Suggestions for the baseline technology standards for DLAs

March 2023

Contents

Abbreviations

BIA: Business Impact Analysis
CI/CD: Continuous integration and continuous deployment
DLA: Digital Lending App
DLG: Digital Lending Guidelines
DR: Disaster Recovery
FACE: Fintech Association for Consumer Empowerment
LSP: Loan Service Provider
IP: Internet Protocol
PII: Personal Identifiable Information
RBI: Reserve Bank of India
RPO: Recovery Point Objective
RTO: Recovery Time Objective
SDLC: Software Development Life Cycle
SSL: Secure Socket Layer
TLS: Transport Layer Security
VAPT: Vulnerability Assessment and Penetration Testing

Context

1. Digital Lending Apps (DLAs) are critical technical infrastructure in digital lending, allowing an interface between customers and lenders at various stages of the loan cycle, including before and beyond the loan term. While some standards are emerging around disclosure, policy, consent, privacy/security and permission from RBI Digital Lending Guidelines (DLG) and App Store[1] requirements, there are no technical standards, mandatory or voluntary for the DLAs may follow.

2. RBI Press Release on Digital Lending Working Group Implementation Annexure II articulates that RBI to lay down baseline technology standards for DLAs which will include:

    - Secure application logic i.e. technical specifications of the DLA to ensure security of applications running on mobile phones, proper authentication, input validation, clear access rules, measures to ensure protection of sensitive data, etc.
    - Keeping auditable log of every action that user performs along with their IP address and device information
    - Monitoring of transactions being undertaken through DLA
    - Multi-step approval for critical activities undertaken on the DLA
    - DLAs should mandatorily reflect these standards in the terms of service. Further it should be ensured that apps have specific technological safeguards to prevent frauds like sanction of loans on stolen identity, data breaches, etc.

3. In this document, we aim to contribute to the regulatory efforts on the DLA baseline technology standards. A FACE Working Group (WG) consisting of CTOs of a few member companies has developed the document. WG also took feedback from the FACE members and a few other stakeholders with domain expertise.

4. For FACE members, this document should serve as base-level implementation guidance.

5. DLAs must also follow all the relevant regulatory standards, including disclosures, data handling, consent architecture, governance and reporting from DLG[2] and other Information Technology (IT) frameworks.

[1] https://support.google.com/googleplay/android-developer/answer/9876821?hl=en
[2] Applicable clauses from DLG with respect to DLAs are captured in section 'Relevant clauses from DLG'

Technology Standards for DLAs

Mobile/Web app security

1. Data transfer between DLA and backend server must happen via Secure Socket Layer (SSL/TLS).
2. Additionally, if not all, at least the data related to transactions like loan booking, banking data, payments etc., Personal Identifiable Information (PII) and authentication data like mPIN, passwords etc. must be encrypted using standard encryption algorithms.
3. Rooted device checks to ensure the DLA alerts users if the device is rooted and blocks users from moving forward. DLA shouldn't work on embedded devices.
4. DLA must undergo comprehensive Vulnerability Assessment / Penetration (VAPT) testing every six months or after any significant releases, whichever is earlier.
5. Internal and external network vulnerability assessments should be conducted every six months.
6. DLA must also incorporate continuous code monitoring tools in the SDLC process, such as SNYK, etc., to catch vulnerabilities early.
7. DLA should perform the code review for all the releases to ensure that newly incorporated code does not pose any new risk for the overall app.
8. DLA must disallow simultaneous sessions.
9. DLA must store the logs of user activity for at least one year and capture IP addresses during all critical stages of the user journey.
10. DLA must enforce basic hardening like password policy, session expiry, debugging disabled etc.
11. DLA must not store sensitive data in unencrypted format on the customer's mobile device.
12. DLA' must request customers' mobile phone access permission in line with the DLG.
13. DLA must not access or use any media on the device beyond what is needed for KYC and underwriting/creditworthiness in line with DLG.
14. DLA's are recommended to use server-side input validation to minimise the probability of cyber-attacks like SQL Injection, cross-site scripting etc.
15. DLA's are recommended to use certificate pinning to reduce the probability of a MitM (Man in the middle) attack.
16. DLA's are recommended to take Anti-Rouge App service to identify any app trying to impersonate DLA actively.
17. DLA should perform the app integrity check on run time to detect unauthorised modifications in the app. If such a modification is detected, the server must terminate the connection.
18. DLA are recommended to implement an OTP validity of 120 seconds to reduce the chances of fraud caused by OTP sharing.
19. DLA shouldn't be allowed to access the user contact list and other data as prescribed in DLG.

Secure design principles

1. **DLAs should implement a strong identity foundation:** Implement the principle of least privilege and enforce separation of duties with the appropriate authorization for each interaction with system resources. Centralised identity management and aim to eliminate reliance on long-term static credentials.
2. **Enable traceability**: Monitor, alert, and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.
3. **Apply security at all layers**: Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of the network, VPC, load balancing, every instance and compute service, operating system, application, and code).
4. **Automate security best practices:** Automated software-based security mechanisms improve your ability to scale more rapidly and cost-effectively securely. Create secure architectures, including implementing controls that are defined and managed as code in version-controlled templates.
5. **Protect data in transit and at rest:** Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenisation, and access control, where appropriate.
6. **Keep people away from data:** Use mechanisms and tools to reduce or eliminate the need for direct access or manual data processing. This reduces the risk of mishandling or modification and human error when handling sensitive data.

Data security

1. DLA should have data access control on the role-based framework with proper authorisation and authentication.
2. All sensitive information must be stored in encrypted form on disk.
3. In transit, data transfer must happen via a secure socket layer (SSL/TLS), and sensitive data should be encrypted.
4. PII Data must be stored in encrypted format in Database and ensure that the backup copy is also encrypted.
5. DLA must use tools to actively monitor the database activities to identify any unauthorised modification in the database.
6. DLA app must store personal and transactional data of the customers in India only as per regulatory directions.
7. DLA must have a process to take back-up of all the data regularly, restoration testing must be performed to verify that the backup is not corrupt and can be restored if restored.
8. DLAs are recommended to demonstrate reasonable point-in-time restore capabilities to prevent catastrophic effects of a compromise.
9. DLA must follow the retention policy and purging procedures as per the DLG, which must be prominently disclosed to customers.

Fraud

1. DLA should have device fingerprinting (i.e. unique identification of digital devices) to identify devices involved in fraud and use this information to discourage fraudsters from attempting fraud from the same machine.
2. DLA should have access to the device's unique identifier, like IMEI number or something equivalent. So that any device used in fraud can be tagged uniformly.
3. RE or LSP owing the DLA should come together to create an Industry Fraud Exchange[3] to report, store and share identified frauds, including device and use information, and the nature of frauds on a real-time basis under the standard protocol.

Business continuity

1. DLA should create a business continuity policy to minimise any loss.
2. DLA should perform Business Impact Analysis (BIA) to identify critical processes, systems, and partners and create redundancy for such assets.
3. DLA must have a Disaster Recovery (DR) site and plan and test it annually.
4. DLA architecture should not have a single point of failure.
5. DLA should ideally implement Infrastructure as code solutions so that provisioning the entire infrastructure in case of DR or otherwise is seamless & automated to mitigate risk.
6. DLA owners should identify and define RTO (Recovery Time Objective) and RPO (Recovery Point Objective) and prepare recovery plans accordingly.

Processes

1. DLA must follow standard SDLC guidelines in building and managing their technology platform.
2. DLA must follow the well-defined incident management process and follow it.
3. DLA's are recommended to CICD Pipelines, especially around production deployments, should have minimal human touch points and should be automated as these environments have PII data.
4. DLA must have change-management and release management policies to control the production environment changes.
5. DLA must avoid using free/open-source libraries in its code, if they use them, then such libraries must be tested thoroughly by a security expert.

[3] FACE is piloting to build Fraud Exchange in partnership with Equifax with a few members, but its value comes only if lenders actively participate in the system.

Relevant clauses from DLG

1. Digital Lending Apps/Platforms (DLAs) is mobile and web-based applications with user interface that facilitate digital lending services. DLAs will include apps of the Regulated Entities (REs) as well as those operated by Lending Service Providers (LSPs) engaged by REs for extending any credit facilitation services in conformity with extant outsourcing guidelines issued by the Reserve Bank.

2. REs shall ensure that digitally signed documents[3] (on the letter head of the RE) viz., KFS, summary of loan product, sanction letter, terms and conditions, account statements, privacy policies of the LSPs/DLAs with respect to borrowers data, etc. shall automatically flow to the borrowers on their registered and verified email/ SMS upon execution of the loan contract/ transactions.

3. REs shall prominently publish the list of their DLAs, LSPs engaged by them and DLAs of such LSPs with the details of the activities for which they have been engaged, on their website.

4. REs shall ensure that their DLAs or DLAs of their LSPs at on-boarding/sign-up stage, prominently display information relating to the product features, loan limit and cost, *etc.*, so as to make the borrowers aware of these aspects.

5. REs shall ensure that DLAs of REs and LSPs have links to REs' website where further/ detailed information about the loan products, the lender, the LSP, particulars of customer care, link to Sachet Portal, privacy policies, *etc.* can be accessed by the borrowers. It shall be ensured that all such details are available at a prominent single place on the website for ease of accessibility.

6. REs shall ensure that they and the LSPs engaged by them shall have a suitable nodal grievance redressal officer to deal with FinTech/ digital lending related complaints/ issues raised by the borrowers. Such grievance redressal officer shall also deal with complaints against their respective DLAs. Contact details of grievance redressal officers shall be prominently displayed on the websites of the RE, its LSPs and on DLAs and also in the KFS provided to the borrower. Further, the facility of lodging complaint shall also be made available on the DLA and on the website as stated above.

7. REs shall ensure that any collection of data by their DLAs and DLAs of their LSPs is need-based and with prior and explicit consent of the borrower having audit trail. In any case, REs shall also ensure that DLAs desist from accessing mobile phone resources like file and media, contact list, call logs, telephony functions, *etc.* A one-time access can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/ KYC requirements only, with the explicit consent of the borrower.

8. The borrower shall be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the app delete/ forget the data.

9. The purpose of obtaining borrowers' consent needs to be disclosed at each stage of interface with the borrowers.

10. Explicit consent of the borrower shall be taken before sharing personal information with any third party, except for cases where such sharing is required as per statutory or regulatory requirement.

11. REs shall ensure that LSPs/DLAs engaged by them do not store personal information of borrowers except some basic minimal data (*viz.,* name, address, contact details of the customer, *etc*.) that may be required to carry out their operations. Responsibility regarding data privacy and security of the customer's personal information will be that of the RE.

12. REs shall ensure that clear policy guidelines regarding the storage of customer data including the type of data that can be stored, the length of time for which data can be stored, restrictions on the use of data, data destruction protocol, standards for handling security breach, *etc*., are put in place and also disclosed by DLAs of the REs and of the LSP engaged by the RE prominently on their website and the apps at all times.

13. REs shall ensure that no biometric data is stored/ collected in the systems associated with the DLA of REs/ their LSPs, unless allowed under extant statutory guidelines.

14. REs shall ensure that all data is stored only in servers located within India, while ensuring compliance with statutory obligations/ regulatory instructions.

15. REs shall ensure that their DLAs and LSPs engaged by them have a comprehensive privacy policy compliant with applicable laws, associated regulations and RBI guidelines. For access and collection of personal information of borrowers, DLAs of REs/LSPs should make the comprehensive privacy policy available publicly.

16. Details of third parties (where applicable) allowed to collect personal information through the DLA shall also be disclosed in the privacy policy.

Resources

1. RBI Cyber Security Framework in Banks
2. RBI Master Direction - Information Technology Framework for the NBFC Sector
3. Draft Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices
4. RBI Digital Lending Guidelines
5. AWS Well-Architected Framework on identity and access management using String Sign-in and Leverage user groups and attributes, data protection, reliability pillar specifically failure management, backup of data and planning for BCP-DR
6. Mobile Application Security Assessment
7. PCI Security Standards
8. Cert-in
9. ISO 270001 Standards for Information Security