DIRI Data Brief: 03

Aadhaar enabled Public Distribution System in Delhi

Siddharth Sekhar Singh and Ashwini Chhatre

June 2018

Key Facts

- The authentication failure rate for active ration cards in Delhi-AePDS in March 2018 was 1.3%. 19,482 ration cards failed authentication during this period
- 97% of all successful fingerprint and iris-based authentication requests received response from UIDAI within 2 seconds.
- Failure rate for OTP-based authentication was 18% as compared to .5% and 2% for fingerprint and iris based authentications respectively.
- High authentication attempt days were marred by frequent disconnection between ePOS devices and PDS server.

Study Methods and Data Sources

Data from the Aadhaar enabled Public Distribution System (AePDS) portal of Department of Food, Civil Supplies and Consumer Affairs, Government of National Capital Territory, Delhi was used for this analysis. AePDS is online portal containing data uploaded from ePOS devices used in fair price shops (FPS) for distribution of subsidized food grains. This website is updated daily. For further information about AePDS, including the data, visit the AePDS website at: http://epos.delhi.gov.in.

All the data for the analysis was scraped from the website for the period of 1st to 30th March 2018 and analysed using open source tools.

Summary

The Public Distribution System (PDS) in Delhi employs Aadhaar to authenticate the identity of its beneficiaries. The authentication takes place at the Fair Price Shops (FPS), wherein an individual eligible to receive subsidized food grains is required to furnish proof of possession of a ration card and must undergo Aadhaar-based authentication. The authentication workflow includes biometric and OTP based authentication.

This data brief characterizes the main attributes of Aadhaar-enabled Public Distribution System (AePDS) in Delhi and reports on the relative impact of essential components of the AePDS system on allocation of entitlements to the beneficiaries of the PDS system during March 2018.

The Aadhar authentication attempts for approximately 1.55M ration cards were made in Delhi's AePDS in the month of March 2018. Out of these, 19,482 ration cards failed authentication in Delhi AePDS. We found that the Unique Identification Authority of India (UIDAI)'s Aadhaar authentication services to be extremely responsive. More than 97% of all successful authentication requests received a response from UIDAI within two seconds of their generation at the ePOS machines and 65% out of these were received within one second. Almost 70% of all OTP based authentications were completed in no more than 20 seconds. Only 149 authentications (out of 1.55M) were found to take more than sixty seconds to authenticate.

Aadhaar enabled public distribution system (AePDS) has three major components. The ePOS machine at the PDS shop, the state PDS server, and the Aadhaar Authentication Services managed and provided by UIDAI. For efficient delivery of Aadhaar authentication enabled services to the beneficiaries these three components must function in tandem with high efficiency. The state PDS server contains the repository of the digitized ration cards of all the beneficiaries and logs each transaction generated by the ePOS device present in the PDS shop. Even temporary unavailability of the state PDS server greatly impacts the time taken to authenticate a beneficiary. We found that the PDS entitlement offtake in Delhi is characterized by abrupt surge in authentications attempts in the first half of each month. Any disruption of services by PDS server during this period aggravates the inconvenience caused to beneficiaries.

During the month of March 2018, the state PDS server of Delhi was found to be frequently inaccessible by the ePOS devices, especially on days with high number of authentication attempts. The state PDS server's throughput was observed to abruptly decrease for short durations of time during exactly the same hours of the day with high authentication attempts.

These observations call for a detailed study of the efficacy of various components of AePDS to identify technical issues or bottlenecks in different parts of the authentication ecosystem and gain insights for improved strategic management of the authentication system.

***Keywords**: Aadhaar authentication; Public Distribution System: Delhi AePDS; State PDS Server*

1. Background

Aadhaar authentication enables residents to prove their identity based on their demographic and/or biometric information captured during Aadhaar enrolment. Aadhaar authentication in public distribution system was introduced to make the process of identification of beneficiaries (a) *convenient*, by avoiding the need of multiple identity documents and (b) *accurate*, by using biometrics and/or OTP to accurately authenticate the identity of a beneficiary. Aadhaar authentication is also expected to bring in transparency and efficiency in the PDS by curbing corruption and leakages.

The Public Distribution System (PDS) in Delhi is Aadhaar-enabled. Delhi AePDS uses three modalities for authentication, two of which are of Biometric (fingerprint and iris)-based and the third one being OTP (One-time password)-based. To receive food grains entitlement from the public distribution system the beneficiaries must correctly establish their identity by utilizing the 'Aadhaar authentication framework'. The authentication takes place at the network of Fair Price Shop (FPS) spread across the nine districts in Delhi. Each FPS is equipped with an ePOS (Electronic Point of Sale) machine. These handheld devices act as an interface between beneficiary and the Aadhar authentication ecosystem.

Aadhaar authentication request for each beneficiary is generated using these ePOS devices. After retrieving the details of a beneficiary's ration card from the state PDS server a request for authentication is sent to UIDAI's Aadhaar authentication services which only responds with a Yes or No and no personal identity information is returned as part of the response. The first modality for authentication available to the beneficiary is finger print-based and if due to some reasons finger biometric based authentication is not successful then iris and OTP are provided as contingency.

The state PDS server contains the repository of the digitized ration cards of all eligible beneficiaries of the PDS system in the state. It also records details of every successful and fail authentication transaction generated by the ePOS devices. The PDS server has an important role in the Aadhaar enabled Public Distribution System (AePDS). For efficient delivery of authentication services to the beneficiaries, high efficiency of PDS server and UIDAI authentication services are extremely important and especially on days with high authentication attempts. Underperformance of either of these components can result in inconvenience to the residents.

We focus on understanding the key features of AePDS in Delhi. The objective is to examine the relative difference in usage and efficiency of different authentication modalities by beneficiaries. We then identify different components of Delhi AePDS and examine their role in delivery of authentication services

2. Key Observations in Delhi AePDS

2.1 Aadhaar authentication failure.

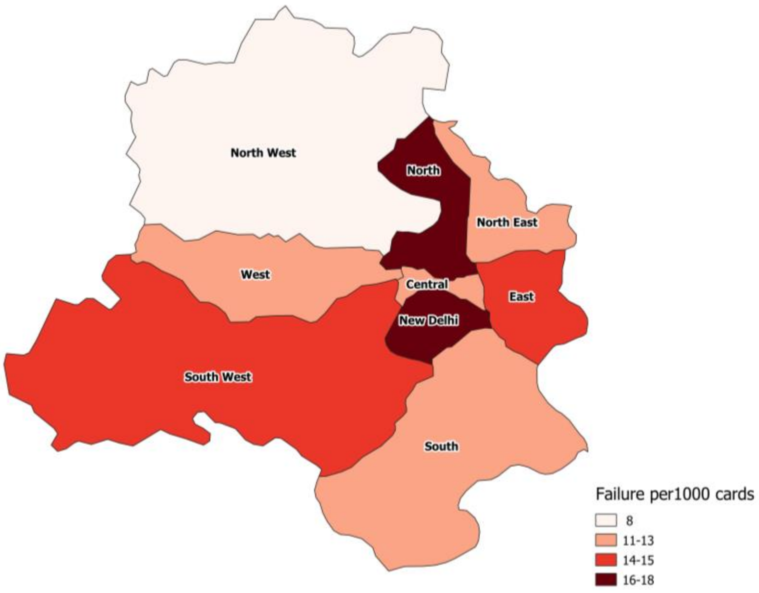

Figure 1: Aadhaar authentication failures for every 1000 active ration cards in Delhi.

Aadhaar authentication attempts for approximately 1.5M ration cards were made in Delhi AePDS in the month of March 2018. In that, about 19,482 ration cards failed authentication during same period.

North West (.27M) has the maximum number of active ration cards followed by North East (.25M). New Delhi district has the least (.06M) number of active ration cards. In absolute numbers South West Delhi (2869) has the highest number of cards which failed Aadhaar authentication.

For every 1000 active ration cards authenticated in Delhi, failure due fingerprint-based authentication was found highest in New Delhi (9) and failure due to OTP-based authentication was highest in North Delhi (9) (Figure 1).

About 90% of the total authentication attempts in Delhi were fingerprint-based while remaining used iris (7%) and OTP (3%) as modalities for authentication.

The higher failures rate in New Delhi district were observed due to relatively greater number of fingerprint-based authentications failing in the district (figure 2). 9 out of every 1000 authentications in New Delhi failed when residents used fingerprint to authenticate themselves. Using the same Metric, we observed that the fingerprint-based authentications performed relatively better in North West Delhi where 3 failures per 1000 authentications were of fingerprint based. .

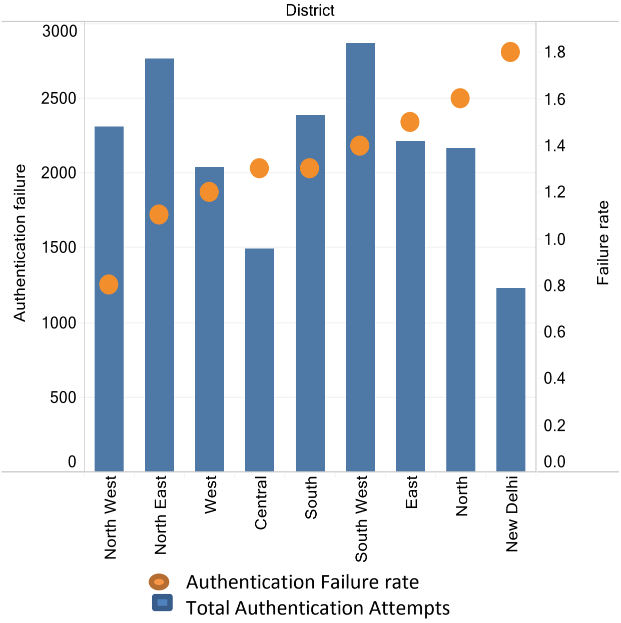

Figure 2: Aadhaar authentication failure rate in Delhi

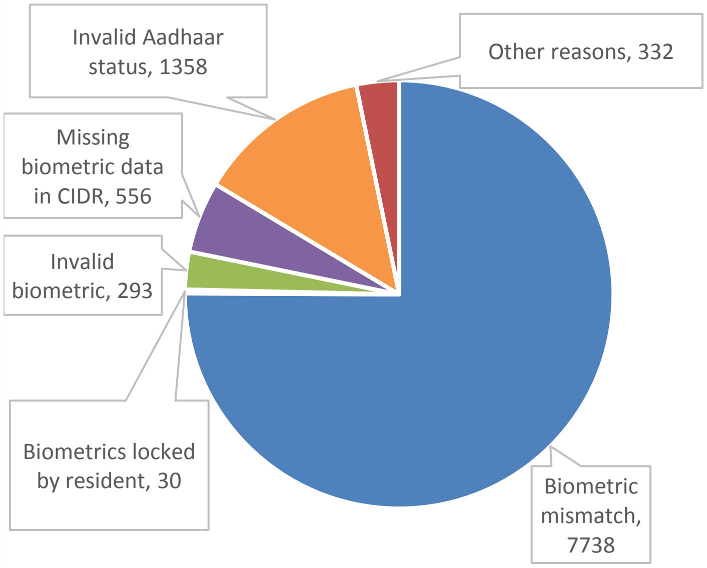

Figure 3: Causes of biometric based Aadhaar authentication failure rate Delhi AePDS.

Three modalities of Aadhaar authentication are provided in Delhi AePDS two of which are biometric based (fingerprint and iris) and the third is OTP-based wherein, a password is sent to the registered mobile number of beneficiary to establish their identity.

Biometric based (fingerprint and iris) authentication constitutes 53% of total authentications failures and remaining (47%) were due to OTP authentication. 'Biometric data mismatch' was the leading cause of finger print based authentication failures (figure3).

The ePOS device accepts fingerprint-based biometric as the preferred mode of authentication before iris and OTP. Out of the total fingerprint-based authentication attempts in the state, less than 1% of these failed. 7% of total authentications were iris-based out of which 2% authentications failed.

It's interesting to note here that OTP-based authentication was used as a modality for authentication by approximately 3% of all active cards ration cards in the state but the authentication failures due to OTP constitute 47% of the total authentication failures. It was also observed that 18% of all OTP based authentication failed.

No OTP-based authentication was observed in Delhi AePDS data after 17th March (figure4). OTP-based authentication can be considered as contingency for cases where biometrics of a resident can't be used for authentication. Number of reasons can cause OTP-based authentications to fail which may include improper seeding of mobile numbers, mobile network issues, lack of awareness among beneficiaries etc .

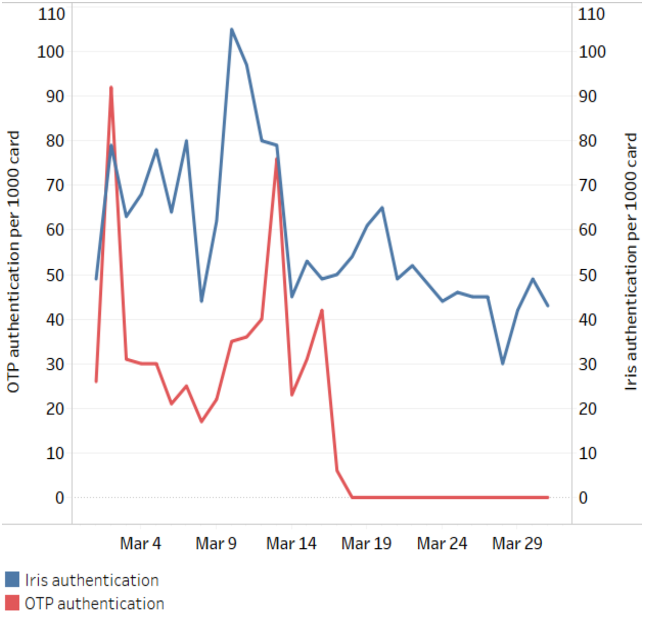

Figure 4: Application of OTP based and iris-based authentication

2.2 Components of Delhi's AePDS and their role in service delivery.

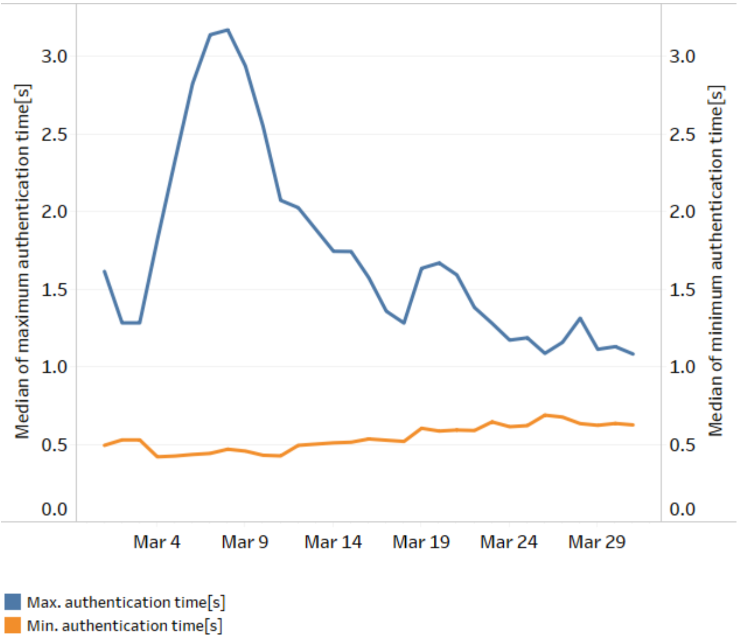

Figure 5: Daily maximum and minimum median authentication time by UIDAI's Aadhaar authentication service.

The efficiency of the UIDAI's Aadhaar authentication service is evident from the daily data available for maximum and minimum time taken by UIDAI's authentication services to authenticate the 1.5M cards of Delhi AePDS in March 2018.

About 97% of these cards were authenticated by UIDAI's authentication services within 2 seconds of generation of authentication request on the ePOS devices. Remaining 2.5% ration cards were authenticated by UIDAI between 15 to 30 seconds. Only 140 cards were found to take more than 70 seconds to authenticate. The daily median of maximum time taken to authenticate a beneficiary was found just above three seconds (figure 5).

ePOS devices in AePDS can be operated only by designated PDS dealers who must establish their identity by using Aadhaar authentication at least once a day. These hand-held ePOS devices connect the beneficiaries with Aadhaar authentication service provided by UIDAI with assistance of the state PDS server.

Using the beneficiary authentication attempt and active ePOS device's reset count data (available on Delhi AePDS portal), we observed that in March days with relatively higher number of authentication attempts were marred by frequent disconnection of ePOS devices from the state PDS server (figure 6).

ePOS disconnections are manifested by frequent restarts of ePOS machines, delayed or no response from the state PDS server and decreased efficiency of the ration shops. The down time of these ePOS machines aggravates the inconvenience of the beneficiaries specially on days with higher authentication attempts.

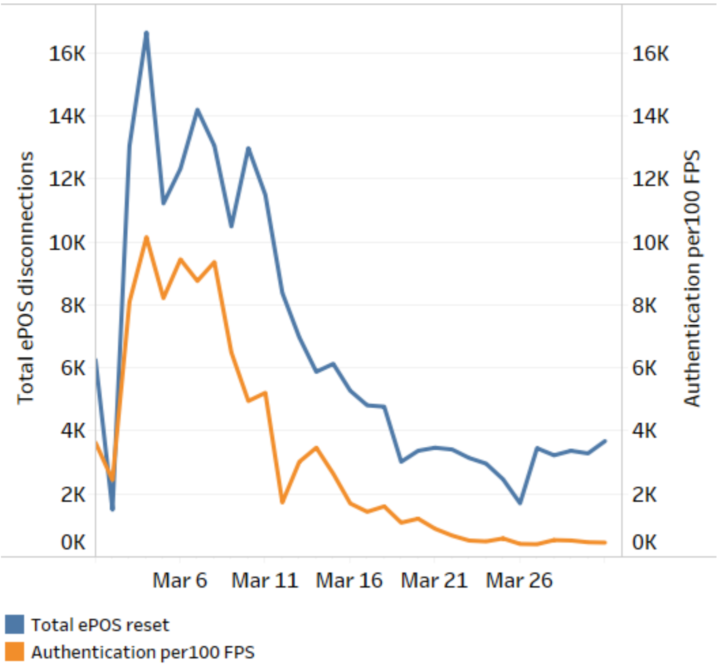

Figure 6: Daily ePOS disconnections and authentications per100 ration shops

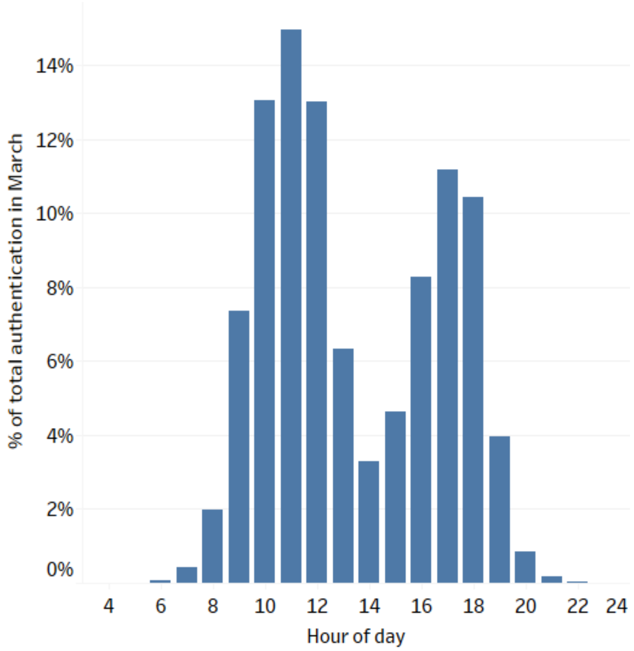

Figure 7: Hourly authentications as percentage of total authentications in March.

In AePDS, particulars of the digitized ration card of beneficiaries are retrieved from the state PDS server before every AePDS authentication attempt. The details of each transaction are logged into the PDS server only after which a transaction is considered successful. Failure of either of these activities results in disruption of delivery of authentication services and results in consequent inconvenience to beneficiaries which is manifested in the form of waiting time in queues or requirement to revisit the PDS shop when PDS server's services are restored.

Using PDS shop level transactional data, we observed that the state PDS server's hourly throughput abruptly fall during peak hours (10am to 1pm & 4pm to 7pm) of authentication activities. These disruptions in authentications were more frequent in the first half of the month. At the FPS shops, these disruptions are manifested in form inability of the ePOS to establish a connection with state PDS and non-responsive ePOS devices.

The Delhi AePDS is characterized by surge in number of authentication attempts during the first half of each month. In the month of March more than 85% of the beneficiaries claimed their entitlement during this period.

It was also observed that on daily basis in March the number of Aadhaar authentications were found to be highest during 10am in the morning up to 1pm in the afternoon. 40% all total successful authentication attempts (1.5M) by beneficiaries were made during these hours. Authentication attempts again pick-up pace in the afternoon starting from 4pm and lasted till 7pm in the evening during which 30% of all successful authentication attempts for the month were made(figure 7).

For efficient delivery of authentication services it is critical thatall components of the state AePDS framework provide uninterrupted service especially during peak authentication data traffic hours.

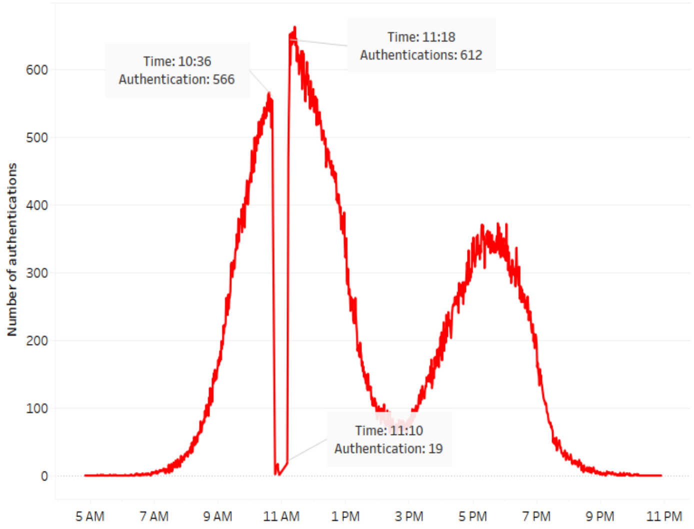

Figure 8: Disruption of services offered by PDS server on March 8th

3. Policy Implications

Delhi's Aadhaar enabled public distribution system (AePDS) provides three modalities for Aadhaar authentication of beneficiaries. The fingerprint-based Aadhar authentication is most frequently used in Delhi AePDS with 90% of all authentications using this modality of authentication and less than 1% of these failing. 97% of biometric-based authentications in Delhi AePDS were found to be authenticated by UIDAI within 2 seconds of their generation on the ePOS machines. Only 1.5% authentications out of total 1.55M authentications were found to take between 15 to 30 seconds. This signifies the responsiveness of the Aadhaar authentication services provided by UIDAI.

OTP based authentications, wherein an OTP is sent to the registered mobile number of beneficiary, constituted 3% of total authentication attempts. The average time taken for OTP-based authentication was 16 seconds whereas for biometric based methods it was less than 2 second. The minimum time of response for authentication of an OTP was found 19 seconds. 70% of all OTP based authentication took more than 20 seconds to authenticate. These observations indicate the inefficiencies in the OTP based authentication mechanism and the effectiveness of biometric of biometric based modalities for identification in Delhi AePDS. OTP based authentication mechanism are generally considered as contingency when biometric based authentication is not possible due to network limitations or poor quality of biometric. OTP based authentications when efficiently utilized could lead to full inclusion of entitled beneficiaries.

Given the proven efficiency of iris-based authentication system, only 7% of all authentications in the state were iris-based. It's interesting to note that 22% PDS shops never used iris scanner for authentication purpose in March. It could be due to unavailability of the device at shops or lack of knowledge of using the iris device. Since only 2% of iris based authentications failed, it requires more frequent use of this modality of authentication and it could even be used as a substitute of OTP based authentication provided the availability and frequent usage of iris scanners at PDS shops.

3.1 Further Research

This data brief seeks to establish a foundation for identifying issues surrounding the AePDS in Delhi and while doing so we were able to pose some questions for further research in following areas:

1. Using the entitlement allocation and authentication failure data, a coherent story of how people access the AePDS in Delhi could be created to get better insights of the beneficiary access to AePDS.
2. Identifying the underlying cause for variation in performance of different modalities of authentication across districts. This study could contribute in limiting exclusion of beneficiaries due to authentication failure.
3. New Delhi district has relatively higher number of fingerprint-based failure. A thorough study of the factors leading to it could help improve authentication services in the district.
4. OTP based authentication is a contingency for biometric authentication failures but considering its poor performance in the state requires scrutiny of the implementation mechanism of this modality of authentication. Findings of which could contribute to improvethe delivery of other social benefit programs using similar authentication framework.
5. A detailed study of the throughput of the PDS server under different load conditions and days to identify existence of any plausible underlaying technical issue or bottlenecks in the AePDS authentication ecosystem is required to minimize inconvenience to beneficiaries due to interruption of authentication services.

About DIRI

This data brief was prepared by the Digital Identity Research Initiative (DIRI), which was launched in July 2017 with funding from Omidyar Network. DIRI is aimed at producing high-quality and timely research on digital identity, engaging relevant stakeholders, and building a global research ecosystem for digital identity. In addition to such briefs, DIRI's activities include Research Fellowships, Summer Fellowships, and the International Conference on

Digital Identity Research Initiative (DIRI)
Indian School of Business, Gachibowli,
Hyderabad – 500032; Phone: 9000877014
E-mail:diri@isb.edu; merlyn_jude@isb.edu