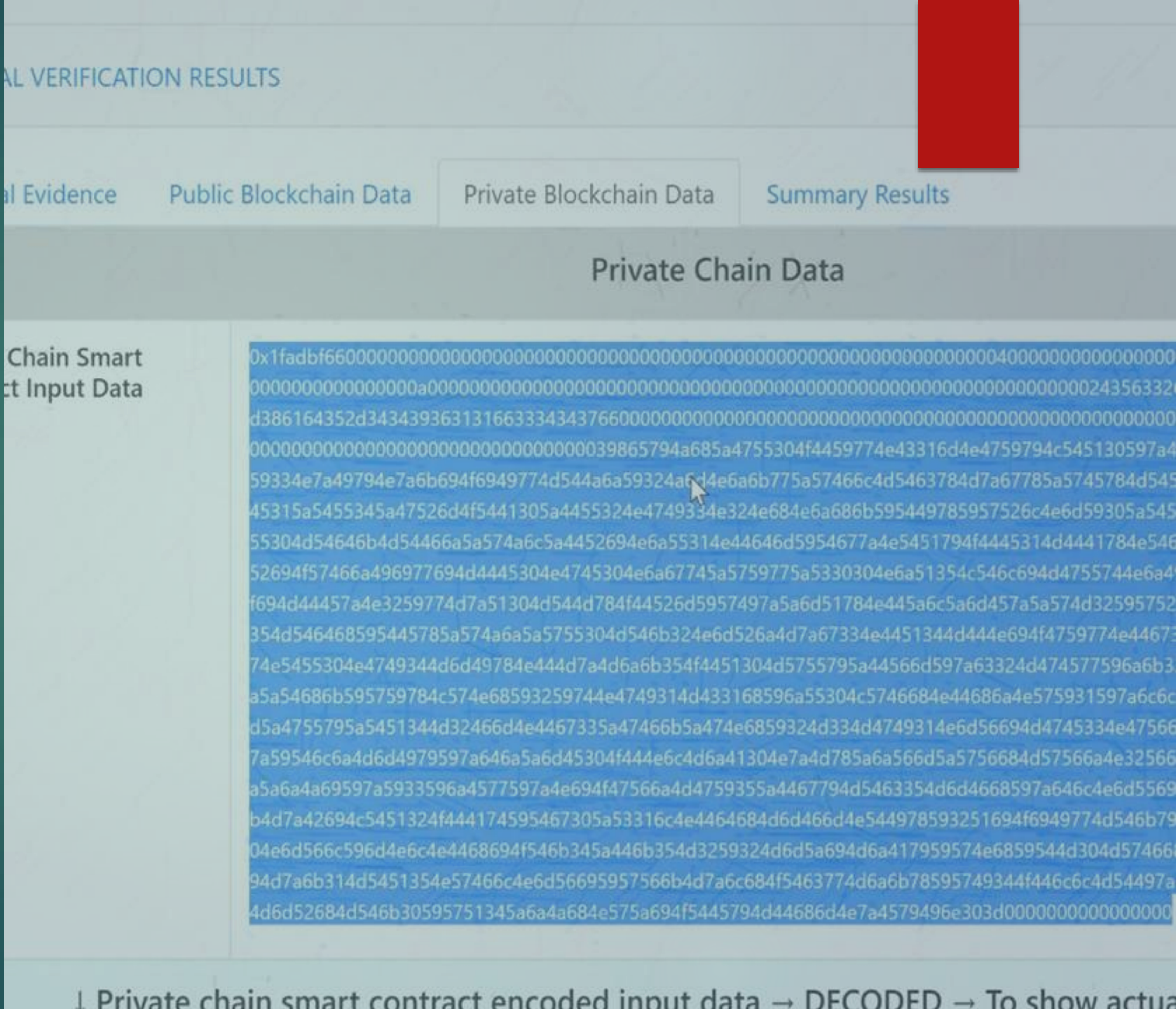


LAB

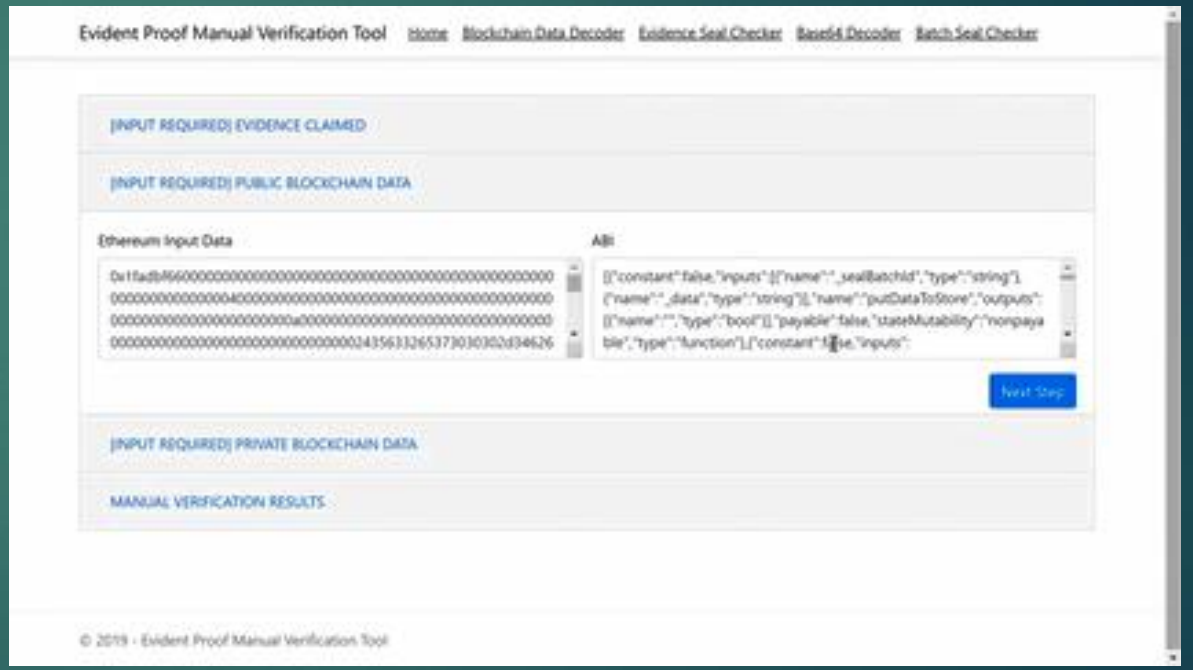
PROOF CERTIFICATE STRUCTURE AND MANUAL PROOF

LAB Overview

- In this Lab – you'll learn how to:
  - Articulate what a Manual Proof is and why it's important
  - Identify the key information of a Proof Certificate that is required to generate a Manual Proof
  - Use the Manual Proof tool and produce your own Manual Proof
- You should follow along, on your dashboard, with the slides.
- At the end of each section – you will be given an exercise to complete.
- Before you begin – you should watch

Before you begin

- Before you begin – you should watch the Anatomy of Proof Certificate video.



Articulate what a Manual Proof is and why it's important

- A Proof Certificate provides all of the information required to Proof the immutable storage and integrity of Evidence data – such that it can be demonstrated, beyond any doubt, that the data stored on the Evident Proof platform has not changed since it was submitted.
- Whilst the Proof Certificate provides all of this information – where cryptography is involved in the proof process, it is useful to be able to demonstrate that the information on the Proof Certificate and the cryptographic and distributed storage mechanisms involved do indeed amount of an immutable, unchanged data record.
- We call this process Manual Proof.

Articulate what a Manual Proof is and why it's important

SECTION EXCERCISE

1. Having watched the video and read the previous slide – you should be able to articulate the importance of Manual Proof
2. Choose the correct answer to the following questions:
    - Manual Proof is a process in which:
        - **A:** we demonstrate that the information on the Proof Certificate and the cryptographic and distributed storage mechanisms involved do indeed amount of an immutable, unchanged data record.
        - **B:** we manually store data on the blockchain that can later be proven

Identify the key information of a Proof Certificate that is required to generate a Manual Proof

- To Prove the immutability of the data presented on the Proof Certificate, we must first extract several key fields from the Proof Certificate.
- The fields we need are:
  - Service Agreement Identifier
  - Source System Dispatch Reference
  - When
  - Where
  - Key
  - Value
  - ABI (*Application Binary Interface)*
    - Note: The ABI is the defined interface, and is used to call functions, and retrieve data, in Ethereum smart contracts
  - Public Chain Input Data
  - Private Chain Input Data

Identify the key information of a Proof Certificate that is required to generate a Manual Proof

SECTION EXCERCISE

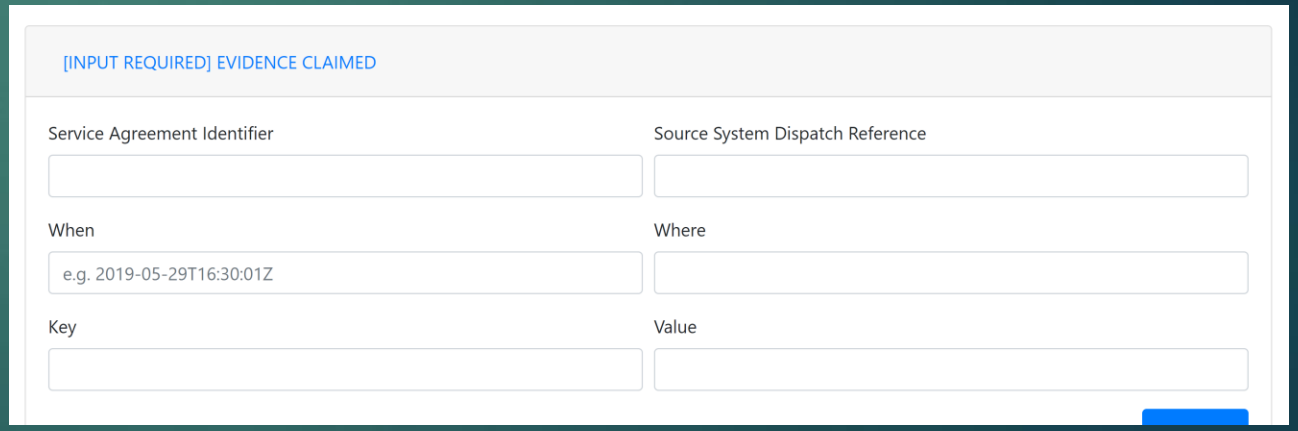
From the example Proof Certificate you have been provided, list the correct values of the following items:

Item	Correct Value
Service Agreement Identifier	
Source System Dispatch Reference	
When	
Where	
Key	
Value	
ABI	
Public Chain Input Data	
Private Chain Input Data	

Use the Manual Proof tool and produce your own Manual Proof

(Slide 1 of 2)

- Now that you have the key data you need to construct a Manual Proof – and having watched the Manual Proof video and demonstrated you can articulate the purpose of Manual Proof – you can now go ahead and create your own Manual Proof.
- Navigate to the Manual Proof tool at: https://blockchainverifytool20190628061548.azurewebsites.net/



Use the Manual Proof tool and produce your own Manual Proof

(Slide 2 of 2)

- Based on the information you successfully extracted from the Proof Certificate – complete the required information throughout the wizard
- The ABI you have identified can be used for both the public chain data and private chain data wizard steps

Use the Manual Proof tool and produce your own Manual Proof

SECTION EXCERCISE

1. From the Manual Verification results, copy and paste/or make a note of the following information:
    - **Original Evidence Sealed**
    - **Public Chain Smart Contract: Isolated Batch Hash**
    - **Hash of Private Chain Seal Batch**
2. Articulate – in your own words, why the results displayed show, beyond doubt, that the data submitted to the Evident Proof platform was stored immutable and has not been changed.