Guideline on the Use of 2D barcodes on CITES Permits/Certificates

Contents

1. Objective of the guideline 2

2. Actors 2

3. Data carrier solution 3

3.1. Introduction 3
3.2. QR Code specification 3

4. Data content solutions 4

4.1. URL to Permit/Certificate 4
4.2. URL to Web site giving access to Permit/Certificate 5
4.3. Plain structured data 5
4.4. Encrypted data with Digital Signature 6
4.5. Encrypted data with Verifiable Credentials 7

5. Access rights management 7

6. Interoperability 8

7. Recommendations 8

7.1. Identification standards 8
7.2. E-permits 8
7.3. Recommended solution 8

Annex: Example of a CITES permit with a digital signature 10

Disclaimer:

It should be noted that as there are significant and continuing developments in the area of barcode-related authentication methods and the topic is a work-in-progress. These guidelines will need to be reviewed and refined on a continuing basis into the future.

1. Objective of the guideline

The objective of this guideline is to provide technical and business details on the possible solutions identified in the study on the use of 2D barcodes on CITES Permits/Certificates. The possible solutions are described, including a reference to the applicable standards. The advantages and disadvantages of each possible solution, and an indication of their cost, are also presented.

2. Actors

The actors involved in issuing and reading CITES permits can vary depending on the country and its specific implementation of the treaty. Below is a general overview of the actors involved:

- **CITES Management Authority**: Each country that is a signatory to the CITES treaty designates a national CITES Management Authority. This authority is responsible for overseeing and regulating the implementation of CITES regulations within their respective countries. They issue permits and certificates for the import, export, and re-export of CITES-listed species.
- **CITES Scientific Authority**: In addition to the Management Authority, each country also designates a CITES Scientific Authority. This authority provides scientific expertise and advice on the status of species and their trade implications. They play a crucial role in determining whether trade in a particular species is sustainable and can be permitted under CITES regulations.
- **Applicants and Permit Holders**: Individuals or entities that wish to engage in international trade of CITES-listed species, whether for commercial, scientific, or other purposes, are required to apply for permits. These permits are issued by the national CITES Management Authority. Permit holders are responsible for complying with the terms and conditions of the permits.
- **Customs and Border Control Agencies**: In many countries, customs and border control agencies are involved in the enforcement of CITES regulations. They inspect shipments of animals and plants to ensure that they are accompanied by the necessary CITES permits and certificates.
- **Wildlife Enforcement Agencies**: These agencies are responsible for investigating and addressing violations of CITES regulations. They work to combat illegal wildlife trade, enforce permit requirements, and collaborate with other law enforcement agencies at national and international levels.
- **Inspectors and Monitors**: Trained inspectors and monitors may be tasked with verifying the accuracy of the information provided on CITES permits and certificates, ensuring that the species being traded match the documentation, and reporting any discrepancies.
- **CITES Secretariat**: The CITES Secretariat is an administrative body that facilitates communication and cooperation among member countries, supports the implementation of the convention, and maintains a database of CITES-listed species. While not directly involved in issuing permits, the CITES Secretariat plays a central role in coordinating international efforts related to the treaty.

Many actors are involved in the processes related to the issuance, management, and use of CITES permits/certificates. It is important to note that the Parties are diversified in terms of trade volume, financial situation, information technology resources, etc. This will impact the choice of a solution by a given party deciding to adopt 2D barcodes on CITES permits/certificates.

3. Data carrier solution

3.1. Introduction

The preferred technical solution for the choice of a barcode is QR Code. The advantages of QR Code versus other barcode solutions include the following:

- QR Codes can encode various types of information and multiple character sets.
- QR Codes can hold small or large amounts of information.
- QR Codes are widely utilised for marketing, ticketing, product labelling, mobile payments, and other applications that require efficient data capture and seamless information retrieval.
- QR Code reading process by a mobile device does not require a special application as it is often embedded in the native software of the device.

The choice of the QR Code and the specifications described in the next section apply to all the data content solutions presented in Chapter 4.

3.2. QR Code specification

Example:

“https://example.com/example of a CITES permit using 2D barcode”

The application parameters for a printed QR Code on a CITES permit/certificate are:

- **Size**: The QR Code should be at least 2x2 cm in size for optimal scanning.
- **Contrast**: The QR Code should have high contrast between the black and white modules. This will make it easier to scan, especially on low-quality paper.
- **Quiet zone**: The QR Code should have a quiet zone around it. This is an area of empty space around the code that helps to prevent errors during scanning.
- **Error correction level**: The error correction level determines how much damage the QR Code can sustain before it becomes unreadable. A higher error correction level will make the code more robust, but it will also make the code larger.

The error correction level to be used for QR Codes on documents depends on factors such as the quality of printing, potential wear and tear, and the desired scanning distance. QR Codes have four error correction levels to choose from: Low, Medium, Quartile, and High. Each level corresponds to a

different percentage of data that can be restored in case the QR Code is partially damaged or obscured. Here's a breakdown of the error correction levels and their typical use cases:

- **Low Error Correction** (L): About 7% of codewords can be restored. Suitable for applications where QR Codes are likely to remain undamaged, such as on high-quality print materials that are handled carefully.
- **Medium Error Correction** (M): About 15% of codewords can be restored. A good balance between error correction and data capacity. Suitable for general-purpose applications where QR Codes might be exposed to moderate wear and tear.
- **Quartile Error Correction** (Q): About 25% of codewords can be restored. Provides higher error correction for applications where QR Codes could be exposed to more challenging conditions or lower print quality.
- **High Error Correction** (H): About 30% of codewords can be restored. Offers the highest level of error correction and resilience against damage or degradation. Suitable for applications where QR Codes might be exposed to extreme conditions, such as harsh environments or low-quality printing.

In general, for documents that will be handled with care and have good printing quality, the Medium Error Correction level is sufficient. If there is a chance the document might be subjected to wear and tear or if the QR Code will be scanned from a distance, considering the Quartile Error Correction level could be a better option.

Here are some additional considerations for printing QR Codes on paper documents:

- **Paper type**: The type of paper used can affect the readability of the QR Code. Glossy paper is generally better than matte paper, as it reflects light more evenly.
- **Printing method**: The printing method can also affect the readability of the QR Code. Inkjet printers are generally better than laser printers, as they produce sharper images.
- **Storage conditions**: The paper supporting the QR Code should be stored in a cool, dry place to prevent it from fading or becoming damaged.

Standards references:

- ISO/IEC 18004 Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification.
- ISO/IEC 15415 Information technology — Automatic identification and data capture techniques — Bar code symbol print quality test specification — Two-dimensional symbols.

4. Data content solutions

4.1. URL to Permit/Certificate

The QR Code contains the URI (Uniform Resource Identifier) of a PDF of the permit stored on a web site. When scanning the QR Code, the user can see the permit on the screen and/or download a PDF copy of the permit/certificate.

Advantages:

- This solution is simple to implement and simple to use.

Disadvantages

- This solution requires online connectivity to access the web site managing the access to the PDF of the permit/certificate.
- When a user scans the QR Code that is printed on the permit and his device is connected to the internet, he can see on the screen an image of the document that he has in his hands, which might give the sense that the permit is genuine. It would however be easy for a rogue user to create a fake permit and a QR Code with a web address showing the permit in PDF format.
- This solution does not facilitate the automatic processing of data since it only enables to show or to download a PDF of a document.

Cost
- Low

Standards references:

- Uniform Resource Identifier (URI): Generic Syntax: https://datatracker.ietf.org/doc/html/rfc3986

4.2. URL to Web site giving access to Permit/Certificate

This scenario is similar to the previous one. Instead of a URI pointing directly to a document, the URL points to a website where the access to the PDF is managed. The access management can be very basic, such as asking the user to fill out a Captcha in order to avoid automated users, such as bots. It can be more sophisticated by requesting for example a user ID and password to access the PDF.

Advantages:
- This solution is simple to implement and to use.
- It provides some level of security through a website that may require users to declare their credentials such as user ID and password.

Disadvantages
- This solution requires online connectivity to access the website managing the access to the PDF of the permit/certificate.
- The Management Authority issuing the permit/certificate needs to manage the access rights to the information.
- The additional sense of security could be counter-productive because it is relatively easy to create a fake permit with a QR Code encoding the address of a fake website.
- This solution does not facilitate the automatic data processing since it only enables to show or to download a PDF of a document.

Cost
- Low to Medium

Standards references:

- Uniform Resource Identifier (URI): Generic Syntax: https://datatracker.ietf.org/doc/html/rfc3986

4.3. Plain structured data

In this scenario, the data encoded in the QR Code is a subset or the full information included in the permit/certificate. The information is encoded in a structured way in compliance with ISO/IEC 15434 and it can be processed by a computer.

Advantages:

- The QR Code is a portable data file that can be processed for rendering the permit/certificate data visually and for feeding IT applications with the permit information in structured format.
- The data can be encoded in a standard format that is compatible with the Electronic Permit Information eXchange (EPIX) specifications.
- The data collected upon reading the QR Code can be used to automatically feed the relevant IT applications.
- Reading the QR Code does not require connectivity and data can be collected and processed later on.

Disadvantages
- Users reading the QR Code need an application capable of processing the structured data.
- There is no inherent security in this solution. It would be easy to create a fake permit with a QR Code encoding the fake data.

Cost
- Medium

Standards references:

- ISO/IEC 15434 Information technology — Automatic identification and data capture techniques — Syntax for high-capacity ADC media

4.4. Encrypted data with Digital Signature

Upon printing the permit/certificate, the issuer generates a QR Code that includes all the relevant permit information in a structured format with a digital signature. The digital signature is generated on the basis of the permit/certificate data and a private key owned by the issuer. Public keys are distributed by the issuer to any party that needs to scan the QR Code. Upon scanning the QR Code, the system gives access to the information that is encoded. This information can be used to check visually if it corresponds to what is printed on the document and for further processing by the user.

The digital signature of the data carrier is standardised by ISO/IEC 20248, an international standard that specifies a method for structuring and digitally signing data stored in barcodes and RFID tags. The purpose of the standard is to provide an open and interoperable method for verifying the originality and integrity of data in an offline use case. The standard defines a data structure for digital signatures that is based on the ISO/IEC 9594-8 standard for public key infrastructure (PKI).

Advantages:
- This solution meets most of the business requirements identified in the study.
- The data collected upon reading the QR Code can be used to feed automatically the relevant IT applications.

Disadvantages
- Users reading the QR Code need an application capable of processing the structured data.
- The issuer of the permit/certificate will need to manage the distribution of the PKI public keys to the target users.

Cost
- Medium to High

Standards references:

- ISO/IEC 20248 Information technology — Automatic identification and data capture techniques — Digital signature data structure schema.

4.5. Encrypted data with Verifiable Credentials

Verifiable credentials are a secure and tamper-proof way to digitally represent and share information about an individual or entity's qualifications, attributes, or personal data. These credentials are based on decentralised identity systems and utilise cryptographic methods to ensure their integrity and authenticity. They enable users to present their credentials to others, such as employers or service providers, without revealing unnecessary personal information, therefore promoting privacy and data control.

Verifiable credentials can be combined with 2D barcodes to create a secure and efficient method of presenting and verifying identity information. Here is how it could work:

- Encoding Credentials: The verifiable credentials, containing relevant identity data, are securely encoded into a QR Code.
- Scanning the Barcode: When a user needs to present their credentials, they can simply show the QR Code on their mobile device or a printed document. The verifier can then scan the QR Code using a compatible scanner or smartphone app.
- Verification Process: The scanned QR Code contains the encrypted verifiable credentials. The verifier's application can decrypt and validate these credentials using cryptographic methods and decentralized identity systems. The verification process can be performed offline, as the necessary validation data is embedded within the credentials themselves.

Advantages:
- This solution meets most of the business requirements identified in the study.
- The data collected upon reading the QR Code can be used to automatically feed the relevant IT applications.

Disadvantages
- Users reading the QR Code need an application capable of processing the structured data.
- The standard does not specify the syntax used to store the data on the barcode.
- The verification of the credentials requires on-line connectivity to a pubic blockchain or a central registry.
- The issuer of the permit/certificate will need to manage the distribution of the PKI public keys to the target users.

Cost
- Medium to High

Standards references:

- Verifiable Credentials Data Model

5. Access rights management

Some of the proposed solutions require to manage the access rights or the distribution of public keys to authorised users. The access rights to the electronic copy the document (solution 4.2) and the distribution of the public keys to authorised Parties (solutions 4.4 and 4.5) are in principle managed by the party issuing the permit/certificate.

There are 184 Management Authorities, and sometimes more than one issuing party per MA. Each authorised party (e.g. customs agencies) will need to get the access rights and public keys from each issuer, which can make the systems complex to manage and to maintain.

A possible solution to this problem is to create regional hubs through the cooperation of several MAs. For example, the MAs could be grouped in 5 regions across the world, resulting in 5 hubs tasked to manage and maintain the access rights to the permits/certificates issued by each MA.

Another option would be to centralise the management and maintenance of the access rights at global level under the responsibility of the CITES secretariat.

The actual operation of the central hub or regional hubs could be sub-contracted to service providers under the governance of the concerned MAs.

6. Interoperability

It cannot be expected that all MAs will adopt the same solution at the same time. The solutions presented in this document are interoperable in the sense that they do not conflict with each other. Some MAs may choose to start with a simple QR Code solution encoding the URL of an electronic copy of the document. Others may opt for a more sophisticated solution like the digital signature with the full permit/certificate data encoded in a secure way. It is even possible to adopt more than one solution at the same time, resulting in more than one QR Code printed on the permit/certificate. From a technical perspective, this is not a problem. However, the eventual adoption of one single solution across the CITES community would be beneficial to the community.

7. Recommendations

7.1. Identification standards

The automatic processing that will be enabled by the introduction of 2D barcodes on CITES permits/certificates will heavily rely on data quality. The unambiguous identification of the Parties, the permit and the species are an essential requirement to the automation enabled by 2D barcodes. This is especially true when the data resulting from the scanning of the 2D barcode will be processed automatically by computer applications.

7.2. E-permits

The issuance of permits/certificates in electronic format is a pre-requisite to the successful adoption of 2D barcodes. CITES Parties willing to engage in the adoption of 2D barcodes need to ensure that their systems support the issuance and processing of electronic permits/certificates.

7.3. Recommended solution

The QR Code encoding encrypted data with a digital signature (see section 4.4) meets the business requirements identified in the study and is the most suitable way forward. Upon endorsement by the CITES Working Group on electronic systems and information technology, this solution should be assessed through pilot implementation projects. However, given the varying level of readiness and financial conditions of the CITES Parties, other options and preferably the URL to web site giving access to permit/certificate may be explored.

An example of a CITES permit (encrypted data) with a digital signature is presented in the Annex.

* * *

Annex: Example of a CITES permit with a digital signature

CONVENTION ON INTERNATIONAL TRADE IN ENDANGERED SPECIES OF WILD FAUNA AND FLORA

CITES PERMIT No. **23ZZ000001**

☒ EXPORT ☐ IMPORT ☐ RE-EXPORT ☐ OTHER

Original

2. Valid until: **2025-01-01**

3. Consignee (Name and address)
Utopia Planetial Importers
54 avenue Peron, Bouvier

4. Permittee (name and address, country)
Lotus exotic animal exports PTY LTD
40 Jalan Sultan Sulaiman 94W, Batang Benar

3a. Country of destination
Utopia

5. Special conditions
Must match ASEAN requirements
For live animals, this permit or certificate is only valid if the transport conditions conform to the Guidelines for Transport of Live Animals or, in the case of air transport, to the IATA Live Animals Regulations

6. Name, address, national seal/stamp and country of Management Authority
Republic of Lilipgal
Minstry of Animal Wellfare and Protection
16, Jalan Robson
77G Sarawak
Jelutong +606-923 5894 ofemand @lilipgal.gov

5a. Objective of the operation
T - Commercial

5b. Security stamp No.
N/A

	7./8. Scientific name (genus and species) and common name of animal or plant	9. Description of specimens, including identifying marks or numbers (age/sex if live)	10. Appendix No. and source	11. Quantity (including unit)	11a. Total exported/Quota
A	7./8. **Myrmecophaga Tridactyla Anteater**	**N/A**	10. **Appendix: II ; Source: W - Specimens taken from the wild**	11. **2 NAR**	11a. **2**
	12. Country of origin * / Permit No. / Date: **N/A** / **N/A** / **N/A**		12a. Country of last re-export / Certificate no. / Date: **N/A** / **N/A** / **N/A**		12b. No of the operation ** or date of acquisition ***: **N/A**
B	7./8.	9.	10.	11.	11a.
	12. Country of origin * / Permit No. / Date:		12a. Country of last re-export / Certificate no. / Date:		12b. No of the operation ** or date of acquisition ***:
C	7./8.	9.	10.	11.	11a.
	12. Country of origin * / Permit No. / Date:		12a. Country of last re-export / Certificate no. / Date:		12b. No of the operation ** or date of acquisition ***:
D	7./8.	9.	10.	11.	11a.
	12. Country of origin * / Permit No. / Date:		12a. Country of last re-export / Certificate no. / Date:		12b. No of the operation ** or date of acquisition ***:
E	7./8.	9.	10.	11.	11a.
	12. Country of origin * / Permit No. / Date:		12a. Country of last re-export / Certificate no. / Date:		12b. No of the operation ** or date of acquisition ***:

* Country in which the specimens were taken from the wild, bred in captivity or artificially propagated (only in case of re-export)
** Only for specimens of Appendix I species bred in captivity or artificially propagated for commercial purposes
*** For pre-Convention specimens

13. THIS PERMIT IS ISSUED BY:

Ministry of Animal Wellfare and Protection
16, jalan Robson 77G
Sarawak Jelutong, Utopia

Place

1693144576
Date

Security stamp, signature and official seal

14. EXPORT ENDORSEMENT:

15. Bill of lading/Air waybill number:

Block	Quantity
A	
B	
C	
D	
E	

Port of export / Date / Signature / Official stamp and title

The 2D barcode contains the following data:

Data field	Description	Value
1. specificationversion:	This field indicates the version of the specification being used	ISO/IEC 20248:2018
2. dauri:	Represents the URI for the domain authority	https://dauri.digsig.tools
3. daid:	Stands for the domain authority ID	QC DEUS
4. cid:	Represents a unique identifier, possibly a certificate ID	202
5. signature:	Holds a digital signature with a binary format of {256}	BgYgPYLWFC436_Tr2HxdqHA3Z8MosZvO_XcLjtZLcwo=
6. timestamp:	A date field indicating when a certain event took place	2023-08-27T14:56:16
7. permit_number:	Holds a unique permit number with a type of string, a binary format of {10}, and a range of [0-9A-Z].	23ZZ000001
8. export:	A boolean field indicating if an item is for export.	TRUE
9. valid_until:	Specifies the validity period of a document or permit	01/01/2025
10. consignee:	Indicates the entity or individual receiving the goods with a type of string and a binary format of UTF8	Utopia Planetial importers
11. consignee_address:	Provides the address of the consignee with a type of string and a binary format of UTF8	54 avenue Peron, Bouvier
12. country_destination:	Indicates the destination country for the goods	Utopia
13. permitee:	Specifies the entity or individual who has been granted the permit	Lotus exotic animal exports PTY LTD
14. permitee_address:	Provides the address of the permitee	40 Jalan Sultan Sulaiman 94W, Batang Benar
15. special_conditions:	Lists any special conditions associated with the permit	Must match ASEAN requirements
16. objective_of_operation:	Indicates the purpose of the operation	Commercial

17. animal_scientific_name:	Provides the scientific name of the animal being traded	Myrmecophaga Tridactyla
18. animal_common_name:	Provides the common name of the animal being traded	Anteater
19. appendix_number_source:	Indicates the source and appendix number related to the animal	Specimens taken from the wild (Appendix: II)
20. quantity:	Indicates the quantity of the items being traded	2
21. quantity_unit:	Specifies the unit of measurement for the quantity	NAR
22. total_exported:	Indicates the total number of items exported	2