The Need for Standardization in Digital Services Delivery

Sundeep Oberoi & Anupam Agrawal

Today a significant of portion of services are being delivered digitally to consumers. The consumer interaction channels may be via a web application, a mobile app, a mobile POS terminal or an IVR interface or a combination of these, in addition to delivery mechanisms for physical goods.

Each service provider uses a different combination of interaction channels with widely differing user interfaces and experiences. These are implemented with various degrees of usability, reliability, security and privacy. Poor implementation results in very high levels of time wasted and possible risk of security breaches leading to financial loss and privacy impact. Since many of these services are essential services such as banking and citizen services delivered by Government departments, there will be significant benefit in standardizing certain important aspects of this service delivery. This note identifies the following important areas for digital service delivery standardization. The issue of payment systems has been left out of this note since the authors believe that electronic systems are incorporated into digital service delivery in a reasonably modular way and there is a whole regulatory and standardization regime that adequately covers this aspect.

1. Registration and Identity Proofing

Many digital services require registration and of those several require an Identity Proofing process that may involve uploading of electronic copies of documents, submission of hard copies of documents, authentication based upon data already available with the service provider of (like mobile number, personal details like birth date, mother's maiden name, postal code etc.) or the use of Aadhaar identity authentication.

2. Recovery of Authentication Credentials

Currently the most prevalent method of recovery of authentication credentials is via a "forgot password" functionality which may authenticate the user over and IVR channel or via an SMS based OTP to a registered mobile number. If authentication is successful a temporary password (or a link that permits an initial login and the creation of a new password) is sent to the registered email-id. In a small number of instances a new credential like a temporary password or new PIN is delivered via post or a courier company.

3. SLA on Synchronous Channels

In many instances the interface for interaction is via an IVR channel. There are deep menus and indeterminate wait times. There may not be a distinction between and emergency type interaction and a routine type interaction. Finally when a human service agent is connected to the user, there may be a call drop and there is no method to reconnect the call and resume the conversation where is was interrupted.

4. Issue Redressal Systems

Some providers provide a method to log issues either via a web interface, email, a phone interface or by physical post. A few providers may assign an issue/problem/request number and that may allow for limited follow up and tracking.