

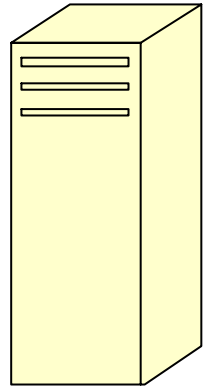
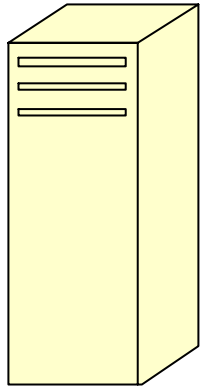
# SMS SC Spoofing

Source: O2

# Normal Flow

SMS-GMSC

VMSC



TCAP Begin (OA=+447711200200)

ACK

TCAP Continue (OA=+447711200200)

(SMSCA=+447711200200)

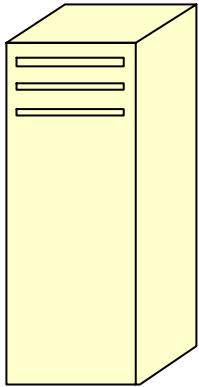


MCC in OA matches that in SMSCA, 44

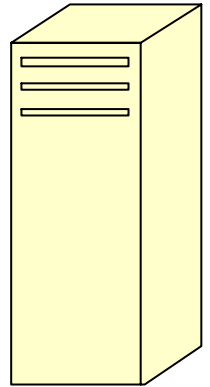
NDC in OA matches that in SMSCA, 7711

# Spoof Flow

Spoof  
SMS-GMSC



VMSC



TCAP Begin (OA=+281231200200)

ACK

TCAP Continue (OA=+ 281231200200)

(SMSCA=+447711200200)



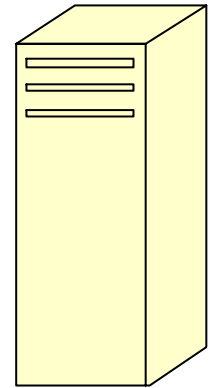
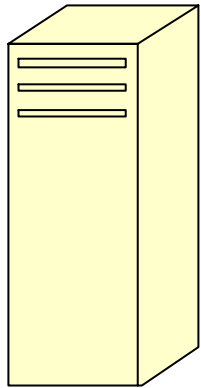
Note: Spoof SMS-GMSC tries to send SMS message apparently from a valid SMSC address, but uses a routeable E.164 number in its own network for the TCAP dialogue. Difference between the two addresses is detected and the SMS is not forwarded.

MCC in OA does not match SMSCA  
NDC in OA does not match SMSCA

# SMS Loadsharing Flow

SMS-GMSC

VMSC



TCAP Begin (OA=+447722200012)

ACK

TCAP Continue (OA=+447722200012)

(SMSCA=+447711200200)



Note: Operator has multiple SMS platforms, all of which are required to present the address +447711200200 to the user in the MT SMS in order that the user is not confused by a different address and that the REPLY via same SMS-SC feature works. However each SMS platform needs its own address in order to be able to return the correct acknowledgement messages for the MT SMS. This results in the difference between the OA and SMSCA. The NDC is different because the operator has more than one NDC range

MCC in OA matches SMSCA, but:  
NDC in OA does not match SMSCA