Gimel Foundation

Gimel Foundation gGmbH i.G.
GiFo-Request for Comments: 0300
Obsoletes: -
Category: Standards Track

Dr. Goetz G. Wehberg
Digital Supply Institute
10. Dezember 2025

The Gimel Authentication Framework 1.0 (GAuthent)

Abstract

The Gimel Authentication Framework 1.0 (GAuthent) describes how to secure quantum-resistant authentication by using DNA based biometrics in terms of Gimel ID or its components.

Current authentication systems, e.g. in terms of multi-factor-authentication (MFA), generally use cryptography based on prime number multiplication. With the future use of quantum computing, this approach will no longer be able to provide the necessary security for authentication. Secure DNA based identities can help to fix this. This is how GAuthent provides a higher security for authentication, by leveraging Gimel ID.

GAuthent makes sure that current RSA algorithms are either improved or replaced by Gimel ID. GAuthent suggests different approaches to use Gimel ID within the authentication protocol: To improve current RSA by integrating Gimel ID, to integrate it within existent quantum-resistant algorithms, to build a proprietary algorithm and/or multivariate schemes with it. Each of these approaches to GAuthent Can be combined with quantum-secure networks.

Status of This Memo

This is a Gimel Foundation Standards Track document.

This document is a product of the Gimel Foundation (GiFo). It represents the current consensus of the Gimel Foundation community. It has performed review and has been approved for publication.

Information about the status of this document, any errata, and how to provide feedback on it may be obtained at https://gimelfoundation.com or https://github.com/Gimel-Foundation.

Legal notice

Notational Conventions

The key words "Must", "Must Not", "Required", "Shall", "Shall Not", "Should", "Should Not", "Recommended", "May", and "Optional" in the following specification are to be interpreted as described in the Internet Engineering Taskforce`s (IETF) RFC 2119.

Credits

We would like to express our sincere gratitude for the invaluable support provided by Stephan Brühl and Eicke Schütze. Their expertise and commitment have greatly contributed to the quality of this document. We truly appreciate their dedication and collaborative spirit throughout the development process.

Table of Contents

***

1. Scope

GAuthent describes how to secure quantum-resistant authentication by using DNA based biometrics, i.e., with Gimel ID.

GAuthent builds on the following standards as building blocks, thus is connected to these standards but adds distinguished complements in terms of its proprietary content, value-added, IP rights and overall license conditions. Building blocks include:

- RSA algorithms provided through a permissive open-source licence,
- Quantum-resistant algorithms provided through a permissive open-source licence,
- Quantum-secure network solutions provided through a permissive open-source licence,
- Gimel ID 0.1 (GiFo-RFC0190) and/or
- Gimel ID 1.0 (GiFo-RFC0200),

and again, the building blocks of Gimel ID 1.0 (GiFo-RFC0200), if applicable:

- OAuth or its alternatives, including but not limited to IETF`s
  - RFC 6749
  - RFC 7636
  - Best Practices for OAuth 2.0 Security
- OpenID Connect or its alternatives, including but not limited to
  - OpenID Connect Discovery 1.0
  - OpenID Connect Dynamic Client Registration
  - OpenID Connect Session Management of the OpenID Foundation

2. Limitations on the right to make derivative works (Exclusions)

GAuthent is freely available as an open-source solution based on Apache 2.0 with the following Exclusions. Users of GAuthent Must Not – whether directly or indirectly – integrate GAuthent with:

- The use of the authorization protocols for authorizing artificial intelligence such as digital agents and/or robots,
  (e.g., GiFo-RFC0110, -0111 and/or -0115),
- The use of AI to detect and/or manage risks associated with the identity and its use (e.g., DefconG),
- The use of web3 technology to store, run and/or share the identity on a blockchain.

These Exclusions are excluded from the GAuthent open-source standard. Users Must Not use, integrate or add all or some of these Exclusions in any form to the GAuthent standard without a separate licensed permission in writing. Users Must exclude these Exclusions from any implementation of GAuthent unless licensed separately. Gimel Technologies GmbH offers separate solutions for this purpose, e.g. in terms of the GAuthent+ feature. These separate solutions are being protected by copyright and patent law.

In line with GiFo-RFC0090, Gimel Foundation May revoke at its soles discretion the rights and licenses granted to a user with respect to Contributions and Documents, if the user does not use Contributions and Documents in line with Legal Provisions of Gimel Foundation.

3. Glossary of key terms and expressions associated with GAuthent

Essential nomenclature used in this document is defined as follows:

OAuth: An open-standard authorisation protocol used to grant third-party applications access to user data without exposing credentials; governed by IETF RFC 6749 and RFC 7636, not limited to it, with various security best practices.

OpenID Connect: An authentication protocol based on OAuth 2.0, enabling secure user identity verification; encompasses standards such as Discovery, Dynamic Client Registration, and Session Management.

GAuthent: An open-source and post-quantum authentication solution provided under the Apache 2.0 licence, with specific Exclusions, which are not open but refer to proprietary licensing.

GiFo-RFC Series: A set of reference documents of the Gimel Foundation governing authorisation protocols and legal frameworks, including GiFo-RFC0090 (revocation of rights) and GiFo-RFC0110, -0111, -0115 (AI authorisation).

Quantum-Resistant Algorithms (PQC): Cryptographic algorithms designed to remain secure against attacks by quantum computers, including lattice-based, hash-based, code-based, and multivariate polynomial algorithms.

Quantum-Secure Networks (QKD): Networks leveraging quantum key distribution to ensure communication security by detecting interception attempts.

Gimel ID: A unique identifier used to enhance security within cryptographic approaches, but not limited to it, including RSA improvements, pseudorandom number generation, and as a marker in quantum-resistant algorithms.

DNA Biometrics: The use of genetic markers for secure authentication, directly (without hashing) or indirectly (hash-based, like Gimel ID) integrated into cryptographic key generation for added protection.

Multivariate Schemes: Advanced cryptographic constructs utilising multiple variables, designed to withstand quantum threats.

Blockchain/Web3: Decentralised technologies enabling identity storage, sharing, and management on distributed ledgers; excluded from GAuthent unless separately licenced.

This glossary collates the principal terminology and expressions central to the document, without being comprehensive, providing succinct definitions for ease of reference and clarity.

4. Approaches to leverage Gimel ID for quantum-resistant authentication

There are two principal approaches to achieving quantum resistance in digital security:

a) **Quantum-secure networks**: These use the principles of quantum physics, such as quantum key distribution (QKD), to create secure communication channels. Any attempt to intercept the key alters its state, ensuring immediate detection and protection against eavesdropping.

b) **Quantum-resistant algorithms**: Also known as post-quantum cryptography, these are cryptographic algorithms designed to be secure against attacks by quantum computers.

With respect to point b), quantum-resistant algorithms, there are basically four cryptographic approaches to create quantum-resistant algorithms as well as private keys associated, while leveraging secure DNA biometrics:

i. The first approach, **leveraging the RSA mechanism but improving it with the Gimel ID**, could benefit from the established security of RSA.

ii. The second approach is focusing on **deriving quantum-resistant cryptography directly from the Gimel ID** itself by leveraging a cryptographically secure pseudorandom number generator.

iii. The third approach, **leveraging other quantum-resistant algorithms and enriching it with Gimel ID** as a unique marker. These algorithms include lattice-based, hash-based, code-based, and multivariate polynomial algorithms, providing robust security even in a future with quantum computing.

iv. While the approaches i. – iii. focus on quantum-resistant primitives, these could be extended to include **multivariate schemes** within the spectrum of "advanced cryptographic constructs designed to withstand quantum threats.

Each of these cryptographic approaches Can be combined with a quantum-secure network.

5. Improving RSA with Gimel ID

To make RSA algorithms quantum-resistant while integrating a DNA-based identity like Gimel ID, the process begins by addressing the fundamental vulnerability of RSA to quantum attacks. The traditional RSA relies on the difficulty of factoring large numbers, a task that quantum computers can potentially perform with ease, thereby compromising its security. To counteract this, one approach is to enhance the RSA protocol by embedding the Gimel ID - a unique biometric identifier derived from an individual’s DNA - into the key generation and authentication steps. This means that, in addition to the usual mathematical complexity, the algorithm now requires a matching biological signature, making it significantly harder for quantum adversaries to forge or compromise private keys.

The integration operates in several layers. During key generation, the user's Gimel ID is cryptographically bound to their RSA key pair, such that the private key is not just mathematically derived but also linked to the individual's DNA profile. This binding can be achieved using secure hash functions or other cryptographic primitives that mix the Gimel ID data with the key material. The result is a hybrid key that cannot be reconstructed or used without access to the correct DNA profile or Gimel ID components associated. In authentication scenarios, the system verifies both the cryptographic signature and the biometric signature, ensuring that even if quantum algorithms break the mathematical barriers, the biological component remains a robust line of defence.

Additionally, to further harden the scheme against quantum threats, the enriched RSA algorithm can be combined with post-quantum cryptographic techniques. For instance, lattice-based encryption or hash-based signatures may be layered on top of the RSA-Gimel ID construct, creating a multi-factor, multi-layered security protocol. This approach not only leverages the established reliability of RSA but also future-proofs the system against emerging quantum attacks, all while ensuring that user identities are uniquely and securely tied to their biological signatures. Such a hybrid solution represents a promising direction for quantum-resistant authentication in the age of advanced computing and biometric technology. It builds on current safeguards and implementation of RSA.

6. CSPRNG using Gimel ID

One way to approach creating a strong private key from the Gimel ID would be to use a cryptographically secure pseudorandom number generator, often called a CSPRNG:

Combining CSPRNG with the Gimel ID offers a highly robust approach to generating private keys that are resistant to both traditional and quantum attacks. The process begins by using the Gimel ID - a unique, immutable identifier derived from an individual's DNA profile - as the core seed input for the CSPRNG. This ensures that the private key is intrinsically linked to a biological trait that is virtually impossible to replicate or forge. To further strengthen the process, additional sources of entropy, such as system-level randomness or environmental noise, can be mixed with the Gimel ID. This fusion of unique biometric and unpredictable random data makes the resulting seed exceptionally secure and individualised.

Once the seed is established, the CSPRNG uses it to generate a sequence of numbers that are both unpredictable and statistically random. The "cryptographically secure" aspect is crucial: even if an attacker were to know the underlying algorithm, they would not be able to predict or reconstruct the output sequence without access to the exact seed - in this case, the Gimel ID component combined with the auxiliary randomness. The output from the CSPRNG can be tailored in length and format to suit the requirements of various cryptographic protocols, ensuring that the resulting private key is sufficiently long and complex to resist brute-force and quantum attacks alike.

To ensure maximum security, the process can be designed so that the Gimel ID and other random inputs are never stored or transmitted in their raw form. Instead, a secure hash function or similar cryptographic primitive can be used to blend these inputs before they reach the CSPRNG, thereby preventing potential leakage of sensitive biometric information. The derived private key is thus not only unique to the individual but also shielded from direct exposure of the underlying DNA-based identifier (while no DNA data are leaving the lab anyway, in line with the Gimel ID protocol). This layered

approach significantly reduces the risk of key compromise, even in the face of advanced computing techniques.

Finally, the integration of a CSPRNG with the Gimel ID aligns well with post-quantum cryptographic strategies. It ensures that the private key generation process remains secure even as quantum computers evolve, since the unpredictability and uniqueness of the seed make it infeasible for quantum algorithms to reconstruct or guess the key. The result is a security model where authentication and encryption are anchored in both the mathematical strength of cryptographic algorithms and the biological singularity of the user, providing a forward-looking defence against emerging threats in the digital landscape.

7. Leveraging Gimel ID for quantum-resistant cryptography beyond CSPRNG

Beyond the use of CSPRNGs, there are several other promising approaches to developing quantum-resistant cryptography based on the Gimel ID. These methods leverage the unique, immutable nature of DNA-derived identifiers while incorporating advanced cryptographic constructs designed to withstand quantum threats:

- **Gimel ID-Based Lattice Cryptography:** Lattice-based cryptography is widely regarded as a strong candidate for post-quantum security. By embedding the Gimel ID as a parameter or seed in lattice-based encryption schemes (such as Learning With Errors or Ring-LWE), the resulting cryptographic keys are directly tied to the user's DNA profile. This creates an additional barrier to attack, as adversaries would need both quantum computational resources as well as access to the specific biometric data including hashing algorithms and/or hashes associated. Moreover, the inherent complexity of lattice problems is believed to be resistant to quantum algorithms, providing robust protection.
- **Hash-Based Signature Schemes with Gimel ID Binding:** Hash-based signature algorithms, such as XMSS or SPHINCS+, are designed to be secure against quantum attacks. These algorithms can be further strengthened by binding the private signature seeds to the Gimel ID (which again is built on quantum-resistant hashing) via secure hash functions. This ensures that each signature generated is not only quantum-resistant by design but also uniquely traceable to a specific individual's DNA-derived identifier, preventing impersonation and unauthorised use. As Gimel ID itself is a kind of super-hash, this approach leverages further hashing for authentication in terms a hashing of a higher order.
- **Code-Based Cryptography with Gimel ID Anchoring:** Code-based cryptographic systems, such as those based on the McEliece cryptosystem, offer another avenue for quantum-resistant encryption. By using the Gimel ID to generate or randomise the error-correcting codes at the heart of these systems, it becomes possible to create encryption keys that are both mathematically and

biologically unique. This dual-layer approach makes it extremely difficult for attackers, even with quantum capabilities, to reconstruct or predict the private keys without access to the individual's DNA profile or the Gimel ID layers based on it.

- **Physical Unclonable Functions (PUFs) Derived from Gimel ID:** Physical Unclonable Functions are hardware-based security primitives that exploit inherent manufacturing variations to create unique, unclonable responses to challenges. In the context of Gimel ID, PUFs could be constructed from DNA-based physical characteristics (Gimel ID components), generating cryptographic secrets that are both physically and biologically impossible to duplicate. These secrets could serve as the basis for key generation, authentication, or secure enclave creation, providing a hardware-anchored, quantum-resistant solution.
- **Multi-Factor Post-Quantum Protocols Integrating Gimel ID:** By combining Gimel ID-derived factors with other post-quantum authentication mechanisms - such as interactive zero-knowledge proofs, multi-party computation, or isogeny-based cryptography - systems can create composite protocols. These protocols would require both biometric-related proof and a quantum-resistant mathematical challenge to be satisfied, substantially increasing security and resilience against both present and future threats.
- **Gimel ID-Based Secret Sharing and Threshold Cryptography:** Secret sharing schemes, where a cryptographic secret is divided into multiple parts, can be enhanced by using the Gimel ID as one or more of the shares. Only when the correct Gimel ID-based share is presented, in conjunction with other factors, can the private key or sensitive data be reconstructed. This method ensures that the key material is never stored or transmitted in entirety, and quantum adversaries would face the dual challenge of breaking the secret sharing scheme and acquiring the correct biologically based component.

Each of these approaches capitalises on the unique, non-replicable properties of DNA-derived identifiers while integrating cryptographic primitives that are either inherently quantum-resistant or can be adapted for post-quantum security. They provide a spectrum of options for building robust, future-proof authentication and encryption systems where the Gimel ID is not just a source of entropy, but a foundational element in the cryptographic design.

8. Multivariate schemes for quantum-resistance based on Gimel ID

Multivariate cryptography employs systems of polynomial equations with multiple variables, creating encryption and signature schemes whose mathematical hardness is believed to withstand quantum attacks. In the context of Gimel ID-based quantum-resistant cryptography, the Gimel ID - being derived from DNA - could serve as a unique secret or parameter for generating the core multivariate equations. This fusion would

ensure that cryptographic keys and signatures are not only quantum-resistant but also inherently tied to an individual's biological identity. The complexity of solving these multivariate equations, especially when randomised or seeded by a Gimel ID (or its components/layers), adds an extra layer of security, as attackers would require both quantum computational power and access to the specific DNA-derived identifier. Such schemes could be used for authentication, digital signatures, or secure key exchange, with each cryptographic operation uniquely bound to the individual. By integrating Gimel ID, multivariate cryptography can provide robust, personalised resistance against quantum adversaries. This approach expands the spectrum of advanced cryptographic constructs, ensuring future-proof security rooted in both mathematical and biological uniqueness. As multivariate schemes are well-studied in post-quantum research, their adaptation to Gimel ID-based systems aligns with the broader goal of leveraging non-replicable biometric data for next-generation cryptography.

While several embodiments have been described in this document, it is understood that various modifications May be made for implementing it without departing from the spirit and scope of GAuthent. Accordingly, alternative implementations also fall within the scope of GAuthent.

* * *