digicert®

BestCert

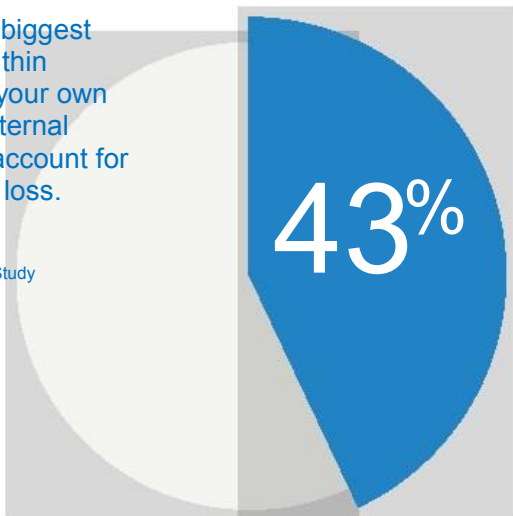Same Certs, Best Price

digicert®

DigiCert Client Certificates:
Prove Identity & Encrypt Communications

Passwords No Longer Cut It

Your information is as essential as any of your business assets. Adding extra layers of security to your critical systems and data is no longer just an option—it's a necessity. In fact, one of your biggest threats lie within the walls of your own company. Internal employees account for 43% of data loss, according to a Ponemon Institute study.

Passwords are part of the problem when it comes to lost data, not the solution. According to LastPass, the average 250-employee company has roughly 47,750 passwords used across their organization. These passwords represent 47,750 entry points into your systems. But, what if you didn't have to rely on the strength of passwords?

One of your biggest threats lie within the walls of your own company. Internal employees account for 43% of data loss.

Ponemon Institute Study

43%

The average 250-employee company has roughly 47,750 passwords used across their organization. These passwords represent 47,750 entry points into your systems.

The Solution: Client Certificates

Client certificates are used to require multi-factor authentication. Unlike weak passwords, client certificates prove the identity of the user attempting to connect to a specific application, website, interface, or other system by using a digital signature.

DigiCert Client Certificates - Secure sensitive emails with S/MIME
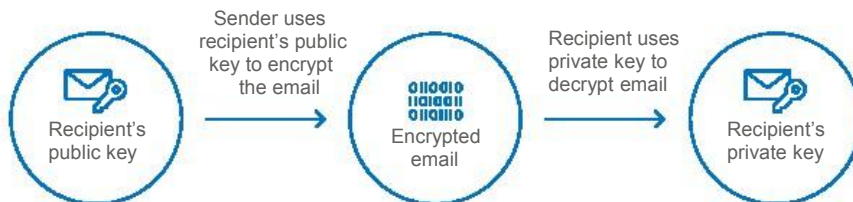
How Client Certificates Work

Client Authentication Certificates

Generally, Client Certificates (authentication certificates) are used for two-factor authentication. Once a server is configured for client certificate authentication, it will only grant user access to it if the client presents the correct client certificate. When using a web browser to connect to the server, without the correct client certificate, the client cannot even access the credentials page.

Step 1

Server requests
Client Certificate

Server   Client

Client provides
Client Certificates

Step 2

Server requests
credentials

Server   Client

Client provides
credentials

Email Client Certificates

Email client certificates have a public/private key pair. Your private key stays with you and is used to sign outgoing emails and decrypt incoming emails encrypted with your public key. Your public key is used to verify your signature and encrypt emails sent to you.

Sender uses
recipient's public
key to encrypt
the email

Recipient's
public key

Encrypted
email

Recipient uses
private key to
decrypt email

Recipient's
private key

Use Case: VPN

Company A has employees across the world connecting to its Virtual Private Network (VPN). To do so, an employee must simply provide a username and password. Since a password can be compromised in a matter of seconds or a few days (depending on the number of characters used), a malicious attacker accesses Company A's VPN and leaks some of its sensitive data.

Company B requires a unique client certificate for each employee connecting to its VPN. In this case, an attacker compromises the employee's password, but can't use it to access the VPN without physical possession over the employee's device. Due to this added layer of security, the attacker is unable to cause any damage.

Benefits of DigiCert Client Certificates

Prevent tampering

Add an extra layer of protection with multi-factor authentication. Even if valid user credentials get into the wrong hands, your organization will be safe because access will still be denied.

Sign & encrypt email

Allow senders and recipients of e-mail to verify that the content they're sharing is legitimate. Encrypt communications using S/MIME, the most trusted e-mail encryption technology.

Automate management

Make managing client certificates easy in account panel, which provides insight and control for all certificate functions.

	S/MIME Client Ceritificate Basic	S/MIME Client Ceritificate Premium
Term Length	1-3 Yr	1-3 Yr
Installation service	Free	Free
Recommended For	Individual	Organization / Business
Validation	Email address	Email address & Organization
Certificate Display	mail@example.com	Email + Company info
Client Authentication	✓	✓
Email Encryption	✓	✓
Email Signing	✓	✓
Document Signing	✓	✓

Manage Digicert's Secure Email Certificates at BestCert

Features	Secure Email Certificates
Digitally signed and encrypted emails	Yes
Secure large file transfer	Yes
Support for desktop, mobile phones, and tablets	Yes
Automated certificate renewal	Yes
FDA policy compliance	Yes
Separate encryption and signing profiles	Yes
Multiple platform support	Microsoft Windows, Mac OS X, iOS, and Android
Document Signing	PDF, MS Office documents, etc.
Real-time monitoring	Utilize to easy-to-use management platform to monitor and avoid expired S/MIME certificates.

Why BestCert?

Easy-to-Use Management Platform

BestCert's easy-to-use platform and tools allow you to automate certificate tasks, making management easy.

24/7 Customer Support

Our technical support team is 24*7 available any time
you need help, and certificates are validated around the clock. Organizations are given a dedicated account representative who is a committed partner in your security.

Product suite

We not only provide all types of SSL Certificates, but also help you evaluate, choose, deploy, and operate the right PKI solution to best fit your needs and existing business systems. Whatever size your company is, it comes to digital security, You may find the right solution at Bestcert.

To learn more, logon https://bestcert.net and talk online, or email sales@bestcert.net