2019-11-27

Happy US Thanksgiving!

Agenda

- Antitrust Policy and introductions - VB duration-depends on participation
- Talk on FATF Digital Identity Guidance. @Stephane Mouy -10 minutes with 3 for questions
- A talk by Nitin Agarwal on India stack: digital lockers & consent layer (expect a Q&A)
- Sovrin Foundation Guardianship white paper published: https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper.pdf
- Future talks (we are working with some of these folks on nailing down dates)
  - A talk by Kim Cameron .
  - DLT/SSI integration (Ajay Jadhav)
  - ID2020: What happened and why is it important Vipin Bharathan
  - A Talk by Darrell O'Donnell on Digital Wallets - Will happen on December 11. No call on December 25
- Ongoing:
  - Identity WG Implementer call - report -
    - Meeting Notes 2019-11-21+Identity+WG+Implementers+Call Daniel Bluhmor Richard Esplin or anyone who was on the call
  - A GitHub repo was created under Hyperledger for IDWG; Details to follow.
  - Discuss IDWG paper
    - Aadhaar section-look at reworked areas - Nitin Agarwal/Kaliya Young
  - Kiva - current status. After the UNGA- any one from Kiva (Matt Raffel or Cam Parra)
  - Implementing metrics from Chaoss... DCIWG- let us discuss.

Zoom Call:

https://zoom.us/my/hyperledger.community

Attendees

- Vipin Bharathan- dlt.nyc - Independent
- Stephane Mouy Independent
- Nitin Agarwal Gio
- Kelly Cooper Educator-independent
- Amit (AyanWorks)
- Gary de Beer
- Kaliya Identity Woman
- Kalyan Kulkarni(AyanWorks)
- Kamlesh Nagware (Snapper)
- Michelle Benham
- Ravikant Agrawal
- Sze Wong
- Todd Gehrke
- Rohit (AyanWorks)
- Swapnali (AyanWorks)
- Lasse (DeutscheBorse)
- Roland - specialist in Air freight
- Drummond Reed - Sovrin
- Dan Bachenheimer- Accenture
- Ankita (AyanWorks)
- Leonard Edwin
- LucaBoldrin - Infocert
- Todd Gehrke - Luxoft

Recordings

Audio

Video

FATF Areas of focus - Please provide feedback.

1. **Are there any specific money laundering / terrorist financing risks, that arise from the use of digital identity systems for CDD, other than those already mentioned in Section IV of the guidance?**
   If so, how can they be addressed and by whom? Are there specific opportunities for combating money laundering / terrorist financing that are not already mentioned in the guidance?

2. **What is the role of digital ID systems in ongoing due diligence or transaction monitoring?**
   a. What information do you capture under authentication at onboarding and during authorization for account access? Who captures this data?
   b. Is the authentication data you capture relevant to ongoing anti-money laundering and counter-terrorist financing due diligence and/or transaction monitoring? If yes, how?

3. **How can digital ID systems support financial inclusion?**
   a. How can digital ID systems with different assurance levels for identity proofing/enrollment and/or authentication be used to implement tiered CDD, allowing clients a range of account functionalities depending on the extent of CDD performed, and particularly in situations of lower risk? Please provide any practical examples.
   b. Have you adopted lower assurance levels for identity proofing to support financial inclusion? What additional measures do you apply to mitigate risks? Please provide any practical examples.
   c. How can progressive CDD via digital ID systems aid financial inclusion (i.e. establishing greater confidence in a customer's identity over time)?

4. **Does the use of digital ID systems for CDD raise distinct issues for implementing the FATF record-keeping requirements?**
   a. What records do you keep when you use digital ID systems for CDD?
   b. What are the challenges in meeting record-keeping requirements when you use digital ID systems for CDD?
   c. If you keep different records when using digital ID systems for onboarding, does this impact other anti-money laundering and counter-terrorist financing measures (for example ongoing due diligence or transaction monitoring)?

Minutes

Introductions

Presentation StMouy (Stefan): Public consultation on FATF draft guidance on digital identity. After months of preparation FATF released guidance in digital identity. Important because it is the first time there is a concerted effort to discuss digital identity – financial regulations. No time left for comment (as of Friday) Areas of focus - where feedback is requested – typically deals with how – a good way to stimulate financial inclusion with digital identity. Proofing is difficult, in emerging and other countries. FATF looking at ways to lower requirements for identity proofing. Balance with higher requirements for authentication. Some of the questions raised by FATF relate to what sort of risks are involved, how to mitigate risks, and whether there is any tradeoff with authentication and collection monitoring processes.

Recommend taking a look, more refined compared to previous versions. A fairly broad overview of the current situation in many countries. If you are not familiar with the level of issues related to AML and prevention, digital identity solution operations, a good way to look at the document. Also, the document includes the decision process for regulated entities. Highlights deal with this most critical part of the report. Set up as a series of three questions. Is there a digital ID system that has been authorized in the banking or financial sector? Yes, then use. No? then do you know the assurance level of the digital ID system, you come to the third question, is that level of assurance appropriate for the level of risk associated? Something reflected in IST guidelines and Europe regulations. If there is no established level of assurance, you can't use the ID system; there is a fairly onerous requirement – effectively any digital ID system contemplating use by financial institutions in the financial sector, will one way or another obtain a level of assurance. Still, a lot of flexibility and room to maneuver. However, this is the core thinking and decision process behind the use of digital IDs.

Kaliya question - Does the document understand the emerging decentralized identity technologies as a way that identity proofing can happen OR is it entirely oriented to be pre-disposed to Phone Home central ID systems?

Meant to be technology-neutral. The document does not advocate one particular ID solution compared to another or one level of assurance or another – even for standard banking collection. Is it consistent or usable with SSI? In principle, the answer is yes. But, of course, that means the solution will have to be LOA rated. That is probably where the difficulty starts.

Vipin - Since most regulatory agencies, like SEC, operate on a technology-neutral basis. Rule-based – need a way of proving LOA.

Dan Bachenheimer - For the highest level of assurance, in-person proofing is required. IAL3 physical presence (disagreement in the group).

Group - Not true as a statement. You can have high LOA identity proofing on a remote basis with biometric solutions. Not US government. That's what everyone's working on. The high cost of proofing and how to get rid of it. Not costly, solutions exist. KDTI - reusing. I was proofed by my government and use as a thrive credential. If I'm not known by the entity. Physical presence required. No universal. In the US. Different interpretations.

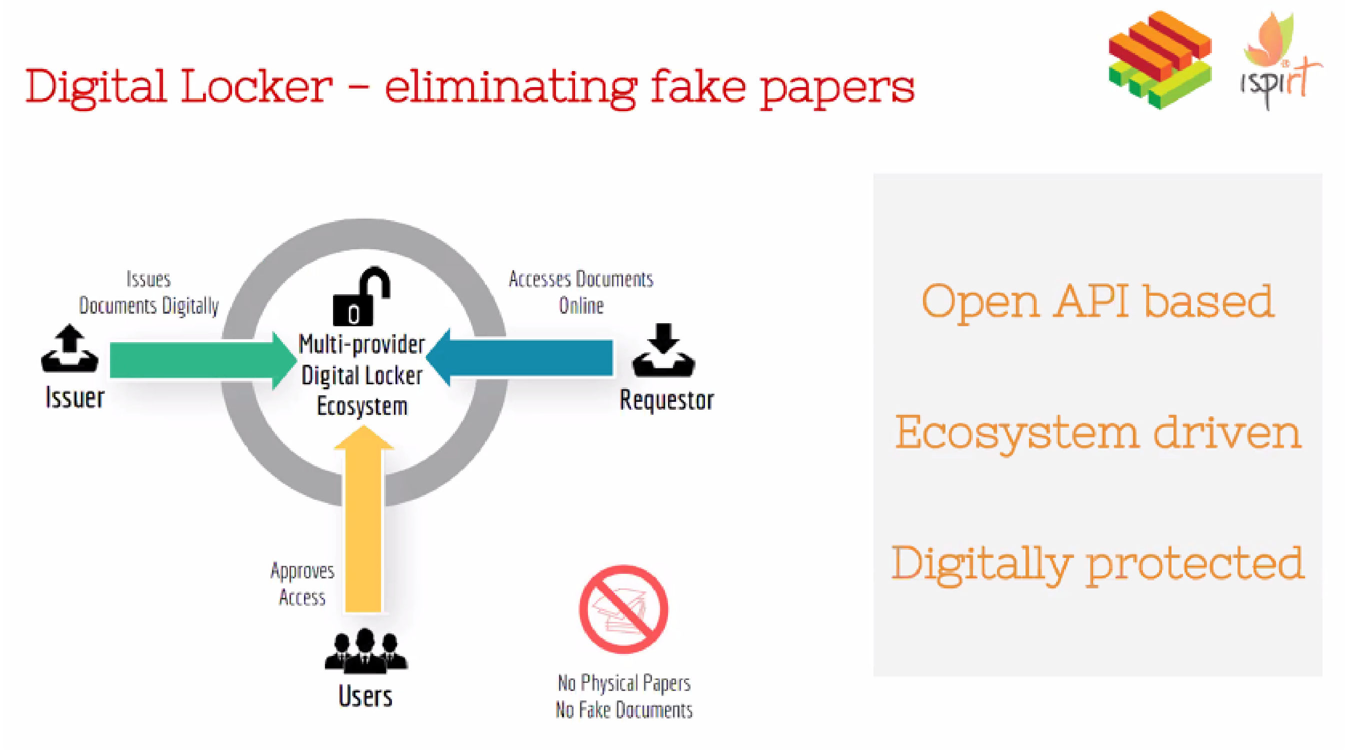
'appropriate for use in customer due diligence' but they don't define measurement.

AML risk-based approached = each financial institution has to look at the customer relationship and assess what risk is involved. What is the level of assurance needed? A retired person with a stable pension is a different risk than a traveler. Also, transaction - a pizza versus high-value transactions. There are a number of factors.

More issues – multiple data points, various ways of looking at the problem.

Nipin – India stack and biometrics. A lot of pushback on biometrics in the US. Digital lockers.

Digital Locker Overview IDentity piece provided by Aadhaar. It started in Maharashtra state, evolved and stayed in India. Open-API ecosystem



Digital Locker – eliminating fake papers

Issues Documents Digitally

Issuer

Multi-provider Digital Locker Ecosystem

Accesses Documents Online

Requestor

Approves Access

Users

No Physical Papers
No Fake Documents

Open API based

Ecosystem driven

Digitally protected

Guidelines on what kinds of electronic documents. Needs to be unique document ID for the publisher. Must go through a partnership agreement authority. The requestor is an entity providing service to a citizen or any entity requiring documents (such as a bank). As requestor, you can access digital locker, you will have access. Apart from that, digital locker service providers. Typically unique URI for documents. It can be owned by issuers or private players who store documents. Issuer maintains own secure storage model available. Simple, only one copy, what flows is the URI. One is the issued document for which the URI is stored in the digital locker. Centralized repository with a document. A lot of legacy documents users already have. Digital lockers can provide service to upload legacy and get 'signed' with a signing service, to share documents. Sign and upload, or from a certain date onward, issuer can issue electronic documents and publish a URI. If we talk about the India stack ecosystem. We are talking about multiple transformations.

Quick explanation on layers on video approximately minute 35.

Sign up, start with mobile, create an account, verify. When you sign in again, use the username password or identifier. Username always linked to Aadhaar. Access documents issued by government organizations. Linking Aadhaar is always recommended.

Question? Digital Locker issues documents on request, do they do that or confirm attributes? Once documents are released they could be tampered with?

Response = issuer issues document. For example, an electronic driver's license. Digital wallet interface, you see the document signed by the transfer document, it is digitally signed by the issuer. If you see the interface it says three issued document, when I click on the URI. URI is transferred, not URI.

Question? Is there a selective disclosure? Is there a revocation? We understand this is a centralized model to a certain extent.

Response = the interface is centralized. The Digital Wallet never contains the document, only the URI. Once the document is requested from the issuer, it can check authentication. The document itself resides in repositories that can be controlled by owner or in a shared repository. The only thing compromised are the URIs.

Question? When I use that document in any context, does the issuing authority know?

Response = no. The only Digital Locker interface that you own has that list. Owners can see activity.

Question? If what you're sharing from the locker is the URI, they are requesting a document from the initial document. The initial issuer would know where you share the document.

Response = Example, submit the document to the passport office. Integrate into solution. Technically, every time I request a document, the issuer has no way to know of the requested document.

Question? Audit trail of a number of requests; not where the request came from?

Who is able to view the log?

Response = Activity log - the owner of a digital wallet. If there is a provider, operations team. Digital Locker Authority - regulatory government entity. Any entity who wants to be a Digital Locker Authority abides by rules of privacy (right now only government).

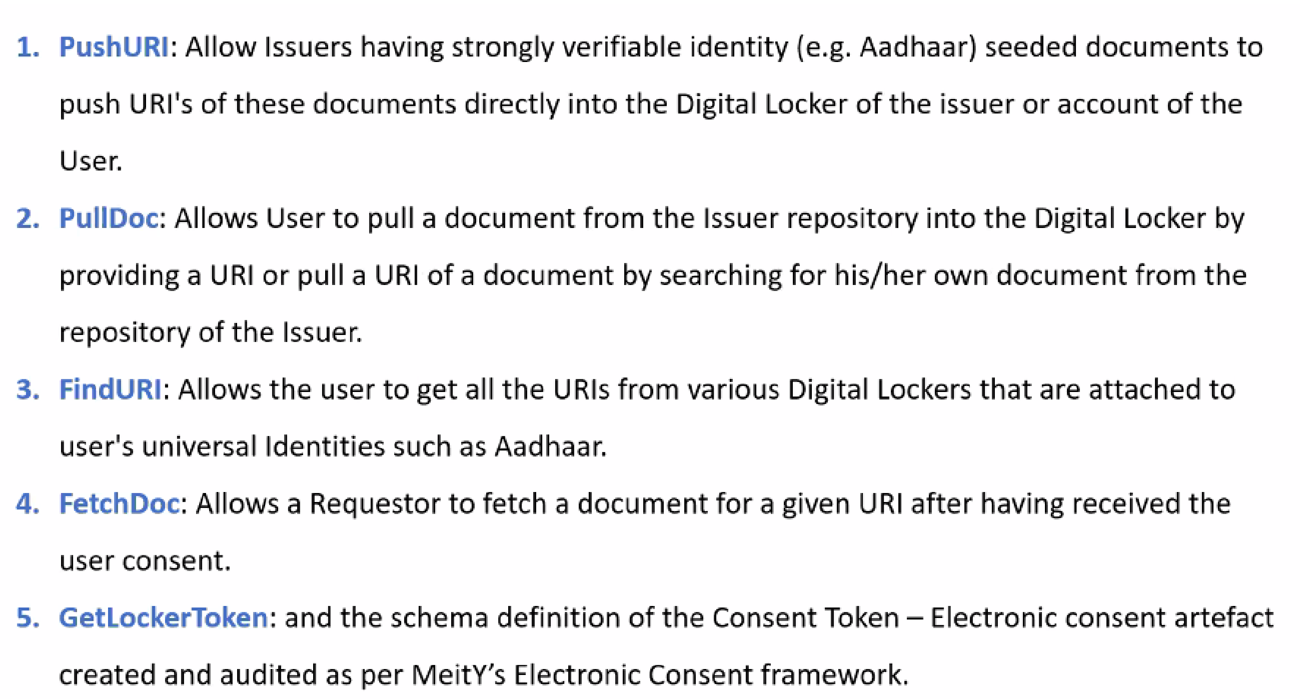
Question? Can documents be subpoena? Has not happened yet, maybe in the future.

Question? Is it, for example, a pdf of driver's license or set of attributes?

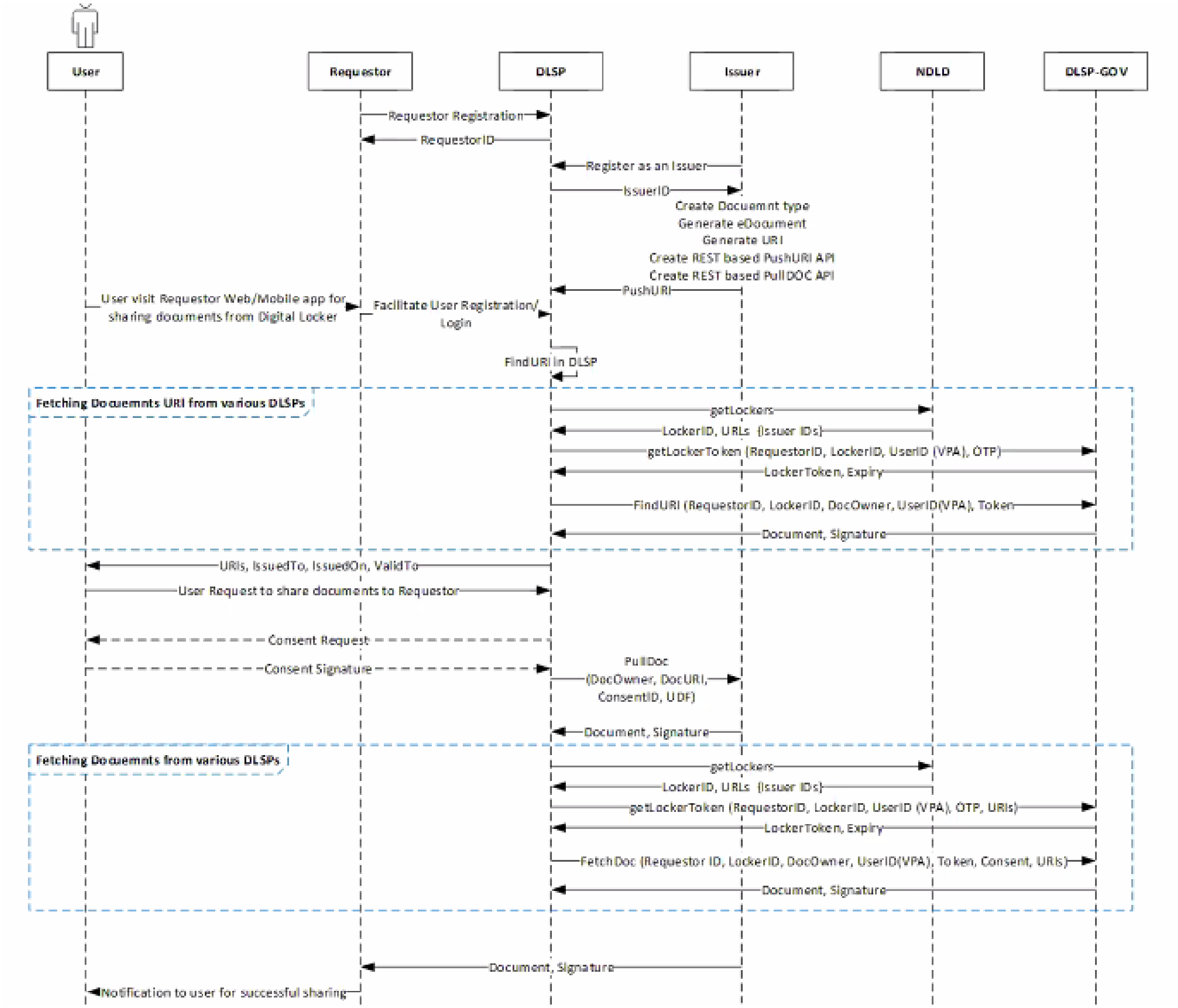
Response = Appears as PDF, proposed XML or JSON. Most, as of now, are in PDF form so can be downloaded and shared with requestors? Signed PDF, according to ISO standard? Not sure on standard is a signed PDF with a valid signature.

Architecture is distributed. Multiple issuers. Multiple service providers. Own, outsource, etc. No single point where you collect and keep data. No central data storage. Strong recommendation Aadhaar strongly recommended. Because of authentication process assurance.

APIs – first meta APIs. List of all issuers registered with the regulator. Issue providers. Certain document types. Get document lookup attributes. To search documents if not linked with Aadhaar number.



1. **PushURI**: Allow Issuers having strongly verifiable identity (e.g. Aadhaar) seeded documents to push URI's of these documents directly into the Digital Locker of the issuer or account of the User.
2. **PullDoc**: Allows User to pull a document from the Issuer repository into the Digital Locker by providing a URI or pull a URI of a document by searching for his/her own document from the repository of the Issuer.
3. **FindURI**: Allows the user to get all the URIs from various Digital Lockers that are attached to user's universal Identities such as Aadhaar.
4. **FetchDoc**: Allows a Requestor to fetch a document for a given URI after having received the user consent.
5. **GetLockerToken**: and the schema definition of the Consent Token – Electronic consent artefact created and audited as per MeitY's Electronic Consent framework.


User
Requestor
DLSP
Issuer
NDLD
DLSP-GOV
Requestor Registration
RequestorID
Register as an Issuer
IssuerID
Create Docuemnt type
Generate eDocument
Generate URI
Create REST based PushURI API
Create REST based PullDOC API
PushURI
User visit Requestor Web/Mobile app for sharing documents from Digital Locker
Facilitate User Registration/ Login
FindURI in DLSP
Fetching Docuemnts URI from various DLSPs
getLockers
LockerID, URLs (Issuer IDs)
getLockerToken (RequestorID, LockerID, UserID (VPA), OTP)
LockerToken, Expiry
FindURI (RequestorID, LockerID, DocOwner, UserID(VPA), Token
Document, Signature
URIs, IssuedTo, IssuedOn, ValidTo
User Request to share documents to Requestor
Consent Request
Consent Signature
PullDoc (DocOwner, DocURI, ConsentID, UDF)
Document, Signature
Fetching Docuemnts from various DLSPs
getLockers
LockerID, URLs (Issuer IDs)
getLockerToken (RequestorID, LockerID, UserID (VPA), OTP, URIs)
LockerToken, Expiry
FetchDoc (Requestor ID, LockerID, DocOwner, UserID(VPA), Token, Consent, URIs)
Document, Signature
Document, Signature
Notification to user for successful sharing

This is a working system. What about the integration – DLSP is more like a wallet? Plus it's more like a traffic policeman that manages the integration of requests and issues. Does document flow through DLSP, central piece to user URI? The virtual piece, but a centralizing group of registries, repositories? Yes.

Challenges/shortcomings debate in the coming weeks.

References:

http://dla.gov.in/ https://digilocker.gov.in/

http://dla.gov.in/sites/default/files/pdf/

DigitalLockerTechnologyFramework%20v1.1.pdf

http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf