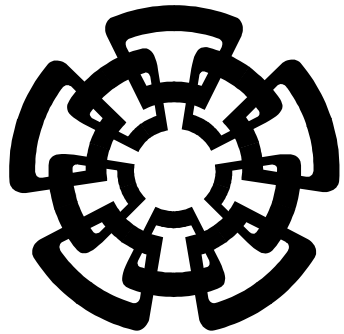


Alcances y realidades del correo-e seguro

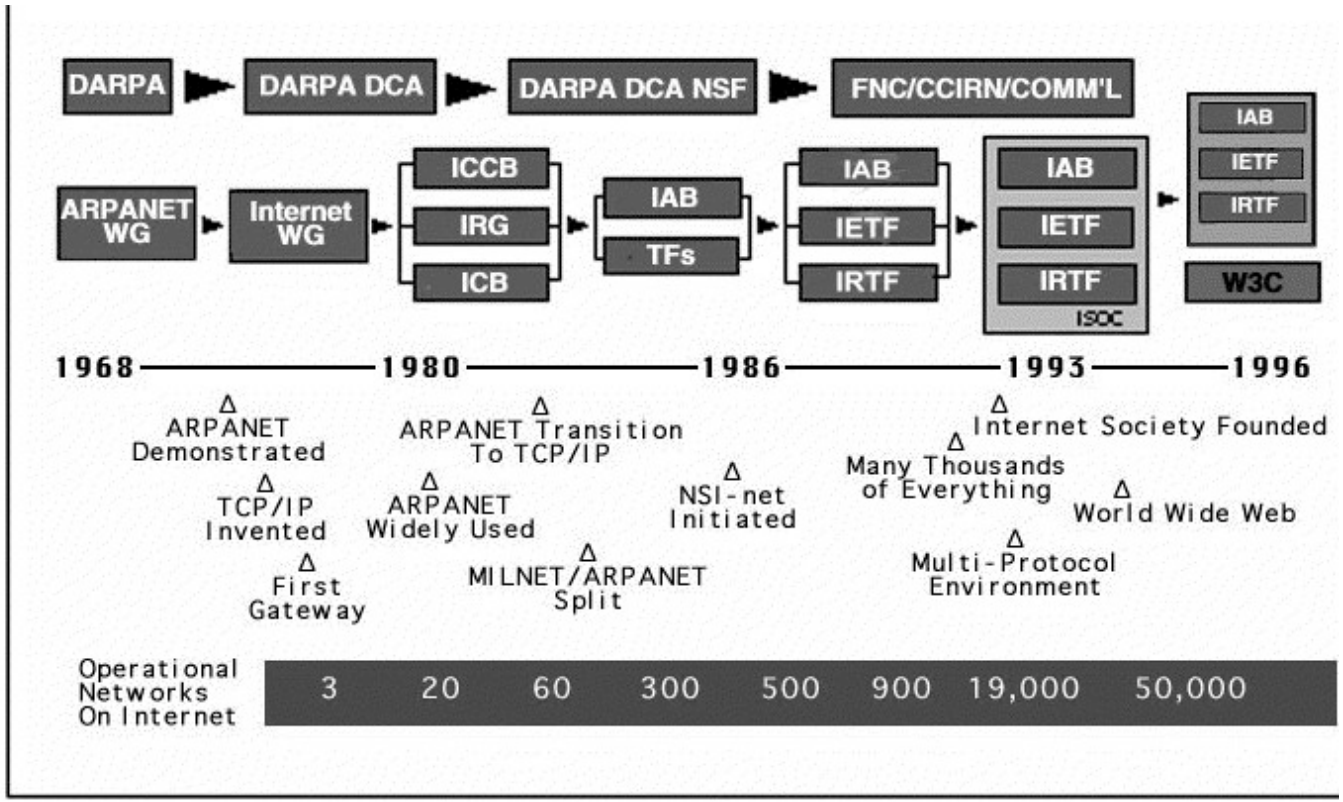
CINVESTAV-IPN

Departamento de Ingeniería Eléctrica

Guillermo Morales Luna (gmorales@cs.cinvestav.mx)

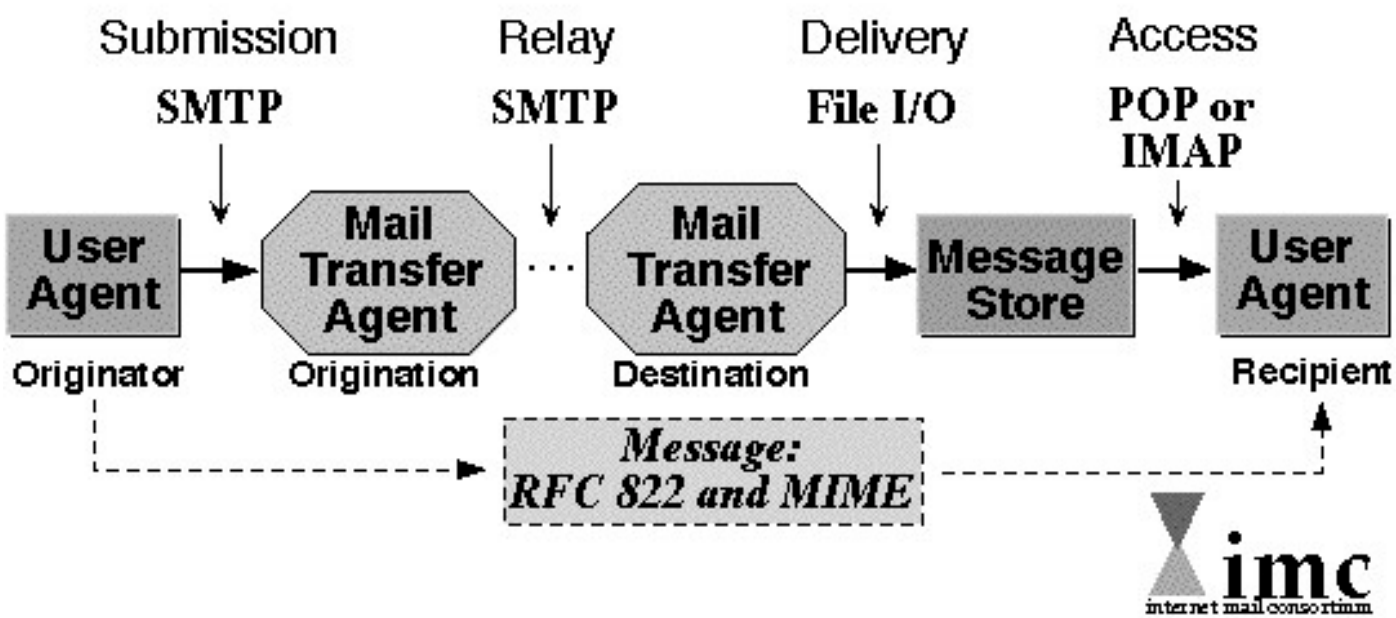
Emilio Rafael Espinosa (respinosa@cs.cinvestav.mx)

Evolución de Internet



Fuente: http://www.imc.org

Internet Mail Standards



Fuente: http://www.imc.org

S/MIME vs OpenPGP

Mandatory features	S/MIME v3	OpenPGP
Message format	Binary, based on CMS	Binary, based on previous PGP
Certificate format	Binary, based on X.509v3	Binary, based on previous PGP
Symmetric encryption algorithm	TripleDES (DES EDE3 CBC)	TripleDES (DES EDE3 Eccentric CFB)
Signature algorithm	Diffie-Hellman (X9.42) with DSS	ElGamal with DSS
Hash algorithm	SHA-1	SHA-1
MIME encapsulation of signed data	Choice of multipart/signed or CMS format	multipart/signed with ASCII armor
MIME encapsulation of encrypted data	application/pkcs7-mime	multipart/encrypted

Fuente: http://www.imc.org/smime-pgpmime.html

Productos S/MIME y PGP

	S/Mime or PGP	Clients Supported			Trust individual certs	Trust CA root certs	Send/receive clear/opaque msg.	Key encription schema
		Win 3.1	Win 32	Mac				
Microsoft Outlook Express	S/Mime	No	Yes	No	Yes (1)	Yes	S/R C; S only O	RC2 (40, 64, 128)
Microsoft Outlook 98 (7)	S/Mime	No	Yes	Yes	Yes (1)	Yes	S/R C/O	RC2 (40, 64, 128)
Netscape Messenger 4.5	S/Mime	Yes	Yes	Yes	Yes	Yes	S/R C; R only O	RC2 (40, 64, 128)
OpenSoft ExpressMail 2.5	S/Mime	Yes	Yes	No	No	No	S/R C/O (5)	RC2 (40, 64, 128, 255)
Lotus Notes	S/Mime	Coming in R5			Yes (1)			
Cyrusoft Mulberry	PGP	No	Yes	Yes	Yes	N/A	S/R C only	DH

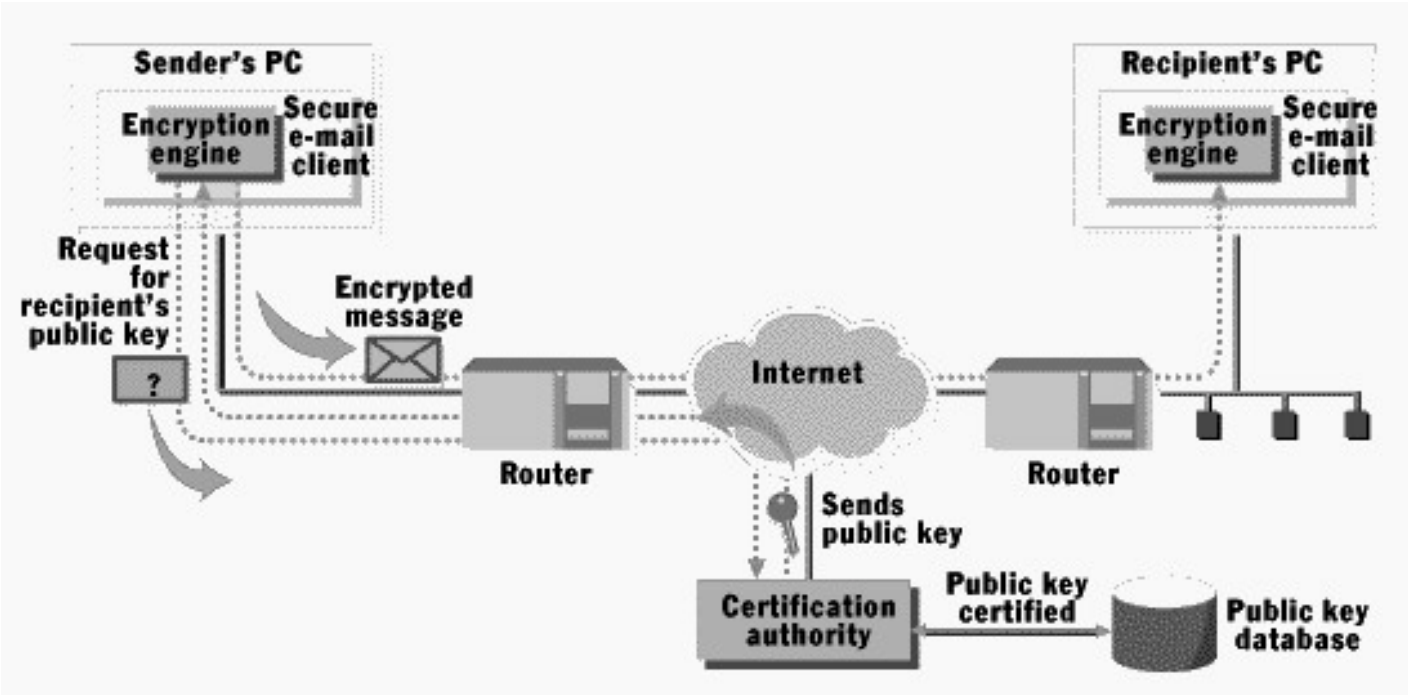
Fuente: http://strom.com/places/smime.html

Plug-ins S/MIME y PGP

	S/Mime or PGP	Clients Support			Trust individual certs	Trust CA root certs	Send/receive clear/opaque msg.	Key encrption schema	Products supported
		W 3.1	W 32	Mac					
WorldTalk WorldSecure Client 2.2	S/Mime	Yes	Yes	No	Yes	No	S/R C/O (5) (6)	RC2 (40, 64, 128, 255)	Eudora, Outlook
Labcal Technologies' IsoShield/Mail	S/Mime	Yes	Yes	No	Yes (1)	No	S/R C/O	RC2 (40, 64)	Notes
LJL Enterprises' ArmorMail	S/Mime	Yes	Yes	No	Yes	Yes	S/R C; R only O (5)	RC4 (40, 128) (3)	MS Mail, cc:Mail, Outlook, Notes, Eudora
Baltimore Mail Secure	S/Mime	Yes	Yes	No	Yes	Yes	Limited (2) (5)	RC2 (40, 64, 128)	Eudora, Outlook
Novell Groupwise w/Entrust	S/Mime	No	Yes	No	Yes	Yes	S/R C/O	RC2 (40, 64, 128)	Groupwise
PGP for Business Privacy (4)	PGP	No	Yes	Yes	Yes	N/A	S/R C only	DH	Eudora, Exchange, Outlook, Claris Emailer
Novell Groupwise w/ PGP	PGP	No	Yes	No	Yes	N/A	S/R C only	DH	Groupwise
Entrust Lite	S/Mime	Yes	Yes	Yes	Yes	Yes	S/R C/O	RC2 (40, 64, 128), DH	MS Mail, Outlook, cc:Mail, QuickMail

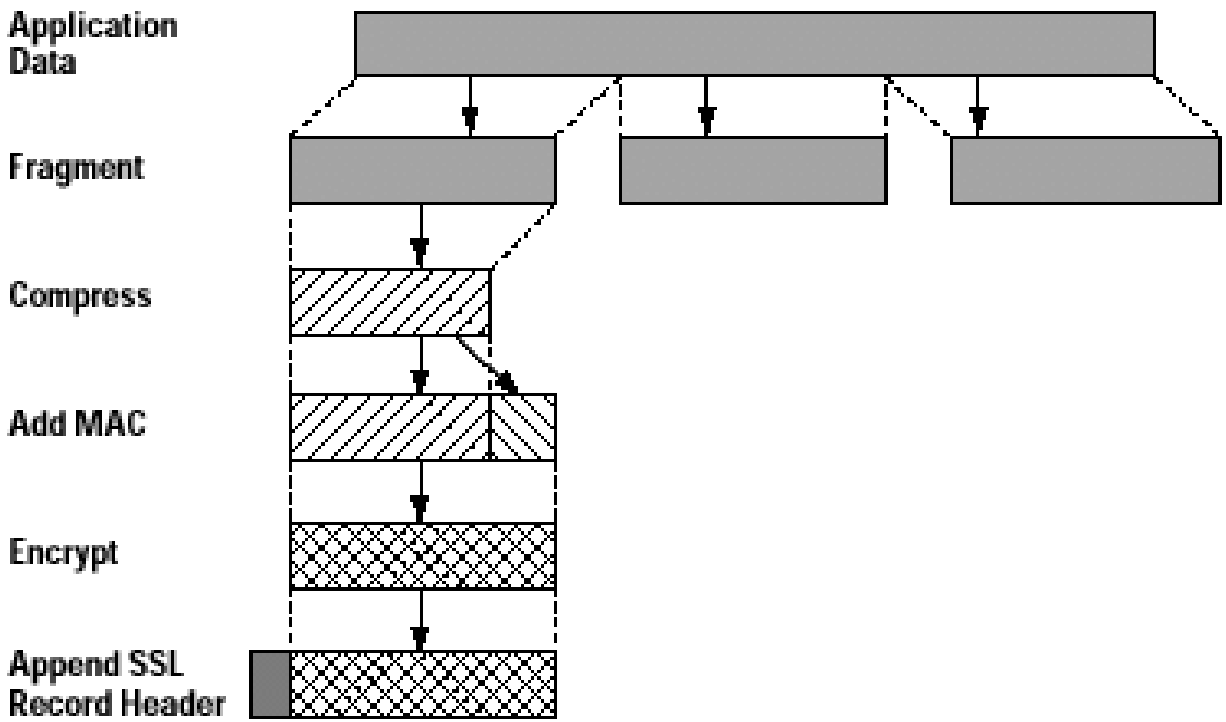
Fuente: http://strom.com/places/smime.html

Arquitectura de un sistema de correo seguro

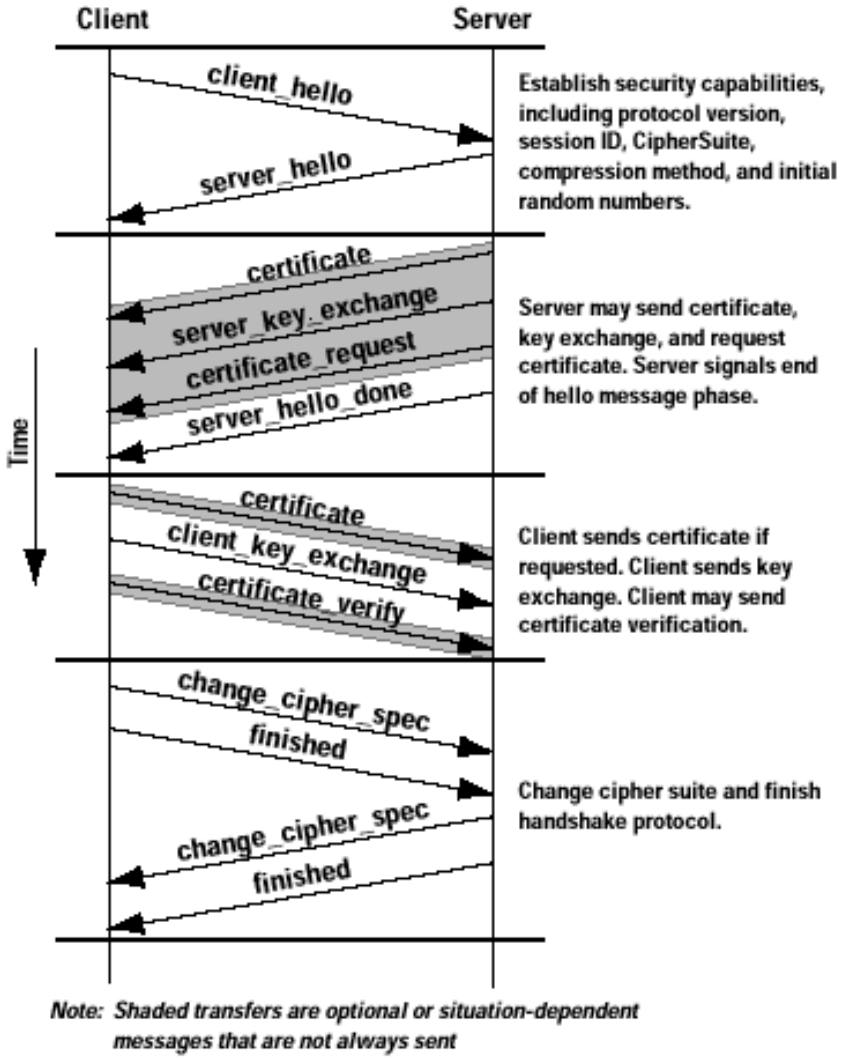


Fuente: http://www.data.com/tutorials/protecting_internet_email.html

Secure Sockets Layer

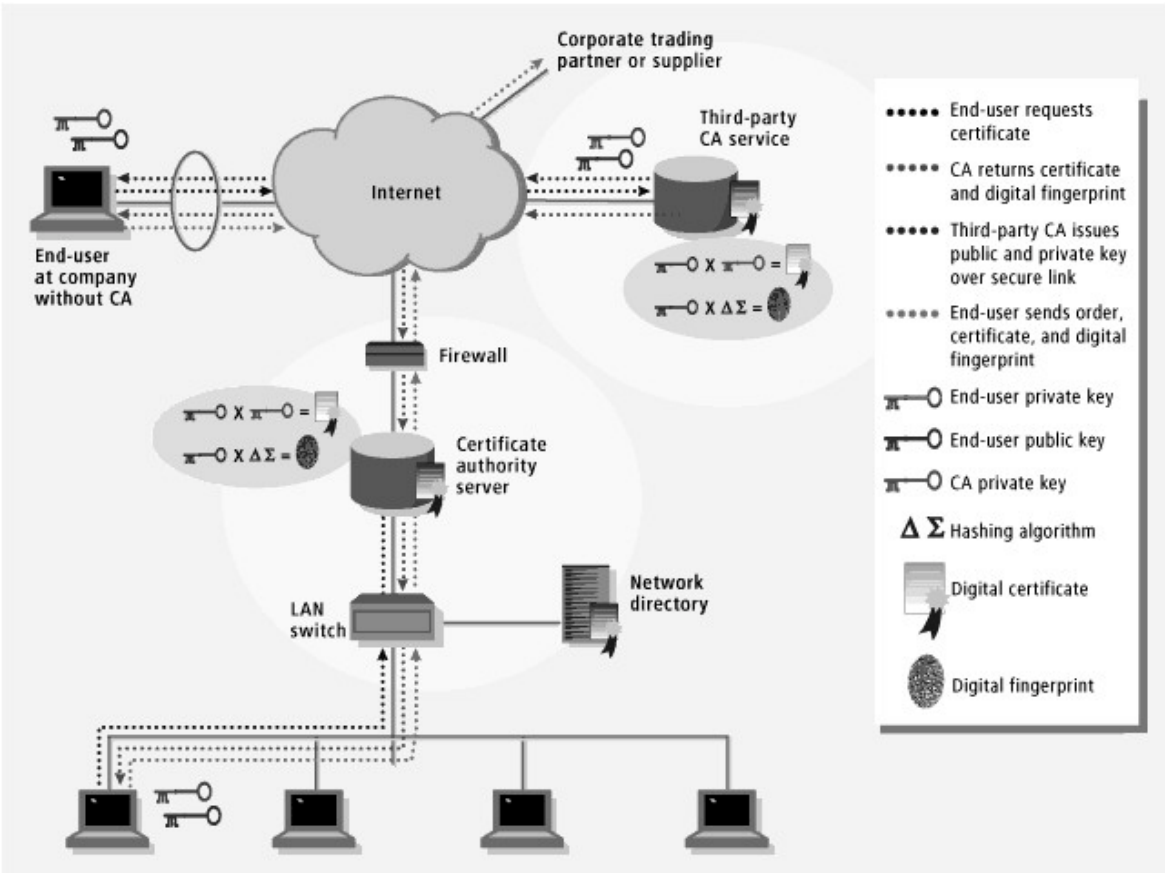


Fuente: http://www.cisco.com/ipj



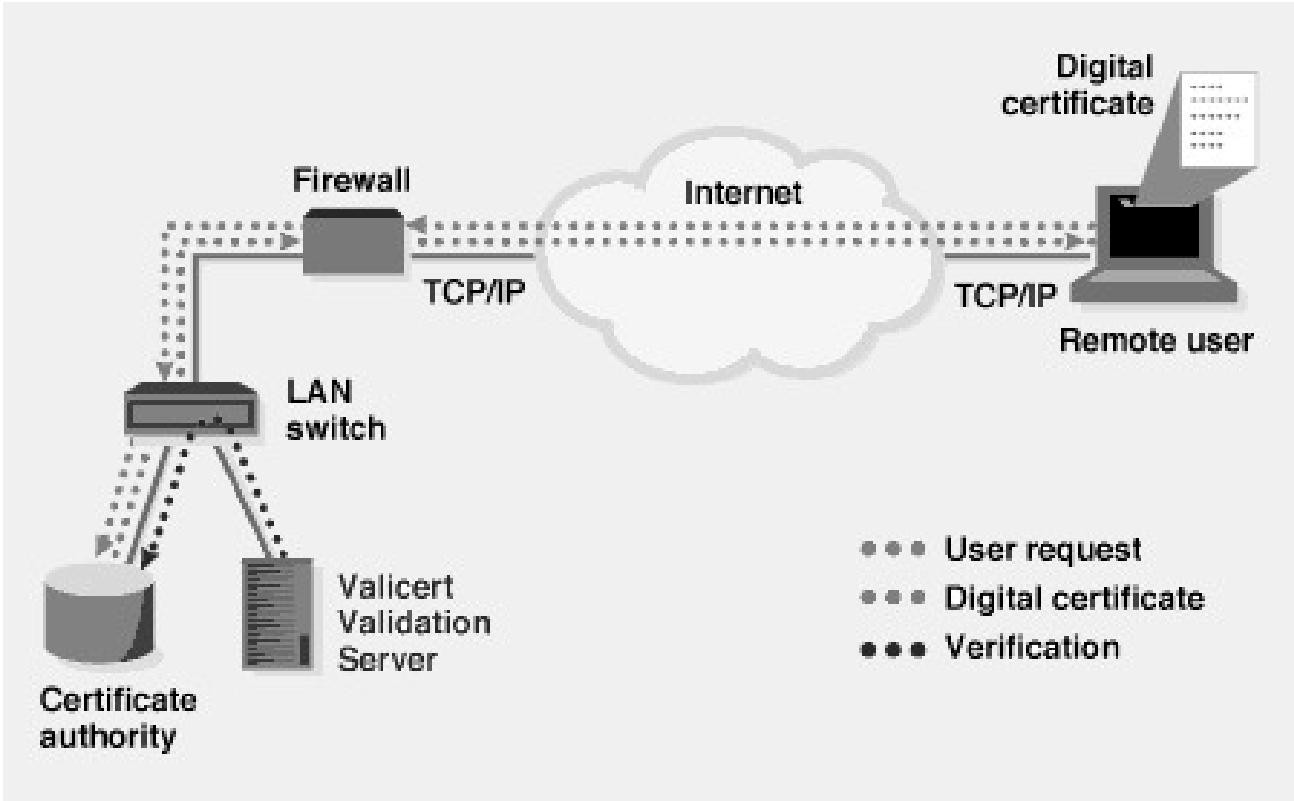
Fuente: http://www.cisco.com/ipj

Seguridad certificada



Fuente: http://www.data.com/roundups/certificate.html

Servidor de validación Valicert



Fuente: http://www.data.com/hot_products/images/validation_figure.html