Chapter

09

National Identity System

Why it is important: Everyone has the right to be recognized as a person before the law, as enshrined in Article 6 of the Universal Declaration on Human Rights and several other international human rights instruments. Legal identity is widely recognized to be fundamental to the exercise of human rights and to benefit from numerous government and private sector services. As such, the 2030 Agenda for Sustainable Development, agreed by all UN Member States in September 2015, established a specific target within the Sustainable Development Goals (SDGs) – Target 16.9 – to establish “legal identity for all, including birth registration, by 2030."[1]

[1] United Nations, Principles of Legal Identity in the Context of the 2030 Agenda for Sustainable Development, New York, September 2018, p. 1.

Introduction

This chapter provides best practices for national identification registration and management of a national identification system. A national identification system is a foundational identification system that provides national IDs - often in the form of a card - and potentially other credentials. Foundational ID systems provide general identification and credentials to the population for public administration and a wide variety of public and private sector transactions, services, and derivative credentials.[2] Foundational ID systems are therefore distinct from functional (sector specific) ID systems, which are created for a particular service or transaction - such as driver and vehicle registration, voting registration, tax administration, and social and transfer programs. Countries may maintain many functional ID systems and issue associated functional identity credentials.[3] In addition, there may be privately issued ID credentials. This chapter addresses a country's national identification system, with a focus on the integration of that system with the civil registration system.[4]

1. Universality

Best Practice: The ability to prove one's identity is fundamental to the exercise of human rights as well as to benefit from government and private sector services. Therefore, as with civil registration, proof of identity should be provided without discrimination or distinction, including discrimination based on geography; racial, ethnic or religious group; status as a member of a nomadic, indigenous, native or aboriginal population; status as displaced, stateless, refugee, asylum seeker, or person of undetermined nationality; or status as a foreign national born in the country, temporary or migrant worker, or any other immigrant; or any other characteristic. Regardless of the type of identity credential issued, it must be legally valid and be sufficient documentation to gain access to rights and services to which the individual is entitled.[5]

While some form of proof of identity must be available to all, a national identity card or other credential is not necessarily compulsory. Country practices vary on whether registering for and obtaining a national identity card or other credential is mandatory, voluntary, or even available. In countries that do not issue a national identity credential, other forms of identification are issued for sectoral purposes (for example, passport, driver's license, etc.) and can be used as proof of identity.[6] In all cases, some form of proof of identity should be available to all persons within the territory of a country without discrimination.

Guidance: Describe whether some form of national identity document or credential is compulsory or available for all persons within the country. Consider all forms of discrimination that may take place, including geography; racial, ethnic or religious groups; nomadic, displaced, native or aboriginal populations; refugees or asylum seekers within the country; foreign nationals born in the country; temporary or migrant workers, or any other immigrant; or any other characteristics. Describe whether different forms of identity documents are provided for different populations (for example, a national ID card for citizens and an immigration card for non-citizens). In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

---

a. Is some form of identity credential available and provided for all, regardless of:

[2] ID4D, ID Enabling Environment Assessment, World Bank, 2018, p.9.

[3] ID4D, ID Enabling Environment Assessment, World Bank, 2018, p.10.

[4] For a broader discussion on all types of ID systems, as well a guide to assessing those systems, see ID4D, ID Enabling Environment Assessment, World Bank, 2018, available at: http://id4d.worldbank.org/legal-assessment.

[5] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 436.

[6] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, Para. 47.

Geography (for example, remote areas)? ____ Yes____ No

Race, ethnicity, religion, gender? ____ Yes____ No

Nomadic, displaced, native or aboriginal population? ____ Yes____ No

Nationality, residency, or refugee/ asylum status? ____ Yes____ No

Other characteristics? ____ Yes____ No

Citation:

Comments:

b. Are different forms of identity documents or credentials provided for different populations?

____ Yes____ No

Citation:

Comments:

2. Enrollment in National ID credential program: Information collected and age of enrollment

Best Practice: Registration for an identity credential entails enrolment in the identity credential system and validation of identity. Enrolment involves capturing and recording key identity attributes from a person who claims a certain identity, which generally includes biographical data (e.g., name, date of birth, sex, etc.), and may include biometrics.[7]

The Information captured at enrollment should be guided by the principle of proportionality and necessity - the principle that personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing. (See Chapter 10, Data Protection and Personal Privacy). If biometrics are collected, the law should state the type of biometrics collected, including any limitations or constraints on the type of biometrics that may be collected and how they are collected. In addition, because biometrics may be hard to capture on certain individuals (for example, manual laborers or the elderly may have worn fingerprints that cannot be captured clearly and iris scans may be difficult to capture on people with cataracts), there should be back-up measures in place for those individuals whose biometrics cannot be used in the system.[8]

There is no best practice for the age of enrollment for a national ID credential. In many countries, particularly those that use biometrics, the age of enrollment is typically between the ages of 15 to 18 years because it has been difficult to reliably capture biometrics on the very young. However, this is changing as biometric technology improves. Regardless of the age at which enrollment is permitted or required (in systems where ID registration is mandatory), enrollment should also be permitted later in life, including for those who immigrate into the country as adults.[9]

Guidance: Describe the biographical information and biometrics, if applicable, captured at enrollment. If biometrics are collected, state any limitations on biometric collection and describe any back-up procedures for individuals whose biometrics cannot be captured or used in the system. State the age of

[7] *Technical Standards for Digital Identity*, World Bank, 2017, page 3.

[8] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 443 - 446.

[9] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 444.

enrollment and whether there are enrollment procedures for those who immigrate or otherwise enter the country after the age of enrollment. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Information collected (biographical and biometric, including any back-up procedures):

Citation:

Comments:

b. Age of enrollment and procedures for later enrollment:

Citation:

Comments:

3. Validation: Birth Registration as basis for ID registration

Best Practice: Once a person has claimed an identity during ID credential enrolment, their identity is then validated by checking the attributes presented against existing data,[10]including data in the civil register.

The civil register should be the underpinning of a person's civil identification record. If there is no formal linking of the civil register and identity register, there are limited means to confirm the identity of those registered in the national identity system.[11] In addition, national identification systems, which generally enroll people at older ages, cannot ensure that children's rights and services are properly supported through legal identity at birth or provide up to date data on this segment of the population for planning purposes.[12] Therefore, for those born in the country, proof of birth registration should be required in order to register for a national ID. For those born in the country that lack birth registration, the process of ID credential registration should concurrently facilitate delayed birth registration.[13] If refugees, migrants, stateless persons and other persons born outside the country do not have legally valid birth certificates from their country of origin, they should be provided alternative means to validate their identity and obtain identity credentials.[14]

Guidance: Describe how identity is validated during identity credential registration. Specifically, state whether proof of birth registration (e.g., a birth certificate) is required in order to register for an identity credential. If a person born in the country lacks birth registration, state whether birth registration is facilitated during identity registration. Describe the process for identity registration for migrants, refugees, asylum seekers, stateless persons and other foreign nationals. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

[10] *Technical Standards for Digital Identity*, World Bank, 2017, page 4.

[11] Principles of Legal Identity in the Context of the 2030 Agenda for Sustainable Development, Working Paper of the Identification for Development Programme – Series 1, United Nations, September 2018, paragraph 10.

[12] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 61.

[13] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 447.

[14] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 62.

a. Describe how identity is validated for ID registration (including whether birth registration is required).

Citation:

Comments:

b. For those born in the country that lack birth registration, is delayed birth registration facilitated concurrently with ID registration? If yes, describe.

Citation:

Comments:

c. Is there a process for ID registration for migrants, refugees, asylum seekers, stateless persons and other foreign nationals? If yes, describe.

Citation:

Comments:

4. UIC assignment

Best Practice: As discussed in Chapter 4, Section 10, for those born in the country in which a UIC is used, a UIC should be assigned at birth. However, if the assignment of a UIC at birth is a new requirement in a country, many people will have been born before the requirement comes into effect. In addition, there will be people that immigrate into a country. These people will not have had an opportunity to receive a UIC at birth.[15]

Therefore, legislation may require all individuals permanently residing within the territorial jurisdiction of the country, who were not previously assigned a UIC, to apply for a UIC by a certain age. For those not previously assigned a UIC, a UIC may be assigned at the time a person registers for a national ID credential. In countries that use a UIC, a UIC should not be denied based on citizenship, nationality or residency status, as it does not confer citizenship or any specific legal rights.[16]

Guidance: For those who have not previously been assigned a UIC, state whether a UIC is assigned during ID credential registration. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

[15] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 440.

[16] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 440.

a. UIC assigned during ID credential registration for those who have not previously been assigned a UIC?
______ Yes _______ No.

Citation:

Comments:

5. Information available from credential

Best Practice: Common types of digital identity credentials fall into three categories: 1) something you know (e.g., a password), 2) something you have (e.g., an ID card, mobile phone or a cryptographic key), or 3) something you are (e.g., a fingerprint or other biometric data).[17] Various types of technology may be used with these types of credentials. For example, an ID card may record a digital cryptographic key and/or biometric on an embedded computer chip or may have an encrypted 2D barcode containing a person's personal data and biometrics, either instead of or in addition to a chip. Mobile devices may have SIM cards with digital certificates. In some cases, identifying information (such as UIC and biometrics) may be stored in the cloud and a physical credential may not be issued.[18]

Regardless of the type of credential, it is important that confidential information and information that may make an individual vulnerable to discrimination not be displayed on the face of the credential (in the case of an ID card) or be obtainable from the credential (e.g., chip, SIM technology) by those who have no legitimate interest in the information. Only limited information is necessary on the face of, or available from, the credential, particularly if a credential has biometrics, a PIN, or other authenticating method associated with it.

Because a UIC is used to access services, it should be closely guarded and protections put in place to protect against its unauthorized use. Placing a UIC on the face of an ID credential creates a risk and it is therefore recommended not to place the UIC on the face of ID credential. However, if a UIC is presented on the face of an ID credential, a second type of authentication (such as biometric match) should be required in order to use the UIC.

Guidance: Describe the type of credential and technology used. Describe what information is accessible to individuals and service providers presented with the credential as a form of identity authentication. State whether this information includes confidential or sensitive information. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

____

a. Credential and technology used:

Citation:

Comments:

b. Information available from the credential (including whether UIC is on the face of the credential):

[17] *Technical Standards for Digital Identity*, World Bank, 2017, page 4.

[18] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 451.

Citation:

Comments:

6. Credential validity and renewal process

Best practice: The period of validity of ID credentials varies from country to country and may be dependent on the type of credential. For example, the Indian Aadhaar system uses only a UIC and biometrics, which never expire. However, in many countries that use an ID card with a photo, the ID card must be renewed with a new photo or other biometric capture periodically. The renewal of an ID card or credential does not, however, imply that the UIC should be changed. As stated previously, a UIC is assigned for life.[19]

Guidance: State the period of validity of the national ID credential. Describe any renewal process. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

____

a. Period of Validity of national ID credential and renewal process:

Citation:

Comments:

7. Authentication

Best practice: Authentication is the process of verifying the claimed identity against the registered identity information;[20]in other words, proving a person is who they say they are. Authentication should not be confused with "authorization", which involves determining whether a person has a right to a particular service.[21]

Authentication may occur using one or more factors that, like credentials, generally fall into one of three categories—something you know, something you have, something you are.[22] Authentication using these attributes can occur through various pathways. For example, a person with a smart card may also need to key in a Personal Identification Number (PIN), or match their fingerprints to those contained in a chip. A person using a mobile phone app may authenticate by use of a PIN, biometrics or a mobile signature. A cloud-based system (like India's Aadhaar system) might rely on biometrics for authentication.[23]

[19] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 459.

[20] *Technology Landscape for Digital Identity*, World Bank, 2018, page 6.

[21] *Technology Landscape for Digital Identity*, World Bank, 2018, page 7.

[22] Other types of information, such as location data or device identity, may be used by an verifier to evaluate the risk in a claimed identity, but they are not considered authentication factors. Grassi, P., et. al, NIST Special Publication 800-63-3, *Digital Identity Guidelines*, page 12.

[23] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 461.

All systems are vulnerable to failure. Biometric authentication can sometimes fail to recognize an individual, even though they are who they say they are. A person may forget their PIN. Authentication failure might result in a risk of exclusion from key services. Therefore, no matter what type of authentication process is adopted, there should be alternative authentication procedures in case of authentication failure, such as mobile one-time password (OTP), alternative biometric, or authentication by a local authority.[24]

Guidance: Describe the authentication process used with a national ID credential. Describe any alternative procedures in case of authentication failure. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Authentication process and alternative procedures in case of authentication failure:

Citation:

Comments:

8. Retirement of Legal Identity

Best practice: Retirement of legal identity - including deactivation of a UIC and identity credential - upon death is important in order to prevent fraudulent use of the deceased's identity. An efficient and effective connection between the civil registration system and the identity management system is the best way to ensure that this deactivated occurs, through the transfer of death record information from the civil registration system to the identity management system. There may be other reasons for deactivation of a UIC or identity credential during a person's life, such as fraudulent use of the identity.[25]

After deactivation of a UIC and identity credential, identity records should be retained and permanently archived. Country practices vary on the reuse of a UIC after closure. In some countries a UIC is never reused; in others a UIC is not reused for at least 50 to 100 years after the person's death.[26]

Guidance: Describe whether and how a legal identity (including a UIC, if applicable, and national ID credential) is retired upon death and for any other circumstances. Specifically address if there is an obligation for death registration information to be transferred from the civil registration authority to the national identity management system. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

---

a. Process and circumstances for retiring a legal identity (including UIC and ID credential):

Citation:

Comments:

[24] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 462-463.

[25] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 464.

[26] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para 465.

9. Fees and Resources

Best practice: There is no best practice regarding charging a fee for identity credential registration and credential issuance. Many countries charge a fee. However, if obtaining an identity credential is mandatory or essential for individuals to benefit from basic services, policy makers should consider providing the original identity credential free of charge or for a minimal fee. In addition, there should be a process for a fee waiver for those who cannot afford the fee. Fees may be charged to replace a lost identity credential.[27]

Public and private sector entities benefit from the authentication services provided by the identity management system. Therefore, some countries charge a fee to these entities for authentication services. Country policies vary on whether to charge government entities - such as the health care system, social services, and others - a fee for authentication services. In some countries, the identity management authority charges other government entities a fee for this service. In other countries, there is a policy of providing this service to other government entities free of charge. Private institutions, such as banks, that wish to use the identity management system authentication services generally are charged a fee.[28]

Any revenue generated by the identity management system should be retained to fund the system rather than going to the central treasury.[29]

Guidance: State the amount of fees charged to individuals for issuance of an identity credential, including fees for an original, renewal and duplicate credential. State the amount of fees charged to institutional users of authentication services, including government and private sector entities. State whether fees generated by the identity management system are retained to fund the system. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Fees charged to individuals for ID credential issuance (original, renewal, duplicate):

Citation:

Comments:

b. Fees charged to government and private sector users of authentication services:

Citation:

Comments:

c. Is revenue generated by the identity management system retained to fund the system?

[27] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para 467.

[28] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 468.

[29] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 211.

Citation:

Comments: