DFS Security recommendations for regulators and providers

Arnold Kibuuka, Project Officer, ITU

dfssecuritylab@itu.int

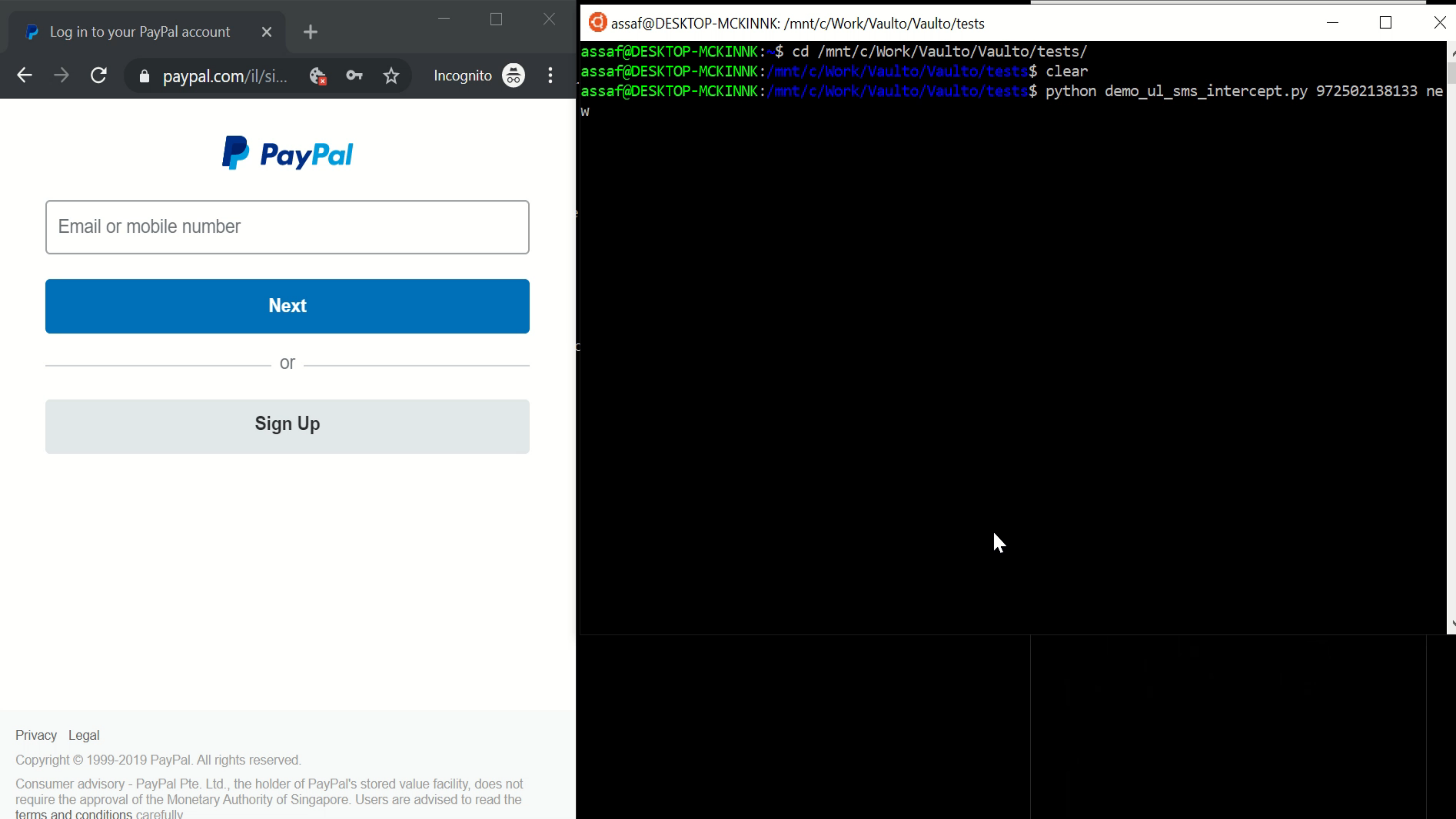
November 2024

DFS Security Recommendations

1. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
2. Recommendations to mitigate SS7 vulnerabilities
3. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
4. Mobile Application Security Best practices
5. DFS Consumer Competency Framework

Guidance to mitigate SS7 threats

Related report: Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions



```
assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 ne
w
```

Copyright © 1999-2019 PayPal. All rights reserved.

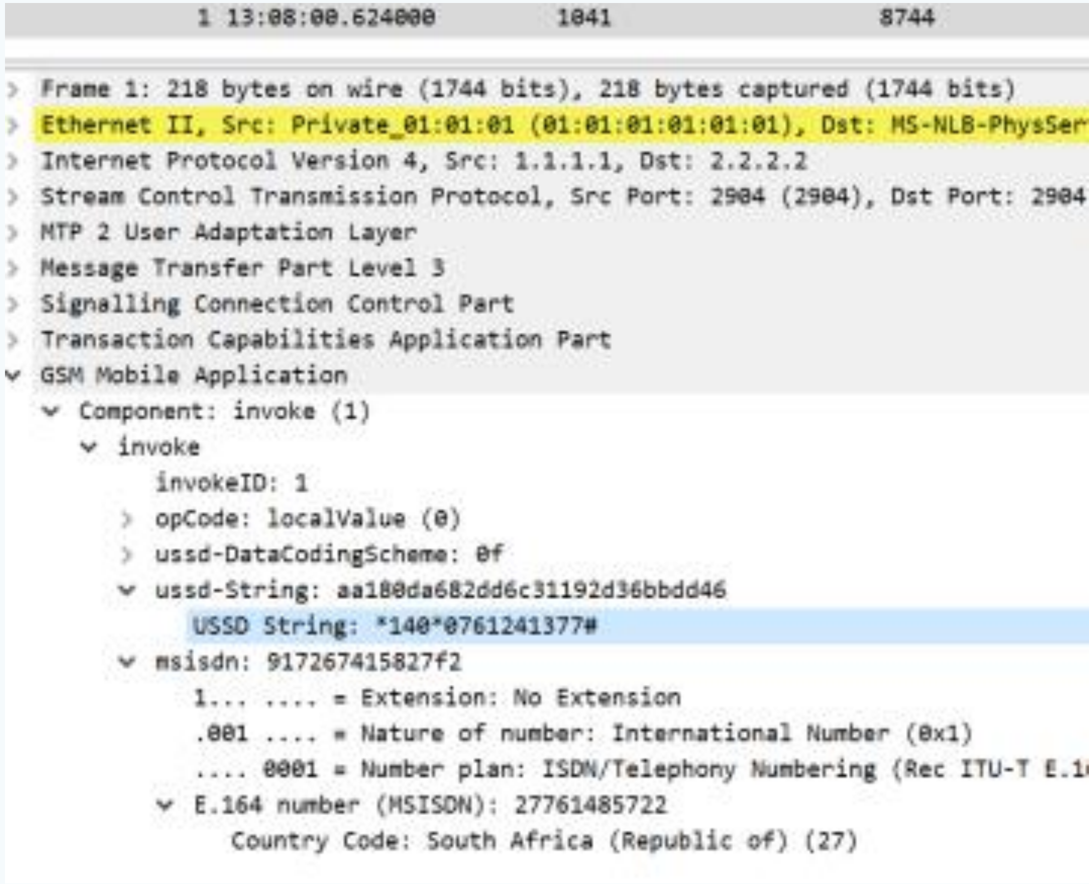
Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully

Regulatory Guidance to mitigate SS7 risks

- Regulatory coordination between telco and DFS regulator on SS7 vulnerabilities.
- Incentivize the industry
- Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS
- Telecom regulators to establish baseline security measures for each SS7 risk category
- IMSI validation gateway: An API that provides status of a number and real time country where client is located.

Recommendations for MNO to mitigate SS7 risks

- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing

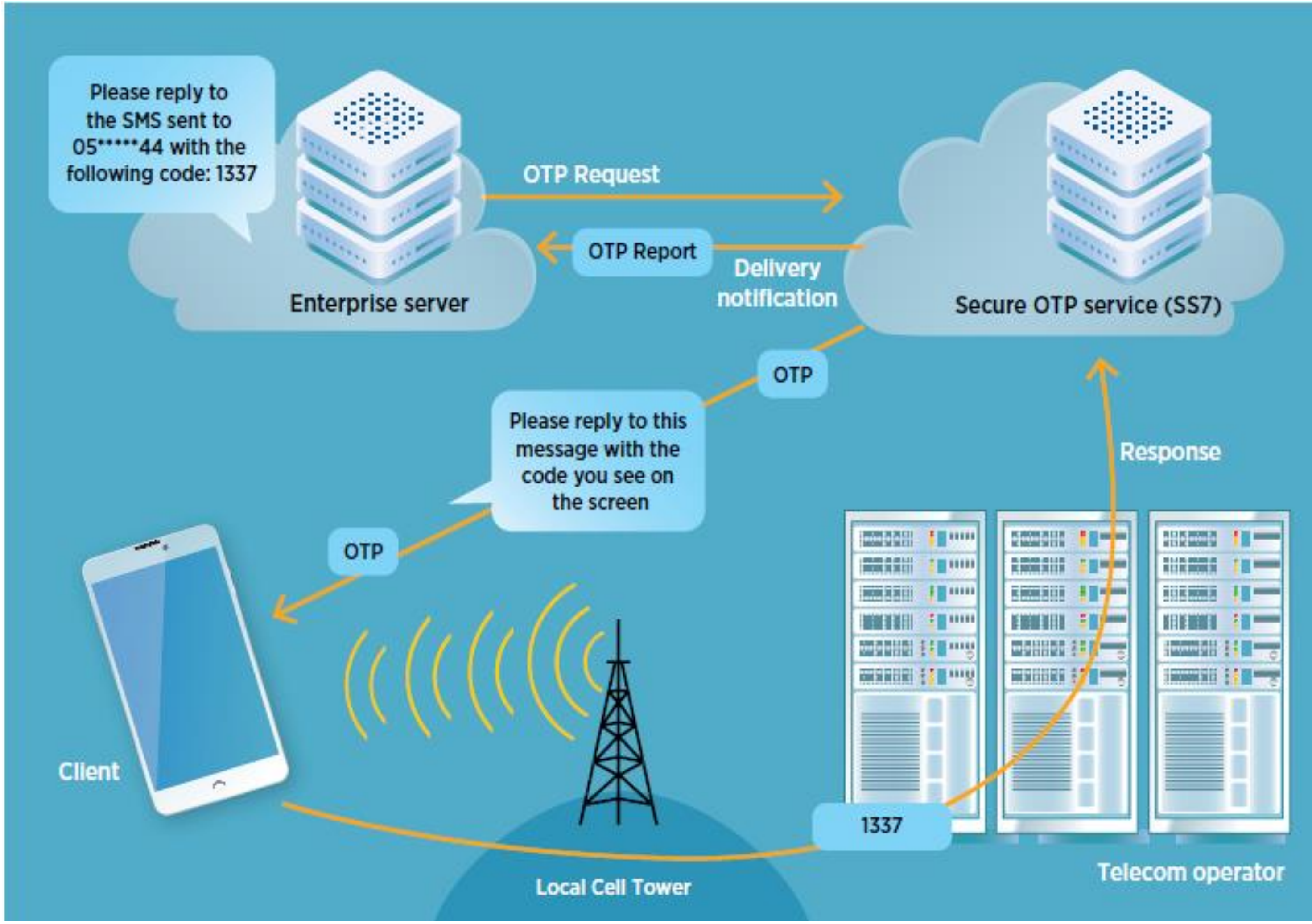


```
        1 13:08:00.624000        1041                     8744

Frame 1: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
Ethernet II, Src: Private_01:01:01 (01:01:01:01:01:01), Dst: MS-NLB-PhysSer
Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.2
Stream Control Transmission Protocol, Src Port: 2904 (2904), Dst Port: 2904
MTP 2 User Adaptation Layer
Message Transfer Part Level 3
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
      ussd-DataCodingScheme: 0f
      ussd-String: aa180da682dd6c31192d36bbdd46
        USSD String: *140*0761241377#
      msisdn: 917267415827f2
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x1)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.1
        E.164 number (MSISDN): 27761485722
          Country Code: South Africa (Republic of) (27)
```

DFS operator controls to mitigate SS7 risks

- Session time out
- Transaction limits for insecure channels
- User education
- Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD
- Bidirectional OTP SMS flow



ITU-T Study Group 11 work on SS7

- **Published Recommendations and Technical Reports:**
- ITU-T QSTR-SS7-DFS (2019): SS7 vulnerabilities and mitigation measures for digital financial services transactions
- ITU-T QSTR-USSD (2021) Low resource requirement, quantum resistant, encryption of USSD messages for use in financial services
- ITU-T Q.3062 (2022): Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks
- ITU-T Q.3063 (2022) : Signalling procedures of calling line identification authentication
- **Ongoing**
- Draft Q.TSCA: Requirements for issuing End-Entity and Certification Authority certificates for enabling trustable signalling interconnection between network entities.
- Draft Q.DMSA: Principles for detection and mitigation of signalling attacks in security signalling gateway

http://www.itu.int/go/dfssl

Contact: dfssecuritylab@itu.int

Thank you!