RDP Certificate

On target server

```
;----------------- request.inf -----------------

[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "C=US, CN=something.example.com"

KeySpec = 1
KeyLength = 2048
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
HashAlgorithm = SHA256

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication / Token Signing
;-----------------------------------------------
```

In the `Subject` line, replace `US` by your country and `something.example.com` by your domain and subdomain name.

Save it somewhere on target server as `request.inf` then run:

```
certreq -new request.inf request.csr
```

This command may not exist on non-server versions of Windows.

Go to Gandi.net

- Log in
- Open *SSL Certificates* section
- Select a *Standard* certificate
- Choose to host it *elsewhere* (**not** on a *Gandi Simple Hosting Instance*)
- Confirm you want a *Standard* certificate and only for a single address.

- Copy the **content** of the `request.csr` file from your server into the form. Check that your domain name appears in the *Common name* box.
- Pay
- Confirm you own the domain (could take a few minutes)
    - Either by clicking a link in an email received on *admin@yourdomain*
    - Or with a DNS record to add (**take more time**)
- Download your certificate

Back on server

Save the certificate next to the two other files, then run:

```
certreq -accept yourdomain.crt
```

Open *Computer Certificates* and looks for your domain in *Personal*. Right click it and choose *Manage private keys*, then give **read** permission to *NETWORK SERVICE*.

Open your certificate and in the *Details* tab look at its thumbprint.

In the registry, go to:

```
HKLM\System\CurrentControlSet\Control\Terminal Server\Winstations\RDP-Tcp
```

Create a new binary value named `SSLCertificateSHA1Hash` and set the thumbprint as value.

Restart the *Remote Desktop* service or reboot the server.

If it doesn't work

None of these steps should be required.

Exportable key

- Open *Computer Certificates* and looks for your domain in *Personal*
- Right click it and choose *Export*
- Choose to export the private key
- Select the *PFX* format and check *Export all extended properties*
- Delete your certificate then import it again:
    - Select the *Personal* store
    - Mark the key as exportable
- Give **read** permission to *NETWORK SERVICE* as explained above

Folder permissions

Before doing this, check you properly gave **read** permission to *NETWORK SERVICE* as explained above. It's probably a **bad idea** to do this step.

Check permissions of this folder:

```
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```

Administrators should have *Full control*.

Install on another server

If another server is reachable at the same domain but another port, it will be able to use the same certificate.

Just export the *PFX* file as explained above but import it (you shouldn't have to mark it as *exportable*) on the other server.

Then set the registry key and you should be done.