Response to Queries ' DL/SA/2020-01' dated 13.02.2020

FIRM NAME	S. NO	QUERY	RESPONSE FROM NeGD
CODE-DECODE	1	If the audits have to be compulsorily conducted at your office or can be remotely conducted at our office. As our set up of tools is located at our office and also the scope of the project is offsite; we would prefer to carry out the audits at our office.	All Audits have to be conducted Onsite only.
BRISKINFOSEC	2	Wesbite / Web Application Testing URL details	https://digilocker.gov.in, https://partners.digitallocker.gov.in
	3	Application users - Who is the audience for the application? (In-house teams/customers/partners/citizens etc.)	Citizens, Partners, and Partner Admin
	4	Technologies Used? (Java/.Net/PHP/Perl / MS-SQL/Sybase/Oracle/MySQL / SOAP/XML-RPC / Ajax, Flash etc.)	The application is built mainly on LAMP (Lnux, Apache, MySQL, PHP) stack but as it is a micro services based architecture components are also developed in Java and dot net as well. The back end is composed of file storage, MySQL and MongoDB
	5	Application architecture? (web based, client server, desktop application, etc)	The deployment architecture is both server based and serverless (containers). Each set of container is hosting a service. Servers are hosting the backend file and data storage as well as Caching services.
	6	Intranet/Internet facing application?	Internet facing
	7	Estimated size of Application ? (In case of more than 1 application, pls provide details for each application) - No. of dynamic pages - No. static pages	For Feature details refer Corrigendum- 1 published earlier
	8	Aproxmiate data entry points (total input fields) in the whole application. Give us an approx number.	For Feature details refer Corrigendum- 1 published earlier
	9	Type of Authentication used (Form Based/Certificate Based)?	Two factor Authentication (User and OTP based)
	10	How many roles defined in the application? No. of roles and type of privileges for the different roles (e.g; admin user, normal user, Supervisor role, user with only view access etc.)	Refer Sl. No. 3
	11	Whether any payment gateway, crypto, digital signature is involved?	Currently there is no payment gateway integration, but in future payment gateway integration will take place. The application platform also uses crypto algorithms to secure data as well as uses Digital and document signing signatures for data and messaging.
	12	No. of web services, if any	The application platform has integration with outside services as part of its service. These include NIC KUA services, SMS gateways, partner APIs for accessing and delivering data (Details of all integrated partners is available at (https://digilocker.gov.in/public/dashboard#!)
	13	No. of methods in all web services	This information shall be provided to selected QAP at the time of audit
	14	Will testing be performed on Test/Production environment or both?	Testing and audit will be conducted on production environment. The auditors can sign up to access their DigiLocker account. It is a freely available public application.
	15	Any additional point that needs to be considered while testing the application?	N/A
CYRAACS	16	Agency's experience in conducting security audit of a minimum of 10 Government projects and 5 private projects. **Can 4 government projects be considered?**	No change in Eligibility criteria
	17	Agency's experience in conducting security and performance audit APIs in a minimum of 5 public or private projects. **We conduct only Security audit**	No change in Eligibility criteria

11/3/20

VALUEMENTOR		**Web Application/Website/Web Services Security Testing**	
	18	Total no of applications	Refer corrigendum 1
	19	Web Application Name & URL	https://digilocker.gov.in, https://partners.digitallocker.gov.in https://play.google.com/store/apps/details?id=com.digilocker.android https://apps.apple.com/in/app/digilocker/id1320618078
	20	Authorization No. of roles & types of privileges for the different roles (e.g. normal user, power user, initiator, approver, administrative user etc.)	Replied at Sl. No 9 and 10
	21	Whether the application contains any content management System (CMS)	There is no CMS being used in the application.
	22	Total number of pages: (Approximate)	Refer corrigendum 1
	23	Dynamic Pages: (Approximate)	
	24	Static Pages :(Approximate)	
	25	No. of login modules: (partner and citizen)	
	26	Total No. of Input Forms: (Approximate)	
	27	Total No. of input fields (Approximate)	
	28	No. of APIs	
	29	Front-end Tool [Server-side Scripts]	Replied at sl. No 4 and 5
	30	(E.g. ASP, Asp.NET, JSP, PHP, etc.)	
	31	Location of Work (Onsite (Internal) or Offsite (External))	Onsite ' NeGD office'
	Mobile Application Services Security Testing		
	32	Total no of applications	Refer corrigendum 1
	33	Mention Platform	
	34	Application Name	
	35	Application Purpose/Type	
	36	No of Forms	
	37	No of Services or functions	
	38	No of Dynamic Pages	
	39	No of Static Pages	
	40	Number of User roles (partner and citizens)	Refer Sl. No. 3
	41	Is it available on application store	Refer Sl. No. 19

11/3/20

SECUREYES	42	Name of Application	DigiLocker
	43	Please provide brief description of Application and its Functionality	Refer Corrigendum -1 also visit https://digilocker.gov.in for details
	44	Name & Contact Details of Developer (Ph No. & Email)	-
	45	Url of the target application on test server for Audit (Please provide test user credentials to access the application to verify the details)	Refer sl. No. 19 and sl. No 14
	46	Type of Application (Internal OR Internet Facing)	Internet facing
	47	Site users (closed user group and/or open to public)	Refer sl. No 3
	48	How many Login Modules are present in the Application? (e.g. for normal user, supervisor, administrator, etc)	Refer sl. No 3
	49	Number of Modules and names of the modules in the application (Lannding Page, Account Summary, etc.)	Refer Corrigendum -1
	50	How may approximate total number of pages are present in the application?	
	51	How many approximate number of dynamic (transactional/taking user input) pages are present in the application?	
	52	How many application roles/privilege levels of users are expected to be in the application? [e.g. end-user with read-only access, supervisors with read and modify access, administrators with create user privileges, help desk engineers with read access etc.]	Refer sl. No 3
	53	Development Platform of the Application (For Ex. Java, .NET, PHP etc)	Refer Sl. No 4 and 5
	54	What are the external systems with which the application interfaces with? (These include systems like external LDAP authentication servers, Databases, content Management systems, third-party Payment Gateways, external application APIs etc.)	Refer Sl. No 11 and 12
	55	Is there a CMS (Content Management System) present to maintain the application? If Yes, is it an in-house built CMS or customization of ready to use CMS like Joomla, PHPNuke, and Drupal etc?	There is no CMS being used in the application.
	56	Is there an admin/super-admin module in the application? Is it included in scope of the audit?	Refer sl. No 3
	57	What would be the tentative Testing environment (Development / Staging / Production Box)?	Production
	58	Please provide any additional comments or information that may be relevant to the application	-n/a-
	59	Is there Provision for e-commerce and/or payment gateway (Yes or NO)?	Refer Sl. No 11
	60	No. of phases to test (number of cycles of audit needed, e.g. 1st Level Audit, 1st Level Audit + 1 Re-audit OR 1st Level Audit + 2 Re-audits)?	3 Rounds, 1st Level Audit + 2 Re-audits
	61	Are web services integrated with the application? If yes, how many?	Refer Sl. No 12
	62	What are the Operating System Details of the Deployed Server (i.e., Windows-2012, Linux, AIX, Solaris, etc.)	Refer Sl. No 4 and 5
	63	What is the Web/Application Server with version (i.e., IIS 5.0, Apache, Tomcat, etc.)	
	64	What is the Server Side Language used [Server side Scripts](i.e., ASP, Asp.NET, JSP, JAVA, PHP, etc.)	
	65	What are the Back-end Database used? (MS-SQL Server, PostgreSQL, Oracle, etc.)	
	66	Location of Audit (Onsite - from your location / Offsite - from our location remotely)	Refer Sl. No 31
	67	Any target date for the audit to be started ?	Audit can be started upon award of Contract to the selected QAP
	68	Any target date for the audit to be completed by?	Within 60 days of commencement of audit
	69	The details of the applications and API's to be audited are not furnished	Refer Corrigendum -1 and Sl. No. 12
	70	Do we need to provide "SAFE TO HOST CERTIFICATE" for all the applications every year?	A successful audit certificate has to be provided for all applications every year
	71	The penalty clause shall be applicable only if the delay is caused by the auditing firm. The auditing firm shall not be imposed of any penalty for the delay caused by the NeGD team in : a. fixing the vulnerabilities b. providing necessary data/access/information / support during the project c.availability of system/personnel/revie wers / approvers	Penalty will be levied for delay caused by Auditing firm (QAP) only.
	72	What are the alternative documents that could be furnished in lieu of supporting Letters of successful completion of projects undertaken in the past.	There shall be no change in eligibility criteria.
	73	As per the details, as and when a new API is added, it has to be tested that means one person needs to do continuous API audits.	Adding of API is a regular feature. It is difficult to provide numbers at this point of time.
	74	Does the activity include ISO 27001, Privacy Policy and IT Act 2000 which is more like process and governance audits/assessments?	This RFP doesn't covers ISO 27001 certification, only security audit certification.
	75	Is the audit activity to be conducted from NeGD premises or from QAP's premises?	Onsite 'NeGD Premise'

		Details of the Web Application	
	76	Intranet Application or available to public	Internet
	77	Web Application Name & URL	https://digilocker.gov.in, https://partners.digitallocker.gov.in https://play.google.com/store/apps/details?id=com.digilocker.android https://apps.apple.com/in/app/digilocker/id1320618078 (Also refer corrigendum-1)
	78	Brief about the website and activities done through the website	Visit https://digilocker.gov.in
	79	Will the website/webapplication/webservice available remotely for auditing (Yes/No) *(If No, then the auditors will have to travel to client premises and the costs may include the travel and accomodation charges)*	Onsite
	80	Number of Roles in the application	Refer sl. No 3
	81	Number of static pages	Refer corrigendum -1
	82	Number of Dynamic Pages	Refer corrigendum -1
	83	Payment Gateway Integrated with the application (YES / No)	Refer Sl. No 11
	84	Number of User Input fields (approximately)	Refer corrigendum -1
	85	Whether the web application contains any Content Management System. If yes, please mention name of the CMS Yes/No	There is no CMS being used in the application.
C	86	Please share sample login credentails , one for each role Yes/No	Testing and audit will be conducted on production environment. The auditors can sign up to access their DigiLocker account. It is a freely available public application.
D A	87	Please share SRS or technical document of the website if any is available Yes/No	Refer weblink below: https://digilocker.gov.in/resource-center.html
C	88	Please share previous audit reports if any are done and available Yes/No	This information shall be provided at the time of Audit Comencement to the QAP.
	89	Are you maintaining application logs Yes/No	Yes
	90	Willing to provide server remote connection to collect the log evidences Yes/No In order to get OWASP Top 10 2018 Complaince, this is mandatory. If you answer No for this, then we will not be able to provide OWASP 2018 complaince certificate.	No
		DETAILS OF MOBILE APPLICATION	
	91	Name of the Mobile application	DigiLocker
	92	Type of Application, Native or Hybrid	Native plus Web Flow
	93	Supportive Operating System	Android and IoS
	94	Does the application has a login interface if so , how many user roles are available	Refer Corrigendum -1
	95	Brief about the mobile application and activities done through the mobile application	
	96	Number of Screens	
	97	Number of Activities	
	98	Number of User Input fields (approximately)	
	99	Is there any webservice which the app interacts with, if so do you want the web service also to be audited	Refer Sl. No. 12
	100	Payment Gateway Integrated with the application (YES / No)	Refer Sl. No. 11
	101	Please share Mobile application User manual or SRS	Refer Corrigendum-1

11/2/20

Corrigendum to RFP Document

'Tender Enquiry No.: DL/SA/2020-01'

Kindly note the following corrigendum is being affected in the RFP Document **'Appointment of QA Partner Agency for conducting Security and Event based Audit of DigiLocker.'**

Section 10. Financial Bid Format. (Page-9 Table 4)

'nterested bidders are required to quote their rates as per below mentioned format.

S. No	Description	Amount in Rupees (to be quoted without Tax)
1	Annual Security Audit of all components of DigiLocker (as per section 3.1) and submission of Audit certificates for a total of 3 years.	
	(a) • DigiLocker web application	
	(b) • DigiLocker Mobile Web	
	(c) • DigiLocker iOS App	
	(d) • DigiLocker Android App	
	(e) • DigiLocker Partner Portal	
	(f) • Repository.	
2	API testing (as per section 3.2) for a total of 3 years. This shall include all API end points, External APIs, API performances and API security. (Price to be quoted for 250 APIs testing).	
Grand Total (Overall Cost):		
Amount in Words:		

The Bidder(s) shall note that modification(s) issued in this corrigendum shall prevail over the existing provisions of the Bid Document and any clarifications/ modifications provided as on date.

24/2/2020
(Debabrata Nayak)

24/2/20
(R A Dhawan)

24/2
(G R Sharma)

24/02/2020
(Tushar Rai)

24.02.2020
(Amit Jain)

24.02.2020
(Anoop Kumar)

Queries received till 22nd Feb,2020 11:00 am

Tender Enquiry No.: DL/SA/2020-01
Appointment of QA Partner Agency for conducting Security and Event based Audit of DigiLocker

QUERY	RESPONSE
Xiarch Solutions Private Limited 1) Please confirm the audit location. 2) Please share the full scope of work of the below applications (kindly fill attached scoping sheets) -DigiLocker web application -DigiLocker Mobile web -DigiLocker Android app -DigiLocker iOS app -DigiLocker Partner portal -Repository 3) Please also share the total no. of functions/ method in 250 API's. We are supposing 250 API's audit to be performed at each year (250*3).	**Response:** 1) Audit location will be NeGD, Electronics Niketan, 6, CGO Complex, New Delhi-110003. 2) DigiLocker Features and Partner Portal features are enclosed. 3) Bidder has to quote for audit of 250 APIs. The number of APIs to be audited will be determined later on. This number may be more or less than 250.
Precise Testing Solution Pvt. Ltd. Only certain empanelled legacy can bid on this but Certin empanelled agency only able to check the security of application but when required to check functionality of application, Performance ,Website testing and GIGW Guidelines, These testing only can do my STQC empanelled Agency .	**Response:** Since, we are not considering functional testing and are going for security audit only. Hence, Bids are invited only from CERT-In (The Indian Computer Emergency Response Team) empanelled agencies only.

24/2/2020
(Debabrata Nayak)

24/2/20
(R A Dhawan)

24/2
(G R Sharma)

24/02/2020
(Tushar Rai)

24.2.2020
(Amit Jain)

24.02.2020
(Anoop Kumar)

DigiLocker

Introduction:

DigiLocker system is a flagship initiative of Ministry of Electronics and Information technology (MeitY) under Digital India Programme, which was launched by the Hon'ble Prime Minister of India in the year 2015. DigiLocker aims at the 'Digital Empowerment' of citizens by providing a document wallet to citizens to access authentic documents/certificates in digital format from the source of truth thereby, promoting the vision of paperless governance. DigiLocker aims to provide a Digital wallet to every citizen so that all the documents can be made available electronically at one place and can be accessed from anywhere anytime.

Indicative list of Features:

These are available all across platforms i.e. Android, IOS and Web (this is not exhaustive list, platform may have other features to be audited).

1) Sign Up

a) Sign up with Mobile plus OTP
b) Profile creation
c) Aadhaar demographic authentication.
d) Sign Up with Aadhaar plus OTP
e) Setting of Account PIN

2) Sign In

a) Sign in with Mobile plus OTP
b) Sign In with Aadhaar plus OTP
c) Setting of PIN
d) Validation of account PIN and resetting of account PIN
e) Setting and Resetting MPIN for device level security.

3) Profile Update

4) Issued Section: Document comes directly from the source of truth (URI based): Documents in issued section of DigiLocker are deemed to be at par with the Original document as per IT Act, 2000. Recent RBI guidelines also promoted KYC through Digital Locker.

a) Pull Document
b) Fetch document
c) Deleting issued documents
d) Sharing feature
e) Download option of issued documents in JSON, XML,PDF format.
f) Mobile view of issued documents and QR code scanning wherever available.
g) Refreshing of Issued documents

5) Upload section:

a) Creation and deletion of folders.
b) Uploading, sharing and deleting of Uploaded documents.

6) APIs for all above features to be tested:

Partner's Portal Features

- **For Organization**
    - Registration Form
    - Statistics Dashboard
    - Password set/reset
    - Configuring Issuer (Pull URI and Pull Doc), Requester, Authorized Partner, Save to Locker, Verifier API settings
    - Doc type mappings for Issuer API (Pull URI and Pull Doc APIs)
    - Addition of bets users for Issuer API testing
    - Verifier console (for manual ad-hoc verification)
    - Issued, Verified and Shared Documents logs
    - Verifier Request and Approval process
    - Key management system for Issuer, Requester, Authorized Partner, Verifier and Trusted Partner (now deprecated) modules

- **For DigiLocker Super Admin**
    - Processing (Approval/ Rejection) of potential Partner's Requests
    - Managing various aspects of API ecosystem- Document Types creation/ update/ deletion, Password policy, Captcha attempts limit, District List, Partner Category and its Priority settings
    - Checking Issuer API settings and testing
    - Check Verification Logs
    - Check Uploaded CSVs (feature now deprecated)
    - Check/ Update Partner Account's details/ login credentials