Gimel Foundation

Gimel Foundation gGmbH i.G.
GiFo-Request for Comments: 0200
Obsoletes: -
Category: Standards Track
ISBN: 978-3-00-085202-2

Dr. Goetz G. Wehberg
Digital Supply Institute
30. November 2025

The Gimel ID 1.0 Identity Framework

Abstract

The Gimel ID 1.0 identity framework (Gimel ID) provides a globally unique identity. This means that it enables people to accurately verify their identity among the eight billion people on Earth and reliably authenticate themselves to a relying party. To do this, Gimel ID performs a proof of personhood. Since an identity is only as secure as the biometrics behind it, Gimel ID uses an individual's DNA data while ensuring that no such data leaves the laboratory and maintaining data privacy.

As current biometric identity verification is comparatively weak, Gimel ID helps to secure digital identities, such as those in the EUDI wallet, thus preventing such weak biometrics from being exploited. Gimel ID can distinguish humans from artificial intelligence (AI), including digital agents and humanoid robots. This helps to prevent deep fakes and scams. In view of the future use of quantum computing, Gimel ID provides the necessary security for authentication.

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.

Table of Contents

***

1. Scope

Gimel ID concerns the field of human identification and the verification of such identities, the enablement of authentication and services associated, like selected trust services.

Gimel ID 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:

- 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

Gimel ID provides a next level of assurance for identity verification, which can, e.g., add to or build on the Level of Assurance 4 of the Authentication Context Class Reference by OpenID Connect (ACR_LOA_4) in terms of a new level 5 (i.e., ACR_LOA_5).

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

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

- The use of the GAuth protocol (see GiFo-RFC0110, -0111 and/or -0115),
- The use of AI to detect and/or manage risks associated with the identity,
- The use of web3 technology to store and/or share the identity on a blockchain.

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

3. Nomenclature

In the following some definitions of terms are being provided, regarding the Gimel ID protocol:

Genome: The complete set of genetic information in an organism.

DNA sample data set: Genetic information of the individual as a sequence of deoxyribonucleic acid (DNA) in the genetic information of the organism, i.e., of those genome segments (known as loci) that are required to determine the genetic fingerprint. This genetic information is based on a selected cell sample from a human being, e.g. skin, blood or saliva. In addition, the DNA sample data can be attached to personal data, a so-called 'temporary identifier' as a label (i.e. a random or pseudonymised identifier assigned by the laboratory, for example) or alternative data, because genetic information is processed pseudonymously in the testing laboratory.

Genetic fingerprint: Genetic information about the human in terms of the sequence of characteristic markers in the genetic information (, which can be attached to personal data, the so-called 'temporary identifier').

Panel: Definition of a specific set of DNA markers or locations on the chromosomes that are analysed for identification purposes, e.g., short tandem repeats (STR) and/or single nucleotide polymorphism (SNP). Each marker exhibits variation, allowing to differentiate between individuals (thus, to statistically discriminate the individual).

Deep sequencing: Deep sequencing, also known as next-generation sequencing (NGS) or massively parallel sequencing, is a technology that allows for the high-throughput and rapid sequencing of large amounts of DNA. Unlike older methods, deep sequencing sequences many DNA simultaneously in a short time. The key to its power is coverage, the number of times a specific region is sequenced, which can be hundreds or thousands of times to ensure accuracy.

Hash value: Sequence of numbers and/or letters formed by a mathematical hashing process from the genetic fingerprint and, if applicable, additional data. The hashing algorithm makes it possible to always reproduce the exact same hash value during hashing. Hashing can be performed at several levels, i.e., hashing of the genetic fingerprint, and – based on this - hashing of the hash value of the genetic fingerprint together with the hash value of personal data combined with a so-called 'salt' to form a 'super-hash'.

Unique identity identifier: a sequence of letters and/or numbers that uniquely identifies a person in digital transactions, e.g., in terms of a hash value or 'super hash'.

Proof of personhood: Verification of an identity of a human, i.e., confirming that someone is who they claim to be, among eight billion humans on Earth based on a

unique identity identifier, thus building on an accurate and reliable identification method.

Global identity: Unique identity identifier that meets the requirements of a proof of personhood.

Authentication: Granting access to a system or resource or accepting someone`s behaviour or action, respectively, based on a verified identification.

MFA: Multi-factor authentication is adding an extra step to the authentication process, requiring multiple pieces of evidence to authenticate, like a password, passkey or a code sent to your phone.

Q/eAA: (Qualified) electronic attestation of attributes, based on eIDAS 2.0 regulation of the European Union for the so called EUDI wallet.

4. Why Gimel ID

Are you really you? This question about the personal identity of a human determines their privacy, integrity and authenticity. It encompasses the verification of who someone is, the protection of their information, and the assurance that they are who they claim to be. The verification of someone`s identity has become more important due to the following key drivers, in particular:

- **Digitalization**: The growth of the volume of digital transactions as well as of the number of digital wallets being used, such as the EUDI wallet, are fostering the use of digital identities. Therefore, we must prevent its biometrics from being exploited.
- **Artificial intelligence**: With AI becoming more powerful and acting autonomously, we must be able to distinguish humans from AI, including digital agents and humanoid robots. This helps to prevent fake identities, deep fakes and scams. A secure identity system must build on robust biometrics that are resistant to forgery.
- **Quantum Computing**: Current authentication systems (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 biometrics can help to fix this.

There are certainly more than these three drivers highlighting the importance of identity verification. The Common European Asylum System (CEAS) for example, is leveraging on human biometrics to manage applications and steer immigration. The EU is seeking for next-level biometrics to facilitate a seamless CEAS procedure. In this publication, though, we would like to focus on the key technological drivers, rather than political ones.

Given that an identity is only as secure as the biometrics behind it, let`s have a closer look at identity biometrics:

Previous identification systems for people are generally based on identity documents issued by authorities, which, in addition to name and address, may also include biometric features such as gender, height, eye colour, hair colour, fingerprints and a biometric passport photo. This makes it possible to identify a person with a high degree of probability. The biometrics used today, however, are neither forgery-proof nor accurate, nor are they suitable for every user. The false negative rate of facial recognition and fingerprinting does not allow for reliable identification of a person among the approximately eight billion people on our planet, in terms of a global identity. In addition, there are people who, for example, due to hard physical labour, no longer have readable fingerprints. Last not least, the way biometric data are handled is not necessarily in line with modern identity templates of regulators.

One approach trying to solve some of these problems has been outlined by World (in the WorldCoin Network white paper). It aims to enable a ‘proof of human’ based on biometric measurement of the iris in a person's eye. Although iris recognition is significantly more accurate than fingerprint or facial recognition, it can still be easily faked. For example, hackers from the Chaos Computer Club managed to fool an iris scanner using a 3D scanner and infrared ink. Furthermore, iris recognition is not suitable as proof of identity for every user, as not everyone has a healthy iris. Last not least, World seems to compete with national identities being issued by national authorities, rather than supporting it.

An even more promising approach to identity biometrics is the use of DNA data. DNA data can enable a high accuracy, forgery-resistant and inclusive way to verifying a personal identity. However, there is no one DNA-based identity. The use of a DNA-based identity is known from Forensics.

Protocols being used in Forensics refer to allele, which can be considered as the standard in Forensics. It builds on analysing the sizes of amplified fragments. Such Forensics protocols typically provide a reliability of 99.5 percent. In well-established laboratories with proper protocols and extremely qualified personnel it can even exceed 99.9 percent. While in theory the discriminating power of selected kits can even be higher, the practice is what counts. These protocols based on allele tables and fragment lengths are good enough for identifying a criminal among a set of suspects. Criminologists typically use DNA data to narrow down the circle of suspects and/or use DNA data as additional evidence. The Forensics approach, however, is not sufficient for performing proofs of personhood among all humans on Earth, and generating a global identity based on it.

Previous attempts to use Forensics protocols for the creation of a global identity, therefore, have failed. A “copy-paste” approach does not consider the specific needs of

such global identity. Some of these attempts even use DNA data and allele tables outside the lab without encryption and thus fail to meet requirements of modern identity templates and data privacy.

Gimel ID goes beyond Forensics practices. It facilitates a real proof of personhood and provides a global identity. Let`s have a closer look what Gimel ID is and how it works.

5. What Gimel ID is

Gimel ID is a global identity based on DNA analyses. Its DNA panel builds on a definition of a specific set of DNA markers that are analysed with respect to its sequencing data for identification purposes. The panel Should be customized for that purpose. As Gimel ID uses hashes as unique identifiers, no DNA data are leaving the lab. The use of sequencing data facilitates an accuracy which meets the requirements of a proof of personhood and a global identity for individuals.

Gimel ID is adding to national identities, complementing and “upgrading” its biometrics. By adding a DNA-based identifier, it enriches national identities towards a higher level of security beyond high assurance. In other words, Gimel ID is adding a next-level security protocol to national identities (like eID in Germany) and backs them up. It is neither replacing nor questioning national identities issued by authorities.

Within the context of the EUDI wallet of the European Union (eIDAS 2.0), the Gimel ID can be introduced as electronic attestation of attributes (eAA) for selected organizations, administrations and corporates as B2B functionality. Many organizations like critical infrastructures and its suppliers are supposed to be eIDAS 2.0 compliant. Gimel ID can also be used among all EU citizens based on a qualified electronic attestation of attributes basis (QeAA), given the necessary alignment among EU member states.

6. How Gimel ID works

Gimel ID builds on hash values being processed in a software layer performing a deduplication step as proof of personhood. This makes it possible to determine whether a global identity has already been created with the available genetic information. It prevents also a person from having multiple global identities.

Since hash values change because of minimal variation, the genetic fingerprint data Must be both very accurate and unique to make sure the Gimel ID can be reproduced. To achieve the required level of accuracy, e.g., Gimel ID Should use more than one genetic sample, standardized DNA extraction and processing methods as well as deep sequencing. Uniqueness determines how frequently a defined DNA profile occurs. The quality of the ideally customized panel in terms of its discriminating power, therefore, is

being considered by a proper selection of highly stable markers. Last not least, Gimel ID Must apply a consistently used hashing algorithm to the generated DNA profile or genetic fingerprint.

The following Figure shows the abstract protocol flow of the Gimel ID (type of data sets in italic):

(1)	Determining the human individual who must be identified	*Genome, personal data (based on national identity)*
(2)	Taking the DNA sample at the sample collection site (e.g., company doctor`s office, hospital)	*DNA sample, label of the sample / personal identifier*
(3)	Sequencing the DNA sample data in the lab (e.g., targeted NGS)	*Genetic fingerprint, label / personal identifier*
(4)	Hashing of genetic fingerprint by identification device in the lab	*Genetic fingerprint hash, label / personal identifier hash*
(5)	Transferring of hashes to software layer / platform (e.g. cloud) and performing the deduplication check (hash collision test)	*Genetic fingerprint hash, label / personal identifier hash*
(6)	Salting of personal identifier in the software layer / platform	*Genetic fingerprint hash, personal data plus salt*
(7)	Hashing of personal-data-plus-salt in the software layer / platform	*Genetic fingerprint hash, personal-data-plus-salt hash*
(8)	Hashing of personal-data-plus-salt hash together with genetic fingerprint hash in the software layer / platform	*Super hash / unique identity identifier*
(9)	Defining a user address for the unique identity identifier	*Global identity*
(10)	Storing the global identity (e.g., in the wallet upgrading the national identity)	*Global identity*
(11)	Sharing the global identity (e.g. zero-knowledge-proof) for authentication purposes	*Public key of global identity / selected attributes*

Figure 1: Abstract protocol flow of Gimel ID

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

7. Benefits

The Gimel ID protocol provides several key benefits, which can be summarized as follows:

Global identity: Gimel ID as a global identity allows an individual to be uniquely identified among eight billion people on Earth (‘proof of personhood’).

Forgery-proof: As current biometric identity verification is comparatively weak, Gimel ID helps to secure digital identities, such as those in the EUDI wallet, thus preventing such weak biometrics from being exploited. Gimel ID helps to distinguish humans from AI, including digital agents and humanoid robots. This helps to prevent deep fakes as well as scams and defend against other threat vectors.

Quantum resistance: In view of the future use of quantum computing, Gimel ID provides a higher security for authentication, beyond current standards of high assurance. In the era of quantum computing, a DNA-based and therefore 100% unique identification solution is necessary. Of course, the hashing algorithm being used in the Gimel ID protocol Should be quantum-resistant itself.

Data privacy: Gimel ID makes sure that no personal genetic information is uploaded to outside or leaves the DNA testing laboratory, but only hash values – which do not allow any conclusions to be drawn about the underlying genetic information of a living being.

Compliance: Gimel ID meets the requirements of modern identity templates of regulators as well as safeguards associated, like eIDAS 2.0 (e.g., ZKP, Unlinkability, etc.).

Compounding: Gimel ID builds on current standards like OAuth and OpenID Connect, so that it is a compounding development of existing protocols and architectures, not “going back to square one”. It builds on the strengths of existing open-source solutions, complementing it rather than competing. Same applies for national identities being issued by regulators, where Gimel ID backs-up and supports with secure biometrics, rather than competing and replacing.

Upgrade: The - within this specification - out-scoped features of Gimel ID (Exclusions) can be upgrading the Gimel ID protocol and even increase security based on a separate license agreement.

Disclaimer: ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN “AS IS” BASIS AND THE CONTRIBUTOR, THE ORGANIZATION THEY REPRESENT OR ARE SPONSORED BY (IF ANY), THE GIMEL FOUNDATION, AND ANY APPLICABLE MANAGERS OF ALTERNATE DOCUMENT STREAMS, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

* * *