Comunicaciones seguras

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

eman ta zabal zazu

Universidad
del País Vasco

Euskal Herriko
Unibertsitatea

BILBOKO
INGENIARITZA
ESKOLA

ESCUELA
DE INGENIERÍA
DE BILBAO

TLS/SSL and HTTPS use the RFC 5280 profile of X.509, as do S/MIME (Secure Multipurpose Internet Mail Extensions) and the EAP-TLS method for WiFi authentication. Any protocol that uses TLS, such as SMTP, POP, IMAP, LDAP, XMPP, and many more, inherently uses X.509. SSH generally uses a Trust On First Use security model and doesn't have need for certificates. However, the popular OpenSSH implementation does support a CA-signed identity model based on its own non-X.509 certificate format.[48]