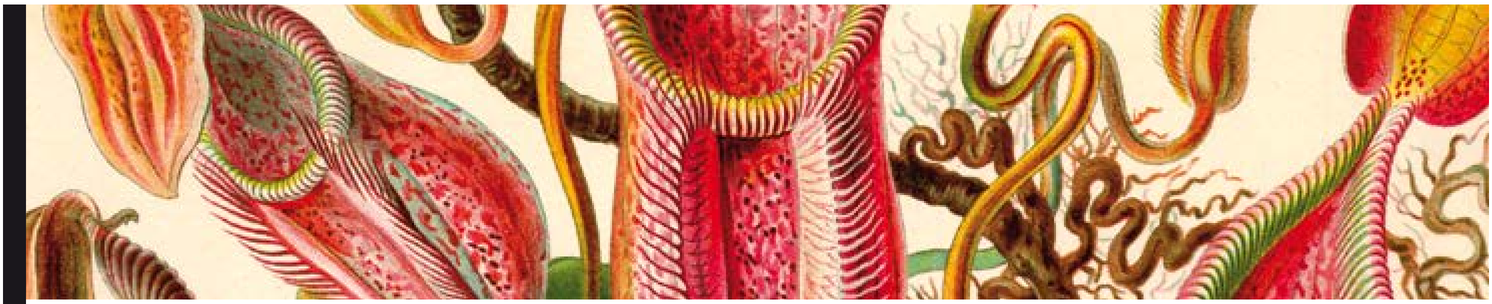
Food and Agriculture Organization
of the United Nations

International Plant Protection Convention
Protecting the world's plant resources from pests

ENG

December 2016



ePhyto Factsheet #10

Security of ePhytos

www.ippc.int

Background

The International Plant Protection Convention (IPPC) Secretariat is working to develop the ePhyto Solution. The Solution and consists of:

1. A generic ePhyto national system (GeNS) available to developing countries for the production, sending and receipt of electronic phytosanitary certificates and
2. An internationally accessible hub to facilitate the transfer of electronic certificates between national plant protection organizations (NPPOs).

Once established and accessible, the Solution should enable Contracting Parties to facilitate trade by communicating phytosanitary certificates in a modern, cost effective and globally harmonized way.
The harmonized exchange of information between countries using their own national system or the GeNS and the hub is based upon standardized transmission rules. A simple schematic diagram of the operation of the Solution is presented in figure 1.

Security of the information

After careful consideration the ePhyto Steering Group has proposed the following security measures:

1. Security of the information during transport

The data that is exchanged between the NPPO will be protected through encryption that is termed **Transport Layer Security (TLS)**. This type of security is similar to what is used in most email services, banking transaction services, etc. TLS protects the information as it moves from the originating service (e.g. the computer of the NPPO) to the receiving service (e.g. the hub) and from hub to receiving NPPO. This should not be confused with "end to end" encryption which encrypts the data throughout the transmission from point of origin (the sending NPPOs service) to point of receipt (the receiving NPPOs service). Countries may choose to agree bilaterally to encrypt data in this manner if they wish. The proposed ePhyto Solution does not include end to end encryption but encrypted messages may be exchanged through the hub.

Key messages on ePhyto security

- The hub will use transport layer security (encryption) to protect the data moving from national plant protection organization (NPPO) to the hub and hub to NPPO;
- The hub will not read the information in the certificate and will only store the certificate until it is received by the NPPO;
- Access to the Solution is based upon public key infrastructure;
- The Solution does not include "end to end" encryption but allows for its use based upon bilateral arrangement;
- The security of data at national systems remains the responsibility of the NPPO;
- Data produced on the GeNS will be stored in secure facilities at the UNICC and will only be available to the NPPO of the country that produced and the NPPO of the country that received the information.

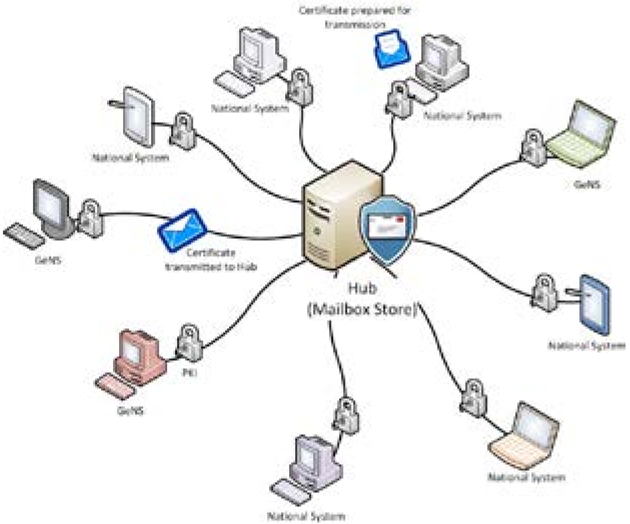


Figure 1

2. Security of the information at the hub

Although data is not encrypted during its temporary presence at the hub, a number of security protocols have been established to ensure that information is secured while at the hub. The hub will only read the information needed to transmit the electronic certificate to its destination, similar to the address information on an envelope. The only data read by the hub consists of the information related to the identity of sending NPPO, the identity of the receiving NPPO and the type of certificate (e.g. phytosanitary certificate, phytosanitary certificate for re-export, certificate number etc.). Once the certificate has been delivered to its destination, the hub deletes the data and only maintains the transaction information for validation purposes. In addition, NPPOs only have access to the certificates addressed to them and all access to the hub system is to be monitored, logged and audited.

3. Access to the hub

Access to the hub by NPPOs will be controlled by way of **public key infrastructure (PKI)**. PKI may be compared to a key and padlock. **The key is a digital certificate sometimes referred to as a client certificate**. Digital certificates are provided by international certificate authorities. The NPPO can only be authorized to access the hub if they have acquired a digital certificate. Each time the NPPOs service communicates with the hub (e.g. to deliver or receive an ePhyto), the hub will verify the certificate of the NPPO's service. At the same time, the NPPO's service should verify the certificate of the hub. In this way, both parties are recognized as authorized users.

The NPPO's GeNS administrator will authorize NPPO users and will provide logon details for each user. The system will be configured to recognize different types of users (e.g. inspectors, authorized officers, clients, etc.) with differing access privileges. Only those NPPO users specified by the NPPO administrator will be permitted to issue certificates or to receive certificates from the hub.

4. Security of the information at the national level

Security of information at the national level remains the responsibility of NPPOs. NPPOs should exercise good data management strategies including limiting access to systems, removing data not required and appropriate archiving and retrieval security practices.

Phytosanitary data produced by the GeNS will be stored by secure servers operated by the United Nations International Computing Centre (UNICC). The data will only be available to the country that owns the information. As with the hub the information will not be read by the UNICC.

Further questions regarding the ePhyto project may be sent to shane.sela@fao.org

Additional resources

The IPPC website has a lot of information on the history of ePhyto development – use the links below to find out more information:

- IPPC ePhyto – home page
- IPPC ePhyto – Steering Group and recent developments
- IPPC ePhyto – codes and schema

Contact us

ePhyto Steering Group
International Plant Protection Convention (IPPC)
Viale delle Terme di Caracalla, 00153 Rome, Italy
Tel: +39 06 5705 4812 | Fax: +39 06 5705 4819
Email: ippc@fao.org | Web: www.ippc.int