

Secure Feature Activation

Kai Schramm and Marko Wolf
escrypt Inc.

Copyright © 2009 SAE International

ABSTRACT

This work shows how vehicular features which are pre-installed but deactivated can be securely enabled later with activation codes. Nowadays, feature activation results in two business models. The first model is a pay-per-use model which drastically reduces one-time acquisition costs for customers while increasing the long-term revenue of manufacturers. The second model is an “activate-once-and-use-always” model, which allows vehicles to come in differently configured variants even though most electronic devices use the same hardware and software components. Since the usage of product features is usually liable to pay costs (e.g., aftermarket business models) and legal obligations (e.g., export restrictions), the underlying security of the feature activation process is essential.

This paper discusses the theoretical background of secure activation codes geared to an automotive context. Typically, activation codes can be used to enable features, such as the usage of pre-installed maps for a certain time in a navigation system, disabling the maximum speed limit of the engine, or enabling a speech control system. Various ways are presented of how to deploy activation codes into a vehicle, for instance, by the driver's using a short alphanumeric sequence, by workshop service personnel transferring a cryptographically robust code using the onboard diagnostic interface, or by the service provider or automotive manufacturer transferring the code remotely using a secure telematics channel. This work presents

various technical aspects of activation codes based on asymmetric and symmetric signatures in combination with flexible key management using cryptographic certificates. The technical requirements of electric control units to allow feature activation processes as well as the secure generation of activation codes in a backend environment are discussed.

INTRODUCTION

Modern vehicles have up to 120 built-in electronic control units (ECUs) which control a vast variety of tasks ranging from simple window lifters to complex navigation systems and telematics applications. Therefore, these ECUs have a broad range of available processing power and available memory resources. Moreover, many automobile OEMs also offer a vast spectrum of features of individualized vehicles within the same series. Thus, some vehicles might come with a speech recognition system while other vehicles of the same series come, for instance, with a disabled maximum speed limit. One method to allow a wide spectrum of variants without complicating the production process is the application of feature activation, which basically means that all vehicles come with an almost identical set of hardware and software components while a different set of features is enabled in each vehicle.

For example, let us assume that a company produces state-of-the-art navigation systems and ships these devices with a multitude of pre-installed but deactivated maps. Due to the fact that maps can be enabled later by the driver with an appropriate, tailored activation code,

the company can offer the navigation systems at a very competitive price, which may attract many additional potential customers, thus increasing sales volume. Then, maps can be activated for a short duration or for good, which allows many individual and flexible business models. Hence, the one-time acquisition costs of the navigation system can be lowered drastically, which may result in an increased turnover and increased long-term revenue. If, however, the security of the feature activation process can be broken, for instance, due to the application of cryptographically weak activation schemes, the underlying business model could collapse, which would result in dramatic financial losses.

After this introductory section, we will briefly review important cryptographic algorithms and methods, which are required to protect activation codes from unauthorized manipulations and usage. In Section 3 we will discuss the basic concept of activation codes and the necessary security architecture of the backend which generates the codes, as well as the necessary security architecture target device which validates the activation codes. In Section 4 we will briefly discuss special properties of short activation codes which usually can be entered manually. In Section 5 we review implementation aspects and applications of feature activation codes in the automotive context. Section 6 finally concludes this work.

CRYPTOGRAPHIC METHODS

In order to protect feature activation codes (FAC) against unauthorized manipulation and usage, cryptographic methods and algorithms are applied. Typical cryptographic measures for information protection and verification of origin are encryption schemes, authentication schemes and hash functions. Encryption and authentication schemes can be generally realized by symmetric and by asymmetric cryptography. Symmetric algorithms basically require that the sender and receiver of an encrypted message jointly share a secret key. Asymmetric algorithms, in contrast, require that a sender use the *public* part of the key of the receiver for encryption, while the receiver has the corresponding *private* part of the key for decrypting the encrypted messages. Hash functions, finally are one-way functions, which map an input of arbitrary length to an output of fixed length. Further readings, however, are helpful and can be found amongst others in [7].

SYMMETRIC CIPHERS

The most common symmetric ciphers are the block ciphers DES (Data Encryption Standard) and AES (Advanced Encryption Standard) [3, 11]. The DES is a block cipher that encrypts and decrypts blocks of a

length of 64 bits and uses a 56-bit key. Due to the short and outdated key size of DES, the AES block cipher was developed. AES encrypts blocks of 128 bits and can either use 128-bit, 192-bit, or 256-bit keys.

ASYMMETRIC CIPHERS

Asymmetric ciphers can be used for encrypting and decrypting data, for signing and verifying data, and for advanced applications such as securely exchanging a symmetric key over an unsecure communication channel (hybrid encryption). The most popular asymmetric ciphers are the RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) systems [7, 9]. As Table 1 shows, ECC key sizes are significantly smaller than RSA key sizes at equal levels of security. Moreover, ECC key sizes grow linear proportionally with symmetric keys sizes, whereas RSA key sizes grow exponentially. This makes ECC more attractive for embedded devices with limited memory resources. However, while RSA is slower than ECC when signing data, RSA is faster than ECC when verifying data from using a short public key exponent. ECC verifications can be sped up with certain algorithmic techniques, but many of these are patented. Moreover, RSA is much simpler to implement than ECC-based systems.

Comparable symmetric key size (bit)	RSA key size (bit)	ECC key size (bit)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: Key lengths of symmetric and asymmetric ciphers at equal levels of security.

HASH FUNCTIONS

Cryptographic hash functions are one-way functions which are used to create a small and virtually unique digital fingerprint of fixed length, the so-called hash value, of an input message of arbitrary length. An ideal hash function is very fast in calculating such a hash value, while it should be computationally infeasible to calculate the original input message for a given hash value. Hash functions are mainly used for message integrity verifications and within digital signatures for message authentication. The two most popular hash functions currently are the SHA-1 (Secure Hash Standard) and the MD (Message Digest) families [6, 12]. However, since both have turned out to have some security flaws, there is currently a contest for a new hash function that will succeed both [10]. Hash functions can also be used to generate Message Authentication codes (MAC) that allow the receiver of a message to verify its