Framework for Issuing, Using, and Validating Identification Documents

ANUPAM SARAPH, LALIT S KATHPALIA, ANAB KIDWAI, ANIRUDDHA JOSHI

Identity frauds and organised crimes are facilitated when identification documents are not based on a compelling logical framework. Unfortunately, most identification documents are issued ad hoc and through a confusion of approaches, technologies and intentions. A logically compelling framework for the issue of identity or address documents is discussed along with the consequences for the individuals, organisation, nation and the world at large when identity documents are not issued on any such framework.

Anupam Saraph (*anupam.saraph@sicsr.ac.in*), a former advisor to the Government of Goa, and Lalit S Kathpalia (*director@sicsr.ac.in*) are with the Symbiosis Institute for Computer Studies and Research, Pune; Anab Kidwai (*anab_kidwai@iiml.ac.in*), Research Associate, Indian Institute of Management Lucknow, is a PhD scholar at the Symbiosis Centre for Research and Innovation; Aniruddha Joshi (*joshiag@pun.unipune.ac.in*) is Director, Centre for Information and Network Security, Savitribai Phule Pune University.

With the world population crossing six billion and people becoming highly mobile, there is a frequent need to identify individuals. Information technology, with its spread and prowess, has increasingly been seen as a savior to identify the billions on the planet (Camp 2004; Lenter and Parycek 2015).

There have been debates and controversies over the issue of identity and address documents in almost every country in the world (London School of Economics 2005). Politics, convenience, and expediency have dominated the debate across different countries. The notion of identification has itself been confused by digital technologies to mean a hashed computer signature of some information, rather than verifying the person-defining characters of the person being identified. It is, however, widely accepted that by issuing certified documents of identification, government authorities create an "official" identity for those receiving them (Hornung and Robnagel 2010). The need for a logically compelling framework for the issue of identification documents, however, has been completely missed.

In the absence of a logically compelling framework, there can be no impartial arbitration of the identification of individuals. This raises serious concerns not only for justice and human rights, but also for the sovereign status of countries that do not use such a framework.

A logically compelling framework must cover the entire life cycle of an identity document. The life cycle of an identity document includes its issue, use, and updation. It must ensure that identification cannot be compromised, and that misuse and theft cannot just be traced, but also checked. It must ensure that the document does not replace the individual, rather empowers the individual.

1 Identity and Address Documents

Identity documents used for identification need to have logically compelling, and therefore legally valid, means to arbitrate identity disputes by impartial third parties. There is, therefore, a need to outline a logical framework for the issue, use, and validation of identity documents. Such a framework not only establishes a best practice, but also allows evaluation of our existing identity or address documents for their usefulness, usability, and validity.

There are six parts in all during the three phases of the issue, use and validation during the life cycle of an identity document or address documents. These parts constitute a logically compelling framework for identification documents.

1.1 Issue of Documents

The first step (Table 1) is identifying an individual and verifying his or her identity and/or address. Unless individuals are identified, they cannot be issued an identity document. It could also be issuing an identity or address document based on the identification and certifying the identification. Unless identity documents are certified, they do not guarantee they were issued after due identification.

Table 1: First Step

Issue
– Identification
– Certification
Use
– Authentication
– Regulation
Validation
– Audit
– Updation

1.1.1 Identification

Identification requires confirming that the information provided matches the individual being identified. This not only requires the presence of the person being identified, but also the ability to verify that the features used to identify the person are comparable with the information about these features.

The information about features for identification could be self-identification by the individual, a document based on identification of the individual based on third-party documents, or an introduction based on identification by third parties who have already been identified.

In the case of self-identification, the document serves as a shortcut to introductions where the risks of high trust are minimal. Visiting cards are an example of a self-identification document. Passports, tax numbers, driver's licence, utility service bills, and election ID cards are examples of using third-party documents to verify the identity (or address) of an individual. Identification using such documents is carried out by matching the identification information on the documents with the individual.

Verifying documents is not verification of identity. These documents shift the liability of identity (or address) information to the organisations who have issued the documents. Having bank account holders introduce new customers is an example of introduction from persons already holding an identity document requested by the individual. In this case, the liability of identity (and address) information rests with the introducer. The verification of an address can be additionally established through a postal delivery to the address of a form to be duly signed and returned.

1.1.2 Certification

In high trust environments it may be unnecessary to certify the identification process. However, when identification documents are to be issued for third parties to rely on, the identification process has to be certified, and the liability fixed on the person and agency that has certified the identification.

Certification establishes that identification or the process of verification of the identity (or address) of the individual has taken place. It provides the assurance that identification of the individual as required by the standards of the certifying agencies has already taken place. It, therefore, becomes convenient for the certifying agency to use this to identify the individual, without requiring a more elaborate process again.

The certified document is usually for its own use, but is sometimes meant to certify the identity, affiliation, or address of the individual to others. For example, other parties use our passports to issue visas or travel documents to us. The use of identity or address documents by third parties is based on their trust of the identification process used by the certifying agency. Usually, the certifier would be legally liable for erroneously or fraudulently certifying identity (or address). Documents that are not certified by the issuing individual or agency are neither valid nor useful. They cannot serve to establish a proof of identity (or address).

1.2 Use of Documents

The third step is providing a means to authenticate the identity or address document. Authentication provides a means to ensure that the identity or address document is genuine. The fourth step is providing a scheme to regulate the use of the identity or address document. Schemes for regulating the use of the document reduce the risk of its misuse by third parties, and safeguard the identity holder. Such schemes can also help track misuse, were it to occur.

1.2.1 Authentication

To serve to identify individuals or their addresses, documents need to be authenticated as genuine. Those that cannot be authenticated or validated as genuine fail to inspire confidence. Authentication establishes that the certification is genuine. Attestation by third parties has been one way, although incorrect, to certify the genuineness of documents.

The ability to query the issuer of a document for its genuineness is a better way to verify its genuineness. It is easier for a certifying agency to establish the authenticity of its own certified document. Using own documents rather than third-party documents to identify individuals reduces risk.

If identity documents are used without identification and authentication, it is possible for third parties to impersonate others. If identification is skipped, impersonators can submit documents that may be authentic, but belong to someone else. If authentication is skipped, impersonators can submit documents that are not issued by the certifying party, yet claim it is so.

1.2.2 Regulation

Identity documents are reused. It is important to ensure that they cannot be used by any third person(s) who come to possess them. Identity theft results from the successful use of an identity document by third person(s) to pass off as the identified person. It is therefore necessary to be able to regulate the use of the identity document, and ensure its use by third person(s) can be traced back in the remote event that it happens.

To reduce the risk of an identity (or address) document being used by impersonators, it can provide the individual a means to authorise use of a document for identification and authentication. This is usually done by requiring consent through two or more independent channels. Popular additional channels include cell phones, emails, or phone-based calls. For example, many banks require a one-time password to be sent to the registered cell phone or email ID to complete an online transaction. Many credit card providers call the individual to confirm their high-value transactions before clearing them. The individual can also be provided access to a log of the individuals or organisations that were granted access to identify and authenticate the individual. For example, Google provides a log of devices and locations from which your user ID was accessed.

1.3 Validation of Documents

The fifth step is an independent third-party audit of the identity or address documents issued and the logs of the use of these documents. A third-party audit establishes trust in the identity or address document. The sixth step

allows the identity or address attributes that change to be added to the identity document. The ability to update the document ensures its validity.

1.3.1 Audit of Documents

To ensure that the process of identification has taken place before the documents are issued, organisations subject their documents to an audit. Such an audit ensures that the document can indeed find and identify the individual it claims to identify. To ensure that the use of the document can be regulated, organisations subject their processes of generating usage logs to the audit.

Such third-party, independent audit helps establish confidence in the documents issued by an individual or organisation. First, the audit establishes that the issuer has indeed identified and verified the individuals and the addresses to whom these documents have been issued. Second, it establishes that these documents have been used only after due authorisation and that it is possible to minimise and track any impersonation.

1.3.2 Updation

Identity attributes are not static and constant. Both demographic and biometric information change with time. Sometimes erroneous information is corrected. An identity document needs to be cancelled when a person dies. All modifications of the original document transform the identity document. These changes need to be traceable so that it becomes difficult to hack, hijack, or destroy identities.

For example, identity or address attributes such as name or residence can change with marriage or through other legal processes. A thorough identity document would allow for every change to be verified (as in the first step) and appended to the document itself. The change trail on the document will capture full information on identity transformations, if any.

2 Discussion and Further Research

In India, an array of official documents can be used for identification, and many others are typically accepted as documents of address.[1]

These have not been evaluated for the processes involving their issue, use, or validity. The logical framework described here provides a basis to evaluate these documents, and ensure that their issue, use, or validation does not compromise the identity of an individual or of the nation. It provides a means to ensure that the human rights of individuals are not compromised. It also ensures that justice will not be prevented in the event of identity documents being stolen, misused, or fraudulently created or used.

The logical framework also provides a basis to design processes for issuing, using, and updating identification documents. Using this framework ensures identification of individuals without compromising their rights, and fixes liabilities. It ensures investigating identity frauds and delivering justice to the aggrieved.

Identification documents serve the purpose of the individuals identified and the agencies that identify them. They are, therefore, a contract between the identified and the identifier. It is the responsibility of those who issue identification documents to ensure the issue, use, and validation will be restricted to this implicit contract. Therefore, identification documents can only be designed in the context of the use to which the agency or the individual issuing them will need them.

3 Conclusions

The six-step process provides a compelling logical framework for the issue and use of identification documents. Practising these six steps provides a basis for impartial arbitration of the identification of individuals. It ensures justice to those who may lack an identity, be the victims of identity crimes or even protect persons from violations of their human rights. It also protects the country from losing its democratic or sovereign status.

Good governance requires that identity documents do not become an end in themselves, but serve the needs of those identified. Good governance requires that identity documents do not expose any person to risks they cannot protect themselves from. It also requires that identity documents are able to protect the independent status of the country.

Using a single identification document across different agencies, in contrast to multiple independent documents issued by different agencies, exposes the individual to complete identity failure across agencies via a single point of failure. This also exposes the country to failure of databases that ensure its democratic or sovereign status.

Good governance, protection of human rights, and upholding justice require that the six-step framework is followed by any identity solution.

NOTE

1 Passport, the PAN Card, Ration/PDS Photo Card, Voter ID, Driving Licence, Government Photo ID Cards/service photo identity card issued by PSU, NREGS Job Card, Photo ID issued by Recognised Educational Institutions, Arms Licence, Photo Bank ATM Card, Photo Credit Card, Pensioner Photo Card, Freedom Fighter Photo Card, Kissan Photo Passbook, CGHS/ECHS Photo Card, Address Card having Name and Photo issued by Department of Posts, Certificate of Identity having photo issued by Gazetted Officer or Tehsildar on letterhead, Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations, and Aadhaar number are used as identification documents.
Passport, Bank Statement/Passbook, Post Office Account Statement/Passbook Ration Card, Voter ID, Driving Licence, Government Photo ID cards/service photo identity card issued by PSU, Electricity Bill (not older than 3 months), Water bill (not older than 3 months), Telephone Landline Bill (not older than 3 months), Property Tax Receipt (not older than 3 months), Credit Card Statement (not older than 3 months), Insurance Policy, Signed Letter having Photo from Bank on letterhead, Signed Letter having Photo issued by registered Company on letterhead, Signed Letter having Photo issued by Recognised Educational Instruction on letterhead, NREGS Job Card, Arms Licence, Pensioner Card, Freedom Fighter Card, Kissan Passbook, CGHS/ECHS Card, Certificate of Address having photo issued by MP or MLA or Gazetted Officer or Tehsildar on letterhead, Certificate of Address issued by Village Panchayat head or its equivalent authority, Income Tax Assessment Order, Vehicle Registration Certificate, Registered Sale/Lease/Rent Agreement, Address Card having Photo issued by Department of Posts, Caste and Domicile Certificate having Photo issued by State Government, Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations, Gas Connection Bill, Passport of Spouse, Passport of Parents, and UID number are typically accepted as documents of address.

REFERENCES

Camp, Jean (2004): "Digital Identity," IEEE Technology and Society Magazine.

Hornung and Robnagel (2010): "An ID Card for the Internet: The New German Card with 'Electronic Proof Of Identity,'" *Computer Law and Security Review*, Vol 26, No 2, pp 151–57.

Lenter, Gabriel M and Peter Parycek (2015): "Electronic Identity (eID) and Electronic Signature (eSig) for eGovernment Services: A Comparative Legal Study," *Transforming Government: People, Process and Policy*, Vol 10, No 1, pp 8–25.

London School of Economics (2005): "The Identity Project," www/lse.ac.uk/management/research/identityprojectreport.pdf.