



AusCERT, University of Queensland

Preparing for the Certificate Service Manager (CSM) Release

A guide for Participant Organisations to prepare for the CSM workshops
which will be held between 24 October and 30 November 2011

06 October 2011

Preparing for the release of the CSM

Roadshow dates

Monday 24 October 2011 to 30 November 2011

Enrolling Participant Organisations and administrative accounts

Prior to the CSM release AusCERT will :

1. enrol POs, called “organisations” in the CSM;¹
2. create one Registration Authority Officer (RAO) account for each PO with full privileges. This will be the **primary RAO account**. AusCERT will select the most appropriate RAO contact from Schedule 1 of the subscriber agreement to be the primary RAO account holder that receives maximum privileges in the CSM.
3. add domains owned by the PO which have been validated by AusCERT, including a wildcard for sub-domains.

As part of the self-provisioning features of the CSM, the primary RAO account holder will then be able to take the following steps in the CSM :

1. change their password
2. add additional domains owned by their organisation, if required and subject to domain control verification approval by AusCERT
3. create appropriate additional RAO accounts for their PO to distribute the workload and be a back-up when other RAOs are unavailable to operate the CSM. **AusCERT recommends that subsequent RAO accounts are created without privileges to create, edit² or delete other RAOs.**
4. request S/MIME certificates for these RAO account holders to use as a second authentication factor to the RAO (and DRAO) account³
5. conduct an SSL certificate scan to locate all certificates deployed on the PO network⁴
6. create DRAO accounts as required.

S/MIME private key escrow

¹ Unless advised otherwise, AusCERT will configure new organisations without escrow. See section on “S/MIME private key escrow”.

² Edit privilege may be useful for recovery of a primary account, but this should be only used with caution.

³ AusCERT recommends two factor authentication for all administrative accounts to prevent unauthorised use.

⁴ This is a useful exercise because it allows POs to see all SSL certificates on their given network (address range) and this enables them to view, renew, revoke these certificates as appropriate.

There is one issue which is very important for participant organisations (PO) to consider before AusCERT can include your organisation within the CSM in October and November 2011, when the sector-wide release of the CSM occurs.

The decision your organisation makes in relation to whether or not it chooses to permit S/MIME private key recovery (escrow) **on an organisation-wide basis** affects every S/MIME certificate issued by your organisation in the future. **The decision your organisation makes now is permanent and irrevocable.** Therefore, your organisation needs to consider the advantages and disadvantages associated with S/MIME private key escrow carefully and prior to your organisation's enrolment in and use of the CSM.

Should you choose not to enable key recovery (escrow) at an organisational level, the option will remain to enable it on a per-department basis, however each department will be required to manage its own master private key - it will not be possible to retain a single, organisation-wide master private key for escrow recovery.

What is an S/MIME certificate?

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that adds digital signatures and encryption to Internet MIME (Multipurpose Internet Mail Extensions) messages described in RFC 1521.⁵ S/MIME certificates are personal certificates issued to authorised subscribers from your organisation with email addresses associated with your organisation's domain. The S/MIME certificate can be used to digitally sign and encrypt email messages. The certificate can also be used as a means by which a person can authenticate to an application. The S/MIME certificate provided through the CSM is a dual use certificate that handles both encryption and signing functions using the same private key.

What is S/MIME private key escrow?

S/MIME private key escrow is the means by which it is possible to recover the private key of an S/MIME (personal) certificate belonging to a person from your organisation if the person is no longer able to do so themselves (eg, their passphrase is lost, they are no longer an employee or no longer have access to the systems where the private key was stored, or if the key has been destroyed (eg, hardware failure)).

Note that this discussion on escrow only applies to S/MIME certificates and is not available for, or relevant to either SSL or code signing certificates.

How does escrow occur?

When an organisation or department is created within the CSM, it is necessary to specify at this time whether the organisation wishes to permit S/MIME key recovery (escrow). If this option is enabled, the RAO and/or DRAO⁶ must generate a master public private key pair before S/MIME certificates may be issued.

⁵ <http://www.rsa.com/rsalabs/node.asp?id=2292>

⁶ A keypair must be generated *for each department* that has escrow enabled.

If escrow is enabled for the organisation, the public key may be used – with appropriate CSM configuration – to encrypt every S/MIME certificate that is subsequently generated for the organisation.

If escrow is enabled when creating a department, the public key will be used to encrypt every S/MIME certificate that is subsequently generated for the department.

In the event that S/MIME recovery is required, the authorised RAO or DRAO can download the encrypted S/MIME certificate after supplying the master private key for decryption of the S/MIME certificate. If this occurs, the S/MIME certificate is automatically revoked because the recovery of the private key for a dual-purpose certificate permanently compromises its ability to be used for non-repudiation.

Benefits of S/MIME private key escrow

The only reason to provide escrow functionality is to ensure that an organisation can decrypt important communications (typically conducted over email)⁷ if ever required in future arising from the loss of access to the private key belonging to the S/MIME certificate holder.

Disadvantages of S/MIME private key escrow

There are risks, including:

- the burden associated with securely storing the master private key used for decrypting all the (encrypted) S/MIME private keys; and
- the risk of a compromise to that key arising from inadequate key management or misuse of legitimate access, resulting in a party inappropriately “downloading” the S/MIME certificate to decrypt confidential information. Should this attack occur, it is likely to be detected (after the compromise has occurred) due to the automatic revocation of the key, and ability to monitor the activity log.

Additionally, there are consequences associated with key recovery, if activated:

Once an S/MIME certificate is recovered, through escrow, the certificate will automatically be revoked. Revocation breaks the ability to verify any digital signatures created using that S/MIME certificate in the past (prior to key recovery and revocation). **This could impact upon the future verification of documents signed with a personal certificate⁸.**

⁷ The certificates can be used to encrypt non-email communications too but the process required involves some knowledge of public key encryption and most users are unlikely to use this feature, outside the S/MIME environment.

⁸ AusCERT recommends against the use of CSM-issued personal certificates as a solution for long-term digital signing of documents.

Balancing the benefits with the disadvantages

In deciding whether there is any value in enabling escrow, organisations need to determine if there are circumstances that make it desirable to recover S/MIME certificates to enable decryption of emails and other documents encrypted with S/MIME certificates⁹.

Revocation of an S/MIME certificate may be desirable, for example when the subscriber is no longer an employee of the organisation and no longer has access to an email address using the organisation's domain. **However, in any situation where the S/MIME certificate is revoked, the ability to verify a digital signature (and provide non-repudiation) is also removed.**

To justify implementing escrow, the benefits should outweigh the disadvantages described above.

How to reduce the requirement for key recovery (escrow)?

In accordance with section 6.2.4 of the CPS, AusCERT strongly recommends that all personal certificate subscribers back up and protect their private key to ensure they continue to have access to their private key in the event of a hardware malfunction. In these circumstances, the need to utilise the key recovery features of the CSM (where it has been enabled) and avoid unnecessary S/MIME certificate revocations, will be minimised.

I want to enable key recovery (escrow) for my organisation – what does this mean?

The RAO for the organisation will generate and retain a master key that – providing the CSM is configured appropriately – may be used to recover any escrowed, personal (S/MIME) certificate subsequently issued using the CSM, either at an organisation (RAO) or department (DRAO) level. Personal certificates issued by the RAO will be automatically escrowed. Personal certificates issued by DRAO will be automatically escrowed (or not) according to the CSM configuration.

I don't want to enable key recovery (escrow) for my organisation – what does this mean?

The RAO for the organisation will be unable to generate a master key and is not able to escrow or recover any personal (S/MIME) certificates generated within the organisation. **The RAO may still create/add department/s with key recovery (escrow) enabled.** If key recovery is enabled for a department, the DRAO will generate and retain a master key that may be used to recover any escrowed, personal (S/MIME) certificate issued for that department. Personal certificates issued by DRAO will be automatically escrowed (or not) according to the CSM configuration.

AusCERT recommends

While ultimately the decision as to whether to enable organisation-wide key recovery (escrow) or not depends on each organisation's particular requirements and risk profile, AusCERT recommends against enabling escrow for the reasons that the benefits are likely to be relatively minor and infrequent, compared to the potential risk of unauthorised access to the private master key. This

⁹ If key recovery is enabled at a departmental level only, the DRAO – not the RAO – will hold the master private key for escrowed certificates.

recommendation is consistent with the default client certificate configuration for the similar InCommon Certificate Manager implementation¹⁰.

In particular, organisations which implement key escrow must be confident of securely managing access to the private key/s used to decrypt all escrowed S/MIME private keys. This occurs by creating a text file of the private key and storing an electronic copy of it somewhere safely, such as in a safe with restricted authorised access to the key.¹¹ Organisations that do not enable organisation-wide key recovery should ensure that delegation of escrow rights to a department (and DRAO) is similarly, securely managed.

For the production rollout of the Certificate Services Manager, unless otherwise advised, AusCERT will create organisations with organisation-wide (RAO) key recovery (escrow) disabled by default.

Further information about Comodo's implementation of escrow

Where escrow is enabled, note that POs are obliged to follow the guidelines in the [CPS](#)¹² regarding escrow:

- 4.12 Key Escrow and Recovery
- 6.23 Private key escrow

See also the [AusCERT CSM RAO Administrator Guide](#)

- 4.5 Encryption and Key Escrow, page 139 - 148

Next steps

We require an authorised RAO contact who has the ability to make decisions for the whole organisation to send an email to cs@auscert.org.au to advise whether your organisation should have escrow enabled or not. **Please notify AusCERT as soon as possible so as ensure that you are able to use the CSM and participate in the roadshow workshop when it comes to your state/region.**

If you wish escrow functionality to be enabled, this will only allow your organisation to recover S/MIME certificates. AusCERT **will not be able to do this on behalf of POs.**

In preparation for each workshop, AusCERT will create an account for each primary RAO and provide them a username and password. If AusCERT does not receive written notification about the PO's decision with regard to escrow, organisations will be added to the CSM using the default (NO) escrow recommendation. This default configuration setup will still allow POs to subsequently create departments that have escrow enabled.

Further information

The CSM is available from:

¹⁰ InCommon serves the U.S. education and research communities. Information about InCommon client certificate escrow policy is at <https://www.incommon.org/cert/clientcerts.html>

¹¹ See 4.5.5 Encrypting the Private Keys, [AusCERT CS RAO Administrative Guide](#).

¹² Available from: <http://cs.auscert.org.au/repository>

<https://cert-manager.com/customer/auscert>

To assist with using the AusCERT CSM, Comodo has released two guides, which are available from the <http://cs.auscert.org.au/repository>:

- [AusCERT CS RAO Administrator Quick Start Guide](#)
- [AusCERT CS RAO Administrator Guide](#) (for RAOs and DRAOs)
- [AusCERT CS User Guide](#) (for those who wish to request SSL, code-signing and/or S/MIME certificates)

In addition, it is important that all RAOs and DRAOs and certificate subscribers be familiar with their roles and responsibilities as outlined in the following key documents:

- [AusCERT CS Certification Practice Statement and Certificate Policy](#)
- [AusCERT CS Relying Party Warranty](#)
- [AusCERT CS Participant Organisation Agreement](#)
- [AusCERT CS Participant Organisation Schedule 1](#)

AusCERT will provide supplementary documentation in addition to documentation already provided and available through the <http://cs.auscert.org.au/repository>.