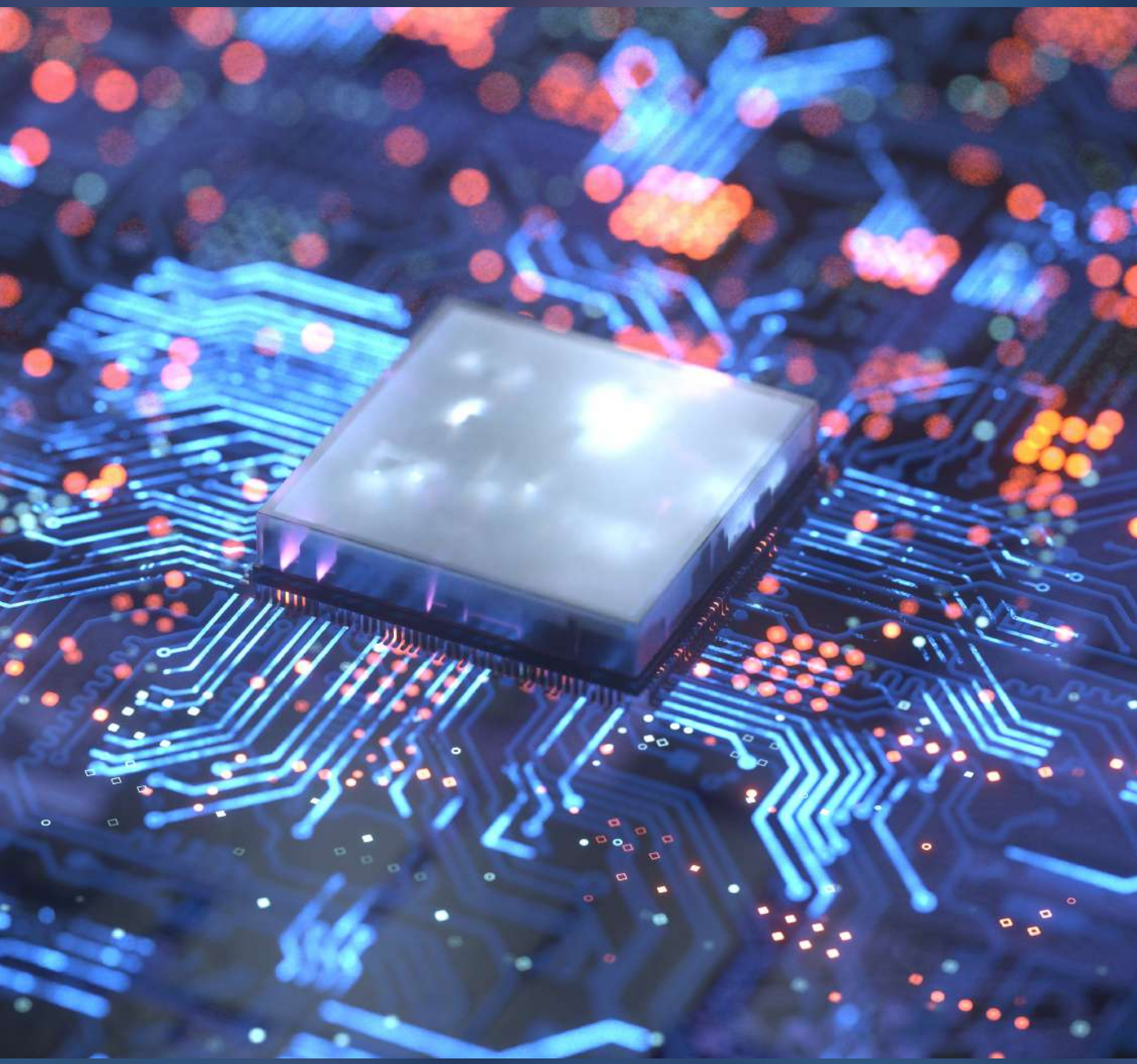
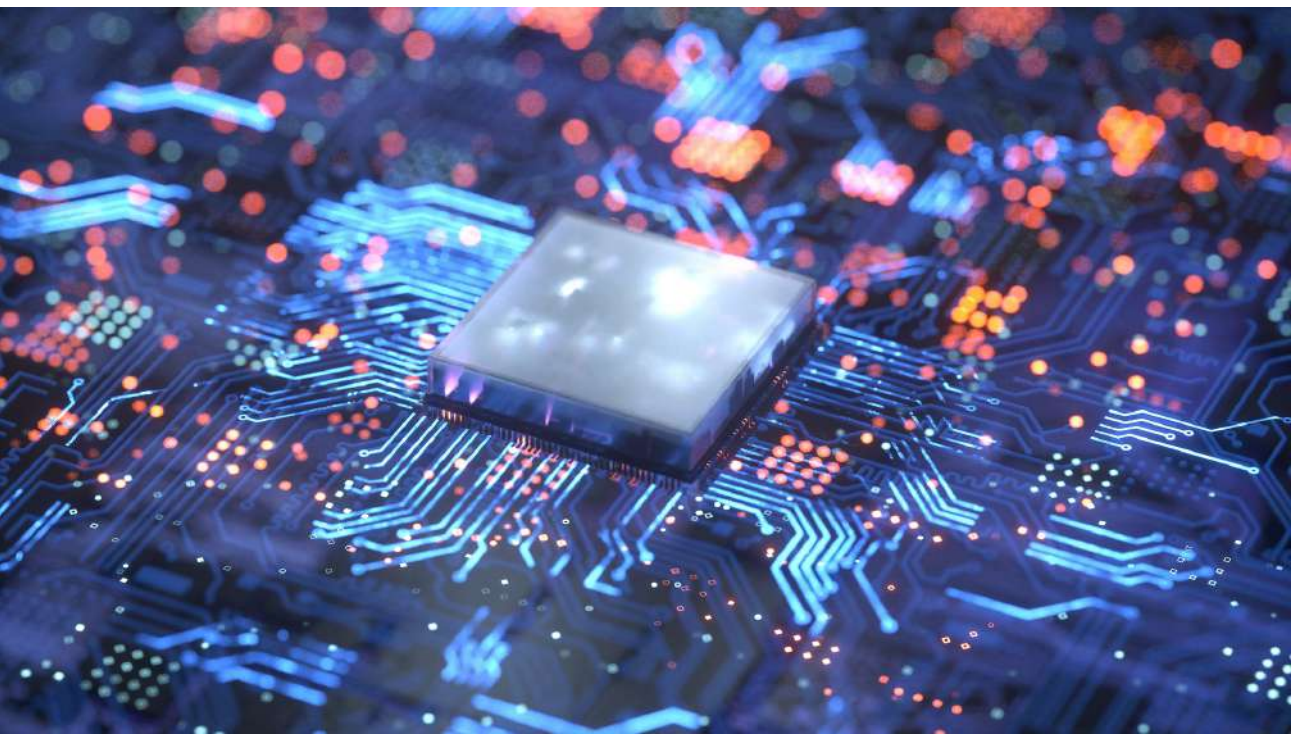


Military-grade Omni Platform

Preeminent Secure Element
Preemptive Protection

S97 Security Chip
for Military-Grade Protection



Today's evolving threat landscape creates a need for preemptive and flexible security solutions. To meet the requirement, solution providers should engage in both defense and attack. Mastery of attack allows for accurate and effective security deployment, minimizing potential loss.

As the prerequisite of effective security lies in acquantance with attack, there should be a customizable platform enabling tailor-made design to cope with a wide range of attacks in various contexts.

The Military-grade Omni platform features a security chip made by one of the most competent semiconductor vendors, Infineon. It has acuqired Common Criteria EAL 5+ (Evaluation Assurance Level 5 plus), equalling military-grade security.

With IKV's expertise, the Military-grade Omni platform fulfills agile reaction to changing atmosphere of security and threat landscape. The use case applications include cryptocurrencies, mobile payment, smartphones, , blockchain, smart factories, firmware and software protection, secure communication, etc.

Key Features of S97 Security Chip

Hardware

- Enhanced 32-bit ARM® SecurCore™ SC300™ CPU
- 1 MByte SOLID FLASH™
- Common Criteria EAL 5+

Parametrics

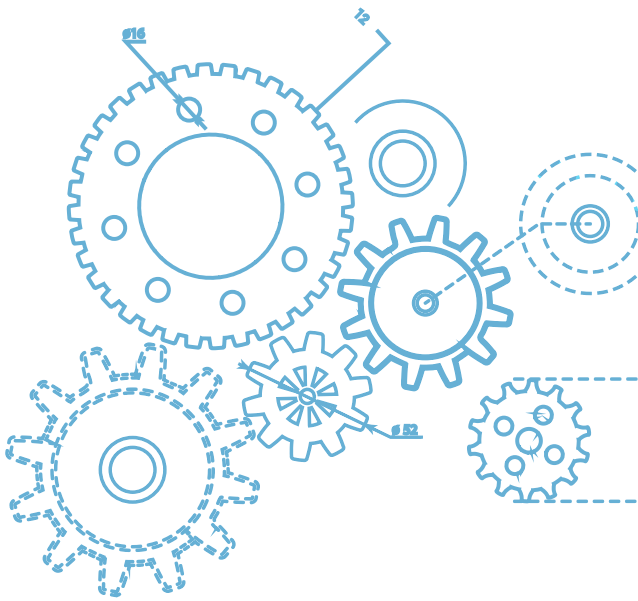
- Asymmetric Cryptography
  - ECC up to 521-bit ; RSA up to 4096-bit
- Symmetric Cryptography
  - AES up to 256-bit ; DES, 3DES
- True Random Number Generator
- Ambient Temperature
  - -25.0 °C 85.0 °C

Applications

- Secure eFlash (SOLID FLASH™) for MCU applications
- Mobile security (4G, 5G)
- Embedded secure element for anti-counterfeiting and content protection
- Finance (and blockchain) security

Leverage IKV Expertise

For systems processing transaction, confidential data and digital content, IKV aims to construct a pertinent subsystem, which can grant possessors complete control over the digital assets in transit and at rest.



Types of digital assets to be protected range from confidential data, which can be files that contain secret information, digital assets, which can be artificial intelligence (AI) codes and other kinds of intellectual properties, and cryptographic keys used for transaction.

Years of experience in embedded security enable IKV to embody robust security in any form factors to fit any system. On the given platform, IKV has exerted its ability to the greatest possible extent. From secure communication for national security to protection of digital content worth millions of US dollars, and cryptocurrency transaction used around the globe without any breaches, extensive exploration of its potential has not been marked with a period.

Competence

I. Tailor-made algorithm and mechanism

The quintessence of security lies in threat modeling and risk assessment. Security takes effect only when potential threats are successfully predicted. In light of it, to tackle security issues in the rapidly evolving threat landscape, we have practical and technical mastery of customizing security solutions for different use case applications.

II. Countermeasure against hardware attack

The never-ending pursuit of new vulnerabilities and attacks propels us to keep up with the top-notch countermeasure know-how. We implement countermeasures against one of the most notorious hardware attacks, side-channel attack (SCA), on both hardware and software, assuring customers a predominate position in the high-end market.

Success Stories about Our Customers

Over the past years, public awareness of security has been raised, specifically for those who confronted imminent attacks or targeted markets that abounded with counterfeit products. Under the circumstance, security becomes a must rather than a choice. A great number of vendors consequently reached us and voiced their concerns. They covered a wide range of use case applications, in which the security mechanism was designed on the Military-grade Omni platform and is still taking effect now. In these cases, the given platform has proven a real-world impact on vendors' cost, trustworthiness and high-end market penetrability.

The Military-grade Omni platform enables "security" and "usability" to go hand in hand because

- it supports a variety of form factors, including the smallest SIM, microSD, USB, PCIe
- a unique hardware root is in every system for identification and authentication
- customizability enables security by design, compliance security by default
- countermeasures are implemented to tackle a wide range of security issues
- a unique 32-bit CPU based on the ARM® SecurCore™ SC300™ controller is inside

Cryptocurrency Hardware Wallet

Complexity in cryptocurrency transaction and blockchain technology has raised the threshold of security related know-how. On the given platform, IKV has assisted several cold wallet vendors and exchanges with stroage schemas for key management and signing mechanisms adaptive to ranges of changing regulations. One of them has become the top global player, and another won the 2020 CES Innovation Award.

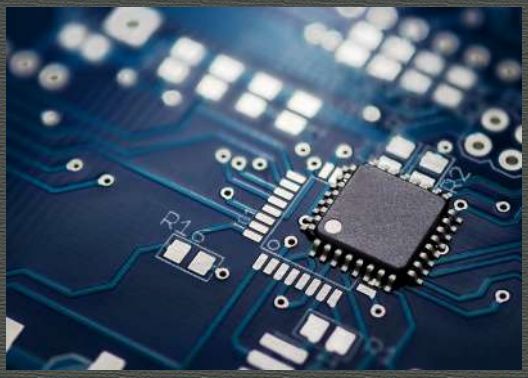
Firmware Protection

Over the past several years, discoveries of firmware vulnerabilites have flourished; partially owing to its ubiquity and robust hardware and operating system security, hackers can only target firmware to attack the system. IKV has provided customers with holistic solution protecting firmware, consequently securing digitial assets in the system. It consists of hardware-based root of trust for secure boot, key management for authentication and storage encryption.

Secure Communication

The number of connected mobile devices has drastically risen in these years, which also indicates user privacy is in jeopardy. Thus, the market for private messaging is picking up. IKV has built a cryptographic infrastructure for the world's first wireless privacy key using blockchain technology to encrypt data, messages, and calls from smartphones. The infrastructure can also be integrated with secure messaging apps, such as Signal and others.

Hardware Security Module



Hardware security modules are embedded with security chips where cryptographic key pairs are pre-stored in secure memory. Providing key pairs in the security chips are cracked, all the data in the system are to be revealed. The platform offers a robust hardware-based root of trust and secure storage of cryptographic secret and other confidential data. Together with KVSoftKey and Fusion FPGA, crypto services will be accelerated and thoroughly safeguarded.

Digital Right Management (DRM)

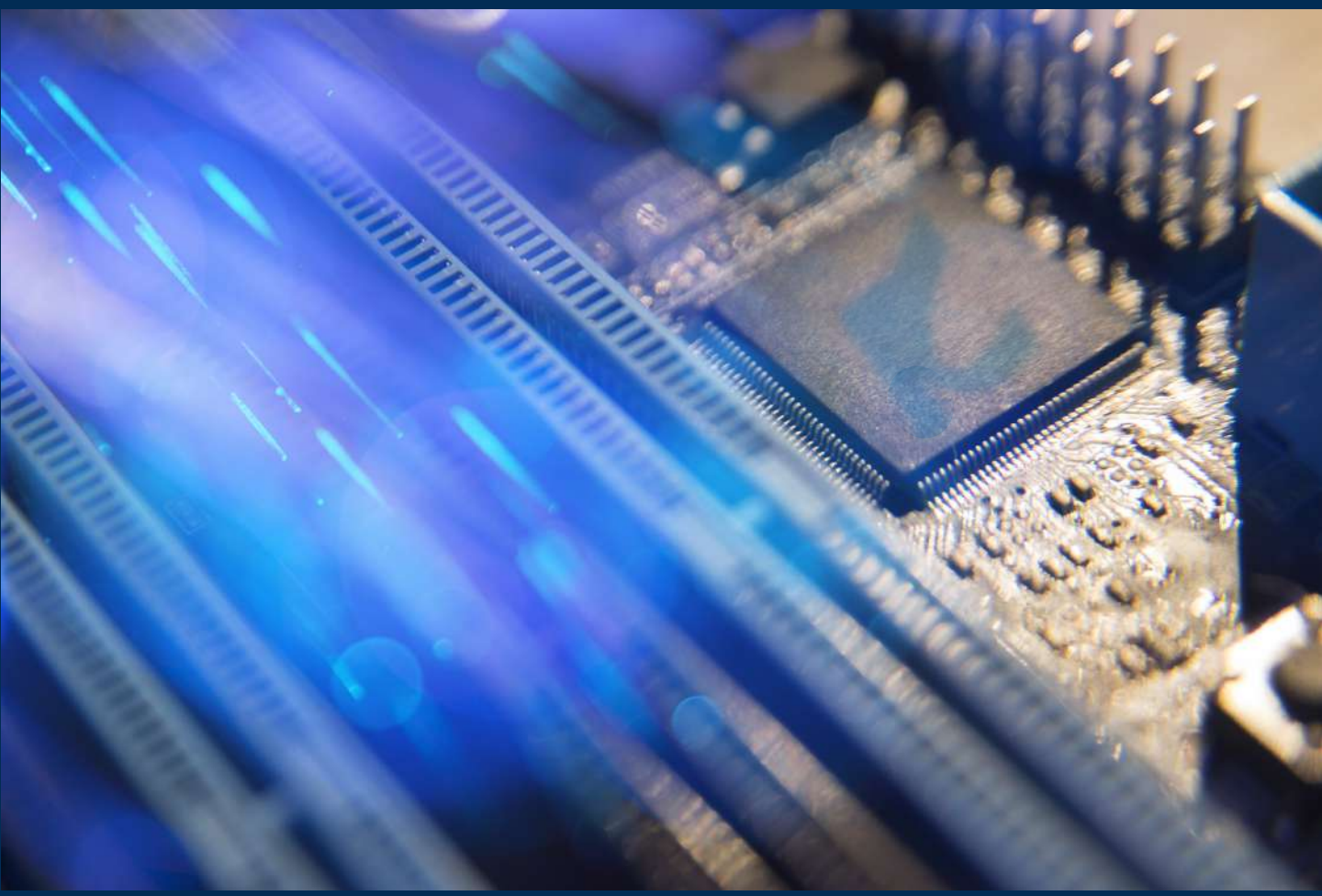
For customers requiring content protection of digital assets, such as game software, intellectual property, etc, IKV leveraged the S97 security chips to design systematic approaches, effectually restricting the way to copy content, preventing unauthorized distribution. Those having adopted our DRM solution have successfully secured their digital asset worth billions of US dollars. Attempts to comprise have also been proven failed.

FIDO Enabler in the Ecosystem

The FIDO strong authentication framework may be a revolutionary practice raising security to a higher level. The reason why it is not a revolutionary “technique” is that strong authentication based on the asymmetric cryptography system has been existing for decades. What FIDO Alliance does is to “assemble” hardware vendors, software vendors, service providers, operating systems, browsers and some consortiums for one aim – replacing vulnerable password-based authentication with the crypto-based one. The benefits accrue to data protection during data transferring, sharing and storage, audit logging, secure logon and access control. FIDO-certified solutions flip a new page of data protection allowing for greater awareness and transparency than accounts and passwords. Especially hardware USB authenticators, despite the downside being the additional efforts to safekeep the device, are sure to root out phishing and unauthorized access.

S97 Security Chip with FIDO Inside

For vendors who intend to implement the FIDO authentication framework on hardware authenticator in any form factor, we provide the ready-to-go crypto core, allowing for FIDO-compliant asymmetric cryptographic algorithms, FIDO-certified authentication mechanism and other value-added cryptographic functions. It is compatible with fingerprint authenticators, USB security keys, security cards, etc.



Secure Vault at your fingertips

With IKV-Tech expertise, a wide range of applications can attain tailor-made security leveraging the Military-grade Omni platform. We help customers optimize their existent security mechanism and enable security and usability to go hand in hand. All in all, our mission is to secure customers' business operation seamlessly in space and time, especially in an era where attacks always keep abreast.

About InfoKeyVault Technology

InfoKeyVault Technology (IKV-Tech) is a service company in embedded security, also an independent design house for security solutions from global security chip vendors, such as Infineon and Microsemi. IKV-Tech specializes in cryptographic implementation, software, firmware and hardware protection, cryptographic key management and countermeasures against hardware attacks so as to secure customers' digital assets and intellectual property.

Contact Us

+886 2-2934-3166

info@email.ikv-tech.com

www.ikv-tech.com

www.facebook.com/InfoKeyVault