零信任产业标准工作组

中国产业互联网发展联盟
Internet+ Development Association of China
IDAC

# 零信任接口应用白皮书（2021）

## --互联互通打造开放生态

零信任产业标准工作组
2021年8月

# 编制组

- 编制单位：

- 编制人员：蔡东赟、王旭、黄超、刘海涛、茆正华、李海宁、焦靖伟、陈妍、龙凡、仇瑞晋、蔡晓萍、王冠楠、杨仕忠、宋磊、李俊、王沐、何艺、赵菁菁、郑强、张楚楚、李程、熊瑛、黄铭恺、徐吉、王德威、石善忠（排名不分先后）

- 版权声明：

落地零信任架构，需要有体系化的思维方式、持续完善的推进策略、客户与厂商的紧密配合，以及产业界的技术协同。不同安全组件/模块间的互联互通是最基础性的工作之一，希望本白皮书的发布为业界带来更多思考和合作的机会。

—— 零信任产业标准工作组秘书长 黄超

零信任接口应用是实现安全行业在零信任安全领域产品合作以及价值共建的基础，接口白皮书的发布为打造行业的合作生态提供了标准指南，期待在白皮书的指导下，各安全厂商携手以零信任构建信任。

—— 腾讯安全总经理 王宇

零信任接口白皮书结合腾讯内网与多家厂商的落地实践经验，形成一致的接口应用共识，奠定零信任体系下安全产品互联互通的基础，有利于促进国内零信任产业的健康发展。

——腾讯企业安全中心高级总监 蔡晨

有幸和零信任工作组一起参与了系列标准的编制，见证了零信任产业的发展，也希望随着接口白皮书的发布，让安全不再孤立，形成更紧密的合作为客户保驾护航。

—— 持安科技有限公司创始人兼CEO 何艺

零信任接口白皮书的发布，是一件值得高兴的事情。这是各厂商合作的开始，零信任产业良好的合作生态的基础。

—— 上海派拉软件股份有限公司CEO 谭翔

恭祝零信任接口白皮书的发布。这对于各厂商在安全领域的合作协同，推进行业技术合规、全球化，促进中国安全产业健康发展，加快零信任技术和服务快速发展有深远意义。

—— e签宝创始人兼CEO 金宏洲

零信任接口白皮书的发布，让复杂的零信任安全架构与价值得以明晰，零信任安全产业生态也在初步形成。一知安全希望发挥自身在数据隔离和攻击检测方面的技术优势，携手共建“零信任”产业生态，构筑“自由连接，安全使用”的可信网络空间。

—— 一知安全创始人兼CEO 宋磊

零信任接口应用白皮书是安全厂商协同合作和企业快速部署零信任架构的行动指南。

—— 北京栖安科技有限责任公司CEO 杨仕忠

零信任白皮书的发布，有助于让更多的人对零信任建立信任，建立零信任的标准体系和产品生态，让网络充满信任。

—— 格尔软件股份有限公司常务副总 朱斌

# 1、零信任接口需求-打造开放生态

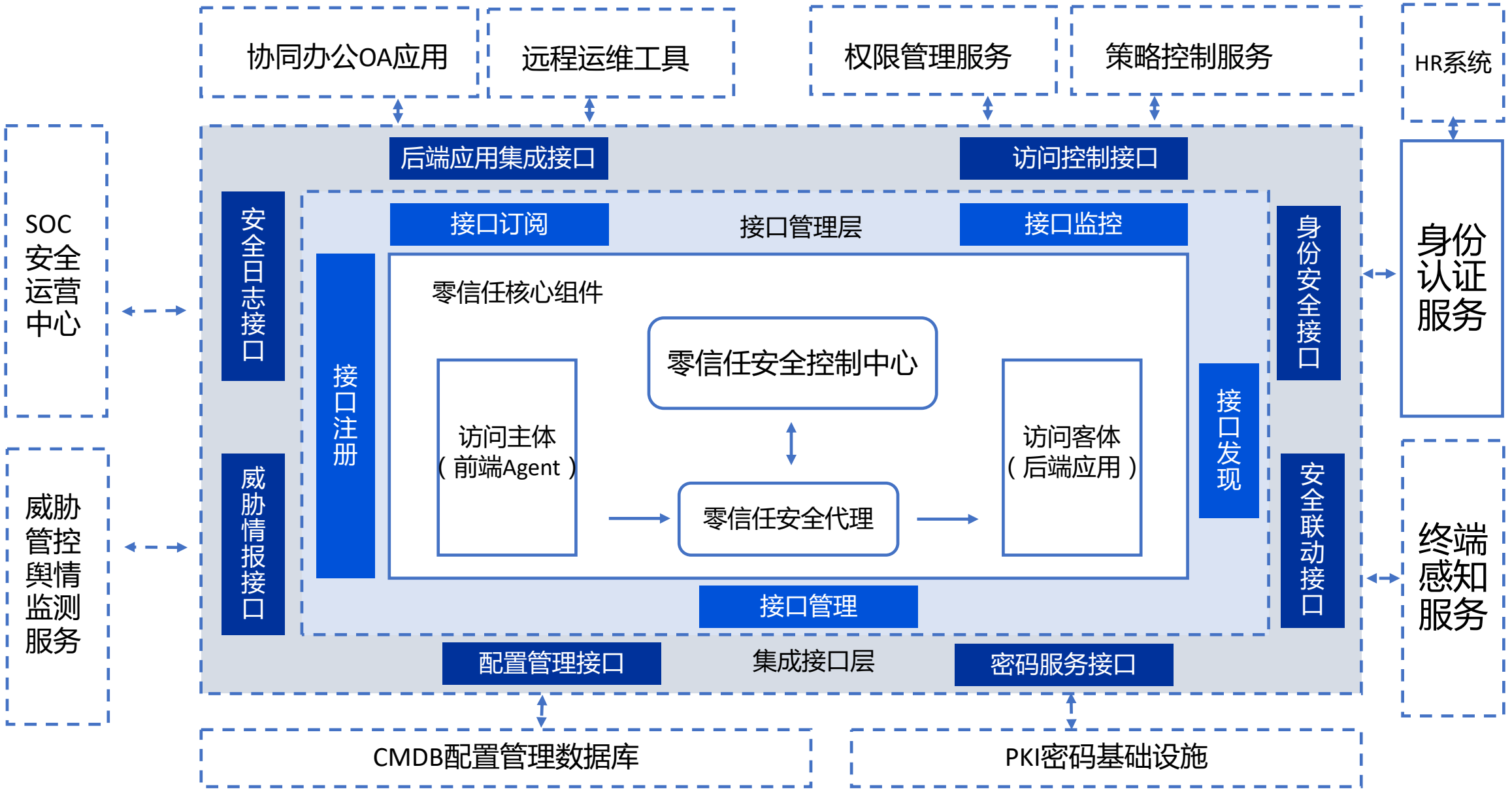
- 众所周知，零信任是一种适应于数字化时代的新的安全理念，其对安全体系的影响涉及到方方面面，这也是造成当前市场上零信任产品、服务、组件百家齐放、五花八门的主要原因。零信任产业发展到今天，对产品需满足功能和性能的认识已经趋于一致，零信任系统的模块架构和模块之间的互联互通就成为要解决的一个关键问题，这个问题的解决可以为不同厂商的产品开发定位提供参考，也为客户选择提供依据，从而促使行业发展更有序。

- 从客户角度，大中型机构（员工人数多、设备数量多、分支机构多）是国内零信任安全的主要需求方和实施先行者，其安全建设一般已有多年积累，在进行零信任改造时，对于如何与企业现有安全架构、安全产品/设备结合，充分利旧，具有强烈的诉求。小微企业，对于理解零信任理念、调用零信任相关接口服务也存在普遍需要。

- 从安全厂商角度，如何明确自身的零信任产品在市场的定位，如何与其他零信任厂商协同、协作，建立强有力的技术门槛和竞争力，面向多行业的潜在客户群，一起扩大市场份额，是业务快速发展的当务之急。

- 白皮书为零信任安全需求方（客户）、厂商和所有从业者，提供了全面的零信任系统服务接口需求、层次划分、接口标准描述和接口应用场景的介绍，为国内零信任产业协同、开放生态的发展贡献力量。

# 2、零信任接口全景图


协同办公OA应用
远程运维工具
权限管理服务
策略控制服务
HR系统
SOC
安全
运营
中心
后端应用集成接口
访问控制接口
安全日志接口
接口订阅
接口管理层
接口监控
身份安全接口
身份
认证
服务
零信任核心组件
接口注册
零信任安全控制中心
访问主体
（前端Agent）
访问客体
（后端应用）
接口发现
威胁
管控
舆情
监测
服务
威胁情报接口
零信任安全代理
安全联动接口
终端
感知
服务
接口管理
配置管理接口
集成接口层
密码服务接口
CMDB配置管理数据库
PKI密码基础设施

# 3、接口分类说明

接口管理层：
负责零信任相关接口的注册、发现、治理、调用鉴权、容错、隔离等能力，实现对接口的全面管理支撑能力。

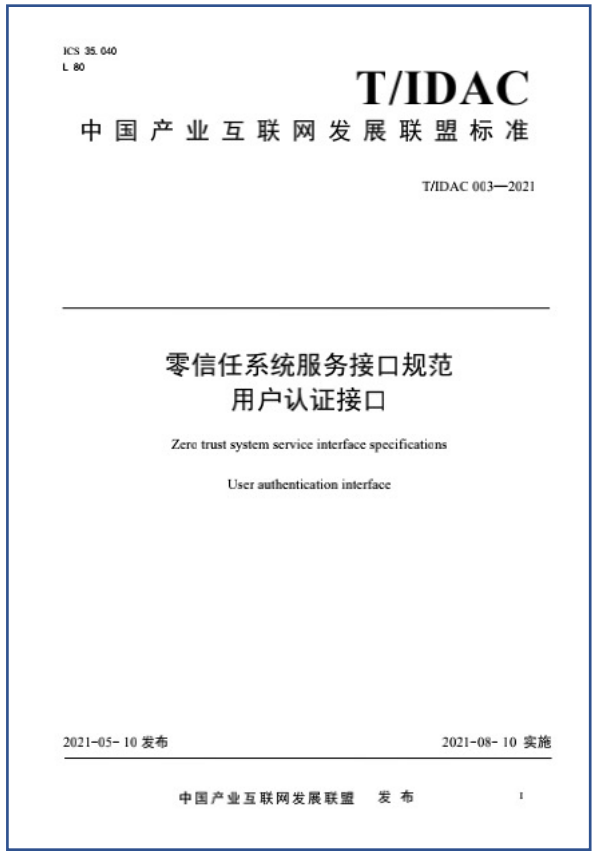
集成接口层：
具体支持零信任核心组件与支撑组件、第三方安全产品/组件的集成开发对接，从而整体上提供完整的零信任安全能力。

本白皮书详细描述了6类接口：
身份安全接口、威胁情报接口、配置管理接口、密码服务接口、访问控制接口和安全联动接口。

# 4、身份安全接口-概述

接口列表：

- 身份数据同步接口：通过该接口将用户身份及组织架构等数据从IAM组件同步至零信任系统。
- 身份认证接口：零信任系统通过该接口对接IAM组件实现对用户登录认证。
- 单点登录接口：通过该接口实现零信任系统各个组件之间以及业务系统之间的单点登录能力。



ICS 35.040
L 80

T/IDAC

中国产业互联网发展联盟标准

T/IDAC 003—2021

零信任系统服务接口规范
用户认证接口

Zero trust system service interface specifications

User authentication interface

2021-05-10 发布　　2021-08-10 实施

中国产业互联网发展联盟　发布

# 4.1、身份安全接口-身份数据同步接口

业务场景：

零信任需要对访问主体（人、设备、服务等）进行持续的身份鉴别。因此需要维护访问主体的身份相关信息，而这些信息一般是通过IAM身份安全组件维护，在零信任执行身份认证前，需要通过该接口将用户身份数据从IAM组件同步至其他零信任系统。

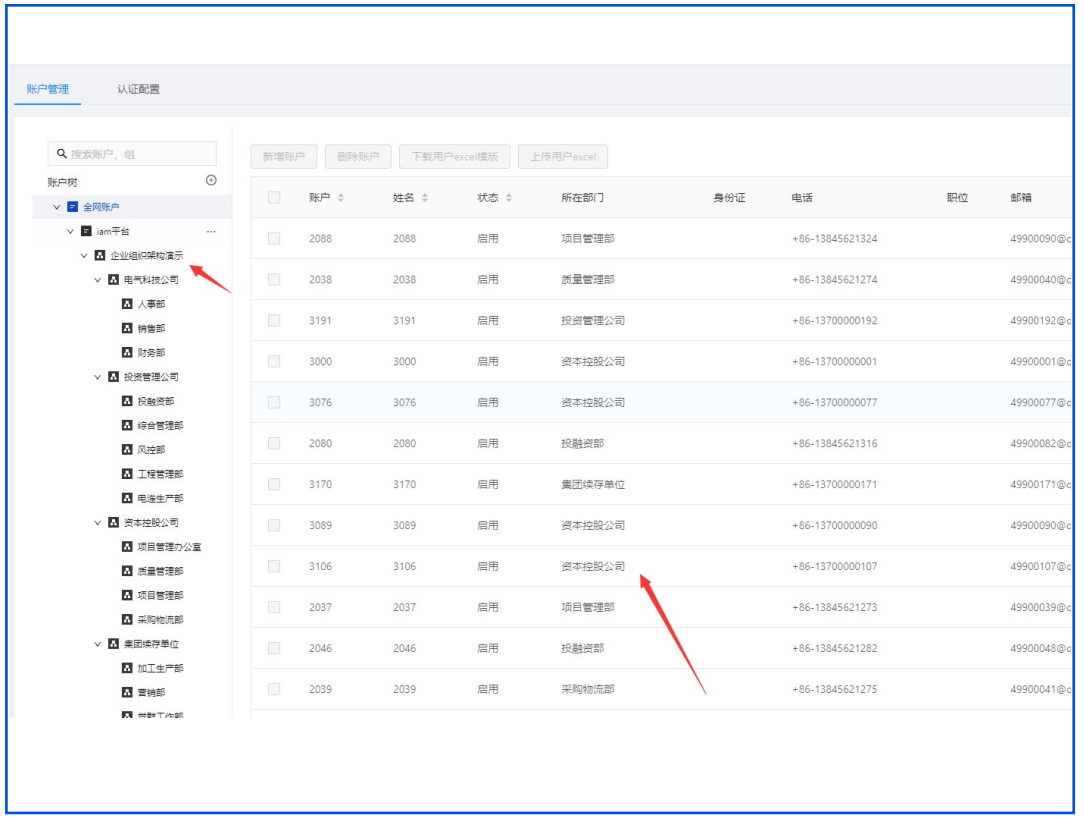
接口详情：

关键协议：SCIM协议或LDAP协议接口

关键字段：用户ID，用户名称、用户所属组织机构用户所属（虚拟）组。

成功案例：

腾讯iOA和腾讯IAM对接，实现将来自于企业不同数据源的数据，包括组织架构、用户组以及用户数据同步至iOA。



# 4.2、身份安全接口-身份认证接口

业务场景：

零信任架构要求对于主体（人、设备、服务等）的访问请求，要先进行认证后连接；因此需要提供统一标准的身份认证接口，用于对访问主体的身份进行认证 ；对人的认证一般通过出示账号密码进行认证，对设备和服务的认证一般通过出示密钥或证书进行认证；并且给主体颁发身份票据，在不同业务接口对接时通过身份票据来确定主体身份。

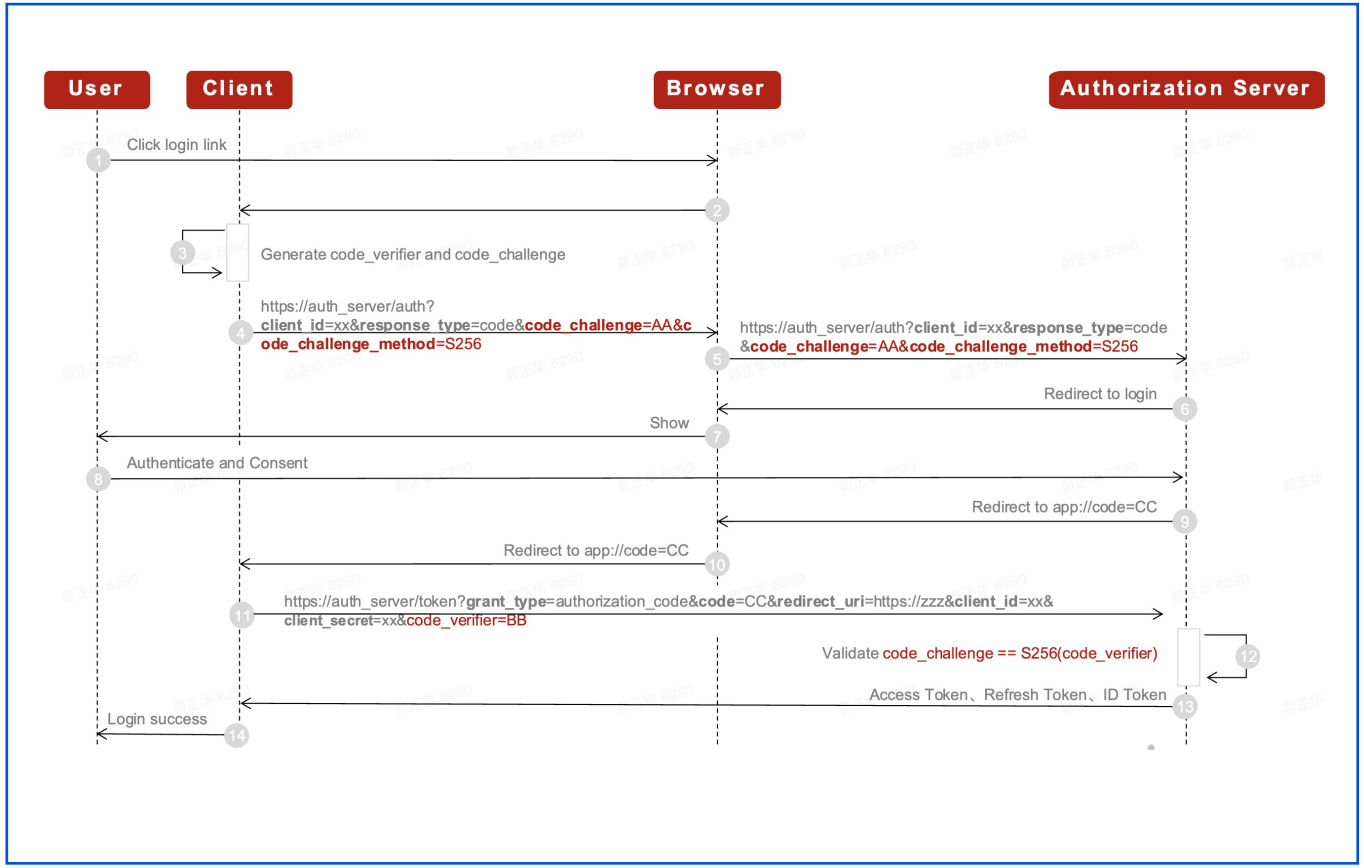
接口详情：

关键协议：OAuth/OIDC协议接口。

关键字段：用户名、密码、client_id、client_secret、access_token、refresh_token、id_token

成功案例：

- 温州市大数据发展管理局零信任安全项目中通过安恒信息提供的OAuth2.0、OIDC协议接口实现对各委办单位用户、应用系统的统一身份认证，并以零信任体系颁发的票据作为凭证，在公共数据共享平台的服务调用流程中证明主体身份。
- 派拉软件零信任产品与派拉身份管理产品通过OIDC协议接口对接。



# 4.3、身份安全接口- 单点登录/登出接口

业务场景：

零信任系统各个组件之间以及业务系统之间的单点登录/登出。

- 单点登录：用户访问组件或业务系统时，在未完成认证的情况下，都被强制到IAM上完成认证。用户在IAM完成认证后，访问任意有权限的组件或业务系统时，都无需重复进行认证（因安全需求要求二次认证的除外）。

- 单点登出：用户在任一组件或业务系统执行注销操作时，即注销所有已经处于登录状态的组件或系统。单点注销完成后，在组件或业务系统上操作受登录保护的资源时，将被要求重新进行登录。

接口详情：

关键协议：**OIDC、SAML、CAS** 协议接口。

关键字段：用户ID、用户姓名

成功案例：

格尔软件航空工业商网零信任安全中的统一认证，实现在办公，党建，教育培训，业务协同等场景下各个业务应用间实现单点登录/登出，满足日活超$10^{}$万用户的远程办公，移动办公，业务协同等工作的单点登录/登出需求。

腾讯ioa与腾讯iam产品对接，完成腾讯内部在办公，运维，研发，业务协同等场景下各个业务系统之间实现单点登录/登出，满足全部员工的远程办公，移动办公，业务协同等工作的的单点登录和登出需求。

# 4.4、身份安全接口- 单点登录(应用接入IAM)

业务场景：

多个业务系统通过IAM实现单点登录，因此业务系统需要根据合适的方式接入IAM。
接入方式可以为标准协议，例如OAuth2、SAML、CAS等，也可以为自定义的接入方式。
自定义接入方式以腾讯企业邮为例，需要先调用企业邮接口，获取登录企业邮的url，再通过访问该url进而登入企业邮。

接口详情：

关键协议：OAuth2、SAML、CAS 协议接口。
关键字段：用户ID、access_token等。

成功案例：

腾讯企业邮箱自定义接入方式，IAM根据该种方实现腾讯企业邮箱单点登录功能。

# 5、 威胁情报接口

业务场景：

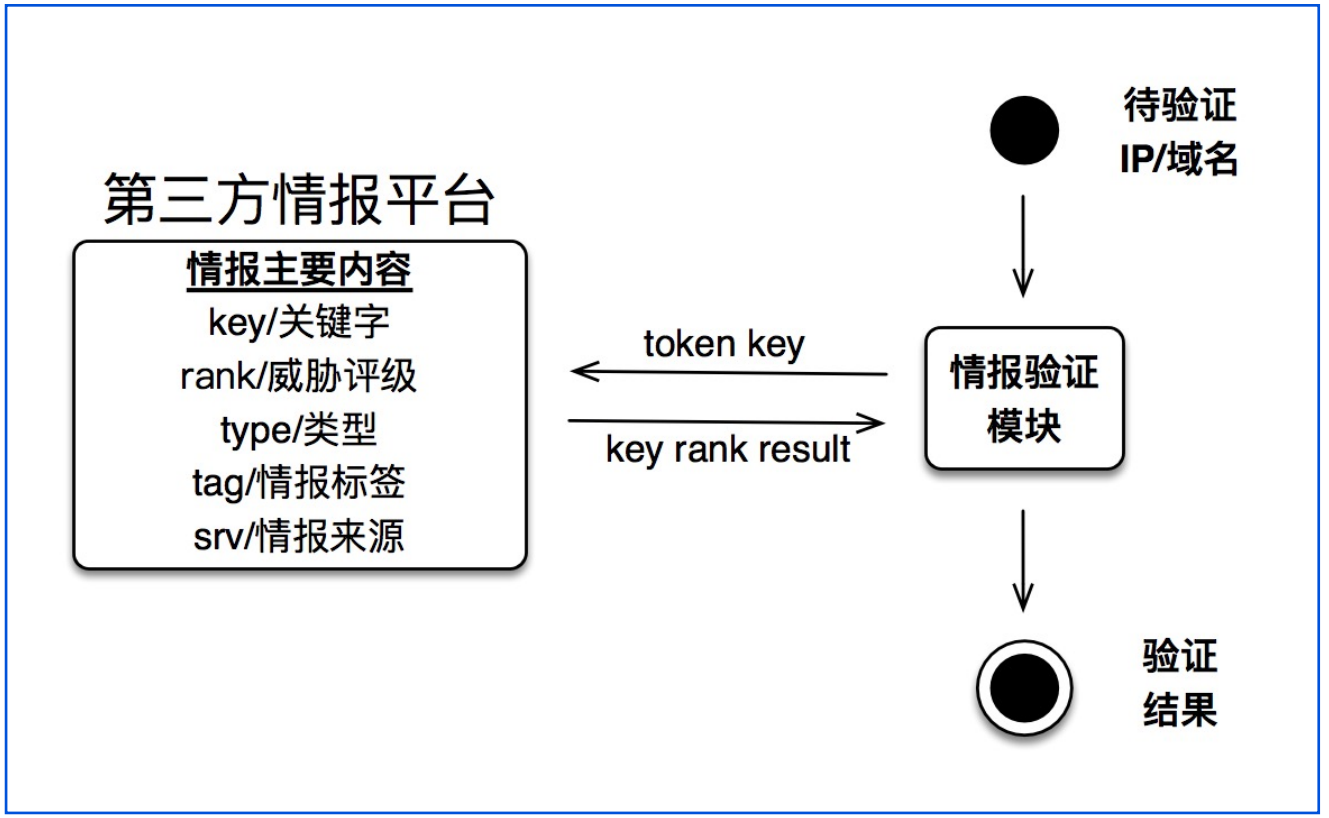
在零信任安全场景下，通过威胁情报对访问来源及外联目标进行辨别，再结合访问控制机制，建立起一道风险保护屏障。
依据服务敏感程度，对访问来源IP进行情报验证，根据结果响应或拒绝来自高风险IP的后续鉴权及通讯过程。
依据资产角色属性，对外联目标IP及域名进行情报验证，根据结果执行或放弃到主控类目标IP/域名的访问请求。

接口详情：

- 通讯协议：restful API
- 关键参数：token,key(ip/domain/url/hash/email), sdate(op),src(op),tag(op)
- 关键字段：key,type,rank,result[src,tag,time,desc,ext]

成功案例：

国家互联网应急中心网络安全威胁情报多源检索平台深圳市信息安全测评中心威胁情报融合联动共享平台均使用该接口进行威胁情报数据的分发与共享。



# 6、 配置管理接口-工作负载数据同步接口



接口概述：

CMDB是一个逻辑数据库，包含了配置项全生命周期的信息以及配置项之间的关系(包括物理关 系、实时通信关系、非实时通信关系和依赖关系)。零信任体系与CMDB的接口，主要用于工作负载相关信息的同步，以便于管理者基于其业务属性制定零信任访控策略。

业务场景：

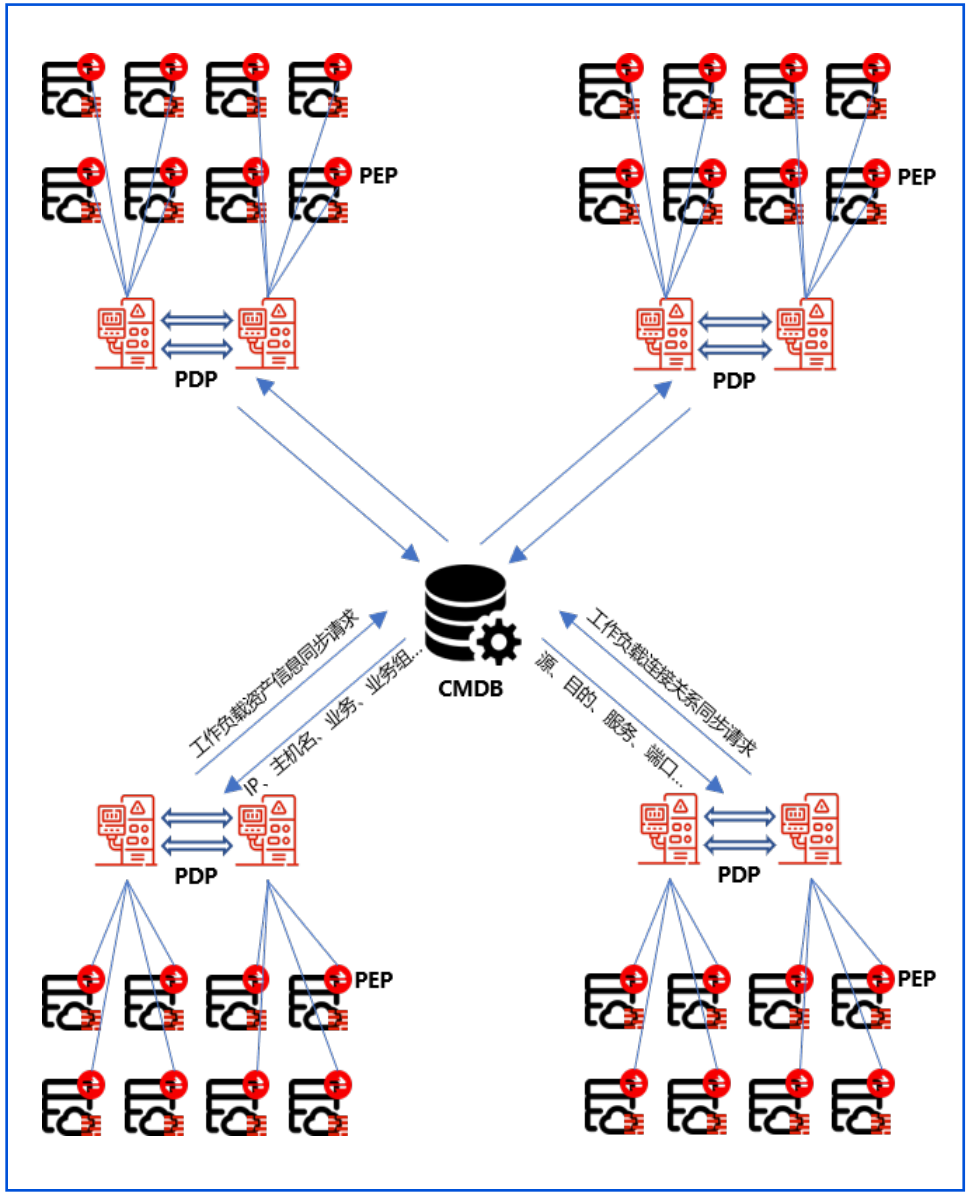
在进行云化数据中心内工作负载间流量（东西向）控制时，需以工作负载的业务角色作为访控条件，工作负载的业务角色则基于其多维属性标定。在工作负载数量规模庞大、类型繁多的场景下，零信任“策略决策点”由用户已有的CMDB系统获取必要信息，可大幅提升数据中心零信任方案部署效率、降低落地难度，同时可有效保障云内工作负载资产属性与零信任防控体系的业务一致性。

接口详情：

- 关键协议：Restful API
- 关键字段：
  - 类型一：工作负载资产信息（主机名、IP、业务应用、所属业务组）
  - 类型二：工作负载访问关系（源业务类型、目的业务类型、服务、端口）

成功案例：

某大型互联网金融企业数据中心已部署虚机、容器等工作负载近2万个，在其进行微隔离防护建设过程中，蔷薇灵动蜂巢自适应微隔离安全平台通过用户自研CMDB系统提供的API接口，调用系统中工作负载资产及访问关系等信息，实现了安全策略的准自动化部署。



# 7、密码服务接口概述

接口列表：

- 证书接口类：通过该接口提供体系内人、事、物各类主体数字证书的相关服务
- 密码服务接口类：通过该接口为体系内各类应用提供基础密码服务

# 7.1、密码服务接口-证书接口（证书生命周期管理）

业务场景：

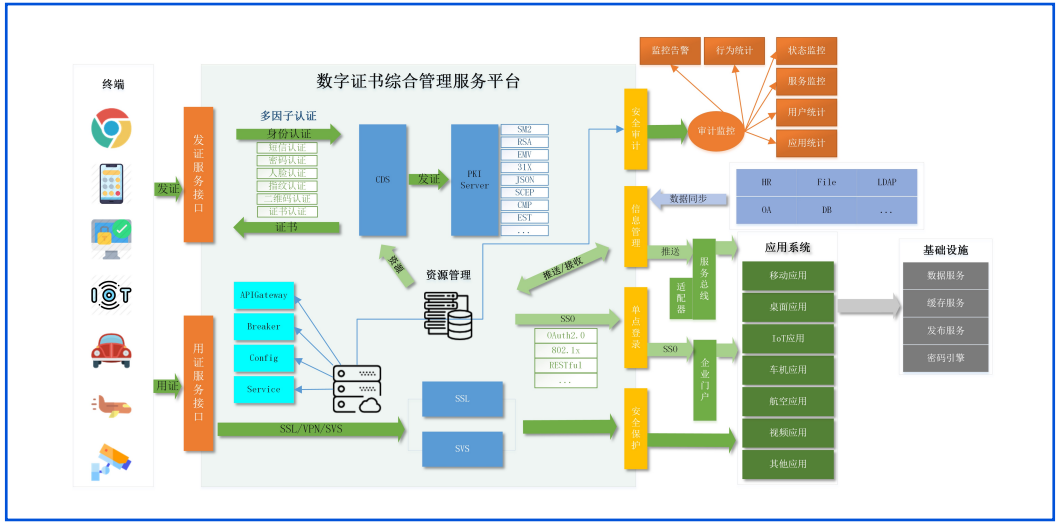
对访问零信任体系的主体（人、终端设备等）颁发数字证书用于加固通信链路、保障数据的机密性、完整性及不可抵赖性。

接口详情：

- 参照标准：GM/T 0014-2012_数字证书认证系统密码协议规范
- 关键字段：主体名、主体组织机构、主体身份信息、有效期、证书类型等。

成功案例：

格尔软件航空工业商网零信任安全中的身份认证体系。



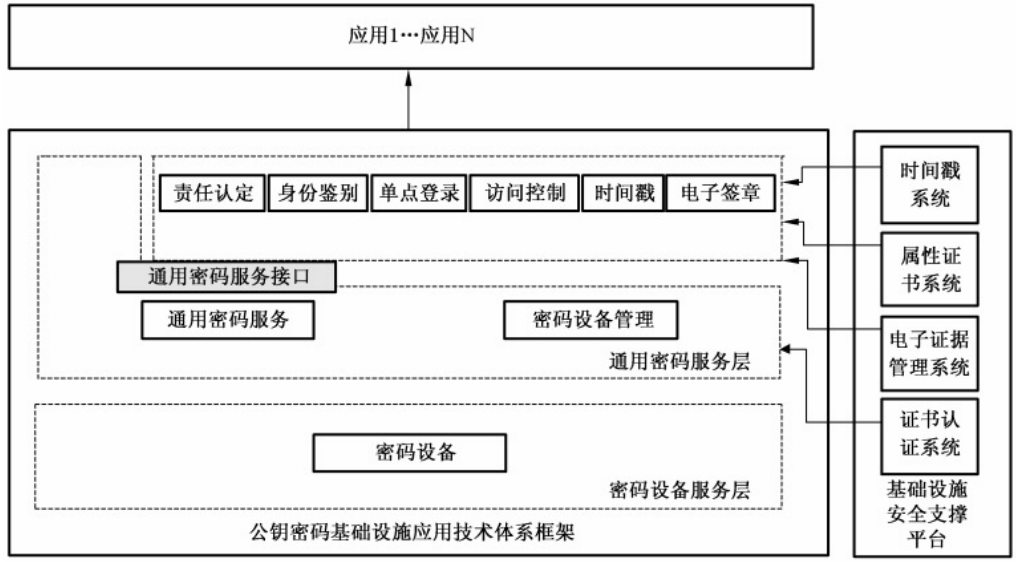
# 7.2、密码服务接口-证书接口（证书应用）

应用描述：

证书应用接口适用于零信任体系中的需要使用证书进行密码应用的服务，接口包含数字签名、数据加解密、文件加解密、签名数据的验证、解析等

接口详情：

- 参照标准：
- GM/T 0019-2012 通用密码服务接口规范；
- GM/T 0020-2012 证书应用综合服务接口规范；
- 关键字段：明文值、密文值、秘钥、签名值、时间等



应用描述：
密码服务接口为零信任体系中提供基础密码服务，包含数据加密保护、协同密钥服务、密钥管理、密钥运算、随机数等

接口详情： 进行对称运算

- 参照标准
- GM/T 0019-2012 通用密码服务接口规范
- GM/T 0088-2020 云服务器密码机管理接口规范

应用描述：
调用服务器密码机/云服务器密码机/密码服务平台提供的基础密码服务时，进行打开设备、建立会话等设备管理操作

接口描述： 进行密码服务设备操作

- ✓ 打开设备：SDF_OpenDevice
- ✓ 关闭设备：SDF_CloseDevice
- ✓ 创建会话：SDF_OpenSession
- ✓ 关闭会话：SDF_CloseSession
- ✓ 获取设备信息：SDF_GetDeviceInfo
- ✓ 产生随机数：SDF_GenerateRandom
- ✓ 获取私钥使用权限：SDF_GetPrivateKeyAccessRight
- ✓ 释放私钥使用权限：SDF_ReleasePrivateKeyAccessRight

应用描述：
调用服务器密码机/云服务器密码机/密码服务平台进行密钥生成、输出、导入、销毁等密钥管理操作

接口描述： 进行密钥管理操作

- ✓ 导出ECC 签名公钥：SDF_ExportSignPublicKey_ECC
- ✓ 导出ECC 加密公钥：SDF_ExportEncPublicKey_ECC
- ✓ 产生ECC 非对称密钥对并输出：SDF_GenerateKeyPair_ECC
- ✓ 生成会话密钥并用内部ECC公钥加密输出：SDF_GenerateKeyWithIPK_ECC
- ✓ 生成会话密钥并用外部ECC公钥加密输出：SDF_GenerateKeyWithEPK_ECC
- ✓ 导入会话密钥并用内部ECC私钥解密：SDF_ImportKeyWithISK_ECC
- ✓ 生成密钥协商参数并输出：SDF_GenerateAgreementDataWithECC
- ✓ 计算会话密钥：SDF_GenerateKeyWithECC
- ✓ 产生协商数据并计算会话密钥：SDF_GenerateAgreementDataAndKeyWithECC
- ✓ 基于ECC算法的数字信封转换：SDF_ExchangeDigitEnvelopeBaseOnECC
- ✓ 生成会话密钥并用密钥加密密钥加密输出：SDF_GenerateKeyWithKEK
- ✓ 导入会话密钥并用密钥加密密钥解密：SDF_ImportKeyWithKEK
- ✓ 导入明文会话密钥：SDF_ImportKey
- ✓ 销毁会话密钥：SDF_DestroyKey

应用描述：
调用服务器密码机/云服务器密码机/密码服务平台进行非对称算法运算操作

接口描述： 进行非对称运算

- ✓ 外部密钥ECC签名：SDF_ExternalSign_ECC
- ✓ 外部密钥ECC验证：SDF_ExternalVerify_ECC
- ✓ 内部密钥ECC签名：SDF_InternalSign_ECC
- ✓ 内部密钥ECC验证：SDF_InternalVerify_ECC
- ✓ 外部密钥ECC加密：SDF_ExternalEncrypt_ECC
- ✓ 外部密钥ECC解密：SDF_ExternalDecrypt_ECC

应用描述：
调用服务器密码机/云服务器密码机/密码服务平台进行对称算法运算操作

接口描述： 进行对称运算

- ✓ 对称加密：SDF_Encrypt
- ✓ 对称解密：SDF_Decrypt
- ✓ 计算MAC：SDF_CalculateMAC

应用描述：
调用服务器密码机/云服务器密码机/密码服务平台进行杂凑运算操作

接口描述： 进行杂凑运算

- ✓ 杂凑运算初始化：SDF_HashInit
- ✓ 多包杂凑运算：SDF_HashUpdate
- ✓ 杂凑运算结束：SDF_HashFinal

应用描述：
调用服务器密码机/云服务器密码机/密码服务平台进行文件操作

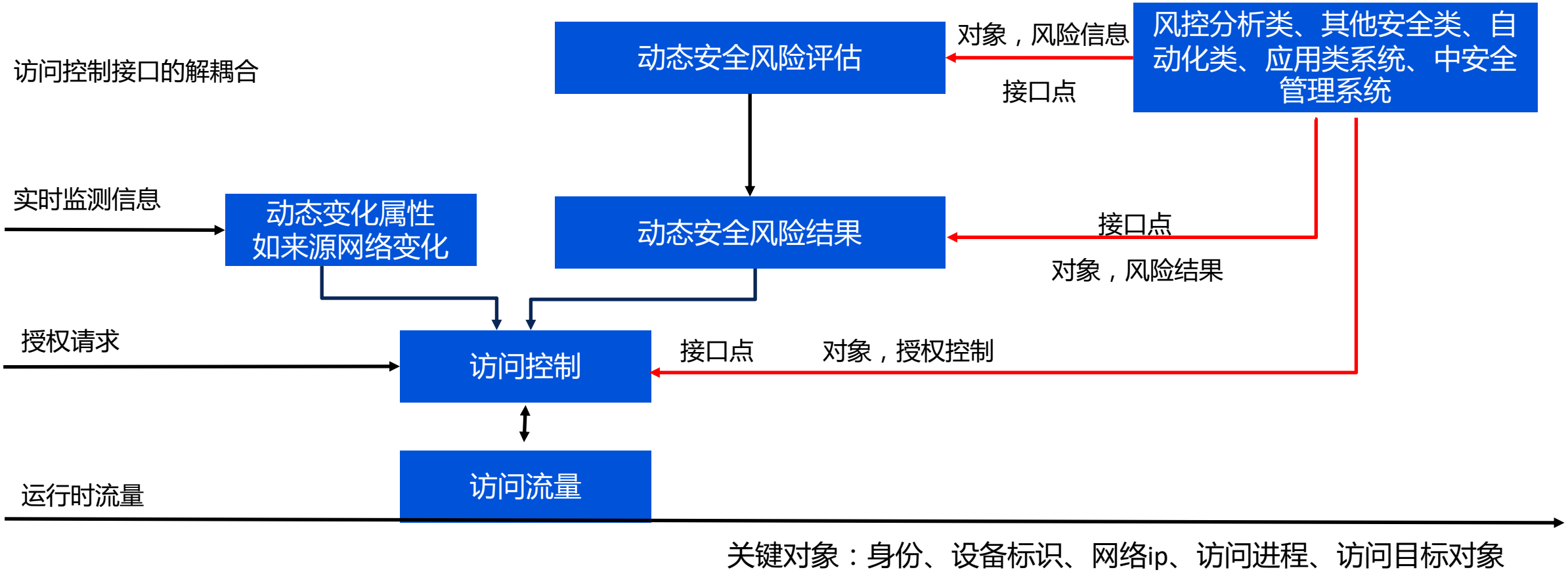
接口描述： 进行文件操作

- ✓ 创建文件：SDF_CreateFile
- ✓ 读取文件：SDF_ReadFile
- ✓ 写文件：SDF_WriteFile
- ✓ 删除文件：SDF_DeleteFile

# 8、 访问控制接口-整体

关键业务接口点

访问控制接口的解耦合




关键对象：身份、 设备标识、网络ip、访问进程、访问目标对象

# 8.1、 访问控制接口-访问和授权控制接口

业务场景：

零信任安全网关完全代理了主体访问客体的数据流量，通过访问和授权控制接口对主体的访问请求放行或阻止需要进行判断； 常见如人员离职，检测到高风险的人、异常地点、异常设备、异常应用程序等，都要及时的阻断主体访问行为，此时接收控制信息的接口提供给外部应用如HR人员管理系统，IAM风控、SOC风控等一些其他安全自动化系统，紧急联动调用阻断对应的身份访问、应用进程访问。

接口描述：

安全控制接口策略参数：身份信息，访问主体的信息（终端类型，终端IP、终端MAC、终端证书、终端设备指纹），访问客体的信息（应用、接口、数据、IP、MAC），访问行为的上下文信息（时间、地点、User-Agent）安全控制接口控制参数：放行/阻止, 风险提示信息。

成功案例：

1、派拉零信任身份管理服务中人员入职、离职、禁用等，触发调用访问控制类系统对指定身份进行基础授权或者吊销权限。

2、派拉零信任风险检测系统通知访问控制系统：检测出指定设备风险，通过工单之类自动化处理系统，调用访问控制接口， 阻断对应设备的服务资源访问，减少企业风险。

3、某大型物流行业腾讯iOA用业务权限审核对接零信任访问权限管理，通过业务权限的申请调用零信任的设置权限，在通道侧阻断对应的资源访问，减少企业风险。

# 8.2、 风险信息联动-SOC、 UEBA、 SIEM、 EDR、 IAM Risk

业务场景：

- 接收来自各类安全分析平台的风险决策数据，将风险信息输入到决策引擎,提供给决策授权进行判断和处理，接收的风险数据可以是经安全分析平台处理判断后的有明确风险等级的数据，也可以是原始数据用于决策引擎二次判断决策，或是作为多决策数据源进行处理。
- 例如通过SOC、UEBA、SIEM、XDR等系统，将输入的各类数据进行综合评估判断后，如异常用户访问行为、失陷IP、关联告警等，将处理结果通过接口允许零信任系统调取，参与到处理判断，抑或是零信任系统需要借助更多的数据维度进行分析时，可以通过接口来获取相应数据，最后根据分析结果，做访问控制系统的配置做丰富的响应（阻断、身份挑战、放行之类）。

接口描述：

风险决策信息接口-关键参数：数据类型（决策数据/原始数据）、风险类型、风险等级、风险描述、目标对象（IP、账号、设备、域名）、原始数据。

成功案例（应用案例）：

天融信零信任身份服务系统与零信任环境感知系统对接。
持安科技零信任系统与完美世界SOC对接。
腾讯iOA与腾讯内网SOC完成对接，实现环境感知数据上报；联动处置等能力。

# 8.3、 传数据给-SOC、 UEBA、 IAM Risk进行分析

业务场景：

将零信任记录的原始信息，如账号登录、用户权限、访问行为、终端数据等数据发送给安全分析类系统，用于安全事件分析，用户行为分析，风控等场景，增强统一事件处理能力，再结合访问控制接口，使得如SOC、SIEM类产品可以通过接口来关联回调拦截操作，闭环安全事件从数据采集、到分析和处理的闭环。

接口描述：

账号登录-关键参数：零信任设备IP、日志类型、账号、来源IP、来源设备、登录方式、登陆状态。
用户权限-关键参数：零信任设备IP、日志类型、账号、应用权限、操作方式（启动/禁用）、操作人。
访问记录-关键参数：零信任设备IP、日志类型、账号、来源IP、来源设备、目标IP、目标端口、目标域名、目标URI、状态终端状态-关键参数：零信任设备IP、日志类型、设备ID、关联账号、终端状态、终端授权时间。

成功案例：

持安科技和Elastic、Splunk、完美世界的SOC等系统对接。

# 9、 安全联动接口

业务场景：

在安装零信任终端的用户设备上，会同时安装各种安全软件，如防病毒软件、安全防护类、防火墙软件等等，这些软件可以检测用户设备的安全状态。零信任终端可以通过接收这些安全软件的信息，对运行的环境进行安全评估，保障零信任安全。

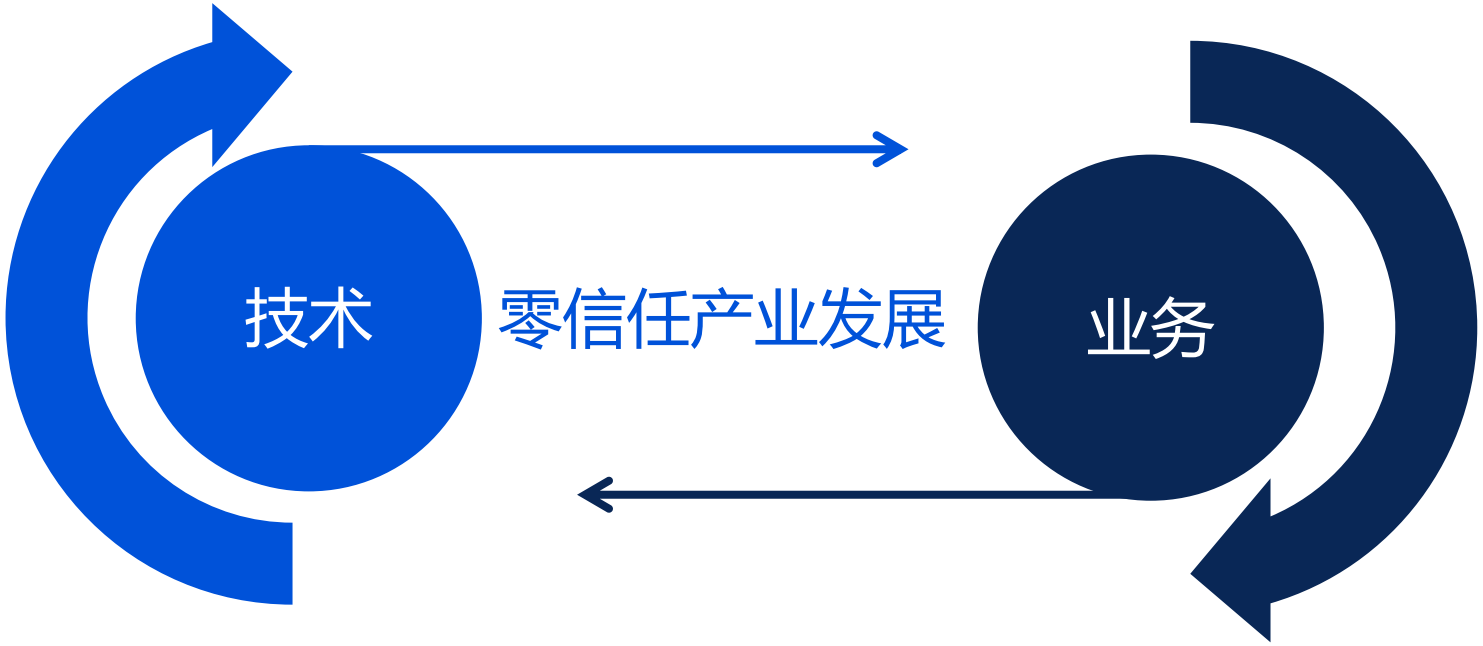
接口描述：

输入评估参数：设备对象、安全类型（病毒、某种安全基线状态、漏洞风险状态、风险软件状态、高危服务状态等）、安全状态(等级或者分数)、其他描述。

作用：当任意安全状态变化时候，输入访问控制更新，提供给访问做决策控制，尽量标准化安全状态，方便做不同的设备风险做统一访问控制决策判断。

成功案例：

某防病毒软件检测当前系统存在安全风险，将该信息上报到零信任终端，零信任终端终止当前的运行，并提示用户解决该风险。



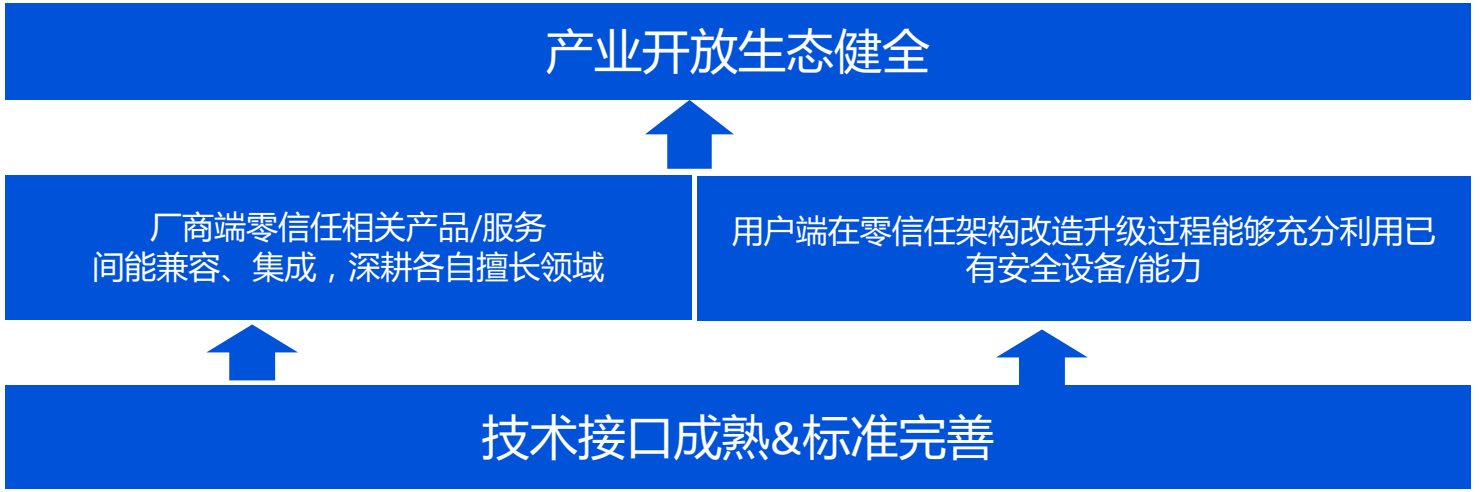

经过十多年的技术发展，以及疫情远程安全办公应用需求的催化，零信任已从概念走向落地实施，零信任的未来发展不完全是技术或产品层面的问题，它同时跟企业的经营、规划、长期发展的管理强相关，并且是一个持续优化的过程。技术与业务需求将双轮驱动零信任产品的未来发展，制定汇聚产业共识的标准规范将能更好的促进产业协同发展。

# 11、零信任发展趋势-开放生态是未来

- 当前零信任已在厂商端被广泛拥抱、相关产品和服务不断推出，在用户端被积极实践、政府和行业应用案例不断丰富。我们预判，零信任将在政策指引下和产业开放协作中走向未来

- 政策方面，我们已经看到国内外政府部门已经陆续出台鼓励发展零信任相关技术和产业的政策文件

- 产业开放协作方面，关键要看产业生态的建立健全。可用于集成、兼容的技术接口的成熟度以及接口标准的完善是零信任开放生态快速健全的基础




## 国内

- 2019年9月，工业和信息化部会同有关部门，为贯彻落实《中华人民共和国网络安全法》，积极发展网络安全产业，发布《关于促进网络安全产业发展的指导意见(征求意见稿)》
- 2021年7月12日，工信部发布《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》均提出要加快发展零信任相关技术和产业

## 国外

- 2019年7月，美国国防部发布2019-2023年《数字现代化战略》
- 2021年4月，美国国防部代理首席信息官（CIO）谢尔曼（John Sherman）宣布：美国国防部计划发布2021年零信任架构战略（zero-trust architecture strategy 2021）
- 2021年5月，美国总统拜登签发名为“加强国家网络安全的行政命令”(Executive Order on Improving the Nation’sCybersecurity)以加强网络网络安全和保护联邦政府网络要求政府部门加快推进采用零信任架构

零信任产业标准工作组

中国产业互联网发展联盟
Internet+ Development Association of China
IDAC

鹅门标局

零信任产业标准工作组

腾讯IT技术

感　谢　关　注