# 密改说明

## 网络和通信改造

按5个大系统（生态环境监测应用系统、生态环境数据应用系统、生态环境业务应用系统、生态环境服务应用系统、生态环境管理应用系统）统一申请国家政务CA RSA2048算法的SSL证书，各子系统配置SSL证书并开通对应网络的访问策略。已有SSL证书的，如果不是自签发的可以不改。

**注：**

1）根据一期的经验，大数据平台配置SSL协议后，各业务系统单点登录策略需做调整。（如果二级系统的子模块单点策略一样，也需要调整）。由于需要通过安全认证网关代理访问大数据平台，代理后的地址也需要调整单点登录策略，代理后的地址为<https://172.20.234.111:8081/1a2b3c/portal/> ，大数据平台获取系统上下文的代码也要做修改，不能使用截取的方式。

2）登录完成后选择系统跳转时需判断访问协议，如上级模块使用SSL协议访问，跳转时也应使用SSL协议。（此处是为了保留现有业务通道，确保业务连续性）

3）APP、小程序等需调用服务端SSL协议接口。

4）开放端口自行联系政务云开通，配置完成后反馈给上级系统

## 设备和计算改造

申请了三台浪潮政务云节点的堡垒机，分别管控互联网域、公共服务域、行政服务域的服务器。若哪个系统需要使用堡垒机运维，需协调浪潮开通对应VPN账号访问该堡垒机的权限。

联通云和计算中心云需要向相关的云服务商申请密码资源。

## 应用和数据改造

应用和数据层的改造包括三个部分，身份鉴别（即用户登录）、重要数据存储机密性和完整性，重要数据传输机密性和完整性

 **1、身份鉴别**

 PC端需支持Key登录和用户名+口令+短信验证码登录两种方式。根据调研，PC端都对接了大数据平台，因此大数据平台做登录改造即可。大数据平台已完成Key登录改造，本期改造用户名+口令+短信验证码登录即可。

 APP、小程序需要支持用户名+口令+短信验证码登录。厅里的APP大多对接了山东智慧环保APP、爱山东、山东通，对接了山东智慧环保APP的，由山东智慧环保APP统一改造登录即可；对接了爱山东、山东通的APP、小程序可不改造登录，等爱山东、山东通改造即可。

 身份鉴别的改造包括两个方面：**登录模块、用户管理模块**

 1）**登录模块的改造包括三个方面：**

1）增加用户名+口令+短信验证码登录入口（验证用户口令后，向用户预留手机号发短信验证码）

2）登录过程中，调用密码服务平台HMAC接口验证用户口令

3）登录成功后，调用HMAC接口验证当前用户权限完整性（跳转到各业务系统获取用户权限时也需要验证用户权限完整性）

 2）**用户管理模块：**

1）用户表增加口令HMAC和SM4密文字段，用户权限表增加HMAC字段

2）修改用户口令调用HMAC和SM4接口进行加密

3）修改用户权限时按规则组合后调用HMAC进行加密

 **2、重要数存储机密性完整性**

 按密评要求，重要数据包括数据安全分类分级中的重要数据、敏感数据和鉴别数据。生态环境厅业务数据基本为一般数据，本次只对敏感数据、鉴别数据进行处理，根据反馈厅里的敏感数据包括手机号、身份证号、统一社会信用代码、车牌号。鉴别数据包括用户口令、权限。

 1）业务表增加敏感数据的HMAC完整性和SM4机密性字段

 2）新增、修改业务数据时调用HMAC和SM4接口加密

 **3、重要数据传输机密性完整性**

通过SSL协议来降低本项风险。

 **4、其他要求**

1）所有系统的登出功能应跳转回大数据平台的登录页，如不好修改，建议隐藏登出功能



2）显示登录人与实际登录信息不符的，建议隐藏显示登录人





3）存储身份证照片的系统，应将照片加水印

