

F. No. 23(5)/2015-Comp.Cell
Government of India
Ministry of Consumer Affairs, Food and Public Distribution
Department of Food & Public Distribution

Krishi Bhawan, New Delhi – 110 001
Dated the 26th September, 2018

To

Principal Secretary/Secretary,
Food & Civil Supplies Department,
All State/UT Governments

Sub: Advisory for ePoS operations and security of data - reg.

Sir/Madam,

I am directed to refer to the subject mentioned above and to say that pursuant to the recent incident of pilferage of PDS foodgrains in the State of Uttar Pradesh (UP) through manipulation of Aadhaar numbers seeded with the Ration Cards, a fact-finding team from this Department was deputed to UP to look into the factors responsible for such an incident. Based on the report submitted by this team, the following advisory is issued to ensure that the systems created under the end-to-end computerization scheme work in an efficient and error-free manner and are not susceptible to any misuse/manipulation in future:

1. FPS Automation:

- 1.1. Access to ePoS application should be given only after biometric authentication of FPS dealer.
- 1.2. FPS dealers should be advised not to note down any login information in routine registers, casual papers, etc.
- 1.3. The ePoS device must have the features to display and announce the message in local/regional language in case of the failure of biometric authentication.
- 1.4. The ePoS application must be stored in the secure memory of ePoS device.
- 1.5. Data must be encrypted before storing in ePoS device or communicating with servers through secure channel (Secure Socket Layer).
- 1.6. Data copy or upload should be completely restricted through USB port or Bluetooth connection of ePoS device.
- 1.7. Installation of unauthorized software/applications/games etc. in ePoS device should be strictly prohibited.



1.8. Installation of latest patch or application updates on ePoS devices should be done through ePoS servers.

1.9. Mapping of Machine ID (MAC ID) of ePoS device and associated FPS ID should be carefully recorded on the server, and communication with ePoS server should be restricted to respective MAC IDs only.

1.10. All ePoS devices should be GPS enabled and geo location of the device should also be recorded against each transaction. ePoS transactions shall not be allowed if coordinates of the device go beyond the geographical range of mapped FPS.

2. Security Audit of PDS Application

2.1. States/UTs should ensure that the all Websites/ Applications/ Web-Services/ APIs/ etc. of PDS operations are Security Audited. An audit clearance certificate must be obtained from STQC or CERT-IN or their empanelled agencies.

2.2. The security audit shall also be done as and when any changes are done to the source code.

2.3. An SSL certificate for data encryption and communication through online channels should be procured and implemented.

3. Database Management

3.1. Change/update of information in database tables / fields shall be restricted to online applications only. Manual modifications/ un-approved scripts/ stored procedures, etc. shall not be allowed.

3.2. Access to databases must be restricted to only database administrator or authorize users.

3.3. Fields containing sensitive personal data / classified information must be secured/encrypted/masked in strict adherence to IT Act, Aadhaar Act and guidelines issued by the Ministry of Electronics and IT (MeitY) dated 4th May 2017, which were earlier shared with all States/UTs by this Department.

3.4. Logs should be maintained for addition/ modification/ deletion of database records or fields.

4. Usage of National/State Data Center for PDS Operations

4.1. States/UTs should leverage National Data Center (NDC) or State Data Center (SDC) or any other Government data centre only for hosting PDS applications including ePoS operations and data thereof.

De

4.2. Data centers must be compliant to security policies and guidelines issued by MeitY, GoI.

4.3. System integrators/vendors of ePoS devices shall have limited access to modify ration card information and ePoS transactions with proper approval and adhering to log management.

5. Ration Card Management System and use of Aadhaar:

5.1. Modification in ration card information should only be done by authorized users and workflow based system should be followed for proper approvals while adhering to log management.

5.2. Appointment of outsourced resources (if any) for above work should be done carefully after proper background check and verification. These should be given limited access of system in respect of processing requests for - new ration card/ modifications with proper approval and adhering to log management.

5.3. Use of digital signature should be made mandatory for issuing new ration card or approving changes in ration card information.

5.4. Aadhaar and mobile numbers of beneficiaries should be masked. Only last four digits may be made visible in RCMS/State portals.

5.5. Seeded Aadhaar numbers of all members in a ration card shall be validated through biometric authentication and validation facility i.e. eKYC.

5.6. Hard copy of Aadhaar cards of beneficiaries (if any) should be retained at any field level office after successful completion of eKYC authentication of PDS beneficiary.

5.7. Photocopies of Aadhaar, ID proofs, address proofs, etc. should be kept in secure environment at all times.

5.8. Modification of Aadhaar number should be immediately followed with real time validation/authentication of Aadhaar number using UIDAI services.

5.9. After successful eKYC, UIDAI server sends demographic information of Aadhaar to respective KUA. Necessary measures should be taken to protect this information.

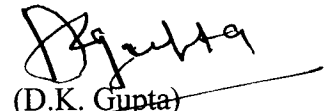
5.10. In case of validation failure such modification should not be allowed in the system, whereas in case of success such modification should be frozen immediately so as not to allow any further modification of Aadhaar number.



5.11. In case Aadhaar number of beneficiary is used for issuance of new ration card, state level de-duplication shall be performed before issuing the same.

2. You are requested to get a detailed examination / verification of the systems done in your State/UT in the light of the points mentioned above.

Yours faithfully


(D.K. Gupta)
Director (PD)

Copy for information to:

1. Secretary, Ministry of Electronics & IT (MeitY), New Delhi
2. CEO, Unique Identification Authority of India (UIDAI), New Delhi
3. Director General, National Informatics Centre, New Delhi
4. Joint Secretary, DBT Mission, New Delhi
5. Dy. Director General, National Informatics Centre, New Delhi