ElectronicID Specification Document (v1.0)

© Akshay Sharma
Authored on 07/26/2015
Last Revised 9/4/2015 9:49:22 AM

ElectronicID Platform: www.electronicid.org

Abstract

This specification defines an electronic identification system: the ElectronicID (e-ID) Platform, the self-identification platform of the web. A system capable of creation, storage and retrieval of digital identities has been defined. In addition to these operations, the system supports an endorsement feature wherein one digital identity holder can 'endorse' another one to create a "web of trust". The specification also defines the possible conflicts that may arise within the system and methods to deal with them.

The goal of the system is to establish an online identity system based on "web of trust" which can eventually complement, if not replace, the existing, more oppressive, government-powered identification systems and infrastructure such as ID cards, birth certificates, driver's licenses, etc. as well as establish a reliable yet non-oppressive digital identity system, powered by the people.

Terminology

This specification refers to both generic terms as well as branded terms in context of the system. The branded terms apply specifically to ElectronicID Platform and its components. The table below maps each generic term to its branded counterpart being used across the ElectronicID Platform.

Generic Term(s)	Branded Term(s)
Digital identity; profile	e-ID; e-ID account; e-ID profile; ElectronicID
System	ElectronicID Platform
Trust score	TrustScore™
Relationships; network	Endorsements

(Multiple) Verified Sources	Verified sources; verification of ownership of assets
System website; domain name	electronicid.org; https://electronicid.org/
Time; trust comes with time	Trust with Time™ principle

Purpose

The purpose of the document is to define the system specification of the platform as well as outline the purpose of the platform in the form of a problem statement.

Problem Statement

Even as of 2015, the identity infrastructure across the world is ineffective, oppressive and outdated and not suitable for a digital age, since it is primarily based on the paper age. It is possible to obtain either counterfeited versions of existing forms of identification documents (IDs) - including State IDs, birth certificates, drivers licenses, or to obtain legitimate IDs from the issuing agency itself (such as a government office, bureau of motor vehicles, etc.) based on fake proof documents (such as forged birth certificates, utility bills, etc.). And it is yet possible to obtain legitimate IDs from official issuing agencies based on real proofs, such as a legitimate utility bill or birth certificates obtained from vital records office simply by (mis)using the information of another citizen.

All of these possibilities and recorded instances make paper documents of today, including IDs based on paper documents, largely ineffective. Ultimately, misrepresentation of identity or establishing dual identities is a problem that cannot be combatted via oppressive identity systems or paper documents. Proposals to create governmental, online national ID databases have been deemed too oppressive for the citizens.

It is possible to obtain both counterfeit and genuine IDs which are misrepresentation of one's identity through monetary means or through enough knowledge, or yet both, however, the only factor deterring an individual with malicious intents is time. Of course, it all starts with some initial amount of trust in the individual, but the longer an individual is *known* by another party, the more the individual can be trusted. For example, you might be obliged to call a stranger who approaches you and introduces themselves as John Eiffel born on January 28th 1970 as John, however, you may not 'trust' them with this information right away or trust them minimally. However, as time passes, by then you would have long *known* this person as John who celebrates his birthday every year on January 28th, which enhances your trust in him. This is simply the time factor governing your trust in or familiarity with that person. The designer(s) of ElectronicID Platform refer to it as the "Trust with Time" principle.

The second factor that governs the trustworthiness of an individual is their network of individuals who form a mutual relationship with the individual. For example, if John's father,

Sam, mother, Lisa, sister, Giselle and friends, Josh and Jill, know him by the name of John Eiffel born on January 28th 1970, then there is a *very* high probability that John is actually who he says he is and is born on that date.

The third factor, which further supplements the trustworthiness of an individual's identity is multiple sources where an individual's information can be corroborated. This could include their digital presence such as social media accounts, their website, and communication devices (such as a cell phone).

The pyramid of factors governing the **trustworthiness** of an individual's identity would therefore look like:

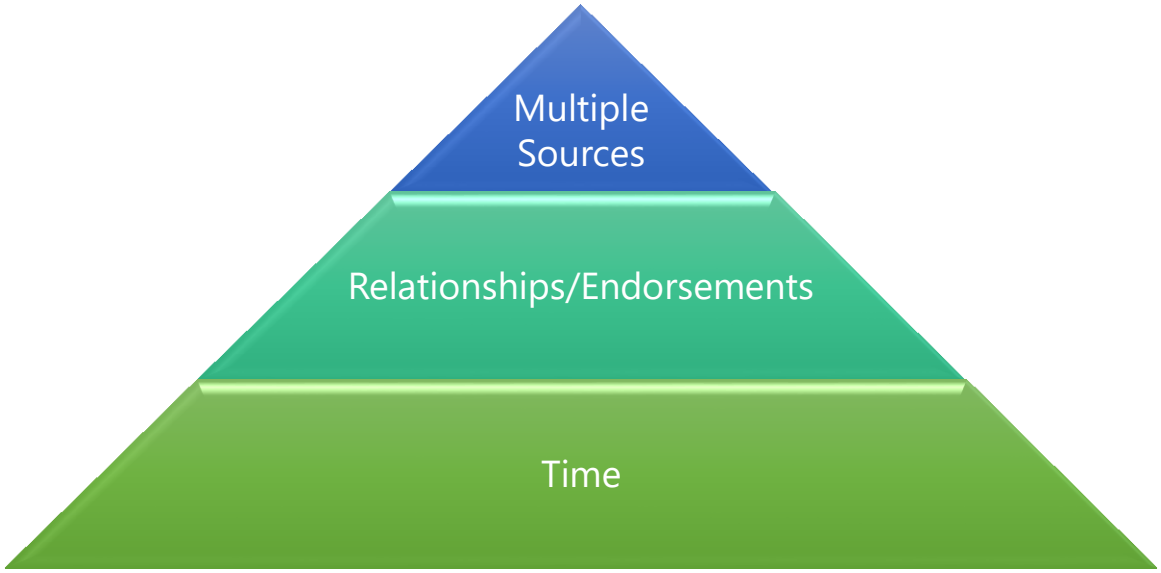

Figure 1: Factors governing the trustworthiness of an individual's identity.

Applying the Terminology to the System

When applied to an identity system capable of creation (issuance), storage and retrieval of identities, or more specifically, ElectronicID Platform, the factors can be implemented as follows:

1. **Time:** The longer the amount of time which has elapsed since the creation of a digital identity (profile of an individual on the ElectronicID Platform), the higher would be its trustworthiness, represented in the form of a numerical figure referred to, henceforth, as 'trust score'. A digital identity created by an individual one year ago would therefore, have a higher trust score than the one created a week ago.

2. **Endorsements:** A(n) (individual of the) digital identity bearing a decent amount of trust score, earned from time or otherwise may endorse another digital identity similar to a process of 'friending' or 'following' an individual on a social network. This action would boost the trust score of the endorsee (the digital identity which was just endorsed) as defined further in this document thereby enhancing the trustworthiness of the endorsee's identity. For example, John Eiffel's father, Sam Eiffel bearing a digital identity (more specifically, an e-ID created with ElectronicID Platform) may 'endorse' John Eiffel, given that Sam, as John's father, *knows* him by the name of John and his date of birth. This will help John boost his trust score and enhance the trustworthiness of his digital identity (e-ID).

3. **Multiple Verified Sources:** The multiple sources which can be referred for corroboration of information can include the individual's digital presence such as social media profiles, website, blogs, cell phone number, credit card information, and home address, however, the ownership of each of these resources must be verified prior to attributing it to the digital identity of an individual. For example, John may verify his cell phone number and 'link' it to his digital identity (e-ID profile) which would boost his trust score. He may also verify his home address listed on his digital identity by agreeing to receive a 'verification code' via snail mail and entering it on the system. His banking or financial information can also be cross-verified from the credit card processors. All of these actions would further boost John's trust score.

Defining Trustworthiness and Trust Score

Within the system, each of the stored digital identities have a trust score associated with them. A trust score is a non-negative, numerical representation of the trustworthiness of a digital identity. The trust score of a digital identity (an ElectronicID or, an e-ID) is a probabilistic measure which determines how 'trustworthy' or authentic a digital identity is. A digital identity with a higher trust score of, say 100, is more trustworthy than the one bearing the trust score of 25.

- All digital identities have a trust score.
- All newly created digital identities have a trust score of **0** at the time of their creation.
- Trust score is always a non-negative integer (whole number).
- Trust score can *never* exceed **730**.

Trust Score Arithmetic

What Boosts and Lowers Trust Score?

Increments in the amount of time elapsed since the creation of a digital identity, the number of endorsements on a digital identity and the number of verified sources (verified ownerships of web and electronic presence) attached to the digital identity lead to a boost of trust score of that digital identity. For example, a digital identity created right now would be initialized with a trust score of 0. After a month it would have a higher trust score and, yet even a higher score after receiving endorsements from bearers of other digital identities.

On the contrary, increments in number and frequency of changes made to the information listed on an individual's digital identity in a given period of time, lead to a drop in its trust score. For example, a name change made once on a digital identity in a given period of time (as defined further in the document) may lead to a slight drop in the trust score, however, another name change, although permitted by the system, made within that same given period of time may lead to a significant drop in the trust score of the digital identity, therefore affecting its trustworthiness.

Creation and Issuance of the ID

A digital identity might be created by an individual via a web (HTTP(S)) interface by navigating to the system's website (domain name) and following the instructions for signing up. The individual would be then asked upfront to provide the following information about them:

- Complete (first and last) name including any Middle Name or Initial(s)
- Any aliases
- E-mail address used to sign in to and manage the digital identity
- Password
- Date of Birth
- Gender
- Eye Color
- Height
- Accessibility Information (optional; recommended for individuals with special needs only)
- Complete Street Address (including any Apartment/Unit number)
- City of Residence
- State or Province, where applicable
- Country
- Postal Code or ZIP code

Note: A photograph of the individual would **not** be requested yet. A request for providing the photograph is made sometime after the digital identity is activated.

Upon entering and submitting the information, a unique identifier known as the digital identity serial number (e-ID serial number) would be generated and attached to the digital identity. An

e-mail containing a verification link and the serial number would also be dispatched to the e-mail address used for signing up.

The process of creating a digital identity is somewhat analogous to creating an account on any other website, such as an online forum, a shopping website, a social media platform, etc.

Activation

The digital identity created would only be activated for use when and if:

- The e-mail address is verified by the user by navigating to the verification link enclosed in the e-mail dispatched to the user.

- At least 7 days have elapsed since the e-mail address has been verified, for security purposes.

- The automated Identity Protection and Fraud Prevention System (IP/FPS) does not detect unusual traffic (multiple registrations from the same network), automated registrations by spam bots, and any information misuse originating from borrowing information from another digital identity pre-existing within the system. This step is to protect all of the parties associated with the information contained on the digital identities. All of the parties associated with the digital identities may or may not be the same entity (e.g. one user creating multiple digital identities for themselves vs. an identity thief creating an identity using information of another user pre-existing on the system). Details about the purpose and implementation of the Identity Protection and Fraud Prevention System (IP/FPS) are given further in the document.

Issuance

Provided that the above conditions are met, a digital identity is 'issued' to the user, in sense the serial number of the digital identity and the profile associated with it are activated for use and management by the user. Because of the digital nature of the product, the digital identity is an intangible asset that may be reached via its URL or the Serial Number. The identity can therefore be represented and stored as a QR code, URL, digitally, or have a paper representation such as a QR code contained within a graphical template printed on paper. The bearer of the digital identity (individual or user) may also simply choose to remember the Serial Number associated with the digital identity.

For users who would prefer carrying a physical "paper ID" card with them instead of remembering or storing Serial Numbers or URLs, the system provides a ready-to-print graphical template (image) resembling a conventional ID card which contains the user's information (name, date of birth, address, etc.) as well as a QR code containing the URL to the digital identity profile, for verification and authenticity purposes.

Integrity of Information

Due to the unreliability and questionable authenticity of paper ID documents and proofs alike, the system does not enforce integrity on its users by asking for paper documents of proofs, however the system does promote integrity of its users.

All of the digital identities created on the system are initialized with a trust score of 0, representing an initial and 'equal' amount of trustworthiness (i.e. no trust or minimal possible trust) in each of the newly created digital identities. This is analogous to a stranger approaching you and introducing themselves as John Eiffel born on January 28th 1970. You likely do not have the precise means or a social right, depending on the situation, to verify the stranger's identity so you *accept* what he tells you as authentic but *trust* him minimally. Trust is gained in you for John as you spend more time with him (over months, years, decades, …), meet the people in his network (who also claim to know him by the name of John Eiffel) and are able to corroborate this information from multiple sources, such as John Eiffel's digital presence.

Integrity and trustworthiness are likewise promoted on the system by factors like Time, Endorsements and Verified Multiple Sources.

Truthfulness of Information

Provision of truthful information is encouraged for the convenience of the users in near future and *required* where applicable by law, however, in practice, such conditions are often hard to enforce given the nature of web and of digital identities. The terms, conditions and policies governing the system therefore encourage the users to provide genuine information about themselves to the best of their knowledge but does not enforce this requirement by using means such as paper documents or by penalizing

users due to the factors (like Time, Endorsements and Verified Sources) already governing the integrity of the system. Misusing another individual's information for malicious actions is, however, forbidden. For example, John Eiffel who has the stage name (alias) of DJ Eiffel may choose to create a digital identity for DJ Eiffel in addition to John Eiffel's pre-existing identity and this action would be allowed. (Although the Identity Protection/Fraud Prevention System (IP/FPS) may initially flag the digital identity, the flag would later be lifted automatically once John Eiffel confirms that he is the one who also created DJ Eiffel's digital identity). However, John Eiffel cannot create a digital identity of an acquaintance by misusing their information with the purpose of impersonating them. This action would be forbidden both by the system's governing policies, the law in most jurisdictions and the automated IP/FPS may deny creation of such a digital identity.

Uniqueness

Given the oppressive nature of uniqueness and practical ineffectiveness in its enforcement, the system does not enforce uniqueness. That means, an individual, although encouraged to create and bear *only one* authentic digital identity for their convenience, are not restricted to do so. For example, a person with a name and a stage name may either create two separate digital identities or for their convenience, create a single digital identity listing all their aliases.

In practice, a user would practically be able to maintain only a limited number (1-2) of identities which *look* authentic (that is, have a high enough trust score) due to the requirements of establishing a trust score, which includes time.

Storage and Retrieval of Information

All of the digital identities are securely stored on the system's servers with retrieval of information available only over a secure (HTTPS) connection protected with SSL/TLS.

Verification of Digital Identity

A digital identity of a user, unlike a paper document (subject to forgery) may securely be retrieved and verified by a third party in one or more of the following ways:

- Navigating to the system's website (domain name) and entering the Serial Number (and other supplementary details, such as a PIN) associated with the digital identity to retrieve the record. In doing so and for decision-making purposes, all of the retrieved information along with the trust score must be noted by the third party.

- Navigating to the URL of the digital identity provided by the user to the third party. Although the URL may be disguised or masked with a URL shortened, it must be verified by the third party that the URL of the final destination page begins with the URL of the system's domain name (https://electronicid.org/). Any other URLs void the authenticity of the digital identity.

- Scanning the QR Code to navigate to the URL of the digital identity. The same rules given above apply to this step as well.

Dealing with Changes

Changes to a user's information over a course of life, and therefore, to their digital identity are inevitable. The system implements processes and procedures to deal with changes and for users to initiate and monitor those changes.

Depending on the governing policies and system configuration, changes to certain parts of user information by the user may or may not be permitted, may require the user to bear a minimum trust score, may affect (lower) the user's trust score or have certain restrictions associated with them, such as their frequency (number of changes which can be made in a given period of time) to promote integrity of the system and its users.

There are three categories of changes occurring on the system:

Type 1 — Permitted Types of Changes – Affecting the Trust Score

The system indefinitely allows the users to initiate changes to the following pieces of information on their digital identity, however, the trust score of the digital identity might be affected.

- Name Changes
    - These changes (whether first, middle or last) are permitted **once a year** without incurring any reduction to trust score.

    - Any subsequent changes made to this entry within the same period of time require a **minimum** trust score of **50** and will incur either **50** trust points or **25**% of the trust score, whichever higher and feasible.
    - These changes appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

- Height
    - These changes are permitted **once a year** without incurring any reduction to trust score.
    - Any subsequent changes made to this entry within the same period of time require a **minimum** trust score of **25** and will incur either **25** trust points or **10**% of the trust score, whichever higher and feasible.
    - These changes appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

- Photograph
    - These changes are permitted **once** every **6 months** without incurring any reduction to trust score.
    - Any subsequent changes made to this entry within the same period of time require a **minimum** trust score of **25** and will incur either **25** trust points or **10**% of the trust score, whichever higher and feasible.
    - Photo changes are **required** every **2 years**. Failure to make a photo change every 2 years causes a reduction in trust score by **-7 points** for every week the photo is not updated until either a total of **60** points have been deducted or trust score drops to **0**, whichever comes earlier.
    - These changes appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

- Accessibility Information (ISA Symbol)
    - These changes are permitted **once** every **3 months** without incurring any reduction to trust score.
    - Any subsequent changes made to this entry within the same period of time require a **minimum** trust score of **25** and will incur either **25** trust points or **10**% of the trust score, whichever higher and feasible.
    - These changes appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR

Code, etc.)

- Address
    - These changes are permitted **once** every **3 months** without incurring any reduction to trust score.
    - Any subsequent changes made to this entry within the same period of time require a **minimum** trust score of **45** and will incur either **45** trust points or **20**% of the trust score, whichever higher and feasible.
    - These changes appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

Type 2 — Permitted Types of Changes – Not Affecting the Trust Score

The system indefinitely allows the users to initiate changes to the following pieces of information on their digital identity without the trust score being affected by the frequency of the changes whatsoever. These changes are also not logged publicly on a digital identity for the third party to view.

- Password
    - These changes are permitted **indefinitely** without incurring any reduction to trust score.
    - These changes are private and **do not** appear in the publicly visible change log.

- Aliases
    - It is only allowed to **add** aliases. An alias once added cannot be removed.
    - A user may add up to **5** aliases to a digital identity without incurring any reduction to trust score.
    - These changes appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

- E-mail address changes, if applicable
    - These changes are permitted **indefinitely** without incurring any reduction to trust score.
    - These changes are private and **do not** appear in the publicly visible change log.

- PIN or QR Code reset requests

    - These changes are permitted **indefinitely** without incurring any reduction to trust score.
    - These changes are private and **do not** appear in the publicly visible change log.

- Deletion of the digital identity
    - These requests are permitted **indefinitely** without incurring any reduction to trust score.
    - These requests are private and **do not** appear in the publicly visible change log.
    - These requests are processed after a **30 day** grace period. Deletion requests may be canceled within the security grace period. After the grace period has elapsed, a deletion request will lead to a permanent, automatic deletion of the digital identity account.

Type 3 — Restricted Types of Changes

The system may not allow the users to initiate changes to the following pieces of information on their digital identity for security purposes:

- Date of Birth
    - These changes are permitted **once in a lifetime**, for correction purposes only. The correction itself requires a **minimum** trust score of **50** and will incur either **50** trust points or **25**% of the trust score, whichever higher and feasible
    - Corrections appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

- Eye Color
    - These changes are permitted **once in a lifetime**, for correction purposes only. The correction itself requires a **minimum** trust score of **25** and will incur either **25** trust points or **10**% of the trust score, whichever higher and feasible
    - Corrections appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

- Gender Identity
    - These changes are permitted **once in a lifetime**, for correction purposes only. The correction itself requires a **minimum** trust score of **40** and will incur either **40** trust points or **15**% of the trust score, whichever higher and feasible
    - Corrections appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

- Serial Number (unique string identifier) associated with a digital identity profile

- These changes are **not** permitted to be made by the user.
- These changes, when exceptionally made by the system administrator(s), *may* or *may not* appear in the change log, which is publicly visible to any third party having access to the user's digital identity (via URL, Serial Number, QR Code, etc.)

Change Security Period / Grace Period

Given the possibility of account compromises and unauthorized password changes with online accounts, most changes made to the information of the digital identity are not published instantly. Rather, to ensure both security of the digital identity and give user a chance to amend any accidental submissions, most changes are processed after a "grade period" (typically lasting from **72 hours** to **30 days**, depending on the change made) during which they may be canceled or reversed by the user. If the trust score is to be affected by the change, the effect will only take place (for example, deduction in trust score) after the grace period has passed and change has been processed.

For example, a change request submitted by the user to change their name which would cost the user about 70 trust points will only be processed automatically after **72 hours**. This change will neither be effective nor be publicly visible on the change log and nor lead to a reduction in the user's trust score until the 72 hour grace period has elapsed.

Certain changes, however, are instantaneous and exempt from grace period, for strengthening the security of the accounts. These include password changes and QR Code/PIN reset requests.

Requests to delete the digital identity profiles permanently are processed after a 30 day grace period during which such requests might be canceled by the user, if desirable. After the 30 day period has elapsed, the deletion of the digital identity would be permanent.

Identity Protection and Fraud Prevention System (IP/FPS)

Given the non-oppressive nature of the system and the ability for the users to self-identify themselves without providing any 'proofs' there remains a possibility of information misuse, automated requests to create digital identities and spam. Such suspicious activities are dealt with by the automated Identity Protection and Fraud Prevention System (IP/FPS), a suite of scripts running periodically on the system for its assurance.

Preventing Information Misuse

The primary purpose of the IP/FPS is to prevent an imposter (identity thief) to create a digital identity using the information of another user already possessing a digital identity on the

system. However, with this also comes a possibility that there exist multiple digital identities on the system, each with highly similar information which owned by the same user. For example, a user who goes by the name of John Eiffel also has a stage name, DJ Eiffel and chooses to create two digital identities for each of the personas.

The IP/FPS simply flags and temporarily blocks any newly created digital identity before it is activated (that is, within the 7-day security period prior to activation) in case its information is determined to be highly similar to an already existing digital identity on the system. The pre-existing user will then receive an e-mail notification enabling them to **block** this registration. The user, in such a scenario, has the following options:

- If the newly created digital identity profile has been created by the same user who has another, pre-existing identity on the system, that user may choose to safely ignore the notification and the new profile will be activated once the 7-day security period passes.

- If the user believes that the newly created digital identity is work of an identity thief or an imposter, they may follow the appropriate instructions to block the registration[+]. This will cause a system conflict which needs resolution, as explained further below within the document.

Conflict Management

There also remains a very small possibility that an imposter was able to create a digital identity based on another user's information *before* that user got a chance to create their digital identity within the system. In such a scenario, the user who now attempts to create their digital identity on the system will have their profile flagged, awaiting a response from the imposter to approve or deny the creation. In case, the request for that user to proceed with registration is blocked by the imposter (via the IP/FPS e-mail notification), the user would be able to appeal the action.

[+]The new user who created the digital identity which was flagged is allowed to appeal to the system administrator if their profile has been wrongfully terminated (blocked) by the action of a pre-existing user on the system. This will raise a **conflict** within the system as, the system, per se does not *know* which of the 2 or more digital identities with very similar information, created by 2 or more separate users are authentic, which further makes distinguishing between honest user and an imposter difficult. In this case, both (or all) parties may then be asked to verify their name, date of birth and address by endorsements, multiple sources including by snail-mail address verification, all of which will determine which of the profiles is authentic.

Endorsements

A digital identity (e-ID) holder may endorse another e-ID holder via endorsement, a process similar to mutually "friending" someone on a social media website.

In order for one digital identity holder (a) to endorse another (b), the digital identity (a) should have the following prerequisites:

- Bear a minimum trust score of at least **150.**
- Be at least **120 days** old.

The digital identity (a) may then be able to endorse up to, but no more than, **5** e-IDs in any given **30 day** period without incurring a penalty to its trust score. For every endorsement made after the 5th endorsement in any given 30 day period, a deduction of **20** points will apply to the trust score (however, the trust score may never drop below **0**).

Multiple Verified Sources

A digital identity holder may further boost their trust score by verifying ownership of an entity via one of the following methods:

- Linking one or more social networks to their digital identity. The ***oldest*** and most comprehensive social network account, with regards to matches of information between social network account and digital identity (e-ID), will be given the utmost priority and importance while calculating and boosting the trust score of the digital identity. The number of trust points added to the e-ID via this method *varies*. One social media account may only be linked to one e-ID account for security purposes.

- Verifying a valid phone number. This will add **50** points to the trust score. One phone number may only be linked to a maximum of **3** e-ID accounts for security purposes.

- Verifying a credit card number. This will add **250** points to the trust score. One credit card may only be linked to a maximum of **3** e-ID accounts for security purposes, assuming there is a possibility of 2 "authorized users" on the same card.

Workflow

Refer to the appropriate document presenting the workflow of the system.