TRUST ALLIANCE LITE PAPER

Launched in July 2019 by the Australian Red Cross, the Trust Alliance is a multi-sector collaboration committed to the shared principles of do no harm, humanity first, open ecosystems, equity, and transparency.

We bring together values aligned stakeholders to:

- Develop identity pilots and programs;
- Advocate for the uptake of decentralised identity standards and design principles to industry and government; and
- Develop and maintain the Trust Alliance Credentials Framework.

As a collaborative initiative built on humanitarian foundations, we bring a diversity of voices and expertise into the governance, research, and design of our digital identity ecosystem. The founding members of the Trust Alliance are; Australian Red Cross, CARE Australia, Engineers Without Borders, Oxfam Australia, RedR Australia, Traverse, TypeHuman, RMIT University and Swinburne University of Technology.

Our mission and goals

Our mission is to lead the emergence of a useful and ethical digital identity ecosystem, and we are collectively working towards the following goals:

- Equal access to digital identity that is universally recognised by everyone;
- Global recognition and adoption of ethical digital identity with the regulatory and technology infrastructure in place to enable it.

Towards decentralised identity

In our digitally enmeshed world, access to a trusted and verifiable digital identity[1] is essential to human dignity. More than 1.1 billion people have no official proof of identity, which stops them from accessing vital services, protections and rights including voting, healthcare, social protection, education and finance.[2] A further 3.2 billion people have some form of identification but cannot use it on digital channels, diminishing their ability to fully engage in contemporary society where digital tools and platforms are ubiquitous in our public and private lives.[3]

Globally, efforts to solve digital identity have so far been led by governments and businesses, with mixed results for citizens and users. Government digitisation schemes can disempower and frustrate as they prioritise departmental over citizens' needs[4] and may expose citizens to state surveillance. Businesses such as banks and technology companies typically focus on proprietary products and business models that treat identity data as an asset to be monetised. The end result is a fragmented digital identity landscape, with many competing platforms and services, costly business integrations, and poor user experiences.

Our efforts are part of a growing movement to define 'good' identity in digital contexts. In 2018, the World Economic Forum (WEF) launched its *Platform for Good Digital Identity*, with the aim of advancing 'digital identities that are collaborative and put the user interest at the center.'[5] Their 2018 report explores the complexity of establishing and verifying digital identities for people in a way that is empowering and secure given the vast range of identity-related data that is being created. The WEF concluded key elements for designing user-centred digital identity are: fitness-for-purpose; inclusivity; usefulness; security; and offering choice to individuals.[6]

Omidyar Network (ON), an impact investment company and a partner of the WEF Platform, has made significant contributions towards raising awareness of the importance of good digital identity that is based on privacy, inclusion, user value and control, and security across the "state-issued, de-facto, or self-asserted digital identity continuum".[7] They support the #GoodID movement which promotes "global dialogue, research, and advocacy between governments, technologists, civil society, and all sectors of business" to inform digital identity policy, technology design, and practice.[8]

Another WEF partner, ID2020—an alliance of businesses, non-profits, governments and individuals—has been influential in advocating for ethical, privacy-protecting approaches to digital identity. In their work, ID2020 refers to the four Ps of good digital ID: private, portable, persistent, and personal.[9,10]

Consistent with these narratives, the Trust Alliance is principle-driven and aims to build a useful and ethical digital identity ecosystem. Although technologies don't solve problems, they do set some of the terms for our online and offline participation, enabling and constraining what we can do. The Trust Alliance ensures that systems are built to enhance privacy and agency. Getting this right means engaging users and vulnerable communities in this process from the outset, which will ultimately benefit all of us.

Humanitarian work requires identifying people in need of assistance and rapidly deploying others who can help. When we get this right, communities recover faster and hopefully grow more resilient.

However, sharing information comes with its own risks. While privacy breaches are tolerated among the general population (for better or worse), poor data practices can have catastrophic outcomes in humanitarian contexts. Moreover, humanitarian organisations need to know that the people they send to provide humanitarian assistance have the necessary qualifications, as well as the assurance that these qualifications have not been revoked as a result of unethical or criminal conduct. The Trust Alliances addresses these needs through what we call trusted credentials.

Put simply, trusted credentials enable people to ***claim*** verified credentials and ***use*** their credentials across organisations. These credentials may be state-issued (from e-passports and birth certificates to police checks) or provided by organisations and businesses (including formal or informal qualifications, work experiences gained through paid employment or volunteering, immunisation and other health records, and more).

Our approach gives people the ability to keep claims about themselves and empowers them to share only the information they need to share. By doing this, we can standardise and simplify how parties in this process come to verify and trust data, reducing the opportunity for data monopolies to form, and giving greater data controls to the user. By empowering users to share information across agencies, the Trust Alliance overcomes siloed services, creating a more effective and efficient humanitarian arena.

Using distributed technologies, an individual can access a credential generated by one Trust Alliance member and share it with another as needed without relying on an intermediary, knowing that their personal information remains safe and secure. For organisations, this reduces duplication in training and compliance, and allows humanitarian actors to rapidly deploy contingent workforces to crisis-affected areas. For beneficiaries, the Trust Alliance is a means for them to share information about themselves across services, so they may access assistance and resources as needed.

The digital credential ecosystem being built by the Trust Alliance aims to safeguard vulnerable people by ensuring that those being sent by organisations to assist have been adequately vetted. This credentialing system also enhances human dignity by giving people the tools to share personal information in a safe manner, including those without government-issued identity.

Trusted credentials

The sharing and verification of an individual's identity involves the exchange of facts, and the verification of those facts. For example, if an individual is claiming to be Priyanka Patel, living at 1 Easy Street, this fact would ordinarily be checked against government records to see if there is a Priyanka Patel at that address.

In the digital identity domain, this exchange of facts is referred to as a claim, and where it can be confirmed, a ***verifiable claim***. Prior to blockchain technology, these digital claims would be verified against a physical or digital ledger. However, a combination of cryptography and blockchain technology has enabled a new type of verifiable claim providing the ability to verify facts without having to check it against a centralised record.

In addition to asserting personal details such as legal name or an address, these verifiable claims are increasingly being used to share and verify facts related to professional and work domains, such as educational qualifications or eligibility to work within certain communities. These types of applications are also known as credentials or micro-credentials.

In decentralised identity systems, a verifiable claim is held in a user's mobile wallet and shared with third parties (also known as ***relying parties***) when requested. The contents of the claim are cryptographically signed by the issuer, which allows a future relying party to verify its authenticity - like a digital wax seal. For the purposes of our work, the Trust Alliance refers to such verifiable and portable credentials as ***trusted credentials***.

Trusted credentials cont.

While the technical foundations for verifiable claims are sound, in order to sustain the momentum towards decentralised identity we need to solve the issue of ***digital coordination and cooperation*** among the many and varied actors in the digital identity space. To meet this challenge, in the short- to mid-term, the Trust Alliance is focused on investment and experimentation in how trusted credentials are established, utilised and governed within the growing network of providers. We hope to accelerate the adoption of trusted credentials standards by identifying organisational needs, connecting these with stakeholders and providing evidence of what works. The Trust Alliance overcomes the problem of centralised services by providing developers with an open standard and credential framework that they can build on, encouraging a flexible and adaptive digital credential system.

Our work on trusted credentials allows us to test and understand how these new technologies work in practice. Presently, we are examining the extent to which trusted credentials reduce the administrative burden on the humanitarian sector, enabling organisations to work together more effectively, and providing greater agency to individuals, local actors and organisations. Over time, we will expand our work, with the aim providing those without access to identity records with a safe and trusted means to share information about themselves.

Technical approach

The Trust Alliance has developed the Trust Alliance Credential Framework; a technical guideline for how decentralised credentials should be implemented by software organisations seeking to issue, verify, or share credentials. It draws upon a combination of open source tools and standards, as well as the concept of a Trust Registry. The Trust Registry contains an Issuer Register and Claim Status Register which is used to verify credential issuer identity and perform credential revocation checks.

The Trust Registry sits within the broader identity ecosystem, which involves products and integrations for issuing and verifying claims, and user wallets.

The Credential Framework

The Trust Alliance Credential Framework describes the technical approach surrounding the main functions required by digital credentials.

Registering a credential issuer: For a credential to be practically useful, it must be linked to a real-world identity. When a credential is verified, the relying party must have confidence that it was genuinely issued by the stated authority. We currently use the Trust Registry for this purpose. The Trust Registry is comprised of two registers; the Issuer Register and the Claims Status Register. An issuing entity (Issuer) is created and registered by storing their public-key and entity name on the Issuer Register.

Issuing a credential: Issuing a credential to an individual is consistent with the W3C verifiable claim standard. Credentials are generated using this standard and are cryptographically secured and anchored back to the Trust Registry's identity register via the issuer's identity. Individual privacy is maintained by ensuring only the issuer identity is registered to the Trust Registry and later used for credential verification.

Storing a credential: No individual credential information is stored on the blockchain.

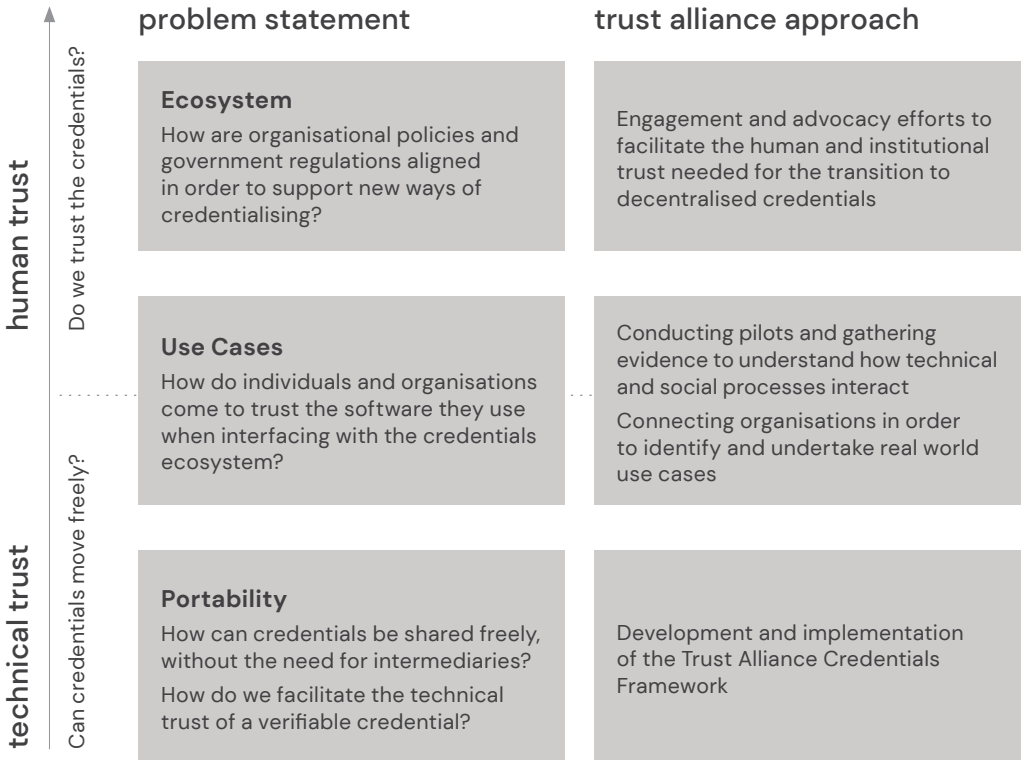
Verifying a credential: Credentials are verified by following a three-step process. First the credential is checked to see whether it has been tampered with. This is guaranteed by using the cryptographic signature attached to the credential when it was issued. The second step checks to see whether the credential was issued by the authority stated on the credential which is achieved by checking the cryptographic signature on the

credential against the Issuer Register on the Trust Registry. The final step is to check the Claims Status Register to see whether a credential has been revoked.

Example

RedR Australia (RedR) provides Hostile Environment Awareness Training (HEAT) to Australian humanitarian workers as part of their mandatory preparation for international deployments. RedR have registered as an issuer on the Trust Alliance Claims Issuer Register using Traverse micro-credentialing software. RedR uses Traverse to issue HEAT Training Certificates (*verifiable claim*) to participants who complete the HEAT program. Participant Sarah (*user*) is required to share the HEAT Training Certificate with Australian Red Cross (*relying party*) to demonstrate competence in order to be deployed as a Red Cross international humanitarian delegate. Sarah's HEAT Training Certificate is received by the Australian Red Cross and verified against the Trust Alliance Claims Issuer Register using the cryptographic signature issued by Red R. The validity of the claim is also checked against the Trust Alliance Claims Status Register.

Transitioning to a decentralised governance model is both a core commitment and a technical focus for the Trust Alliance. We need to ensure that the governance frameworks reflect the Alliance principles, and are well designed and understood, before being encoded in a smart contract. We are planning to transition to a decentralised governance model by 2025. Human trust remains important even in a decentralised model, as illustrated in the following diagram:



Next steps

In 2020, the Trust Alliance is focussed on establishing the **legal entity** and the **governance structure**, publicly releasing the first Trust Alliance Credentials Framework, and implementing stakeholder **engagement activities** to grow our membership and build momentum for the decentralised identity ecosystem.

Until the legal entity is finalised, the Australian Red Cross will provide backbone support, under the leadership of the Steering Committee and supported by Working Groups on Technical standards (Credentials Framework development), Pilots and Programs (identification, prioritisation and development of digital identity use cases), and Research and Insights (developing a research and evaluation agenda for the initiative).

Over a 5-year horizon, we plan to grow our coalition and to establish the Alliance as an independent not-for-profit organisation, funded by its members and governed by a member-elected Board.

- In **year 1** (2020/21) our goal is to have organisations creating, sharing and accepting trusted credentials within the Trust Alliance ecosystem.
- by **year 3** (2021/22) we aim to influence the Australian Government to adopt trusted credentials standards, and
- by **year 5** (2023/24) we want to introduce a funding mechanism for decentralised identity grants.

Contributors

Professor Ellie Rennie (RMIT) Nick Byrne (Typehuman), Ivana Jurko (Australian Red Cross), Drasko Kraguljac (RedR Australia), Amanda Robinson (Australian Red Cross), Katy Southall (Australian Red Cross), Associate Professor Samuel Wilson (Swinburne University)

Endnotes

1. Digital identity involves data that uniquely describes a person or object. For people, this can include legal identity as well as other information, such as their qualifications.
2. World Bank 2017 Identification for Development (ID4D) initiative
3. McKinsey Global Institute 2019 *Digital Identification – A key to Inclusive Growth*
4. InnovationAus.com, "Govt's Digital ID is in trouble" by Denham Sadler, accessed August 2018
5. https://www.weforum.org/projects/digital-identity
6. http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
7. Omidyar Network 2019. ON unpacks Good ID. https://www.omidyar.com/sites/default/files/ON%20Unpacks%20Good%20ID_Final_3.7.19.pdf
8. https://www.good-id.org/en/about/#section-3
9. https://id2020.org/digital-identity
10. While there are no agreed definitions of digital identity, a good overview of latest discussions and thinking is available at https://www.good-id.org/en/glossary/