Preauth module pkinit (17) (real) returned: -1765328307/Inconsistent key purpose

- Parallels Secure Workspace

Symptoms

First see How to analyze the log files to identify single-sign on (SSO) issues .

Single sign-on fails. In **awingu-worker-smc.service.log**, a similar error can be seen:

```
2021-12-13 08:52:20.908884 awnode01 awingu-worker-smc.service[python3:891]:
Generating a RSA private key
2021-12-13 08:52:20.987952 awnode01 awingu-worker-smc.service[python3:891]:
.....................................................+++++
2021-12-13 08:52:21.069409 awnode01 awingu-worker-smc.service[python3:891]:
.....................................................+++++
2021-12-13 08:52:21.069647 awnode01 awingu-worker-smc.service[python3:891]:
writing new private key to 'private_key.pem'
2021-12-13 08:52:21.069775 awnode01 awingu-worker-smc.service[python3:891]:
-----
2021-12-13 08:52:21.134823 awnode01 awingu-worker-smc.service[python3:891]:
writing RSA key
2021-12-13 08:52:21.622454 awnode01
awingu-worker-smc.service[manage.py:1995]: Password for
someuser\@SOMEDOMAIN.ORG@SOMEDOMAIN.ORG:

2021-12-13 08:52:21.623175 awnode01
awingu-worker-smc.service[manage.py:1995]: Using specified cache:
/etc/awingu/domains/SOMEAWINGUDOMAIN/5ffa26d4-cb79-45a5-a30f-b1e9c43c6f50/kerberos/k
Using principal: someuser\@SOMEDOMAIN.ORG@SOMEDOMAIN.ORG
PA Option X509_user_identity =
FILE:/etc/awingu/domains/SOMEAWINGUDOMAIN/5ffa26d4-cb79-45a5-a30f-b1e9c43c6f50/certi
[8062] 1639385541.497992: Getting initial credentials for
someuser\@SOMEDOMAIN.ORG@SOMEDOMAIN.ORG
[8062] 1639385541.497994: Sending unauthenticated request
[8062] 1639385541.497995: Sending request (210 bytes) to SOMEDOMAIN.ORG
[8062] 1639385541.497996: Resolving hostname dc01.SOMEDOMAIN.ORG
[8062] 1639385541.497997: Sending initial UDP request to dgram 10.1.2.3:88
[8062] 1639385541.497998: Received answer (197 bytes) from dgram 10.1.2.3:88
[8062] 1639385541.497999: Sending DNS URI query for _kerberos.SOMEDOMAIN.ORG.
[8062] 1639385541.498000: No URI records found
[8062] 1639385541.498001: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[8062] 1639385541.498002: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[8062] 1639385541.498003: No SRV records found
[8062] 1639385541.498004: Response was not from master KDC
[8062] 1639385541.498005: Received error from KDC: -1765328359/Additional
pre-authentication required
[8062] 1639385541.498008: Preauthenticating using KDC method data
```

```
[8062] 1639385541.498009: Processing preauth types: PA-PK-AS-REQ (16),
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[8062] 1639385541.498010: Selected etype info: etype aes256-cts, salt
"SOMEDOMAIN.ORGsomeuser", params ""
[8062] 1639385541.498011: PKINIT loading CA certs and CRLs from FILE
[8062] 1639385541.498012: PKINIT client computed kdc-req-body checksum
9/36558379DAE15AC1C60E0616AB3B877DE76B60C6
[8062] 1639385541.498014: PKINIT client making DH request
[8062] 1639385541.498015: Preauth module pkinit (16) (real) returned:
0/Success
[8062] 1639385541.498016: Produced preauth for next request: PA-PK-AS-REQ
(16)
[8062] 1639385541.498017: Sending request (4793 bytes) to SOMEDOMAIN.ORG
[8062] 1639385541.498018: Resolving hostname dc01.SOMEDOMAIN.ORG
[8062] 1639385541.498019: Initiating TCP connection to stream 10.1.2.3:88
[8062] 1639385541.498020: Sending TCP request to stream 10.1.2.3:88
[8062] 1639385541.498021: Received answer (4126 bytes) from stream
10.1.2.3:88
[8062] 1639385541.498022: Terminating TCP connection to stream 10.1.2.3:88
[8062] 1639385541.498023: Sending DNS URI query for _kerberos.SOMEDOMAIN.ORG.
[8062] 1639385541.498024: No URI records found
[8062] 1639385541.498025: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[8062] 1639385541.498026: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[8062] 1639385541.498027: No SRV records found
[8062] 1639385541.498028: Response was not from master KDC
[8062] 1639385541.498029: Processing preauth types: PA-PK-AS-REP (17)
[8062] 1639385541.498030: PKINIT client verified DH reply
[8062] 1639385541.498031: PKINIT client config accepts KDC dNSName SAN
dc01.SOMEDOMAIN.ORG
[8062] 1639385541.498032: PKINIT client found dNSName SAN in KDC cert:
DC01.SOMEDOMAIN.ORG
[8062] 1639385541.498033: PKINIT client matched KDC hostname
DC01.SOMEDOMAIN.ORG against dNSName SAN; EKU check still required
[8062] 1639385541.498034: PKINIT client found no acceptable EKU in KDC cert
[8062] 1639385541.498035: Preauth module pkinit (17) (real) returned:
-1765328307/Inconsistent key purpose
[8062] 1639385541.498036: Produced preauth for next request: (empty)
[8062] 1639385541.498037: Getting AS key, salt "SOMEDOMAIN.ORGsomeuser",
params ""
kinit: Cannot read password while getting initial credentials
```

On the domain controller against which the authentication was attempted: You may see this event in the Windows Event Viewer:

```
Event ID 32
The Key Distribution Center (KDC) uses a certificate without KDC Extended Key
Usage (EKU) which can result in authentication failures for device
certificate logon and smart card logon from non-domain-joined devices.
Enrollment of a KDC certificate with KDC EKU (Kerberos Authentication
template) is required to remove this warning.
```

Cause

The certificate for this particular Kerberos Domain Controller (KDC) does not contain "KDC Authentication" as an intended purpose.

Note: There may be a certificate that shows "<All>" as the intended purpose. However, the certificate may still be missing some extended properties which enable KDC Authentication.

Resolution

Reissue the KDC Authentication certificate for all Kerberos Domain Controllers (see procedures for customers). Note: if there were other certificates being used by the KDCs, it may be necessary to restart the "Kerberos Key Distribution Center" service on the Microsoft Windows Server to make sure the Kerberos service uses the new certificate.

See Reissue KDC Authentication certificate for domain controllers

---