Tencent Real-Time Communication

Protocols and Policies

Product Documentation

Contents

Protocols and Policies
Compliance

Last updated：2023-10-13 17:27:46

TRTC meets the compliance requirements of multiple countries and industries. We are dedicated to ensuring the **security, compliance, availability, confidentiality**, and **privacy** of our services. We offer support that helps you and your customers **meet different regulatory requirements so you can reduce auditing costs and improve your auditing and management efficiency.**
TRTC has passed SOC 1, SOC 2, and SOC 3 audits, meets the requirements of China Cybersecurity Law MLPS 2.0, and is certified to ISO 9001, ISO 20000, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 29151, CSA STAR, NIST CSF, BS 10012, and K-ISMS.

Security White Paper

Last updated：2023-10-13 11:36:43

1. Overview

Leveraging Tencent's years of experience in network and audio/video technologies, TRTC offers unified and standardized application programming interfaces (APIs) for group audio/video call and low-latency interactive live streaming solutions. It also provides software development kit (SDK) solutions compatible with mainstream operating systems and platforms for different industries and scenarios. With TRTC, you can quickly develop low-latency and high-quality interactive audio/video services at low costs.
As an industry leader in real-time audio/video PaaS cloud services, TRTC places great importance on data and user privacy security. TRTC always gives top priority to data and user privacy security and incorporates them in day-to-day development of security capabilities. To help you understand the security protection capabilities of TRTC, the following describes the security development and security compliance audit of TRTC PaaS services.

2. Security Compliance and Privacy Protection

Security compliance is the foundation for the development of TRTC, which meets the compliance requirements of different countries and industries. In addition to ensuring the security, compliance, availability, confidentiality, and privacy of the services it provides, TRTC also provides relevant support for you to meet your and your customers' compliance requirements, reduce repeated investment in audit work, and improve auditing and management efficiency.
TRTC has passed SOC 1, SOC 2, and SOC 3 audits, meets the requirements of China's Cybersecurity Classified Protection 2.0, and is certified to ISO 9001, ISO 20000, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 29151, CSA STAR, NIST CSF, BS 10012, and K-ISMS.

Security Compliance and Privacy Protection	Description
ISO/IEC 27001: 2013 Information security management standard	ISO/IEC 27001: 2013 is a fundamental, internationally recognized standard for information security management systems. TRTC is certified to ISO 27001:2013, which reflects enterprise commitment to security and demonstrates that a set of scientific and effective systems for enterprise information security management is in place to provide reliable information services.
ISO/IEC 27017: 2015 Guidelines for	ISO/IEC 27017: 2015 is a practical standard for the information security of cloud services which provides specific security controls and their implementation guidelines for cloud

information security controls applicable to the provision and use of cloud services	service providers and customers. ISO 27017 is a supplementary standard to ISO 27002. It is designed to provide a security specification for cloud-based development and Ops for cloud vendors. TRTC is certified to ISO/IEC 27017, demonstrating sufficient information security management and protection capabilities.
ISO/IEC 27018: 2019 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	ISO/IEC 27018: 2019 is a code of practice for protection of personally identifiable information in public clouds. Based on the ISO/IEC 27001 information security standard, it provides supplementary controls applicable to the protection of personally identifiable information in public clouds and strengthens public cloud capabilities for protection of personally identifiable information. TRTC has passed ISO 27018 certification, which demonstrates that enterprises have reached a high standard of industry best practices in protecting the security of enterprise data, intellectual property, documentation, and cloud IT systems.
CSA STAR Certification	Based on the Cloud Control Matrix (CCM) of Cloud Security Alliance (CSA), an international not-for-profit organization, CSA Security Trust Assurance and Risk (STAR) is a global cloud computing security certification which validates that cloud computing vendors meet the specific requirements in the field of cloud computing security. As an enhanced version of ISO/IEC 27001 for information security management systems, it visualizes cloud security issues and provides an intuitive framework for cloud vendors to assess their security management capabilities. TRTC has received CSA STAR Certification, demonstrating its cloud service protection capabilities.
SOC Audit	SOC reports are a series of reports related to internal controls of a service organization issued by professional third-party accounting firms in compliance with the applicable guidelines of the American Institute of Certified Public Accountants (AICPA). As a leading cloud service provider, Tencent Cloud adopted the 2017 version of the trust service criteria during the SOC audit in 2017, becoming the first provider in China to follow the 2017 version. The service certification report validates that TRTC has established and implemented effective internal controls and will regularly submit to third-party audits to ensure compliance with the requirements of the certification report.
Cybersecurity Classified Protection Certification	Cybersecurity Classified Protection 2.0 (CCP 2.0) came into force as of December 1, 2019. CCP 2.0 focuses more on active protection as well as the security and reliability, dynamic perception, and full audit from passive protection to the entire pre-event, mid-event, and post-event process, fully covering traditional information systems, basic information networks, cloud computing, mobile internet, IoT, big data, and industrial control systems. In line with CCP 2.0 and applicable regulations, Tencent Cloud public cloud TRTC PaaS service platform has been registered and evaluated for compliance with Cybersecurity Classified Protection Level 3, indicating that it provides services required for CCP compliance for enterprise users engaging in varied industries and businesses on the cloud platform.

3. Data Security

Data security is one of the top concerns of TRTC. TRTC processes your data in a lawful and compliant manner as necessary to ensure data security. This section describes the data security technical controls and management policy implemented by Tencent Cloud and TRTC.

3.1 Data security policy

TRTC focuses on confidentiality, integrity, and high availability as prerequisites for the development of data security and incorporates data security management and development into its development practices. Tencent Cloud will always be committed to ensuring the availability, confidentiality, and integrity of your data as follows:
Availability: It guarantees the high availability of data through Tencent Cloud's private network transfer protocol.
Confidentiality: It prevents unauthorized access and eavesdropping.
Integrity: It ensures the integrity of your data and protects the data from being forged.
TRTC provides all of its employees with regular training in data security, privacy compliance, and data encryption protection and enters into a confidentiality agreement with the employees to ensure the data availability, confidentiality, and integrity during daily operations.

3.2 High data availability

TRTC strives to provide highly available audio/video PaaS data services:
Globally distributed IDCs: TRTC has many IDCs providing services globally. Any attack on one IDC cannot affect others or the overall services, implementing isolation-based protection.
Fault isolation and recovery: If an IDC is subjected to malicious attacks that are difficult to prevent, such as a denial-of-service (DoS) attack, TRTC will reasonably handle the faulty server to ensure the overall service stability and availability.
DDoS mitigation: TRTC has deployed anti-DDoS firewalls in each IDC and has sufficient capabilities and resources to control the risk of DDoS attacks.

3.3 Data collection

TRTC collects only data fields with the user's consent and only those necessary for the services and at the minimum granularity. User data collected by you such as application login information, identification, passwords, payment information, name, and address is kept by you, not on the TRTC platform.

3.4 Data masking

To protect your data privacy, TRTC masks the enterprise and personal information in the console before displaying it. This policy applies also to TRTC's internal systems and other products, such as the internal management platform, log printing, and monitoring and alarming channels.

3.5 Data usage and storage

Your personal or enterprise user data, end user data, audio/video call data, and system operation and security data are categorized before being stored to ensure the compliance and security of your data.
The development, test, and production environments are strictly isolated during TRTC development to ensure that your actual data will not be directly used for development and testing. In addition, the confidential information of you and users, such as passwords, will be stored in an encrypted manner.
Developers and users who use the recording SDK on the on-premises server and the on-cloud recording feature provided by TRTC can record all or part of the call content, and all video/audio recordings are directly written to the storage server provided by the developers and users, not on the TRTC server for storage.

4. Security of TRTC PaaS Services

A low-latency and high-quality real-time interaction solution has demanding requirements for TRTC. In the process of developing audio/video PaaS services, TRTC fully assesses the technical and security risks to its architecture, follows the security risk control system in the compliance standard to the greatest extent, and implements it across the development of audio/video PaaS services so as to provide a set of high-quality, stable, and secure audio/video PaaS solutions for developers and users.

4.1 Security of the transfer network

Based on the Tencent Cloud private transfer network, TRTC has developed an audio/video platform that features ultra low-latency, high-quality transfer and supports real-time interaction for millions of users. The private transfer network is one of the core TRTC PaaS services. It offers compliant and secure service support for signaling connection, authentication, real-time scheduling, and real-time transfer of audio/video data on the TRTC terminal. In addition, to provide secure and stable services for developers and users, taking into account the security factors faced by the current internet environment, the architecture design of Tencent Cloud private transfer network incorporates the following controls.

Security Control of Transfer Network	Description
Encrypted transfer	To ensure the confidentiality of audio/video data during transfer, TRTC provides built-in encryption and custom encryption for the transfer linkage. By default, built-in encryption is enabled globally for TRTC PaaS, covering the entire data linkage. This ensures the encryption security of data transfer.
Resource isolation	TRTC allocates dedicated resources for each TRTC application (SdkAppId) to ensure its independence of other projects and provide a secure and reliable guarantee of computational resources. After registering in the TRTC console, developers and users only need to perform

	simple operations in the console to create TRTC applications (SdkAppId) and allocate corresponding resources.
Room isolation	TRTC creates an independent isolation channel (Roomid) for the transfer of each type of audio, video, or message data. All rooms are logically separate, and only if a user uses the TRTC application with the same `SdkAppid` and the same room name can the user join the same channel. A room is created when a session starts and terminated when the session ends (when the last user leaves). In this way, transfer isolation is implemented at the room level.
Identity verification	When a user uses a TRTC application and connects to the TRTC PaaS services, TRTC will use the authentication information generated based on the `SdkAppid` and key to perform authentication for room entry, so as to help developers and users authenticate their users through strong authentication.

4.2 Security of the SDKs

TRTC provides SDKs for different platforms such as iOS, Android, macOS, Windows, web, and mini program for integration as needed. It not only offers simple, secure, and stable audio/video SDKs that are easy to integrate for developers and users.
TRTC also strives to create compliant and secure audio/video PaaS services for developers and users, in an attempt to reduce their efforts to cope with compliance regulation and security threats to data and information.

SDK Security Support	Description
SDK security and compliance	The reliability and security of TRTC SDKs are one of the guarantees of basic TRTC capabilities. During feature iteration, TRTC will fully assess the reasonableness of feature requirements in terms of compliance and privacy and their security risks, so as to ensure compliance with Tencent Cloud's compliance and privacy policy. During feature implementation, TRTC will perform adequate and necessary quality security tests and perform security checks where third-party SDKs or library files are imported or integrated, particularly compliance verification.
SDK content encryption	TRTC SDKs can use AES-128 symmetric keys to encrypt all audio/video data streams and messages at the data level. The encrypted data is sent to the nodes in the TRTC room over the Tencent Cloud private transfer protocol and eventually decrypted by the receiving terminal for rendering, ensuring data security and confidentiality during transfer.
Benefits of SDK security and compliance to developers	TRTC is dedicated to providing high-quality, secure, and lawful audio/video PaaS services for developers. TRTC SDKs come with built-in secure encryption to help developers and users improve the data security and privacy compliance of TRTC, meet customers' security and privacy requirements to the greatest extent, and reduce the development costs.

4.3 Security of basic computing resources

The basic computing resources of TRTC consist of more than one hundred distributed IDCs deployed around the globe and Tencent Cloud CVM instances, which guarantee the high scalability, security, and availability of the basic computing resource environment of TRTC.

Security of Computing Resources	Description
Security management of devices in IDCs	TRTC has developed a complete specification for the day-to-day management of devices in its IDCs. This specification defines detailed management measures and service implementation standards, which are fully reflected in the physical environment security, routine inspection, exception monitoring and reporting, and power resource support in the IDCs and meet the security compliance and basic security development requirements of TRTC.
Security of computing resources such as servers, databases, and middleware	Resources necessary for the operation of TRTC such as CPU, memory, and disks will be reasonably scheduled and allocated based on the business load. In actual security operations, TRTC develops appropriate security baselines and vulnerability management guidelines and implements in-depth threat detection to fully ensure the load security of basic computational resources in basic service scenarios.
DDoS mitigation	Given the significant impact of DDoS attacks on the system and business availability of TRTC PaaS services, TRTC leverages Tencent Cloud public cloud capabilities to deploy a DDoS mitigation scheme on core services. This scheme can detect and defend against DDoS attacks from the network and transport layers in real time. It monitors network traffic in real time, promptly cleanses the traffic as soon as an attack is detected, and enables protection in seconds for TRTC.

4.4 Security of web APIs

To make it easy for developers to efficiently develop and manage their own audio/video businesses, TRTC provides some of the features in the console in the form of RESTful APIs for developers to call. The RESTful APIs provide the following security protection:

Security protection	Description
Authentication	Before using TRTC RESTful APIs, developers need to first log in to the Tencent Cloud console and create their dedicated `SecretId` and `SecretKey` to ensure the uniqueness of the service provider's identity.
Input verification	The validity of developer request parameters will be verified on the TRTC server backend to filter out invalid parameters, so as to avoid common attack-prone vulnerabilities.
Transfer	RESTful APIs only support the HTTPS protocol to ensure encryption of all API

security	communications with SSL/TLS. This helps protect API credentials and transferred data.
API rate limit	There is a limit on the API request rate on the server, restricting API requests from malicious users while ensuring responses to normal user requests.

5. Security Operations

Sticking to a reasonable security operations policy is the foundation for TRTC to ensure customer security, lawfulness, and compliance. Based on its business characteristics, TRTC guarantees business operations security in the following ways:

5.1 Security emergency response mechanism

Based on its own audio/video PaaS business characteristics, TRTC develops criteria for categorizing different security events, classifies services, and systematically assesses security and threat levels to ensure prompt and efficient handling of security exceptions according to the complete and efficient process.
To put it simply, TRTC handles feature security exceptions as follows:

5.2 Business continuity management

To provide low-latency and high-quality audio/video services to developers and users on a 24/7 basis, TRTC's professional and efficient development and Ops team is available for the availability support and management of audio/video services.

Emergency Response Mechanism	Description
Business monitoring and alarming	TRTC has a 24/7 efficient monitoring mechanism in place to monitor the business service and system operation status. It has set up a complete set of unified monitoring tools to implement event monitoring and automated alarming for metrics such as the running status and resource load of system components involved in the business services such as applications, middleware, computational loads, databases, and network devices. In addition, a bot is leveraged to promptly notify the personnel on duty of any problems, so as to ensure prompt problem discovery and service recovery and availability.
Disaster recovery and	TRTC has developed solutions for the redundant architecture development of its core IDCs, taking into account the disaster recovery security of devices as well as the infrastructure

redundancy	layer, computational load, and network structure for various extreme business scenarios. Tencent Cloud public cloud servers are utilized to further guarantee the availability of the basic resources of TRTC in unexpected situations.
Continuity drill	To safeguard the continuous and efficient operation of important business systems and constantly improve its stability, TRTC regularly conducts security emergency disaster recovery drills for the IDC network, middleware, and business systems, carries out a review based on the data from each emergency drill, and improves the technical architecture, operation management process, and emergency plan.

5.3 Security monitoring and anti-intrusion

In terms of implementing defense in depth to tackle threats, the TRTC security team will collect logs based on the principle of least privilege for security log analysis. Prompt alarms will be sent for the security exceptions identified based on the log data generated by the business every day, and security operations personnel will further perform association and traceability analysis review. The verified potential risks will be handled and tracked by the emergency response mechanism of TRTC to guarantee the security and stability of business systems.

6. Employee Security

TRTC strictly follows the principle of ensuring data and information security in the course of ordinary operations and management from the perspective of employee management. It fully recognizes the importance of employee security to overall security and considers whether the professional ethics and basic qualities of employees suit Tencent Cloud's values and meet security compliance requirements and business needs in the recruitment, onboarding, training, and separation processes.

Process	Description
Recruitment	In the early stages of the employee recruitment process, TRTC assigns professional human resources specialists to verify the education and work experience of candidates to ensure that they are competent.
Onboarding	New employees must study the employee security policy to meet Tencent Cloud's requirements for security compliance awareness. In addition, an appropriate level of confidentiality agreement is entered into with each employee. Employees in a position exposed to important data are required to complete a detailed study of the security compliance policy and pass the exam before they can participate in the daily development of TRTC.
Employment	Employees are required to regularly attend security and privacy protection training and pass required examinations. Furthermore, TRTC irregularly organizes internal security- and privacy-related activities to constantly raise employees' security awareness.
Separation	Before departing the team, employees must complete the handover according to the

	established separation process and disable their access. TRTC will audit their performance during the advance notice period as specified in the confidentiality agreement and inform the employees of their information security and confidentiality responsibilities after separation. Employees may be separated on approval only after the work handover and data cleanup.

7. Security Responsibility Sharing

As a real-time interactive audio/video PaaS cloud service platform, TRTC will manage the security of the platform and SDKs. Developers connecting to the services need to manage the security of their own application and system environment and reasonably use the security management feature of TRTC as needed to safeguard their information, platform, system, and network.

8. Summary

Providing secure, compliant, and stable audio/video PaaS services for customers is one of the top concerns for TRTC. It systematically pushes forward the implementation of the information security plan, performs its regulatory compliance obligations, and uses the plan as guidelines for product and service development during daily operations. In addition, TRTC actively studies new technologies with a view to implementing more efficient, secure, and automated security safeguards.
To guarantee its continuous high availability and protect the legitimate rights and interests of end users, TRTC continuously endeavors to create secure and compliant real-time interactive audio/video services.

Notes on Information Security

Last updated：2023-10-13 11:38:04

The following statement is hereby made for this document:

1. This document is intended to provide an overview of Tencent Cloud's security measures for Tencent Real-Time Communication (TRTC). It explains how to manage information and protect the security of your and end users' data. If you have any mandatory requirements, we recommend you enter into a service level agreement (SLA) with Tencent Cloud. Tencent Cloud disclaims any express or implied undertakings and warranties as to the content of this document.
2. This document only involves "part of" the technical security features among the wide range of security features.
3. This document is not intended as a reference document for national or industry-specific information security standards or requirements.
4. This document has been adapted for readability. In the event of any ambiguity or inaccuracy, refer to Item 1.
5. Tencent Cloud reserves the right to interpret this document.

1. Overview

TRTC has passed and meets the security requirements of the following certifications:
ISO 9001 Certification
ISO 20000 Certification
ISO 27001 Certification
ISO 27017 Certification
CSA STAR Certification
GDPR
For more information, see Compliance.

2. Information Security Protection

The management security and technical security requirements of TRTC comply with the General Data Protection Regulation (GDPR).

2.1 Information and data security

Communications between users and the TRTC server are protected by protocols such as Tencent Cloud's private transfer protocol, Transport Layer Security (TLS), and Web Socket Secure (WSS). During transfer, TRTC has no key that can decrypt the transferred information. The call content can be decrypted only with your authorization key on the terminal device (such as the client application or the on-premises recording server).

2.2 Data availability

Globally distributed IDCs: TRTC has many IDCs providing services globally. Any attack on one IDC cannot affect others or the overall services, implementing isolation-based protection.
Fault isolation and recovery: If an IDC is subjected to malicious attacks that are difficult to prevent, such as a denial-of-service (DoS) attack, TRTC will reasonably handle the faulty server to ensure the overall service stability and availability.
DDoS mitigation: TRTC has deployed anti-DDoS firewalls in each IDC and has sufficient capabilities and resources to control the risk of DDoS attacks.

2.3 Data categorization and storage

Personal Information	Purpose	Legal Basis
Data configured in the console: The TRTC application ID and name, whether recording and relayed push are enabled, and the selected billing mode	For billing purposes, we use this information to determine your usage of the corresponding feature. Note that such data is stored in our Elasticsearch Service (ES) feature.	We will process this information as necessary to make the corresponding feature available to you as part of our performance of the contract entered into with you.
Backend log data: The user ID, room ID, client IP and SDK version, and OS type of any participants in live streaming events	We use this information to ensure that corresponding features run as required and to	We will process this information as necessary to make the corresponding feature available to you as part of our performance of

	perform troubleshooting. Note that such data is stored in our ES feature.	the contract entered into with you.
Dashboard information: Audio/Video quality information during call: The end user's `APPID` , data about the features controlled by the end user (enabling/disabling audio/video), room entry/exit, room ID, muting feature, CPU utilization, memory usage, network latency, data packet loss, resolution, bitrate, frame rate, and volume level	We use this information to ensure that corresponding features run as required and to perform troubleshooting. Note that such data is stored in our ES feature.	We will process this information as necessary to make the corresponding feature available to you as part of our performance of the contract entered into with you.
SDK log data (of the end user): The user ID, room ID, client SDK version number, and the OS type of the TRTC room	We use this information to ensure that corresponding features run as required and to perform troubleshooting. Note that such data is stored in our ES feature.	We will process this information as necessary to make the corresponding feature available to you as part of our performance of the contract entered into with you.
UIN	We use this information to determine your usage of the corresponding feature. Note that such data is stored in our ES feature.	We will process this information as necessary to make the corresponding feature available to you as part of our performance of the contract entered into with you.
SDK `APPID` (created for different applications with your UIN)	As part of the corresponding feature, we use this information to determine the	We will process this information as necessary to make the corresponding feature available to you as part of our performance of

	usage of your application. Note that such data is stored in our ES feature.	the contract entered into with you.
Troubleshooting data: The end user's `APPID` , data about the features controlled by the end user (enabling/disabling audio and video), room entry/exit, room ID, CPU utilization, memory usage, network latency, data packet loss, resolution, bitrate, frame rate, and volume level	We use this information to detect and locate the issues encountered by the end user for troubleshooting. Note that such data is stored in our ES feature.	We will process this information as necessary to make the corresponding feature available to you as part of our performance of the contract entered into with you.

TRTC offers the on-premises recording and on-cloud recording features, which allow you to record all or part of call content. During the use of the on-cloud recording feature, all audio/video call recordings are stored in your cloud storage service, and TRTC does not store your audio/video files.
TRTC stores the above data in the Chinese mainland for Tencent Cloud customers and in the Singapore IDC for Tencent Cloud International customers to meet the storage requirements for data security compliance.

2.4 Access authorization

When entering a TRTC room, end users are required to authenticate with a dynamic signature, so as to protect your right to use of the Tencent Cloud service from malicious attacks. For more information, see UserSig.

2.5 Access control

TRTC implements strict access control and management for all internal systems. All users have an independent internal account and authorization system and must pass two-factor authentication. All access records are recorded. All servers involving user data are strictly audited and protected. TRTC will only access your server when necessary. If TRTC has to access your server for security reasons, it will get temporary authorization first. The whole process will be recorded, and all operation records will be kept.

2.6 Internal security audit

We will store personal data processed in connection with the corresponding features as described below:

Personal Information	Retention Policy
Your temporary key information: The SDK	We retain this data during your use of the corresponding

`APPID` , username, and private key	feature. If your use of the feature is terminated or your account is deleted, we will delete this data within seven days.
Application-related customer log data: The SDK `APPID` , application name, tag, service status, creation time, and operation	We retain this data during your use of the corresponding feature. If your use of the feature is terminated or your account is deleted, we will delete this data within seven days.

You can request deletion of such personal data in accordance with the DPSA.

2.7 Employee security awareness training

TRTC provides all of its employees with regular training in information security awareness and security compliance. All employees receive regular courses and training in information confidentiality awareness on an annual basis.

2.8 Handling of Violations

TRTC employees are required to comply with the confidentiality agreement and internal security policy. Appropriate actions will be taken in case of any violation, including but not limited to strengthened training and education, termination of employment, and pursuit of other legal liability.

2.9 Potential vulnerabilities

If you identify any potential vulnerability in the TRTC platform, you are free to submit a ticket, and our technical experts will promptly respond and address the potential vulnerability.
To make it easier to locate and verify the vulnerability, you need to submit the following content:
Your contact information
A description of the feature affected by the identified potential vulnerability
The necessary steps and methods needed to locate and reproduce the potential vulnerability.

Service Level Agreement

Last updated：2023-10-13 11:38:53

To use the Tencent Real-Time Communication ("TRTC") service (the "Service"), you should read and observe this Tencent Real-Time Communication Service Level Agreement (this "Agreement", or this "SLA") and the Tencent Cloud Service Agreement. This Agreement contains, among others, the terms and definitions of the Service, indicators of the Service availability, compensation plan and release of liabilities. Please carefully read and fully understand each and every provision hereof, and the provisions restricting or releasing certain liabilities, or otherwise related to your material rights and interests, may be in bold font or underlined or otherwise brought to your special attention.
Please do not purchase the Service unless and until you have fully read, and completely understood and accepted all the terms hereof. By clicking "Agree"/ "Next", or by purchasing or using the Service, or by otherwise accepting this Agreement, whether express or implied, you are deemed to have read, and agreed to be bound by, this Agreement. This Agreement shall then have legal effect on both you and Tencent Cloud, constituting a binding legal document on both parties.

1.Terms and Definitions

1.1 **Real-Time Communication (TRTC) Service**: the comprehensive real-time audio and video solutions, including without limitation audio communication, video communication, video retouching, relayed live streaming, video recording, and mixing and transcoding, which provide a complete set of functions such as WebRTC support, terminal SDK integration and back-end interface. For details, please refer to the Service purchased by you and the content of the Service provided by Tencent Cloud.
1.2 **Service Month**: the respective calendar month(s) within the service period for the Service you purchased. For example, if you purchase the Service for a three-month period and the Service is activated on March 17, there are four Service Months (i.e., the first Service Month is from March 17 to March 31, the second from April 1 to April 30, the third from May 1 to May 31, and the fourth from June 1 to June 16). The availability of the Service will be calculated independently for each Service Month.
1.3 **Monthly Service Fee**: the aggregate service fees for the Service actually you consumed within one Service Month. If you make a one-time purchase of multiple pre-paid service packages, the Monthly Service Fee will be subject to the actual consumption during the then current Service Month, and the portion yet to be consumed will be excluded.
1.4 **Communication Success Rate**: Your request for entering a room is deemed as a request for initiating communication, and once you make such a request, it will be counted as one request. Once you enter a room, it will be deemed that the communication is successful.

Communication Success Rate = (number of successful communications / total number of communication requests) × 100%

1.5 **Service Downtime Calculated in Minutes**: If the Communication Success Rate is lower than 99% within one unit time (each 5 minutes as one calculation time unit) due to any reason attributable to Tencent Cloud, it shall be deemed that the Service is unavailable within such unit time; when such situation lasts for five (5) minutes or more, such time shall be counted into the service downtime, while any such situation that lasts less than five (5) minutes will not be counted into the service downtime.

Note:

5 minutes will be deemed as one measurement unit, resulting in 288 measurement points each day. The measurement point of 00:00:00 represents the time slot from 00:00:00 to 00:04:59, and the rest can be deduced by analogy.

1.6 **Total Time within a Service Month Calculated in Minutes**: the total number of days within such Service Month × 24 (hours) × 60 (minutes).

2. Service Availability

2.1 Calculation of Service Availability

Service Availability = (1 -- Service Downtime within a Service Period Calculated in Minutes / Total Time within a Service Period Calculated in Minutes) × 100%

For example, assuming that the Communication Success Rate from 10:00 a.m. to 10:30 a.m. on a certain day in March 2019 is 98% (i.e., the Communication Success Rate is lower than 99% and the situation lasts for more than five (5) minutes), the Service Downtime Calculated in Minutes would be 30 minutes, and the Service Availability of March 2019 is 99.93% (i.e., 1 -- (30 / 31 × 24 × 60) × 100%).

2.2 Service Standard Indicator

The Service Availability of the Service provided by Tencent Cloud will be no less than 99.9%. You are entitled to the compensation as set forth in Section 3 below if the Service Availability fails to meet the aforementioned standard, other than in any circumstance as provided for in the release of liabilities provisions below.

3. Service Compensation

In respect of this Service, if the Service Availability fails to meet the abovementioned standard, you will be entitled to compensations in accordance with the following terms:

3.1 Standards of Compensation

(1) Compensations will be made in the form of voucher by Tencent Cloud, and you should follow the rules for using the voucher (including the valid term; for details, please refer to the rules of vouchers published on Tencent Cloud's official website). You cannot redeem such voucher for cash or request to issue an invoice for such voucher. Such voucher

can only be used to purchase the Service by using your Tencent Cloud account. You cannot use the voucher to purchase other services of Tencent Cloud, nor should you give the voucher to a third party for consideration or for free.
(2) If the Service Availability of a Service Month fails to meet the standard, the amount of compensation will be calculated for such month independently, and the aggregate amount shall be no more than the applicable Monthly Service Fee paid by you for such month (the Monthly Service Fee referred to herein shall exclude the portion deducted by a voucher or promotional credit, due to discounted service fee or otherwise deducted).

Service Availability	Value of Voucher
≥ 99.5% and < 99.9%	10% of the Monthly Service Fee
≥99% and < 99.5%	20% of the Monthly Service Fee
< 99%	50% of the Monthly Service Fee

3.2 Time Limit for Compensation Application

(1) If the Service Availability of a Service Month fails to meet the abovementioned Service Availability standard, you may apply for compensation through (and only through) the support ticket system under your relevant account after the fifth (5^th^) business day of the month immediately following such Service Month. Tencent Cloud will verify and ascertain your application upon receipt of such application. If there is any dispute over the calculation of the Service Availability for a Service Month, both parties agree that the back-end record of Tencent Cloud will prevail.
(2) You should apply for such compensation no later than sixty (60) calendar days following the expiry of the applicable Service Month in which the Service Availability fails to meet the standard. If you fail to make any application within such period, or make the application after such period, or make the application by any means other than that agreed herein, it shall be deemed that you have voluntarily waived your right to apply for such compensation and any other rights you may have against Tencent Cloud, in which case Tencent Cloud has the right to reject your application for compensation and not to make any compensation to you.

4.Release of Liabilities

If the Service is unavailable due to any of the following reasons, the corresponding Service downtime shall not be counted towards Service unavailability period, and is not eligible for compensation by Tencent Cloud, and Tencent Cloud will not be held liable to you:

4.1 Any failure on the part of a user.
4.2 Any negligence of a user or any operation authorized by a user.
4.3 Any loss or leak of data, pin or password due to improper maintenance or improper confidentiality measures of a user.
4.4 Any hacker attack on a user's website, application or data.
4.5 Any failure of a user to observe the documentation or guideline for using the TRTC.

4.6 Any impromptu increase of traffic of a user (concurrent volatility over 3,000) without five (5) business days prior written notice to Tencent Cloud.
4.7 Any use of products, functions and access for trial operation which are not made public by the official website of Tencent Cloud.
4.8 Any use by a user of any illegal information relating to pornography, gambling, illegal drugs, political party, politics, military affairs, fraud, etc.
4.9 Any significant event or promotion publicly announced by Tencent in advance.
4.10 Any system maintenance with prior notice by Tencent Cloud to a client, including system cutover, maintenance, upgrade and failure simulation test.
4.11 Any failure or configuration adjustment of network or equipment that is not Tencent Cloud facility.
4.12 Any force majeure event or accident.
4.13 Any Service unavailability or failure of the Service to meet the availability standard not attributable to Tencent Cloud.
4.14 Any other circumstances in which Tencent Cloud will be exempted or released from its liabilities (for compensation or otherwise) according to relevant laws, regulations, agreements or rules, or any rules or guidelines published by Tencent Cloud separately.

5.**Miscellaneous**

1. **The parties hereto acknowledge and agree that, for any losses incurred by you during the course of using the Service due to any breach by Tencent Cloud, the aggregate compensation amount payable by Tencent Cloud shall under no circumstance exceed the total service fees you have paid for the relevant Service which is not performed.**
2. Tencent Cloud has the right to amend the terms of this Agreement as appropriate or necessary in light of changes in due course. You may review the most updated version of relevant Agreement terms on the official website of Tencent Cloud. If you disagree with such revisions made by Tencent Cloud to this Agreement, you have the right to cease using the Service; by continuing to use the Service, you shall be deemed to have accepted the Agreement as amended.
3. As an ancillary agreement to the Tencent Cloud Service Agreement, this Agreement is of the same legal effect as the Tencent Cloud Service Agreement. In respect of any matter not agreed herein, you shall comply with relevant terms under the Tencent Cloud Service Agreement. In case of any conflict or discrepancy between this Agreement and the Tencent Cloud Service Agreement, this Agreement prevails to the extent of such conflict or discrepancy. (End of Document)

Apple Privacy Policy: PrivacyInfo.xcprivacy

Last updated：2024-07-09 17:17:39

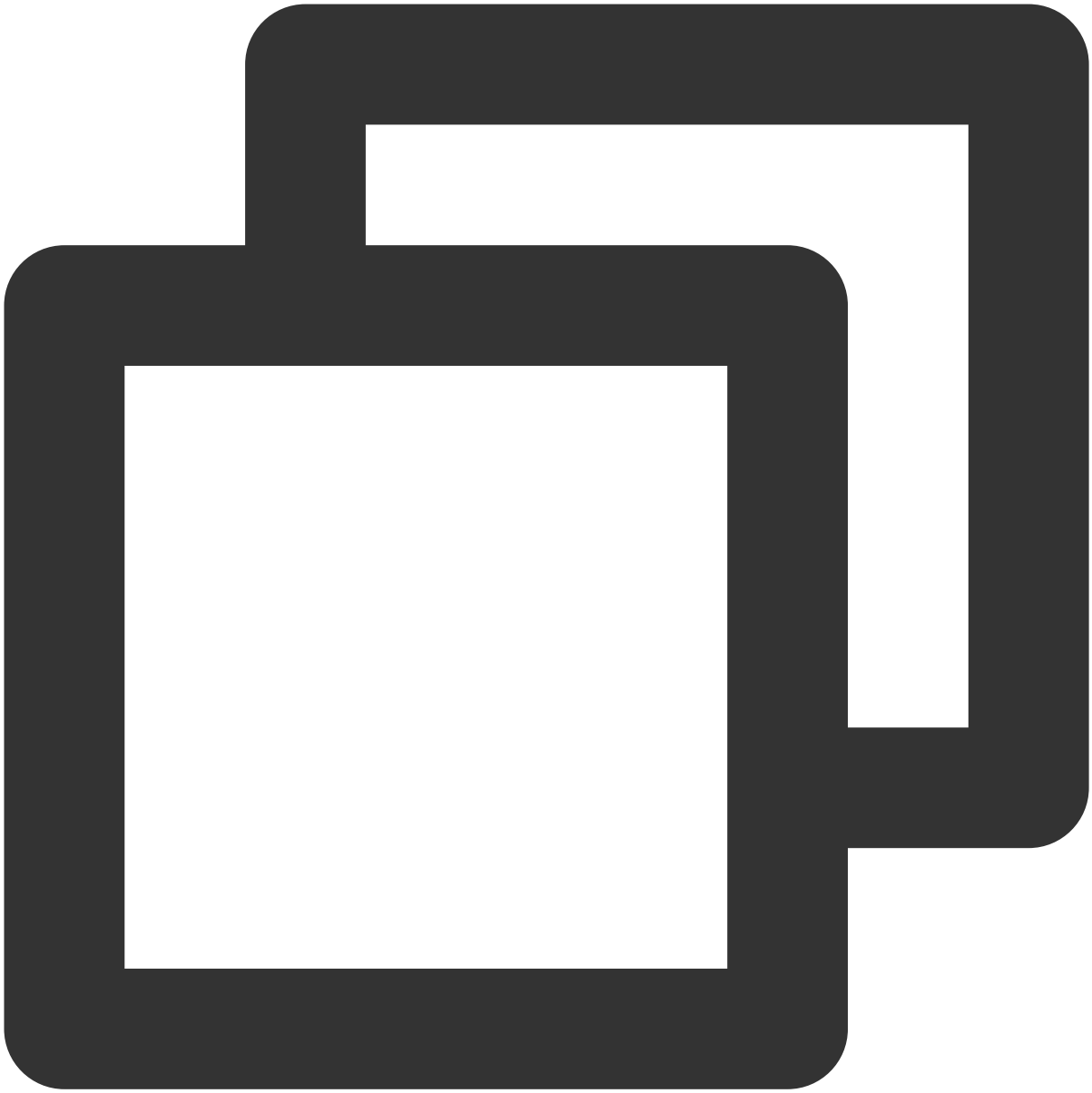
According to Apple Inc.'s App Store privacy update, starting from spring 2024, apps listed in the App Store must also offer a **privacy manifest**.
When you are ready to distribute your app, Xcode will combine the privacy manifests of all third-party SDKs used by the app into an easy-to-use report.
This report completely summarizes all the third-party SDKs in the app, allowing you to create privacy tags in an easy and accurate manner.
Therefore, the SDKs embedded in the app and third-party libraries all need to include **PrivacyInfo.xcprivacy**.

Adaptation of Tencent Real-Time Communication (TRTC)

In TRTC SDK **11.7** and later (including the simplified and full-feature editions), the **PrivacyInfo.xcprivacy** file is included by default.
In TUICallKit **2.3.0.920** and later, the **PrivacyInfo.xcprivacy** file is included by default.
In TUIRoomKit **2.3.0** and later, the **PrivacyInfo.xcprivacy** file is included by default.
In TUILiveKit **2.1.1** and later, the **PrivacyInfo.xcprivacy** file is included by default.
When you go integrating with CocoaPod, **PrivacyInfo.xcprivacy** will be added to your project through Pod, so that **no extra work is needed**.
When you go integrating manually, please make sure to **copy PrivacyInfo.xcprivacy under the source code directory to your code project**.
Note:
The TUIKit scheme and TRTC SDK full-feature edition (Professional) include several SDK products, and **PrivacyInfo.xcprivacy** may have slight differences in content. So you can choose the corresponding file version as needed.

TRTC-related PrivacyInfo.xcprivacy

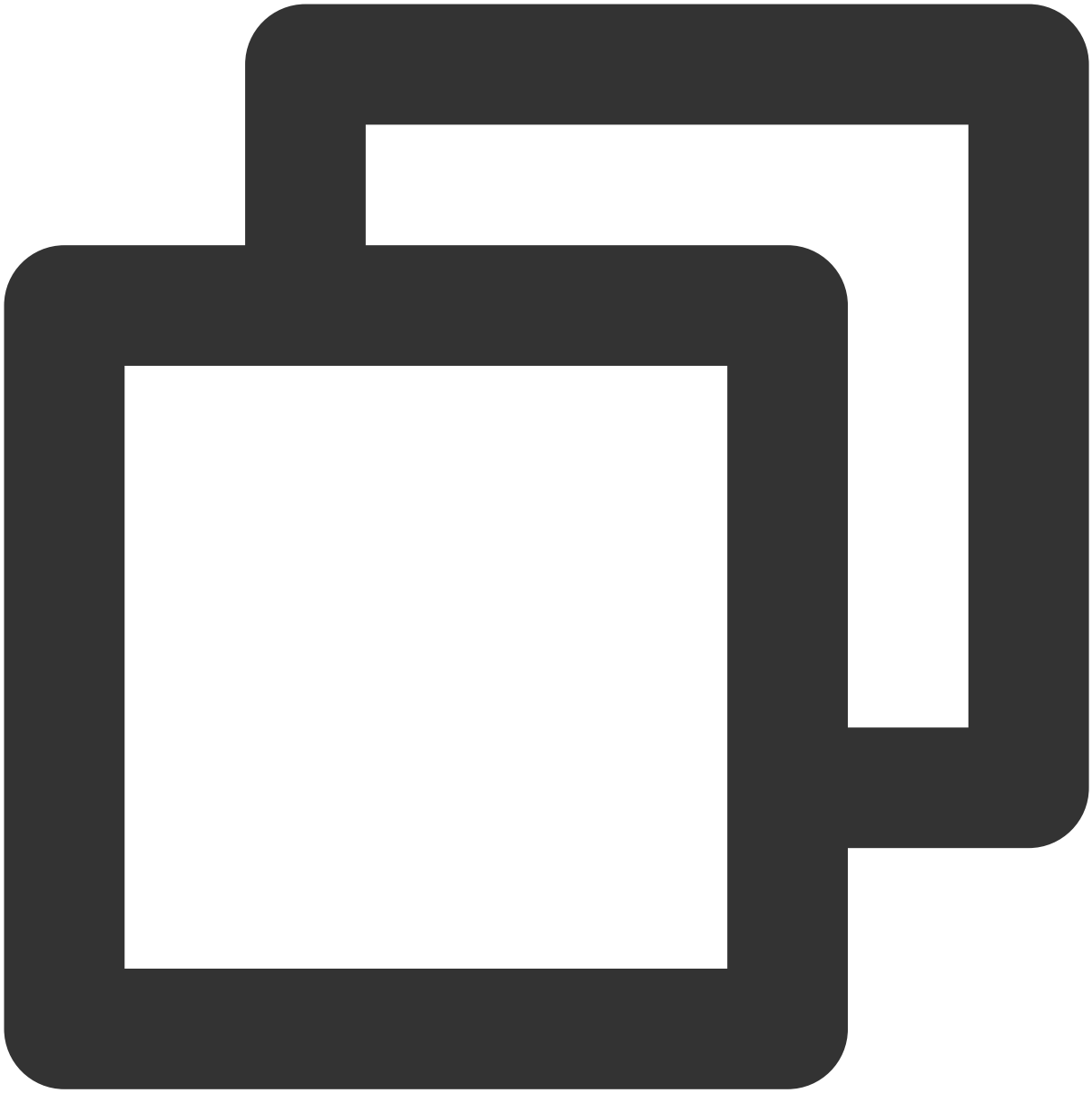
Simplified Edition (TRTC) SDK
Full-feature Edition (Professional) SDK
TUICallKit
TUIRoomKit
TUILiveKit



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Pro
<plist version="1.0">
<dict>
        <key>NSPrivacyCollectedDataTypes</key>
        <array>
                <dict>
                        <key>NSPrivacyCollectedDataType</key>
                        <string>NSPrivacyCollectedDataTypeUserID</string>
                        <key>NSPrivacyCollectedDataTypeLinked</key>
                        <false/>
```

```
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypeOtherDiagnosticData</stri
                <key>NSPrivacyCollectedDataTypeLinked</key>
                <false/>
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypePhotosorVideos</string>
                <key>NSPrivacyCollectedDataTypeLinked</key>
                <false/>
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypeAudioData</string>
                <key>NSPrivacyCollectedDataTypeLinked</key>
                <false/>
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypePerformanceData</string>
                <key>NSPrivacyCollectedDataTypeLinked</key>
```

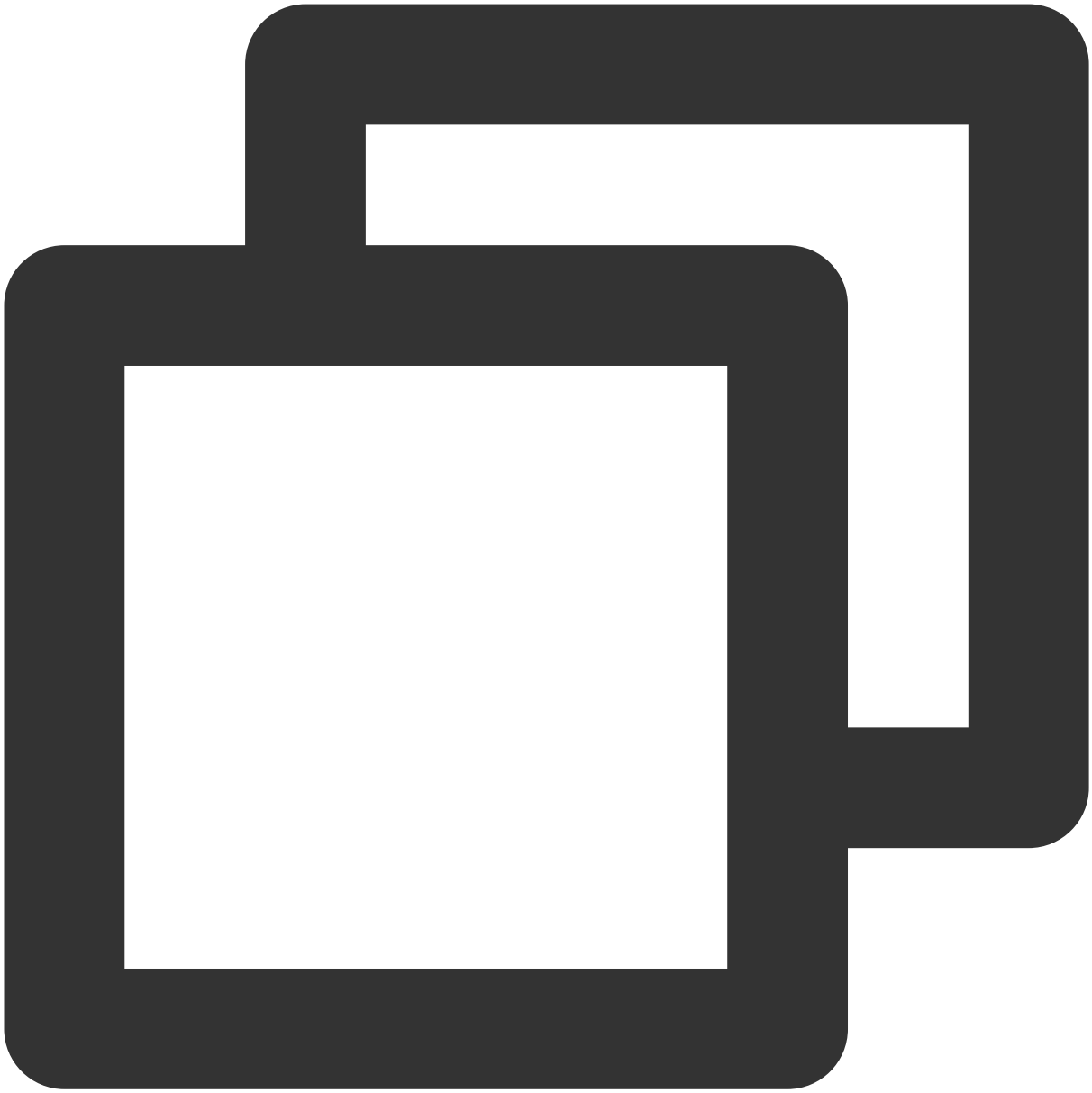
```
                        <false/>
                        <key>NSPrivacyCollectedDataTypeTracking</key>
                        <false/>
                        <key>NSPrivacyCollectedDataTypePurposes</key>
                        <array>
                                <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                        </array>
                </dict>
        </array>
        <key>NSPrivacyAccessedAPITypes</key>
        <array>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategoryUserDefaults</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>C56D.1</string>
                        </array>
                </dict>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategoryFileTimestamp</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>0A2A.1</string>
                        </array>
                </dict>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategorySystemBootTime</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>35F9.1</string>
                        </array>
                </dict>
        </array>
</dict>
</plist>
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Pro
<plist version="1.0">
<dict>
        <key>NSPrivacyCollectedDataTypes</key>
        <array>
                <dict>
                        <key>NSPrivacyCollectedDataType</key>
                        <string>NSPrivacyCollectedDataTypeUserID</string>
                        <key>NSPrivacyCollectedDataTypeLinked</key>
                        <false/>
```

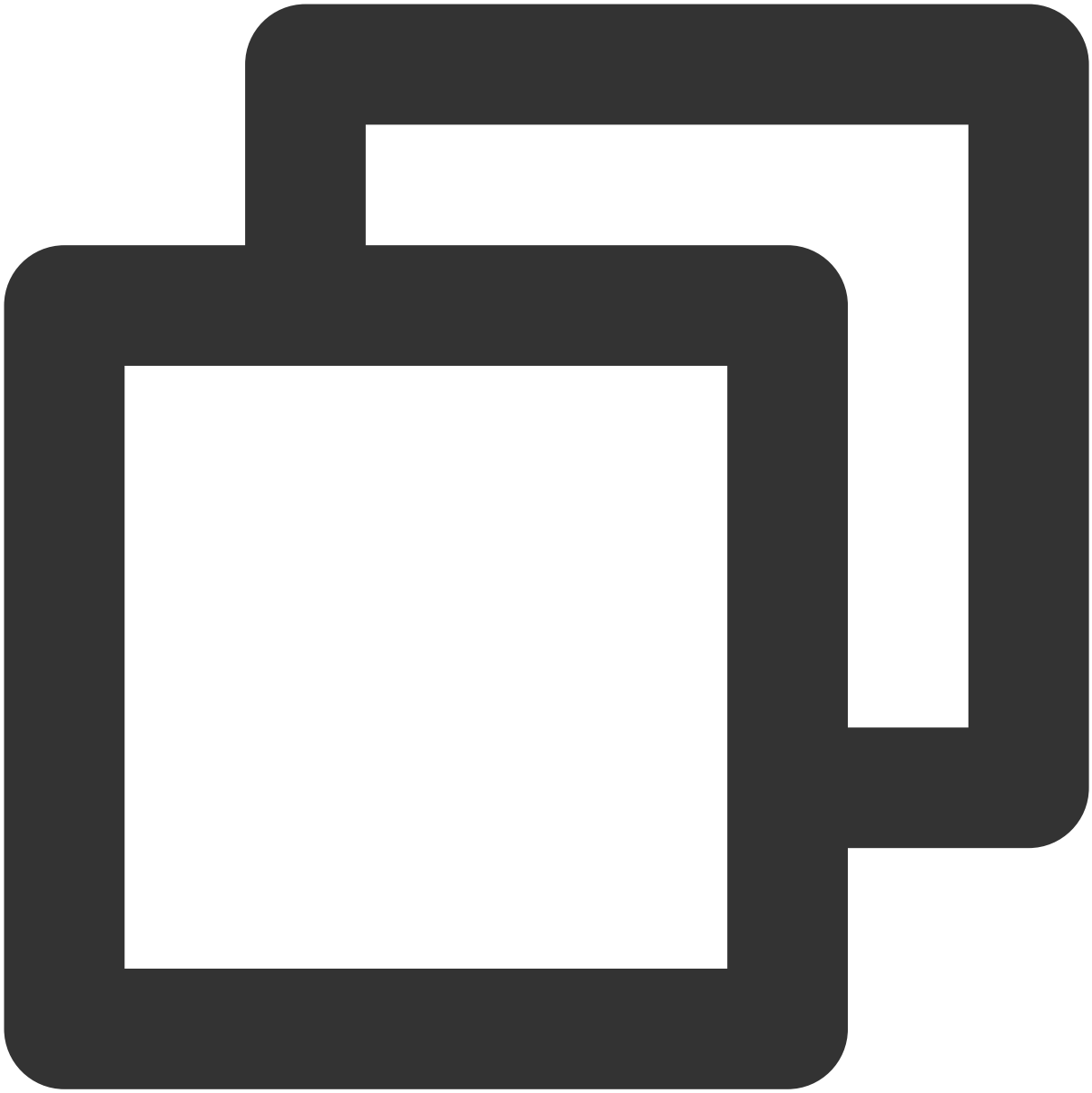
```
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypeOtherDiagnosticData</stri
                <key>NSPrivacyCollectedDataTypeLinked</key>
                <false/>
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypePhotosorVideos</string>
                <key>NSPrivacyCollectedDataTypeLinked</key>
                <false/>
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypeAudioData</string>
                <key>NSPrivacyCollectedDataTypeLinked</key>
                <false/>
                <key>NSPrivacyCollectedDataTypeTracking</key>
                <false/>
                <key>NSPrivacyCollectedDataTypePurposes</key>
                <array>
                        <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                </array>
        </dict>
        <dict>
                <key>NSPrivacyCollectedDataType</key>
                <string>NSPrivacyCollectedDataTypePerformanceData</string>
                <key>NSPrivacyCollectedDataTypeLinked</key>
```

```
                        <false/>
                        <key>NSPrivacyCollectedDataTypeTracking</key>
                        <false/>
                        <key>NSPrivacyCollectedDataTypePurposes</key>
                        <array>
                                <string>NSPrivacyCollectedDataTypePurposeAppFunctio
                        </array>
                </dict>
        </array>
        <key>NSPrivacyAccessedAPITypes</key>
        <array>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategoryDiskSpace</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>E174.1</string>
                        </array>
                </dict>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategoryUserDefaults</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>C56D.1</string>
                        </array>
                </dict>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategoryFileTimestamp</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>0A2A.1</string>
                        </array>
                </dict>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategorySystemBootTime</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>35F9.1</string>
                        </array>
                </dict>
        </array>
</dict>
</plist>
```



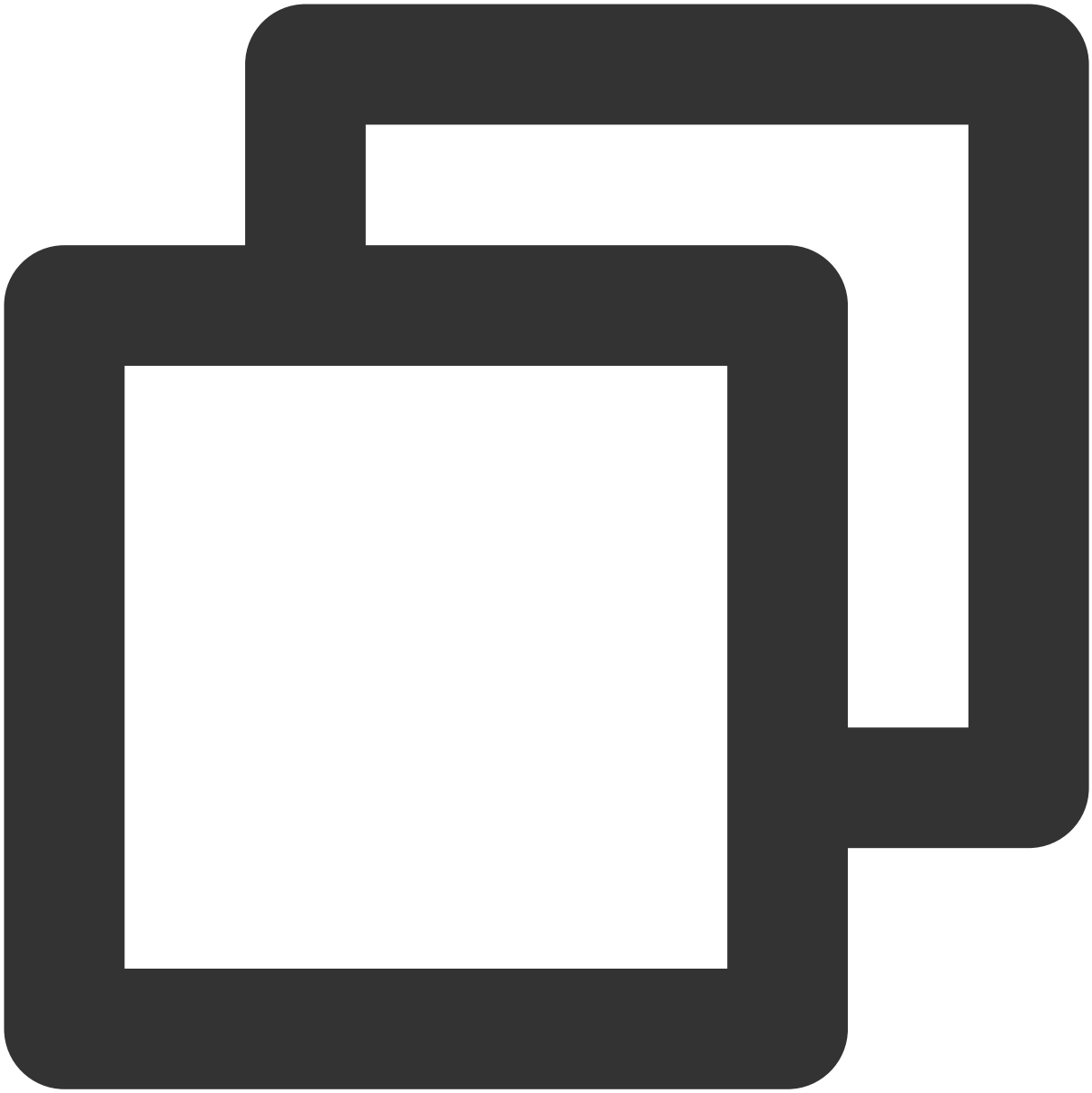
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Pro
<plist version="1.0">
<dict>
        <key>NSPrivacyTracking</key>
        <false/>
        <key>NSPrivacyTrackingDomains</key>
        <array/>
    <key>NSPrivacyCollectedDataTypes</key>
    <array>
        <dict>
```

```
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypeUserID</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>
                <string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
        <key>NSPrivacyAccessedAPITypes</key>
        <array>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategoryDiskSpace</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>E174.1</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategoryUserDefaults</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>CA92.1</string>
            </array>
        </dict>
        </array>
</dict>
</plist>
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Pro
<plist version="1.0">
<dict>
        <key>NSPrivacyTracking</key>
        <false/>
        <key>NSPrivacyTrackingDomains</key>
        <array/>
    <key>NSPrivacyCollectedDataTypes</key>
    <array>
        <dict>
```

```
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypeUserID</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>
                <string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
        <key>NSPrivacyAccessedAPITypes</key>
        <array>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategorySystemBootTime</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>35F9.1</string>
                        </array>
                </dict>
        </array>
</dict>
</plist>
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Pro
<plist version="1.0">
<dict>
        <key>NSPrivacyTracking</key>
        <false/>
        <key>NSPrivacyTrackingDomains</key>
        <array/>
    <key>NSPrivacyCollectedDataTypes</key>
    <array>
        <dict>
```

```
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypeUserID</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>
                <string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
        <key>NSPrivacyAccessedAPITypes</key>
        <array>
                <dict>
                        <key>NSPrivacyAccessedAPIType</key>
                        <string>NSPrivacyAccessedAPICategorySystemBootTime</string>
                        <key>NSPrivacyAccessedAPITypeReasons</key>
                        <array>
                                <string>35F9.1</string>
                        </array>
                </dict>
        </array>
</dict>
</plist>
```

Manual import into your own app

In addition to importing PrivacyInfo automatically through CocoaPod, you can also directly complete the terms in **PrivacyInfo.xcprivacy** of the TRTC SDK (or relevant version) into your own app's **PrivacyInfo.xcprivacy**. For specific completion methods, you can refer to the following content:

Adding with source code

In Xcode, use source code to open **PrivacyInfo.xcprivacy** under the app project. Copy the entries from Tencent Cloud's **PrivacyInfo.xcprivacy**, being careful not to add duplicates or misplace lines.

Adding with property list

In Xcode, double-click to open the **PrivacyInfo.xcprivacy** file, click +, and Xcode will prompt optional terms and configurable items. Supplement them according to your needs.