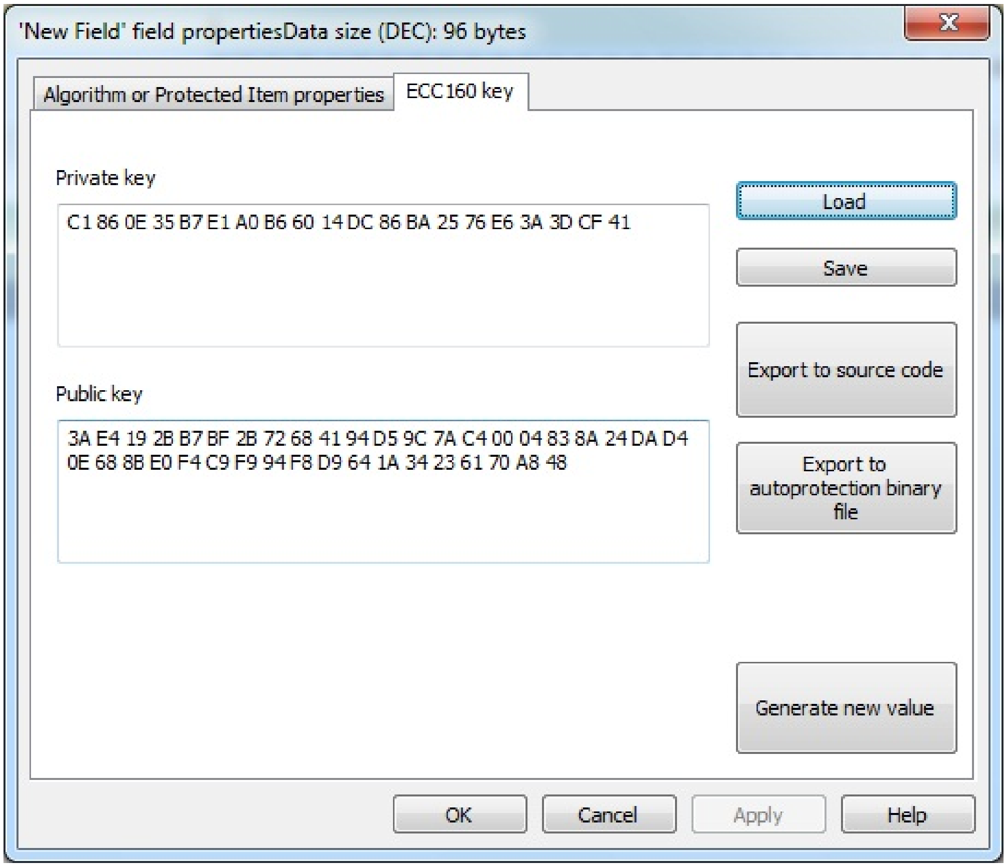
ECC160 key pair

When creating/editing an elliptic curve digital signature algorithm (ECC160), the **Determinant Editing** dialog is replaced with **ECC160 Key**.

The **ECC160 Key** dialog serves to generating the key pair of the digital signature algorithm ECC160.

The private key appears in the top part of the dialog box, and the public key – in the bottom of the dialog box. To the right there are buttons for performing service operations on the key pair.


'New Field' field propertiesData size (DEC): 96 bytes
Algorithm or Protected Item properties
ECC160 key
Load
Save
Export to source code
Export to autoprotection binary file
Generate new value
OK
Cancel
Apply
Help

Private key

C1 86 0E 35 B7 E1 A0 B6 60 14 DC 86 BA 25 76 E6 3A 3D CF 41

Public key

3A E4 19 2B B7 BF 2B 72 68 41 94 D5 9C 7A C4 00 04 83 8A 24 DA D4
0E 68 8B E0 F4 C9 F9 94 F8 D9 64 1A 34 23 61 70 A8 48

By default a key pair of an ECC160 algorithm is generated randomly. The pair can be changed by automatically creating a new one using the **[Generate new value]** button.

The **[Save]** button allows for saving the key pair into an external file (*.ecc). Clicking **[Load]** allows the previously saved pair to be loaded from a *.ecc file.

In order to use ECC160 algorithm for autoprotection you need to specify the path to the file with a public key as the parameter of SIGN option. **[Export to autoprotection binary file]** allows saving the public key into a file (PublicKey.bin, by default).

The **[Export to source code]** button saves the key pair into the C++ header file (EccKeySource.h, by default).

***

After editing the determinant (or ECC160 key pair) and clicking **[Finish],** the algorithm creation dialog box will close and a new algorithm will appear in the list of mask fields. Whereas GrdUtil.exe will automatically assign an index number (*Unified numbering is used for protected items and hardware algorithms*) to the algorithm and correct the bound of hardware locks taking the added algorithm into account.

Now all you have to do is to write the mask into the dongle and the newly created algorithm will be available for use.