|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CONFIG. | SERVER VERY-MOBILE & ILIAD | SERVER TIM | SERVER GSMA | SERVER GOOGLE | SERVER INFINEON |
| Tutto corretto (inclusa la signature) coi certificati custom | Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2] | Verification failed on EUM certificate | HTTP\_INTERNAL\_SERVER\_ERROR | gli ID delle CI Public Key non sono validi | BAD\_REQUEST |
| Tutto corretto (eccetto la signature) coi certificati custom | Internal error while verifying token signature: | Unknown eSIM CA RootCA Public Key. The eSIM CA is not a trusted root for the SM-DP+, or not the root elected by the SM-DP+ in InitiateAuthentication response. | HTTP\_INTERNAL\_SERVER\_ERROR | gli ID delle CI Public Key non sono validi | BAD\_REQUEST |
| TransactionId corretto + certificati custom + signature e serverChallenge dalla cattura originale | Internal error while verifying token signature: | eUICC signature is invalid or serverChallenge is invalid. | HTTP\_INTERNAL\_SERVER\_ERROR | gli ID delle CI Public Key non sono validi | BAD\_REQUEST |
| TransactionId corretto + lettura dei certificati GSMA da file + signature e serverChallenge dalla cattura originale | Internal error while verifying token signature: parsing issue: DEF length 68 object truncated by 64 | eUICC signature is invalid or serverChallenge is invalid. | HTTP\_INTERNAL\_SERVER\_ERROR | gli ID delle CI Public Key non sono validi | BAD\_REQUEST |
| TransactionId dalla cattura originale + lettura dei certificati GSMA da file + signature e serverChallenge dalla cattura originale | transactionId has got an invalid value | The RSP session identified by the TransactionID is unknown. | HTTP\_INTERNAL\_SERVER\_ERROR | gli ID delle CI Public Key non sono validi | BAD\_REQUEST |
| Campi in base64 perfettamente copia-incollati dalla cattura originale | HTTP\_BAD\_REQUEST | “Status: Failed” generico | The RSP session identified by the TransactionID is unknown. | gli ID delle CI Public Key non sono validi | BAD\_REQUEST |
| Indirizzo IP al posto di hostname | FORBIDDEN | NOT\_FOUND | FORBIDDEN | FORBIDDEN | BAD\_REQUEST |

**CRAWLING FATTO PIÙ SERIAMENTE**

GOOGLE (sgp-brp)  
1) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“message”: “Execution Failed”* 🡪 none of the proposed Public Key Identifiers is supported by the SM-DP+.  
2) n.d.  
3) n.d.  
4) n.d.  
5.1) n.d.  
5.2) n.d.  
5.3) n.d.  
6.1) n.d.  
6.2) n.d.  
7.1) n.d.  
7.2) n.d.  
8) n.d.  
9) n.d.  
10) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“message”: “Execution Failed”* 🡪 none of the proposed Public Key Identifiers is supported by the SM-DP+.  
11) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“message”: “Execution Failed”* 🡪 invalid SM-DP+ address.  
12.1) **if len(svn) != 3 byte**: HTTP\_INTERNAL\_SERVER\_ERROR (500) al primo messaggio di risposta.  
**else**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.3”*, *“reasonCode”: “3.1”*, *“message”: “Execution Failed”* 🡪 svn not valid.  
12.2) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“message”: “Execution Failed”* 🡪 none of the proposed Public Key Identifiers is supported by the SM-DP+.  
13.1) Common Cancel Session Procedure completata con successo.  
13.2) n.d.  
14.1) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“message”: “Execution Failed”* 🡪 the RSP session identified by the TransactionID is unknown.  
14.2) n.d.  
15) n.d.Cert) n.d.

GSMA  
1) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “eUICC”*, *“message”: “serverChallenge is invalid”*.  
3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.11.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “CI Public Key”*, *“message”: “Unknown CI Public Key. The CI used by the EUM Certificate is not a trusted root for the SM-DS”*.  
4) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
5.1) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
5.2) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
5.3) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
6.1) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
6.2) n.d.  
7.1) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
7.2) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
8) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
9) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
10) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
11) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.9.1”*, *“reasonCode”: “3.8”*, *“subjectIdentifier”: “SM-DS Address”*, *“message”: “Invalid SM-DS Address”*.  
12.1) **if len(svn) != 3 byte**: HTTP\_INTERNAL\_SERVER\_ERROR (500) al primo messaggio di risposta.  
**else**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.9.3”*, *“reasonCode”: “3.1”*, *“message”: “Execution Failed”* 🡪 svn not valid.  
12.2) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.9.2”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Security configuration”*, *“message”: “None of the proposed Public Key Identifiers is supported by the SM-DS”*.  
13.1) HTTP\_NOT\_FOUND (404) al primo messaggio.  
13.2) HTTP\_NOT\_FOUND (404) al secondo messaggio.  
14.1) HTTP\_NOT\_FOUND (404) al primo messaggio.  
14.2) HTTP\_NOT\_FOUND (404) al secondo messaggio.  
15) n.d.  
Cert) **Algorithm**: ecdsaWithSHA256; **issuer organizationName**: GSM Association; **issuer commonName**: GSM Association – RSP2 Root CI1; **validity notBefore**: 2023-06-21; **validity notAfter**: 2026-06-20; **countryName**: DE; **localityName**: Frankfurt; **organizationName**: Thales SA; **organizationalUnitName**: IT; **commonName**: GCP EW3 PROD SMDS; **crLDistributionPoints**: http://gsma-crl.symauth.com/offlineca/gsma-rsp2-root-ci1.crl; **authorityKeyIdentifier**: rsp2.

ILIAD & VERY MOBILE  
1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
2) HTTP\_NO\_CONTENT (204) al secondo messaggio di risposta.  
3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: ”*.  
4) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
5.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
5.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
5.3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
6.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
6.2) n.d.  
7.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
7.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “<transactionId value>”*, *“message”: “The transactionID is not correct”*.  
8) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“subjectIdentifier”: “<smdpAddress value>”*, *“message”: “The server address is not correct”*.  
9) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “1.2”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “Function provider”*, *“message”: “Internal error while verifying token signature: Invalid Certificate Policies: [2.5.29.35, 2.23.146.1.2.1.2]”*.  
10) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “1.6”*, *“reasonCode”: “2.1”*, *“subjectIdentifier”: “Function”*, *“message”: “Euicc challenge format is not Octet[16]”*.  
11) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“subjectIdentifier”: “<smdpAddress value>”*, *“message”: “The SM-DP address sent by the LPA is unknown”*.  
12.1) **if len(svn) != 3 byte**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “1.6”*, *“reasonCode”: “2.1”*, *“subjectIdentifier”: “Function”*, *“message”: “euiccInfo1 tlv is invalid”*.  
**else**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.3”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Specification Version Number”*, *“message”: “The version SVN sent by the card is not in range[2.0, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 3.0, 3.1, 3.2]”*.  
12.2) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.3”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “SM-DP+ Certificate”*, *“message”: “The SM-DP+ has no CERT.DPauth.SIG which chains to one of the eSIM CA RootCA Certificate with a Public Key supported by the eUICC”*.  
13.1) Common Cancel Session Procedure completata con successo.  
13.2) Common Cancel Session Procedure completata con successo.  
14.1) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “<transactionId value>”*, *“message”: “Cannot retrieve the bound profile package with the current transactionId [<transactionId value>]”*.  
14.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “<transactionId value>”*, *“message”: “Cannot retrieve the bound profile package with the current transactionId [<transactionId value>]”*.  
15) n.d.  
Cert) **Algorithm**: ecdsaWithSHA256; **issuer organizationName**: GSM Association; **issuer commonName**: GSM Association – RSP2 Root CI1; **validity notBefore**: 2021-10-28; **validity notAfter**: 2024-10-27; **countryName**: DE; **localityName**: Frankfurt; **organizationName**: Thales SA; **organizationalUnitName**: IT; **commonName**: SMDP+ GCP EW3 MULTITENANT; **crLDistributionPoints**: http://gsma-crl.symauth.com/offlineca/gsma-rsp2-root-ci1.crl; **authorityKeyIdentifier**: rsp2.

INFINEON (sgp-brp)  
1) HTTP\_BAD\_REQUEST (400) al primo messaggio di risposta.  
2) n.d.  
3) n.d.  
4) n.d.  
5.1) n.d.  
5.2) n.d.  
5.3) n.d.  
6.1) n.d.  
6.2) n.d.  
7.1) n.d.  
7.2) n.d.  
8) n.d.  
9) n.d.  
10) HTTP\_BAD\_REQUEST (400) al primo messaggio di risposta.  
11) HTTP\_BAD\_REQUEST (400) al primo messaggio di risposta.  
12.1) HTTP\_BAD\_REQUEST (400) al primo messaggio di risposta.  
12.2) HTTP\_BAD\_REQUEST (400) al primo messaggio di risposta.  
13.1) HTTP\_BAD\_REQUEST (400) al primo messaggio di risposta.  
13.2) n.d.  
14.1) HTTP\_BAD\_REQUEST (400) al primo messaggio di risposta.  
14.2) n.d.  
15) n.d.  
Cert) n.d.

TIM  
1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8.4”*, *“reasonCode”: “2.1”*, *“subjectIdentifier”: “SMDP+ Certificate”*, *“message”: “Invalid”*.  
3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.11.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “GSMA CI”*, *“message”: “Unknown”* 🡪 unknown CI Public Key. The CI used by the EUM Certificate is not a trusted root for the SM-DS.  
4) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
5.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
5.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
5.3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
6.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
6.2) n.d.  
7.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “Transaction ID”*, *“message”: “Unknown”*.  
7.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “Transaction ID”*, *“message”: “Unknown”*.  
8) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
9) *“status”: “Failed”* al secondo messaggio di risposta, senza ulteriori informazioni.  
10) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”*, *“message”: “Execution Error”*.  
11) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“subjectIdentifier”: “SM-DP+ Address”*, *“message”: “Refused”*.  
12.1) **if len(svn) != 3 byte**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”*, *“message”: “Execution Error”*.  
**else**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.3”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Specification Version Number”, “message”: “Unsupported”*.  
12.2) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Security configuration”, “message”: “Unsupported”*.  
13.1) Common Cancel Session Procedure completata con successo.  
13.2) Common Cancel Session Procedure completata con successo.  
14.1) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “Transaction ID”, “message”: “Unknown”*.  
14.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”, “message”: “Execution Error”*.  
15) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”, “message”: “Execution Error”*.  
Cert) **Algorithm**: ecdsaWithSHA256; **issuer organizationName**: GSM Association; **issuer commonName**: GSM Association – RSP2 Root CI1; **validity notBefore**: 2021-12-08; **validity notAfter**: 2031-12-07; **countryName**: FR; **localityName**: Paris; **organizationName**: IDEMIA; **commonName**: Azure SM-DP 401; **crLDistributionPoints**: http://gsma-crl.symauth.com/offlineca/gsma-rsp2-root-ci1.crl; **authorityKeyIdentifier**: rsp2.

GEMELLO DI TIM  
1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8.4”*, *“reasonCode”: “2.1”*, *“subjectIdentifier”: “SMDP+ Certificate”*, *“message”: “Invalid”*.  
3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.11.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “GSMA CI”*, *“message”: “Unknown”* 🡪 unknown CI Public Key. The CI used by the EUM Certificate is not a trusted root for the SM-DS.  
4) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
5.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
5.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
5.3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
6.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
6.2) n.d.  
7.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “Transaction ID”*, *“message”: “Unknown”*.  
7.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “Transaction ID”*, *“message”: “Unknown”*.  
8) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.2”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “EUM Certificate”*, *“message”: “Verification Failed”*.  
9) *“status”: “Failed”* al secondo messaggio di risposta, senza ulteriori informazioni.  
10) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”*, *“message”: “Execution Error”*.  
11) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“subjectIdentifier”: “SM-DP+ Address”*, *“message”: “Refused”*.  
12.1) **if len(svn) != 3 byte**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”*, *“message”: “Execution Error”*.  
**else**: *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.3”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Specification Version Number”, “message”: “Unsupported”*.  
12.2) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Security configuration”, “message”: “Unsupported”*.  
13.1) Common Cancel Session Procedure completata con successo.  
13.2) Common Cancel Session Procedure completata con successo.  
14.1) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “Transaction ID”, “message”: “Unknown”*.  
14.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”, “message”: “Execution Error”*.  
15) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8”*, *“reasonCode”: “4.2”*, *“subjectIdentifier”: “SM-DP+”, “message”: “Execution Error”*.  
Cert) **Algorithm**: ecdsaWithSHA256; **issuer organizationName**: GSM Association; **issuer commonName**: GSM Association – RSP2 Root CI1; **validity notBefore**: 2017-04-13; **validity notAfter**: 2027-04-12; **countryName**: RO; **localityName**: Otopeni; **organizationName**: Oberthur Technologies Romania SRL; **commonName**: Oberthur Technologies SM-DP 01; **crLDistributionPoints**: http://gsma-crl.symauth.com/offlineca/gsma-rsp2-root-ci1.crl; **authorityKeyIdentifier**: rsp2.

OSMO-SMDPP (sgp-brp)  
1) *“status”: “Executed-Success”*.  
2) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.11.1”*, *“reasonCode”: “3.9”*, *“message”: “Unknown”* 🡪 unknown CI Public Key. The CI used by the EUM Certificate is not a trusted root for the SM-DS.  
4) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1”*, *“reasonCode”: “6.1”*, *“message”: “Verification failed”* 🡪 eUICC signature is invalid.  
**Caso particolare di lunghezza della signature errata**: HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
5.1) *“status”: “Executed-Success”*.  
5.2) *“status”: “Executed-Success”*.  
5.3) *“status”: “Executed-Success”*.  
6.1) *“status”: “Executed-Success”*.  
6.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.2.6”*, *“reasonCode”: “3.8”*, *“message”: “Refused”* 🡪 matchingID does not match a valid order.  
7.1) *“status”: “Executed-Success”*.  
7.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“message”: “Unknown”* 🡪 The RSP session identified by the TransactionID is unknown.  
8) *“status”: “Executed-Success”*.  
9) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1”*, *“reasonCode”: “6.1”*, *“message”: “Verification failed”* 🡪 eUICC signature is invalid.  
10) HTTP\_INTERNAL\_SERVER\_ERROR (500) al primo messaggio di risposta.  
11) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“message”: “Invalid SM-DP+ Address”*.  
12.1) *“status”: “Executed-Success”*.  
12.2) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“message”: “None of the proposed Public Key Identifiers is supported by the SM-DP+”*.  
13.1) Common Cancel Session Procedure completata con successo.  
13.2) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
14.1) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“message”: “The RSP session identified by the TransactionID is unknown”*.  
14.2) HTTP\_INTERNAL\_SERVER\_ERROR (500) al secondo messaggio di risposta.  
15) HTTP\_INTERNAL\_SERVER\_ERROR (500) al primo messaggio di risposta.  
Cert) **Algorithm**: ecdsaWithSHA256; **issuer organizationName**: RSPTEST; **issuer organizationalUnitName**: TESTCERT; **issuer commonName**: Test CI – RSP2 Root CI1; **issuer countryName**: IT; **validity notBefore**: 2020-04-01; **validity notAfter**: 2030-03-30; **organizationName**: ACME; **commonName**: TEST SM-DP+; **crLDistributionPoints**: http://ci.test.example.com/CRL-A.crl - http://ci.test.example.com/CRL-B.crl; **authorityKeyIdentifier**: sgp.

SIMULATORE  
1) *“status”: “Executed-Success”*.  
2) Secondo messaggio di risposta vuoto.  
3) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1.3”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “eUICC Certificate”*, *“message”: “Verification Failed”* 🡪 eUICC Certificate or any Certificate in the trust chain is invalid.  
4) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “eUICC”*, *“message”: “Verification failed”* 🡪 eUICC signature is invalid.  
5.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1”*, *“reasonCode”: “3.11”*, *“subjectIdentifier”: “eUICC”*, *“message”: “Value has Changed”*.  
5.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Security configuration”*, *“message”: “Unsupported”*.  
5.3) *“status”: “Executed-Success”*.  
6.1) *“status”: “Executed-Success”*.  
6.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.2.6”*, *“reasonCode”: “3.10”*, *“subjectIdentifier”: “Matching ID”*, *“message”: “Invalid Association”* 🡪 Indicates that a different matchingID is associated with this ICCID.  
7.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “TransactionId”*, *“message”: “Unknown”*.  
7.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “TransactionId”*, *“message”: “Unknown”*.  
8) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“subjectIdentifier”: “SM-DP+ Address”*, *“message”: “Refused”*.  
9) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1”*, *“reasonCode”: “6.1”*, *“subjectIdentifier”: “eUICC”*, *“message”: “Verification failed”*.  
10) *“status”: “Executed-Success”*.  
11) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.8.1”*, *“reasonCode”: “3.8”*, *“subjectIdentifier”: “SM-DP+ Address”*, *“message”: “Refused”*.  
12.1) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.1”*, *“reasonCode”: “3.11”*, *“subjectIdentifier”: “eUICC”*, *“message”: “Value has Changed”*.  
12.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Security configuration”*, *“message”: “Unsupported”*.  
13.1) Common Cancel Session Procedure completata con successo.  
13.2) Common Cancel Session Procedure completata con successo.  
14.1) *“status”: “Failed”* al primo messaggio di risposta, con *“subjectCode”: “8.10.1”*, *“reasonCode”: “3.9”*, *“subjectIdentifier”: “TransactionId”, “message”: “Unknown”*.  
14.2) *“status”: “Failed”* al secondo messaggio di risposta, con *“subjectCode”: “8.8.2”*, *“reasonCode”: “3.1”*, *“subjectIdentifier”: “Security configuration”*, *“message”: “Unsupported”*.  
15) Il server non è in grado di processare più richieste in parallelo.  
Cert) **Algorithm**: ecdsaWithSHA256; **issuer organizationName**: Fanfa Association; **issuer commonName**: Fanfa Association – RSP2 Root CI1; **validity notBefore**: 2024-04-12; **validity notAfter**: 2034-04-10; **countryName**: FR; **localityName**: Tours; **organizationName**: Thales DIS France SA; **organizationalUnitName**: ODC; **commonName**: SMDP Plus Torus Platform; **crLDistributionPoints**: http://gsma-crl.symauth.com/offlineca/gsma-rsp2-root-ci1.crl; **authorityKeyIdentifier**: fanfa.

**LEGENDA**1) Il simulatore client si comporta perfettamente come da specifiche.  
2) Manomissione 2° messaggio: authenticateResponseError anziché authenticateResponseOk.  
3) Manomissione 2° messaggio: utilizzo di altri certificati lato client.  
4) Manomissione 2° messaggio: calcolo errato della signature.  
5.1) Manomissione 2° messaggio (campo euiccInfo2): utilizzo di un svn non atteso.  
5.2) Manomissione 2° messaggio (campo euiccInfo2): utilizzo di euiccCiPKIdListForVerification ed euiccCiPKIdListForSigning non attesi.  
5.3) Manomissione 2° messaggio (campo euiccInfo2): sasAcreditationNumber = stringa vuota.  
6.1) Manomissione 2° messaggio (campo ctxParams1): eliminazione del sotto-campo imei.  
6.2) Manomissione 2° messaggio (campo ctxParams1): matchingId = stringa a caso / stringa vuota.  
7.1) Manomissione 2° messaggio: transactionId non valido all’interno di euiccSigned.  
7.2) Manomissione 2° messaggio: transactionId non valido fuori da tutto.  
8) Manomissione 2° messaggio: smdpAddress non valido.  
9) Manomissione 2° messaggio: serverChallenge non valida.  
10) Manomissione 1° messaggio: euiccChallenge malforme (e.g. 0x00).  
11) Manomissione 1° messaggio: smdpAddress non valido.  
12.1) Manomissione 1° messaggio: utilizzo di un svn non atteso.  
12.2) Manomissione 1° messaggio: utilizzo di euiccCiPKIdListForVerification ed euiccCiPKIdListForSigning non attesi.  
13.1) Avvio della Common Cancel Session Procedure come 1° messaggio.  
13.2) Avvio della Common Cancel Session Procedure come 2° messaggio.  
14.1) Invio di getBoundProfilePackage come 1° messaggio.  
14.2) Invio di getBoundProfilePackage come 2° messaggio.  
15) Invio di getBoundProfilePackage come 1° messaggio col transactionId pari a un ID di transazione di un’altra connessione messa appositamente in sleep.  
Cert) Informazioni sul certificato inviato dal server.