# Electronic Consent Framework

**Technology Specifications, Version 1.1**

# 1. Overview

With the advent of Digital India there has been an impetus towards enabling digital service delivery of both government and private services to citizens. Aadhaar based Authentication, eKYC[1], and eSign[2] have enabled the service providers to onboard customers in a seamless manner. Digital Locker offers a standardized mechanism to issue government documents to individuals and entities in electronic and printable formats, store them, and make them shareable with various agencies. All these systems require a mechanism for obtaining and preserving user consent to operate effectively and securely.

Guiding principles for the sharing of user data across different services with user consent have been previously outlined in two key policy documents: namely, the "Policy on Open Application Programming Interfaces (APIs) for the Government of India"[3] published by the Ministry of Electronics and Information Technology (MeitY), and the "National Data Sharing and Accessibility Policy (NDSAP) - 2012"[4] by the Department of Science & Technology. The IT Act[5] also requires that any entity sharing user data that is sensitive in nature must collect consent from the user prior to such sharing.

There is a requirement for a comprehensive technology framework to enable effective and secure implementation of the aforementioned policies with respect to user consent management. The technology framework outlined in this document is designed to be open, secure, user-centric, and application-agnostic. Using this framework, data consumers (like Govt departments, employers, lenders, etc.) can access data of users from providers (like Govt departments, banks, etc.) using electronic consent, rather than requiring users to share credentials like passwords or to sign paper documents.

**In the rest of the document, the term "Data" is used to depict any electronic data and/or document and the term "user" is used to depict either a person or an entity whose data is being shared/accessed.**

# 2. Need for Electronic Consent

In the last 6 years, more than 110 crore Aadhaar numbers have been issued, smartphone count has risen from 2 crore to over 20 crore, and more than 24 crore new bank accounts have been opened under the Pradhan Mantri Jan Dhan Yojana. This foundation is collectively referred to as the "Jan Dhan-Aadhaar-Mobile" or "JAM" trinity and is propelling India from a data-poor to a data-rich economy. Collecting and

[1] https://uidai.gov.in/
[2] http://cca.gov.in/esign
[3] http://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf
[4] http://ogpl.gov.in/NDSAP/NDSAP-30Jan2012.pdf
[5] http://www.cca.gov.in/cca/?q=it_act.html

sharing user data in digital form is a key requirement for ensuring that the interaction between a user and the service provider can be consummated seamlessly in a paperless, fully electronic, and high trust way.

Efforts to share digital data about users must overcome the challenge of easy access across various systems in a secure and traceable manner. It is imperative that all user data sharing is fully consented to, in electronic form, by the user(s) whose data is shared. Collecting, managing, auditing and tracing paper based consents is costly, inefficient, and also risky. In the current world, some service providers seeking user data from trusted sources are implementing unsafe data sharing practices like collecting user passwords and using these passwords to obtain such data.

Within the financial domain, a legal framework was put forth by the RBI's notification titled "Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016"[6] for financial data sharing. This notification clearly articulates the need for a consent framework to enable data sharing. An interoperable technology framework is still needed to implement such frameworks in practice.

Thus it is necessary to create a technology framework for electronic consent. This document proposes a technical framework for electronic consents to allow data providers and users to enable data sharing only if both parties consent electronically in a secure and reliable manner.

# 3. Definitions

3.1. **Data —** Any electronic information that is held by a public or private service provider (like a government service department, a bank, a document repository, etc). This may include both static documents and transactional documents.

3.2. **User —** any person or entity who wishes to share data about them for availing a service.

3.3. **Data Provider (DP) —** Any entity which has data about users in their system that can either be given to the user (whose data it is) or to another entity based on the consented request of the user.

3.4. **Data Consumer (DC) —** Any entity which accesses data for providing a service to the user.

3.5. **Consent Collector (CC) —** An entity that interacts with users and obtains consent from them for any intended access to data. This role may be played by the Data Consumer (in most cases) or the Data Provider or could be another service provider.

[6] https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

# 4. Guiding design principles

4.1. **User Centricity:** Users should be at the center of any data sharing and should be given adequate control and decision-making power on how data associated with them is shared.

4.2. **Trustable and IT Act Compliant:** Use digital signatures to guarantee integrity of access permissions given by users in consent flows. This avoids security issues faced by existing approaches and also makes the framework fully legal under the IT Act.

4.3. **Universal Identity:** The technical framework should leverage universal, authenticable, non-repudiable, and digital identities to allow interoperability across service providers.

4.4. **Granular Control:** The framework should allow users to set permissions and rights for data access at a granular level.

4.5. **Open Standards Based:** The framework should use open technology and legal standards available in the country. It should be agnostic to applications, programming languages, and platforms.

# 5. Electronic Consent

Electronic consent is the digital equivalent of a physical letter of permission given by the user which, when presented, allows the data provider to share information regarding the user with a data consumer, for a particular purpose. Just as Aadhaar e-KYC, eSign, and Digital Locker provides digital equivalents of the corresponding physical paper based process, electronic consent allows for data to be electronically and securely shared with service providers on an as-needed basis, while maintaining traceability to ensure that the data trails can be audited in the future.

## 5.1. Consent Artifact

A consent artifact is a machine-readable electronic document that specifies the parameters and scope of data share that a user consents to in any data sharing transaction. In this framework, consent must be digitally signed, either by the user (using the services of a signature service provider) or by the consent collector or both. Thus, it is essential that a digital signature be included in every consent artifact that is then used to facilitate data sharing.

The consent collector must ensure the scope of data sharing and purpose is clearly provided to the user. Once the user agrees to the scope of sharing, he/she may be requested to sign the consent digitally, in which case the resulting artifact would contain the user's digital signature. The consent collector may also obtain data sharing authorization from the user differently (e.g., by having the user click a button or by signing a paper form). In such situations, the consent artifact that is generated would

contain the consent collector's digital signature. Subsequently, the data provider may provide the requested data to the data consumer, after validating the consent artifact, which involves verifying the embedded signature.

Following sections provide the high level structure of the consent artifact:

- ***Identifier* Section:** Specifies all the entities that are involved in the transaction: the data provider holding the data, the data consumer accessing the data, the consent collector, and the user. To identify the user, a User element provided by an identity service provider is used. Additionally, account IDs assigned by the players within the ecosystem can be used. Account IDs enable distinguishing multiple accounts of the same user with the same service provider; these may not be included in case the user ID is sufficient for account disambiguation.

- ***Data* Section:** Second section is comprised of fields describing the type of data that is being accessed and the access permissions associated with each of them. This section also describes the specific data that is shared, date range for which data is requested, duration of storage by data consumer, frequency of access, along with a set of attribute filters that can be used to further subset data. Data access permissions can be of three types: the data consumer can either get VIEW access to the data, which implies that the consumer is not allowed to store the data or reuse it later. Or they could get a COPY of the data which they can store and use within the period defined in datalife. In advanced mode, using a secure container, data consumer could get a data packet that cannot be read as-is, but, only be queried. **All data must be exchanged between the provider and the consumer in a secure fashion using either data and/or channel encryption**.

- ***Purpose* of data access:** This may include information about the application domain (e.g., finance) and the application within that domain that is enabled through the data access (e.g., loan offer computation) and a free-form textual description. A more detailed ontology for purpose descriptions may be created for various domains that can be included in future versions of this document.

- ***Logging* of consent and data flows:** The consent artifact includes identifiers for entities which collect and store logs. Logging could be done by the consent collector or by other entities e.g., logs could be sent to the users' own email addresses, if the user desires so. Data providers and data consumers could also independently maintain logs (without explicit mention in the consent artifact) for auditing and analytics purposes.

- ***Signature*:** Finally, each consent artifact contains a digital signature. The signature is included in a signature block which also includes information like the signature service provider's ID, the signature creation timestamp and the user certificate required for verifying the signature.

*Exhibit 1: Consent Artifact XML*

```
<Consent xmlns="http://meity.gov.in" timestamp="YYYY-MM-DDThh:mm:ssZn.n">
    <Def id="" expiry="" revocable="" />
    <!-- Identifiers -->
    <Collector type="URI" value="" />
    <DataConsumer type="URI" value="" >
        <Notify event="REVOKE" type="URI" value="" />
    </DataConsumer>
    <DataProvider type="URI" value="" >
        <Notify event="REVOKE" type="URI" value="" />
    </DataProvider>
    <User type="AADHAAR|MOBILE|PAN|PASSPORT|..." value="" name="" issuer="" >
       <!-- User's account IDs at DP/DC/CM; required to disambiguate-->
       <Account dpID="" dcID="" cmID="" />
    </User>
    <!-- Revoker details should be specified if consent is revocable -->
    <Revoker type="URI" value="" />
    <!-- Logging; logTo can be any valid URI including an email address -->
    <ConsentUse logTo="" type="URI" />
    <DataAccess logTo="" type="URI" />
    <Data-Items>
        <!-- following element repeats -->
        <Data id="" type="TRANSACTIONAL|PROFILE|DOCUMENT">
            <Access mode="VIEW|STORE|QUERY" />
            <!-- how long can consumer is allowed to store data -->
            <Datalife unit="MONTH|YEAR|DATE|INF" value="" />
            <!-- frequency and number of repeats for access repeats -->
            <Frequency unit="DAILY|MONTHLY|YEARLY" value="" repeats="" />
            <Data-filter>
                <-- Data access filter, any encoded query string
                    as per data provider API needs -->
            </Data-filter>
        </Data>
    </Data-Items>
    <!-- Purpose attributes -->
    <Purpose code="" defUri="" refUri="">
          <!-- purpose text goes here -->
    </Purpose>

    <!-- (OPTIONAL) User Signature block -->
    <Signature />
    <!-- Consent collector Signature block -->
    <Signature />

</Consent>
```

# 6. Overview of consent and data flows

Consent capture and use process is comprised of two flows: *consent flow* wherein consent is created and the consent parameters are shared with the relevant entities; and a data flow, where the actual data access, based on user consent, happens. In the data flow, the consent artifact is utilized to enable the data consumer to access the data held by the data provider.

In ***consent flow***, where the user grants permission for a certain kind of data access between a data consumer and a data provider. The consent flow must necessarily involve an interaction between the consent collector, and the user, at the end of which a consent artifact — an electronic representation of the consent given by the user — is generated and shared by the consent collector with either the data consumer or the data provider, depending upon who initiates the data share.

This consent artifact is used in the second flow, the ***data flow***, for the actual data share to happen, sometimes repeatedly. In the case of data shares initiated by the data consumer, the data provider must verify the signature in the consent artifact before granting access to data. In the case of data shares initiated by the data provider, the data consumer must verify the signature before accepting data. The consent and data flows operate asynchronously in an API-driven manner, which ensures efficiency and resilience. Events at various stages of the consent and data flows are logged and digital signatures are used to ensure security in each of the flows.

The separation of the consent and data flows is a key feature of the consent framework. It is important for data flows to be executable asynchronously without the engagement of the user. This framework specifically enables this separation.

## 6.1. Consent Revocation

If the consent is marked as "revocable", then users have the ability to revoke that consent at a later date, by requesting the data provider, the data consumer or other entities. The consent artifact has provision for defining Revoker for revoking the consent and options for Data Consumer and Data Provider to get notified on various events such as this. In most situations, Revoker would be a URI owned by the Data Provider. Revocation requests sent to the revoker must follow a standard format which is specified below. Requests must be digitally signed, just like the original artifact being revoked.

While verifying signatures in consent artifacts (in the data flow), the data provider/consumer must also check that the consent artifact has not been revoked by the user, and only when this is true should the data share be allowed to occur.

*Exhibit 2: Revocation Request Specification*

```
<RevocationReq xmlns="http://meity.gov.in" timestamp="YYYY-MM-DDThh:mm:ssZn.n">
    <!-- entity creating the request -->
    <From type="URI" value="" />

    <!-- consent artifact -->
    <Consent> base-64 encoded consent artifact as-is </Consent>

    <!-- OPTIONAL User signature block -->
    <Signature />

    <!-- Requestor signature block -->
    <Signature />
</RevocationReq>
```

## 6.2. Logging and Notification

All events in the consent flow and data flow must be logged and notified as necessary using Consent *Log artifact*. A log artifact contains the consent artifact along with information about when and by whom the log was created. Two types of consent flow events must be logged - CONSENT-CREATED and CONSENT-REVOKED. For data flow events, logs must be created for DATA-REQUESTED (when a new data request is received by the data provider), DATA-SENT (when data is sent by data provider to data consumer) and DATA-DENIED (when data request is denied by data provider). Additionally, for DATA-SENT event, the list of data items shared by the data provider / received by the data consumer must also be logged.

*Exhibit 3: Consent Flow Log artifact*

```
<ConsentLog xmlns="http://meity.gov.in" timestamp="YYYY-MM-DDThh:mm:ssZn.n">
    <!-- entity creating the log request -->
    <LogFrom type="URI" value="" />
    <Event type="CONSENT-CREATED | CONSENT-REVOKED | DATA-REQUESTED | DATA-SENT
| DATA-DENIED" note="">

    <!-- consent artifact -->
    <Consent />

    <!-- information about data items shared -->
    <Data-Items>
        <!-- following element repeats -->
        <Data-Item id="" desc="" />
    </Data-Items>

    <!-- Log creator's signature block -->
    <Signature />
```

```
</ConsentLog>
```

# 7. Conclusion

This document provides a technology framework for electronic consent for any data access/sharing across entities. It is important that such an electronic framework is created for better management of user consent in a paperless system. Various authorities and regulators may extend this framework including the artifact definition as necessary for use within their domain.

**** END ***