mechanism, which is described in detail in chapter *3.4 The class registration mechanism*. You usually do not have much if any contact with this class unless you work on the DEC code base.

Method	Purpose
Identity	This class method delivers a number which should be unique of a class derived from this base class. You can store this number in a file to encode the hash- or cipher algorithm used for creating this file and by using the appropriate registration mechanism you can later on quite easily create the required hash or cipher instance needed based on this identity.
FreeInstance	This method is only available if use ASM routines in DECOptions.inc has been turned on. It has to do with safely clearing memory on its release by overwriting it with zeroes.
SelfTest	???
RegisterClass	Adds the class reference to the global list of registered classes which is passed as parameter. This method is usually not called in user code, as each relevant DEC class is already being registered in the initialization section of the unit implementing the class.
UnregisterClass	Removes the class reference from the global list of registered classes which is passed as parameter. This method is usually not called in user code, as each relevant DEC class is already being unregistered in the finalization section of the unit implementing the class.
GetShortClassNameFromName	Returns the short class name of a class name being passed as parameter. For instance the short class name of *TCipher_Skipjack* is *Skipjack*.
GetShortClassName	Returns the short class name of this class.

3.3.2 Using the formatting routines

Why do we start our tour through the DEC libraries with the formatting routines? That's simple: because they can be used together with all other categories of routines. They are being used to format data in various ways and to pass that to the other methods and functions or to convert the data returned by those into one of the provided standard formats. And sometimes it's simply helpful to have a quick way to display a hexadecimal representation of returned binary data to check something while debugging.

All the provided formatting classes have a common ancestor: *TDECFormat*.

The formatting classes provide their complete functionality in form of class procedures and class functions, so you never need to create an instance of a formatting class.

The following methods are being provided:

Method	Purpose
Encode	Formats a given byte array into the format of the formatting class. The output is a byte array. Two deprecated overloads for use with RawByteString and untyped data are being provided as well. These overloads have a RawByteString as result.
Decode	Formats a given byte array in the format of the formatting class back into the original format. Output is a byte array.
IsValid	Checks whether the data passed to it is valid for that particular formatting. This is useful as some formats only allow a certain range of input values.
UpCaseBinary	This method works similar to the *UpCase* routine of *system.pas* with the following differences: it only works for the character range a-z and input and output are not a char but a byte instead.
TableFindBinary	This method looks for the first occurrence of a given byte within a given byte array. If the byte has been found the index within the byte array is being returned, otherwise -1 is returned.

List of provided formatting classes

Format class	Format / purpose
TFormat_Copy	This class doesn't apply any formatting change on the data passed in. It can be used in places where a formatting class is being expected but when you do not want to have any format change applied.
TFormat_HEX	Converts the input into hexadecimal representation. One byte of the input will be converted into a two bytes hex representation. Be aware that Unicode strings are UTF16 encoded, which means that each character you see in the string consists at least of 2 bytes, even if it is in the ASCII range. The 2nd byte will simply be 0 in that ASCII case. The letters A-F in the hexadecimal representation will be uppercase A-F characters.
TFormat_HEXL	The same as format *TFormat_HEX*, just with lower case letters a-f.
TFormat_Base16	Alias for *TFormat_HEX* for compatibility reasons.
TFormat_Base16L	Alias for *TFormat_HEXL* for compatibility reasons.
TFormat_DECMIME32	This is a special format created by Hagen Reddmann, the original author of DEC. We do not recommend using this one, as it will only be compatible with DEC itself!
TFormat_Base64	This format converts 8 bit bytes into some code page invariant ASCII representation. Means: each input byte will be encoded in su8ch a way that it can be written with an ASCII character which is encoded the same on all ASCII DOS or ANSI codepages since it belongs to the 7 bit ASCII range. While this means you can transmit such binary data with an ordinary e-mail application within the message body it also means, that data encoded with this scheme requires a bit more space as from each bytes of the Base64 representation only the lower 7 bit can be used.
TFormat_MIME64	Alias for *TFormat_Base64* for compatibility reasons.
TFormat_Radix64	This is a variant of *TFormat_Base64* used in the OpenPGP context.

	It is basically a *TFormat_Base64* with an added 24 bit checksum.
TFormat_PGP	Alias for *TFormat_PGP* for compatibility reasons.
TFormat_UU	The UUEncode formatting is slightly similar to Base64. From the name it is Unix to Unix and is being used to transfer binary data via e-mail. 24 bit of input are being re-encoded into 4x 6 bit. For this only the ASCII characters 33 to 96 are being used.
TFormat_XX	This format is quite similar to *TFormat_UU*. It just further reduces the characters used to encode the binary data to just the letters, digits and the plus and minus sign. This shall reduce the danger that some application somehow interprets special characters as something else and thus ruins the encoding.
TFormat_ESCAPE	This is a variant of the Hex format but with the addition that certain characters are treated as escape characters.

In addition to the methods listed above the formatting classes do have this class variable, which they inherit from their base class:

ClassList – this public class variable contains the hash algorithm registration list, which provides access to all hash classes. For details about the registration mechanism see chapter *3.4 The class registration mechanism*

3.3.3 Using the CRC algorithms

The CRC algorithms are located in the *DECCRC* Unit. There are two sorts of routines being provided. The first and easier to use ones calculate the CRC value in one single step and are thus most suited for smaller amounts of data to be processed, as any progress reporting during their runtime is not possible.

There exist the following 4 variants:

- *CalcCRC* with a buffer as parameter. Pass in any array or TBytes type you like and pass a parameter telling how many bytes from that buffer, starting at its beginning, go into the CRC calculation.
- *CalcCRC* with a callback as parameter. As callback you need to pass a method having an untyped buffer as var parameter and an Int64 typed size parameter specifying how many bytes from the beginning of your buffer parameter will go into the CRC calculation. The *CalcCRC* routine will call your callback as often as needed until it has *Size* bytes for calculating the CRC.
- *CRC16* is a variant which does not let you specify which algorithm to use. It will use the IBM/ARC/MODBUS RTU CRC16 algorithm.
- *CRC32* is a variant which does not let you specify which algorithm to use. It will use the CRC32-CCITT algorithm. It works on an untyped *Buffer* parameter and processes *Size* bytes of that buffer, beginning at the start of it.

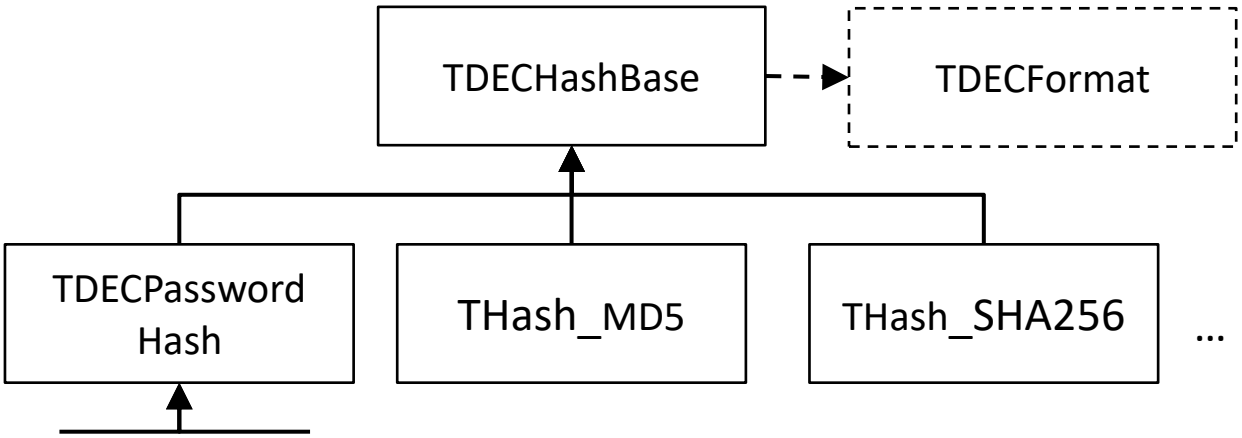
The other sorts of routines split the CRC processing into several steps and thus they give you finer control about what to do at a given place in your code.

Caution: when using the CRC16 or CRC32 functions in a multithreaded application, you need to call *CRCInitThreadSafe* first!

3.3.4 Using the hash algorithms

3.3.4.1 Base structure of the hash algorithms

The hash algorithm classes have a mostly common API. Parts of this API are implemented in abstract ancestor classes. For future use a *TDECPasswordHash* class has been introduced. All hash algorithms specifically well suited for password hashing will inherit from this one. As of now DEC does not contain any specific password hashing classes. The following diagram illustrates this:



In order to make it easy to find out whether a given hash class is specifically designed for password hashing, all hash classes contain a class function named *IsPasswordHash*. This method checks, whether the class inherits from *TDECPasswordHash*.

3.3.4.2 Methods for using the hash classes

Since all the hash classes inherit from TDECHashBase, they mostly share a common API for using them. Exceptions to this rule will be explained in the next chapter.

Method	Purpose
Init	This method needs to be called directly before each hash value calculation. It initializes the properties of the algorithm and clears all required buffers with default values.
Done	Finalizes hash calculation and clears the buffers used in a safe way to prevent stealing of data. Must be called at the end of each hash value calculation.
Calc	Calculates the hash value over a chunk of data.
DigestAsBytes	Returns the calculated hash value as TBytes byte array.
DigestAsString	Returns the calculated hash value as an Unicode string. If one of the formatting classes is being passed via the optional *Format*

	parameter this formatting is being applied to the return value, e.g. you can get the hash value hex formatted this way for instance. If no formatting is being passed, the returned string is simply the interpretation of the calculated hash value bytes as a string. In case of an UnicodeString, which is being returned here, the result might be undesired.
DigestAsRawByteString	Returns the calculated hash value as a *RawByteString*. If one of the formatting classes is being passed via the optional *Format* parameter this formatting is being applied to the return value, e.g. you can get the hash value hex formatted this way for instance. If no formatting is being passed, the returned string is simply the interpretation of the calculated hash value bytes as a string.
DigestSize	Returns the length of a calculated hash value in bytes.
BlockSize	Returns the size of a data block in bytes. The data given to the hash algorithm is being processed in blocks of this size internally and if the data does not fill the last block completely it will be automatically filled with the *PaddingByte* specified.
ClassByName	Will most likely get removed as *ClassList* provides this already.
ClassByIdentity	Will most likely get removed as *ClassList* provides this already.
IsPasswordHash	Returns true if this class implements a hash algorithm particularly designed for hashing passwords.
CalcBuffer	Calculates the hash value over a given buffer of data. The size of the buffer in bytes needs to be specified as well and the result is the calculated hash value as *TBytes* array.
CalcBytes	Calculates the hash value over a given *TBytes* buffer of data. The result is the calculated hash value as *TBytes* array.
CalcString	Calculates the hash value over a string. There exist two overloads: one for Unicode strings and one for *RawByteStrings*. Both have an optional parameter where you can pass a formatting class. The formatting will be applied to the calculated hash value, e.g. you can get the hash value hex formatted this way for instance. If no formatting is being passed, the returned string is simply the interpretation of the calculated hash value bytes as a string. In case of an UnicodeString, which is being returned here, the result might be undesired.
CalcStream	Both overloads of this method calculate the hash value over the contents of a stream. The stream may be a file stream or a memory stream or any other kind of stream. You have to specify the size of the stream as a parameter. One of the overloads returns the hash value as a *RawByteString* return value and for this it contains an optional format parameter for passing a formatting class used to format the output. The other one contains a *TBytes* parameter where it will return the calculated hash value in. There cannot exist overloaded methods in Delphi which only differ in the data type of the return value. The last parameter is optional. You can supply a callback method here which will be called by the method to report calculation progress. This is especially useful for big sized data, as you can display the progress of the operation via this callback method. Be aware though, that if the hash method is running in the application main thread any message pump required for updating display

	controls might not be run. So if calculating hash values over large amounts of data and wishing to display progress you should run the hash calculation in a separate thread. This allows display updates to work and keeps your main thread responsible.
`CalcFile`	Both overloads of this method calculate the hash value over the contents of a file. The file is specified by its path and file name. One of the overloads returns the hash value as a *RawByteString* return value and for this it contains an optional format parameter for passing a formatting class used to format the output. The other one contains a *TBytes* parameter where it will return the calculated hash value in. There cannot exist overloaded methods in Delphi which only differ in the data type of the return value. The last parameter is optional. You can supply a callback method here which will be called by the method to report calculation progress. This is especially useful for big sized data, as you can display the progress of the operation via this callback method. Be aware though, that if the hash method is running in the application main thread any message pump required for updating display controls might not be run. So if calculating hash values over large amounts of data and wishing to display progress you should run the hash calculation in a separate thread. This allows display updates to work and keeps your main thread responsible.
`MGF1`	Beide Overloads
`KDF2`	Beide Overloads
`KDFx`	Alle Overloads

In addition to the methods listed above the hash classes do have this class variable, which they inherit from their base class:

`ClassList` – this public class variable contains the hash algorithm registration list, which provides access to all hash classes. For details about the registration mechanism see chapter *3.4 The class registration mechanism*

All classes also have this common property:

`PaddingByte` – the value assigned to this byte is being used to fill up data passed to the hash algorithm if the data does not completely fill the last block. Means: if the size of the data passed cannot be divided by `BlockSize` without reminder.

3.3.4.3 Exceptions to the common API for the hash classes

There are a few hash classes which provide additional API methods or properties. The following paragraphs list those.

THash_Haval128, THash_Haval160, THash_Haval224, THash_Haval256 and THash_Tiger

All of them have an additional property *Rounds*. Both algorithms use several rounds of calculation where the result of the preceding round will be the input for the next round. This property sets the number of rounds to use.

For the *THash_Tiger* class the minimum number of rounds is 3 and the maximum accepted number is 32.

For the *Haval* algorithms the allowed number of rounds is between 3 and 5. If a number outside this range is assigned, the number actually picked depends on the *DigestSize* set. For a *DigestSize* of 20 or lower it will be 3 rounds, for *DigestSize* 28 or lower but bigger than 20 it will be 4 rounds and for values bigger 28 it will be 5 rounds.

THash_Snefru128 and THash_Snefru256
This one has a property called *SecurityLevel*, which is nearly the same as the rounds property of THashHaval

THash_Sapphire
This one has a property *RequestedDigestSize*. With this you can define how many bytes of the calculated hash value will be returned via the *DigestAsBytes* method. The *Digest* method is not affected by this. Values bigger 64 do not make sense, as the hash value is only 64 byte long. If the *RequestedDigestSize* is set to 0 the default value of 64 byte is being used.

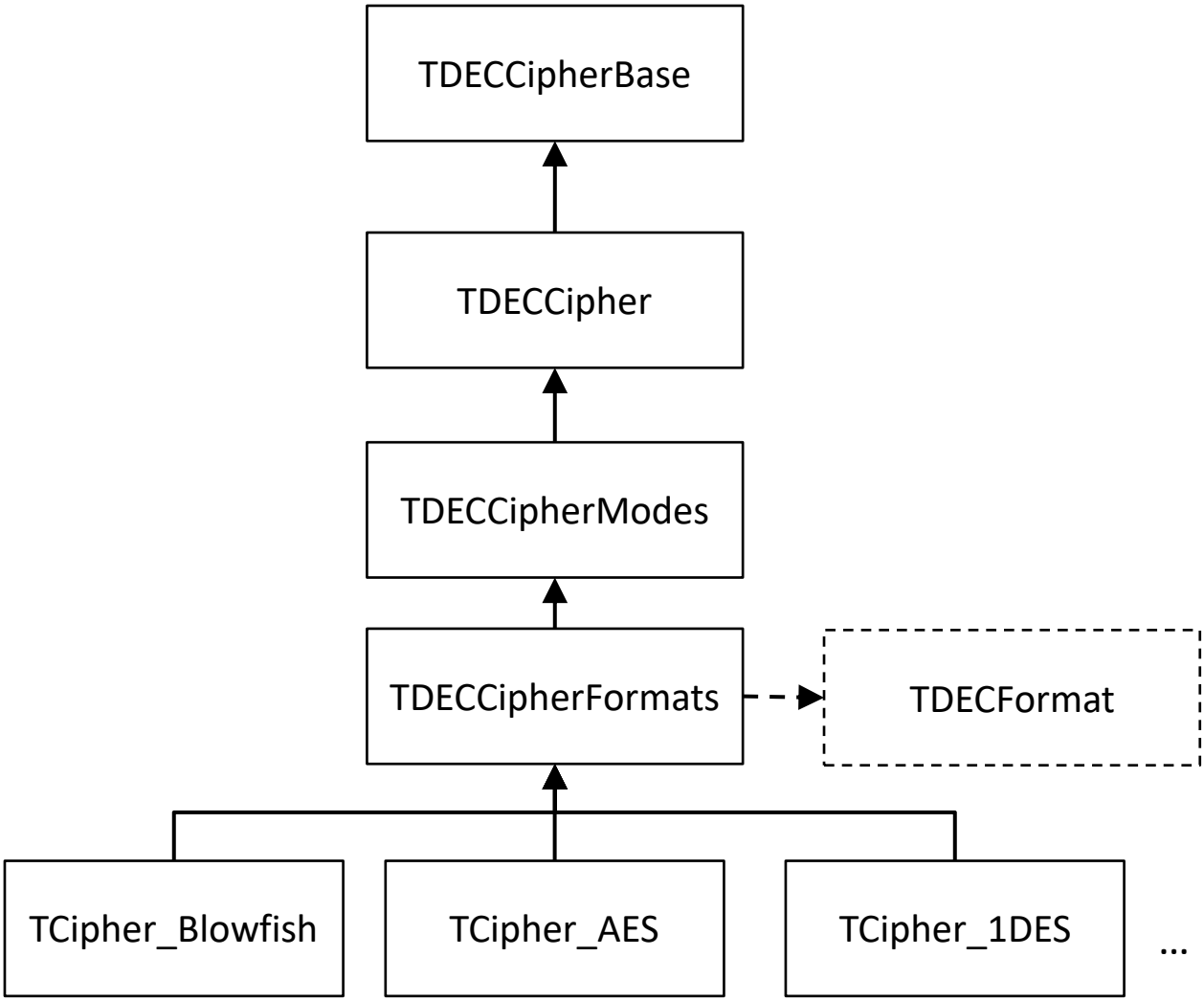
3.3.5 Using the key deviation algorithms

Key deviation algorithms are used for deriving further keys from already existing keys. A simple scheme for deriving a 2nd key from of a first one could be to calculate the hash sum of the first key via some well-defined hash algorithms. If a 3rd key is needed, one would simply calculate the hash sum on the 2nd key, using the same algorithm. That way nobody can tell whether different keys descend from each other by just looking at the keys.

3.3.6 Using the cipher algorithms

3.3.6.1 Base structure of the cipher algorithms

The cipher algorithm classes have a mostly common API. Parts of this API are implemented in abstract ancestor classes. The following diagram illustrates this:



TDECCipher

This is the abstract base class for all cipher implementations. Many of the cipher algorithms are block ciphers, which means that they work on equally sized blocks of data. Often on blocks of 8 or 16 byte size. *TDECCipher* only provides abstract methods for encrypting and decrypting a single block of data. The individual cipher classes will override those abstract methods in order to actually provide the encryption/decryption functionality.

⚠ Do not inherit directly from this class if you want to add additional block ciphers, as not using one of the chaining methods from *TDECPaddedCipher* will result in vulnerable encryption for any data larger than the block size of the algorithm used!

TDECCipherModes

If you want to encrypt data larger than the block size you need to chain blocks. For this several methods have been developed which normally carry over information from one block to another, so the following blocks are dependent on their preceding block. This is being done to make it harder to crack the encryption. If somebody cracks the encryption of one block, he cannot necessarily decrypt any of the previous blocks. Another necessity is to fill up the last block if it is not completely filled with data. This happens when your data doesn't match block size. Filling up is called padding.

Both kinds of operations, padding and block chaining, are implemented in the *TDECCipherModes* class.

TDECCipherFormats

All the methods for encrypting and decrypting data which do not directly work on blocks of data but on *TStreams*, strings or files are added in the *TDECCipherFormats* class. All cipher algorithm classes like *TCipher_AES* inherit from it in order to be able to provide these comfort methods without needing to implement those all over again. When adding further ciphers in form of additional classes they always need to inherit from this class.

TDECFormat

This is the abstract base class for the formatting classes. The methods in *TDECCipherFormats* provide an optional class reference parameter of this type. It can be used to pass a concrete formatting class to be used in that encoding or decoding method.

Ciphers

The actual implementations of the ciphers currently provided are in *DECCiphers.pas*. In order to encrypt or decrypt data include this unit in your uses clause and create a concrete instance of one of the cipher classes contained in it. If you are free to choose which cipher algorithm to use, be sure to read our comments found in the summary XMLDOC comments, as we try to point out algorithms which are being considered as unsafe nowadays. Such algorithms are only being provided for backward compatibility.

3.3.6.2 Picking the right block chaining method

The following padding methods do exist. Each is shortly being described in order to allow you to pick the most suitable for your task.

3.3.7 Using the random number generators

3.3.8 Useful helper routines

3.3.9 DECOptions.inc

The *DECOptions.inc* include file contains a few global defines which influence how DEC works. Most of those should be left alone as they are needed to proper function of DEC on different platforms.

If you want to disable some define simply put a . between the { and the $.
Example: *{.$DEFINE NO_ASM}*

To enable a disabled define simply remove the . between { and $.

Those defines which may be enabled or disabled without problems are in the section titled “User configuration”. These specifically are:

- *{$DEFINE AUTO_PRNG}*, when used DEC always uses his own pseudo random number generator instead of the Delphi standard *random* function.

- *{$DEFINE NO_ASM}*, when used none of the assembler versions of the routines are used. Only pure Pascal implementations are used then. If you want to use DEC on a non Win32 platform this define needs to be on! On Win32 disabling the define can give you some smaller speed gains.

- *{.$DEFINE DEC52_IDENTITY}*, when used this DEC version uses the same identity identifier value DEC 5.2 used. This enables to read files created with DEC V5.2 which used that identity identifier.

- *{.$DEFINE DEC3_CMCTS}*, when enabled the CTS3 block cipher mode is made available. It is not recommended to be used, since it is a less secure mode! This option is only there for cases where one needs to deal with data which has been encoded with the *cmCTS* mode of DEC V3.0.

- *{.$DEFINE FMXTranslateableExceptions}*, enable this if you intend to use DEC in a Firemonkey mobile project and want to be able to translate the exception messages without needing to capture the exceptions.

-

3.3.10 Translating exception messages

By default all exception messages used by DEC have been declared as resource strings.

On Win32/Win64 resource strings are stored in special tables inside the generated exe-file automatically and most application translation tools are able to pick them up and provide some mechanism for translating those. This works equally well for VCL and for Firemonkey (FMX) applications.

Firemonkey on the other hand doesn’t support this scheme on mobile platforms. On those resource strings do compile but are treated as normal string constants. Translation tools are not able to replace them, unless the places where they are displayed on screen are wrapped into a call of the *Translate* function from *FMX.Types*.
In order to fix this, the *FMXTranslateableExceptions* define must be enabled. This enables special constructors for the *EDECException* class and its descendants. Those will use the defined resource strings but feed them to the FMX *Translate* function before assigning them to the exception class.

Your translation tool still might not identify those texts (some do) as it would be complicated for it to follow your source, but they usually allow to manually add texts to be translated. The output of such tools will be a *.lng file* usually, which you load into a *TLang* component you place on your main form. That component will provide all texts to your components and for the translate function of *FMX.Types*.

3.4 The class registration mechanism

The classes *TDECHash*, *TDECCipher* and *TDECFormat* do contain a registration mechanism where all descendant classes are registered as meta classes in a generic list. This mechanism is helpful when you build an application which shall contain a list of algorithms to pick from, so you can dynamically list the available algorithms and create instances of those. All those classes inherit this mechanism from the *DECBaseClass* unit, where it is implemented in *TDECClassList*.

Each of the formatting, cipher or hash classes is being registered into the appropriate class list in the initialization section of the und implementing the particular class. The class list is implemented as a generic *TDictionary* and provided as a public *class var* of the base class of the formatting, cipher or hash classes. Each class type is registered with a property called *identity* as key. This identity is a unique *Int64* number specifying the class. You may for instance store this number in the header of some encrypted file to record with which algorithm it was encrypted. Besides the ability to loop through all registered class types in the list, the mechanism provides two methods for searching a class type reference:

- *ClassByName* – searches for a given long or short class name. Examples: *TDECFormat_HEXL* is a long name or *HEXL* would be the short name. If such a class is registered in that list the class reference will be returned and you can call the *Create* constructor on this to create an object reference of this type returned. If no class with such a name is registered an exception is being thrown.
- *ClassByIdentity* – searches for a given unique ID. If a class with the given *Identity* is registered in that list the class reference will be returned and you can call the *Create* constructor on this to create an object reference of this type returned. If no class with such a name is registered an exception is being thrown.

It is also helpful if you have some data which describes the algorithm used by its DEC identity value. With the list you can find the correct class and create the necessary instance.

Example:

```
Uses
  Generics.Collections, DECHashBase;

var
  MyClassRef : TPair<Int64, TDECClass>;
  Identity : Int64;
begin
  Identity := 123;
  If TDECHash.ClassList.TryGetValue(Identity, MyClassRef) then
    ShowMessage(MyClassRef.Value.ClassName);
end;
```

If you like to search for a class reference by its ClassName, you can use the `ClassByName` class function of the corresponding base class.

Example for finding a class reference and creating an object instance from it:

```
Uses
  DECHashBase;

var
  Hash:TDECHash;
begin
  Hash := TDECHash.ClassByName('THash_MD5').Create;
  try
    Hash.Init;
  finaly
    Hash.Free;
  end;
end;
```

The class type list mechanism allows for registering and unregistering new classes at runtime and it is implemented in such a way that if the DEC Unit implementing a registered class type is being unloaded because it belongs to a package which is being unloaded, the class type will be unregistered. This prevents you from retrieving class references of classes no longer available from a registration list. You cannot try to create an object reference from it and cause an access violation because the class implementation is no longer available.

3.5 Extending DEC

This chapter describes what to consider when adding new formatting, cipher or hash classes to DEC. If you do extend DEC in any way it would also be nice if you would send us your source code modification so we can add it to the next release if deemed useful for the general audience of DEC! Of course we will mention you in the DEC hall of fame: the list of contributors!

And remember: whatever you add needs to have unit tests implemented by you!


If you add a new formatting class, a new hash class or a new cipher class do not forget to register it via the RegisterClass class procedure as otherwise demo applications will not automatically pick it up.

3.5.1 Adding new ciphers

New cipher classes added to DEC should always descend from *TDECPaddedCipher* from the *DECCipherPaddings* unit. They need to provide at least implementations for the following methods, from *TDECCipher* from the *DECCipherBase* unit. This means they need to be overwritten:

- *DoInit*
- *DoEncode*
- *DoDecode*

While you can overwrite the *Encode*, *Decode* and the protected *EncodeXXX/DecodeXXX* methods from *TDECPaddedCipher* you normally do not need to. This would be rather uncommon.

After implementing your new cipher class it is good practice to implement the basic set of unit tests for it as well. Simply look at the unit tests already available for the other cipher classes and follow their structure.


If you add some new cipher algorithm we would like to know about it and it would be nice if you could share it with us so it becomes part of the standard version of DEC.

3.5.2 Adding new cipher paddings


If you add some new cipher padding algorithm we would like to know about it and it would be nice if you could share it with us so it becomes part of the standard version of DEC.

3.5.3 Adding new hash algorithms


If you add some new hash algorithm we would like to know about it and it would be nice if you could share it with us so it becomes part of the standard version of DEC.

3.5.4 Adding new formatting classes


If you add some new formatting algorithm we would like to know about it and it would be nice if you could share it with us so it becomes part of the standard version of DEC.


When adding a new formatting class make sure it only contains class functions / class procedures and class vars. Otherwise some places where your class is being used in DEC might not function, as DEC expects not to work on object instances of these formatting classes but on the class itself via class methods.

3.5.5 Adding new CRC variants

If you add some new CRC polynomial we would like to know about it and it would be nice if you could share it with us so it becomes part of the standard version of DEC.

Please ensure you have valid test data for the new CRC variant you would like to add before actually doing so. Just adding new variants without proper unit tests does not help anybody.

Adding a new CRC variant requires to add a new enumeration value to the `TCRCType` type in `DECCRC.pas`. The enumeration value should be added at the end. It further requires adding an entry to the `CRCTab` constant. The entry should be added at the end of the table. The entry consists of the polynomial value, the number of bits the CRC operates on, the start value with which the CRC is to be initialized and ???

After adding the necessary definitions to the `DECCRC` unit you need to add a unit test for it. To do so open the `TestDECCRC` unit and add a nthe following new published methods XXX

3.5.6 Adding unit tests

There are unit tests available for nearly all methods etc. shipping in the default DEC distribution. These unit tests have been written in a way that they can run as *DUnit* tests and as *DUnitX* tests as well. This has been done because *DUnit* still has the better GUI test runner, while *DUnitX* tests can basically be run on other platforms as well.

For this there are two unit test projects provided. One for *DUnit* and one for *DUnitX*. If you want to switch between those you need to either define or undefine the *DUnitX* define in *defines.inc* of the unit tests. Otherwise you will get compilation and/or runtime errors.

4 Demos

In order to make your life easier, DEC ships with some demo applications. This chapter lists them and their purpose.

- Hash_FXM
  This is some simplistic demo of the use of DECs hash algorithms paired with the use of the formatting classes. You can pick some hash algorithm to use, pick the input and output formatting and after entering an input value you click the *run* button and get the hash value of your input.
-

5 Overview of changes made between DEC 5.2 and 6.0

This chapter describes the most important changes made between DEC 5.2 and DEC 6.0. It is only important to users already having used DEC 5.2 who want to update to DEC 6.0 now.

The main changes are:

- The names of all units have been changed to more verbose ones making them clearer. New units have been added to better structure the code. In some cases things have been divided in a base unit, implementing base functionality shared by all algorithms and defining the basic public API of the individual implementing classes, and another unit with the actual implementations of the actual algorithms. This is the case for the formatting routines, the ciphers and the hashes.

- The directory structure has been changed with DEC_Part_II having been removed. That was a DCU only compilation of some advanced algorithms coded by the original author of DEC. But only DCUs for Delphi 7 were shipped, so it was not of use for most DEC users anymore. We do not have the code of these units.

- The use of assembler within the library has been made optional and it also has been cut back at a few places where it really did not bring much if any speed improvements. If you want to turn on the use of assembler you have to change the conditional define in the *DECOptions.inc* include file. Be aware that you lose cross platform compatibility (even with 64 bit Windows!) by doing this.

- All uses of `PAnsiChar` have been replaced, since that data type is not available on mobile compilers and most likely will never be.

- Various methods using `TBytes` as buffer for binary data have been introduced. Since Delphi XE7 there is improved support for handling dynamic arrays e.g. by providing support for `Insert`, `Delete` and `Concat` on them. Now there is no longer any need to use string like data types for storing binary data. Back in the ANSI days it was simply convenient, as ANSI based strings provided this functionality usually without data loss.

- All methods which used the data type *Binary* have been changed to directly use `RawByteString` and their name also changed to reflect this. But at the same time they have been deprecated in favour to the `TBytes` oriented methods.

- Some more CRC variants have been added after looking up whether the already commented out data was correct.

- Some basic Demos have been added.

- DUnit tests are now being provided for the formatting classes, the CRC-, hash- and crypto-algorithms.

- The register method used when creating non-visual components based on DEC has been removed as we decided that support for components would be too much of a hassle.

- A way to easily get the exception messages translated on Firemonkey mobile projects has been implemented. For using it you must enable the *FMXTranslateableExceptions* define in *DECOptions.inc*.

- A new class method *IsPasswordHash* has been introduced to the hash classes. Currently this will always return false as we do not have any classes which inherit from the new *TDECPasswordHash* class yet. But in future versions this can be used to easily find out if a certain hashing class is particular designed for hashing passwords.

- The Cipher context record got a new field *CipherType* added. This is a set and can be used for easily finding out some properties about the cipher algorithm like whether this is a block algorithm or a stream algorithm, whether it is symmetric or asymmetric. Be aware that DEC 6.0 doesn't contain asymmetric ciphers yet.