TERTIARY EDUCATION AND RESEARCH NETWORK OF SOUTH AFRICA NPC

TENET

House Vincent, Wynberg Mews
10 Ebenezer Road
Wynberg 7800
Cape Town
Republic of South Africa

(Non-Profit Company)
Registration Number 2000/020780/08
Registered Nonprofit Organisation: 014-801 NPO
VAT Registration Number: 4190191926

Tel: +27 +21 763 7140

Email: ceo@tenet.ac.za
Web: http://www.tenet.ac.za

26 February 2021

Minister of Home Affairs
Per email: oimbpolicy@dha.gov.za

Submission in respect of the draft Official Identity Management Policy

The Tertiary Education and Research Network of South Africa NPC (TENET) welcomes the publication of the draft Official Identity Management Policy (IdMP) for public comment in Government Notice 1425 of 31 December 2020.

TENET operates the South African Identity Federation[1], an academic identity federation that facilitates identity interchange amongst higher educational and research institutions on a global scale. In the process of establishing this federation, we've tackled a number of issues raised in the draft IdMP and have both a conceptual and first-hand understanding of some of the challenges.

It is with this background that we, therefore, respectfully submit the following contribution to the public participation process.

1. Principle 3 / Structure of identity numbers

1.1. TENET strongly believes that any new identity number format should be immutable - that is to say, once assigned to an individual, it should never need to be changed.

1.2. The current mutability of identity numbers causes innumerable problems for systems that rely on it as a personal identifier, from the creation of duplicated records to the loss of structural integrity in database systems. It also creates interoperability issues between systems that have different versions of the identity number for the same person.

1.3. Section 7.3 of the IdMP correctly identifies two of the three scenarios in which the current identity number changes, but fails to consider the fact that citizenship is also encoded in the eleventh digit of the current ID number format.

1.4. Moreover, the proposal for encoding gender as the character "X" as an alternative to retain the existing coded form does nothing to address the mutability of identity numbers. Because individuals gender identity can be fluid, it is possible that such an encoding would require multiple changes of identity number over a lifetime.

[1] https://safire.ac.za/

1.5. For this reason, TENET is of the opinion that the proposed new identity number format should **not** encode any characteristics - including date of birth, gender, citizenship or race - of the person to whom it is assigned.

1.6. TENET strongly favours the approach of assigning a randomized, opaque, privacy-preserving pseudo-anonymous identifier as the new national identity number. We note that this identifier need not be a number, and could include alphanumeric characters in a fixed-length string.

1.7. However, the current identity number format encodes a checksum as the 13th digit that facilitates the detection of transcription and data capture errors. This is not mentioned in the IdMP, and we believe that the loss of such a checksum would be detrimental.

1.8. Thus, while we favour the use of an opaque identifier, we believe that the last digit of such an identifier should remain a checksum calculated using the Luhn algorithm. If necessary this algorithm can be modified[2] to suit the size of the character set used.

2. Principle 4 / Interoperability / Identity number as an attribute

2.1. Regardless of the choice of new identity number, there will remain legacy systems that make use of the current identity number format long after the proposed implementation timeframe. These will include privately owned systems not linked to the NIS but that nevertheless make use of an identity number as a unique person identifier.

2.2. To ensure backwards compatibility for as long as possible, the existing number format should not change; instead a new format should be introduced as a separate, new identifier. It is imperative that the NIS retain both the old and new identity number, and store these as separate attributes associated with an individual’s identity.

2.3. Over the timeframe envisioned in the IdMP, the old format should be deprecated and should become read-only and should no longer appear on any official documentation. However, it should continue to be preserved in the NIS as an attribute to facilitate cross-referencing from legacy documents.

2.4. For these reasons, the implementors may want to consider adopting alternative terminology to differentiate the old “National Identity Number” as a separate field to the proposed new identity number.

3. Principal 4 & Principal 5 / Federated authentication

3.1. We welcome the call for interoperability and the use of open standards but believe the scope of this needs to be extended to include the use of the NIS as a basis for federated authentication.

3.2. Individual government departments should not be requiring the creation of usernames and passwords for citizen services, nor should they be maintaining separate identity databases for the purpose of facilitating authentication. Instead, there should be a single federated authentication system for all citizen services.

3.3. Such a system should be based on widely adopted, open standards such as the Security Assertion Markup Language (SAML) and/or OpenID Connect (OIDC).

[2] See https://en.wikipedia.org/wiki/Luhn_mod_N_algorithm

3.4. Correctly implemented, such a system should also be interoperable with, and capable of being augmented by existing federated authentication platforms, such as the one in use by the higher education and research community.

4. Principle 10 / The information regulator as a chapter 9 entity

4.1. The IdM recognises the importance of protecting privacy and identifies that some legislative protection might be required to safeguard this and provide oversight. In particular, it identifies the role of the Information Regulator established under the Protection of Personal Information Act, 2013 currently does not have sufficient independence.

4.2. TENET is of the opinion that the Information Regulator plays a key role in preventing the abuse of personal information, both by the private sector and within Government itself. This role applies to all aspects of the protection of personal information, not just of the NIS proposed by the IdMP. Thus, the issue of the independence of the Information Regulator has far wider implications than that identified in the IdMP.

4.3. Moreover, the implementation of a single NIS envisioned by the IdMP carries with it the grave risk that such a rich source of population information might be exploited, either for commercial gain, with malicious intent, or to undermine our democracy as a whole. Indeed, our own history has shown how the information contained in population registers can be used against citizens.

4.4. These issues are of such critical importance that we believe it makes sense to guarantee the continued independence of the Information Regulator by elevating it to the same status as other institutions that strengthen our constitutional democracy, as outlined in chapter 9 of the constitution.

4.5. This would not be unprecedented: throughout Europe, data protection agencies are granted sufficient independence to allow them to effectively exercise oversight of both government and the private sector. In South Africa, such independence would give the Information Regulator both the necessary protection envisioned by the IdMP and serve the greater purpose of protecting the constitutional right to privacy.

5. Policy gap: identity proofing & levels of assurance

5.1. The IdMP correctly identifies in 7.3 that gaps in the registration of births and the collection of biometric data create opportunities for criminal elements. Fundamentally this occurs because the information in the current HANIS may not be entirely accurate or trustworthy, leading to a loss of trust in the system as a whole.

5.2. The need for identity proofing at enrolment is well understood, and the IdMP proposes to address this via a more robust registration process. However, despite the best efforts in this regard, it is likely that there will always be some individuals for whom it is not possible to collect information reliably or first hand.

5.3. Indeed, within the higher education and research sector, the quality of identity information varies widely. For this reason, at a global level, the sector has adopted the notion of “levels of assurance” for identity proofing which provide an indication of the veracity and trustworthiness of such information. This allows service providers that consume such information to make informed risk decisions about its fitness for purpose.

5.4. In many countries, these levels of assurance are based on a national framework built within the national identity management policy. Examples of such frameworks exist in

Denmark[3], the United States of America[4], and other countries. In many cases these are based on the corresponding ISO standard[5].

5.5. TENET would strongly encourage the development of such a framework in South Africa, and its incorporation within the NIS and the IdMP. This would allow the veracity of identity information to be accurately recorded at an individual level, and help identify gaps that might need additional attention. Moreover, the adoption of a national assurance framework would go a long way to realising some of the interoperability goals envisioned by the IdMP.

TENET trusts that these submissions assist in the finalisation of the draft Official Identity Management Policy and extends its congratulations to the drafters of what is overall an excellent document.

Kind regards

Guy
Antony
Halse

Digitally signed by
Guy Antony Halse
Date: 2021.02.26
12:54:29 +02'00'

Guy Halse
Executive Officer: Trust & Identity

[3] National Standard for Identity Assurance Levels (NSIS), *Danish Agency for Digitisation*. [available online https://digst.dk/media/22920/nsis-engelsk-version-201_final.pdf]
[4] NIST Special Publication 800-63-3 Digital Identity Guidelines, *National Institute of Standards and Technology*. [available online https://pages.nist.gov/800-63-3/sp800-63-3.html]
[5] ISO/IEC 29115:2013 Entity authentication assurance framework, International Standards Organisation. [available online https://www.iso.org/standard/45138.html]