1. Integration Approach

1.1 Integration Process

Steps to generate request & read response messages.

- Agent Institution will first send request to Customer OU to get AES Key.
- This Request will contain Agent Institution ID and token shared with Agent Institution at the time of on-boarding. Request will be encrypted using Customer OU RSA Public Key.
- Agent Institution will generate Digital Signature on RRN, Timestamp and Cipher Text using Agent.

  Institution RSA Private Key.
- Request Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.
- Customer OU will verify Digital Signature using Agent Institution RSA Public key.
- Customer OU will decrypt the request using Customer OU Agent Institution Specific RSA Private Key.
- Customer OU will verify if the token is valid and not expired. If token is valid, Customer OU will generate Random AES (256) Key. Generated key will remain in memory and will not be stored in the database. ● Customer OU will encrypt Random AES Key using RSA Agent Institution Public Key to get Cipher Text.
- Customer OU will generate Digital Signature using Customer OU Agent Institution Specific RSA Private Key.
- Request Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.
- Agent Institution will first verify Digital Signature using Customer OU RSA Public key.
- Agent Institution will decrypt Cipher Text using Agent Institution RSA Private Key to get AES Key.
- Agent Institution will validate the timestamp. Timestamp cannot be older than 3 minutes (configurable).
- Agent Institution will generate the transaction request.
- Agent Institution will encrypt Complete Transaction Request payload using decrypted AES Key.
- Agent Institution will generate Digital Signature on Cipher Text using Agent Institution RSA Private Key.
- Request Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.
- Customer OU will verify Digital Signature using Agent Institution RSA Public key.
- Customer OU will validate RRN and fetch AES Key from memory based on RRN.

- Customer OU will validate the timestamp. Timestamp cannot be older than 3 minutes (configurable).
- Customer OU will decrypt Cipher Text using AES Key.
- Customer OU will process the transaction request.
- Customer OU will encrypt Complete Response payload using AES Key to get Cipher Text.
- Customer OU will generate Digital Signature on Cipher Text using Customer OU RSA Private Key.
- Response Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.
- Agent Institution will verify Digital Signature of Response using Customer OU RSA Public key.

Agent Institution will validate the timestamp. Timestamp cannot be older than 3 minutes (configurable).

1.2 Encryption and Decryption Logic

COU will share **"integration kit jar"** library and RSA Public Key <PUBLIC_KEY> and token <Token>. Using this library agent institution can encrypt and decrypt data wherever required.

AI will have to share the RSA Public Key <PUBLIC_KEY> with COU.

Note: PUBLIC_KEY and Token will be shared over email or AI Portal

Request/ Response Generation Mechanism

Step 1: AI has to call getAccessToken API to get the AES Symmetric key from the COU, this key will be used to encrypt the JSON text.

This Request will contain Agent Institution ID and token shared with Agent Institution at the time of onboarding. Request will be encrypted using Customer OU RSA Public Key.

Plain Text Request Message:

```
{
  "agentInstitutionId":  "SB22",
  "token": "6ffbeb77133c15ca241565135e103a78"
}
```

Encrypted Request Message:

GMELR96RXtz2r72zwp2J3wv0chLwcP5q68XNokss9SUmZisApzJ+nBcs88bvE+9bc/Urupx+9b6sCBLCkV6xowgXD
98/Z9osqpb6OrZ+4pLN1yC9gONhB69Jv1RAmp8jHIwR9hBd3om1Op3FvBJxQyr2XZrLQs4bczT4zESq6lNNN5UkK
ms6+F5DQdE61xZGSJWYfG71OT4I9GY9CiUzhTtZKsbLD4Hk4RW/1Vw/tAvk5Q5fJu4U5+RGAO2PQdbvIMMai/z+
g1mcubsFZw1IC0X+OfJC5dHL9epytRDPNYQQwhQO5+cM0AU7tanJt6LI2mpPl7sBDxyo7MGapznCnP8AGSRc8ai
HZHQRzIa+XkZ2ueEIPpRtam2rg+SIFe9oHKzvNwK0ORfau8USBtkEAuqh37TIMFSuUMe+rZj8u77prbS1SVekX+jjU
0z918rC+MyO4tiZKzNszJSZ7VWKKKFMBYrB8KsLqcC7e0ya5Fwt4SRvtt0aH0G2Rw9EzlPq

Step 2: *Agent Institution will generate Digital Signature on Cipher Text using Agent Institution RSA Private Key.*

Request Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.

Encrypted Request:

```
{
  "rrn": "SBI3c6db50ac7454fe9904a20de4e07fc78",
  "cipherText":
"wSQjywJsV4SjN5M5b3TvKAra3m9l4wSM7A03tISQXoxBzTFdw918Y/mjZtEyiSMzI8+v4uwqTGSyiCm+xQMK/c
W4TkeyXMsiAhe1Vv5E+x3pcVhfvPRmSxe9zmLqnKkOYCADFQNV85tdeOlJ6K6LAtw/i4yKgRYMG/VH/H3KRLXF0
ZnU3O+aDdG0IRfLwaxuPOr7mooDqMbOxdk8V1oIbgBpXWe0yIabw++F546Pm7C1ffW+Qskpm/uXbH+nAgA6H
hrBR5po4Wi9lp2L9Rt3ia8Sn4rK4Jec8AH7EW3LCnw6LqT2uatol2WRf1TRG4mWHOLYjYkazg0yVaG6CcP4QNpdv
qTwjuJkctOy90opJxqEbdSdwkN1lHOXPQJhbw5Ruw/oPgn0LunGpK5IRUSaVAEpURiucrnPdBE58IKZI2MyHYpslP
8QtMB9eXyOFs0UR2mr9smu9sKSLutWdaVZDgg1rV/fyXUEMUvATlnOb2eX+uDNRYOkE3DCdtXrl5rI",
"digitalSig":
"C/00U1lV07QBRqkMXPyHg1YEibePqA6ORyd0FFeW7NdAIRCyiLKG+qj4XN/d8d5eZSsQGP6e4NGGu8I17c8J5wi
8/c6gz/kPKtiR9xVxNtm0Ok3KDA7EumJ4B1MkKiJrQ9l+p03/NpIV9zogYZRbOqAHrSMMEpQXGDtuDwQSBx01oy
tpoosVdt2CLaEqtveOyvn3GY49P2F5ya243foxFXsdxjNA+e4fTkE38y/mMZyv8C4tnulXE9KdvffPFRncyITsblFfFHjtn
k+ZAPI6jDBf8gumguLXVjJmfkqtrdjAUMDBDsYBm+QGzrCNsCErd5zf3ROGta8xfqbZ9ksUmw==",
"ts": "2020-10-26T22:00:35+05:30"
}
```

Step 3: *Customer OU will generate the response and send it to the Agent Institution.*

Response Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.

Encrypted Response:

```
{
  "rrn": "SBI3c6db50ac7454fe9904a20de4e07fc78",
  "cipherText":
"fX6FhBMlEeMS2qb8N477SDSWH/D3r3aKvcIwJk6dvqEwmiLR2+ZctcDYSMkCkrgzZmXBCGYn2TPoiBXjvPOWG1
Q2FQkmuUrOEAakkzxgZadyOEljy8QkC/o07dPne5g5vEe+djAMkbtya+RTqCILRXIoEqxgamDOrPcvQFtqF7KpQTek
u1fjrOiug5oMW665HvBDBw6qI/JN3+DU4YEOoNk+LO8Ks+Ij3cWxYxhYtYp1tJzSkDtovwG5EDrM39i6aL4UeFAGS
qQP7sQMHFC5JKlTGA+/x+5GOMF9YpMZSAsmbtzvv6u8V2x9bHElfgBCP1fsPLZScl7Dhm/4nUATDA==",
"digitalSig":
"aoATRDAyk7xFfaYRSFngBK7eYBmOGSK1xersfeMHPDv5bxqE1xJdy7072EGTrPCxJx660lOfEorHFWercDOaCOiJu
7tnWfvhKfUM1UsVuymTJ12MkcecQOcZ/ynoQaTzWECWud7gKKvGNp/W/8gTl65R+jbNz0u5kP4xukUVedN+AjK
2DhYf9IfdkJJ6DAtPG6uP0ol3ScjbqBy5WVmODpX1rtS3cQ95WVC56+vAuZLUK00W3Y5efEZ05F/E1RM3C1oRHYg
3gXR3ZIWeU+kVr401Q3l5mwVwD+uZrG1UQ+xuPkDo7by0WT/JRbKBltHikOa+x8h5ZsGhQ9a9HkOG6w==",
"ts": "2020-10-26T22:01:08+05:30"
}
```

Step 4: *Agent Institution will first verify Digital Signature using Customer OU RSA Public key.*

Agent Institution will decrypt Cipher Text using Agent Institution RSA Private Key to get AES Key.

Encrypted Response Message:

fX6FhBMlEeMS2qb8N477SDSWH/D3r3aKvcIwJk6dvqEwmiLR2+ZctcDYSMkCkrgzZmXBCGYn2TPoiBXjvPOWG1Q
2FQkmuUrOEAakkzxgZadyOEljy8QkC/o07dPne5g5vEe+djAMkbtya+RTqCILRXIoEqxgamDOrPcvQFtqF7KpQTeku
1fjrOiug5oMW665HvBDBw6qI/JN3+DU4YEOoNk+LO8Ks+Ij3cWxYxhYtYp1tJzSkDtovwG5EDrM39i6aL4UeFAGSq
QP7sQMHFC5JKlTGA+/x+5GOMF9YpMZSAsmbtzvv6u8V2x9bHElfgBCP1fsPLZScl7Dhm/4nUATDA==

Plain Text Response Message:

```
{
  "reason": {
    "responseCode": "000",
    "responseReason": "Successful",
    "complianceRespCd": "",
    "complianceReason": ""
  },
  "accessToken": "5aaf9baf5988cecef01b041fca54eed9"
}
```

Step 5: *Agent Institution will generate the transaction request.*

Agent Institution will encrypt Complete Transaction Request payload using decrypted AES Key.

Plain Text Request Message:

```
{
  "head": {
    "requestId": "OU01OU02INT522274495200721ahbcj2123", "ts":
    "2020-07-21T22:02:35+05:30"
  },
  "search": {
    "status": ""
  }
}
```

Encrypted Request Message:

GMELR96RXtz2r72zwp2J3wv0chLwcP5q68XNokss9SUmZisApzJ+nBcs88bvE+9bc/Urupx+9b6sCBLCkV6xowgXD
98/Z9osqpb6OrZ+4pLN1yC9gONhB69Jv1RAmp8jHIwR9hBd3om1Op3FvBJxQyr2XZrLQs4bczT4zESq6lNNN5UkK
ms6+F5DQdE61xZGSJWYfG71OT4I9GY9CiUzhTtZKsbLD4Hk4RW/1Vw/tAvk5Q5fJu4U5+RGAO2PQdbvIMMai/z+
g1mcubsFZw1IC0X+OfJC5dHL9epytRDPNYQQwhQO5+cM0AU7tanJt6LI2mpPl7sBDxyo7MGapznCnP8AGSRc8ai
HZHQRzIa+XkZ2ueEIPpRtam2rg+SIFe9oHKzvNwK0ORfau8USBtkEAuqh37TIMFSuUMe+rZj8u77prbS1SVekX+jjU
0z918rC+MyO4tiZKzNszJSZ7VWKKKFMBYrB8KsLqcC7e0ya5Fwt4SRvtt0aH0G2Rw9EzlPq

Step 6: *Agent Institution will generate Digital Signature on Cipher Text using Agent Institution RSA Private Key.*

Request Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.

Encrypted Response:

```
{
  "rrn": "SBI3c6db50ac7454fe9904a20de4e07fc78", "cipherText":
"fX6FhBMlEeMS2qb8N477SDSWH/D3r3aKvcIwJk6dvqEwmiLR2+ZctcDYSMkCkrgzZmXBCGYn2TPoiBXjvPOWG1
Q2FQkmuUrOEAakkzxgZadyOEljy8QkC/o07dPne5g5vEe+djAMkbtya+RTqCILRXIoEqxgamDOrPcvQFtqF7KpQTek
u1fjrOiug5oMW665HvBDBw6qI/JN3+DU4YEOoNk+LO8Ks+Ij3cWxYxhYtYp1tJzSkDtovwG5EDrM39i6aL4UeFAGS
qQP7sQMHFC5JKlTGA+/x+5GOMF9YpMZSAsmbtzvv6u8V2x9bHElfgBCP1fsPLZScl7Dhm/4nUATDA==",
"digitalSig":
"aoATRDAyk7xFfaYRSFngBK7eYBmOGSK1xersfeMHPDv5bxqE1xJdy7072EGTrPCxJx660lOfEorHFWercDOaCOiJu
7tnWfvhKfUM1UsVuymTJ12MkcecQOcZ/ynoQaTzWECWud7gKKvGNp/W/8gTl65R+jbNz0u5kP4xukUVedN+AjK
2DhYf9IfdkJJ6DAtPG6uP0ol3ScjbqBy5WVmODpX1rtS3cQ95WVC56+vAuZLUK00W3Y5efEZ05F/E1RM3C1oRHYg
3gXR3ZIWeU+kVr401Q3l5mwVwD+uZrG1UQ+xuPkDo7by0WT/JRbKBltHikOa+x8h5ZsGhQ9a9HkOG6w==", "ts":
"2020-10-26T22:01:08+05:30"
}
```

Step 7: *Customer OU will generate the response for transaction and send it to the Agent Institution.*

Response Body will contain RRN, Cipher Text, Timestamp, and Digital Signature.

Encrypted Response:

```
{
  "rrn": "SBI3c6db50ac7454fe9904a20de4e07fc78", "cipherText":
"fX6FhBMlEeMS2qb8N477SDSWH/D3r3aKvcIwJk6dvqEwmiLR2+ZctcDYSMkCkrgzZmXBCGYn2TPoiBXjvPOWG1
Q2FQkmuUrOEAakkzxgZadyOEljy8QkC/o07dPne5g5vEe+djAMkbtya+RTqCILRXIoEqxgamDOrPcvQFtqF7KpQTek
u1fjrOiug5oMW665HvBDBw6qI/JN3+DU4YEOoNk+LO8Ks+Ij3cWxYxhYtYp1tJzSkDtovwG5EDrM39i6aL4UeFAGS
qQP7sQMHFC5JKlTGA+/x+5GOMF9YpMZSAsmbtzvv6u8V2x9bHElfgBCP1fsPLZScl7Dhm/4nUATDA==",
"digitalSig":
"aoATRDAyk7xFfaYRSFngBK7eYBmOGSK1xersfeMHPDv5bxqE1xJdy7072EGTrPCxJx660lOfEorHFWercDOaCOiJu
7tnWfvhKfUM1UsVuymTJ12MkcecQOcZ/ynoQaTzWECWud7gKKvGNp/W/8gTl65R+jbNz0u5kP4xukUVedN+AjK
2DhYf9IfdkJJ6DAtPG6uP0ol3ScjbqBy5WVmODpX1rtS3cQ95WVC56+vAuZLUK00W3Y5efEZ05F/E1RM3C1oRHYg
3gXR3ZIWeU+kVr401Q3l5mwVwD+uZrG1UQ+xuPkDo7by0WT/JRbKBltHikOa+x8h5ZsGhQ9a9HkOG6w==", "ts":
"2020-10-26T22:01:08+05:30"
}
```

Step 8: *Agent Institution will first verify Digital Signature using Customer OU RSA Public key.*

Agent Institution will decrypt Cipher Text using Agent Institution RSA Private Key to get AES Key.

Encrypted Response Message:

```
fX6FhBMlEeMS2qb8N477SDSWH/D3r3aKvcIwJk6dvqEwmiLR2+ZctcDYSMkCkrgzZmXBCGYn2TPoiBXjvPOWG1Q
2FQkmuUrOEAakkzxgZadyOEljy8QkC/o07dPne5g5vEe+djAMkbtya+RTqCILRXIoEqxgamDOrPcvQFtqF7KpQTeku
1fjrOiug5oMW665HvBDBw6qI/JN3+DU4YEOoNk+LO8Ks+Ij3cWxYxhYtYp1tJzSkDtovwG5EDrM39i6aL4UeFAGSq
QP7sQMHFC5JKlTGA+/x+5GOMF9YpMZSAsmbtzvv6u8V2x9bHElfgBCP1fsPLZScl7Dhm/4nUATDA==
```

Plain Text Response Message:

```
{
 "head": {
  "requestId": "OU01OU02INT522274495200721ahbcj2123", "ts":
  "2020-07-21T22:02:40+05:30"
 },
 "reason": {
  "responseCode": "000",
  "responseReason": "Successful"
 },
 "categories": [ {
   "order": 1,
   "categoryName": "Insurance",
   "categoryDesc": "Insurance",
   "status": "Active",
   "icon": "https://IP:PORT/AgentPortal/resources/images/biller.png", "modifiedDate":
   "21-07-2020",
   "subCategories": [
    {
     "subCategoryOrder": 1,
     "subCategoryName": "Life Insurance",
     "subCategoryDesc": "Life Insurance",
     "status": "Active",
     "icon": "https:// IP:PORT /AgentPortal/resources/images/biller.png", "modifiedDate":
     "09-04-2019"
    },
    {
     "subCategoryOrder": 2,
     "subCategoryName": "Health Insurance",
     "subCategoryDesc": "Health Insurance",
     "status": "Inactive",
     "icon": "https:// IP:PORT /AgentPortal/resources/images/biller.png", "modifiedDate":
     "09-04-2019"
    }
   ]
  },
  {
   "order": 2,
   "categoryName": "DTH",
   "categoryDesc": "DTH Recharge",
   "status": "Inactive",
   "icon": "https:// IP:PORT /AgentPortal/resources/images/biller.png", "modifiedDate":
   "09-04-2019"
  }
 ]
}
```