Primary Contact Details

Company Name

ShareRing Ltd

Solution Name

ShareRing Me

Lead Contact

[redacted]

Lead Contact Email

[redacted]

Lead Contact Phone (with country code)

[redacted]

Please describe how your system and practice statement are kept under continuous and regular review, including by your top management

Our 'ShareRing Me' product is formally reviewed by an accredited third party expert in digital identity verification on an annual basis under the terms of the United Kingdom Digital Identity and Attributes Trust Framework. Our product was certified under the UK framework in 2023. This practice statement for the AATT will reuse much of the material that has been created for the UK accreditation. These materials are constantly under review to ensure they are accurate and understandable for all our stakeholders, especially our clients who use our self-sovereign digital identity product to prove some aspect of their age or identity safely and securely.

Are you

Age Assurance Provider (an entity responsible for providing age assurance results to a relying party)

Practice Statement by Age Assurance Provider

Age eligibility requirements

'ShareRing Me' verifies a person's identity in a digital environment. The ShareRing solution implements a self-sovereign identity model that is built on blockchain technology. Privacy by design is at the heart of the ShareRing Me self-sovereign model. We place control of identity in the hands of the user. No identity data is stored by ShareRing as this remains on the device in the user's encrypted vault.

The ShareRing Me product uses age verification with the age of our customer determined from the date of birth held by an epassort embedded with an NFC chip. Our self-sovereign solution means that our customers control their date of birth data in their self-sovereign ShareRing vault, and can select to share a statement verified by ShareRing to a relying party confirming that they are above, below or within any age range specified by the relying party. The relying party on the other side of the transaction can confirm that the ShareRing age confirmation statement has not been tampered with by the user by checking against the data hash that was created on the blockchain by ShareRing at the point of identity verification.

The self-sovereign design means that data minimisation is embedded into the transaction, and no further identity details need be shared with the relying party, not even the actual date of birth. If the relying party requires the actual date of birth then this can be submitted by the user if they choose to share this data.

Outside of specialist services for scanning documents and biometric analysis there are no further intermediaries involved in the ShareRing Me solution.

Age assurance components

The 'ShareRing Me' App uses an epassport authoritative source as the basis for identity verification by ShareRIng as an accredited identity service provider, which then enables the identity data of the customer that is held in their self-sovereign vault in the ShareRing Me App to be used to share a ShareRing verified statement that the customer is above, below or within any age range specified by a relying party.

Indicators of confidence

Under the UK Digital Identity and Attributes Trust Framework (DIATF), ShareRing's ShareRing Me product achieves a "Medium" level of confidence, ensuring that identity attributes accurately represent the individual to relying parties.

In Australia, ShareRing aligns with the Digital ID Act 2024, which establishes a secure and inclusive digital identity system. Our processes adhere to the standards set by the Australian Government Digital ID System (AGDIS), ensuring compliance with national regulations.

To enhance our confidence level to "High", we are implementing additional fraud detection measures, including checks against lost or stolen passports.

Our identity verification approach incorporates biometric and cryptographic verification to ensure identity integrity. This methodology aligns with both the UK DIATF and Australia's Digital ID legislation, providing a robust framework for digital identity verification.

To date, there have been no reported incidents of identity fraud through the use of ePassport identity verification on the ShareRing Me app.

Binding process

ShareRing executes remote digital identity verification using a combination of in house built technology and the use of specialist third party OCR and biometrics technology for evidence validation and verification. Our solution leverages a combination of: near field communication (NFC); optical character recognition (OCR); expiration check; MRZ checks; liveness detection; and face matching.

ShareRing Me reads and extracts the data stored on the NFC chip on an ICAO biometric passport. The authenticity of the epassport is verified, and checks are made that the data in the visible zone, the MRZ and on the chip all cross reference. It matches a user taken selfie against the biometric information on the NFC chip. A successful match that also passes liveness detection results in a successful outcome with the age of the user being bound within that identity. Our liveness detection service meets high security requirements of facial recognition in different verification scenarios. It guards against spoofed images, videos, and static 3D models.

One point to highlight for the AATT project is that only "ShareRing Verified" data will be in scope for the scheme as this equates to a Medium level of confidence under the UK digital identity trust framework. ShareRing can extend the scope to "ShareRing Checked" if the stakeholders wish to analyse the equivalent of a Low confidence of ShareRing assuring an age threshold attribute. "ShareRing Verified" equates to data successfully verified from an epassport with an NFC chip. "ShareRing Checked" equates to data successfully verified from OCR checks combined with the same biometric checks.

Privacy and data protection

Privacy by design is at the heart of the ShareRing identity service solution with the self-sovereign model putting control of identity data in the hands of the user, and with ShareRing reducing the extraction, flow and storage of sensitive data to the absolute minimum.

The self-sovereign identity model gives a paradigm shift of control to the user in terms of how their sensitive identity data is stored by authorised IdSPs. The model enables a massive benefit for the user in terms of significantly reducing the risk of data breaches on traditional IdSP honeypots. For ShareRing the self-sovereign model enables a privacy by design solution that effectively simplifies our ability to meet GDPR requirements, as the model design minimises the processing, transport and storage of user PII.

A user who wishes ShareRing to remotely verify their identity will actively consent to undergo a process that executes both document validation and biometric verification. The majority of the data processing will occur within the ShareRing App on the user device, with the bare minimum of user data leaving the confines of the device. No additional user data is stored by ShareRing as a result of the identity verification process. (As part of user onboarding ShareRing requests and validates the user's registered email, and this remains the only PII retained by ShareRing as part of the identity verification process.)

The process requests the user to take a photo of their NFC enabled document in order for ShareRing to extract their identity information from the chip in the document. (The data extracted by OCR from the photo of the document MRZ is required in order to access the chip.) The data extracted from the chip includes the name, date of birth and document ID, as well as a digital copy of the photo of the user that is shown on the document. ShareRing performs checks at this stage to check that the chip is properly signed by the issuing authority and that the chip has not been cloned. ShareRing also performs a cross reference of the data that appears in the MRZ and visual zone of the document, as well as checking that the document has not expired.

At this point in the process there has been no transport of any identity data outside of the ShareRing App on the user's device.

If the document passes validation checks that are made within the ShareRing App, then the user is requested to take a video selfie.

The extracted photo and selfie video are then sent to a ShareRing API for onward transmission to a third party API provided by a biometric specialist for biometric processing to determine liveness and face match the video to the extracted photo. The biometric specialist purges all data after their liveness and face match processing. No other PII data is sent outside of the App, ie no name, DoB.

Once ShareRing completes the document validation and biometric verification, it then creates a non-reversible hash of the data, including the passport image from the OCR (which is important in terms of preventing dictionary attacks from pseudoanonymised data), which is written by ShareRing to the ShareLedger blockchain as a verifiable credential (W3C standard.) It should be noted that the hash is generated from within the App such that the PII like name and date of birth never get sent to a ShareRing API. This hash can be subsequently recreated by relying parties on receipt of data from a user who claims a ShareRing Verified Identity in order for the relying party to confirm that the data has not been changed since verification by ShareRing (ie any change to the data will result in the generation of a different hash value.)

No identity data is processed or stored by ShareRing on our back end platforms with the exception of transport of the photo and selfie to a sub-processor, and storing of the user email address as part of the account setup process.

The user holds their data on their device in their encrypted vault. The user then controls with which relying party they choose to share their verified identity data.

In summary:

ShareRing at all points in the process:
- minimises the data is processed in the App on the user device,
- and minimises the data set sent through to the ShareRing APIs for processing in the ShareRing backend,
- and minimises the set of data that is sent to any specialist third party for further data processing.

The use of distributed ledger technology as an immutable register to hold the ShareRing issued proof of the data verification as a non-reversible hash is the key to allowing the user to have control of their identity data whilst allowing relying parties to verify that the data has been verified by an authorised IdSP but without ShareRing storing the identity data. This makes ShareRing very different to other IdSPs who necessarily need to store identity data on behalf of the user.

Ease of use

The ShareRing Me App ensures that its age assurance methods align with Australian digital identity and accessibility standards, making the service appropriate for users of all ages and abilities.

Our approach follows Australian Government Digital Identity System (AGDIS) guidelines and incorporates privacy-by-design principles to ensure that users, including young people, can verify their age securely and independently.

The existing Accessibility Statement under the UK Digital Identity and Attributes Trust Framework provides a strong foundation, and ShareRing continues to enhance accessibility features to align with Australian accessibility standards, including the Web Content Accessibility Guidelines (WCAG) 2.1.

The following is an extract of our Accessibility Statement under the UK Digital Identity and Attributes Trust Framework.

1 Accessibility statement for the ShareRing Me App
This accessibility statement applies to the ShareRing Me App, which is accessible to download for free from the Google and Apple stores for use on Android and iOS smart phones respectively.
A key objective for ShareRing is that no one is excluded from using the ShareRing Me App, and we have designed and built our App such that it is accessible to as many people as possible, including those who are visually impaired or with mobility issues.
For those with a visual impairment the App works for large font and also for integrated voice capability like VoiceOver and TalkBack on iOS and Android devices respectively. The App has also been designed and built to allow use via a switch device like a joystick for those with a mobility issue.
The user experience does not rely on sounds and therefore the App is accessible for those with a hearing impairment.

The following is a quote from our audit for the UK DIATF accreditation:

“Simple to follow process, terms and conditions and privacy policy clearly available, accessible and requiring positive confirmation to proceed. UI clear and easy to follow.”

The ShareRing Me App is multi-language.

ShareRing is dedicated to enhancing digital inclusion for Indigenous Australians by aligning with the First Nations Digital Inclusion Plan (2023–26), which emphasizes access, affordability, and digital ability.

Recognising the unique cultural practices and community structures, we are committed to:
- Culturally Appropriate Identity Verification: Incorporating traditional naming conventions (if appropriate)

and community-based attestation methods to respect Indigenous identities.
- Community Engagement: Collaborating with Indigenous communities to co-design digital solutions that address specific needs and preferences.
- Digital Literacy Initiatives: Providing resources and training to enhance digital skills, ensuring that all users can navigate our platform effectively.

By embedding these practices, ShareRing aims to create an inclusive digital environment that honors the cultural heritage and supports the autonomy of Indigenous Australians.

Security

Security is taken incredibly seriously by ShareRing. We are accredited under ISO 27001 for Information Security Management Systems.

We execute third party penetration testing against our infrastructure on an annual basis.

The section under data protection and privacy highlights that our approach to sensitive data is to minimise our handling of such data, and place control back into the hands of the owner of that PII.

The ShareRing vault is self-sovereign. Only the customer has access to their vault. The App itself is protected by a user selected 6 digit PIN or biometric controls from their smart phone.

Overall our risk of data breaches is vastly reduced compared to other identity service providers due to our self-sovereign data model that puts control of data into the hands of the user. Our servers do not store user PII outside of the user's email address.

Human rights protections

The following is our Inclusion Statement under the UK Digital Identity and Attributes Trust Framework.

1 Inclusion statement for the ShareRing Me App
The ShareRing service for identity verification that will verify a user's identity under the UK Digital Identity and Attributes Trust Framework is necessarily restricted to users with access to the following resources:
a government issued document that has an embedded NFC chip
a smart phone running a version of Android 9 or above, or a version of iOS 7 or above.
This restriction on the requirement for an NFC enabled government issued document is mandated by Good Practice Guide (GPG) 45 on how to prove and verify someone's identity.
2 What we are doing to improve inclusion
For UK users the scope of government issued NFC enabled documents is currently limited to ePassports issued by the UK government. The range of documents that ShareRing can support will increase with the range of NFC enabled documents that are issued by the UK government.
Some countries are starting to embed NFC chips into their national identity cards or driving licences, and ShareRing will extend coverage of available documents in line with the growth of offerings from national governments.

Our product for age verification has no limitation beyond the requirement for a government issued epassport. We recognise the limitation for those adults and young adults who do not possess such a document. We also recognise that the adoption of ShareRing as a safe and secure route to a self-sovereign digital identity that embodies ease of access to age related content, goods and services may support an increase in the demand for epassports as owning a passport is itself a universal right, and therefore the percentage of people who cannot use our solution for age assurance should decrease over time.

Audit, certification and review

The product for ePassport processing is certified under the UK Digital Identity and Attributes Trust Framework. The full audit was conducted by ACCS in Q4 2023 with a surveillance audit following in Q4 2024.