# Preventing financial fraud by using UE PEI / IMEI from 5G-EIR

Tech Con 2025 Abstract 6

HPE Edge;

# Abstract

*Modern world with technological advancement in recent years online payment/transactions become an inseparable part of banking and e-commerce industry. Recent data from cyber security suggests a rise in online payment frauds across the world. Cybercriminals are constantly on the lookout to rob people of their money using Phishing attacks, Fake delivery OTP scam etc.*

*In our solution we propose a mechanism to deliver OTP to customers for online banking transaction based on validation of IMEI /PEI from Equipment Identity Register (EIR). This avoids fraud transactions when OTP is delivered to an unauthorized device. Even in case of SIM swap where a fraudster requests OTP for banking transactions will not receive the OTP due to a mismatch of UE PEI or IMEI validated using 5G EIR database.*

## Problem statement

Online transactions are not entirely new, the COVID-19 pandemic has only accelerated the use of online payment methods like UPI, debit/credit cards and mobile banking across the world. The importance of these e-payment services is increasingly becoming more of a necessity for both vendors and customers.

As more and more people are shifting to online payments, so are cybercriminals. One of the main disadvantages of online payments is the technological illiteracy among many people, especially the older generation. Since they don't have enough knowledge on how to go about using technology or smartphones. There have been many cases in which criminals duped bank customers into revealing OTP or accessed it by hacking the smartphone.

OTP fraud involves tricking people into revealing their temporary security codes by calling the person or using a SIM swapping (clone) technique, that enable them to log into their digital accounts with an extra layer of authentication, letting scammers steal money, data, and more.

## Our solution

We are proposing a solution to deliver OTP to only prior registered devices. In most banking transactions customers use smart phones or mobile devices as primary devices. These mobile devices come with unique identification numbers like IMEI (International Mobile Equipment Identity) in case 4G/LTE network technology or PEI (Permanent Equipment Identifier) in case 5G network technology.

Banking security server (which generates OTP) should have an algorithm to validate the customer pre-registered PEI/IMEI against the present PEI/IMEI retrieved from network operator EIR database before delivering the OTP to its customers.

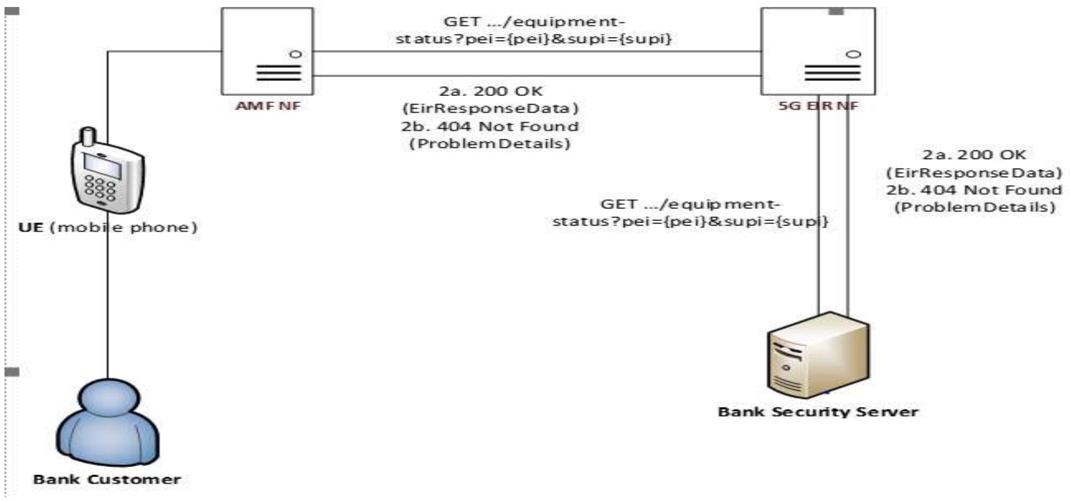

GET .../equipment-status?pei={pei}&supi={supi}
AMF NF
2a. 200 OK (EirResponseData)
2b. 404 Not Found (ProblemDetails)
5G EIR NF
2a. 200 OK (EirResponseData)
2b. 404 Not Found (ProblemDetails)
GET .../equipment-status?pei={pei}&supi={supi}
UE (mobile phone)
Bank Security Server
Bank Customer

Figure 1. Proposed Solution Diagram

The proposed solution is based on the following approach:

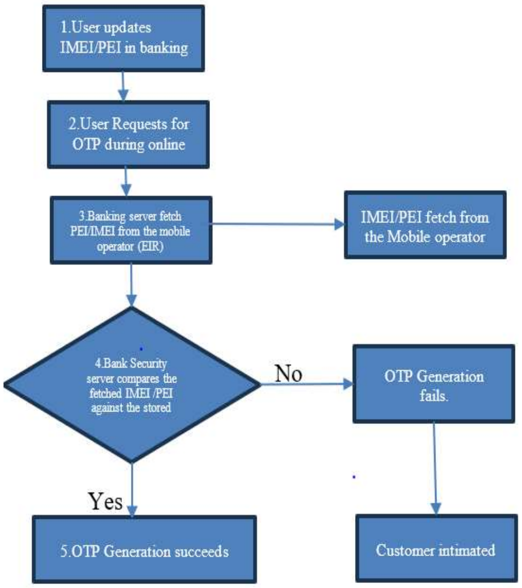
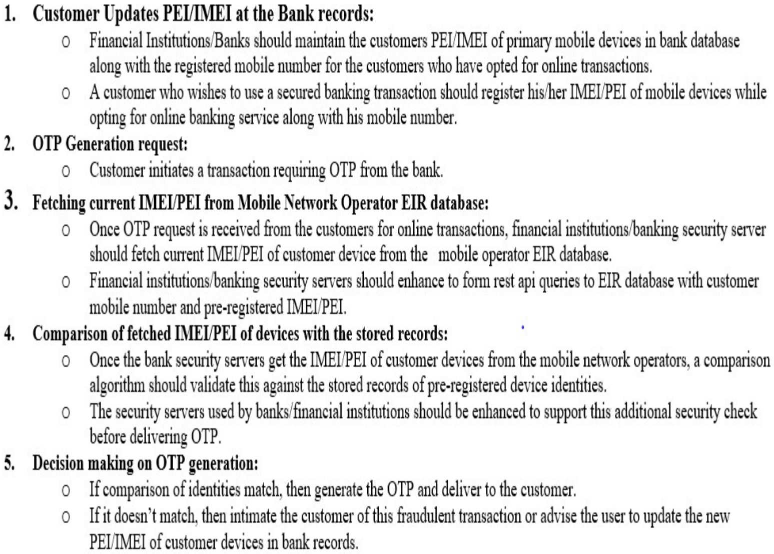

1.User updates IMEI/PEI in banking
2.User Requests for OTP during online
3.Banking server fetch PEI/IMEI from the mobile operator (EIR)
IMEI/PEI fetch from the Mobile operator
4.Bank Security server compares the fetched IMEI /PEI against the stored
No
OTP Generation fails.
Yes
5.OTP Generation succeeds
Customer intimated

Fig 2: Flow diagram



1. **Customer Updates PEI/IMEI at the Bank records:**
   - Financial Institutions/Banks should maintain the customers PEI/IMEI of primary mobile devices in bank database along with the registered mobile number for the customers who have opted for online transactions.
   - A customer who wishes to use a secured banking transaction should register his/her IMEI/PEI of mobile devices while opting for online banking service along with his mobile number.
2. **OTP Generation request:**
   - Customer initiates a transaction requiring OTP from the bank.
3. **Fetching current IMEI/PEI from Mobile Network Operator EIR database:**
   - Once OTP request is received from the customers for online transactions, financial institutions/banking security server should fetch current IMEI/PEI of customer device from the mobile operator EIR database.
   - Financial institutions/banking security servers should enhance to form rest api queries to EIR database with customer mobile number and pre-registered IMEI/PEI.
4. **Comparison of fetched IMEI/PEI of devices with the stored records:**
   - Once the bank security servers get the IMEI/PEI of customer devices from the mobile network operators, a comparison algorithm should validate this against the stored records of pre-registered device identities.
   - The security servers used by banks/financial institutions should be enhanced to support this additional security check before delivering OTP.
5. **Decision making on OTP generation:**
   - If comparison of identities match, then generate the OTP and deliver to the customer.
   - If it doesn't match, then intimate the customer of this fraudulent transaction or advise the user to update the new PEI/IMEI of customer devices in bank records.

## N5G EIR:

The N5g-eir_Equipment Identity Check service is provided by the 5G-EIR to check the Permanent Equipment Identifier (PEI) whether it is in the blacklist or not. The service can be consumed by AMF which initiates ME identity check by invoking the N5g-eirEquipmentIdentityCheckGet service operation. During the initial registration the Permanent Equipment Identifier is obtained from the UE.

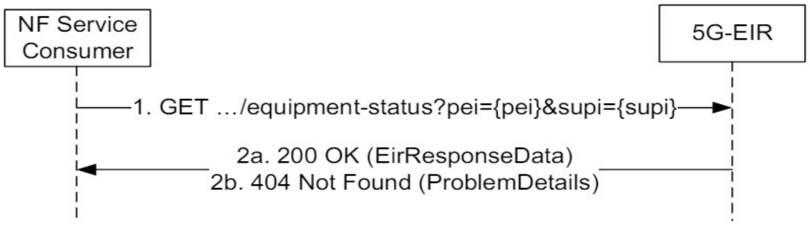

NF Service Consumer
5G-EIR
1. GET …/equipment-status?pei={pei}&supi={supi}
2a. 200 OK (EirResponseData)
2b. 404 Not Found (ProblemDetails)

Fig 3: 3GPP 5G EIR message flow

**Use case 1:** Criminals can dupe a bank customer to contact mobile operator with fake identity proof and getting a duplicate SIM card. The operator deactivates the original SIM, and the criminals generate OTP on the new number and try to conduct online transactions using a new device with a different IMEI/PEI. With this solution since IMEI/PEI of pre-registered device is already stored in the bank records and customer IMEI/PEI of device validation will fail and OTP is not generated.

**Use case 2:** In case of customer lost the primary device like mobile, banking transactions can never be done from this stolen mobile. Customer will block the SIM card and device will be blacklisted in EIR . When the fraudster tries to use the stolen mobile for banking the Response received from telco EIR will be IMEI/PEI blacklisted and OTP wont be generated. In such cases this solution can be enhanced to notify the cybercrime department as well to track the fraudsters.

## Evidence the solution works

HPE Telco 5G Equipment Identity Register (HPE Telco 5G EIR) enables checking the equipment status. The Equipment Identity Check (EIC) service checks the equipment status and returns it to the consumer network function (NF) as blacklisted, provisional listed, or allow listed.

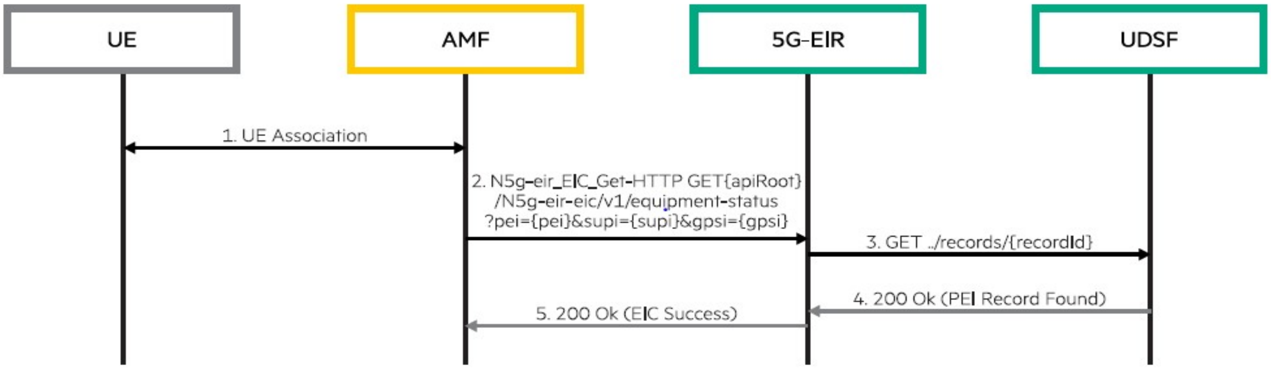

UE
AMF
5G-EIR
UDSF
1. UE Association
2. N5g-eir_EIC_Get-HTTP GET{apiRoot}
/N5g-eir-eic/v1/equipment-status
?pei={pei}&supi={supi}&gpsi={gpsi}
3. GET ../records/{recordId}
4. 200 Ok (PEI Record Found)
5. 200 Ok (EIC Success)

Figure 4. HPE Telco 5G EIR data flow diagram

## Advantages of Proposed Solution:

- With this approach the telco operators can generate revenue by providing this additional security feature to banks and any financial institutions where user authentication is crucial.
- This solution requires only data read access from EIR; any third-party application will not be able to make changes to EIR database.
- Bank or Financial institutions can advertise to customers on secure mechanism they provide for online transactions. (secured multi factor authentication)

## Competitive approaches

OTP tokens are one of the simplest methods of strong authentication and are very commonly deployed by organizations looking for a quick and effective way of boosting their login security.The most common alternative to OTP is an authenticator application that requires customers to obtain a password from another application on the phone. Service providers have developed other as well like tokens within the mobile app.

## Current status

HPE already provides standalone 5G-EIR to telco operators with other 5G NFs like UDR, UDM. Even for 4G LTE network 5G EIR offered along with containerized c-IHSS which interacts with 5G EIR DB using interworking function (IWK).

## Next steps

5G EIR should be enhanced to provide a secure mechanism to connect with REST clients along with AMF NF. This enhancement will help Telco operator to provide EIR access to bank/financial institutions for authentication mechanism with additional security.

# References

https://www.etsi.org/deliver/etsi_ts/129500_129599/129511/15.01.00_60/ts_129511v150100p.pdf

http://cmsgvm05.gre.hpecorp.net:8080/products/hpe-nf-eir-prod/1.6.0-202407090248