Algorithm Agility Frequently Asked Questions (FAQs)

FAQ

For Symantec Website Security Solutions Channel Partners

PRODUCT/SOLUTION:

Q. What is DSA?
A. 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. (1024, 2048, 3072, 7680-bits)

Q. What is ECC?
A. 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. (160,224,256,384-bits)

Q. Why have you released these two new types of algorithms?
A. We believe that our partners and customers should have expanded choice in choosing the right encryption methods for their businesses and needs. DSA and ECC have benefits over RSA in a number of scenarios and by making them available in our Enterprise and Symantec branded products for no extra charge, ensures that we are giving our partners the optimum flexibility and differentiation to be successful in the market place.

Q. Which type of certificate will make my web server faster?
A. There are many factors that can affect web server speed. Symantec offers three different kinds of algorithms so that our customers and partners can discover which certificate is the best option for their environment, or try out a combination in tandem.

Q. Are both ECC and DSA accepted by all browsers and devices?
A. 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. If you choose to implement ECC and/or DSA, you will need to install the full intermediate chain in implementation.

Q. What is my business reason for installing additional certificates?
A. 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.

Q. Will adding or changing certificates save me any money in infrastructure costs?
A. 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.

Q. Can I cover more than one server with the same certificate?
A. 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.

Q. Can I get a trial ECC or DSA certificate the same way I get a regular RSA one?
A. DSA and ECC cannot be accessed through the 30 Day Free Trial Program. The RSA certificate must be chosen for the 30 Day Free Trial and then once the 30 day passes, then the free upgrade can commence for DSA or ECC.

Q. How do I install multiple certificates on a server?
A. Each server has its own installation methods and customization plans. Please review the instructions available in our knowledge base for how to install a certificate. As stated above, you will need to install the full intermediate chain of certificates.

Q. How do I handle multiple certificates at renewal?
A. 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.

Q. What if I need to replace a certificate?
A. You can replace the certificate as usual.

Q. What happens if I need to revoke a certificate?
A. Alternative certificates can be revoked independently of one another.
CHANNEL AVAILABILITY:
Q. What is the availability of DSA on regular single certificates?
A. On April 1, 2013, DSA will be available on all Symantec branded certificates including: Symantec Secure Site, Symantec Secure Site with EV, Symantec Secure Site Wildcard, Symantec Secure Site Pro, and Symantec Secure Site Pro with EV.

Q. When will ECC be available in the channel and what certificates are applicable to ECC?
A. ECC will be available for channel later in 2013, around the same time as it is available through our Retail websites. Applicable products to ECC will be Symantec Secure Site Pro and Symantec Secure Site Pro with EV only.

Q. Do I need to be authorized to sell DSA and ECC?
A. Any partner can sell DSA and ECC as they become available on single certificates.

RESOURCES AND TOOLS:
Q. What tools are available to me today on ECC and DSA?
A. There are multiple tools that partners can utilize today to read up on these technologies:

White Paper: [Algorithm Agility](#)
Data Sheet: [Symantec SSL Certification with ECC Algorithm](#)
Data Sheet: [Symantec SSL Certificates with the DSA Algorithm](#)
PR Release: [New SSL Algorithms and Web Security Products Prepare Enterprises for the Hyper-Connected Internet and New Encryption Requirements](#)