SAML logon stops working after making some changes to PKI

- Parallels Remote Application Server

Symptoms

SAML logon stops working after making some changes to PKI infrastructure (e.g., updating a certificate of CA being used)

Users get error **The user name or password is incorrect**:

Windows **Security** log on RDSH contains corresponding events with ID **4625**, status **0xC0000006D** and Sub Status **0xC000038A**:

Cause

Sub Status **0xC000038A** means that an untrusted certificate authority was detected while processing the smart card certificate that is used for authentication:
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-erref/596a1078-e883-4972-9bbc-49e60bebca55

However, you can see that CA certificate chain is fully trusted when checking properties of the user certificate being used for SAML logon.

The information about CA certificates is cached in the OS and is still used for user certificate validation.

Resolution

Execute this command under admin account on all affected RDS hosts:

```
certutil –urlcache * delete
```