

## Guide to Creating Certificate for RDS

This document aims to act as a guide to creating a proper certificate for RDS. Microsoft RDS Certificates need to be created with certain names or it simply doesn't work. RDS has 2 locations that need to have certificates. 1 on the broker and 1 on the web/gateway. It's easier to create and manage with just 1 certificate rather than 2.

### Certificate Requirements:

#### Name:

Per Microsoft documentation: For 5 or less in the RDS farm you can go with

For 6 or more in the Farm (it's better to use a wildcard)

Name:

Web/Gateway frontend url fqdn (alias to server name like rdweb.domain.com)

web/gateway Server fqdn

web/Gateway Server fqdn (if you need it)

Broker fqdn

Session1 host fqdn

Session1 host fqdn

*If you are using a high availability broker that will also need an alias created from the teamed machines.*

### Subject Alternative Name (Should/must match Name)

Copy Exactly as the name field:

See example below of a custom certificate request from Windows.:

#### Under the Subject Tab

The user or computer that is receiving the certificate

Subject name:

Type: Common name	Add >	CN=rdweb.domain.com
Value:	< Remove	CN=webgateway1.domain.
		CN=webgateway2.domain.
		CN=rdsbroker.domain.com
		CN=sessionhost1.domain.c
		CN=sessionhost2.domain.r

Alternative name:

Type: DNS	Add >	DNS
Value:	< Remove	rdweb.domain.com
		webgateway1.domain.com
		webgateway2.domain.com
		rdsbroker.domain.com
		sessionhost1.domain.com
		sessionhost2.domain.com

Below is an example of one using a wild card with a high availability broker. Rds.domain.com is the alias.

The user or computer that is receiving the certificate

Subject name:

Type:  
Common name

Add >

< Remove

Value:

Value:

Alternative name:

Type:  
DNS

Add >

< Remove

Value:

Value:

CN=rdweb.domain.com  
CN=\*.domain.com  
CN=rds.domain.com

DNS  
rdweb.domain.com  
\*.domain.com  
rds.domain.com

### Under the Extensions Tab

Certificate Key Usage should be Digital Signature and Key Encipherment

Key usage

The key usage extension describes the purpose of a certificate.

Available options:

CRL signing  
Data encipherment  
Decipher only  
Encipher only  
Key agreement  
Key certificate signing  
Non repudiation

Add >

< Remove

Selected options:

Digital signature  
Key encipherment

☒ Make these key usages critical

Extended Key Usage should be Server Authentication

Extended Key Usage (application policies)

An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Available options:

Client Authentication  
Code Signing  
Secure Email  
Time Stamping  
Microsoft Trust List Signing  
Microsoft Time Stamping

Add >

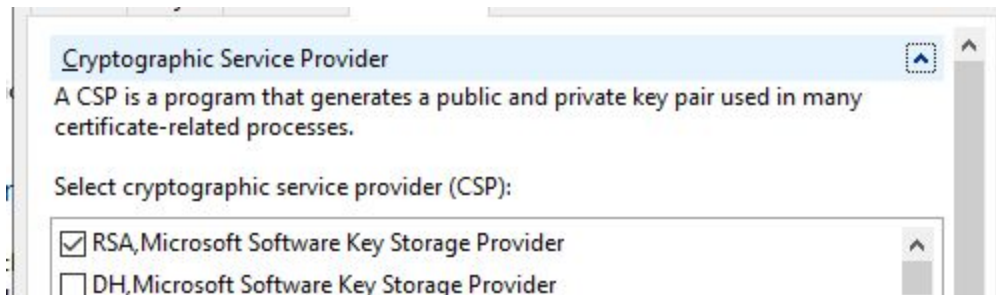
< Remove

Selected options:

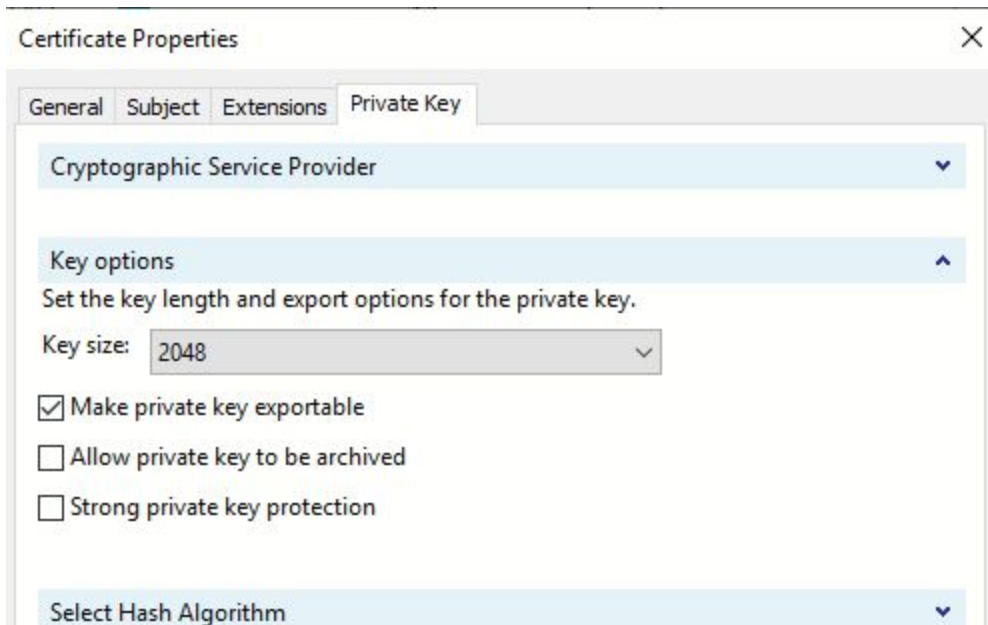
Server Authentication

### Under the Private Key Tab

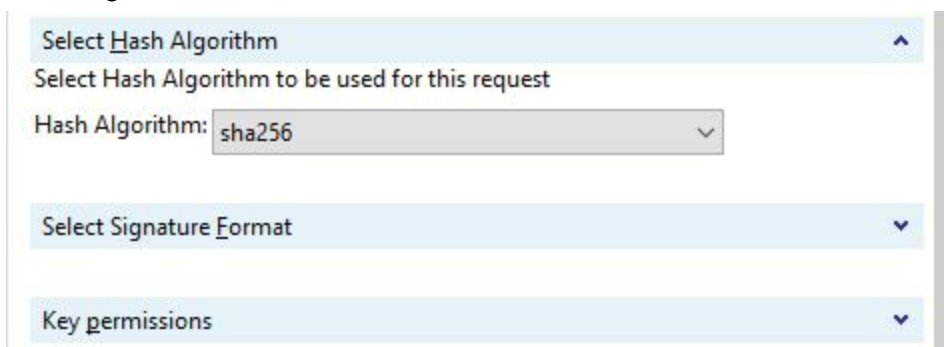
Cryptographic Service Provider should be Microsoft's most modern one:  
RSA Microsoft Software Key Storage Provider



Key length should be a Minimum of 2048 and make the key exportable



Hash Algorithm should be Sha256



When getting the key install it onto your system.  
Run MMC.exe and add certificates, Select Computer Account  
Locate the certificate under Personal and copy the serial number.

Open command prompt and run the following to get your certificate's private key:  
Certutil -repair my "serial number"  
Export this to a .pfx for Use for RDS.