物聯智慧股份有限公司
ThroughTek Co., Ltd.

ThroughTek Information Security White Paper

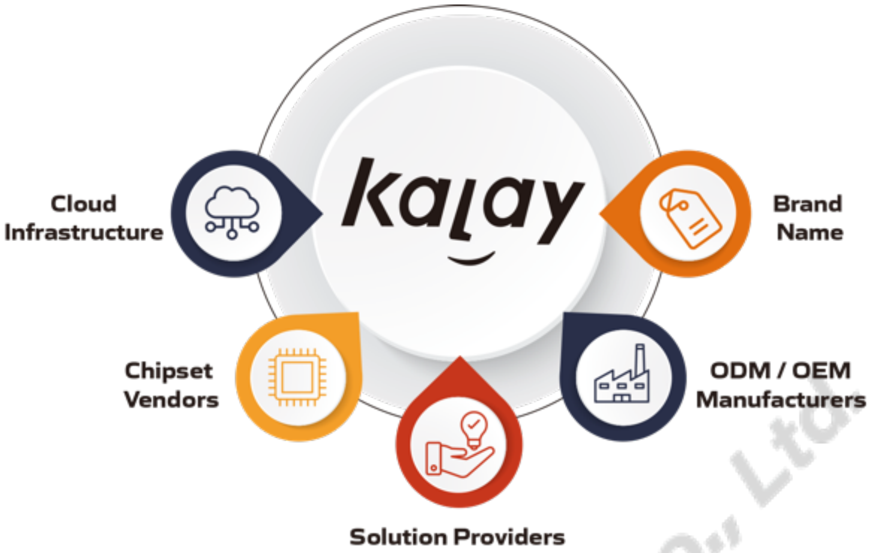
2023/6/30

TABLE OF CONTENTS

1. THROUGHTEK (TUTK) INTRODUCTION

ThroughTek (TPEx 6565, hereinafter referred to as TUTK or the Company) was established in 2008 in Taipei, Taiwan, as a cloud service platform solution provider for the Internet of Things (IoT). TUTK is actively dedicated to device connectivity technology and cloud service platform development. Initially, TUTK focused on developing easy-to-configure and easy-to-operate peer-to-peer (P2P) connection technology, primarily for consumer video surveillance products. With the rise of the Internet of Things (IoT), there has been a continuous increase in demand for software connectivity solutions applied to various hardware products. Leveraging its extensive experience in hardware and software integration, TUTK has further introduced the Kalay Cloud Platform. This platform expands the service scope for enterprise customers who are looking to enter the IoT market.

Kalay Cloud Platform is built upon excellent peer-to-peer (P2P) connection technology, enabling seamless operation across various operating systems. It offers flexible and modular services that empower brands or hardware manufacturers to enhance the value of their products with cloud-based services. With its core Kalay Cloud Platform, TUTK has fostered close partnerships with major OEM/ODMs, brands, system integrators, and chip vendors worldwide. These partnerships enable TUTK to facilitate rapid product development, expedite time-to-market, and achieve cost savings while catering to diverse customer requirements. Kalay Cloud Platform allows for API integration with third-party services, enabling customers to adopt diverse business service models. Currently, the platform provides over ten functional modules, including video transmission, cloud recording, data collection and analysis, remote control and management of hardware devices, push notifications, and more. Customers have the flexibility to choose and combine these modules based on specific market requirements and their needs.



Picture: The Ecosystem of Kalay Cloud Platform

1.1 INTRODUCTION OF KALAY CLOUD PLATFORM

Based on peer-to-peer (P2P) connectivity technology, Kalay Cloud Platform offers a range of modular functions to assist customers in developing diverse IoT products with seamless software and firmware integration. Kalay Cloud Platform ensures that the products are user-friendly, reliable, and secure.

Kalay Cloud Platform is widely used in various applications, offering customizable services, project management, and application development to cater and meet specific customer requirements. This comprehensive support empowers customers to introduce their smart products or services to the market quickly.

Furthermore, customers have the option to adopt TUTK's products, including Cloud VMS (Video Management System), Hausetopia App, or DMP (Data/Device Management Platform), which are developed using the core technology of the Kalay Cloud Platform. By doing so, customers can expand and enhance their own products and services.

1.2 KEY FEATURES OF KALAY CLOUD PLATFORM

Through Kalay Cloud Platform, users have the ability to develop a reliable, secure, and scalable IoT solution. The platform encompasses essential functions, including device connectivity, data management, application development, and security protection. These features empower users to effectively harness IoT technology and achieve intelligent and efficient IoT applications. The following are the key features of the platform:

- **Device Connectivity and Management:** Kalay Cloud Platform offers device connectivity and management features that facilitate seamless communication between devices and the platform. It supports diverse communication protocols and connection methods, including Wi-Fi, Bluetooth, Ethernet, and more, to cater to various device types.
- **Data Collection and Analysis:** Kalay Cloud Platform enables real-time data collection from connected devices and offers data storage and analysis capabilities. This empowers users to capture and analyze data generated by devices, providing valuable insights and decision support.
- **Application Development and Deployment:** Kalay Cloud Platform provides tools and environments for application development, allowing developers to build and deploy IoT applications quickly. It supports various programming languages and frameworks, while offering a rich set of APIs and SDKs for easy integration and extension of functionalities.
- **Security and Privacy Protection:** Kalay Cloud Platform prioritizes security and privacy protection by implementing multiple security measures to safeguard device and data security. It provides features such as identity authentication, data encryption, and access control to ensure that only authorized users can access and operate devices and data.

2. SECURITY RESPONSIBILITY ATTRIBUTION

The protection of data security on the client side and device side is fundamental to all cloud services. Users control devices using their cell phones, and important data is transmitted end-to-end through the network. As a pioneer in the IoT platform service field, TUTK prioritizes being a stringent gatekeeper for its customers. The Company implements multiple protections, including cloud servers, software and firmware technologies, encryption verification mechanisms, etc. Data security protection is held to the highest standard within the Company. TUTK continually pays attention and adopts the latest security technologies and measures to ensure the utmost protection of its customers' data. TUTK is committed to building a secure and reliable Internet of Things platform, providing its customers with the most secure and dependable services.

2.1 RESPONSIBILITY ATTRIBUTION

TUTK is responsible for security management, including operating services and data exchange, on the cloud platform. Furthermore, TUTK holds the responsibility for ensuring the security of the cloud platform and servers. However, if customers develop their own applications (Apps), self-hosted servers, or hardware to connect to our software technology (including the utilization of our SDK), they are solely responsible for securing their applications and data. This responsibility encompasses adhering to security specifications for hardware, servers, and applications. With the exception of the chart provided below, customers bear the responsibility for their own security.

Type	Hosted or co-located by TUTK			
Server	Alibaba Cloud	Google Cloud	Amazon	IDC/ Telecoms
Responsibility	TUTK and the cloud platform service provider share joint responsibility			
Application, Cloud Platform	Both TUTK standard edition and full customization options			
Responsibility	TUTK takes on the responsibility			

2.2 TUTK SECURITY RESPONSIBILITY

TUTK collaborates with various cloud hosting service providers, including Amazon, Google, Alibaba Cloud, etc., and deploys hosted server/co-located server service areas according to customer requirements to ensure the quality of customer service and the security of device connections.

Additionally, TUTK collaborates with cloud hosting service providers to ensure that the connections provided to customers maintain a high level of security. This primarily involves safeguarding the security of customer data, preventing vulnerabilities, and hacking attacks, and ensuring the security of equipment management and upgrades.

Furthermore, when it comes to user privacy information, the Company acknowledges the importance customers and users place on their privacy rights. TUTK upholds its commitment to privacy protection, as outlined in the privacy protection policy document.

2.3 CUSTOMER SECURITY RESPONSIBILITY

When utilizing TUTK's solutions, customers should strictly adhere to the Company's documentation, configuration security, and interfacing requirements. Additionally, customers must ensure the security of their own servers, clients, or hardware products. For applications (Apps)/platforms developed by customers using TUTK's SDK, TUTK only provides technical support and cannot guarantee overall security. Customers are responsible for related to the applications (Apps)/platforms that TUTK modifies or customizes on their behalf.

3. TUTK INTERNATIONAL COMPLIANCE AND CERTIFICATION

As a global cloud service platform solution provider, TUTK offers products and services that comply with international standards and certifications. The following are TUTK's international compliance and certifications:

3.1 ISO/IEC 27001

ISO 27001 is the Information Security Management System (ISMS) standard developed by the International Organization for Standardization (ISO). By obtaining this certification, TUTK confirms that it has established and implemented a comprehensive information security management system capable of ensuring the security, availability, and integrity of its information.

The ISO 27001 certification encompasses the following areas:

Risk Management: Ensuring the security of data, systems, and services by assessing and managing risks.

Security Controls: Meeting the latest security control requirements to protect against unauthorized access and use.

Audit and Control: Ensuring the ongoing effectiveness of the information security management system through dedicated audit and control mechanisms.

By obtaining ISO 27001 certification, TUTK demonstrates its commitment and expertise in information security for its customers and partners. It also reflects the Company's dedication to continuous optimization and improvement in security management and the recognition and acceptance by international.

3.2 GDPR (GENERAL DATA PROTECTION REGULATION)

GDPR (General Data Protection Regulation) is a data protection regulation implemented by the European Union on May 25, 2018. It aims to protect the privacy and rights of personal data while requiring organizations to comply with specific legal requirements for processing and protecting personal data. The following are key regulations under GDPR:

Data Protection: As a company providing IoT and connected device solutions, TUTK may process and store large amounts of personal data. According to GDPR, the processing of personal data must meet specific legal requirements, including legality, transparency, purpose limitation, data minimization, accuracy, and security. By complying with GDPR, TUTK ensures the proper protection of personal data, reducing the risk of data leakage and privacy violations.

Protection of User Rights: GDPR grants individual data subjects specific rights, such as access, correction, deletion, restriction of processing, and data portability. As a data processor, TUTK can implement processes and controls to ensure users can effectively exercise their rights. This fosters trust in TUTK and demonstrates the Company's commitment to privacy and data protection compliance.

Risk Management: Compliance with GDPR enables TUTK to assess and manage risks and implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, or corruption.

3.3 CCPA (CALIFORNIA CONSUMER PRIVACY ACT)

CCPA (California Consumer Privacy Act), effective January 1, 2020, is designed to protect the personal information privacy rights of California residents. The Act grants consumers several rights, including:

Access to Personal Information: Consumers have the right to request access to the personal information collected by organizations.

Deletion of Personal Information: Consumers can request that an organization delete their personal information.

Disclosure: Organizations are obligated to provide transparent information regarding the purposes for collecting and using personal information when it is collected.

No Sale of Personal Information: Consumers have the option to restrict organizations from selling their personal information to third parties.

TUTK is CCPA certified and is dedicated to complying with the law. This entails taking several measures to ensure complete protection and respect for the privacy of its customers' personal information. By obtaining CCPA certification, TUTK demonstrates its commitment to safeguarding the privacy of its customers' personal information, providing you with added confidence and reassurance.

3.4 OTHERS

The company places a high level of importance on information security compliance. It has implemented a range of measures to safeguard the data and information of its customers. The following outlines the company's practices regarding information security compliance:

Compliance with Applicable Laws and Regulations: The Company complies with applicable information security laws and regulations, including but not limited to the GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act) and other applicable privacy protection laws.

Data Encryption: The company employs robust data encryption technology to ensure the security of customer data during transmission and storage. By utilizing encryption protocols and secure algorithms, TUTK guarantees the confidentiality and integrity of sensitive data.

Access Control: TUTK has implemented stringent access control measures to ensure that only authorized employees can access and process customer data. TUTK restricts data access to only necessary personnel, ensuring that only individuals with a legitimate need-to-know can handle the relevant data.

Security Audits and Monitoring: The Company conducts regular security audits and monitoring to promptly identify and protect its systems and networks. TUTK closely monitors for potential security threats and unusual activities, taking appropriate measures to address and prevent them.

Employee Training and Awareness: The Company provides comprehensive employee training to enhance awareness and understanding of information security compliance. TUTK encourages employees to follow best safety practices and regularly update their knowledge and skills.

Through these information security compliance measures, the Company is dedicated to safeguarding the security and privacy of its customers' data. TUTK will continue to allocate resources and efforts to continually improve its information security practices, addressing emerging threats and risks.

4. TUTK TECHNICAL SAFETY COMPLIANCE

Technical Safety Compliance entails ensuring that the Company adheres to applicable safety regulations and standards during the implementation and operation of its technology. The following outlines its approach to technical safety compliance.

4.1 SECURE DEVELOPMENT PRACTICE：

The Company adheres to the Secure Development Lifecycle (SDL) and best practices to integrate security measures into software and system development processes. TUTK conducts code reviews and vulnerability scans to identify and mitigate potential security vulnerabilities and weaknesses. The following practices are followed:

- **Secure Coding Guidelines:** The Company has established secure coding guidelines that outline best practices and specifications to be followed during the development process. These guidelines cover areas such as input validation, output coding, security configuration, and error handling to mitigate common security vulnerabilities.
- **Security Audits:** The Company conducts code audits to identify potential security vulnerabilities and weaknesses. Regular code reviews allow TUTK to identify and address security issues at an early stage, ensuring code quality and security.
- **Security Testing:** The Company performs system-level and application-level security testing, including black-box and white-box testing. By conducting simulated attacks and vulnerability testing, TUTK can evaluate the security of the system, identify potential vulnerabilities, and take appropriate measures to address them.
- **Security Training:** The Company provides security training to its development teams, enabling them to understand common security threats and attack techniques, and equip them with defensive measures. This helps enhance the security awareness and skills of its developers, ensuring that security is considered throughout the development process.

4.2 AUTHENTICATION MECHANISMS AND ACCESS CONTROL：

TUTK employs multiple authentication mechanisms to ensure that only authorized users can access the system and data. It has implemented stringent access control policies, including role and permission management, to grant only the necessary permissions. All servers require PKI key access, which is issued only to a limited number of personnel or authorized administrators.

- 24-hour automatic/manual monitoring to detect abnormal visits and behaviors on servers.
- Servers are distributed across multiple locations worldwide to eliminate any single point of failure.
- Regular system updates to address potential security vulnerabilities.
- Continuous testing and scanning for any unexpected vulnerabilities.

4.3 CLOUD SERVICE STORAGE：

TUTK’s global servers are hosted at trusted cloud service providers, such as AWS, Google, and Alibaba Cloud, among others. By leveraging these data centers, TUTK gains access to their advanced security measures and stringent access policies, guaranteeing the confidentiality and security of its customers' data.

TUTK is fully committed to implementing best security practices, which include continuous monitoring and updating of systems and servers to ensure the highest level of protection for customer data. TUTK regularly assesses and enhances its security measures, employs encryption technology to safeguard data during transmission and storage, implements stringent authentication and access control measures, and takes proactive and contingency measures to address potential security threats.

4.4 APPLICATIONS：

- TUTK utilizes advanced AWS or Softlayer security services, which offer advanced attack detection, prevention, and analysis capabilities.
- TUTK implements strict rules-based firewall blocking, which ensures that only necessary ports are open and accessible via specific access protocols.
- TUTK performs large-scale log analysis to strengthen server security and optimize resource allocation.
- Additionally, TUTK collaborates with Trend Micro Inc. for enhancing security.

4.5 DATA TRANSMISSION：

The Company has implemented various encryption and protection measures to ensure secure data transmission and security. These measures are in place to establish secure connections and facilitate data transfer between devices and cloud services, as well as between different cloud environments. The following are some of the security measures employed by the company:

- **HTTPS connection:** The company utilizes the HTTPS protocol to establish secure communication between devices and cloud services. By encrypting the SSL/TLS protocol layer over HTTP communication, data confidentiality and integrity are ensured during transmission. This measure enhances the security of data exchange between devices and the cloud service.
- **Data encryption:** TUTK utilizes the AES256 (Advanced Encryption Standard 256-bit) symmetric encryption algorithm, which employs a 256-bit key for data encryption and decryption. AES256 offers a higher key length and stronger security, making it widely used for safeguarding sensitive data. Through multiple rounds of encryption operations, it ensures the confidentiality of data and requires the correct key for decryption.
- **Secure communication:** Depending on the device's capability and configuration, customers can choose to utilize TLS 1.2 or DTLS 1.2 for secure communication. TLS 1.2 and DTLS 1.2 are protocols designed to

ensure the protection of network communication by providing encryption, integrity verification, and authentication. TLS 1.2 is suitable for reliable transmission protocols, such as TCP, while DTLS 1.2 is suitable for real-time communication and data transmission based on unreliable transport protocols, such as UDP. TUTK also has plans to periodically upgrade the versions of TLS and DTLS.

- **Packet scrambling:** TUTK supports the scrambling of packets using compatible devices. Spoofing technology enhances the randomness and complexity of data, thereby enhancing data security and making it more challenging for unauthorized individuals to parse and decrypt the data.

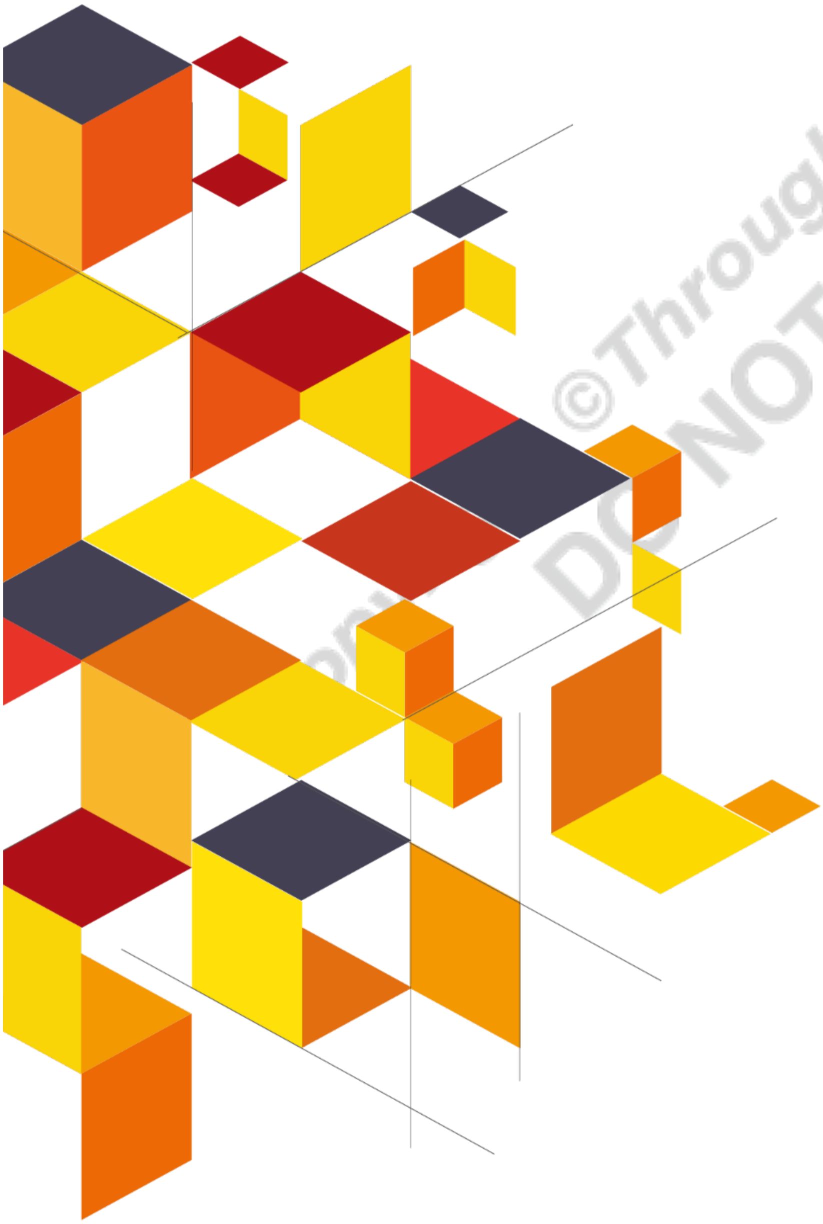
Through the aforementioned encryption and protection measures, TUTK is dedicated to ensuring secure data transmission between devices and safeguarding the confidentiality and integrity of its customers' data. TUTK continuously researches and implements the latest security technologies and algorithms to mitigate emerging security threats and offer dependable data protection solutions.

5. PRODUCT SECURITY INCIDENT RESPONSE TEAM（PSIRT）

The Security Incident Response Team (PSIRT) is responsible for handling security incidents related to our products. This includes assessing, mitigating, and publicly reporting security issues with our products.

The mission of the PSIRT is to address product safety issues. If a safety issue is reported through internal testing, by researchers, or by customers, the Company will promptly evaluate the incident. If the issue is confirmed, the Company will collaborate with the R&D team to resolve the safety concern.

To safeguard users, the Company will not disclose all the details of a safety issue. Instead, only the necessary information will be released prior to providing a fix or resolution. This approach ensures that users are protected while the necessary steps are taken to address the safety issue.



Follow Us On

or visit www.throughtek.com