## SNMP Analysis

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Technology | Latency | Cardinality | Bi-directional | Confidentiality | Integrity | Pseudonymity | Unlinkability | Non-repudiation | Bandwidth Efficiency |
| SNMPv1/UDP/IP | < 10 sec | Unicast | Command/response | None | None | No | No | No | Low |
| SNMPv3/(D)TLS | < 10 sec | Unicast | Command/response | High | High | No | No | Yes | Low |

**Other factors**

Effort to define message contents: average (3)

SNMP exchanges data elements that are defined in a Management Information Base (MIB). The effort to define this data is similar for most other formats.

Effort to implement solutions: average-low (2)

SNMP is a well-defined protocol, which has broad industry support in off-the-shelf tools. As long as the standard is used per industry norms, implementations are not too complex.

Processing requirements: average on-demand

Managers and agents are largely idle; when a request is received, the processing is generally not overly complex; although the exact level varies depending on whether encryption is being used and the logic underlying the request.

Platform support: Extensive

SNMP is a widely adopted technology that is available with off-the-shelf solutions for most platforms.

Readiness: SNMPv1 ready; SNMPv3 approximately 2 years

SNMPv1 is widely deployed today within ITS. As an IETF standard, SNMPv3 is a mature technology, but it is not widely used within ITS and the profiles and core data definitions have not been standardized for ITS, although work is in progress.

Able to support common data: yes