PEARL eSE

The cornerstone of secure mobile and IoT services

Connected Objects

With the growing trends of smartphones being used as payment devices, storing and processing sensitive biometric data, or improving transport ticketing experience, increasing concerns regarding users' authentication, data protection and privacy are arising. And smartphones are only the first wave of connected objects. Tomorrow we will use wearables such as watches for keyless access to corporate facilities, homes or vehicles. We will also purchase and pay fuel, road map updates, video content and a lot of other services directly from car dashboards. And, very soon, autonomous vehicles will also need to be able to check the integrity of data received from road infrastructures and other cars and protect data they exchange in order not to be at the mercy of hackers.

Security embedded in the end-point devices

With the increasing number of devices connected, and more and more data stored and processed within these devices, new security concerns emerge. At IDEMIA, we believe that in order to be effective, security systems must be embedded within connected objects and equipment. IDEMIA has accumulated significant experience in storing and managing secure information in secure elements, notably with its flagship eSE, PEARL eSE, and can now also apply this strong security legacy to the M2M and IoT markets, starting with the Automotive.

An application vault trusted by major OEMs

Currently deployed in 180M+ units in the most popular smartphones, PEARL eSE is the most advanced multi-application eSE on the market. It offers an unattained level of security, the largest memory on the market and the latest NFC capabilities. This all-in-one eSE allows easy deployment of secure mobile contactless payment, transit, governmental and automotive applications, as well as secure access to online services for enterprise and consumer markets. It is the safest possible place to store secret information and execute sensitive applications.

End-to-end solutions for business-critical data and security-related services

PEARL eSE protects credentials and data applications against software and hardware attacks, ensuring that mobile, M2M and IoT devices are strongly authenticated and that information exchanged over networks remain protected. Combined with IDEMIA's secure authentication, encryption and service deployment platforms, it brings the highest level of security in and around the devices by addressing security challenges at both the device and Cloud levels. PEARL eSE for instance allows service providers to deploy strong personal authentication with standard solutions such as FIDO.

IDEMIA

Deploy innovative services at high speed and with high security

PEARL eSE is delivered with an Android/Tizen software stack designed to help integration in OEMs' design boards, and with high-level APIs for mobile application developers.

The latest generation of PEARL eSE also supports a remote management capability at OS level. This innovation extends the current capabilities of PEARL eSE of downloading new JavaCard applets and enables device manufacturers to deploy new OS capabilities such as new algorithms or hardware-related function activation (e.g. memory extension).

PEARL eSE supports a high-speed direct communication link (SPI*) with the device application processor. This link facilitates the access to security services of the eSE from any application, for example to secure sofware licences or personal data such as fingerprints, etc.

Feature set	Pearl V4
Available form-factors	Wafer, WLCSP, VQFN-32
Flash Memory	700KB free memory for user applications
Personalization capabilities	Wafers and packages delivered pre-loaded with applications and management keys Final personalization performed on-Package or on-Device, e.g. via IDEMIA's Universal Credential Platform
Built-in self-test checks	Flash, RAM, Crypto-processor
Automatic NFC configuration	With all key NFC controller vendors

PEARL eSE Key benefits

Banking-grade security level

PEARL eSE embeds an EAL5+ and EMVCo certified component with the largest memory available on the market. PEARL eSE is certified by all major payment schemes for mobile payment: VISA, MasterCard, AMEX, CUP (China UnionPay). PEARL eSE also supports the integration of mobile contactless payment acceptance in existing wallets for small shops or mobile merchants such as taxis or food trucks but also for person-to-person payments by any wallet user.

Transport and access control applications

PEARL eSE is the best solution on the market to address the fragmented market of transport systems throughout the world. It is the sole component to support multiple Mifare Classic virtual cards, Calypso™ and CIPURSE™ standards, as well as Chinese transit technologies.

It also enables physical and logical access control thanks to Mifare, HID SEOSTM, LEGIC and PIV technologies support.

Authentication, data integrity & confidentiality

While the use of biometric data today appears as the most efficient way to authenticate users, it also raises new security challenges: a compromised PIN can easily be replaced, but not a finger or an eye... The latest generation of PEARL eSE comes with two new fingerprint matching algorithms allowing the eSE to be used not only to securely store biometric data but also to securely run the fingerprint verification inside the eSE, thereby preventing users biometric data from being exposed outside the eSE.

IDEMIA

Join us on

www.idemia.com