20 March 2026

IETF 125 Security Area Open Meeting (SAAG)

This session is being recorded

Internet Engineering Task Force
© 2025 IETF Trust
Production by Meetecho

Note Well

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies. For a linked version of this text, please visit **www.ietf.org/note-well** or use the QR code below

- IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times (see **RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy**). If you have any concerns about behavior, please contact the *Ombudsteam* who have a duty of confidentiality and extensive powers to act, as set out in **RFC 7776: IETF Anti-Harassment Procedures**.
- If you are aware that any IETF contribution (as defined in **RFC 5378: Rights Contributors Provide to the IETF Trust**) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see **RFC 8179: Intellectual Property Rights in IETF Technology**).
- For detailed process information consult **RFC 2026: Internet Standards Process** and *RFC 2418:* **IETF Working Group Guidelines and Procedures** and updates to those.
- The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the **IETF Privacy Statement**.

For advice, please talk to Working Group chairs or Area Directors.

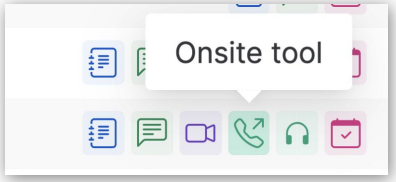
IETF

This session is being recorded

IETF 125 Meeting Tips

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to:
  - join the mic queue
  - participate in shows of hands
- *Keep audio and video off if not using the onsite version.*
- *Do not use personal hotspot / mifi devices - it interferes with IETF wifi*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session.
- Use of a headset is strongly recommended.

Resources for IETF 125

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda

- Welcome, Administrivia, and Agenda Bashing (5 mins)
- WG and AD Reports (15 mins, chairs/ADs)
- Bob Beck and Jeff Haas: TLS for BGP and related PKI considerations (draft-hbq-bgp-tls-auth) (10 min)
- Introduction to the Next Generation Commercial Cryptographic Algorithms Program for China (10 min)
- Benjamin Dowling: Securing QUIC with MLS (draft-tian-quic-quicmls-01) (10 min)
- Open Mic (remaining time)

IETF

Farewell to Paul Wouters as AD

Paul was the Responsible SEC AD for:

- 18 WGs
- 3 BoFs
- 41 RFCs + 23 in RFC-Editor Queue

IETF

New Security Area Director: Chris Inacio

Chris elected by NomCom to replace Paul.

https://datatracker.ietf.org/person/inacio@cert.org

WG Changes since IETF 124

BOFs	
Chartering (charter is at IESG)	
New Working Groups	PLANTS
Closed Working Groups	OHAI TEEP
Rechartered Working Groups	LAKE
In Rechartering (charter at WG or IESG)	SPICE

IETF

WG Chair changes since IETF 124

WG	Departures	Additions
PLANTS		Thom Wiggers Russ Housley
SCITT	Chris Inacio	Nicole Bates
PQUIP	Sofia Celi	

Helping Out

- If you are interested in becoming a **WG chair**, let your ADs know.
- Become a **Document Shepherd**. Learn about IETF processes while helping advancing documents! Ask your AD if shepherding is right for you!
- Errata processing - help your WG resolve reported erratas. We also have errata in closed WGs that no one is looking at.
- Attend BoFs (virtually or in person)
- Volunteer right now for being minute taker for this meeting :)

IETF

Working Group Summaries

Send highlights and summaries to saag@ietf.org

ACE	LAKE	SCIM
ACME	LAMPS	SCITT
COSE	MLS	SEAT
DANCE	OAUTH	{SEC}DISPATCH
DULT	OPENPGP	SPICE
EMU	PLANTS	SSHM
HPKE	PPM	SUIT
IPSECME	PQUIP	TLS
JOSE	PRIVACYPASS	UTA
KEYTRANS	RADEXT	
KITTEN	RATS	

IETF

Related Non-SEC Area Activities

Security Topics in Related WGs

ADD
ANIMA
DIEM
DISPATCH
DMARC
DRIP
HTTPBIS
MIMI
NETCONF
NTP
QUIC
SATP
SIDROPS
STIR
TIPTOP
WEBBOTAUTH
WIMSE

Security related IRTF work

CFRG
HRPC
PEARG
SPACE
UFMRG

IAB Programs
datatracker.ietf.org/group/

check for reports on recent workshops

External related

ICANN
W3C
IEEE
ITU
3GPP
CA/B Forum
PKI Consortium
NIST Lightweight Crypto
NIST PQC

New non-WG Mailing Lists since IETF 124

List Name	Purpose
ZIP	ZKP in practice
practical-security	discussion of cyber security strategies
RFC4082-update	updating TESLA (Timed Efficient Stream Loss-Tolerant Authentication)
CFR	Customer Facing Relay

AD sponsored drafts

Draft	**Sponsoring AD**	**Status**
Push-Based Delivery For Multiple Security Event Token (SET) Using HTTP **draft-deshpande-secevent-http-multi-set-push**	Deb	work in progress - comments welcome!
Updates to SFrame Cipher Suites Registry **draft-barnes-sframe-iana-256-00**	Orie/Deb	Finished IETF Last Call

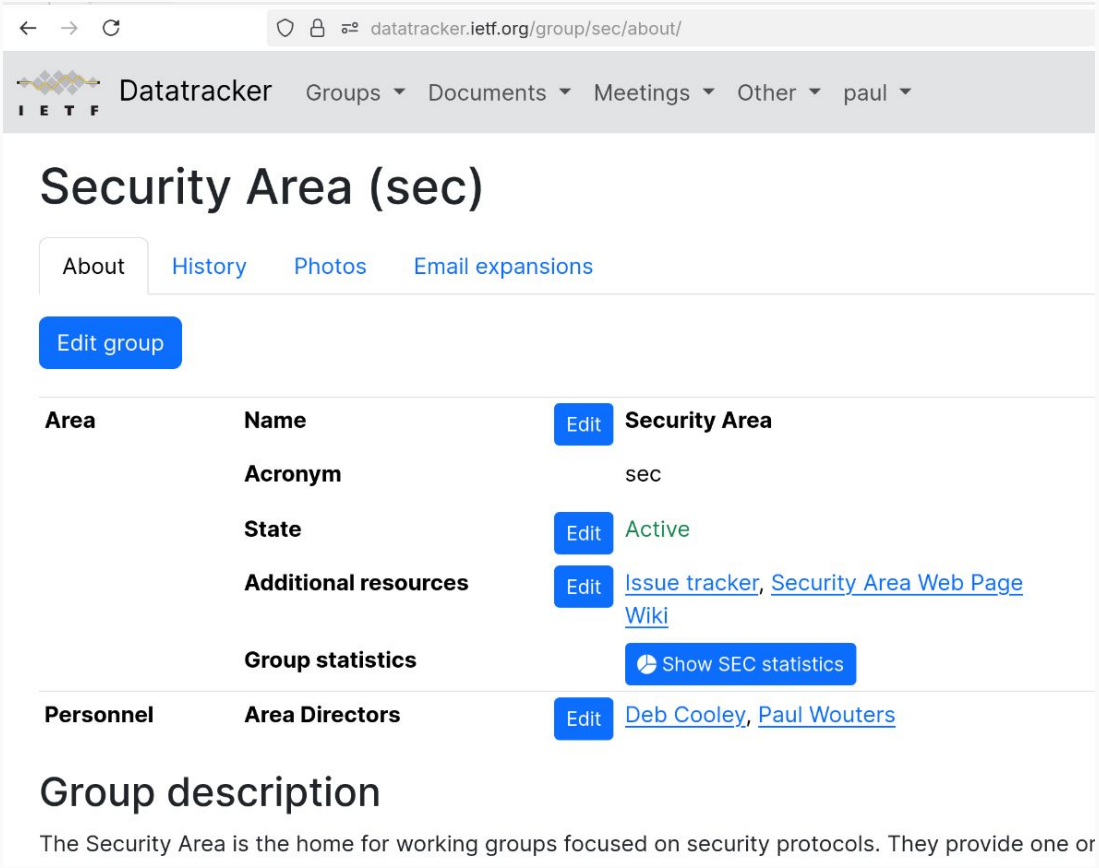
IETF

Security related DISPATCH outcomes of IETF 125

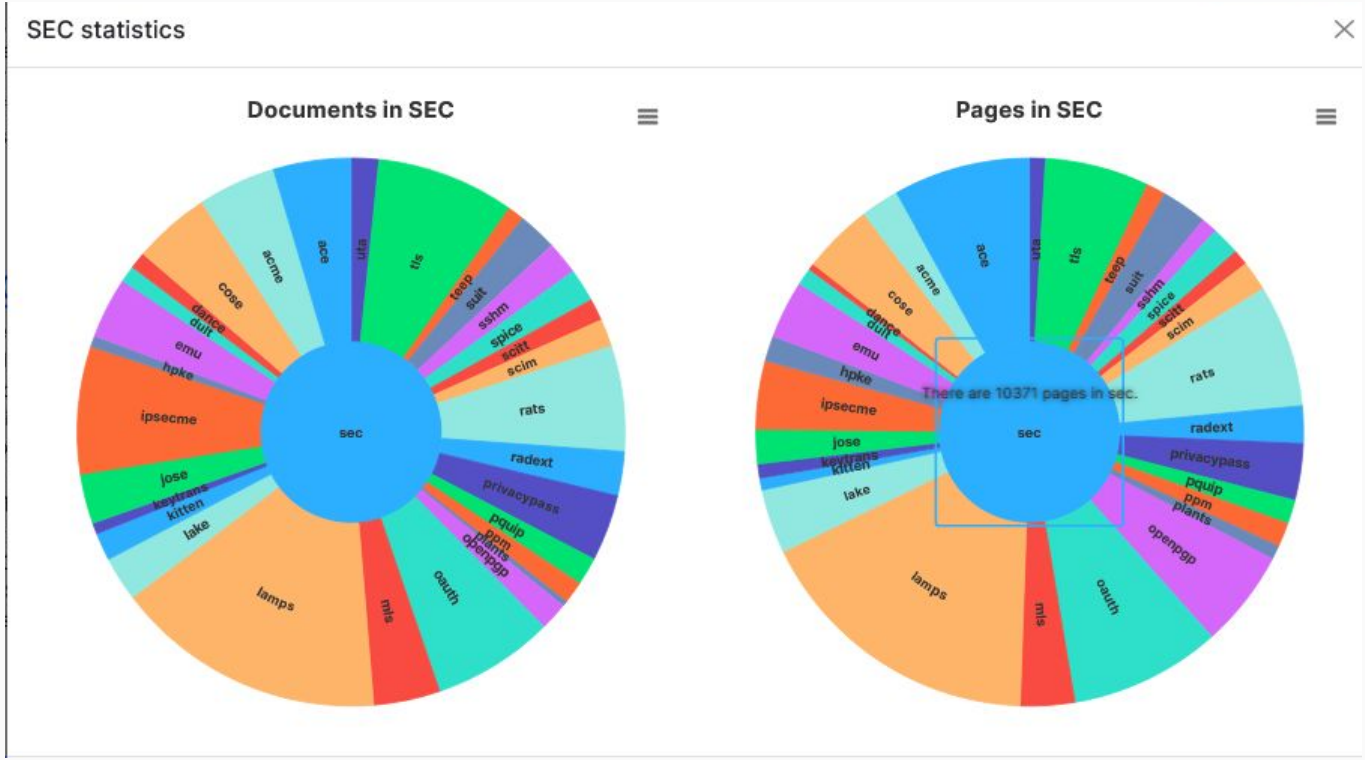
Draft	Outcome
Process Attestation for Human Authorship Verification	TBD*
Security Protocols that optimized for non-web and PQC	TBD*
AI Agent Authentication and Authorization	TBD*

*the results from dispatch/secdispatch will be determined after the meeting due to technical difficulties during the session.

Datatracker WG page statistics



SEC workload:
188 documents, 6695 pages, 32 working groups



Errata processing

	Total Open SEC Errata (non-editorial)	**Since last meeting**	
		Closed	**Reported**
IETF 125	214	48	67
IETF 124	195	31	8
IETF 123	218	21	34
IETF 122	205	n/a	n/a
IETF 121	250	23	18
IETF 120	257	50	27
IETF 119	279	33	17
IETF 118	295	16	15

IETF

Security Area Pointers

- Security Area
  - https://wiki.ietf.org/en/group/sec
- Common SEC AD DISCUSS items
  - https://wiki.ietf.org/group/sec/typicalSECareaissues
- Where is my document that is with AD?
  - https://datatracker.ietf.org/doc/ad/deb.cooley
  - https://datatracker.ietf.org/doc/ad/christopher.inacio
- What is on the next IESG telechat?
  - https://datatracker.ietf.org/iesg/agenda/documents/

IETF

Thanks to all SECDIR reviews !

- The Security Directorate attempts to (security) review all drafts
- Thanks to Tero Kivinen for managing the SECDIR Directorate
  - https://datatracker.ietf.org/group/secdir/about/
- SecDir meets on Tuesday of each IETF during lunch time
  - Free Lunch provided!
- Membership is SEC area Working Group chairs and willing alumni
- Statistics slides will be in the SAAG meeting materials

TLS for BGP and related PKI considerations

IETF

TLS Authentication for BGP
draft-hbq-bgp-tls-auth

Jeffrey Haas, Bob Beck, Yingzhen Qu

Motivation

- BGP, and several other IETF control plane protocols, run over TCP today.
- Most transport security considerations for such protocols hand-wave addressing transport security by saying, “We can use IPsec”.
  - IPsec is mostly not used. It is operationally cumbersome for the control plane.
- BGP provides transport security using TCP-AO (and previously, TCP-MD5) which provides integrity. Authentication is incidentally addressed through pre-shared keys.

Motivation (2)

- There are many proposals to run BGP and other control plane protocols over QUIC.
  - We're not going to talk about these here. See prior talks in RTGAREA in IETF-123/124.
- QUIC uses the **TLS handshake** to get started.
- TLS uses certificates.
  - Most people are familiar with the web PKI when discussing TLS.
  - Web PKI is inappropriate for control plane protocols.
- Today, we're discussing a proposal for a BGP PKI.
  - (**This is really about the TLS handshake... and that's about it**.)

Why are we here at SAAG/SIDROPS?

- To socialize this idea among the security smart part of IETF.
- This work is difficult to dispatch:
  - TLS? We're using TLS? Boring.
  - IDR? BGP is getting new security? Interesting, but IDR doesn't specialize in security.
  - SIDROPS? Lots of expertise about BGP security and certificates, but mostly about RPKI.
- The work is hybrid. It lands between SEC and RTG. We're chatting with both sets of ADs.

Operations

- BGP has an “Autonomous System Number” that represents the network in the protocol.
- BGP is typically (manually) provisioned between routers by the remote (neighbor) IP address for the session.
  - Current security mechanisms are provisioned per-neighbor.

High Level PKI

- A leaf (end-entity) “BGP session certificate” is created for each BGP session. Such a certificate has the AS and (optionally) IP as SAN names.
  - This binds the AS with the IP addresses for the session together.
- Leaf certificates may be generated on demand by the AS, using an intermediate certificate also with the AS SAN name.
- The AS intermediate may distributed to your neighbor AS to be used as a trust anchor for your BGP session, or trusted via it’s issuer.

Certificate Lifetimes

- The lifetime of the AS intermediate should be reasonably long. For example, a year.
- BGP session certificates *SHOULD* be short-lived. Perhaps two weeks. Such certificates *SHOULD* be automatically provisioned.
  - As with any TLS session, the operator might choose to ignore expired session certificates when operationally necessary.
- A goal is to avoid problematic revocation issues when the CRL might not be reachable when establishing BGP session.
  - After all, this is getting your Internet working in the first place!

Establishing Trust

- The desired model is to establish trusted “introducers” for the BGP AS intermediate.
  - An ideal “introducer” is a mutually trusted third party CA.
  - A third party may decide to sign an AS intermediate by validating proof of possession of a key already present in the RPKI (as proof of “AS control”)
    - We are not trying to put these certificates in the RPKI itself!
    - We are not trying to re-use RPKI keys!
- The “introducer” could then be used as a trust anchor itself, or, once validated, the AS intermediates could be trusted directly (Intermediate elision).

Main certificate details

8.2.4.4. Subject Alternative Name (SAN) - Critical

The ASN is carried within the GeneralName type using a specific OID.

Field	Requirement	Specification
subjectAlternativeName	**MUST**	**MUST** be present and **MUST** be marked as CRITICAL.
ASIdentifier	**MUST**	The ASN **MUST** be carried in a GeneralName of type otherName. The OID and structure of this otherName are defined below.
IPAddress	**MAY**	One or more IP addresses **MAY** be carried in the certificate.

Table 6

Validation Procedure

- Rtr-A with AS-X and IP address a.b.c.1
  peers with
  Rtr-B with AS-Y and IP address a.b.c.2
- Rtr-A trusts AS-Y's AS intermediate.
  Rtr-B trusts AS-X's AS intermediate.
- During the TLS handshake, the BGP session certificate is verified and the remote AS number is checked along with the remote IP address.

... that's it.

Next Steps

- Find a home for this BGP work.
  - ... Ideally without starting a whole new Working Group.
    - The core proposal here is small and mostly operationally simple.
      - ... but operational tooling can create a lot of nice-to-haves, such as an ACME-like extension for managing session certificates
        - ... and certificate-anything related to BGP is likely to create a “land grab” to manage an overly complex ecosystem. It’s important that the simple use case can be used on its own, without gaining cross-protocol security concerns.
- Realize that the non-BGP use cases will interest others looking to solve similar transport security issues.
  - ... and thus the simple idea may be a “victim of its own success”.
  - (See the appendix of the draft.)

Questions?

Introduction to the Next Generation Commercial Cryptographic Algorithms Program for China

IETF

新一代商用密码算法征集活动情况

Introduction to Next-generation Commercial Cryptographic Algorithms Program (NGCC)

商用密码标准研究院
INSTITUTE OF COMMERCIAL CRYPTOGRAPHY STANDARDS

2026年3月 March,2026

商用密码 Commerical Cryptography

根据《中华人民共和国密码法》《商用密码管理条例》等法律法规，商用密码是指采用特定变换的方法对不属于国家秘密的信息进行加密保护、安全认证的技术、产品和服务。

According to *Cryptography Law of the People's Republic of China* and *Regulation on the Administration of Commercial Cryptography*, commercial cryptography refers to technologies, products, and services utilized for encryption protection and security authentication on information that does not involve anything of State secrets and the like by using specific transformation methods.

现用商用密码算法体系 Current Commercial Cryptographic Algorithm System

密码算法 Cryptographic Algorithm	行标编号 Industry Standard Number	国标编号 National Standard Number	ISO/IEC标准编号 ISO/IEC International Standard Number
ZUC	GM/T 0001-2012	GB/T 33133-2016	ISO/IEC 18033-4/AMD1:2020
SM4	GM/T 0002-2012	GB/T 32907-2016	ISO/IEC 18033-3/AMD1:2021
SM2	GM/T 0003-2012	GB/T 32918-2016	数字签名算法（Digital Signature）： ISO/IEC 14888-3:2018
SM3	GM/T 0004-2012	GB/T 32905-2016	ISO/IEC 10118-3:2018
SM9	GM/T 0044-2016	GB/T 38635-2020	数字签名算法（Digital Signature）： ISO/IEC 14888-3:2018 标识加密算法（Identity-based Encryption）： ISO/IEC 18033-5/AMD1:2021 密钥交换算法（Key Exchange）： ISO/IEC 11770-3:2021

说明：以上算法按照成为行业标准时间先后进行排序。
Note: The above algorithms are listed in the order of being industry standards.

商用密码标准研究院 Institute of Commercial Cryptography Standards

商用密码标准研究院主要承担商用密码标准战略研究和标准体系实施，商用密码标准制修订，标准试验验证、测试评价、宣贯培训及其科研成果推广应用，标准资源库建设与标准信息服务，以及商用密码国家标准和行业标准秘书处等工作。地址：北京市丰台区南四环西路188号17区10号楼。

Institute of Commercial Cryptography Standards (ICCS) is mainly responsible for conducting research on commercial cryptography standardization strategies, implementing the system of commercial cryptography standards, developing and revising commercial cryptography standards, conducting validation, verification, testing, evaluation, publicity and training of commercial cryptography standards, promoting and applying related scientific achievements, establishing the commercial cryptography standard resource library, offering information services of commercial cryptography standards as well as acting as the Secretariat of national and industry commercial cryptography standards.

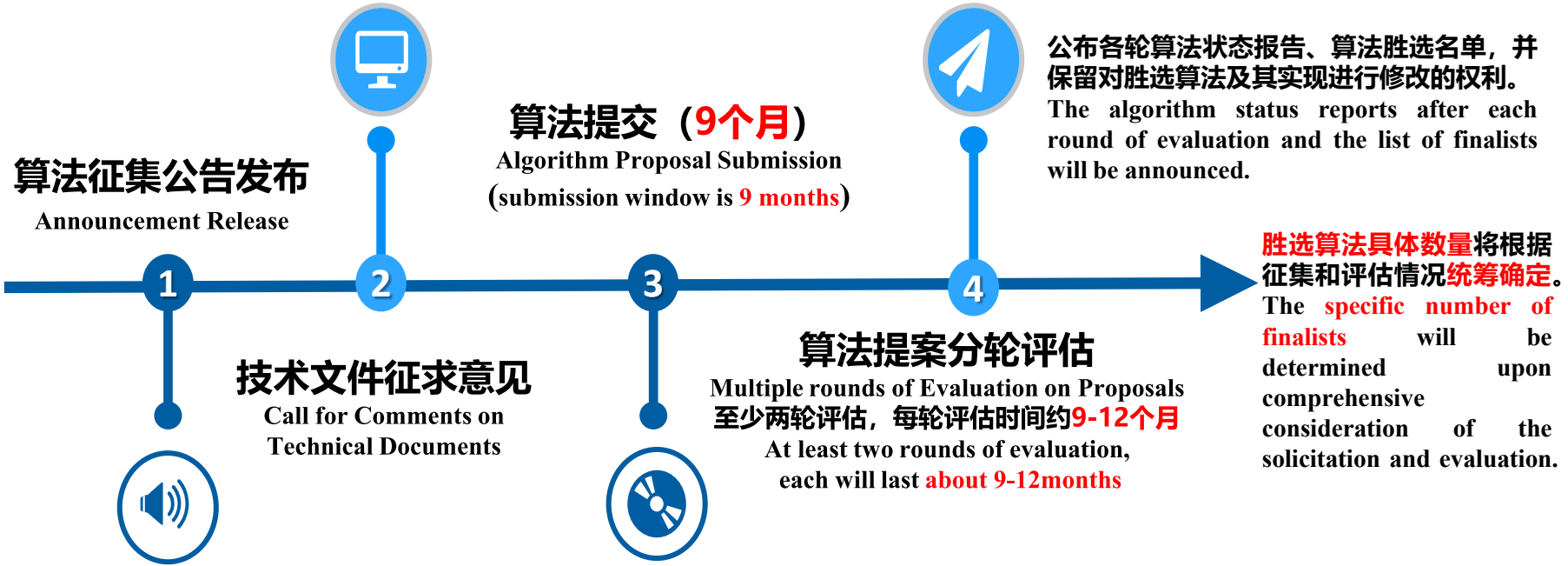
Address: Bldg 10, Area 17, No. 188, South 4th Ring Road West, Fengtai District, Beijing

新一代商用密码算法征集活动(NGCC)

为了抵抗量子计算风险，同时满足大数据、物联网、云计算、人工智能等新技术新应用的发展需求，商用密码标准研究院计划征集公钥密码算法、密码杂凑算法和分组密码算法等3类算法，在前期国际密码研究工作取得的成果基础上做出新探索，希望进一步促进密码算法设计与分析技术发展创新，进一步丰富密码算法特别是抗量子计算密码算法的新颖性、多样性，进一步推动国际密码学术交流、繁荣密码学科发展，以期形成相互适配的新一代商用密码算法体系，推动新一代商用密码算法标准制定。

In response to the threat of quantum computing and to accommodate the evolving demands of emerging technologies such as big data, Internet of Things, cloud computing and artificial intelligence, ICCS plans to call for proposals for public-key cryptographic algorithms, cryptographic hash algorithms and block cipher algorithms. This represents a new exploration building upon acquired research achievements of the international cryptography community, seeking to further stimulate innovation in cryptographic algorithm design and analysis techniques, to enhance the novelty and diversity of cryptographic algorithms (particularly post-quantum public-key cryptographic algorithms), to drive more international academic communications and promote the advancement of cryptography. NGCC expects to establish an interoperable cryptographic algorithm suit and facilitate the standardization of the next-generation commercial cryptographic algorithms.

新一代商用密码算法征集活动(NGCC)



新一代商用密码算法征集活动(NGCC)

2025年2月5日，发布算法征集活动公告，正式启动算法征集工作。

On February 5, 2025, ICCS released the announcement of launching NGCC on its official website (https://www.niccs.org.cn), marking the beginning of the program.

新一代商用密码算法征集活动(NGCC)

同步，发布技术文件征求意见通知。

ICCS issued a global call for comments on submission requirements and evaluation criteria (draft) for public-key cryptographic algorithms and cryptographic hash algorithms.

新一代商用密码算法征集活动(NGCC)

Next-generation Commercial Cryptographic Algorithms Program (NGCC)

Home > Notice

Call for Proposals for the Next-generation Public-Key Cryptographic Algorithms

2025-10-09

Font size: Big Middle Small

On February 5, 2025, the Institute of Commercial Cryptography Standards (ICCS) launched the Next-generation Commercial Cryptographic Algorithms Program (NGCC), and released the call for global comments on *Submission Requirements for Public-Key Cryptographic Algorithms (Draft)* and *Evaluation Criteria for Public-Key Cryptographic Algorithms (Draft)*. After the public comment period, ICCS convened experts to conduct a thorough review and evaluation on all the received comments, and revised these two documents. Now ICCS officially releases the *Submission Requirements for Public-Key Cryptographic Algorithms*, and the *Evaluation Criteria for Public-Key Cryptographic Algorithms*.

From now on, ICCS commences the collection of public-key cryptographic algorithms proposals. The deadline for algorithm submission is 24:00 Beijing Time (UTC+8) on June 30, 2026. From May 1 to June 30, 2026, submitters could update the previously submitted proposals but could not submit new proposals. After the deadline, ICCS will conduct initial examinations and then announce the candidate algorithms for the first round of evaluations.

Packages should be sent to ICCS in both electronic and printed forms prior to the deadline (based on the sending time). For electronic packages, please send to *pkcsubmit@niccs.org.cn*. For printed packages, please mail to Institute of Commercial Cryptography Standards, Building 10, Area 17, No. 188 South 4th Ring Road West, Fengtai District, Beijing, P.R.China (postal code: 100160, phone number for receiving deliveries: +86-10-63057171). For further inquiries, please contact us via email: *pkccomment@niccs.org.cn*.

Attachments:

1. *Submission Requirements for Public-Key Cryptographic Algorithms*
2. *Evaluation Criteria for Public-Key Cryptographic Algorithms*
3. *Feedback on the Comments Received on the Draft Submission Requirements and Evaluation Criteria for Public-Key Cryptographic Algorithms*

Institute of Commercial Cryptography Standards, China

October 9, 2025

Copyright © 2025 Institute of Commercial Cryptography Standards
Address: Bldg 10, Area 17, No. 188, South 4th Ring Road West, Fengtai District, Beijing
Registration Number: 2024100746
Email: svr@niccs.org.cn
Visits: 148812

Next-generation Commercial Cryptographic Algorithms Program (NGCC)

Home > Notice

Call for Proposals for the Next-generation Cryptographic Hash Algorithms

2025-10-09

Font size: Big Middle Small

On February 5, 2025, the Institute of Commercial Cryptography Standards (ICCS) launched the Next-generation Commercial Cryptographic Algorithms Program (NGCC), and released the call for global comments on *Submission Requirements for Cryptographic Hash Algorithms (Draft)* and *Evaluation Criteria for Cryptographic Hash Algorithms (Draft)*. After the public comment period, ICCS convened experts to conduct a thorough review and evaluation on all the received comments, and revised these two documents. Now ICCS officially releases the *Submission Requirements for Cryptographic Hash Algorithms*, and the *Evaluation Criteria for Cryptographic Hash Algorithms*.

From now on, ICCS commences the collection of cryptographic hash algorithms proposals. The deadline for algorithm submissions is 24:00 Beijing Time (UTC+8) on June 30, 2026. From May 1 to June 30, 2026, submitters could update the previously submitted proposals but could not submit new proposals. After the deadline, ICCS will conduct initial examinations and then announce the candidate algorithms for the first round of evaluations.

Packages should be sent to ICCS in both electronic and printed forms prior to the deadline (based on the sending time). For electronic packages, please send to *crypthashsubmit@niccs.org.cn*. For printed packages, please mail to Institute of Commercial Cryptography Standards, Building 10, Area 17, No. 188 South 4th Ring Road West, Fengtai District, Beijing, P.R.China (postal code: 100160, phone number for receiving deliveries: +86-10-63057171). For further inquiries, please contact us via email: *crypthashcomment@niccs.org.cn*.

Attachments:

1. *Submission Requirements for Cryptographic Hash Algorithms*
2. *Evaluation Criteria for Cryptographic Hash Algorithms*
3. *Feedback on the Comments Received on the Draft Submission Requirements and Evaluation Criteria for Cryptographic Hash Algorithms*

Institute of Commercial Cryptography Standards, China

October 9, 2025

Copyright © 2025 Institute of Commercial Cryptography Standards
Address: Bldg 10, Area 17, No. 188, South 4th Ring Road West, Fengtai District, Beijing
Registration Number: 2024100746
Email: svr@niccs.org.cn
Visits: 148811

2025年10月9日，发布公钥和密码杂凑算法征集通知，正式接收算法提案。

On October 9, 2025，ICCS issued a notice soliciting proposals for public-key cryptographic algorithms and cryptographic hash algorithms. ICCS released the official version of the requirements and evaluation criteria for the two algorithms, along with feedback on related issues.

新一代商用密码算法征集活动：

开始提交公钥、杂凑算法提案！

Next-generation Commercial Cryptographic Algorithms Program (NGCC)：

Call for proposals!

新一代商用密码算法征集活动(NGCC)

注 意:

- 以上两个算法提交时间为2025年10月9日至2026年6月30日
  其中，2026年5月1日至6月30日仅可对已提交的算法提案进行更新，不可提交新的算法提案
- 算法提案电子文件提交方式:
  公钥密码算法提交邮箱：pkcsubmit@niccs.org.cn
  密码杂凑算法提交邮箱：crypthashsubmit@niccs.org.cn
- 算法提案纸质文件递交地址:
  商用密码标准研究院（收件地址：北京市丰台区南四环西路188号17区10号楼)

Attentions:

- The submission period for these two algorithms is from October 9, 2025, to June 30, 2026.
  From May 1 to June 30, 2026, submitters could update the previously submitted proposals but could not submit new proposals.
- For electronic packages, please send to pkcsubmit@niccs.org.cn and crypthashsubmit@niccs.org.cn
- For printed packages, please mail to Institute of Commercial Cryptography Standards, Building 10, Area 17, No. 188 South 4th Ring Road West, Fengtai District, Beijing, P.R.China .
- Packages should be sent to ICCS in both electronic and printed forms prior to the deadline.

新一代商用密码算法征集活动(NGCC)

ICCS will conduct initial examinations and then announce the candidate algorithms for the first round of evaluations.

将按照算法提交要求开展形式审查，并统一公布进入第一轮评估的候选算法。

ICCS组建算法征集专家组，负责相关技术工作；算法遴选从算法安全性、性能、特点等方面进行综合评估，鼓励进行理论创新、结构创新。

ICCS established expert groups responsible for the technical work of NGCC; the candidate algorithms will be comprehensively evaluated in terms of security, performance, features and etc. Innovation in theories and structures is expected.

ICCS promotes active participation of social forces in public review of algorithms. ICCS will release mailing lists of public review.

鼓励社会力量积极参与算法公开评议，后续将发布公开评议的邮件列表。

鼓励在算法设计工作中加强国际合作。

ICCS encourages international cooperations in algorithm design.

新一代商用密码算法征集活动(NGCC)

算法征集相关技术问题和意见建议，请通过电子邮箱反馈：

For further inquiries, please contact us via emails:

公钥密码算法咨询邮箱(public-key algorithms)：pkccomment@niccs.org.cn

密码杂凑算法咨询邮箱(hashing algorithms)：crypthashcomment@niccs.org.cn

欢迎访问官方网站：https:// www.niccs.org.cn

感谢关注！

Thank you for your attention!

Securing QUIC with MLS

IETF

Security Considerations for Space Settings

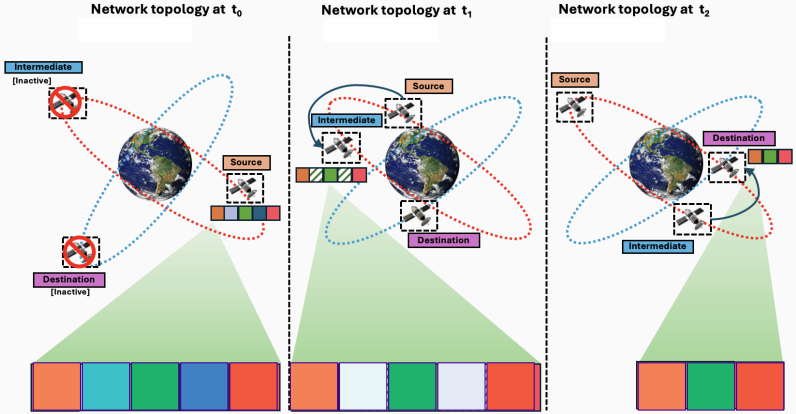
IETF Security Area Open Meeting

Benjamin Dowling
benjamin.dowling@kcl.ac.uk

March 20, 2026

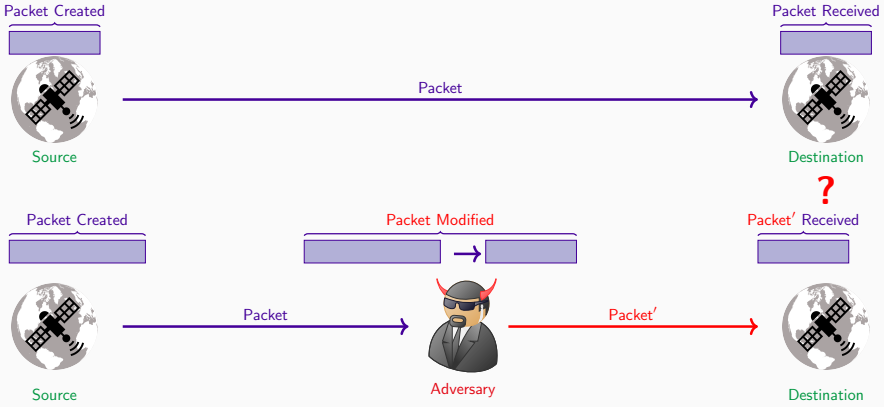
Functional Requirements

"Until full coverage..., the orbiters and other assets that are facing intermittent communications should provide store-and-forward capability." - **IP in Deep Space: Key Characteristics, Use Cases and Requirements**



Security Requirements

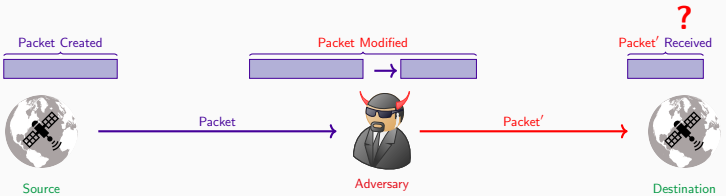
Need a mechanism to ensure confidentiality / authenticity.



But these properties can be quite fine-grained. Will address soon!

Realistic Threat Model?

"... over time it is possible that connectivity to the Internet may become available for some mission assets, and eventually interplanetary networks could become part of the Internet."

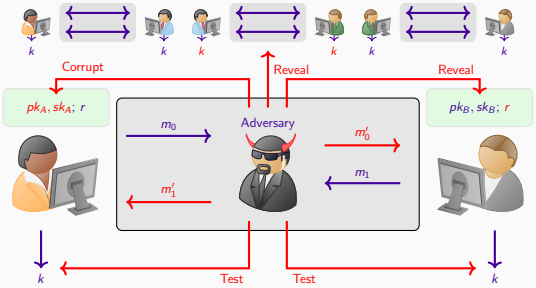


"Space exploration is more than ever carried by multiple stakeholders. A mixture of assets operated by government, commercial, and academic/research organizations from multiple nations are deployed." - **IP in Deep Space: Key Characteristics, Use Cases and Requirements**

Threat Modelling for Space

Security properties inform the design of the protocols we will use. What is an appropriate threat model? Typically, in the analysis of real-world cryptographic protocols (TLS, SSH, Signal, etc) we tend to consider security against an attacker that:

- is in complete control of the network,
  - Cryptographic modelling norm for network adversaries
- can **Compromise** derived keys k,
- can **Corrupt** long-term secrets (pk, sk),
- can **Exploit** bad randomness r



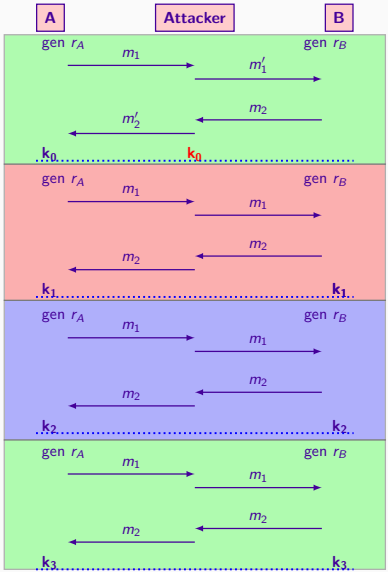
Threat: Network adversary capable of compromising one or more of the endpoints. Security should be resilient against such an advesary.

Fine-grained Security Considerations

Secure Channel protocols today realise advanced security properties:

- **P**erfect **F**orward **S**ecrecy
  - The adversary cannot read ciphertexts sent before a compromise.
- **P**ost **C**ompromise **S**ecurity
  - The adversary cannot read ciphertexts sent after a "healing" period post-compromise.

Both consider security in the face of adversary compromise, and both are standard expectations of security for long-lived protocols, such as those used in the space setting.

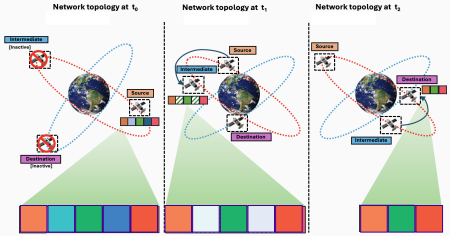


Space Setting Challenges

"Compared to Internet on Earth, deep space communications and networking have multiple challenges, such as:

- *Significant and variable delays (e.g. ... multiple seconds, minutes, or hours).*
- *Frequent and long interruptions of communications, often with no alternate path."*

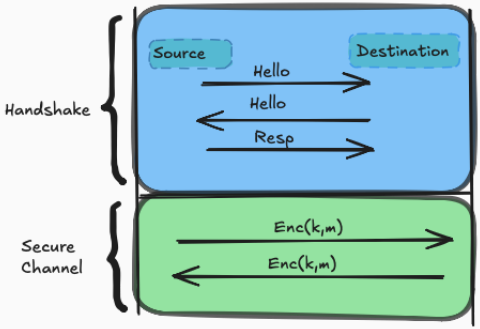
- IP in Deep Space: Key Characteristics, Use Cases and Requirements



Packet loss is even more difficult to address in space setting, since the delays and interruptions hide whether packet loss occurred (and lead to incomplete secure channel establishment).

Handshakes and Packet Loss

To achieve confidentiality and authentication, we need to establish keys for secure communication. In secure communication these are typically called handshakes



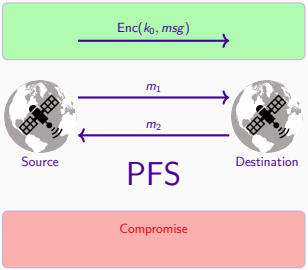
Any delay or dropping of packets prevents key establishment.

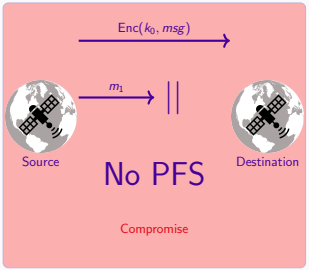
Let's assume you have some probability of packet loss P_{pl}. Logically, as the number of messages in the handshake increases, then so too does the probability of the handshake failing due to packet loss:
$(1 - P_{pl}), (1 - P_{pl})^2, (1 - P_{pl})^3, \ldots$

Thus, delays or dropping of handshake messages extends impact of compromise due to delayed secure payload communication.

Impact of Delay/Dropping on Security

Any delay in a handshake extends the window/impact of compromise.

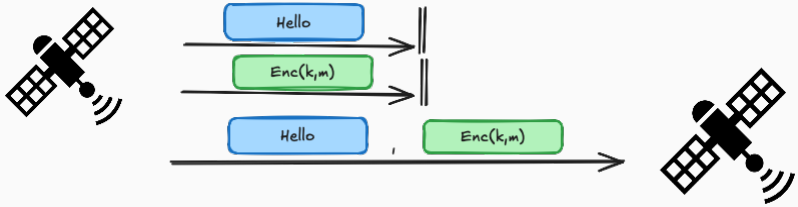




More communication needed to establish goals gives more changes for delays to key refresh, and thus extends the impact of compromise.

Async vs Sync Handshakes

Asynchronous support allows for entities to be offline, thus massive delays in handshake messages can be resolved.



Asynchronous handshakes allow for key establishment (and key refresh) without both parties being interactive.

This allows for resilience against packet loss during key establishment, shortening the impact of the window of compromise.

What would an appropriate protocol look like?

Goals – Setting

- **Asynchronous key agreement protocol**
- **Standardised**, composes with different symmetric protocols
- **Sessions are long-lasting** to avoid costly handshake authentication
- Low bandwidth & complexity
- (Optional) Can handle groups of devices and dynamic group membership

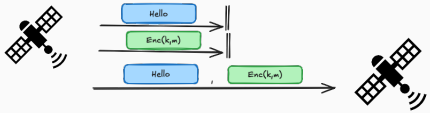
Goals – Security

- E2E Authenticity and Confidentiality
- Adversarial Model
  - MiTM: Network, Delivery Service compromised
  - Corruption: Can heal from state compromise
  - Adaptive and Active Adversary
- **Forward and Post-Compromise Security**

So, what now?

There are a number of Working Groups that are starting to look at what network protocols should be used in space settings:

- **TIPTOP: Taking IP to Other Planets**
  - IP in Deep Space: Key Characteristics, Use Cases and Requirements
  - An Architecture for IP in Deep Space
  - QUIC Profile for Deep Space
- **DTN: Delay Tolerant Networking**
- **SPACERG: Systems and Protocol Aspects for Circumstellar Environments Research Group**



Whatever security we put up there in space will be hard to upgrade and replace, so let's make sure that we get it right the first time.

Thank you for your time.

Any Other Business / Open MIC

IETF