



# Interconnect Signalling Security

David Maxwell  
Senior Working Group Director






# GSMA Interconnect Security Recommendations



Interconnect Signalling Security Recommendations

**FS.21**


Overview



IR.70: SMS SS7 Fraud  
IR.71: SMS SS7 Fraud Prevention  
IR.77: Inter-operator IP Backbone Security Requirements  
SG.22: SMS Firewall Best Practices and Policies

**SG.22**

SMS



SS7 and SIGTRAN Network Security

**FS.07**


SS7 Interconnect Security Monitoring and Firewall Guidelines

**FS.11**

SS7 Security Network Implementation Guidelines

**IR.82**

SS7



Diameter Interconnect Security

**FS.19**

LTE and EPC Roaming Guidelines

**IR.88**

Diameter



GTP Security

**FS.20**



## Business case for implementing countermeasures

- Protect customer -> Protect Brand  
-> Protect Business
- Network resilience
- Fraud protection
  - Including mobile financial services
- Support partners
  - Digital financial services using SMS or USSD





# Response & Controls Implementation

## Considerations

- Risk tolerance
- Skill sets needed
- Network / signalling node & architecture changes
- Upfront and ongoing costs
- Current vs. needed signalling visibility
- How might attacks evolve in future?

## Approaches

- Passive Monitoring
- Active Testing / Auditing
- SMS Home Routing
- Filtering on STPs and End Nodes
- Firewalls (SS7, Diameter, GTP)
- Advanced Analytics



## Communications

- All members
- CEO level
- Fraud and Security Group (FASG)
- Regional outreach

## Intelligence Sharing

- Telecommunication Information Sharing and Analysis Centre ([gsma.com/t-isac](https://gsma.com/t-isac))
- Submission and sharing of alerts amongst GSMA members

