April 15, 2016

Example Anchor, Inc. (“Example") is the operator of public certification authorities (CAs). Our CAs were the subject of the following audit reports by EY for periods ending December 31, 2015:

* Trust Service Principles and Criteria for Certification Authorities Version 2.0
* WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security - Version 2.0
* WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL - Version 1.4.5
* WebTrust Principles and Criteria for Certification Authorities - Extended Validation Code Signing

We continue to maintain the system and the control environment as described in these reports. Our control environment continues to be operated and monitored as documented and has not “materially” changed since that last report. We are not aware of any deficiencies in the criteria supporting the Security and Availability principles stated in that report as of April 15, 2016, and intend on continuing the operation of the controls. You should also be aware that we, as a normal part of our operations, continually update our services and technology as appropriate.

On April 14, 2016, Example created two new root CAs. These CAs, listed below, operate according to the certification practices disclosed in the Example Certificate Policy and Certification Practice Statement. Example commits to include these CAs in its next WebTrust audit reports for a period ending not after December 31, 2016.

|  |  |  |
| --- | --- | --- |
| CA Distinguished Name | SHA-256 Hash of Public Key Information | Key Identifier |
| CN=Example RSA Root CA – G2, O=Example, C=XX | fedaa0e62f2767c5ea658e196cd8e6df1dc2a8e3e7f516476595d58ef4ecb113 | c198adaed97c9855fe2f5465283a2386110b0982 |
| CN=Example EC Root CA – G2, O=Example, C=XX | dfcc775c644db4a33ad71293433f463c8e31057ce22cb267f9d31a0353f4fc2f | fe196207e836b7167289cdb1f912b507c59c3fc1 |

Example has securely generated Root CA Key Pairs, consisting of a public key and a private key, in a key generation ceremony witnessed by our external auditor. The auditor's report is available at <https://www.example.com/repository/xxxx.pdf>.

Management is not aware of any material security breaches or violations, or any other circumstances or conditions since the Root Key Generation Ceremony that would compromise the integrity of the Root CA Key Pairs.

This letter is not intended to be a substitute for the WebTrust reports, or to provide you with a certification of our internal controls, or to suggest to you that we have performed a separate evaluation of our internal controls for the purposes of producing this letter.

Very truly yours,

Trusty McTrusterson

Trusty McTrusterson

President

Example Anchor, Inc.

April 15, 2016

Example Anchor, Inc. (“Example") is the operator of public certification authorities (CAs). On April 14, 2016, Example created two new CAs. These CAs, listed below, operate according to the certification practices disclosed in the Example Certificate Policy and Certification Practice Statement. Example commits to include these CAs in its next WebTrust audit reports for a period ending not after December 31, 2016.

|  |  |  |
| --- | --- | --- |
| CA Distinguished Name | SHA-256 Hash of Public Key Information | Key Identifier |
| CN=Example Server CA 2016, O=Example, C=XX | 6c7d614032ed47551083d57f161b96d2b09fe5474c2bba0ecdb7777dd45e2b42 | 5f86bfcb52509d7c645758c8b1b7d92ef971db1e |
| CN=Example Extended Validation Server CA 2016, O=Example, C=XX | 9f09034bcd4f471371d0d19d710658187e2cd4b8005c9761dd0b627d69dbd715 | ccf4fa6cceddf776298ff983f3139cd7eb98d688 |

Example has securely generated the CA Key Pairs, consisting of a public key and a private key, in a key generation ceremony which was videotaped.

Management is not aware of any material security breaches or violations, or any other circumstances or conditions since the key generation ceremony that would compromise the integrity of the CA Key Pairs.

Very truly yours,

Trusty McTrusterson

Trusty McTrusterson

President

Example Anchor, Inc.

May 1, 2016

Digital Airlines Holdings LLC (“DAH") is the operator of public certification authorities (CAs). On April 14, 2016, DAH created one new CA. This CA, listed below, operates according to the certification practices disclosed in the DAH Certificate Policy and Certification Practice Statement. DAH commits to include this CAs in its next WebTrust audit reports for a period ending not after February 15, 2017.

Certificate Authority DN: /C=XX/O=Digital Airlines Inc./CN=Digital Airlines IT CA 2

Key Id: 1c22ce7fb4cd10cd09d4944f06eda01e47a5f4c8

SPKI SHA-256: e83af57c93612115579bf3fa039ee880e23431c5f64d0b2c50ae923d6256cee6

DAH has securely generated the CA Key Pair, consisting of a public key and a private key, in a key generation ceremony witnessed by Patricia Williams, CISA, a qualified auditor. The auditor's report is available at <https://pki.digitalairlines.com/xxxx.pdf>.

Management is not aware of any material security breaches or violations, or any other circumstances or conditions since the Key Generation Ceremony that would compromise the integrity of the CA Key Pairs.

Very truly yours,

Alexis Schmidt

Alexis Schmidt

Chief Information Officer

Digital Airlines Holdings, Inc.