

**Unique Identification Authority of India (UIDAI)
Planning Commission, Government of India**

Reference Number: A.11016/74/2010-UIDAI/Auth-Server



INVITATION FOR EXPRESSION OF INTEREST

FOR

**Providing Biometric SDKs and Participating in the testing and
benchmarking of the Solution for Authentication Server**

1st August 2011

Unique Identification Authority of India (“UIDAI”) invites Expression of Interest (EOI) from Biometric Solution Provider for providing Biometric SDKs and participating in the testing and benchmarking of the Solution for Authentication Server. The Biometric Solution intended to perform the following function:

1. Verification (1:1) of biometric records.
2. Identification (1:n) Up to 10 fingers.
3. Segmentation of fingerprints.
4. Feature extraction & Template Generation.
5. NFIQ quality check.

UIDAI will provide the required hardware infrastructure at UIDAI Greater Noida Data Centre. Biometric SDK/Solution is to be installed on Linux operating system.

Vendor SDK should support for Fingerprint as well as Iris Templates extraction and verification, however, this testing & benchmarking will be conducted only for fingerprints.

Vendor SDK/Solution should have JAVA support.

Scope:

- (i) ISO Fingerprint template generation.
- (ii) The biometric authentication solution provisioned by the vendor should be capable of 1:1 comparisons of enrolled references with incoming ISO/IEC 19794-compliant fingerprint, iris or 19794-2 compliant fingerprint minutiae sets without proprietary extended data.
- (iii) The templates will be maintained in memory resident database by the UID authentication server application. If the incoming requests contain a biometric image, the Authentication server will use SDK to extract the feature. SDK will also be used to generate comparison score of the sample.

FP Verification (1:1): The SDK will be able to compare features extracted from a FP image against specified reference templates and return a scaled comparison score between [0,100] or [0,maximum], with 0 indicating least similarity.

Iris Verification (1:1): The SDK will be able to compare features extracted from a query iris image against a specified reference template and return a scaled comparison score between [0,100] or [0,maximum], with 0 indicating least similarity.

Functions required:

1. *Support for FMR (Fingerprint Minutiae Record, ISO 19794-2).*
2. *Support for FIR (Fingerprint Image Record, ISO 19794-4).*
3. *Support for Iris Image matching (ISO 19794-6).*
4. Verification (1:1) of biometric records.
5. Identification (1:n) Up to 10 fingers.
6. Segmentation.
7. Feature extraction & Template Generation.
8. *NFIQ quality check.*
9. *Cluster server capability.*
10. *Interoperability.*

Load and Performance requirements:-

1. Fingerprint template: 10 Lakh (1 Million) requests/hour.
2. Iris image: 10,000 requests/hour.
3. Accuracy:-False Acceptance Rate < 0.01% at False Rejection Rate < 2%.
4. Response time:- < 0.1 second average for biometric verification using ISO FP template while using SDK.

Technical Support:-

Deployment of Technical manpower for installation, configuration, testing and benchmarking of Biometric SDK at UIDAI Data Center, Greater Noida.

System Architecture requirements:

The solution proposed by vendor should meet the following requirements.

Scalability

- (i) Dynamic or rule based ability to scale the system within servers, across servers without inherent bottlenecks and code changes.
- (ii) Ability to scale across data centers.
- (iii) The system shall have ability to scale dynamically within a server depending upon the load.
- (iv) The system shall have ability to add nodes dynamically without bringing the system down.
- (v) The system shall have ability to utilize dynamically increased CPU, RAM and storage.
- (vi) The system shall have ability to utilize network bandwidth provided through multiple interfaces.
- (vii) The system shall have ability to load balance across servers
- (viii) Should supported multiple instances of databases (or datastore if datastore is used for storing gallery)
- (ix) Should support horizontal partitioning of database (or datastore if datastore is used for storing gallery) across multiple physical databases
- (x) Should support horizontal sharding of database (or datastore if datastore is used for storing gallery) across multiple physical databases
- (xi) The system should not have a single point of failure and inherent design bottlenecks that stops it from scaling.

Security

- (i) The solution should have the ability to secure all data from thefts, tampering, unwanted modifications, network attacks, and other security threats using physical and logical measures as per UIDAI specified security and data protection policies.

Interoperability

- (i) The solution should have the ability to interoperate with other systems/services within and across any open interfaces and ability to continually re-factor and/or replace specific components without affecting rest of the system.
- (ii) The solution shall support:
 - a. Open standard protocol based communication
 - b. Command line based interface for interaction

- c. Re-factor/replace individual services without bringing the whole system down
- d. Automated integration from external management products such as systems management, network management, and other tools

Manageability

- (i) The solution should feature the ability to manage end-to-end solution and its components to ensure solution health and SLAs using external data center management tools.
- (ii) The solution shall support:
 - a. monitoring of its services using management tools
 - b. ability to bring its services up and down
 - c. monitoring its CPU/network/storage utilization
 - d. monitoring the response time of individual services
 - e. maintenance of its services without affecting client access

Upgradeability

- (i) The solution should have the ability to seamlessly upgrade services, components, and modules without affecting services and open interfaces and ability to upgrade without bringing down the solution.
- (ii) The solution shall support:
 - a. upgrade of individual modules without bringing the solution down.
 - b. backward compatibility
 - c. upgrading using third party software delivery systems
 - d. reverting back to original configuration in case of an upgrade failure
 - e. reverting back to old configuration after a successful upgrade

Installation and Configuration

- (i) Ability to configure the solution using wizard and other end user tools.
- (ii) Ability to install the solution using installation script.
- (iii) The solution shall support:
 - a. integration with change management system
 - b. integration with software delivery systems
 - c. installation and configuration without super user privileges

Maintainability

The solution shall have the:

- (i) Ability to continuously maintain, enhance, re-factor solution without breaking other parts.
- (ii) Ability to support maintenance, enhancement and refactoring the solution without breaking other parts

Open Standards Based

- (i) Technology choices should be based on open standards and widely adopted frameworks as long as they meet the needs of the system.
- (ii) The solution shall have:
 - a. technologies that are based on open standards
 - b. frameworks that are widely adopted

Cloud Enabled

The biometric solutions proposed should support deployment on a virtualized platform. The solution should support:

- (i) The ability to deploy and run the application within a private cloud platform to take advantage of next generation cloud features.
- (ii) Running services in virtualized environments
- (iii) Metering of CPU, network and storage utilization
- (iv) Throttling of CPU, network and storage utilization
- (v) Multi client capable services

1 Benchmarking

1.1 Objectives of benchmarking

The Benchmarking exercise is intended at evaluating ability of the proposed SDK/solution for UIDAI Authentication Services. The Benchmarking process does not intend to simulate **all** the aspects of UID Technology Solution but all the design parameters shall be considered.

1.2 Vendor's role in benchmarking

- (i) Vendor has to provide full functional trial or full version of SDK/Solution for testing & benchmarking purpose.
- (ii) Vendor has to provide Technical support/manpower during configuration of SDK and thereafter for troubleshooting.
- (iii) Vendor has to create test data based on the UIDAI guidelines for test data
- (iv) Demonstrate at least one successful (live run) run to UIDAI

1.3 UIDAI's role in benchmarking

- (i) UIDAI shall provide the raw data required to create the test data perform the benchmarking.
- (ii) Vendor shall be allowed to use UIDAI's data centre facility in Bangalore/ Greater Noida for setting up of benchmarking environment.
- (iii) UIDAI shall appoint a Third Party agency at its own cost to verify and validate the benchmarking environment and certify the results of the benchmarking.

Timelines:

Milestone	Completion Date
Last date and Time for submission of clarification on EOI	10th August 2011 15:00 Hrs
Latest date and time for receipt of EOI	12th August 2011 15:00 Hrs
Likely Date of EOI Presentations	17th August 2011
Likely Date of start of Testing & Benchmarking	23rd August 2011

Interested vendors for participating in the EOI needs to be provided in template provided in Annexure 1 duly sent by post to: Shri. Yashwant Kumar, ADG, UIDAI, 3rd Floor Tower II, Jeevan Bharti Building, Connaught Place, New Delhi -110001. Email: yas_its@hotmail.com

Annexure 1 – Response Template

One such table to be filled for each model being brought for the PoC:

S.No	Parameter	Vendor's Response	
1.	Name of Organization		
2.	Contact Person's Name		
3.	Contact Person's address & contact details(phone and email)		
SDK Related:			
4.	Biometric Algorithm SDK Name		
		Yes/No	Remark
5.	Support for FMR (Fingerprint Minutiae Record, ISO 19794-2)		
6.	Support for FIR (Fingerprint Image Record, ISO 19794-4).		
7.	Support for Iris Image matching (ISO 19794-6).		
8.	Verification (1:1) of biometric records.		
9.	Identification (1:n)		
10.	Fingerprint Segmentation		
11.	Feature extraction & Template Generation (ISO Templates).		
12.	NFIQ quality checks function.		
13.	Cluster server capability.		
14.	Interoperability.		
15.	Fingerprint matching per second speed.		
16.	Fingerprint ISO Templates extraction speed.		
17.	Iris Image matching speed		
Other			
18.	Support for Red Hat Advance Server 5		
19.	Other Operating System supported		
20.	Support for JAVA		
21.	Other Programming languages supported.		
Technical Support:			
22.	No. of technical manpower that can support integration & on-field troubleshooting		