Frequently Asked Questions

FAQ: ECC and DSA Certificates Website Security Solutions

ECC and DSA Certificates
Website Security Solutions

CONTENTS

Q1: What is DSA?

The Digital Signature Algorithm (DSA) was developed by the United States government. DSA is a pair of large numbers that are computed according to the specified algorithm within parameters that enable the authentication of the signatory, and as a consequence, the integrity of the data attached. Digital signatures are generated through DSA, as well as verified. A DSA key pair will be the same size as the equivalent security RSA key. The key size will increase exponentially, the same way RSA does.

Q2: What is ECC?

Elliptic Curve Cryptography (ECC) provides similar functionality to the RSA algorithm, but requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair. The ECC key pair size will increase linearly, and is smaller than the equivalent security RSA key.

Q3: Which type of certificate will make my web server faster?

There are many factors that can affect web server speed. Symantec offers three different kinds of algorithms so that our customers can discover which certificate is the best option for their environment, or try out a combination in tandem.

Q4: Are both ECC and DSA accepted by all browsers and devices?

Not necessarily. While DSA is a requirement for dealing with certain Government Agencies, neither DSA nor ECC have the ubiquity of RSA in terms of client acceptance. For standard website transactions in the near future, RSA is and will likely remain the most used algorithm for SSL Certificates.

Q5: What is my business reason for installing additional certificates?

The usage of each certificate type may depend greatly on the type of transaction intended, reviewed against the capability of the client device in terms of computation, storage and speed. Factors to consider here include the processing power of the end device, storage space, bandwidth, power consumption, and algorithm ubiquity. For servers that allow you to install multiple certificates in tandem, there is no cost, no risk, and 100% coverage.

Q6: Can I get these with any SSL Certificate type?

For Enterprise customers, DSA is available with any SSL Certificate. ECC is available with any Premium SSL Certificate.

Q7: Will adding or changing certificates save me any money in infrastructure costs?

In testing, ECC has an improved server-side benefit of being able to accept more simultaneous handshakes compared to RSA. However, again, this must be weighed against what the client-side browsers, devices, or capabilities are.

Q8: Can I cover more than one server with the same certificate?
No. Each algorithm's certificate will be issued for the same server. One server can have more than one certificate loaded, but the alternative certificates only include one server license.

Q9: Can I get a trial ECC or DSA certificate the same way I get a regular RSA one?
MPKI for SSL does not offer trial certificates regardless of the algorithm. However, you can get a free DSA certificate for the corresponding certificate product if you currently have a valid RSA-based Standard EV SSL, Standard SSL, or Standard Intranet SSL certificate.

You can also get a free DSA and/or ECC certificate for the corresponding certificate product if you currently have a valid RSAbased Premium EV SSL, Premium SSL, or Premium Intranet SSL certificate.

Q10: How do I install multiple certificates on a server?
Each server has its own installation methods and customization plans. Please review the instructions available in our knowledge base here for how to install a certificate. https://knowledge.verisign.com/support/ssl-certificates-support/index.html?tid=symc_vrsn_kb

Q11: If I have an SSL Certificate currently, can I get these additional certificates any time?
Both algorithm alternative certificates will be available starting February 25, 2013 for MPKI customers.

Q12: How do I handle multiple certificates at renewal?
You renew your basic certificate in the usual fashion: Authorization and authentication review, then issue of the renewal certificate. After issuance, you will have the option to create one of these alternative certificates.

Q13: What if I need to replace a certificate?
You can replace the certificate as usual, except for the alternative certificate(s) you won't be able change the Subject Alternative Names (SANs) in the certificate.

Q14: What happens if I need to revoke a certificate?
Alternative certificates can be revoked independently of one another. However, you will not get the units back until you have revoked all certificates (RSA/DSA/ECC) for the same Domain Name/SANs within 30 days.

More Information

Visit our website

https://www.symantec.com/ssl-certificates

To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec

Norton SECURED
powered by VeriSign

UID 149/1/13