Australian eSafety Commissioner - Restricted Access System Call for Submissions

1account is a UK based international and innovative digital identity and age-verification company with a mission to better provide access to goods and services, especially for that demographic which does not have access to traditional forms of identity such as passports or driving licenses, and to better protect children by restricting access to age-inappropriate goods and services both online and offline.

1account's suite of products helps retailers prevent unlawful access to alcohol, knives, vaping and tobacco products as well as online services such as gambling or adult content online and on the high street within the UK and internationally.

Our advisory board includes Murray Perkins, formerly Policy Director at the British Board of Film Classification and who was responsible for the implementation of age-verification under the UK's Digital Economy Act 2017.

Just as 1account welcomes the UK government's Digital Identity and Attributes Trust Framework, and works directly with the UK's Department for Digital, Culture, Media and Sport on its development, 1account supports the Australian government in its intention to legislate for a Trusted Digital Identity Framework. We recently responded to the Australian Digital Identity Position Paper and welcome efforts to ensure products maintain the highest standards on privacy and data security so that they can be trusted by consumers.

We believe this work on digital identity also supports the use of age-verification online, in this case in the context of a Restricted Access System, where trust is a paramount consideration.

Our consumer digital identity app complements our existing online verification technology which cross references consumers' information against data sources that enable it to validate its authenticity, such as a user's mobile phone network.

1account welcomes the opportunity to contribute to the restricted access system call for submissions and would be more than happy to elaborate on the information and comments we provide as this important work moves forward.

We have responded to those questions copied below which are most relevant to 1account's considerable expertise in this area.

Question 5 What factors should be considered when assessing the effectiveness and impacts of systems, methods and approaches to limiting access or exposure to age-inappropriate material?

At a high level, of course a system has to effectively limit access or exposure to age-inappropriate material. If it's ineffective – such as simply ticking a box to say one is 18 or over – it does little or nothing to limit access or exposure.

What effective means might look different in different contexts and arguably relative to the nature of the material in question. But, if the decision has already been taken that a particular type of material is age-inappropriate and should be restricted, then proportionality in relation to the nature of the restriction must take a back seat to genuine effectiveness.

An effective system therefore should be one which means it isn't normally possible for a child to access that material which is judged to be age-inappropriate. It cannot be a system which means it is impossible for a child to access or be exposed to age-inappropriate material in all circumstances all of the time. No system to restrict child access to material online can be without limitations and any attempt to build such a system would inevitably end in failure.

An effective system must therefore be pragmatic and realistic.

Such a system would accept that there will be some circumvention but that some circumvention does not diminish the value. To use a simple example, it would be impossible to prevent an 18 year old who can legitimately access material online from sharing that material with their 17 year old sibling. But this doesn't diminish the value of the same system when it very effectively prevents an 11 year old child being exposed to the same potentially harmful material. In other words, by using effective controls, far more children – and younger children – will be protected from age-inappropriate / harmful material than those still occasionally exposed, whether through deliberate circumvention or inadvertent exposure (content shared by others, for example).

An effective system must be a system which will be carried by industry. Which is not to say that industry should be left to come up with their own solutions without clear principles defining what is required. But an effective system will establish the principles of what is required, what outcomes must be achieved, and not necessarily dictate particular or limited solutions. The latter could limit choice, competition, innovation and have damaging cost implications.

An effective solution must also be a system which respects adults' right to access content and aims to mitigate disruption to their experience as a consumer.

Of particular importance, an effective solution must protect the privacy of the consumers it serves and be trusted by them. Work in both Australia and the UK on trust frameworks for digital identity will go a long way to underpin this trust as the frameworks support the use of digital identity to, for example, facilitate financial transactions. If a solution is not trusted by consumers, and consequently not used by consumers, then it won't work for industry either and such a solution would fail.

Question 6 What systems, methods and approaches do you consider effective, reasonable and proportionate for verifying the age of users prior to limiting access age-inappropriate material?

Being both an age-verification and digital identity provider, 1account doesn't doubt that age-verification and digital identity provide effective and proportionate approaches. Ticking a box, by comparison, is entirely ineffective.

We're conscious that the Australian Government has recently consulted on its intention to legislate for a Trusted Digital Identity Framework. This mirrors developments in other territories and further underscores that digital identity will increasingly become a part of our everyday lives. A digital identity is an extremely effective, robust means of age-verification and one of the most privacy protecting methods. Once a digital identity has been set up, it allows for the sharing of single attributes. So, for example, by scanning a QR code, a digital identity can share with a merchant or website the single attribute that the person holding that digital identity is 18 years or older. In an environment where the only relevant consideration is that a person is an adult, no other information

needs to be shared. In this case, a website offering digital identity as an option for age-verification receives no other information or data on the consumer.

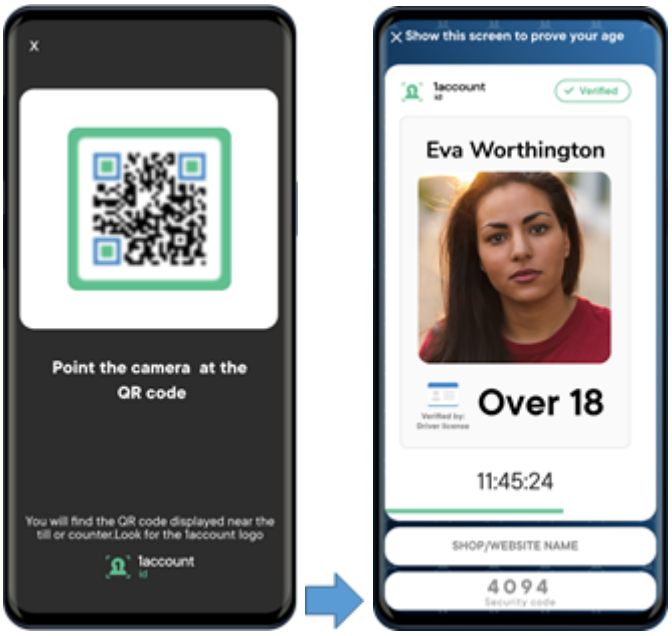
The setting up of a digital identity is an easy but robust process which affords confidence that the person creating the digital identity is who they say they are. As Australia's Trusted Digital Identity Framework evolves, alongside the UK's Digital Identity and Attributes Trust Framework, the security and trust in digital identity, and its eventually ubiquitous nature will make it a very effective solution to better protect children online.

To create a 1account ID a user downloads the iOS app from the Apple App Store or the Android app from the Google Play Store. On installation, the user is shown some simple tutorial screens and is prompted to accept the app's term of service. They are then directed to scan a photo ID document and to allow their image to be captured (take a selfie) with a 'liveness' check. These are checked by IDScan, third-party identity document verification software provided by GBG Group plc.

The document must be determined to be a valid original document, the user must be live rather than a photo, and the images of the user must match the photo on the document. If all these elements are verified, the user will be approved and directed to complete the creation of their 1account ID by validating their phone number and adding a username and password. The user will then be able to use their 1account ID to verify their age.

A failure to verify any of the above will result in a fail or referral for a manual check by trained staff.

Once created, a digital ID can then be used simply by scanning a QR code with a relevant attribute being shared either in person via the screen of a mobile device, or online.



There are of course other approaches, including the use of different biometric information. But on the whole these still need to be captured as attributes linked to a verified identity. Or they remain imperfect estimations with limitations and they become increasingly less accurate the closer one gets to the age being estimated.

Question 7 Should the new RAS be prescriptive about the measures used to limit children's exposure to age-inappropriate material, or should it allow for industry to determine the most effective methods?

Continuing from the immediate point above, there are a range of methods to age-verify or age-estimate in order to limit children's exposure to age-inappropriate / harmful material and the Restricted Access System should allow for industry to determine what methods to deploy.

However, determining what methods to deploy is not the same as determining what methods are effective and acceptable. Giving industry the freedom to choose from a potentially open-ended range of solutions should not extend to freedom to determine what constitutes effective methods. Instead, the Restricted Access System should establish the principles, determining what acceptable methods need to achieve, but then allow industry the freedom to work with companies to provide that service.

It would be a reasonable expectation that some, or most, services will use more than one age-verification / estimation method and potentially more than one company to deliver that service. Preventing or unnecessarily limiting this choice would be detrimental to industry, potentially undermining competition and innovation, and it would risk increasing cost.

Question 8 Is there any additional information eSafety should consider in drafting a new Restricted Access System declaration?

While age-verification, including, if not most especially, digital identity, can be straightforward to integrate, this doesn't mean it can be done in a short time. It should be expected that online companies will need to know exactly what is required of them before they will enter into meaningful conversations with providers of age-verification / estimation solutions.

A transparent roadmap for industry, establishing clearly the principles which need to be adhered to, will help ensure they can plan for a new regime and be in a position to select the solution which is right for them in knowledge that it will also meet the regulatory requirement.

1account is more than happy to continue to engage on these matters and help where we can.