```
# http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslverifyclient
#
#           none: no client Certificate is required at all
#   optional_no_ca: the client may present a valid Certificate
#                   but it need not to be (successfully) verifiable.
#        optional: the client may present a valid Certificate
#         require: the client MUST present a valid Certificate
#
SSLVerifyClient optional

SSLOptions +FakeBasicAuth
SSLRequireSSL
SSLRequire %{SSL_CLIENT_VERIFY} eq "SUCCESS"

# the above lines mean that we must verify with a valid cert
# but if we don't, we display a nice(ish) 403 error page

ErrorDocument 403 /certs/403.html

# http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslverifydepth
# maximum number of certificates deep to look when following a client cert to the CA root
#
# the default depth of 1 means the client certificate can be self-signed or has to be
signed by a CA
# which is directly known to the server (i.e. the CA's certificate is under
SSLCACertificatePath), etc
SSLVerifyDepth 5

# http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#ssloptions
#
# +ExportCertData ...
# When this option is enabled, additional CGI/SSI environment variables are created:
# SSL_SERVER_CERT, SSL_CLIENT_CERT and SSL_CLIENT_CERT_CHAIN_n (with n = 0,1,2,..).
# These contain the PEM-encoded X.509 Certificates of server and client for the current
# HTTPS connection and can be used by CGI scripts for deeper Certificate checking.
# Additionally all other certificates of the client certificate chain are provided, too.
# This bloats up the environment a little bit which is why you have to use this option to
enable it on demand.
#
<Files ~ "\.(html|php)$">
```

```
    SSLOptions +StdEnvVars +ExportCertData
</Files>

# Force a redirect to HTTPS
RewriteEngine On
RewriteCond %{ENV:usingSSL} !=yes
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [L,R=permanent]
```