National Office for Identity Data
*Ministry of the Interior and Kingdom Relations*

# Identity Management in 2030

# Content

# Foreword

In the past decades, the pace of development has increased in the field of identity management. Governments have realized that identity management is crucial to their operations and that a reliable identity infrastructure is a precondition for a successful implementation of identity management. But changes, especially in the digital domain, are so fast that further development and improvement of the identity infrastructure is a constant topic of attention and sometimes of concern to governments.

The number of countries that issue electronic passports and electronic identity cards and also offer electronic services to citizens is growing rapidly. The questions that arise here are: what is the impact of these developments on identification and ID verification, on the documents and tokens, on the application and issuance processes, on document control, on the instruments to be used and on their interoperability? These questions are not only of concern to governments, but they are also embedded in the TRIP Strategy established by the ICAO in 2013.
In July 2015, The Dutch National Office for Identity Data organised an 'Expert Meeting Identity Management 2030' in The Hague, during which international experts shared their experience and knowledge of identity management and discussed the future of identity infrastructure. The present white paper deals with the outcome of the experts' meeting. The paper will be of particular interest to officials and policymakers in governments responsible for sections of the identity infrastructure. Identity management is a vital part of my office responsibilities. I therefore warmly recommend this paper to you.

Director, National Office for Identity Data,
Ministry of Interior and Kingdom relations
The Netherlands

**Gerdine Keijzer-Baldé**


Expert
Meeting
Identity
Management 2030

# Introduction

**This paper is the outcome of a two-day 'Expert Meeting on Identity Management 2030' held on July 1st and 2nd 2015. The meeting was organised by the Dutch National Office for Identity Data (RvIG) at The Hague in The Netherlands and supported by the International Civil Aviation Organisation (ICAO). It involved the active participation of 36 international experts[1] in the field of ID[2] management. Most of the participants were representatives of public, national and international organisations. About a third of them came from the Netherlands, a sixth from European countries, a quarter from African, American, Asian and Oceanian countries and another quarter from international organisations.**

The objective of the meeting was to exchange knowledge and experience and to explore directions for ID management for the coming 15 years.

This document has been written to look forward to the situation as it will be in 2030, therefore most of the topics are introduced by the sentence: 'In 2030…'. It attempts to answer the questions addressed in the foreword and to summarise the key points made by the experts during the discussions, as captured by the organizers of the meeting. Nevertheless, they are not to be understood as agreed upon outcomes by the meeting participants and responsibility for the content lies exclusively with the author. After this introduction, the paper is structured in 5 chapters:

2 Concepts and infrastructures
3 Technology and data
4 Roles and processes
5 Directions
6 Conclusion.

[1] *Listed at the end of the document.*

[2] *Hereinafter referred to as ID management: the acronym ID stands for "identity".*

# 2 Concepts and infrastructures

## In 2030, the concept of identification is relative, quantitative and dynamic

In 2030, general acceptance has been reached on the fact that identity can be approached but not completely established, and that no conclusive proof of identity exists [1-2]. As a result, evidence of identity is used to challenge the hypothesis of identity during the core ID management processes of creating, checking and ending identities, rather than proving identity. The concept of absolute, qualitative and static identification, promising binary and error-free statements of identity independently of the scenario, technology and circumstances, has given way to a more realistic concept of identification as relative, quantitative and dynamic. Evidence of identity allows to differentiate between individuals and to recognize people to a certain degree. The degree of recognition depends on the scenario (e.g. identification in a closed set of 10 individuals is easier than in an open-set of 500 million people), on the information available at the time of the identity check (e.g. a full set of 10 complete fingerprints is an information of higher quality than a low quality face picture) and on prior knowledge about identity (e.g. more information is available for an already known individual than for completely unknown people).

In 2030, the public, private, national and international organisations operating ID management infrastructures no longer aim towards establishing processes capable of identifying individuals absolutely, uniquely and definitely in any scenario and any circumstance. The ID management processes exploit official but also public, restricted, structured and unstructured sources of information to quantify the evidence of identity contained in the information retrieved. Once quantified, this evidence of identity is combined with prior knowledge about the identity already available in the ID management infrastructures to produce informed decisions about the identity of people. The organisations are conscious that error rates are inevitably associated with binary decisions of identification or identity verification. These error rates are quantified and monitored, and the decision trade-offs in the ID management infrastructures are adapted to master the risks and costs associated with errors.

## In 2030, the foundation of ID management is revisited

In 2030, National Civil Registration Authorities (NCRAs) exist in every country and are in charge of ID management at the national level for their authorities, public organisations and private partners. The International Identity Management Organisation (IIMO) has been created and the NCRAs recognize it as the international harmonization and coordination body in the field of ID management. The IIMO supports the vision of a global identity [3] based on the trusted ID information of the NCRAs rather than on information from breeder documents, as breeder documents were found to be unreliable, as pointed out by the OSCE at the end of 2013: *'It was stressed that currently there are no reliable figures on how many travel documents are issued to fraudsters who have either forged breeder documents or applied for travel documents by abusing other weaknesses in the civil registry process'* [4].

One role of the IIMO is to guide the NCRAs towards recommended practices for all organisations developing and operating ID management infrastructures, whether they are public, private, national or international. Recommended practices aim at improving the operational efficiency of processes, at harmonizing the procedures and at offering friendly and secure environments to the users and operators interacting with ID management infrastructures. Through recommended practices, the IIMO also pursues the goal of establishing a common basis in terms of ID data, ID management infrastructure and processes amongst the NCRAs. Such a common basis is a prerequisite for the IIMO to fulfil its role of international coordinator of the NCRAs, managing their international requests and delivering them trusted ID information.
At a national level, the digital ID infrastructures of the NCRAs and their databases containing the personal and biometric data are centralized. The NCRAs, conscious of the limited robustness of such centralization, have requested the expertise and guidance of the IIMO to ensure the long-term sustainability of their own and of the global ID management infrastructure. The solution proposed by the IIMO and adopted by the NCRAs consists in creating a decentralized backup of the data of each NCRA on the infrastructure of the other ones using cloud-computing technology, compliant with the data protection and privacy regulations. This dynamic backup system has a cost, in terms of storage and processing time for synchronization, but it offers the critical advantage of enabling the reconstruction of the databases of any NCRA in case of loss.

## In 2030, digital ID infrastructures take over the paper-based processes

In 2030, the NCRAs have migrated from paper-based to digital infrastructures to manage their ID processes. The benefits are remarkable. The digital ID infrastructures

allow for a comprehensive traceability of the activities of the people involved in the identification processes, operators and users, and of the interactions between different ID infrastructures. This traceability enables a level of transparency beneficial both for operational efficiency and security, promoting accountability of the NCRAs and all the organisations operating digital ID infrastructures for their actions and decisions.

Digital ID infrastructures are also an opportunity for the NCRAs to extend their offer for trusted ID management services, not only to public and international organisations but also to private partners requesting tailor-made physical and digital identification and identity verification solutions. For the NCRAs, such public-private partnerships are a source of revenues that can be reinvested to maintain, improve or even replace their ID infrastructures. Such trusted ID management services are a concrete means to secure the electronic transactions underlying online trading of products, services and resources, ranging from the retailing of commodities like food, clothing or electronics, to the preclearance of airlines passengers, from distant health care services including the prescription and the controlled retailing of drugs, to distant learning and research programmes including access to online examination sessions, scientific literature and restricted research databases. A common interest such as security proves to be a powerful incentive for public and private partners to collaborate and perform optimally.

In 2015, the 'Happy Flow' project jointly runs by the Netherlands and KLM in Aruba offers an example of such a collaboration that has smoothly enabled compliance with the UN Security Council Resolution 2178 on 'threats to international peace and security caused by terrorist acts': *'Aruba Happy Flow is a process in which the passenger is only required to show his or her passport once at the airport. The use of facial recognition then allows the passenger to proceed to check-in, drop off baggage, pass border control and board the aircraft, all without being asked to show a passport or boarding pass again. The pilot scheme, according to Aruba Airport, is "unique in the world and has been designed to streamline the passenger process, making it fast and secure". The move could be significant in enhancing commercial dwell times, potentially offering a boost to retailers'* [5].

The interoperability of the core ID management processes of the NCRAs has followed a staged implementation, first bilateral, then regional and finally global. The early adopters of digital ID infrastructures have applied a trial and error process to achieve the implementation of basic interoperable functionalities between their digital ID infrastructures. In a second stage, implementation at regional level has led to an extension of the range, the security and the performance of the interoperable functionalities and to refine and harmonize the procedures in order to achieve a basic recommended practice. This basic recommended practice has been the source for the IIMO to develop more elaborate recommendations and

guidance and to establish specifications and standards in the field of ID management, in collaboration with the NCRAs. The IIMO which, since its creation and development, has expanded its leadership role and gained recognition for its harmonization and coordination roles; has been instrumental in reaching interoperability of ID management on a global scale, and in a time frame compatible with the urgency and the scale of the challenge of the global migration phenomenon observed in the first part of the twenty-first century. This success overcomes past missed opportunities in the development of international ID management.

In the late 1990s, Malaysia had pioneered the development of the first electronic passport. The designers included in the document an electronic chip containing one biometric modality (face) and later a second one (face and fingerprint). They also developed and implemented an ID verification infrastructure for Automatic Border Controls (ABCs) in the form of autonomous gates, without the need for a central database. Unfortunately, the Malaysian government couldn't benefit from ICAO specifications as currently prescribed in ICAO Doc 9303. At the time, ICAO had not yet established specifications for the digital storage and use of personal and biometric data in electronic chips for ID management purposes. Later, this lack of specifications led to the need for a complete redefinition of the concept of the Malaysian electronic travel document, in order to fulfil the ICAO specifications developed *a posteriori*, unfortunately without input of the knowledge, the experience and the technological and management solutions developed during the Malaysian project. Luckily a lot has been learned from this experience.

In 2030, digital ID management processes integrate the flexibility of a relative, quantitative and dynamic identification process, and they also benefit from an significant quality improvement resulting from the global networking of the ID infrastructures and the widespread automation of the identity control processes. One of the consequences of the migration from isolated paper-based to connected digital ID infrastructures is the phenomenon of net-widening in the detection of ID fraud and minor irregularities, reducing drastically the grey zone of tolerance between legal and illegal identity [6]. Political discussions take place to solidify a new balance between rigorous process and flexibility for digital ID management, and when agreed upon, decisions will be enforced technically and administratively by the NCRAs.

# 3 Technology and data

## In 2030, data integrity is managed and assessed

In 2030, the NCRA of every country offers efficient and trusted ID management services, compliant at the same time with recommended practices of the IIMO and with the regulations on data protection and privacy. The enrolment process consists for the NCRAs of attributing a Unique Personal Number (UPN) that accompanies all new born people from birth to death. This UPN is linked to the biometric and personal data containing evidence of identity for these people. At the time of birth, the data collected are the usual set of data requested for enrolment (date of birth, first name, name, gender, home address). This initial set of data is enriched over the course of an individual's lifetime with other official data including changes in home address or marital status. But the official set of data is also enriched with structured and unstructured data collected from public or restricted sources, and used for identification and identity verification under the condition that they comply with data protection and privacy regulations, that their integrity can be assessed and that they contain some evidence of identity.

The use of personal and biometric data available online, particularly on social networks, is not new. It has been used for a long time in the forensic context. For more and more people, a large variety of pictures of their face can be found online and a lot of these pictures appear to be more recent and of far better quality than the official ones present in their ID documents. What is new in 2030, is the fact that NCRAs accumulate evidence of identity across the entire lifespan of individuals, and that they assess the integrity of these data to improve the reliability and the security of their ID management processes. In this context, biometric data play a significant role in providing evidence (or not) of the same individual in time and in reinforcing (or not) the link between the personal data, the UPN assigned by the NCRAs and THE individual to which this number has been assigned at birth.

## In 2030, a large variety of biometric technologies are mature

In 2030, ID management processes are implemented following a problem-oriented approach and are not only technology

| | Origin Identity | Use Identity | Identity Check | End Identity |
|---|---|---|---|---|
| Registrations | Civil registry | Passport | SLTD | |
| Documents | Breeder | ID & Travel | Fraud | Destroying documents |
| Processes | | | Verification identity | |
| Expertise | | | | |

driven. Biometric solutions are no longer implemented following the incremental pace dictated by innovation. They are considered critically and chosen only when no alternative solution fulfils the requirement for integrity and performance of the identity chain. Such a chain is typically encountered in complex processes of civil registration, where the challenge is common to multiple NCRAs to maintain the evidence of identity in a time span of the several decades that comprise an average human life, or in air transportation, where the challenge is to maintain the evidence of identity in real time at any place on the planet reachable by an airplane.

In 2030, a large variety of biometric technologies are robust and adaptable to the conditions of everyday life scenarios and therefore suitable to be implemented in ID management processes. These technologies are developed according to the recommendations, specifications and standards of the IIMO to ensure compliance and interoperability by design. Most of these technologies are efficient enough to recognize people in large sized populations, and some are even scalable to distinguish the entire world population, particularly when used in combination.

Any use of personal and biometric data is privacy sensitive, and a key factor to gain user acceptance is to reinforce trust in the security of the ID management processes embedded in the biometric technologies. One solution consists of integrating the concept of privacy by design at each step of the development and implementation of the technology and processes in the digital ID infrastructures, the inspection tools and the tokens containing the electronic chip storing the personal and biometric data digitally. For example, the concept of privacy by design requires the examination of the possibilities and limits of cryptography to combat the tampering, the cloning and the revocability of such tokens. And when integrated in a digital ID infrastructure, the concept of privacy by design facilitates the demonstration of the compliance of such infrastructure with the data protection and privacy regulations, in revealing the existence of a privacy chain and highlighting its coherence.

The IIMO also recommends the integration of ergonomics in the design of the technologies and processes relating to a digital ID infrastructure, in order to enhance usability, soften, streamline and speed up operations, while improving user acceptance and maintaining or even increasing security. Ergonomics plays a crucial role in achieving identity controls that operate dynamically and without constraint for the individuals whose identity is checked, for example during the (dis)embarking operations of airline passengers.

In 2030, the tokens storing digitally the personal and biometric data are designed to be multipurpose and cost-effective and their form factor is left to the discretion of their owners. Most people opt for having it in their mobile phone, their smart watch or their interactive glasses, but other usual accessories like rings, earrings or cuff links are common choices as well.

Particularly sighted users even choose to have several tokens, each of them being a backup in case of loss, technical failure or theft. Radio Frequency Identification (RFID) microchip implantation is another mature technology, but its spread is still limited in 2030 due to its invasiveness for users as well as its tagging aspect recalling some inglorious historical precedents. In this respect, biometric technology remains a non-invasive solution for identification and a credible alternative to the use of microchip implants.

## In 2030, biometric solutions are chosen based on fit for purpose

In 2030, commercial off-the-shelf (COTS) technology is available for a wide variety of biometric modalities, ranging from instantaneous genetic profiling to contactless fingerprint recognition, and from long distance iris or face recognition to body odour or body movement coordination recognition. The NCRAs are aware of the strength and weaknesses of these different technologies and modalities, and they take advantage of this knowledge to select and implement them selectively in their processes. Some modalities, like DNA, fingerprint and iris are stable enough in time to provide evidence of the same individual over a period as long as a human lifespan and distinctive enough to allow scalability up to the world population. When used in combination, these are the modalities of choice for civil registration, securing the link between an individual, its UPN and its personal data. These modalities are also chosen for activities requiring a fast and high level of identification, for example, in law enforcement or a military environment.

The NCRAs collaborate with public organisations and private partners to propose to them solutions tailored to the environments in which they are deployed and to provide an adequate level of evidence of identity while remaining practical and balanced from a data privacy point of view. Activities like accessing online digital resources or air transportation are limited in time and take place in less controlled environments. Therefore, they can exploit biometric modalities that are less stable in time and more balanced from a data protection and privacy perspective, like the face. Airlines and authorities involved in air transportation value biometric recognition solutions that can be operated dynamically and without constraint for the passengers, for example combining the capture by tracking (from far away) and recognition of the face and of the coordination of body movements.

The combination of several modalities is an essential parameter for the implementation of biometric technology in the ID management processes, in order to reach a sufficient degree of universality in operational conditions.
A vast majority of people are easily recognised by the biometric technologies implemented in practice, but for most of these technologies, certain individuals remain difficult to recognise (goats), or easy to impersonate (lambs) or are successful in impersonation (wolves), as described by George Doddington in his famous biometric zoo [6].

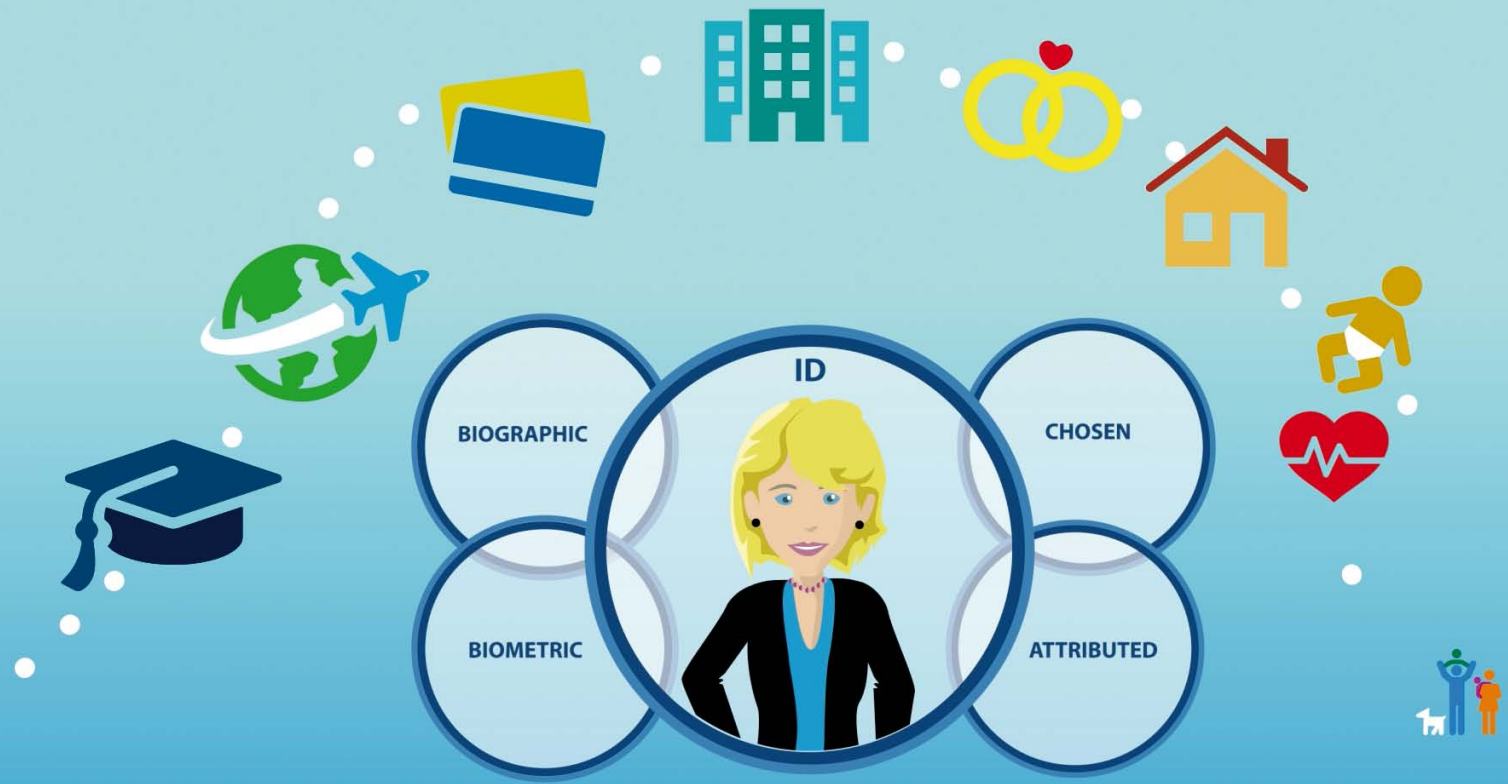
# 4 Roles and processes

## In 2030, roles and mandates regarding ID management are clarified

In 2030, the NCRAs are in charge of, and responsible for, at a national level, the ID management policy, the implementation of digital infrastructures supporting ID management processes compliant with recommended practices and making trusted ID management services available digitally to users, public and international organisations and private partners. The NCRAs focus in particular on the following tasks: the enrolment of individuals, the management of the identities including the integrity of the personal and biometric data, the security and logistics of the tokens (issuance, control and destruction), the ID control and ending the identities. The NCRAs fully exercise their national sovereignty in fulfilling these prerogatives, but the challenge consists of fulfilling them in harmony with international recommendations, specifications and standards of the IIMO.

The IIMO is the guarantor of the availability of a trusted digital ID infrastructure at an international level, ensuring the scalability, the interoperability and the integrity of ID management processes (enrolment, control and end), of the tokens and of the personal and biometric data used. These requirements of scalability, interoperability and integrity are necessary for the IIMO to fulfil its role of international coordinator, managing the international requests of the NCRAs and of all the other public or international organisations and private partners operating digital infrastructures and managing ID processes. These organisations are active, *inter alia*, in the fields of migration (e.g. the International Organisation for Migration – IOM), of transportation (e.g. the International Civil Aviation Organization – ICAO and the airline companies), of tourism (e.g. the United Nations World Tourist Organisation), of law enforcement (e.g. Interpol) and more generally in the fields of international trading and business (e.g. import-export companies, credit card issuance companies and other financial institutions).

Due to its leading role in the field of international civil air transportation, the ICAO was historically *de facto* in a central position, providing guidance, standardization and coordination at a global level in the field of ID management,


ID
BIOGRAPHIC
CHOSEN
BIOMETRIC
ATTRIBUTED

before the creation of the IIMO. The creation of the IIMO has offered the opportunity for the ICAO to refocus on its core business regarding ID management. In 2030, the ICAO concentrates on guidance, standardization and coordination in the field of air transportation in order to mitigate the risks linked to ID management activities in this field. More generally, the international bodies involved in ID management operate similarly, concentrating on their area of activity and interacting with the IIMO for guidance and coordination of the ID management between areas of activity.

## In 2030, there is balance between privacy and trust

In 2030, technology-driven data protection and privacy regulations are in place globally. Their enforcement increased the trust of citizens and users regarding the organisations managing ID processes. The regulation focuses particularly on the ownership, collection, custody and the processing of the personal and biometric data. At national, regional and global levels, mechanisms are in place to foster swift legislation to oversee, and if necessary to address through legal means as may be required, the rapid and sometimes undesirable developments in ID technology and ID management.

In 2030, the IIMO has set up an accreditation system as a quality management tool to accredit the public, private, national and international organisations operating digital ID infrastructures and managing ID processes. The aim is to certify the competence of their staff, to assess the compliance of their data, technology and processes with the regulations and to assess the validity, reliability, neutrality and the impartiality of the collection, custody and processing of personal and biometric data.

Concretely, these quality management activities are organised and supervised jointly by the NCRAs and by the National Accreditation Bodies (NABs). They are performed nationally for national organisations and regionally for international organisations. The international Standardisation Organisation (ISO) and the IIMO are also involved, providing the framework of standards and specifications necessary for quality management.

## In 2030, there is balance between control and facilitation

In 2030, substantial experience of managing ID processes has been accumulated by the NCRAs and all the other public or international organisations and private partners operating digital ID infrastructures. The information related to the traceability of events and to decisions that have been made are of particular interest to establish a balance between control and facilitation in operation, knowing why, when, who and what to be checked (and not to be

checked). This information is used to monitor the mobility of people and their access to services and benefits, with the aim to improve and streamline the service but also to detect threats linked to irregular immigration, public health or security. This information also helps to determine if and for whom controls can be anticipated and performed remotely. For example, border preclearance processes are intended to streamline border procedures on the spot. Finally, a traveller's health and travel history, financial record, criminal record (or absence thereof) and even the content of their luggage are potentially informative of their intentions.

# 5 Directions

**In 2015, after the expert meeting, a series of directions were identified for the identity (ID) management progressing towards 2030:**

**IDENTIFICATION**
The concept of identification will evolve from an absolute, qualitative and static definition of identification relying on a proof of identity, towards a relative, quantitative and dynamic definition of identification relying on evidence of identity

**NCRA**
In each country, a National Civil Registration Authority will be created to develop efficient and trusted ID management services based on a Unique Personal Number (UPN), informative and integer data, and will comply at the same time with the recommended practices of the IIMO and data protection and privacy regulations

**IIMO**
The Identity Management Organisation will be created to harmonize and coordinate ID management at a global level and support the development of digital ID infrastructures within the National Civil Registration Authorities (NCRAs)

**TRUST**
The IIMO will support the vision of a global identity chain growing the trusted ID information of the NCRAs and no longer based on the ill-trusted information of breeder documents

**DIGITAL**
Digital ID infrastructures will replace paper-based processes and allow for NCRAs to align their operational efficiencies to the challenges arising from a rapidly-growing and more mobile population and to cope with the amplification of the migration phenomenon, desired or forced, for personal, economical, political, religious, climatological or other safety reasons

**CHAIN**
ID management is integrated more and more into complex processes operated in parallel by multiple organizations, whether they be public, private, national or international. None of them will master the complete identity chain. The quality and integrity of this chain will only be achieved by collaboration and cooperation between NCRAs and the IIMO.

**BIOMETRICS**
A large variety of biometric technologies will reach sufficient maturity to be implemented in practice, but a set of minimum common criteria needs to be defined to achieve a general acceptance for biometric ID management. The combination of several modalities is an essential parameter for the implementation of biometric technology in ID management processes, in order to reach a sufficient degree of universality in operational conditions.

**TOKEN**
The tokens storing the personal and biometric data digitally are designed to be multipurpose and cost-effective, and their form factor is left to the discretion of their owners

**PRIVACY**
The enforcement of data protection and privacy regulations and the accreditation of the organisational operating digital ID infrastructures will enhance the trust of citizens and users regarding ID management.

**BALANCE**
A new balance between efficiency and flexibility for digital ID management is discussed at the political level and when agreed upon, decisions will be enforced technically and administratively by the NCRAs.

# 6 Conclusion

The 'Expert Meeting on Identity Management 2030' offered the opportunity for 36 international experts in the field to exchange knowledge and experience and to explore directions for identity management for the coming 15 years. A rapidly growing number of countries issuing electronic ID documents raised a series of questions, not only of concern to governments but also embedded in the TRIP Strategy established by the ICAO in 2013, about the impact of these developments:

- What is the impact on identification and ID verification?
- What is the impact on documents and tokens?
- What is the impact on application and issuance processes?
- What is the impact on document check?
- What is the impact on the instruments to be used and on their interoperability?

These questions were debated during 2 days, focusing on the concept of identification and ID infrastructure, on biometric and digital technology and data and on the role of the different organisations and authorities in the ID management processes. This conclusion summarizes the key points made by the experts, as captured by the organizers, in the form of a series of assumptions relating to the state of identity (ID) management in 2030, as they can be perceived in 2015, after the expert meeting.
The concept of **identification** will evolve towards a relative, quantitative and dynamic definition of identification relying on evidence of identity; an **International Identity Management Organisation** will be created to harmonize and coordinate ID management at a global level; in each country, a **National Civil Registration Authority** will develop efficient and trusted ID management services based on **Unique Personal Numbers**; a global identity chain will grow from **trusted** ID information and not from the ill-trusted information of breeder documents; quality and integrity will only be achieved in the identity **chain** by collaboration and cooperation; the enforcement of data protection and **privacy** regulations will be crucial to increase trust regarding ID management; a set of minimum common criteria needs to be defined to achieve a general acceptance of **biometric** technology in ID management; **tokens** will be multipurpose and cost-effective and integrated in widely accessible objects and finally, a new balance between efficiency and flexibility for digital ID management is discussed at the political level.

# A word of thanks

The National Office for Identity Data would like to thank the participants for their valuable contributions to the 2015 Expert Meeting Identity Management 2030.

We would like to express our appreciation to the government experts from Australia, Belgium, Botswana, Canada, Estonia, Hong Kong Special Administrative Region, New Zealand, Portugal, Tanzania, The Netherlands, United Kingdom, United States of America, Switzerland and to the delegates from the Dutch Association of Civil Service, Core Group ID fraud (UNODC), European Commission, IATA, Interpol, IOM, ISO, OSCE, Universities of Twente and Utrecht and UNWTO.

We would especially like to thank Jim Marriott, Deputy Director Aviation Security and the facilitation of the International Civil Aviation Organization for the generous support and Prof Dr Didier Meuwly, the author of this white paper.

# References


1 Meuwly D. and Veldhuis, R.N.J., *Forensic Biometrics: From two communities to One Discipline*, Proceedings of the BIOSIG 2012, International Conference of the Biometrics Special Interest Group - (BIOSIG). 2012. p. 207-218.

2 Meuwly D.; *Identity and its Value*, in F. Knopjes and D. Ombelli (Eds), The Developer's Toolkit, IOM and Via Occidentalis. 2008. p.171-193.

3 Grijpink, J. H. A. M. *Chain Communication Systems*. Journal of Chain-computerisation, 2014, 5, Art # 2.

4 Organization for Security and Cooperation in Europe (OSCE), *Addressing the Link between Travel Document Security and Population Registration/Civil Registration Documents and Processes*. Office for Democratic Institutions and Human Rights (ODIHR) – Expert Roundtable, Warsaw, Poland, 26-27 November 2013. 5p.

5 Davitt, D. *Aruba Airport Launches 'world First' Scheme to Ease Passenger Journey*. The Moodie Report.com. January 6, 2015, Moodie International edition.

6 Doddington, G., Liggett, W., Martin A., Przybocki, M., and Reynolds D.. *Sheep, Goats, Lambs and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation*. DTIC Document, 1998.

7 Brown, Alison P. *Anti-social behaviour, crime control and social control*. The Howard Journal of Criminal Justice. 2004. 43.2, p.203-211.

# List of participants

| Country | Participant |
|---|---|
| Australia | Anne Moores |
| Belgium | Bart Vrancken |
| Botswana | Neo Lepang |
| Canada | Caitlin Imrie |
| Estonia | Viktor Kaljukivi |
| Hong Kong Special Administrative Region | Raymond Lok |
| New Zealand | Dion Chamberlain |
| Portugal | Luis Gonçalves Leitão |
| Tanzania | Viktoria Lembeli |
| | Sokolo Sam Kaseko |
| The Netherlands | Jacqueline Rutjens |
| | Renee Ong |
| | Frans Rijkers |
| | Wim Schepers |
| | Rob Koster |
| | Jasper Mutsaers |
| | Fred Jacob |
| | Diana van Driel |
| | Cynthia Henskens |
| | Gerdine Keijzer-Baldé |
| | Fons Knopjes |
| United Kingdom | Chetan Patel |
| United States of America | Bill Seaman |
| Switzerland | Roman Vanek |

| Organization | Participant |
|---|---|
| **International Organizations** | |
| Dutch Association of Civil Services | Dagmar Winkelhorst |
| UNODC Core Group ID fraud | Anko Blokzijl |
| European Commission | Silvia Kolligs-Tuffery |
| IATA | Chris Hornek |
| INTERPOL | Maria Tibulca |
| ICAO | Jim Marriott |
| IOM | Florian Forster |
| ISO/IEC JTC1 SC17 WG3 | Tom Kinneging |
| OSCE | Simon Geignan |
| UNWTO | Dirk Glaesser |
| **Universities** | |
| University of Utrecht | Jan Grijpink |
| Netherlands Forensic Institute | Didier Meuwly |

National Office for Identity Data (RvIG)

Ministry of the Interior and Kingdomrelations
Turfmakt 147 | Postbox 10451 | 2501 HL The Hague
info@rvig.nl | www.rvig.nl

T + 31 (0)88 900 10 00