Global Alliance
for Genomics & Health

# GA4GH Encrypted Format

## Minutes and Actions 2023 - 2025

These are the minutes for the Encrypted Format meetings, a subgroup of the GA4GH Large Scale Genomics Work Stream. For further information, please visit the GA4GH Work Stream page.

**Table of Contents**

Global Alliance for Genomics & Health



# Meeting Protocols

- Please note that by participating in meetings, attendees agree to adhere to the GA4GH Standards of Professional Conduct.
- Meetings may be recorded for note-taking purposes. Recordings will be deleted within three months of the meeting taking place.
- Dates should be specified in the international format yyyy-mm-dd

## 2025-MM-DD: Template

Chair: Rob Davies (Sanger), Frédéric Haziza
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | | |
| | A.O.B. | |

# Agendas, Minutes and Actions

## 2025-10-??:

Chair: Rob Davies (Sanger), Frédéric Haziza

Global Alliance
for Genomics & Health

Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Python implementation | Fred |
| 4. | ML-KEM in SSH:<br>● https://www.ietf.org/archive/id/draft-ietf-sshm-mlkem-hybrid-kex-03.html<br>● Post-Quantum Kex: https://www.openssh.com/pq.html<br>● OpenSSH 10.1: https://www.openssh.com/releasenotes.html#10.1p1<br>● Add warning in implementations for risk of "store now, decrypt later" attacks.<br>● SSH uses:<br>**** WARNING: connection is not using a post-quantum key exchange algorithm.**<br>**** This session may be vulnerable to "store now, decrypt later" attacks.**<br>**** The server may need to be upgraded. See https://openssh.com/pq.html**<br>We could adapt the text for the header encryption (and maybe add a link to some documentation, like crypt4gh.readthedocs.org/post-quantum.html) | Fred |
| 5. | ML-KEM in OpenSSL v3.5:<br>https://github.com/openssl/openssl/blob/master/doc/man7/EVP_KEM-ML-KEM.pod<br>Docs: https://docs.openssl.org/3.6/man7/EVP_KEM-ML-KEM/ | |
| 6. | Note: FIPS 203: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf<br>(aka ML-KEM) | |
| | A.O.B. | Reggan |

Meeting recording:

Meeting minutes:

Global Alliance for Genomics & Health

# 2025-09-16:

Chair: Rob Davies (Sanger), Frédéric Haziza
Attendees “Name (Affiliation)”: Reggan Thomas , Oscar Martinez (EGA)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Python implementation | Fred |
| 4. | Possible solutions to the AES-256-GCM file size limit<br>https://github.com/C2SP/C2SP/blob/main/XAES-256-GCM.md<br>https://eprint.iacr.org/2025/758.pdf | Rob Davies |
| | A.O.B.<br><br>Connect poster - GA4GH poster template blank.pptx<br>Deadline - 25th Sep | Reggan |

Meeting recording:
https://us02web.zoom.us/rec/share/Hdr0ek6FbsojB3Vwkma80mo_3F1Lbkl8Ebxg_5mFFCQW3z6Bw1ATyQtfBEO2008q.MCh9ClHz2ndM8wU9

Meeting minutes:

Progress on Python and Encryption Implementation

•Fred reports no progress on the Python implementation and suggests adding a flag for version 2.
•Fred mentions the need to set a deadline for implementation in Python and C.
•Rob discusses limited time to work on the project due to other commitments.
•Fred and Rob discuss the quantum project and its impact on encryption.

Quantum Resistance and Encryption Standards

•Rob talks about the potential threat of quantum computers to current encryption methods by 2035.
•Fred and Rob discuss the replay problem and the need for quantum-resistant encryption.
•Oscar mentions a federal meeting where quantum resistance was discussed but not a major concern currently.

•Rob keeps an eye on the maturity of quantum key exchange libraries.

FIPS Standard Encryption and Data Limits

•Rob introduces a question from American friends about FIPS standard encryption.
•Rob discusses a paper on expanding data limits using new key generation methods.
•Fred and Rob discuss the notation and combinatorial aspects of the paper.
•Rob suggests using the method to comply with FIPS standards and keep American friends happy.

Implementation Details and Specification Changes

•Fred and Rob discuss the need to implement the new method as part of version 2.
•Reggan mentions the need to submit landscape, use case, and implementation details documents.
•Fred suggests implementing the new method for version 1 to make American friends happy.
•Rob and Fred discuss the limitations of GCM and the need for a new algorithm.

Poster Preparation and Deadline

•Reggan mentions poster and the need to finalize the contents.
•Fred offers to create a graphic of the new header for the poster.
•Reggan states the deadline for the poster is 25th September and needs to be reviewed by the comms team.
•Fred agrees to create the graphic and send it to Reggan.

Discussion on Edit List and Data Integrity

•Fred discusses the limitations of the edit list and the potential for adding non-relevant data.
•Rob suggests that the edit list is for user requests and not for preventing data reading.
•Fred proposes adding a specification to limit the number of blocks that can be skipped.
•Rob and Fred discuss the complexity of implementing the limit and its effectiveness.

Quantum Programming Demo
•Rob introduces a demo on quantum programming and its applications.
•Rob explains the process of encoding data on a quantum state and its potential uses.
•Rob mentions the use of quantum computers for phylogenetic tree generation and optimization problems.
•Rob discusses the types of quantum computers available and their limitations.

Conclusion and Next Steps

•Fred thanks everyone for the meeting and sets the next meeting date for 14th October.
•Rob and Fred discuss the need to stop the recording for the quantum programming demo.
•Rob explains the process of running a quantum circuit and its potential failures.
•Rob mentions other demos and applications of quantum computing, including error correction and optimization.

Global Alliance
for Genomics & Health

## 2025-06-22:

Chair: Rob Davies (Sanger), Frédéric Haziza (SGDL Health)
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Possible solutions to the AES-256-GCM file size limit<br>https://github.com/C2SP/C2SP/blob/main/XAES-256-GCM.md<br>https://eprint.iacr.org/2025/758.pdf | |
| | A.O.B. | |

Meeting recording:
Meeting minutes:

## 2025-06-24: Age encryption format

Chair: Rob Davies (Sanger), Frédéric Haziza (SGDL Health)
Attendees “Name (Affiliation)”: Dmitry R (BSC / Elixir- ES), Reggan Thomas
Apologies: Oscar Martinez (EGA)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | age encryption format | |

| | | |
|---|---|---|
| | A.O.B.<br>Connect session proposals - Deadline - July 3rd. Submit your proposal here | |

Meeting recording:
Meeting minutes:

## 2025-05-27:

Chair: Rob Davies (Sanger), Frédéric Haziza (SGDL Health)
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | | |
| | A.O.B. | |

Meeting recording:
Meeting minutes:

## 2025-05-06: Specification - V2

Chair: Rob Davies (Sanger),
Attendees “Name (Affiliation)”: Oscar Martínez (EGA), Reggan Thomas (GA4GH)
Apologies : Frédéric Haziza (SGDL Health)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | Rob |
| 2. | Previous Actions Review | Rob |
| 3. | Specification version 2 progress | Rob |
| | A.O.B.<br>Next meeting - 27 May, 2025 | |

Meeting recording:
https://us02web.zoom.us/rec/share/vvpFXIuygzseIcCIknpk3MZUn8TNIRWHKQyqPJmSqZJYFVGd0Gi8XgtwDY0sI5DE.JV6WXGTJ75aHfm_C

Meeting minutes:

**Specification Updates and Encryption Methods**
- Rob mentions working on the specification and fixing errors, such as using the wrong type of random number generator.
- Oscar brings up the GitHub report and the need to add signatures and time-based features.
- Rob talks about the experimental nature of quantum encryption and the availability of a new quantum computer at PSC.
- Oscar explains the public access process for using the quantum computer.

**Encryption Issues and Meeting Planning**
- Oscar shares a user issue with decrypting files due to generating a new keypair for each file.
- Rob notes the difficulty in diagnosing encryption failures without binary data analysis.
- Reggan mentions the planning for a meeting in May or June due to a busy schedule in May.
- Rob confirms the next meeting date as the 27th of May and suggests getting back to regular updates.

## 2025-04-08: DRS integration with Crypt4gh

Chair: Rob Davies (Sanger), Frédéric Haziza (SGDL Health)
Attendees “Name (Affiliation)”: Oscar Martínez (EGA)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |

| | | |
|---|---|---|
| 3. | Cloud workstream / DRS requirements | |
| | A.O.B. | |

Meeting recording:
https://us02web.zoom.us/rec/play/IeoG9tb2rezaEdeir1-qWNoqHB2CftTi4R5Alb_oEY3je3IEGBWrCyDZA0u2ZA_4ToErQUOjmLOJbDb-.Gdv_hoysEqfy6OJY?accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fus02web.zoom.us%2Frec%2Fshare%2FXnf7f2G7il5ULUWkiEYXVk6l1VHZ78Ct0C_4LUQBU0HIb_DwZCmFwi0Y0JvM0xZP.uo3OdGS_LmivH0EQ

Meeting minutes:
Discussed about DRS integration with crypt4g.

## 2025-03-04:

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | Rob / Fred |
| 2. | Previous Actions Review | Rob/Fred |
| 3. | Quick review of team leads meeting on 25/2 | Rob/Fred |
| 4. | Priorities for 2025 | Rob/Fred |
| 5. | Product approval timeline | Reggan |
| | A.O.B.<br><br>Next meeting - 1st April - Cancel or reschedule? | |

Meeting recording:
Meeting minutes:

List of documents to be produced for v2.0

22. Final presentation to Product Steering Committee for approval that the product development has followed this Product Development and Approval Process

22.1 The following should be shared with Product Steering Committee at least two weeks before the call where a vote is scheduled:
22.1.1 outputs listed under **point 10** and under **point 14**
22.1.2 evidence of outreach
22.1.3 evidence that those who registered interest in the product were kept informed.

Point 10
10. The PRC reviews the outputs from the Study Group/phase.
10.1 Outputs to be reviewed include:
10.1.1 landscape analysis
10.1.2 use cases (and whose use cases they are)
10.1.3 list of potential adopters who have expressed interest
10.1.4 Problem Statement defining the topic and stating clearly what will be in and out of scope
10.1.5 if the product is from outside GA4GH or an update to an existing product, a summary of the views of those who adopted the previous version of the product

Point 14
4.8 Outputs:
14.8.1 decision record documenting the major decisions taken during development, and why they were taken
14.8.2 the product specification
14.8.3 implementations
14.8.3.1 There should be at least two implementations created by independent groups (i.e. not two implementations created by the same entity for two different projects). Ideally, the second implementation would be built from the specification to demonstrate a clear specification.
14.8.3.2 At least one of these implementations should be open. This can be a reference implementation and need not be in use for any purpose other than acting as a reference. Implementations produced by the GA4GH staff Tech Team can be used to fulfil this criteria, but no guarantee is made of the Tech Team being able to provide support.
14.8.3.3 Interoperability of these implementations should have been demonstrated.
14.8.3.4 In client server models (or any two-part system, including read and write), there should be both two client and two server implementations, operating in different systems.
14.8.3.5 Work Streams do not need to build the implementations. The intention is that these would be built by Driver Projects.
14.8.3.6 Implementation work should inform the development process.
14.8.3.7 In exceptional circumstances, where a second implementation cannot be taken forward and there is strong reason to believe benefits to the community are being blocked, a group can proceed without a second implementation but must clearly present the rationale for this decision. An example where this might apply could be file format compression encoders. In such a case, many decoders could be expected, but few anticipate implementing an encoder. As such, it might be judged appropriate to move forward with one encoder and two decoders. A decision should be made based on available information and in the best interests of the established user community. This is intended for exceptional circumstances only and is not the appropriate route in most cases.

14.8.4 documented feedback from adopters
14.8.5 a road map for taking the product forward from approval to adoption, identifying future work to support adoption
14.8.5.1 Examples of such activities could include: working with key stakeholders to support adoption; addressing specific blocks to adoption; developing documentation, outreach efforts, demonstrations of utility of the product; and more.
14.8.5.2 We should acknowledge that adoption should be driven by the community choosing freely, but should seek to remove impediments obstructing adoption, making adoption as accessible as possible

Sample :
Output :
**Landscape** :
10.1.1 landscape analysis
https://docs.google.com/spreadsheets/d/1Mynb5DJg5fBjliLdTffjCtZCbHoc0AIx/edit?gid=918240547#gid=918240547
10.1.2 use cases (and whose use cases they are)
https://seqcol.readthedocs.io/en/latest/specification/#use-cases
10.1.3 list of potential adopters who have expressed interest
https://docs.google.com/presentation/d/1RfS1q3lG9BpxiNrrqv2MSQmoNcRFPM5FvEjaZ7r86xU/edit#slide=id.g41b4775345_0_2
22.1.2 evidence of outreach -
https://www.ga4gh.org/announcement/refget-sequence-collections-v1-0-open-for-public-comment/
22.1.3 evidence that those who registered interest in the product were kept informed. – Minutes of the meeting ? -
https://docs.google.com/document/d/18VIGjcEC7B8XMbqh1E2afTMdbEo9WMK1/edit#heading=h.gjdgxs
10.1.4 Problem Statement defining the topic and stating clearly what will be in and out of scope
14.8 Outputs:
14.8.1 decision record documenting the major decisions taken during development, and why they were taken -
ADR - https://seqcol.readthedocs.io/en/latest/decision_record/#architectural-decision-record
14.8.2 the product specification Specification URL -
https://seqcol.readthedocs.io/en/latest/specification/
**14.8.3 implementations**
Web Front End / Client Implementation 1 URL
https://github.com/refgenie/refget
https://github.com/refgenie/refget/blob/master/refget/seqcol_client.py
Web Front End / Client Implementation 2 URL
*https://seqcolapi.databio.org/links_demo.html*
Server Implementation 1 URL
Code: https://github.com/refgenie/seqcolapi
https://github.com/refgenie/refget
Live server: https://seqcolapi.databio.org/
Server Implementation 2 URL
*https://github.com/EBIvariation/eva-seqcol*
*https://45.88.81.158:8081/eva/webservices/seqcol/*

Global Alliance for Genomics & Health

14.8.4 documented feedback from adopters - https://docs.google.com/spreadsheets/d/1NScZPC34tZ2MTel1lyTBDb645_XDlQc0/edit?gid=1990768165#gid=1990768165
14.8.5 a road map for taking the product forward from approval to adoption, identifying future work to support adoption
https://docs.google.com/document/d/16W5w9mlt8NtMSB1VByMNUenUeiM1PDOD/edit

## 2025-02-04:

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”: Denis Akzam (Ariadne Geometry),Reggan Thomas (GA4GH), Oscar Martinez Llobet (EGA)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Completing V2 spec | Rob | |
| 2 | Completing V2 python implementation | Fred | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | | |
| | A.O.B.<br>Next meeting is on March 4th at 3 pm | |

Meeting recording:
Meeting minutes:

The meeting discussed updates to the encryption method, including a revised PDF document with new encryption and decryption instructions. The team debated whether to stop on the first error during decryption or continue. Version 2 of the header was updated to include new packet types and algorithms. The implementation in Python is ongoing, with plans to add extra headers and signatures. The team considered the impact of quantum computers on symmetric ciphers and decided to wait for more mature post-quantum algorithms. The next steps include finalizing the spec and implementation by March, aiming for approval at the April Connect meeting.

Progress on Encryption Method and Document Updates

Rob shares updates on a revised PDF document with new encryption methods
Fred and Speaker 1 discuss error handling during decryption
Rob mentions a list of differences and additional packets
Denis inquires about the versioning of the encryption method

Global Alliance
for Genomics & Health

Discussion on Versioning and Header Changes
Fred explains the differences between version 1 and version 2 of the header
Denis asks about the possibility of version 3 if the header changes again.
Rob mentions a list of differences and additional packets.
Denis4 discusses the importance of wording in the specification, such as "must" versus "should

Key Management and Security Considerations
Rob and Denis discuss the separation of key management from the crypto spec.
Rob mentions the various key management solutions available
Denis asks about the date on the document and the versioning process.
Fred and Rob discuss the importance of secure key storage and the role of key management systems

Next Steps and Meeting Schedule
Reggan asks about the timeline for releasing version 1.2
Fred suggests using the Connect meeting in April as a deadline
Reggan outlines the steps needed for product approval and regulatory compliance
Fred and Reggan discuss the process for getting approval from the Global Alliance.

## 2024-12-10: Post-quantum cryptography

Chair: Rob Davies (Sanger)
Attendees “Name (Affiliation)”:Reggan Thomas (GA4GH) , Oscar Martinez Llobet (EGA), Denis Akzam (Ariadne Geometry)
Apologies:  Frédéric Haziza (GIP-CAD

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Post-quantum cryptography:<br>Open Quantum Safe<br>Post-Quantum Cryptography Alliance | |
| | A.O.B.<br><br>- Connect meeting - 1 to 4 April 2025 • Broad Institute of MIT and | |

| | | |
|---|---|---|
| | Harvard, USA<br>**Register for Connect**<br><br>- Add your connect session proposal to the Easyretro board here by 6th Jan<br>  - Need to submit proposals in the form by 13th Jan<br><br>Next meeting is on Jan 7th,2025 at 3 pm BST | |

Meeting recording:

Meeting minutes :

- Cosmian kms

https://swissbiotechday.ch

Summary:
The meeting focused on the development and implementation of post-quantum cryptography, particularly for genomic data protection. Key points included the current limitations of post-quantum libraries, the need for a background document detailing adoption barriers, and the importance of standard libraries for mainstream use. The discussion also covered the use of asymmetric and symmetric encryption, key management systems, and the potential for quantum computers to break current encryption methods. The participants emphasized the importance of confidential computing and trusted enclaves, and discussed upcoming events like Swiss Biotech Day for showcasing their work. The next Connect meeting was scheduled for April 1-4, 2024.

Action Items
- Provide a "backgrounder" document outlining the roadmap and milestones for post-quantum crypto support.
- Investigate the possibility of presenting the crypt4GH work at the Swiss Biotech Day event.
- Review the easy retro board for the Connect meeting and consider adding a session proposal.

**Review of Previous Actions and Post-Quantum Interest**

Rob Davies notes that many previous actions have not been completed due to busy schedules.
Speaker 2 expresses interest in post-quantum cryptography and mentions involving their chief scientific officer
Rob Davies discusses the current state of post-quantum library support and the lack of readiness of NIST-type algorithms
Speaker 2 emphasizes the importance of an open source or open architecture approach and the scope of encryption needed.

**Current State of Cryptography and Encryption Approaches**
Rob Davies explains the limitations of asymmetric cryptography in the presence of a working quantum computer.
Speaker 2 describes their approach to physical and logical encryption, using a partner for physical encryption and a KMS for logical encryption.
Rob Davies inquires about the key management partner, and Speaker 2 mentions using Thales.
Speaker 2 provides additional details about the scientific director involved in NIST and the quality of the KMS used.

**Challenges with Post-Quantum Algorithms and Symmetric Encryption**
Rob Davies discusses the current state of post-quantum algorithms and their integration into mainstream libraries
Speaker 2 mentions the flexibility of the current version of Crypto for GH to replace algorithms if needed
Rob Davies and Speaker 2 agree on the importance of a backgrounder document to outline the roadblocks and maturity levels of post-quantum encryption.
Rob Davies highlights the need for a downloadable library that doesn't discourage use, mentioning plugins for OpenSSL

**Federated Environments and Trusted Research Environments**
Speaker 2 inquires about the involvement of the Global Alliance in other groups related to trusted enclaves and federated environments.
Rob Davies admits to limited interaction but acknowledges the importance of client-side encryption and confidential computing.
Speaker 2 mentions the recent development of confidential computing and its potential for sharing data while encrypted.
Rob Davies discusses the challenges of processing data while encrypted and the limitations of current implementations.

**Swiss Biotech Day and Potential Presentation**
Speaker 2 introduces the idea of presenting at the Swiss Biotech Day in May, highlighting the international nature of the event.
Rob Davies and other participants discuss the potential benefits and logistics of presenting at the event.
Speaker 2 provides details about the event, including the expected participants and the focus on health, science, and innovation
Rob Davies and Speaker 2 agree to exchange information and decide on the best approach for presenting at the event.

**Connect Meeting and Session Proposals**
Speaker 2 inquires about the Connect meeting in April and the potential for presenting Crypto 4GH.
Rob Davies mentions the upcoming Connect meeting at the Broad Institute in Harvard and the possibility of presenting Crypt4GH v2.

Speaker 2 highlights the importance of the Connect meeting for promoting Crypto for GH and the detailed reports from the plenary.
Rob Davies discusses the need to finalize Crypto for GH v2 by the Connect meeting and the potential for a session.

**Meeting Schedule and Future Plans**
Participants discuss the timing of the next meeting, considering the proximity to the new year.
Rob Davies suggests postponing the next meeting to February to allow for more progress.
Speaker 6 checks the meeting schedule and confirms the next meeting is scheduled for January 7th.
Participants agree to postpone the meeting to January 14th to ensure better progress and preparation.

**Final Discussions and Contact Information**
Participants discuss the importance of cross-workstream topics and the process for proposing sessions at the Connect meeting.
Rob Davies and Speaker 6 explain the process for submitting session proposals and the criteria for approval.
Speaker 2 expresses interest in understanding the inner workings of the group and the importance of the backgrounder document.
Participants exchange contact information for further communication and agree to follow up on the backgrounder document.

## 2024-11-19: Post-quantum cryptography

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”: Oscar Martinez Llobet (EGA), Reggan Thomas

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Completing V2 spec | Rob | |
| 2 | Completing V2 python implementation | Fred | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Post-quantum cryptography: | |

| | | |
|---|---|---|
| | Open Quantum Safe<br>Post-Quantum Cryptography Alliance | |
| | A.O.B.<br><br>1) Next meeting on Dec 10, 2024<br>2) Connect meeting - 1 to 4 April 2025 • Broad Institute of MIT and Harvard, USA<br>**Register for Connect**<br>Fill out the **session proposal form** by 5 December 2024. | |

Meeting recording:
https://us02web.zoom.us/rec/share/RJFIRXBFFqTjycqpnIBv2sQRS3nQJ4TPBe4l6RW1iwMXlzme96wkBcmnxxMRhws.GV5nd0z_KpimqSnf

Meeting minutes:

https://aws.amazon.com/security/post-quantum-cryptography/

https://github.com/aws/aws-lc/blob/main/crypto/fipsmodule/PQREADME.md

**Summary** : The meeting focused on the status and future of post-quantum cryptography, specifically the Open Quantum Safe library and its integration with OpenSSL. Rob Davies and others discussed the current limitations and potential of quantum-resistant algorithms like MLK1024 and the challenges of implementing them. They also addressed the 64GB limit of AES-GCM for FIPS compliance, considering solutions like using multiple keys or waiting for updated standards. Additionally, they explored key management and security concerns, including the use of agents for secure key storage and the potential for quantum-resistant encryption in future versions of their software.

## Action Items

- Implement post-quantum key encapsulation or investigate library availability.
- Complete implementation of v2 of the protocol.

**Post-Quantum Cryptography Overview**

- Rob Davies introduces the topic of post-quantum cryptography and mentions the agenda for the meeting.
- Discussion on the Open Quantum Safe project, which is a library part of the Linux Foundation project.
- Rob Davies explains the integration of Open Quantum Safe with OpenSSL and its current status.
- Oscar joins the conversation, and they discuss the algorithms implemented in the Open Quantum Safe library

**Current Status of Quantum-Resistant Libraries**

- Rob Davies mentions that the Open Quantum Safe library is not recommended for critical applications.
- Discussion on the key encapsulation mechanisms and the algorithms like MLK1024 and Strawberrim.
- Rob Davies explains the difference between symmetric and asymmetric encryption in the context of quantum computers
- They discuss the potential use of MLK1024 in addition to the elliptic curve for added security.

**Implementation and Integration Challenges**

- Rob Davies and Speaker 1 discuss the need to wrap the quantum-resistant library in Python to call C code.

- Discussion on the challenges of using different encryption methods and the need for a new header format.
- They consider the potential impact on key sizes and the need to update the specification to accommodate new encryption methods.

**AWS and Other Implementations**

- Discussion on AWS's implementation of post-quantum cryptography and its library based on BoringSSL.
- Rob Davies and Speaker 1 review the standards and algorithms published by NIST and their security categories.
- They discuss the potential timeline for widespread adoption of post-quantum cryptography.
- Rob Davies mentions the need to keep an eye on other implementations and their progress.

**AES-GCM and FIPS Compliance**

- Rob Davies discusses the limitations of AES-GCM for FIPS compliance, particularly the 64 gigabyte limit per key.
- They explore potential workarounds, such as using multiple keys or waiting for an updated standard.
- Discussion on the challenges of implementing AES-GCM in a way that meets FIPS requirements.
- They consider the possibility of deriving keys from a master key to overcome the limitation.

**Key Management and Security Concerns**

- Oscar highlights common user questions about key management and secure storage.
- Discussion on the use of agents to manage keys and the challenges of implementing such a solution.
- They consider the security implications of using agents in different environments, such as private clouds.
- Rob Davies and Speaker 1 discuss the need for better documentation and guidance on key management.

**Encryption and Decryption Workflows**

- Fred describes a file system implementation that uses SQLite to manage encrypted headers and keys.
- They discuss the potential for users to access only specific regions of files, enhancing security.
- Rob Davies and Speaker 1 consider the challenges of implementing such a system and the need for user education
- They discuss the potential benefits of this approach for managing large datasets in a secure manner.

**Next Steps and Action Items**

- Rob Davies summarizes the action items, including completing v2 and keeping an eye on post-quantum cryptography.
- They discuss the need to update the specification and Python implementation to accommodate new encryption methods.
- Rob Davies mentions the next meeting date and the importance of aligning it with other schedules.
- They consider the potential for a session at the Connect meeting to discuss their work and progress.

**Final Remarks and Future Plans**

- Rob Davies and Speaker 1 discuss the importance of finishing v2 before implementing new encryption methods.
- They consider the potential impact of quantum computers on their current encryption methods.
- Rob Davies mentions the upcoming Plenary meeting and the need to prepare for it.
- They conclude the meeting with a plan to follow up on the discussed topics in the next meeting.

Global Alliance for Genomics & Health

# 2024-09-24: Survey & PQE

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)” :
Apologies: Reggan Thomas (GA4GH)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | Rob Davies/ Fred H |
| 2. | Previous Actions Review | |
| 3. | Latest Results from the survey | Rob / Reggan |
| 4. | Version 2 specification | Rob Davies |
| 5. | Consider adding post-quantum encryption, following the recent standards announcement by NIST. | Rob Davies |
| 6. | FIPS compliance option (see hts-specs issue 780) | Rob Davies |
| | A.O.B.<br>3) Next meeting on Oct 15, 2024 | |

Meeting recording:
https://us02web.zoom.us/rec/share/FDjoNkRqw6PaNbypqZ8ja7XzbdcxeSLSjneLLWAW3tRB7TFCdp-TLb4wz7mjLT9A.bEHpwTmCyeSsGTQo

Meeting minutes :
**Summary:**

The team reviewed a survey on the implementation of crypt4ght, noting dissatisfaction with performance and security. They also discussed the need for post-quantum cryptography and the potential use of AES-GCM to address FIPS 143 compliance. The conversation included technical details on header version 2, key management, and the integration of ChaCha 20 and AES-GCM. They agreed to continue working on these issues and to explore the use of quantum computers for alignment algorithms. The next meeting is scheduled for October 15th.

**Action items:**

- Implement support for post-quantum key encapsulation in the crypt4gh file format v2.
- Investigate library availability and integration options for the post-quantum algorithms.
- Evaluate the impact of the 64GB file size limit with AES-GCM and explore potential solutions.
- Reach out to the marketing team to discuss creating better documentation and guidance for users on implementing the crypt4gh format.

**Post-Quantum Encryption and Homeomorphic Encryption**

- introduces the topic of post-quantum encryption and homeomorphic encryption, explaining the concept of adding random errors to data to confuse quantum computers.
- discuss the mathematical complexity of homeomorphic encryption and its practical applications.
- explains the idea of adding errors to data during encryption and removing them during decryption using the correct key.
- the need to discuss post-quantum encryption further and shares a document on the topic.

**Survey Results and Implementation Challenges**

- review the survey results, noting the slow response rate and the lack of detailed comments.
- They discuss the challenges mentioned in the survey, such as performance, ease of use, and security.
- highlights the importance of security and the need for better integration with other tools.
- discuss the need for benchmarking and testing to ensure the strength of the encryption.

**Key Management and AWS Integration**

- emphasizes the importance of key management and the need for better documentation on how to implement the encryption.
- discuss the potential integration with AWS Key Management Service (KMS) and other encryption tools like GPG.
- challenges of using GPG for large files and the need for better key management and exchange mechanisms.
- suggests that a marketing team could help with promoting the encryption tools and their benefits

**Post-Quantum Crypto and Hybrid Encryption**

- discuss the potential use of post-quantum cryptography and the need to replace ChaCha 20 with more quantum-resistant algorithms.
- They explore the idea of using a hybrid encryption method that combines lattice-based and elliptic curve algorithms.
- suggests encrypting the header with a post-quantum algorithm while keeping the session key and ChaCha 20 for symmetric encryption

- discuss the challenges of implementing post-quantum cryptography and the need to wait for library availability.

**Specification Updates and Implementation Details**

- review the specification updates, including the addition of a data key and segment number for better encryption management.
- They discuss the potential use of multiple keys for large files and the need to handle offsets and segment numbers
- suggests implementing a map to keep track of the keys and offsets during decryption.
- Rob Davies and Fred agree to work on the v2 implementation and discuss the need for better documentation and examples.

**FIPS 143 Compliance and AES-GCM**

- Rob Davies mentions an issue about FIPS 143 compliance and the need to consider using AES-GCM instead of ChaCha 20.
- Fred explains the differences between AES-GCM and ChaCha 20, including the 64 gigabyte file size limit for AES-GCM.
- They discuss the potential benefits of using AES-GCM, such as hardware acceleration and better security.
- Rob Davies and Fred agree to explore the feasibility of using AES-GCM and the need to address the file size limit

**Next Steps and Meeting Schedule**

- Rob Davies and Fred discuss the next steps, including working on the v2 implementation and exploring post-quantum cryptography.
- They agree to talk to Reagan about the marketing team and the need for better documentation and examples.
- The next meeting is scheduled for October 15th, and they plan to continue working on the specification updates and implementation details

## 2024-08-27: Survey & PQE

Chair: Rob Davies (Sanger),
Attendees “Name (Affiliation)” : Reggan Thomas (GA4GH),Denis Akzam (Ariadne Geometry)
Apologies: Frédéric Haziza (GIP-CAD)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | Rob Davies |
| 2. | Previous Actions Review | |
| 3. | Results from the survey | Rob/Reggan |
| 4. | Version 2 specification progress | Rob Davies |
| 5. | Consider adding post-quantum encryption, following the recent standards announcement by NIST. | Rob Davies |
| 6. | FIPS compliance option (see hts-specs issue 780) | Rob Davies |
| | A.O.B.<br>4) Next meeting on Sep 17, 2024 (Plenary week - Cancel and reschedule ?) | |

Meeting recording:
https://us02web.zoom.us/rec/share/eMzCUtw5OH7h2Q3bOuTnXnH1WJxv2XcjYqNlCW95sscXj6A2M2ZlE5n7sFV4dL-l.xBuqg-aJPpXRlNKT

Meeting minutes:

Intro - Denis Akzam
Discussed about Survey results
Post-quantum encryption

## 2024-07-23: Header and timestamp

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |

| | | |
|---|---|---|
| 3. | Branch with “link” headers and “timestamp” headers | Fred |
| 4. | Branch with beginning of the version 2 specification | Rob |
| | A.O.B.<br>5) Next meeting on Aug 20, 2024 (MFW - Cancel or reschedule ?)<br><br>2) Planned survey here | |

Meeting recording:
Meeting minutes:

## 2024-06-25: Future work

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Create a PR for detached headers and limited access | Fred | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Look at moving the writer’s key in the header. | Rob |
| 4. | Work on the python implementation: Storing header in a separate file | Fred |
| | A.O.B.<br>Next meeting on Jul 23, 2024 | |

## 2024-05-28: Connect Meeting and Future work

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”: Oscar Martinez Llobet (EGA), Reggan Thomas

Global Alliance for Genomics & Health

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Create a PR for detached headers and limited access | Fred | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | How did the Connect Meeting go? | Rob |
| 4. | Suggestions for future work<br>- Full-file integrity (ongoing)<br>- Move writer's key<br>- Detached headers<br>- Header signing<br>- Time-limited access | Rob |
| 5. | Work on the python implementation: Storing header in a separate file | Fred |
| | A.O.B.<br>Next meeting on Jun 25, 2024<br><br>Webinar on The Role of Trusted / Secure Environment - June 13 at 1 pm ET<br>https://www.eventbrite.ca/e/federated-analysis-the-role-of-trustedsecure-environments-tickets-849849481677?aff=CyberImpact&utm_source=Cyberimpact&utm_medium=email&utm_campaign=Join-us-for-Federated-Analysis-The-Role-of-TrustedSecure-Environments | |

Meeting recording:
https://us02web.zoom.us/rec/share/5Dn1Hr3Wt3dC_qlUq5qHsvzRaPuCtRWpm_2LF08_XVm8mslieuHiE6ZER8VF4KIp.ZCx9kD3mM-8u88pk

Meeting minutes:

- Connect meeting recording here

Connect de-briefing
Fred working on https://github.com/samtools/hts-specs/pull/736

Global Alliance
for Genomics & Health

## 2024-05-07: Connect Meeting and Future work (moved to 28th May)

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”: Reggan Thomas

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | How did the Connect Meeting go? | |
| 4. | Suggestions for future work<br>- Full-file integrity (ongoing)<br>- Move writer’s key<br>- Detached headers<br>- Header signing<br>- Time-limited access | |
| | A.O.B. | |

Meeting recording:
Meeting minutes:

- Connect meeting recording here

Due to low attendance, the agenda has been moved to 28th May

## 2024-4-02: Connect topics

Chair: Rob Davies (Sanger), Frédéric Haziza (GIP-CAD)
Attendees “Name (Affiliation)”:
Apologies:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |

| | | | |
|---|---|---|---|
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Digital rights management | |
| 4. | Expiration date to the header | |
| 5. | Items for the connect meeting | |

| | Previous Actions | Assigned To | Deadline |
|---|---|---|---|
| 1 | Continue working on the implementation to bring back the edit list | Fred | |
| 2 | | | |

Meeting recording:
https://us02web.zoom.us/rec/play/XUb5BNS6xMo3P2H3AyCJ5SayRqrv8meT_-1VzfG_O6lf21FMZCmW9G1ZsjuUEeziWYq_w4Xb9FoeHq2H.Wg-mtjfEb74MMCYW?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fus02web.zoom.us%2Frec%2Fshare%2F1b67MHm0XkPvA-AFuKMNQAeubJMt7OUB3aymYgpEbQbHOSJmzaEtb-Zpu3WpxH6z.1totFtDKaNYcWXvl

Meeting minutes:

FH - https://github.com/silverdaz/crypt4gh-sqlite

## 2024-3-05: Connect prep

Chair: Rob Davies (Sanger)
Attendees “Name (Affiliation)”: Tim Hefferon (NCBI - Variation),Reggan Thomas
Apologies: Oscar Martinez (EGA TB), Frédéric Haziza (GIP-CAD)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Prepare an agenda for connect.<br><br>Topics to include: | Rob | Apr 2, 2024 |

| | | | |
|---|---|---|---|
| | 1) Key management (Custom key exchange protocol)<br>2) Cloud - DRS and TES | | |
| 2 | Move Apr 30 meeting to May 7, 2024 | Reggan | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Connect session items<br>Agenda doc here | Robert |
| 4. | | |
| | A.O.B<br>- Next meeting on Apr 2,2024<br>- Meeting on Apr 30, 2024 - Meeting Free Week - Cancel or re-schedule? | |

| | Previous Actions | Assigned To | Deadline |
|---|---|---|---|
| 1 | Continue working on the implementation to bring back the edit list | Fred | |
| 2 | | | |

Meeting recording:
https://us02web.zoom.us/rec/play/Ch3lTKvmMUpgnQ3M6YRA5ehauPEguDQUCpwoWTWIbLumNldGe3uqG_uzOD_t_vX0_A7PhKM8VHBq-YAe.yZpOpB4hUuAmyehz?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fus02web.zoom.us%2Frec%2Fshare%2F9sYaPLaJVErkT88cWbzQODY7HZLCwAxt-Y-TsiPIgDURt1zPh3KiDqlwvjLHjXHe.y3hWbv_jG57DrhBS

Meeting minutes:
RD - How do we store all data in EGA - dbgap?
TH - Would like to know how you manage and allow access to the data.
TH - Tim can act as a point of contact for NCBI
TH - Tim will figure out how dbGap stores the data.

## 2024-2-06: PR 736 and New location

Chair: Rob Davies (Sanger) , Frédéric Haziza (GIP-CAD)

Global Alliance for Genomics & Health

Attendees “Name (Affiliation)”: Reggan (GA4GH), Oscar Martinez (EGA), Kahlil Lawless (Illumina),
Apologies:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Continue working on the implementation to bring back the edit list | Fred | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | Discussion - Adding AEAD support as new encryption method https://github.com/samtools/hts-specs/pull/736 | |
| 4. | Moving Github repo to new GA4GH location https://github.com/EGA-archive/crypt4gh<br><br>https://github.com/ga4gh/ga4gh-crypt4gh | |
| | A.O.B<br>- Connect meeting (April 21 - 24) at Ascona, Switzerland. Hybrid participation available.<br>- Submit your connect meeting proposal here (deadline - Feb 16,2024)<br>- Next meeting on March 5,2024 | |

Meeting recording:https://us02web.zoom.us/rec/play/PpIZtwEK3NxkUxgifRueiaBKyoZlCpNxQgjHcDWL78XDB4b1CLPRITxk1v1osWizPfj138iNSs9qZXMC.wXujq4agJMZ9Lt2r?autoplay=true&startTime=1707231277000

Meeting minutes:
Review of 736 - Background : Take the original file, cut it in blocks and blocks of fixed size and then you encrypt each block with a symmetric key.

So the key that is used to encrypt is the key that you use to depict. And you keep the order the new version. Crypt4gh will inject. Inside the encrypted data it will inject the order of the blocks so that if you reorder them you can't really decrypt it, it will fail at the decryption.
now you need to actually save that symmetry key and we put it at the beginning of the file.
We call that the Crypt4gh header. And in order to encrypt that key.
You actually need to specify a few parameters. With the key that are all embedded inside this header.

there were 2 types of packets that are in the middle of the header and one suggestion was to add a third type.
Change something and another suggestion was to use one of the existing 2 types, but change some of the parameters.
Fred : issue for me there was, it was designed so that we could also concatenate files.
Edit list - was to make the format compatible with Htsget. And the edit list, it's one of the separate packets that says you should read that many bytes.
Fred - Let's say that the original the original file is 10 segments and you're going to send to the user that downloads with HTTP, 2 of those segments.Now you should actually include. A bit of offset and discard data so that you read the part of the segment that was meant to be instead of sending the data.
Fred - So instead of getting the entire file, you get a range so that you say skip this beginning of the file I'm not interested in.
And just give me for example chromosome 2. Instead of the entire file. And when we do that with Griffo GH, the chromosome 2 he's in the middle of the file it's been encrypted so it spans a few segments.
maybe the segment is slightly bigger than the data that you wanted to have. So you include in one of the packet in the header, the edit list where you say discard that much, read that much discard that much and so on.
Fred - My issue is when we combine that with AED. You could actually change the sequence number. So that it matches the segment of the HTTP you want to send.

Fred - done an implementation with the AEAD. And this implementation does not support the edit list. If we bring back the edit list it will work.
but there is this problem of and at least combined with AID and several sequence numbers. And we could say we don't support that.
Fred - I'm more convinced now that we should actually separate to have a new packet.
RD - I think what I wanted to see in the same thing is the data encryption key because basically, they'll do Basically, sit as a unit.
So these data encryption packages should have everything you need to encrypt. And block of data.
Fred - I'll keep working with this. Implementation to bring back the edit list and maybe Did at least is Only working with the old format
RD - this was probably a mistake in the original format as having the writers public key.
KL - Is this currently in use with any of these projects and is it to get people to share the data for download transfer?
Is it for API access? What are the, what are the current usage environments for this tool?
KL - but who's using it for what you know in in what in what context
So like, like a hospital system doing a whole genome sequence that needs to store the data but wants to keep it from being, you know, utilized by hacker, but wants to keep it, that needs to store the data, but wants to keep it, that needs to store the data but wants to keep it from being, you know, utilized by hacker could use this encryption system
Fred - Hospitals no take the EGA for example. All the lines are encrypted with. They are downloaded.
KL - Over the wire.?
Fred - Over the wire. And the transport is HCTP is the same whatever wants but the user will receive the file on their disk.
KL - we've been thinking about systems where we'd have a whole genome but we'd be only able to decrypt and access through API specific regions for a specific panel, right?
Fred - Yeah, and that's actually already the case. And at the GA and the new place where I am, the files are encrypted, the increase for GH and then you could build a tool with, a file system

with fuse that actually decrypt only the block that you wanted to read because the tool that you're using wanted to jump to the middle of the file and read
Fred - It didn't decrypt the entire file, it decrypted only the block where the data was.data is encrypted in. At rest. And then during the transfer, it's also encrypted.
Global Alliance recommends, I mean, we could decrypt the file, send to the user and say, do whatever you want with that file.global Alliance suggests to not, Leave traces of sensitive data. On disk decrypted.
KL - Can I ask how many keys you can have? Like, cause we've been, you know, envisaging a system where you might have So a key for consent, a key for
a clinician to say, there's a requirement, a key for government, payer to say, yes, we'll pay for it a government for a vendor to say, he will do it
KL - How do you safely store that key? If the key is the one retrieval key that you have is the key to keeping that data safe, what do you actually do with that key?
If you want to keep the data encrypted on your own server in case of a hack and access, you know, what do you do with that key?
RD - so depends on your use case. So mostly what we've covered is kind of your running in locally.my implementation, you could, you basically have an encrypted file with a key in and you give passphrase to Open it up
Fred: The key on the server is locked. With the bus phrase. What you could do is that, any tool that wants to decrypt, gets prompted for the pass phrase.

## 2024-1-09: General discussion

Chair: ~~Alexander Senf~~
Attendees “Name (Affiliation)”: Fred (GIP-CAD), Robert, Reggan
Apologies:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | | |
| 4. | | |
| | A.O.B<br>- https://github.com/ga4gh/TASC/issues/40 - James Eddy is working on the documentation around “when do products move into their own repo”?<br>- Connect meeting (April 21 - 24) at Ascona, Switzerland. Hybrid participation available. | |

| | | |
|---|---|---|
| | - Submit your connect meeting proposal here (deadline - Feb 16,2024)<br><br>- Next meeting on Feb 6,2024 | |

Meeting recording:

https://us02web.zoom.us/rec/share/id4ZqrraBdTTm9KGVsuX1EX1iVZ7yo41ohG48TqP76pcwQRZ5oFH12SKurpnvkbE.KAkmR8rhrWa80VV7

Meeting minutes:

## 2023-12-11:

Chair:
Attendees “Name (Affiliation)”: Robert Davies, Pavel Nikonorov, Reger Mikaeel, Justina Chung
Apologies: Fred (coinciding with the EGA SAB), Alexander Senf,Reggan Thomas

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | | |
| 4. | | |
| | A.O.B<br><br>- Next meeting on Jan 09,2024 | |

Meeting recording:

Meeting minutes:

- Alex/Fred unable to join today
- Welcome Reger Mikaeel who is new to Crypt4gh
- PN: on track to establish laboratory in Armenia and applying to ELIXIR as a member; decided to provide open draft specification for GA4GH APIs enhanced with Confidential Computing. It will allow researchers to use federated data access without data disclosure.
    - connected with Fred.
- Next meeting is on January 9, 2024.

Global Alliance
for Genomics & Health

# 2023-11-14: Crypt4gh Rust

Chair: Alexander Senf
Attendees “Name (Affiliation)”: Rob Davies, Fred H, Reggan Thomas
Apologies:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | https://github.com/EGA-archive/crypt4gh-rust/pull/3 - Crypt4GH in htsget | |
| 4. | | |
| | A.O.B. - https://elixir-europe.org/events/elixir-bioinformatics-industry-forum-2023<br><br>EBI and BBMRI for the **Bioinformatics Industry Forum**, which will take place in London on 21st of November 2023, with a focus on “Trusted research environments for sharing data in life sciences<br><br>- Next meeting on Dec 12,2023 | |

Meeting recording:https://us02web.zoom.us/rec/play/cgLq8FVRZ8c72tmfBc5UqAN8hP2WBLgVJyH8QANCNrkKKVB2p4d8K2Amk_xsiMyRaE5vARZzvkkiqK7L.a5TXzYHkLBStqaYb?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fus02web.zoom.us%2Frec%2Fshare%2Fx6Jd3P4DHtCnYizoa-7Qy7X0DLU7YIcN6UNWuYRyjElMFxIAvkBc8A4k_e10Qbo.O-TnIVDH87Yy8xOc

Meeting minutes:

AS - Oliver H has made some progress to the Rust based htsget server. Oliver Hofmann requested feedback in the pull request. One of the things happening is the GDI (genomic data infrastructure) will make crypt4gh. More GDI projects will use crypt4gh.

FH - About the PR, how bad making them the maintainers. Roberto moved to another place. How about Australian genomics being the maintainer.
They wanted to be the maintainer of Rust Crate? Fred to check with Oliver and provide access.

RD - fixed few bugs in htslib.
FH - tried to work on version 2.

## 2023-10-17: Connect/Plenary Recap

Chair: Alexander Senf
Attendees “Name (Affiliation)”: Pavel Nikonorov ,Ruslan Vakhitov (Genxt)
Apologies: Reggan Thomas

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Discussion with task team leads - poll | Alexander | EOD today |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | fixed a few bugs that had accumulated in htslib's implementation - should be fully resolved with the next release | |
| 4. | GA4GH Connect/Plenary Recap | |
| | A.O.B. | |

Meeting recording:
https://us02web.zoom.us/rec/share/qWbsBfkTt5oGKm1GXCBitwTNNvk_BqCLY8HT9K2sPGwNLqfLqS7J-3qvVizlvJM-.zzpRBucKTnZiqM4J

Meeting minutes:

AS - Rob mentioned that he did worked on the htslib and corrected few bugs which will be part of next release of Htslib

AS - Plenary recap. Analytics platform for indigenous plantform. Presentation from Genxt. Running bioinformatics pipelines. Both are very effective way to secure data.

Major Use case - GDI. using crypt4gh as the standard for securing the data.
PN : Enclaves. Standard adopted more across the globe.

Signed Letter of Intent with Armenian bioinformatics institute
Adoption of open source platforms which are compliant with GA4GH for research purpose

Global Alliance
for Genomics & Health

# 2023-08-22: AEAD

Chair: Rob Davies
Attendees “Name (Affiliation)”: Fred, Pavel N, Reggan Thomas
Apologies: Alexander Senf

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Make the following as the admin for the new repo<br>1) Alexander Senf (github user: asenf? ← confirm)<br>2) Robert Davies (github user: daviesrob)<br>3) Frédéric Haziza (github user: silverdaz) | Reggan | Done |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | https://github.com/ga4gh/ga4gh-crypt4gh | |
| 4. | AEAD PR https://github.com/samtools/hts-specs/pull/736 | |
| | A.O.B.<br>Connect session agenda<br>Presentation - template<br><br>Deadline - **05-Sep for agenda items**<br>**Session summary - by Friday, Aug 25, 2023** | |

Meeting recording:

Meeting minutes:
Discussion on PR 736
Additionally, an attacker can inject a segment, with a its own sequence number with the AEAD method, and add its header packet to the header list. However, if we enforce that the writer’s public key must all be the same for the AEAD encryption method, we circumvent the issue. We prefer to slightly update the spec rather than changing the header format/version and/or break implementations.

Global Alliance for Genomics & Health

# 2023-07-25: AEAD support

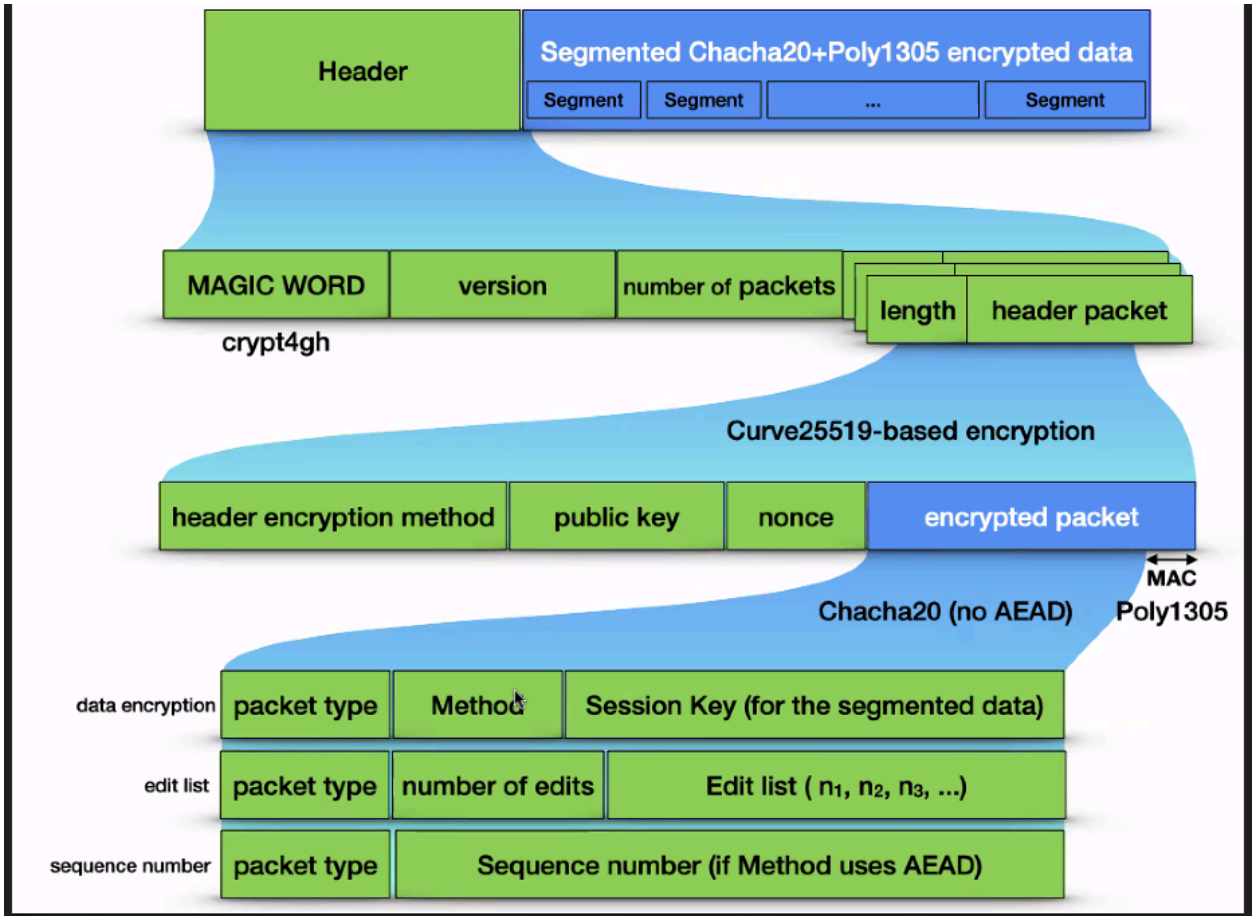
Chair: Alexander Senf
Attendees “Name (Affiliation)”: Fred, Rob Davies (Sanger), Andrejs Puckovs (MGI-Tech),Reggan Thomas (GA4GH)

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions | |
| 3. | AEAD support:<br>• Python Implementation (separate branch)<br>• Documentation<br>• PR for Crypt4GH specs<br>Introducing a new encryption method and packet type. | Fred |
| 4. | | |
| 5. | | |
| | | |
| | A.O.B.<br>Connect/Plenary 2023 - ideas for Crypt4GH Session (Ideas Document) | |

Meeting recording:
https://us02web.zoom.us/rec/share/yAh_pNE5viAmrErPr-yBrA-Hg29xZGZET1FJiIgiQ1Cl-IjyXqYVzu0MnsVdO6J0.O1t3qQEjAKT9UR8-

Meeting minutes:
Discussed about AEAD support




Quick background to this discussion: It is about an update to the standards documentation we have been thinking about for a long time, this is the first time we have something tangible to talk about. We would add an additional way to encrypt data, which contains additional data that is validated upon decryption, which can be used to ensure that packets are validated to be in sequence

FH – Injecting AEAD into each segment, instead of injecting 0,1,2,3
We will final one at the end. To tag it as the last one We add one more. When we decrypt we check if the last one or the extra one is there.
If we decrypt, if it is less a segment, then that the end.
If it is exactly a segment, will continue and next one should be an empty segment
Tried to implement that, but need to check with other implementors

The problem come from the header, the sequence number start from 0 and we don't change the number

But if want to have a TCP sequence number

Global Alliance
for Genomics & Health

## 2023-06-27: Spec Updates, DRS Protocols

Chair: Alexander Senf
Attendees “Name (Affiliation)”: Rob Davies, Reggan Thomas

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions<br>● AEAD PR<br>● U.S. AES-256 requirements<br>● Split header/payload | |
| 3. | Cloud API Support (e.g. DRS) - protocols (CRG, PA, GHGA, …)<br>(Some more specifications in Crypt4GH Use Cases) | |
| 4. | Connect/Plenary 2023 - ideas for Crypt4GH Session (Ideas Document) | |
| 5. | | |
| | | |
| | A.O.B. | |

Meeting Recording:

Meeting minutes:

## 2023-05-30: Spec Updated

Chair: Alexander Senf
Attendees “Name (Affiliation)”: Rob Davies, Reggan Thomas

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |

| | | | |
|---|---|---|---|
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions<br>● AEAD PR<br>● U.S. AES-256 requirements<br>● Split header/payload | |
| 3. | Cloud API Support (e.g. DRS) - protocols (CRG, PA, GHGA, …) | |
| 4. | Connect/Plenary 2023 - ideas for Crypt4GH Session (Ideas Document) | |
| 5. | | |
| | | |
| | A.O.B. | |

Meeting Recording:
https://us02web.zoom.us/rec/share/sKeN96BPaKo4xIEo-jgGOO42Py_dB_GKGMlYcvsyYK4YJQmun14pzcxdqmOYTrY.CYknuz1nqjiOqO_Z

Meeting minutes:

RD - Discussed very briefly, an idea I had for basically having a packet type which tells you where to get the data. So that means you can have headers with no data attached. Which would make use cases like Fred's easier, I think, because he wouldn't need complicated servers which have to return headers onto bits of data anymore. So the client would do it.

RD - basically you can give people a file, which then tells them to open another file

AS - writing a DOS server just now, I mean, what I would really want to do is just what Fred did, and have the data component in an s3 bucket and have the header in a Mongo database so that I can just store them in separate places and just deal with a small amount of data within a secure storage and the rest is just a string doesn't have to be super secure. But the client would have to deal with it.

AS - like the idea of the extra header so that you can really just say, this is your 10 gigabyte file in 100 bytes, and then just run your tool and it takes care of the rest. Yeah. So that would, for example, be the best way to handle it within tests. It's an easy file, it tries to open it and then the software itself knows how to get it right at the point of access.

AS - The question is just so if I was a data owner, I would say okay, if this key comes from a Trusted Execution Environment, and no human being knows about it, then I released the data. If there's any chance that someone created the key at some point and replaced it.

RD - probably need to have some sort of certificate which is signed by the Trusted Execution Environment or some sort of signature because I think they have basically registers that you can read. Use the source to store information about the environment itself, don't they? So you can then know that your environment itself has a certificate which says it's what you expected it to be

AS - Expecting a demo from GENXT during September connect
Clinical data and Open EHR

- There are many platforms that exist both open source and commercial, that implement the data persistence layer, how you actually then store the clinical data on this on a database. The data model itself apparently is also to a large degree available open source already. But yeah, there was a little bit of work done years ago, adding crypto GIS to that and that would be a fun implementation project as well, at some point just to bridge the difference between clinical and genomic data and bring them together.

AS - clinical and the genomic side though. Yeah. Because that's going to be just a big thing. As you know, always says the clinical genomic data will be produced in the clinical space. So if you're not doing anything, and I'm sure there's other companies that will provide great proprietary solutions, that will be a pain to interoperate with in the future

AS - We might present the integration with a trusted execution environments

## 2023-05-02: AES-256 and AEAD

Chair: Alexander Senf
Attendees “Name (Affiliation)”: Rob Davies, Andrew P,Fred H,Reggan T

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | AEAD - Make a PR | Fred | |
| 2 | Find documentation of U.S. AES-256 requirements | Andrew | |

Global Alliance
for Genomics & Health

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Connect meeting summary<br><br>Key Takeaways and next action items<br><br>Meeting recording | |
| 3. | AES-256 support? | |
| 4. | AEAD plans | |
| 5. | Split payload from header? | |
| | | |
| | A.O.B. | |

Meeting Recording:
https://us02web.zoom.us/rec/share/F24-3yUhUo8cQfU4-Vhu68CZxwPOc0z9tme1cEeGtyGctWrY8sLTXGF8YK7_kK4x.r6dckBAH2eIxgG_K

Meeting minutes:
Presentation - Andrew -
https://docs.google.com/presentation/d/1gnmTAtKliCtExc5KFnKJsu-cexj_gR3diN7CREYs0UM/edit?usp=sharing

Discussed on AES 256 and AEAD Support to the exisiting specification.

## 2023-04-4: CANCELLED (Due to connect meeting)

Chair: Alexander Senf
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

Global Alliance
for Genomics & Health

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| | A.O.B. | |

Meeting Recording:

Meeting minutes:

## 2023-03-07: Cloud Integration and Spec updates

Chair: Alexander Senf
Attendees “Name (Affiliation)”: Rob Davies, Frederic Haziza,Reggan Thomas

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Proof of concept for enclaves and attestation on AWS | Andrew | |
| 2 | | | |

Global Alliance for Genomics & Health

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | GA4GH Connect 2023: April 19-21, London: 1 session requested (Crypt4GH Developments and Demo) | |
| 4. | Update on Cloud Integration Developments<br>● htsget-rs (UMCCR Melbourne; repo, issue)<br>● ELIXIR Switzerland GSoC<br>● DRS PoC (want to present something at GA4GH Plenary 2023)<br>(Revisit Crypt4GH Use Cases to cover ongoing developments) | |
| 5. | Crypt4GH Spec Updates<br>● Status of a possible implementation / spec PDF version?<br>● Should it be part of any new development? (i.e. should any of the above projects try to use an updated version of Crypt4GH?) | |
| | A.O.B. | |

Meeting Recording:https://us02web.zoom.us/rec/share/hJod7TI9ved47hy5DwUhsSGRjMac-SfeZ4IgQOgQxNt2tHporV9RNXG2i218Xa2y.6lW2eN9DWGdWV05_

Meeting minutes:
Discussed about Connect meeting
Discussed about cloud integration.

## 2023-02-07: Product graphics and Cloud integration

Chair: Alexander Senf
Attendees “Name (Affiliation)”: Frederic Haziza,Reggan Thomas,Rob Davies

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | Proof of concept for enclaves and attestation on AWS | Andrew | |
| 2 | look into htsget implementations | Rob | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |

| | | |
|---|---|---|
| 3. | GA4GH Connect 2023: April 19-21, London (Call for Session, by March 1)<br>• Special Sessions? Special Meetings? Demos?<br>• Who plans on attending? | |
| 4. | Review GA4GH Product Graphics (Feedback by Friday, February 10)<br>• the graphic and the graphical representation of the concepts<br>• the text in the graphic<br>• the caption that will accompany the graphic | |
| 5. | Who is working on Cloud integrations?<br>(possible funded work in Australia) | |
| 6. | Just for interest: GA4GH Strategic Refresh (Public) | |
| | A.O.B. | |

Meeting recording :
https://us02web.zoom.us/rec/share/8NwAp4Vlh6Yoj1CAaDWXkm3NQ22qP4kOarPESaRKzSGaHOJPFAkQtTCGmrLBazkn.OwTHhAdKhjms5zNU?startTime=1675781901000

Meeting minutes:
High level discussion on upcoming Connect meeting
Discussed about product graphics

Group to take a look at the GA4GH Strategic refresh document.

## 2023-01-10: CANCELED

Chair:
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| | A.O.B. | |

Meeting Recording:

Meeting minutes:

## 2023-MM-DD: Template

Chair: Alexander Senf, Rob Davies
Attendees “Name (Affiliation)”:

| | Actions Arising | Assigned To | Deadline |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

| | Agenda Item | Person/Time |
|---|---|---|
| 1. | Welcome, Introductions & Confirm Agenda | |
| 2. | Previous Actions Review | |
| 3. | | |
| | A.O.B. | |

## Previous Minutes

2022 Meeting Minute

Global Alliance
for Genomics & Health

2021 Meeting Minutes
2020 Meeting Minutes
2019 Meeting Minutes
2018 Meeting Minutes