统一身份认证平台单点登录认证

技术白皮书

杭州双驰信息技术有限公司

2013 年 06 月

系统支持不同开发语言、不同应用服务器平台实现的应用系统的认证集成方式（Java、.NET、ASP、PHP 等）。

1．统一身份认证

a) 认证集成模式

认证集成可以采用以下定义的模式：

- ✧ URL 单点模式

b) URL 单点模式

i. 认证过程

用户通过集中的单点登录界面进入业务系统时，系统通过 URL 向业务系统传递认证需要的参数，业务系统通过校验这些参数确定认证是否通过。

ii. 传递的参数

用户通过单点登录界面访问业务系统时，系统向业务系统传递如下七个参数，其中 Name、Datetime、jsName、verfiy、recordId 等参数是必须的，其中 gndm 等参数是可选的：

Name：业务系统中的用户帐号，即需要登录到系统的账号；

Datetime：时间戳，自 1970 年 1 月 1 日午夜起至现在的时间差，精度为秒，标准格式为 yyyy-mm-ddhh24:mi:ss；

jsName：业务系统中的用户角色名，如果业务系统不需要显示表明角色，可以使用默认字符串：’default’，；

verify：校验码，由 Name、Datetime、jsName 及公钥通过 MD5 加密方式加密产生；

gndm：被访问的业务系统模块在业务系统中的模块代码；

recordId：从统一身份认证平台中进行跳转的业务系统时产生的 ID，用于信息记录的反馈。

iii. 参数的加密

校验码 verify 由 Name、Datetime、jsName 及公钥通过 MD5 加密方式加密产生。其中公钥是双方约定一个字符串，通过 MD5 加密的字符串统一都是小写格式。

iv. 参数的传递

参数通过 URL 的方式由单点登录界面传递给业务系统，格式如下：

url?verify=校验码&Name=用户名&Datetime=时间戳&jsName=角色名&gndm=模块代码&recordId=记录 id

v. 认证过程和结果判断

业务系统获取各个参数后，首先比较数据库服务器时间同传递过来的 Datetime 是否在允许的时间差范围内（注意双方服务器时间需保持标准时间），若在时间差范围内，则需将 Name、Datetime、jsName 及公钥通过加密算法提供的公共包进行加密后返回的结果同 verify 进行比较，若一致，则可以正常登录。否则不允许登录。

vi. 参数的配置和保存

系统提供技术手段配置和保存“平台用户”和“业务系统用户”对照表、“平台角色”和“业务系统角色”对照表、业务系统访问地址、业务系统可访问模块的访问地址、业务系统模块代码表。