REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of DigiCert, Inc. (“DigiCert”):

We have examined DigiCert management’s assertion that for its Symantec Certification Authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Sydney, Australia; Cape Town, South Africa; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan, throughout the period November 1, 2017 to October 31, 2018 for CAs as enumerated in Attachment B, DigiCert has:

- disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in the applicable versions of its DigiCert Certificate Policy for Symantec Trust Network (STN) and DigiCert Certification Practices Statement for Symantec Trust Network (STN) enumerated in Attachment A, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated

based on the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2. DigiCert’s management is responsible for its assertion. Our responsibility is to express an opinion on management’s assertion based on our examination.

The relative effectiveness and significance of specific controls at DigiCert and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.
Because of the nature and inherent limitations of controls, DigiCert’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion management’s assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of DigiCert’s services other than its Symantec CA operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Sydney, Australia; Cape Town, South Africa; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan, nor the suitability of any of DigiCert’s services for any customer’s intended purpose.

DigiCert’s use of the WebTrust for Certification Authorities – Extended Validation SSL Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

BDO USA, LLP

St. Louis, Missouri
January 29, 2019
Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>DigiCert Certification Practices Statement for Symantec Trust Network (STN)</td>
<td>3.9</td>
<td>September 11, 2018</td>
</tr>
<tr>
<td>Symantec Trust Network (STN) Certification Practice Statement</td>
<td>3.8.28</td>
<td>September 8, 2017</td>
</tr>
<tr>
<td>DigiCert Certificate Policy for Symantec Trust Network (STN)</td>
<td>2.9</td>
<td>September 11, 2018</td>
</tr>
</tbody>
</table>
## Attachment B - List of CAs In-Scope

<table>
<thead>
<tr>
<th>Root CA</th>
<th>Serial Number</th>
<th>SHA1 Thumbprint</th>
<th>SHA2 Thumbprint</th>
</tr>
</thead>
</table>

### Class 3 CA

<table>
<thead>
<tr>
<th>Root CA</th>
<th>Serial Number</th>
<th>SHA1 Thumbprint</th>
<th>SHA2 Thumbprint</th>
</tr>
</thead>
</table>

5
DIGICERT, INC. MANAGEMENT’S ASSERTION

DigiCert, Inc. (“DigiCert”) operates the Symantec Certification Authority ("CA") for its CAs as enumerated in Attachment B and provides EV SSL CA services.

DigiCert management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in providing its EV SSL Certification Authority (CA) services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Sydney, Australia; Cape Town, South Africa; Dublin, Ireland; Sapporo, Japan; and Kawasaki-shi, Japan, throughout the period November 1, 2017 to October 31, 2018, DigiCert has:

• disclosed its extended validation SSL (“EV SSL”) certificate lifecycle management business practices in the applicable versions of its DigiCert Certificate Policy for Symantec Trust Network (STN) and DigiCert Certification Practices Statement for Symantec Trust Network (STN) enumerated in Attachment A, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on its website, and provided such services in accordance with its disclosed practices

• maintained effective controls to provide reasonable assurance that:
  o the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  o EV SSL subscriber information is properly authenticated

based on the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.2.

DigiCert, Inc.

Jeremy Rowley
Executive VP of Product

January 29, 2019
## Attachment A - Certification Practice Statement and Certificate Policy Versions In-Scope

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>DigiCert Certification Practices Statement</td>
<td>3.9</td>
<td>September 11, 2018</td>
</tr>
<tr>
<td>Symantec Trust Network (STN) Certification Practice Statement</td>
<td>3.8.28</td>
<td>September 8, 2017</td>
</tr>
<tr>
<td>DigiCert Certificate Policy</td>
<td>2.9</td>
<td>September 11, 2018</td>
</tr>
</tbody>
</table>
### Attachment B - List of CAs In-Scope

<table>
<thead>
<tr>
<th>Root CA</th>
<th>Serial Number</th>
<th>SHA1 Thumbprint</th>
<th>SHA2 Thumbprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 3 CA</td>
<td>Serial Number</td>
<td>SHA1 Thumbprint</td>
<td>SHA2 Thumbprint</td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>

### Class 3 CA

- **C-US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G2**
  - Serial Number: 3665850778A86767A5 8FA094F8103733

- **C-US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3**
  - Serial Number: 7EE14A6F6EFF2D37 F3F6AD540D3A1DAB4

- **C-US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL SGC CA - G2**
  - Serial Number: 7AOF41DF1CD14DC B269298EE22C6A3
<table>
<thead>
<tr>
<th>Country</th>
<th>Organization 1</th>
<th>Organization 2</th>
<th>Organization 3</th>
<th>Certificate Type 1</th>
<th>Certificate Type 2</th>
<th>Certificate Type 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>C=US</td>
<td>O=GeoTrust, Inc., OU=Extended Validation SSL, CN=GeoTrust Class 3 Web PKI ECC EV CA - G1</td>
<td>C=US, O=Symantec Corporation, OU=Symantec Trust Network, OU=Extended Validation SSL, CN=Symantec Class 3 Web PKI ECC EV CA - G1</td>
<td>C=US, O=thawte, Inc., OU=Extended Validation SSL, CN=thawte Class 3 Web PKI ECC EV CA - G1</td>
<td>C=US, O=GeoTrust Inc., OU=Extended Validation SSL, CN=GeoTrust Class 3 Web PKI RSA EV CA - G1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>