SMP8634 Certificate Request Form

Please fill **ONE** form per certificate. All fields are required. For assistance in filling out the form please see the instructions on page 2 of this form.

(•) Development Key Domain[a] ( ) Production Key Domain[a] Date[b]

Contact Information

First Name[c]

Last Name[c]

Company Name

Phone

Fax

Email[d]

Product Information

Enter PGP Fingerprint[e]

Select Certificate Type[f]

Select Session Key Encryption[g]

Enter Certificate Public Key[h]
(PEM Format)
RSA 2048 bit

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1LMbT33Mz29elVjyCtbm
9y0sc57y+oVdETeakc4c0pYRhZTIxlLflXMfqHDMN6mI6F36Dg7andbddgy+gpxA
AODmFWjj9IcHFHYIlA8YiydmIx4QmdH/pArB8w9mC9LDSWvsZUxfUmcySxPjSxO0
o4oFOvOcNbH7Q0lxIn00xN37NL9j1cQUwDY+pt8//7F47vJ0y1PXx2hCGAmgb2wD
67i589t/ljGfHqhATsh6JW5YjxT6MI8iePm1155rFNfmZVaohXdqeGe5eAEFIfgx
HxKJc/i+rQMdISfgT8xs1XMCFHlwNwUOcxz7J52afFQhF0vX3ytYapUTxB4jr7Uc
sQIDAQAB
-----END PUBLIC KEY-----
```

Submit by Email Print this Form

It is required that the completed form be both faxed **AND** emailed to Sigma Designs for the request to be processed.
Fax: +1 408 957 9741
Email: drmla@sdesigns.com

All the documents included in the kits and via support are covered by the Sigma Designs NDA.

The certificates are signed every Thursday. The signatures and keys are then posted on the developer website on Friday. The cut-off date is Tuesday noon PST. Pending verification of the public key and the PGP key, a certificate request received before Tuesday noon PST will be processed the same week.

Note: there will be a $300 administrative fee to generate lost certificates or to change a PGP key.

a **Development/Production Key Domain** The SMP8634 has a bonding option to choose between two sets of keys. The SDK boards include the development SMP8634-ES. The development versions are marked as SMP8634 -ES6 and the production versions are marked as SMP8634-RevA

b **Date** Date of the request.

c **Name** Name of the owner of the PGP key.

d **Email** Email address of the owner of the PGP key (must be contained in the PGP key).

e **PGP Fingerprint** Copy the PGP fingerprint (Hexadecimal).

f **Certificate Type** The choices for the certificate types are described in the table below:

0	**cpu Bootloader** zboot	CPU zone	Generates a certificate that can be used to authenticate the first bootloader of the CPU (zboot).
1	**cpu code,** used to sign cpu kernels and applications	CPU code	Generates a certificate that can be used to authenticate cpu code (consequent to the CPU bootloader).
2	**xtask1,** used to develop and release SDK DRM implementations	XPU zone	Generates a certificate that can be used to authenticate xpu code.
3	**video microcode,** used internally by Sigma Designs	Video RISC	Requests to generate type 3 certificate are rejected.
4	**audio microcode**used internally by Sigma Designs	Audio DSP	Requests to generate type 4 certificate are rejected.
5	**transport demux microcode,** used internally by Sigma Designs	Transport demux RISC	Requests to generate type 5 certificate are rejected.
6	**irq handler,** running on xpu, used internally by Sigma Designs	XPU zone	Requests to generate type 6 certificate are rejected.
7	**xtask2,** used for Sigma Designs DRM implementations	XPU zone	Generates a certificate that can be used to authenticate the xpu code. Reserved for Sigma Designs.
8	**xtask3,** XPU zone	XPU zone	Generates a certificate that can be used to authenticate the xpu code. Reserved for future use. No certificates are generated at this time using this type.
9	**xtask4,** XPU zone	XPU zone	Generates a certificate that can be used to authenticate the xpu code. No certificates are generated at this time using this type.
0xff	**xos update**	XPU zone	Generates a certificate that can be used to authenticate an xos update (xos is already signed by Sigma Designs).

g Session Key Encryption The choices for session key encryption are:

1. RSA Key Numbers 0-6: 7 RSA public keys are sent with your certificate. One of the RSA keys can be used to encrypt the session key. The xos knows the 7 correspondent private keys. The RSA decryption in the xos takes 2 seconds. This option is not recommended.
2. AES Key Numbers 0-6: 7 AES symmetric keys are sent with your certificate. One of the AES keys can be used to encrypt the session key. The xos knows these keys. This option is recommended.
3. No Encryption: The binary will not be encrypted with a session key.

Sigma Designs strongly recommends using AES0 if encryption is needed. The RSA session key encryption is strongly discouraged since it requires 2 additional seconds to process the RSA decryption operation during loading.

h Public Key Copy *pubkey.txt* into this field. The instructions to generate the keys are given below:

1. Generate a 2048-bit Public/Private key using openSSL (linux or Windows/Cygwin). Or, download openSSL for Windows from, http://www.slproweb.com/products/Win32OpenSSL.html.

To create a password-protected private key file, use the following command: $ openssl genrsa -aes128 -f4 -out key.pem 2048
When this command is executed, the program prompts for a pass phrase (password), which is used to encrypt the key file. You must enter the correct pass phrase to view the key.

2. Print the public key using the following command: $ openssl rsa -pubout < key.pem > pubkey.txt

When this command is executed, the program prompts for your pass phrase (password). Use notepad to open *pubkey.txt* and copy the public key.