ICS 35.100.70
L 79

团　体　标　准

T/CHEAA 0001.2—2020
代替：T/CHEAA 0001.2—2019

智能家电云云互联互通
第 2 部分：信息安全技术要求与评估方法

Cloud to cloud interconnection for smart household appliances

Part 2 : Information security technical requirements

and assessment methods

2020-08-25 发布　　2020-08-25 实施

中国家用电器协会 发布

目 次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件是 T/CHEAA 0001《智能家电云云互联互通》的第 2 部分。T/CHEAA 0001 已经发布了以下部分：

----第 1 部分：基本模型和技术要求

----第 2 部分：信息安全技术要求与评估方法

----第 3 部分：用户界面设计指南

文件代替 T/CHEAA 0001.2—2019《智能家电云云互联互通 第 2 部分：信息安全技术要求》，与 T/CHEAA 0001.2—2019 相比，除结构性调整和编辑性改动外，主要技术变化如下：

----更改了“范围”，对各方面要求增加了评估方法，并增加了评估方法的适用性场景表述（见第 1 章）；

----增加了“云云互联整体架构”（见第 4 章）；

----增加了“对用户数据和隐私保护的特别要求”（见 5.3）；

----增加了“信息安全技术评估方法”（见第 6 章）；

----删除了“附录 对用户数据和隐私保护的特别要求”（见 2019 年版附录 A）。

本次为第一次修订。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。本文件的发布机构对由于自愿采用本文件而引起的一切损失不承担任何责任及相关连带责任。

本文件由中国家用电器协会提出。

本文件由中国家用电器协会标准化委员会归口。

本文件起草单位：中国家用电器协会、杭州涂鸦信息技术有限公司、海尔优家智能科技（北京）有限公司、美的集团股份有限公司、广州云智易物联网有限公司、博西家用电器投资（中国）有限公司、康佳集团股份有限公司、TCL 鸿鹄实验室、四川虹美智能科技有限公司、青岛聚好联科技有限公司、宁波奥克斯电气股份有限公司、联想(北京)电子科技有限公司、惠而浦（中国）股份有限公司、广东格兰仕集团。

本文件主要起草人：姜风、刘龙威、武天旭、王妮娜、井皓、徐祥智、胡协斌、苏州、廖杰、林舜大、李昱兵、徐立耀、刘复鑫、张云停、谢厂节、黄明拓。

引　言

近年，随着越来越多的家用电器具接入了互联网、物联网，众多家电厂商的智能云平台从私有走向开放共享，而信息安全风险也随着被扩大，所以，实施云云互联互通的厂商间达成一致的信息安全要求就势在必行。

本文件针对家电云云互联面临的信息安全风险，提出了实施云云互联的云平台接口的信息安全能力要求与评估方法、出现安全事件的协同管理机制、用户数据和隐私的保护规定、应满足或参考的国内外标准和技术法规。旨在帮助云云互联的企业达成一致的信息安全规范，保障双方利益，遏制因共享而产生的安全风险。鉴于具体的应用场景下存在若干特殊情况，在实施中可对本文件进行裁剪及补充。

智能家电云云互联互通

第 2 部分： 信息安全技术要求与评估方法

1. 范围

本文件规定了在中国开展云云互联互通业务的各关联厂商云平台（以下简称云平台）之间云云互联互通接口及相关要素的信息安全技术要求（包括接口信息安全、安全事件协同管理、对用户数据和个人信息保护的特别要求）及其评估方法。

本文件提出的评估方法适用于第三方评估机构对云云互联互通业务的各关联厂商云平台（以下简称各云平台）的信息安全评估。也适用于开展云云互联互通业务的各关联厂商对相关范围业务的自评估。

本文件不涉及对各云平台上非云云互联互通业务的安全和隐私性做要求。

2. 规范性引用文件

下列文件中的内容通过本文件的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 16264.8 信息技术 第 8 部分：开放系统互联目录

GB/Z 20985 信息技术 安全技术 信息安全事件管理指南

GB/Z 20986 信息安全技术 信息安全分类事件分级指南

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

IETF RFC 5246 安全传输层协议 1.2 版本［The Transport Layer Security（TLS）Protocol Version 1.2］

T/CHEAA 0001.1-2020 智能家电云云互联互通 第 1 部分：基本模型和技术要求

3. 术语和定义及缩略语

3.1 术语和定义

以下术语和定义适用于本文件。

3.1.1

安全传输层协议 transport layer security

在两个通信应用程序之间提供身份鉴别、数据保密性和数据完整性功能的协议。

[IETF RFC 5246，The Transport Layer Security (TLS) Protocol Version 1.2]

3.1.2

证书认证机构 Certificate Authority（CA）

负责创建和分配证书，受用户信任的权威机构。用户可以选择该机构为其创建密钥。
[GB/T 16264.8-2005，定义 3.3.16]

3.1.3

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：关于个人信息的范围和类型详见 GB/T 35273-2020 附录 A。

[GB/T 35273-2020，定义 3.1]

3.1.4

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：关于个人敏感信息的范围和类型可详见 GB/T 35273-2020 附录 B。

[GB/T 35273-2020，定义 3.2]

3.1.5

个人信息主体 personal data subject

个人信息所标识的自然人

[GB/T 35273-2020，定义 3.3]

3.1.6

收集 collect

获得对个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集，以及通过共享、转让、搜集公开信息间接获取等方式。

[GB/T 35273-2020，定义 3.5]

3.1.7

密钥 key

一种用于控制密码变换操作(例如加密、解密、密码校验函数计算、签名生成或签名验证)的符号序列。

[GB/T 25069-2010，定义 2.2.2.106]

3.1.8

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

[GB/T 35273-2020，定义 3.13]

3.1.9

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段 替代对个人信息的标识。

[GB/T 35273-2020，定义 3.14]

3.1.10

重放攻击 replay attack

一种主动攻击方法，攻击者通过记录通信会话，并在以后某个时刻重放这个会话或者会话的一部分。

[GB/T 25069-2010，定义 2.2.1.138]

3.1.11

信息安全事件 information security incident

一个信息安全事件由单个的或一系列的有害或意外信息安全事态组成，他们具有损害业务运作和威胁信息安全的极大可能性。

[GB/T 20985-2007，定义 3.3]

3.2 缩略语

以下缩略词适用于本文件。

SM4：分组密码算法（Block Cipher Algorithm）

SM3：密码杂凑算法（Cryptographic Hash Algorithm）

AES：高级加密标准（Advanced Encryption Standard）

API：应用程序接口（Application Programming Interface）

HMAC：哈希消息认证码（Hash-based Message Authentication Code）

JSON：对象标记（Java Script Object Notation）

TLS：安全传输协议（Transport Layer Security）

APP：应用程序（Application）

4. 云云互联整体架构

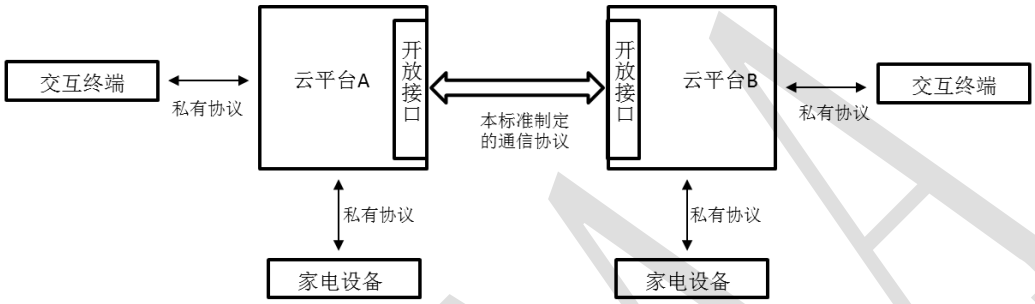

图1　云云互联整体架构

如图 1 所示，不同云平台实现互联需要各自云平台提供开放接口，另一方云平台通过对方云平台提供的开放接口实现其智能家居业务应用的开发，云平台的开放接口提供用户信息、设备控制和查询等互联功能。

［T/CHEAA 0001.1-2020，5］

5. 信息安全技术要求

5.1 接口信息安全

5.1.1 通信安全

a) TLS 安全：各云平台之间的通讯接口均应采用 TLS 安全机制，应使用不低于 1.2 的安全版本。同时需要通过各自的证书进行双向认证或单向认证，只允许证书校验通过后，才能完成请求。
b) 证书安全：各云平台均应向证书认证机构（CA）申请证书或通过特定组织统一自建证书，并在云平台上部署证书。证书有效期不超过 24 个月。

5.1.2 身份鉴别和授权

5.1.2.1 平台登录接口

a) 标识符安全：各云平台的唯一标识符 PlatID 应满足随机性。
b) 令牌自身安全：各云平台的身份令牌 AuthToken 应根据 PlatID 和时间戳、随机数等计算得出，应通过 SM3 或 HMAC 等 Hash 函数算法生成，长度不应低于 16 字节。

注 1： PlatID 和 AuthToken，来源于 T/CHEAA 0001-2017 《智能家电云云互联互通标准》 。

注 2： 时间戳精度毫秒级，采用东 8 区（北京时间）的网络时间。

c) 令牌适用安全：每对 PlatID 和 AuthToken 应仅适用于对接的两个平台。

例：A 平台给 B 平台发送的 PlatID 和 AuthToken，仅适用于 B 平台对 A 平台的身份鉴别，其他平台需要重新协商。

d) 身份校验：应采取双向身份鉴别或单向鉴别。

例：以双向身份鉴别为例，A 平台发送验证信息给 B 平台，B 平台再确认 A 平台身份正确后，也发送自己的鉴别信息给 A 平台。

5.1.2.2 访问令牌管理

a) 令牌访问安全：完成身份鉴别后，A 平台应通过 AuthToken 提交获取访问令牌 AccessToken 的请求，B 平台下发给 A 平台访问令牌 AccessToken、更新令牌 RefreshToken 和 AccessToken 的有效时长，A 平台所有的请求都应在有效时长内，且包含该 AccessToken 才能正常请求。

注： AccessToken 和 RefreshToken，分别用来做请求和刷新的 token。

b) 令牌自身安全：AccessToken 和 RefreshToken 应根据 PlatID 和时间戳、随机数等计算得出，应通过 SM3 或 HMAC 等 Hash 函数算法生成，长度不应低于 16 字节。

c) 令牌时效安全：AccessToken 有效期不应超过 2 小时，过期或登出操作后应自动销毁。RefreshToken 有效期不应超过 30 天，过期或登出操作后应自动销毁。

d) 令牌更新安全：应主动更新 AccessToken，应使用 RefreshToken 进行请求更新，RefreshToken 应仅可使用一次，更新一次 AccessToken 后，RefreshToken 也应进行更新。

5.1.2.3 授权

平台的访问权限控制应包含但不限于能够根据平台账号分配最小、仅必要的权限的功能。

5.1.3 数据安全

5.1.3.1 数据传输

a) 加密密钥获取

1) 需进行数据传输的平台之间进行身份鉴别后，各厂商之间应相互下发密钥以加密个人敏感信息。

例如：A 厂商的 APP 通过 A 厂商的云请求控制 B 厂商的云，需要拿到 B 厂商下发的动态密钥，进行数据加密。

2) 各商云平台之间共享的数据，如果涉及个人敏感信息，需要分发密钥，用来加密传输，密钥有效期 60 分钟。

3) 密钥应保证随机性，应结合用户 ID，以及时间戳和随机数的哈希函数生成 128 比特及以上字符串。

4) 每次用户登录鉴别后，应下发最新密钥，废弃旧密钥。用户登出操作后，也要废弃旧密钥。

5) 密钥应使用 SM4 或 AES 等加密算法加密存储。

b) 安全传输

1) 个人敏感信息传输前应使用动态获取的加密密钥加密。

2) 加密算法应使用 SM4 或 AES 等加密算法。
3) 涉及个人身份信息、密码和口令的传输应通过安全的 Hash 方式处理，应通过 SM3 或 HMAC 方式进行加盐 Hash。
4) 其他个人敏感信息的传输应根据实际业务中的应用场景，视具体情况选择去标识化、匿名化等处理方式。

表 1 个人敏感信息举例

个人敏感信息类型	举例
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康 状况产生的相关信息等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

注：关于个人敏感信息的范围和类型可详见 GB/T 35273-2020 附录 B.1。

5.1.3.2 消息认证

a) 防重放：对所有请求应有效手段防止重放攻击。
例：可采取时间戳均存储在缓存中，且仅一次性有效的策略，以防止重放的可能性。
b) 时间戳安全：所有请求应携带毫秒级时间戳标记，时间的有效期设置为前后 10 分钟内有效。
c) 算法安全：应使用 SM3 或 HMAC 等算法对数据内容和所有接口字段进行校验。

5.1.3.3 数据过滤

a) 传输格式：数据传输，应使用 PUT 或 POST 传输 JSON 格式的数据，请求头部应指明类型 application/json，并且使用明确恰当的字符集。并验证数据范围、长度和类型。
例：指定明确的字符集，比如 UTF-8。
b) 参数校验：JSON 中的所有参数，均应使用强类型和固定长度的校验。
例：PlateID 使用 Long 数字类型，长度为 16 字节。
c) 参数过滤：应使用白名单形式对所有的参数进行安全过滤，应对内容包含特殊字符和注入攻击的行为应进行严格检测，只允许设定的数据通过。

5.1.4 错误信息处理

各云平台在云云对接过程中请求失败的情况下，应通过错误编码来表示错误类型，不应暴露任何平台或用户的敏感信息。

5.1.5 接口稳定性

5.1.5.1 服务与系统安全

提供 API 的平台和对应的服务器，应执行系统和服务的加固，包括开放端口的白名单限

制和对外服务的加固。应满足 GB/T 22239-2019《信息安全技术 网络安全等级保护保护基本要求》第三级安全要求中的设备与应用安全要求。

5.1.5.2 风险评估与监控

各云平台应每年至少执行一次对云计算平台进行风险评估，确保云计算平台的安全风险处于可接受水平。宜采取第三方机构进行风险评估、服务商安全监控预警等方式加强风险评估能力，并共享评估结论。

5.1.6 日志审计

a) 日志系统部署：各云平台应具备自动化请求日志收集和审计系统，监控采集云端云云互联互通业务相关的日志及网络流量，通过离线分析和实时分析两种方式识别并发现潜在的网络攻击行为，及时预警并采取相应的应对措施。
b) 日志内容：日志收集和审计系统中应包括 API 接口日志和其他相关业务的服务和流量日志。日志中不应记录用户敏感数据信息。
c) 审计系统安全：日志收集和审计系统应根据安全需求，制定可审计事件清单，明确审计记录内容，实施审计并妥善保存审计记录，对审计记录进行定期分析和审查。同时应防止非授权访问、篡改或删除审计记录。
d) 日志保存时间：日志收集和审计系统的接口请求日志保存时间应不少于 6 个月。
e) 异常日志处理：针对异常日志，应自动告警到相关运维人员并进行对应的分析和处理。

5.2 安全事件协同管理

5.2.1 安全事件的分类和分级

5.2.1.1 安全事件分类

a) 数据泄露事件：云云互联的数据出现泄露。
b) 服务不可用事件：服务出现不稳定或者不可用情况，并且影响到云互联的其他厂商的事件。
c) 其他事件：除了上述事件以外的其他事件。

5.2.1.2 事件分级

a) 特别重大事件：是指能够导致特别严重影响或破坏的信息安全事件。
b) 重大事件：是指能够导致严重影响或破坏的信息安全事件。
c) 较大事件：是指能够导致较严重影响或破坏的信息安全事件。
d) 一般事件：是指不满足以上条件的信息安全事件。

注：事件详细说明请参考 GB/Z 20986。

5.2.2 责任模型

a) 针对数据泄露事件，各云平台相互间的追责，基本依据是责任归属于直接导致数据泄露的云平台或客户端所属的厂商。
b) 针对服务不可用事件，应根据导致服务不稳定或不可用的节点判断，责任应归属于该节点所有者平台。
c) 在责任未明确的时候，双方应共同协商、承担并调查原因。在双方对于数据泄露事件无法达成一致的情况下，应由独立的第三方介入调查。如调查无果，双方应共同承担责任。

5.2.3 服务条款

5.2.3.1 服务条款

a) 云云互联企业双方的服务内容。
b) 云云互联企业双方各自的权利和义务。
c) 涉及用户数据、用户个人敏感信息，需要明确数据的所有权，使用权限。
d) 保密条款，包括用户数据、用户个人敏感信息不允许主动向第三方披露等。
e) 服务期限和终止，并且终止后双方对于信息安全的义务。
f) 违约责任和免责条款。

注：云云互联双方签订的具有法律效应的服务条款应包含以上内容。

5.2.3.2 平台数据所有权说明

a) 个人信息数据：个人信息所有权应归属于信息所标识的自然人，即使用物联网服务的实际个人用户。个人信息所有者应拥有信息数据的完全访问和控制权限，并且有权利要求提供服务的厂商对其信息数据进行对应的操作。
b) 匿名化数据：经过匿名化处理后的数据和信息，应归属于这些信息的提供者，即提供信息的云平台主体。数据归属的云平台应具有对数据的完全访问和控制权限。
c) 云平台与合作平台数据：云平台的用户数据和归属合作平台的数据，不能执行任何未获用户授权的使用和披露，但是以下情形除外：在国家有关机关依法查询或调阅用户数据时，平台具有按照相关法律法规或政策文件要求提供配合，并向第三方或者行政、司法等机构披露的义务。

5.2.3.3 平台数据使用权限说明

a) 数据的披露

1) 未在双方书面允许和用户授权的情况下，不允许向第三方披露个人信息。
2) 只允许为提供或改进产品、服务的目的而与第三方共享。
3) 不允许为第三方的销售目的而与第三方共享数据，更不允许销售共享数据。

b) 数据的删除

1) 用户有权申请删除其在双方平台交互过程中产生的个人数据。平台双方需要在 7 天内完成数据删除。
2) 非个人数据，数据归属平台有权利要求共享平台对数据进行删除操作。
3) 所有数据删除的操作，需要在企业内部有明确的流程和制度保障。
4) 在服务终止后，必须安全删除通过云云互联接口同步过来的用户数据及用户个人敏感信息。
5) 对于已删除的个人数据，不能对其进行恢复操作。

c) 数据的访问控制

1) 对访问平台数据的用户进行唯一标识和鉴别。
2) 对访问特权账号的数据访问实施多因子鉴别。
3) 在允许访问数据前，对访问数据的方式进行授权。
4) 实时监测非授权的访问控制连接，并在发现非授权连接时，采取恰当的对应措施。

5.2.4 明确责任部门和人员

a) 负责人责任：应明确各云平台主要负责人对信息安全负全面领导责任，包括为信息安全工作提供人力、财力、物力保障等。

b) 接口人责任：应明确各云平台对接的安全接口人和备用接口人及其职责。

5.2.5 应急响应

a) 事件责任方：各平台协同诊断，认定安全事件和确认事件的责任方。
b) 责任方职责：事件责任方应根据合作服务条款内的明细，在指定时间内抑制受害范围并恢复业务服务。同时责任方应负责整个事件调查，并在事件处理结束后编写事件调查记录，调查记录中应明确信息安全事件起因、受影响时间、追责过程、应急过程、故障解决、事件复盘、改进措施等内容。

5.2.6 事件通告

a) 义务和权利：云云互联任何一方应有义务和权利向各相关方通告详细的安全事件原因。
b) 重大影响通告：如果因特别重大事件、重大事件或较大事件，而导致对业务可用性和稳定性的影响时间超过 1 个小时，应按照与各相关方的服务条款进行事件的对外通告。
c) 法律义务通告：需要向在有关事件响应的法律、法规和/或规章中要求的地方、省、国家有关部门通告。在牵涉到法律强制的地方，事件责任方负责与法律强制部门的联络。

5.2.7 持续改进

云云互联各相关方应对重大事件和特别重大事件进行持续的跟踪。责任方应给出相应的改进措施，并通过管理手段或技术手段真实落地。

5.3 对个人信息保护的特别要求

5.3.1 数据生产和收集

5.3.1.1 基本原则

a) 合法性：对各方的所有行为应进行合法要求，同时明确对应的法律责任。
b) 信息主体授权：应通过有效的渠道获取信息主体的授权，不允许超过信息主体授权行为以外的数据收集和操作。
c) 用户权限保障：各方需要通过技术或管理流程让用户的权限能够得到有效的保障。
d) 数据最小化：各方不应收集、存储、请求、提供、传递与服务无关的数据。
e) 数据分类：应区分个人数据和平台信息数据。

5.3.1.2 用户权限

a) 知情权

1) 用户应能通过隐私条款等方式知悉信息收集主体及其所提供服务的基本情况。
2) 用户应能通过隐私条款等方式知悉要收集的数据及这些数据的用途。
3) 用户应能通过隐私条款等方式知悉其所享有的权利信息。
4) 用户应能通过隐私条款等方式知悉数据共享、数据接收方的信息。

注：隐私条款模板应参考《GB/T 35273—2020 个人信息安全规范》的附录 D。

b) 选择权

当某位用户不选择上传数据或不同意隐私条款时，不应收集该用户的数据，同时仅可以不提供该数据相关的服务，其他服务应照常提供。

c) 处置权

用户应能通过电邮或联系客服等方式履行访问、迁移、删除等权力。信息收集主体和云云互联中各关联厂商应支持用户账号注销等机制，某一用户要求删除用户数据或注销用户账号时应删除与之相关的用户数据。

5.3.2 数据的使用

5.3.2.1 数据展示

各方应对需展示的个人信息采取去标识化处理等措施，以降低个人信息在展示环节的泄露风险。

5.3.2.2 数据审计

a) 各方均应具有完备的自动化数据库操作审计记录。
b) 针对可能有风险的操作，比如 A 厂家要求删除其所有数据，需要进一步沟通和需要一定的审批流程。

5.3.3 数据保存

a) 数据存储：各方均应对敏感数据进行集中地分布式存储、统一监控管理、通过 VPC 隔离。并实施数据库加密，对所有隐私信息进行加密或散列函数处理后存储。加密应使用 SM4 或 AES 等算法，散列函数应使用 SM3 或 HMAC 等算法。
b) 数据传输：各方均应将用户数据和用户个人敏感信息存储在中国境内，对于数据传输至境外的，应符合中国大陆相关法律法规要求。
c) 数据备份：各方均应采用分布式架构，所有业务服务器需要同时部署在多个不同的机房，数据应同时存放两个以上机房，并实时备份。
d) 存储时间：各方对用户个人敏感信息保存时间均不应超过 1 年。在服务期届满、服务提前终止时，可以按照平台约定的缓冲期内继续存储对方平台的用户数据，缓冲期不超过 7 天，平台应在 7 天缓冲期后执行删除所有相关用户数据的操作，包括缓存或者备份的副本。

5.3.4 数据销毁

a) 销毁策略：各云平台应对平台内部的数据制定相应的安全销毁策略，包括云主机内部的数据以及实体介质的数据。应明确记录数据销毁的过程以及对销毁过程进行全程记录和监督。
b) 法律责任：如果一方平台存在违约未销毁数据的行为，须依法承担违约责任。

6. 信息安全技术评估方法

6.1 接口信息安全

6.1.1 通信安全

6.1.1.1 TLS 安全

a) 评估方法：

1) 访谈安全管理员等相关人员，询问其是否有对云平台之间的通讯接口提供安全保护机制，有则符合要求；
2) 检查通讯接口安全保护机制说明文档或源代码，查看通讯接口是否使用了不低于 TLS

1.2 版本的通讯协议，是否通过证书认证对方身份，满足则符合要求；

3) 测试云平台之间的通讯接口，验证其是否使用了不低于 TLS 1.2 版本的通讯协议，是否要求通过各自证书完成双向校验或单向校验后才能完成请求，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.1.2 证书安全

a) **评估方法：**

1) 访谈安全管理员等相关人员，询问其是否有对云平台之间通讯证书的管理机制，有则符合要求；

2) 检查证书管理机制说明文档，查看其是否使用了证书认证机构颁发的证书或特定组织统一的自建证书；查看证书的有效期是否在 24 个月以内，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2 身份鉴别和授权

6.1.2.1 平台登录接口

6.1.2.1.1 标识符安全

a) **评估方法：**

咨询相关人员，检查源代码，查看生成唯一标识符 PlatID 的函数是否为安全的随机数生成函数，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.1.2 令牌自身安全

a) **评估方法：**

咨询相关人员，检查源代码，查看其身份令牌 AuthToken 的生成方法，验证生成因子中是否包含了 PlatID、时间戳和随机数，使用的 Hash 算法是否为安全的 Hash 算法，长度是否高于 16 位，组成因子是否包含了数字和字母，满足则符合要求；检查时间戳源代码，查看时间戳的精度是否是毫秒级，是否采用了东 8 区（北京时间）的网络时间，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.1.3 令牌适用安全

a) **评估方法：**

1) 咨询相关人员，检查源代码，查看其是否对相应的 PlatID 和 AuthToken 的使用做了限

制，使其仅适用于对接的领个平台，做了限制则符合要求；

2) 测试云平台对接行为，验证 PlatID 和 AuthToken 的有效性是否仅限于对接的两个平台，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.1.4 身份校验

a) **评估方法：**

1) 咨询相关人员，检查源代码，查看其是否对请求对接的云平台做了身份校验，满足则符合要求；
2) 测试云平台对接行为，验证数据流中是否双向或单向传输了身份鉴别信息，并尝试篡改或伪造校验信息，观察身份校验能否会被拦截，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.2 访问令牌管理

6.1.2.2.1 令牌访问安全

a) **评估方法：**

1) 咨询相关人员，检查源代码，查看其是否定义了获取 AccessToken 的请求，是否根据收到的AccessToken的有效时长做了有效性限制，是否在请求中包含了AccessToken参数，满足则符合要求；
2) 测试完成身份鉴别后的操作，查看平台是否提交了获取 AccessToken 的请求，是否收到了对方发回的 RefreshToken、AccessToken 及其有效时长信息，满足则符合要求；测试在定义的有效时长外能否正常请求，不包含 AccessToken 的请求能否被正常处理，不满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.2.2 令牌自身安全

a) **评估方法：**

咨询相关人员，检查源代码，查看其 AccessToken 和 RefreshToken 的生成方法，确认生成因子中是否包含了 PlatID 和时间戳、随机数，使用的 Hash 算法是否是安全的 Hash 算法，长度是否高于 32 位，组成因子是否包含了数字和大小字母和特殊字符，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.2.3 令牌时效安全

a） 评估方法：

1） 咨询相关人员，检查源代码，查看对 AccessToken 的有效期定义是否不超过 2 小时，在超过规定时间或用户登出后对 AccessToken 是否做了自动销毁处理，满足则符合要求；
2） 咨询相关人员，检查源代码，查看对 RefreshToken 的有效期定义是否不超过 14 天，在超过规定时间或用户登出后对 RefreshToken 是否做了自动销毁处理，满足则符合要求；
3） 测试 AccessToken 和 RefreshToken 的处理有效性，在获取到 AccessToken 和 RefreshToken 后，退出登录。之后重新登录并在重新登录后将新的 AccessToken 和 RefreshToken 替换为旧的数据，查看其请求是否能够被正常处理，不能够正常处理则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.2.4 令牌更新安全

a） 评估方法：

1） 咨询相关人员，检查源代码，查看是否主动的对 AccessToken 进行更新，对 AccessToken 的更新请求中是否包含了 RefreshToken 参数，RefreshToken 是否在使用一次后也进行更新，满足则符合要求；
2） 测试 AccessToken 和 RefreshToken 的更新有效性，在获取到 AccessToken 和 RefreshToken 后，退出系统。之后重新登录并获取到新的 AccessToken 和 RefreshToken，对比两次的数据是否一致，一致则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.2.3 授权

a） 评估方法：

1） 检查信息安全策略与规程等相关文档，查看其是否有权限管理策略，有则符合要求；
2） 检查权限管理策略，查看其是否规定了平台账号的访问权限应满足最小、仅必要的权限要求，满足则符合要求；
3） 分别以授权用户和非授权用户身份登录，验证是否只有授权用户才具有访问权限，以及验证权限管理策略中对权限要求的有效性，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.3 数据安全

6.1.3.1 数据传输

6.1.3.1.1 加密密钥获取

a） 评估方法：

1） 咨询相关人员，检查源代码，查看在请求其他云服务时，是否接收了对方发回的动态密

钥，是否用该动态密钥进行数据加密，满足则符合要求；

2) 测试请求其他云服务，验证请求数据是否通过对方的动态密钥做了加密，满足则符合要求。
3) 检查信息安全策略与规程等相关文档，查看其是否定义了个人敏感信息，满足则符合要求；
4) 咨询相关人员，检查源代码，查看是否有针对个人敏感信息的分发密钥机制，是否使用该密钥对数据做加密传输，密钥的有效期是否定义为60分钟，满足则符合要求；
5) 测试访问云平台之间的共享数据，查看是否针对已定义的个人敏感信息做了加密，并测试同一密钥在使用60分钟后是否失效，满足则符合要求。
6) 咨询相关人员，检查源代码，查看密钥的生成方法，确认生成因子中是否包含了用户ID、时间戳和随机数，使用的 Hash 算法是否是安全的 Hash 算法，密钥长度是否高于128位，满足则符合要求。
7) 咨询相关人员，检查源代码，查看其在登录后，是否下发了新的密钥，废弃旧的密钥；在登出操作后，是否废弃了现有密钥，满足则符合要求；
8) 测试两次相同的登录，对比在登录后请求中的数据是否一致，不一致则符合要求。
9) 测试用户登出操作，在重新登录后查看旧的密钥是否不可用，不可用则符合要求。
10) 咨询相关人员，检查存放密钥的数据库，查看密钥与真实密钥是否经过了二次加密，并且加密算法使用了 SM4 或 AES，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.3.1.2 安全传输

a) **评估方法：**

1) 咨询相关人员，检查源代码，查看是否有动态获取加密密钥的机制，是否使用获取的加密密钥对数据进行加密，满足则符合要求；
2) 测试不同登录后的数据请求，对比数据内容，观察个人敏感信息是否做了加密，满足则符合要求，以及加密后的数据内容是否一致，不一致则符合要求。
3) 咨询相关人员，检查源代码，查看加密算法是否使用了 SM4 或 AES 算法，并且使用的方式满足安全要求，满足则符合要求。
4) 咨询相关人员，检查源代码，查看是否针对个人身份信息、个人生物特征识别信息或者密码和口令通过 SM3 或 HMAC 方式进行加盐 Hash，满足则符合要求；
5) 测试请求，观察是否有明文的个人身份信息、个人生物特征识别信息或者密码和口令，没有则符合要求；观察 Hash 后的数据内容是否一致，不一致则符合要求。
6) 咨询相关人员，检查源代码，查看是否对个人敏感信息做了去标识化、匿名化等处理，满足则符合要求；
7) 测试请求，查看个人敏感信息是否做了加密，个人敏感信息是否根据业务场景做了去标识化、匿名化等处理，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.3.2 消息认证

6.1.3.2.1 防重放安全

a） **评估方法：**

1) 宜检查信息安全策略与规程等相关文档，查看其是否有说明防范重放攻击的方法；
2) 宜测试重放请求数据，验证重放是否能成功。

b） **观察项：**

上述评估情况记录为观察项，不做判定。

5.1.3.2.2 时间戳安全

a） **评估方法：**

1） 咨询相关人员，检查时间戳源代码，查看时间戳的精度是否是毫秒级，时间的有效期是否设置为前后 10 分钟内有效，满足则符合要求；
2） 测试请求数据，验证请求是否携带毫秒级别时间戳标记，时间的有效期限是否符合前后 10 分钟有效的要求，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

5.1.3.2.3 算法安全

a） **评估方法：**

1） 咨询相关人员，检查源代码，查看对数据内容和所有接口字段进行校验的算法是否是 SM3 或 HMAC 算法，满足则符合要求；
2） 通过使用算法工具进行实际数据的测试，验证该算法是否是符合要求的 SM3 或 HMAC 算法，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.3.3 数据过滤

6.1.3.3.1 传输格式

a） **评估方法：**

1） 咨询相关人员，检查源代码，查看其对 HTTP 请求方法的定义，是否只允许使用 PUT 或 POST 传输 JSON 格式的数据；并查看其是否对参数数据的范围、长度和类型做了验证，是否对不符合要求的数据包做了丢弃处理，满足则符合要求；
2） 测试系统请求，验证其数据包中的请求头部是否指明了类型 application/json，是否使用了明确恰当的字符集。构造不同的参数数据，查看其是否验证了参数数据的范围、长度和类型，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.3.3.2 参数校验

a） **评估方法：**

咨询相关人员，检查源代码，查看其 JSON 中的所有参数是否使用了强类型和固定长度的校验，满足则符合要求。

b） **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.3.3.3 字符编码

a） **评估方法：**

咨询相关人员，检查源代码，查看在对传入的参数进行过滤前是否将参数数据按照常用字符进行编码，满足则符合要求。

b） **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.3.3.4 参数过滤

a） **评估方法：**

1） 咨询相关人员，检查源代码，查看其是否对传入参数使用了白名单验证，满足则符合要求；
2） 测试系统参数，构造不同的参数数据，验证其白名单机制是否可以绕过，不能绕过则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.4 错误信息处理

a） **评估方法：**

1） 访谈安全管理员等相关人员，询问是否有对云云对接过程中请求失败的处理机制，满足则符合要求；
2） 构造错误请求触发请求失败，查看其在请求失败的情况下，是否仅通过错误编码来表示错误类型，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.5 接口稳定性

6.1.5.1 服务与系统安全

a） **评估方法：**

1） 检查信息安全策略与规程等相关文档，查看其是否有服务安全加固策略，满足则符合要求；
2） 检查服务安全加固策略，查看其是否规定了对服务器进行系统和服务的加固，包括开放端口的白名单、中间件版本及安全配置、口令复杂度等，满足则符合要求；
3） 访谈安全管理员等相关人员，要求其演示所执行的安全加固措施，确认安全加固措施是

否效性，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.5.2 风险评估与监控

a） **评估方法：**

1） 检查信息安全策略与规程等相关文档，查看是否有风险控制策略，满足则符合要求；
2） 检查风险控制策略，查看其是否规定了应当定期或者在威胁环境发生变化时，对云计算平台进行风险评估与安全监控，有该规定说明则符合要求；
3） 访谈安全管理员等相关人员，询问是否定期或威胁环境发生变化时对平台进行风险评估，险评估工作、服务商安全监控是否由第三方进行，满足则符合要求；
4） 检查风险评估报告，并询问安全管理员报告中所列出的风险项目是否有做进一步的安全防范措施，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.6 日志审计

6.1.6.1 日志系统部署

a） **评估方法：**

访谈安全管理员等相关人员，询问其是否部署了自动化日志收集与审计系统以监控采集云端云云互联互通业务相关的日志及网络流量，检查其是否通过离线分析和实时分析两种方式分析日志，对于发现的攻击行为是否做到了及时预警并采取应对措施，满足则符合要求。

b） **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.6.2 日志内容

a） **评估方法：**

检查日志收集和审计系统，查看其是否包含 API 接口日志和其他相关业务的服务和流量日志，确认日志中不存在用户敏感数据信息，满足则符合要求。

b） **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.6.3 审计系统安全

a） **评估方法：**

1） 检查审计策略与规程等相关文档，查看其是否定义了可以审计的事件清单，是否规定了需要审计的内容，是否要求保留审计记录，是否规定了分析和审查的频率，是否根据规定的频率对日志进行分析和审核，是否有防止审计记录非授权访问、篡改和删除的机制，满足则符合要求；

2) 访谈安全管理员等相关人员，询问其可审计的事件清单、需要审计的内容、对日志进行分析和审查的频率，查看其是否与文档中规定的一致，一致则符合要求；
3) 检查日志的审计记录，查看其是否包含了所规定的内容，如审计的内容、审查的频率等，确认与策略文档中规定的一致，一致则符合要求；
4) 测试审计记录保护机制，验证审计记录是否能被非授权访问、篡改或删除，不能被非授权访问、篡改或删除则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.1.6.4 日志保存时间

a) **评估方法：**

1) 检查审计策略与规程等相关文档，查看其是否规定了日志保存时间应不少于 6 个月，满足则符合要求；
2) 访谈安全管理员等相关人员，询问其对接口请求日志保存时间，时间不少于 6 个月则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

e）异常日志处理

a) **评估方法：**

检查日志收集和审计系统，测试异常日志，确认在产生异常日志后自动告警到相关运维人员，并由运维人员进行对应的分析和处理，满足则符合要求。

b) **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2 安全事件协同管理

6.2.1 安全事件的分类和分级

6.2.1.1 安全事件分类

a) **评估方法：**

1) 检查信息安全策略与规程等相关文档，查看其是否对不同类型的信息安全事件做了定义，包括数据泄露事件、服务不可用事件、其他事件，满足则符合要求；
2) 检查信息安全事件记录等相关文档，查看是否依据不同类型的信息安全事件定义对已发生的信息安全事件做了分类记录，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.1.2 事件分级

a) **评估方法：**

1) 检查信息安全策略与规程等相关文档，查看其是否依据国标 GB/Z 20986 对不同等级的信息安全事件做了定义，或者是否引用了国标 GB/Z 20986 中的安全事件分级定义，包括特别重大事件、重大事件、较大事件和一般事件，满足则符合要求；
2) 检查信息安全事件记录等相关文档，查看是否依据不同等级的信息安全事件定义对已发生的信息安全事件做了分级记录，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.2 责任模型

a） **评估方法：**

1） 检查信息安全策略与规程等相关文档，查看其是否依据不同类型的信息安全事件定义了相对应的责任模型，包括针对数据泄露事件的责任模型、针对服务不可用事件的责任模型、针对其他事件或责任未明确情况下的责任模型，满足则符合要求；
2） 检查信息安全事件记录等相关文档，查看其是否依据不同类型信息安全事件的责任模型对已发生的信息安全事件进行追责并做了追责记录，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.3 服务条款

6.2.3.1 服务条款

a） **评估方法：**

检查云云互联双方签订的具有法律效应的服务条款，查看其是否包含了以下内容：
1) 云云互联企业双方的服务内容;
2) 云云互联企业双方各自的权利和义务;
3) 涉及用户数据、用户个人敏感信息，需要明确数据的所有权，使用权限;
4) 保密条款，包括用户数据、用户个人敏感信息不允许主动向第三方披露等;
5) 服务期限和终止，并且终止后双方对于信息安全的义务;
6) 违约责任和免责条款。

b） **结果判定：**

服务条款中包含上述内容则判定结果为符合，其他情况判定结果为不符合。

6.2.3.2 平台数据所有权说明

6.2.3.2.1 个人信息数据

a） **评估方法：**

1) 检查个人权利处理政策等相关文档，查看其是否对实际个人用户所拥有的权利做了详细说明，包括对个人信息的完全访问权、控制权等，满足则符合要求；
2) 检查个人权利处理政策等相关文档，查看在处理个人用户执行相关权利的请求时，是否有详细的处理流程说明，包括但不限于接收请求、确认请求、处理请求等，满足则符合要求；

3) 访谈相关流程处理执行人员，询问处理用户执行其访问权和控制权的情况，确认是否符合个人权利处理政策中的要求，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.3.2.2 匿名化数据

a） **评估方法：**

1) 检查数据保留政策等相关文档，查看其是否定义了需要做匿名化的数据以及匿名化数据的归属权，确认匿名化的数据是否归属于提供信息的云平台主体，满足则符合要求；
2) 访谈安全管理员等相关人员，询问云平台是否对匿名化的数据有完全的访问权和控制权，有则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.3.2.3 云平台与合作平台数据

a） **评估方法：**

1) 检查信息安全策略与规程等相关文档，查看其是否对用户数据和归属合作平台的数据的使用、披露流程、例外情况做了详细的说明，使用和披露包括应当有严格的权限控制机制，任何未获授权的使用和披露均不能执行，满足则符合要求；
2) 例外情况包括在国家有关机关依法查询或调阅用户数据的情况下，可以越权使用和披露相关数据，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.3.3 平台数据使用权限说明

6.2.3.3.1 数据的披露

a） **评估方法：**

1） 检查数据隐私政策等相关文档，查看其是否详细说明了向第三方披露数据的情况，满足则符合要求，包括：

----未在双方书面允许和用户授权的情况下，不允许向第三方披露个人信息。

----只允许为提供或改进产品、服务的目的而与第三方共享。

----不允许为第三方的销售目的而与第三方共享数据，更不允许销售共享数据。

2) 访谈安全管理员等相关人员，询问向第三方披露数据时的情况，确认是否符合向第三方披露数据的要求，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.3.3.2 数据的删除

a） 评估方法：

1） 检查个人权利处理政策等相关文档，查看其是否对个人用户所拥有的数据删除权做了详细说明，满足则符合要求，包括：

----用户有权申请删除其在双方平台交互过程中，产生的个人数据。平台双方需要在 7 天内完成数据删除。

----非个人数据，数据归属平台有权利要求共享平台对数据进行删除的操作。

----所有数据删除的操作，需要在企业内部有明确的流程和制度保障。

----在服务终止后，必须安全删除通过云云互联接口同步过来的用户数据及用户个人敏感信息。

----对于已删除的个人数据，不能对其进行恢复操作。

2） 访谈相关流程处理执行人员，询问在用户执行其删除权的情况，确认是否符合个人权利处理政策中的要求，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.3.3.3 数据的访问控制

a） 评估方法：

1） 检查标识鉴别策略与规程等相关文档，查看其是否有描述访问平台数据的用户进行唯一性标识与鉴别的要求，满足则符合要求。

2） 访谈系统安全负责人或账号管理员等相关人员，询问访问平台数据的用户类别、角色以及对用户的管理实施情况，实施情况和文档说明一致则符合要求。

3） 检查标识鉴别策略与规程等相关文档，查看其是否有描述对特权账号的数据访问实施多因子鉴别的要求，满足则符合要求。

4） 访谈特权账号的使用人员，询问在实际中数据访问时是否实施了多因子鉴别，满足则符合要求。

5） 检查特权账号的数据访问机制，查看其是否实施多因子鉴别，满足则符合要求。

6） 检查数据访问机制，查看其是否对数据访问方式进行授权，满足则符合要求。

7） 测试数据访问机制，验证在对平台数据访问前是否进行授权，满足则符合要求。

8） 检查数据访问机制，查看其是否有措施实时监视非授权的连接，满足则符合要求。

9） 检查数据访问连接监视机制，查看其在发现非授权连接时是否可以采取恰当的对应措施，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.4 明确责任部门和人员

6.2.4.1 负责人责任

a） 评估方法：

1） 检查信息安全策略与规程等相关文档，查看是否定义了云平台主要负责人及其对应的信息安全领导责任，满足则符合要求；

2） 访谈定义的云平台主要负责人，询问是否收到过相应的策略与规程，是否为信息安全工

作提供人力、财力、物力保障等，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.4.2 接口人责任

a） **评估方法：**

1) 检查信息安全策略与规程等相关文档，查看是否定义了云平台对接的安全接口人与备用接口人，是否定义了相关人员的职责，满足则符合要求；
2) 访谈定义的云平台安全接口人与备用接口人，询问是否收到过相应的策略与规程，是否知晓其相应的职责，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.5 应急响应

6.2.5.1 事件责任方

a） **评估方法：**

检查应急响应策略与规程等相关文档，查看其是否规定了在产生紧急事件时，各平台应协同诊断，认定安全事件和事件的责任方，有相关描述则符合要求。

b） **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.5.2 责任方职责

a） **评估方法：**

1） 检查应急响应策略与规程等相关文档，查看其是否规定了事件责任方应根据合作服务条款内的明细，在指定时间内抑制受害范围并恢复业务服务，有相关描述则符合要求。
2） 检查事件责任方编写的应急响应事件调查记录，调查记录中是否明确记录了本次事件的起因、受影响时间、追责过程、应急过程、故障解决、事件复盘、改进措施等内容，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.6 事件通告

6.2.6.1 义务和权利

a） **评估方法：**

1） 检查应急响应策略与规程等相关文档，查看其是否有建立安全事件发布机制，满足则符合要求；
2） 访谈安全管理员等相关人员，询问是否在必要时发出过安全事件通告；

3) 检查相应的发布记录（如有），查看其是否按要求详细说明了安全事件的原因，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.6.2 重大影响通告

a) **评估方法：**

1) 访谈安全管理员等相关人员，询问是否因特别重大事件、重大事件或较大事件导致对业务可用性和稳定性的影响时间超过 1 个小时的条件下发出过安全事件通告；
2) 检查相应的发布记录（如有），查看其是否按照与各相关方的服务条款进行事件的对外通告，满足则符合要求。

b) **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.6.3 法律义务通告

a) **评估方法：**

1) 访谈安全管理员等相关人员，询问是否对有关事件响应的法律、法规和/或规章中要求的地方、省、国家有关部门发出过安全事件通告；是否有过与与法律强制部门联络的记录；
2) 检查相应的发布记录与记录文件（如有），查看其是否符合相关的法律规定，满足则符合要求。

b) **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.2.7 持续改进评估方法

a) **评估方法：**

1) 检查事件责任方在事件发生后给出的事件调查记录是否包含改进措施说明，包括管理层面的改进措施或技术层面的改进措施，满足则符合要求；
2) 访谈安全管理员等相关人员，询问改进措施是否真实落地，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3 对个人信息保护的特别要求

6.3.1 数据生产和收集

6.3.1.1 基本原则

6.3.1.1.1 合法性

a) **评估方法：**

1) 检查数据隐私政策等相关文档，查看其是否包含了对数据收集与数据处理等行为的法律依据说明，查看其是否明确了相对应行为的法律责任，同时是否明确了相对应的安全的数据处理措施，满足则符合要求；
2) 访谈法务等相关人员，询问其是否知晓公司在对用户数据收集与数据处理方面的行为与相对应的法律责任，是否知晓对应的安全的数据的处理措施，知晓则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.1.1.2 用户授权

a) **评估方法：**

1) 检查信息安全策略与规程等相关文档，查看其是否有敏感操作授权策略，满足则符合要求；
2) 检查对应策略，查看其是否规定了应通过有效的渠道获取信息主体的授权，不允许超过信息主体授权行为以外的数据收集和操作，满足则符合要求；
3) 访谈安全管理员等相关人员，要求其演示在对用户信息进行收集与操作时，是否经过信息主体授权，经过信息主体授权则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.1.1.3 用户权限保障

a) **评估方法：**

1) 检查个人权利处理政策等相关文档，检查其是否对用户所属的权利做了详细说明，说明应包含用户何时行使该权利、用户行使该权利的方式、如何支持用户行使该权利等，满足则符合要求；
2) 访谈安全管理员等相关人员，询问用户行使相应权利时双方所做的工作，确认是否满足对用户权利的保障，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.1.1.4 数据最小化

a) **评估方法：**

1) 检查数据隐私政策等相关文档，查看其是否列出了收集用户数据的类型，满足则符合要求；
2) 访谈安全管理员等相关人员，询问列出的每个收集的用户数据类型的用途和场景，以及数据在存储、请求、提供、传递等服务过程中，使用了哪些用户数据，确认是否满足数据最小化原则，满足则符合要求。

b) **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.1.1.5 数据分类

a） 评估方法：

1） 检查信息安全策略与规程等相关文档，查看其是否定义了个人数据和平台信息数据，满足则符合要求；
2） 访谈安全管理员等相关人员，询问其是否按定义对个人数据和平台信息数据做了分类，以及如何实现该分类，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.1.2 用户权限

6.3.1.2.1 知情权

a） 评估方法：

1） 检查数据隐私政策等相关文件，查看其是否规定了信息收集主体及其所提供服务的基本情况、要收集的数据及这些数据的用途、用户所享有的权力信息等，满足则符合要求；
2） 访谈安全部门相关人员，询问用户在何时以何种方式可以阅读到隐私政策，检查隐私政策是否放在显眼的位置，是否需要用户手动点击已阅读，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.1.2.2 选择权

a） 评估方法：

访谈安全管理员等相关人员，要求其演示在收集数据时是否明确告知用户并征求用户同意，在用户选择拒绝后是否仅不提供该数据相关的服务而其他服务应照常提供，满足则符合要求。

b） 结果判定：

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.1.2.3 处置权

a） 评估方法：

1） 检查个人权利处理政策等相关文档，检查其是否对用户所属的访问权、迁移权、删除权等权利做了详细说明，说明是否包含用户行使该权利的方式，如客服电邮、客服电话等，是否包含如何支持用户行使相应的权利，满足则符合要求；
2） 访谈安全管理员等相关人员，询问是否支持用户账号的注销机制，在用户要求删除用户数据或注销用户账号时是否删除与之相关的用户数据，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.2 数据的使用

6.3.2.1 数据展示

a） 评估方法：

1） 检查信息安全策略与规程等相关文档，查看其是否有敏感数据脱敏策略，满足则符合要求；
2） 检查敏感数据脱敏策略，查看其是否有规定对外展示的个人信息要做脱敏处理，满足则符合要求；
3） 访谈安全管理员等相关人员，要求其演示对需展示的个人信息是否采取去标识化处理等措施，确认个人信息在展示环节的安全，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.2.2 数据审计

a） 评估方法：

1） 检查审计策略与规程等相关文档，查看其是否定义了自动化数据库操作审计记录行为，以及对可能有风险的操作的审批流程，满足则符合要求；
2） 检查数据库操作审计记录，查看其是否与定义的操作审计记录行为一致，一致则符合要求；
3） 检查有风险操作的审批流程，查看是否与定义的审批流程一致，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.3 数据保存

6.3.3.1 数据存储

a） 评估方法：

1） 检查信息安全策略与规程等相关文档，查看其是否规定了对敏感数据进行集中地分布式存储、统一监控管理、通过 VPC 隔离，是否有隐私信息策略，是否对隐私信息做了定义，满足则符合要求；
2） 访谈安全管理员等相关人员，询问其实际中是否对敏感数据进行了集中地分布式存储、是否进行了统一监控管理、是否通过 VPC 隔离，满足则符合要求。
3） 检查数据库加密机制，查看其是否根据隐私信息的定义对所有隐私信息进行加密或 hash 后存储，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.3.2 数据传输

a） 评估方法：

访谈安全管理员等相关人员，询问在中国产生的用户数据是否都存储在中国境内，是否有跨境传输行为，如有跨境传输是否符合中国大陆法律法规，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.3.3 数据备份

a） 评估方法：

1） 检查容灾备份计划，查看其是否有异地容灾备份的说明，满足则符合要求；
2） 访谈安全管理员等相关人员，询问云服务是否采用分布式架构，所有业务服务器是否同时部署在多个不同的机房，数据是否同时存放两个以上机房并实时备份，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.3.4 存储时间

a） 评估方法：

1） 访谈安全管理员等相关人员，询问是否有对个人敏感信息提供保护的机制，满足则符合要求；
2） 检查个人敏感信息保存机制说明文档，查看对用户个人敏感信息的保存期限，确认保存期限是否不超过 1 年，查看其是否有数据删除与销毁策略，满足则符合要求；
3） 检查数据删除与销毁策略，查看其是否规定了删除和销毁数据的流程与方法，满足则符合要求；
4） 检查具有法律效力的合作合同与其附属条款，查看其是否规定了在服务期届满、服务提前终止时，可以按照平台约定的缓冲期内继续存储对方平台的用户数据，缓冲期不超过 7 天，平台应在 7 天缓冲期后执行删除所有相关用户数据的操作，包括缓存或者备份的副本，满足则符合要求。

b） 结果判定：

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.4 数据销毁

6.3.4.1 销毁策略

a） 评估方法：

1） 检查信息安全策略与规程等相关文件，查看其是否有数据删除与销毁策略，满足则符合要求；
2） 检查数据删除与销毁策略，查看策略中是否包含了对云主机内部的数据以及实体介质的数据的删除与销毁，满足则符合要求；
3） 访谈安全管理员等相关人员，询问是否发生过数据销毁记录。
4） 检查删除与销毁数据过程记录（如有），查看其是否明确记录了数据删除与销毁的过程，满足则符合要求；
5） 检查删除与销毁数据的审批记录（如有），查看其是否明确记录了数据删除与销毁的审批过程，满足则符合要求。

b） **结果判定：**

上述评估结果均符合要求则判定结果为符合，其他情况判定结果为不符合。

6.3.4.2 法律责任

a） **评估方法：**

检查具有法律效力的合作合同与其附属条款，查看其是否规定了在违约未销毁数据的情况下，应承担的法律责任，满足则符合要求。

b） **结果判定：**

上述评估结果符合要求则判定结果为符合，其他情况判定结果为不符合。

附 录 A

（资料性）

相关法规、标准、认证规则

A.1 导则

以下列举当前（2020.04）对于云平台和个人信息保护具有重要指导作用的法规、标准、认证规则，为了保障互联双方具有能力共同保障互联业务的信息安全，云云互联双方应基于具体的业务特点，在参考以下一项或多项标准及技术法规的基础上，实现云云互联互通。

A.2 国内相关标准和认证规则

a) 可信云服务认证（TRUCS）
b) 信息技术 安全技术 信息技术安全评估准则（GB/T 18336）
c) 信息安全技术 云计算服务安全能力要求（GB/T 31168）
d) 信息安全技术 云计算服务安全指南（GB/T 31167）
e) 信息安全技术 个人信息安全规范（GB/T 35273-2020）

A.3 国际相关法规、标准、认证规则

a) ISO 15408 信息技术安全评估准则
b) ISO 27001 信息安全标准
c) ISO 27017 云服务安全标准
d) ISO 27018 云服务隐私保护操作规范
e) CSA STAR 云安全保障认证
f) 欧盟一般数据保护条例（GDPR）