



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
61/422,574	12/13/2010		220	RALEP045+		

CONFIRMATION NO. 9531

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FILING RECEIPT



OC000000045344810

Date Mailed: 01/10/2011

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Gregory G. Raleigh, Woodside, CA;

Power of Attorney:

Michael Schallop--44319

If Required, Foreign Filing License Granted: 01/07/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/422,574**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

SECURITY AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international

patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Attorney Docket No. RALEP045+

PROVISIONAL APPLICATION FOR
UNITED STATES PATENT

SECURITY AND FRAUD DETECTION FOR DEVICE
ASSISTED SERVICES

By Inventors:

Gregory G. Raleigh
Woodside, CA
A Citizen of the United States

Assignee: Headwater Partners I LLC

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Telephone 408-973-2585

ItsOn Security and Fraud Overview

Revision 1.1

December 10, 2010



ItsOn, Inc. and Headwater Partners



Document Revision History

Revision Date	Version	Description
11/29/2010	1.0	Created Document
12/9/2010	1.1	Revised with internal feedback

Disclaimer

This document contains forward-looking statements based on current expectations, forecasts and assumptions of the Company that involve risks and uncertainties. Forward looking statements are subject to risks and uncertainties associated with the Company's business that could cause actual results to vary materially from those stated or implied by such forward-looking statements.

This document is intended for use as a guideline and for information purposes only, and represents ItsOn, Inc's current view of its product direction. This information is subject to change without notice.

As ItsOn, Inc. develops product using an Agile development process, any one of the milestones, features, release products, release periods or versions could change. None of the information herein should be interpreted as a commitment on the part of ItsOn, Inc.



Contents

Document Revision History	2
Disclaimer	2
Introduction: Layering in Security.....	5
Building Security into the Service Processor.....	5
Building Security into the Service Processor/Controller communications	7
Security Practices	7
Building Security into the MSP.....	8
Physical Security.....	8
SAS70 Type 2 Certified	12
Log monitoring and management (SEM and SIM).....	13
Vulnerability Assessments	13
Network Security	13
Ensuring continued security	15
FRAUD	16
ACTIVE SERVICE PROCESSOR VALIDATION	18
SGSN Notification of Start/Stop Data Session	19
GGSN Notification of Start/Stop Data Session.....	21
Service Processor/Service Controller Authentication.....	23
SC Receives UDRs From SP After Receiving “Data Session Stopped” Trigger From Network	24
Service Controller Receives CDRs But Does not Receive UDRs	24
SC Receives CDRs and UDRs But the Usage Counts Don’t Align	25
SC Receives CDRs and UDRs but SC Detects Usage Over Charging Policy (CP) Limit(s).....	25
SC Receives UDRs but Charging Codes do not Correspond to CP(s) for Current Active Services.....	26
SC receives CDRs and UDRs, counts align, but usage velocity within a Service Component or Service Activity is greater than rate limit(s) set via CP.....	26



SC receives CDRs and UDRs, counts align, but usage velocity at the Service Activity or Service Component level deviates “significantly” from average user usage velocity.....	27
CDR-based Verification Algorithm	28
FDR-based Verification Algorithm	29
Behavior-based Verification Algorithm.....	30
Production Deployment considerations	31
Fraud Analysis Considerations	32
Fraud Sampling	33
ICR & CDR Fraud Analysis Flow	35
FDR Fraud Analysis Flow	36



Introduction: Layering in Security

The key to security for many years has been a layered defense or defense in depth. Defense in depth is a military strategy, it seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defense in depth relies on the tendency of an attack to lose momentum over a period of time or as it covers a larger area. The idea of defense in depth is now widely used to describe non-military strategies.

This is the approach ItsOn has taken realizing that no one system is completely impenetrable. The Android device like many other phones is not completely secure and for a skilled in the art hacker quite penetrable. The client is obviously the first point of concern in any network. We have put considerable thought in how to detect if our software has been tampered with or compromised. Our approach is to detect this both on the handset from within and at the network or Service Controller. This document outlines the steps we have taken to secure the Service processor on the handset to prevent tampering and also to detect fraud using the network in conjunction with the Service Controller. In reviewing this document you should also keep in mind that Android also affords us a level of security also which details can be found here:

<http://developer.android.com/guide/topics/security/security.html>

It should be noted that ItsOn will be performing penetration testing of all the systems and as such the architecture could change over time as we strive to improve our defense in depth.

Building Security into the Service Processor

The Client software will have a signed manifest which lists all files in the software distribution. The listed files will also be paired with a SHA1 hash. The manifest itself will be signed with a private/public key rsa strength key combination. This is standard Android application security. Once installed in the OEM distribution Android enforces that the app can only be upgraded if signed with the same key. This will make it difficult to install over the top.



The private key will be kept only within ItsOn's build environment and used during the build process. Access to the ItsOn build environment will be limited to a small number of named personnel. The private key will only be held offsite in a secured environment beside the build server.

The public key will be shipped with the ItsOn binaries and in the default distribution as part of the framework.

Figure 1.0 Integrity checking

Upon loading of the APK it will query the additional ItsOn framework code to perform a Manifest check. It will then perform an integrity check of the ItsOn apk. If the apk has integrity it is allowed to run and then will validate the ItsOn and IOInterface kernel objects. If the ItsOn apk is running and reporting data usage then it is considered that the system has not been tampered with. If the ItsOn apk is not running and there is data usage this is a standard fraud case. Thus putting the device in a fraud state for data rating/charging.

This integrity check will happen every time the apk is loaded for execution and every boot.

The kernel objects will be named in such a way that it is not obvious what they are. So user who has rooted the device cannot identify them easily.

Intermediary storage for service processor will be encrypted



ItsOn Client Java code will also be obscured to prevent decompiling or reverse engineering.

Building Security into the Service Processor/Controller communications

The SP/SC communication will happen over TLS encrypted data pipe. We will use RSA/SHA cyphersuite. The SP/SC systems will use mutual authentication (client-side and server-side certificates). We will get the client side certificate installed as part of an activation/bootstrapping algorithm on the client when it first connects. ItsOn would get its certificates issued by a standard certificate authority.

We will either encrypt or add a message digest to messages in transit. This would be implemented in the communication layer at the client and server. Session initiation will be much like in TLS, after the authentication occurs the server will send the client a session key that would be used to encrypt/sign all data exchanged (in both directions) for that session. Client to server communication sessions typically only last a few seconds at most. There are no persistent sessions.

Security Practices

ItsOn will also perform source code audits using tools like RATS or Fortify360 to ensure that coding vulnerabilities are prevented.

ItsOn will detect Rogue application by comparing hashes of known good applications. These hashes will be held with the service activity and pushed down to the SP from the SC.

Penetration testing of the Service Processor software will also be carried out on a regular basis. The scope of which will be determined in contracts.



Building Security into the MSP

ItsOn will be using a managed service partner (QTS) to host the Service Controller/Gateway and SDC.

Physical Security

Physical security procedures are safeguards enacted to ensure only authorized individuals have access to various physical locations, such as the data center, warehouse, computer operational centers, and any other critical areas.

Exterior Security Elements

The Santa Clara facility meets all local, state, and federal regulatory requirements for building codes and has been constructed of post and beam framework with the exterior of the walls made of tilt up concrete. The building was acquired by QualityTech in 2007 and has been modified accordingly to enable the secure delivery of data center services. The facility has a total of approximately 67,200 square feet of usable space, with 20,000 square feet allocated to an 18" raised floor data center area on the first floor of the building, and 19,500 square feet allocated to a 24" raised floor data center area on the second floor of the building. The remaining usable space is allocated to office areas, storage space, and infrastructure accommodations.

Exterior lighting is appropriate for adequate visibility outside the facility during night hours, helping to ensure potential intruders are unable to approach the building unseen. Grounds and vegetation surrounding the building are appropriately maintained to prevent potential intruders from shielding or hiding themselves. Exterior windows leading into the data center area on the first floor are protected by 1/4" thick Kevlar panels to prevent the glass from being penetrated by projectiles or by other forceful means. Windows leading into the data center area on the second floor are protected by 5/8" thick sheetrock. The exterior of the building is also protected by strategically placed security surveillance cameras for monitoring and recording of external building activity.

Roof access to the main two story portion of the facility is accommodated from the inside of the building via a ladder in a stairwell. Access to the stairwell is protected by a badge reader and only authorized personnel are permitted in that area. The roof hatch at the top of the ladder is latched from the inside so it cannot be opened from the outside, and is tied to the building alarm system to notify security personnel when the hatch is open. In



addition, the building has an expansion wing that is one story high with roof access gained from the outside within the courtyard area located adjacent to the expansion wing. The courtyard houses the facility's backup generators, fuel for the generators, and other electrical & environmental infrastructure, and is surrounded by cement walls and wrought iron fencing. Access to the courtyard area can be gained from inside or outside the facility, and is protected by badge readers and biometric readers to ensure only authorized individuals can gain entry to the courtyard area.

Interior Security Elements

The Santa Clara facility is manned by QualityTech security staff 24x7, with a minimum of two (2) security personnel onsite at all times during business hours. The security team performs regularly scheduled rounds looking for anything unusual, suspicious, or out of the ordinary, and surveillance cameras are placed strategically throughout the building for monitoring and recording of internal building activity. To facilitate the secure shredding and disposal of sensitive documents, the Santa Clara facility maintains a contract with a local vendor.

The Santa Clara security team is responsible for a variety of critical activities and functions, including but not limited to:

- Controlling and monitoring data center access, prevention of unauthorized access
- Ensuring compliance with access procedures
- Controlling the movement of items removed via the facility main entry point, loss prevention
- Issuance and retrieval of ID access badges
- Administration of the computerized access control system
- Administration and maintenance of physical security systems
- Monitoring of, response to, and resolution for security alarms
- Conducting scheduled and unscheduled security, fire, and safety patrol inspections
- Enforcement of policy to prevent unauthorized photography
- Enforcement of policy prohibiting food or drink in the data center areas
- Escorting of visitors without access credentials
- Assisting customers with cage lockouts
- General compliance with security policies and procedures

The data center area raised floor on the first floor of the facility is secured with heavy tiles made of concrete, while on the second floor the data center area raised floor is secured with hollow core tiles to reduce the weight strain on the second floor. No data center entry/exit is possible from under the raised floors in either data center area. The area under the raised floor of the data center area on the first floor is used to deliver power,



network cabling, and cooling to customer cabinets and cages. On the second floor, the area under the raised floor of the data center area is for the delivery of power and cooling while accommodations for network cabling are provided overhead. Cabinets and cages are constructed of metal and are of appropriate strength and rigidity to secure customer equipment from unauthorized access. All data center cabinets and cages in the facility are fastened to the floor, are clearly labeled, and are inspected periodically to ensure their proper physical condition. All cabinets and cages are secured with traditional lock & key mechanisms with keys safeguarded by the security team, and a select few are also equipped with electronic badge readers at the request of customers occupying those environments. Independent holding rooms are present on both the first and second floors of the facility and must be cleared prior to accessing the data center areas on those floors.

Access Control Elements

General access to the Santa Clara facility is gained via the front door, which is open for public access during normal business hours. The front door remains locked during non business hours and is secured by an electronic badge reading system. All other external doors remain locked when not in use, and are protected by badge readers and/or traditional lock & key. The Santa Clara facility is equipped with an electronic badge reading system to prevent unauthorized access to all areas of the building, managed and maintained by the security team. Each area of the building is considered a separate security zone and is configured individually within the electronic badge reading system for access to that specific area.

All visitors to the Santa Clara facility must have their visit logged by the security team, and must be escorted at all times unless they have access rights that do not require an escort. All persons requiring unescorted access to the Santa Clara facility must have an electronic access identification badge issued to them by the security team. Each electronic access badge is unique to the individual so that logging of access by electronic badge readers can be tied to specific persons. Electronic access badges are issued to customers by the security team under a structured enrollment program requiring a government issued picture ID such as a driver's license or passport. The type and duration of access is determined by the customer's access needs and the security team assigns access rights based on the specific parameters.

In addition to the electronic badge reading system the facility is equipped with biometric iris scanning devices and biometric fingerprint reading devices in select areas throughout the facility, managed and maintained by the security team. Like the electronic badge reading system, each area of the building protected by these biometric devices is considered a separate security zone and is configured individually within the systems for access to that specific area. Customers have their biometric attributes configured in these systems by the security team in accordance with customers' access requirements.



Access to the data center areas on both the first and second floors can only be gained by clearing holding rooms that require two-factor authentication. Individuals requiring access to a data center area first use their electronic access badge and their biometric fingerprint to gain entry to the holding room, and then have their iris scanned by an iris reader inside the holding room to gain access to the applicable data center floor.

Monitoring Elements

The facility has in place forty (40) fixed position security cameras for video surveillance of critical areas in and around the building. The exterior and interior of the building are continuously monitored by cameras placed strategically for optimum coverage of critical areas, with images from the security cameras being displayed on two (2) 42 inch monitors each with sixteen (16) split screens for viewing multiple security cameras simultaneously. The monitors are maintained in the Security Office and are viewed by a member of the security team at all times when not engaged in other security duties.

All video surveillance streams are channeled through a digital video recorder (DVR) that archives the video captured by the security cameras. The DVR is located in a secure cabinet in the first floor data center and is accessible only to QualityTech security personnel and data center technicians. Video archives are maintained online for a period of one week before they are transferred to tape. Tape archives of the captured video are maintained for a period of ninety (90) days before they are overwritten, and the entire video surveillance system is protected by an uninterruptable power supply in the event there is a loss of power.

Fire, Life, Safety Elements

The Santa Clara facility is equipped with a comprehensive set of controls to ensure adequate protection as it relates to fire, life, and various safety elements. A central monitoring control panel is located in the Security Office that displays the status of various fire, life and safety elements throughout the facility. The central monitoring control panel aggregates data from several other control panels in various locations of the facility that are tied to their particular elements. In addition to onsite monitoring efforts undertaken by QualityTech security personnel, a third party security service provides remote monitoring of critical fire, life and safety elements including fire and smoke detectors, HVAC alarms, water sensors, and annunciators. The remote monitoring service will contact Santa Clara personnel in accordance with an escalation contact list in the event an alert is triggered by any critical fire, life or safety element.

A wet pipe fire suppression system protects the common office areas of the facility as well as the generator area in the adjacent courtyard. All other areas within the facility on both floors, including the data center areas, mechanical & electrical rooms, and other



infrastructure areas, are protected by a pre-action dry pipe fire suppression system. A common water supply feeds the fire suppression system on both the first and second floors, however, the system operates independently on the two floors and an alert condition that causes the dry pipes to fill on the first floor does not cause the dry pipes to fill on the second floor, and vice versa. Leak detectors are located under the CRAC units on both floors to ensure that any water escaping from the fire suppression system or CRAC units is detected in a timely manner. The entire fire suppression system is inspected annually by the local Fire Marshal to ensure its operability and compliance with fire codes.

In addition to the pre-action dry pipe fire suppression system, a Fenwall FM 200 system is in place in the data center area on the first floor of the facility that provides an additional level of fire protection in the first floor data center. The FM 200 system is a chemical based waterless fire suppression system that deploys quickly without leaving behind any residue or particulates, and operates independently from the water based pre-action dry pipe fire suppression system. The fire suppression system in the second floor data center area is enhanced by the implementation of Very Early Smoke Detection Apparatus (VESDA) type smoke detectors. The VESDA smoke detectors provide enhanced protection from fire conditions by reading air samples with highly sensitive laser technology that detects smoke particulates during the earliest stages of a fire condition. The second floor data center area incorporates three (3) VESDA air sampling control panels to ensure adequate coverage of the data center space. Fire extinguishers are positioned strategically throughout both floors of the facility to aid in the suppression of small incipient fires.

SAS70 Type 2 Certified

Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 ("SAS 70 Audit") is widely recognized, because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on the effectiveness of internal control over financial reporting. *(For more information see www.sas70.com)*

Quality Technology Services has engaged NDB, LLP (*Formerly Dupont & Morgan, LLP*) as the exclusive SAS 70 audit provider for QualityTech data center facilities in the continental



US. NBD is an international accounting and consulting firm that concentrates on providing high quality, cost-effective services to meet the challenges of today's complex and competitive business environment. NBD's emphasis on SAS 70, in particular their years of experience working in and with data center providers, was an important factor in our decision to engage NDB.

Log monitoring and management (SEM and SIM)

Splunk is used to implement real-time monitoring and alerting of incidents and attacks. System and application log files are monitored to find security and compliance issues as well as maintaining an audit trail of system activity.

Vulnerability Assessments

ItsOn will utilize QualysGuard to perform regularly scheduled vulnerability assessments. QualysGuard provides a robust scanning service that analyzes the security of your network devices by referencing an inventory of thousands of known vulnerabilities covering all major operating systems, services and applications.

Network Security

In addition to the MSP security ItsOn will also take the following precautions to protect data and systems within the Service controller etc.

- Front-facing DMZ implementation
 - External services are isolated in a restricted perimeter network (a.k.a. DMZ) and separated by functional classification.
- VLAN isolation of servers by function:
 - 3 DMZ VLANs
 - The device services VLAN allows traffic from a range of device IPs to a limited number of application specific IP ports.
 - The web portal VLAN allows SSL traffic to Apache servers that proxy to the Service Design Center. Traffic can be restricted to a specific range of source IPs but that requirement has not been defined.



- The carrier services VLAN allows traffic from the carrier for the purpose of file transfers and/or accounting record streams. This traffic is expected to be encapsulated in a secure VPN tunnel over the Internet from the carrier.
- Application VLAN
 - The application VLAN protects the business logic processors from the external traffic.
- Database VLAN
 - The database VLAN isolates the database servers and restricts traffic to that coming from the application servers.
- ItsOn Ops VLAN
 - The Ops VLAN separates ItsOn management and monitoring servers from the business layers.
- MSP Backup/Monitoring VLAN
 - The MSP uses a dedicated VLAN for monitoring and backup traffic.
- Inter-VLAN security via ACL
 - ACLs are used to restrict traffic between VLANs.

Host Level:

- No shared logins
 - Users are required to maintain separate and secure logins
- Remote logging and monitoring of access
 - Systems logs are mirrored to a remote server for real-time analysis to identify unauthorized access

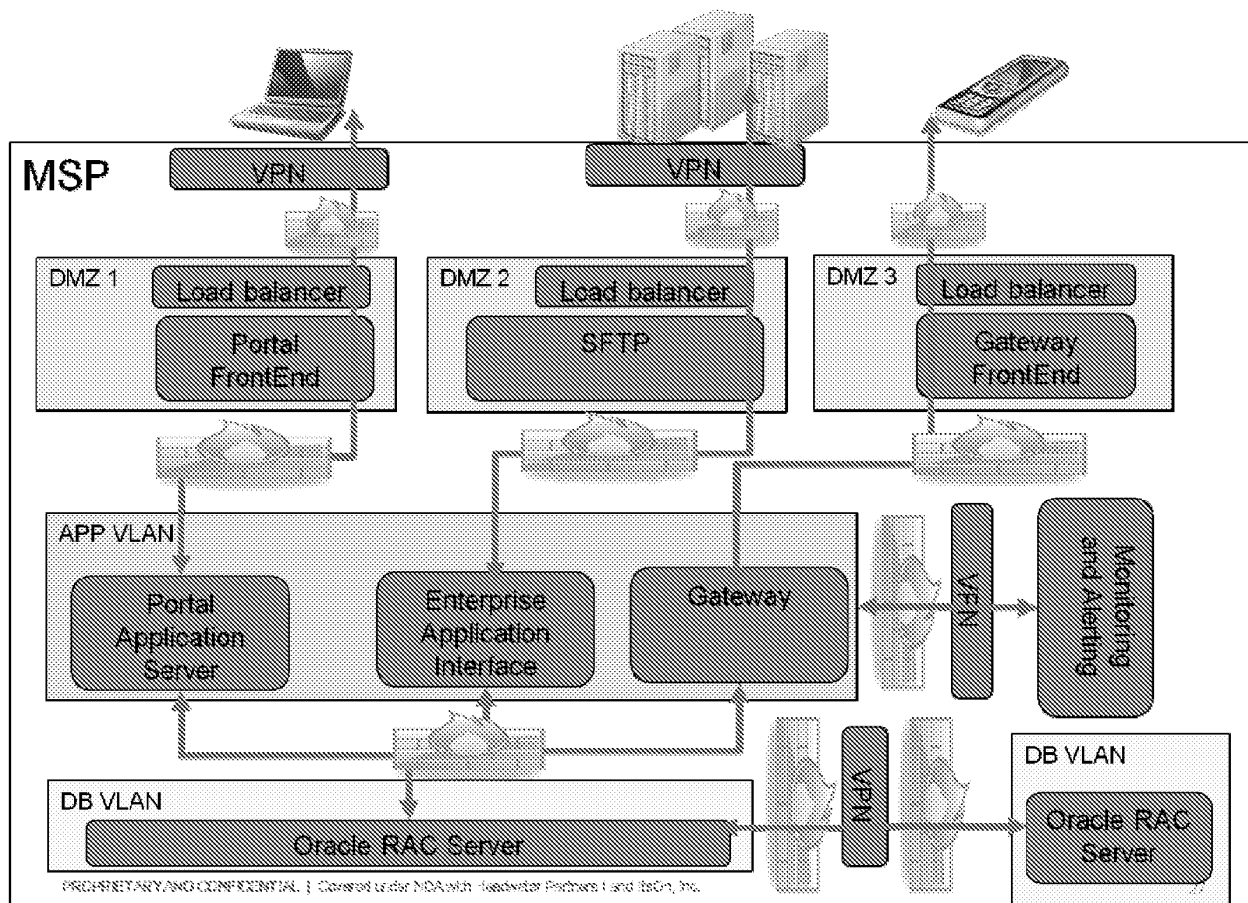


FIGURE 2 ItsOn NOC security layout

Ensuring continued security

ItsOn will work with the MSP to implement vulnerability scanning for both the server and application vulnerabilities using QualysGuard. This tool will be run on a frequent basis (TBD). Results will be analyzed and corrective action taken within the contracted days.

ItsOn will also ensure that any patching of the software required for security purposes is also applied in the contracted timeframe. The MSP actively monitors OS related patch releases. OS patch updates are scheduled based on severity and applicability.



ItsOn will also use a product like McAfee Secure or QualysGuard to perform vulnerability scanning of the Service Control Center to ensure that customer data is safe from internal and external threat. This will ensure that SQL injection or XSS scripting is not an issue.

Penetration testing can also be carried out on a predetermined timescale based on contract.

FRAUD

These following bullets outline the fraud detection methods ItsOn will use and the fraud event it will capture:

- Service Processor (SP) doesn't attempt authentication within acceptable window after the Service Controller (SC) receives "data session started" indication from the network
 - ❖ Cause: SP disabled, SIM in a non-ItsOn enabled device (non-fraud)
- SP fails authentication with SC
 - ❖ Cause: Invalid credentials, device spoofing
- SC receives Usage Data Records (UDR) from SP after receiving "data session stopped" trigger from the network
 - ❖ Cause: Device spoofing
- Service Controller receives CDRs but does not receive UDRs
 - ❖ Cause: SP disabled, SIM in a non-ItsOn enabled device (non-fraud, unless SP has authenticated with SC during this data session)
- SC receives CDRs and UDRs but the usage counts don't align
 - ❖ Cause: SP tampering
- SC receives CDRs and UDRs but the UDRs indicate usage over Charging Policy (CP) limit(s)



❖ Cause: SP tampering

- SC receives UDRs but charging codes do not correspond to CP(s) for current active services

❖ Cause: SP tampering, device spoofing

- SC receives CDRs and UDRs, counts align, charging codes are correct, but data is miss-categorized (needs FDRs to corroborate)

❖ Cause: SP tampering

- SC receives CDRs and UDRs, counts align, but usage velocity within a Service Component or Service Activity is greater than the rate limit(s) set via the Control Policy

❖ Cause: SP tampering

- SC receives CDRs and UDRs, counts align, but usage velocity at the Service Activity or Service Component level deviates “significantly” from average user usage velocity

❖ Cause: SP tampering, Service Activity/Component usage patterns changing (e.g., service adds streaming content) (non-fraud)

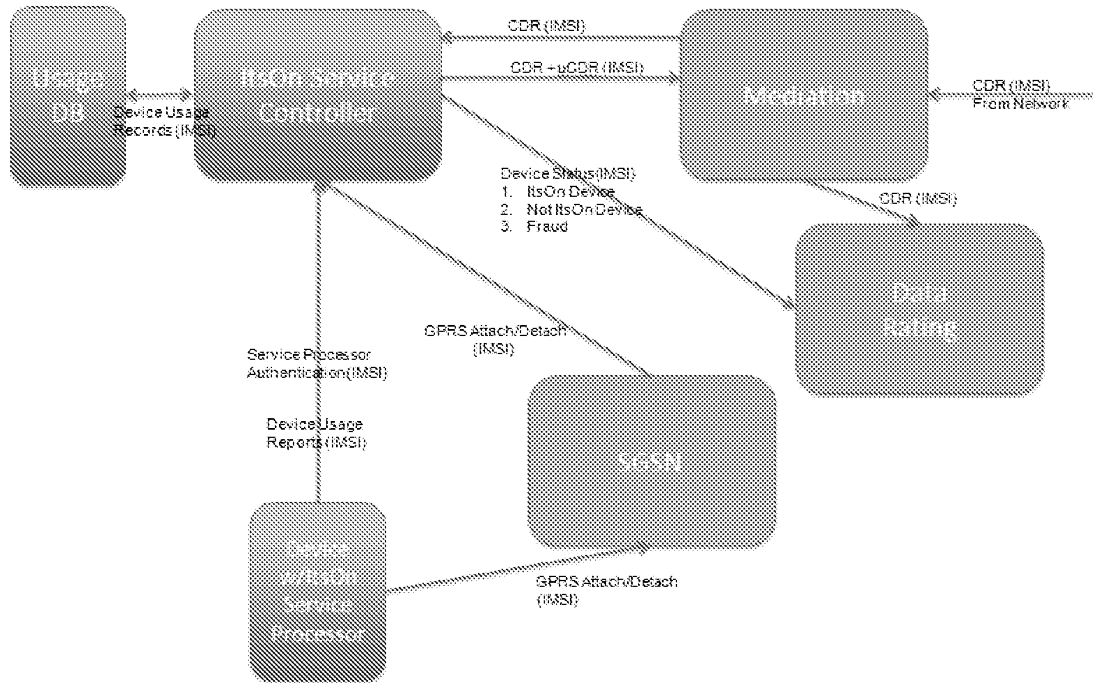


ACTIVE SERVICE PROCESSOR VALIDATION

- Service Controller receives a start session message from the network
 - Could be a “Start Accounting” RADIUS message from a GGSN, AAA or PDSN, or successful “GPRS Attach” notification from an SGSN
- Service Controller sets an “Expecting Service Processor Login” timer
- If Service Controller successfully authenticates the Service Processor within the timer interval, Service Processor is deemed to be running and valid.
- If the Service Controller does not successfully authenticate the Service Processor within the timer interval, it is assumed that: 1) the device does not contain a Service Processor; or 2) the Service Processor on the device has been disabled.
 - When this event occurs, the Service Controller can either 1) trigger to the network to charge for usage at “standard” bulk rates; or 2) specify a “standard” bulk rate charging code in the CDRs sent to data mediation
- Following slides depict sample high-level implementation options of this functionality in a GSM/GRPS core data network



SGSN Notification of Start/Stop Data Session



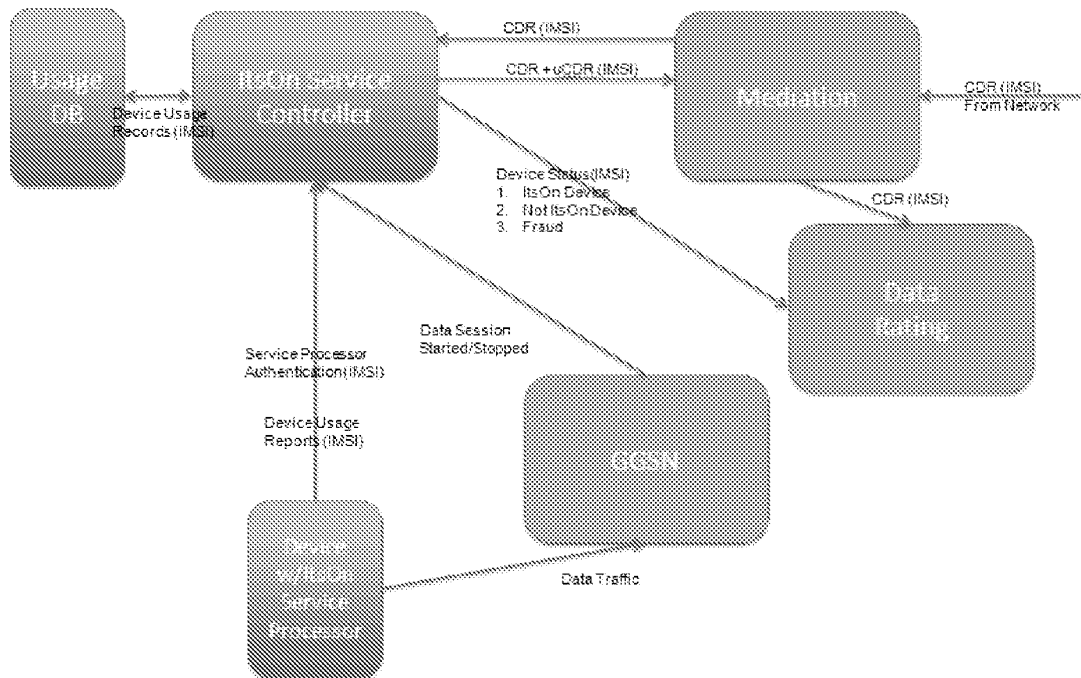
- Device attempts data session and sends GPRS Attach to SGSN
- SGSN notifies ItsOn Service Controller that the device has started a data session
- ItsOn Service Controller waits for a pre-determined time (e.g., one minute) to receive a login/authentication request from the ItsOn Service Processor on the device
 - If the ItsOn Service Controller sees the request, it sends a notification to Data Rating to indicate that the device has an ItsOn Service Processor and expect uCDR reports via Data Mediation.
 - If the ItsOn Service Controller does not see the request, it sends a notification to Data Rating to indicate that the device does not have an ItsOn Service Processor and to process usage based on carrier CDR reports.
- ItsOn Service Controller receives usage reports from the ItsOn Service Processor



- If ItsOn Service Controller does not receive usage reports from the device based on time/usage intervals, it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- Data Mediation sends CDRs to ItsOn Service Controller.
- ItsOn Service Controller queries its device usage database for uCDRs for the device.
- ItsOn Service Controller compares carrier CDR data usage byte counts vs. uCDRs.
 - If ItsOn Service Controller determines that the carrier usage counts don't match the uCDR usage counts (e.g. Fraud), it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- ItsOn Service Controller sends carrier CDR and ItsOn uCDRs to Data Mediation.
- When GPRS Detach is received by the SGSN, SGSN sends a notification to the ItsOn Service Controller that the device data session is closed.



GGSN Notification of Start/Stop Data Session



- Device starts data session.
- GGSN recognizes start of a new data session.
- GGSN notifies ItsOn Service Controller that the device has started a data session
- ItsOn Service Controller waits for a pre-determined time (e.g., one minute) to receive a login/authentication request from the ItsOn Service Processor on the device
 - If the ItsOn Service Controller sees the request, it sends a notification to Data Rating to indicate that the device has an ItsOn Service Processor and expect uCDR reports via Data Mediation.



- If the ItsOn Service Controller does not see the request, it sends a notification to Data Rating to indicate that the device does not have an ItsOn Service Processor and to process usage based on carrier CDR reports.
- ItsOn Service Controller receives usage reports from the ItsOn Service Processor
 - If ItsOn Service Controller does not receive usage reports from the device based on time/usage intervals, it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- Data Mediation sends CDRs to ItsOn Service Controller.
- ItsOn Service Controller queries its device usage database for uCDRs for the device.
- ItsOn Service Controller compares carrier CDR data usage byte counts vs. uCDRs.
 - If ItsOn Service Controller determines that the carrier usage counts don't match the uCDR usage counts (e.g. Fraud), it sends a notification to Data Rating to indicate that the device is in a Fraud state and usage should be billed based on carrier CDR reports.
- ItsOn Service Controller sends carrier CDR and ItsOn uCDRs to Data Mediation.
- When GGSN determines that the data session has closed, it sends a notification to the ItsOn Service Controller that the device data session is closed.



Service Processor/Service Controller Authentication

- Device starts data session
- Service Controller receives “Start Data Session” notification from Operator network and starts “Expected Login” timer for device
- Service Processor on the device establishes data session with Service Controller
- Service Controller cancels “Expected Login” timer
- Service Controller attempts to authenticate Service Processor (algorithm TBD)
- If authentication fails, Service Controller either 1) sends trigger to network to charge device data usage at “standard” bulk rate (implementation TBD based on operator network implementation); or 2) specifies a charging code for “standard” bulk rate on uCDRs sent to operator data mediation in response to CDRs received from data mediation
- If authentication succeeds, Service Controller marks the device as “Successfully Authenticated”.
- If “Expected Login” timer interval expires, Service Controller either 1) sends trigger to network to charge device data usage at “standard” bulk rate (implementation TBD based on operator network implementation); or 2) specifies a charging code for “standard” bulk rate on uCDRs sent to operator data mediation in response to CDRs received from data mediation



SC Receives UDRs From SP After Receiving “Data Session Stopped” Trigger From Network

- Authenticated SP active on operator network
- SC receives “Data Session Stopped” trigger from operator network
- SC marks the SP as “inactive”
- SP attempts session with SC via operator network
- SC detects device status as “inactive”
- SC closes data session
- SC marks the device a “fraudulent”
- SC generates “potential fraud alert” to operator CRM

Service Controller Receives CDRs But Does not Receive UDRs

- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- No UDRs with charging codes associated with 3G/4G access are returned for the time period specified by the CDR
- SC marks the device a “fraudulent”
- SC generates “potential fraud alert” to operator CRM



SC Receives CDRs and UDRs But the Usage Counts Don't Align

- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- SC verifies that UDR totals vs. CDR total for the same time period are within the "fraud discrepancy" threshold.
- If the discrepancy is outside the "fraud discrepancy" threshold, SC marks the device a "fraudulent" and generates a "potential fraud alert" to operator CRM

SC Receives CDRs and UDRs but SC Detects Usage Over Charging Policy (CP) Limit(s)

- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- SC verifies that UDR totals vs. CDR total for the same time period are within the "fraud discrepancy" threshold.
- Usage counts verify
- SC computes "total usage" per active Charging Policy
- SC verifies that aggregate usage within each active Charging Policy is under the usage cap defined by the charging policy



- If SC detects usage within an active Charging Policy that is over the usage cap, SC marks the device a “fraudulent” and generates a “potential fraud alert” to operator CRM

SC Receives UDRs but Charging Codes do not Correspond to CP(s) for Current Active Services

- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- SC verifies that UDR totals vs. CDR total for the same time period are within the “fraud discrepancy” threshold.
- Usage counts verify
- SC detects charging codes not associated with CP(s) for current active services on the device
- SC marks the device a “fraudulent” and generates a “potential fraud alert” to operator CRM

SC receives CDRs and UDRs, counts align, but usage velocity within a Service Component or Service Activity is greater than rate limit(s) set via CP

- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- SC verifies that UDR totals vs. CDR total for the same time period are within the “fraud discrepancy” threshold.



- Usage counts verify
- SC detects usage associated with charging codes that have rate limits set is greater than the maximum rate limit for a continuous stream over the time period specified by the UDR (check performed on a UDR-by-UDR basis)
- SC marks the device a “fraudulent” and generates a “potential fraud alert” to operator CRM`

SC receives CDRs and UDRs, counts align, but usage velocity at the Service Activity or Service Component level deviates “significantly” from average user usage velocity

- SC receives CDR from operator data mediation
- SC attempts to verify usage by requesting all UDRs for the time period indicated in the CDR
- SC aggregates all of the usage counts associated with charging codes assigned to 3G/4G access
- SC verifies that UDR totals vs. CDR total for the same time period are within the “fraud discrepancy” threshold.
- Usage counts verify
- SC detects usage velocity (bps) associated a Service Activity or Component over the time period specified by the UDR (check performed on a UDR-by-UDR basis) is “significantly” greater than average user usage velocity (bps)
- SC marks the device a “fraudulent” and generates a “potential fraud alert” to operator CRM`



CDR-based Verification Algorithm

- Assumes CDR input contains: start time, end time, MO bytes, MT bytes
- Collect ItsOn Charging Reports from the device, order them by network time, store on the server
- Collect CDRs from carrier for each device, order them by network time, store on the server
- Verify device usage is consistent with the sum of all active service usage allowances (caps)
- Verify that usage within services is within service-level caps
- If a service has an “associative traffic” filter
 - Verify that the ratio of associative traffic vs. non-associative traffic is within service policy limits
 - Verify that the ratio of traffic between the filters in the service are within policy limits
- For the time window specified in a CDR:
 - Sum device usage based on all of the charging reports received from the device for the same period
 - For windows where the CDR and the charging reports don’t match exactly, compute “average usage/minute” for the charging interval and add that to the device usage total
 - Compare totals
 - If comparison is within <x>% everything is OK
 - If Charging Report < CDR by <y>% then either ItsOn bug or potential fraud



- If Charging Report > CDR by <z>% then ItsOn bug, carrier reporting error or failed fraud attempt
- Generate micro-CDRs to the carrier based on time window specified in the original CDR

FDR-based Verification Algorithm

- Assumes FDR input contains: start time, end time, remote IP/port, MO bytes, MT bytes
- Perform CDR algorithm on FDRs to get totals
- If total usage is within policy, everything is OK so far
- For each “non-bulk-allow” service reporting during that period
 - Get service policy definition
 - Translate hostnames to IP addresses
 - Count all FDR matching Policy's IP addresses
 - Count all device usage records for the service
 - If the service has an “associative traffic” filter
 - Verify that the ratio of associative traffic vs. non-associative traffic is within service policy limits
 - Verify totals of non-associative filters vs. FDR counts
 - Verify that the ratio of traffic between the filters in the service are within policy limits
- Compare totals
 - If comparison is within <x>% everything is OK
 - If Charging Report < FDR by <y>% then either ItsOn bug or potential fraud



- If Charging Report > FDR by <z>% then ItsOn bug, carrier reporting error or failed fraud attempt
- If there is a “bulk-allow” service
 - Sum the charging report totals for all non-bulk services (including associative traffic)
 - Subtract charging report total from carrier FDR total
 - Compare previous result with charging records for bulk service
 - If comparison is within <x>% everything is OK
 - If Charging Report < FDR by <y>% then either ItsOn bug or potential fraud
 - If Charging Report > FDR by <z>% then ItsOn bug, carrier reporting error or failed fraud attempt

Behavior-based Verification Algorithm

- Service Controller keeps a database, based on service and filter that contains the following information:
 - Service Name
 - Filter Name
 - Average use per time period (e.g. per day, actual value TBD)
 - Average ratio of non-associative vs. associative traffic for the service
 - Expected ratio of filter matches vs. total service usage
 - Allowed percentage of variance (before indicating potential fraud event)



- Service controller keeps a data warehouse to track both aggregated usage within a service and usage at the filter level to compute the above information
- Periodically (e.g., daily), Service Controller compares user usage within a service and/or filter to the “average” usage data in the database
- If user usage within the service/filter is outside the parameters specified for the service/filter, a “potential fraud” alert is generated
- Example:
 - Amazon service:
 - 2 filters: amazon.com and images-amazon.com + associative
 - Service cap of 10 MB/day
 - Ratio of usage within the service is: amazon.com: 20%, images-amazon.com: 70%, associative: 10%
 - Ratio of non-associative vs. associative is 9:1 (or 90% non-associative)

Production Deployment considerations

- CDR-based Verification can be accomplished on all devices all of the time
 - CDR feed delivered to ItsOn Service Controller via operator Data Mediation
- Behavior-based Verification can be accomplished on all of the devices on a daily basis
 - Requires ItsOn Service Processor usage reporting records only (no operator dependency)
 - Can be augmented by FDR to validate the non-associative traffic counts within a service
- FDR-based Verification should be used when there is a discrepancy in one or more of the following checks:



- ItsOn Service Processor reported service-level usage is statistically higher than defined caps (e.g., Amazon Sponsored Service has a 10 MB daily cap, but the ItsOn Service Processor is reporting 15 MB of usage within the daily period)
- CDR reported usage is statistically higher than ItsOn Service Processor reported usage
- Average ratio of non-associative vs. associative traffic within a service is statistically higher than expected
- Behavior-based Verification indicates usage within a service does not follow statistical norms
- FDR-based Verification can also be used to randomly verify ItsOn Service Processor usage reports at the service level (e.g., Amazon Sponsored Service usage reported by ItsOn Service Processor matches FDR-based usage reports)
- Ideally, retrieval of FDR's by ItsOn Service Controller would be via a request mechanism (e.g., UserID, start time, end time)

Fraud Analysis Considerations

- ItsOn Charging Record (ICR) verification is sufficient to detect the following fraud
 - Singly Defeating the Service Processor Controls
 - Service cap violation detected by comparing total usage to service maximum
 - Service throttle violation detected by comparing usage over time to expected bandwidth
 - Singly performing Charging Record Spoofing
 - Per filter bucketing of traffic classification method allows comparison to expected classification ratios



- Service level ratio of non-associative vs. associative traffic
 - Filter level ratio of filter matches as a percent of overall service usage vs. expected percentage
- Behavioral analysis allows usage over time period comparisons to user population statistics (at the service level)
- Carrier CDR-based verification is sufficient to detect the following fraud
 - Disabling the Service Processor
 - Carrier CDR's without ItsOn Charging Records (ICR) signal ItsOn service interruption
 - Defeating Service Processor Controls & Performing Charging Record Spoofing
 - Carrier usage will show discrepancy from ICR reported usage
- Carrier FDR-based verification is sufficient to detect the following fraud
 - Substituting Sponsored Service charging for bulk service usage
 - Per filter totals of non-associative classification must match FDR totals otherwise fraud has occurred

Fraud Sampling

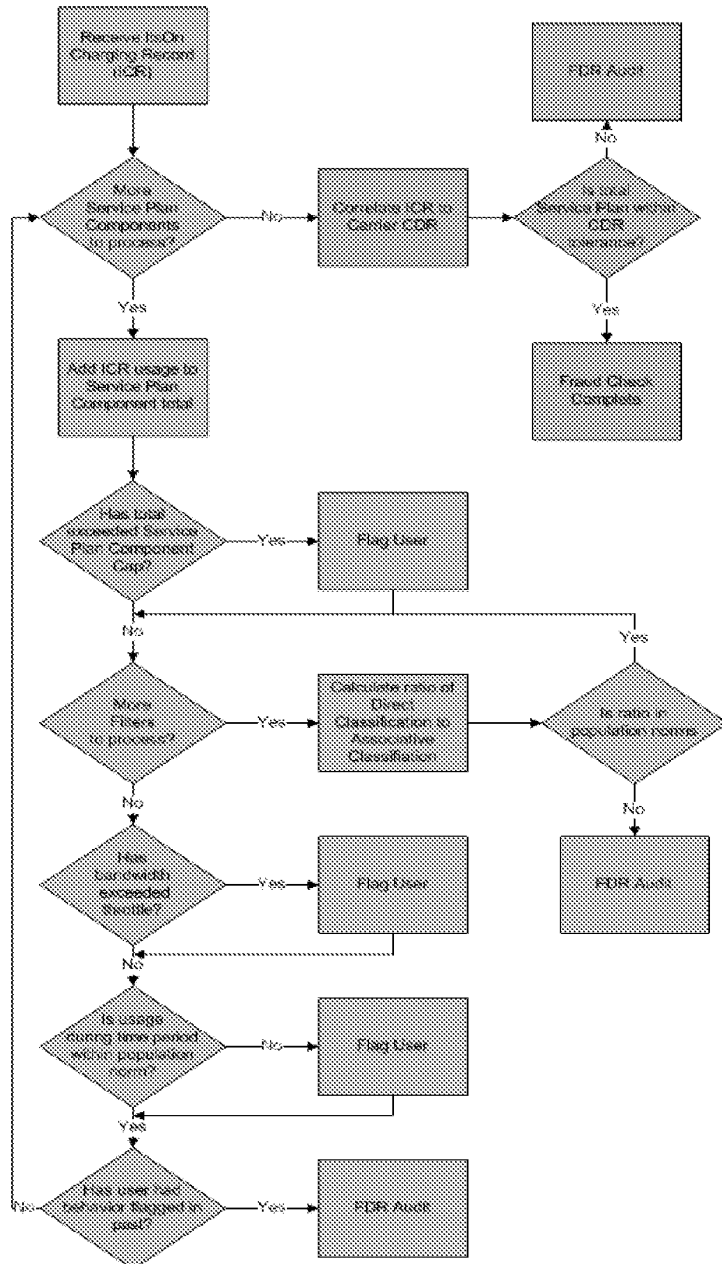
- Analysis of every ICR must be performed on every ICR received
 - If ItsOn Service Processor is running in secure method/area on device this is sufficient.
 - Carrier CDR validation must be performed if Service Processor not secure
 - Based on the specific Service Plan it may be a post process activity
 - Low caps on Services limit liability



- User will be charged for data, the fine grain mediation will be lost
 - Can be addressed in the contract
- CDR's may not be available in near/real time
 - Roaming
- Near-real time CDR validation can be used when ICR validation detects problem
- Carrier FDR validation only needed when fraud audit is required
 - ICR & CDR validation sufficient for all but the most sophisticated fraud attempts

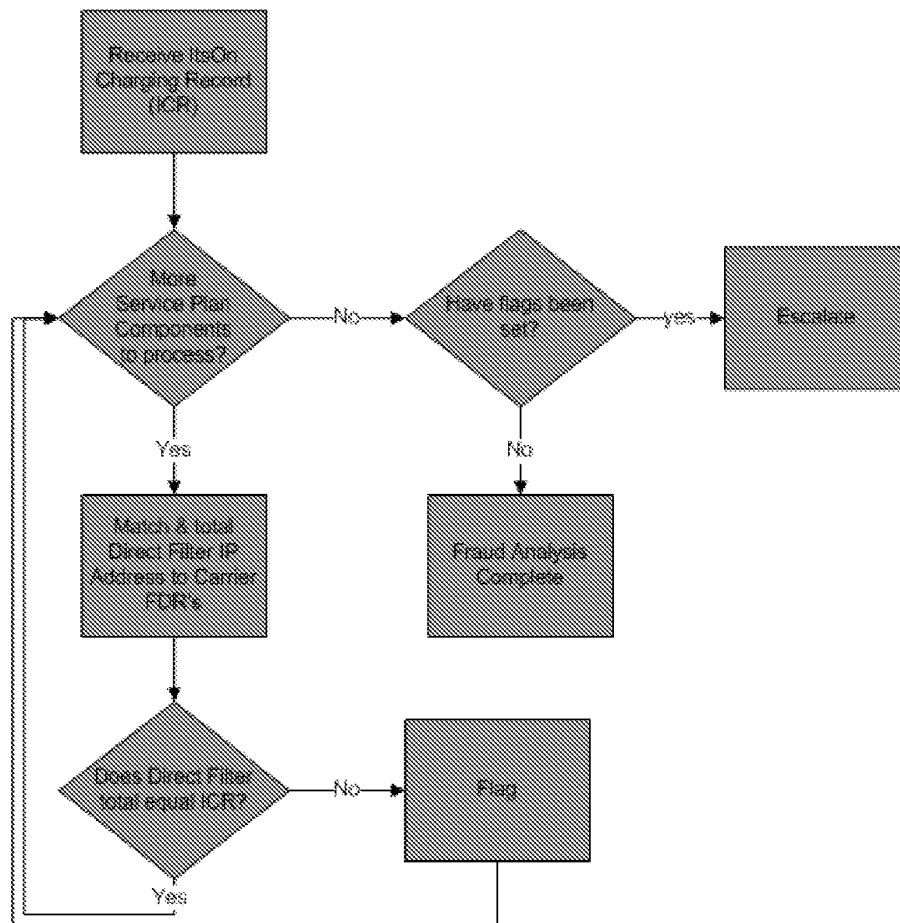


ICR & CDR Fraud Analysis Flow





FDR Fraud Analysis Flow



Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SECURITY AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		Michael J. Schallop/Veronica Pula		
Attorney Docket Number:		RALEP045+		
Filed as Large Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional application filing	1005	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				220

Electronic Acknowledgement Receipt	
EFS ID:	9024487
Application Number:	61422574
International Application Number:	
Confirmation Number:	9531
Title of Invention:	SECURITY AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	21912
Filer:	Michael J. Schallop/Veronica Pula
Filer Authorized By:	Michael J. Schallop
Attorney Docket Number:	RALEP045+
Receipt Date:	13-DEC-2010
Filing Date:	
Time Stamp:	18:48:41
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 220
RAM confirmation Number	6326
Deposit Account	500685
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Provisional Cover Sheet (SB16)	RALEP045plus_Provisional_Coversheet_Transmittal.pdf	1000002 31246c67193e8c6cad7762b5f98c5ce5e690f45	no	3
Warnings:					
Information:					
2		RALEP045plus_App.pdf	926495 db61cefb23bf89c4123409ac760888fa0e59029c	yes	37
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal of New Application		1	1	
	Specification		2	37	
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	29329 55e1d6c567ae5ccd0b24dc6c0c33bd7c8805c61e	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1955826		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (04-07)

Approved for use through 06/30/2010 OMB 0851-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name	Middle Name	Family Name	City	State	Country i
Gregory	G.	Raleigh	Woodside	CA	US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention	SECURITY AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES
Attorney Docket Number (if applicable)	RALEP045+

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number ☐ Firm or Individual Name

Customer Number 21912

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

- ☐ Yes, applicant qualifies for small entity status under 37 CFR 1.27
- ☒ No

Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Michael J. Schallop/			Date (YYYY-MM-DD)	2010-12-13
First Name	Michael	Last Name	Schallop	Registration Number (If appropriate)	44319

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.