Blockchain Technology for Aircraft Maintenance and Engineering

September 19, 2019

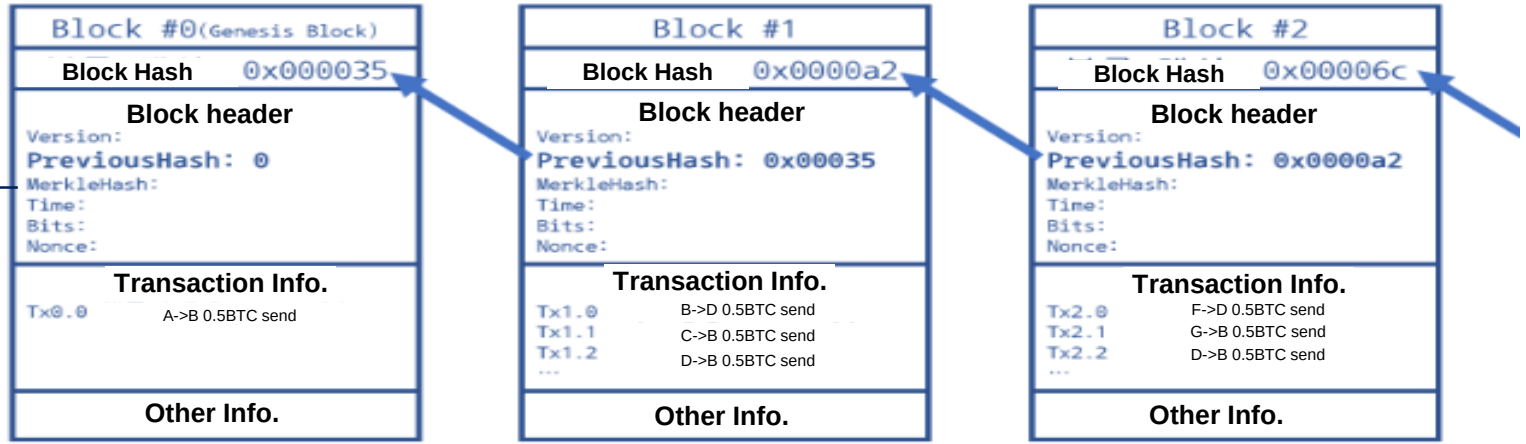
Prepared by **Albert S. Choi**

STX Aero Service
Korea University

Contents

Contents

• Shape of Blockchain



Block header : **version**
+ previousblockhash
+ merklehash
+ time
+ bits
+ nonce

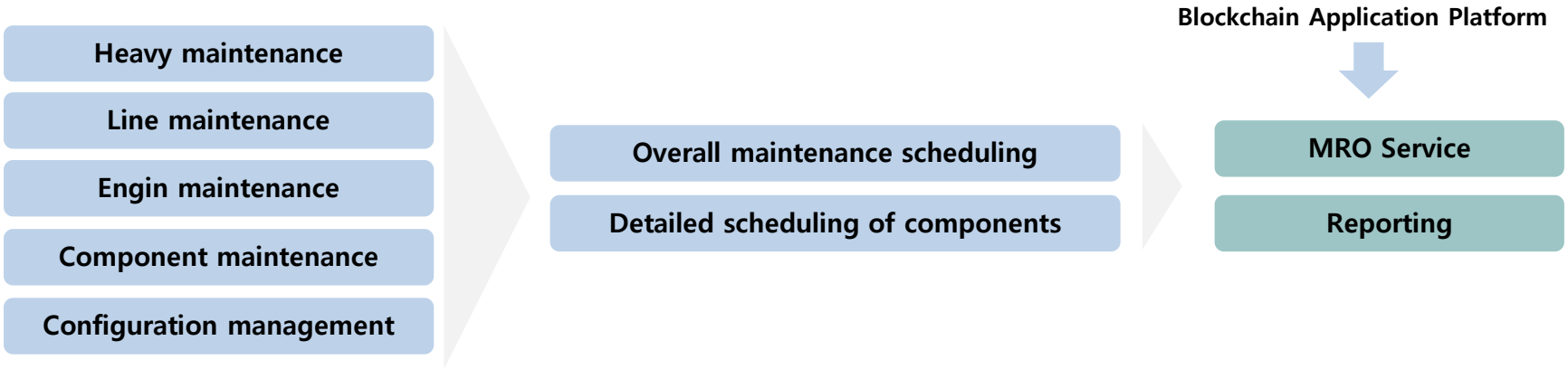
Merkle Patricia Trie -→ Key Value Database

- **Properties of Blockchain**
  - Irreversibility
  - Information symmetry among network nodes
  - Public chain vs. private chain by DID(Distributed ID)
  - Token generation (included within private chain)

- **Current trends of Blockchain technology**
  - Speed : block creation & finality
  - Storage : needs new concept to store old data outside
  - Multi-blockchain: imitates the legacy DB functionalities
  - DID: Self sovereign ID and universal classification method including users, network, IoT, component, document and so on.
  - Block consensus :PoW, PoS, BFT

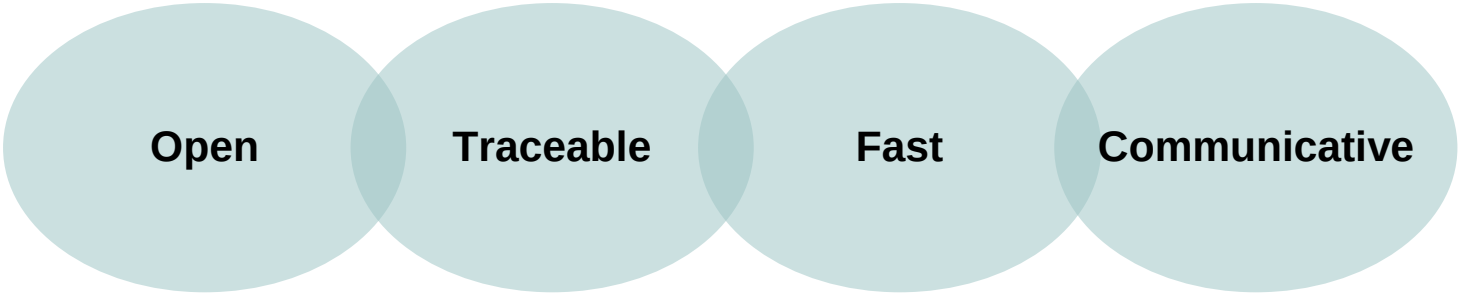
- **Major Problems to be solved**

  - Closed operation of MRO service among participants
  - Difficult traceability in Components including Life Limited Part
  - Limited sharing of document by relevant users
  - Burdensome document generation
  - Non-communicative document storage



- **Advantages by blockchain technology**

  - **Open operation of MRO service among participants**
  - **Easy traceability in components and their history**
  - **Open sharing of document by relevant users**
  - **Fast document generation**
  - **Communicative tools for document storage**



Contents

DID - Actors - DID & Credential Issuer

DIDs for organization ID should be issued by IATA Task Group commonly and component ID are issued by authorized manufacturers when component comes out to the commercial market. All relevant documents relating to MRO service, credentials, can have the credential ID. Component ID plays a key tor retrieve the all activity data of MRO service.

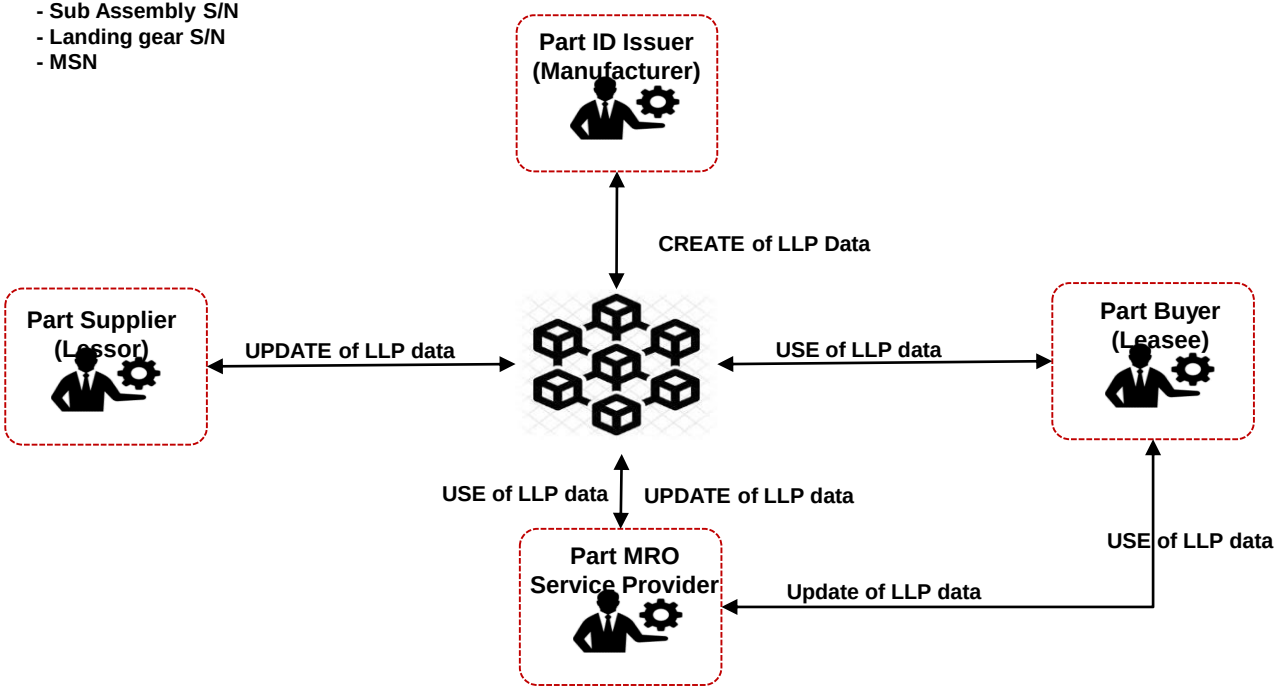
DID Issuer	Organization ID Issuer 	Component ID Issuer 	Credential Issuer 
Player	• IATA • IATA MCG	• Boeing • Airbus	• Airline MRO • Independent MRO
Blockchain Ledger Data	• Airline MRO Unit ID • MRO company ID • Supervisor ID • Certified Engineer ID	• Aircraft Model • MSN • Registration Number • Engine Type • ESN • Engine Position • APU Type • APU SN • Nose Landing Gear PN/SN • Main Landing Gear RH PN/SN • Main Landing Gear LH PN/SN • .Detailed Part Information	• Document(Credential) ID • Document Length • Document Hash • Document format Number • State • Issuer ID • Reference Code : Document Hash • Starting Date • Ending Date • Issuer Signature
Storage Data	• Airline MRO Unit –Detailed Info. • MRO company –Detailed info. • Supervisor –Detailed info. • Certified Engineer –Detailed info.		• Authorized Release Certificate • LLP Removal & Installation • Life Limited Part Status Sheet • Aircraft Equipment List Report

DID - Actions – LLP Data Create/Update/Use

LLP data is created by LLP manufacturer and is maintained by supplier, buyer and MRO service provider. All of data manipulation is recorded into Distributed Ledger and any errored input should be reentered to trace the activity history.

Data

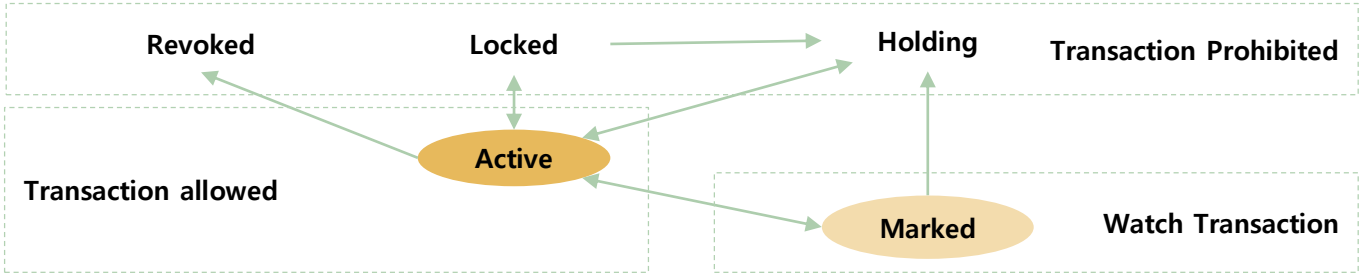
- **LLP Data for Data with DID and Action (S/N, Total Hour , Total Cycle)**
  - **Minimal LLP S/N**
  - **Sub Assembly S/N**
  - **Landing gear S/N**
  - **MSN**



DID

- **User : DID : Credential = 1 : 1 : n**
- **Additional Credential issue & update is only executed by CA which issue the current DID**
- **DID is recorded on the block by CA on the request of wallet.**

	DID Issue	Issuer Verifier	Credential				
			Issue	Update	Locked	Revoked	Marked
Private CA	O	O	O	O	O	O	O
Public CA	O	X	O	X	O	O	O



DID = 10 bytes

DID Example

Master CA's 1st Credential	0x0001 000000000001 0002
Master CA's 2nd Credential	0x0001 000000000001 0003
1st CA's 1st Credential	0x0002 000000000001 0002
1st CA's 2nd Credential	0x0002 000000000001 0003
1st CA's 1st User's 1st Credential	0x0002 XXXXXXXXXXX 0002
1st CA's 1st User's 2nd Credential	0x0002 XXXXXXXXXXX 0003
1st CA's 2nd User's 1st Credential	0x0002 YYYYYYYYYYY 0002

DID - Data Structure

- Every user has unique DID with multiple credentials
- DID is created by CA(Certified Access) node and consist of 10 byte random number, which guarantees the singularity and integrity,
- Transactions on the blockchain are written with DID so that the storage capability would be enhanced, while existing blockchain platforms use 20-byte public key for transactions.
- An user can create ID and all Credentials by using smart wallet.
- DID and all Credentials are written on ID blockchain.
- Private key is stored in the smart wallet safely placed into the key store.

DID consists of 10 bytes.

- **Version (2bit)**
- **Citizen ID (CA ID 14 bit + random 6 Bytes)**
  = 256 *256*256*256*256*256
  = 281,474,980,000,000 accounts
  = IATA User ID
  = Certified and Trusted ID
- **Sequence Number (2 Bytes)**

B: Byte(s) b:bit(s)

SSII (Self Sovereign Identity Information)				
Field			Size	Description
DID	Version		2 b	0: version
	Citizen ID	CA ID	14 b	0x0001 : Master CA 0x0002 ~ 0x3FFF : CA
		Random	6 B	0x00…01:CA Random Number : general user (check duplicacy)
			2 B	1: General Credential 2 ~ : Basic Credential

DID - Data Structure

- Credential contains public key, role, verification flag, state, credit, country, reference code, country, validity starting date, validity ending date.
- Issuer Signature (65B ECDSA encryption method)
- Role : classification of account usage
- State : account status

Structure of Basic Credential

- Public key = hashed key = account
- Role = role of CA node (cf) verisign
- Verification flag
- State : Account status
- Credit : data can be written by oraclizer
- Country

Credential (Basic)	PublicKeyHash	20 B	Hashed Public Key
	Role	2 B	0x0001: General 0xF0F0: Master CA 0xF0F1 : CA
	Verfication Flag	3 b	Reserved
		1 b	Deposit
		1 b	Face to Face confirmation
		1 b	National Identity confirmation
		1 b	Mobile phone number confirmation
		1 b	E-mail confirmation
	State	1 B	0x01: Active 0x02: Revoked 0x03: Locked 0x04: Hoding 0x05: Marked // IATA setting (Oracled transaction)
	Credit	1 B	Credit Grade // IATA setting (Oracled transaction)
	Country	1 B	Country code

■ General Credential

- Document ID
- Document Length
- Document : format N bytes
- State
- Issuer ID
- Reference Code
- Starting date
- Ending date
- Issuer Signature

▪ Role of General Credential(Document Format)

Field		Size	Description
SymID		10 B	
Credential (General)	DocID	20 B	Document ID
	Length	2 B	Document length

	Document	N B	{
			Type : Doc or Format
			Format ID : DID.DocID
			Contents : { … }
			}

	State	1 B	0x01 : Active, 0x02 : Revoked
	Issuer ID	10 B	Issuer DID
	Ref. code	4 B	Issuer reference (dApp ID, CA assign, Big data usage)
	NotBefore	8 B	Validity starting date // yyyymmdd + (00:00:00), UTC+0
	NotAfter	8 B	Validity ending date // yyyymmdd + (00:00:00), UTC+0
Issuer Signature		65 B	

Contents

Blockchain Ledger Platform – Required Properties

LLP data is created by LLP manufacturer and is maintained by supplier, buyer and MRO service provider. All of data manipulation is recorded into Distributed Ledger and any errored input should be reentered to trace the activity history.

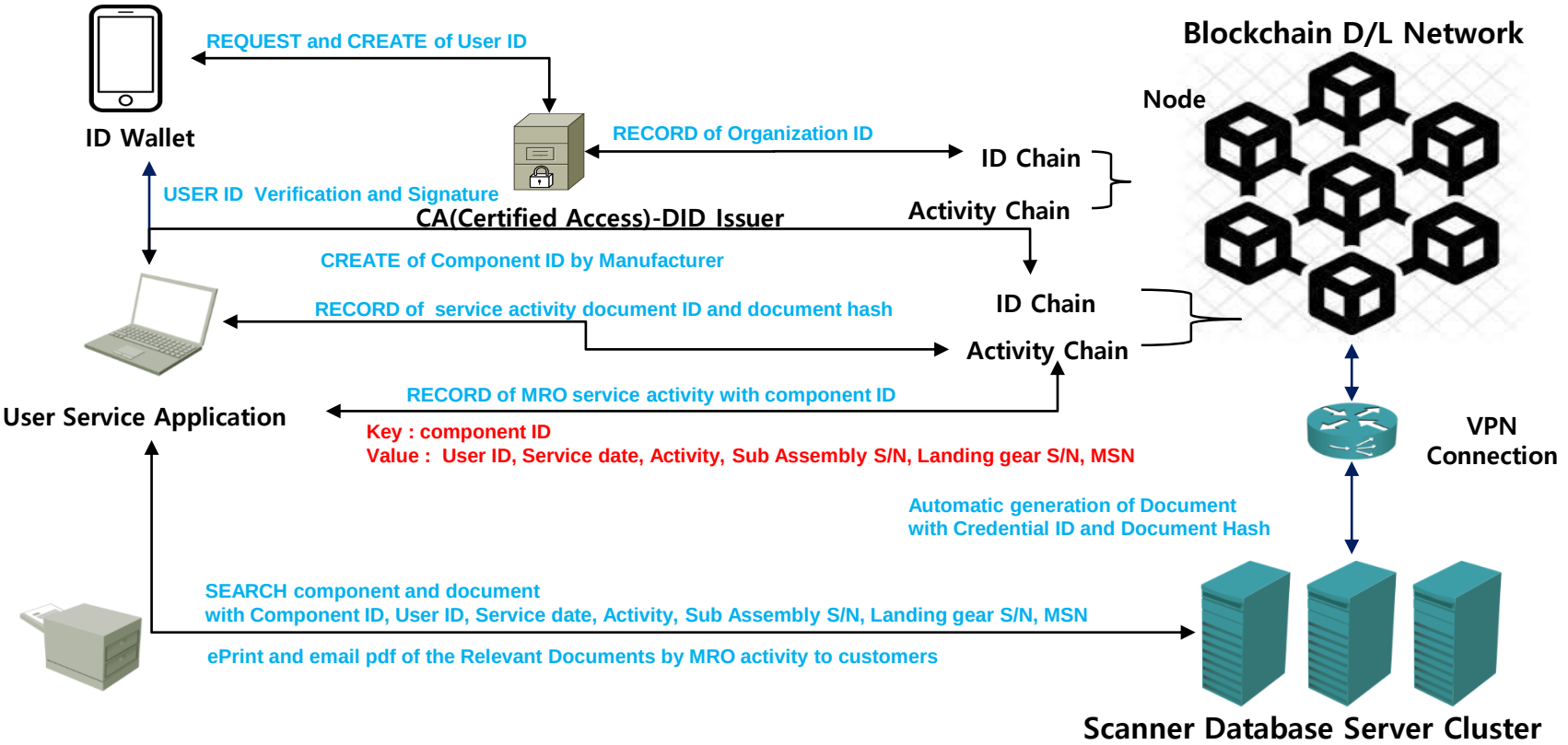
Required Platform Properties

Minimality	• The least component in sub-assembly should be the index key of D/L • Example – Main landing gear - Gear Shock Strut(2.1.1) –Inner Cylinder(2.1.2.3)
Irreversibility	• Any data in D/L cannot be modified so that the D/L should automatically generate the scanner database in read-only mode.
Integrity	• Any data and related document can be retrieved by use of the Aircraft MSN, Component P/N and S/N.
Individuality	• LLP-related data should be retrieved by any hierarchical level of component.
Traceability	• LLP can be traceable by the combinational data retrieval of both D/L and centralized scanner database.
Deliverability	• DID wallet and HTML5 compliant user interface can automatically generate the relevant MRO activity documents from MRO service provider to interested parties including airline operator and others.

Blockchain Distribute Ledger Platform – Structure and Characteristics

- **Blockchain D/L platform consists of D/L network nodes, ID issuer node and Scanner Database server cluster.**
- **These platform is basically private blockchain platform.**
- **ID Wallet requests ID issue to CA(Certified Access), after it generates Public Key and Private Key. ID wallet has a self sovereign ID that has no password to access platform .**
- **Blockchain D/L node has two blockchains including ID chain and Activity chain.**
- **Number of Blockchain D/L nodes can be extended from 7 nodes (at minimum) to 25 nodes at maximum.**
- **It is also possible to add one more blockchains for the further service activity needs like market transaction.**
- **Scanner database is automatically updated by the new data entry of blockchain D/L Activity chain.**
- **Relevant documents are generated by MRO users or Manufacturer based upon the D/L data, requested by the users such as airlines or MRO service providers or traders.**

Blockchain Distribute Ledger Platform – Structure and Service Flow



Contents

Aircraft Status Data Structure -737NG

(From Non-Incident & Accident Statement)

Target of Component ID :Key

Target of Component ID : Value

Total Hour | Total Cycle

Aircraft Model:
MSN:
Registration Number:

Engine Type:
ESN:
Position:

Engine Type:
ESN:
Position:

APU Type Type:
APU SN:

Nose Landing Gear

Main Landing Gear RH

Main Landing Gear LH

Target of Component ID : Key

Aircraft Model: MSN: Registration Number:	737 800-86N 2 TC-AAR	Total Hour	Total Cycle
		58866:29	26381
Engine Type: ESN: Position:	CFM56-7B26/3 87 #1	Total Hour	Total Cycle
		56040:19	24705
Engine Type: ESN: Position:	CFM56-7B26/3 8 #2	Total Hour	Total Cycle
		56434:16	24953
APU Type: APU SN:	131-9B P-6	Total Hour	Total Cycle
As of 17 Jan 2019		18860.7	30576
Nose Landing Gear	P/N 1 -5 S/N T	62680:29	30865
Main Landing Gear RH	P/N 16 S/N MAL01	58861:29	26517
Main Landing Gear LH	P/N 1 -35 S/N MAL01	58861:29	26517
		Total Hour	Total Cycle

Case Study – 737NG- Landing Gear- Nose Landing Gear

Nose Landing Gear

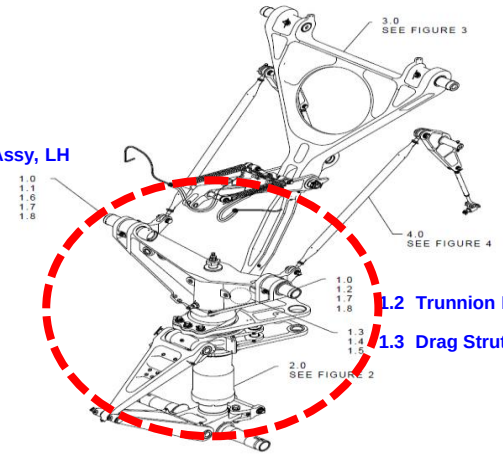


Figure 1. Nose Landing Gear Installation (737NG Shown)

Target of Component ID :Key

Nose Landing Gear –Shock Strut

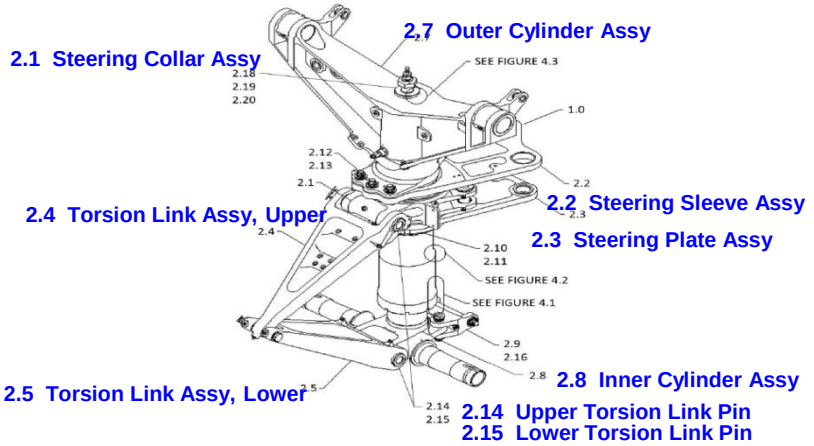


Figure 2. Nose Landing Gear Shock Strut Assy (737NG Shown)

Case Study – 737NG-Landing Gear- Main Landing Gear

Main Landing Gear

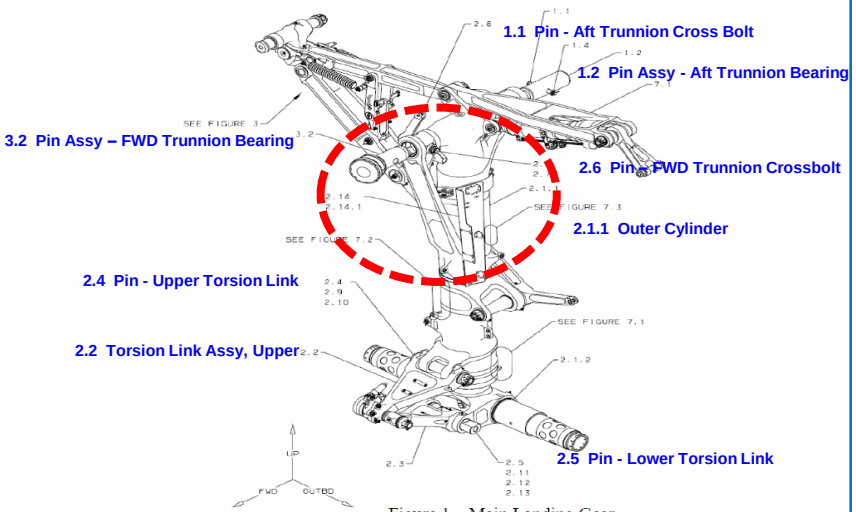


Figure 1. Main Landing Gear

Target of Component ID :Key

Main Landing Gear –Shock Strut

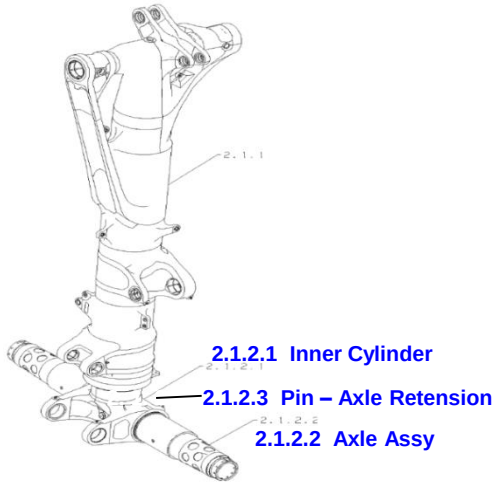


Figure 2. Main Landing Gear Shock Strut Assembly

Case Study – Life Limited Part - Landing Gear

Target of General Credential ID : Key

Component Traceability Record

COMPONENT TRACEABILITY RECORD

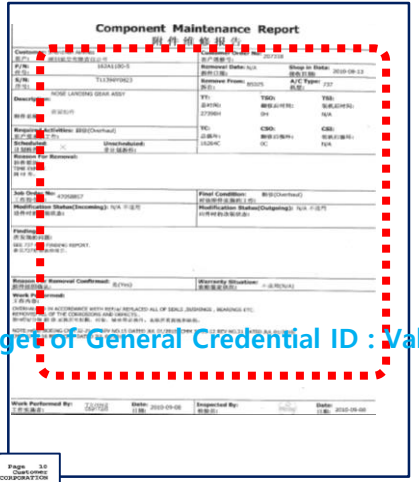
LH Main Landing Gear Assembly

P/N : 161A1100-35 S/N : MAL01087Y0534

Seq	Movement History	A/C or NHA	Date	CSN	Reference	Source
1	Manufactured and Installed	TC-AAO/MSN 28619	18-May-00	0	①	Boeing
2	Removed for Overhaul	TC-AAO/MSN 28619	18-Nov-09	9,955	②	Pegasus Airline
3	Overhauled by Turkish Technic		29-Dec-09	9,955	③	Turkish Technic
4	Installed for service	TC-AAR/28624	8-Jan-10	9,955	④	Pegasus Airline
5	Removed	TC-AAR/28624	21-Feb-19	26,517	⑤	Pegasus Airline

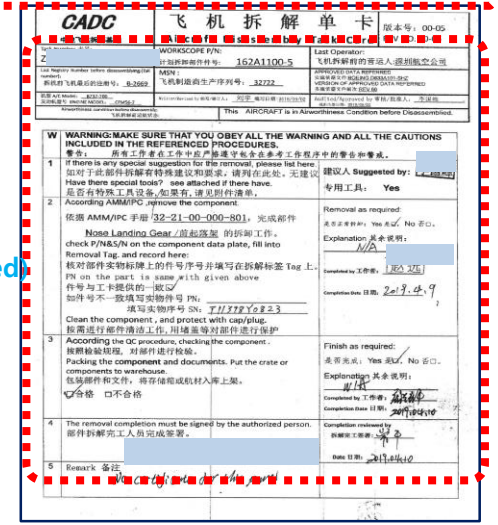
Target of General Credential ID : Value (hashed)

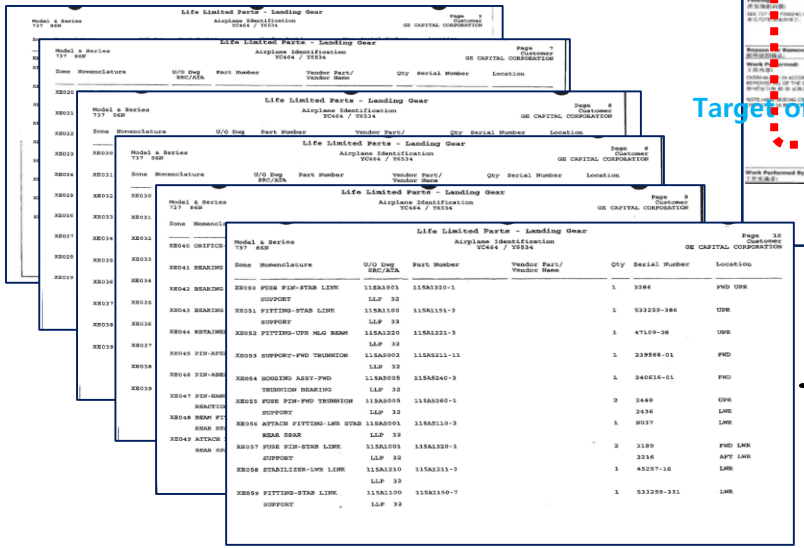
Component Maintenance Report



Target of General Credential ID : Value (hashed)

Disassembly Task Card





Target of Component ID :Key

Target of Component ID : Value

Total Hour

Total Cycle

- **Component Traceability Record**
  - **Authorized Release Certificate (FAA Form 8130-3 /EASA Form ONE)**
  - **LG Removal & Installation Record**
  - **Life Limited Part Status Sheet**
  - **Aircraft Equipment List Report**

Aircraft LLP Data Structure

Target of General Credential

COMPONENT TRACEABILITY RECORD

Target of Component ID :Key

LH Main Landing Gear Assembly

P/N : 161A1100-35 S/N : MAL0123456789

Target of Component ID : Value - Activity

Each Record by date

Seq	Movement History	A/C or NHA	Date	CSN	Source	Reference
1	Manufactured and Installed	MSN XXX	18-May-00	0	Boeing	①
2	Removed for Overhaul	MSN XXX	18-Nov-09	9,955	P-Airline	②
3	Overhauled by T-MRO		29-Dec-09	9,955	T-MRO	③
4	Installed for service	MSN YYY	8-Jan-10	9,955	P-Airline	④
5	Removed	MSN YYY	21-Feb-19	26,517	P-Airline	⑤

Target of Component ID : Value

- Thank you