certin
Handling Computer Security Incidents

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0088

Aadhaar Enabled Payment System

Original Issue Date: December 28, 2016

Description

Aadhaar Enabled Payment System (AEPS) is a payment model which allows financial transactions at PoS (Micro ATMs) via banks using the Aadhaar authentication. This payment system empowers the marginalized and excluded segments to conduct financial transactions (Credit, Debit, Remittances, Balance Enquiry, etc) through microATMs deployed by Banks in their villages. To make transactions via AEPS, customers and merchants need to link their Aadhaar card with their bank accounts.

Types of banking transactions using AEPS are as follows:

- Balance Enquiry
- Cash Withdrawal
- Cash Deposit
- Aadhaar to Aadhaar Funds Transfer

AEPS requires the following inputs from a customer for transactions:

- IIN (Identifying the Bank to which the customer is associated)
- Aadhaar Number
- Fingerprint

How it Works - Customer Side

Transaction via AEPS involves the following process:

- The customer provides his/her Aadhaar number and the fingerprint impression at the microATM device.
- The customer provides the details of financial transaction to be done.
- The digitally signed and encrypted data packets are transferred via Bank Switch to NPCI to UIDAI.
- UIDAI processes the authentication request and communicates the outcome in form of Yes/No.
- If the authentication response is Yes, bank carries out the required authorization process and advises microATM on suitable next steps.

Best Practices

- At enterprise level, there are processes to use multifactor and multimodal authentication to maintain security.
- Liveness detection methods should be used to prevent spoofing attacks to avoid the use of fake fingerprints to impersonate a legitimate user and gain unauthorized access.
- Physical devices used for transaction (micro ATMs) must be tamper resistant to avoid unauthorized use.
- Bank accounts should be monitored and unauthorized transactions should be reported immediately.
- Do not get carried away by strangers who try to help using the microATM.

References

CERT-In
Security of Micro ATMs (CIAD-2016-0063)
http://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0063

Securing Biometric Devices (CIAD-2016-0074)
http://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0074

UIDAI
https://authportal.uidai.gov.in/web/uidai/home-articles?urlTitle=aadhaar-enabled-payments

NPCI
http://www.npci.org.in/aepsoverview.aspx
http://www.npci.org.in/documents/aepsfaqcust.pdf

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India