

Secure Flash Programming in the Vehicle

Cryptographic algorithms offer protection against tampering in flash programming



Stuttgart, 06-06-2007 - To assure that flash programming of ECUs is protected against tampering, Vector is integrating cryptographic algorithms from cv cryptovision in its bootloaders. Vector is relying on the use of this tested technology of cryptographic algorithms, which supports security mechanisms required by car manufacturers for software updates.

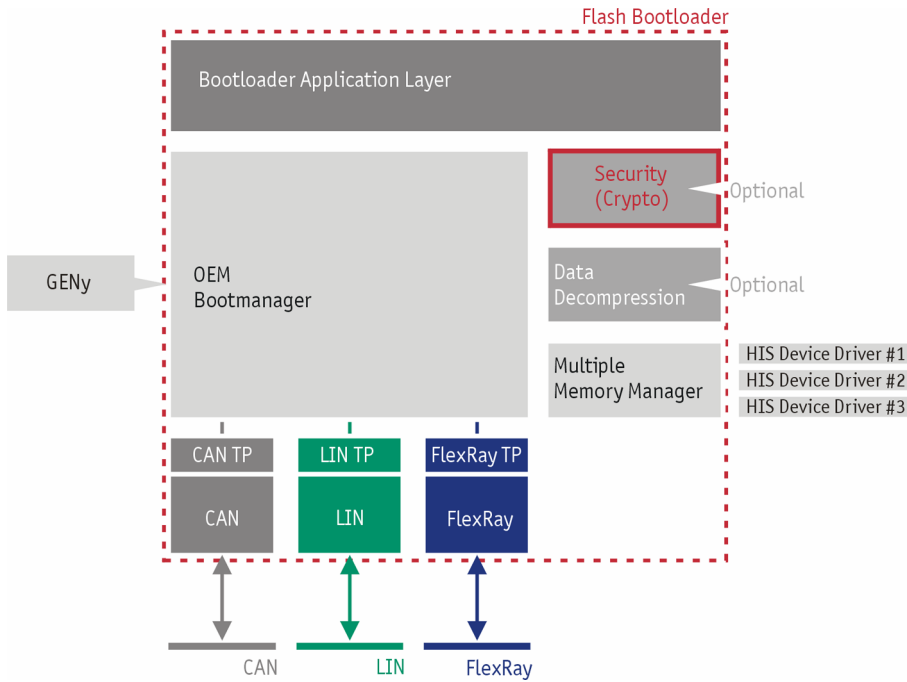
Re-programmability (flashing) is a key requirement of OEMs for updating software in the ECUs of motor vehicles and this process must be protected against tampering, e.g. circumventing the immobilizer function, altering the odometer reading, or introducing malicious sections of software code.

Vector is collaborating with cryptographic experts from cv cryptovision GmbH, Germany. This strategic alliance combines cv cryptovision's many years of experience in implementing cryptographic routines for PCs and microcontrollers with Vector's competence in the area of embedded software for the automotive industry.

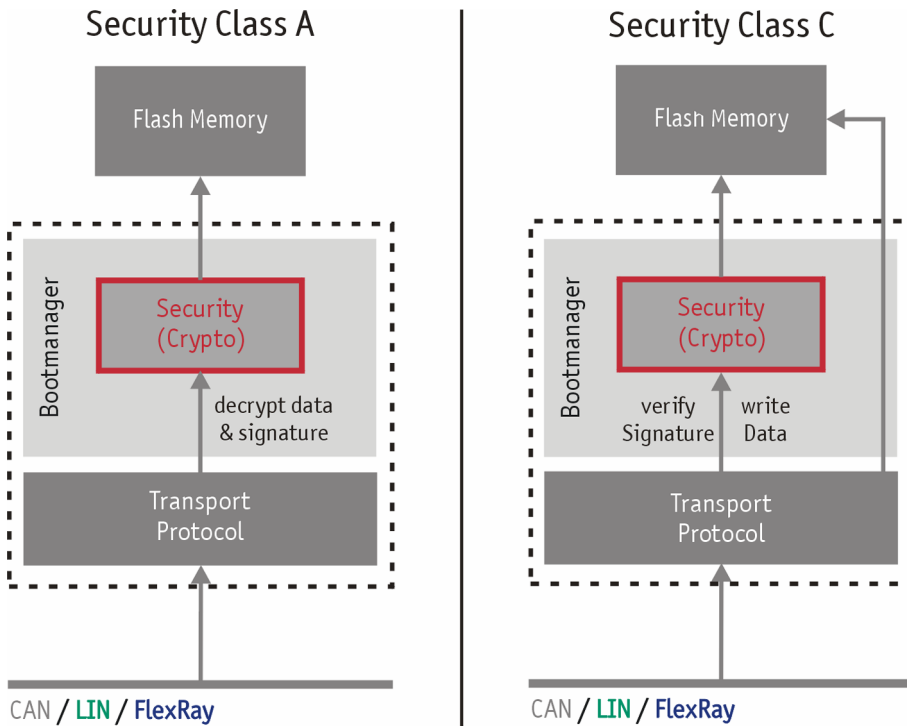
This collaboration results in efficient implementations of complex mathematical algorithms. Particular emphasis is placed on execution time and efficiency, factors that are especially important in the automobile.

Since security requirements for different ECUs are OEM-specific, the Vector bootloader utilizes a variety of methods: Asymmetrical keys for complex ECUs, as well as

symmetrical keys and one-way hash functions for low security requirements. These methods have already proven themselves in the PC world.



[Figure 1: Architecture of the bootloader with cryptographic modules for protection against tampering.]



[Figure 2: In practice, bootloaders of different security classes are implemented.]



[Figure 3: Cryptographic mechanisms in the bootloader prevent manipulation of ECU software]

Revised: 6/2007
Word count: 217
Character count: 1,596

Vector Informatik GmbH
Ingersheimer Str. 24
70499 Stuttgart
Germany
www.vector-informatik.com

We would appreciate it if you would send us a specimen copy.
If you have any questions before publication we would be glad to assist you:

Vector Informatik, Germany (Article available in English and German)
Holger Heit,
Tel. +49 711 80670-567, Fax. +49 711 80670-555,
E-mail: holger.heit@vector-informatik.de

Vector CANtech, North America (Article available in English)
Angela Aceti,
Tel. +1 248 504 6447, Fax. +1 248 449 9704,
E-mail: angela.aceti@vector-cantech.com

Vector France (Article available in French)
Françoise Grandjean,
Tel. +33 1 4 231 4000, Fax. +33 1 4 231 4009,
E-mail: francoise.grandjean@vector-france.com

Vector Scandinavia, Sweden (Article available in Swedish)

Henrik Pihlgren,
Tel. +46 31 764 76 10, Fax. +46 31 764 76 19,
E-mail: henrik.pihlgren@vecscan.com

Vector Japan (Article available in Japanese)
Takushi Hieda,
Tel. +81 3 5769 6981, Fax. +81 3 5769 6975,
E-mail: takushi.hieda@vector-japan.co.jp

You can find this and other press releases on our homepage at:
www.vector-informatik.com/press

About Vector Informatik GmbH (Revised: 06/01/2007):

Vector Informatik is the leading producer of software tools and components for networking in electronic systems based on CAN, LIN, FlexRay and MOST as well as a number of CAN-based protocols.

This know-how is conveyed in the form of products or as a comprehensive consultation package with system and software engineering. Workshops and seminars round out our multifaceted training program.

Worldwide customers in the automotive, heavy-duty vehicle, transport and control engineering fields rely on solutions and products from the independently-owned Vector Group.

Vector Informatik, founded in 1988, currently employs 720 people together with Vector Consulting GmbH and in the year 2006 achieved sales of 105 million euros. In addition to its headquarters in Stuttgart, Vector Informatik also has an international presence with subsidiaries in the USA, Japan, France and Sweden.