SIGMA DESIGNS

SMP8634 Security
zboot2

Goals

- CPU bootloader (zboot2) is now digitally signed and optionally encrypted
- xos, starting with version Ma6, will enforce the verification of the digital signature
- OS kernel is also digitally signed and optionally encrypted
- zboot2, by using xos functions, will enforce the verification of the digital signature of the OS.
- The process does not require a secure manufacturing line

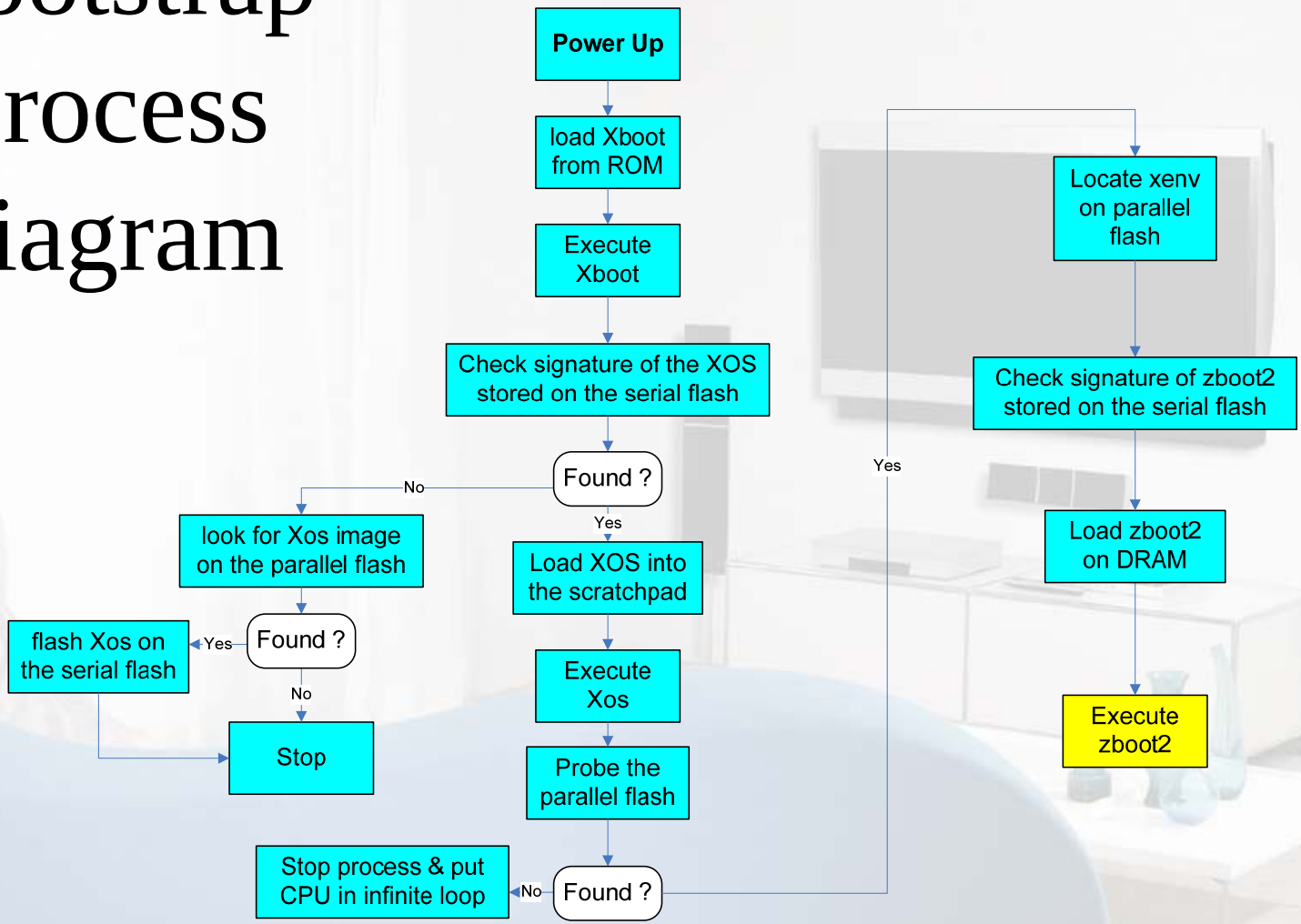
Development SDK

- The Development SDK (and development chips) will include facsimile keys for signing zboot2 and the OS
- Certificate 0xa will be used by default in the development kit to sign zboot2
- Certificate 0xb will be used by default in the development kit to sign OS

Production chips

- Sigma Designs will provide facsimile keys and certificates to sign production bootloaders and OS
- But we strongly recommend to request a certificate to be used in production
- Each customer will have to order its own certificates (one for the bootloader and one for the OS).

Bootstrap process diagram



Secure Boot Loader

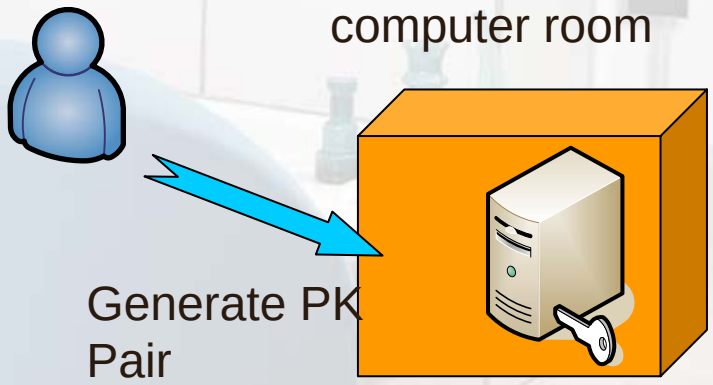
- SMP8630 contains two RSA 2048 public keys and two AES 128 bit keys (serial and parallel flash).
- xboot is located on masked rom inside the SMP8630
- xboot initializes the xpu
- xboot tries to boot first from serial then from parallel flash.
- xboot decrypts the content of the flash and then verify its signature (RSA-PKCS#1).
- The content of the flash is xos (secure OS).

Secure Boot Loader

- When xos starts, it tries to find zboot on the parallel flash by reading its signature.
- zboot is signed and can be encrypted and will run on the main CPU.
- zboot initializes the main cpu and loads the main bootloader (for CE, or YAMON for Linux).
- Main bootloader loads OS

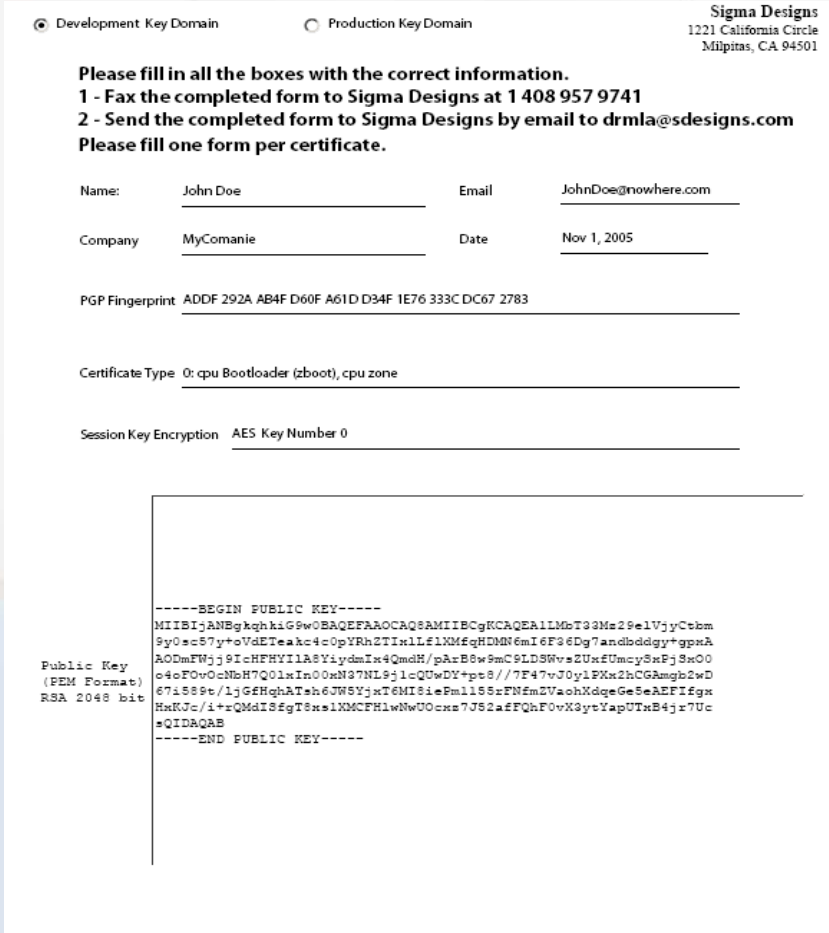
Certificate Request

- Customer generates an RSA 2048 Private/Public key on a secure computer
- We recommend to key the private key part in a Hardware Security Module



Certificate Request

- Customer fills the Certificate Request PDF using the instructions.
- The Certificate Request is emailed and faxed to Sigma Designs
- The public part of the key is included in the Certificate request



Development Key Domain Production Key Domain

Sigma Designs
1221 California Circle
Milpitas, CA 94501

Please fill in all the boxes with the correct information.
1 - Fax the completed form to Sigma Designs at 1 408 957 9741
2 - Send the completed form to Sigma Designs by email to drmla@sdesigns.com
Please fill one form per certificate.

Name: John Doe Email: JohnDoe@nowhere.com

Company: MyComanie Date: Nov 1, 2005

PGP Fingerprint: ADDF 292A AB4F D60F A61D D34F 1E76 333C DC67 2783

Certificate Type: 0: cpu Bootloader (zboot), cpu zone

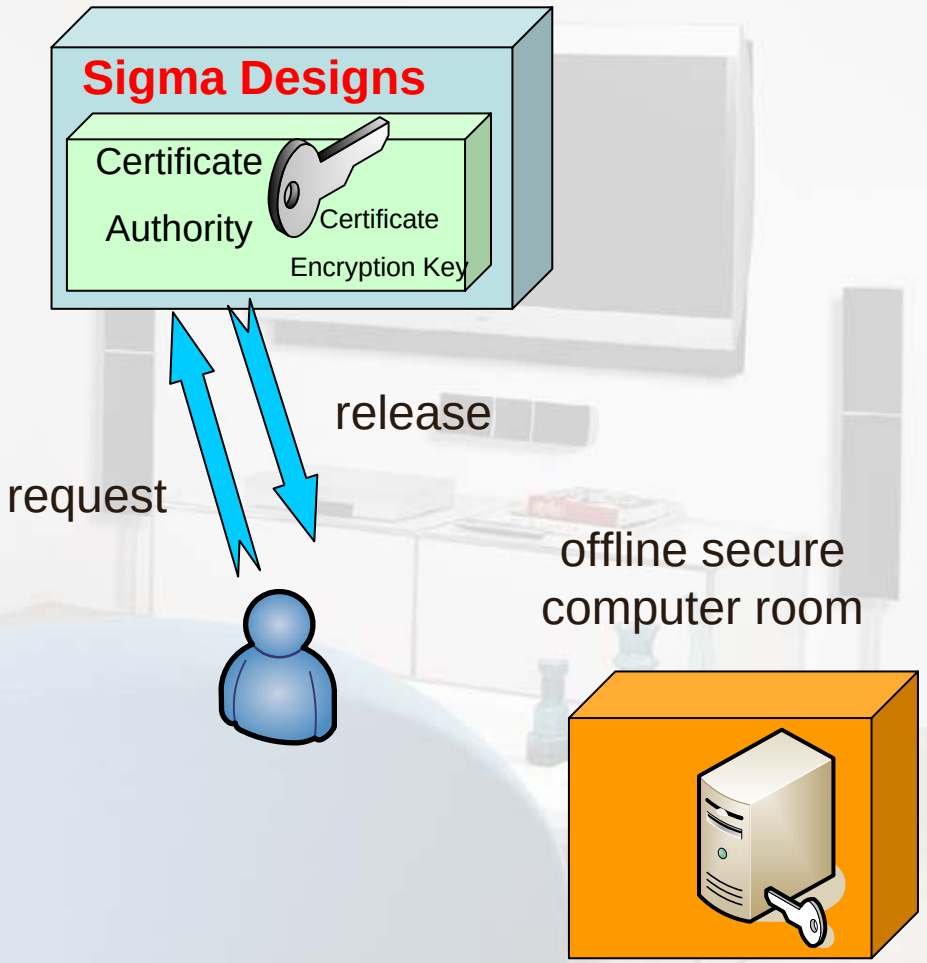
Session Key Encryption: AES Key Number 0

Public Key (PEM Format) RSA 2048 bit

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1LMbT33Mz29elVjyCtbm
9y0sc57y+oVdETeakc4c0pYRh2TIx1Lf1XMfqHDMN6mI6F36Dg7andbddgy+gpxA
AODmFWjj9IcHFHYI1A8YiydmIx4QmdH/pArB8w9mC9LD8WvsZUxfUmcy5xPj3xO0
o4oF0vOcNbH7Q0lxIn00xN37NL9j1cQUwDY+pt8//7F47vJ0ylPXx2hCGAmgb2wD
67i589t/ljGfHqhATsh6JW5YjxT6MI8iePml55rFNfmZVaohXdqeGe5eAEFIfgx
HxKJc/i+rQMdI8fgT8xs1XMCFH1wNwUOcxs7J52afFQhF0vX3ytYapUTxB4jr7Uc
sQIDAQAB
-----END PUBLIC KEY-----
```

Certificate Request

- Sigma Designs will generate the certificate and will sign it
- Sigma Designs will generate a Highly Confidential key used to encrypt the content (bootloader or OS) protected by the certificate.
- We recommend storing the Highly Confidential Encryption key on a Hardware Security Module



Binding

- During board production, customers can bind their certificate to the SMP8634
- After the binding process, the SMP8634 will only boot bootloader and CPU code that has been signed by the customer private key.
- The binding process prevents unauthorized replacement of the bootloader and CPU code inside the STB.

SDK Certificates for dev chips

Certificate items/xload_certificates/xload_certificate_8634_ES4_dev_000a.bin

Certificate for development chip for zboot2, AES encryption

ID = 000a

Type = 00 (cpu bootloader (zboot), cpu zone)

XOSKEYId = 0c (session key encrypted with XOSAESSymmetricKey(5))

Certificate items/xload_certificates/xload_certificate_8634_ES4_dev_000b.bin

Certificate for development chip for kernel, AES encryption

ID = 000b

Type = 01 (cpu code, cpu zone (cpu kernels and applications))

XOSKEYId = 0a (session key encrypted with XOSAESSymmetricKey(3))

SDK Certificates for production chips

Certificate items/xload_certificates/xload_certificate_8634_ES4_prod_0009.bin
Facsimile certificate for production chip for zboot2, AES encryption
ID = 0009
Type = 00 (cpu bootloader (zboot), cpu zone)
XOSKEYId = 07 (session key encrypted with XOSAESSymmetricKey(0))
Certificate items/xload_certificates/xload_certificate_8634_ES4_prod_000a.bin
Facsimile certificate for production chip for kernel, AES encryption
ID = 000a
Type = 01 (cpu code, cpu zone (cpu kernels and applications))
XOSKEYId = 07 (session key encrypted with XOSAESSymmetricKey(0))
Certificate items/xload_certificates/xload_certificate_8634_ES4_prod_000b.bin
Facsimile certificate for production chip for zboot2, NO encryption
ID = 000b
Type = 00 (cpu bootloader (zboot), cpu zone)
XOSKEYId = ff (binary not encrypted)
Certificate items/xload_certificates/xload_certificate_8634_ES4_prod_000c.bin
Facsimile certificate for production chip for kernel, AES encryption
ID = 000c
Type = 01 (cpu code, cpu zone (cpu kernels and applications))
XOSKEYId = ff (binary not encrypted)

Information

- For more information, email drmla@sdesigns.com and request the "Certificate Request for SMP8634L" document
- Recommendation for the Certificate Request: if you want to encrypt your bootloader and OS, use AES Key 0 option in the certificate request.