

ID	TSS001360	Creation date	May 12, 2009
Platform	S60 3rd Edition FP1, S60 3rd Edition, FP2	Devices	Eseries devices
Category	Symbian C++	Subcategory	OMA DM

Keywords (APIs, classes, methods, functions):

Description

Establishing trust between a device and the DM server is described in [OMA Device Management DDF for Policy Management](#) available at Forum Nokia. This article explains the possible ways of establishing trust and the different policies that can be used.

Solution

There are two ways to create corporate trust.

Separate mapping for certificate and roles

First, the certificate mapping policy is sent.

[File:Certificate mapping.zip](#)

The above policy creates a mapping between the certificate and the `alias_id`. The policy does not create the trust but simply describes that `COMCOM` is the "short name"/alias for the given certificate.

After this, the roles mapping policy is sent.

[File:Roles mapping.zip](#)

The above policy maps the `COMCOM` role to be the `trustedadmin` which is the `role_id` of the `COMCOM`. This policy will display the device security indicator § in the status pane.

Alternative approach

In this approach, both the certificate and role mappings are done at the same time with a single policy:

[File:Certificate roles mapping.txt](#)

The command: `use_bearer_certificate = "true"` will cause the certificate to be searched directly from the HTTPS session. In Approach 1, the certificate is taken from the policy file itself.

The second approach is an easy way to establish trust as both certificate mapping and roles mapping are handled automatically.

See also

[OMA Device Management DDF for Policy Management](#)