ICS 35.080
L 77

SZDB/Z

深圳市标准化指导性技术文件

SZDB/Z 17.8-2008

深圳市电子政务应用服务规范 第8部分：单点登录服务接口规范

Electronic Government Application Service Specification—

Part 8 : Single-sign-on Service API Specification

2008-11-18 发布　　2008-12-01 实施

深圳市质量技术监督局发布

目　　次

前　言

SZDB/Z 17-2008《深圳市电子政务应用服务规范》目前分为10个部分：

——第1部分　《总则》

——第2部分　《应用系统分类及代码规范》

——第3部分　《应用系统描述规范》

——第4部分　《组织身份模型数据规范》

——第5部分　《应用服务运行管理框架规范》

——第6部分　《组织身份服务接口规范》

——第7部分　《访问控制服务接口规范》

——第8部分　《单点登录服务接口规范》

——第9部分　《电子表单服务接口规范》

——第10部分　《业务流程服务接口规范》

本部分为SZDB/Z 17-2008的第8部分。

本技术规范适用于深圳市各级党政机关的信息化建设工作。对于本部分未能涵盖的内容将依据本技术规范的编写原则对本部分内容进行扩充。

本技术规范文件由深圳市信息化领导小组办公室、深圳市福田区信息中心提出。

本技术规范文件由深圳市信息化领导小组办公室归口。

本技术规范文件由深圳市信息化领导小组办公室、深圳市福田区信息中心、北京有生博大软件技术有限公司共同起草。

本技术规范文件主要起草人：贾兴东、陈朝祥、张雁、高新辉、王克照、石卫宁、赵斌、李淼、周礼洪、杨海波、王姝、张焕焕、刘用军、梁文龙等。

本技术规范文件为首次发布。

深圳市电子政务应用服务规范
第8部分：单点登录服务接口规范

1 范围

本部分规定了单点登录服务接口，定义了单点登录票据的模式。

本部分主要用于深圳市各级党政机关的信息系统规划与建设，以及电子政务信息系统建设的系统集成商、软件开发商和监理单位进行信息化规划、建设。适用于需做单点登录整合的应用系统，也适用于应用系统间实现基于票据传递的单点登录整合。用于指导开发商对应用系统进行单点登录整合，约束应用系统单点登录接入的实现。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

SZDB/Z 17.1 -2008　电子政务应用服务规范 第1部分：总则

SZDB/Z 17.4 -2008　电子政务应用服务规范 第4部分：组织身份模型数据规范

SZDB/Z 17.6 -2008　电子政务应用服务规范 第6部分：组织身份服务接口规范

3 术语和定义

票据：

用户在通过单点登录验证后获得，包含用户的基本信息，如唯一标识、登录名、票据的有效期等。

票据标识：

用户在通过单点登录验证后获得票据的唯一标识。

4 作用

通过单点登录服务让用户在一次输入用户名密码验证登录后，访问所有应用系统而不需要再输入用户名和密码进行验证；用户在一次注销后，即可在所有应用系统实现注销。

单点登录服务以组织身份模型为数据基础，以组织身份服务为运行支撑。实现单点登录服务的前提是，各应用系统采用统一的组织身份数据模型。单点登录服务中的认证及获取用户信息均应调用组织身份服务接口。

5 单点登录服务逻辑

5.1 服务代理

为用户提供单点登录认证，认证成功后为该用户颁发对应的票据。将票据和票据标识保存在服务器上，同时将票据的标识保存在用户的客户端。在用户请求注销时，负责通知各应用系统注销该用户。

5.2 访问拦截组件

拦截用户对应用系统的访问请求，根据保存在客户端的用户票据标识，向单点登录代理服务器请求用户的票据，如果正确地得到了用户的票据，则调用应用系统二次认证接口（参见6.4）。如果二次认证通过，则允许用户访问该应用系统；如果票据标识不存在或者票据无效，则不允许用户访问该应用系统。

5.3 对应用系统的约束

5.3.1 应用系统二次认证

根据用户的票据标识从单点登录代理服务器中获得用户票据，从票据中获得用户的基本信息，再进行应用系统的本地认证。

5.3.2 应用系统本地注销

用户在入口点注销后，由单点登录服务代理通知各应用系统，在所有的应用系统中注销该用户。

6 接口定义

本接口所处的命名空间为：egov.appservice.sso。

6.1 单点登录认证接口

服务名称	SSOAgentBaseService.authenticate()	
服务说明	应用系统向单点登录服务代理请求认证指定用户。	
参数列表	参数名称	参数说明
	username	String类型，用户的登录名
	password	String类型，用户的密码
异常处理	SSOAuthenticateFailedException	如果认证失败，则抛出此异常
返回值	返回认证通过后为用户颁发的票据唯一标识	
备注		

6.2 获取单点登录票据接口

服务名称	SSOAgentBaseService.getTicket()	
服务说明	应用系统根据客户端的票据标识向单点登录服务代理请求票据。	
参数列表	参数名称	参数说明
	ticketed	String类型，用户持有的票据唯一标识
异常处理	TicketExpiredException	如果票据已过期或者失效，则抛出此异常
返回值	String类型，返回被认证通过后为用户颁发的票据。	
备注		

6.3 单点登录注销接口

服务名称	SSOAgentBaseService.logout()	
服务说明	消除用户的票据，并通知各应用系统注销该用户	
参数列表	参数名称	参数说明
	ticketId	String类型，用户持有的票据唯一标识
异常处理	TicketExpiredException	如果票据已过期或者失效，则抛出此异常
	SSOLogoutFailedException	如果用户注销失败，则抛出此异常
返回值	无	
备注		

6.4 应用系统二次认证接口

服务名称	SSOAppLocalService.authenticate()

服务说明	用户在通过单点登录服务代理认证后，应用系统需要实现的本地系统认证接口。	
参数列表	参数名称	参数说明
	username	String 类型，用户的登录名
	password	String 类型，用户的密码
异常处理	无	
返回值	boolean 类型，如果认证成功返回 true，如果认证失败则返回 false	
备注		

6.5 应用系统本地注销接口

服务名称	SSOAppLocalService.logout()	
服务说明	在本应用系统中注销用户	
参数列表	参数名称	参数说明
	ticketeId	String 类型，用户持有的票据唯一标识
异常处理	无	
返回值	无	
备注		

6.6 单点登录服务异常规定

异常名称	异常描述
SSOException	单点登录服务根异常。
TicketExpiredException	票据过期，抛出此异常。
SSOAuthenticateFailedException	用户认证失败，抛出此异常。
SSOLogoutFailedException	用户注销失败，抛出此异常。

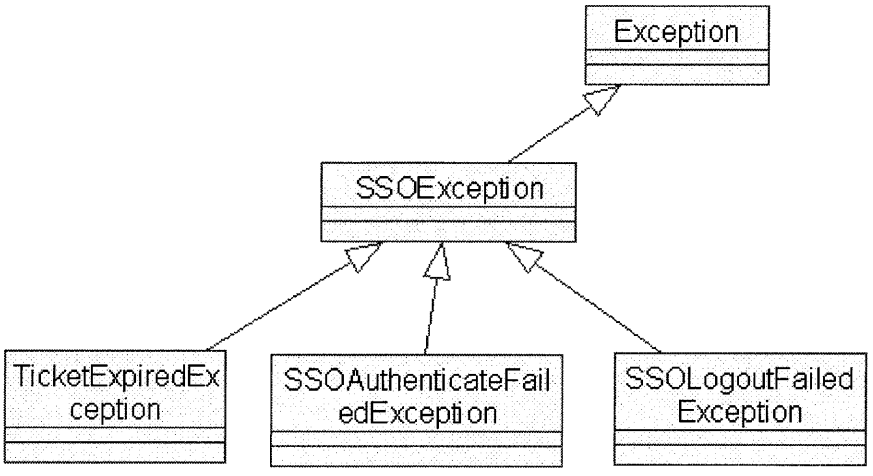

图1 单点登录服务异常关系示意图

附 录 A
（规范性附录）
单点登录用户票据 Schema 定义

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xs:element name="SSOTicket">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ticketId"/>
                <xs:element ref="guid"/>
                <xs:element ref="userName"/>
                <xs:element ref="validTime"/>
                <xs:element ref="pwd"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="guid">
        <xs:simpleType>
            <xs:restriction base="xs:string">
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="pwd">
        <xs:simpleType>
            <xs:restriction base="xs:string">
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="ticketId">
        <xs:simpleType>
            <xs:restriction base="xs:string">
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="userName">
        <xs:simpleType>
            <xs:restriction base="xs:string">
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="validTime">
        <xs:simpleType>
```

```
            <xs:restriction base="xs:long">
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
</xs:schema>
```

参考文献

[1].白殿一.GB/T1.1－2000《标准化工作导则 第1部分：标准的结构和编写规则》实施指南.中国标准出版社.2001

[2].胡毅时,怀进鹏; 基于Web服务的单点登录系统的研究与实现[J]; 北京航空航天大学学报; 2004年03期

[3]J Park,R Sandhu; Secure Cookies on the Web [M];IEEE Internet Compu-ting; 2000

[4] 申婷,李晖,于明喆 :Token-based single sign-on protocol and its formal analysis 西安电子科技大学学报（自然科学版）: 2006年05期