***Partner Management***:

1. ***Roles***:
2. *MOSIP Admin*:
   1. Create MISPs
   2. Create/Manage Users (MISP, Policy Manager and Partner Manager roles)
3. *Policy Manager*:
   1. Create and publish policies
   2. Manage policies
4. *Partner Manager*:
   1. Approve/Reject Partner API Key requests post scrutiny.
   2. Associate policy to API Key
   3. Deactivate / Activate API Key of Partner.
   4. Deactivate / Activate Partner
5. *MISP*:
   1. Billing, Usage related activities.
6. *Partners*
   1. Partner creation request
   2. Certificate uploading etc
7. Regulators are Partner Manager and Policy Manager. Also, What is the difference between Partner Manager and Policy Manager? Why can’t the policy manager and partner manager be the same role? The work might be assigned to different agencies or one. Therefore we will only look at roles. Multiple roles might be assigned to the same user possibly. Let us not worry about Regulators but only about the roles.
8. Whitelisting of IPs at MISP level is taken care at proxy OR API gateway layer not at application layer? This will be handled by IPSec outside of the application layer.
9. MISP - Partner License Key Revocation / Deactivation. Is this Partner Api key? Why MISP are allowed to do this? Does partner/policy manager have any control here? MISP role will not do this. Partner Manager role will.
10. Partners creation on a self-service mode is a new requirement. Please confirm. So, these requests are without interference from any other roles. Partners directly contact MISP for registration while auth/eKYC request is through MISP only. Please confirm. Potential partners will go to the portal and sign up. Partner manager will facilitate approval and creation of partner. This includes any offline legal process as well as providing their digital Certificates/Keys.
11. ***PartnerAPIKeyRequest***:  
      
    - Id  
    - RequestCode  
    - PartnerCode  
    - ApplicationCode   #This can be "Other" if there are no pre-defined application types suitable for this person. Use case can be described.  
    - UseCaseDescription  
    - SupportingInfo #Business permits and other supporting info that shows that they are authorized, if needed  
    - Status (Requested, In Process, Rejected, Accepted)
12. What is RequestCode in PartnerAPIKeyRequest? Is this code to track the request for the api key? Yes. Once approved the PartnerKey will refer to this. Use case description is present here only and not in the PartnerKey table.
13. Workflow management of PartnerAPIKeyRequest is a new scope addition. Please clarify. Association of Key to Policy, Issue of key is done by partner manager, while the resuest itself is done by the Partner.
14. ***Admin Console***:  
      
    Admin console will be used for the following with respect to the Auth Partner Ecosystem  
    - Manage MISPs (Add, Activate, Deactivate). It will use the Partner Management Services API for this.  
    - Manage Regulators (Add, Activate, Deactivate). It will use the Partner Management Services API for this.
15. Partner Management will provide services for the above features and the UI will be from Admin. Please confirm
16. Policy Management, Partner Self-service Registration UI will be from Partner Management which is scoped for a later version and the corresponding apis are scoped in the current version
17. ***Partner*** specifies nature of business / use case (descriptive text and not an application type or code) and asks for an API key  
    Partner Manager reviews the application and grants a license key with the right auth policy  
      
    Partner Management Admin Flow (Played by Partner Manager)  
    =============================  
    1. Approve/Reject Partner API Key requests post scrutiny.  
    2. Associate policy to API Key
18. Who will associate a policy to api key? Partner Manager
19. Will a partner be associated to a partner manager during creation of partners? Else which partner manager will approve which partner’s request. Excellent question. Partner requests will have to be tagged with Regulator Name. For example if TRAI decides to host a portal for issuing MOSIP access, then partners will apply there. That portal will call the API with a user created for TRAI for partner manager role. This role can only see TRAI applications.
20. Will all the partners be managed by a single partner manager or how are the partner managers defined? If MOSIP manages partners this will be true. It is a special case. Generally we will have to assume multiple partner managers.
21. ***PartnerKeys***:  
      
    - Id  
    - RequestCode #from API Key Request which was approved  
    - PartnerCode (ARTLBANK)  
    - ApiKey (some-real-lycr-ypti-ckey)  
    - IssuedOn  
    - ValidTill  
    - IsActive  
    - More fields
22. What is PartnerKeys? When is it generated ? How is this used. This is the list of issued partner API keys. This is generated when a partner api key request is approved and a policy is associated.
23. A partner can be associated to multiple api keys. As long as the api key is valid for a partner the partner authentication will be successful. Please confirm. Correct. For each API key associated with a partner, this table will have an entry.
24. So applicationtype is just internally used by the partner manager to map the appropriate apikey(policy) to partner and not mapped to partner. Please confirm. No application type exists any more. That concept is removed.
25. ***Relationship:***  
    What is the relationship to be maintained in the system between partners, MISP, partner and policy Manager? Who will be linked in the system? We do not maintain any relationship between partner and MISP or partner and policy manager. Partner and Partner Manager will be linked via “Regulator” field.
26. As we can see from the entities above that there is no relationship between MISP and Partner. MISPs will have their own billing and partner management system where they will maintain this partner code for their agreements.
27. Can you clarify on the above point? Yes
28. ***Policy Manager Flow***:  
      
    i. Create and publish policies

ii.. Manage policies

1. What exactly is meant by creation of policy? Creation of the json / xml file in config used by Auth and adding an entry into the policy list available. Note: Policy will also have a “Regulator” tag. And multiple policy manager users might be there where they can create and manage their own policies.
2. Who will associate a policy code to an application type? No application type any more.
3. ***Partner My Usage Statistics***:  
    a. Is this a new scope addition? This is not scoped in currently. This is new and need not be addressed now.