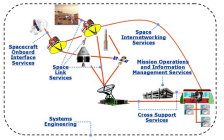


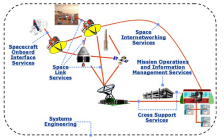
Thoughts about CCSDS Security Architecture

Peter Shames

CCSDS Systems Engineering Area Director

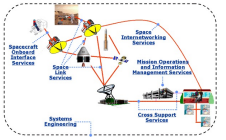
8 Dec 21

Background



- Most current interoperability is for “single hop” missions, MOS => ground station => spacecraft.
  - The SCCS-ARD calls these ABA configurations.
- Multi-agency, multi-spacecraft, networked (DTN) missions are being planned (and built).
  - The SCCS-ARD calls these SSI configurations.
- The terrestrial “security & threat landscape” is changing quickly and CCSDS (and the member agencies) are not yet completely ready to deal with this, particularly in a multi-agency DTN/SSI environment.
- This presentation is intended to briefly explore some of the issues and to frame some solutions for further discussion.
  - There is this joke about “security through obscurity”
  - The real laugh is that security approaches, themselves, can be pretty opaque
  - We’re trying here for a KISS approach, Keep It Simple … details to follow

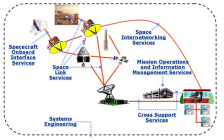
CCSDS future deployment assumptions



- Multiple agencies will operate one or more “space assets”
  - Space assets may be orbiters, landers, rovers, (attached devices, hosted components, …)
- Integrity of space (and ground) assets and data must be protected, and privacy must be provided for certain classes of data and communications (human related)

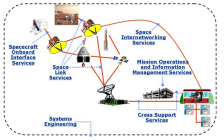
- Agencies may deploy their own “private” networks and use whatever security is satisfactory for them, but …
- For communications coverage, cross support, and reliability agencies will likely collaborate among themselves to deploy space networking, using both in space and Earth based assets
  - Must all use some agreed, interoperable, subset of CCSDS comm link protocols, and …
  - Must all use DTN for networking, and …
  - Must have some unambiguous way to identify user, service provider, and service management assets, and …
  - Must be able to secure their systems, and the network itself, to prevent problems.

CCSDS current link layer security approaches



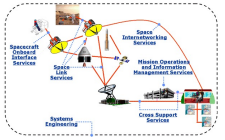
- Current operational posture is very close to “if you are in space, and we have an agreement, we will try to support interoperations”
  - Many of the protocol architecture security arrangements are rather ad hoc
  - There is little link layer security in use now, the only available “identity” checks are on CCSDS link layer SCIDs, frequency assignments, and antenna beam patterns
  - SDLS and key management is available and can be used, but are not yet widely deployed
- Uplink data for deep space missions tends to be transmitted in the clear, but many near Earth missions have protected uplinks
- Security at service interfaces uses pair-wise agreements and negotiated service provider login credentials and network access
- Cross support agreements are documented and managed terrestrially, and use login credentials and firewall rules to validate operational access
- Operational coordination involves pair-wise agreements to manage contact scheduling and data volumes, Service Management is still “to be”

Future SSI multi-mission security assumptions

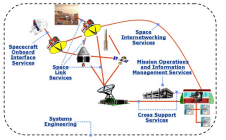


- Participating agencies / organizations must agree on a trust framework, a set of roles, policies, and a governance model
- Cross support and interoperability at DTN layer are essential for effective SSI deployments and should be as automated as possible
- All assets will have identities that can be unambiguously validated
  - Authentication of communicating assets will be validated as the norm
- Uplinked commands should be secured (encrypted), other uplink products may only be authenticated (digitally signed)
- Downlink products may be authenticated to provide integrity checks, and encryption may be used, but this will not necessarily be the norm
- Network layer authentication, and possibly data encryption, will be preferentially used (DTN/BPSec)
  - Application layer encryption / authentication may also be adopted where needed
  - Authentication of the assets that provide and manage the network itself must be secured
- These security features all rely on use of security keys and some sort of key management tied to the identities of participating entities

So … assigning and managing identities becomes very important



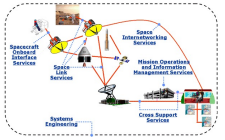
- Link layer SCID is a weak, and non-unique identifier
- DTN Node ID, by itself, is also weak and can be “faked” or hijacked (unless optional security mechanisms are used)
- For multi-agency trust relationships to work effectively there must be an agreed and adopted trust framework, policies, roles, and governance approaches
- All entities/assets (spacecraft, DTN nodes, ground stations, end users) must have assigned and documented identities and roles
- Interoperating / cooperating agencies need some way to catalog, manage, verify and cross-check identities of assets
- Each identity is associated with sets of keys used for authentication and/or encryption, and with roles they may be assigned
- NOTE: DTN, and BPSec, can operate with keys that include (but are not limited to):
  - Pre-placed keys selected based on local policy.
  - Keys extracted from material carried in the Bundle security blocks.
  - Session keys negotiated via a mechanisms external to the Bundle security blocks.



Propose a phased approach

- Agree on basic security framework for multi-agency interoperability
  - Develop agreed set(s) of policies, roles, and governance approaches
  - Assume use of BPSec and simple, pre-placed keys for initial deployments
- Agree on how to assign unambiguous, unimpeachable, identities to all participating assets
  - All communicating entities should have a certificate to provide identity
  - Certificates may be pre-placed onboard
  - Consider adoption of a new, trusted, InterGovernmental Certificate Authority (IGCA)
    - Leverages existing terrestrial PKI framework
    - Agree to federated approach that allows agency autonomy and also interoperability
    - NOTE: The SANA operator runs the IANA CA for the Internet DNS system, it has expressed willingness to run the IGCA for CCSDS
- Develop plan and protocols for secure DTN / space interoperability
  - Document policies, roles, and governance procedures
  - Use identities and certificates for space interoperability
  - Define, implement, and deploy more advanced BPSec and network management features
  - Define necessary secure network management and key management standards

CCSDS implementation IGCA
(CCSDS Sec WG, Chuck Sheehe)



IGCA Root CA
a. Trust anchor that all participants can chain to
b. Managed by the IGCA PKI service contract

IGCA Bridge CA signed by the IGCA Root CA
a. managed by the IGCA PKI service contract
b. This Bridge CA cross-certifies with other agency/organization/corporation CAs

IGCA Policy Root

Root CA level

Rapid Update rate

Issuing CA level

IGCA Issuing CA
a. Managed by the IGCA PKI service contract
b. This CA would issue certificates to devices/users for smaller participant groups do not have their own PKI nor resources to stand one up

IGCA Issuing CA

Agency B Root

1 year certs or 3 year certs

Agency B Issuing CA

Self Signing

Agency A Root

National Bridge CA

Bridge Member CAs
a. The cross-certified external partners CAs
b. Issue certificates to their end-entities
c. This cross-certified CA, ACA below the external partner's, issuing CA

1 year certs or 3 year certs

Agency A Issuing CA

USER B

SDLS

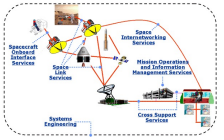
BPSec

PROTECTED SIMPLE AUTHENTICATION

IPsec

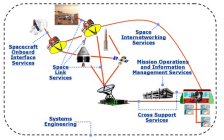
USER A

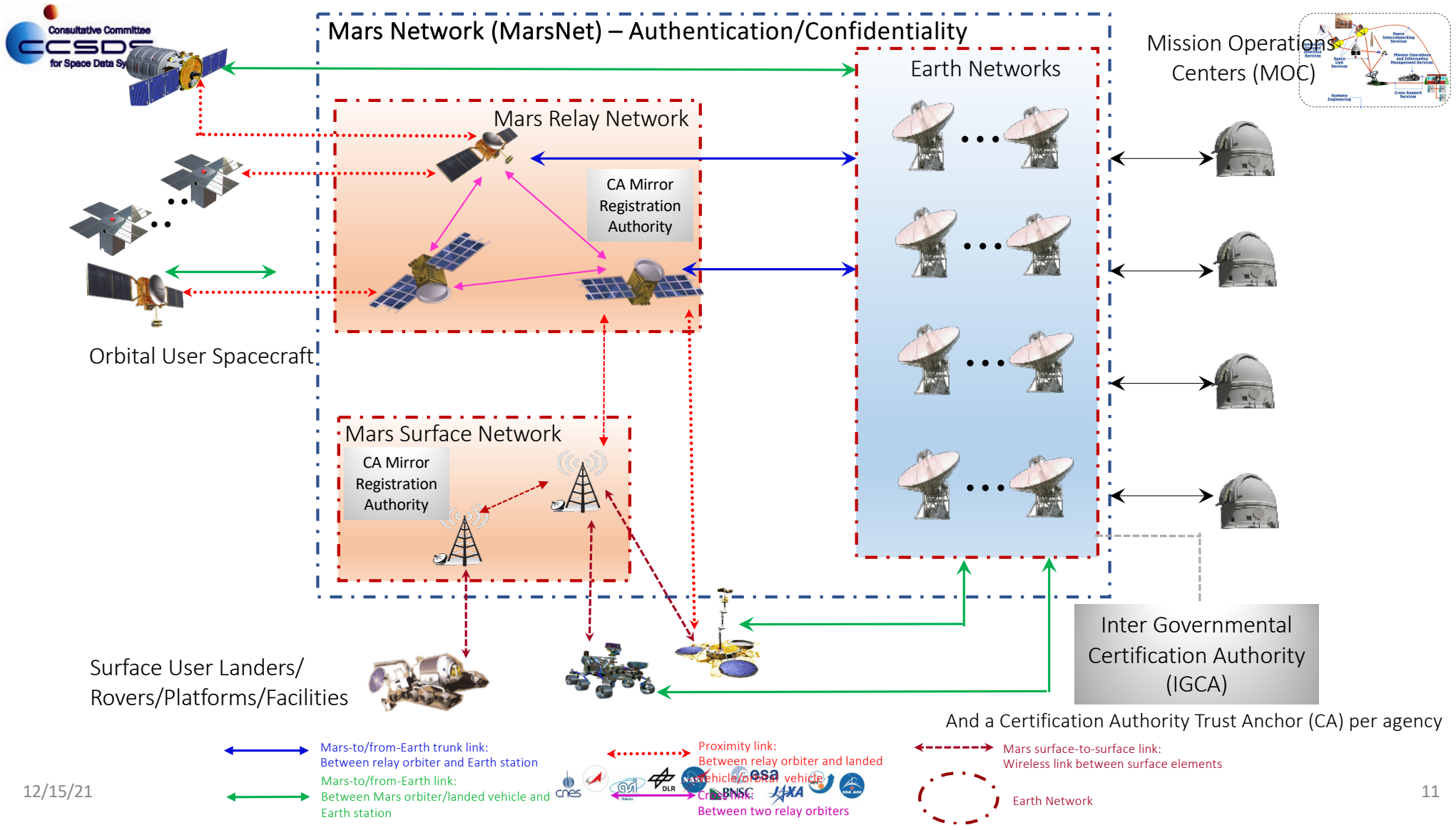
A “Modest Proposal”

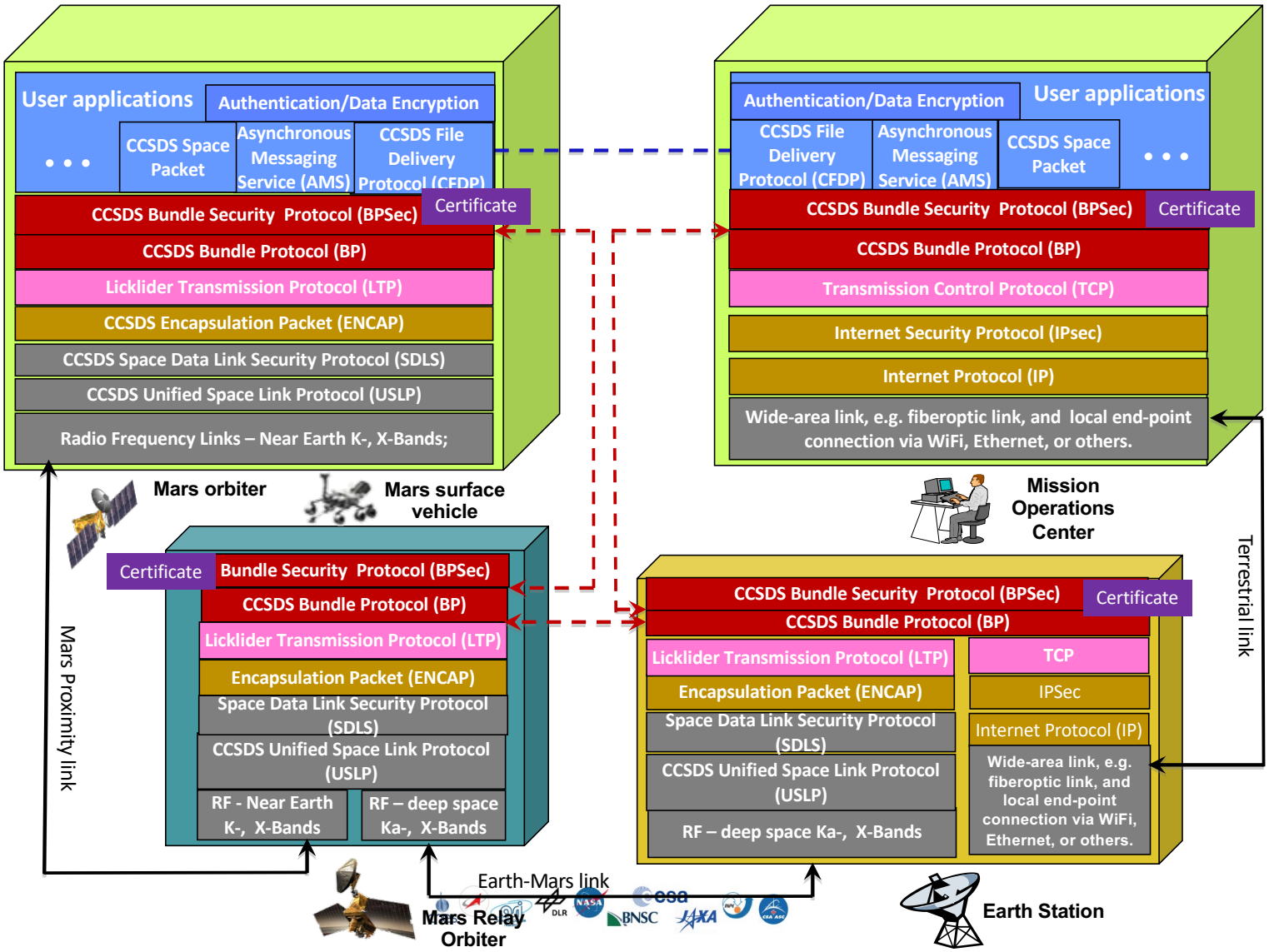


- Use this presentation, and all the available supporting materials, to initiate discussions of the motivations, assumptions, and consequences of agency missions and different deployment choices
- Involve the security and mission experts in each agency, and in CCSDS and the IOAG, in this discussion
- Identify the common ground, shared assumptions, shared goals, and acceptable shared policies
- Develop an agreed trust framework, policies, and governance approaches that can make this interoperable, multi-agency / organization venture work effectively and securely
- Identify and develop, jointly, the necessary standards, protocols, technical framework and infrastructure that will support this venture as missions are deployed

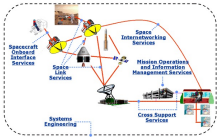
BACKUP




Mars Network (MarsNet) – Authentication/Confidentiality
Earth Networks
Mission Operations Centers (MOC)
Mars Relay Network
CA Mirror Registration Authority
Orbital User Spacecraft
Mars Surface Network
CA Mirror Registration Authority
Surface User Landers/ Rovers/Platforms/Facilities
Inter Governmental Certification Authority (IGCA)
And a Certification Authority Trust Anchor (CA) per agency
Mars-to/from-Earth trunk link: Between relay orbiter and Earth station
Mars-to/from-Earth link: Between Mars orbiter/landed vehicle and Earth station
Proximity link: Between relay orbiter and landed vehicle/orbital vehicle
Cross link: Between two relay orbiters
Mars surface-to-surface link: Wireless link between surface elements
Earth Network


User applications
Authentication/Data Encryption
CCSDS Space Packet
Asynchronous Messaging Service (AMS)
CCSDS File Delivery Protocol (CFDP)
Certificate
CCSDS Bundle Security Protocol (BPSec)
CCSDS Bundle Protocol (BP)
Licklider Transmission Protocol (LTP)
CCSDS Encapsulation Packet (ENCAP)
CCSDS Space Data Link Security Protocol (SDLS)
CCSDS Unified Space Link Protocol (USLP)
Radio Frequency Links – Near Earth K-, X-Bands;
Authentication/Data Encryption
User applications
CCSDS File Delivery Protocol (CFDP)
Asynchronous Messaging Service (AMS)
CCSDS Space Packet
CCSDS Bundle Security Protocol (BPSec)
Certificate
CCSDS Bundle Protocol (BP)
Transmission Control Protocol (TCP)
Internet Security Protocol (IPsec)
Internet Protocol (IP)
Wide-area link, e.g. fiberoptic link, and local end-point connection via WiFi, Ethernet, or others.
Mars orbiter
Mars surface vehicle
Mission Operations Center
Terrestrial link
Mars Proximity link
Certificate
Bundle Security Protocol (BPSec)
CCSDS Bundle Protocol (BP)
Licklider Transmission Protocol (LTP)
Encapsulation Packet (ENCAP)
Space Data Link Security Protocol (SDLS)
CCSDS Unified Space Link Protocol (USLP)
RF - Near Earth K-, X-Bands
RF – deep space Ka-, X-Bands
CCSDS Bundle Security Protocol (BPSec)
Certificate
CCSDS Bundle Protocol (BP)
Licklider Transmission Protocol (LTP)
TCP
Encapsulation Packet (ENCAP)
IPSec
Space Data Link Security Protocol (SDLS)
Internet Protocol (IP)
CCSDS Unified Space Link Protocol (USLP)
Wide-area link, e.g. fiberoptic link, and local end-point connection via WiFi, Ethernet, or others.
RF – deep space Ka-, X-Bands
Earth-Mars link
Mars Relay Orbiter
Earth Station

Notes:



- This protocol stack diagram shows too much “security” unless it is trying to show all possible options at once
  - Choose:
    - user data auth / encrypt, or …
    - BPSec, or …
    - SDLS.
  - NOT all three.
- BPSec says:
  - Sec 2.2.1 “When the integrity mechanism incorporates signatures, this service can also provide authentication for the relevant data.” The operative word is “when”, it does not say not “how”.
  - Sec B1.2.4: Authentication of Communicating Entities “BPSec does not provide a service for authentication of communicating entities. This authentication can be accomplished by combining BPSec services with other components, such as encapsulation [or use of signatures].”
  - There “security context” mechanisms defined as an adjunct to BPv7 and BPSec. They depend upon “security contexts” where the “identities” of the participants may be associated with pre-loaded keys, or keys carried within Bundle security blocks, or by session keys negotiated outside the security blocks.
  - Keys may be symmetric or asymmetric using adapted PKI(X) mechanisms.

Adapted "Zero Trust" Security Approach

(Derived from: NIST 800-207: Zero Trust Architecture)