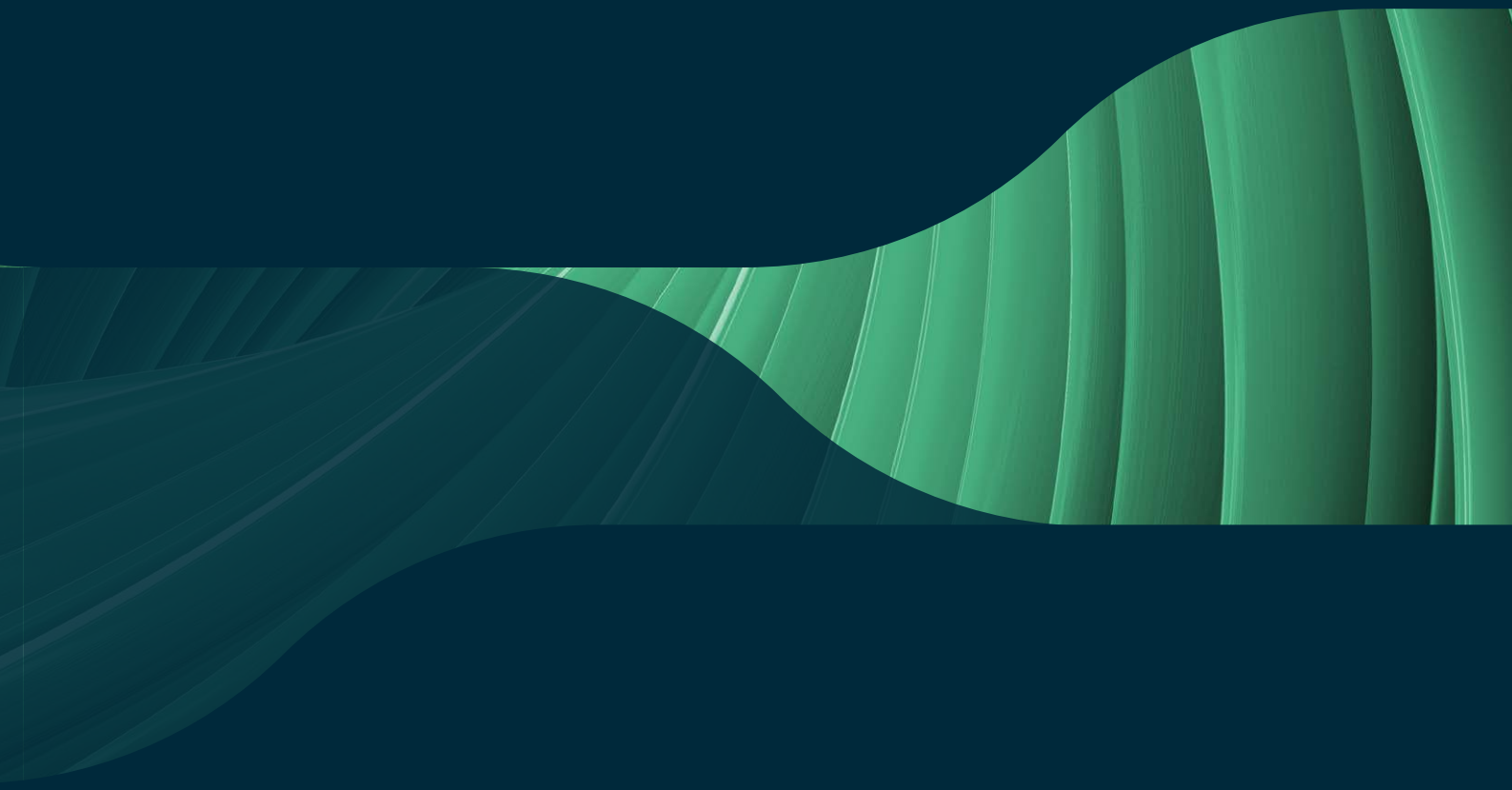
trace:original

A DIGITAL ORIGINAL DOCUMENT | How it works

AUGUST 2022



enigio

Introduction

Fig.1 | trace:original is like a freely transferable container for data

A large share of the communication in a trade finance transaction is already digitalised. Banks structure customer communication through portals, negotiate via safe e-mail and sign using e-signatures, not to forget SWIFT which has already enabled the digitalisation of many products and process steps between banks. A major obstacle for achieving a completely digital trade finance world has been the requirements to be able to manage and present documents in their original form, something that is still normally only done with paper.

Our focus has therefore been to create a digital document with the same properties as its paper equivalent. The trace:original document is designed to be able to keep all functional capabilities of paper, to hold all necessary data to execute a transaction and at the same time not being tied to any specific transaction infrastructure. More importantly it can also be managed freely by anyone with access to a computer and the internet, without having to on-board or sign up to a specific platform.

If we want to see rapid digitalisation of trade and trade finance and corresponding processes and infrastructures, paper and digital documents must co-exist. We will have countries being early digital adopters and others lagging. An infrastructure agnostic digital trade finance document that can represent any trade document type and cater for any industrial standard can serve all the aspects of the global digital ambition.

Interoperability can be achieved on different levels and by using different tools. One of the most common ways of achieving interoperability is by standardisation of data definitions and data formats. A widely used standard is JavaScript Object Notation (JSON Schemas). Using JSON Schemas increases the usability significantly as it enables trade finance systems and other software to exchange data in a defined way regardless of which transaction platform or messaging system the transacting parties are using. A combined JSON Schema library for trade finance documents coupled with data definitions standards would significantly boost digital interoperability between transacting parties' through a step by step approach. This, without the need for any major re-engineering of the current IT infrastructures in banks and corporates. JSON Schemas defined data objects and the trace:original document is a perfect combination to achieve digital interoperability not only between blockchain based trade finance platforms but for all trade finance platforms.

How does trace:original work?

The trace:original solution is a method to achieve all properties needed to create, manage and invalidate a digital document such as a digital negotiable instruments or document of title or any other document that needs to be represented as an original.

Enigio provides technology that can create transferable, fraud safe and at any time verifiable digital original documents, where the holder can evidence possession and full control over the latest version of the document.

The trace:original document could be seen as "digital paper". When created it becomes a unique digital asset with unique identity, it is represented by a file with content that has been "printed" to the "digital paper". The content can be the same type of content printed to paper but it can also be structured data that can be interpreted by machines. It has the same functionality as its paper equivalent but enables faster, safer and significantly more cost-effective management of these documents and does this in a digital environment.

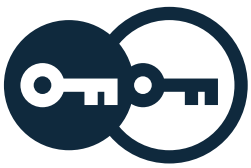
Solution

trace:original is unique, patented and differs from other current approaches that are trying to digitise documents using data in central platforms or data records in blockchains or distributed ledgers. It introduces a new possessable digital asset and digital information class; the trace:original document. The document, the asset, can be a PDF document and it can be kept secret and be digitally stored in any way the holder finds suitable.

The trace:original document is also a cryptographically secured file which means that all data, be it text, images, other files or structured data (all of which by technicians is referred as the payload) of every version of the document is cryptographically locked by hashes evidenced both in the document and on a publicly distributed ledger. The full function of the distributed ledger will be further explained below.

The trace:original solution consists of three components:

- the trace:original document, a file (a data "container" with a defined beginning, end and content).



- a secret private key, with which the current holder of the document can legitimise possession

- a public ledger, with the function of being a cryptographic notary service that can be used to trace and verify trace:original documents.

The document

The document, the file, is in a PDF format. By using PDF format the document can be easily recognized read and accepted as a document by most users globally. It can be sent over most channels and opened and read on most devices. A PDF also makes it possible to represent most digital documents that are already created today in organisations workflow systems and then printed to paper. A Word template or PDF template can be "printed" to a newly created trace:original document (digital paper) instead. Apart from being able to contain normal document content, the PDF original can also cater for standard electronic signatures and seals, as well as attachments of other files and also structured data of any format. The document is stored by the holder and no business content from within the document is published on the trace:original public distributed ledger.

To ensure that no content that has been added ("printed") to the document can be altered or manipulated without detection, both content and file are secured using mathematical one-way algorithms, "Hash-functions". The Hash function used is a standardised mathematical function that produces a string of characters that is a unique identification of the data set, a "digital fingerprint" of the content and the document. Every time a data set or a file is processed by the Hash function it gives the exact same result as long as the data stays exactly the same.

For a trace:original document, Hash functions are used to create cryptographic evidence proving the properties of the trace:original document. Enigio currently use a Secure Hash Algorithm developed by the US National Security Agency based on 256 bits (SHA256). SHA256 produces a number that can be represented by a 64 character hexadecimal string , the number of possible unique character strings are ca. 2^{256} strings, i.e. more combinations than the number of atoms on the planet earth. The hash becomes unique for the document and is also time stamped. By publishing all cryptographic evidence of the existence of a new document, new versions and added content to the document in a publicly available blockchain the evidence of the existence and the integrity of the document can be evidenced with mathematical certainty. Therefore, hash functions are ideal when:

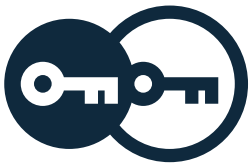
- you want to ensure that digital data has not been manipulated and
- you do not want to publicize the content of the document.

Hash functions have been in common use since the 1950s and are used in most aspects of creating IT security and trusted services today as for example the integrity of passwords.Anyone coming in contact with a trace:original document can verify its status and authenticity by using the public cryptographic ledger or by verifying the document at the Enigio notary webapplication for verification against the ledger at https://www.traceoriginal.com. If the hash of the document produces the same hash that has been published as the last version of the document in the blockchained ledger you know with certainty that your copy corresponds perfectly with the original. If it corresponds to a hash published earlier than the latest ledger entry for the document the copy is obsolete. If the hash does not correspond to any entry for the document on the ledger, or if the id of the document is not found on the ledger at all, the document is either corrupted, forged or not a trace:original document at all which is issued on that block chain.

The holder of the original document has complete and exclusive control of the asset. All business information is contained in the document and stored "off chain" by the document holder. That is, no business details are stored on the blockchain. When signing a transaction and registering a document update to the ledger, only the cryptographic hash-references, digital signatures and public key data is logged in the ledger – like digital fingerprints

of document integrity and proof of the current holder and that only the holder could have done the latest update. Therefore, the public ledger is only only a "publicly available digital notary service".

A holder in possession of the correct document and the correct cryptographic key has full control of the document and is allowed to register amendments (additions, what have been written can never be changed, not even by the holder) to the document in the ledger. Anyone receiving a copy of the document can verify if the copy corresponds to the current version of the original by testing it against entries in the ledger.



Cryptographic key pairs

To enable control and possession of the trace:original document each document version is linked to an asymmetric key-pair. The key pair consists of a public and a private key. The public key is inserted in the document and published on the distributed ledger. The private key is kept secret and must be used to manage and prove possession of an original. If the private key signature match with the public key you receive the value" true", in all other cases the value is "false". In the trace:original solution a distributed ledger is used as an "incorruptable mathematical notary service" holding the evidence of the state of the document and to which public key (who is the current holder) the document is tied to.

To be able to prove ownership (possession) and amend, transfer or invalidate the document you do not only need the correct private key you also need the latest version of the document. When the holder is identified and accepted the holder will be able to update the document and the new cryptographic references will be logged and signed on the distributed and public ledger. However, you cannot alter anything previously written in the document, you can only append new amendments after the previous amendment. To be able to create new trace:original documents you must have access to a trace:original Fullnode (a digital printer), to own your own Fullnode you need to be a trace:original customer.

As a holder you can transfer the document to a new holder, this is equivalent to moving the document to another public key for which the associated private key is controlled by the new holder in due corse.

The Distributed Ledger

The distributed ledger functions as a mathematical and incorruptible notary holding the history and the audit trail for a document without revealing anything about the content of the document. All is a "proof of the truth" hidden in plain sight as cryptographic references, ready to be used to verify the trace:original documents that are stored "off chain" with the current holder.

Possession, Transfer and Endorsement of a trace original document

Proving Possession

If someone holding a copy of a trace:original document wants to verify that the holder really is in possession of the document the holder can create a "proof of possession". The holder will use his private key and create a digital signature to proof possession of the private key for the document.

Transfer

If the holder wants to transfer the document to a new holder, this can be done in three different ways;

- By initiating a transfer to the receiver's e-mail (the receiver only needs to have an e-mail address, access to a computer and internet to accept the original)
- By transferring directly to a known public key for the receiver
- By transferring directly to the receiver Fullnode (if the receiver has a registered Fullnode)

The receiver needs to;

- Click in link to received e-mail and accept the document to an existing public key, create a new public key to the computer or accept to an own Yubikey device.
- Receive the updated transferred file via any channel to be able to manage it with the key
- The document will appear in the document storage of the Fullnode receiving it

When the document is transferred to the receiver ket the holder has lost control of the document, but the new holder cannot manage the document until they have received the latest transferred version of the file.

When the document is transferred to the receiver ket the holder has lost control of the document, but the new holder cannot manage the document until they have received the latest transferred version of the file.

Enigio offers API's, software and free web services to do all the above.

As any valuable physical asset, you need to store your digital assets safely, i.e. the private key needs to be kept safe and not disclosed. If you lose the private key, you have lost the original just as in the physical world. The advantage of the digital original is that if you have backup of the last version of the document it can still be verified as the latest original. And if the document in its latest transfer endorsement is endorsed to you it is still possible to prove possession even of the document cannot be amended, transferred or invalidated after the key is lost.

Endorsement

Legal endorsement is achieved by adding endorsement text as and amendment (addition) to the document and then electronically sign the endorsement text. The control of the document is transferred by digitally signing over the document to a new public key. In some use cases it might not be legally necessary to endorse and electronically sign in the document, then the transfer to the new public key could be enough as the receiver can proof possession. Endorsements and transfers can be performed in several different ways depending on the use case.

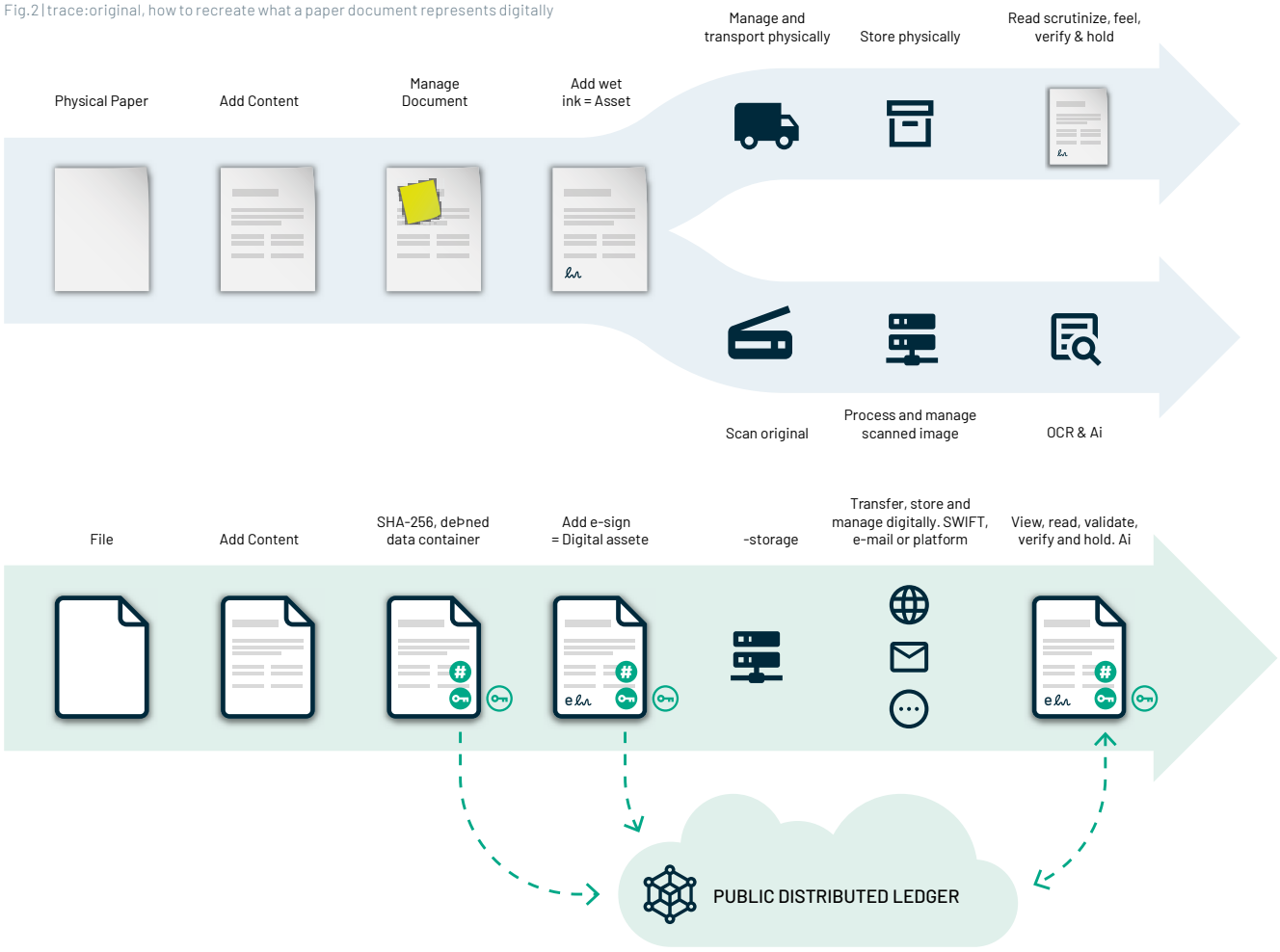
How to implement and use trace:original

To be able to create a trace:original document you have access to a Fullnode (digital printer) managed by someone else that give you access or you need to subscribe for an own Fullnode. Banks or their software suppliers can integrate trace original into their workflow systems by integrating with the trace:original Fullnode/Document API.

Creating a trace:original document

In the most simple integration scenario a new digital printer function is added to produce digital original documents from already produced digital documents that should otherwise be printed physically. This can be done stand-alone with Enigio Fullnode GUI or via call to the Create method in the API. Next level of integration is to add structured data (not only plain documents) as content to the newly created tracs:original document. The user can choose a selection of already supported Key stores or implement a Keystore interface to use a current KeyStore.The only requirement is that the Keystore is compatible with ECDSA (Elliptic Curve Digital Signature Algorithm) using the curve secp256r1 (same as Corda).

Fig.2 | trace:original, how to recreate what a paper document represents digitally



How to receive a trace:original document

A receiver of a trace:original document must inform the sender of the address (public key) to which the document should be assigned or simply the e-mail address so as a receiver you can accept the document to a certain key yourself. As possession of a trace:original document is defined by holding the private key associated to the original documents public key, the sender assign the control of the document to the receiver's public key.

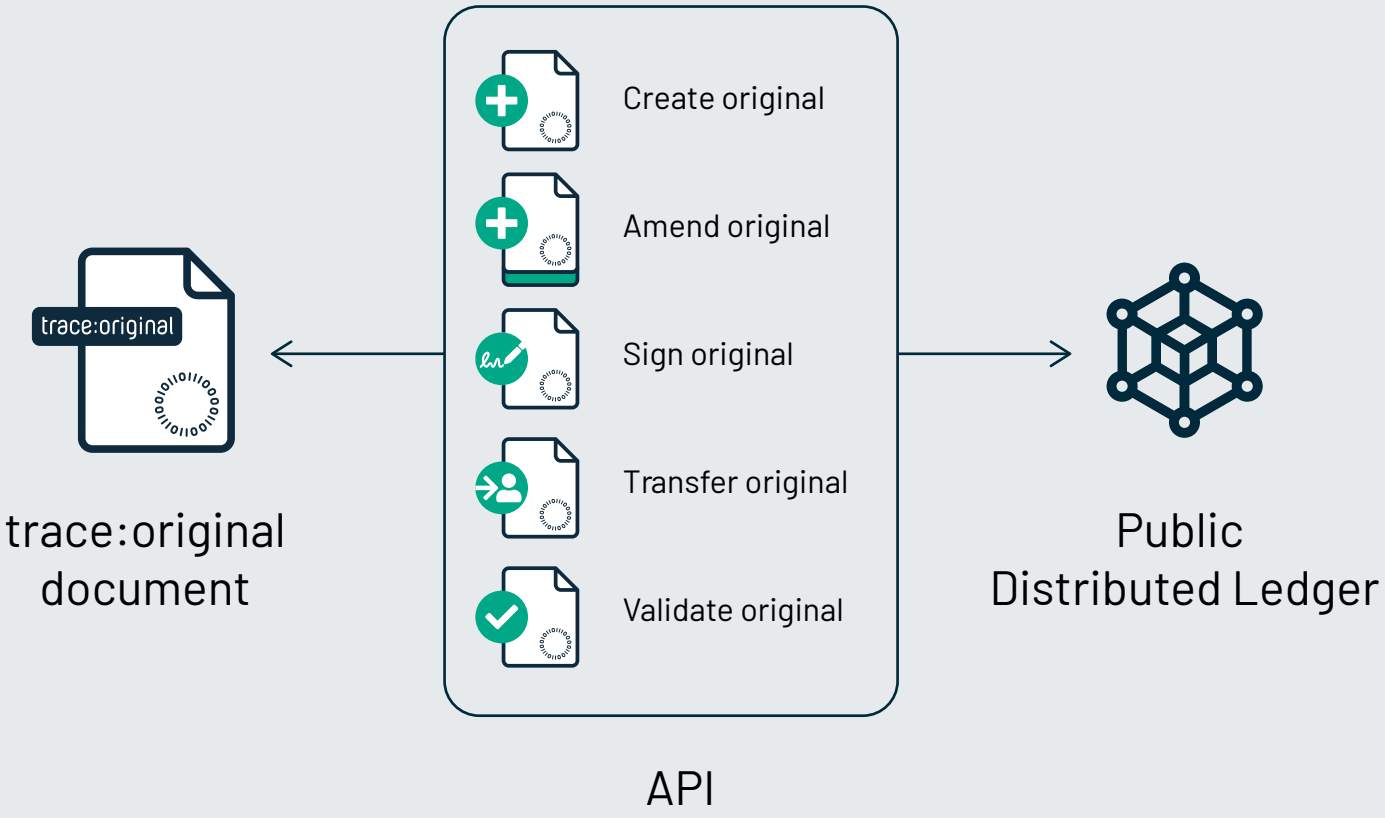
If the private key is lost the new holder of the document cannot evidence possession of the document. Hence control of the private key is essential. Once the document has been transferred to the new public key (registered in document and on the trace:original ledger) and the new updated document file is with the receiver, the transfer of possession is complete.

Tools to manage trace:original documents

High volume users of trace:original would typically integrate their front and back office systems to the trace:original APIs. Customers to trace:original have an own node with API enabling the creation and management of trace:original documents on the node. The node maintain a synchronized and fully updated copy of the ledger. Other typical high-volume receivers of documents can, once in possession of a document, make additions to, invalidate and transfer the document using APIs on a Stakeholder node, basically a Fullnode without capability for create (e.g. a customs authority department handling customs guarantees). A node can be installed on premises, in own cloud or as Software as a Service (SaaS) managed by Enigio.

User with lower volumes with limited need for auto- mated processing can use a any trace:original compatible web portal supporting this or the Enigio

Fig.3 | trace:original APIs



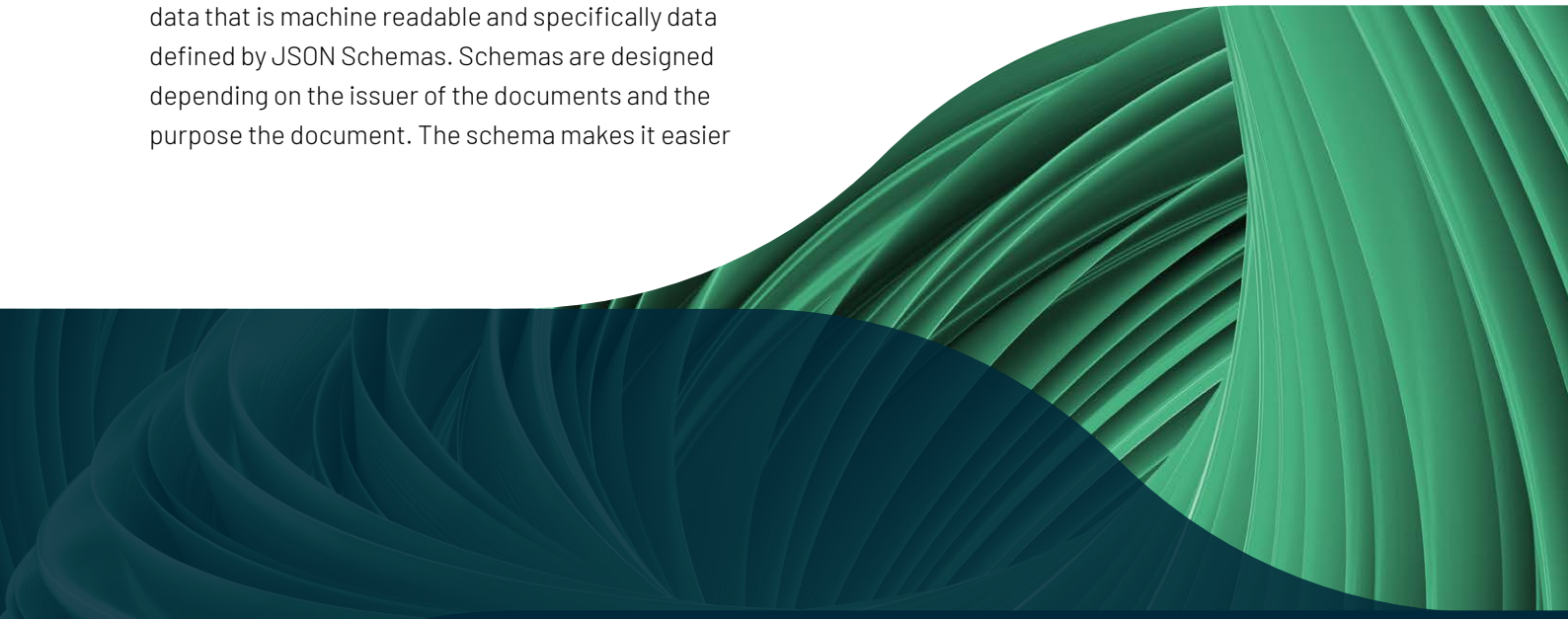
notary service (https://www.traceoriginal.com) where the user can verify, receive and manage trace:original documents. Use of traceoriginal.com is free of charge and available to everyone, making it possible for any person or organisation to receive and manage a trace:original document even without being on-boarded or being a customer. However, on https://traceoriginal.com, you cannot create new digital originals. Thus, what is needed for anyone who needs to receive or handle a trace:original document is access to a computer with a modern web browser and access to the internet.

JSON Schemas

The trace:original solution supports structured data that is machine readable and specifically data defined by JSON Schemas. Schemas are designed depending on the issuer of the documents and the purpose the document. The schema makes it easier to process the document content, for all parties concerned, as it defines objects in the document file. If a JSON Schema

is used in a document the document's schema is published on an internet URL by either the document issuer or an organisation responsible for a JSON Schema standard. This schema can be downloaded by anyone coming in contact with the document.

All trace:original documents are Ricardian contracts and are therefore capable of being interpreted and read by both man and machine.



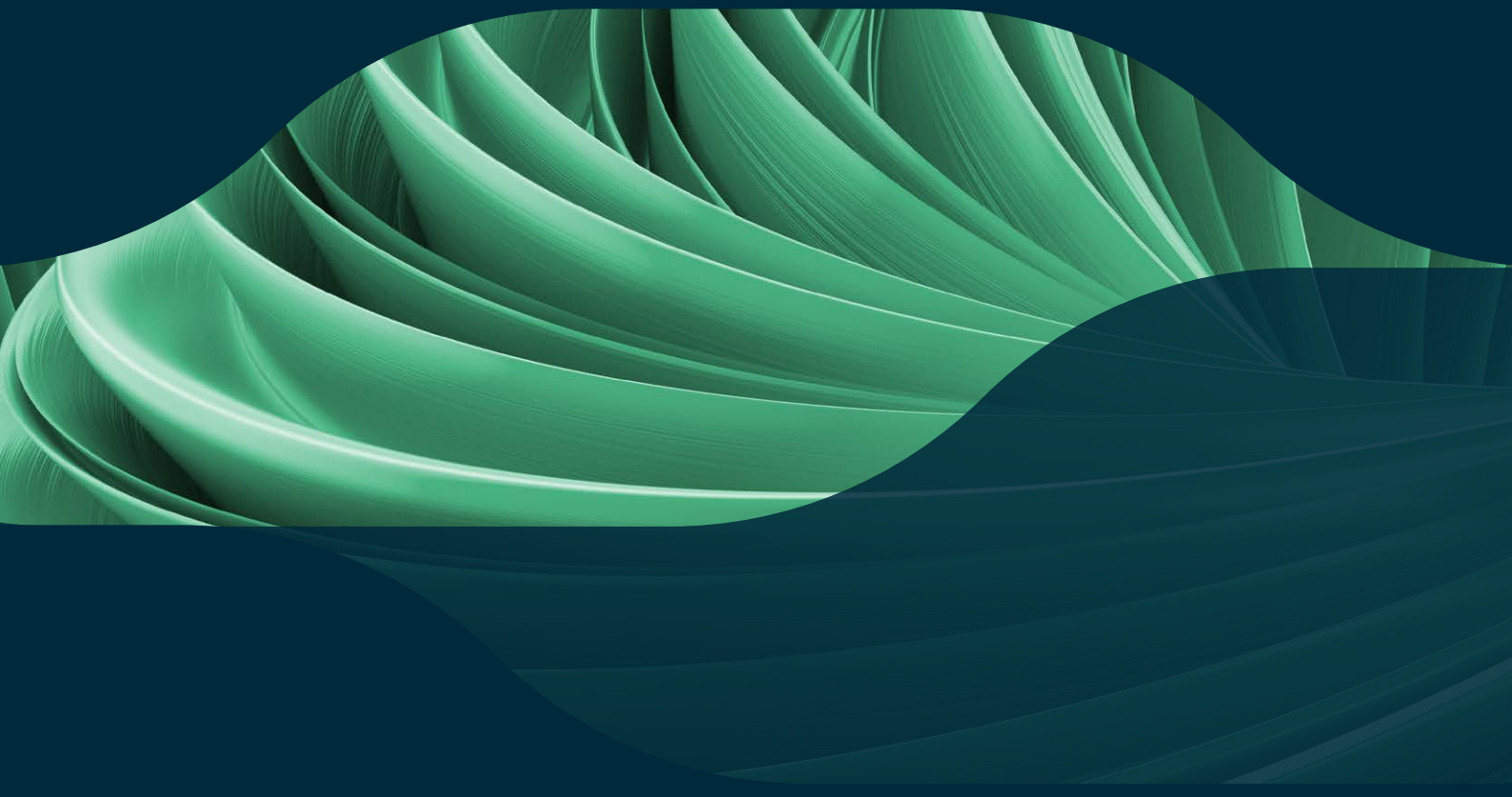
enigio

ENIGIO AB
Drottningholmsvägen 10
112 42 Stockholm, Sweden

Enigio offer solutions that ensure integrity and traceability of all your information to enable true and complete digital processes.

For more information, whitepapers and ways to contact us, please visit www.enigio.com.

Enigio's trace:original is freely transferable digital original documents. It has the same functionality and properties as paper documents but enables faster, safer and significantly more cost-efficient management.



enigio