The ECDSA-128 Library version 1.1

Email: witeg@mail.com
Homepage: http://www.witeg.prv.pl

Introduction:

Elliptic Curve DSA (ECDSA) is one of the digital signature schemes which operates on elliptic curve group. Elliptic curves used in cryptography are defined usually over GF(p) , where p is “big” prime number, or over GF(2^m).
The ECDSA-128 is an ECDSA implementation written in pure assembly language, using GF(p) with paramaters size choosen to be secure for ie. software serial verification, but NOT intended to give even moderate security for high-value e-commerce.
The length of a key, in bits, for a conventional encryption algorithm (like DES or AES) is a common measure of security. The ECDSA-128 library works over 128-bit prime field, what provide security equivalent to 64-bit AES key.
The ECDSA-128 Library uses an elliptic curve verifiably at random – *RandomCurve1-P128-WiteG*.

```
RandomCurve1-P128-WiteG:
p    340282366920938463444927863358058659863
seedE     0x9E39F75ADE0AE5CFDBE0BD847F7B7EAFC484C48F
r    0x5E0AE5CFDBE0BD847F7B7EAFC484C48F
a    -3
b    103744651967215942079424252318256895516
xG   0x504E0BD39A2B41A161174BA8FD79309F
yG   0x9A45FA6D7279A790BB0D8845D469DED4
n    340282366920938463450938462077435853809
h    1
```

Exported functions:

The **ECDSA_Keygen** function generates ECDSA public/private key-pair.

BOOL ECDSA_Keygen(
    [OUT] **LPTSTR** *lpPubKey*
    [OUT] **LPTSTR** *lpPrvKey*
);

Parameters:
lpPubKey
    Points to the buffer to receive the null-terminated string containing ECDSA public key, at least 45 bytes.
lpPrvKey
    Points to the buffer to receive the null-terminated string containing ECDSA private key, at least 25 bytes.

Remarks:
lpPubKey and *lpPrvKey* should be distinct.

Return Value:
If the function succeeds, the return value is TRUE. If the function fails, the return value is FALSE.

The **ECDSA_Sign** function is used to sign a piece of data using given private key.

BOOL ECDSA_Sign(
    [IN] **LPTSTR** *lpPrvKey*
    [IN] **BYTE** **pbMessage*
    [IN] **UINT** *dwMessageLen*
    [OUT] **LPTSTR** *lpSignature*
);

Parameters:
lpPrvKey
    Points to the the null-terminated string containing ECDSA private key.
pbMessage
    The address of the data to be signed.
dwMessageLen
    The number of bytes of data to be signed.
lpSignature
    Points to the buffer to receive the null-terminated string containing ECDSA signature, at least 45 bytes.

Return Value:
If the function succeeds, the return value is TRUE. If the function fails, the return value is FALSE.

The **ECDSA_Verify** function is used to verify a signature of the data using given public key.

BOOL ECDSA_Verify(
    [IN] **LPTSTR** *lpPubKey*
    [IN] **BYTE** **pbMessage*
    [IN] **UINT** *dwMessageLen*
    [IN] **LPTSTR** *lpSignature*
);

Parameters:
lpPrvKey
    Points to the the null-terminated string containing ECDSA public key.
pbMessage
    The address of the signed data.
dwMessageLen
    The number of bytes of signed data.
lpSignature
    Points to the null-terminated string containing ECDSA signature to verify.

Return Value:
If the function succeeds, the return value is TRUE. If the function fails, the return value is FALSE.

History version :

```
14.05.2006 - version 1.0
20.05.2006 - version 1.1, bugfix
    Overwrite bug (+1 dword) in ECP_Zero_J.
    The bug MAY affect stability and/or security of your code if you use
one of 1.0 LIBs.
    This bug DOES NOT affect security nor stability of the DLL version.
```

License :

"Software" means the program supplied by WiteG herewith.

Permission is hereby granted to any individual, organization or agency to use the Software for any legal NON-COMMERCIAL purpose, without any obligation to the author. You may distribute the Software freely, provided that the original distribution package (binaries and any other files included in it) is left intact. You may also disassemble, reverse engineer or modify the Software, but you MAY NOT distribute it in modified form.
Any COMMERCIAL use of the Software without commercial license obtained from the author is strictly prohibited.

Warranty:

This software is provided by WiteG as-is, without warranty of ANY KIND, either expressed or implied, including but not limited to the implied warranties of merchantability and/or fitness for a particular purpose. The author shall NOT be held liable for ANY damage to you, your computer, or to anyone or anything else, that may result from its use, or misuse. Use it at YOUR OWN RISK.
However, the author of this software does hereby declare that there are no hidden weaknesses or trapdoors inserted by him.

Please report any bugs, comments, questions or suggestions to me