GRC Report Exchange
draft-moriarty-mile-grc-exchange-02

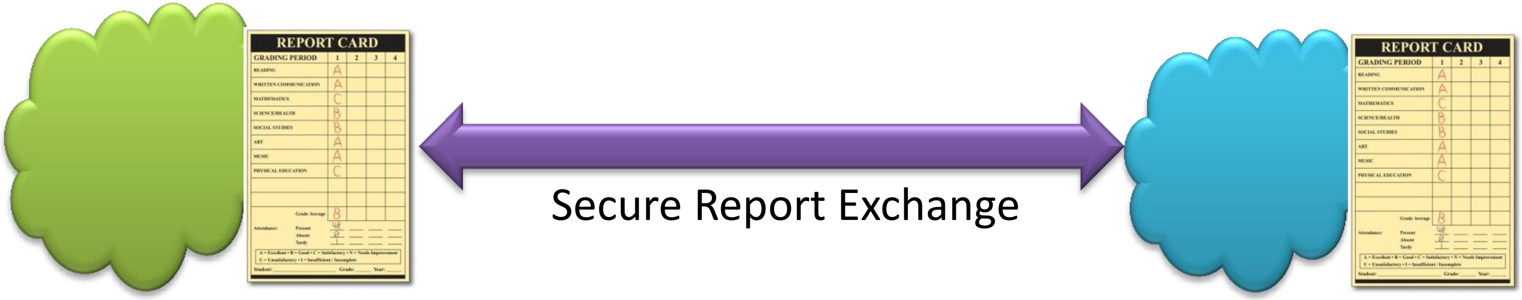
Purpose

This draft is a generalized format derived from the secure exchange of incident information defined by RFC6545, Real-time Inter-network Defense (RID) and RFC 5070, The Incident Object Description Exchange Format.

The purpose of this draft is to:

- Describe a common method to securely transport Governance, Risk and Compliance (GRC) data and other XML reports
- Provide policy options and markings in an XML schema
- Provide options for confidentiality at the document/report level
- Enable security for the end-to-end communication
- Allow XML reports to be shared between service providers and clients, enterprises, or within enterprises.

Use Cases



Secure Report Exchange

Provides a consistent method to securely exchange reports for:

- Continuous Monitoring (vulnerability, configuration, control compliance)
- Legal Documents (e.g. LI-XML, policy exchange)
- Regulatory Compliance Reporting (e.g. eFilling)
- Operational Reports (e.g. change mgmt, capacity, availability)
- Business Operational Reports (e.g. quantifying risk/costs)

Relevance to the MILE WG Charter

- Addresses the need for a generalization of RID for secure exchange of other security-relevant XML formats
- Represents the start of a Standards Track document for GRC Report Exchange.

Next Steps – New Work

- Refinement of the model/schema
- Address information sharing WITHIN enterprises
- Discuss the addition of a message type that requests data to be collected for future reporting (tasking)
- Definition of a transport protocol for GRC Report Exchange derived from RFC-to-be 6546 or other binding based on WG consensus.
- Other items based on WG feedback

Recommendations

- Accept draft as MILE WG document
- Update the MILE Charter’s Goals and Milestones:
  - Sep 2012 (was May 2012): WGLC GRC Report Exchange
  - Oct 2012 (was Jun 2012): Submit GRC Report Exchange to IESG for consideration as Standards Track document
  - Add work item for GRC Report Exchange Transport