Second Laureate Applied Research

Scientific Committee
Electronics & Computer

Research Work Title

SADAF Hardware Security Module (SADAF HSM)

Executive Organization
Parsa Sharif Research Center

Representative
Behnam Sattarzadeh (Ph.D.)

Collaborators
Seyyed Amin Habibi, Ali Jahanian, Hossein Homaei, Seyyed Mohammad Sebt, Reza Karkon Varnosfaderani, Hamed HosseinTalaee, Javad Zandi, Zeinab Iranmanesh

Collaborator Organization
Mobile Telecommunication Company of Iran

Abstract

Cryptography is one of the essential methods to protect the sensitive information. However, the security of cryptographic schemes mainly depends on the security of the confidential keys involved in such schemes. A hardware security module (HSM) is a secure computing hardware that was particularly designed to guarantee the security of cryptographic keys during their lifecycle, i.e., generation, cryptographic operation, and destruction. The most important keys of information systems are managed by HSMs which are equipped with the most advanced protection mechanisms to prevent, detect, and respond to any security threats. Indeed, HSMs are considered as a Root-of-Trust as they are trusted to perform all critical cryptographic operations while keeping security keys safe from exposure.
SADAF is an HSM that was designed and implemented by the experts of Parsa Sharif Research Center. SADAF has met all functional and security requirements that were specified in international industrial standards such as FIPS 140-2 Level 3 and PKCS#11. It supports all de-facto cryptographic algorithms and provides an advanced multi-layer protection mechanism for security keys. Computing performance of SADAF is comparable to the foreign HSMs currently available and utilized in Iran providing a viable option for the large information systems such as banks and mobile operators.