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

Seventieth meeting of the Standing Committee
Rosa Khutor, Sochi (Russian Federation), 1-5 October 2018

DEVELOPMENT OF ELECTRONIC PERMIT INFORMATION EXCHANGE (EPIX) FOR CITES

This document has been submitted by Switzerland as Chair of the Standing Committee's intersessional working group on electronic systems and information technologies in relation to agenda item 39.*

* *The geographical designations employed in this document do not imply the expression of any opinion whatsoever on the part of the CITES Secretariat (or the United Nations Environment Programme) concerning the legal status of any country, territory, or area, or concerning the delimitation of its frontiers or boundaries. The responsibility for the contents of the document rests exclusively with its author.*

Development of

Electronic Permit Information Exchange (EPIX) for CITES

Summary: This document has been drafted by the Chair of the CITES Working Group (WG) on electronic Systems and Information Technology and the Secretariat to provide an overview for the development of standards and solutions for electronic permit information exchange (EPIX) between Parties.

Chapter 1 provides a brief introduction into electronic permitting systems.

Chapter 2 gives a definition of EPIX and its benefits.

Chapter 3 introduces some of the issues related to electronic permits and their exchange between Parties.

Chapter 4 discusses Architecture options for EPIX exchanges that Parties can implement.

Chapter 5 provides a brief outline of the standards and recommendations that the WG should develop to ensure compatibility of EPIX exchanges between Parties.

The text outlined in grey contains recommendations for further work to be conducted by the Working Group.

1. Introduction

The *eCITES Implementation Framework*[1] provides the concept for automation of permit processes and electronic information exchange. The concept allows Parties to adapt an eCITES implementation to their needs in a stepwise approach:

1. ePermit - Simplified permit issuance: This step provides automation mainly between the CITES Management Authority and the exporters and importers. It automates business processes related to request of certificates by traders; assessment of risks and scheduling of inspections; logging of inspection results; issuance of certificates, including electronic records of the certificates; and electronic payment of fees.

2. eControl - Border agency collaboration for better controls: This pillar implements automated procedures between the Management Authority and other control agencies, thus providing automation on the national level. This includes exchange of permit data with Customs and other border agencies; use of CITES risk management by Customs; exchange of actual quantities exported with the Management Authority; and Single Window integration of permits.

[1] *https://cites.org/sites/default/files/20180219eCITESImplementationFramework.pdf*

3. eExchange – electronic permit exchange with other countries: This pillar implements automated exchange of electronic permits between CITES trading countries. It automates business processes for cross border exchange of permits for secure and integrated management of the trade transaction between the exporting, importing and transit countries.

4. eReport - automated reporting: This pillar implements automated exchange of data between the Management Authority and the CITES Secretariat to meet annual reporting requirements.

The third step in the eCITES implementation focusses on the exchange of electronic permit information (EPIX) with other administrations in other countries. The purpose of this paper is to provide an outline of concepts, standards and best practices that CITES should develop over the coming years to assist Parties in the implementation of electronic permit exchange.

2. What is Electronic Permit Information Exchange?

The objective of EPIX is to:

- allow safe, secure and reliable exchange of information of electronic Permits and permit-related information between Parties;
- reduce costs and efforts of Parties for implementing, testing and maintaining electronic exchanges;
- ensure conformity with the provisions of the Convention;
- ensure that permit information exchange is compatible with international standards and complements standards already included in the CITES ePermitting toolkit;
- ensure compatibility of solutions implemented by the Parties for permit information exchange.

Definition: Electronic Permit Information Exchange (EPIX) is the exchange of electronic information related to CITES Permits between Government administrations of two or more countries using standards and best practice recommended by CITES.

.

The above definition implies that EPIX is not a software solution or a system. Rather, it is a set of specifications that should be applied by Parties when they implement software solutions for the exchange. Also EPIX focuses on permit exchange between Parties and does not deal with annual reporting.

A Government administration in the EPIX definition is any authority that has been designated by the Management Authority (MA). This can be, for example the MA itself, the Scientific Authority, the Customs organization or a Single Window Operator.

Countries may also use EPIX standards to implement exchanges between the Government agencies of their own country, for example between the MA and the Customs organization.

The CITES ePermitting Working Group will develop the **EPIX Toolkit** (TK) which is a set of standards, recommendations and training materials to support Parties in the implementation of EPIX.

The application of EPIX standards is voluntary. Parties may establish at any time Permit exchanges on the basis of their own arrangements.

3. What are the challenges in exchanging electronic permit information between Parties?

This chapter provides a brief introduction into specific issues when implementing electronic permit information exchanges.

3.1 Difference between the workflow of paper and electronic permits

There are fundamental differences in the use of paper and electronic Permits: An electronic permit can be easily changed using a text editor while changes in a paper permit require at least some effort in forging the document. In addition, an electronic permit that has been used for an export or import operation cannot be stamped by Customs like a paper permit. Therefore, it could potentially be used again. To overcome these difficulties, the document workflow for an electronic CITES Permits has to be different from the paper Permit workflow.

3.1.1 Document workflow for CITES paper Permits

Figure 1 describes the workflow of a paper permit. The Exporter requests a paper permit from the Management Authority (MA) (Step 1). The MA creates a record in the permit database and prints and signs a paper permit (Step 2). The exporter sends the paper permit to the importer (Step 3). The importer presents the Permit to Customs together with the Customs import declaration and/or to the MA (Step 4).

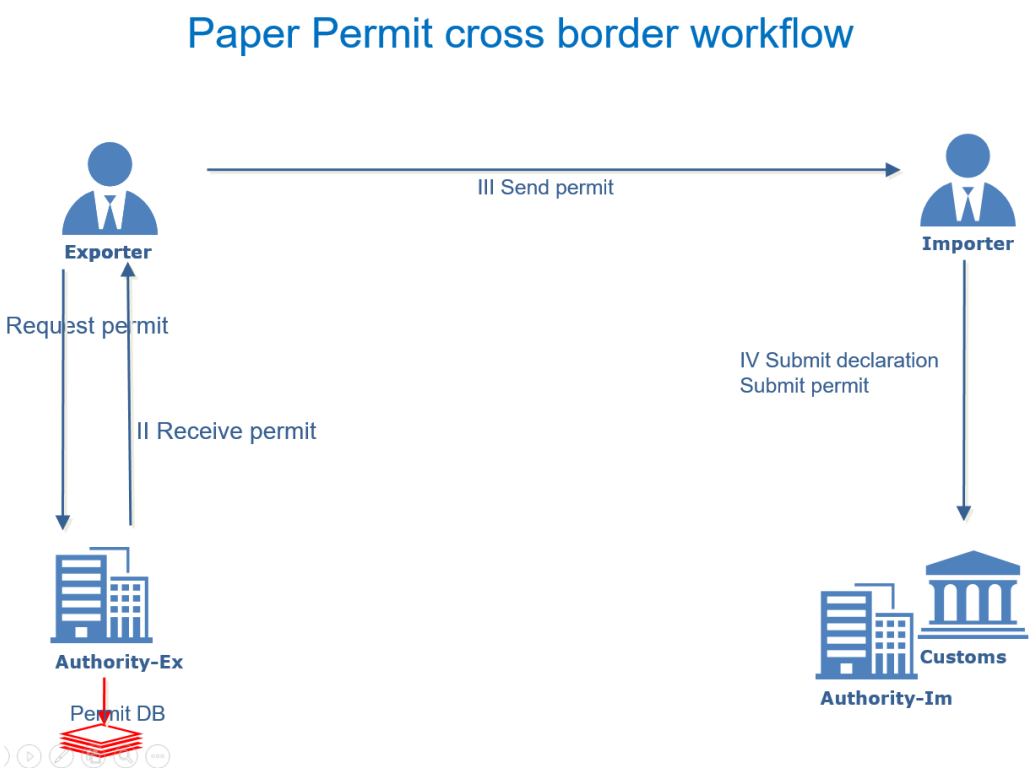

Figure 1 Cross border document flow of paper permits. Electronic components are marked in red

3.1.2 Document workflow for electronic CITES Permits

Figure 2 describes the workflow of an electronic permit exchange. The exporter requests a permit from the MA (Step 1). The MA creates a record in the permit database and issues a permit identifier[2] (ID) (Step 2). The MA may also print a hardcopy of the electronic permit. However this copy will be marked as "COPY" and cannot be used for official use. The exporter sends the permit ID to the importer (Step 3). The importer sends the Permit ID to Customs and/or to the MA (Step 4). Customs/MA send an electronic request for the permit data (permit information) to the issuing MA (Step 5). The issuing MA sends an electronic message with the permit data to the MA in the importing country (Step 6).

[2] *On CITES permits the ID is referred to as the "PERMIT/CERTIFICATE No.", printed in box 1 of the Permit.*

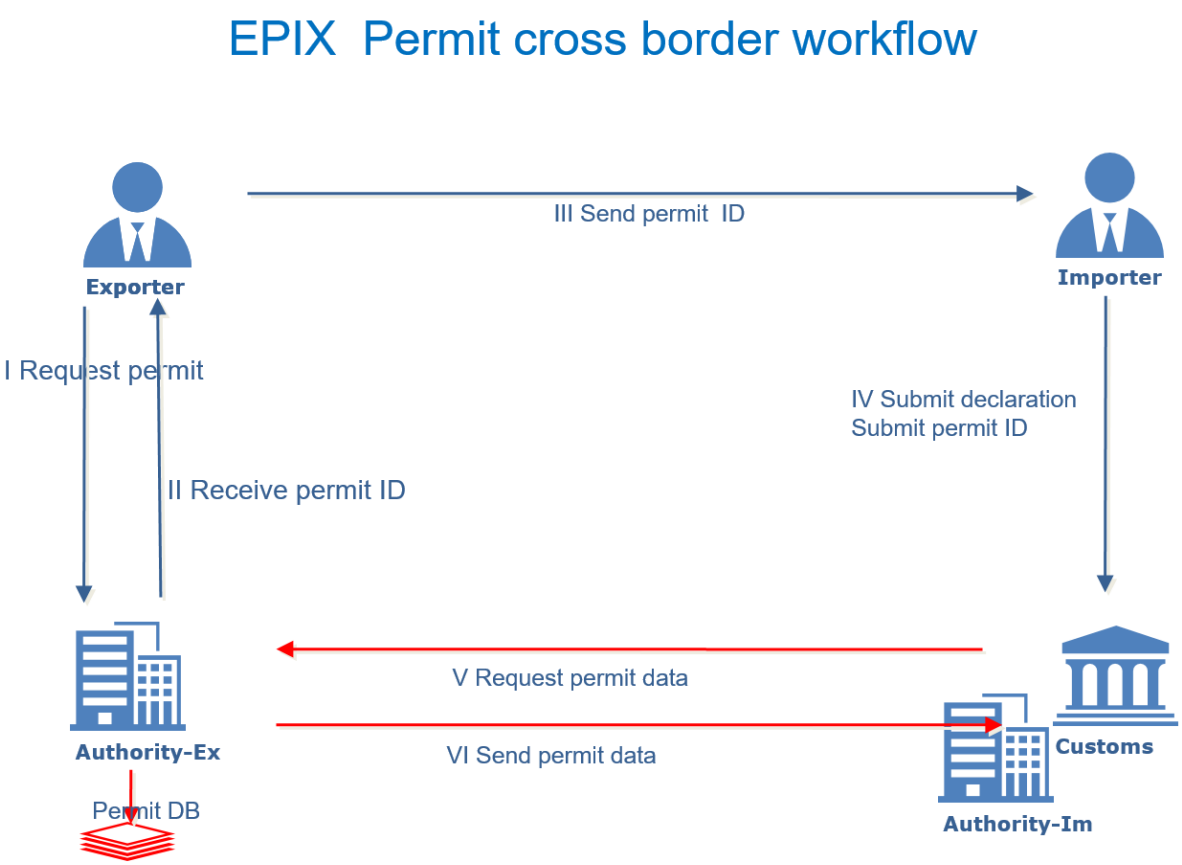

Figure 2 EPIX electronic permit workflow Electronic components are marked in red

This workflow is substantially different from the paper workflow as the permits are now exchanged between the MAs. The exporter and importer only exchange the Permit ID.

This means that responsibilities for providing and exchanging the Permit now lies with the authorities in both countries. The authorities are responsible to the trader for the success of the exchange. The authorities are also responsible for data confidentiality and security.

The WG should make Parties aware of their changed responsibilities when using EPIX exchanges.

The WG should recommend Parties to put appropriate measures in place for secure, confidential and reliable EPIX.

3.2 Electronic permit exchange requires agreements between Governments

Exchange of electronic CITES permits requires an explicit, written agreement between the two MAs to use electronic permits instead of paper permits for official use. This agreement could be in the form of an MoU. Such an agreement should also specify other relevant aspects of the EPIX exchange between the two Parties, for example:

- Responsibility of Parties
- Management of the MoU
- EPIX standards used
- Procedures for testing and upgrade
- Retention period of permits
- Sharing of costs

As Parties frequently involve the CITES Secretariat in matters relating to verification of issued Permits, the Parties are encouraged to provide the Secretariat with a copy of their EPIX agreements.

The WG should develop a template for EPIX agreements between Parties. This template should take into account existing agreements that Governments have already established for electronic permit exchanges, for example for electronic Phytosanitary exchanges.

The WG should recommend Parties to provide the Secretariat with copies of agreements they have signed.

3.3 Signatures in electronic CITES permits

CITES decision Conf. 12.3 (Rev CoP16)[3] states that Parties that use electronic Permits need to use an electronic equivalent for the physical signatures in the Permit.

Different methods exist to implement an electronic signature in a document. UN/CEFACT Recommendation 14 on authentication of trade documents advises Governments to avoid over engineering of electronic signature solutions and recommends as best practice that electronic signatures in a trade document should match the level of security provided by a physical signature on a paper Permit..

In most administrative systems the electronic equivalent of a physical signature is implemented by authenticating the user, for example through a username and password. The system will then log all activities of this user, for example which documents were approved by the user. This audit trail ensures that the Authority can at any time identify who signed and approved documents.

The WG should provide guidance to Parties on criteria for use of electronic equivalences of physical signatures in in CITES permits[4].

3.4 Secure exchange of CITES permits over the Internet

Electronic CITES permits are exchanged through the Internet, which is an open and anonymous network with the risk that messages can be intercepted or changed. Therefore,

[3] https://cites.org/sites/default/files/document/E-Res-12-03-R17.pdf

[4] *The WG will present a recommendation on the use of electronic signatures in CITES permits and certificates at SC70.*

it is important that EPIX provides rules for secure exchange of CITES permits using a potentially unsecure transport network.

There are three major security aspects that EPIX needs to address:

1) **Authentication**: An EPIX message is sent by the computer system of an MA, the Customs authority or the designated Single Window service provider. In a message exchange the sending server will identify itself with an Internet address that is associated with a specific administration.
   Authentication is a mechanism that verifies that this address is really associated with the administration in question. It provides an answer to the question "*Is the authority that sent me the Permit really the authority that it pretends to be (and not an imposter)*?"
   In message exchanges, authentication is implemented through certificates[5] that are issued by certification agencies. Numerous private sector companies exist that provide reliable certificates for the Internet community.

2) **Authorization:** verifies that the Authority that requests a permit is authorized to do so. It provides an answer to the question "*The Ministry of Finance of country XYZ requested a CITES permit that has been issued by us. Is this Ministry authorized to request this permit from us?*"

   To manage authentication, CITES needs to implement a repository (i.e. a list) of all Authorities that can participate in EPIX exchanges.

   The Secretariat should maintain a list of national Authorities identified by each MA as an authorized agency for EPIX exchanges.

3) **Security during transport:** Ensures that no one between the sending and receiving Party can interfere with the EPIX message during the exchange over the Internet, i.e. read or change the message content. The most common transport security standard is Transport Layer Security (TLS), which implements military grade security for Internet message exchanges through encryption.
   Computer systems using TLS will encrypt a message directly before it is sent and decrypt the message immediately after it is received. If an EPIX exchange is implemented through a central Hub then the message is decoded in the Hub and vulnerable to changes. Therefore message exchange using a Hub is potentially unsecure and requires special agreements between the Parties regarding the security and liability of the Hub operator.

[5] *See also https://en.wikipedia.org/wiki/Authorization_certificate*

- The WG should recommend use of TLS 3.0 or later for EPIX exchanges over the Internet.

- The WG should define minimum security requirements for EPIX Hubs for those Parties that wish to exchange information through a central hub.

4. EPIX Architectures

There are different concepts to exchange electronic information between countries. These concepts are often referred to as an "*Architecture*" as they describe the high level structure of a system. In the following we describe the two Architectures that are available to Parties for electronic Permit Information Exchange, the point-to-point (P2P) connection and the Hub connection[6] and introduce into the specific issues of the two Architectures.

Recently Blockchain (BC) technology has made significant advancements and Government agencies are researching the potential of BC as a solution for secure and trusted exchange of electronic licenses, permits and certificates. In the future BC may provide an alternative to point-to-point or Hub architectures. A BC solution is not discussed in this chapter due to lack of experience with this technology at the time of drafting. However, the potential of BC for electronic permit information exchange should be evaluated as new experience becomes available. To encourage research in BC technology for EPIX the Secretariat has drafted the *CITES Blockchain Challenge*[7].

4.1 Point-to-Point (P2P) Architecture: Direct exchange of permits information between Parties

In a *point-to-point* connection, the MAs will directly exchange permits with each other. There is no requirement to establish and maintain an Intermediary that operates a Hub.

P2P Architectures are straightforward to implement and robust. Each Party is responsible for the security and proper management of their own eCITES system, in conformance with national legislation and requirements. The communications between the Parties is encrypted using Internet Transport Security Layer (TLS) throughout.

P2P exchanges provide a very robust and failure secure system. If one Party is not available, for example because of system failure this will not affect the communication of the other Parties.

---

[6] *The Secretariat is currently working with the IBM Research department on a demonstrator for permit exchange using Blockchain technology. In the future Blockchain might provide an alternative to P2P and Hub architectures.*

[7] *CITES SC69 Inf. 33*

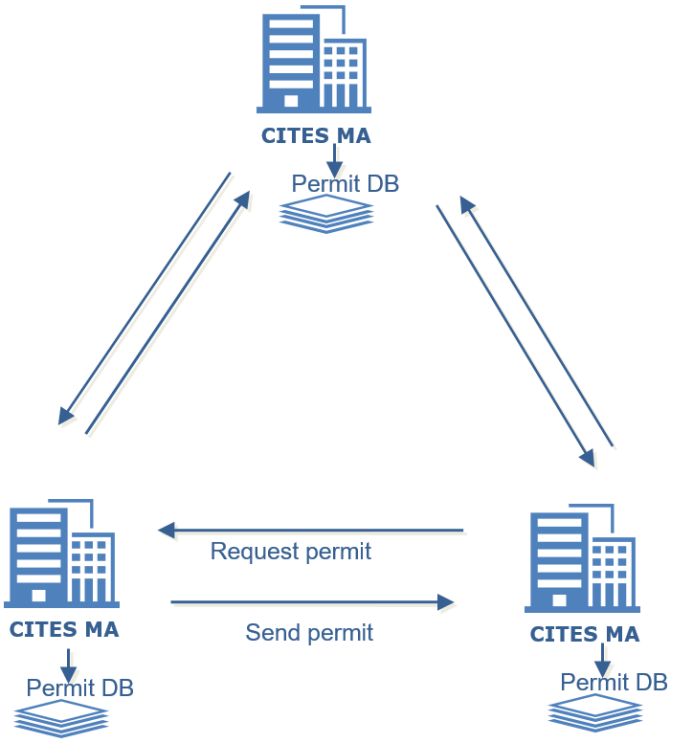

Figure 1 P2P Information flow for electronic permit exchange between 3 MAs: Messages are exchanged directly between the MAs

4.2 Hub Architecture: Communication through a central Hub

In a Hub architecture the message exchange between two Management Authorities has three major components:

- The eCITES systems of the two Management Authorities
- A Hub hat relays messages between the two Management Authorities

The Hub does not store permits, rather it is a pipeline to transmit information similar to a postal service. The main role of the Hub is to identify the MA to which the message needs to be forwarded.

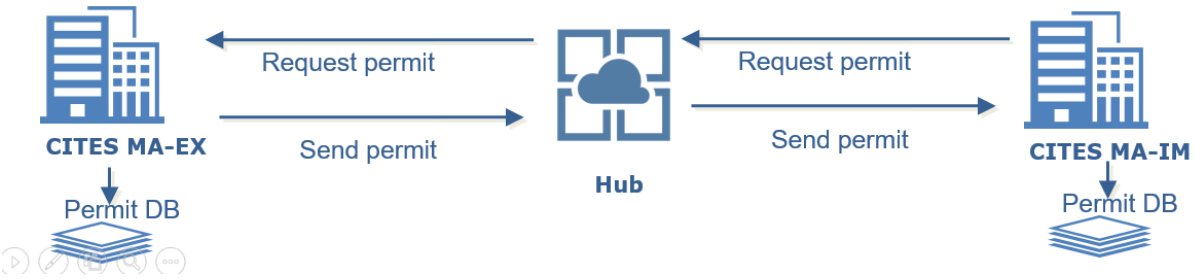

Figure 3 Information flow for electronic permit exchange between two MAs (example): The importing country MA requests an electronic permit from exporting country MA which has issued the permit. The request is routed through the Hub. The exporting country MA selects the permit in its permit database and sends it to the importing country MA. The message is routed through the Hub.

From the perspective of the participating Management Authorities the Hub is transparent, i.e. the permits are exchanged directly between the sending and receiving Authorities. At any moment there is only one valid and authenticated permit, which is the one that is stored in the permit database of the issuing MA. By sending a permit request message the requesting Authority will receive an authenticated copy of this permit.

Hub architectures are significantly more complex to implement and manage than P2P solutions as the Hub additional system that needs to be integrated, tested and managed and the Hub itself will require additional software components that need to be developed. The Hub is a potential single source of failure as all message exchanges will fail if the Hub is not available.

4.3 Hybrid Architectures: Meeting the realities of international trade relations

Most countries have already started to implement exchange Platforms for Government information, such as Singe Window Systems and regional exchange platforms of bilateral Governmental agreements for point-to-point exchanges.

For example, the European Union has already established networks for point-to-point Customs and transit information exchange. ASEAN countries have agreed to exchange certificates through the ASEAN regional Single Window hub. For ePhyto permit exchanges many countries have implemented direct, point-to-point exchanges, and other countries are working in parallel on a central ePhyto hub. Globally there are numerous other initiatives of Governments to organise and improve electronic information exchange between Government agencies across borders.

When implementing Electronic Permit Information Exchanges it is likely that the Management Authority is not free choose its preferred solution. Rather it is likely that MAs will have to integrate into the overall trade policy and information technology strategy of their Governments. In this scenario it is also likely that Parties support different architectures at the same time, i.e. they will develop direct P2P exchanges with some countries while exchanging documents through Hubs with other countries.

As a consequence, CITES should aim to define standards for EPIX in a way that they are Architecture neutral so that Parties may use these standards for different Architectures and technical implementations.

4.5 Comparing CITES Point-to-Point and Hub Solutions

Point-to-point solutions are simple to implement and robust. Each Party is responsible for their own eCITES system and there is nothing between the Parties.

Hub solutions are similar to point-to-point architectures but require additional safeguards, standards and agreements to control the Hub that sits between the Parties.

For Hub solutions a number of additional points need to be taken into account:

- The Hub is a potential single point of failure: If the Hub is not operational all Parties fail to communicate.
- Development and maintenance of the Hub require additional funding, in particular if high availability of the Hub is required
- Hubs require establishment of managerial structure and controls for operation of the Hub (Service level contracts, cost recovery, investment policy ..)
- The operation of the Hub needs to meet the minimum legal requirements of all participating Parties. For example, legislation of some countries requires that Government data can only be stored on Servers operated under their own jurisdiction. Agreement on the legal and technical requirements for the Hub services may require a long negotiation process and result in a solution that is still not acceptable to all CITES Parties.
- When the server of the Hub receives a message it will decode the message with the session key of the sending Party and then encode the message with the session key of the receiving Party. This has to be done with every message exchanges. This means that during an exchange the message is temporarily not encoded on the Hub server and is potentially subject to interception or tampering.

For both architectures it is important that an efficient solution for the Onboarding[8] of new Parties is found. CITES needs to establish an audit/assessment process that can assess and test the compliance of the new Party with regards to EPIX standards and assist this Party to meet the required standards. If CITES does not establish such an Onboarding process the burden of testing will rely on the Parties themselves.

With regard to Architecture the ePermitting WG should make the following recommendations:

[8] *Onboarding is the process through which a new party can join into already established EPIX agreements between Parties.*

The WG should suggest to Parties that Parties should evaluate the short, medium and long term costs and benefits for both Architecture options and make informed decisions.

The WG should ask the Secretariat to support Parties in the evaluation of Architectures, for example by developing background documents and checklists.

The Secretariat should monitor new technical developments and in particular Blockchain for their potential to provide solutions for electronic Permit information exchanges.

MAs should be aware that national Single Window strategies and priorities of national trade policy have an impact on the architecture for permit information exchanges. Architecture choices need to be coordinated with the relevant ministries in the country.

4.4 EPIX Onboarding assessment: Integrating new Parties into an existing EPIX exchange

An important aspect of an Architecture is that it is scalable. For EPIX this means that a new Party can join into an existing EPIX data exchange (*Onboarding*) without putting burden on the Parties that are already exchanging electronic Permits among each other. In particular, a mechanism is necessary so that the new Party can join without requiring bilateral tests and agreements between the new Party and all of the existing Parties.

It is suggested that the new Party be audited for its compliance and readiness for EPIX (*Onboarding assessment*) prior to joining. The Onboarding assessment will assess full compliance of the Party with the agreed EPIX standards. This ensures that the Party meets all EPIX standards and makes individual testing with all other Parties obsolete.

The Onboarding assessment is required independent from the Architecture that Parties choose, i.e. it is required both for point-to-point and Hub architectures.

The Secretariat has drafted a proposal for an EPIX onboarding process[9] that will be discussed by the CITES Working Group on electronic systems and information technologies.

The WG should acknowledge the importance of an efficient Onboarding process for the broad implementation of electronic permit exchange in CITES both for point-to-point exchanges and Hub solutions. The WG should draw the attention of Parties and donors to provide resources to the Secretariat for the development of Onboarding tools.

The WG should make Parties aware that an efficient Onboarding process requires central development of standards and tools and a procedure to test that the new Party in the exchange meets all required standards. This means that CITES Parties will have to agree how the Onboarding process is managed and funded in the long run.

[9] *EPIX Onboarding: Simplifying the implementation of Electronic Permit Information Exchanges between Parties*

4.6 Decision matrix for Parties to compare options for EPIX exchanges

In this chapter we provide a decision matrix for Parties with a list of criteria to compare different point-to-point or Hub solutions that may be available to them. It is suggested that Parties add columns on the right side of the table for each option available to them and then evaluate each option on these criteria.

When making this evaluation Parties should be aware that they need to take into account their specific circumstances, i.e. the specific offers that they have received from service providers, the eBusiness competence of these service providers, funding available to them, etc. Also there may be additional criteria that are relevant for the Party.

Comparing Point-to-Point and Hub architectures
Onboarding: Efficiency of EPIX depends very much on the costs/effort to integrate a new Party into an EPIX exchange (Onboarding). This requires that CITES provide a detailed set of EPIX standards. Parties will also need a centrally managed automated test environment to test their eCITES systems for compliance with EPIX standards. Onboarding of a new Party will require some assistance from the Secretariat or a competent advisor. The costs for Onboarding depend on the quality of the standards and tools provided. They are independent from the architecture.
Tests, debugging and exemption handling: Parties need to test whether their eCITES systems can handle all situations of real exchanges, including exceptions (lost messages, systems not responding, etc.). Testing of Hub solutions may be more complex as the test, debugging and exemption handling of the Hub in the middle of the connection needs to be tested as well.
Software development: The software development costs for making a national eCITES system EPIX-compatible are independent from the architecture choice.
Security (national system): Parties are responsible for taking appropriate measures to ensure security of their national systems. Costs for security of the national system are independent from the architecture decision.
Security (exchange): Point-to-point exchange between Parties occurs through encrypted communication (TLS standards). If properly implemented this communication is highly secure. Parties using a Hub need to implement the same security measures as in P2P. In addition, Parties need to audit the security of the Hub Service provider: In exchanges using a Hub, the message is decrypted by the Hub service provider. This creates an important potential security risk that needs to be addressed. The costs and effort in a Hub solution to reach the same level of security are considerably higher than in point-to-point solutions.

Stability of exchange: Stability in point to point exchanges depends on the availability of the eCITES system of the sending and receiving Parties. Parties need to take appropriate measures to ensure stability of their national systems. Hub solutions need to take the same measures as point-to-point implementations do. In addition the Hub itself is a potential single point of failure. Parties need to take appropriate measures to ensure availability of the Hub. The costs and effort in a Hub solution to reach the same level of availability as in point-to-point solutions are considerably higher.
Funding for Hub: A Hub solution requires substantive funding for the Hub. Funding includes development of the Hub solution, operational costs, implementation of adequate measures for availability, disaster recovery, security and management, and operation and steering of the Hub.

5. Standards and tools for CITES EPIX

5.1 Reference Model for CITES EPIX standards and tools

This chapter describes standards that are required for CITES electronic Permit information exchange, both for point-to-point and Hub solutions. If Parties use a Hub solution, then the Hub also must be compliant with the requirements outlined in 5.2

For EPIX we distinguish 7 layers that describe the layers of EPIX message exchanges and the standards, tools and recommendations required to support the message exchange:

- Data Model Layer (Layer 0): Standards to encode the CITES Permit in electronic format, including use of codes in permits. This standard has been already developed and is published as the *CITES ePermitting Toolkit V2.0*10. Compatibility with this standard can be checked using the eCITES automated validating tool provided by GEFEG.

  EPIX Data Model standards include:

a) Use of standard data format and structure for electronic permit exchange
   Based on CITES ePermitting Toolkit 2.0 data model11, UN/CEFACT CCTS data mapping
b) Valid CITES XML permit verified through test with GEFEG eCITES XML Permit AutoCheck12

  The WG has already developed the data standards for electronic CITES permits. The WG should review these standards on a regular basis for their completeness.

- Message Exchange Layer (Layer 1): A set of EPIX standard messages that are exchanged between the Parties. These standards are currently developed and tested in the pilot project between France and Switzerland.

  EPIX Message Exchange standards include:
  - Communication Standards

[10] *https://cites.org/eng/prog/e/e-permitting-toolkit.php*

[11] *https://cites.org/eng/prog/e/e-permitting-toolkit.php*

[12] *https://portal3.gefeg.com/ecites/page/about*

        - WebService/SOAP

    - Standard Service Calls
        - GET FINAL
        - GET NON FINAL
        - CONFIRM QUANTITIES
    - Standard Status of ePermits
    - A CITES application and permit processed in the national eCITES system may go through a sequence of status during its lifetime that depends on the workflow in the MA and national requirements and legislation. When permits are exchanged with other Parties, a common understanding of the Permit status is essential. For EPIX exchanges the following permit status are allowed:
        - VALID
        - CANCELLED
        - NOT AVAILABLE (any other internal/national status except VALID/CANCELLED)

The WG should approve these standards when the current pilots are completed. It is expected that these standards will need to be revised as more experience becomes available.

- Message Authentication and encryption Layers (Layer 2): Authentication and security in the message exchanges (transport layer) between the IT systems of the Government agencies that send and receive the permit. This layer includes

    - Authentication of the sending and receiving server and encryption, i.e. ensuring that the sending and receiving system really belongs to the Government administrations and that the message is encrypted throughout the interchange.
      This can be achieved by using Transport Layer Security (TLS), the standard security mechanism of the Internet.
      However, the WG should specify general EPIX best practices for the Transport Authentication Message layer. For example, the WG should decide whether Hub Service providers are authorized to decrypt and store the information exchanged between the Parties.

  EPIX Message Authentication and encryption standards include:

    - Security Standards
        - Use of a TOKEN together with ePermits

- Authentication Mechanisms
- Encryption and Cryptographic Mechanisms

The WG should recommend TLS for exchange of Permits.

The WG should specify the best practices for security and authentication of EPIX message exchange in collaboration with the legal unit of the Secretariat.

- Party Authentication Layer (Layer 3): Standards and mechanisms to authenticate the Parties authorized to participate in an EPIX message exchange. This layer essentially addresses the organization of an efficient Onboarding mechanism that ensures that only qualified parties can join an EPIX exchange.

  It is suggested that the WG establishes a set of rules for Onboarding of Parties.
  The WG should work with the Secretariat to organise an efficient Onboarding process.
  The Secretariat should support Parties that want to enter into EPIX exchanges in in the Onboarding process.

- Permit Authentication Layer (Layer 4): A CITES permit contains signatures and seals to identify the issuing MA, Customs officers and the requester of a Permit. The convention requires that an electronic Permit contains the electronic equivalent of these signatures and seals.

  The WG shall provide guidance on what qualifies for an electronic equivalent of signatures and seals in CITES permits[13].

- Business Process Layer (Layer 5): Collaboration between two MAs through electronic exchange requires that both MAs have a clear understanding of how their CITES permit processes work and how the exchanged messages fit into this workflow.
  The WG should develop a Business Process Model of the CITES permit process and how the exchanged messages change this process. This specification should include permit states and transitions (issued, used, cancelled, ..). It is suggested that a formal description (UML or similar) is used[14].

[13] *The WG has already discussed a proposal which will be presented at the SC70 meeting.*
[14] Switzerland has already started an initial draft of the CITES business process layer. The WG should oversee the completion and approval of this specification.

- Government Layer (Layer 6): A CITES permit is a legal, official trade document. Official exchange of this document between two government agencies of different states touches upon legal and policy relevant issues. For example,
    - Certain jurisdictions require minimum retention policies for official documents, so agreements need to be in place that the issuing MA can procure the electronic document during the whole period.
    - If goods arrive but the issuing MA is not capable of submitting the Permits, for example because of technical failure of their own servers or of the Hub, the MA may become liable. The agreement should specify the liability issues.

Electronic exchanges between Government agencies of different countries typically require that both Governments sign a Memorandum of Understanding (MoU) to specify their respective reasonability in the exchange. The WG should provide best practice advice for the content of these MoUs.

5.2 Additional standards required for electronic permit exchanges using a Hub architecture

The above standards are required for point-to-point exchanges and for Hub exchanges.

However, a Hub implies significant complications in the exchange because a 3rd Party (the Hub Service Provider) is now involved in the Government to Government exchange of CITES Permits. As the Hub Service Provider is appointed by the Government agencies, the agencies are fully responsible for the actions of the Hub Service Provider.

This means that software development, governance, liability and security and availability agreements for the Hub Service Provider need to be defined, agreed and funded by the Parties. This means that a complete operational and legal environment regarding the Hub Service provider needs to be developed. Governments will also be responsible for the Auditing of the Hub Service provider.

The development of a Governance Framework for the Hub Service provider is rather complex and requires extensive research. It is suggested that the WG engages a group of legal and technical experts that will conduct further research on this topic. This group should also consult with the Legal Unit of the Secretariat.