HTplus2

Hitag-PRO, Hitag-PRO2, Hitag-AES, Hitag-EXT, Hitag-3 transponder programmer

Hitag-PRO / PRO2:
Covers PCF7939PA and compatible mcu based transponders - e.g. PCF7x45PTT and PCF7953PTT, used by BMW (starting from F-series), Range Rover, Porsche. Security is based on 128-bit security key (SK). It is possible to prepare new key according to vehicle specific demands: key configuration, SK, VIN, key number, page locks etc.

Some transponder basics - there are 1024 bytes of EEPROM available for user access. It is split into eight individually configurable pages with individual access rights. According to configuration each page can be read in plain or crypto. Or read may be disabled at all. Similar rules applied to write operations.

Last 32 bytes are left for EEPROM configuration settings, usually all page sizes are already preconfigured for specific use and locked against size change. If no locks are set it is possible to configure them using XMA config button or manually. Blank chip must be configured first to grant XMA access.

Page0 contains transponder ID, SK and some important bytes essential for HitagPro operation. If key is blank or preconfigured it is usually accessible for both read and write operations in plain mode. In this case stored SK is not important, you can replace it with necessary one and lock page if you wish.

In case of used key, it is possible to read and write pages according to page configuration . By default programmer tries to read/write key in plain mode (if allowed). If crypto is allowed you can uncheck "read plain" check box to force operation in crypto mode.

It is possible to enter SK manually into 4 fields inside SK group box. Button "SK to buffer" updates memory buffer. Values not currently matching are displayed on yellow background on hex editor screen. You must use MODIFY or WRITE buttons to update / store them into transponder. Button VERIFY SK checks SK for validity, if success SK background becomes green. Same principles are used when exploring and updating BMW key data - it is altered only on screen (buffer), not key itself. It is done to avoid mistakes and to allow to check what happens. How to get BMW key screen: go to any page, press BMW icon.

Hitag2-AES:
Covers: PCF7939MA itself and MCU based derivatives - e.g. PCF7x41MTT, PCF7x61MTT, PCF7953MTT. Widely used by PSA. Security is based on 128-bit AES key, there are 512 bytes of EEPROM memory where additional data are stored. XMA (extended memory access) is based on similar principles like HitagPro - 8 pages with individual access rights.

Hitag2-EXT:
Covers: PCF7937EA and MCU based derivatives - e.g. PCF7x41ETT, PCF7x61ETT, widely used by GM (Opel, Chevrolet). Security is based on 48-bit secret key, principles are very similar to basic Hitag2 (PCF7936) transponder operation. Main advantage is 512 byte EEPROM memory for additional data. XMA (extended memory access) is based on similar principles like HitagPro - 8 pages with individual access rights.

Hitag3:
Covers: PCF7938X and MCU based derivatives – e.g. PCF7x41ETT, PCF7x61ETT. Similar to Hitag2extended except cryptography: it is based on 96-bit secret key.

Mass production mode:
Designed for production purposes. It allows to prepare blank transponders in some seconds. It is necessary to prepare two files: one contains data (full EEPROM), second one contains mask (which bytes to write).