Trusted Remote Update

Trusted Remote Update is used in modern Guardant dongles. The main advantage of this technology lies in the fact that all information required for remote update is decrypted and processed only inside the dongle.

Trusted Remote Update – technology of safe remote dongle memory update eliminating the possibility of data compromise and/or counterfeiting. The ideology of Trusted Remote Update guarantees that information once recorded into a dongle cannot be rerecorded into it, and data generated for one dongle will not work with another.

Important information

The Trusted Remote Update procedure presumes the use of unique data, specifically, the remote update password for the each dongle. Therefore it is strongly recommended to use the database mode for registering and saving templates and dumps. Otherwise, the remote update procedure will become hindered or even impossible.

Remote programming of dongles located at end-users inevitably leads to problems related to ensuring secured data exchange.

During remote programming the developer must make sure that, first, the enduser is going to update the data in the right dongle. For this purpose the respective dongle ID is included into the encrypted number-question generated by the dongle in the beginning of the remote programming session.

Secondly, the developer needs to verify the validity of the numberquestion, i.e. the end-user did not send a counterfeited or changed num-ber-question. The hardwareimplemented hash function with a secret key is used for validity verification (HASH64 for Guardant Sign/Time/Net or SHA256 for Guardant Code /Code Time). Number-question is sent to the developer along with the result of calculating the hash function. Having the dongle with the same algorithm, the developer can verify the validity of the number-question by calculating the hash function and comparing its result with the received value. Thus, a sort of digital signature of data is implemented.

Third, the developer needs to be sure that the number-answer will be sent to the dongle of the end-user in unchanged form. For this we also use hardware calculation of HASH64 (or SHA256).

Fourth, the end-user may not know exactly what data is being sent. A hacker very well may be in the end-user's place trying to analyze the remote programming protocol. For this reason, all data sent from the end-user to the developer and back is obligatory encrypted with symmetric algorithm (GSII64 for Guardant Sign/Time/Net or AES128 for Guardant Code /Code Time).

The security of remote programming protocol (Trusted Remote Update) is implemented by the means of hardware encryption and hashing algorithms, as well as through keeping the secret codes inside the dongles in the process of conversion. All operations related to decrypting and data integrity checks are handled inside the hardware unit. This eliminates the possibility of compromising or substituting data recorded into the dongle.

Important Information

In order for the whole mechanism of Trusted Remote Update to operate, unique secret keys of GSII64 (AES128) algorithm are programmed into the dongles during the presale preparation. Copies of these keys along with dongle IDs, where they have been recorded, are kept by the developer in a secret database accessed only by the authorized personnel.

Remote update password

Remote update password is a 16-byte sequence of hexadecimal symbols used in the Trusted Remote Update procedure to convert update data. You may use the same remote update password for a batch of dongles or apply the unique password for each dongle.

Important information

For successful performing of Trusted Remote Update the password contained in the remote dongle should match the password stored in the database.

The remote update password is contained in the non-addressable and available for editing field located in the mask right after the special purpose fields.

GrdTRU_SetKey function serves for setting the remote update password from within the application.

In order to view/edit the password for remote update, load the required mask, select **Remote Update Password** field and execute **Edit | Field Properties** menu command.

Edit the password in the **Remote Update Password Field Properties** dialog box that appears as a hexadecimal editor.

By default GrdUtil.exe automatically forms the remote update password. When necessary it can be changed by forming the password yourself. You can do it by entering the new value directly into the editor's window or generating the new password automatically (**[Generate new value]** button).

The dialog will also allow defining whether unique or permanent a password will be used. If **Unique value for each dongle record** flag is set, then during each session of programming the dongle the password value will be replaced with a new random sequence. Thus, each dongle will get a unique update password stored in the dongle memory and its dump.

Remote Update Password dialog box control elements:

Interface element	Description of purpose
Hexadecimal editor window	Enter the password for remote update
[Generate new value] button	Replace the current password value with a new random sequence
Unique value for each dongle record checkbox	Use unique/permanent password. The permanent password is used by default with the checkbox unmarked
OEM checkbox	Select Windows/DOS encoding. Windows (ANSI) encoding is used by default with OEM checkbox unmarked
[Load] button	Load dump from *.dmp file
[Save] button	Save dump into a *.dmp file

After entering the data click **[Apply]** button and close the dialog box.

Special features of Trusted Remote Update

The Trusted Remote Update procedure is practically not any different to regular remote update when used with GrdUtil.exe (see Section **Remote Update)** with the following exceptions:

1. When executing command **Dongle | Dongle Update** GrdUtil.exe will automatically record special algorithms into the memory of ‘master’ dongle connected to the port. These algorithms participate in processing of update query and encoding of update data using the password stored in the dump of the dongle being updated.
   After the update dump is created, the contents of ‘master’ dongle is automatically restored.
   These actions appear only as warnings.

2. If the remote update is done without using the database, i.e. based on the mask file, GrdUtil.exe will display a warning that the update query will not be decrypted with mismatch of remote update passwords in the mask file and the remote dongle.