



北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

让冬奥更安全 让世界更精彩

奇安信可信应用检控 产品彩页

地址：北京市西城区西直门外南路26号院1号

邮编：100044

1 产品概述

可信应用检控部署在业务应用与应用服务之间，接受零信任体系控制，通过令牌检查、协议格式检查、业务应用访问权限检查与控制等安全措施，确保全程用户可信、业务应用可信、服务可信，为业务应用对应用服务资源的访问提供安全保障。满足《GA/DSJ350-2020 公安大数据安全安全访问与数据交换技术设计要求》中可信应用检控能力要求。

2 产品功能

2.1 加密流量解密

2.1.1 功能描述

提供 SSL/TLS 加密流量解密能力，确保数据通信安全。

2.1.2 设计思路

在业务应用与业务服务交互全过程中，需要采取相应的安全措施，确保业务网络通信数据的安全。通常，业务网络通信需要考虑以下三个方面的安全风险：

- (1) 窃听风险：第三方可以获知通信内容。
- (2) 篡改风险：第三方可以修改通信内容。
- (3) 冒充风险：第三方可以冒充他人身份参与通信。

SSL/TLS 是一种为网络通信提供安全性及数据完整性保障的安全协议，已成为网络通信中使用最广泛的标准安全技术。SSL/TLS 基于加密技术，实现通信双方之间数据信息的安全传递，实现数据信息的保密性、完整性，从而确保所传送的数据不容易被网络黑客截获和破解，并能够通过校验证书，实现对通信双方的身份鉴别确保身份的可信。综上所述，SSL/TLS 提供以下安全机制：

(1) 传输数据的机密性：利用对称密钥算法对传输的数据进行加密，从而确保所有信息都是加密传播，第三方无法窃听。

(2) 身份验证机制：基于证书利用数字签名方法对服务端和客户端进行身份验证，当中客户端的身份验证是可选的，从而防止身份被冒充。

(3) 消息完整性验证：消息传输过程中使用 MAC 算法来检验消息的完整性，一旦被篡改，通信双方会立刻发现。

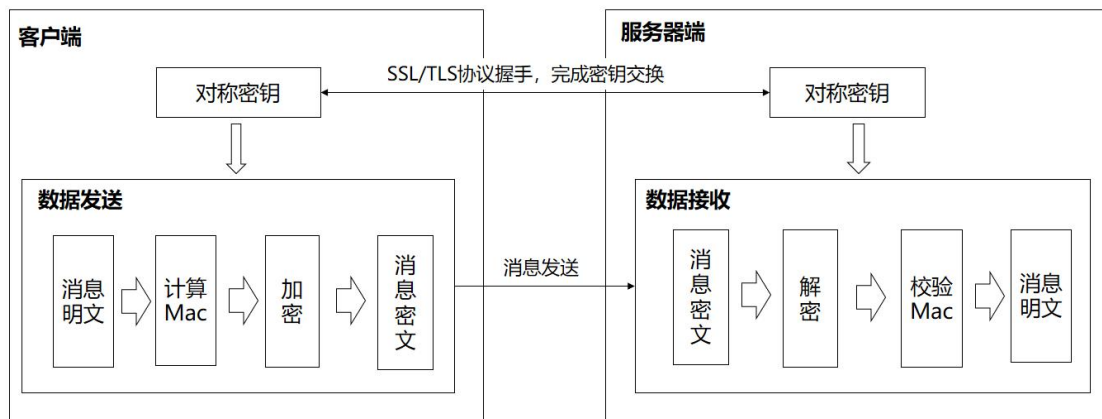
2.1.3 技术原理

SSL/TLS 协议的技术原理是采用公钥加密法，也就是说，客户端先向服务器端索要公钥，然后用公钥加密信息，服务器收到密文后，用自己的私钥解密。SSL/TLS 协议的基本过程是这样的：

- (1) 客户端向服务器端索要并验证公钥。
- (2) 双方协商生成“对话密钥”。
- (3) 双方采用“对话密钥”进行加密通信。

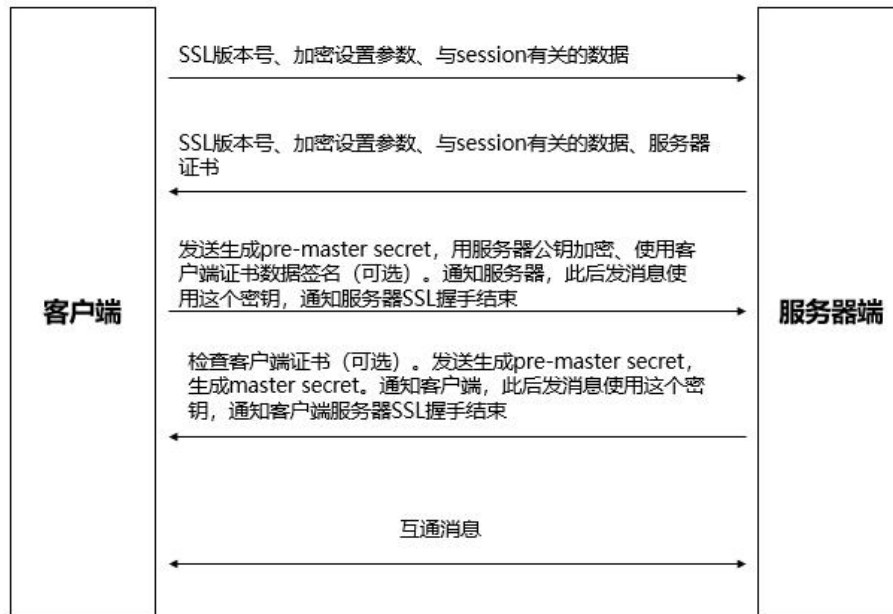
上面过程的前两步，又称为“握手阶段”（handshake）。

采用 SSL/TLS 进行数据传输技术原理如下所示：



如上图所示，客户端和服务端通过握手完成密钥的交换。后续客户端发送时，采用该密钥对数据发送进行 Mac 计算保证完整性，对数据进行加密确保机密性，将数据密文形式发送出去；服务器端接收时，采用该数据进行解密，并做校验 Mac 确保数据没有被篡改，从而得到数据明文。

采用 SSL/TLS 进行安全通信的主要工作流程如下：



(1) 客户端将其 SSL 版本号、加密设置参数、与 session 有关的数据以及一些其他必要的信息发送到服务器。

(2) 服务器将其 SSL 版本号、加密设置参数、与 session 有关的数据以及一些必要的信息发送到浏览器，同时发给浏览器的还有服务器的证书。如果配置服务器的 SSL 需要验证用户身份，还要发出请求浏览器提供的用户证书。

(3) 客户端检查服务器证书，如果检查失败，提示不能建立 SSL 连接，如果成功继续。客户端浏览器为本次会话生成 pre-master secret（预先掌握的密匙），并将用服务器公钥加密后发送给服务器。如果服务器需要鉴别客户身份，客户端还有再对另外一些数据签名后并将其与客户端证书一起发送给服务器。客户端通还要通知服务器此后发送信息都要使用 master secret 进行加密，并通知服务器客户端已经完成本次 SSL 握手。

(4) 如果服务器要求鉴别客户身份，则检查签署客户证书的 CA 是否可信，如果不在信任列表中，结束本次会话。如果检查通过，服务器用自己的私钥解密后收到 pre-master secret，并用它通过某些算法生成本次会话的 master secret。服务器通知客户端此后发送的信息都是用 master secret 进行加密，并通知客户端服务器端已经完成本次 SSL 握手。

2.2 协议格式检查与控制

2.2.1 功能描述

在安全访问模式下，实现对 HTTP、HTTPS 类应用 API 服务代理，提供请求和响应报文头、报文格式检查功能，支持 HTTP、WebSocket 的通信协议，根据检查结果阻断或放行，并能支持 WebSocket 类应用 API 服务代理，能够基于控制策略实施相应的阻断或放行控制措施。

提供开放接口，实现对接联调；支持 IPV4 和 IPV6 协议。

2.2.2 设计思路

不同的业务应用对应用服务的调用有不同需求，应用服务可以发布成基于 HTTP、HTTPS 的 API 服务接口，也可以发布成基于 WebSocket 协议的 API 服务接口，以满足不同业务应用场景的需求。可信接入检控按照不同协议类型的应用服务，充分考虑各种应用服务协议的特点，有针对性的采用不同的应用服务代理技术，实现应用服务的代理以及协议检查和控制。

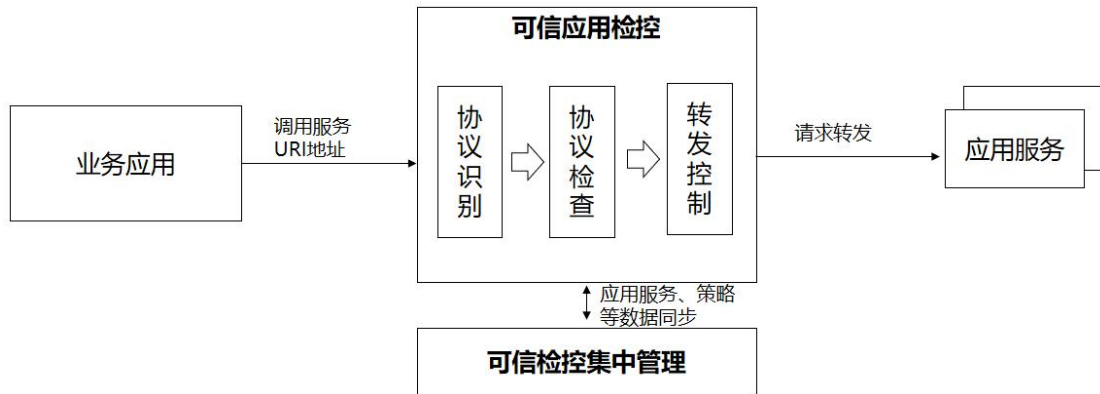
2.2.3 技术原理

协议格式检查与控制，主要涉及可信检控集中管理和可信应用检控两个部分，其中：

可信检控集中管理实现控制面的能力，主要是提供基于 HTTP、HTTPS 等协议的应用服务 API 发布、代理和管理，提供应用服务 API 相关检查策略的配置和管理，并将这些配置信息自动同步到可信接入检控。

可信应用检控实现数据面的能力，其根据可信检控集中管理的策略对代理的应用服务 API 和协议进行检查和控制。

在业务应用通过可信应用检控对应用服务 API 进行调用时，协议格式的检查与控制主要分为三个阶段，首先是协议识别，以便区分识别出不同类型的应用服务 API。接着是应用调用请求协议检查，根据协议进行按照既定的要求逐项进行检查。最后是应用服务请求转发控制，是根据策略对于符合要求的请求进行放行，对于不满足要求的请求进行阻断或者其他处置。



当业务应用访问应用服务 API 时，可以通过应用服务 API 的 IP 地址和路径、域名和路径的 URI 地址，访问到应用服务 API。当访问流量到达可信应用检控后，可信应用检控首先进行协议识别，以区分出 HTTP、WebSocket 不同协议的服务访问请求。接着，根据协议类型分别对相关参数数据进行检查。当所有检查都符合要求时，可信应用检控将正常转发相应访问请求到后端的应用服务 API。当发现不符合要求时，可信接入检控则根据相应的策略进行阻断或进行其他处置。

2.3 令牌检查与控制

2.3.1 功能描述

提供用户令牌、应用令牌检查能力，通过调用认证服务提供的服务接口，向认证服务进行令牌格式、签名、内容、有效期的安全检查，按照制定的策略依据检查结果执行阻断或放行控制措施。

2.3.2 设计思路

令牌是用户访问业务应用过程的一种重要凭证，只有具有相应令牌的用户才能访问业务。为了更细粒度的访问控制，将令牌分为用户令牌和应用令牌两种。用户令牌是由认证服务在用户完成登录认证之后颁发，代表用户的身份；应用令牌是用户对应用访问发起访问时，由认证服务颁发的应用令牌，代表用户访问该应用所具备的凭证，用户只有携带相应的应用令牌才能访问到应用。当业务应用访问应用服务 API 时，也需要携带相应的应用令牌才发起对应用服务 API 的访问。为了保证访问过程的安全，当对应用服务 API 的访问请求通过可信应

用检控时，可信应用监控需要对令牌的签名、有效期等情况进行检查，确保只有携带了正确的并且是合法应用令牌的服务访问请求，才能够通过，否则阻断。

2.3.3 技术原理

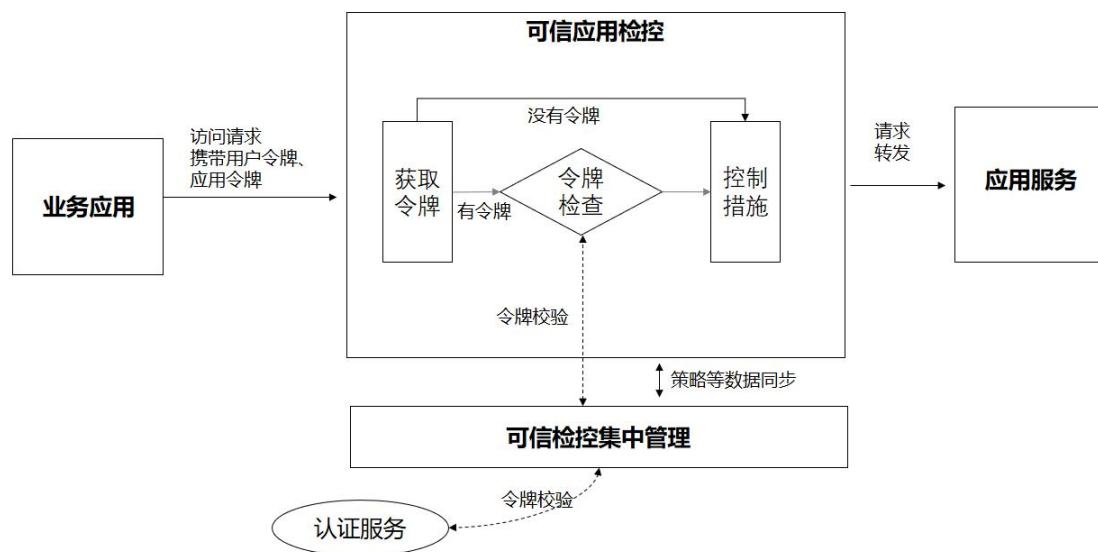
令牌检查与控制主要涉及以下服务：

可信检控集中管理提供策略管理、认证服务对接能力，其与认证服务对接，与认证服务进行业务交互，完成令牌的接收以及令牌的验证；

可信应用检控通过可信检控集中管理，向认证服务进行令牌的验证，并根据策略实施相应的控制措施。

认证服务提供令牌颁发能力，实现用户令牌、应用令牌的颁发，并提供相应的令牌验证服务。

令牌检查和控制分为获取令牌、令牌检查、控制措施三个阶段。当应用服务 API 访问请求经过可信应用检控时，可信应用检控会从请求 Header 或 URL 中提取相应的令牌，如果没有令牌，则按照既定的策略执行相应的控制措施，比如阻断访问。如果有令牌，进入令牌检查阶段，此时可信应用检控将通过可信检控集中管理向认证服务进行令牌检验，令牌验证将对令牌的格式、签名、有效期、内容等依次校验，只有这项全部验证通过之后，可信接入检控将根据既定的策略进行应用服务请求转发，如果有任何一项验证失败，可信接入检控将根据既定的策略实施控制措施，比如阻断应用服务访问。



2.4 业务应用访问权限检查与控制

2.4.1 功能描述

在安全访问模式，提供业务应用对应用服务/数据服务访问权限检查能力，并根据策略实施相应的阻断或放行控制措施。

2.4.2 设计思路

在业务应用访问应用服务 API 的过程中，应对业务应用的访问权限进行检查，确保只有拥有权限的业务应用才能进行访问，防止非授权的访问。当应用服务 API 访问请求经过可信应用检控时，可信应用检控使用权限服务的提供的权限检查服务接口，完成业务应用权限的检测，并根据可信集中管理制定的策略实施相应的控制措施。

2.4.3 技术原理

用户访问权限检查与控制主要涉及以下服务：

可信检控集中管理提供策略管理、权限服务对接能力，其与权限服务对接，调用权限服务接口，完成应用访问权限的检查。

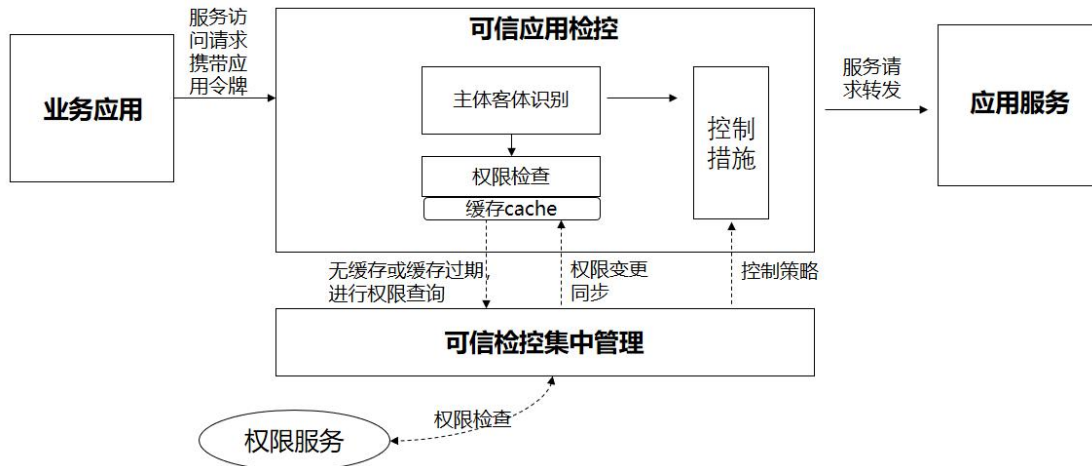
可信应用检控通过可信检控集中管理，向权限服务进行访问权限检查，并根据策略实施相应的控制措施。

权限服务实现权限的管理，提供访问权限检查服务。

业务应用访问权限检查和控制分为主体客体识别、权限检查和控制措施三个过程。

当应用服务访问请求经过可信应用检控时，可信应用检控会从请求消息中提取应用令牌，经过令牌验证后，从令牌中取得相应的访问主体和客体标识 ID，从而完成主体客体识别。接着，根据主、客体的 ID，进行访问权限检查。当进入访问权限检查阶段时，可信应用检控首先从缓存 cache 中检索权限，如果没有权限或者缓存过期，则向可信应用检控集中管理发起权限检查请求，可信应用检控集中管理调用权限服务的接口，完成访问权限检查。如果检查通过之后，可信应用检控将根据既定的策略进行请求转发，如果检查不通过，可信应用

检控将根据既定的策略实施控制措施，比如阻断访问。此外，为了提高可信应用检控的处理效率，可信应用检控采用了权限缓存 cache 机制，对业务应用的访问权限进行一定时间的缓存，当权限发生变更时，将根据可信检控集中管理权限变更同步清空缓存，并在下次的权限检查时对访问权限再次进行缓存，从而确保权限的一致性。



2.5 限流限速控制

2.5.1 功能描述

针对应用服务 API 的访问，可信接入检控能够支持对业务应用访问应用服务 API 的限流限速，以防止访问请求流量过大，过度消耗应用服务 API 资源，导致应用服务 API 崩溃或服务中断。具体如下：

- (1) 支持对按请求数、按请求速率限制，包括请求并发数、请求流量大小、请求数、单位时间内请求速率；
- (2) 支持对响应传输速度大小限制。

2.5.2 设计思路

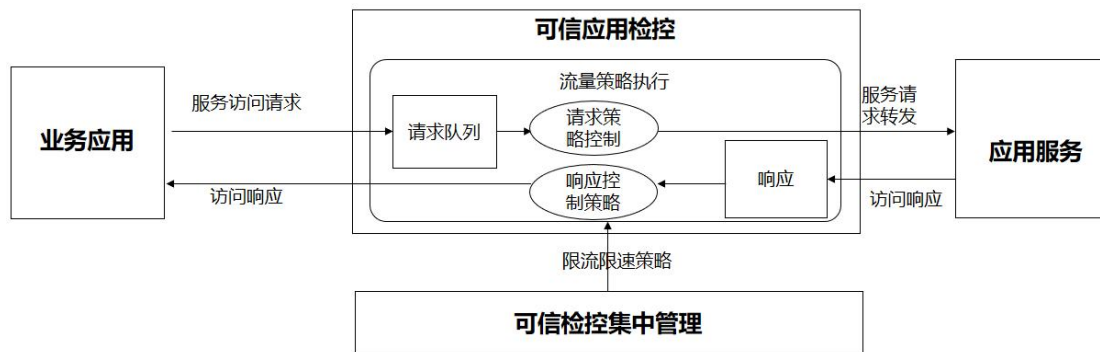
业务应用访问应用服务 API 的过程中，针对网络流量发起攻击，导致应用服务 API 无法正常工作是很常见的一类安全问题，比如恶意的频繁调用、恶意爬虫行为等。针对这类攻击，除了借助于第三方的网络安全设备或系统之外，可信应用检控也应该具备基本的防御能力，以便更好的保护应用服务 API。

可信应用检控分别从上行的访问请求和上行的访问响应两方面入手,提供基本的限流限速控制能力。针对上行的访问请求,主要是从按请求连接数限速、按请求速率限速等多个维度进行控制;针对下行的请求响应,则从响应速率来进行控制,从而确保请求和响应均能在可信应用检控的控制范围之内,缓解恶意调用的网络流量攻击,保证应用服务 API 正常稳定运行。

2.5.3 技术原理

可信检控集中管理为管理人员提供限流限速的策略配置和管理功能,相应的策略自动同步到可信接入检控,由可信接入检控在代理和转发访问请求时,根据策略的执行相应的控制。

可信应用检控采用漏桶算法 (Leaky Bucket) 进行实现限流限速。也就是,当访问请求到达可信应用检控时,可信应用检控使用事先准备的请求队列进行缓存,如果队列未满,则进入队列等待处理。如果队列已满,则丢弃请求并返回错误消息。进入队列的访问请求,按照 FIFO (先进先出) 的原则依照策略依次进行处理,从而保证应用服务 API 请求都是几乎是匀速、平稳的转发。相应的,应用服务 API 的响应也类似处理,从而实现根据限流限速策略,响应能够匀速的转发给业务应用。



2.6 数据校验

2.6.1 功能描述

提供对基于 HTTP 协议的 RESTful 应用服务 API 访问请求消息体 body 中 JSON 数据格式的校验,支持 POST、PUT、PATCH 等 HTTP 协议方法。提供业务应用访问日志、检控告警记录及上报功能。

2.6.2 设计思路

当前，基于 HTTP 协议的 RESTFUL 形式发布应用服务 API 接口，是业内的主流做法。它采用标准 JSON 格式进行数据交互，使得业务应用与应用服务 API 之间的调用和通信，更加简单，易于实现和管理，得到了广泛的使用。针对 RESTful 形式的应用服务 API 接口，为了防止注入型安全问题，首要的安全措施就是需要对访问请求数据进行检查，确保符合要求格式的请求数据才能被传递到应用服务 API 接口，从而避免应用服务 API 接口受到安全威胁。

2.6.3 技术原理

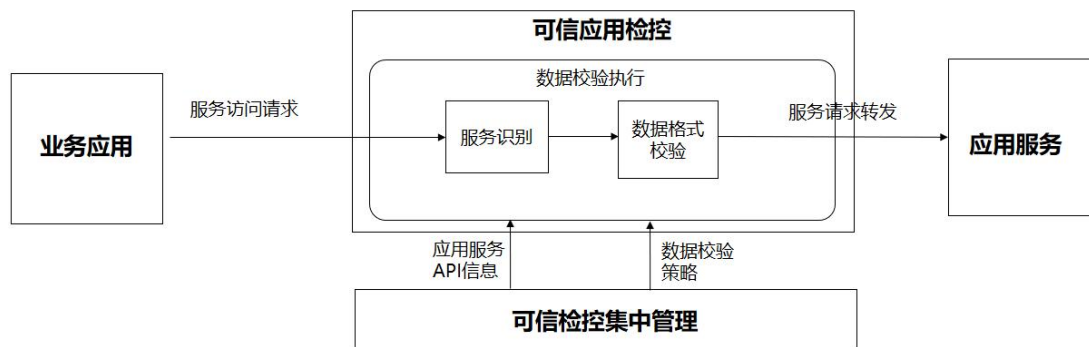
可信应用检控的数据校验，主要涉及以下组件：

可信检控集中管理提供应用服务 API 的管理，数据校验策略的管理。

可信应用检控代理应用服务 API，接受可信检控集中管理制定的数据校验策略，对数据访问请求数据进行校验检查。

可信应用检控数据校验主要分为服务识别、执行数据校验两个阶段。

当业务应用通过可信应用检控访问应用服务 API 时，可信应用检控会根据协议和服务地址路径等信息，明确服务请求方法和完整的 URI 信息，从而完成服务识别。接着，根据请求方法和应用服务 URI，检索是否存在校验数据的规则策略。如果不存在，则表示不要进行数据校验，则可信应用检控继续转发该服务访问请求。如果存在相应的校验规则策略，则对请求消息的 body 中 JSON 格式进行解释，并根据校验规则，依次对各数据项进行校验。一旦发现数据格式不符合要求，则向业务应用返回错误消息。如果各项检验通过，则可信应用检控继续转发该服务访问请求。



3 产品配置

(1) 硬件形态

a. 可信检控集中管理硬件配置：

尺寸：2U 机箱宽（435mm）/高（87mm）/长（779.5mm）
CPU：国产化 CPU 16c
内存：32G
硬盘：4T 企业级 3.5 寸硬盘
网卡：4 个千兆电口，2 个万兆光口
电源：冗余电源
操作系统：国产化操作系统麒麟 V10

(2) 软件形态

尺寸：2U 机箱宽（435mm）/高（87mm）/长（779.5mm）
CPU：需要提供 国产化 CPU 16c
内存：32G 以上
硬盘：4T 企业级 3.5 寸硬盘 以上
网卡：4 个千兆电口，2 个万兆光口
电源：冗余电源
操作系统：国产化操作系统麒麟 V10