ICS 07.060
CCS A45

HY

中 华 人 民 共 和 国 海 洋 行 业 标 准

XX/T XXXXX—XXXX
代替 XX/T

海洋应用软件集成规范 统一身份认证

Specification for oceanic application software integration—
Unique identity authentication

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国自然资源部　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规则起草。

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专利的责任。

本文件由中华人民共和国自然资源部提出。

本文件由全国海洋标准化技术委员会（SAC/TC 283）归口。

本文件起草单位：国家海洋信息中心、广西壮族自治区海洋研究院、南宁师范大学、自然资源部北海海域海岛中心。

本文件主要起草人：刘金、曹盛文、吕憧憬、李焰、文莉莉、邬满、严小敏、姜晓轶、宋丽丽、何隆、孙苗、曹磊、赵龙飞、徐晓玮、雷艳。

海洋应用软件集成规范　统一身份认证

1　范围

本文件规定了海洋应用软件集成统一身份认证的总体要求，明确了组织机构信息、用户信息、权限信息的管理要求，给出了统一身份认证的实现方式。

本文件适用于海洋应用软件集成统一身份认证系统的建设以及各级海洋应用软件的建设、改造和集成。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语、定义和缩略语

3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1

统一身份认证 unique identity authentication

用户通过使用同一套认证凭证，可访问集成系统中与该用户身份对应的应用软件的过程。

[来源：GB/T 31072-2014，3.1.1]

3.1.2

单点登录 single sign-on

在多个应用系统中，平台用户只需要登录一次就可以访问所有相互信任平台应用系统的过程。

[来源：GB/T 31072-2014，3.1.2]

3.2　缩略语

下列缩略语适用于本文件。

CAS　中央认证服务

HTTP 超文本传输协议

SAML 安全断言标记语

4　总体要求

4.1　基本要求

4.1.1　统一用户管理

应集中存储和管理组织机构及用户资料，保证组织机构和用户信息的一致性。

4.1.2　统一身份认证

应对海洋应用软件用户的身份进行集中、统一认证。

4.1.3　实现单点登录

应实现海洋应用软件的单点登录。

4.1.4　统一命名规则

应对海洋应用软件的组织机构代码、用户编码实施统一的命名规则。

4.1.5 权限分配管理

宜采用两级授权机制，集成平台中各海洋应用软件及其信息资源的访问权限应由各应用软件管理员管理，集成平台基础功能模块的访问权限应由平台管理员管理。

4.2 基本流程

4.2.1 基础组成

海洋应用软件集成的身份认证应通过构建统一身份认证系统来实现，基于统一用户数据库存储用户身份信息，并提供统一的认证接口。

海洋应用软件应采用统一身份认证系统完成组织机构、用户和权限信息的审核及管理。

统一用户数据库应包含必要的组织机构信息和用户信息，根据实际需求可适当扩展。

统一身份认证系统应具备独立运行并通过接口提供服务的能力。

4.2.2 技术流程

统一身份认证的技术流程如图1所示：

a) 访问请求：用户通过浏览器访问应用系统，访问入口为集成平台，图 1 中步骤①；
b) HTTP 重定向：平台通过 HTTP 重定向，将访问请求指向统一身份认证系统，图 1 中步骤②；
c) 认证请求：统一身份认证系统处理认证请求，图 1 中步骤③；
d) 认证响应：通过统一用户数据库的身份信息核验判断该用户是否具有访问权限，图 1 中步骤④；
e) 访问应用：根据认证响应结果，允许合法用户访问应用系统，阻止非法访问，图 1 中步骤⑤；
f) 认证声明：对用户权限之内的海洋应用软件及海洋信息资源进行授权访问，同时进行认证声明，图 1 中步骤⑥；
g) 返回结果，图 1 中步骤⑦。

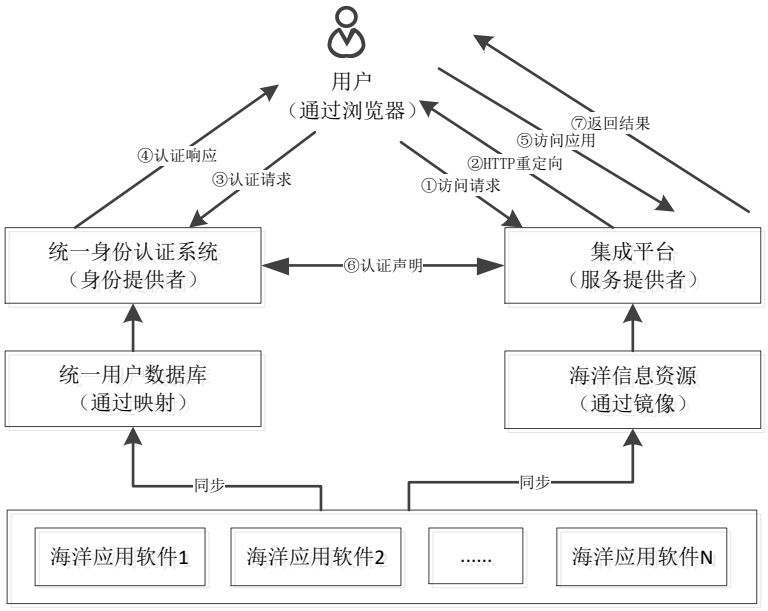

图1 统一身份认证技术流程

5 组织机构信息管理

海洋应用软件集成统一身份认证应构建完整、统一、可信的组织机构信息库，满足以下要求：

a) 组织机构应包括各级海洋主管部门、各级海洋事业单位、涉海部门和单位；
b) 采用统一社会信用代码作为组织机构的标识码；
c) 统一身份认证系统应提供组织机构信息访问接口；
d) 统一身份认证系统应提供对组织机构信息更新、变更或注销的操作界面及访问接口；

e) 组织机构注册应包含如表 1 所示的注册信息。

表1 组织机构注册信息表

序号	组织机构注册信息	说明
1	单位ID	数字，长度为6，系统自动生成
2	单位名称	字符串，长度为60
3	单位名称拼音首字母	字符串，长度为30
4	统一社会信用代码	字符串，长度为18
5	单位性质	字符串，长度为8。政府机关、事业单位、科研院所、高等院校、企业、其它
6	单位简称	字符串，长度为20
7	单位地址	字符串，长度为100
8	邮政编码	字符串，长度为6
9	办公电话	字符串，长度为12
10	传真	字符串，长度为12
11	E-Mail地址	字符串，长度为50
12	网站地址	字符串，长度为200。如有多个网站，可依次列出，中间用“;”分隔
13	机构状态	字符串，长度为4。正常、删除、注销
14	备注	字符串，长度为2000

6 用户管理

6.1 用户信息

海洋应用软件集成统一身份认证应构建完整、统一、可信的用户数据库保存用户信息，应包含如表2所示的基本内容。

表2 用户基本信息表

序号	用户注册信息	说明
1	用户ID	数字，长度为8，系统自动生成
2	登录名	字符串，长度为20
3	中文名	字符串，长度为20
4	中文名拼音字母	字符串，长度为50
5	身份证号码	字符串，长度为18位
6	性别	字符串，长度为4
7	手机号	字符串，长度为11
8	办公电话	字符串，长度为12
9	通讯地址	字符串，长度为200
10	E-Mail地址	字符串，长度为50
11	职称级别	字符串，长度为6。院士、正高级、副高级、中级、初级、其他
12	职务级别	字符串，长度为4。部级、厅级、处级、科级、其他

序号	用户注册信息	说明
13	是否接收短信	数字，长度为1。1是、2否
14	备注	字符串，长度为2000

用户与组织机构为一对多的对应关系，采用表 3 进行关联。

表3　用户单位信息关联表

序号	用户注册信息	说明
1	记录顺序号	数字，长度为9，系统自动生成
2	用户ID	数字，长度为8，系统自动生成
3	单位ID	数字，长度为6，系统自动生成
4	职务名称	字符串，长度为20
5	从事本职工作时间（年）	数字，长度为4
6	在职情况	字符串，长度为4。在职、借调、离职
7	到职日期	短日期格式
8	离职日期	短日期格式
9	记录添加时间	长日期格式
10	记录修改时间戳	长日期格式

6.2　用户注册

用户注册具体要求如下：

a） 应提供用户注册的操作界面及与其它海洋应用软件的用户注册同步接口；
b） 应提供用户进行实名认证的界面和接口；
c） 应保留用户的历史注册记录。

6.3　用户审核

用户审核具体要求如下：

a） 应提供用户审核的操作界面；
b） 宜采用分级审核制度，各海洋应用软件管理员审核本应用软件的用户，平台管理员审核各应用软件管理员，通过审核后才能成为集成平台正式用户；
c） 应保留历史的用户审核记录。

6.4　用户信息管理

用户信息管理具体要求如下：

a) 应提供用户信息管理的操作界面及与其它海洋应用软件的用户信息管理同步接口；
b) 宜采用分级用户信息管理制度，各海洋应用软件管理员对本应用软件用户进行管理，平台管理员对各应用软件管理员进行管理；
c) 应保留历史的用户信息管理记录。

6.5　用户注销

用户注销具体要求如下：

a） 应提供用户注销的操作界面及与其它海洋应用软件的用户注销同步接口；
b） 宜采用分级用户注销制度，各海洋应用软件管理员对本应用软件用户进行注销操作，平台管理员对各应用软件管理员进行注销操作；
c） 应保留历史的用户注销记录。

6.6 用户日志

应对用户各类操作过程进行日志记录，具体要求如下：

a) 应对注册、审核、管理、注销过程进行日志记录，包括用户名、IP 地址、操作时间、操作方式；
b) 应对用户登入/登出过程进行日志记录，包括用户名、IP 地址、操作时间、登入/登出方式、关联应用软件；
c) 应对用户操作过程进行日志记录，包括用户名、IP 地址、操作时间、操作类型、操作方式、关联应用软件、操作结果；
d) 应实现用户日志统计分析功能。

7 权限管理

7.1 角色设置

7.1.1 平台管理员

平台管理员的职责如下：

a） 管理各海洋应用软件管理员；
b） 管理集成平台的用户和用户分组；
c） 设置用户对集成平台的访问权限。

7.1.2 应用软件管理员

应用软件管理员的职责如下：

a） 管理本应用软件的用户和用户分组；
b） 设置用户对本应用软件的访问权限。

7.1.3 日志审计员

日志审计员的职责如下：

a） 负责日志的备份；
b） 对 6.6 条中各类日志信息进行全面审计；
c） 对日志进行分析，为平台故障处理、安全事故追责等工作提供客观依据。

7.2 权限分配

权限分配的要求如下：

a） 集成平台中注册的各类海洋信息资源，在为其它应用软件及用户提供资源服务时，访问权限应由资源发布人或委托授权人管理，并通过统一身份认证系统进行权限分配；
b） 应用软件的访问权限应由各应用软件管理员分配；
c） 集成平台的功能权限应由平台管理员分配。

7.3 群组管理

群组管理的要求如下：

a） 采用群组策略管理用户，宜按照业务领域或业务单位（部门）划分群组，每个群组对应若干授权访问的应用软件或信息资源；
b） 同一个群组中，宜根据需要设置多种角色，对资源的具体操作权限由用户角色决定；
c） 用户与角色、用户与群组宜为一对多对应关系。

8 统一身份认证的实现方式

8.1 统一身份认证系统

海洋应用软件集成应构建具有单点登录功能的统一身份认证系统，应对所有纳入整合集成的应用软件开展统一身份标识与访问权限控制。

海洋应用软件可以分为三类不同登录类型，一是基于 CAS 协议的系统登录，二是基于 SAML 协议的系统登录，三是映射类系统登录。为适应应用软件现状的差异性，统一身份认证系统应适配三种不同类型的系统登录，供应用软件配置选择。图 2 是基于单点登录技术的统一身份认证系统，服务功能及流程如下：

a) 集成平台登入。用户通过集成平台账号和密码完成身份认证，登入集成平台后，用户能够访问平台的功能模块及集成并授权的应用软件；
b) CAS单点登入。在应用集成内，采用CAS协议登录的应用软件，应选用CAS单点登入方式完成用户身份认证，实现系统登入，如图2中的应用软件1；
c) SAML单点登入。在应用集成内，采用SAML协议登录的应用软件，应选用SAML单点登入方式完成用户身份认证，实现系统登入，如图2中的地理信息门户；
d) 映射类单点登入。对于没有实现单点登录的应用软件，应选用映射类单点登入方式完成用户身份认证，实现系统登入，如图2中的应用软件2、3、4；
e) 系统登出。用户进行登出操作或连接超时。

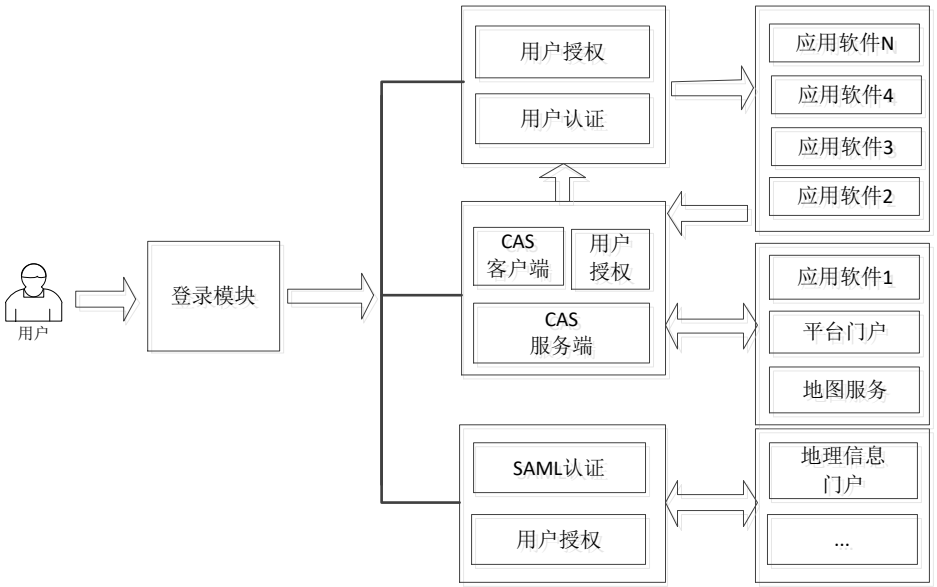

图2 基于单点登录技术的统一身份认证系统

8.2 身份认证接口

身份认证接口应包括获取公钥串接口、用户单点登录和用户单点登出接口，如表 4 所示。

表4 身份认证接口

接口名称	实现功能	返回
获取公钥串接口	获取身份认证公钥串	公钥和模
用户单点登录接口	弹出登录页，输入用户名、密码后登录应用软件	登录成功后跳转至登录前请求的页面
用户单点登出接口	单点登出后，访问集成平台里的任何应用软件都需要重新登录	显示退出成功的页面

8.3 海洋应用软件接入

海洋应用软件通过集成平台提供的统一身份认证系统及服务接口实现集成，遵守以下要求：

a) 海洋应用软件应支持基于CAS协议或基于SAML协议的单点登录；
b) 海洋应用软件应支持不同域内多个系统间的单点登录；
c) 海洋应用软件宜采用两种方式实现单点登录：调用集成平台统一认证界面或改造原登录界面后台调用统一身份认证接口；
d) 海洋应用软件应支持单点登录的安全退出。

参 考 文 献

[1] GB/T 25064-2010 信息安全技术 公钥基础设施 电子签名格式规范
[2] GB/T 31072-2014 科技平台 统一身份认证
[3] GA 397.2-2002 经济犯罪案件管理信息系统技术规范 第2部分:角色分类及权限
[4] GA 464-2004 治安管理信息系统用户访问控制及权限管理