

Work Items & Priorities Survey Results

9/8/2006

2 I am concerned with fraud as it relates to:		Weights used	
Voice/SMS services	14	6	high
Packet data services	12	3	med
General business policies	6	1	low
		0	not needed

Unique responses = 15. Participants:
Bell Mobility, Fair Isaac, Iusacell, Gemalto, KDDI, Pelephone, Sasktel, Sprint Syniverse, Qualcomm, US Cellular, Verisign, Verizon, Vivo, ZTE

4 Potential work items			Weighted Score
FRAUD TOOL RECOMMENDATIONS - provide information and recommendations on tools such as high-usage reporting, notification of suspicious activities, visibility, statistics, etc...	High priority	11	76
	Medium priority	3	
	Low priority	1	
	Not needed	0	
RECOMMENDED AUTHENTICATION POLICIES/SETTINGS - provide recommendations on issues such as when to use unique challenges, how frequently to update SSD, whether to use PAP or CHAP, etc...	High priority	9	68
	Medium priority	4	
	Low priority	2	
	Not needed	0	
FRAUD TRAINING - offer a CDG training course that covers voice and data fraud issues, solutions, recommendations, etc...	High priority	8	65
	Medium priority	5	
	Low priority	2	
	Not needed	0	
DATA AUTHENTICATION INFORMATION - review and, if needed, expand on data security information provided in CDG #136 (EV-DO Roaming Whitepaper)	High priority	8	63
	Medium priority	4	
	Low priority	3	
	Not needed	0	
UPDATES TO CDG QUALIFICATION FORMS AND TDS DOCUMENTS - review these documents to ensure that issues related to fraud management are sufficiently represented	High priority	5	60
	Medium priority	10	
	Low priority	0	
	Not needed	0	
VOICE AUTHENTICATION INFORMATION - review, complete, and release CDG #138 (CDMA Authentication Whitepaper)	High priority	6	55
	Medium priority	5	
	Low priority	4	
	Not needed	0	
BROWN-OUT PROCEDURES - provide guidelines on how to facilitate brown-outs of areas with roaming partners	High priority	4	46
	Medium priority	6	
	Low priority	4	
	Not needed	1	
VLR REMOVAL PROCEDURES - provide guidelines on how to facilitate removal of unauthorized VLR records with roaming partners	High priority	3	40
	Medium priority	6	
	Low priority	4	
	Not needed	2	

New work item recommendations
How the working group should function
Provide a bridge between the carriers and vendors to improve the security of the network
Provide an interface to other standard bodies or research groups to working out the solution to prevent fraud from network
Identifying fraud issues and scenarios
Identify scenarios where technical fraud can occur and work to eliminate/mitigate them
Provide a form for indentifying fraud issues and how they were found/fixd
Identify ways to protect against subscription fraud and identity theft that are often vehicles for roaming fraud
Share participant experiences in preventing, detecting, and combat fraud (after detected)
Identifying high fraud markets and types of fraud per market
Identify the most common kind of fraud in each network and country (for example, kind of calls - local, long distance national, or international)
Identify high fraud markets and work with operators in those markets to start reducing the fraud. By reducing fraud, and even the perceived threat of fraud, another hurdle to international roaming will be removed.
Develop a list of the most common high fraud markets. Maybe each operator provides their top 5 markets where they have experienced fraud in the last 6 months, so the group can develop action plans to work with the serve carriers to start eliminating the issues.
Address exposure in Asia and on GSM networks (current near real-time record exchange protects CDMA carriers in the Americas)
Data
Provide guidelines to firewall vendors to support RADIUS inspection similar to the GTP inspection in the GSM world
Standardize the DOMAIN to VRF method within the PDSN product
Specifically define what constitutes data fraud
Identify how we can be pro-active in protecting data roaming against data/content services fraud
Identify and know how to prevent data fraud
Other types of fraud/security issues
Address fraud protection for inter-standard roaming
Address PTT security (SBC for mobile)
Address handset security for mobile operating system (Windows mobile)
Identify carrier process information
Identify how various carriers structure their fraud operations
Address revenue assurance
Tools
Specify guidelines/recommendations to security vendors for a platform that could be located in the Mobile access and provide capabilities as antivirus, spam, spyware, malware, MMS vulnerability, etc.
Provide recommendation on HUR reporting vs near real time CDR exchange
Authentication
Standardization and implementation of Authentication
Identify one standard method to implement terminal authentication for EVDO (use Akey ,Dkey, MIN OR ESN)