DRAFT

evident proof

DIGITAL DATA EVIDENCE PROOF CERTIFICATE

# AUDIT CERTIFICATE

| | |
|---|---|
| PROOF CERTIFICATE NUMBER | 0718-21567-0000 |
| DATE GENERATED | 01.11.2017 06:56:42 +0000 (UTC) |
| PRIMARY SERVICE USER | XXXX City Council, Taxi Driver Licencing Department |
| REQUESTER NAME | Thomas Smith - Vehicle Administrator, XXXX City Council |

| | |
|---|---|
| Receipts Sent | 7 |
| Evidence Seals | 7 |
| Service Agreement ID | 977ff380-c93d-47b5-bb6b-6abb45358fe5 |
| Request ID | a2b94822-006a-44ed-a7b6-b6f44fcf1372 |
| No. of Proof Seal Bundles | 2 |
| Service Agreement ID | 0111-21000-0000 |
| Request ID | 0718-55588-0000 |
| Requester ID | 0718-21567-0000 |
| API Key | |
| PSU Identifier | |

## DATA EVIDENCE EVENT DETAILS

| | |
|---|---|
| Event Statement | Proof of taxi driver identity and licence. Proof of XXXX City Council compliance with taxi driver licence evaluation protocols and licence issuing processes. |
| Submitted By | Thomas SMITH |
| Submitter ID | |
| Driving Licence number | TS1228229:456 |
| Submitted Date | 01 .11.2017 06:56 |

| | |
|---|---|
| Data Evidence PASS / FAIL | FAIL |
| See Data Evidence Metadata Report for Details | 1. Evidence Key. Result Driver Jane issued a taxi licence incorrectly on 8.6.2017. For proof see:<br>a) Licence issued Data Evidence Key in Metadata Report in proof seal bundle 1.<br>b) Criminal Record Data Evidence Key in Metadata Report in proof seal bundle 2. |

## DISTRIBUTION INFORMATION

| | |
|---|---|
| For Attention Of | XXXX City Crown Court |
| Legal Advisor | D. Brett, Blandy and Blandy Solicitors |
| Case Nunber | BCC/1234 |
| Case Name | Passenger SMITH claims theft by taxi driver JANE |
| Confidentiality Request | Public |
| Viewing Restrictions | Public |
| Secondary users / viewer IDs | |
| Certificate Delivered to | Blandy and Blandy Solicitors |
| Certificate Requested by | XXXX City Council |
| Data Subject Permission Granted by | XXXX City Council |
| Data Owner | XXXX City Council - Driver JANE |
| Data Custodian | XXXX City Council |

See overleaf for an explanation of terms. For a detailed list of definitions, terms and interpretations see “Key Definitions and Interpretations” in the Proof Certificate Guide attached.

# Proof Certificate Terms

## Guide to terms used in the Proof Certificate

### API KEY
The API key used to generate the request (where applicable).

### CONFIDENTIALITY REQUEST
The level of confidentiality for this document.

### DATA CUSTODIAN
The name of the custodians of the data.

### DATA CUSTODIAN CONTACT DETAILS
The contact details of the above.

### DATA EVIDENCE METADATA REPORT
A Report listing information that is associated with the data and relevant to the context of the evidence. Did the data pass or fail checks. Times, dates.

### DATA NOT AUTHENTICATED ON BLOCKCHAIN
Data that is in the process of being authenticated using Blochchain.

### DATA OWNER
The name of the owner of this data.

### DATA OWNER CONTACT DETAILS
Contact details for Data Owner.

### DATA OWNER PERMISSION GRANTED BY
The owner of the data may be different from the person who submitted it, so permission must be sought to use it as evidence.

### DATE GENERATED
The date/time the request was made.

### DISPATCH REFERENCE
A receipt/dispatch level identifier that details what the all pieces of evidence in the submission are related to.

### EPT TOKEN SENT
The number of EPT tokens used to process the transaction.

### EVENT STATEMENT
A free text description of the data this proof certificate represents, limited to 2000 characters.

### EVENT SUPPORTING EVIDENCE ID
The identifier of a receipt within the proof seal bundle or an external document that supports this statement.

### EVIDENCE KEY
The "key" pertaining to the key value pair of the evidence submitted. This is the data that is resubmitted as part of this request process.

### EVIDENCE SEALS
A count of the number of pieces of evidence relating to this request.

### EVIDENCE VALUE
The "value" pertaining to the key value pair of the evidence submitted. This is the data that is resubmitted as part of this request process.

### FOR ATTENTION OF
The person or entity that has requested the certificate.

### INTERESTED PARTIES
The name of any interested parties for this data.

### INTERESTED PARTIES INTEREST
The reason why they are interested in this data.

### ITEMIZED RECEIPTS SENT – RECEIPTS ID
Identifier for the proof that the seal associated with a particular evidence key, with a particular PSUXRef received by Itemized Receipts Sent.

### LIST OF DATA ITEMS WITHIN THE PROOF SEAL BUNDLE
A predefined list of the components that make this type of dispatch.

### PRIMARY SERVICE USER
The name for the client entity associated with the Service Agreement relating to the request.

### PRIVATE TRANSACTION ID
The private blockchain address that relates to this piece of evidence.

### PROOF CERTIFICATE DELIVERED TO
The person or entity who the Proof Certificate is delivered to.

### PROOF CERTIFICATE REQUESTED BY
The person or entity that has requested the certificate.

### PROOF CERTIFICATE NUMBER
The proof certificate ID generated when a Proof Certificate is requested.

### PROOF SEAL BATCH ID
The GUID of the proof seal batch.

### PROOF SEAL BATCH HASH
The hash of hashes created for this proof seal batch, and subsequently stored on the public blockchain.

### PSU IDENTIFIER
An organization that uses the service will have a unique service identifier, a service agreement with the service provider, and responsibilities under that agreement.

### RECEIPT EVENT STATEMENT
A free text description of the data this receipt represents, limited to 2000 characters.

### RECEIPT GENERATED TIMESTAMP
The timestamp relating to when the receipt was issued

### RECEIPT ID
The ID of the receipt contained within the proof seal bundle

### RECEIPTS SENT
The total number of Evident Receipts sent.

### REQUEST ID
The GUID that is created when a request is made.

### REQUESTER ID
THE GUID of the person requesting the data

### REQUESTER NAME
The name of the EPT user who generated this request.

### RESULT
There are four possible states, MATCH, NO MATCH, ADDITIONAL EVIDENCE (i.e. they supplied a key/value EP has not seen before) and MISSING EVIDENCE (i.e. they supplied a key/value before but not this time) .

### SEAL
The seal submitted with the data as part of the request.

### SECONDARY USERS / VIEWER IDS
Other named parties who should receive a copy of this certificate.

### SERVICE AGREEMENT NUMBER
An identifier uniquely identifying a particular service agreement with a particular Primary Service User.

### SERVICE AGREEMENT ID
The GUID that identifies the service agreement relating to this request.

### SUBMITTED BY
The EPT user who enters this data - defaulted by the system.

### SUBMITTED DATE
The date/time that this entry was added - defaulted by the system.

### SUB OWNERS
The name of the sub owners (where relevant).

### SUB OWNERS CONTACT DETAILS
The contact details of the above.

### TOKEN TRANSFER TRANSACTION – ETHEREUM TRANSACTION ID
The transaction ID on the public Ethereum network that shows the transfer or tokens (i.e. that the service was paid for).

### TOKEN TRANSFER TRANSACTION - TIMESTAMP
The date and time that the transaction was written to the public blockchain.

### TIMESTAMP
The "when" attribute relating to this data OR the date/time the data was initially submitted.

### TRANSACTIONAL METADATA
A table that lists data seal and transaction identification keys.

### VIEWING RESTRICTIONS
Viewing restrictions that are applied.

This Proof Certificate will only be issued to an authorised Primary Service User or a Secondary Service User nominated by the Primary Service User. Any warranties or confirmations provided by this Proof Certificate are limited to the listed Data Event and are valid only at the time of issue of this Proof Certificate.

## Key Terms Interpretations

A sample of key definitions and rules of interpretation that apply in this Certificate:

| | |
|---|---|
| Data Event | The original transmission of data by the Primary Service User to the Evident Proof digital platform. |
| Primary Service User (PSU) | The customer to which Evident Proof provides access to the Evident Proof digital platform and associated services as set out in the relevant agreement. |
| Proof Certificate | This report issued to the PSU verifying the correctness, completeness and integrity of the Data Event. |
| Proof Seal Bundle | The complete record from the Evident Proof digital platform listing all interactions with and events in relation to the Data Event. |
| Receipt ID | The unique identifier issued each time data is uploaded to the Evident Proof digital platform. |

## Certification

This Proof Certificate is provided to [CLIENT NAME] to verify the proof, security and integrity of the data event or events. Supporting data event technical proof and blockchain ID's evidence are recorded in the Proof Certificate Technical Evidence Section of this document.

## Warranties

Evident Proof warrants that:

1. The SHA-3 and EThash hashing algorithms being used in the Evident Proof service will produce the same output based on the same input.
2. The Evident Proof system has established and implemented policies, programmes, and procedures that are consistent with applicable industry practices, including technical, administrative [and physical] safeguards to protect the confidentiality, integrity and security of data against unauthorised access, use modification, disclosure or misuse.
3. The Evident Proof system has not experienced any [material] loss, damage, or unauthorised access, disclosure, use, breach of security of any data held on behalf of Primary Service Users.
4. It has and will continue to comply with all applicable laws, statutes, regulations relating to anti-bribery and anti-corruption including but not limited to the Bribery Act 2010.
5. Evident Proof make no warranty or representation whatsoever as to the accuracy or integrity of data which is originally input by the Primary Service User and accepts no liability in this regard.

## PROOF CERTIFICATE TECHNICAL EVIDENCE

Data events technical proof and blockchain ID's evidence.

| | |
|---|---|
| Data Evidence Event description statement | |
| Submitted by | |
| Submitted on | |
| Data Event statement supporting Evidence ID | |

## DATA PROOF SEAL BUNDLE 1 BATCH & RECEIPT DATA

| | |
|---|---|
| Proof Seal Batch ID | XXXXXXX |
| Proof Seal Batch Hash | 000000000000000000 |

| ID | Receipt ID | Receipt Generation Timestamp | Dispatch Reference |
|---|---|---|---|
| 1 | 97c28b2d-3f7f-48f5-bd98-12edac7754e9 | Tue, 01 Apr 2017 15:00:20 +0000 | Operations |
| 2 | 91269e3a-1e17-4a91-be8b-9c1535f11911 | Tue, 01 Apr 2017 12:00:10 +0000 | Operations |

## DATA RECEIPT EVENTS DEFINITION

| | |
|---|---|
| Data Receipt Event 1 description | |
| Submitted by | |
| Submitted on | |
| Event statement supporting Evidence ID | |

## DATA RECEIPT DETAILS

| | |
|---|---|
| Dispatch/Receipt reference | |
| List of data items within the proof seal bundle | |
| Evidence seals | |
| Data subject(s) | |
| Data subject(s) contact details | |
| Sub owners | |
| Sub owners contact details | |
| Data custodians | |
| Data custodian contact details | |
| Interested parties | |
| Interested parties interest | |

## DATA EVIDENCE METADATA REPORT

| Dispatch Reference | Evidence Key | Evidence Value | Timestamp | Certifcate Result |
|---|---|---|---|---|
| Driver Jane | Application for Taxi Licence | 12345 | 1/4/2017 15:33:10 | PASS |
| Driver Jane | License Granted | 12350 | 1/4/2017 16:40:00 | PASS |
| Driver Jane | Criminal Record | 12355 | 1/6/2017 16:40:00 | FAIL |
| Driver Jane | Traffic Offence Notice | 12360 | 1/4/2017 12:00:10 | PASS |
| Driver Jane | License Revoked | 16670 | 1/4/2017 15:00:20 | PASS |

## TRANSACTIONAL META DATA

| Dispatch Reference | Evidence Key | Seal | Private Transaction ID |
|---|---|---|---|
| Operations | Regulations for Taxi License | eed5d0bd1fc853ca70553ffdd16f7 3d25cf78211cd2a4da2a632b35b | 0xd1f5bcbcca548d1a8ec8784a699b49e40a 80256342f6efa390107f68d02a3082 |
| Operations | Regulations for Taxi License | eed5d0bd1fc853ca70553ffdd16f7 3d25cf78211cd2a4da2a6329ii7 | 0xd1f5bcbcca548d1a8ec8784a699b49e40a 80256342f6efa390107f68d029O34N |

## DATA PROOF SEAL BUNDLE 2 BATCH & RECEIPT DATA

| | |
|---|---|
| Proof Seal Batch ID | XXXXXXX |
| Proof Seal Batch Hash | 000000000000000000 |

| ID | RECEIPT ID | RECEIPT GENERATION TIMESTAMP | DISPATCH REFERENCE |
|---|---|---|---|
| 1 | 188077f7-0216-455c-b684-78d97949f379 | Wed, 01 Apr 2016 12:00:00 +0000 | Driverjane |
| 2 | 80c032b1-b70d-49bb-a0ad-fa662b55c932 | Tue, 01 Apr 2017 16:40:00 +0000 | Driverjane |

## DATA RECEIPT EVENTS DEFINITION

| | |
|---|---|
| Data Receipt Event 1 description | |
| Submitted by | |
| Submitted on | |
| Event statement supporting Evidence ID | |

## DATA RECEIPT DETAILS

| | |
|---|---|
| Dispatch/Receipt reference | |
| List of data items within the proof seal bundle | |
| Evidence seals | |
| Data subject(s) | |
| Data subject(s) contact details | |
| Sub owners | |
| Sub owners contact details | |
| Data custodians | |
| Data custodian contact details | |
| Interested parties | |
| Interested parties interest | |

## DATA EVIDENCE METADATA REPORT - AUDIT CERTIFICATE

| Dispatch Reference | Evidence Key | Evidence Value | Timestamp | Certifcate Result |
|---|---|---|---|---|
| Driver Jane | Application for Taxi Licence | 12345 | 1/4/2017 15:33:10 | PASS |
| Driver Jane | License Granted | 12350 | 1/4/2017 16:40:00 | PASS |
| Driver Jane | Criminal Record | 12355 | 1/6/2017 16:40:00 | FAIL |
| Driver Jane | Traffic Offence Notice | 12360 | 1/4/2017 12:00:10 | PASS |
| Driver Jane | License Revoked | 16670 | 1/4/2017 15:00:20 | PASS |

## TRANSACTIONAL META DATA

| Dispatch Reference | Evidence Key | Seal | Private Transaction ID |
|---|---|---|---|
| Driver Jane | Application for Taxi Licence | 472ce6288d1bb3e6f99b49129274<br>114c7a00b452874ae1edacebf9c0 | 0xd1f5bcbcca548d1a8ec8784a699b49e40a<br>80256342f6efa390107f68d22a3087 |
| Driver Jane | License Granted | c9886357869b28ec19ddca561b1<br>bf912daae11efd2e7c80c5589f448 | 0xd1f5bcbcca548d1a8ec8784a699b49e40a<br>80256342f6efa390107f68d22a3028 |
| Driver Jane | Letter | 85350a6800055155c85df6299fcf<br>ae7d9170c64ccda3ee358463d0f8 | 0xd1f5bcbcca548d1a8ec8784a699b49e40a<br>80256342f6efa390107f68d22a3182 |
| Driver Jane | Traffic Offence Notice | 098224018e426c64662b70fd8ab<br>92c96cb851cfd7cea7d3ce6614c41 | 0xd1f5bcbcca548d1a8ec8784a699b49e40a<br>80256342f6efa390107f68d22a3283 |
| Driver Jane | License Revoked | 456c4e2b478c61eb0396a5c0433<br>97caa383c99884e2905adca51b2d1 | 0xd1f5bcbcca548d1a8ec8784a699b49e40a<br>80256342f6efa390107f68d22a4928 |

# Contents

## Summary of Evident Proof Service

Evident provides a commercial data proof, verification and compliance service to allow its Service Users to submit any data and have that data cryptographically proven to an untrusting 3rd party. Proof that it has not been not been modified at a later date in any way. This is provable beyond both reasonable doubt and the balance of probability and would be admissible as evidence in court.

The Evident Proof Service uses a combination of Public Ethereum Blockchain, Private Ethereum Blockchain and proprietary software owned by Evident Proof to prove the provenance of data and transactions.

To evidence this, a "Proof Certificate" is issued by the Evident Proof Service containing the data and instructions needed to re-constitute the mathematical proof. This means that 3rd parties can report on the integrity of the source data subject to them having access to: the source data, a copy of the publicly available hashing algorithm, the Proof Certificate and access to the Public Ethereum Blockchain network.

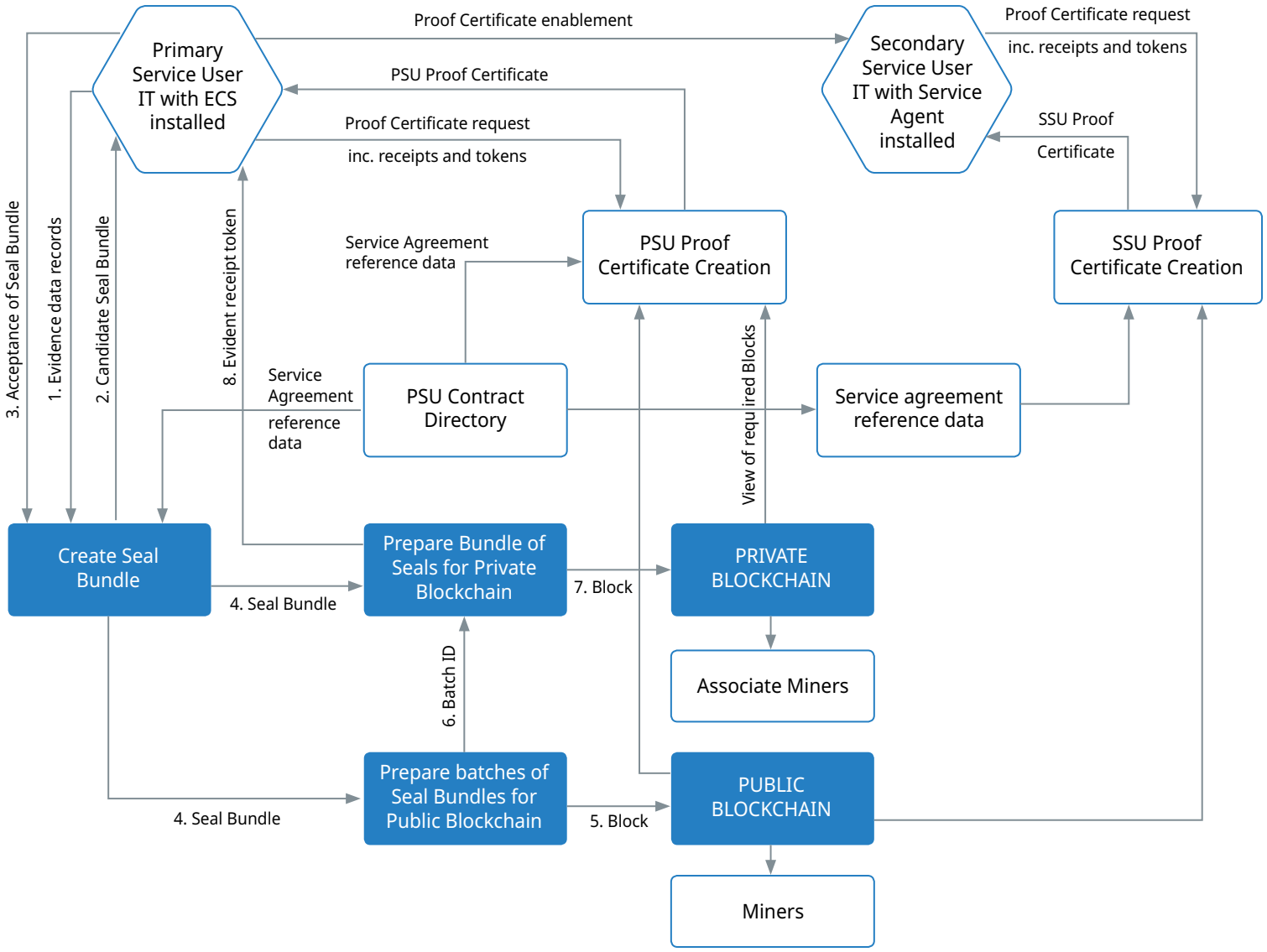
## Non-technical description of what is being proved

- The Evident Proof service combines the use of multiple blockchains, proprietary IP, mathematical algorithms (similar to ones used in Online Banking, Cryptocurrencies, Secure Messaging Apps, commercial document signing services etc) to perform the following actions:
- Take original source data, which could be any digital data eg. photograph, database record, document, stream of data from a piece of industrial machinery, workflow, barcode etc.
- Put this data through a "hashing algorithm" which has the mathematical property of turning any data into a fixed digital fingerprint. Even a small difference (eg. changing 1 pixel in a photograph) will produce a completely different hash/fingerprint.
- For example: As hashes themselves can be combined with other data into blocks and be hashed again, the result is blocks of data that are chained together in multiple blockchains. If anything is changed in the chain, the resultant hash will be different. This is this basic mathematical principle that allows the Evident Proof service to prove that the original data has not been changed.
- In order to prevent the scenario where the original data owner changes the original data and recalculates a new set of hashes, Evident stores the original hashes (not the source data) in both public and private blockchains, which is a public immutable record that cannot be modified.
- Note that a hashing algorithm is a one way "trapdoor" function. If you have the source data you can create the hash/fingerprint, but if you only have the hash/fingerprint you cannot re-create the source data.

It is not the purpose of this document to provide a detailed description of topics like Hashing Algorithms, Consensus Algorithms or Public/Private key cryptography. There is an animated explanation of the Evident process available which is linked in the References Appendix.

## Technical description of how the proofs are constructed

The platform workflows are detailed in the workflow diagram below. Please see the Evident Proof Technical Whitepaper for more details.




Notes:

Numbered flows show data acquisition sequence.

## Evident Service ID Numbers / Data Structures

Examples of some relevant Evident Proof service ID numbers and data structures.

### Evident Seal Bundle

"header"
"sourceSystemDispatchReference": "string",
"serviceAgreementIdentifier": "string",
"where": "string",
"when": "2019-05-04T15:27:53.252Z"
"evidence":
"key": "string",
"value": "string"

### Evident Proof Certificate ID Number

SA-DEV-A54A4DC4-05FA-40C6-A0FE-812920F556BE-20190418-000001

### Evident Receipts ID number

3c3327e0-b48e-4220-88b8-c72f55a2dae1

### Evident Service Agreements ID Number

SA-DEV-A54A4DC4-05FA-40C6-A0FE-812920F556BE

### Evident Data Receipt

"id": "string",
"header":
"sourceSystemDispatchReference": "string",
"serviceAgreementIdentifier": "string",
"where": "string",
"when": "2019-05-04T14:47:25.114Z"

### Evident Data Receipt (cont'd)

"evidence":
"id": "string",
"key": "string",
"seal": "string",
"tokenFractionStorageCost": 0,
"tokenFractionEarned": 0,
"sealStorageBand": 0

### Evident Proof Certificate Request

"serviceAgreementIdentifier": "string",
"requesterName": "string",
"receipts":
"header":
"id": "string",
"sourceSystemDispatchReference": "string",
"where": "string",
"when": "2019-05-04T15:26:37.814Z"
"evidence":
"key": "string",
"value": "string",
"status": 0

## Use of EPT Utility tokens

EPT utility tokens are purchased by either Primary Service Users or nominated 3rd party users of the Evident service wishing to produce a proof certificate. EPT tokens are used to drive the utility of the service but are not intrinsic to the actual proofs themselves.

## Scenario specific implementations

This document describes the generic Evident service. There may be other specific details of implementations used by specific clients that add to the base Evident service. By default, Evident never see the original source data, only a hash of that data. However, there may be scenarios where the customer asks Evident, or a 3rd party to do something specific, for example:

- Store copies of the original data - for example where it is public data.
- Store copies of Evident Receipts and Proof Certificates.
- Provide some pre-processing to the original data - for example to de-duplicate or compress it.

## Key assumptions

In order to be confident that the Evident proof is accurate you will need to assume the following to be true.

- The SHA-3 and EThash hashing algorithms being used will produce the same output based on the same input.
- Public/Private key cryptography is secure
- The data stored on the Public Ethereum blockchain is immutable
- The majority of Blockchain servers have accurate clocks

To test the service it is possible to make a “manual” proof of a piece of data from having only the following:-

- The unmodified source data from the Primary Service User or a 3rd party holding that data in escrow.
- A copy of the hashing algorithm
- The Evident Proof Certificate in any format
- Access to the Public Ethereum blockchain
- A copy of the Evident Receipts
- A copy of the Private Blockchain if a private blockchain has been used.

## Creating a Proof Certificate

### How to perform a "manual" proof

If you need to prove that a Proof Certificate is valid (and that therefore the original data has not been modified) then there is a way to do this.

The steps to perform a "manual" proof are detailed in an online video (see References section for URL).

Link to Video : TBD

Text instructions:
https://ept.gi/assets/files/ManualProofVerificationDocument.pdf

### What is not being proved

It is useful to understand what is not being proved.

- If the original submitted data was false or doctored, then the proof will show that the data is still false. You can think of this as "falsehood in, falsehood out"
- When preparing a Proof Certificate: If the original data is modified then the proof will fail.

### Use of data as evidence in Court

Evident Proof Digital Data Event Evidence Submission Protocol 1.02 is a protocol for the storage retrieval and submission of digital data evidence (EPDEES Protocol 1.02).

The information contained in this Proof Certificate is stored and structured according to the EPDEES Protocol 1.02. EPDEES Protocol 1.02 for the storage retrieval and submission of digital data evidence goes above the thresholds for presenting evidence to Civil and Criminal courts. EPDEES Protocol 1.02 system beyond reasonable doubt and balance of probability that the source data has not been modified since the date/time it was submitted to the Evident Proof service. A sufficiently expert witness could confirm this in a court of law.

### How to request a copy of a Proof Certificate

The Primary Service User or a Secondary Service User, who could be a third party relying on the data in question, can obtain their own copy of a Proof Certificate as follows:-

A Proof Certificate is provided in one of two types:

- A VALIDATION Proof Certificate which illustrates the consistence of Evidence provided to the Platform
- An AUDIT Proof Certificate identifies the specific Evidence items that have been submitted to the Platform for a given Source System Dispatch Reference.

## Creating a Proof Certificate

### How to request a copy of a Proof Certificate (cont'd)

Audit Proof Certificates can be created by Primary Service users via the client dashboard by selecting the "Request Audit" option from the Proof Certificates menu. Once here, a user can use filter the data displayed based upon the Source System Dispatch Reference, or by a date range, and subsequently generate a proof certificate.

A Validation Proof Certificate can only be created systematically via an API call this is due to the complex nature of its contents, it contains the same core information as an audit proof Certificate, with the key difference being that the user provides the evidence so that it can be rehashed and compared to what was provided previously.

Once a certificate is created, there will be a further function allowing a Primary user to "Nominate" a secondary user, who will receive a timeboxed link to it, which they can access once they have completed the new user sign up journey. Secondary users will be able to view a list of all Proof Certificates that they have been provided access to, but they will only be able to view the data contained within them if the viewing expiration date has not yet been met.

### Frequently asked questions

For FAQ go to: www.ept.gi/faq

## Key definitions and interpretations

Whilst working with the Evident Proof Platform, it is important to understand some key terms which relate both to data stored within the application and the way in which data is submitted to the application for storage. This section provides information on several terms that are later referred to within this document:

The Evident Proof Platform or 'the Platform' refers to the collection of technical elements that provide functionality to submit evidence, submit proof certificate requests, monitor the status of submissions of both types and monitor cost associated with the operations being performed.

### Applicable Law

Any and all applicable laws, statutes, orders, rules, treaties, decree, regulations, directives, edicts, bye-laws, schemes, warrants, other instruments made under or to be made under any statute, any exercises of the royal prerogative and codes of conduct and regulatory rules or guidelines, whether local, national, international or otherwise existing from time to time, together with any other similar instrument having legal effect in the relevant circumstances.

### API Key

API Key An API key, generated from within the Client Dashboard, is used in conjunction with the SAID submitted in a request to validate the authenticity of the request. A submission must have an API key that corresponds to the specified Service Agreement, else the request is considered invalid.

### Business Day

A day other than a Saturday, Sunday or bank or public holiday in England;

### Certificate Date Generated

The date the Proof Certificate was generated.

### Completion certificate

The certificate issued by the Supplier and signed by the Customer pursuant to clause 2.5.6 of the client agreement.

### Consultancy Phase

The initial phase of where the Supplier will supply to the Customer the Consultancy Services; services to be provided by including the analysis of (1) which sets of Customer Data are to be recorded on the Platform and (2) the format of that data; the recommendation of a strategy by the Supplier for integration of Customer Data onto the Platform, software development, construction of APIs and components necessary to enable the Customer to make use of the Service.

### Certificate Number

The unique identity number identifying the proof certificate.

### Confidentiality Request

Where the client has listed any and all confidential information and viewing restrictions (whether in oral, written or electronic form) including technical or other information imparted in confidence or disclosed by one party to the other or otherwise obtained by one party relating to the other's business, personal data, finance or technology, know-how, Intellectual Property Rights, assets, strategy, products and customers, including information relating to management, financial, marketing, technical and other arrangements or operations of any person, firm or organisation associated with that party;

## Key definitions and interpretations

### Customer Data

All information provided by the Customer to the Supplier when using the Service.

### Support Services

The support services provided by the Supplier to the Customer and described in schedule 1 .

### Client Dashboard

The Client Dashboard provides a public-facing user interface for consumers of the Platform, allowing administrators for a Service Agreement to view the status of submissions, complete requests for Proof Certificates, retrieve existing Proof Certificates and monitor costs associated with transactional operations in the Platform.

### Customer Systems

Hardware and systems whether cloud based or otherwise belonging or licensed to the Customer which are to be used to access the Platform and use the Services.

### Customer's Wallet

The Customer's digital wallet used to store, send and receive platform tokens.

### Data Event

A transmission of data from the Customer to the Platform. The original transmission of data by the Primary Service User to the Evident Proof digital platform.

### Dispatch

A Dispatch relates to the submission of Evidence to the Platform. A Dispatch consists of a header (explained in Submitting Evidence) and either one or many Evidence items to be submitted.

### Data Custodian / Data Controller

The name of the data custodian or controller of the data or part of the data in the proof certificate.

### Data not authenticated on Blockchain yet

Data that is in the process of being authenticated using Blochchain.

### Documentation

The documents (in whatever media) provided to the Customer to facilitate use of the Service by Users.

### Evidence

Evidence. Evidence relates to any data being submitted by a consumer of the Platform for storage. The data can be of any type – text, images, other files or representations of a collection of any of these things – provided that the data can be provided in some textual format, for example a base64 encoded string.

### Evidence API

Evidence API The Evidence API is the most commonly used API within the Platform and is responsible for receiving, validating and processing requests for the submission of Evidence and Proof Certificate requests by consumers of the Platform.

## Key definitions and interpretations

### Evident Proof Digital Data Event Evidence Submission Protocol 1.02

A protocol for the storage retrieval and submission of digital data evidence (EPDEES Protocol 1.02).

### Force Majeure

An event or sequence of events beyond a party's reasonable control (which could not reasonably have been anticipated and avoided by a party) preventing or delaying it from performing its obligations hereunder, including war, revolution, terrorism, riot or civil commotion, or reasonable precautions against any such; strikes, lock outs or other industrial action, whether of the affected party's own employees or others; blockage or embargo; acts of or restrictions imposed by government or public authority; explosion, fire, corrosion, flood, natural disaster, or adverse weather conditions. Force Majeure does not include inability to pay, mechanical difficulties, shortage or increase of price of raw materials, over-commitment or market or other circumstances which may make the terms of this Agreement unattractive to a party;

### Hot Wallet

A Hot Wallet is an Ethereum wallet, created and maintained by the Evident Proof platform on behalf of a consumer and directly related to their Service Agreement. On the creation of a Hot Wallet, the private key to access the wallet will be shared with the Primary User, such that EPT can be deposited and withdrawn.

### Hashing Algorithms

Hashing Algorithms The SHA-3 and EThash hashing algorithms being used in the Evident Proof service will produce the same output based on the same input. A secure hash algorithm, often known simply as an "SHA," is a hashing algorithm that is considered cryptographically secure.

### Infringing Data

Information or data that (i) infringes Applicable Law; or (ii) infringes any third party Intellectual Property Rights; or (iii) includes any material which is obscene, indecent, pornographic, seditious, offensive, defamatory, threatening, liable to incite racial hatred, menacing or blasphemous.

### Intellectual Property Rights

Copyright, patents, rights in inventions, rights in confidential information, know-how, trade secrets, trade marks, service marks, trade names, design rights, rights in get-up, database rights, rights in data, semi-conductor chip topography rights, mask works, utility models, domain names, rights in computer software and all similar rights of whatever nature and, in each case: (i) whether registered or not, (ii) including any applications to protect or register such rights, (iii) including all renewals and extensions of such rights or applications, (iv) whether vested, contingent or future and (v) wherever existing.

### Platform

The Evident Proof digital platform.

### Primary Service User

The Primary User for a Service Agreement is the individual who creates the Service Agreement and is the first registrant within the Client Dashboard for that agreement. The Primary User has elevated permissions within the Client Dashboard, including the ability to create other users within the system. The customer to which Evident Proof provides access to the Evident Proof digital platform and associated services as set out in the relevant agreement

## Key definitions and interpretations

### Proof Certificate

A Proof Certificate is provided in one of two types: a validation Proof Certificate illustrates the consistency of Evidence provided to the Platform, whilst an audit Proof Certificate identifies the specific Evidence items that have been submitted to the Platform for a given Source System Dispatch Reference.

### Proof and Validation Certificate

A report issued to the Customer by the Supplier upon receipt of the agreed number of Tokens and a copy of the data originally submitted for verification that verifies the correctness, completeness and timing of Data Events in a proof seal bundle.

### Proof Seal

A Proof Seal is an artifact generated by the Platform in response to the submission of Evidence. To ensure that the data submitted by consumers is not visible to administrators of the system, the Evidence submitted to the Platform is irreversibly hashed into a Proof Seal. This Proof Seal is then submitted to the blockchain to ensure the irrefutable proof of data.

### Proof Seal Bundle

Data comprising a proof seal bundle as defined in Schedule 1 clause 11 of client agreement. The complete record from the Evident Proof digital platform listing all interactions with and events in relation to the Data Event.

### Receipt ID

Information or data that (i) infringes Applicable Law; or (ii) infringes any third party Intellectual Property Rights; or (iii) includes any material which is obscene, indecent, pornographic, seditious, offensive, defamatory, threatening, liable to incite racial hatred, menacing or blasphemous.

### Retained Data

Data retained on the platform in the event of a cessation or suspension of the service.

### Service

The remote provision of the Shared Platform to the Customer for the benefit of Users.

### Service Hours

Available 24 hours a day, seven days a week.

### Services Phase

The phase which commences immediately following completion of the Consultancy and Integration Phases as per clause 2.7.

### Service Commencement Date

The day after completion of the Consultancy and Integration Phases.

### Service Agreement

A ‘Service Agreement’ is a representation of a contract between Evident Proof and a consumer of the platform. It consists of a number of cost specifications for transactions performed using the platform and a unique identifier, known as the Service Agreement Identifier or SAID, which is one of the elements used to identify the origin of requests to the Platform.

### Source System

A ‘Source System’ is any platform that connects to the Evident Proof Platform with the purpose of storing Evidence or creating Proof Certificate requests. This is typically another line-of-business application, responsible for capturing and storing transactional data that is to be stored in the Platform as Evidence.

## Key definitions and interpretations

### Source System Dispatch Reference

The Source System Dispatch Reference is a unique ID, provided by the Source System, which binds a number of Evidence Dispatches to a single logical entity. In the case of Evidence submitted in relation to a car, for example, the Source System Dispatch Reference may be a unique, database generated ID relating to the car, or the vehicle registration number. Submissions relating to the maintenance record for a bespoke product may use the serial number of the manufactured item.

### Subscription Term

The Initial Subscription Term together with any subsequent Renewal Periods.

### Users

The users that are authorised to use the Service as specified in Schedule 1 of the Client Service Agreement.

## References

URL for Ken Boness Academic Whitepaper

https://developer.evident-proof.com/documents/Evident-Proof-Service-Technical-Whitepaper-v3-0-updated.pdf

URL to Mathematical Proof of Public Chain Hashing Mechanism:
Dr James Anderson

To follow

URL to Wikipedia for the hashing algorithm

https://en.wikipedia.org/wiki/SHA-3

URL to Evident Source Code Escrow

To follow

URL to Public Ethereum Blockchain scanner

https://etherscan.io/

URL to explanation of Blockchain

https://en.wikipedia.org/wiki/Blockchain

URL to QC Opinion

To follow

URL to animated explanation of Evident service

https://developer.evident-proof.com/index.html

URLs to previous Case Law which is relevant

To follow

URL to a video “worked example” of a proof from first principles

To follow

## Terms of Use

BY USING THE SERVICE, YOU VOLUNTARILY AND IRREVOCABLY ASSUME ALL RELATED RISKS. EVIDENT-PROOF LTD MAKES NO REPRESENTATION, WARRANTY, OR COVENANT REGARDING THE SERVICE OR ANY CONTENT, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, OR NON-INFRINGEMENT, AND ALL SUCH REPRESENTATIONS, WARRANTIES, AND COVENANTS ARE HEREBY FULLY DISCLAIMED. Without limiting the foregoing, Evident-Proof Ltd does not warrant or represent that (i) the service will meet your specific requirements, (ii) the service will be uninterrupted, timely, secure, or error-free, (iii) the results that may be obtained from the use of the service will be accurate or reliable, (iv) the quality of any products, services, information, or other material purchased or obtained by you through the service will meet your expectations, (v) any errors in the Service will be corrected; (vi) Content will be free from defects; (vii) Content will be free from claims as to infringement of third party rights; (viii) Content will be secure or not subject to partial or total loss.

EVIDENT-PROOF LTD SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF EVIDENT-PROOF LTD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM: (i) THE USE OR THE INABILITY TO USE THE SERVICE; (ii) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES RESULTING FROM ANY GOODS, DATA, INFORMATION OR SERVICES PURCHASED OR OBTAINED OR MESSAGES RECEIVED OR TRANSACTIONS ENTERED INTO THROUGH OR FROM THE SERVICE; (iii) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA; (iv) CONTENT ON THE SERVICE; (v) STATEMENTS OR CONDUCT OF ANY THIRD PARTY ON THE SERVICE; (vi) OR ANY OTHER MATTER RELATING TO THE SERVICE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF CERTAIN CATEGORIES OF DAMAGES AND AS A RESULT, SOME OF THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. IN SUCH JURISDICTIONS, THE LIABILITY OF EVIDENT-PROOF LTD IS LIMITED TO THE FULLEST EXTENT PERMITTED BY LAW.

BY USING THE SERVICE YOU AGREE THAT IN NO EVENT WILL EVIDENT'S LIABILITY TO YOU OR ANYONE CLAIMING THROUGH YOU FOR ACTUAL DAMAGES EXCEED THE AGGREGATE AMOUNT OF SUBSCRIPTION FEES PAID BY YOU IN THE SIX (6) MONTHS PRIOR TO THE EVENT OR OCCURRENCE GIVING RISE TO THE CLAIM.YOU AGREE TO INDEMNIFY, DEFEND, AND HOLD EVIDENT-PROOF LTD AND ITS SHAREHOLDERS, OFFICERS, DIRECTORS, AGENTS AND EMPLOYEES HARMLESS FROM AND AGAINST ANY AND ALL CLAIMS, COSTS, LOSSES, AND CHARGES (INCLUDING WITHOUT LIMITATION ATTORNEYS' FEES AND COSTS) ARISING FROM YOUR REGISTRATION TO USE THE SERVICE, ACTUAL USE OF THE SERVICE, OR BREACH OF THESE TERMS OF SERVICE.