One ID Glossary

V5.0

Edits to this One ID Glossary follows the 2020 expansion of the One ID Technology Document's annex on Terminology that was agreed within the One ID Task Force early 2018, then updated in August 2019, in January 2020 and July 2022 to be able to adopt the same terminology while discussing and producing documentation around One ID. This version is correct as of January 2026.

The terminology in this glossary will be constantly revisited and updated if need arises, and as this will inform the development of the messaging standard, some definitions will need to be agreed and approved as final with no further edits.

Contents

Admissibility

- The permission granted to a person to enter a State by the public authorities of that State in accordance with its national laws.

Alternative process

- A process that does not include biometrics handling and may include manual verification of identity claims against physical documents.

Application Program Interface (API)

- An application programming interface is a connection between computers or between computer programs. A document or standard that describes how to build or use such a connection or interface is called an API specification.
- A web service within the IATA Common-Use Web Services (CUWS) standard which is used to identify an individual using a captured biometric.
- Contextual information and/or metadata may be provided in the Identify Request to reduce the size of the dataset (using a gallery or equivalent) for improved performance and accuracy.

Attestation

- Validations from a third party that a claim made is true, can be device stored as verifiable credentials.

Binding

- The passenger enrolled identity is securely linked/bound to the associated metadata to ensure that the retrieval of the appropriate and accurate data is possible throughout the touchpoints. Sometimes referred to as 'association'.

Biometric-capable touchpoint

- Biometric-capable touchpoint is a touchpoint that has the capacity to capture real-time biometric data and process it for the purpose of facilitating contactless travel.

Biometric Enrollment

- Binding one or more biometrics (face, fingerprint, iris, etc.), that have been captured and authenticated, with correlating flight data and storing securely for later matching. The passenger is then enrolled for identity verification and/or identification via biometric recognition at a biometric touchpoint.

Biometric matching

- One-to-one (1:1): is a system that compares one new biometric to one enrolled/registration biometric in order to make a match.
- One-to-few (1:n or 1:few): is a system that compares one new biometric against a subset sourced from the 'many' enrolled, based on defined criteria e.g., passengers cleared as 'ready to fly' within a defined time period or pulled into the database at first airport touchpoint.
- One-to-many (1:N) is a system that compares one new biometric to all enrolled biometrics.

Biometric handling system

- A system that uses biometric data (such as facial recognition, fingerprint scans, or iris recognition) to automate and streamline various processes. This technology enhances security, improves operational efficiency, and provides a smoother passenger experience by replacing manual identity verification with automated biometric checks at different points, such as check-in, security screening, and boarding.

Biometric recognition

- Capturing an individual biometric for instant **identity verification (1:1) or identification (1:n)**
- This is included in the identity verification and identification terminology.

Centralized Database

- This refers to a model where the data is maintained and stored in a single physical location (database).
- In a centralized environment, one node does everything with processing involving a message and response through one system.

Claim

- As defined by World Wide Web Consortium (W3C), [1] an assertion made about a **subject**.

Credential

- A credential is any document in paper or digital form that the passenger may be required to possess and/or share data from to demonstrate the admissibility to travel. It may have been issued by an airline, government authority, or other 3rd party authorized to issue credentials.
- Attributes, tokens or documents showing that a person is entitled to or has a right to exercise a claim to an identity

  As defined by W3C, a set of one or more claims made by an issuer. A **verifiable credential** is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects.

Consent

- Consent requires that individuals (data subjects) not only be actively informed that their data is being collected and for what purpose, but that they provide by a clear affirmative and explicit action agreement to the processing of any personal data where necessary according to the local or applicable regulations.
- Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes which by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.

Data Controller/Data Processer

- For the purposes of One ID this EU definition will apply.

[1] W3C Verifiable Credentials Data Model v1.1

Decentralized Database

- A decentralized database is an environment where the data is stored on systems that are geographically located at different locations but not linked through a data communication network.

Decentralized Identifier (DID)

- As defined in W3C[2], a DID is a globally unique persistent identifier that does not require a centralized registration authority because it is generated and/or registered cryptographically. The generic format of a DID is defined in the DID Core specification.

- A specific DID scheme is defined in a DID method specification. Many—but not all—DID methods make use of distributed ledger technology (DLT) or some other form of decentralized network.

- A portable URL-based identifier, associated with an entity. These identifiers are most often used in a verifiable credential and are associated with subjects such that a verifiable credential itself can be easily ported from one repository to another without the need to reissue the credential.

Decentralized Identifier Document

- Also referred to as a DID document in W3C Verifiable Credentials, this is a document that is accessible using a verifiable data registry and contains information related to a specific decentralized identifier, such as the associated repository and public key information.

- Also referred to as a DID document in W3C Verifiable Credentials, this is a document that is accessible using a verifiable data registry and contains information related to a specific decentralized identifier, such as the associated repository and public key information.

Derived Verifiable Identity

- A self-derived digital identity credential created using an existing authority-issued identity or travel document, such as passport.

Digital Identity

- Digital identity is a term used broadly and can have different interpretations depending on the context or use. In general terms, digital identity is a set of electronically captured and stored attributes and credentials that can uniquely identify a person.
- For the purposes of One ID, digital identity covers biographic and biometric information of the passenger. It can also include their Digital Travel Credential (DTC), authenticated eMRTD data, existing travel authorizations (Visa, eVisa, ETA, ESTA etc.), and possibly other documents necessary to the facilitation of the passenger (vaccinations, minor handling forms, arrival cards, etc.)
- Binding the digital identity to the DTC or the eMRTD using biometrics enables a persistent trusted digital identity. This, combined with verifying the DTC or eMRTD as genuine and unaltered, provides confidence that the passenger links to this digital identity.

[2] W3C Decentralized Identifiers (DIDs) v1.0

Digital Identity Enrollment Service

- In the context of One ID, a Digital Identity Enrollment Service is used by passengers who have opted in to using their digital identity credentials to process the personal information required for travel.
- The Digital Identity Enrollment Service provider will assess the information presented and, once satisfied that the presenter of the information is the legitimate owner, will then provision one or more verifiable credentials to the passenger's digital wallet, enabling them to selectively disclose verifiable identity attributes when required to access a service.
- A Digital Identity Enrollment Service application is ideally integrated into the passenger preferred user interface for travel booking and management, e.g., the application that the passenger uses to book their flight and manage their trip. Most likely to be an airline, alliance or travel agent/aggregator, loyalty program, etc.
- This is on the passenger's device, which is known as a user agent, e.g. smart phone.

Digital Signature

- A digital signature refers to a cryptographic code that is generated and authenticated by public key encryption. This code is then linked to any document or credential and can then be used to verify its contents, and to identify the issuer and the holder.
- As defined by ICAO[3], digital signatures are unique and can be verified using their respective certificates (Country signing Certificate Authority – Document Signer Certificate). A digital signature refers to the result of a cryptographic operation enabling the validation of information by electronic means.
- As defined by W3C[4], a digital signature is a mathematical scheme for demonstrating the authenticity of a digital message.

Digital Travel Credential

- The (proposed) Digital Travel Credential (DTC) is a digital representation of a passenger's travel document that meets the standards and specifications set by ICAO. [5] It contains both the biographic and biometric information of the holder, either derived directly from the e-MRTD (DTC type 1 known as eMRTD-Bound) or issued by the issuing authority (DTC type 2, known as eMRTD-PC Bound, and 3, known as PC-Bound).
- Data is digitally stored in a globally consistent and secured manner (Logical Data Structure or LDS) to enable interoperability.
- Through identity document authentication, any inspecting authority can determine that the data has not been tampered with; and that it has been put there by a legitimate authority and can also use the contained biometric for 1:1 matching against the holder.
- The DTC is always a hybrid, with a Virtual Component (**DTC-VC**) and a Physical Component (**DTC-PC**) that can act as a physical authenticator when a scenario requires this. In the case of the DTC type 1, the physical authenticator is the ePassport that the DTC-VC is derived from. In types 2 and 3, the DTC-PC is a device in possession of the holder, such as a smart phone.

Digital Wallet

- Digital Wallet is an application that securely stores Verifiable Credentials, in such a format that the holder of the Digital Wallet can present or selectively disclose required data to any verifying party, such as to demonstrate admissibility to travel to an airline. Verifiable Credentials can be issued to the passenger's digital wallet by an airline, government authority or other 3rd Party authorized to issue.

[3] ICAO Security and Facilitation ePassport Basics
[4] W3C Verifiable Credentials Implementation Guidelines 1.0 - Terminology
[5] ICAO doc 9303 Machine Readable Travel Documents

- A repository in the secure hardware of a device (such as a mobile phone) that stores and protects access to holders' verifiable credentials.
- Can also refer to a secure cloud based repository that a holder can chose to store their credentials in and then interface with from a device.

Distributed Database

- A distributed database is where the data is not stored on a single logical database, but rather is installed on a set of computers that are geographically located at different locations and linked through a data communication network.

Distributed Ledger

- A distributed ledger is similar to a distrusted database where data is stored, shared, and synched across multiple locations however has no central administration.
- A Blockchain is a type of distributed ledger.
- Defined by W3C as a distributed database in which the various nodes use a consensus protocol to maintain a shared ledger in which each transaction is cryptographically signed and chained to the previous transaction.

Enrol

- To register for biometric processing at selected touchpoints at the airports

False acceptance

- When a biometric system incorrectly identifies a person based on the biometric presented or incorrectly authenticates a biometric presented against a claimed identity. This is common with twins, for example.

False rejection

- The failure of a biometric system to identify a person by the biometric presented or to verify the legitimate claimed identity of a presented biometric. For example, this can occur when a facial image has been dated given a person's change with age.

Gallery

- Collection of biometric data (e.g., image(s) or template(s)) of passenger(s) along with an identifier that can be linked with passenger's journey details that may be held in a local IDMS.

Holder

- As defined in W3C, a role an entity might perform by possessing one or more verifiable credentials and generating verifiable presentations from them.
- For One ID, the passenger is the holder.
- A holder is usually, but not always, a subject of the verifiable credentials they are holding. Holders store their credentials in credential repositories

Identification (Identify)

- Capturing and matching a live biometric representation of a passenger with an enrolled biometric through 1:N, against all known biometrics or 1:n, against a subset of known biometrics (e.g. a gallery).

- This confirms that this is the same person as the enrolled individual, during subsequent process steps.
- Note: for the purposes of One ID, 1: n (few) is preferred as it is both faster and less prone to errors with false acceptance or false rejections than 1:N (all).

Identity

- The means for keeping track of entities across contexts. Digital identities enable tracking and customization of entity interactions across digital contexts, typically using identifiers and attributes. Unintended distribution or use of identity information can compromise privacy. Collection and use of such information should follow the principle of data minimization.

Identity Authentication

- Capturing and matching a live passenger biometric with the biometric stored in a registered identity document, token or credential, through a process of 1:1 biometric matching.
- This ascertains that the passenger is who they say they are and through the process can bind the digital identity to the passenger through matching the biometric stored on the authority issued identity document, token or credential.

Identity Document

- Any document which may be used to identify a person or verify aspects of a person"s personal identity. If issued in a small, standard credit card size form, it is usually called an identity card. Some countries issue formal identity documents, while others may require identity verification using informal documents. When the identity document incorporates a person"s photograph, it may be called photo ID.

Identity Document Authentication

- Usually referred to as ePassport validation, this is the Border Authority process of validating the authenticity and integrity of an electronic Machine-Readable Travel Document (eMRTD) by verifying the digital signature on the chip to confirm that the information stored on the chip was written to the chip by the proper authority and has not been altered or tampered with.

Identity Management System (IDMS)

(note: this is sometimes referred to as Identity Management Platform in existing One ID implementations)

- A service that manages the identity information needed for the facilitation of passengers throughout their journey, such as on-airport control points where biometric identification and/or access authorization is required. Commonly referred to as an IMP in One ID implementations, trials and pilots e.g. local on- airport database for the **temporary** management of the **minimum** identity information necessary to facilitate such as bag drop, security, exit/entry border control, and boarding.
- It can be managed by a single stakeholder, such as an airport, or it could be managed by a collaboration of connected stakeholders (e.g. local airport stakeholders or an airline alliance.)
- For One ID implementations, the ISO/IEC definitions for a framework for identity management[6] applies. Therefore, an IDMS mechanism comprising of policies, procedures, technology and other resources for maintaining identity information (including associated metadata).

[6] ISO/IEC 24760-1:2019 IT Security and Privacy - A framework for Identity management - Part 1: Terminology and concepts

- An identity management system is typically used for identification, verification or authentication of entities. It can be deployed to support other automated decisions based on identity information for an entity recognized in the domain for the identity management system

Identity Provider

- An identity provider, sometimes abbreviated as IdP, is a system for creating, maintaining, and managing identity information for holders, while providing authentication services to relying party applications within a federation or distributed network. In this case the holder is always the subject. Even if the verifiable credentials are bearer credentials, it is assumed the verifiable credentials remain with the subject, and if they are not, they were stolen by an attacker. This specification does not use this term unless comparing or mapping the concepts in this document to other specifications. This specification decouples the identity provider concept into two distinct concepts: the issuer and the holder.

Identity Registration (Identity Establishment)

- Prior to the travel journey, approved authority establishes identity based on evidence, and issues a persistent physical or virtual token (e.g., e-passport; other government issued secure token, etc.).
- This involves biometric registration with the approved authority.
- Identity establishment is the civil registration process of verifying and associating identity attributes with a person, which can then enable one or more biometrics (face, fingerprint, iris) to be stored securely for later matching through enrolment into an identity management system.
- Identity establishment relies on three principles:
  1. Identity is genuine (exists and is a living person)
  2. Presenter links to Identity (confidence that the identity is unique to the authority's system and the presenter is the sole claimant and not an imposter)
  3. Presenter uses the claimed identity (confidence of the presenter's consistent use of this identity)
- NB: Refer ICAO Guidance on Evidence of Identity

Identity Verification (Verify)

- Identity verification is the process of confirming a biometric claim; e.g., from an ICAO eMRTD, through comparison of a biometric sample; e.g., the facial image captured in a touchpoint.
- In One ID, this would happen when a passenger is matched directly to their enrolled biometric that is bound to their flight data as opposed to 1:n identification against a gallery. This is most likely to occur in an exception handling process.

Inadmissible

- A passenger who is refused admission to a country by authorities of such country, or who is refused onward carriage by an airline or government authority at a point of transfer, e.g. due to lack of a visa, expired passport, etc.
- As defined by ICAO in Annex 9[7], a person who is or will be refused admission to a State by its authorities.

[7] ICAO Annex 9 Facilitation

Issuer

- As defined in W3C, a role an entity performs by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. Example issuers include governments, corporations, non-profit organizations, trade associations, and individuals.

Machine Readable Travel Document (MRTD)

- As defined by ICAO, an MRTD is an Official document, conforming with the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine.
- An eMRTD (electronic MRTD) is a passport, visa or ID card that has a contactless integrated circuit (chip) embedded in it and the capability of being used for biometric identification of the holder in accordance with the standards specified in the relevant Part of Doc 9303.
- Sometimes abbreviated to 'travel document' or simplified as 'passport' in One ID documents.

Machine Readable Zone (MRZ)

- As defined by ICAO, an MRZ is the fixed dimensional area located on the MRTD, containing mandatory and optional data formatted for machine reading using Optical Character Recognition (OCR) methods.

Mobile Driver's License (mDL)

- Digital version of a physical driver's license stored on a mobile device, such as a smartphone. It contains the same information as a traditional driver's license but can be updated in real-time and offers enhanced security features

Metadata

- Metadata is data information that provides information about other data.
- It can be used for discovery and identification, or to manage and organize data structures and relationships, permissions, and processes, and for statistical and analysis purposes.
- An example in One ID could include information about the biometric such as file size, the date and location the file was created, and gallery stored or held in.

Multi-Modal Biometrics

- An authentication technology using different biometric technologies such as fingerprints, facial features, and vein patterns in the identification and verification process.
- As a multi-biometric system captures more than one type of biometric for enrolment, it improves the accuracy in authenticating or verifying identity.
- In addition, where a person is not able to provide one of the biometric features, they can still enroll the second biometric feature and are therefore enrolled with at least one biometric to enable a seamless travel experience.

Operational Framework

- An operational framework (sometimes also called a trust framework or liability framework) is a set of specifications, rules, and agreements that govern a multi-party collaboration established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements.

Opt out

- An action a passenger takes to request their registration to be removed from a biometric system.

Passenger Data Set

- The passenger data set refers to all the necessary digital identity information, and the flight information (similarly to current API flight information). It may include additional process information (e.g. record of the passenger's transaction through a touchpoint. Note: This data is decentralized and not stored as a complete set.

Presentation Attack Detection

- The automated task of determining whether the attempt at being recognized by a biometric recognition system is being made by a genuine person and not an artefact (mask, video, bit etc.) attempting to fool the system into a false acceptance. It is often referred to as liveness detection.

Presentation

- As defined by w3c. Data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier. A **verifiable presentation** is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but do not contain, the original verifiable credentials (for example, zero-knowledge proofs).

Privacy by default

- Data protection by default requires you to ensure that the only data processed is the data that is necessary to achieve the specific purpose.
- Privacy by default solutions ensure that data needs are specified before the processing starts, individuals are appropriately informed and only the data needed for the purpose is processed.
- It does **not** require adoption of a 'default to off' solution.

Privacy By design

- Quoting the privacy Regulator in the UK, privacy by design means integrating or 'baking in' data protection into processing activities and business practices, from the design stage right through the lifecycle.

- In Privacy by Design solutions, data controllers must put technical and organizational measures - such as pseudonymization in place – to minimize personal data processing.

Pseudonymization

- Pseudonymization is a de-identification/depersonalization process by which personally identifiable data fields are replaced by one or more artificial identifiers, or pseudonyms

Proof

- Authentication or verification that act as the evidence for a claim, such as a Digital Travel Credential (DTC), ID card, a mobile drivers license, etc.

Ready to Fly

- The passenger has "confirmed" or "standby" status for the flight and, if confirmed, has assigned seating.
- Where applicable, the authenticity of the passenger's identity has been validated [is this passenger who they say they are?]
- Where applicable, the authenticity of the identity document/credential has been validated [is the credential genuine and has it not been tampered with?]
- The passenger's admissibility has been validated [is the passenger authorized to travel to destination?]
- The passenger is biometrically enrolled such that (s)he can be biometrically recognized at subsequent touchpoints (optional).

Selective Disclosure

- The ability of a holder to make fine-grained decisions about what information to share.

Self-Sovereign Identity

- As with digital identity, Self-Sovereign Identity is used broadly depending on the context, and as such is difficult to define.
- For the purposes of One ID, Self-Sovereign Identity implies that the passenger has sole ownership of their digital and analog identities, and control over how their personal data is shared and used.
- This adds a layer of security and flexibility allowing the identity holder to only reveal the necessary data for any given transaction or interaction.

Subject

- As defined in W3C, an entity about which claims are made. In many cases the holder of a verifiable credential is the subject, but in certain cases it is not. For example, a parent (the holder) might hold the verifiable credentials of a child (the subject).

Touchpoint

- Physical location/device where a passenger can claim access to a restricted area or claim entitlement to service.

Travel Authorization

- Travel authorizations are one aspect of the entry requirements defined as per the legislation of the departure, destination and transit countries. Guidance principles will vary for pre-travel authorizing and verifying a passenger's acceptance to a country. When meeting the current acceptance and verification requirements, a passenger's authorization to travel to a State can be granted. Refer to Admissibility/Inadmissibility.

Unique Identifier (UID)

- An identifier, comprising, for example, a set of random or serial numbers, hash functions, codes, or names, which is guaranteed to be unique among all identifiers used for those objects and for a specific purpose
- In many use cases, a single object can have more than one unique identifier each of which is used to identify it for a different purpose or audience.

User Agent (Wallet Agent)

- As defined in W3C, a program, such as a browser or other Web client, that mediates the communication between holders, issuers, and verifiers.

Verifiable Credentials

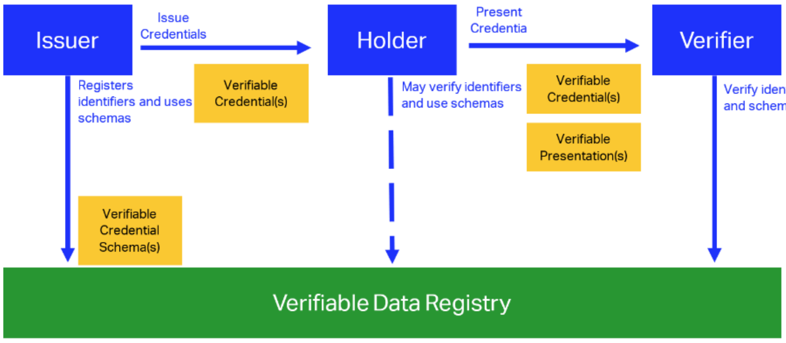
- Verifiable Credential is a credential in a digital form. Examples of credentials and data contained in credentials include
    - Biographic and biometric data from the passport or other identity document
    - Visas, travel authorizations and residence permits
    - Health-related status, contact tracing information (such as Passenger Locator Form –PLF),digital arrival declarations
    - Other captured verified biometrics (such as a face image or 'selfie')
    - Passenger's itinerary

- As defined in W3C, a verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.

- Holders of verifiable credentials can generate verifiable presentations and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics.

- Both verifiable credentials and verifiable presentations can be transmitted rapidly, making them more convenient than their physical counterparts when trying to establish trust at a distance.

- Based on the W3C model for the roles and information flows that form the basis for the Verifiable Credential specifications:


Issuer
Issue Credentials
Holder
Present Credentia
Verifier
Registers identifiers and uses schemas
Verifiable Credential(s)
May verify identifiers and use schemas
Verifiable Credential(s)
Verifiable Presentation(s)
Verify identifiers and schemas
Verifiable Credential Schema(s)
Verifiable Data Registry

Verifiable Data Registry

- As defined in W3C[8], a role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials. Some configurations might require correlatable identifiers for subjects. Some registries, such as ones for UUIDs and public keys, might just act as namespaces for identifiers.

- Some configurations might require correlatable identifiers for subjects. Example verifiable data registries include trusted databases, decentralized databases, government ID databases, and distributed ledgers.

- Often there is more than one type of verifiable data registry utilized in an ecosystem.

[8] W3C Recommendation Verifiable Credentials Data Model v1.1

Verifier (Verifying party)

- Verifying party is the party which requests, for legitimate business purposes, the presentation of the Verifiable Credentials. An example is an airline that requires proof that the passenger has the necessary documents required by the authorities for their travel. The verifying party can, subject to business and regulatory requirements, request all the data contained in the Verifiable Credentials, a subset of that data or simply proof that the Verifiable Credential is in the passenger's possession. The verifying party should check that the credentials authentic. This includes checking that it conforms to the specification, was issued by the appropriate issuer and has not been tampered with.
- As defined in W3C, a role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation, for processing. Example verifiers include employers, security personnel, and websites.

Zero Knowledge Proof

- In cryptography, a zero-knowledge proof or protocol is a method by which an individual or system 'proves' to another individual or system that they have knowledge of certain information without revealing the information itself, nor any additional information.
- An example based on the One ID concept would be where a passenger can prove the authenticity of their biometric or biographic data, without revealing any identifying detail of that biometric or biographic data.

References

W3C Verifiable Credentials Note: the World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web.
W3C Decentralized Identifiers
ISO/IEC 24760-1:2019 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts
ICAO doc 9303 Machine Readable Travel Documents