"Digital Locker" Technology Specification (DLTS)

Version 2.3, March 2015

Abstract

*This document offers a standardized mechanism to issue government documents to Aadhaar holders in electronic and printable formats, store them, and make it shareable with various agencies. This allows government issued documents to be moved to electronic form and make it available for real-time access in a set of "digital repositories". This solution also offers multiple digital locker providers and access gateways to co-exist to enable healthy ecosystem play. Usage of Aadhaar ensures that document owner is strongly authenticable eliminating document frauds. In addition to supporting new documents to be made electronic and online accessible, this solution also offers a way to digitize older documents. Proposal also offers a mechanism by which "digital lockers" can be offered by service providers and suggestion to provide "a **default** digital locker" portal and mobile application to residents to view a consolidated list of documents using their Aadhaar number.*

Introduction

Currently, in India, almost all of the government issued documents are in physical form across the country. This means every time a resident needs to share the document with an agency to avail any service, an attested photo copy either in physical form or on scanned form is shared. Use of physical copies of document creates huge overhead in terms of manual verification, paper storage, manual audits, etc. incurring high cost and inconvenience. This creates problem for various agencies to verify the authenticity of these documents, thus, creating loopholes for usage of fake documents/certificates. Due to the nature of these documents not having a strong identity attached to it, anyone with same name can indeed misuse someone else's document.

Digital India Vision

The Digital India programme cleared by the cabinet in August 2014 seeks to '*prepare India for a knowledge future*'. There are three key objectives; (a) to create a digital infrastructure for online digital identity, mobile phone and a bank account, (b) to service and govern a real-time online financial transaction platform, and (c) ***to digitize all documents and records of the residents and make them available on a real-time basis***.

This vision of electronic resident document system should address two key aspects:

1. ***Minimizing usage of physical documents*** (no scan/photocopies, no physical papers) via electronic formats and sharing across agencies; and
2. ***Eliminating usage of fake documents*** (no fake govt/degree certificates, no fake usage

of someone else's certificate) via a mechanism to verify "authenticity" of government issued documents online.

3. ***Provide a default "digital locker"*** for people to store and access Government issued documents in the Government cloud if they wish to subscribe.

Solution Objectives

Objectives of such digital repository solution are:

1. Eliminate need for the residents to maintain hard copy of government issued documents.
2. Eliminate need for the residents to produce (in hard format) government issued documents, while applying for services.
3. Provide secure and consented access of government issued documents to user agencies.
4. Reduce administrative burden, service fulfillment time, and costs by enabling paperless transactions.
5. Ensure all the documents issued to the residents are available to him/her anywhere anytime, in a standard format which can be shared with any other department.
6. Provide an open, interoperable, multi-provider architecture to ensure departments and states have flexibility to use best document repository for their purposes.
7. Provide an architecture that can support well structured future documents as well as a mechanism to digitize older documents that may not have machine readable formats.
8. Provide a default portal and mobile application for residents to view their documents in a consolidated way.

Characteristics of Electronic Documents

To meet the key goals and the solution objectives, architecture should ensure that all government issued "*electronic documents*" stored in digital repositories are:

1. ***Machine Readable*** – documents in electronic format should be machine readable eliminating human workflow for viewing and verifying the documents. Document structure should adhere to common XML structure for application usage and interoperability.
    a. Documents should have a common set of "meta" attributes such as "issuer agency code", "document ID", "issue date", "Aadhaar number(s) of the individuals to who the document is issued to", "expiry if any" along with document type (domain) specific sub data structure (e.g. school certificates will have different data elements compared to marriage/caste certificates).
2. ***Printable*** – all electronic documents should have a printable format "attached" to it allowing continued printing of certificates for individuals and for backward compatibility with existing paper based systems.
3. ***Shareable*** – residents can easily share the documents with other agencies/departments just by proving the unique document URI without having to share photocopies, scan copies, document uploads, etc. Since all one needs is a small URI, such sharing can easily

be done even on feature phones even via SMS and text based systems.

4. ***Tamper Evident*** – documents in electronic form should be digitally signed by the issuing department/agency which allows any tampering to be detected electronically. This also allows agencies to be compliant to IT Act.
5. ***Verifiable*** – most importantly, government documents and certificates issued can be verified online for "authenticity" (validating if the document shared by an individual indeed was issued by appropriate authority) eliminating the use of fake documents/certificates. In addition, Aadhaar attached documents/certificates ensure ONLY the owner Aadhaar holder can indeed use the certificate, thus eliminating misuse of someone else's certificates.
6. ***Secure*** – it is critical that documents in the repositories are secure in terms of storage and access. In addition, specific documents (based on type of document) may only be shareable via owner authentication to ensure sharing and access is "authorized" by the document owner.

It is highly recommended that government issued resident documents have the Aadhaar number(s) of the people. When digital documents/certificates are not attached to Aadhaar, it is important to note that, while those documents can be still made available online in electronic format, it can potentially be misused by another person who has same name/gender etc. It is impossible to verify if the certificate/document was issued to same individual without affixing a "*real identity*" using Aadhaar number. Hence it is important to mandate use of Aadhaar number in all resident documents to strongly "*assert*" ownership.

Assumptions

1. Considering states and various departments, solution should provide a scheme for multiple repositories to co-exist and interoperate seamlessly. This also avoids a design requiring a single central database for all across the country.
2. Resident documents in electronic formats are stored in federated fashion (no centralized single document repository). Designated set of central repositories would be part of the system (e.g. central repositories dedicated to universities and educational institutions, a dedicated repository for health centres, etc). Each agency responsible for issuing documents/certificates in electronic form and storing them in a designated repository.
3. Departments/agencies should be able to digitize older existing documents and bring them into this common electronic document system and provide seamless access.
4. All documents in electronic formats must be digitally signed by the issuing department/agency to be "trustable" by other agencies and be compliant with IT Act.
5. In future, all documents must be issued to an Aadhaar holder to ensure ONLY that person can indeed claim ownership. If a strong identity is not attached, a government document may be misused by people with same demographics (name/age/gender).
6. All future electronic documents are available in both machine readable and printable formats. Old documents that are digitized may or may not a corresponding machine

readable form. This allows departments to easily start digitizing documents and gradually adopt a fully electronic form.

Proposed Architecture

This section covers solution architecture in detail including terminology used, high level architecture diagram, document identification scheme, document issuance lifecycle, document sharing scheme, and some examples.

Key Terminology

1. ***Electronic Document or E-Document*** – A digitally signed electronic document in XML format issued to one or more individuals (Aadhaar holders) in appropriate format compliant to DLTS specifications. Examples:
    - Degree certificate issued to a student by a university.
    - Cast certificate issued to an individual by a state government department.
    - Marriage certificate issued to two individuals by a state government department.
2. ***Digital Repository*** – A software application complying with DLTS specifications, hosting a collection (database) of e-documents and exposing a standard API for secure real-time access.
    - While architecture does not restrict the number of repository providers, it is recommended that few highly available and resilient repositories be setup and encourage everyone to use that instead of having lots of repositories.
3. ***Digital Locker***- A dedicated storage space assigned to each resident, to store authenticated documents. The digital locker would be accessible via web portal or mobile application.
4. ***Issuer*** – An entity/organization/department issuing e-documents to individuals in DLTS compliant format and making them electronically available within a repository of their choice.
5. ***Requester*** – An entity/organization/department requesting secure access to a particular e-document stored within a repository. Examples:
    - A university wanting to access 10th standard certificate for admissions
    - A government department wanting to access BPL certificate
    - Passport department wanting to access marriage certificate
6. ***Access Gateway*** – A software application complying with DLTS specifications providing an online mechanism for requesters to access an e-document in a uniform way from various repositories in real-time.
    - Gateway services can be offered by repository providers themselves.
    - While architecture does not restrict the number of repository providers, it is suggested that few resilient and highly available central gateway systems be setup and requesters can signup with any one of the gateways for accessing documents in the Digital repositories.
7. ***Document URI*** – A unique document URI mandatory for every document. This unique

URI can be resolved to a full URL to access the actual document in appropriate repository.

- Document URI is a persistent, location independent, repository independent, issuer independent representation of the ID of the document.
- The existence of such a URI does not imply availability of the identified resource, but such URIs are required to remain globally unique and persistent, even when the resource ceases to exist or becomes unavailable.
- While document URI itself is not a secret, access to the actual document is secure and authenticated.

Proposed Architecture at High Level

In the diagram below, top side represents the issuance part and bottom side represents the real-time access part.

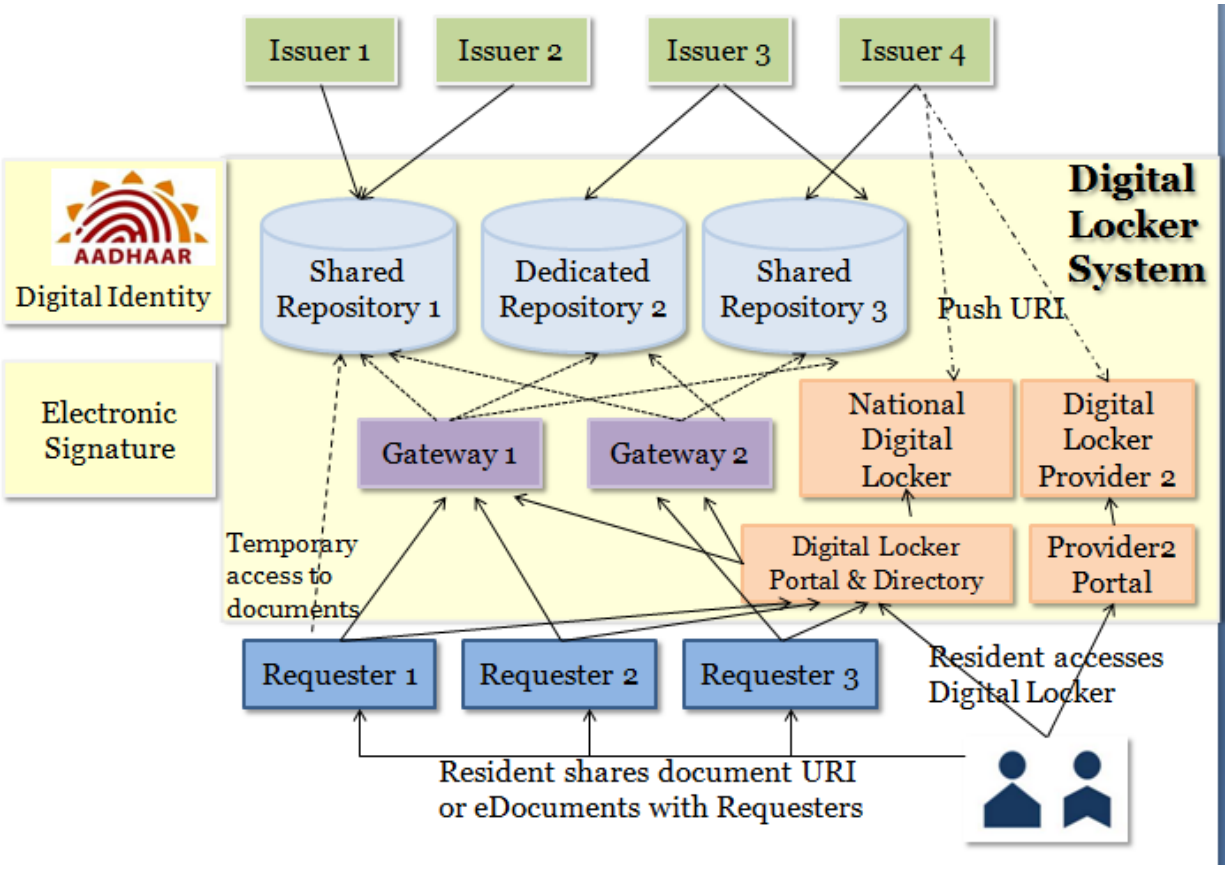

Diagram depicts the federated model of document storage via designated dedicated digital repositories. It also depicts the co-existence of highly available document access gateway(s) (one or two) that can be used to access these documents stored in these repositories. Individuals (Aadhaar holders) may be provided a "default digital locker" mechanism to directly access the repository via secure access scheme and viewing a consolidated list of URIs in their inbox.

Core features of the architecture:

1. Digital "certified" repositories and gateway providers (Government provided or 3rd party provided) using an interoperable DLTS compliant standard for scalability and to avoid one single central registry.
2. Storage and access using unique document URIs and by Aadhaar numbers (access using a document URI points to one e-document while access via Aadhaar number can point to multiple e-documents issued to him/her).
    a. All access via auditable and non-repudiable mechanism (API access control) to ensure no "public anonymous" access is allowed
    b. Access via document URI may or may not require Aadhaar holder authentication depending on the document type (some doc types may mandate Aadhaar authentication before every access while publicly available documents may not).
    c. Access via Aadhaar number must ALWAYS be after authentication to ensure access is authenticated and authorized by owner (Aadhaar holder).
3. Issuers can issue new e-documents in DLTS compliant format completely independently of each other issuers at their own pace.
4. Issuers can also choose to digitize older documents without having a machine readable representation and allow a verifiable and secure access to older (legacy) documents. They can focus on new documents in DLTS compliant format while progressively providing digitization of older (existing) documents.
5. Residents can also choose to convert their existing certificates using "self signed" or "notary signed" mechanism and store them in a digital locker. Acceptance of such documents will depend on the requester rules.
6. Issuers can provide a printed copy of the document to the individual after storing them in their repository making it verifiable, shareable, accessible, and re-printable.
7. Issuers can choose their own print formats and styles as they do today.
8. Issuers can use their own document numbering scheme and introduce new scheme for new documents without having to stick with one numbering scheme for ever.
9. Issuer can choose one of the designated repository provider for all their documents or choose separate repository providers for different document types.
10. States can choose to use a common repository provider or build their own.
11. Residents can share the document with other agencies/departments (e.g., sharing CBSE mark sheet with a university) just by sharing the document URI printed on their certificate instead of providing a photocopy or scanned copy.
    a. Sharing via simple URI allows document sharing via mobile, SMS, website, etc easily. Whenever owner authentication is required, Aadhaar authentication (OTP or biometrics) can be used to authenticate every access.
12. Requesters can dynamically obtain the list of document types defined by issuers by querying the metadata of the repository allowing issuers to add new document types dynamically.
13. Requesters to use highly available gateway system to access URIs of the required document. The requesters would get temporary access to the documents directly from

the repositories for download.

14. DLTS solution uses open standards and multi-provider ecosystem strategy. Both government and private players could play the role of repository and gateway providers so that issuers and requesters get the best "choice" that fits their needs.
15. Solution addresses all core objectives as described earlier in this document while keeping entire system open via common standards.

It is important to note that interface between Repository, Gateway, and Digital Locker MUST BE via DLTS APIs only to ensure these are loosely coupled. This loose coupling allows providers to refactor, scale, administer, price, etc independent of each other. If a provider offers both repository and gateway features, it must be ensured that users (Issuers and Requesters) can sign up for individual services instead of bundling everything into a monolithic offering.

Unique Document URI

Every document that is issued and made accessible via DLTS system must have a unique way to resolve to the correct repository without conflict. This is critical to eliminate the need for all documents reference to be in one system. Federated repositories storing documents issued by various departments/agencies must be "reachable" via the gateway in a unique fashion.

All documents issued in compliance to DLTS should have the following URI format:
`IssuerId-DocType-DocId` where

`IssuerId`	is a unique issuer entity ID across the country
`DocType`	is the document type optionally defined by the issuer
`DocId`	is a unique document ID within the issuer system

Issuer ID (mandatory)

All departments/agencies within government issuing resident documents, termed as "*Issuers*" must have a unique identification to ensure all documents issued by them are accessible via DLTS gateway.

It is recommended that list of unique issuer codes be derived via their domain URL whenever available and be published as part of e-governance standard codification scheme with ability to add new issuers on need basis. When URL is not available for a department, a unique (alpha) code may be assigned.

Examples of issuer Ids are "maharashtra.gov.in" (Maharashtra State Government), "kseeb.kar.nic.in" (Karnataka School Board", "cbse.nic.in" (CBSE School Board), "UDEL" (Delhi University), etc. These codes **MUST BE unique across India** and published as part of standard e-governance codification list.

Document Type (optional)

Issuers can freely define a list of document types for their internal classification. For example, CBSE may classify certificates into "MSTN" (10th mark sheet), "KVPY" (certificate issued to KVPY scholarship fellows), etc. There are no requirements for publishing these via any central registry.

Classifying documents into various types allows issuers to choose different repositories for different types. This is to future proof the design without making assumption that all certificates issued by the issuer are available in same repository. This also allows migration from one repository to another in a gradual way. Issuers are free to define their document types without worrying any collaboration across other issuers. Keeping the length minimal allows manual entry of document URI without making it too long. Hence it is recommended to keep length to be only up to 5.

It is recommended that issuers define document types either using pure alpha case-insensitive strings of length up to 5. These document types MUST BE unique WITHIN the issuer system. This classification within the issuer system also allows versioning of documents making future documents to be of different formats and in different repositories without having the need to have all documents in one repository. **If need arises in future to go beyond length 5, maximum length of doc type can easily use increased without breaking compatibility any existing systems and documents.**

Document ID (mandatory)

A document ID determined by the department/agency (issuer) should be assigned to every document. It MUST BE unique either within the document types of that issuer or it can be unique across all document types of that issuer.

Document ID is an alpha-numeric string with maximum length of 10. It is recommended that issuers define document IDs either using pure alpha case-insensitive string using a RANDOM number/string generator. Document IDs MUST BE unique WITHIN the issuer system within a document type. If need arises in future to go beyond length 10, maximum length of doc ID can easily use increased without breaking compatibility any existing systems and documents.

Using random string eliminates the possibility of "guessing" next sequence number and accessing a list of documents in a sequential way. This is critical to ensure security of documents and ensures document can be accessed ONLY IF the requester "knows" the actual document ID (instead of guessing sequential numbers).

It is highly recommended that issuer needing to issue a total of ***n*** documents within a document type use at least ***10n*** random space from which the strings/numbers are chosen to randomly allocate. Notice that since document types allow further classification, it is suggested to keep

the length **minimal**. Since issuers can easily add a new document type without any collaboration and approvals across other issuers, if more numbers are required, a new document type may be introduced.

Examples

Following are few examples of document URI printed on the document using QR code and a human readable string.

CBSE-MSTN-22636726	KARMR-MCA-7385491	DLSSB-HSMS-GJSGEJXS

Document Issuance Flow

Document issuance flow is given below:

1. Create a new digitally signed e-document complying to DLTS specification with a unique URI and an attached optional printable version.
    a. Issuer entity uses the unique code for itself (obtain a new one if not already listed) that is available in common DLTS Issuer Codification e-governance standards. This is a country wide "Unique Issuer ID.
    b. Document type codification and ID numbering is left to the freedom of issuer. Doc types are issuer specific and need not be unique across issuers. If a new type is required, they should simply register the new type in the repository and start using them.
2. Issuer should have tied up with a repository provider for storing documents and making it available online.
3. Store the new e-document in the repository. There are two ways to add a new document to a repository:
    a. via "add" API allowing online live addition of new documents (programmatic)
    b. via "web portal" of the repository provider in a manual fashion (human interface)
4. Issue the printed document to the individual(s) for whom the document is issued to with a barcode and human readable document URI.
    a. In addition to printed document, issuer may also share the e-document via email or other offline sharing schemes.
    b. Issuer should also offer an option to people to push the document URI with or without attachment (e-document) via SMTP to their digital locker address.

Every document issued must have this unique document URI in the format "`issuerId-`

`docType-docId`" printed (human readable) along with a barcode (machine readable, using "QR code").

Older documents being digitized should be defined under published list of document types so that just by using document ID, corresponding URI can be dynamically formed and document accessed from its repository.

Document Sharing and Access Flow

Residents wanting to share their documents to requester agencies will have the following flow:

1. Requester (department/agency wanting access to an e-document of their customer) asks the resident to provide the e-document URI
    a. There are three ways to share:
        i. Share the document URI (since this is simply a text string, this can be collected easily) along with Aadhaar number. Requesters can pull the document via their gateway.
            1. For older documents with just document ID (no full DLTS formatted URI), requester can ask the user to choose the issuer and document types from a list, collect document ID, and then internally form URI.
        ii. Or if it is a legacy self-signed document stored in digital locker, share the self-signed document access URL.
        iii. Or send/upload the copy of the e-document to requester's application directly (when requester has no gateway or digital locker access)
2. For e-documents stored in repositories, requester can access them using the URI and access credentials via a gateway. For accessing self-signed, scanned documents in digital locker, requesters can use digital locker "share" schemes.
3. Requester uses one of the gateway providers to access documents stored across federated DLTS repositories.
4. Requester uses DLTS Gateway API to access the document based on the URI.
    a. Note that some document types of some of the issuers may require online user authentication (via Aadhaar or Aadhaar enabled authentication provider such as e-Pramaan). This is based on Issuer rules.
    b. If the document type requires document owner authentication, appropriate authentication credentials (biometric/OTP/password, etc) also must also be captured.
5. Gateway system looks up its internal database and maps the URI to an actual repository URL and forwards the request to the appropriate repository.
    a. If authentication credentials are also sent by the requester, gateway system must do online authentication and only on successful authentication, request can be forwarded to repository.
    b. Gateway forms the URL and sends the request to repository based on the DLTS Repository API along with authentication success response.

6. Repository provider returns the digitally signed XML document after gateway authentication.
    a. Repository provider must validate credentials of gateway (API license key, digital signature, etc)
    b. Repository provider must validate if the Aadhaar number of the input and what's inside the document are matching.
    c. If the document type requires authenticated access, before returning the document, it must verify the authentication response provided by the gateway.
7. E-Document returned by the repository goes back to requester via gateway. For large printable documents, **a temporary printable URL** can be provided so that requester can directly download from repository without going via gateway (this must be one time download URL that expires).
8. Gateway MUST not store URI, e-document, and other authentication credentials as is. It MUST ONLY be used for transient access. Anonimized audit must be stored.
9. Requester uses the e-Document for its purposes and provides the intended service to the resident.
10. Repository provider publishes access audit via public URL for transparency and notification subscription.

National Digital Locker Directory, Portal/Mobile Application and Dashboard

DeitY, as the Digital Locker nodal agency would include an Digital Locker directory (providing details on Issuer ID, requestor ID, Gateway ID, etc.) on the national Digital Locker portal. The portal would also provide all Standards published via electronic documents for public access. Following key features must be incorporated within this Digital Locker Directory:

1. Provide public access to view the list of Issuers (name, ID, registration date), empanelled repositories (name, URL, date of empanelment, contact details), gateways (name, URL, date of empanelment, contact details), etc.

2. Provide repository and gateway empanelment guidelines, application form, and other details.

3. Provide link to request Issuer ID ï this application must allow new issuers to request a unique ID. This should be a simple electronic workflow to request, approve, and publish new ID.

The Digital Locker directory will play a critical role in ensuring that the e-Documents repositories which are under consideration for on boarding follow a defined work flow to ensure eligibility prior to becoming certified repositories and are listed on the directory.

The Digital Locker Directory will serve as a single window for discovery/browsing of various e-Documents repositories, issuers, requesters, gateways, and document types.

Digital Locker Interface

To provide a central view (inbox of sort) of all his/her documents and storing self-signed legacy documents, it is recommended that this "***digital locker***" feature is added via the National Digital Locker portal along with a mobile application.

Digital locker may provide the following features:

1. Ability for residents to register for digital locker service with optional Aadhaar verification.
    a. Also, a mechanism to "opt-out" or "de-register" should be provided if residents do not want to the digital locker.
2. Ability to "download" a "copy" of the e-document from appropriate repository to this digital locker by providing URI for backup and portability.
3. Ability to "upload" a self-signed or notary signed legacy certificate/document into the digital locker.
    a. A limited storage may be provided for storing such legacy documents.
    b. A mechanism to manage (tags them, delete them, etc) will have to be provided for completeness.
4. Additional features such as "share" (either URI or e-document) can be added as a value-added feature. This feature can allow residents to share with departments/agencies who may not have full provisions to automatically access via gateways. This feature also allows legacy documents to be shared.
    a. Features such as "document sets" can be created and shared (like shared folder)
    b. Sharing can be one time (via unique secure URL) or using push authentication via mobile application, OTP, etc). Sharing can be at document or document sets level.
5. Authentication, auditing, etc should be built-in to ensure security of the digital locker.
6. Digital locker must provide a mechanism to "subscribe" to "access notifications" (if any entity accesses a document within a repository, digital locker software can pull the anonymized audit and provide a notification scheme).
7. Ability to request Issuers to "push" document copy or just URI to resident's digital locker ID (e.g., user-id@mygov.in) via SMTP protocol.

Security & Privacy Aspects

- Document Security
    - Proposed solution avoids all e-documents to be stored in one central repository to minimize the risk of security and availability.
    - Since documents are mandatorily digitally signed, NO alteration can be done for misuse. It is ONLY the privacy aspect of the document that needs to be addressed.
- Access Security
    - Repository and gateway providers must comply with DLTS security and API

specifications.

- While some document types may be available to "trusted" requesters without electronic authentication and authorization of the owner (a simple consent may suffice), some document types may mandatorily require explicit electronic authentication and authorization of the document owner for every access.
- Access to repositories is only protected by API license keys, secure transport, and access level audits.
- If explicit authentication is required for a particular document type, a trusted authentication of the owner is mandated during access.
  - Architecture allows owner authentication via Aadhaar or other Aadhaar enabled trusted authentication schemes (e.g., e-Pramaan).
- Gateway provider MUST NOT store the document URI, e-document, authentication credentials, etc.
- Mandatory audit logs must be maintained both by gateway and repository providers.
- Repository provider MUST publish anonymized access logs in public for transparency as well as notification subscriptions by the document owners.

DLTS Detail Specifications

This section describes technical specifications for each of the aspect of DLTS solution including repository and gateway provider specifications at a high level.

NOTE: Following high level specifications must be expanded and completed before actual implementation of the whole system.

E-Document Specifications

Document URI

All documents issued in compliance to DLTS should have the following URI format:

`<IssuerId>[-DocType]-<DocId>`

Where,

`IssuerId` (mandatory) - is a unique issuer entity ID. This is a unique pure alpaha case-insensitive string. To easily make it unique, department's domain URL can be used whenever available. The list of issuer Ids must be published and should have a mechanism to add new ones as required. **Unique list of Issuer IDs MUST BE unique and published via central e-governance codification scheme**.

`DocType` (optional) - is the document type optionally defined by the issuer. This is highly recommended for document classification and versioning purposes. Issuers may decide their own classification mechanism. This is a 5 char pure alpha string which can

be expanced in future as needed.

DocId (mandatory) - is a unique document ID of length up to 10 within the issuer system. It is highly recommended that this is either purely numeric or alpha to avoid confusion with "0" with "o" etc. Also, it is highly recommended to use random strings to avoid guessing the sequence of document IDs.

Document Owner

For avoiding document misuse, it is critical that all documents are "attached" to one or more Aadhaar holders. For example, a cast certificate may be attached to one Aadhaar holder while a marriage certificate is attached to two Aadhaar holders. Proposed DLTS solution offers a mechanism for issuers to secure access via Aadhaar authentication of any of the owners.

Document Format

All e-documents must be represented in XML format complying to DLTS specifications. This ensures that a standardized XML structure is used to capture common attributes of all documents.

All e-documents MUST BE digitally signed by the issuer to ensure documents/certificates are verifiable for authenticity and are unalterable.

It is important to note that issuer specific extensions are allowed to this XML for representation of the actual document data. For example, actual details of a cast certificate will be different from actual details of a driver's license. DLTS allows this to ensure that issuers can choose a domain specific XML for their extensions.

It is also important to note that DLTS solution does not insist on a common printing format allowing issuers to freely choose a print format for their document. Use of logo, colors, etc are freely possible within the print format.

Following is the suggested common XML format for e-document (note that issuer specific extensions are embedded witin DocBody element).

```
<Edoc ver="" xsd="">
   <Meta issuerId="" docType="" docId="" issuedOn="" expiresOn="">
      <Owners>
         <Aadhaar uid="" name=""/>
      </Owners>
      <Print format="" highResUrl="" lowResUrl=""/>
   </Meta>
   <DocBody>
       <!-- any custom issuer specific XML can be embedded here -->
       <!-- Describes other elements and attributes of this particular doc -->
```

```
   </DocBody>
   <Signature/>
<Edoc>
```

E-document Examples

A sample marriage certificate is given below. Note that the DocBody which is specific to marriage certificate format is left to issuer to standardize. While it is a good idea to standardize specific types of document and their formats, issuers must be allowed to change and adapt as they wish to provide flexibility and easy adoption.

```
<Edoc ver=”1.0” xsd=”http://dlts.deity.gov.in/xsd/edoc-1-0.xsd”>
   <Meta issuerId=”KARMR” docType=”MCA” docId=”7385491” issuedOn=”20060326” expiresOn=””>
      <Owners>
         <Aadhaar uid=”234567890123” name=”Kishan Singh”/>
         <Aadhaar uid=”345678901234” name=”Laxmi Agarwal”/>
      </Owners>
      <Print format=”image/jpeg”
url=”/print/bc1f48e586a66eefbdfe96b08700423b21c6c4f93654e5b39f0c1c6e3edb6d17”>
   </Meta>
   <DocBody>
      <Mca ver=”1.0” xsd=”http://dlts.deity.gov.in/xsd/karmr/mca-1-0.xsd”>
         <Marriage date=”20060322” state=”Karnataka” district=”Bangalore” address=”32, 10th
Main, 14th Cross, Bangalore, 560001”>
            <authority name=”Bangalore Marriage Registrar” officer=”Ramesh Pai”
witness=”Bunty Singh”/>
         </Marriage>
      </Mca>
   </DocBody>
   <Signature/>
<Edoc>
```

A sample school leaving certificate is given below. Note that the DocBody of this is very different from the marriage certificate example above.

```
<Edoc ver=”1.0” xsd=”http://dlts.deity.gov.in/xsd/edoc-1-0.xsd”>
   <Meta issuerId=”CBSE” docType=”MSTN” docId=”22636726” issuedOn=”20020514” expiresOn=””>
      <Owners>
         <Aadhaar uid=”345678901234” name=”John Alex K”/>
      </Owners>
      <Print format=”application/pdf” url=”/print/
ef77ea76524929d6b7059a15568ec601e9d409f05a3235e24685435c115097d5”>
   </Meta>
   <DocBody>
      <Mstn ver=”1.0” xsd=”http://dlts.deity.gov.in/xsd/cbse/mstn-1-0.xsd”>
         <Marksheet date=”20020514” school=”Tilak Nagar Public School” class=”10”>
            <Official officer=”Neela Lal” schoolHead=”Teressa Mathew”/>
            <Mark>
               <Subject name=”Science” mark=”92” max=”100” grade=”A+”/>
               <Subject name=”Mathematics” mark=”96” max=”100” grade=”A+”/>
               <Subject name=”English” mark=”91” max=”100” grade=”A+”/>
               <Subject name=”Hindi” mark=”86” max=”100” grade=”A”/>
               <Subject name=”Social Studies” mark=”83” max=”100” grade=”A”/>
            </Mark>
         </Marriage>
      </Mca>
```

```
   </DocBody>
   <Signature/>
<Edoc>
```

Repository & Gateway Specifications

A detailed API and compliance specifications must be prepared before actual start of implementation. At a high level following items need to be covered in that detail specification document:

1. Repository APIs
    a. Document management APIs - addDoc, deleteDoc, updateDoc, readDoc
    b. Meta data APIs – getDocTypes
2. Gateway APIs
    a. Document management – readDoc
    b. Meta data APIs – getIssuers, getDocTypes, addDocType, deleteDocType, updateDocType
3. Compliance
    a. Security – document storage, issuer access control, gateway access control, validations, etc.
    b. Audits – access and document management audits