



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

奇安信可信接入检控 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

● 版权声明

Copyright © 2006–2020 奇安信集团，保留所有权利。

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。

对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“本声明”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“本产品”）。如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分內容。您有责任定期检查免责声明部分的内容，以了解是否发生了变更。如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。

1. 您明确理解并同意，本产品按“现状”提供，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的身份安全风险以及访问控制措施不保证完全正确】，您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。

3. 您明确理解并同意，您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1) 被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2) 因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3) 因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4) 计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5) 政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力或不可预见的情形造成的各类直接或间接损失，均不承担任何责任。

4. 对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。

5. 对于从非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。

6. 上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。



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

7. 奇安信集团保留在不发布通知的情况下随时采取以下行动的权利：**在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

目 录

1	引言	错误！未定义书签。
2	产品概述	1
3	产品功能	1
3.1	错误！未定义书签。
3.1.1	功能描述	1
3.1.2	设计思路	1
3.1.3	技术原理	2
3.2	错误！未定义书签。
3.2.1	功能描述	错误！未定义书签。
3.2.2	设计思路	错误！未定义书签。
3.2.3	技术原理	错误！未定义书签。
4	产品性能	错误！未定义书签。
5	产品价值	错误！未定义书签。
5.1	错误！未定义书签。
5.2	错误！未定义书签。
6	典型应用场景及安装部署	错误！未定义书签。
6.1	典型应用场景	错误！未定义书签。
6.2	产品部署	错误！未定义书签。
7	产品配置	12

1 产品概述

可信接入检控部署在用户与业务应用之间，接受零信任体系控制，通过对终端和用户身份检查和控制、用户权限的检查和控制等安全措施，确保终端可信、用户可信，为终端接入以及用户访问提供安全保障。

产品设计满足《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》中可信接入检控能力要求。

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

在业务访问的全过程中，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。

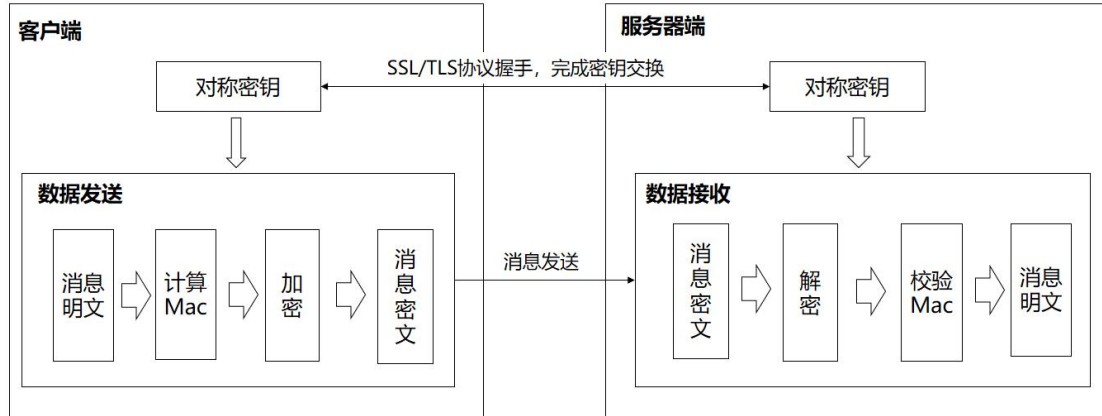
2.1.3 技术原理

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。

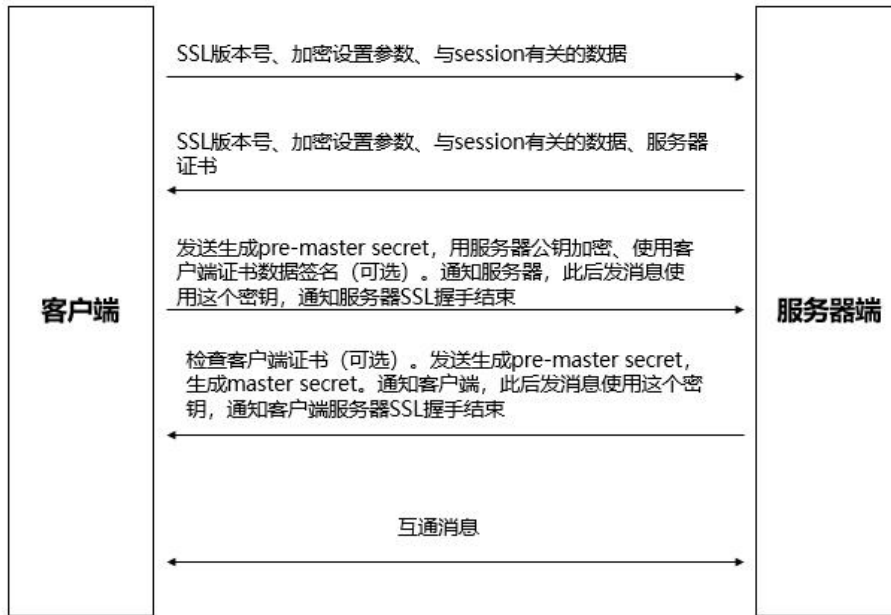
上面过程的前两步，又称为“握手阶段”（handshake）。

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) 用户浏览器将其 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

实现对 HTTP、HTTPS 类 WEB 应用层协议代理，并能支持 WebSocket 类应用层协议代理，支持通过终端侧 CS 客户端完成云桌面流量协议导流，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，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

通常，应用可分为基于 B/S 架构 Web 应用和基于 C/S 架构的客户端-服务器应用程序。Web 应用的访问一般是基于 HTTP 协议通过域名或者 IP 地址访问；C/S 架构一般通过 TCP/IP 协议通过 IP 地址进行访问。可信接入检控按照不同类型的业务应用，充分考虑各种应用类型的特点，有针对性的采用不同的应用代理技术，实现应用的代理以及协议检查和控制。

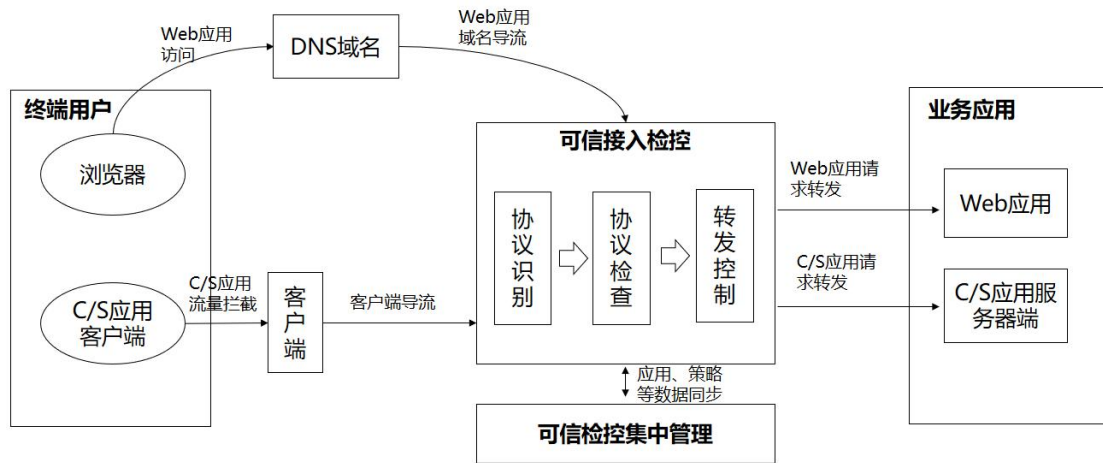
2.2.3 技术原理

协议格式检查与控制，主要涉及可信检控集中管理和可信接入检控两个部分，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 协议的 Web 应用、基于 TCP/IP 协议的 C/S 应用的信息管理和维护，以及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。

可信接入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应用和协议进行检查和控制。

在应用通过可信接入检控进行代理时，应用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业务应用。接着是应用协议检查，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。



当用户访问 Web 应用时，通过 DNS 域名导流方式，将访问流量导流到可信接入检控。当用户访问 C/S 应用时，通过可信接入检控配套的客户端程序，将访问流量导流到可信接入检控。访问流量到达可信接入检控后，可信接入检控首先进行协议识别，以区分出 HTTP、WebSocket、TCP/IP 不同协议的应用。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，可信接入检控将正常转发相应访问请求到后端的业务应用。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。为了保证业务访问过程的安全，当用户的访问请求通过可信接入检控时，可信接入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

法令牌的用户访问请求，才能够通过，否则阻断。

2.3.3 技术原理

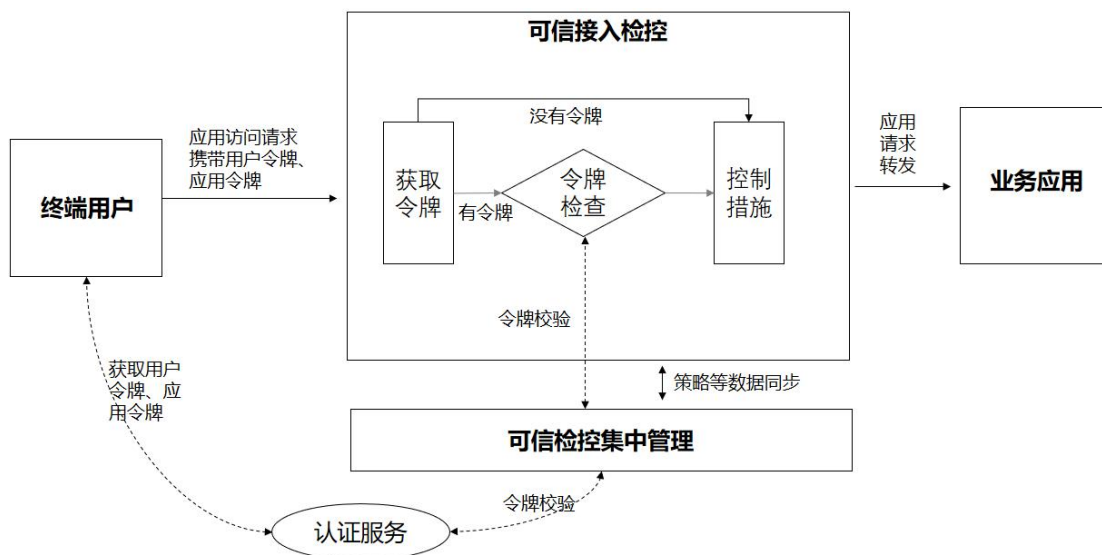
令牌检查与控制主要涉及以下服务：

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；

可信接入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。当用户访问请求经过可信接入检控时，可信接入检控会从请求 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，此时可信接入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，比如阻断访问。



2.4 终端身份检查与控制

2.4.1 功能描述

实现对接入终端的身份核验能力，通过调用环境感知服务的接口，向环境感知服务对终端身份进行校验并获取终端信任分，支持终端身份签名、格式、时间戳、唯一性的安全检查，按照制定的策略依据检查结果执行阻断或放行控制措施。

2.4.2 设计思路

在用户访问业务应用的过程中，应确保只有身份可信的用户终端，才能接入网络并能发起访问。不安全、不可信的用户终端，存在巨大安全隐患。因此，需要对终端的身份进行检查并根据策略实施控制措施。终端身份验证基于环境感知客户端进行采集并上报终端信息开展，在用户访问过程中，由可信接入检控通过调用环境感知服务验证终端身份接口，完成终端身份的验证，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

终端身份检查与控制主要涉及以下服务：

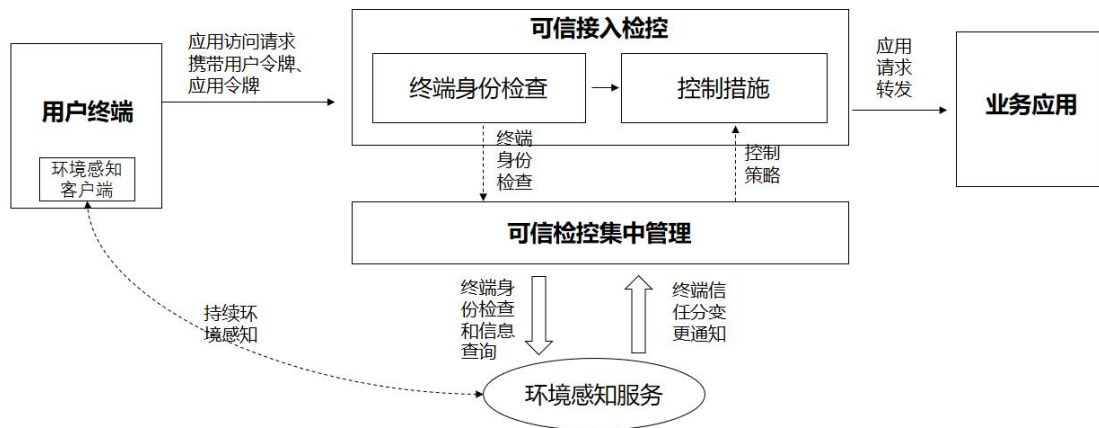
可信检控集中管理提供策略管理、环境感知服务对接能力，其与环境感知服务对接，与环境感知服务进行业务交互，完成终端身份的验证以及终端信息的查询；

可信接入检控通过可信检控集中管理，向环境感知服务进行终端身份的验证，并根据策略实施相应的控制措施。

环境感知服务通过部署在终端上的环境感知客户端采集终端信息，为终端设备分派唯一的设备 ID 作为设备标识，建立完整的终端信息库，提供终端身份验证和信息查询服务。

终端身份检查和控制分为终端身份检查、控制措施两个过程。当用户访问业务应用时，终端上的环境感知客户端会持续的感知和采集终端信息，上报给环境感知服务。当用户访问请求经过可信接入检控时，可信接入检控会从请求消息中提取被加密过的终端设备 ID，如果没有获取到终端设备 ID，则按照既定的策略执行相应的控制措施，比如阻断访问。如果提取到终端设备 ID，此时可信接入检控将通过可信检控集中管理，向环境感知服务传递终端设备 ID 查询并验证终端设备身份。如果验证通过之后，可信接入检控将根据既定的策略

进行请求转发，如果验证失败，可信接入检控将根据既定的策略实施控制措施，比如阻断访问。



2.5 用户访问权限检查与控制

2.5.1 功能描述

提供用户对应用访问权限检查能力，根据检查结果阻断或放行。

2.5.2 设计思路

在用户访问业务应用的过程中，应对用户的权限进行检查，确保只有拥有权限的用户才能进行访问，防止非授权的访问。当访问请求经过可信接入检控时，可信接入检控使用权限服务的提供的权限检查服务接口，完成用户权限的检测，并根据可信集中管理制定的策略实施相应的控制措施。

2.5.3 技术原理

用户访问权限检查与控制主要涉及以下服务：

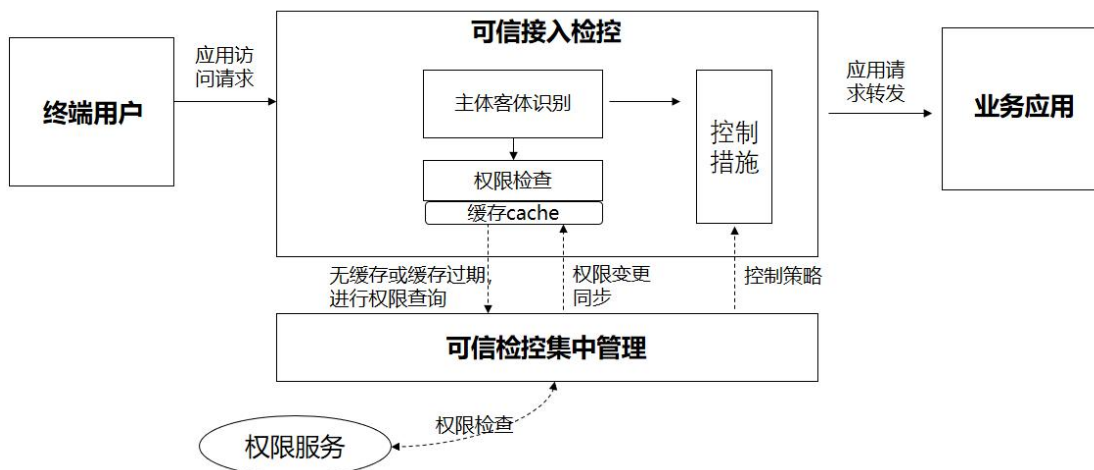
可信检控集中管理提供策略管理、权限服务对接能力，其与权限服务对接，调用权限服务接口，完成用户访问权限的检查。

可信接入检控通过可信检控集中管理，向权限服务进行用户权限检查，并根据策略实施相应的控制措施。

权限服务实现用户权限的管理，提供权限检查服务。

用户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。

当用户访问请求经过可信接入检控时，可信接入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，进行权限检查。当进入权限检查阶段时，可信接入检控首先从缓存 cache 中检索权限，如果没有权限或者缓存过期，则向可信接入检控集中管理发起权限检查请求，可信接入检控集中管理调用权限服务的接口，完成权限检查。如果检查通过之后，可信接入检控将根据既定的策略进行请求转发，如果检查不通过，可信接入检控将根据既定的策略实施控制措施，比如阻断访问。此外，为了提高可信接入检控的处理效率，可信接入检控采用了权限缓存 cache 机制，对用户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用户权限再次进行缓存，从而确保权限的一致性。



2.6 风险指令和控制

2.6.1 功能描述

接收策略控制服务的风险指令，并按照指令实施访问阻断的控制措施，提供用户访问日志，检控告警记录及上报功能。

2.6.2 设计思路

用户访问业务的过程，不仅需要确保终端身份、用户身份的可信，还需要根据用户访问业务应用的时间、空间等环境上下文信息，进行综合各类因素进行风险分析和信任评估，并

根据信任评估和指令，实施相应的措施控制，以此构建更加全面的安全访问控制机制，最大程度确保用户访问业务的安全。在用户访问业务的过程中，由策略控制服务进行持续的风险分析和信任评估，发现风险发送控制指令，最后由可信接入检控执行相应指令实施控制。

2.6.3 技术原理

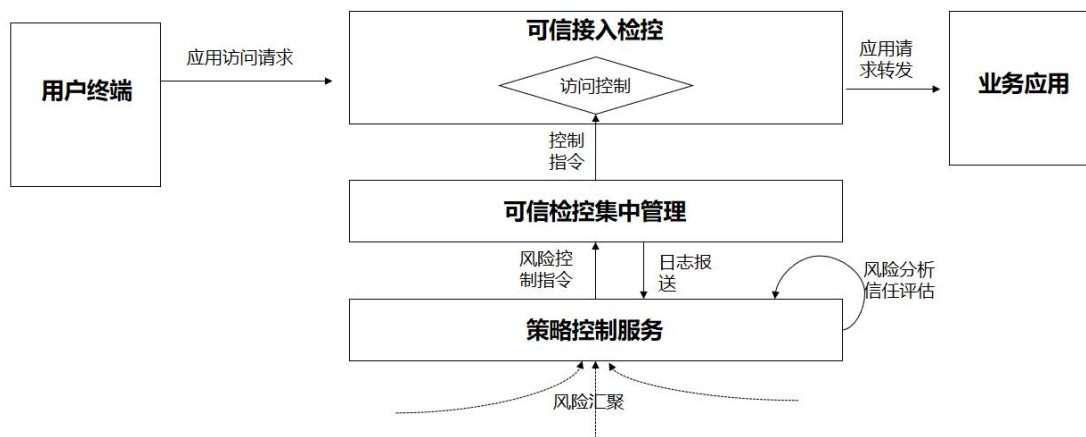
风险指令和控制主要涉及以下服务：

可信检控集中管理提供策略管理、策略控制服务对接能力，其与策略控制服务对接，向策略控制服务报送访问日志，接收策略控制服务的风险指令，并向可信接入检控发送指令控制措施。

可信接入检控接收可信检控集中管理的统一管理，根据可信检控集中管理发送的指令实施控制措施。

策略控制服务实现各类信息的收集以及风险的汇集和分析，对访问主体进行信任评估，并根据风险控制策略发送控制指令。

在用户访问业务应用的过程中，策略控制服务持续收集认证服务、权限服务等服务报告的风险信息，以及可信接入检控上报的日志信息，进行风险汇聚，基于汇聚各类数据，进行风险分析和对访问主体进行信任评估。当发现风险时，根据制定的风险控制策略，向可信检控集中管理发送相应的控制指令，比如阻断访问、锁定用户等指令。可信检控集中管理在收到指令之后，将向可信接入检控进行一步传递控制指令，可信接入检控将根据指令实施访问控制措施。



2.7 限流限速控制

2.7.1 功能描述

针对 Web 应用，可信接入检控能够支持对用户访问业务应用的限流限速，以防止访问请求流量过大，过度消耗业务应用资源，导致业务应用服务中断。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。

2.7.2 设计思路

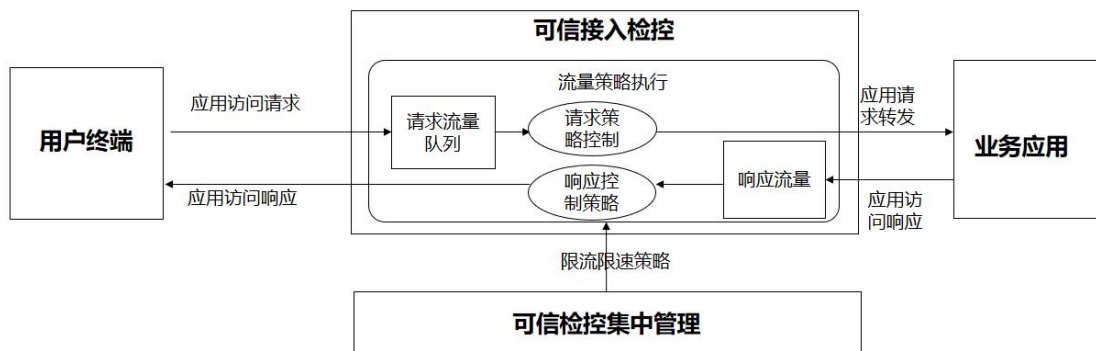
用户访问业务应用的过程中，针对网络流量发起攻击，导致业务应用系统无法正常提供服务是很常见的一类安全问题，比如拒绝服务攻击 DDoS 等。针对这类攻击，除了借助于第三方的网络安全设备或系统之外，可信接入检控也应该具备基本的防御能力，以便更好的保护业务应用系统。

可信接入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接入检控的控制范围之内，缓解恶意访问的网络流量攻击，保证业务的连续性。

2.7.3 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用户访问时，根据策略的执行相应的控制。

可信接入检控采用漏桶算法（Leaky Bucket）进行实现限流限速。也就是，当访问请求到达可信接入检控时，可信接入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，则丢弃请求向返回错误消息。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，从而保证应用请求都是几乎是匀速、平稳的转发到业务应用。相应的，业务应用的响应也类似处理，从而实现根据限流限速策略，响应能够匀速的转发给用户侧。



3 产品配置

(1) 硬件形态

可信接入检控硬件配置：

尺寸：2U 19 寸标准上架机箱
CPU：国产化 CPU 16c
内存：32GB
硬盘：4T 企业级 3.5 寸硬盘
网卡：4 个千兆电口，4 个万兆光口
电源：550W
接口：1 个管理口，1 个 USB 接口
新建连接数：国产化麒麟操作系统
最大并发连接数：国产化麒麟操作系统
用户并发数：≥5000
吞吐：≥20G
操作系统：国产化麒麟操作系统

(2) 软件形态

可信接入检控软件配置：

CPU：要求提供国产化 CPU 16C 以上
内存 32 及以上
硬盘：4TB 及以上
操作系统：国产化麒麟操作系统