RDP-Dateien unter Ubuntu signieren

Erstellt mit Unterstützung von ChatGPT

Allgemein

Ich nutzte diese Lösung um unter Ubuntu RDP-Dateien zu signieren.

1. Pakete auf Ubuntu installieren

```
sudo apt update && sudo apt install -y openssl curl python3
```

Das Linux-Tool installieren:

```
sudo curl -L https://raw.githubusercontent.com/nfedera/rdpsign/master/rdpsign.py -o
/usr/local/bin/rdpsign && sudo chmod +x /usr/local/bin/rdpsign
```

Das Tool nutzt laut README Python und OpenSSL; der Beispielaufruf ist `rdpsign test.rdp test-signed.rdp signer.crt -k signer.key`.

2. Verzeichnisstruktur erstellen

```
sudo mkdir -p /opt/rdp-ca/{private,certs,csr,out}
sudo chmod 700 /opt/rdp-ca/private
cd /opt/rdp-ca
```

3. OpenSSL-Konfiguration für Root-CA erstellen

```
sudo tee /opt/rdp-ca/root-ca.cnf >/dev/null <<'EOF'
[ req ]
```

```
default_bits = 4096
prompt = no
default_md = sha256
distinguished_name = dn
x509_extensions = v3_ca

[ dn ]
C = DE
O = RDP Secure Access
CN = RDP Secure Access Root CA

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, keyCertSign, cRLSign
EOF
```

4. Root-CA mit 10 Jahren Laufzeit erstellen

```
sudo openssl genrsa -out /opt/rdp-ca/private/rdp-secure-access-root-ca.key 4096
```

```
sudo openssl req -x509 -new -nodes -key /opt/rdp-ca/private/rdp-secure-access-root-ca.key -sha256 -days 3650 -out /opt/rdp-ca/certs/RDP-Secure-Access-Root-CA.cer -config /opt/rdp-ca/root-ca.cnf
```

Die Datei, die du später den Windows-Usern gibst, ist:

```
/opt/rdp-ca/certs/RDP-Secure-Access-Root-CA.cer
```

Der private Key bleibt geheim:

```
/opt/rdp-ca/private/rdp-secure-access-root-ca.key
```

---

5. Konfiguration für das RDP-Signing-Zertifikat erstellen

Der sichtbare Name im Windows-Dialog kommt aus dem Zertifikat, daher setze ich hier:

```
CN = RDP Secure Access
```

```
sudo tee /opt/rdp-ca/rdp-signer.cnf >/dev/null <<'EOF'
[ req ]
default_bits = 4096
prompt = no
default_md = sha256
distinguished_name = dn
req_extensions = v3_req

[ dn ]
C = DE
O = RDP Secure Access
CN = RDP Secure Access

[ v3_req ]
basicConstraints = critical, CA:false
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, codeSigning
subjectKeyIdentifier = hash
EOF
```

Ein Code-Signing-EKU ist hier wichtig; mehrere aktuelle Anleitungen und Fehlerberichte weisen darauf hin, dass ein normales TLS-Zertifikat für `.rdp`-Dateisignatur nicht ausreicht und Code Signing als EKU benötigt wird.

---

6. RDP-Signing-Zertifikat mit 10 Jahren erstellen

```
sudo openssl genrsa -out /opt/rdp-ca/private/rdp-secure-access-signer.key 4096
```

```
sudo openssl req -new -key /opt/rdp-ca/private/rdp-secure-access-signer.key -out /opt/rdp-ca/csr/rdp-secure-access-signer.csr -config /opt/rdp-ca/rdp-signer.cnf
```

```
sudo openssl x509 -req -in /opt/rdp-ca/csr/rdp-secure-access-signer.csr -CA /opt/rdp-ca/certs/RDP-Secure-Access-Root-CA.cer -CAkey /opt/rdp-ca/private/rdp-secure-access-root-ca.key -CAcreateserial -out /opt/rdp-ca/certs/RDP-Secure-Access-Signer.cer -days 3650 -sha256 -extfile /opt/rdp-ca/rdp-signer.cnf -extensions v3_req
```

---

7. Thumbprint für Registry-Datei ermitteln

Windows braucht den **SHA1-Thumbprint des Signer-Zertifikats**, nicht den Thumbprint der Root-CA.

```
openssl x509 -in /opt/rdp-ca/certs/RDP-Secure-Access-Signer.cer -noout -fingerprint -sha1 | cut -d= -f2 | tr -d ':'
```

Beispielausgabe:

```
A1B2C3D4E5F60718293A4B5C6D7E8F9012345678
```

Diesen Wert brauchst du gleich in der `.reg`.

Microsofts Policy heißt **„Specify SHA1 thumbprints of certificates representing trusted .rdp publishers“**. Wenn ein `.rdp`-File mit einem Zertifikat signiert ist, dessen SHA1-Thumbprint in dieser Liste steht, soll der Benutzer beim Start keine Warnmeldung bekommen.

---

8. Beispiel-Registry-Datei für Windows-Clients

Auf Ubuntu erzeugen:

```
SIGNER_THUMBPRINT="$(openssl x509 -in /opt/rdp-ca/certs/RDP-Secure-Access-Signer.cer -noout -fingerprint -sha1 | cut -d= -f2 | tr -d ':')"
```

```
sudo tee /opt/rdp-ca/out/RDP-Secure-Access-Client-Trust.reg >/dev/null <<EOF
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services]
"AllowSignedFiles"=dword:00000001
"TrustedCertThumbprints"="$SIGNER_THUMBPRINT"
EOF
```

Die fertige Datei liegt dann hier:

```
/opt/rdp-ca/out/RDP-Secure-Access-Client-Trust.reg
```

Diese `.reg` muss auf dem Windows-Client **als Administrator** importiert werden.

Zusätzlich muss die Root-CA auf dem Client installiert werden:

```
RDP-Secure-Access-Root-CA.cer
→ Lokaler Computer
→ Vertrauenswürdige Stammzertifizierungsstellen
```

Optional kannst du auch das öffentliche Signer-Zertifikat mitgeben:

```
RDP-Secure-Access-Signer.cer
→ Lokaler Computer
→ Vertrauenswürdige Herausgeber
```

Der zentrale Punkt bleibt aber: Root-CA vertraut + Signer-Thumbprint in `TrustedCertThumbprints`.

---

9. Eine RDP-Datei auf Ubuntu signieren

Beispiel:

```
cp /pfad/zur/original.rdp /opt/rdp-ca/out/test.rdp
```

Signieren:

```
rdpsign /opt/rdp-ca/out/test.rdp /opt/rdp-ca/out/test-signed.rdp /opt/rdp-ca/certs/RDP-Secure-Access-Signer.cer -k /opt/rdp-ca/private/rdp-secure-access-signer.key
```

Danach gibst du dem Benutzer nur noch:

```
test-signed.rdp
```

Nicht mehr die unsignierte Datei.

---

10. Wichtig: Datei nach dem Signieren nicht mehr verändern

Nach dem Signieren darfst du die `.rdp`-Datei nicht mehr ändern. Auch kleine Änderungen wie Zielhost, Username, Gateway, Drucker-Redirect oder Clipboard-Redirect machen die Signatur ungültig.

Ablauf also immer:

```
1. .rdp vollständig erzeugen
2. .rdp signieren
3. signierte .rdp ausliefern
```

---

11. Dateien, die du den Windows-Usern bereitstellst

Minimal:

```
RDP-Secure-Access-Root-CA.cer
RDP-Secure-Access-Client-Trust.reg
```

Optional zusätzlich:

```
RDP-Secure-Access-Signer.cer
```

Die privaten Keys bleiben ausschließlich auf dem Server:

```
/opt/rdp-ca/private/rdp-secure-access-root-ca.key
/opt/rdp-ca/private/rdp-secure-access-signer.key
```

Diese Dateien niemals an Kunden geben.

---

12. Auf einem Windows-Client installieren

```
certutil -addstore -f Root "RDP-Secure-Access-Root-CA.cer"
certutil -addstore -f TrustedPublisher "RDP-Secure-Access-Signer.cer"
reg import "RDP-Secure-Access-Trust.reg"
```

13. Test auf einem Windows-Client

Nach Import von Zertifikat und `.reg`:

```
gpupdate /force
```

Dann `mstsc.exe` vollständig schließen und die signierte `.rdp` öffnen.

Wenn alles passt, sollte als Herausgeber erscheinen:

```
RDP Secure Access
```

Und die wiederkehrenden Warnungen für die signierte `.rdp`-Datei sollten verschwinden beziehungsweise die in der `.rdp` gesetzten Umleitungen wie Zwischenablage und Drucker sollten wieder greifen. Microsofts offizielles `rdpsign.exe` überschreibt beim Signieren die Eingabedatei; das Linux-Tool erzeugt stattdessen eine separate Ausgabedatei.

Revision #10
Created 17 May 2026 08:59:09 by Stefan Kittel
Updated 17 May 2026 09:33:33 by Stefan Kittel