某局点S6850 ssh RSA公钥方式登入设备失败问题

SSH　胡晓东　2020-02-28 发表

组网及说明

现场业务场景是pc，通过SCRT创建public-key，由于登入设备无法根据**display public-key local public**命令去显示公钥，现场只能直接将key.pub文件打开，然后再通过手工输入的，这种方式登录失败。

问题描述

某局点想利用公钥认证的方式进行SSH登录，根据业务场景，服务器端的设备需要通过手工配置的方式来导入客户端的公钥。该局点在导入过程中，出现导入失败，以及导入后无法正常登录的故障现象。

过程分析

手工输入的主机格式必须满足一定的格式要求，发现是输入的主机公钥编码格式不对。手工方式仅支持DER编码（16进制字符串），现场打开的pub.key不是DER格式。

解决方法

解决方法：

1. 在支持传文件的设备A上以文件方式导入，然后display出来，以display的16进制字符串导入不支持传文件的设备B。
2. 公钥在设备间传递不会失真，也不存在随机字符。我司设备的内部实现是一致的，涉及密钥格式转化的逻辑也很少改动，不用担心公钥和最初的文件发生变化。