Data Communications Company

SEC Modification Proposal, SECMP0067, DCC CR355

Service Request Traffic Management

Worked Example

Version:	**0.54**
Date:	**8th April, 2020**
Author:	**DCC**
Classification:	**DCC PUBLIC**

How Will the Mechanism Work for a User?

The following is a worked example of how Service Requests (SRs) would be throttled. User traffic rate is mapped over a period and compared to a resulting profile if SECMP0067 was active for a User with an allocation equating to 400 requests/second.

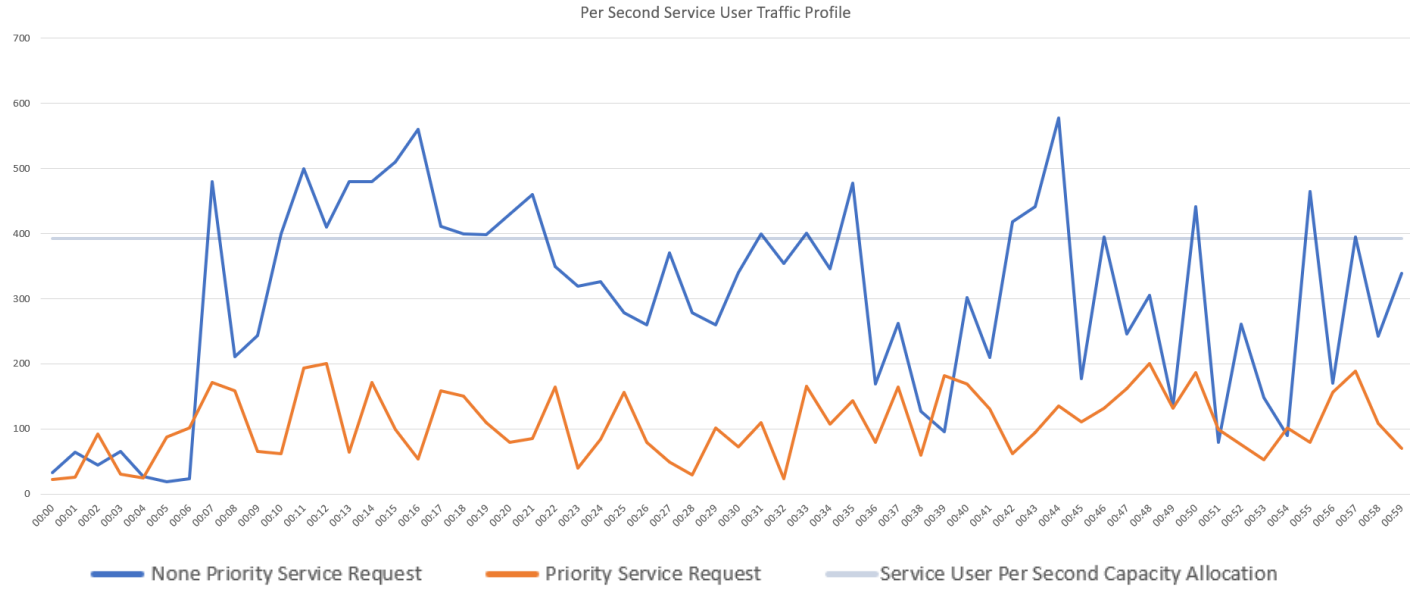

Figure 1: Traffic Management Inactive

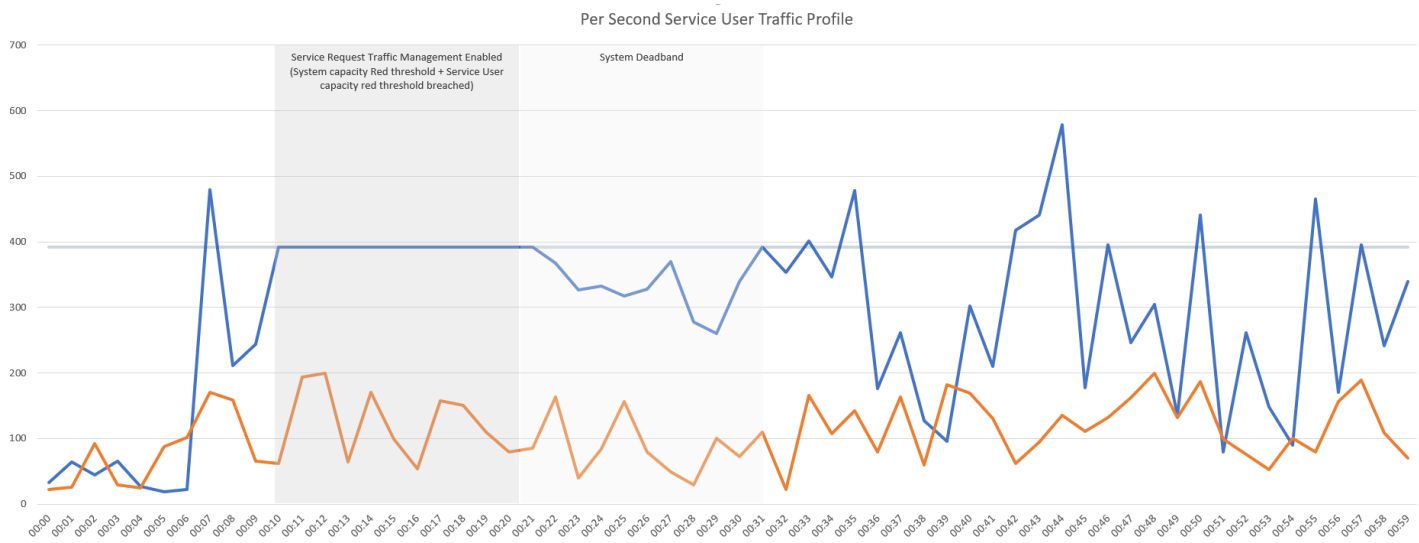

Figure 2: Traffic Management (SECMP0067) Active

Time	Req/Sec	Limit/Accepted	Rejected
00:10	400	400	0
00:11	500	400	100
00:12	410	400	10
00:13	470	400	70
00:14	470	400	70
00:15	500	400	100
00:16	560	400	160
00:17	410	400	10
00:18	405	400	5
00:19	405	400	5
00:20	420	400	20
00:21	460	400	60
Total	5410	4800	610

The impact of the Service Request Traffic Management Enabled (System capacity Red threshold + Service User capacity red threshold breached) is clear as the number of Service Requests are throttled. Also note that the "recovery period" during System Deadband shows that the number of SRs passed is increased towards, but not over, the Capacity Allocation value.

It should be noted that the HTTP Header field contains a RETRY-AFTER value which indicates the time that should elapse before the message is resent by the Service User.

In the example above, the Service User could resubmit the "Rejected" Service Requests 25 seconds after the initial threshold breach, and these would processed as usual. It will be the responsibility of the Service User to amend their systems to retry the Service Requests, and guidance is provided in the FIA and the WG Consultation response. It will also be in the proposed amendment to DUIS in Annex G of the MRC. This says they should re-submit after a minimum delay as specified in the RETRY-AFTER header.