# Proposed; Inclusion of an additional field in OpenC2 messages to assure integrity. 05/23/2016

## **[RESOLVED]**

## **Proposed**:

The OpenC2 protocol shall define an optional extension to enable integrity protections.

|  |  |
| --- | --- |
| **Affirmative Construct** | **Negative Construct** |
| * The actuators must be able to detect changes in the message. * In some cases it will not be practical to use external message integrity mechanisms. | * The OpenC2 design principles encourage a ‘lightweight’ protocol and to leverage preexisting standards to the greatest extent practical * Integrity can be achieved by multiple means and to define a particular means places an unnecessary (and possibly sub-optimal) constraint on the implementer |
| **Negative Rebuttal** | **Affirmative Rebuttal** |
| * Future technologies may not have practical integrity mechanisms available. * Integrity mechanisms are not overly burdensome, a simple hash could provide the means | * All seven layers of the OSI stack have integrity mechanisms available, it is reasonable to assume that some sort of integrity mechanism is available. * We should explicitly state that the OpenC2 contains no provisions for anti-tamper and that external provisions are required in order to be secure/reliable. |
| **Resolution** | |
| The language specification will not define an optional field to provide integrity, however the documentation shall explicitly call out the fact that anti tamper is not provided by the OpenC2 specification and that external provisions for integrity are required. | |
| **Minority Report** | |
| No minority report provided. | |