Partner Best Practices

DigiCert Certified Partners not only have the ability to sell high quality DigiCert products, but they also have access to DigiCert's wealth of knowledge about best practices in computer security, and DigiCert is happy to assist our partners in providing the best possible experience for our mutual customers.

Partners should pay special attention to:

Maintaining a Secure Website

Partners should make sure their website and any associated functionality is free from exploitable vulnerabilities.

This can be broken down into three main categories:

1. Serve all pages over HTTPS and check your server configuration to make sure it complies with industry best practices (see https://www.ssllabs.com/ssltest/)
2. Make sure operating systems, web servers, and any other components are regularly patched and updated
3. Make sure any custom software is free from common vulnerabilities like injection flaws (https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)

Protecting Subscriber Keys

A subscriber's private key is what is used to uniquely authenticate the subscriber. It is a significant security risk if the subscriber's private key can be accessed by anyone other than the subscriber. In certain situations (for example, hosting environments), it is necessary for the hosting provider to have access to the subscriber's private key, but otherwise Partners should not have access to private keys unless absolutely necessary.

Section 6.1.2 of the Baseline Requirements states that parties other than the Subscriber SHALL NOT archive the Subscriber private key without explicit authorization by the Subscriber. Again, the best way to meet this requirement is for the Subscriber to generate the private key themselves, and for the Partner to never have access to it.

Protecting Subscriber Information

Partners should make sure that any information submitted by customers as part of the process of obtaining a certificate remains secure. As always, the best way to guarantee that subscriber information remains confidential is to not retain it any longer than it is needed.

If subscriber information needs to be stored, it should be stored in encrypted form, and access to the information should be restricted only to those who have a legitimate need to access the data.

In some cases, subscriber information is personal identifiable information (PII). In those cases, it must be handled and stored in accordance with all applicable regulations and laws.

Protecting Payment Information

Sensitive payment information like credit card numbers needs to be protected in line with all applicable local laws and compliance requirements. Payment information should only be processed by services which are designed to handle payment information, and payment information should not be stored insecurely.

Providing DigiCert Tools

DigiCert provides a number of excellent tools, including tools to assist subscribers in creating CSRs (https://www.digicert.com/csr-creation.htm). Partners are encouraged to point customers to these tools, which have been vetted to make sure they appropriately protect subscriber information.

More Information

If you are not sure how to accomplish one of the above goals, or have other questions about how to provide a secure experience for our customers, please feel free to reach out to partner-bestpractices@digicert.com.