ICS 35.040
L 80

# 中华人民共和国国家标准化指导性技术文件

GB/Z 24294.2—2017
部分代替 GB/Z 24294—2009

# 信息安全技术 基于互联网电子政务信息安全实施指南 第2部分：接入控制与安全交换

**Information security technology—Guide of implementation for Internet-based e-government information security—Part 2：Access control and secure exchange**

2017-05-31 发布　　2017-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

GB/Z 24294《信息安全技术　基于互联网电子政务信息安全实施指南》分为4个部分：

——第1部分：总则；

——第2部分：接入控制与安全交换；

——第3部分：身份认证与授权管理；

——第4部分：终端安全防护。

本部分为GB/Z 24294的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分部分代替GB/Z 24294—2009《信息安全技术　基于互联网电子政务信息安全实施指南》，与GB/Z 24294—2009相比，主要技术变化如下：

——给出了接入控制组成结构与实施办法；

——对接入控制功能、网络适应性提出了新的基本要求，详细细化了接入认证、接入控制规则以及接入控制管理要求，更加适合电子政务安全接入控制需求；

——针对安全交换补充了信息安全交换模式分类；

——针对安全交换补充了定制数据安全交换模式技术要求和数据流安全交换模式技术要求。

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这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：解放军信息工程大学、中国电子技术标准化研究所、北京天融信科技有限公司、郑州信大捷安信息技术股份有限公司。

本部分主要起草人：陈性元、杜学绘、孙奕、夏春涛、曹利峰、张东巍、任志宇、罗锋盈、上官晓丽、董国华。

本部分所代替标准的历次版本发布情况为：

——GB/Z 24294—2009。

# 引　言

互联网作为我国电子政务的重要信息基础设施，尽管提高了办公的效率，节约了资源与成本，但是互联网的开放性，接入用户、接入终端、接入手段的多样化，电子政务系统的安全要求与电子政务系统的开放性之间的矛盾等，将使得电子政务系统面临着非法接入、非授权访问、信息无法安全共享等安全问题，应该引起高度重视。为确保政务用户能够合法接入互联网电子政务系统安全区域，防止非法接入与非授权访问，以及域间信息安全交换特制定本部分，推动互联网在我国电子政务中的安全应用。

本部分提出了安全接入与安全交换两个阶段的安全功能要求，对基于互联网电子政务信息安全系统结构设计、网络接入方式、信息安全共享提供指导。本部分首先对分域控制与域间信息安全交换模式进行描述，然后分别从接入控制和信息安全交换技术两个阶段进行描述。在接入控制阶段，首先对接入控制模式进行了描述，明确了接入控制的组成、功能以及接入方式的要求；接着对接入认证、分域控制要求进行了规范，明确了接入认证、接入设备功能等要求，并描述了分域控制实施细则；最后对接入控制规则、接入管理进行了描述，明确了不同情况下接入控制策略以及安全管理要求。在安全交换阶段，首先对互联网电子政务信息安全交换的安全需求进行描述；明确了基于互联网电子政务信息安全交换的模式；然后分别对在定制数据安全交换模式和数据流安全交换模式下实施信息安全交换的关键环节提出相关要求。

本部分主要适用于没有电子政务外网专线或没有租用通信网络专线条件的组织机构，基于互联网开展非涉及国家秘密的电子政务建设，当建设需要时，可根据安全策略与电子政务外网进行安全对接。

# 信息安全技术
# 基于互联网电子政务信息安全实施指南
# 第2部分:接入控制与安全交换

## 1 范围

GB/Z 24294的本部分明确了互联网电子政务分域控制的两个阶段,在接入控制阶段,对接入控制结构、接入安全设备功能、接入认证、接入控制规则、接入控制管理等方面给出指南性建议要求;在安全交换阶段,对安全交换模式、定制数据安全交换要求、数据流安全交换要求给出指南性建议要求。

本部分适用于没有电子政务外网专线或没有租用通信网络专线条件的组织机构,基于互联网开展不涉及国家秘密的电子政务安全接入控制策略设计、工程实施与系统研发,为管理人员、工程技术人员、信息安全产品提供者进行信息安全规划与建设提供管理和技术参考。涉及国家秘密,或所存储、处理、传输信息汇聚后可能涉及国家秘密的,按照国家保密规定和标准执行。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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。

GM/T 0022—2014 IPsec VPN技术规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**接入鉴别方式 access authentication method**

对接入主体进行身份合法性检查所采用的方法与手段,以保证接入主体的合法性。

3.2

**接入控制规则 access control rule**

针对不同的接入主体,制定相应的安全规则,防止接入主体对内部网络资源的非法访问和越权访问。

3.3

**接入主体组 access subject group**

将属于同一安全域内的用户、主机、子网、地址段、物理网络接口、服务等按照相同的访问属性归属为同一个组,每个组内成员访问的资源内容是相同的,组由组对象名来标识。

3.4

**接入主体 access subject**

能够接入到内部网络中的终端用户、设备、区域、网段等。接入到内部网络的访问者均有相应的别名,该别名被称为对象名。

3.5

**定制交换　customized exchange**

基于交换策略对特定格式的、静态的异构数据进行统一适配、转换、过滤、传输与加载的处理过程。

3.6

**交换管理平台　exchange management platform**

对交换用户、交换任务、交换策略、交换行为审计等功能进行统一管理的平台。

3.7

**交换节点　exchange node**

在内部数据处理区域和公开数据处理区域之间，实现信息安全、可信、可控传递和处理的一套信息安全交换运行环境的集合，交换节点分为主交换节点和从交换节点两类。

3.8

**专用交换进程　private exchange process**

为信息安全交换提供特定操作的应用程序。

3.9

**主交换节点　primary exchange node**

为从交换节点提供路由信息、信息完整性验证、信息过滤等功能的交换节点，主交换节点通常部署于网关，用于控制从交换节点之间的信息安全交换。

3.10

**基于用户的安全审计　security audit based on user**

对接入主体的访问行为进行审计，审计的粒度限定到用户级，使得管理人员能够识别用户的操作行为，便于事后追踪与责任认定。

3.11

**流交换　stream exchange**

一种连续的、无限的、不可预测的流进行跨域请求与响应的过程。

3.12

**从交换节点　secondary exchange node**

为交换对象提供数据源提取、转换、过滤、传输及加载等功能的交换节点，从交换节点通常部署于需要交换数据的政务系统、数据库系统或数据中心等。

## 4　缩略语

下列缩略语适用于本文件。

AS　认证服务器(Authentication Server)

CA　数字证书认证中心机构(Certification Authority)

DNAT　目的网络地址转换(Destination NAT)

HTTP　超文本传送协议(Hypertext Transfer Protocol)

ICMP　Internet 控制报文协议(Internet Control Message Protocol)

IP　互联网协议(Internet Protocol)

IPAD　平板电脑或手机(I PAD)

NAT　网络地址转换(Network Address Translation)

PC　个人计算机(Personal Computer)

SNAT　源网络地址转换(Source NAT)

## 5 分域控制

分域控制是将基于互联网电子政务系统划分为内部数据处理区域、公开数据处理区域、安全服务区域和安全管理区域，制定安全策略，实施基于安全域的接入控制，提供有效的域间信息安全交换功能，分域控制示意图如图 1 所示。

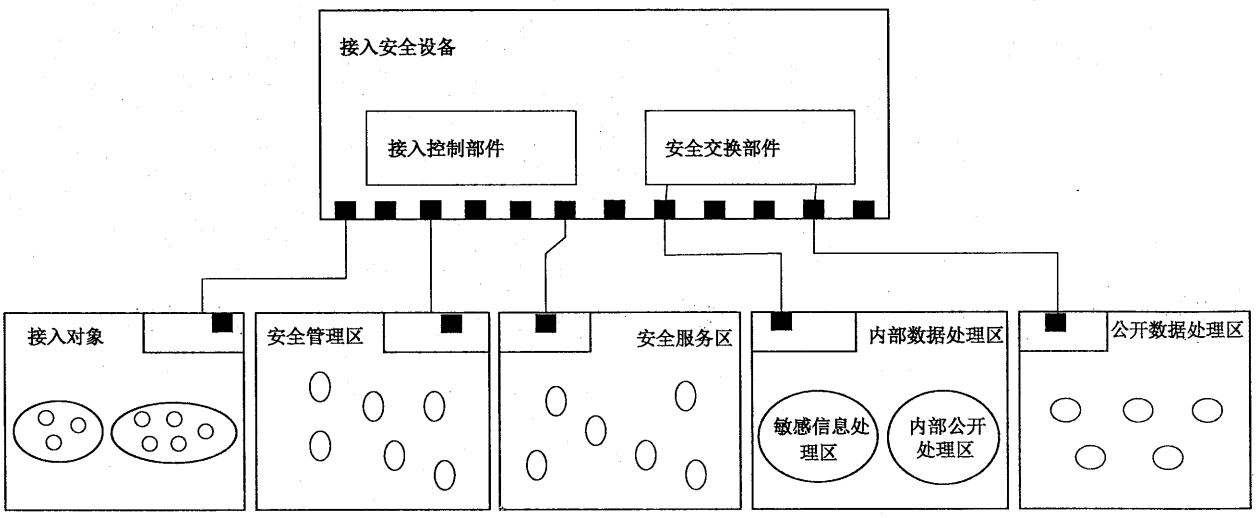


图 1 分域控制示意图

为防止域间信息的泄漏，宜制定域间安全防护策略，具体要求如下：

a) 安全管理区可对内部数据处理区、公开数据处理区进行管理。

b) 公开数据处理区的数据流可流入内部数据处理区，但内部数据处理区的数据流未经允许禁止流向公开数据处理区。

c) 在特定情况下，若内部数据处理区数据流需流入公开数据处理区，宜符合访问控制策略，进行数据敏感度的检查、过滤，防止内部敏感信息的泄漏。

d) 内部数据处理区可对服务进行标识，便于接入用户数据的分流，实现对政务信息的分类访问。

e) 公开数据处理区提供的公开服务，宜避免数据聚合引起敏感信息的泄漏。

## 6 接入控制

### 6.1 接入控制结构

#### 6.1.1 接入控制组成

在基于互联网电子政务系统中，接入控制的实施主要通过对接入主体的合法性认证，依据接入控制规则与安全传输机制，来保障电子政务系统接入访问的合法性、保密性、完整性与可控性。接入控制组成结构示意图如图 2 所示。

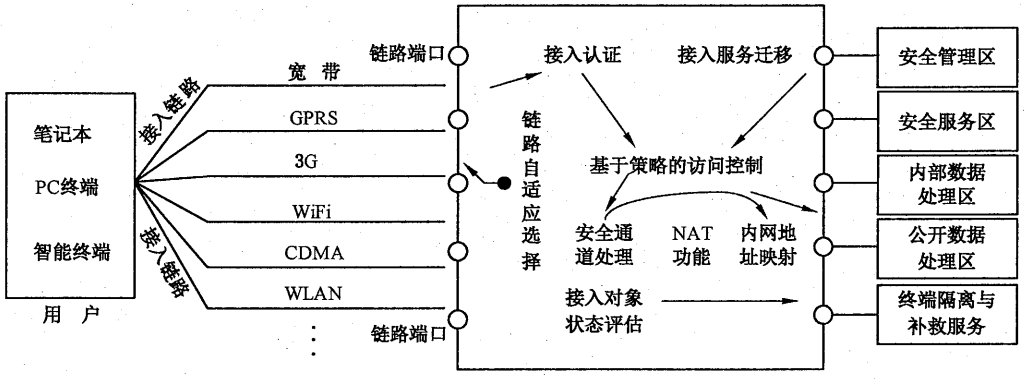


图 2 接入控制组成结构

在互联网电子政务系统中，接入控制主要由接入主体、安全接入设备、接入区域组成。

接入主体是接入电子政务系统的请求者，依托的平台宜支持多样化，如笔记本、智能终端、PC 终端等，以适应各类应用环境。

接入安全设备是集接入认证、访问控制、安全通道处理等多种安全功能为一体的用户接入控制设备，具有多个链路接入端口，是接入控制的主要实施者。

接入区域一般包括安全管理区、安全服务区、内部数据处理区、公开数据处理区。

终端隔离与补救服务，为接入终端环境提供安全评估与补救服务，对未通过评估的接入终端，宜进行安全隔离与补救。

### 6.1.2 接入控制方式

#### 6.1.2.1 接入链路

用户接入政务系统时，接入设备宜具有广泛的网络适应性，宜支持电信、联通、移动等多家运营商提供的互联网接入方式，如移动通信网、基站等。

#### 6.1.2.2 多线路接入

为提高互联网电子政务的接入访问效率，增强接入的网络适应性，基于互联网电子政务系统宜支持多线路接入，具体要求如下：

a) 支持电信、联通、移动等多线路接入，满足不同地域、不同网络、不同用户的接入访问需求。

b) 支持接入安全设备的集群化管理，保证安全接入的可靠性。

c) 接入客户端宜能够根据接入环境的变化，动态选择接入线路、接入安全设备，提高接入访问的成功率。

d) 接入安全设备宜满足大容量多用户的安全接入需求。

## 6.2 接入控制功能

### 6.2.1 接入控制安全功能

依据电子政务系统的安全需求，接入安全设备宜具有的功能包括：

a) 接入认证。采用统一身份认证技术，将用户认证与接入设备认证相结合，验证接入用户的合法性，获取接入访问权限。

b) 基于安全策略的访问控制。将<地址、协议、端口>三元组与<接入主体、接入区域、接入服务>相关联，建立访问控制策略库，实施基于安全策略的访问控制。

c) 安全通道建立与处理。针对移动安全接入、网络安全互联两种模式，在接入用户与访问对象之

间，建立静动态安全通道，提供政务数据传输的保密性、完整性、抗重放攻击服务等。具体见GM/T 0022—2014 第6小节。

d) NAT处理。支持正向SNAT功能，为电子政务系统内部用户提供互联网访问服务；支持反向DNAT功能，为互联网公共用户提供政务网络内部公开服务；支持反向SNAT功能，将远程用户地址虚拟映射为政务网络内部地址，以方便安全接入与接入控制。

e) 接入安全状态评估。通过安全状态评估，和终端隔离与补救服务的联动，确保接入终端的安全，防止风险的传递。

f) 域间安全防护。采用基于安全策略的访问控制、信息内容检测等技术，对不同区域的信息进行检测、过滤与控制，实现域间安全防护。

#### 6.2.2 接入控制适应性

良好的网络适应性是接入控制得以正常运行的关键。其基本要求如下：

a) 无缝接入。支持安全接入的无缝化，满足不同接入链路下不同用户的接入需求。

b) 透明性。为用户的多种应用，如http、ftp、POP3、SMTP等，提供透明的安全服务。

c) 部署与实施灵活性。支持路由、网桥等网络互联模式。

d) 兼容性。应与其他安全系统兼容，避免影响其工作效率，进而影响电子政务系统的正常运转。

e) 平滑迁移。宜支持平滑迁移能力，支持系统的容灾备份，防止单点失效，保证电子政务系统的正常运行。

### 6.3 接入认证

#### 6.3.1 用户接入认证策略

按照电子政务系统各安全域的功能及其安全需求，宜明确各安全域的用户接入策略，以限定不同类型用户的接入访问区域，防止非授权访问。用户接入策略如下：

a) 互联网公众可接入访问公开数据处理区域。

b) 仅允许政府单位办公人员和其他授权用户接入访问内部数据处理区。

c) 仅允许电子政务系统安全管理人员接入访问安全管理区域。

d) 仅允许政府单位办公人员、注册用户接入访问安全服务区。

e) 宜禁止接入用户的越权访问、跨区域访问，防止内部数据的泄漏与破坏。

#### 6.3.2 用户接入平台

接入平台是用户安全接入政务网络所依托的终端设备，其安全性也是保证用户安全接入的关键。为防止外部风险传递到电子政务网络，用户接入平台须满足以下要求：

a) 接入平台环境安全。不论接入平台是PC机，还是智能终端，其系统环境宜是安全可信的，未被木马、病毒等感染。

b) 接入进程合法性验证。当用户接入访问政务内部网络时，接入进程可进行合法性验证，防止接入进程被木马注入，保证接入进程的可信性。

c) 便携式终端安全接入。当采用便携式终端进行安全接入时，则须与不可信环境及其平台进行系统的有效隔离，防止风险的交叉传递。

#### 6.3.3 用户接入认证

接入认证是接入控制的前提，用于验证用户的合法性。用户在接入政务网络时，宜满足以下接入认证要求：

a) 电子政务系统宜支持多种接入鉴别方式，以适应于不同类别的接入用户。如口令认证、数字证书认证、多认证方式组合等。

b) 接入认证的时机。在用户联网成功以后，当访问政务网络时触发接入认证。

c) 接入认证的撤销。为保证接入认证的时效性及系统的安全，宜在用户完成访问，或在一段时间内用户未进行访问时，撤销其认证。

d) 个人终端接入项。当接入平台为 PC 机、笔记本、IPAD 时，接入认证项宜为用户 ID、数字证书以及随机数 R，接入认证数据格式如图 3 所示，即 $K_s$(Protocol Head，UserID，Certificate，R)。通过认证服务器 AS 验证数字证书的合法性，裁决用户是否可以进行接入。

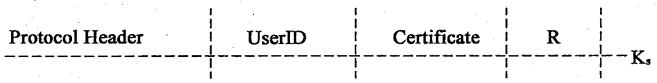


图 3 个人终端接入认证数据格式

e) 智能终端接入项。当接入平台为智能手机时，接入认证项宜为用户 ID、手机号码、SIM 卡号以及随机数 R，接入认证数据格式如图 4 所示，即 $K_s$(Protocol Head，UserID，Phonenum，SIM num，R)。通过手机号码、SIM 卡号，获取用户数字证书，AS 验证数字证书的合法性，裁决用户是否可以进行接入。

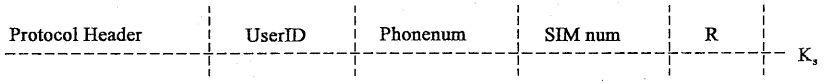


图 4 智能终端接入认证项

## 6.4 接入控制规则

### 6.4.1 用户接入控制规则

在基于互联网电子政务系统中，用户的接入控制规则满足以下要求：

a) 当为网络互联模式时，用户接入控制规则的格式可包括用户 IP 地址、服务 IP 地址、协议、端口号、接入安全区域标识、策略等，控制粒度限定在 IP 地址和端口，可实现粗粒度的接入控制。

b) 当为移动安全接入时，用户接入控制规则的格式可包括用户对象名、权限、资源、接入安全区域标识、策略等，控制的粒度限定在资源，可实现细粒度访问控制。

c) 当接入用户的 IP 地址动态变化时，宜依据用户数字证书判定其合法身份，动态生成用户接入控制规则。若接入用户身份无法得到确认，仅允许接入到公开数据处理区。

d) 支持用户接入控制规则的动态变化。当用户可信度降低，或接入平台可信性较差时，可适当调整用户的接入控制规则。

### 6.4.2 分组接入控制规则

在电子政务系统中，宜支持组、子网的接入控制，以降低接入控制规则管理的复杂度。分组接入控制规则满足以下要求：

a) 子网接入控制规则的格式可包括 IP 地址、子网掩码、接入的安全区域标识、服务 IP 地址、策略等；或为子网对象名、接入的安全区域标识、服务 IP 地址、策略等。

b) 组的接入控制规则的格式可包括接入主体组对象名、接入的安全区域标识、服务 IP 地址、策略等。

#### 6.4.3 终端隔离与补救规则

终端隔离与补救规则满足以下要求：

a) 当终端接入政务网络时，检测其是否已遭受木马病毒的攻击，若遭受，则禁止其接入政务网络，并将其接入补救区域，进行病毒库的升级，强制要求病毒查杀。

b) 当终端接入政务网络时，检测其是否存在严重的系统漏洞，若存在，则将其接入补救区，进行在线的系统补丁下载与更新。

c) 当接入终端无法进行病毒、木马的查杀，以及系统漏洞无法修复时，宜禁止其接入政务网络。

d) 当终端接入政务网络时，宜对接入进程进行认证，防止非授权进程的接入。

### 6.5 接入控制管理

#### 6.5.1 统一接入安全管理

在互联网电子政务系统中，安全管理要求如下：

a) 统一安全管理要求。支持接入安全设备、接入用户的集中、统一化管理。

b) 可视化安全管理要求。对电子政务系统中的接入安全设备、接入用户、网络状态等进行可视化的管理，更加直观、形象地进行管理。

c) 远程安全管理要求。统一接入安全管理宜支持远程安全管理，使得管理用户无须亲临现场就能进行接入安全设备的管理与调试。

d) 统一接入安全管理宜包括安全策略管理、安全通道管理、系统管理、网络管理以及安全审计管理等。

e) 安全管理宜支持三权分离，即安全管理、系统管理、审计管理的相互隔离。

#### 6.5.2 接入用户管理

接入用户管理要求如下：

a) 用户注册。接入到电子政务系统的用户，宜在统一接入安全管理系统中进行注册。注册用户具有唯一的标识。

b) 用户撤销。支持用户的撤销功能，防止失效用户的非法接入访问。

c) 用户接入策略模板。支持用户接入策略模板，可实现安全策略的生成、下载、编辑、删除等功能。

#### 6.5.3 安全策略管理

接入控制安全策略管理要求如下：

a) 支持安全策略的添加、删除与修改。依据电子政务系统的安全需求，可灵活地对安全策略进行调整。

b) 支持安全策略的下发。对接入用户、接入安全设备的安全策略进行分发、加载。

c) 支持组策略管理。主要包括组的管理、组策略的添加、删除与修改等。

d) 支持安全策略的一致性检测。通过检测安全策略的一致性，保证安全策略的可用性。

e) 支持策略冲突与消解。检测并消除安全策略间的冲突，防止由于策略冲突而引起的安全隐患。

#### 6.5.4 安全审计管理

##### 6.5.4.1 基于数据流的安全审计

基于数据流的安全审计，主要依据数据报文信息，对过往接入安全设备的数据流进行日志记录。其

实施与管理要求如下：

a) 安全审计格式。审计格式可为序号、源 IP 地址、目标 IP 地址、源端口号、目标端口号、协议、策略以及审计时间等。
b) 审计转存。支持审计日志的转储功能，实现审计数据的长期保存。
c) 审计操作。具有审计日志存储、查询、删除等功能。
d) 审计分析。支持基于 IP 地址的访问行为分析功能，依据分析结果，可评估电子政务系统存在的安全风险。

#### 6.5.4.2 基于用户的安全审计

基于用户的安全审计，主要依据用户身份与数据流的关联，对过往接入安全设备的数据流进行安全审计，以防止 IP 地址假冒攻击。其实施与管理要求如下：

a) 用户身份与数据流绑定。将用户身份标识与数据安全处理进行关联绑定，依据绑定关系，审计到用户。
b) 审计格式。审计格式主要为序号、用户、访问服务信息、策略以及审计时间等。
c) 审计操作。具有审计日志存储、查询、删除等功能。
d) 审计分析。支持基于用户的访问行为分析功能，依据分析结果，可评估用户访问行为对电子政务系统的安全威胁。

## 7 信息安全交换

### 7.1 信息安全交换需求

#### 7.1.1 信息安全隔离需求

根据信息的重要程度和不同类别，采取不同的保护措施，实施分类防护；根据系统和数据的重要程度和敏感程度不同，进行分域存储。按照电子政务应用系统信息和应用分类的安全需求，划分为内部数据处理区域和公开数据处理区域；根据安全系统的功能不同，划分为安全管理区域和安全服务区域。要求对不同区域实施安全隔离，应能够实施各安全域间的信息流控制，防止域间信息的非授权流动。

#### 7.1.2 信息安全共享需求

根据基于互联网电子政务信息分域控制的要求，互联网电子政务安全域划分为内部数据处理区域、公开数据处理区域、安全管理区域和安全服务区域。其中公开数据处理区域用来承载处理公开信息的电子政务应用系统及其数据库，处理对公众和企业开放的服务，如政策发布、政府网站或便民服务等，这些都是提供给公众访问的公开数据。内部数据处理区用来承载处理内部信息的电子政务应用系统及其数据库，处理政府内部和部门之间的业务，这些是仅允许系统内部人员访问的内部数据。依据基于互联网的电子政务办公需求，需要内部数据处理区域和公开数据处理区域进行信息共享。

#### 7.1.3 交换策略定制需求

为了保证内部数据处理区域和公开数据处理区域之间信息的安全隔离和共享，需要在内部数据处理区和公开数据处理区之间实现信息的安全交换。由于内部数据处理区和公开数据处理区属于不同的安全域，在互联网环境下除了要应对来自互联网的攻击，还要防止内部数据处理区的敏感信息泄露到公开数据处理区。因此需要对内部数据处理区域和公开数据处理区之间交换的行为和信息进行控制，需要根据交换任务和安全需求，制定安全交换策略并实现对安全交换策略的动态管理。

### 7.1.4 交换数据安全性需求

在域间进行信息安全交换时，需要保证交换数据的安全性。交换数据的安全性主要包括交换数据源可信、交换信息保密、交换信息完整及交换内容过滤等。交换数据源可信应支持交换数据生成者对交换数据的数字签名，确保交换数据源的真实性和不可否认性。交换信息保密宜支持对交换信息的加密存储和传输，确保交换信息的保密性。交换信息完整宜支持对交换信息的完整性验证，防止交换过程中的木马夹带攻击与信息非法篡改。交换内容过滤应支持对交换信息实施基于安全交换策略的内容过滤。

### 7.1.5 交换行为监管需求

为了防范木马夹带攻击和敏感信息的泄漏，要求在安全策略控制下实施受控交换，要求使用专用的交换进程，要求对交换进程行为进行全周期管控，保证交换行为的可管可控。

## 7.2 信息安全交换模式

### 7.2.1 定制数据安全交换模式

基于互联网电子政务信息安全交换模式宜支持定制交换及流交换两种交换模式。定制数据交换模式是指基于交换策略对特定格式的、静态的异构数据进行统一适配、转换、过滤、传输与加载的处理过程。这种模式的特点是一般面向特定的交换对象，对信息安全交换行为的控制能力较强，主要适合于交换信息固定、交换行为可预定义的跨域交换，如文件交换、数据库同步等。

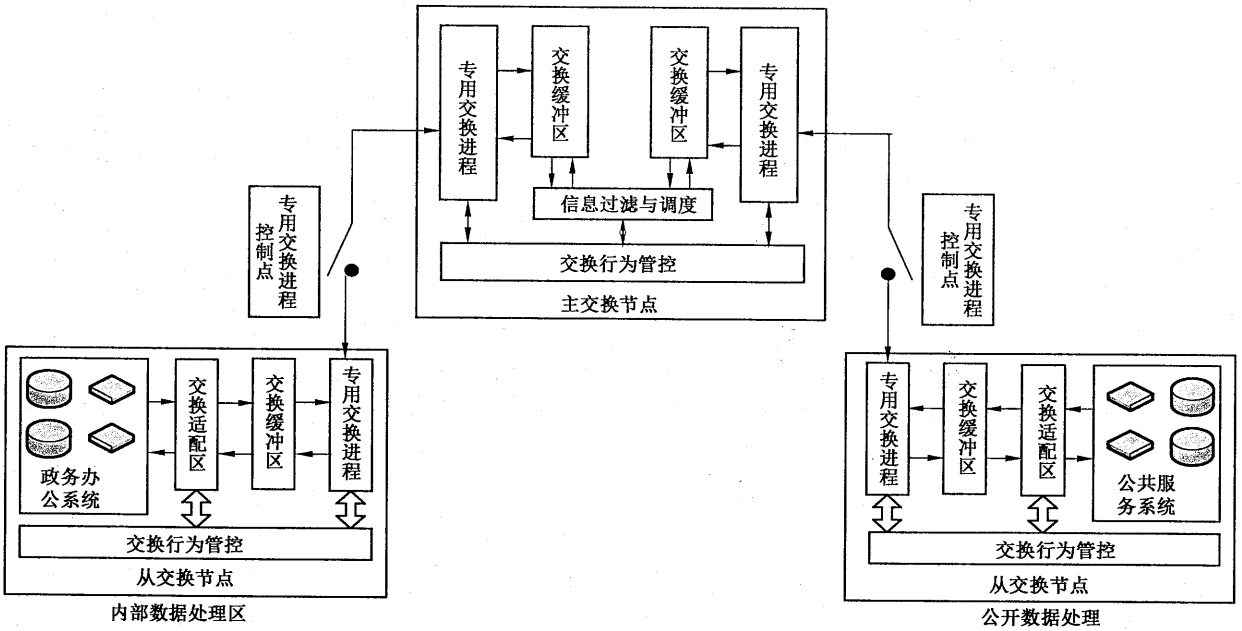


图 5 定制数据安全交换模式

定制数据安全交换模式的示意图如图 5 所示，分别在内部数据处理区和公开数据处理区部署从交换节点，在网关处部署主交换节点和交换管理平台，具体交换步骤如下：

a) 交换数据生成过程。内部数据处理区中的交换适配区根据定制的交换策略从政务办公系统中提取交换信息，将交换信息转换为统一的格式，放入交换缓冲区。

b) 交换数据传递过程。合闭专用进程控制点，启动内部处理区和交换主节点的专用进程将信息从内部处理区的缓冲区交换到主节点的缓冲区中，任务完成后打开专用进程控制点。

c) 交换数据过滤过程。对缓冲区中的信息进行过滤并依据定制的交换任务将过滤后的信息调度到相应的接收缓冲区中。

d) 交换数据加载过程。交换主节点和公开数据处理区的专用交换进程控制点合闭，启动专用进程将信息交换到公开数据处理区的交换缓冲区中，经过适配区的转换发送给公共服务系统。

整个交换过程均在交换行为的管控下进行，当出现异常行为时立即终止信息交换。

### 7.2.2 数据流安全交换模式

一种连续的、无限的、不可预测的流进行跨域请求与响应的过程。这种模式的特点是一般面向不可知的交换对象，对信息安全交换行为的控制能力较弱，主要适合于交换实时性高、交互性强、交换终端计算能力较弱的跨域交换，如视频会议、实时监控等。

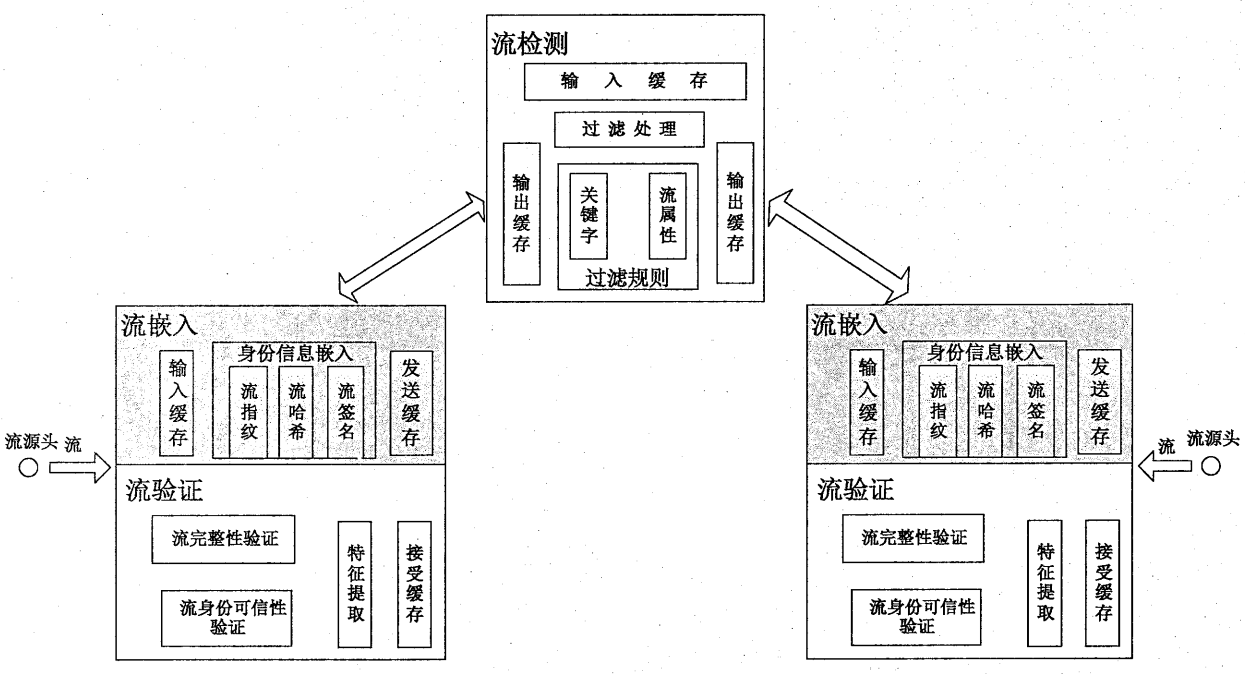


图 6 数据流安全交换模式

数据流安全交换模式的示意图如图 6 所示，具体工作步骤如下：

a) 流连接建立过程。在流交换开始之前进行的会话连接建立。发送端通过请求建立连接，接收端基于安全连接检测机制，依据制定的策略对请求进行检测，从而判断请求建立的连接是否安全可信。

b) 流嵌入过程。流从流源头产生后进入输入缓存，在流身份信息嵌入器中对流进行处理将流指纹、流摘要等流身份相关的信息嵌入到流中，并将嵌入身份信息的流转移到发送缓存。流指纹是指具有一定长度和特定结构的流身份序列。

c) 流检测过程。嵌入身份信息的流传输到边界网关处首先进入输入缓存，待过滤的流基于流交换策略对流进行过滤检测，只有符合策略的流才能通过过滤并流入输出缓存中。

d) 流验证过程。经过流过滤后流入接收缓存。从流的包头、包时间间隔等载体中提取流指纹或流散列等流身份相关的信息进行流身份可信性验证。同时利用流签名、流认证等技术进行流完整性验证。最终通过验证的流传送到接收端进行数据处理。

## 7.3 定制数据安全交换模式技术要求

### 7.3.1 定制交换策略

定制交换模式的策略制定应包括以下几个方面：

a) 从公开到内部的策略。允许通过制定交换流向、交换任务和交换方式等将数据从公开处理数据区交换到内部数据处理区。

b) 从内部到公开的策略。允许通过制定交换流向、交换任务和交换方式等将不涉及政务办公敏感信息的数据从内部数据处理区交换到公开数据处理区。

c) 交换任务的制定。允许制定交换任务的交换目录。

d) 交换内容的制定。允许制定交换的内容，如对交换信息的属性、粒度等进行定制。

e) 交换方式的制定。允许制定交换的方式，如一次交换、周期交换、定时交换、自动交换、手动交换等。

### 7.3.2 定制数据安全交换适配

交换数据适配要求应包括以下几个方面：

a) 交换数据源提取。应支持 Java、.Net、C、C++等多种语言开发业务系统；应支持办公自动化系统、文件传输系统、数据库同步系统、公共服务等多种类型应用的业务系统；应支持文件级、数据库级、表单级、字段/域级等不同粒度数据的提取。

b) 交换数据转换。应支持不同业务应用系统的数据结构按照不同业务数据格式的要求，遵循统一的数据规范、数据字典和数据编码，进行统一转换，传给底层网络传输接口。

c) 交换数据传输。应支持不同类型的底层网路传输接口，如：Socket 接口、SSL 接口、IPSec 接口与消息中间件接口等。

### 7.3.3 交换数据内容安全

定制交换数据安全性要求应包括以下几个方面：

a) 定制交换数据源可信。应支持基于密码技术的对数据源生成者的身份认证，确保交换数据源的真实性和不可否认性。

b) 定制交换数据完整。应支持对交换信息的完整性验证，防止交换过程中的木马夹带攻击与信息非法篡改。

c) 定制交换数据保密。应支持对交换信息的加密存储和传输，确保交换信息的保密性。

d) 定制交换数据过滤。应支持基于域间信息安全交换策略的信息过滤；应支持不同粒度的信息过滤；应支持基于黑/白名单的过滤规则的过滤管理。

### 7.3.4 交换进程安全

交换进程安全要求应该包含以下几个方面：

a) 在信息交换中，专用交换进程的交换行为应该是可预知、可控制的。专用交换进程的交换行为应受到安全策略的约束、其轨迹应是平稳有序的。

b) 专用交换进程的任何行为都是经过授权和认证的，一切未经授权或认证的行为都是非法并且被禁止的。其中包括专用交换进程对于数据、网络等客体的操作。

c) 在交换进行过程中，宜对交换行为进行实时地评估，保证其符合正常行为。

d) 应在安全的环境下，收集正常的交换行为序列，在该行为序列上建立交换行为评估模型。交换行为评估应具有良好的完备性和精确性。

e) 交换进程行为评估应具有高效的行为收集方法，使行为的收集对交换进程透明，不影响交换的正常进行及效率。

#### 7.3.5 交换网络连接安全

交换网络连接安全主要用于保证交换网络连接的可信性，应包括以下几个方面：

a) 应保证接入到交换网络的专用交换进程的可信性，防止木马等恶意程序接入到交换网络中，在网络中传输数据。

b) 专用交换进程运行环境安全。应保证专用交换进程执行时所依赖的软件包可信；应保证进程运行所依赖的内核环境可信，内核环境主要包括内核代码段、内核只读数据段、系统调用表、中断描述符表、全局描述符表以及内核模块。

c) 专用交换进程运行时安全。应保证专用交换进程的关键段的可信，如防止代码段篡改、栈溢出、堆溢出。

#### 7.3.6 交换行为审计

交换行为审计应支持对所执行的交换任务进行记录，记录每次交换任务的源节点/目的节点的 IP 地址、端口号、交换时间、交换文件的 hash 值等信息，当出现违规交换时应能记录下相应的违规事件，以便日后审查。

### 7.4 数据流安全交换模式技术要求

#### 7.4.1 数据流源认证

在流交换中，宜基于流签名、流指纹等鉴别技术从不同方式主动认证流源头信息，保证流源头信息的真实性和不可否认性。

方式 1：基于流签名的数据流源认证要求应该包括以下几个方面：

a) 采用流签名算法应符合国家商用密码管理规定，建议优先采用 SM2 算法。

b) 采用的流签名算法应对数据流进行高效的签名和验证。具有高效性、实时性、所需计算资源少等特点。

c) 采用的流签名算法应能够容忍包丢失、包延时，实现对数据包实时验证。

d) 采用的流签名算法应支持流分片签名功能，无需预先缓存整个流数据。

e) 采用的流签名算法应支持在适应性选择消息攻击下是不可伪造的。

方式 2：基于流指纹的数据流源头可信性验证要求应该包括以下几个方面：

a) 应不受到通信系统异构性的影响，适应电子政务系统对时延敏感、多流交汇和资源有限的特点。应不依靠系统间的通信协议和流数据的内容获取流身份等相关信息。应将系统作为“黑盒”处理，具有不受加密影响的特点。

b) 流指纹信息编码与解码应具有保密性、可信性和可用性。宜采用 SM3 等基于国产摘要算法实现流指纹信息机密性保护；宜采用绑定算法、引入随机数等方式，防止流指纹信息的篡改，实现流指纹信息的可信性；宜采用门限方案、双重或多重指纹的技术，保证流指纹信息在遭到一定程度的流变换后的可用性。

c) 流指纹嵌入与提取过程：应满足鲁棒性、隐蔽性和大容量。应通过选择鲁棒性强的载体，或者

通过量化索引、直序扩频等辅助技术，实现在一定程度上抵御流变换问题的能力；应选用容量大的载体，或通过组合载体提高载体容量，从而保证嵌入流身份信息的载体容量应该足够大；流指纹信息应具有良好的隐蔽性。通过 K-S 实验、EN 测试和 CCE 测试等方法，对嵌入指纹前后的载体差异控制在阈值范围内，以保证嵌入的信息应该对正常用户是透明的、让攻击者很难辨别。

d) 流指纹算法应该具有高正确性。能从理论上证明指纹信息编码解码、调制解调算法的正确性，并且在实际条件下具有较高的正确率和低误报率和漏报率。

e) 宜支持多种流身份鉴别功能。如：基于包序列的流身份鉴别功能、基于直接序列扩频的流身份鉴别功能、基于时隙间隔重心的流身份鉴别功能。

### 7.4.2 数据流完整性验证

在流交换中，应采用流摘要、流水印等技术，保证流的完整性，防止流夹带与非授权篡改。数据流完整性检测要求应该包括以下几个方面：

a) 宜支持基于 hash 函数或流水印的数据流完整性验证功能。

b) 宜能够容忍网络拥塞、网络抖动等问题。

c) 宜能够容忍流间变换问题，如流混杂、流分离和流合并等问题。

d) 宜能够容忍流内变换问题，如虚假数据包添加、包丢失、包重组、包乱序等问题。

e) 宜能够抵御恶意网络攻击，如多流攻击、统计检测攻击等。

### 7.4.3 数据流内容检测

数据流内容过滤要求应该包括以下几个方面：

a) 宜支持 XML 流、数据流等多种不同类型的流检测功能。

b) 宜支持基于协议的流检测功能。如：IP 协议、IPx 协议、ICMP 协议、HTTP 协议等。

c) 宜支持基于流属性的流检测功能。如：基于字段的流检测、基于时间的流检测、基于包长度的流检测等。

中 华 人 民 共 和 国
国家标准化指导性技术文件
信息安全技术
基于互联网电子政务信息安全实施指南
第2部分：接入控制与安全交换
GB/Z 24294.2—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室：(010)68533533 发行中心：(010)51780238
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 32 千字
2017年6月第一版 2017年6月第一次印刷
*
书号：155066·1-55837 定价 21.00 元



GB/Z 24294.2—2017

GB/Z 24294.2-2017

打印日期：2017年6月16日 F007