Creating Algorithm

To create a hardware algorithm execute command Edit | Add field.

In Add field dialog box that will appear select Algorithm field type, specify the name and the type of the new algorithm as well as the size of its determinant.

Add new algorithm dialog box:

Constant storage memory editor [from file]	Guerdent Sign2015_04_27.nsd*) Miscelaneous View session key for API Dia Create with	te protected 99 template	- 6 <u>×</u>
hole in ange anne acou proget d'anget to a dange Dangte operations Dangte operations Sign Dio3Minut Address Sign Sign Dio3Minut Address Sign Sign Sign Sign Sign Sign Sign Sign	Control Anterpreterminy Control Control Control Contro Contro	Save Save Je Anno Range Save Je Anno Range Sa	Children forch Preserve Cc Lines and maps image to write to Preserve Cc Lines and maps image to write to Concerning with switchings or constants concerning with switchings or constants control and the switchings or constants
000 000 000 000 001 001 002 000 000 000 000 000 000 000	Unsigned range Counter 4 (2) Unsigned range Counter 4 (2) Unsigned range of the counter 4 of the counter 4 (2) Unsigned range of the counter 4 Particles of	With an experiment With an experiment experiment With an experiment experiment High (rests minimized)	Weight in the second seco
Dongle damps: Found 1 secols ime of writing Dongle type Dongle ID ZAR205115640 Sign 2666661h (804880156)	Imgenane Venion Type Application 1.0 Sym	Claret Compilion Ib Comment Anonymous Compile	
Add new filed			×
Select the field f	or adding to the don	igle image and click 'Next>'	
Field type		New Field	
		Determinant size (DEC):	
<u>C</u> ounter Memory du	ump	Algorithm type	
		GSII64 Stealth II/III: Symmetric encr	yption 🔻
Protected	ltem		
🔘 User loada	ble code		
		<back next=""> Ca</back>	ncel Help

Algorithm type

Select an algorithm type from the dropdown list.

The type of algorithm being created depends on the dongle mask:

Mask type	Algorithm type
Guardant Time/ Time Net	1. Symmetric encryption: CSII64
Guardant Sign/ Sign Net	 Symmetric encryption: Solida Symmetric encryption: AES128 Digital signature generation: ECC160 Hash function generation: HASH64 Hash function generation: SHA256 Random numbers generation: RND64
Guardant Code/ Code Time	 Symmetric encryption: AES128 Digital signature generation: ECC160 Hash function generation: SHA256
Guardant Stealth III / Net III	 Symmetric encryption: GSII64 Hash function generation: HASH64 Random numbers generation: RND64
Guardant Stealth II / Net II	 Symmetric encryption: GSII64 Unidirectional algorithm Stealth I and its modifications: Fast, Random, AutoProtect
Guardant Stealth / Net	Unidirectional algorithm Stealth I and its modifications: Fast, Random, AutoProtect
Guardant Fidus	-

Size of determinant

Determinant – the main part of hardware algorithm descriptor, which defines the specific type of encryption function. Algorithm determinants in Guardant dongles have fixed even length, Using GrdUtil.exe you can set the size of determinant and edit its type.

In order to select (or set - for unidirectional algorithm Stealth) the size of determinant, use the combined field-list.

The size of determinant depends on the algorithm type:

Algorithm type	Size of determinant, bytes	
Symmetric encryption: AES128	16	
Digital signature generation: ECC160	20	
Symmetric encryption: GSII64	16 or 32	
Hash function generation: SHA256	-	
Hash function generation: HASH64	16 or 32	
Random numbers generation: RND64	16 or 32	
Unidirectional algorithm Stealth I – obsolete	4 – 200 (optimum - 32)	

After setting the type and size of determinant of a new algorithm you need to edit its properties. Click **[Next]** in the lower part of the dialog box to move to the next page.