Carillon
INFORMATION SECURITY

We Build **TRUST**

Software Solutions

PATHFINDER LSAP SUITE

CREDENTIALS

SOFTWARE SOLUTIONS

MANAGED SERVICES

WE BUILD TRUST BY SECURING THE DATA THAT GOES ON AN AIRCRAFT

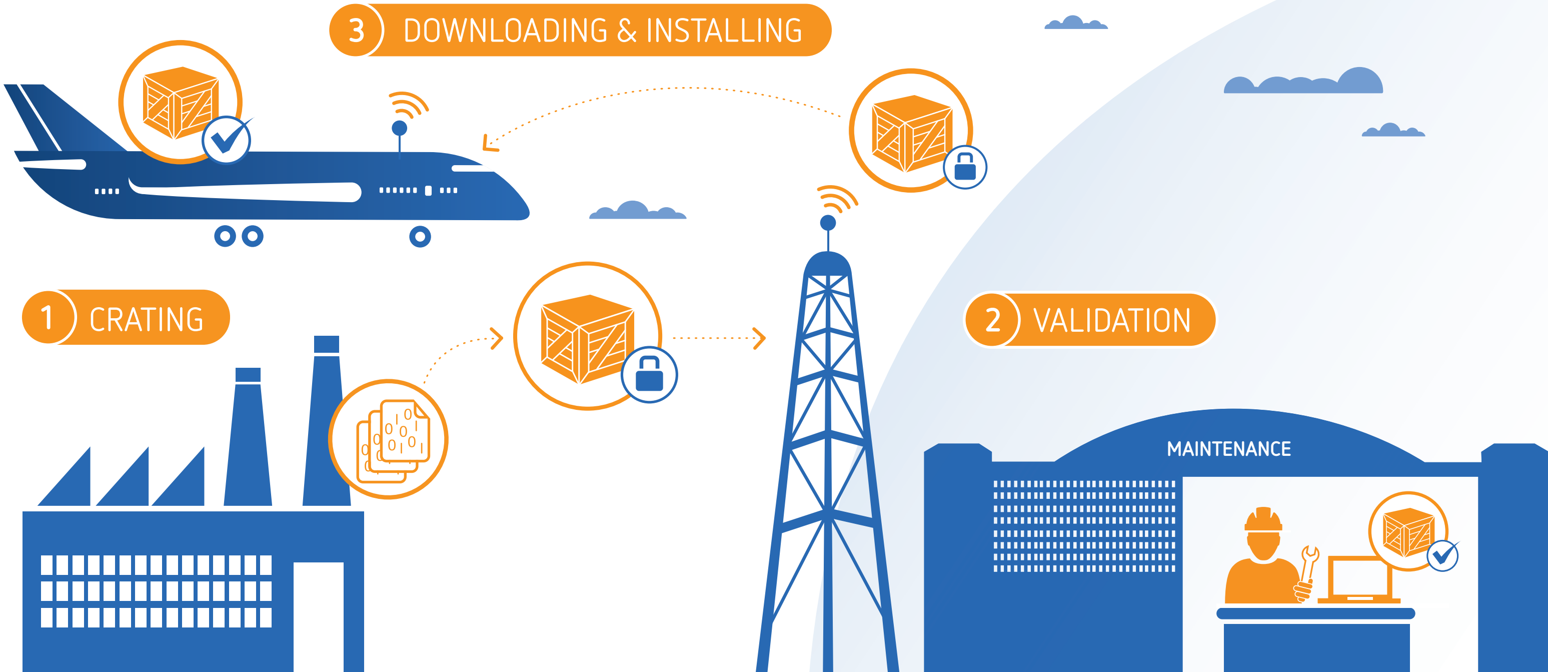
The Challenge: Secure Electronic Delivery of Software to the Aircraft

Conventional methods of updating software of a Line Replaceable Unit (LRU) required the removal of the LRU from the aircraft. The LRU is either returned to the manufacturer for update or an operator uses a specialized Portable Data Loader (PDL) to update the part. Both of these methods involve a significant amount of time, effort and money.

Newer aircraft have the capability to perform on-wing updates of the software using Loadable Software Airplane Parts (LSAP) and Field Loadable Software (FLS).

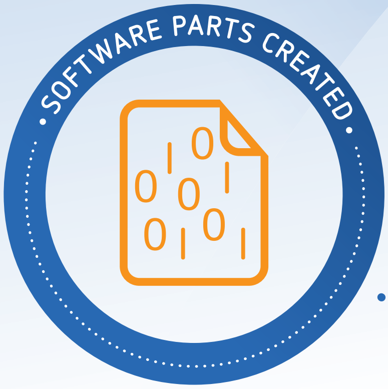
Current rulemaking does not provide for a clear and simple method of performing these on-wing updates and are subject to special conditions. The current security methods are complex and impose unnecessary burden on aircraft operators.

The FAA published policy statement (PS-AIR-21.16-02) which states that the FAA will issue special conditions for initial type certificate (TC), supplemental type certificate (STC), amended TC, or amended STC applications for aircraft systems that directly connect to external services and networks where the network is non-governmental and the aircraft system receives information via the non-governmental network. Examples of these networks include the Internet, Cellular network, airport and operator wireless (i.e. Gatelink, Wi-Fi) networks and portable devices that (iPad, EFB, etc.) that connect to aircraft systems.



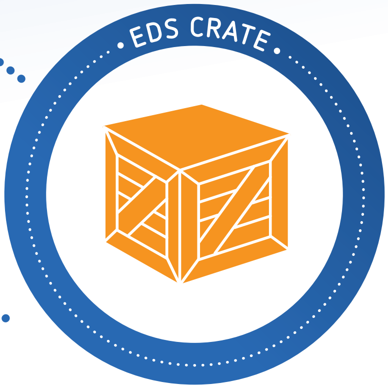
Carillon INFORMATION SECURITY

EDS CRATING AND UNCRATING TODAY



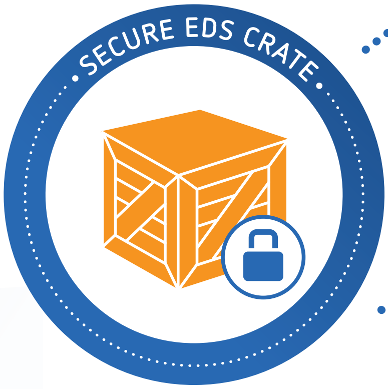
SOFTWARE PARTS CREATED

LSAP and FLS are created at the factory in an environment based on DO-178B or DO-178C.



EDS CRATE

The software is placed into a Electronic Distribution of Software (EDS) crate based on ARINC 827 at the factory prior to delivery to the operator.



SECURE EDS CRATE

The EDS can be secured based on ARINC 835 and ARINC 842 at the factory prior to delivery to the operator, or by the operator prior to delivery to the aircraft. This additional method imposes additional IT requirement on the part of the manufacturer and operator.

EDS VALIDATION

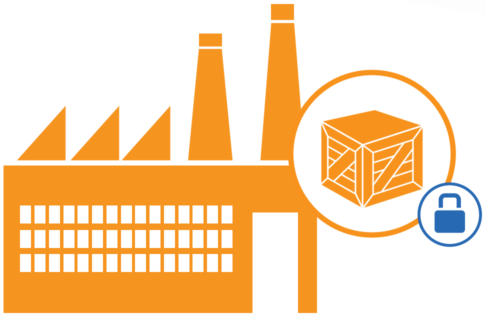
The EDS crate is delivered to the operator via electronic means, such as a web portal, e-mail, etc. The software is uncrated and validated using computer workstation.

SOFTWARE PARTS INSTALLED

The software is delivered to the aircraft using wireless interface, a USB memory stick or connecting a laptop computer to the appropriate interface(s) in the aircraft.

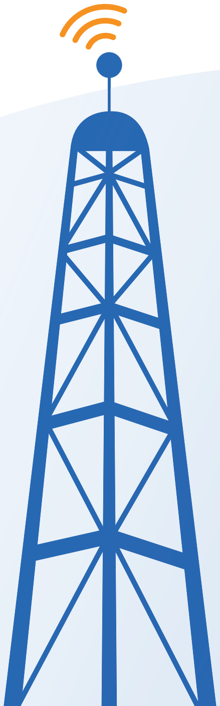
Carillon
INFORMATION SECURITY

EDS CRATING AND UNCRATING MOVING FORWARD



1 Software is placed into an ARINC 827 EDS crate. The EDS crate is digitally signed and validated using SCVP service according to ATA Spec. 42. The EDS crate can include the "Electronic 8130-3, Form One and Form 1" Authorized Release Certificates. SCVP will be incorporated into ARINC 835 and ARINC 842 in the near future. Using SCVP at the factory means less of an impact on maintenance operations and requires little to no additional IT overhead on the part of the operator thereby reducing operator costs.

2 As the amount of software required for digital aircraft increases and the cost of wireless communications decreases, operators are increasingly asking to automatically transfer and load software on the aircraft via digital methods. These methods typically involve the use of public networks such as the Internet, Cellular & Satellite networks along with airport and operator Wi-Fi networks. Communication networks that are not controlled by government agencies are generally considered to be insecure. The use of public networks for software delivery to aircraft systems is of greater concern to the authorities.



3 As the aircraft environment is generally considered to be secure, established procedures and rulemaking exists for certain types of software delivery to aircraft systems. Implementing the use of SCVP on the aircraft simplifies the security process and enables operators to take advantage of existing procedures with minimal process changes and remain compliant to current special conditions and comply with future special conditions with minimal process changes. Using SCVP enables the uncrating of software in the aircraft and performing on-wing installation with no further ground communication requirements.

Carillon's Pathfinder LSAP Suite was built for next generation aircraft and provides all the necessary tools to migrate to today's best practices in cyber security surrounding the aircraft.

LSAP Modules

Workstation Signer: This web based application allows the data provider to take electronic data files. This tool will then crate the information and digitally sign it to guarantee authenticity of signer and data integrity of the crate. This customized solution can easily be integrated with a corporate electronic data management solution.

Workstation Validator: Very similarly to the Workstation Signer, the Workstation Validator is designed to allow the ground crew to confirm data crate integrity and signers authenticity. Thus confirming crate was signed by an approved content provider.

On Aircraft Validator: This application performs the same function as the Workstation Validator, but all of the EDS crate validation is performed on the aircraft, no ground station interaction is required.

The LSAP modules allow software providers to crate data with a few clicks. Validation is just as quick. No more CD's or data failures, Carillon's Pathfinder LSAP Suite is a quick and efficient way to get updates completed and get an aircraft off the ground quickly and efficiently.

Trusted Credentials

Spec 42 compliant credential platform issuance service: Carillon provides a variety of digital credentials that meet or exceed Spec 42 requirements. As part of the deployment of the LSAP modules, trusted credentials are part of the trust fabric that makes up the Pathfinder LSAP Suite.

About Carillon

Carillon provides a complete spectrum of identity management solutions that are designed to prevent identity theft, promote the migration from paper to electronic authentication, and avoid loss of intellectual property. From consulting services, to validation software and managed identity services, Carillon can provide the skill sets and tools to help companies take control of their corporate digital credentials.

CREDENTIALS

Digital Certificates
PIV-I Credentials
Specialty Digital Certificates

SOFTWARE SOLUTIONS

CertServ Identity Management Suite

- Certificate Authority
- Identity Management
- Key Recovery Server
- Online Status Certificate Protocol Responder
- Certificate Revocation List Publisher
- Time Stamp Server

Pathfinder Suite

- SCVP Server
- SCVP Client
- Web Proxy
- Radius Server
- LSAP
- Web Registrar

Trust Validator
e-ARC
Certificate Discovery Services

MANAGED SERVICES

Managed PKI for Airlines
Managed Corporate PKI
Managed PIV-I Services
PKI Consulting

Carillon INFORMATION SECURITY

www.carillon.ca
info@carillon.ca
+1 514 485-0789