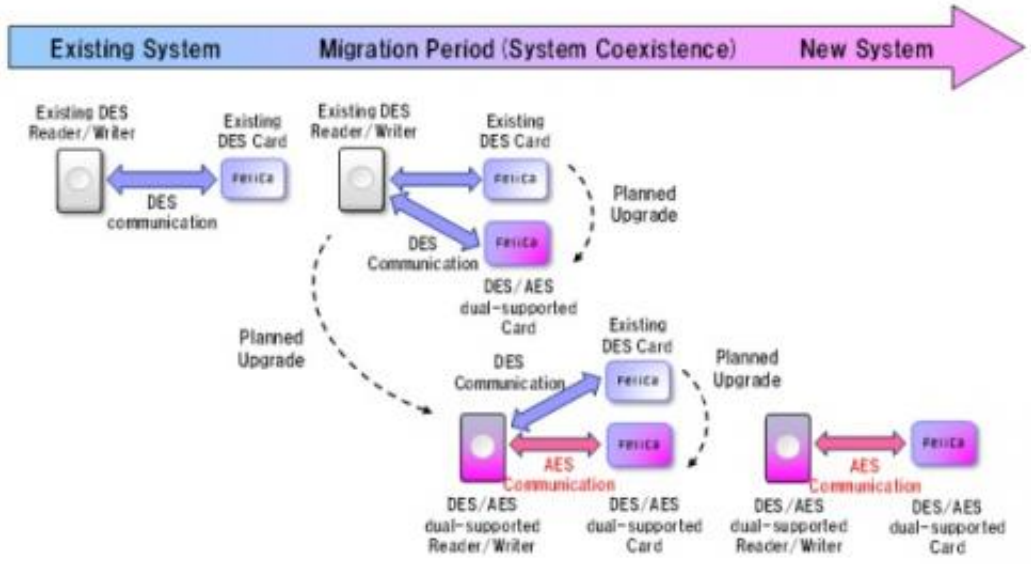
Next generation FeliCa contactless IC chip to be launched

June 13 2011



Comparison with the current FeliCa(Standard) IC chip

Sony Corporation announces today the launch of the next generation FeliCa IC chip with enhanced security adopting the Advanced Encryption Standard (AES) encryption. The new IC chip will support AES as well as the existing DES encryption system for mutual authentication and data communication. The sample chip will be available for shipment from this winter, and mass production will start in the spring of 2012.

Sony's contactless smart card technology "FeliCa" is widely deployed in card or mobile phone products for various applications including transit and payment where high performance and security is required. To date, more than 500 million FeliCa cards and mobile phone IC chips in total have already shipped throughout the world.

The newly developed IC chip will have the same command sets as the current DES-based FeliCa card system so that the FeliCa card with the new chip can easily be introduced into existing services. The new chip will have a security-migration function so that it will easily be able to migrate from the existing security system to the new AES encryption-based security.

JR East Group cooperated with Sony regarding the specification for the new OS.

With the new IC chip, Sony will develop and market a variety of forms of card, and in addition plans to develop next generation compatible products for mobile devices and reader platforms. The new IC chip will create a new lifestyle and range of applications where users feel daily convenience simply by "tapping" in an expanded FeliCa world.

Features of next generation FeliCa contactless IC chip

• Highest level of security for contactless smart card chips
It is planned to achieve the highest security level for this product by adding AES cryptographic functionality in addition to the current DES encryption for communication between card and reader/writer. Leading-edge anti-tampering technology will be implemented to achieve higher than EAL5+ certification level according to ISO/IEC15408 common criteria.

• Multi-application platform with higher performance and reliability

Both higher transaction speed and longer communication distance will be achieved for every type of card application such as transportation ticket and electronic money. This will be achieved by pursuing further lower power consumption than the current FeliCa IC chips. It will improve reliability of nonvolatile memory data by implementing new Error Checking and Correcting (ECC) functionality.

• Security-migration function and backward compatibility with the current FeliCa IC chips
New FeliCa IC chip will be compatible with the current product in terms of the command set both for DES cryptography and without security. It will be compatible to existing infrastructure using cryptographic communication with existing reader/writers supporting DES encryption and non-secure-based communication with readers such as FeliCa Port and PaSoRi. In addition, it will include a security-migration function in order to support the existing DES cryptography-based system as well as future upgrades to the AES based system.

Source: Sony