digicert

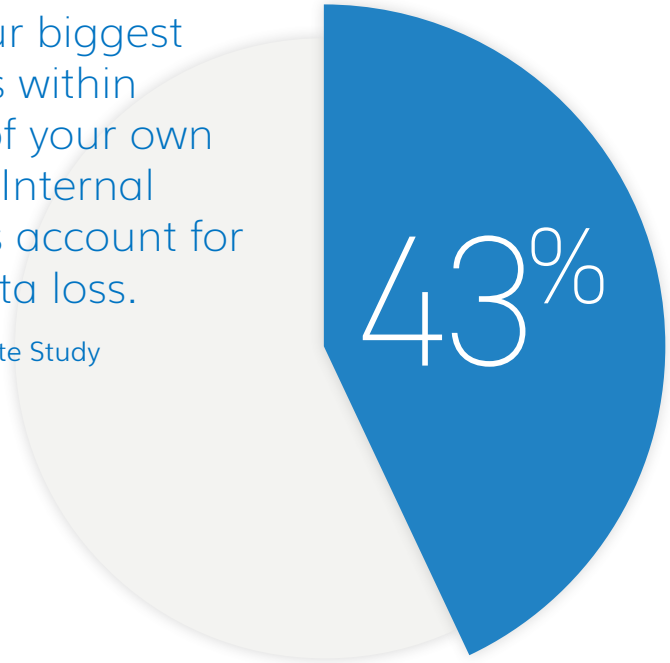
DigiCert Client Certificates: Prove Identity & Encrypt Communications

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 lies within the walls of your own company. Internal employees account for 43% of data loss, according to a Ponemon Institute study.

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

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?

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.

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.

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.

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 with DigiCert CertCentral®, which provides insight and control for all certificate functions.

	Premium	Digital Signature Plus	Authentication Plus	Email Security Plus
Client Authentication	✓	✓	✓	
Document Signing	✓	✓	✓	
Email encryption	✓			✓
Email Signing	✓	✓		

digicert

Why Choose DigiCert?

Market-Leading Platform & Tools

Maintaining a secure network goes beyond purchasing and installing SSL certificates—it includes proper configuration, vulnerability scanning, ongoing monitoring, and timely renewal. The DigiCert platform and tools allow you to automate certificate tasks, making management easy.

24/7 Customer Support

DigiCert's award-winning technical support team is 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.

Securing Top Brands

As the world's leading high-assurance digital certificate provider, we're lucky enough to work with some of the most innovative companies in the world, including those shaping the Internet of Things (IoT). Along the way, we secure more than 26 billion web connections every day.

facebook Nintendo IBM CISCO NASA hp invent Microsoft SONY Medtronic

To learn more, call 1.855.800.3444 or email sales@digicert.com.