fcs

federation of
communication
services

making sense of converging markets

FCS
Fraud Mitigation Standard
Specification

Contents:

1. Introduction

This document attempts to set out standards that compliant SIP trunking providers will adopt in order to be awarded an FCS fraud mitigation 'standard of excellence'. The purpose is to:

1. Provide users standard benchmarks whereby their fraud liability is mitigated.
2. Protect the critical reseller and client relationship by enabling end users and/or resellers to control access to destinations.
3. Creation of industry benchmarks.
4. Ensure that a reseller's entire client base retains service (as a reseller's total pre-payment or credit limit with a supplier could be reached resulting from fraud perpetrated to a single client).

2. Scope

The document is intended to detail minimum standards of fraud mitigation to be implemented by SIP trunking providers.

Traditional TDM telephony lies outside of the scope of this document.

It is assumed that:

a) a PBX is inherently vulnerable both physically and via external hacking or routing manipulation.
b) a PBX can only make outbound calls via SIP trunks, i.e.: traditional TDM connections are assumed to be outbound call barred (OCB)

A provider's infrastructure in terms of SIP proxying / session controlling, reliability and resilience, firewalls / gateway devices – including such aspects as blocking of IP addresses that show malicious signs (e.g.: port scanning, repeat connection attempts) – all lie outside of the scope of this document.

Finally, any requirements detailed in sections 6 Additional Best Practise Requirements and 8 Future currently lie outside of the scope of this specification.

3. Readership

The document current restricted to (a) the FCS anti-fraud panel, (b) TUFF, (c) any personnel these members invite to read. It is not for general publication or distribution until formally approved.

4. Definitions & Terminology

Term	Definition
Carrier	A telecoms entity capable of routing calls via their own network.
CDR	Call Detail Record.
FCS	Federation of Communication Services (http://www.fcs.org.uk/).
HTTPS	Hypertext Transfer Protocol Secure; is a communications protocol for secure network access.
IP	Internet Protocol.
ISDN	Integrated Services Digital Network, a voice, video and data communications standard supporting transfer rates of up to 64 Kb/s.
OCB	Outbound Call Barred.
PBX	Public Branch Exchange but has also come to mean a telephone system / switch.
Provider	Refer to 'Carrier'.
PSTN	Public Switched Telephone Network; traditional circuit-switched telephone networks.
SIP	Session Initiated Protocol, a communications protocol used over IP networks; the industry adopted VoIP standard.
TDM	Time Division Multiplexing but has also come to mean a collective term encompassing traditional analogue lines, PSTN and ISDN services.
TUFF	Telecommunications UK Fraud Forum (http://www.tuff.co.uk/)
VoIP	Voice over IP

5. Requirements

5.1. Service Registration

5.1.1. Overview

There are two common methods for registering SIP trunk services:

(a) authentication based
(b) IP addressed based

The former will only permit the routing of calls via a trunk typically registered by (i) domain/realm, (ii) user name and (iii) password; the later does not check domain/realm, user name and password but instead relies upon the provider only accepting traffic from a specific IP address (usually that of the PBX registering the SIP trunk).

5.1.2. Requirement

It is not proposed that either authentication based or IP addressed based are considered more favourable that the other with respect to fraud mitigation but it is a requirement that when IP address based authentication is employed that a password of suitable complexity (ref. to 5.3 Passwords) is used.

5.2. Channel Restriction

5.2.1. Overview

Appling reasonable client-specific limits to the permitted number of SIP trunk channels (concurrent calls) will lessen the chance, in the event of a breach, that numerous calls exceeding a client's typical usage could take place.

5.2.2. Requirement

The number of channels for a trunk must be limited and not permitted to be exceeded. For the avoidance of doubt, the number of channels, 'n', that are permitted must be actioned in real time such that at 'n+1' call is immediately barred.

5.3. Passwords

5.3.1. Overview

Passwords may be used to register a trunk or to gain access to an online portal or for some other related use.

Note that where a password is used to authenticate a trunk it is not proposed that it must be changed within a time period as this places an unnecessary support burden on PBX maintainers.

5.3.2. Requirement

Passwords may only be used if they are automatically system generated, or if user generated, to be valid with the following rules:

(a) must be a minimum length of 14 characters
(b) must contain at least one number and at least two letters
(c) must contain both an upper case letter
(d) must contain both a lower case letter

5.4. Mandatory Fraud Mitigation

5.4.1. Overview

It must not be possible to bypass a provider’s fraud-mitigation service.

5.4.2. Requirement

Fraud-mitigation must be implemented for every enlivened SIP trunk.

5.5. Limit Setting, Destinations (Basic)

5.5.1. Overview

A facility must be in place to set either outbound minutes-based, or cost-based, limits. This must at a basic level be able to be broken down by destination in order to mitigate fraud for certain types of calls without hampering normal business activity to other types of call. For example, a business may never wish to allow international calls and so would wish to bar such calls at the outset.

5.5.2. Requirement

The ability to set limits by either (i) outbound call minutes, and/or (ii) cost, broken down by at least the following destinations, headings:

(a) UK premium rate
(b) UK local / national
(c) international

For the avoidance of doubt, limit settings must be enforced in real time, not via any delayed post-processing of CDR’s: e.g. if a limit has been set for UK Premium Rate of 30 minutes, of which all 30 minutes has been used, a further call to a number in that destination will immediately be barred (for ‘gold’ and ‘silver’, refer to 7 Bands) or within a 10-15 minute period (for ‘bronze’, refer to 7 Bands).

5.6. Limit Setting, Destinations (Enhanced)

5.6.1. Overview

In addition to 5.5 Limit Setting, Destinations (Basic) above, setting limits at a more granular level must be provided. This must contain are more detailed breakdown by destination (again, in order to mitigate fraud for certain types of calls without hampering normal business activity to other types of call). For example, a business may wish to call international numbers, including numbers in the African subcontinent for example, but not to a particular country within it, for example Burundi.

5.6.2. Requirement

The ability to set limits by either (i) outbound call minutes, and/or (ii) cost, broken down by at least the following destinations, headings:

(a) UK premium rate
(b) UK local / national
(c) UK mobile
(d) UK non-geographic
(e) UK special / other
(f) UK directory enquiries
(g) UK international operator
(h) international regions (Africa, Asia, Australasia, Europe, North America, South America)
(i) country within international region
(j) satellite/other

For the avoidance of doubt, limit settings must be enforced in real time, not via any delayed post-processing of CDR's: e.g. if a limit has been set for UK Premium Rate of 30 minutes, of which all 30 minutes has been used, a further call to a number in that destination will immediately be barred (for 'gold' and 'silver', refer to 7 Bands) or within a 10-15 minute period (for 'bronze', refer to 7 Bands).

In addition, advised additional best practise will be to implement further granularity within country where possible to default/landlines, mobile phone operator(s).

5.7. Limit Setting, Period (Basic)

5.7.1. Overview

The minutes-based or cost-based limits must apply over a period of time, as a minimum, monthly.

5.7.2. Requirement

Limits must be able to be set for a period no longer than monthly. Limits must automatically reset after the period has elapsed.

For the avoidance of doubt, limit settings must be enforced in real time, not via any delayed post-processing of CDR's: e.g. if an overall monthly limit has been set of 1,000 minutes, of which all 1,000 minutes for that month has been used, a further call will immediately be barred (for 'gold' and 'silver', refer to 7 Bands) or within a 10-15 minute period (for 'bronze', refer to 7 Bands).

5.8. Limit Setting, Period (Enhanced)

5.8.1. Overview

In addition to 5.7 Limit Setting, Period above, a further enhance requirement is to divide the minutes-based or cost-based limits into a daily proportion such that a whole period's allocation could not be used within one day's worth of fraudulent activity, only one day's worth of the monthly limit can be used in any given day.

Notwithstanding, in order not to impinge upon business activity, the bespoke allocation of a daily proportion of an overall monthly limit should be employed to cater for businesses that have certain days of higher usage, with lower usage on other days.

5.8.2. Requirement

Limits must be able to be set for a period no longer than monthly but divided into daily proportions of the overall monthly limit. Limits must automatically reset after the period has elapsed.

For the avoidance of doubt, limit settings must be enforced in real time, not via any delayed post-processing of CDR's: e.g. if an overall monthly limit has been set of 1,000 minutes, equating to a daily limit of circa. 30 minutes per day, of which all 30 minutes for that month has been used, a further call will immediately be barred (for 'gold' and 'silver', refer to 7 Bands) or within a 10-15 minute period (for 'bronze', refer to 7 Bands)

It must also be possible to set a bespoke / exception daily limit.

5.9. Limit Setting, Out of Hours Limits

5.9.1. Overview

It is widely acknowledged that most fraudulent activity takes place outside of usual business hours. This must be recognised in fraud mitigation modules.

5.9.2. Requirement

The ability to be able to reduce minutes-based or cost-based limits outside of the specified working hours of the end client business. This must be able to be defined by the reseller who has the option to set client-specific working hours.

For the avoidance of doubt, limit settings must be enforced in real time, not via any delayed post-processing of CDR's: e.g. if an overall monthly limit has been set of 1,000 minutes, of which 500 minutes are permitted out of hours, of which all 500 out of hours minutes have been used, a further out of hours call will immediately be barred (for 'gold' and 'silver', refer to 7 Bands) or within a 10-15 minute period (for 'bronze', refer to 7 Bands)

5.10. Cascading Templates / Profiles

5.10.1. Overview

The provider must be able to set reseller-specific limits for underlying resellers for a variety of reasons (e.g. the result of credit check / credit scores). In turn, reseller must be able to set client-specific limits for similar reasons.

5.10.2. Requirement

Appropriate logic must be applied such that a client cannot create/set limits greater than those set by the reseller and similarly the reseller cannot create/set limits greater than those set by the provider.

In addition end clients must have the ability to manage and control their own cost or minute based limits.

5.11. Automatic Barring, Limit Breach

5.11.1. Overview

Minutes-based or cost-based limits must be set with a view to bar further outbound calls when the limit is reached; this must be immediate and not based upon notification and subsequent action, or upon processing CDR's after the event.

5.11.2. Requirement

Automatic barring of calls must take place when the minutes-based or cost-based limits are reached.

For the avoidance of doubt, barring when a limit has been breached must be real time (for 'gold' and 'silver', refer to 7 Bands) or within a 10-15 minute period (for 'bronze', refer to 7 Bands). Barring in the case of a limit break must not be dependent on any delayed post-processing of CDR's.

5.12. Notifications/Alerts

5.12.1. Overview

In order to take both preventative and corrective action, real time notifications are to be employed to provide an alert in the event that a minutes-based or cost-based limit is reached and/or is nearing being reached. In addition, for audit purposes, any substantive changes to limits must also trigger an alert.

5.12.2. Requirement

It must be possible to define the following notifications:

(a) limit is nearing being reached. This can be sent via a set or user defined percentage, cost value or minutes value.
(b) limit has been reached. This can be set via a set or user defined percentage, cost value or minutes value.
(c) limit has been created, changed or deleted.
(d) the information contained in the notifications must detail as a minimum (i) client/trunk, (ii) which limit has been reached / is nearing being reached / has been created, changed or deleted.

Notifications must be configured to be sent via:

(e) SMS/text to one or more numbers.
(f) email to one or more email addresses.

For the avoidance of doubt, notifications/alerts must be real time.

In addition end clients must have the ability to manage and control their own notifications/alerts.

5.13. Logging/Reporting

5.13.1. Overview

In addition to real-time notification/alerts, details of limit configuration and of limits being reached must be able to be viewed historically.

5.13.2. Requirement

It must be possible to historically view:

(a) limit has been reached.
(b) limit has been created, changed or deleted.
(c) the information contained in the log must detail as a minimum (i) client/trunk, (ii) which limit has been reached / is nearing being reached / has been created, changed or deleted.

This information must be able to be provided to FCS/TUFF on request in the event of a breach / complaint.

5.14. Online Portal, Access

5.14.1. Overview

Where the requirements of this specification are fulfilled by providing access to an online portal, this portal access must be secure, given that unauthorised access to it could undermine all other requirements.

5.14.2. Requirement

Online portal access:

(a) must be via HTTPS or other similarly secure access method.
(b) portal user account password is of suitable complexity (ref. to 5.3 Passwords).

In addition, advised additional best practise will be to implement dual factor authentication access.

5.15. Online Portal, User Permissions

5.15.1. Overview

Further to 5.14 Online Portal, Access, it must be possible to allow user access to be non-ubiquitous: a user who is required portal access in order to manage one account/trunk (or a subset of accounts/trunks) must not have access to other accounts/trunks. 'Admin' level access must not be provided to every portal user; accounts must be able to be permissioned.

5.15.2. Requirement

'Admin' level access must not be provided to every portal user and accounts must be able to be permissioned either by (a) allocating user permissions to manage one account/trunk (or a subset of accounts/trunks), and/or (b) allocating user permissions to enable functional based restrictions (e.g. a user may have ubiquitous access if they can only view settings, not amend them.

6. Additional Best Practise Requirements

6.1. Introduction

Further best practise requirements are listed in this section. These currently lie outside of the scope of this specification (typically for reasons such as they cannot at this time be adequately defined).

6.2. Automatic Barring – Algorithm

6.2.1. Overview

Whilst limits are considered to be the best method to mitigate fraud, automatic detection algorithms are advised in order to adopt a 'belt and braces' approach.

6.2.2. Requirement

Implement automatic detection algorithms to automatically detect:

(a) Unusual / repeat / out of context calls to 'exotic' (e.g. high cost) UK destinations.
(b) Unusual / repeat / out of context calls to 'exotic' (e.g. high cost) international destinations.

Upon detection of such calls, call to that region must be automatically barred.

7. Bands

The compliance or otherwise to the requirements detailed in section are placed in 'bands'; this will allow the lion share of providers to warrant the award of the standard of excellence and it will also allow providers to be distinguished by their level of compliance.

Section / Requirement	Gold	Silver	Bronze
5.1 Service Registration	✓	✓	✓
5.2 Channel Restriction	✓	✓	✓
5.3 Passwords	✓	✓	✓
5.4 Mandatory Fraud Mitigation	✓	✓	✓
5.5 Limit Setting, Destinations (Basic)	✓	✓	✓
5.7 Limit Setting, Period (Basic)	✓	✓	✓
5.11 Automatic Barring, Limit Breach	✓	✓	✓
5.13 Logging/Reporting	✓	✓	✓
5.6 Limit Setting, Destinations (Enhanced)	✓	✓	
5.8 Limit Setting, Period (Enhanced)	✓	✓	
5.9 Limit Setting, Out of Hours Limits	✓	✓	
5.12 Notifications/Alerts	✓	✓	
5.14 Online Portal, Access	✓	✓	
5.10 Cascading Templates / Profiles	✓		
5.15 Online Portal, User Permissions	✓		

8. Future Requirements for Consideration

This section details future requirements. These currently lay outside of the scope of this current specification but are detailed in order to start to plan a 'roadmap' of future requirements for review.

8.1. Blacklisting

A logical next step regarding fraud mitigation is to manage known-to-be, and/or suspected to be, fraudulent numbers.

8.1.1. Blacklisting, Provider

It must be possible to bar certain numbers with the effect that any call attempted via any trunk registered on their service is automatically barred.

8.1.2. Blacklisting, Inter Provider File Sharing

Further to 8.1.1 Blacklisting, Provider, there must be an industry-recognised format and method of sharing blacklisted numbers between carriers/providers. Such providers being potentially authorised to share information with any national fraud database(s).

8.1.3. Blacklisting, TUFF / FCS Approval

Further to 8.1.2 Blacklisting, Inter Provider File Sharing, in order to provide control and prevent potential misuse, blacklisted number must be able to be marked as verified in some way by FCS / TUFF.

8.2. Trunk Encryption

Whilst not mandatory, trunk encryption, such as TLS, is preferred where it is possible.

9. Document Version / Change Control

Version	Date, Author	Details
0.1	23/12/2014, SR	Initial draft.
0.2	20/01/2015, SR, JR	Changes based on review, inclusion of bands, inserted additional best practices section.
0.3	23/02/2015, SR, JR	Removed ‘kite mark’ from title and elsewhere. Re. 5.11 Automatic Barring, Limit Breach: added in scope to bar with 10-15 minute period for ‘bronze’ level. (Also sections 5.5, 5.6, 5.7, 5.8 and 5.9.) Re. 5.8 Limit Setting, Period (Enhanced): amended to cater for businesses that have days of higher usage.