Operation Management Policies

For

KARNATAKA STATE RESIDENCE DATA HUB (KRDH)
AUA&ASA SOLUTION

Centre for Development of Advanced Computing

Gulmohar Cross Road No. 9, Juhu, Mumbai 400 049.

Telephone: +91 22 2620 1606, +91 22 2620 1574,
Fax: +91 22 2621 0139, +91 22 2623 2195
Website: www.cdac.in

Revision History

Version	Date	Author(s)	Contributors	Reviewed By	Review Submission Date	Reason for Change
Draft 0.1	14-08-2017	Vijay Jain				
Draft 0.2		Vijay Jain	Shilpa			Addition of Aadhaar Vault
Draft 0.3		Vijay Jain				API updation

Table of Contents

Purpose of the Document

Operational Management Policy document has been prepared for applicable policy and managing the technical solution of ASA. The purpose of this document is to distill information and requirement with clarity for compensative understanding of the policy in force for ASA technical solution, as applicable. Scope of this document is limited to the policies being applied for technical solution of KRDH ASA.

Intended Audience

The intended audience for this document includes "Center for e-Governance (CeG)", Government of Karnataka, and all other associated stakeholders of this project. The audience is expected to have knowledge of web Services, java and related tools and technologies proposed in the current document.

Comments and Suggestions

For comments, suggestions and feedback on this document, kindly email at krdh-ceg@cdac.in

Glossary

AUA	Authentication User Agency
ASA	Authentication Service Agency
KUA	KYC User Agency
KRDH	Karnataka Residence Data Hub
CeG	Center for e-Governance

1 Introduction

Karnataka Resident Data Hub (KRDH) has been architected and implemented by CeG to facilitate efficient citizen service delivery by various departments to the right beneficiaries. In the above context, KRDH provides various supporting functions to enable departments to streamline the process to authenticate the beneficiary to ensure that the services are delivered to the right person.

KRDH has become Authentication User Agency (AUA), Authentication Service Agency (ASA), KYC User Agency (KUA) and KYC Service Agency (KSA) of UIDAI to render Aadhaar based Authentication and e-KYC services to various customers, partners and stakeholders.

As one of the objectives of KRDH, it also supports every department to become AUA/ KUA. Due to current goal set by the Govt. to disburse the services to the citizens, various departments in the state are in a need to become AUA/KUA in a centralized manner through KRDH. Purpose of centralized AUA/KUA is to overcome the efforts involved for carrying out regular changes in AUA-KUA as per UIDAI guidelines at department level.

2 Document Overview

This document is organized as follows:

Section 1. : Introduction - This section provides a brief overview of the KRDH AUA Solution.

Section 2.: Document Overview - This section describes the structure of the document.

Section 3.: Assumption and Dependencies- This section describes the assumption and dependencies being considered for the implementation of the project

Section 4.: KRDH AUA Solution- This section describes major disciplines for KRDH AUA solution ecosystem and various components of it.

Section 5.: This section describes the system requirement detailing out functional and non functional requirements.

Annexure A. Description about Tools and Technologies

3 Assumptions & Dependencies

3.1 Assumptions

- All required IT & non-IT infrastructure for deployment of ASA solution will be provided by CeG, KRDH.
- Acquiring necessary permissions for hosting/integration of applications with developed AUA-KUA.

- KRDH can appoint a third party agency for carrying out audit of the ASA solution and ensuring its compliance as per UIDAI guidelines. C-DAC will extend its full support for such audits.
- Department co-ordination and necessary approvals to on-boarding team for integration of AUA-KUA solution will be managed by KRDH.
- Service provider for Infrastructure procurement/management under the purview of KRDH will be managed by KRDH.
- Required network connectivity between ASA-KSA and UIDAI will be ensured by KRDH.
- Coordination with UIDAI and line departments for signing of agreement, payment of AUA-KUA, ASA-KSA license fees, transaction fees of UIDAI etc will be coordinated and managed by KRDH.
- Integration of various AUAs will be tested first on the pre-production environment and then will be integrated with production environment with updated version as per UIDAI guidelines issued from time to time.

3.2 Dependencies

- 24 X 7 network and infrastructure availability at data center.
- Availability of high volume and high velocity communication transmission between ASA and ASA-UIDAI.
- Timely approvals and infrastructure availability for deployment of ASA-KSA solution.
- Timely availability of required infrastructure proposed by C-DAC for maintaining the scalability of the developed solution.

4 Overall Ecosystem

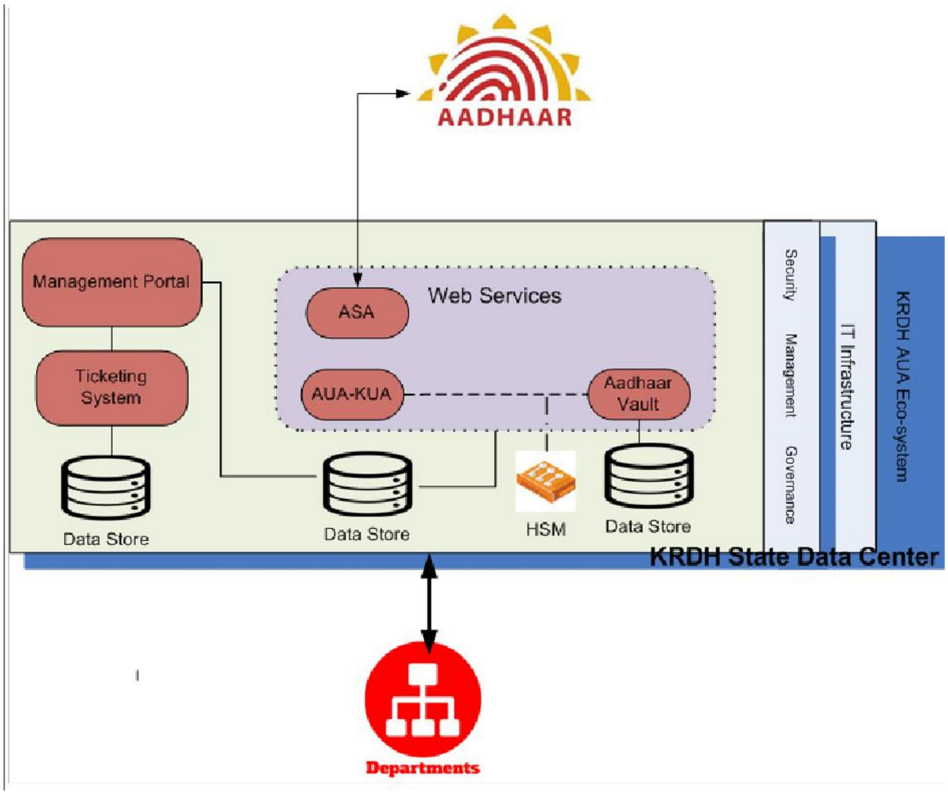

Figure 1. Overall KRDH Solution Ecosystem

Figure 1 demonstrates an overall ecosystem for KRDH AUA Solution. Table 1 describes the functionality for each component as being shown in Figure 1.

Table 1.Component Details

Sr. No.	Layers	Description
1.	AUA	AUA will receive request for Authentication (Demo, OTP and biometrics), Request for an OTP and e-KYC (OTP and Biometrics) from the department application and will validate the received XML and log the transactions before forwarding it to ASA.
2.	ASA	ASA will receive the request f for Authentication (Demo, OTP and biometrics), Request for an OTP and e-KYC (OTP and Biometrics) from the AUA and will validate the received XML and log the transactions before forwarding it to UIDAI.
3.	Management Portal	Management portal will provide seamless management of the department specific activities. Management portal will act as one stop portal for all departments and a role assigned for each department will allow them to manage their license keys and viewing of transactional details of AUA-KUA.
4.	Ticketing System	Open source ticketing management system/customized solution will be configured and deployed. An access to the ticketing system will be provided to department to log the issues faced while utilizing the AUA-KUA APIs.
5.	Monitoring System	Monitoring system will be deployed and configured for providing hardware and software resource utilization details along with timely inputs to KRDH for scaling up of the hardware infrastructure.

5 IT and Non-IT Infrastructure Details

Sr. No.	VM/Server Name	VM Configuration			Components Installation		Components Installed
		RAM (GB)	vCPU/CPU	Hard-Disk (GB)		IP	
Production Environment							
1.	AUA-ASA Solution-VM1	32	16	360	Pre-Production AUA, ASA and Vault Web Services	10.10.28.115	
2.	AUA-ASA Solution-VM2	32	16	360	Production AUA, ASA and Vault Web Services	10.10.28.116	
3.	AUA-ASA-Solution-VM3	32	16	360	Production AUA, ASA and Vault Web Services	10.10.28.121	
4.	AUA-ASA-Solution VM4	32	16	360	Production AUA, ASA and	10.10.28.122	

					Vault Web Services			
5.	AUA-ASA-Solution-VM5	32	16	360	Testing AUA, ASA and Vault Web Services	10.10.28.142		
6.	AUA-ASA-Solution VM6	32	16	360	Testing DB AUA, ASA and Vault Web Services	10.10.28.143		
7.	e-KYC AUA-ASA-VM-1	32	16	360	Pre-Production AUA, ASA and Vault Web Services	10.10.31.54		
8.	e-KYC AUA-ASA-VM-2	32	16	360	Pre-Production AUA, ASA and Vault Web Services	10.10.31.55		
9.	Management Portal-Vm1	32	16	360	Management Portal and Ticketing System	10.10.28.144		
10.	Management Portal-VM2	32	16	360	Management Portal and Ticketing System	10.10.28.145		
11.	Monitoring System-VM-1	16	16	240	Nagios Monitoring System	10.10.28.119		
12.	Server- DB1	64	16	100	Vault-Database Server 1 (Primary)			
13.	Server- DB2	64	16	100	Vault-Database Server 2 (Standby)			
14.	Server- DB1	64	16	100	Database Server 1 (Primary)			
15.	Server- DB2	64	16	100	Database Server 2 (Standby)			
16.	VM-DB-Pooler cum LB	16	16	100				
17.	VM-DB-Pooler cum LB (Failover)	16	16	100				
18.	SAN Storage		5 TB					
Integration Environment								
19.	AUA-ASA Solution-VM1	32	16	360	AUA, ASA, Vault and e-KYC Web Services			
20.	DB VM-1	64	16	360	AUA-ASA and Vault			
Testing Environment								

21.	AUA-ASA Solution-VM1				AUA, ASA, Vault and e-KYC Web Services		
22.	AUA-ASA Solution-VM2				AUA, ASA, Vault and e-KYC Web Services		
23.	DB VM-1	64	16	100	Database for ASA,AUA and Vault		

6 Deployment Management

7 Password Management

- We have changed all the password which provided by SDC team at in initial level.
- All User passwords (including administrator passwords) remains confidential and do not share, post or otherwise we will be divulged in any manner.
- We do not write on anywhere, message or send record of passwords, unless this can be stored securely.
- We did not stored password in database.
- Change passwords whenever there is any indication of possible system or password compromise.
- We have set strong password policies (length of password (8 characters, types of passwords, expiry of passwords, different password for different system/user) as per UIDAI guidelines.
- We do not keep password hardcoded in codes, login scripts, any executable program or files.
- We do not store or transmitted password in applications in clear text or in any reversible form.
- There is not any facility regarding password for automated log-on process, e.g. stored in a macro or function key.

8 Change Management

9 Incident Management

The motive of incident management policy is about maintaining the incidents that can occur at OS level, Network level and Application level and elaborate about the process how the issue escalates from lowest in hierarchy to higher level in hierarchy with utmost priority to resolve the issue at earliest.

The incident that occur at OS level are as follows:

1. Updating the default Java environment to point to Oracle JDK instead of default JDK.
2. Unable to login as root for ssh access i.e. remote access.
3. There can be issues related to permission denied if the user accessing the folder does not have appropriate access privileges.
4. There can be issues related to permission denied while deleting a file thus providing ownership rights like deletion with owner of that file thereby making a system robust.

The incident that occur at Network level are as follows:

There can be two types of failures for network scenarios:

1. Internal Communication network failure:
    - Network failure between client to AUA.
    - Network failure between AUA to ASA.
    - Network failure between AUA to crypto service.
    - Network failure between AUA to Vault.

2. Outside Communication network failure:

    - ASA to UIDAI network failure.
    - If domain name is not mentioned properly then the dns server might fail.

The incident that occur at Application level are as follows:

These incidents can occur at:

- Tomcat level (Container level)
- Application War level.

Tomcat Level:

- The user won't be able to start tomcat as non-root user.
- If appropriate permission is not given, then tomcat start might fail to start.

Application Level:

- If appropriate permission and ownership are not given, then the war might fail to get deployed.
- The war might fail to deploy if the webapp.root.key is same for two wars present in webapps.
- The war might fail to deploy if the log properties path is not mentioned correctly.

To manage and review the issues one separate file of Issue tracker is created and we are able to track the issues.

The action to be taken to resolve the issue is mentioned in the Standard Operation Procedure.

The issue is reported through ticketing portal in place.

10 Patch Management

Application Level patch management :

1. The cipher suites were missing therefore the SSL handshake wasn't taking place. Therefore, we had to patch the java jdk with unlimited jars.
2. Whenever we receive too many ASA-C-01 i.e. network connectivity issues we have to patch the servlet-context.xml with patch that includes change in read timeout and connect timeout values.
3. When we faced connectivity issue with database we had to patch the tomcat configuration values with appropriate query and its parameters.

Network Level patch management:

1. Though the system being isolated and secure from outside web, we have to patch the load balancer with OpenSSL for heightened security.

OS level patch management:

11 Data Privacy

1.0 Purpose

Centre for e-Governance, Government of Karnataka (CEG) must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of in scope data is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

2.0 Scope

- Any CEG device which handles customer data, sensitive data, personally identifiable information or company data. Any device which is regularly used for e-mail, web or other work related tasks and is not specifically exempt for legitimate business or technology reasons.

- The CEG information security policy will define requirements for handling of information and user behavior requirements. This policy is to augment the information security policy with technology controls.

3.0 Policy

- CEG's data leakage prevention (DLP) technology will scan for data in motion.

- In scope data is defined as:

  a. E-mail addresses, names, addresses and other combinations of personally identifiable information
  b. Documents that have been explicitly marked with the 'CEGConfidential' string.

- DLP will identify specific content, i.e.:

a. Sales data – particularly forecasts, renewals lists and other customer listings.

b. Exports of personally identifiable information outside controlled systems (this is data that you are particularly concerned about losing and wish to ensure is detected by the DLP policy).

- DLP will be configured to alert the user in the event of a suspected transmission of sensitive data, and the user will be presented with a choice to authorize or reject the transfer. This allows the user to make a sensible decision to protect the data, without interrupting business functions. Changes to the DLP product configuration will be handled through the CEG IT change process and with security management approval, to identify requirements to adjust the information security policy or employee communications.

- DLP will log incidents centrally for review. The IT team will conduct first level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and there is a concern of inappropriate use. These events will be escalated to HR to be handled through the normal process and to protect the individual.

- Access to DLP events will be restricted to a named group of individuals to protect the privacy of employees. A DLP event does not constitute evidence that an employee has intentionally, or accidentally lost data but provides sufficient basis for investigation to ensure data has been appropriately protected.

4.0 Technical guidelines

Technical guidelines identify requirements for technical implementation and are typically technology specific.

- Data retention policies must be framed, SPD must not be stored for longer than necessary, and all data is to be deleted after a specific period.

- Biometric data collected for authentication cannot be stored.

- The Aadhaar Act had prescribed these requirements only with respect to Aadhaar numbers or databases containing Aadhaar numbers. This guideline broadens the scope of the data retention limitation requirement.

12 Information Security

1. Policy Statement

The purpose of this policy is to provide a security framework that will ensure the protection of CEG ASA information from unauthorized access, loss or damage while supporting the authentication services. The confidentiality, integrity and availability of these shall be maintained at all times by these partners by deploying controls commensurate with the asset value.

1.1. Control Objective

CEG shall ensure the security of CEG information assets handled by third parties by:

- Providing ASAs with an approach and directives for implementing information security of all information assets used by them for providing services to CEG and AUAs.

- Establishing review mechanism to ensure that the ASAs adhere to all provisions of the CEG Information Security Policy – External Ecosystem ASA.

1.2. Scope

The CEG Information Security Policy – External Ecosystem partner ASA is applicable to all Authentication Services Agencies that provide CIDR connectivity to AUAs/KUAs.

- Authentication Service Agency (ASA): Authentication Service Agency is an organization or an entity that transmits authentication requests to the CIDR on behalf of one or more AUAs.
- ASAs have established secure leased line connectivity with the CIDR compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies (AUA) and transmit AUAs' authentication requests to CIDR. Only agencies contracted with UIDAI as ASAs shall send authentication requests to the CIDR; no other entity can directly communicate with CIDR. An ASA could serve several AUAs; and may also offer value added services such

as multi-party authentication, authorization and MIS reports to AUAs.

- This Policy is applicable wherever UIDAI information is processed and/or stored by Authentication Service Agencies.

2. Information Security Policy for Authentication Service Agencies

2.1 Purpose

This section outlines the Information Security policy and Information Security controls applicable for Authentication Service Agencies (ASAs).

2.2 Policy

Authentication Service Agencies shall ensure the confidentiality, integrity, and availability of UIDAI related data and services.

3. Information Security Domains and related Controls

3.1 Human Resources

- ASA Team handled all aadhar related activities and communication with UIDAI.

- ASA conducted background check or sign an agreement/NDA with all personnel/agency handling aadhaar related authentication data.
- UIDAI had already validated this information.
- ASA conducted induction for new employees as well as periodic functional and information security trainings.
- In case any update came from UIDAI then conducted information security trainings for existing employees.
- This training included all relevant security guidelines as per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
- Before accessing any UIDAI information assets all employees done their induction at the time of joining.
- In case any update or new assets came from UIDAI/ASA, first we have conducted training existing as well as new employees as per UIDAI guidelines.

3.2 Asset Management

- All assets used by the ASA (servers, network devices, etc.) for the purpose of delivering services to UIDAI have identified, labelled and classified. Details of the information asset have recorded.
- Still, from the starting of the ASA services, we didn't dispose of any assets. In the future, we need disposing of any asset we follow the disposal policy of the organization. Information systems containing UIDAI information shall be disposed-off

securely only after obtaining approvals from UIDAI authorized personnel.

- Before sending any equipment out for repair, the equipment shall be sanitized to ensure that it does not contain any UIDAI sensitive data. (NOTE: ASA will take care about this point)
- ASA have already implemented controls to prevent and detect any loss, damage, theft or compromise of the assets.

3.3 Access Control

- Only authorized technical persons provided access to information assets (such as servers, network devices etc.) processing UIDAI information.
- ASA personnel with access to UIDAI information assets have limited access for getting information and processing. After finished the work individual operator logged out from the servers.
- The systems have auto lock out feature i.e. after a 15 minutes if system goes in idle state.
- In case if any employee leave the job from CeG, first we will deleted all information and changed credentials of that particular person and after that we will changed all credentials of assets
- Access rights and privileges to information facilities processing UIDAI information shall be reviewed on a quarterly basis and the report shall be stored for audit purposes.
- Users did not provided with local admin access rights on their system. Users can not change in any administrative policies. Users can just do their task in limited access.
- We have set three successive login failures as per the password policy of the organization after third successive login failure user's account being locked; they should not be

able to login until their account is unlocked and the password reset in case of server logins. The user should contact the System Engineers/Administrators for getting the account unlocked. For applications there should be an automatic lock out period of 30 mins in case of three consecutive login failures or as per the password policy of the organization.

3.4 Password Policy

- We have changed all the password which provided by SDC team at in initial level.
- All User passwords (including administrator passwords) remains confidential and do not share, post or otherwise we will be divulged in any manner.
- We do not write on anywhere, message or send record of passwords, unless this can be stored securely.
- We did not stored password in database.
- Change passwords whenever there is any indication of possible system or password compromise.
- We have set strong password policies (length of password (8 characters, types of passwords, expiry of passwords, different password for different system/user) as per UIDAI guidelines.
- We do not keep password hardcoded in codes, login scripts, any executable program or files.
- We do not store or transmitted password in applications in clear text or in any reversible form.
- There is not any facility regarding password for automated log-on process, e.g. stored in a macro or function key.

3.5 Cryptography

3.6 Physical and Environmental Security

This should be provided by SDC Team.

3.7 Operations Security

- All ASAs shall complete the AADHAAR ASA on-boarding process before the commencement of formal operations .
- We are only engage with the AUAs / KUAs approved by UIDAI and Keep UIDAI informed of the list of AUAs it serves. In case of disengagement with an AUA / KUA at that time we are informing to UIDAI within a period of 7 days
- We are developed Standard Operating Procedure (SOP) for all information systems and services related to UIDAI operations .The sop include network failover script, maintain host file, IP table status
- We are segregating duties and process which include such as monitoring of activities i.e. alert management system, Nagios monitors systems, issue tracker logs sheet, VM tracking excel sheet etc. In Maintenance supervision activities we have log backup scripts, network failover script, deployment script, transaction summary report, excel sheet to monitor issues etc. In audit trails we are ensuring about fraud detection, UIDAI transaction reports and counts, security audit etc
- We have separate environments for Test , pre-production and production physically and logically all are separated.
- ASA personnel shall conduct integrity checks to verify the completeness of the data packet and authenticity of the authentication user agency before processing the authentication request. A formal Patch Management

Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and server level.

- We already conducted VA exercise for maintaining the security of the authentication applications and we have report VA exercise reports.
- We don't do intentionally any other activities like write, generate, compile copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access because necessary permission and ownership are given at server level and password policy setup also done at server level.
- We did the activities for ASA servers connected to the CIDR shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed for that purpose we installed SSL at server level.
- We are ensure that the event logs i.e application server logs, exception logs for the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring.
- We are Regularly monitoring the logs for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only so for these activity password policy setup already done,
- In authentication audit logs contain transaction details, we can identify of the requesting entity with respected to Ac code, for authentication request and authentication response we identify the requesting entity with respected to transaction-id.
- We did not store Aadhaar number, PID information, device identity related data and eKYC response data in the ASA logs.
- We are maintained logs of authentication transactions for a period of 6 months, during which an Aadhaar number holder

shall have the right to access such logs, in accordance with the procedure as may be specified.

- Upon expiry of the period of 6 months, the logs shall be archived for a period of 6 months by the laws or regulations governing the ASA as well as supreme court, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes.
- At the time of on-boarding ASA ensure about these activities i.e. ASA server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities.
- We ensured about the Service Continuity and service availability for that purpose we informing to UIDAI if service unavailable or any other service related issue happen as well as mail system also created.

3.8 Communications Security

This should be provided by SDC Team.

3.9 Compliance

Related to all laws, permissions and security testing by authorized organization.

3.10 Change Management

13 SOP

Standard Operating Procedure:

1. Network Related Issue:

To Test ASA to UIDAI network:

- Use telnet command to check network connectivity.
- Once network connectivity is correct, check whether port is open using the traceroute command for a finding routing path.

To Test client to Application Server network:

- Use ping command to check network connectivity.
- Once network connectivity is correct, check whether the port is open using telnet command for tomcat port.
- Once you confirm that port and network connectivity is in place try to hit the Application Server with appropriate XML request using curl command if proper response is received then application server is checked.
- If any type of error is received then check the error code and identify the reason.
- If still unable to resolve issue, then forward to higher support level for access to application logs and identify the cause.

2. VM Related Issue:

Unable to access VM:

- Try to login using root password.

- Monitor the storage space using Nagios**.**
- Delete unnecessary logs and clear cache at appropriate interval of time.

3. Application Related Issue:

- If invalid XML is received, then one has to enable the debugger logs and extract the invalid xml from appropriate file where invalid xml's are stored and disable the debugging logs.
- If the issue is unable to be resolved by looking at the error codes set by application servers then check for the application server logs for appropriate exceptions.

4. Tomcat starting Issue :

- Tail the catalina.out for exception.
- If Exception is permission denied, then give appropriate permission the required folder.
- If Exception is related to Address already in use.
- Then fire command ps aux | grep tomcat, and post running the command the screen will display the running tomcat.
- Kill that tomcat explicitly using command kill -l process id.
- Then try to restart tomcat.

- If the error is related to "Unable to start using root user" , then first check whether any tomcat is running kill that tomcat.
- Then post stopping the tomcat, change the ownership of the log files affected to "tomcat" user.
- Then change the user to tomcat using su tomcat command from root user.
- And post changing the user run tomcat.

5. **HSM related network issue:**

- Initially ping the HSM appliance using ping command.
- If unable to ping, then report to network team for the network down issue.
- Post getting positive reply to the ping command, run telnet command on the HSM appliance port to check whether port is open or not.
- If the telnet command is unsuccessful then report to the network team about the same.
- If successful, then to further debug run the TestLuna.java code with appropriate credentials, and identities to test signing.
- If the code is running fine, then restart tomcat to clear out caches within tomcat.
- Is the code does not work share the exception with the and raise a ticket with them to resolve the issue.

6. **SSL Setup or Handshake related exception**

- Run InstallCert.java program with appropriate domain name and port 443.

e.g. java InstallCert <uidai-domainname>:<portnumber>

7. **Too many ASA-C-01 :**

    - Increase the read timeout and connect timeout values at ASA end for servlet-context.xml.
    - And in corresponding to that increase the read timeout and connect timeout values at AUA end for servlet-context.xml.

8. **Too many AUA-C-01 :**

    - Confirm that the readtimeout and connectimeout values at AUA end is greater than the readtimeout and connectimeout at ASA end. (check servlet-context.xml)

9. **Updating the certificate for signing, decryption and encryption.**

    - Please refer certificate insertion and updating document.

10. **Pulling the logs from AUA, ASA, KUA and KSA servers:**

    - Using pscp tool or log pulling application.

11. **Cryptoservice related errors : (AUA-OTP-11, AUA-AUTH-09)**

    - Follow the process mentioned in Pt. No. 5 i.e. **HSM related network issue.**

- If still issue persist then check if cryptoservice war is properly deployed by hitting the cryptoservice url with specific XML request.

12. For other error codes:

Refer the error code document.