Global Alliance
for Genomics & Health

GA4GH Encrypted Format

Minutes and Actions 2023 - 2026

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

Meeting Protocols

- 2025-MM-DD: Template

Agendas, Minutes and Actions

- 2026-10-13
- 2026-09-15
- 2026-08-25
- 2026-07-21 -Cancelled
- 2026-06-23
- 2026-05-26
- 2025-06-22:
- 2025-06-24: Age encryption format
- 2025-05-27:
- 2025-05-06: Specification - V2
- 2025-04-08: DRS integration with Crypt4gh
- 2025-03-04:
- 2025-02-04:
- 2024-12-10: Post-quantum cryptography
- 2024-11-19: Post-quantum cryptography
- 2024-09-24: Survey & PQE
- 2024-08-27: Survey & PQE
- 2024-07-23: Header and timestamp
- 2024-06-25: Future work
- 2024-05-28: Connect Meeting and Future work
- 2024-05-07: Connect Meeting and Future work (moved to 28th May)
- 2024-4-02: Connect topics
- 2024-3-05: Connect prep
- 2024-2-06: PR 736 and New location
- 2024-1-09: General discussion
- 2023-12-11:
- 2023-11-14: Crypt4gh Rust
- 2023-10-17: Connect/Plenary Recap

2023-08-22: AEAD
2023-07-25: AEAD support
2023-06-27: Spec Updates, DRS Protocols
2023-05-30: Spec Updated
2023-05-02: AES-256 and AEAD
2023-04-4: CANCELLED (Due to connect meeting)
2023-03-07: Cloud Integration and Spec updates
2023-02-07: Product graphics and Cloud integration
2023-01-10: CANCELED
2023-MM-DD: Template
Previous Minutes

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

2026-MM-DD: Template

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR)
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.	

Global Alliance
for Genomics & Health

Agendas, Minutes and Actions

2026-10-13

Chair:

Attendees: Thomas Conner (Broad, GA4GH), Oscar Martinez (EGA, CRG), Robert Davies (RD), Frédéric Haziza (IFB/Elixir-FR) (FH), Venkat Malladi (VM), Jessica Seegobin (JS).

	Actions Arising	Assigned To	Deadline	Status
1	Continue discussions regarding encryption and the progress updates related to v2 at the next meeting	All	October 13	
2	Explore discussions related to the format of the post-quantum header.	All	October 13	
3				

	Agenda Item	Person/Time
1.	Welcome, Introductions	Robert Davies / Frédéric Haziza
2.	Upcoming November 10 meeting - Cancel or reschedule to November 17 or November 24?	Jessica
3.	Review Previous actions	All
3a.	Post-quantum key exchange X-Wing	
4.	PRs and Issues on Github: Gigantic “All-or-Nothing” pull requests: A very good idea, but touching different files that has no business touching. I didn’t know how to respond, it was all over the place. So I split and created several (smaller) issues to enable the discussion. Problem with external PRs: can participate in it.	Fred

5.	Idea: a plugin system for loading keys: We could allow multiple file formats and locations to be loading the keys. After all, we only need to get 32 bytes out of them. Whether there is a passphrase, or the keys is already loaded in the kernel (see keyctl)... this might be a good feature. In the above PRs, another package was suggested to parse the Openssh-formatted keys: but that requires some custom python code. Not a big deal, but probably a pain to maintain in case there is a rounding error or so.	Fred
6.	*AOB*	All

Meeting Minutes:

Scheduling conflict

- RD and JS noted the November 10 meeting conflicts with the GA4GH meeting free week. JS asked whether to cancel or reschedule to November 17 or November 24.
- JS flagged having a meeting overlap on November 17, which may prevent her attendance.
- RD and FH agreed to reschedule the meeting to November 24, accounting for upcoming holidays.
- JS noted that the December meeting will take place on December 8
- **Action**: JS to reschedule the upcoming meeting to November 24

Post-quantum key exchange X-Wing

- RD mentioned that not much has been done on post-quantum; interest in potentially X-Wing hybrid post quantum KEM. X25519 is currently used with ML-KEM768, which is post quantum one - as long as you use one of these, it maintains security. It is a combination of both methods
- RD noted that X25519 will fail with the advancement of quantum computers
- VM and RD suggested this is more future proofing, but for our use case, you can take the file and you can decrypt it later.
- FH suggested that Section 5.7 uses TLS 1.4, which was RSC. 1.024.; there's a post-quantum key agreement
- The current Crypt4GH header format tells you which algorithm to use to decrypt the rest of the bytes. This may involve adding an additional algorithm on the list. Once we've implemented it, it should be easy to spot.

- FH flagged that open SSL4 came out, so this may be a point to include this there. If it's already in Open SSL and there is a binding to it, we could put that into the code and use the algorithm. He also noted that following the previous action item regarding changing the header, there would be no need to change anything if we use this algorithm.

PRs and Issues on GitHub

- In the python code, FH has written a C extension that pulls the code out of libsodium that implements the algorithm we are using, which needs to be custom compiled for each machine based on different types of CPUs, machines, etc. There was a suggestion from someone else to use a cryptography package to do the binding, but our package would be a dependency with pure Python code. This individual made three pull requests, but we would like to find a way to keep his contribution inside the repo. However, he also touches on other files that are outside his scope in the PR.
- VM suggested cherrypicking the comments.
- FH has chatted with Oscar about next steps, where he has opened four issues in GitHub to start discussions.
- RD shared this link: https://github.com/samtools/htslib/blob/develop/CONTRIBUTING.md ; there's a section on complexity.
- FH flagged the PR is not inside the Crypt4GH repo, since it was done in the individual's repo.
- RD suggested that you can minus the author and his email address. FH agreed this allows him to control the code. In the link above, FH recommended the 'signing your work' section. This would note that the project is allowed to use the code that's contributed, and they sign it off.
- VM suggested the utility of the AI policy across all of GA4GH. RD also flagged the importance of the AI policy, shown in the link above.
- FH noted that one possibility is to redo the code, or approach this though a 'dictator style' (take his code and redo it ourselves)

Idea plugin system:

- FH suggested splitting the code and making the rest cryptography-dependency, which can be externalized to another package which is loading keys from different formats that is 32bytes that is passed onto Crypt4GH. This allows inserting inside the Crypt4GH code how to read the formatted keys. You could also load from an agent, PKS, etc. There's lots of formats for storing the keys, and unlocking them. If we externalize that and have plenty of plugins, it makes the code of Crypt4GH able to load plugins. However, there is a question of how Crypt4GH can talk to that agent - do you get the key out of the agent or do you actually give the header that you're trying to decrypt? RD noted that the decrypted header can be returned back.

- RD noted that by keeping the header keys in the agent, it's similar to linking things like AJS which are not ideally secure. You could make the agent more secure because it's a smaller piece of software.
- FH asked whether this would include creating an ephemeral key. RD clarified that it has encryption in the communication between the client and the server, so the agent takes the headers and returns the file keys.
- FH suggested that if the channel is encrypted, perhaps the re-encryption isn't needed. What you get back is the header decrypted inside this channel, and you move onto decrypting the rest of the file.
- FH asked if you pip install the package, the agent might be a dependency. He questioned whether you would start an agent already inside that you point the utility to. RD clarified that you could start an agent that started a shell in which you run all the Crypt4GH functions.
- FH noted that having an agent or separating loading keys into another package, it can be a nice way to split to allow the Python package to be pure-python dependency.

2026-09-15

Chair:
Attendees: Robert Davies, Frédéric Haziza, Oscar Martinez Llobet, Lishuang Shen, Shu (Sue) Chen, Jessica Seegobin, Venkat Malladi, Daniel Uribe, Titus Njoku

	Actions Arising	Assigned To	Deadline	Status
1	Continue discussions regarding encryption and the progress updates related to v2 at the next meeting	All	September 15	
2	Discuss the format of the post-quantum header			
3				

	Agenda Item	Person/Time
1.	Welcome, Introductions	Jessica
2.	Review Previous actions	All

3.	*AOB*	All

Meeting Minutes:

Open discussion

- Robert Davies (RD) opened the floor for general comments and questions.
- Shu (Sue) Chen (SC) provided an introduction being based at NIH, supporting work on implementation and responsible data sharing across different platforms, et cetera.
- RD noted a key topic of discussion is exploring how DRS and Crypt4GH can work better together. Venkat Malladi (VM) noted interest in integrating Crypt4GH into DRS and federated analysis. RD noted the concern with sending keys to each other.
- VM noted ongoing work with the tech team, putting implementations into the reference cloud with the goal of a compute implementation, either TES or WES.
- VM asked what is the most mature implementation of Crypt4GH, noting that there would be DRS URIs that would be passed to the workflow. Frédéric Haziza (FH) mentioned that the challenge lies in the key and loading it, especially if it's locked in the system. One can also use SAM tools and points directly to the Crypt4GH file. FH also noted that the file system is already mounted including the key, and if you have the passphrase, the file system will show the files as if they were decrypted where you can point the DRS URI to the file. The issue with the latter, however, is who is responsible for mounting.
- FH flagged another scenario, where the key is already in the virtual machine; all that's missed is the passphrase to unlock the key and headers and then point to the files.
- VM asked for a hands-off approach, how would the worker nodes get the headers to decrypt the files. RD noted the issues of trust if running remotely.
- VM asked if a key vault could be used to mount to the worker notes, preventing the user from access. In this case, FH mentioned that two keys would be used; when the header is generated with the public key, the user will login in, inspect the files, and open the header.
- RD highlighted that the compute node has a passbot that it's using to get access to all this data. FH noted this would imply that both the headers and payloads have a full Crypt4GH file on the system, but it would be the issue of opening the private key to open the headers with the passphase. RD flagged a workaround that would involve making ephemeral keys.
- Daniel Uribe (DU) mentioned his work does not require secrecy in terms of genomic processing of BAM fuels, but rather privacy focused on consent and transparency. He noted that enclaves and secrecy vaults are not required for genomics, since the key challenge for patients is understanding what researchers are doing with their data and preventing sharing with insurance companies. Enclaves are more related to secrecy computation, and are not required by GDPR.

- DU flagged that computational environments are sensitive to cost. He mentioned that blockchain technology can be used to trace signatures and permissions inside the tokens, helping to verify who's having access to data.
- RD noted Cryt4GH might not necessarily relate to homomorphic encryption. He explained that it involves having a large set of data, keeping it encrypted while they're sitting on the disk to prevent unauthorized access. DU flagged his work as designed by file systems that are encrypted, and are owned by the patient. VM shared that this doesn't work in a shared system of people. FH noted that you can mount at scale if you detect the incoming connection. RD mentioned the Crypt4GH is similar to what an encrypted file system is but works differently re. Individual files; if you give someone the key to read it, they can just stream off the unencrypted data which means there's a specific level of trust.
- DU noted that UK Biobank is a central repository, transparent towards the patient. RD flagged the latter as working towards an airlock where someone inspects the data in order for it to be released. VM noted that these are similar concerns in the FAWS, where you have a test environment and production environment and access to the production environment is only given if you prove with specific evidence before getting approved. RD added that the UK Biobank has ten analyses that you can run, and you can choose from them; if you want to add a new one to it, you have to go through a fairly arduous process to prove it's not malicious.
- VM asked while decrypting on the node, whether the expectation is that the output files are also encrypted again before it proceeds. RD clarified that if you're local to the node, it isn't a problem if you've managed to arrange an encrypted file system as long as the encrypted file system kind of self-destructs after it's utilized. VM noted that the next version of DRS will involve a write-back , providing the public key afterwards into DRS.
- VM noted that the TES / WES itself will download the URLs. FH shared that with file systems, the node does not need to be owned; it can be outside elsewhere where you can connect remotely to it, and transport the Crypt4GH files and need to locally decrypt it. Alternatively, the administrator has an ephemeral key, transports the file into the virtual machine decrypted. FH noted that the transport itself is encrypted. He flagged the latter has the challenge of the server containing all of the decrypting burden (e.g. NFS server), but the benefit is that one can cache.
- FH noted there's a remote remote server that transports Crypt4GH files back over SSH, and the machine decrypts them without streaming the entire file.

Progress updates

- FH noted that he's written the implementation of V2 in Python, but verification is pending. He mentioned interest in doing another implementation, looking at Zig. The disadvantage is that it's unstable, which could require rewriting the code. FH mentioned the advantage is that it comes with tooling, extra libraries, and the post quantum SHA number already selected. Another benefit is that you can compile the code for a

particular target machine with a small binary that you can stick to some web page that people can download and run. This would allow shipping of the binary. FH also shared this could compile to WASM, which can be sticked into a JavaScript environment and have a webpage with a graphical interface to drag and drop your files to become encrypted. At EGA, they'd like to stick into it a SSH connection to upload the file. VM flagged this would be client-side encryption.

- FH shared that the issue of drag and drop is related to the name that's given to the remote one.
- FH mentioned that his current work stopped at Zig 1.0, noting it's still not a guarantee but rather good confidence. He mentioned the benefit of someone else writing the code could be useful.
- RD noted work on v1.0 either works completely or not at all. FH noted you can write tests inside the source code in Zig, whereas Python allows putting the test elsewhere and running the tests.
- VM asked if you give Claude code the spec, would it be able to confidently recreate it? RD encouraged sending the latest version. RD noted that he's attempted using Claude, but it didn't produce good results. There were also some parts that Claude missed. VM agreed that Claude can only perform the simple parts of coding.
- Regarding V2 and the spec, FH noted that the public key of the sender was moved with two more pacers showing up; there's one timestamp packet that contains an expiration date that can be passed and stops the decryption. FH shared that it's hard to control the clock of the machine. He also mentioned the second was the payload URL, and ongoing discussions of using JSONLD to describe all the details needed to open the URL. He mentioned this should be outside Crypt4GH in SQLite, which contains the header and a path to the payload. RD noted the token would be short-lived.
- RD shared that if you apply only the URL, you can only send the data to get the information you want possible in the URL line, but a full web request can have all sorts of other headers attached to it, including an authorization token.
- FH asked about the format of the post-quantum header. RD noted ongoing revisions need to be done on this offline, but shared the benefit of brainstorming on this call.
- VM noted interest in taking python implementation of V1 to integrate into DRS.

Global Alliance
for Genomics & Health

2026-08-25

Chair: Frédéric Haziza (IFB/Elixir-FR), Robert Davies
Attendees: Dmitry Repchevsky, Tom Conner, Robert Davies, Venkat Malladi , Jessica Seegobin, Dan Imbrogno,

	Actions Arising	Assigned To	Deadline	Status
1	Continue discussions regarding encryption and the progress updates related to v2 at the next meeting	All	September 15	
2				
3				

	Agenda Item	Person/Time
1.	Welcome, Introductions	Jessica
2.	Review Previous actions	All
3.	*Postponed from previous meetings:* Review progress updates for v2 - **OPTIONAL**	Frédéric
4.	AOB	

Meeting Minutes:

Review of the progress updates:

- Frédéric Haziza (FH) described the updates that have been explored in v2. Please refer to the progress updates here.
- FH noted most updates have been related to the implementation of v2, compatible with v1. The V2 implementation is currently in a separate branch and has not yet been merged.

- He stated that his tests allow for converting between v1 and v2 , but not all conversions are possible. When you export the header in v2, it needs reorganizing of the header.
- FH explained that if it's reimplemented in another language, it can help address the mistakes. Previous discussion involved having a timestamp, which is not possible to enforce but it may be informative; some implementations that read the timestamp and realized that it's expired can just reject the file. There is also a link URI packet, where we create a header and within that, insert a payload link.
- FH also highlighted questions about pointing to an S3 bucket and how it can be accessed with tokens. He also mentioned that the range option was removed.
- Downloading the package is complicated because it requires identifying which shell people want; to address this, FH made a command to install the appropriate completion. He also mentioned that implementation includes a C extension that reuses code.
- It also used PyPackage CI build wheels where users can install precompile versions where available, while retaining the option to download the source.
- FH explained that there are several architectures that have been created, with more information available in the links. The CICD in GitHub involves the creation of the different wheels and also pushes to test, allowing it to push to PyPi. He also noted the code is much cleaner

- Dmitry Repchevsky (DR) asked whether there's a draft specification. Robert Davies (RD) shared the GH repo branch here with a PDF file called Crypt4GH Version 2.
- DR mentioned participating in ELIXIR Human Data Study using Crypt4GHfor Galaxy workflows, where they're trying to infer the encrypted data as well as determine if there's a BAM file. This might help with users who may otherwise need to indicate if an encrypted file contains BAM, FASTA.
- RD noted that from a file formats perspective, you should not rely on extensions since it emerged from the 1970s.
- FH shared that the decrypted part is after the first bytes, though DR highlighted that a problem in sensitive data is that a galaxy can have no keys to decrypt.
- DR asked whether t knowing the first few bytes of BAM files could help to decrypt. RD suggested that ideally, the encrypted files should be resistant to that. FH also recommended continuing discussions on this.
- There are also concerns that unencrypted metadata could identify the underlying file format revealing information about the encrypted content.
- VM noted the querying of a person interested in the data should have access to the metadata, which is a different API from Crypt4GH. The workflow can be agnostic to that.

Progress Update 4b:

- FH shared that queries around the storage of keys, which relates to the concept of the SSH agent where some agents store the private payload and it would not be inside the code. He mentioned that the code would retrieve that by talking to the agent, retrieve the private payload, or use it remotely without giving the key.
- FH mentioned that in the Linux kernel, there is a way to store the keys. FH also shared that the variable environment involves the Passphrase to decrypt the locked key on disk. He mentioned that his goal was to prevent the key on disk from being locked, followed by passing the passphrase so the Crypt4GH code would receive the passphrase from an environment viral, would decrypt the key and then use the key. This would support storing the keys somewhere else where someone can manually add the keys to the agent securely, and then having a communication between the agent to use the keys and decrypt the files.
- RD noted that his HTSLib implementation had an agent process, where the information is passed to the agent. He shared that the goal was to explore a model closer to SSH agents, where the header is sent and decrypts it somewhere else.
- FH mentioned that there is also a way with these keys inside the kernel to allow someone to load them and then delegate. He also described the possibility of an administrator securely loading keys into the kernel and delegating access to a particular process/user without exposing the keys
- DR noted work with generating an elliptic curve from OpenSSL for EDDSA,. This involves connecting through the web service providing the private certificate for the user, and extracting the public key, encrypt file. This is private for this public key, which will get sent back to the user to decrypt it with their SSL private key. DR also highlights that this is a REST API that's installed locally as a service for encryption (Encrypta). FH mentioned that there's a debate to remove that, but we haven't talked about decrypting a header or decrypting the payload. He also shared that at EGA, re-encrypting the header is one way to delegate the access to that file to some other compute node.

Progress Update 4c:

- FH noted that there is one bare minimum for File on Disk. He also shared that In the code, the Crypt4GH implementation is different from the specification.
- Venkat Malladi (VM) recommended using a DRS URI, where you need to hit DRS to get the header back. He noted this is also an implementation issue. VM mentioned ongoing work in ServiceInfo to look at adding capabilities.
- RD showed the response that you get from an HTTPS GET server, where it sends a little bit of JSON to ignore the class body. FH indicated that JSON can have flexibility, but it can also be verbose if the aim is to minimize things.
- RD explained that if you send back a header with a DRS URL, if the library reading the header can't understand it, it won't work.
- RD suggested having an offset file to seek into before you start reading, though it overlaps with the ranger header. FH mentioned that this may already be part of the edit

test store, and may repeat the hts-get. FH recommended calling it ‘metadata’ rather than a header.
- RD asked what do you get back if you look something up in DRS; VM explained that a list of JSON payload can be retrieved, but it doesn’t describe access authorization given Passports. FH clarified that the DRS URI is just pointing to where the data is, and then there's another mechanism to retrieve access.
- RD suggested creating short-lived links to buckets for S3, though VM noted the complication with the compute given the timeout issue. FH mentioned that the EGA part of EBI involves first retrieving the token, using it to hit another endpoint. Once it timeout, you can retry with that same token. RD recommended this could also be in the JSON, where if the timestamps run out, a new header can be retrieved. FH suggested another option could be to merge the link and timestamp.
- DR asked whether the timestamps can be signed like a standard token, and if there’s an external link for the data, it can be provided in the header for the data provider to check and validate the timestamp.
- DR shared a link to the standard HTTP protocol - https://datatracker.ietf.org/doc/html/rfc9728
- RD noted that it would be useful for Crypt4GH to know very little about the underlying technology that's used.

Progress Update 4d:
- regarding Zig, FH noted that the disadvantage is that its programming language has not reached 1.0, allowing them to break anything they’d like to. Zig implementation is up until 0.16, containing all the algorithms inside the standard.
- One benefit is that it knows how to statically compile without the need for OpenSSL, meaning the binary at the end is not a dynamic file that would load dependencies. This would allow folks to download the binary easily, reducing the burden on the administrator.
- FH mentioned another merit is that it contains the implementation for MLKEM. He noted that he didn't write the code because he wasn’t sure about the format to use for post-quantic.

Next Steps:
- Continue discussions regarding encryption and the progress updates related to v2 at the next meeting - September 15

2026-06-23

Chair: Rob Davies (Sanger)

Global Alliance for Genomics & Health

Attendees: Oscar Martinez (OM) (EGA CRG), Dan Imbrogno(DI), Rob Davies (RD), Lishuang Shen (LS), Silvia Llorente (SL), Jessica Seegobin (JS), Ann Novakowski (AN)

	Actions Arising	Assigned To	Deadline	Status
1	Cancel the July 21 meeting; reschedule August meeting to Aug 25, 2026	Jessica		Completed
2	Register for the DSWS virtual hackathon (July 20 & 21 - 8am-12pm ET) - sign-up sheet here.	All	July 13	Completed
3	Progress update for v2 - review at August Meeting	Frédéric	August 25	

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	Status of July 21 & August 18 Encrypted file formats meeting - cancel/reschedule?	Jessica
4a	Review progress updates for v2: ● Implemented (in a separate branch) version 2 of Crypt4GH: ○ includes refactoring the code, and I like much more the new version ○ supporting both v1 and v2 ○ Still reading files with edit lists (but not generating them) ● v2 includes the expiration timestamp. Note: We know it's hard to enforce it, when the user has control over the machine's time anyway. So, no guarantees, it's only checking the value and bails out if it has expired. ● v2 includes the "link/URI" packet (see next point). ● v2 includes more tests to cover the implementation of version 2 (even with conversions between v1 and v2, when possible). ● Removed "—range" options. This was not the right place for it. ● Includes shell completions (bash and zsh) with an extra command. Not via the install script. ● Since I have C-extension code in the python package, I adjusted the deployment (using pypa/cibuildwheel) targeting several architectures	Frédéric

	• The CI/CD in GitHub now deploys to PyPI if I specifically tag branches. There is a test version and a production version. • Removed dependency to docopt-ng	
4b	I investigated the keyring/agent. So far, I like very much what I've seen but it's only for Linux. I am still curious about Mac. I also checked if I could read the data from the SSH-agent (both Linux/Mac) but that wouldn't work for c4gh-v1 keys	Frédéric
4c	**Requesting a discussion about the "link/URI" packet.** What format to support? Leaving it free text is ok, but then we push the issue down to the implementations. So far, I implemented a simple version. I find it better to implement a plugin system that would allow extending it with different "link-fetcher". If we go the plugin-road, then anyone choosing to split header/payload will find a way to link them together, as I did in the SQLite file system. Therefore: we need a discussion, it might *not be necessary* to have the URI packet.	Frédéric
4d	**Interested in implementing v2 in Zig**. Zig already has chach20ploy1305(+aead), bcrypt, scrypt, Curve25519 in its crypto package (as a part of its Standard Library). That's a great advantage: we'll retain C-like performance and avoid dependencies. The Zig toolchain is great and can target many architectures. Well… that's an exciting language to learn. Note that I've also looked for MLKEM768 and found it: Potentially helping our PQC attempts.	Frédéric
5	AOB	

Meeting recording:

Previous actions:

- Schedule a follow-up meeting with Rob, Tom, Jaime, and Fred - completed.

Meeting minutes:

Discussion:

- Group completed a quick round of introductions
- RD noted that the Crypt4GH specification enables you to encrypt any file, and you can do random access into those files, which is useful for our genomics formats.
- RD mentioned that the specification was developed in 2019, and there have been a few ideas for updates. One challenge is that the encryption can tell if the file has been tampered. The current method uses encryption of the file in blocks, but you can't tell if somebody's rearranged those blocks or added a new one. He mentioned there's interest in adding whole file integrity. Another focus area involves exploring quantum resistant encryption.
- DI asked about methods of maintaining whole file integrity that have been explored. RD suggested it involves encrypting the file and including an authentication code at the end of each block, and noted this can also include an extra piece of information to the authentication that is separate from the encrypted data, which allows to incorporate a counter. In order to determine when you've got to the end of the file, you need to ensure all of the blocks are the same length. He also noted that there's a slight issue related to leaking information.
- OM is interested in archives with data to serve up, but this can be complicated to perform in web servers.
- AN noted that Sage BioNetworks is interested in implementing Passports/Visas. RD highlighted the link with encrypting files via management of keys.
- RD noted that more experimentation and research is needed into quantum resistance algorithms, similar to NIST.
- RD highlighted that Frederic has been involved in exploring some implementations.
- DI mentioned his use case with a small segment of biodata, (e.g.,a GHCR38 reference from a memory-constrained environment) which needs proof that the small segment of data did come from the canonical original root file. RD suggested there may not be, given the public nature. RefGet may involve a hash to read a reference, hashing bits of it. There may not be an edge case yet. Crypt4GH has a block-based system to check that the block you read hasn't been tampered, but it's a different use case.

Meeting Updates

- Group agreed to cancel the July 21 meeting, and shift the August meeting to August 25 (10am ET)
- Progress update for v2 tabled until subsequent meeting
- JS shared details regarding the upcoming DSWS virtual hackathon (July 20&21 - 8am-12pm ET).Participants are invited to register via the sign-up sheet here. JS encouraged folks to join the DSWS meeting on **June 29** (3pm ET) as the group aims to continue hackathon discussions.

2026-05-26:

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR)

Global Alliance for Genomics & Health

Attendees “Name (Affiliation)”: Rob Davies (RD), Oscar Martinez Llobet (OML), Tom Conner (TC), Reggan Thomas (RT), Jessica Seegobin (JS)

	Actions Arising	Assigned To	Deadline
1	Schedule a follow-up meeting with Rob, Tom, Jaime, and Fred	Jessica	Completed
2			

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	Org Change - Encrypted file format to DSWS	Jessica
	A.O.B. GA4GH 14th Plenary - GA4GH 14th Plenary will take place from **28 September to 2 October 2026 in Singapore** at the One Farrer Hotel. Details here: https://broadinstitute.swoogo.com/ga4gh-14th-plenary/11059298 Regular registration closes on 14-Aug-2026	Reggan

Meeting recording:
https://us02web.zoom.us/rec/play/-q84oxwWmNhzLZGELmOW4Mx7PgJJGZfHkXSuPL-KTKY2h_F5InHSTmLAaLxQKCQeMCGG1um7gSlrVXKS._JkQ9qTupcakbDzQ?accessLevel=meeting&canPlayFromShare=true&from=my_recording&continueMode=true&oldStyle=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fus02web.zoom.us%2Frec%2Fshare%2FOORZYHJgUCmP5WEE4BDi1ofZj3KCNTN7xRLLH0QZpcvSJ7Sp5dd7jVkjLuWj7Xw.fUt_5NV7vow43mX3%3Ffrom%3Dhub

Previous actions:

- Investigate and potentially implement a Crypt4GH agent for key/passphrase handling to replace environment variables and callbacks
- Explore integrating OS-specific keyring services for secure key retention on Linux and Mac
- Share updated Crypt4GH pull request code and performance improvements with the team
- Investigate GitHub Actions or similar CI pipelines to build and publish Crypt4GH wheels for multiple platforms to PyPI
- Continue optimizing Crypt4GH v2 support and resolving issues related to partial encryption segment handling

Meeting minutes:

Global Alliance
for Genomics & Health

Welcome

The group provided introductions.

Organizational change

- TC mentioned crypt4GH will move to DSWS. He expressed interest to discuss the continued involvement of crypt4gh
- RD mentioned that he doesn't currently have any priorities for crypt4gh, but expects to explore improving data integrity and quantum resistance.He flagged that Frederic is more active in generating implementations
- OML noted the interest in implementing version 2.0, once it's out, but Crypt4GH is also not deemed a high priority because version 1.0 has been quite effective
- TC noted there are no current product owners, aside from Frederic who's more involved. RD flagged that the EGA is the main implementer. TC flagged for product owners to move Crypt4GH to new releases and/or address new issues to move it forward from a product perspective. He mentioned that we should also discuss with Sasha about the lack of product owner/lead.
- RT shared a document with the description of the product lead responsibilities
- RD flagged the current version is still effective for EGA's needs

Other

- TC mentioned that the Crypt4GH meetings have been around for some time.
- RD flagged that Crypt4GH was previously in the LSG Work Stream; the original aim was to encrypt bioformats but AGE also does something similar to Crypt4GH. More details about AGE here, which uses certain encryption algorithms.
- TC asked about the rationale for using Crypt4GH and the main use cases. RD suggested that you don't necessarily need to use this if you have encrypted file systems.
- TC asked if there is a reference implementation available; RD noted that there was a GIF AMA event held a few weeks ago.
- TC suggested that crypt4gh is in good shape and should continue to have meetings
- TC noted that we should get crypt4gh into the cloud WS, federated ML group regarding implementation of GA4GH APIs
- He also flagged that there's a DSWS hackathon coming up, and welcomed someone from crypt4gh to join
- The group also discussed possibility of servicing https://samtools.github.io/hts-specs/crypt4gh.pdf into the DSWS roadmap
- JS asked about whether we should amalgamate Crypt4GH meetings into the biweekly DSWS meetings. TC recommended keeping them separate, so the Crypt4GH monthly meetings will continue as planned.

- JS asked about scheduling a follow up meeting, since Jaime Delgado and Frederic Haziza weren't able to attend; TC agreed.
- RT noted that the next meeting is on June 23 at 10am ET
- JS shared the meeting details for the upcoming DSWS biweekly meeting on June 8 (3pm ET)

Join Zoom Meeting
https://us02web.zoom.us/j/81746162406
Passcode: GA4GH
Add event to calendar

- RT shared there's an organizational shift of LSG products to other Work Streams. He also mentioned the upcoming Plenary and encouraged folks to register.

From Zomm Chat :

00:15:57 Reggan Thomas: Product lead - https://docs.google.com/document/d/1a0O3mFceDBzupaceF9DtAzjRbu4FQtJXN8nmPCk1S-Y/edit?tab=t.0#heading=h.mc11oyljuolv

00:21:05 Robert Davies: https://github.com/FiloSottile/age

00:27:06 Jessica Seegobin: https://docs.google.com/document/d/1DHr5abv-xI1iw85qWvYcXUzDUBjuZWxp1qILjQxSZ74/edit?tab=t.0 GIF AMA

00:27:07 Robert Davies: https://docs.google.com/document/d/1DHr5abv-xI1iw85qWvYcXUzDUBjuZWxp1qILjQxSZ74/edit?tab=t.0

00:27:22 Reggan Thomas: https://docs.google.com/document/d/1DHr5abv-xI1iw85qWvYcXUzDUBjuZWxp1qILjQxSZ74/edit?tab=t.0 ?

00:32:39 Robert Davies: https://samtools.github.io/hts-specs/crypt4gh.pdf

00:33:34 Jessica Seegobin: DSWS Biweekly Meetings:

Join Zoom Meeting: https://us02web.zoom.us/j/81746162406

Meeting ID: 817 4616 2406

Passcode: GA4GH

Global Alliance for Genomics & Health

Add event to calendar

Next meeting: June 18 - 3pm ET/ 19:00 UTC.

00:36:52 Reggan Thomas: June 23 at 3 pm BST

00:37:36 Reggan Thomas: GA4GH 14th Plenary - GA4GH 14th Plenary will take place from 28 September to 2 October 2026 in Singapore at the One Farrer

Hotel. Details here:

https://broadinstitute.swoogo.com/ga4gh-14th-plenary/11059298

Regular registration closes on 14-Aug-2026

2026-04-28:

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR)
Attendees “Name (Affiliation)”:

	Actions Arising	Assigned To	Deadline
1			
2			

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	AMA session review GIF AMA: Crypt4GH	Rob
4.	Python C extension: 8x improvements. PR#53	Fred
5.	Refactored crypt4gh-keygen PR#54	Fred
6.	Todo: Packaging v1.8 and publish to PyPI	Fred
	A.O.B.	

Meeting recording:
Meeting minutes:

- **Connect Event Success:** Over 40 AI use cases collected; plans for further engagement and collaboration on VCF use cases were discussed.

- **Crypt4gh Implementation Discovery:** Java-based version discovered; interest expressed in expanding support to more programming languages.
- **Performance Gains:** C extension reduced encryption time for 10GB file from 2 minutes to 18 seconds; packaging challenges discussed for multi-platform support.
- **Security Enhancements:** Proposal for key agent to improve security and user experience; agent would cache keys securely in memory.
- **Protocol Extensions:** Patch for OpenSSH's SFTP to include decrypted file size; discussions on extending SFTP for better integration with Crypt4gh features.
- **Next Steps:** Focus on multi-platform C extension deployment, follow-ups for collaboration, and enhancements on file transfer and key management.

Notes

Event Recap and Use Case Collection

The meeting reviewed recent participation at the Connect event and progress on collecting AI use cases.

- **Successful Connect event participation with diverse subgroup updates and AI workstream kickoff** involved day one covering all LSC subgroups including GRIP4GH and an AI stream that generated enthusiasm with around **40 AI use cases collected** (02:45)
    - The AI use cases are currently being categorized for further analysis and prioritization
    - Augustine Randon from Genomics England showed interest in future VCF use cases, indicating potential collaboration opportunities
    - The meeting discussed continuing engagement by following up with interested parties from the AMA session to convert interest into actionable commitments
    - Some attendees noted session timing and engagement issues, particularly with late sessions like Passport, suggesting scheduling improvements
- **Discovery of previously unknown implementation within Crypt4gh ecosystem** surfaced during the AMA, revealing a Java-based version maintained by Dimitri that uses certificate-driven key encryption for HTTP servers (08:00)
    - This implementation adds to the ecosystem covering multiple languages: Rust, Go, Java, JavaScript, Python, and C
    - The team expressed interest in expanding support to other languages such as OCaml, Ada, Nim, Julia, and Zig to broaden scientific computing reach

Crypt4gh Encryption System and Technical Challenges

Deep discussion on Crypt4gh's encrypted file system and ongoing technical challenges around connection stability and key management.

- **Rob detailed Crypt4gh's encrypted file system in use at EGA, efficiently handling over 2 petabytes of encrypted data with live re-encryption on file retrieval** (15:30)
    - The system auto-manages user permissions and encrypts files on the fly without manual intervention, enhancing security and usability

    - A core unresolved issue is handling partial encryption when connections drop mid-segment, leading to potential file corruption or incomplete data without private key access on the server
    - Proposed solution involves ephemeral key usage stored temporarily on the server to decrypt the last segment if the connection breaks, mitigating data loss risks
    - The complexity arises because the server lacks the private key for security reasons, complicating recovery of half-written segments
- **Potential enhancements leveraging Crypt4gh version 2 features to report decrypted file sizes and enable safer resumptions were discussed** (21:30)
    - The idea is to checkpoint file transfers at segment boundaries and report sizes to allow restarting from last complete segments without private key exposure
    - Different transfer protocols like SFTP and Aspera were noted to have varying capabilities in detecting dropped connections, complicating a universal solution
    - Future HTTP/3 and QUIC protocol support could improve detection and recovery of partial transfers

Performance Improvements via C Extension and Packaging

Significant performance gains were achieved by rewriting core encryption functions in C and improving Python packaging.

- **Rob created a C extension for Crypt4gh's core encryption and decryption functions, reducing encryption time on a 10GB file from 2 minutes to 18 seconds** (26:40)
    - The C code tightly integrates with Libsodium and removes overhead from repeated memory allocations in the prior Python implementation
    - Profiling revealed debug hex conversion calls added 10 seconds, which were removed to maintain the improved speed
    - The approach uses minimal C code covering only seven critical Libsodium functions, avoiding large dependency compilations
- **Packaging challenges include compiling the C extension on target machines, requiring GCC and build tools, and distributing platform-specific wheels to ease installation** (31:00)
    - Rob explored using GitHub Actions for automated building and publishing pre-compiled wheels for Linux, MacOS, and Windows to PyPI
    - They referenced successful models like PyNaCl and PySAM which maintain multi-platform wheel builds via CI pipelines
    - Windows support was considered optional given the user base primarily uses Linux and MacOS environments
    - Source-only distribution remains as a fallback where build tools are unavailable

Security and Passphrase Management Enhancements

The team debated best practices for handling passphrases securely and explored agent-based key management as a strategic improvement.

- **Concerns were raised about the insecurity of passing passphrases via environment variables, which exposes secrets in process listings and logs** (44:00)

    - The current approach prints passphrases to standard error, which some users find insecure, though suppressing these messages risks hiding real errors
    - The team proposed introducing an explicit environment variable toggle for users who understand the risks and want to suppress warnings
- **A strategic proposal to require Crypt4gh to operate exclusively with a key agent was discussed to improve security and user experience** (47:00)
    - This agent, similar to SSH agent, would prompt once for the passphrase and securely cache key material in memory for subsequent operations
    - The agent would interface with OS-specific key stores or kernel key retention services on Linux, MacOS, and possibly fallback to manual input on Windows
    - Agent forwarding over SSH connections was considered to allow remote command executions to retrieve keys securely from the local machine
    - Implementation would require code changes to avoid passphrase callbacks and rely on agent communication, improving security by avoiding environment variable exposure

Protocol Extensions and Forward Compatibility

Technical work on extending existing protocols to support Crypt4gh features and improve metadata transmission was covered.

- **A patch to OpenSSH's SFTP implementation was created to include decrypted file size as part of file attribute listings** (55:20)
    - This addition is within the protocol specification but not implemented by default in OpenSSH, enabling clients to know the true decrypted file size without extra queries
    - Such extensions facilitate better client-side handling of encrypted files and improve integration transparency
- **Discussions highlighted the possibility of extending SFTP protocol operations to better support Crypt4gh features including agent forwarding and advanced file metadata** (53:00)
    - The team acknowledged that OpenSSH's SFTP supports optional extensions that could be leveraged for forwarding agent requests and richer file info transfer
    - However, practical adoption depends on server and client implementations supporting these optional protocol features

Next Steps and Development Focus

The team agreed on priorities and ongoing work to enhance Crypt4gh usability, performance, and security.

- **Rob plans to push the new C extension code to PyPI after establishing a robust multi-platform build pipeline using GitHub Actions** (56:30)
    - This will allow users to install Crypt4gh with precompiled binaries, reducing setup complexity and increasing adoption
    - A fallback source-only package will remain for environments lacking build tools
- **Follow-up engagement is needed with AMA session participants who showed interest in Crypt4gh to convert curiosity into concrete collaboration or testing** (07:00)

    - Regan volunteered to reach out to interested individuals for scheduling follow-up meetings
- **Further development on Crypt4gh version 2 features is pending to solve file transfer resumption and partial segment issues, enhancing robustness in unstable network environments** (01:01:30)
    - This aligns with the goal of making Crypt4gh production-ready for large-scale encrypted genomic data handling with minimal user friction
- **Security enhancements around key handling and agent integration remain a high priority to reduce reliance on insecure passphrase methods and improve cross-platform support** (48:30)
    - Work will include exploring kernel key retention APIs, agent forwarding, and OS-specific secure key stores for seamless user experience across Linux, MacOS, and Windows platforms

Action items

- Follow up with participants who showed interest in the AMA session to organize a follow-up or meeting to maintain engagement (07:40)
- Investigate and potentially implement a Crypt4GH agent for key/passphrase handling to replace environment variables and callbacks (48:30)
- Explore integrating OS-specific keyring services for secure key retention on Linux and Mac (49:19)

Unassigned / Rob

- Share updated Crypt4GH pull request code and performance improvements with the team (25:00)
- Investigate GitHub Actions or similar CI pipelines to build and publish Crypt4GH wheels for multiple platforms to PyPI (32:52)
- Continue optimizing Crypt4GH v2 support and resolving issues related to partial encryption segment handling (18:19)

General / Team

- Collect and consolidate chat notes and session recordings to produce detailed minutes and summaries from meetings (01:02:50)

2026-03-31: AMA

Chair: Mallory Freeberg (EBI)
Attendees “Name (Affiliation)”: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR),

	Actions Arising	Assigned To	Deadline
1			

2			

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	Slides for AMA session https://docs.google.com/document/d/1DHr5abv-xI1iw85qWvYcXUzDUBjuZWxp1qILjQxSZ74/edit?tab=t.0	Rob
4		
	A.O.B.	

Meeting recording:
Meeting minutes:

GIF AMA: Crypt4GH

2026-03-03:

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR)
Attendees “Name (Affiliation)”: Oscar Martinez (EGA)

	Actions Arising	Assigned To	Deadline
1			
2			

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	Slides for AMA session https://docs.google.com/document/d/1DHr5abv-xI1iw85qWvYcXUzDUBjuZWxp1qILjQxSZ74/edit?tab=t.0	Rob
4	Crypt4gh-sqlite file system (docs)	Fred
	A.O.B.	

Global Alliance for Genomics & Health

Meeting recording:
Meeting minutes;

AMA agenda here - GIF AMA: Crypt4GH

Slide deck - 20260331-GIF-AMA-Crypt4GH

- How did you decide that implementing Crypt4GH was right for your project?
- What challenges did you encounter planning implementation (technical, legal, social, ethical, etc.)?
- What challenges did you encounter getting your implementation in production?
- What challenges did/do your users facing using your implementation?
- How did you overcome these challenges?
- What aspects of implementing Crypt4GH have gone well?
- What are the next steps on your roadmap to developing and/or implementing Crypt4GH?
- What new features are being worked on or planned for the future?
- How would you like to collaborate in the future to implement or improve Crypt4GH?

Oscar - https://github.com/EGA-archive/ega-quickview

2026-02-03: Cancelled

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR)
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.	

Global Alliance for Genomics & Health

Meeting recording:
Meeting minutes;

2026-01-06: Post Quantum

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR)
Attendees “Name (Affiliation)”: David Salgado (IFB/Elixir-FR), Reagan Thomas (GA4GH)

	Actions Arising	Assigned To	Deadline
1			
2			

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	Post-quantum encryption - openssl. See also RFC 9180 - Hybrid Public Key Encryption	
4.	A.O.B. - Ask me anything (AMA) meeting - when should we schedule this meeting? 3rd or 31 March? - Typically asked questions here - Passports AMA and Beacon AMA. 2) Priorities for 2026? Next meeting - Feb 3, 2026	
	Connect proposal - Submit through Nolt - https://ga4gh-connect-session-proposals.nolt.io/ 📅 Proposal Timeline Opens: 1 December **Closes: 30 January** Secretariat review: 2 to 13 February Sessions confirmed: 20 February Register for connect - https://broadinstitute.swoogo.com/connect26/10375924	

Meeting recording:
Meeting minutes:
The meeting discussed the implementation and future of cryptographic protocols, particularly Crypto GH v2 and quantum-resistant encryption. Fred reported no progress since the last

meeting due to holidays and a new position. Rob highlighted the availability of quantum-resistant algorithms in OpenSSL and IBM's roadmap predicting quantum computers' impact by 2029. The team debated whether to integrate quantum resistance into Crypto GH v2 or wait for v2.1. They also discussed the need for concrete user questions for an upcoming "Ask Me Anything" session to ensure relevance and usefulness. The meeting concluded with plans to gather user questions by mid-February and schedule the session for March 31st.

Action Items

- Focus on completing the crypto-GH v2.0 specification before potentially adding quantum-resistant features in a v2.1 release
- Reach out to the organizers of the AMA session to get concrete questions from the target audience by mid-February, and potentially cancel the session if no relevant questions are received
- Implement quantum-resistant encryption algorithms in the crypto-GH v2.0 specification
- Explore using the hybrid encryption approach to future-proof the crypto-GH specification
- Ensure the crypto-GH specification is in a good state by the time of the Connect conference in April

2025-12-09: Cancelled

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB/Elixir-FR)
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:

Global Alliance
for Genomics & Health

2025-11-18: Python V2 Header

Chair: Rob Davies (Sanger), Frédéric Haziza (IFB-CNRS)
Attendees “Name (Affiliation)”: Oscar, Reggan

	Actions Arising	Assigned To	Deadline
1			
2			

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	Good read on PQC: https://www.ietf.org/archive/id/draft-ietf-pquip-pqc-engineers-14.html	Fred
4.	Python v2 headers	Fred
5.	Todo: ● Fix tests and add new ones for v2, including v1 <-> v2 conversion ● Fix docs ● Update the PyPI package ● Fix bash completion ● Implement S3 fetcher (for v2 header with URI)	Fred
6.	API update => fix LocalEGA dependency (eg use package 1.7/1.8) https://github.com/EGA-archive/LocalEGA/blob/master/src/handler/requirements.txt	Oscar
7.	Python PQC: ● WolfCrypt: https://www.wolfssl.com/wolfcrypt-python-pqc-algorithm-support/ ● Or C binding to OpenSSH ML-KEM implementation ? https://github.com/openssh/openssh-portable/blob/master/libcrux_mlkem768_sha3.h	
8.	Drop edit list for v2? Idea: segments are S1:S2:S3:...:S10:S11:...S20 and we send S1:S10:S17:S20 With AEAD, after we tried S1 with sequence number 1, we should try S10 with 2, but need to jump to 10. That’s what we can in case aead fails. We must therefore send the sequence numbers, 1:10:17:20 in order. That’s a new “edit list” packet.	Fred

	I suggest to drop edit list with v2, since we are building it so we can't "drop" packets. Therefore, not working well with the combo HTSGET+Crypt4GH.	
	A.O.B. - Next meeting - Dec 9, 2025 - Ask me anything (AMA) meeting - when should we schedule this meeting?	

Meeting recording:
https://us02web.zoom.us/rec/play/Deh-03lpP2yS7WVGoa_E_smeerSK6e21lT1WYMzlc-tbj4-6Qe2Um6P13LyaITQBt2k5xRWf644k57CK.DM-SzR7W0lC3YgFv?eagerLoadZvaPages=&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fus02web.zoom.us%2Frec%2Fshare%2FgYQSzn9dFlI_EURv_KfgIEBMChKXBdFYQGbr7OMUkxFmiXx-nCRpwJatjSVm5iin.B4I3YESs6KAyOili

Meeting minutes:
Summary
The meeting discussed several technical updates and future plans. Fred and Rob reviewed the implementation of Python v2, which includes new headers, refactored code, and additional tests for header and payload conversion. They also discussed the potential removal of the edit list feature in v2, arguing it adds unnecessary complexity. Oscar mentioned using auto.ai for transcription and the integration of quantum computing concepts. The team debated using open SSL or wolfSSL for quantum encryption. They also planned to update the Python package index and fix bash completion. The next meeting is scheduled for March 9, with preparations for an Ask Me Anything session in Q1.

Action Items

- Implement version 2 of the crypt4gh library without the edit list feature.
- Investigate integrating a quantum-resistant algorithm, such as MLKP, into the crypt4gh library.
- Pin the Python package version for localEGA usage to 1.7 or 1.8.
- Prepare for the upcoming "Ask Me Anything" meeting on crypt4gh, including identifying common questions and preparing visual aids.

2025-10-14: Python Implementation

Chair: Rob Davies (Sanger), Frédéric Haziza
Attendees "Name (Affiliation)": Oscar Martinez (EGA), Reggan Thomas (GA4GH)

	Actions Arising	Assigned To	Deadline

Global Alliance
for Genomics & Health

1	Decide on approach for adding post-quantum key exchange support to v2 header format.	Rob / Fred	
2	Prototype post-quantum key exchange implementation in Python.	Rob / Fred	
3	Review OpenSSH and OpenSSL post-quantum key exchange implementation details.	Rob / Fred	

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	Rob/ Fred
2.	Previous Actions Review	Rob / Fred
3.	Python implementation	Fred
4.	ML-KEM in SSH: ● https://www.ietf.org/archive/id/draft-ietf-sshm-mlkem-hybrid-kex-03.html ● Post-Quantum Kex: https://www.openssh.com/pq.html ● OpenSSH 10.1: https://www.openssh.com/releasenotes.html#10.1p1 ● Add warning in implementations for risk of "store now, decrypt later" attacks. ● SSH uses: **** WARNING: connection is not using a post-quantum key exchange algorithm.** **** This session may be vulnerable to "store now, decrypt later" attacks.** **** The server may need to be upgraded. See https://openssh.com/pq.html** 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: https://github.com/openssl/openssl/blob/master/doc/man7/EVP_KEM-ML-KEM.pod 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 (aka ML-KEM)	
	A.O.B. Next meeting - Nov 11th. (Meeting Free Week). Cancel or reschedule ? Reschedule to November 18 at 3pm BST	Reggan

Meeting recording:

Global Alliance for Genomics & Health

Meeting minutes:
The meeting discussed updates on the Python implementation, specifically the upgrade from docopt to docopt-ng, which involved minimal code changes. The team also explored post-quantum key exchange, focusing on the MLKM algorithm and its integration with OpenSSL and OpenSSH. They considered adding a new header type to support post-quantum keys in version 2. The next meeting is scheduled for November 18th. Additionally, there was a brief discussion on the importance of understanding the key format for post-quantum encryption. The team plans to prototype and test the new implementations.

Action Items

- Decide on approach for adding post-quantum key exchange support to v2 header format.
- Prototype post-quantum key exchange implementation in Python.
- Review OpenSSH and OpenSSL post-quantum key exchange implementation details.

Python Implementation and Documentation

•Fred discusses the Python implementation and a tiny upgrade to the code.
•The upgrade involves changing "docopt" to "docopt-ng" in the import statement.
•Fred mentions the pull request and the minimal changes required.
•Discussion on the benefits of fewer dependencies and the potential to use "argparse" instead.

OpenSSL and Post-Quantum Key Exchange

• Fred talks about the post-quantum key exchange and its implementation in OpenSSH.
• Mention of the MLKM key exchange module and its standardization.
•Discussion on the use of OpenSSL and OpenSSH in different implementations.
•Fred suggests adding a new header type in the protocol to support post-quantum keys.

Prototype and Implementation Considerations

•Fred proposes prototyping with Python and using a wrapper around OpenSSL.
•Discussion on the need to update the header format to include a new packet type.
•Rob suggests making the new encryption method the default in future versions.
•Fred mentions the need to test and validate the new implementation.

Future Meetings and Post-Quantum Encryption

•The next meeting is scheduled for November 18th.
•Fred expresses interest in working on post-quantum encryption during their holidays.
•Discussion on the potential for creating a presentation on post-quantum encryption.
•Fred mentions the importance of understanding the key format and its implementation.

2025-09-16:

Chair: Rob Davies (Sanger), Frédéric Haziza

Global Alliance for Genomics & Health

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 https://github.com/C2SP/C2SP/blob/main/XAES-256-GCM.md https://eprint.iacr.org/2025/758.pdf	Rob Davies
	A.O.B. Connect poster - GA4GH poster template blank.pptx Deadline - 25th Sep	Reggan

Meeting recording:
https://us02web.zoom.us/rec/share/Hdr0ek6FbsojB3Vwkma80mo_3F1LbkI8Ebxg_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.

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 https://github.com/C2SP/C2SP/blob/main/XAES-256-GCM.md 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. 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. Next meeting - 27 May, 2025	

Meeting recording:
https://us02web.zoom.us/rec/share/vvpFXluygzseIcCIknpk3MZUn8TNIRWHKQyqPJmSqZJYFVGd0Gi8XgtwDY0sI5DE.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. Next meeting - 1st April - Cancel or reschedule?	

Global Alliance
for Genomics & Health

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/
14.8.4 documented feedback from adopters - https://docs.google.com/spreadsheets/d/1NScZPC34tZ2MTeI1lyTBDb645_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. 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

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: Open Quantum Safe	

	Post-Quantum Cryptography Alliance	
	A.O.B. - Connect meeting - 1 to 4 April 2025 • Broad Institute of MIT and Harvard, USA **Register for Connect** - Add your connect session proposal to the Easyretro board here by 6th Jan - Need to submit proposals in the form by 13th Jan 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	

Global Alliance
for Genomics & Health

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions Review	
3.	Post-quantum cryptography: Open Quantum Safe Post-Quantum Cryptography Alliance	
	A.O.B. 1) Next meeting on Dec 10, 2024 2) Connect meeting - 1 to 4 April 2025 • Broad Institute of MIT and Harvard, USA **Register for Connect** 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. 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. 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			

Global Alliance
for Genomics & Health

	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. 5) Next meeting on Aug 20, 2024 (MFW - Cancel or reschedule ?) 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. Next meeting on Jul 23, 2024	

Global Alliance for Genomics & Health

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

	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 - Full-file integrity (ongoing) - Move writer’s key - Detached headers - Header signing - Time-limited access	Rob
5.	Work on the python implementation: Storing header in a separate file	Fred
	A.O.B. Next meeting on Jun 25, 2024 Webinar on The Role of Trusted / Secure Environment - June 13 at 1 pm ET 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_qIUq5qHsvzRaPuCtRWpm_2LF08_XVm8mslieuHiE6ZER8VF4Klp.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 - Full-file integrity (ongoing) - Move writer’s key - Detached headers - Header signing - 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

Global Alliance
for Genomics & Health

1	Prepare an agenda for connect. Topics to include: 1) Key management (Custom key exchange protocol) 2) Cloud - DRS and TES	Rob	Apr 2, 2024
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 Agenda doc here	Robert
4.		
	A.O.B - Next meeting on Apr 2,2024 - 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.

Global Alliance for Genomics & Health

2024-2-06: PR 736 and New location

Chair: Rob Davies (Sanger) , Frédéric Haziza (GIP-CAD)
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 https://github.com/ga4gh/ga4gh-crypt4gh	
	A.O.B - Connect meeting (April 21 - 24) at Ascona, Switzerland. Hybrid participation available. - Submit your connect meeting proposal here (deadline - Feb 16,2024) - 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	

	- https://github.com/ga4gh/TASC/issues/40 - James Eddy is working on the documentation around “when do products move into their own repo”? - Connect meeting (April 21 - 24) at Ascona, Switzerland. Hybrid participation available. - Submit your connect meeting proposal here (deadline - Feb 16,2024) - 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 - 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.

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 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 - 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-.zzpRBucKTnZigM4J

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.

Global Alliance for Genomics & Health

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

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 1) Alexander Senf (github user: asenf? ← confirm) 2) Robert Davies (github user: daviesrob) 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. Connect session agenda Presentation - template Deadline - **05-Sep for agenda items** **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

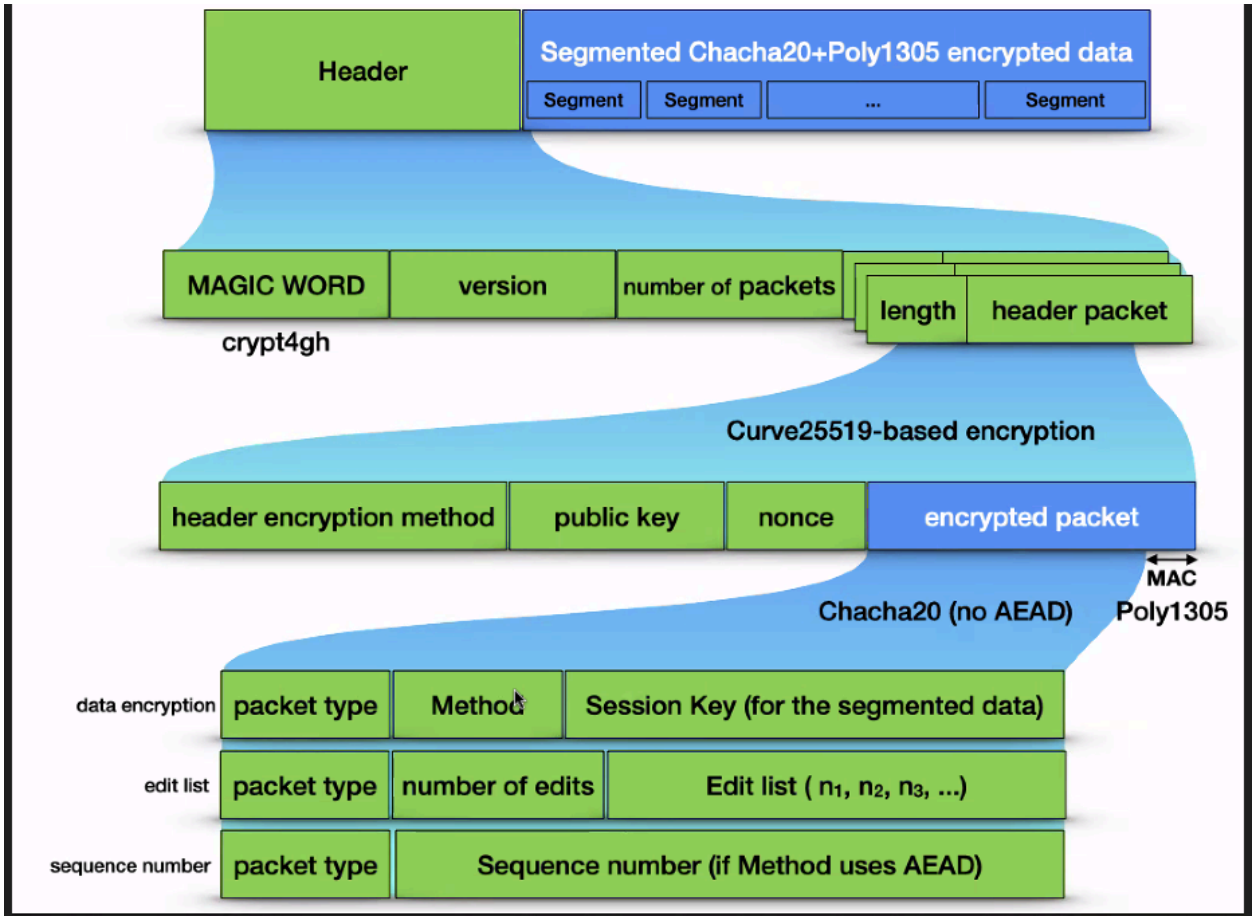
Chair: Alexander Senf
Attendees “Name (Affiliation)”: Fred, Rob Davies (Sanger), Andrejs Puckovs (MGI-Tech),Reggan Thomas (GA4GH)

	Actions Arising	Assigned To	Deadline
1			
2			

	Agenda Item	Person/Time
1.	Welcome, Introductions & Confirm Agenda	
2.	Previous Actions	
3.	AEAD support: • Python Implementation (separate branch) • Documentation • PR for Crypt4GH specs Introducing a new encryption method and packet type.	Fred
4.		
5.		
	A.O.B. 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 ● AEAD PR ● U.S. AES-256 requirements ● Split header/payload	
3.	Cloud API Support (e.g. DRS) - protocols (CRG, PA, GHGA, …) (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 • AEAD PR • U.S. AES-256 requirements • 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 Key Takeaways and next action items 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 ● htsget-rs (UMCCR Melbourne; repo, issue) ● ELIXIR Switzerland GSoC ● DRS PoC (want to present something at GA4GH Plenary 2023) (Revisit Crypt4GH Use Cases to cover ongoing developments)	
5.	Crypt4GH Spec Updates ● Status of a possible implementation / spec PDF version? ● 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) ● Special Sessions? Special Meetings? Demos? ● Who plans on attending?	
4.	Review GA4GH Product Graphics (Feedback by Friday, February 10) ● the graphic and the graphical representation of the concepts ● the text in the graphic ● the caption that will accompany the graphic	
5.	Who is working on Cloud integrations? (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