Привязать к типу ключа

Привязать к типу ключа:

/GS3S[=[N]:[L]:[ID]:[S]:[<FileName.bin>]],

/GN3S[=[N]:[L]:[ID]:[S]:[<FileName.bin>]],

/GC[=[N]:[L]:[ID]:[S]:[<FileName.bin>]],

/GS3[=[N]:[L]:[ID]],

/GN3[=[N]:[L]:[ID]],

/GS2[=[N]:[L]:[ID]],

/GN2[=[N]:[L]:[ID]],

/GSP[=[N]:[L]:[ID]:[S]:[<FileName.bin>]]

/GSPN[=[N]:[L]:[ID]:[S[<FileName.bin>]]

Описание:

Указание модели ключей, к которым будет привязано приложение:

GS3S	GN3S	GC	GS3	GN3	GS2	GN2	GSP	GSPN
Time/Sign	Time/Sign Net	Code	Stealth III	Net III	Stealth II	Net II	SP	SP Net

Дополнительные параметры:

N	Номер симметричного алгоритма шифрования GSII64 или AES, который будет использован при автозащите. Для **Guardant Code** обязательный параметр
L	Длина вопроса алгоритму, 8 <= L<= 256, где L - число, кратное 8 (для GSII64) или кратное 16 (для AES128)
ID	ID электронного ключа, к-й будет использован при установке защиты
S	Номер алгоритма электронной цифровой подписи ECC160
FileName.bin	Файл, содержащий открытый ключ ЭЦП для алгоритма ECC160.По умолчанию - PUBKEY_08.BIN, расположенный в текущей директории

Если при защите использовались опции этой группы, запуск защищенного приложения будет возможен только при наличии электронного ключа, т. к. приложение при защите настраивается на код доступа и привязывается к ключу заданного типа, подсоединенному к компьютеру на момент защиты.

Можно задавать одновременно несколько опций из этой группы – в любом сочетании. При этом защищенное приложение будет запущено, если хотя бы один из заданных типов электронных ключей Guardant будет подсоединен к компьютеру.

1. Нотация

Дополнительные параметры указываются через символ-разделитель – двоеточие. Необязательные параметры можно пропускать, при этом если за пропущенным следуют другие параметры, то символ **:** требуется печатать.

Пример:

/GS3S=:::2

Привязка к Guardant Sign с умолчательным алгоритмом шифрования и алгоритмом типа ECC160 под номером 2 (с открытым ключом по умолчанию); ID не указывается.

2. Алгоритм шифрования

При задании дополнительных параметров **N** и **L** в процессе защиты будут использоваться симметричные алгоритмы шифрования GSII64 или AES с указанным номером и длиной вопроса.

Если параметр **N** не задан, то процесс защиты будет выполнен с алгоритмом по умолчанию.

Параметры алгоритма по умолчанию зависят от типа ключа:

Модель	Умолчательные параметры симметричного алгоритма шифрования
Sign/Time	GS3S=0:8
Sign/Time Net	GN3S=0:8
Code	Умолчательный алгоритм отсутствует. Параметр **N** обязателен
Stealth III	GS3=0:8
Net III	GN3=0:8
Stealth II	GS2=4:8
Net II	GN2=4:8
SP	GSP=3:16

Если алгоритм по умолчанию для указанного типа ключа отсутствует в прошивке ключа, будет выдана соответствующая ошибка.

Если параметр **L** не задан, алгоритм будет вызван с длиной вопроса по умолчанию. При использовании неверного значения **L** будет выдана соответствующая ошибка.

3. Выбор ключа для защиты из нескольких подсоединненых к портам

Если к компьютеру подсоединены несколько ключей одной модели, то чтобы выбрать для проведения защиты определенный ключ, следует указать его ID при помощи одноименного параметра. **ID** задается в десятичном (ID=1234), или в шестнадцатеричном (0xABCD) виде.

4. Проверка цифровой подписи

При установленном параметре **S** защищенное приложение будет автоматически, наряду с регулярными вызовами GrdTransform, вызывать последовательность функций GrdSign – GrdVerifySign для выработки и проверки ЭЦП случайного числа.

Модель	Пример использования опции алгоритма ЭЦП
Sign/Time	GS3S=:::8:PUBKEY_08.BIN
Sign/TimeNet	GN3S=:::8:PUBKEY_08.BIN
Code	-
Stealth III	Не поддерживается
Net III	Не поддерживается
Stealth II	Не поддерживается
Net II	Не поддерживается
SP	GSP=:::2:PUBKEY_08.BIN

Важно!

1. В ключах, которые передаются клиентам вместе с защищенным приложением, должны быть созданы алгоритмы с таким же номером, определителем и длиной запроса, какие были указаны при защите.
2. Если опции этой группы не использовались, приложение не будет привязано к электронному ключу (т. е. оно будет запускаться и в случае, когда ни один из электронных ключей не подсоединен к компьютеру). Однако оно будет защищено **от отладчиков**. Вы можете использовать эту возможность, например, для защиты приложений, которые без электронного ключа работают в демо-режиме.

Пример:

NwKey32.exe /GS3S=5:::2 /GS3::12345678 MyProg.exe

Защищенное Win32-приложение **MyProg.exe** будет запускаться в случае, если к компьютеру подсоединен ключ *Guardant Sign* с симметричным алгоритмом #5 (длина вопроса по умолчанию) и ECC-алгоритмом #2 (открытый ключ по умолчанию) или *Guardant Stealth III* с умолчательными параметрами и ID=12345678.

Причем для ключа *Guardant Sign* в процессе работы будет вырабатываться и проверяться цифровая подпись случайного числа, генерируемого вакциной.