ID32b

ID32b

An innovative approach to identity

Mike McWilliams

August 2020

What is identity?

ID32b

- In the past your name was a unique identity.
  - In your village there was only one smith (metal worker) called John.
  - For reference outside the village, the village name, county and possibly even country, could be added to make this identity unique.
- With growing populations, urbanisation and globalisation there are not enough names to go round.
- We need a better system to provide a unique identity for all.

Is identity and security the same?

ID32b

- No. Identity was confused with security for technological reasons.
- Passports, identity cards, driving licences etc, as stand-alone documents, had to contain personal and security details.
- Other non-secure personal information has started to be used for security (email address, mother's maiden name, passwords). At present these provide limited security; with quantum computing they will be worthless.
- Technology has moved on – a single unique identity number can obviate the need for these documents and for on-card security. Personal and security details can be held remotely.
- Access to personal information can be restricted to "need-to-know".
- Security details can be held remotely, and if held securely, are less vulnerable to theft.

What is ID32b?

ID32b

- An integrated suite of base32 identification numbers providing unique identification for:
  - People: 8+1 code gives 1 trillion unique permutations
  - Places: 9+1 code gives 35 trillion unique permutations
  - Things: 10+1 code gives 1000 trillion unique permutations
- base32 uses all characters and digits except for I,1,O and 0 to prevent confusion (easily confused in handwriting and many fonts).
- “+1” is a check character initially set to 32; the number of permutations can be expanded by allowing other check characters.

Numbers of permutations are approximate, and allow for screening out offensive words.

Why do we need ID32b?

ID32b

- **People** need ID32b as a unique identifier that can be linked to secure biometric data (eg iris scan, face scan, finger print, voice print and dna);

- **Places** need ID32b to enable registration of precise locations for deliveries, ownership and …., especially where existing addresses or post-codes are confusing or too granular.

- **Things** need ID32b to enable blockchain, internet of things (IoT) and tracking to function.

How does ID32b work?

ID32b

- ID32b provides **people** with a unique identification number using a simple 9-character code – eg **HVG3 VC86 2**
- In decimal notation this translates to: 07 19 06 25 19 02 30 28 24
  24 is the character that is added to the sum of the other 8 characters to make the total sum divisible by 32.
- In binary notation this can be represented by a matrix:

	•		•	•		•	•	•
			•			•	•	•
•		•				•	•	
•	•	•		•	•	•		
•	•		•	•				
H	**V**	**G**	**3**	**V**	**C**	**8**	**6**	**2**

This matrix can be used to create dog tags, analogue readable cards, jewellery or even tattoos, as well as PIN cards and other digital media.

No other data needs to be held on the card, although for some low security applications a PIN may be included on “chip and pin” cards.

How do we prove identity?

ID32b

Traditional paper based	Future ID32b
Data held on paper: passports, ID cards, driving licences, credit cards, loyalty cards, parking permits, season tickets etc	No data held on cards (apart from chip and pin for low security applications). Data is held on various databases with appropriate levels of security.
Cards / passports can be stolen	Nothing to steal – ID32b only provides a link to the secure data.
Security is based on identifiers on the card, allowing forgery	Forgery is irrelevant
Insecure data used for security (email addresses, utility bills, passwords)	Security level is appropriate for the application: • Contact details: low / no security (eg phone directory) • Payments: PIN, contactless, bio-security according to value • Identification: various levels of bio-security based on importance Data security for the core biometric database is critical.

Who manages ID32b?

ID32b

- ID32b should be managed by an international entity created specifically to manage the core database. The core database will only contain ID32b numbers, biometric data and the name of the issuing authority.
- Blocks of numbers may be allocated to national or pan-national authorities that will be responsible for registration. These authorities will submit the registration details for validation that the biometrics are unique, and registration in the core database.
- As biometrics become increasingly sophisticated, new data can be added to the core database.

Registration

ID32b

- Important that each individual has only one ID32b number
- This is checked on the central ID32b core database when any new number is added, comparing finger prints, facial features and/or other biometric data as additional high security parameters are added(eg dna) .
- Other identifiers (eg name, address, licences, registrations, contact details, physical features, photographs, shopping preferences etc) are held on subsidiary databases, and the data can be changed as needed.
- Subsidiary databases can be held by different organisations (government, banks, shops, trade unions, social security, health systems, professional organisations etc) with appropriate levels of security.

Data security

ID32b

- Data security is a key requirement for the core ID32b database. This needs to have the highest level of security using encryption, firewalls, and continuously evolving techniques to prevent unauthorised access. The core database would only hold high security information that enables ID32b to be linked to its owner (eg biometric data).
- Subsidiary hardened databases can be held by other organisations, such as banks, health and social security services, national identity authorities, with their own security features.
- Other subsidiary database may link ID32b to other less confidential data, such as names, email addresses and phone numbers will minimal security.

Use of ID32b off-line

ID32b

- ID32b provides access to the full range of web-connected services through use of a single 9-digit number and an appropriate security parameter (finger-print, face scan etc).
- It also allows off-line identification:
  - A government official visiting a village with ID32b numbers and some rudimentary security (eg a fingerprint scanner on a mobile phone) to dispense financial or health support;
  - A field clinic may use ID32b to link patients to medical records and treatment.
  - A farmer may use his ID32b to label his goats or cattle (although more sophisticated systems will use the 10 character ID32b to give a unique identity to each animal).
- The opportunities are endless

ID32b for dispossessed people

ID32b

- Validation of ID32b through the core database enables identities to be confirmed, and the source of the original registration. Whether this can be linked to other data depends on the compliance of the registering authority.

- At the very least, validation of identity (linking of ID32b with biometrics) can enable a new identity to be built, with the prospect of linking it to the national registration details in due course.

Summary

ID32b

The innovative ID32b system provides:

- ability to issue a unique ID number to every individual in the world (up to 1 trillion permutations)
- 9 digit alpha-numeric number can easily be remembered and divulged
- 9th digit verifies that the number is valid (divisible by 32)
- ID32b can be represented by a 9 x 5 matric of dots, enabling dog tags, jewellery and possibly tattoos for those not literate in Roman script and Arabic numerals, and for the visually impaired.
- A single ID32b replaces all passport, ID, licence, credit card, health service, national insurance and other identity numbers.