CICM BOF

IETF 81

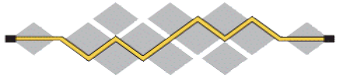
Quebec, July 2011

It’s Pronounced Kick-Em

IETF®

Note Well

- Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
  - The IETF plenary session
  - The IESG, or any member thereof on behalf of the IESG
  - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
  - Any IETF working group or portion thereof
  - Any Birds of a Feather (BOF) session
  - The IAB or any member thereof on behalf of the IAB
  - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.
- Please consult RFC 5378 and RFC 3979 for details.
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.



CICM

- Current charter:

  http://code.google.com/p/ietf-cicm/wiki/WGCharter
- Mailing list:

  cicm@ietf.org

Agenda

- Blue sheets, Jabber scribe, bashing, intro (5 min)
- Problem Statement– Vincent (10 min)
- The CICM Model– Lev (20 min)
  - Use cases: draft-lanz-cicm-lm
  - Management
    - Channels: draft-lanz-cicm-cm
    - Modules: draft-lanz-cicm-mm
    - Keys: draft-lanz-cicm-km
- Charter discussion/Open mic (20 min)
- Hum….

Proposed CICM Charter

Description of Working Group

The Common Interface to Cryptographic Modules (CICM) defines an abstract API for the security services provided by cryptographic modules developed by multiple vendors. The API is intended to support high assurance cryptography, security domain separation, and enhanced module, key, and channel management capabilities that are vendor neutral.

The purpose of the CICM Working Group is to publish an API for high assurance cryptographic devices and to provide guidance for any new submissions related to high assurance cryptos.

Specifically, the Working Group will:

- Complete existing requests:
  - replace algorithm strings with OIDs
  - use ABNF notation for unique identifiers syntax
  - add module events for symmetric and asymmetric key fill
  - add unprotected-side APIs for:
    - moving data into / out of the module
    - performing administrative functions (e.g., supply IV, header-bypass data)
- Propose the following documents to the Working Group:
  - draft-lanz-cicm
  - draft-lanz-cicm-lm
  - draft-lanz-cicm-mm
  - draft-lanz-cicm-km
  - draft-lanz-cicm-cm

Polling the Group…

- There is a problem that needs solving and the IETF is the right place to solve it.
- The scope of the problem is well-defined and the deliverables are understood.
- It is the right set of deliverables
- Who is willing to participate (edit drafts, review drafts, etc)?
- A WG (if formed) has a good probability of completing its deliverables in a timely manner.