RULES AND PROCEDURES FOR CERTIFICATION OF DIGITAL LOCKER SERVICE PROVIDERS(DLSP)/ DL REPOSITORIES

January 2017

DLCS-01-01, Issue-1

STQC Directorate, Ministry of Electronics & Information Technology,
Electronics Niketan,
6 CGO Complex, Lodi Road,
New Delhi – 110003.

Amendment Log

Version Number	Date	Change Number	Brief Description
ISSUE 1			

Table of Contents

List of Tables

1. Introduction & Background

Digital Locker is a Digital India initiative. It is aimed at making available certificates and digital documents issued by the government (any government agencies) on the cloud (obviating the need for citizens to repeatedly submit printed or digitized copies of government issued certificates to other government agencies, while interfacing with government for services) and providing private space (1 Gb) to all interested citizens in public cloud to store their documents in a safe and secure manner. It would thus enable less paper or paperless government, providing efficiency and convenience to public.

Towards the above, a DigiLocker was set up by NeGD/MeitY and a large number of users are already using it, with many issuers (e.g. motor vehicle departments) making available certificates of citizens in the repository which in turn is pushed to the Digital Locker portal for citizens and Requestors (other government agencies).

It is now proposed to extend the above by licensing many Digital Locker service providers and empanelling many repositories so that government agencies can choose their issuers who in turn can make available their digital documents (authenticated and with unique document number) in the repositories.

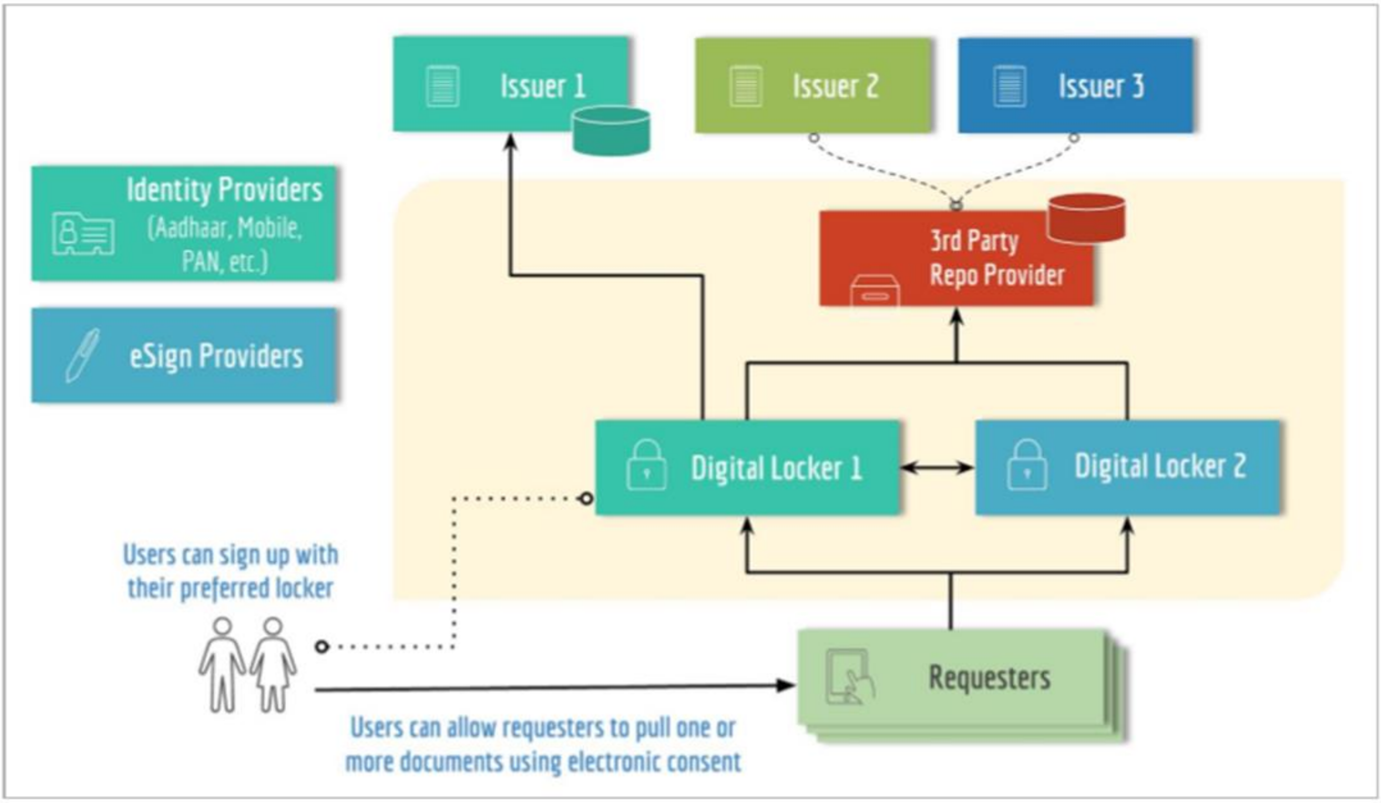
These in turn can be pulled by users or requestors or pushed by government agencies to the digital lockers. The documents themselves will only be stored in repositories but the URI/URLs will be available in Digital Lockers for users/citizens to search and pull when they need them.

Digital Lockers (multiple of them) and Repositories (many) form the core components that work in a federated manner, provide seamless delivery of government issued authenticated digital documents to citizens and requestors (other government agencies) in a secure and trusted manner.

This competitive, federated model is supported by a number of features in the architecture of Digital Locker – a number of APIs defined for supporting Pull, Push, Fetch etc. being some of them. The DLTS for Technical Specifications, DLTF for Technical Framework, Introduction to Digital Locker and API specification documents are some documents that clearly specify various details (references indicated below).

For realizing the approach outlined above, rules and procedures for Certification of Digital Locker Service Providers including audit and testing criteria need to be spelt out. The objective of this document is to outline of these rules and procedures.

Architecture of the Digital Locker is given in the figure below.


Issuer 1
Issuer 2
Issuer 3
Identity Providers (Aadhaar, Mobile, PAN, etc.)
eSign Providers
3rd Party Repo Provider
Digital Locker 1
Digital Locker 2
Users can sign up with their preferred locker
Requesters
Users can allow requesters to pull one or more documents using electronic consent

2. Relevant Standards, Tests and Scope for Audit and Certification of Digital Locker Service Providers

It is important to ensure that Digital Lockers and DL Repositories are compliant to Information System Security Management Standard, ISO 27001 and Security testing –

OWASP Top 10, Vulnerability check, SQL injection, Hardening and Security Controls check.

In addition, in respect of Digital Lockers, compliance to standards relating to Accessibility (GIGW/ISO 40500), Web Application Security (ISO27034), and Service Management, including performance - ISO-20000-1 will be valuable.

In respect of DL Repositories, given that the repositories store a large number of citizens' documents, compliance to Information Security as it is applicable for storage, ISO 27040, will be necessary, atleast in the second stage. Again, compliance to Information System Security Management standard – 27001, Protection to PII in the system through compliance to those aspects spelt out in ISO 27001, and Service Management, including performance -ISO 20000-1 (as per criteria) will be necessary to ensure governance & operational aspects of quality of service delivery and performance.

One more aspect to be ensured is compliance to APIs, based on use cases. This can be achieved based on interoperability with current implementation of DigiLocker and associated repositories. List of APIs relevant to each interface of Digital Locker and Repository are indicated in the references.

Functional Testing and end-to-end testing based on Use-Cases can also be included for DLSPs and DL Repositories. Input Validation, Error conditions for the error codes provided, Proxy Testing, Capture messages – check for compliance to the API format, including request and response are additional tests to be conducted.

3. STQC Assurance Framework

Audit criteria for licensees or potential licensees of Digital Lockers and repository agencies (provisionally empanelled or to be empanelled) is given in section 3.1 below. Based on the same, certifying authority of STQC will certify them and ONLY then can they commence operation. Relevant attributes and standards against which Digital Lockers and Repositories will be audited and certified are given below:

Table 1:Relevant attributes and standards against Digital Lockers and Repositories

S #.	Attribute	Relevant, Standard	Applicability to a given architectural component	Agency whose Audit/Certification/Test report to be enclosed*
1.	Information Security Management System	27001; Controls for Protection of PII to be included in the second phase as elaborated in ISO 29100/29101 and 27018 where applicable; OWASP Top 10, Vulnerability Assessment, SQL injection, Hardening, Penetration testing, Security Controls check	DLs, Repositories	Test and Audit reports from STQC labs, STQC empanelled Test labs and authorized ITTLs
2.	Accessibility	GIGW/ISO40500 (limited to accessibility)	DLs	Test and Audit reports from STQC labs, STQC empanelled Test labs and authorized ITTLs
3.	Portal & Application Security	ISO 27034	DLs	Test and Audit reports from STQC labs, STQC empanelled Test labs and authorized ITTLs
4.	Storage Security	Additional Controls relating to Storage Security vide ISO 27040 to be included in the second phase	Repositories	STQC Labs, Other authorized labs who are in a position to take up the effort
5.	Functional Testing, end-to-end testing based on Use-Cases, Input Validation, Error conditions for the error codes provided, Proxy Testing, Capture	Against Digital Locker Technology Framework 1.0, and APIs indicated therein	DLs, Repositories	STQC Labs

S #.	Attribute	Relevant, Standard	Applicability to a given architectural component	Agency whose Audit/Certification/Test report to be enclosed*
	messages – check compliance to the API format, including request and response.			
6.	Service Management, Performance and Scalability	ISO 20000-1 preferred; As per declared requirement given in references or as indicated at the time of licensing	DLs, Repositories	Certificate from recognized certification agencies

*In addition, audit, testing and certification from any CERT-In empanelled test agencies or nationally accredited certification agencies will be accepted for 27000-1 and another security testing audit/certification. For 20000-1, again, certification from any nationally accredited certification agency will be accepted.

The licensee/potential licensee or empanelled repository need to submit an application to STQC and provide self-declaration signed by an authorized signatory with seal.

Schedule of Charges for STQC audit, testing and certification is indicated in DLCS-01-03.

Format of Application form for Digital Locker Service Provider Certification is given in DLCS-01-02.

Format of Nondisclosure Agreement shall be signed by the applicant and STQC is given in DLCS-01-04.

Scope of Audit and Audit criteria is given in section 3.1.

The applicant shall submit their test plan, test cases and test reports. STQC will conduct an audit covering 10% of total high risk test cases which are critical/strategic in nature.

- Audit report format is given in 3.3 below.
- Certification framework is given in 3.4 below.
- Format of Certification Agreement is given in DLCS-01-05.
- Format of Certificate of Approval that shall be issued by STQC Digital Locker Service Providers is given in DLCS-01-06.

Only on obtaining Certification from STQC and fulfilling other conditions as specified by Digital Locker Authority or relevant agency specified by MeitY and getting their authorization shall a Digital Locker Licensee or a Repository commence operation.

List of certified licensees shall be indicated in the STQC web-site as indicated in DLCS-01-07.

3.1. Audit Criteria

Audit criteria for Digital Lockers and Repositories are given respectively below:

3.1.1 Digital Lockers

Table 2:Audit criteria for Digital Lockers

S. #	Attribute	Relevant Standard	Mandatory or Optional	Audit Criteria: Requirements, Controls and Guidance	Acceptable Audit and Certification agencies*	Means of compliance demonstration*
1.	Accessibility	GIGW/ISO40500 (limited to accessibility)	Mandatory	http://guidelines.gov.in/compliance.php	-	Test and Audit reports from STQC labs, STQC empanelled Test labs, authorized ITTLs – Production of Reports/Certificates
2.	Portal & Application Security	ISO 27034	Mandatory	https://www.owasp.org/index.php/Main_Page	-	Test and Audit reports from STQC labs, STQC empanelled Test labs and authorized ITTLs – Production of Reports / Certificates
3.	Information Security Management System	ISO 27001	Mandatory	As per Standard Criteria	Audit and Certification reports from STQC labs, STQC authorized labs and recognized certification agencies	-
4.	Functional Testing, end-to-end testing based on Use-Cases, Input Validation, Error conditions for the error codes provided, Proxy Testing, Capture messages –	Against Digital Locker Technical Specifications Ver.2.3, Digital Locker Technology Framework 1.0, and APIs indicated therein	Mandatory	DLTF 1.1	-	STQC Labs

S. #	Attribute	Relevant Standard	Mandatory or Optional	Audit Criteria: Requirements, Controls and Guidance	Acceptable Audit and Certification agencies*	Means of compliance demonstration*
	check compliance to the API format, including request and response.					
5.	Service Management, Performance and Scalability	ISO- 20000-1	Optional	As per Standard Criteria	Audit and Certification reports from STQC labs, STQC authorized labs and recognized certification agencies	--

*In addition, audit, testing and certification from any CERT-In empanelled test agencies or nationally accredited certification agencies will be accepted for 27000-1 and another security testing audit/certification. For 20000-1, again, certification from any nationally accredited certification agency will be accepted.

3.1.2. Repositories

Table 3:Repositories

S. No.	Attribute	Relevant Standard	Mandatory or Optional	Audit Criteria: Requirements, Controls and Guidance	Acceptable Audit and Certification agencies*	Means of compliance demonstration*
1.	Information Security Management System	ISO 27001	Mandatory	As per Standard Criteria	Audit and Certification reports from STQC labs, STQC authorized labs and recognized certification agencies	-
2.	Protection of PII	ISO-27001 controls, as elaborated in ISO 29100/29101 and 27018, where applicable	Optional in the first phase	Additional Controls (over ISO 27001) as applicable to protection of PII	STQC labs (If STQC authorized labs or recognized labs/certification agencies provide audit and certification,	

S. No.	Attribute	Relevant Standard	Mandatory or Optional	Audit Criteria: Requirements, Controls and Guidance	Acceptable Audit and Certification agencies*	Means of compliance demonstration*
					that will be acceptable).	
3.	Storage Security	ISO 27040	Optional in the first phase	Additional Controls (over ISO 27001) as applicable to Storage	STQC labs (If STQC authorized labs or recognized labs/certification agencies provide audit and certification, that will be acceptable.)	-
4.	Functional Testing, end-to-end testing based on Use-Cases, Input Validation, Error conditions for the error codes provided, Proxy Testing, Capture messages – check compliance to the API format, including request and response.	Against Digital Locker Technical Specifications Ver.2.3, Digital Locker Technology Framework 1.0, and APIs indicated therein	Mandatory	DLTF 1.1	-	STQC Labs
5.	Service Management, Performance and Scalability	ISO - 2O000-1	Optional	As per Standard Criteria	Audit and Certification reports from STQC labs, STQC authorized labs and recognized certification agencies	-

*In addition, audit, testing and certification from any CERT-In empanelled test agencies or nationally accredited certification agencies will be accepted for 27000-1 and other security testing audit/certification. For 20000-1, again, certification from any nationally accredited certification agency will be accepted.

3.2 Procedure for maintenance approval

The Certified DLSPs and DL Repositories, once audited/tested and certified and commence operation, shall undergo surveillance or maintenance audit every year and submit the report to STQC. Such a requirement is mandatory.

3.3 Audit report

Audit Team shall submit the audit report.

3.4 Certification framework

Certification framework would consist, as per standard STQC process, of a governance mechanism. It shall, inter alia, involve a CEO (Certification) who shall issue the final STQC certification for a DL licensee / potential licensee or an empanelled repository. He shall report to DG, STQC and will be supported by Technical Advisory Committee, Operational division, Oversight mechanism and Certification guidelines (based on examination of audit reports) etc.

4. Road-map

It is recommended that while the above constitute rules and procedures for Digital Locker Certification scheme (including audit procedures thereof), it might be appropriate to proceed with a balanced approach which ensures priority to factors like security, interoperability and accessibility while progressing in a more graded manner in respect of Service Management, Functional testing, Privacy and the like. This will lead to a lighter load on Digital Locker licensees, atleast initially. Besides, one can expect competition and market forces to push up innovation, quality and performance as adoption picks up, with the promotional efforts of Digital Locker Authority and MeitY.

5. References

I. Reference resources on Digital Locker, https://digilocker.gov.in/resource-center.php

II. Digital Locker, User manual, https://digilocker.gov.in/assets/img/DigiLocker-User-Manual.pdf

III. DigiLocker – Introduction, https://img1.digitallocker.gov.in//assets/img/DigiLocker-Intro.pdf

IV. Digital Locker Technology Framework, https://static.mygov.in/rest/s3fs-public/mygov_147643905233847684.pdf

V. Issuer APIs, https://digilocker.gov.in/resource/issuer-APIs.php

VI. Requestor APIs, https://digilocker.gov.in/resource/requester-APIs.php

VII. DLCS-01-01, Rules and Procedure for Digital Locker Service Provider (DLSP) and DL Repositories Certification, Issue-1, January 2017

VIII. DLCS-01-02, Application form for DLSP and DL Repository Certification, Issue-1, January 2017

IX. DLCS-01-03, Schedule of charges, Issue-1, January 2017

X. DLCS-01-04, Nondisclosure Agreement, Issue-1, January 2017

XI. DLCS-01-05, Certification agreement, Issue-1, January 2017

XII. DLCS-01-06, Certificate of approval for DLSP and DL Repository, Issue-1, January 2017

XIII. DLCS-01-07, List of certified DLSPs and DL Repositories, Issue-1, January 2017