2.2.1.3 AttestationResultType

AttestationResultType represents the type of the content being requested or returned by the Attestation Service.

Value		Meaning
VSMIdentityEncryptionKeyCertificate 0x00000001		A certified Virtual Secure Mode Identity Key for Encryption is being requested in the form of a health certificate.
VSMIdentitySigningKeyCertificate 0x00000002		A certified Virtual Secure Mode Identity Key for Signing is being requested in the form of a health certificate.
VSMCAIntermediateCertificate 0x00000003		An intermediate certificate authority intermediate certificate is being requested in the form of a health certificate.

Deleted: Request or Reply Type

Deleted Cells

Deleted: 0x00000001

Deleted: The VSMIDK

Deleted: as

Deleted: The VSMIDK is passed as part of the request, in a **TupleOfAttestationResultTypebase64Binary** with the content type so that it is recognizable by the server.

Deleted: ADRequest

Deleted Cells

Deleted: 0x00000001

Deleted: The virtual secure mode identity key

Deleted: signing (VSMIDKS)

Deleted: as

Deleted: The VSMIDKS will be determined from the contents of the Windows Boot Counter Log (WBCL), containing the Stored Measurement Log (SML) as defined in [TCG-Architect], after the RTPM exchange.

Deleted: AttestationRequest

Deleted Cells

Deleted: AttestationRequest

Deleted: A

Deleted: authorized

Deleted: as

Deleted: It will be generated based on the contents of the provided VSMIDKS, CaTrustletUserData, CaTrustletVsmReport, and CaTrustletVsmReportSignature.

3.1.5.1.1.3 Processing Details

If the request received is **TpmRequestInitial** or **TpmRequestContinue** and the received URI terminates with "/domainattest", the server MUST return **PayloadErrorReply** to the client.

If the server is configured to **TPM** mode, request received is **ADRequest** and received URI terminate with "/domainattest, the server MUST return **OperationModeErrorReply** to the client.

If the request received is **TpmRequestInitial**, the server MUST perform the following:

- Check if a matching entry is found between registered **EKPub** modules and the EKPub of the client that initiated the request.
  - If a matching entry is not found, set **isauthorized** to FALSE and return an **UnauthorizedErrorReply** message to the client.

    If a matching entry is found, set **isauthorized** to TRUE and construct a **TpmReplyContinue** message in an implementation-specific manner to the client's **RtpmPublicEndorsementKey**.

If the request received is **TpmRequestContinue** or **AttestationRequest** from the client, the server MUST process the following:

- Check if a matching entry is found between registered EKPub modules and the EKPub of the client. Update **isauthorized** to TRUE if a matching entry is found.
- If **isauthorized** is FALSE for **RtpmPublicEndorsementKey** received from client, return **UnauthorizedErrorReply** to the client.
- If **isauthorized** is TRUE and **RtpmNewContext** received from the client is empty, return **TpmReplyContinue** message to the client with the empty context.

Otherwise,

- Perform the policy evaluation against the list of policies the server is configured to, in an implementation-specific manner with the WBCL that is retrieved from the underlying RTPM protocol and the **RtpmPublicEndorsementKey**.
- If the policy evaluation is successful, the server MUST do the following:

Deleted: return **HealthCertificateReply** with the new **AttestationHealthCertificate** to the client.

- If AttestationResultType in AttestationRequest or TpmRequest is VSMIdentityEncryptionKeyCertificate, return **HealthCertificateReply** in the form of certified Virtual Secure Mode Identity Key for Encryption with **AttestationHealthCertificate** to the client.

- If AttestationResultType in AttestationRequest or TpmRequest is VSMIdentitySigningKeyCertificate, return **HealthCertificateReply** in the form of certified Virtual Secure Mode Identity Key for Signing with **AttestationHealthCertificate** to the client.

- If AttestationResultType in AttestationRequest or TpmRequest is VSMCAIntermediateCertificate, return a **HealthCertificateReply** in the form of intermediate certificate authority with **AttestationHealthCertificate** to the client.

Otherwise,

return **PolicyEvaluationErrorReply** with **EvaluationLog** to the client.

3.1.5.2.1.3 Processing Details

If the request received is **ADRequest** and received URI terminate with "/attest", the server MUST return **PayloadErrorReply** to the client.

If the server is configured to AD mode, request received is **TpmRequestInitial** or **TpmRequestContinue** and received URI terminate with "/attest", the server MUST return **OperationModeErrorReply** to the client.

If the request received is **ADRequest**, the server MUST perform the following:

- If policy evaluation is successful, update **AttestationHealthCertificate** and do the following:

  Deleted: return **HealthCertificateReply** to the client.

  - If AttestationResultType in ADRequest is VSMIdentityEncryptionKeyCertificate, return **HealthCertificateReply** in the form of certified Virtual Secure Mode Identity Key for Encryption to the client.

  - If AttestationResultType in ADrequest is VSMIdentitySigningKeyCertificate, return **HealthCertificateReply** in the form of certified Virtual Secure Mode Identity Key for Signing to the client.

  - If AttestationResultType in ADRequest is VSMCAIntermediateCertificate, return **HealthCertificateReply** in the form of intermediate certificate authority to the client.

- Otherwise, return **UnauthorizedErrorReply** to the client indicating that the host is not authorized.

  Deleted: PolicyEvaluationErrorReply

  Deleted: with **EvaluationLog**

  Deleted: policy evaluation has failed on the server side.

If the **VSMIKD** received is invalid, the server MUST return **VirtualSecureModeErrorReply** to the client.