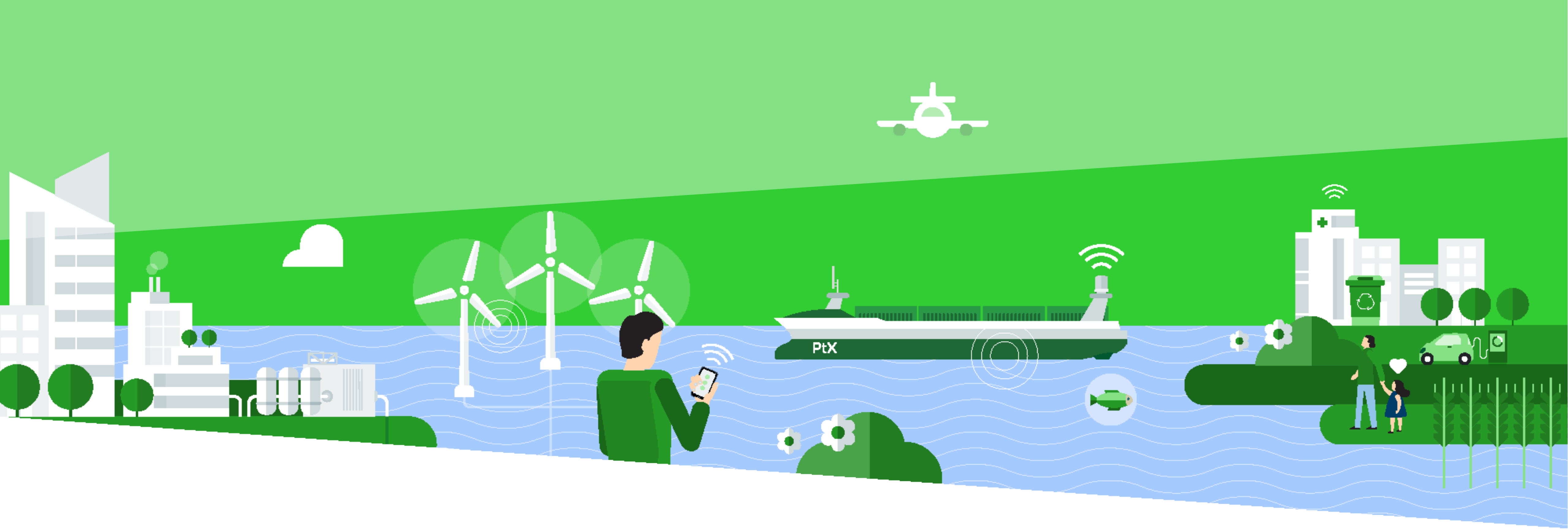


High Level Security Architecture for DCC Exchange

ahkl@forcetechnology.com

Ahmed Khan Leghari
09.10.2023

What is a Calibration Certificate?

- A calibration certificate is a document that contains information about a device's calibration.
- This certificate provides valuable **information** on the **quality** and measurement **accuracy** of the device.

- At present each device that gets calibrated is issued with a paper based **manual** Calibration Certificate

➢ **A sample calibration certificate for a temperature and relative humidity data logger sensor**

CIQA

Certificate of Calibration

Certificate Number: 4 - 101535
Instrument Name: Temperature & Humidity Datalogger
Model: EZ-TrH Humidity F2.5 -35 C 16K
Serial Number: 10153
Instrument Number: 4
Manufacturer: EZLOGGER

Cal Date: 10/9/2019 Calibration Due Date: 10/9/2020

Instrument Condition: ☐ Out of Tolerance, ☑ In Tolerance

CIQA, Inc. certifies that the above instrument meets or exceeds published measurement specifications (unless otherwise noted) and has been calibrated using standards traceable to the National Institute of Standards and Technology. This certificate shall not be reproduced, except in full, without the written approval of CIQA Inc.

Room Temp 80.9 °F, % Relative Humidity 41.9 %

Standard{s} Used:

Manufacturer	Model Num	Serial Num	Due Date	NIST Num
VAISALA	HMI41	X3810015	10/01/2020	ISO/IEC-17025-2005

Datalogger # 4

TEMPERATURE °F

Scale	Nominal Std Ref. Vaisala Reading	Datalogger Reading	Datalogger Accuracy	As Found Deviation	Corrected Final Reading	Pass/Fail
Low	59.5	59.3	0.5	0.2	59.5	Pass
Medium	80.9	80.5	0.5	0.3	80.9	Pass
High	99.8	101.6	0.5	-1.8	99.8	Pass

% RELATIVE HUMIDITY

Scale	Nominal Std Ref. Reading	Datalogger Reading	Datalogger Accuracy	As Found Deviation	Corrected Final Reading	Pass/Fail
Low	16.4	24.1	3.0	-7.7	16.4	Pass
Medium	41.9	50.3	3.0	-8.5	41.9	Pass
High	66.3	65.8	3.0	0.5	66.3	Pass

Completion Report	
Calibration Performed by: (Electronic Signature) Print Name Quintana *Quintana*	Date: 10/9/2019
Calibration Review by: (Electronic Signture) Print Name: Cayuela	Date: 10/9/2019

Reference: https://ciqa.net/what-is-a-calibration-certificate/

Digital Calibration Certificate

- Paper based Calibration Certificates can be digitized as a PDF document
- Technically a PDFized DCC is a Digital Version of the Calibration Certificate
- PDFized DCC Version is good for human readability, however, the goal is to make a DCC that is machine readable.
- Machine readability ensures machine to machine communication and exchange of DCC without any human intervention.
- M2M DCC exchange would result in faster, error free, transparent and globally compatible solution.

Temprecord International Limited
Unit D, 239 Burswood Drive, Auckland, New Zealand
Website: www.temprecord.com

Calibration Certificate

REPORT No 201410109
CLIENT
DESCRIPTION Medical Logger Red
TEMPERATURE CALIBRATION DATE 20/01/2014 10:54:48
CALIBRATION EXPIRES 21/03/2016 10:54:48
LOGGER SERIAL No S0087228
TEMPERATURE REFERENCES HART 1502A - Platinum Resistance Thermometer

Temperature Calibration Method: This temperature data logger has been tested and adjusted using Temprecord method 05/2006/02. The temperature scale used is ITS-90.

Temperature Calibration Results: The logger was calibrated at -15.00 °C, 0.00 °C, +40.00 °Celsius. Any required corrections were programmed into the logger at the time of calibration.

Temperature Calibration Uncertainty: The expanded uncertainty for the logger is 0.2 °C over the temperature range from -20 °C to +50 °C. The expanded uncertainty is expressed at a 95 % confidence level. The coverage factor is k=2.09.

Reference Temperature	Logger Temperature	Reference S/N
-0.56 °C (30.99 °F)	-0.54 °C (31.03 °F)	HART,1502,69637,4.30
-15.14 °C (4.75 °F)	-15.14 °C (4.75 °F)	HART,1502A,A29923,5.
40.67 °C (105.21 °F)	40.68 °C (105.22 °F)	HART,1502A,A8C195,5.

Signed
Name Joanne Chen
Position Approved Signatory
Date Tuesday, 21 January 2014 9:14:24 a.m.

This certificate may not be reproduced except in full
Page 1 of 1

Reference: https://temprecord.com/wp-content/uploads/2018/10/PDF-REDO-01.png

Digital Calibration Certificate

XML Schema for a DCC by Physikalisch-Technische Bundesanstalt (PTB)

```
<xs:complexType name="digitalCalibrationCertificateType">
    <xs:annotation>
        <xs:documentation>
            The root element that contains the four rings of the DCC.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="administrativeData" type="dcc:administrativeDataType"/>
        <xs:element name="measurementResults" type="dcc:measurementResultListType"/>
        <xs:element name="comment" minOccurs="0">
            <xs:complexType>
                <xs:sequence>
                    <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="document" type="dcc:byteDataType" minOccurs="0"/>
        <xs:element ref="ds:Signature" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="schemaVersion" use="required">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="3\.2\.1"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
```

Temprecord International Limited
Unit D, 239 Burswood Drive, Auckland, New Zealand
Website: www.temprecord.com

Calibration Certificate

REPORT No 201410109
CLIENT
DESCRIPTION Medical Logger Red
TEMPERATURE CALIBRATION DATE 20/01/2014 10:54:48
CALIBRATION EXPIRES 21/03/2016 10:54:48
LOGGER SERIAL No S0087228
TEMPERATURE REFERENCES HART 1502A - Platinum Resistance Thermometer

Temperature Calibration Method: This temperature data logger has been tested and adjusted using Temprecord method 05/2006/02. The temperature scale used is ITS-90.

Temperature Calibration Results: The logger was calibrated at -15.00 °C, 0.00 °C, +40.00 °Celsius. Any required corrections were programmed into the logger at the time of calibration.

Temperature Calibration Uncertainty: The expanded uncertainty for the logger is 0.2 °C over the temperature range from -20 °C to +50 °C. The expanded uncertainty is expressed at a 95 % confidence level. The coverage factor is k=2.09.

Reference Temperature	Logger Temperature	Reference S/N
-0.56 °C (30.99 °F)	-0.54 °C (31.03 °F)	HART,1502,69637,4.30
-15.14 °C (4.75 °F)	-15.14 °C (4.75 °F)	HART,1502A,A29923,5.
40.67 °C (105.21 °F)	40.68 °C (105.22 °F)	HART,1502A,A8C195,5.

Signed
Name Joanne Chen
Position Approved Signatory
Date Tuesday, 21 January 2014 9:14:24 a.m.

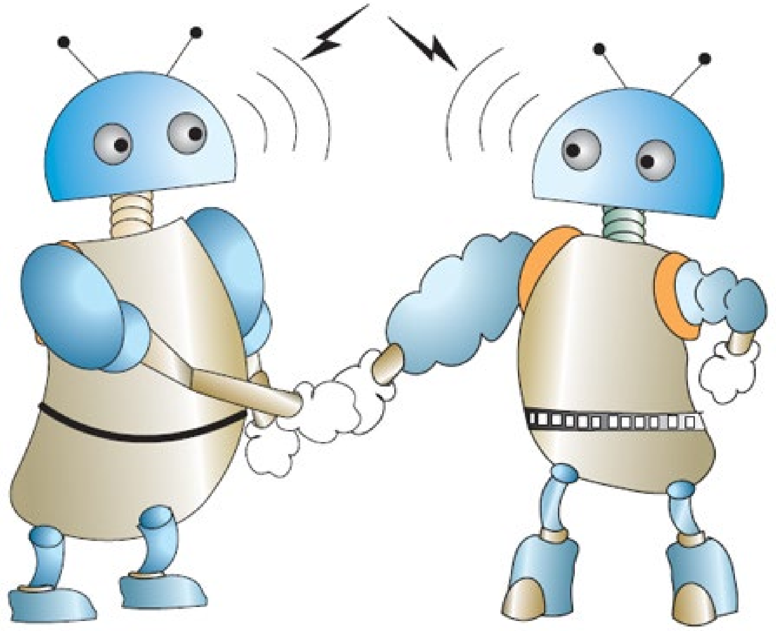
This certificate may not be reproduced except in full
Page 1 of 1

Reference: https://temprecord.com/wp-content/uploads/2018/10/PDF-REDO-01.png

FORCE TECHNOLOGY

Exchange of DCC over Network Has it's Own Challanges

- DCC can be issued for devices, sensors and machines installed in domains such as **health, secuirty, miltary banking sectors.**
- So **securing** a DCC exchange over a network is important
- Indeed data is an asset, and securing data (sensitive or non- sensitive) over a network is nowadays a new normal.



Ref: https://techstory.in/machine-to-machine-12781212/

FORCE TECHNOLOGY

Challenges : Sending DCC over a Network

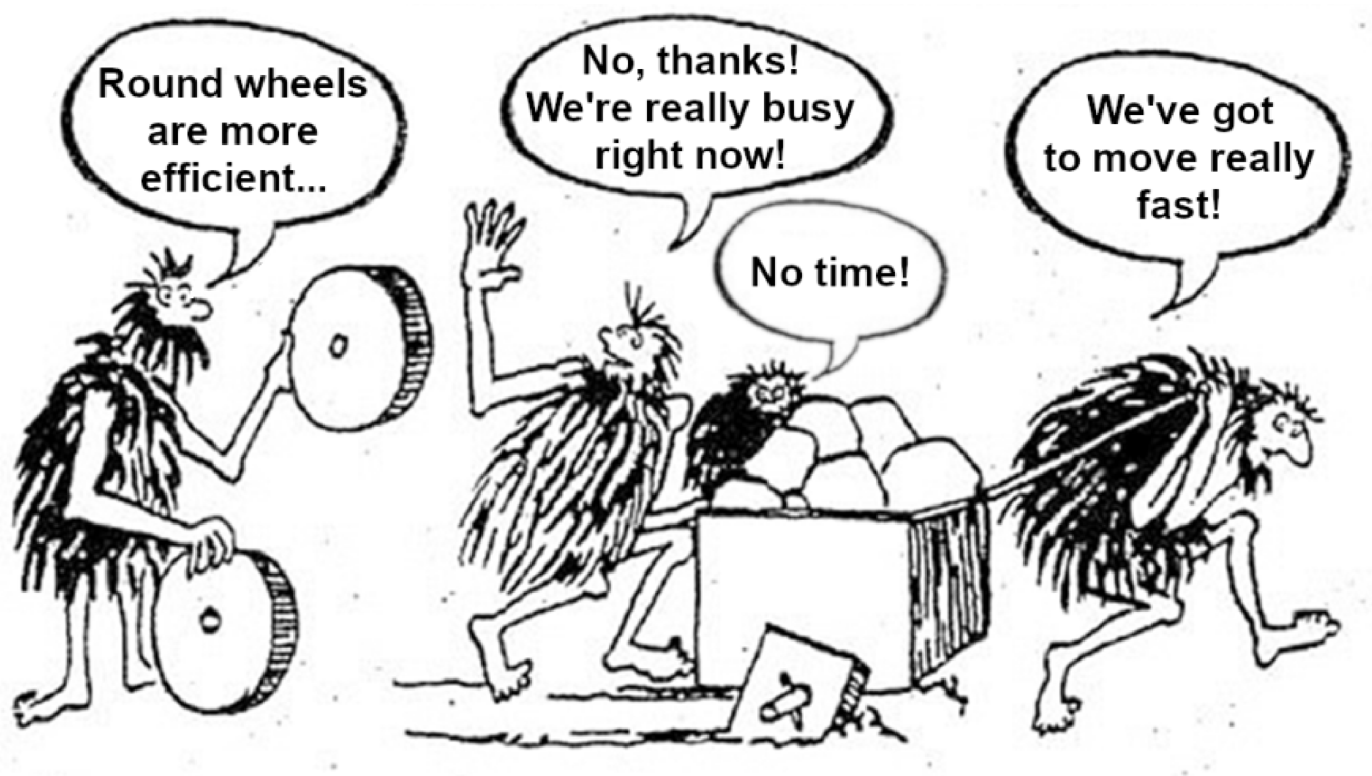
- **Integrity**: the DCC hasn't been altered in transit
- **Authenticity**: the author of the DCC is really who they claim to be
- **Non-repudiation**: the author of the DCC can't later deny that they were the source
- **Security and Privacy** : To secure the contents of the DCC

FORCE TECHNOLOGY

Infrastructure for generation and distribution of DCC

- Why should we reinvent the wheel? When already tried and trusted methods of secure data communication are available.

- A combination of **cryptographic techniques** can be used to securely transmit the DCC, ex. Public-key cryptography.



https://smartstudios.io/blog/covid-19-is-not-a-time-to-reinvent-the-wheel/

Let’s use cryptography to secure the contenets of the DCC

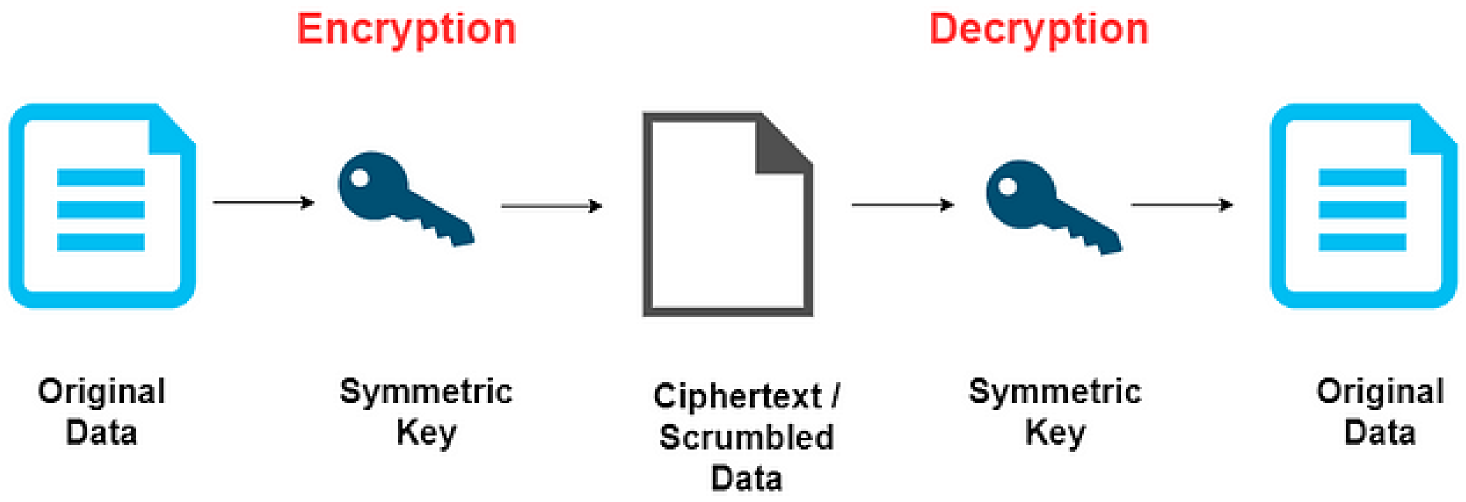
- **Cryptography** uses mathematical techniques to transform data and prevent it from being read or tampered with by unauthorized parties.

- **Encryption** is the process by which a readable message is converted to an **unreadable format** to prevent unauthorized parties from reading it.

- **Decryption** is the process of converting an **encrypted** message back to its **original (readable) format**.

Two most common cryptography techniques

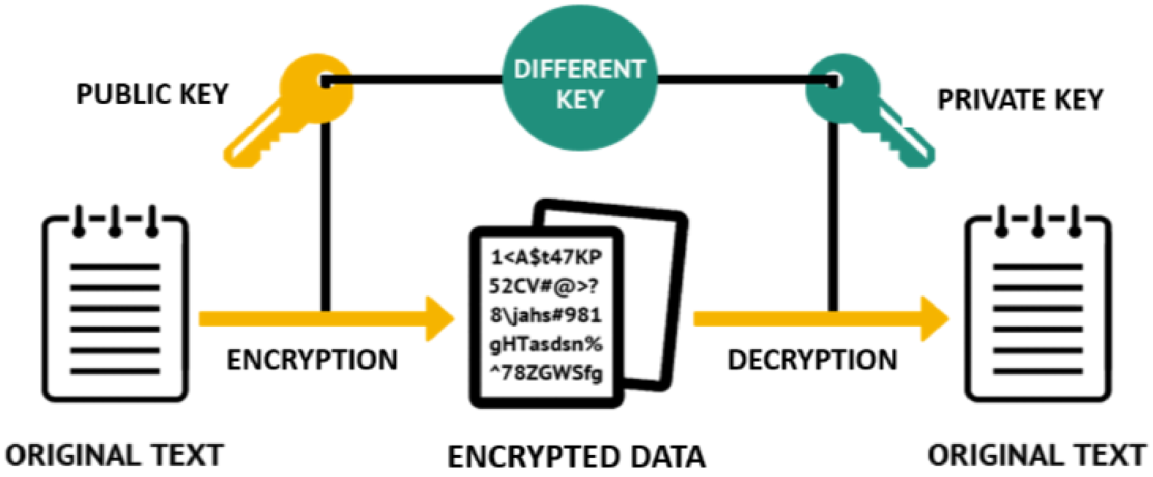
1. **Symmetric key encryption / private key Encryption:** Same key is used to encrypt and decrypt messages



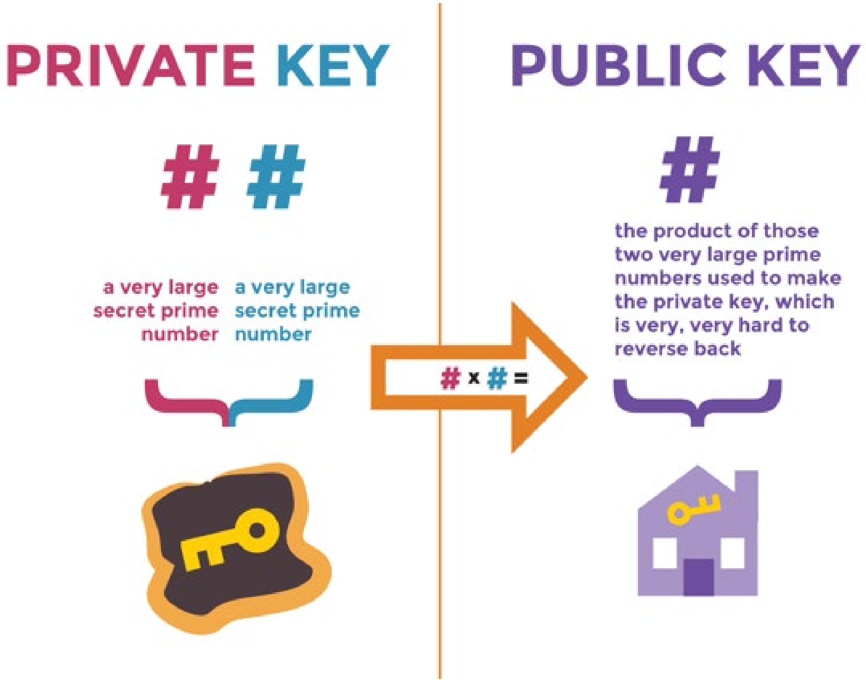
https://medium.com/@rajithabhanuka/symmetric-key-cryptography-private-key-encryption-3edbaed70e4a

2. Public-key cryptography / asymmetric cryptography: It uses **pairs** of related keys.

- Each key pair consists of a **public key** and a corresponding **private key**.



Using separate keys for encryption and decryption, as seen in the figure above, has helped eliminate key exchange, as seen in the case of symmetric encryption.



https://hackernoon.com/generating-rsa-private-and-public-keys-b82a06db6d1c

https://cheapsslsecurity.com/blog/private-key-and-public-key-explained/

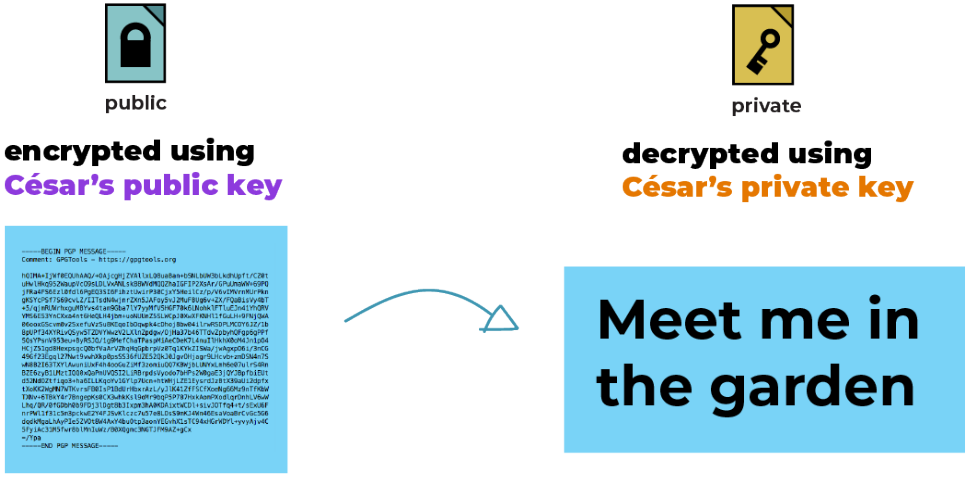
FORCE TECHNOLOGY

Public Key Cryptography / Asymmetric cryptography

We need two pairs of Encryption Keys

1. One pair (public + private) keys from the client to encrypt the DCC

   a. The DCC is encrypted using client's public key
   b. The DCC is sent over the network to the client (machine)
   c. Client (machine) using the private key decrypts the contents of the DCC
   d. Successful decryption means client's public key was used to encrypt the DCC



- **But, what if the DCC issuer later denies issuing any DCC?**
- **As the public key is not meant to be kept secret**

Digital signature : Public Key Cryptography / Asymmetric cryptography

- **But, what if the DCC issuer later denies issuing any DCC? As the public key can is not meant to be kept secret**

- **Digital signature:** This issue can be solved by digitally signing the DCC before sending it to the client over the network

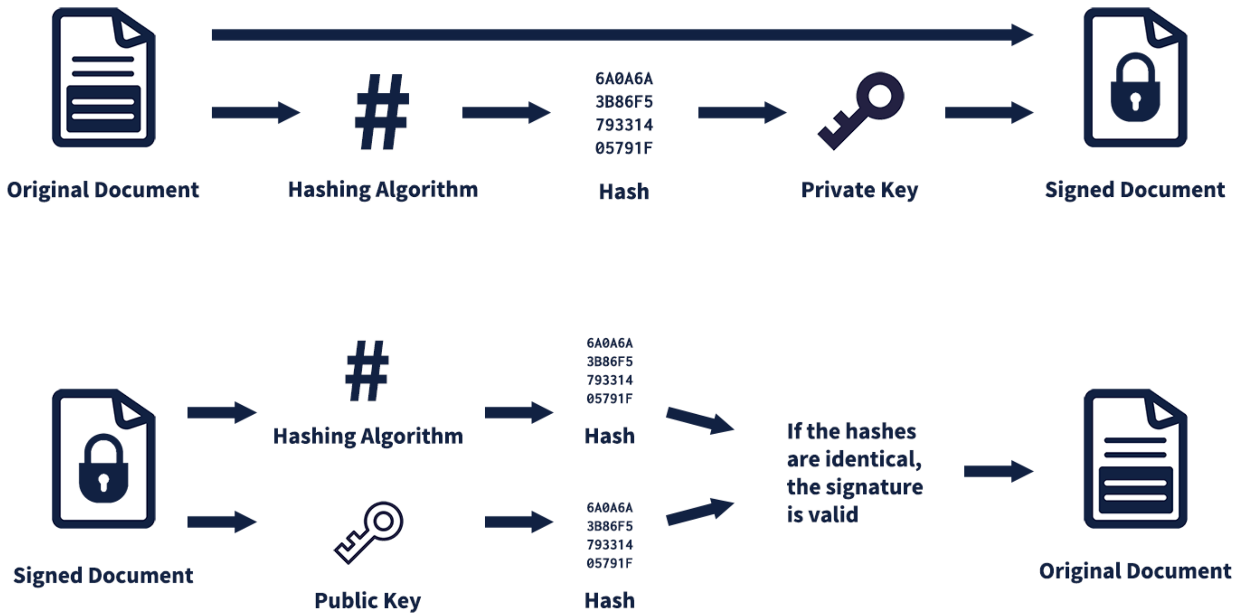
- Now we'll use the **2nd** pair of the (public + private) keys , this pair is owned by the DCC issuer to digitally sign the already encrypted DCC

- The DCC issuer will use his private key to sign the encrypted DCC, the DCC receiver (Client/machine) will verify the authenticity by the DCC issuer's public key.

Digital signature : Public Key Cryptography / Asymmetric cryptography

- **Digital signature insures the following:**
    - **Integrity**: The DCC hasn't been altered in transit
    - **Authenticity**: The author of the DCC is really who they claim to be
    - **Non-repudiation**: The author of the DCC can't later deny that they were the source.

The Client using DCC issuer's public key verifies that the DCC is authentic, integrity has been maintained over the network and the issuer can not deny the issuance of the certificate



Digital Signatures

Digital signature

- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents.

- A **valid digital signature**, where the prerequisites are satisfied, gives a recipient very high **confidence** that the message was **created** by a **known sender** (authenticity), and that the message was not **altered** in transit (integrity).[1

Encryption + Digital signature = Secure and Trusted Exchange of DCC

DCC sharing over a network for M2M communication is two step process:

Step-1: DCC Encryption:

- When encrypting, FORCE Technology will use client's **public key** to encrypt the DCC and client use their **private key** to read it.

Step-2: By Digitally Signing:

- When signing, FORCE Technology will use its **private key** to digitally sign an encrypted DCC, and client use FORCE Technology's **public key** to check if the DCC has been issued by FORCE.

FORCE TECHNOLOGY

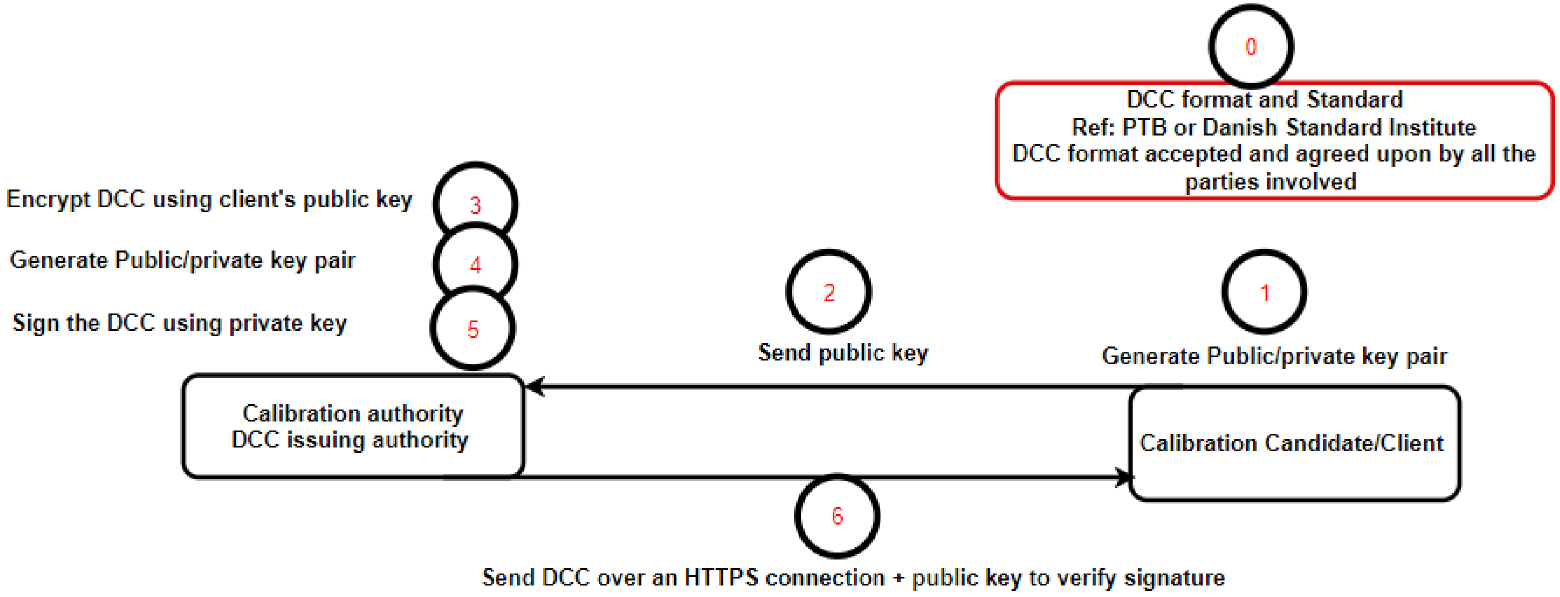
Digital signature

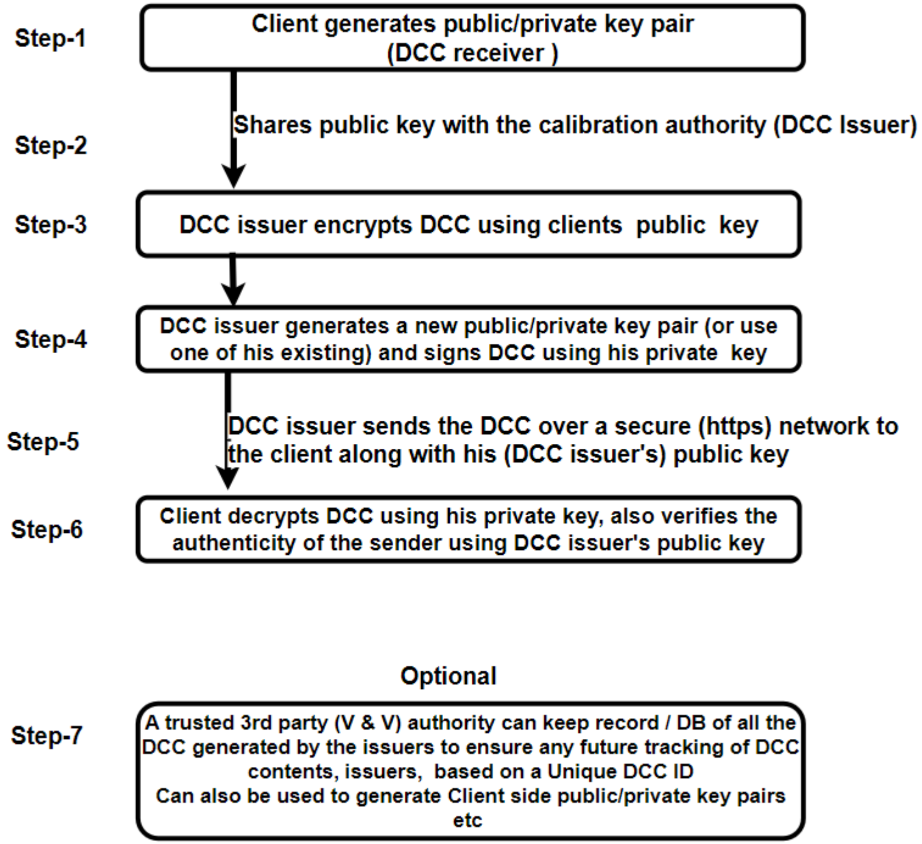
- If the **recipient can't open the document** with the signer's public key, that indicates there's a problem with the document or the signature. This is how digital signatures are authenticated.

- Digital signature technology requires all parties trust that the person who creates the signature image has kept the private key secret.

- If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder.

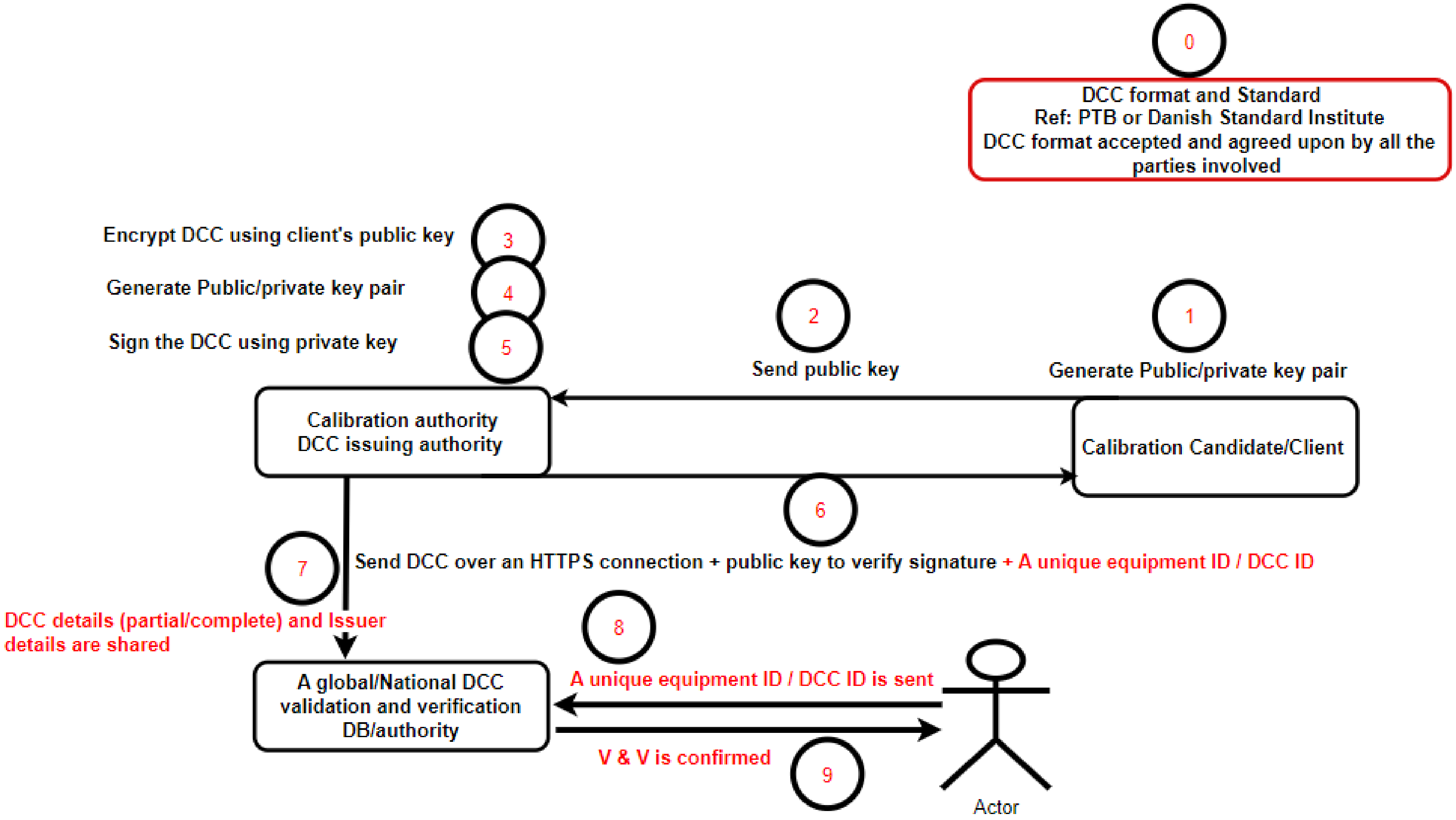
The Entire DCC Exchange in Steps





The Entire DCC Exchange in Steps

- Is FORCE technology the only one issuing DCCs?
- How to achieve a globally compatible and for ex. Backword compatible DCC V and V mechanism ?
- **An independent body can help us solve these issues**



An Independent V & V Authority Can Ensure

Advantages:

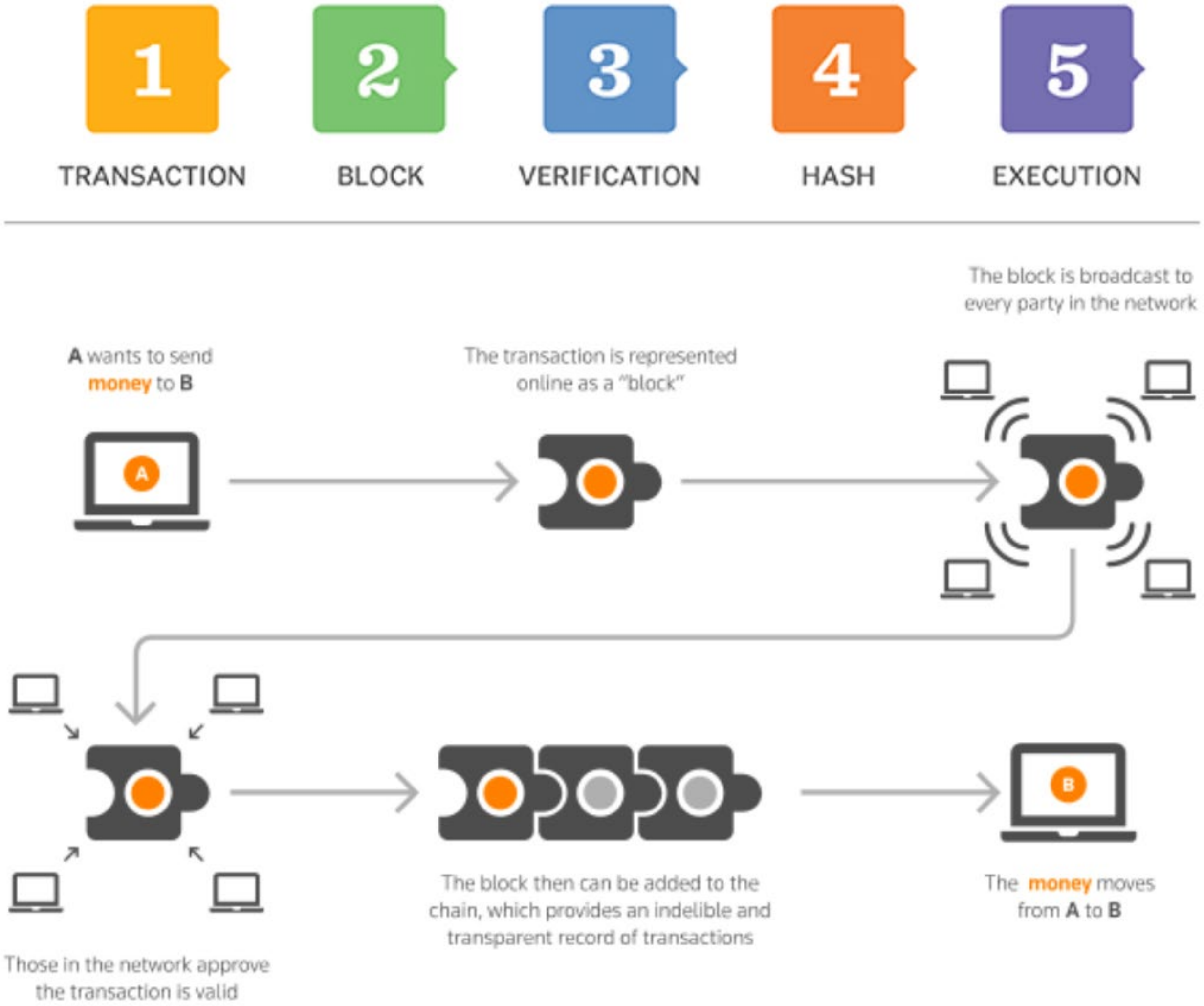
- **M2M capable:** Secure m2m comm. without any manual intervention is possible.
- **Transparent:** Independent and transparent DCC V&V authority, so no conflict of interests.
- **Safe:** What if the DCC issuer link is down? Potentially Safe from MiTM, DoS attacks and avoids SPoF for DCC V&V (if correct architectural techniques such as controlled redundancy are applied) .
- **Flexible:** If required DCC generation logic, Public/private key generation logic can be placed with / handed over to the DCC V&V authority.
- **Compatibility**: DCC format compatibility/conversion logic can be placed here.
- **Single point for any V & V:** Several companies doing calibration for miscellaneous equipment, a single online resource could provide just one API request with unique DCC / equipment ID to provide DCC issuer and equipment calibration details, as well as all the past equipment calibration history for that equipment.

FORCE TECHNOLOGY

Homework

Blockchain technology ensures trust, security, transparency, and the traceability of data shared across a network, so can we use blockchain for DCC exchange ?

- Advantages ?
- Drawbacks?



https://www.garyfox.co/wp-content/uploads/2017/07/how-blockchain-works-infographic-featured.png

Questions???

Keep in touch

Name
Title
+45 43 25 00 00
info@forcetechnology.com
forcetechnology.com

Follow us on:

FORCE TECHNOLOGY