



InfoKeyVault Technology

Secure Vault at your fingertips

 +886-2-2934-3166

 info@email.ikv-tech.com

 <http://www.ikv-tech.com>



Contents



- Background** •
- Milestone** •
- Philosophy** •
- Service & Solution** •
- Expertise** •
- Partnership** •
- News** •



InfoKeyVault Technology

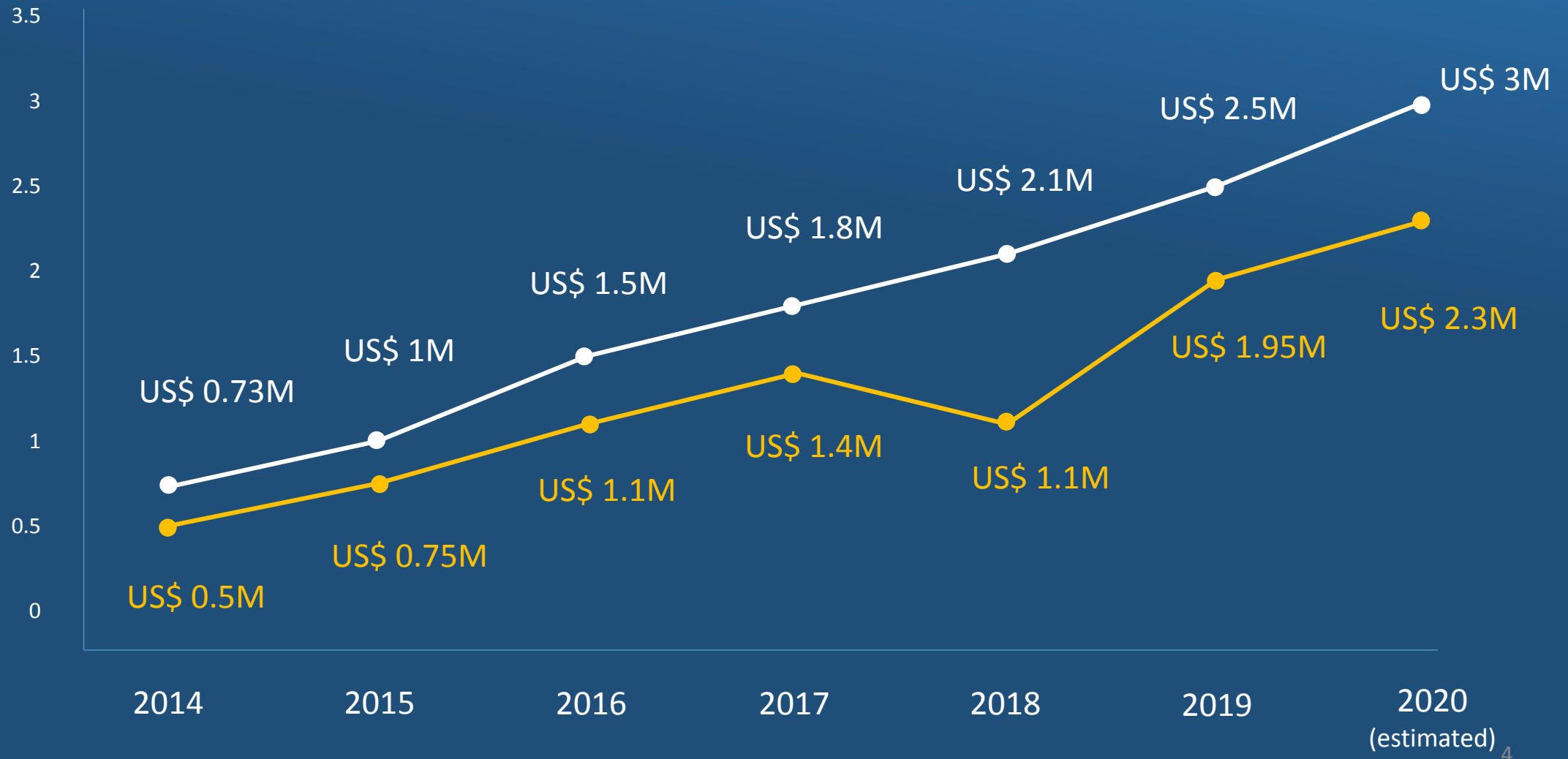
founded in 2006

Is a service company specializing in embedded security, also an independent design house (IDH) for security solutions from global chip vendors, such as Infineon

- Capital US\$ 0.65M
- Staff 23 personnel
- Revenue US\$ 2.5M/ 1.95M (gross margin)
- Customer government, military, company in AI, blockchain, gaming, communication

Catching up with the trend empowers profitability and sustainability

million US dollars revenue and **gross margin** per year





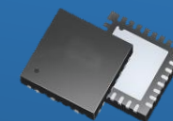
Be founded and Initiated collaboration with National Taiwan University



Collaborated with IBM in the establishment of OTA NFC key management system



Launched DSGuard security platform to protect online shoppers' privacy



Initiated the development of KV33/S-97 security chip platform

2006-2011

2012-2016

2017-2020



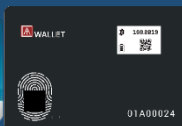
Initiated the development of hardware-based encryption scheme



Launched iBadge, a platform for IoT security solution



Announced partnership with global security chip vendors, Infineon and NXP



Engagement in cold wallets bringing success to customers



INTRINSIC ID

SONY

Initiated collaboration with Intrinsic ID and Sony

PHILOSOPHY

Mission Statement

Software-based cryptography is more **vulnerable to attacks** since the primitive and keys tend to reside in memory, posing threats to privacy, digital content and intellectual property.

Our mission is to build the “**root of trust**” on **reliable hardware-based platforms** to secure your privacy and digital assets.





Silicon IP of Algorithms



KVSoftKey with SRAM PUF



S10 Authentication Chip



iBadge Device Management



SLE97 Security Chip



Fusion FPGA Security Module



Cryptocurrency Hardware Wallet

SERVICE & SOLUTION





Algorithms

Available IP include

- AES
- SHA2 family
- SHA3 family
- ECC family
- SM2/SM4 (for China)

Key lengths and modes of operation are configurable. We also analyze potential threats in our customers' scenarios in order to tailor countermeasures against hardware attacks.

```
std::string ol_name = item->Attribute( "name" );
std::string type = item->Attribute( "type" );

if ( type == "sprite" )

    std::string item_name = item->Attribute( "name" );
    std::string spritename = item->Attribute( "spritename" );
    float x = boost::lexical_cast<float>( item->Attribute( "x" ) );
    float y = boost::lexical_cast<float>( item->Attribute( "y" ) );
    float offset = boost::lexical_cast<float>( item->Attribute( "offset" ) );

    SpriteDescList::iterator sp = sprite_descs.begin();
    for( ; sp != sprite_descs.end(); ++sp )
        if ( sp->name_ == spritename )
            break;

    if ( sp == sprite_descs.end() )
        throw "error";
```


KVSoftKey with SRAM PUF



Use case

KVSoftKey uses SRAM PUF technology to generate the hardware root of trust for software-based environments to perform cryptographic functions.

It also serves as the access key to secure elements, ensuring the key inside them are protected by secure channels and extracted only when authorization occurs.

KVSoftKey can achieve scalability in security and efficacy in cost and business operation for the following applications

- IoT & Smart factory
- Automobile ECU & Sensor
- Secure communication
- Hardware security module
- Cryptocurrency hardware wallet



We collaborate with Intrinsic ID and use Physically Unclonable Functions (PUF) to generate a root key, resembling a “fingerprint”, which is irreproducible, unique and unpredictable.

S10 Authentication Chip



Use case

S10 authentication chips aim to protect devices, circuit boards and other embedded systems from counterfeiting. It performs strong authentication featuring Elliptic Curve Cryptography (ECC) 163 bits, ensuring the security of application use cases as follows.

- Printer Cartridges
- Accessories
 - Earphones, docking stations, game controllers, chargers
- Peripherals (adaptors, etc.)
- Original replacement parts
- Diagnostic & medical equipment



Success story about our customers

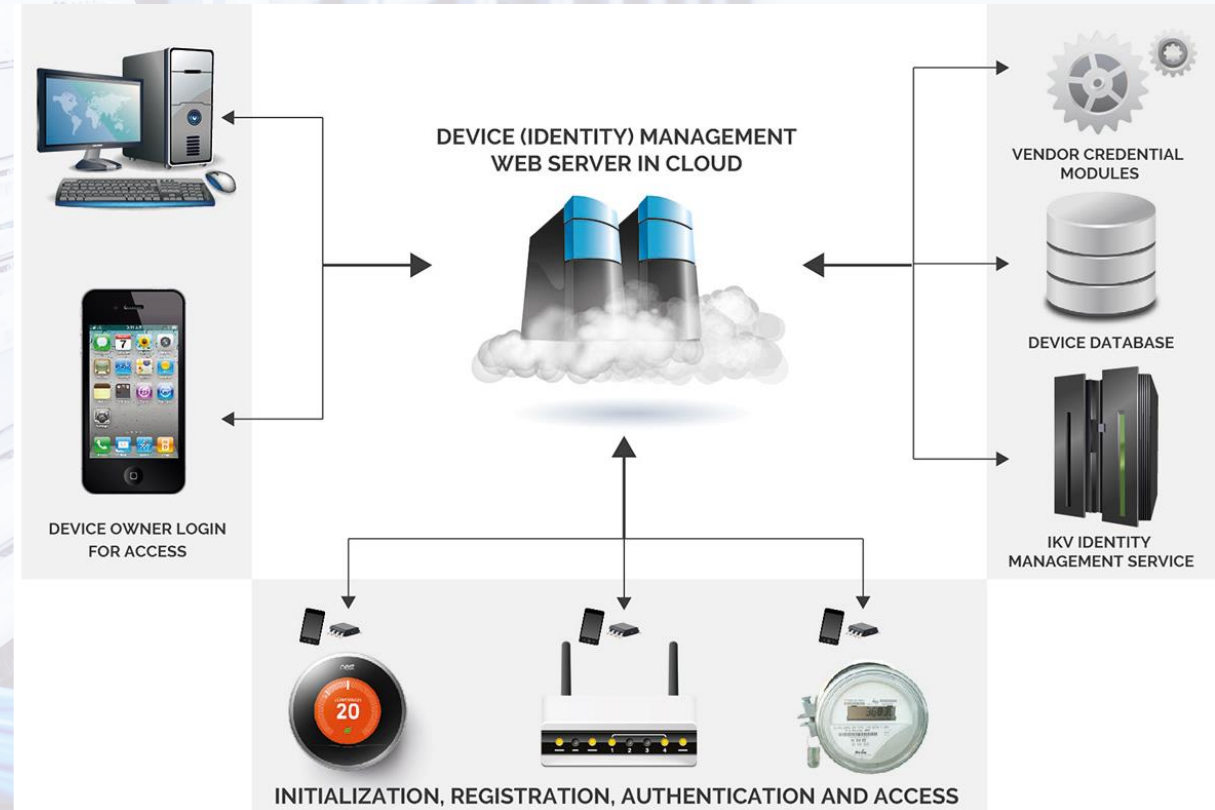


International Game System (IGS), a leading game software developer in Asia, has developed hundreds of popular video games. They use S10 authentication chips to protect devices from counterfeiting so as to manage the digital rights of their game software. An estimation of 120,000 gaming machines have been protected by S10 authentication chips. Attempt to compromise the content have also failed in these years.

Use case

iBadge device management platform aims to ensure legitimacy of client-side access to servers. By integrating security chips into devices, each device acquires a unique identification to log into the cloud. The server tests devices' authenticity via Elliptic Curve Cryptography (ECC) strong authentication. It can reduce the risk of counterfeiting, unauthorized access, DDoS and protect IoT systems. The applications include

- Smart lock
- Smart meter
- Surveillance web camera
- Smart city infrastructure



SLE97 Security Chip



Use case

Leveraging SLE97, Infineon's security chip with CC EAL 5+ certification, we tailor military-grade security solutions for different application use cases, including

- blockchain key management
- game software protection
- encrypted communication
- software IP protection
- firmware protection



Success story about our customers



AUTHENTREND



SecuX



CoolBitX



Injoy Motion



SAINT-FUN

Hardware wallets used to transact cryptocurrencies, **AT.Wallet**, **SecuX Hardware Wallet**, and **CoolWallet**, are integrated with SLE97 as well as tailor-made security mechanisms.

Saint-Fun and **Injoy motion** use SLE97 to protect game software. **I.X** designed privacy key cards integrated with SLE97 for secure communication.



Use case

The spirit of Fusion FPGA lies in robustness of security and eclectic cryptographic functions. Fusion FPGA uses physically unclonable function (PUF) to generate innate keys dwelling not in memory and extracted on need-basis only. The establishment of secure channels among MCUs and secure elements mitigates the risk of data breach in transit and at rest.



Success story about our customers

ZYXEL



Taiwan.gov.tw

We tailored a security mechanism for encrypted communication in collaboration with **Zyxel**. We also customized cryptographic algorithms for **Taiwanese Government**, providing them with Fusion FPGA implemented on PCIe cards and USB dongles, fulfilling storage encryption and cloud-based authentication.

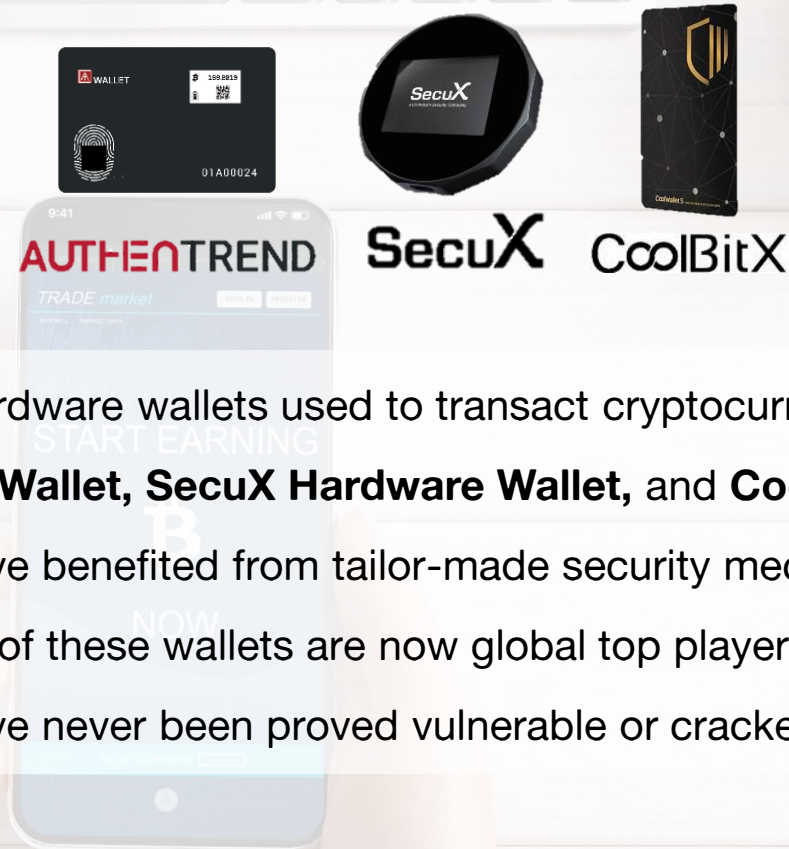


Use case

The essentials of securing crypto assets consist in key management, and the aspects of hardware and software should be covered. IKV has a great command of how transaction and cryptography work in blockchain-based applications, also the notion of implementation in both hardware and software to resist attacks.



Success story about our customers



Hardware wallets used to transact cryptocurrencies, **AT.Wallet**, **SecuX Hardware Wallet**, and **CoolWallet**, have benefited from tailor-made security mechanism. All of these wallets are now global top players and have never been proved vulnerable or cracked.

Why do our customers need us?



SERVICE & SOLUTION



Diverse threats and tailor-made security



Secure supply chain management



Threshold of domain knowledge



Security more than chip level security

Why do our customers need us?



SERVICE & SOLUTION



Diverse threats and tailor-made security

Security takes no effect if threats are falsely preassumed. We approach threats in various user scenarios and tailor solution specified for customers' environments.

Secure supply chain management

Supply chains of security chips should be adequately managed and monitored as those available online have been proven vulnerable. We import security chips from reputable vendors, assuring customers reliability and protected roots of trust.

Security is far more than just chip level security

Security is a system-level issue. Problem with a voice type may break the overall harmony. We specialize in building a holistic and system-level security mechanism, which is far beyond just integration of security chips.

Threshold of domain knowledge

Cryptographic implementation has a high mastery threshold. It requires resources from academic or research institutions, years of experience, and restricted access to supply chains.

A close-up, macro photograph of a computer chip, likely a CPU, mounted on a circuit board. The chip is dark and square, with a prominent shield-shaped logo in the center. It is surrounded by numerous gold-colored pins and solder points. The background is a blurred blue and white, suggesting a technical or industrial setting.

EXPERTISE

Our competence is centered on cryptography. We embody security concepts in any form and on any platform. We also analyze threat model, proposing solutions sticking to “security by design” and beyond just compliance.

EXPERTISE



Cryptographic
Implementation



Cryptographic
Key Management



Software, Firmware
and Hardware Protection



Countermeasures
against Hardware Attacks

EXPERTISE



Cryptographic
Implementation

Hardware-based cryptographic implementation requires specialities in mathematics, electrical engineering, and computer science. Mastery in these fields enables us to provide tailor-made algorithms and standard ones, and to implement them in software-based or hardware-based environments. The advantage allows for holistic risk mitigation mechanisms “from soft to hard” and a streamlined process of security by design.

Cryptographic
Key Management

Software, Firmware
and Hardware Protection

Countermeasures
against Hardware Attacks

EXPERTISE



Cryptographic
Implementation



Cryptographic
Key Management

Whether it is data in transit or at rest, master keys, encryption keys, derived keys and others should be taken great care of to prevent leakage. We manage cryptographic keys in a manner that complies with NIST SP 800-57/130, elucidating possible threats to our customers before implementing solutions. It is applicable from clouds to devices, from micro SD cards, USB dongles, PCIe cards to ARM-based circuit boards.

Software, Firmware
and Hardware Protection

Countermeasures
against Hardware Attacks

EXPERTISE

In the era of digitization and pervasive computing, our data are at risk of exposure as long as they are stored in digital forms. Computing even raises the possibility of leakage as physical parameters, such as power consumption can be measured in the process. We leverage characteristics of hardware and software to protect digital contents, to verify integrity, to resist tampering and counterfeiting, securing customers' digital assets and business profits.

Cryptographic
Implementation

Cryptographic
Key Management



Software, Firmware
and Hardware Protection



Countermeasures
against Hardware Attacks

EXPERTISE



Cryptographic
Implementation

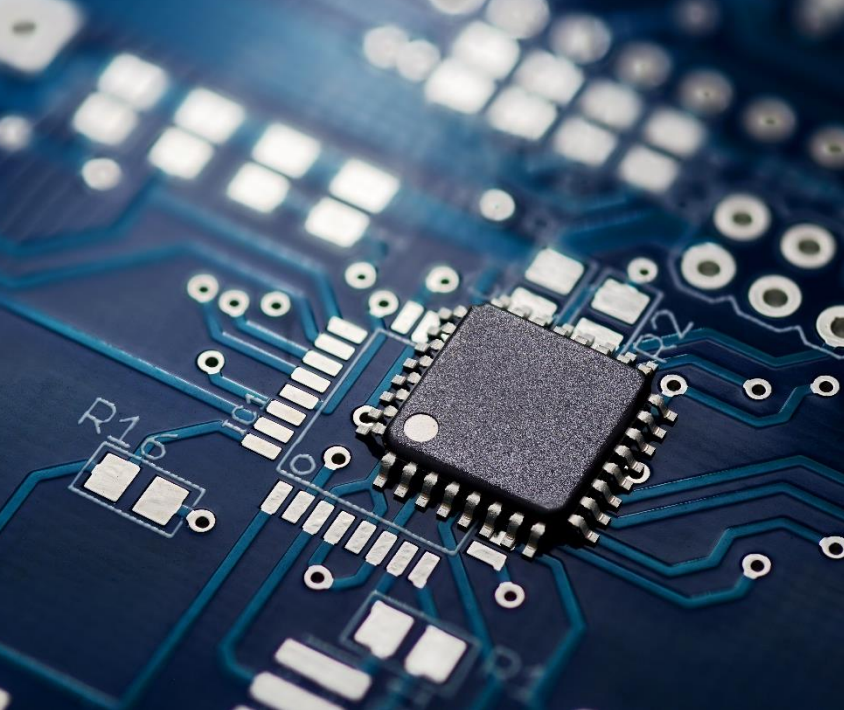
Security is dynamic. It is effective when assumed attacks are truly imminent. Without threats or if risks are falsely assumed, security takes no effect. Our research and development team keeps exploring top-notch hardware attacks and reacts by implementing countermeasures compliant with FIPS and Common Criteria. The one we have accumulated experiences of addressing is side-channel attack (SCA).

Cryptographic
Key Management

Software, Firmware
and Hardware Protection



Countermeasures
against Hardware Attacks



Enterprises Should Prepare for Quantum-Computer Attack as Early as Possible

CONFERENCE



Device Identity Management Solution for Smart Homes




IKV-Tech Secures the Last Mile to IoT Security

NEWS

SOLUTION



THANKS

 +886-2-2934-3166

 info@email.ikv-tech.com

 <http://www.ikv-tech.com>

