

[MS-HGSA]: Host Guardian Service: Attestation Protocol

This topic lists the Errata found in the MS-HGSA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



Errata are subject to the same terms as the Open Specifications documentation referenced.

Errata below are for Protocol Document Version [V5.0 – 2018/09/12](#).

Errata Published*	Description
2019/02/19	<p>The following new sections have been added to the document:</p> <p>3.1.5.5 Receiving SigningCertificates</p> <p>3.1.5.5.1 GET</p> <p>The operation can be invoked through the following URI and transported by HTTP GET.</p> <p><code>http://<configuredServiceName>.<configuredDomain>/Attestation/VersionMajorMinor/signingCertificates</code></p> <p>VersionMajorMinor: Represents the major and minor version numbers separated by a decimal—for example, v2.0. This method is available starting with v2.0.</p> <p>The following is an example of a complete URI for this operation.</p> <p><code>http://attest.hgs151209.com/Attestation/v2.0/signingCertificates</code></p> <p>3.1.5.5.1.1 Request Body</p> <p>There is no request body.</p> <p>3.1.5.5.1.2 Response Body</p> <p>The response body for this method contains the following:</p> <p>SigningCertificates: A byte array in the format of a PKCS7-encoded object representing the public signing certificate(s) used by the service to issue health certificates.</p> <p>3.1.5.5.1.3 Processing Details</p> <p>The server MUST return the PKCS7-encoded object representing the public signing certificate(s) used by the service to issue health certificates.</p> <p>...</p> <p>3.2.4.3 Application Requests SigningCertificates</p> <p>The client requests SigningCertificates to get the certificates in the PKCS7-encoded object format representing the public signing certificate(s).</p>

*Date format: YYYY/MM/DD