SSL/TLS Certificates and Secure Domain Configuration

This presentation covers SSL/TLS certificate installation and configuration for AlmaLinux, Ubuntu, and Debian using Apache and Nginx web servers. We'll explore Let's Encrypt and premium SSL options.

DK **by Dan K**

Let's Encrypt Installation

1

AlmaLinux

Install EPEL repository and Certbot with Apache/Nginx plugins.

2

Ubuntu/Debian

Update and install Certbot with Apache/Nginx plugins.

3

Obtain Certificate

Use Certbot to obtain and install SSL certificate for your domain.

Verifying SSL Installation

1 Check Website

Open your website using HTTPS protocol.

2 Verify Certificates

Use Certbot to list installed certificates.

3 Check Expiration

Use OpenSSL to check certificate expiration date.

Auto-Renewal and Manual Renewal

Automatic Renewal

Let's Encrypt certificates expire every 90 days. Enable automatic renewal with systemd timer.

Manual Renewal

Use the command: sudo certbot renew --dry-run to manually renew certificates.

Premium SSL Certificates

Domain Validation

Basic domain authentication.

Extended Validation

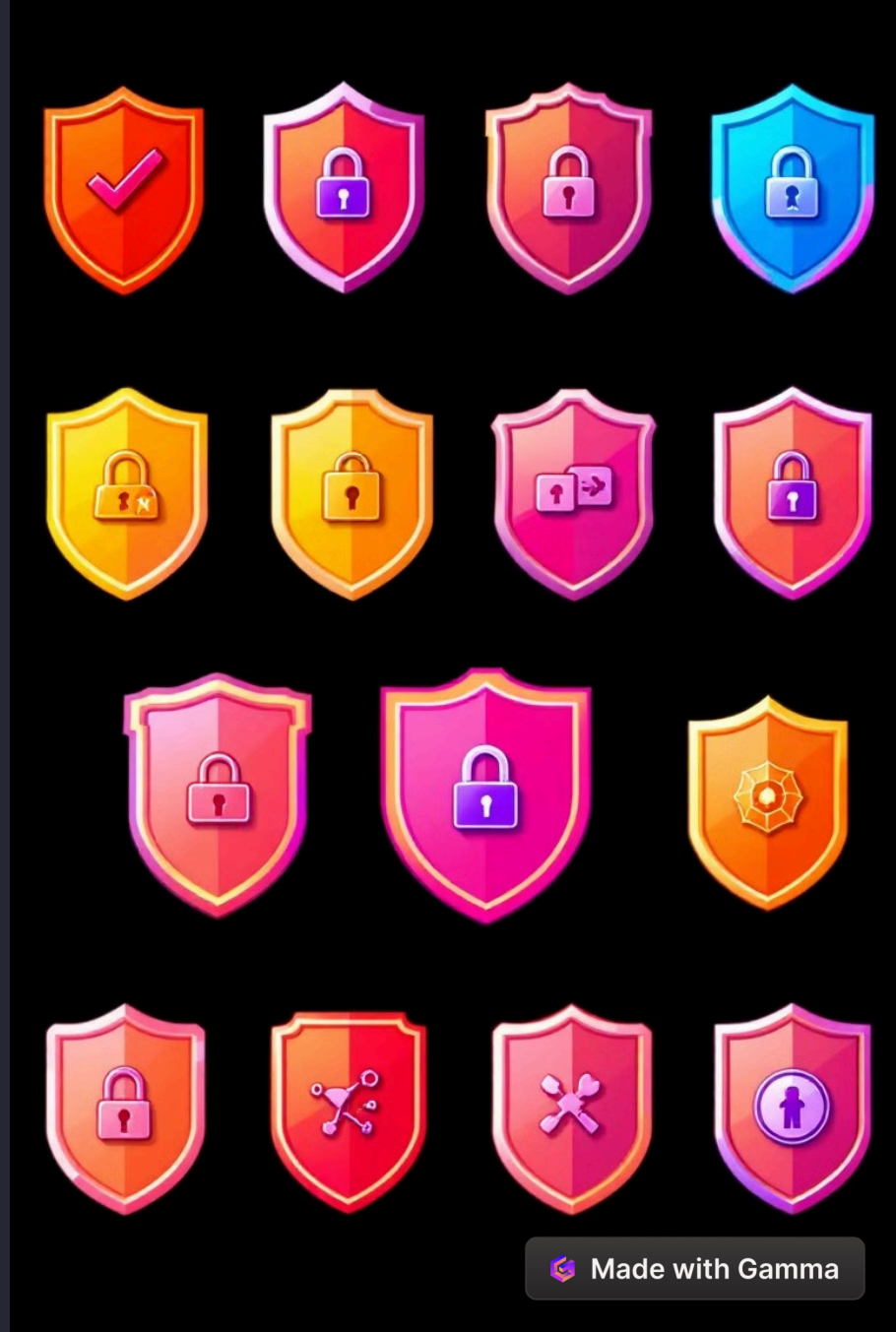
Strongest authentication level.

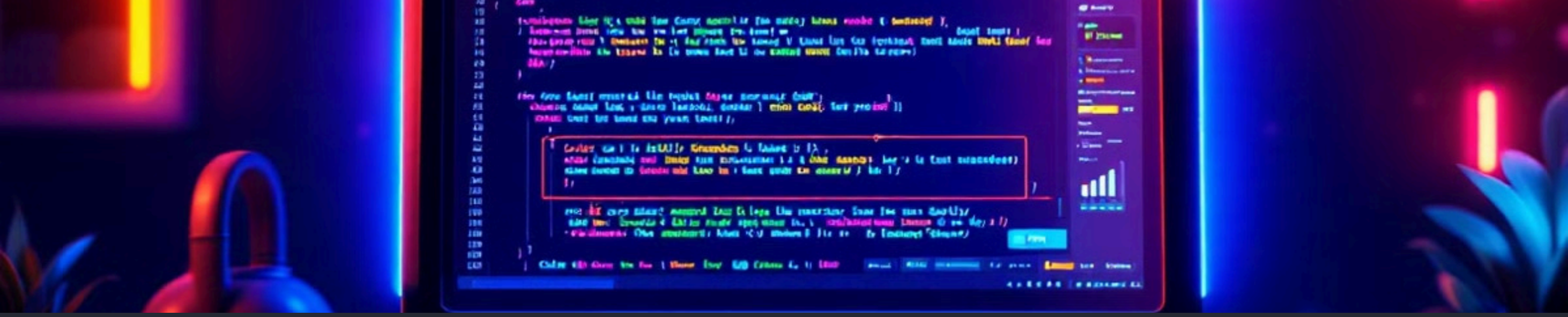
Organization Validation

Verifies business legitimacy.

Wildcard SSL

Secures multiple subdomains.





Generating CSR via SSH

1

Navigate to SSL Directory

Change to /etc/ssl/certs/ directory.

2

Generate Private Key and CSR

Use OpenSSL command to create key and CSR files.

3

Enter Required Details

Provide information like country, state, organization, and domain name.

Submitting CSR and Receiving Certificate

1

Submit CSR

Send the generated CSR to your SSL provider.

2

Receive Certificate

SSL provider sends back a certificate file (.crt).

3

Create Certificate Files

Create .ca and .crt files in /etc/ssl/certs/ folder.

Installing SSL on Apache

1 **Upload SSL Certificate**

Move certificate files to appropriate directories.

2 **Edit Virtual Host File**

Add SSL configuration to Apache's virtual host file.

3 **Restart Apache**

Apply changes by restarting the Apache service.

Installing SSL on Nginx

1 **Upload SSL Certificate**

Move certificate files to appropriate directories.

2 **Edit Server Block**

Add SSL configuration to Nginx's server block.

3 **Restart Nginx**

Apply changes by restarting the Nginx service.

Testing SSL Installation

OpenSSL Check

Use OpenSSL to test SSL connection.

Online SSL Test

Use SSL Labs or SSL Shopper for comprehensive tests.

Browser Check

Verify padlock icon in browser address bar.

Always test your SSL installation to ensure proper setup and security.