DIACC Identity Networks Paper

Verified.Me by SecureKey Technologies Inc., Self-Assessment

This document is intended to be used by identity network providers that want to demonstrate how their solution fits into the framework and requirements as described in the “Making Sense of Identity Networks” whitepaper. This self-assessment is an informal way to illustrate the concepts discussed in the whitepaper and has been reviewed by Consult Hyperion to ensure it is objective, accurate, and aligns with the framework.

1. Introduction

Verified.Me is a service (live and in production as of May 1, 2019) offered by SecureKey Technologies Inc., in conjunction with a consortium of seven of Canada’s major financial institutions – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD.

Verified.Me is a privacy-respecting digital identity and attribute sharing network. The service simplifies identity verification processes by allowing individuals (subjects) to share identity and attribute information from trusted sources (including financial institutions, mobile operators, credit bureau, and government) with the services that they wish to access.

The network is based on permissioned distributed ledgers operated by the consortium. It is built using the IBM Blockchain Platform which is based on Linux Foundation’s open source Hyperledger Fabric and is aligning with W3C decentralized identity standards[1], to enable interoperability with other networks. SecureKey’s Triple Blind® approach means that no network participant alone, including SecureKey, can have a complete view of the user journey - the subject can't be tracked.

The service is free for consumers to use, either using their web browser, or by downloading the mobile app through the App Store (iOS) or Google Play (Android).

[1] W3C DID and Verifiable Credentials

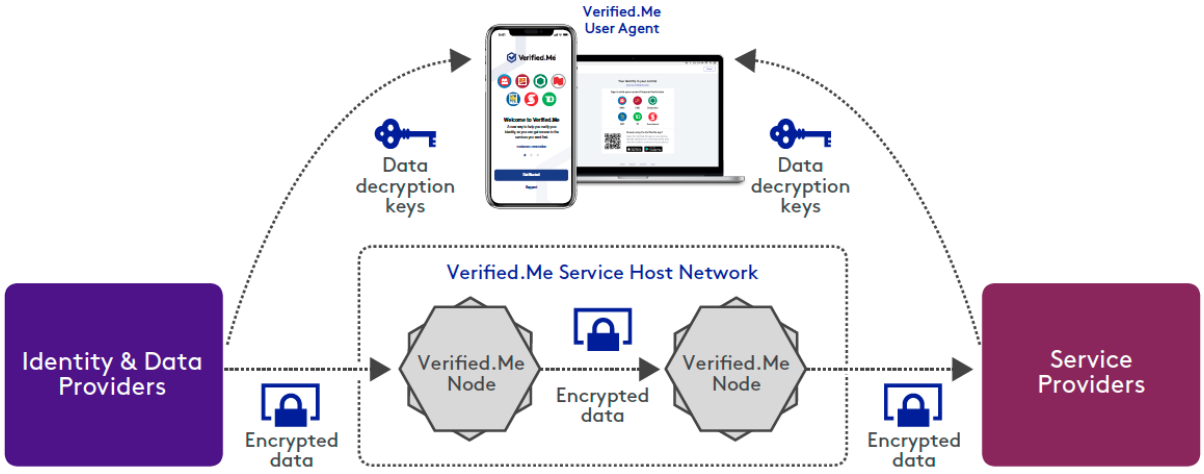

Figure 1 - Verified.Me context diagram

The above diagram illustrates the main components of the network as follows:

- **Identity & Data Providers (IDPs):** Eligible organizations in Canada that participate in Verified.Me that generate or hold certain information about the subject. Examples of IDPs include financial institutions, credit bureaus, telecommunications providers and other eligible trusted sources. This corresponds to the "Provider" role in the Identity Networks paper.
- **Relying Parties (RPs), or "Service Providers"**: These are eligible organizations in Canada that participate in Verified.Me that ask subjects to provide certain information through Verified.Me to facilitate interactions, for example, to help verify the subject's identity and/or eligibility for product or service offerings. This could, for example, enable the organization to identify the subject ahead of providing them with a service. This corresponds to the "Relying Party" role in the Identity Networks paper.
- **Financial Institution Identity & Data Providers (Financial Institutions, or "Service Hosts")**: Seven of Canada's major financial institutions that are responsible for authenticating subjects wishing to access the Verified.Me service, and also for hosting the core components of the Network. Service Hosts operate the decentralized nodes on the network, and also act as primary IDPs.
- **Verified.Me User Agent**: The tool provided to the subject to interact with the Verified.Me Network and consent to the sharing of their attributes via the network (via mobile app or web browser).

As illustrated above, the network architecture separates the transmission of encrypted identity and attribute data from the transmission of the associated decryption keys. This, combined with the management and administrative functions provided by the network, results in a service where:

- Service Providers can request the specific attribute they require (enabling the Service Providers to ask for only the information needed for the business purpose) and specify the type of Identity & Data Providers (IDPs) (e.g. from a financial institution) the data should be sourced from, in order to meet their requirements.
- Service Providers cannot, however, see which Identity & Data Provider (IDP) the identity and attribute came from but can be confident it came from the type of IDP requested, in line with the Triple Blind® philosophy of the service.

- Identity and attributes are encrypted end-to-end (from IDP to RP), providing no opportunity for the Verified.Me network to see the data itself, preventing data leakage (unintentional or otherwise).
- Subjects have full control over when their identity and attribute data is shared.

2. Identity Network Elements

For reference, this self-assessment section relates to Section 2 of the "Making Sense of Identity Networks" whitepaper. Included below is a description of how this identity network operates at each of the defined layers.

Connections

Definition
Before any communications can occur between parties in a network, there needs to be a means for parties to discover each other. In some cases, this may be automatic, as the parties wishing to share attributes may already be communicating about the service being requested, for example. In other cases, a directory or something equivalent, allows parties to find and connect with each other.
Self-Assessed Network Description:
Verified.Me is a permissioned network operated by SecureKey in conjunction with a consortium of financial institutions. Identity & Data Providers (i.e. IDPs) and Service Providers (i.e. Relying Parties) are eligible organizations in Canada that participate in Verified.Me, providing or consuming attributes pertaining to their existing customers (i.e. subjects). Examples of Identity & Data Providers include financial institutions, credit bureaus, telecommunications providers, governments and other eligible trusted sources. Examples of anticipated Service Providers include financial institutions, telecommunications service providers (e.g., for account opening and service or device eligibility), governments (for accessing online records or services) and online merchants (e.g., for account creation, faster checkout, age verification). To use Verified.Me, the subject is required to select a participating financial institution with whom they have an active and existing online banking relationship. Upon initial registration with Verified.Me, and prior to each subsequent use of the service, subjects are required to authenticate with their financial institution, using their login credentials with that organization, and leveraging the same financial grade systems and processes used by that organization for the course of its own business with the subject. Verified.Me users can discover Service Providers within the Verified.Me User Agent by selecting the "where I can use it" screen. They can also discover them through a variety of other forms of communication, such as the service provider's website, specific campaigns or promotions, through Verified.Me marketing channels and promotion activities operated by the network participants including from their financial institution.

Communications

Definition
The communications between parties carry the credentials that are to be shared. In some networks, this information is communicated directly from the provider to the relying party. In others, the information is only communicated indirectly, for example via a centrally operated hub or via the subject.
Self-Assessed Network Description:
The Verified.Me service is designed to allow credentials (containing attributes) to be sent from Identity & Data Providers to Service Providers (Relying Parties) confidentially. The credentials are encrypted end-to-end with dynamically generated cryptographic keys, which are communicated independent of the credential transmission. The architecture ensures that subjects have full control over which credentials are shared while maintaining the principle of Triple Blind®. All data is transmitted from the Identity & Data Providers to the Service Provider via the network and only after the subject provides consent. The network supports both real-time and subscription type consent models. In the real-time consent model, the Service Provider obtains the data in real-time following the subject's consent. In the subscription consent model, the subject can provide consent for the Service Provider to have access to a particular set of data for a defined period of time. Identity & Data Providers (IDPs) and Service Providers/Relying Parties (RPs) typically interact with the network via an adaptor that allows for seamless integration of participant systems using standards such as OpenID Connect. Within the network, distributed ledgers operated by SecureKey and permissioned consortium members provide necessary supporting functions such as discovery, routing, auditing, and billing.

Credentials

Definition
The information that is to be shared includes attributes together with the associated metadata that links those attributes to the subject and describes their provenance. The structure, content, and format of this information may vary between network types.
Self-Assessed Network Description:
Verified.Me supports open standards, to include W3C Verifiable Credentials, in the delivery of credentials containing attributes across the network. Verified.Me defines attribute bundles to address the needs of different use cases. For example, for a 'know your client' (KYC) identity check, the attribute bundle will include the attributes and metadata required to address the requirements of FINTRAC[2]. Attribute bundles are constantly being added to the Verified.Me service as use cases and requirements are identified. The service is flexible to support many different bundles going forward.

2 https://www.fintrac-canafe.gc.ca/intro-eng

The integrity of credentials and the attributes they contain is ensured by recording cryptographic transaction proofs onto the distributed ledgers operated by the permissioned consortium members.

All attributes are obtained from reputable Identity & Data Providers who are vetted by and contracted with SecureKey, and securely connected to the network.

Certifications

Definition
For a relying party to have confidence in the credentials received via an identity network, the relying party will need to be confident in the processes involved in the establishment of the credentials, and the attributes they contain, as well as in the secure transmission of it across the identity network. Often this will involve certification or audit of parties that are being relied upon to ensure the credentials and attributes are robust.
Self-Assessed Network Description:
Verified.Me enables the sharing of attributes from reputable and trusted sources that were securely onboarded to the network. They have contractually agreed to maintain specified levels of security and various industry-leading standards, including the stringent security measures and processes adopted by the participating financial institutions in support of their role as Service Hosts and IDPs. The process is driven by the Service Provider, who specifies what attribute(s) (or attribute bundle(s)) they need and the type of organisation(s) from where that data should be obtained in order to meet their requirements. The network then facilitates this. On receipt of attributes, the Service Provider is assured of the type of source (e.g. participating financial institution, mobile operator, credit bureau, government), and verifiable cryptographic processes ensure that the data was not modified in transit.

3. Requirements of an Identity Network

For reference, this self-assessment section relates to Section 4 and Section 5 of the "Making Sense of Identity Networks" whitepaper. Identity networks are more than technology. For multiple parties to collaborate in a safe, secure and predictable way there need to be clearly defined legal, business, and technical rules that determine how participants behave.

The requirements are grouped into two areas:

- **Governance**: setting and enforcing the rules of the identity network
- **Operation**: implementing and operating the rules of the identity network

Identity networks meet the requirements of the network users through a combination of:

- **Trust**: The network user needs to trust the network to ensure that their requirements are met, and
- **Agency**: The network user can act independently and make their own free choice over how their requirements are met

Some identity networks place a greater emphasis on trust and the need to ensure that the participants in the network are trustworthy. Other identity networks place a greater emphasis on agency, seeking to give greater control to network users – which of course also brings with it, greater responsibility. In the end, all identity networks rely on a combination of trust and agency.

To work, identity networks need to serve and meet the needs of all network users. Included below is a description of how the Verified.Me identity network meets the requirements as defined in the whitepaper.

Governance

Participation			
Network User	Requirement	Self-Assessment	Basis
Subject	Be able to participate (inclusion)	Subjects need to hold an eligible account with one of the financial institutions participating in the consortium. Between 85-90% of adults in Canada have such an account[3]. Where subjects hold multiple eligible accounts with different financial institutions, they can choose which to use for Verified.Me. To be eligible, accounts have to meet defined minimum criteria established by the particular financial institution, such as length of time the account has been opened. The minimum criteria help protect the network from fraud and abuse. Where a subject's account is not eligible, the	Agency

3 https://cba.ca/banks-and-consumers

		financial institution will help the subject understand what they need to do to meet the minimum criteria.	
Provider	Clear rules for participation and confidence in other participants	Participation is on the basis of standardized agreements. The agreements for Service Hosts, Identity & Attribute Data Providers and Service Providers/Relying Party (RPs) are specific to those roles but ensure each party in the network can be confident of the behavior of all other parties in the network. The agreements that SecureKey has entered into with Service Hosts and Identity & Attribute Data Providers require parties to comply with all applicable laws, maintain specified security and related standards, provide regular attestations and include other information sharing processes and detailed obligations and procedures in the event of any incident.	Agency
Relying Party	Clear rules for participation and confidence in other participants	As above. The standardized agreements that SecureKey has entered with Service Providers/Relying Parties (RPs) include terms mandated by SecureKey and the Financial Institution consortium members acting as Service Hosts to ensure network security and trust. Furthermore, it includes minimum requirements and standards for the operation of the network adapters, compliance with applicable laws, maintenance of industry-leading security processes and standards, maintaining specific eligibility requirements, using attributes only for approved uses, etc…	Agency

Transparency			
Network User	Requirement	Self-Assessment	Basis
Subject	Transparency over how credentials, and the attributes they contain, are used and clear straightforward means to manage credentials	The Verified.Me User Agent allows subjects to review the attributes about to be shared, including the source (Data Provider) and destination (Service Provider) of the attribute data, prior to obtaining the express authorization (consent) from the subject. All this is achieved while preserving the Triple Blind® approach.	Agency
Provider	Assurance that consent is correctly obtained, from the subject, to release credentials (when the consent is not obtained directly by provider) Transparency over downstream use of credentials.	A clear standardized consent process is employed. Providers are not permitted to know the specific identity of the Service Provider that receives subject data, however, the agreements in place between SecureKey, as the network operator, and participants require that a Service Provider uses such data in accordance with the approved use case, and also that such credentials/attributes are used in compliance with applicable laws. The agreements between SecureKey and each Service Provider place limitations on the types of organizations that are permitted to become Service Providers, and therefore eligible to request and receive subject attributes.	Trust
Relying Party	Transparency over the production and provenance of credentials that are relied upon	Service Providers can request, and are aware of, the type of organization from which attributes/credentials are obtained, e.g. financial institutions, mobile operators, credit bureau, etc, and in limited scenarios (for example, where required by law), the Service Provider will be aware of the identity of the Data Provider The Verified.Me service also offers attribute bundles, e.g. “Identity Check (KYC)”, “Financial Institution – Base Profile” intended to enable regulated Service Providers to comply with regulatory requirements.	Trust

		Service Providers need to determine that attributes from an organization type are suitable for their needs.	
Accountability			
Network User	Requirement	Self-Assessment	Basis
Subject	Have recourse in the event something goes wrong, including being able to repair erroneous personal data and seek redress for harm caused	The subject will access Verified.Me via their relationship with one of the financial institutions participating in the network as Service Hosts. If certain issues arise (for example, if the subject is unable to login to their financial institution using their existing credentials, or certain information made available by their financial institution is incomplete or incorrect, the subject will be required to request support from their financial institution. Depending on the issue, the financial institution may or may not be able to resolve this by themselves. For example, if the subject's Verified.Me account is erroneously linked to an incorrect Data Provider, an investigation involving SecureKey, the relevant financial institution, and possibly the Data Provider in question, would be required using predefined processes agreed to by all consortium members and tools offered by the Network. If the subject becomes aware that attribute data held by a Data Provider concerning them is incorrect, the subject will be required to notify the Data Provider.	Trust
Provider	Relying parties of credentials are responsible and will be held accountable in the event of a breach	The standardized Relying Party or Service Provider agreement requires each Service Provider to use all information received from Data Providers in accordance with applicable laws, and places obligations on the Service Provider to protect subject information it receives in accordance with its existing customer service agreements and privacy notices. These agreements also require them to proactively notify SecureKey, as the network operator, in the event of an incident affecting that	Trust

		information and to assist SecureKey and its suppliers in the resolution of such incident. These agreements also include specific clauses preventing Service Providers from claiming against data providers and SecureKey and limiting liability for damages, even in cases where subject data was incorrect or out of date, unless such party acted illegally or negligently in performing its obligations.	
Relying Party	Clear liability arrangements Verifiable or audited evidence of provider processes	The standardized agreement that SecureKey enters into with each Service Provider specifies that all subject attribute data is provided on an 'as is' basis, and Service Providers are presumed to utilize other lawful methods of securing subject information in addition to Verified.Me. As between SecureKey and each Service Provider, potential liability for errors or other breaches is limited, with exceptions for a party's breach of applicable law or confidentiality or its negligence. However, Service Providers get some level of comfort from knowing the type of trusted organization it originates from, that such Data Providers have contractually agreed with SecureKey to share subject information in their files or databases at the time of the subject authorized sharing transaction, and that such information is shared directly from the Data Provider to the Service Provider through the network. For example, if the attributes originate from a participating financial institution, then the Service Provider will take some comfort knowing that the organization is regulated and also has a legitimate commercial interest in maintaining current and up-to-date information about its clients.	Trust

Operation

Confidentiality			
Network User	Requirement	Self-Assessment	Basis
Subject	Credentials are only shared with consent Data is only used for purposes that the subject agrees to Network does not enable tracking or surveillance of a subject Network does not include honeypots that if breached would impact many subjects.	All subject data is kept in the Data Provider's systems and is only transferred to Relying Parties (Service Providers) after a subject has expressly consented to the transaction request. The Verified.Me service is Triple Blind®, meaning that no network participant, including the operator (SecureKey), can have a complete view of the subject journey – the subject can't be tracked.	Trust
Provider	Legal basis to share data Being confident no data protection issues arise from downstream use of credentials	The legal basis to share data is the agreements between SecureKey and each network participant. Relying parties (Service Providers) must be authorized to receive data and their obligations are handled contractually. Service Providers are contractually obligated to only use subject data as permitted in their service agreements with those subjects, and at all times in accordance with applicable law.	Trust
Relying Party	Credentials received are minimized to mitigate data protection risks Data is only used for purposes that the subject agrees to.	The agreements with Service Providers place restrictions on the data that may be shared and the purpose for which it is shared based on the type of service provided by the Service Provider and for specified agreed use cases. Data is shared in clearly defined bundles. These agreements complement the consent given by the subject when using the Verified.Me service.	Agency

Integrity			
Network User	Requirement	Self-Assessment	Basis
Subject	System protects against identity theft and other abuse	The system cryptographically secures personal data end-to-end. Transaction proofs (i.e. cryptographic evidence that a transaction occurred) and other system data enables the network to monitor for potential fraud and support the investigation of reported fraudulent transactions, while preserving the privacy that is fundamental to the system. Fraud can be investigated without the involvement of the subject if necessary and appropriate.	Trust
Provider	Credentials cannot be altered downstream, resulting in fraud, disputes and/or inconvenience to subject	Credentials are cryptographically verified to reduce the likelihood of and subsequently the detection of any alteration. Providers who are not consortium members cannot directly check transaction proofs. With the support and cooperation of the network operator and applicable consortium members, they can request that the network does this on their behalf. All parties agree to facilitate audit and investigations to resolve fraud and each Service Host, Data Provider and Service Provider has contractually agreed to cooperate with SecureKey and other network participants, as required.	Trust
Relying Party	Credentials are issued to the subject, have not been revoked and are received unaltered from the provider Network detects and mitigates against fraud	As above.	Trust

Availability			
Network User	Requirement	Self-Assessment	Basis
Subject	Digital identity can be used when required Digital identity cannot be inappropriately taken away	Subjects are required to have an eligible account with a participating financial institution to access the service. The terms and conditions permit SecureKey to block or terminate access to the service at any time. This allows SecureKey to close dormant accounts as well as support lawful requests and fraud investigations. As the network has no visibility of the real identity of subjects, it is not possible for it to discriminate between subjects. Because the attributes that a subject authorizes to be shared are shared directly with the Service Provider by one or more Data Providers and also because the Verified.Me network stores no personally identifiable data, loss of access to the service would not directly impact the relationships the subject has with network participants or the services received from them.	Trust
Provider	System does not place onerous service level requirements on provider	Reasonable service level requirements consistent with a Data Provider's own customer-facing systems are addressed in the contractual agreement between the Data Provider and SecureKey. These will need to be sufficiently high to support the real-time nature of the service.	Trust
Relying Party	System is available when needed, depending on whether it supports offline or online transactions	The system is designed to handle only online transactions and does not currently support offline. Service Providers will rely on the service and ecosystem of Data Providers being sufficiently available, including from Financial Institutions acting as Service Hosts and using their existing customer facing systems, etc...	Trust

4. Choosing an Identity Network

For reference, this self-assessment section relates to Section 6 of the “Making Sense of Identity Networks” whitepaper. There are many factors in determining whether to participate in an identity network or not. Included below is a self-assessment description of how this identity network meets the various factors to consider when choosing an identity network, as defined in the whitepaper.

Utility	
Identity transactions supported	Verified.Me is designed to be flexible supporting a growing range of use cases and transactions. Examples of currently supported use cases include: • Check credit score for free; • Remotely and securely verify subject identity to open an account with (Sign-Up) or access services from (Sign-In and Step-Up) a participating Relying Party • Remotely and securely sign documents with enhanced verification of the document signer; Other use cases are in development and being piloted.
Sector	Verified.Me is designed to be usable across all vertical sectors.
Scope	Verified.Me enables individuals to share their attributes.
Mode	Attributes are shared in real-time from the Data Provider to the Service Provider, meaning that they are fresh and by definition still valid from the Data Provider’s own perspective and business needs. .
Identity migration	The subject is required to have an eligible account with a participating financial institution. Currently, no mechanism is provided to allow a subject to move their Verified.Me account from one financial institution to another, however since no attributes are held in the network (data remains at the source, i.e. Data Provider), there is nothing to migrate.
Interoperability	Verified.Me can interoperate with other systems and is implementing support primarily through the evolving and maturing W3C standards. The general model is that Service Providers, Data Providers and Service Hosts will be identified using DIDs and their public keys are included in their associated DID document.
Adoption	Verified.Me is a new service but is continually adding uses cases to those already provided. By partnering with a consortium of seven major financial institutions the service is already accessible to a significant portion of the Canadian adult population. The Verified.Me network continues to

	evolve to add new service providers, to view the full list please visit www.verified.me.
Trust	
Governance	Legal agreements are provided to and agreed on by members of the network. There is also a Service Oversight Committee including the Service Hosts (Financial institutions) and SecureKey; Multiple Governance Frameworks (Contractual, Legal, Liability, Business, Privacy, Data and Infosec). These agreements are proprietary and confidential.
Transparency	The software behind Verified.Me is based on open standards and protocols, however, it is a permissioned network. It is operated by trusted and regulated financial institutions in conjunction with SecureKey.
Assurance	The network is designed to enable fraud monitoring and detection, while preserving privacy. When fraud is suspected or detected, processes are in place to investigate and take appropriate action. This can include suspending or revoking subject profiles, and may also result in the temporary suspension or permanent removal of an Identity & Data Provider or Service Provider. SecureKey has implemented security in our Software Development Lifecycle through to deployment, as well as Supply Chain integrity for delivery of components to partners and customers. Controls ensures security involvement from design and architecture through to production deployment and continuous monitoring of our services. Further, SecureKey engages 3rd party security assessment organizations to perform security architecture reviews, source code reviews, and penetration testing (web application and infrastructure).
Funding	The network was initially funded with investment from the consortium members. The ongoing operation will be funded by usage fees levied on Service Providers.
Maturity	The service was launched in production in May 2019 following a significant period of design, development and testing. It leverages SecureKey's expertise and experience developed as a result of its provision of its Concierge Service to the Canadian Government over many years. SecureKey Concierge has over 15+ million registrations using credentials from 16 Financial Institutions Partners to access over 80 Government of Canada services such as CRA and Service Canada.

Privacy	
Choice	Verified.Me provides choice to subjects in two ways: • The choice to have their trusted providers share their data for them, in a secure and privacy-preserving way. This enables subjects to forego inconvenient in-person identity verification or time consuming, lengthy processes where PINs or other information must be mailed to them before access to the service can be granted. • When using the Verified.Me service, subjects are provided with control over sharing of their data via the need for explicit consent before any data or attributes are shared. Subjects are provided with a clear understanding of what data is being requested by the Service Provider and the purpose for which the data is being requested. Armed with this information, subjects can make meaningful decisions on whether to share their data.
Data protection	Data protection is at the core of the design of Verified.Me. The service embraces the 'privacy by design' approach and is intended to exceed data protection requirements – both federal and provincial. Data Providers and Service Providers are also required to meet all relevant data protection requirements. The agreements with Data Providers and Service Providers place specific requirements on them, to ensure the protection of personal information across the network, and to define clear boundaries of responsibility. Verified.Me enables Service Providers with the ability to select or request only those attributes that they need for their business purposes. This improves their ability to meet regulatory requirements for data minimization.
Transparency	Verified.Me is a service provided by SecureKey with the direct involvement of a consortium of regulated financial institutions that place a heavy emphasis on security and protection of subject information. Subjects therefore can have a reasonable expectation that the service is secure and will protect their personal information. Verified.Me (and SecureKey) uses the Triple Blind® concept to communicate the privacy respecting design of the network including no tracking or performing surveillance on subjects. Some use cases (e.g. KYC) require a transparent exception to the Triple Blind® approach, for example, when the name of the Data Provider is required by regulation to be provided to the Service Provider as part of an account opening transaction. Verified.Me achieves this by making the name of the Data Provider an attribute that the subject consents to share.

Accountability	SecureKey enters into comprehensive agreements with each participant in the Verified.Me service mandating certain performance levels, security requirements and compliance with privacy and other laws. In addition, agreements between SecureKey and Service Providers prohibit the use of subject information for purposes other than the approved sharing transaction. These arrangements ensure that the network provides a safe and secure environment for subjects sharing their data. The network itself holds no personal information and so the primary recourse that individuals have is via the Verified.Me service terms and privacy notice, any existing agreements between individuals and data providers and agreements between individuals and service providers that they choose to share information with.