IP²

Information Professional
Intellectual Property Lawyer

Report
SWOT and GAP Analysis of the Proof of Provenance project

This report is commissioned by the Netherlands Institute for Sound & Vision

SOUND&
VISION

Author: Maarten Zeinstra, IP Squared
Date: May 2022

Table of contents

Introduction

"A lie is halfway round the world before the truth has got its boots on".

A quote with unclear provenance perfectly sums up a current challenge in the use of digital information technologies. Misinformation, disinformation and deep fakes have become prominent phenomena in our daily newsfeeds. Often followed at some distance by initiatives that try to debunk, rectify or contextualise these harmful publications. Harmful media expressions undermine a properly functioning digital discourse. They can enforce polarising debates, discredit valid sources and change public opinion.

Deep fakes and doctored plain text have taken away the ability to trust media expressions on face value. A media expression in itself has become an insufficient medium to determine authenticity, authorship, or provenance. This challenge has become so pervasive that even good faith actors fall in the trap of trusting doctored social media publications for the truth.

One of the conditions to halt this is to have certainty of the authenticity of a media expression. Without authenticity, a proper functioning of the digital 'public space' is challenging. Knowing and being able to prove the authenticity of a media expression is one of the ways that misinformation is combatted. Other valid means like regulatory frameworks enforced by watchdogs, content moderation, media literacy, are just as necessary, but out of the scope of this comparative study.

"Proof of Provenance", or PoP is a project[1] that develops a means for institutions and persons to create a certificate of authenticity that indicates that a person with certain characteristics (attributes) vouches for the authenticity of a media expression. As, strictly speaking, a consumer can only determine that the signer of that expression has signed that expression, it does not prove that they are also the author of that expression.

This publication is part of the first phase of the project, it introduces aspects of the PoP project and provides a SWOT analysis based on a comparative study of similar initiatives (Addendum 1) and a GAP analysis (Addendum 2) in order to strengthen the development of the PoP and to reflect upon the project's goals and means. It does not contain a full description of the final capabilities of PoP.

[1] See PublicSpaces start met Proof of provenance project (Dutch)

Proof of provenance

Proof of Provenance, or PoP, is a project that investigates how online media expressions can be provided with a proof of authenticity. PoP is not a Proof of Accuracy, a Proof of Truthfulness, or even a Proof of Authorship[2] of media expressions. None of these can be verifiably be achieved with the investigated technologies. PoP is a way to authenticate the source of the expression. I.e. that an entity with a certain authority or trust places a PoP signature on the expression.

The project aims to have an expression signed by an attribute of a digital identity. This is not necessarily their legal name, but a characteristic of this person (e.g. Older than 18 years, a journalist, Medical Doctor, etc.). The identity or its characteristics should be able to be independently verified, without making the signer necessarily traceable. The project believes that this feature maximises the privacy of the signer.

For example, it is not always necessary that journalist Alice signs a media expression with her name. She might want to exclude her name to avoid prosecution in a conflict region. And, as said before, information captured in plain text cannot be trusted on face value. Even if Alice signed the media expression with her name, that still does not make her a verified journalist. There is a need to sign a media expression as a journalist, working for a trusted publisher, vouched by an independent party. The independent party should be a trustworthy source, creating the assumption that this makes the signed expression trustworthy as well.

Signing of media expressions is in itself not new. eSignature services such as DocuSign and PandaDoc are often used for document signing, mostly for contracts and similar documents that have specific audiences. In these cases provenance itself is not a big challenge, as the parties involved in the signed documents are usually known to each other. Most of these market solutions use a centralised authority to check the validity of the applied eSignature. PoP wants to adopt a decentralised authority system.

A decentralised authority system allows for the distribution of authority and trust among all partners in the distributed system. By sharing and confirming transactions within a decentralised authority system the user does not need to trust a single institution, but a majority of organisations in the collaboration.

The project does not want to store more personal data than strictly needed. When signing a media expression with PoP, Public Key management, however, is still required. Cryptographic keys of specific ‘authorities’ must be findable, and for verification of that signature. PoP uses the IRMA (I Reveal My Attributes)[3] infrastructure and technology to acquire this functionality. IRMA is an identity management platform that enables users to reveal personal properties (attributes) – and only specific attributes – in a secure manner.[4]

[2] It could however be possible to expose your legal name via IRMA when you sign your media expression, however that does not proof that you are the author. It merely communicates that you claim to be the author.

[3] IRMA is developed and maintained by the Privacy by Design Foundation and supported by SIDN.

[4] Hampiholi, Brinda & Alpar, Gergely & Broek, Fabian & Jacobs, Bart. (2015). Towards Practical Attribute-Based Signatures. (DOI: 10.1007/978-3-319-24126-5_18).

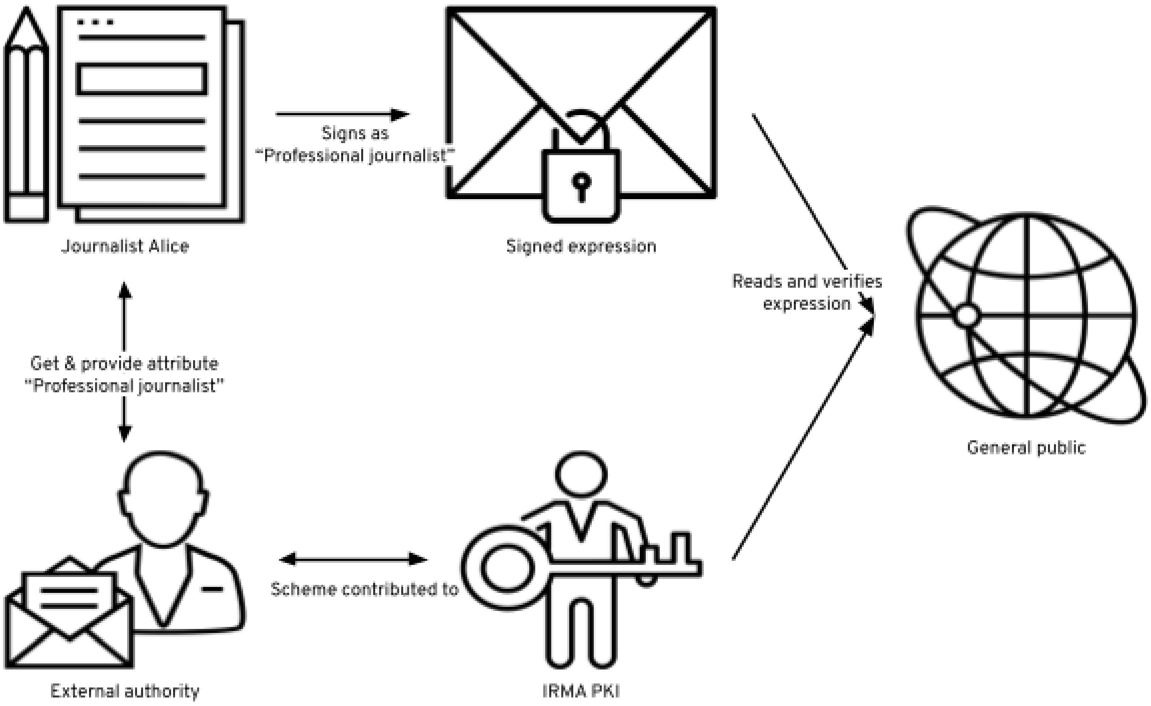

Journalist Alice
Signs as "Professional journalist"
Signed expression
Reads and verifies expression
General public
Get & provide attribute "Professional journalist"
External authority
Scheme contributed to
IRMA PKI

Fig. 1 Global overview of the working of PoP

Needs requirements analysis

Below, the main requirements of the PoP are outlined, these have been gathered through desk research and interviews with selected representatives of the stakeholders within the development of this proof of concept project.

The requirements analysis is divided into three sections that are based on a concept of an information life expression. Media expressions have an information life cycle. Each part of this cycle has its own needs and requirements. This section reflects upon these needs. The lifecycle is broken down into three parts:

- Creation and publication of media expressions
- Consumption and reuse of media expressions
- Archiving of media expressions

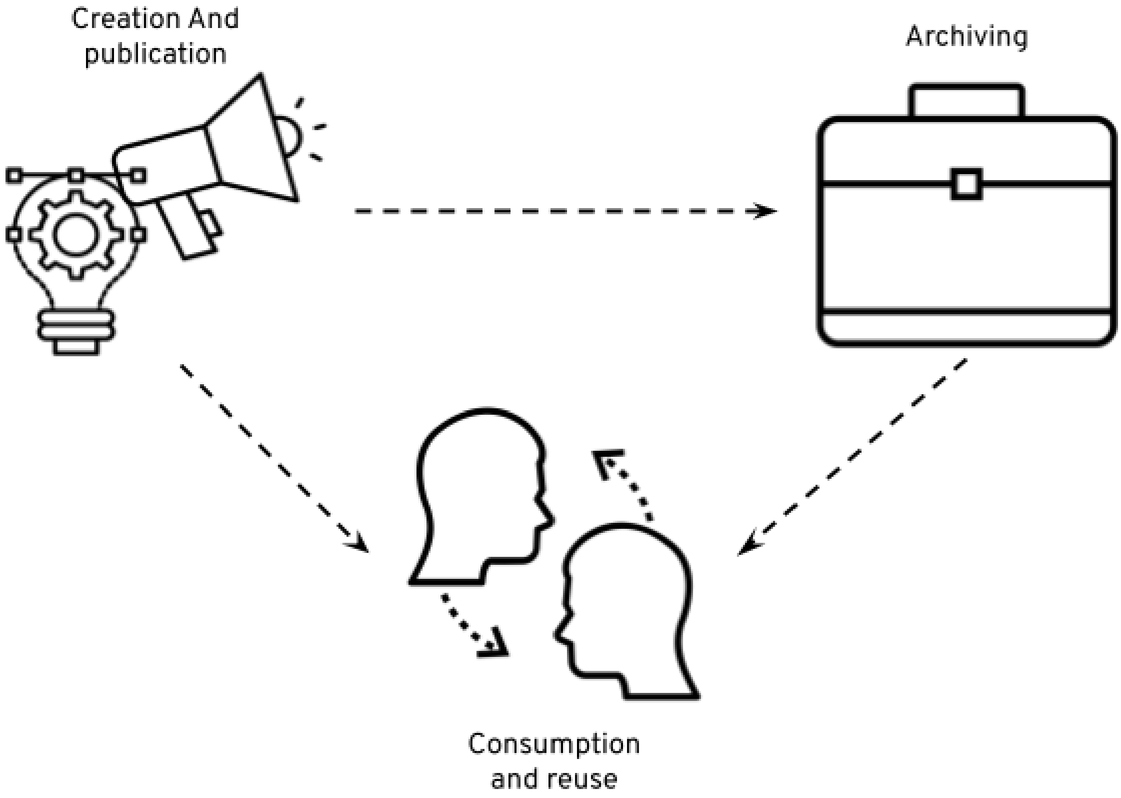


Fig. 2 Media Expression life cycle

Creation and publication of expressions

The producing parties in this project are professional media companies in the public sector. The Netherlands has several public service broadcasters that are tasked to produce entertainment, but also information and news. Some of them, like the VPRO and the umbrella organisation NPO, are partners in this project.

The general public remains to have trust in these public broadcasters.[5] However, these institutions are increasingly competing with social media for the attention of their audience.[6] To strengthen the position and authority of these public broadcasters as reliable sources of information they want to provide proof that a media expression is actually produced by them, regardless of where that media expression is consumed. By doing this they hope to increase the relevance and trust of their media expressions in the online world. Additionally they want to be able to sign an expression not solely as a journalist, as in the example of the introduction, but as their organisation as well. This will allow them to promote their own institution as a source of truthful information, as well as vouch for the journalist that writes the media expression.[7] They want to be able to sign, or have expressions signed, from external sources and journalists as

[5] Reuters Institute – Digital News Report 2021, pagina 90
[6] Marketing Facts – Social media in Nederland 2022
[7] They of course already provide some measure of provenance authority by using SSL for their web platforms.

well.[8] They also considered images and video as part of the comprehensive html document and would like to sign these media expressions as well. Either through signing the url as part of the text that is hashed, or by independently signing the image by using a cryptographic and or perceptual hash.

They are interested in possible traceability features of a signature. Which makes it possible to always find the original context of a selection or quote of a media expression. For example, by adding the canonical URL of the original publication into the signature. Which means that they need to keep that URL attached to the expression in order to have the signature validated.

Finally, the public service broadcasters point out that reuse of selected material is usually done by quoting a selection of another publication. Not by copying the whole, whereas the media expression is signed on the whole or at most at the level of paragraphs. They would be interested in functionality that allows the selection of a quote that provides crafted HTML that hides the non-quoted section to keep the signature intact on the platform where the quote is used.

One of the project's partners is the VPRO. They use the Magnolia CMS to write and publish their media expressions. They want to integrate the signature service of PoP to sign and publish the media expression in tandem with the signature. They indicated that they want to sign the contents of the expression (i.e. the paragraphs of the text), not the expression in its entirety (i.e. the webpage), because the entire message can be updated or changed depending on the platform (e.g. mobile, different browser, etc.) If signing of their own content works successfully they are interested in extending this to having external parties sign their contributions.

Consumption and reuse of expressions

The project intends to increase trust when consuming media expressions by introducing independently verifiable signed expressions. The project aims to provide this by developing web technology that consists of three parts.

First, a data standard that allows publishers to attach a signature in a machine readable manner. Developing a data standard allows others, outside of the project, to adopt the PoP without needing to contact the project's partners. Initially only textual media expressions in HTML will be included in the standard.

Then an open source browser plugin/library is developed to scan the webpage that a user visits in order to detect signatures following the data standard.[9]

Finally, a user interface will be developed as a special provenance view akin to the reader view of browsers. that shows the signed expression without its context or CSS mark-up as intended by the original producer. CSS mark-up can significantly alter a media expression, it is not difficult to hide whole paragraphs using css or javascript so this view is necessary to ensure that consumers of the expression are not misled. The viewer instead adopts its own CSS mark-up to ensure that the entire text is presented.

[8] E.g. from external sources of the investigative journalism platform argos

[9] See gitlab.waag.org/code/proof_of_provenance

Reuse of the content can be done by using a built-in copy function, this will be placed in a html crafted fragment including machine readable signatures on the user's clipboard, they can use the signed expressions as a whole on different platforms, while keeping the signature intact. This raises the question whether the copy-able sections are sufficient, given common practices of copying quotes from other sources, instead of whole paragraphs and articles.

Archiving of media expressions

The heritage institutions that are part of the consortium have a different perspective on the provenance of media expressions. Provenance has a slightly different meaning in this sector. For heritage institutions, provenance of an expression is the provenance of an object that is ingested into their collection. It is usually described in collection management systems at ingestion or added later through research and metadata enrichment of its collections.

They see it as their task to archive the expression and its context (the whole webpage/website) while keeping the context unaltered. This context can contain a signed expression. This subsection, the signed expression, is for them just as interesting as the context where the expression is found. They would not just archive the signed expression but also the webpage or domain that it is found in.

Additionally, heritage institutions see themselves as sources of authority and trusted partners to guarantee the authenticity of their collections. Note that they do not vouch for the truthfulness of their collection, merely its authenticity. They justify being this source of authority and trusted partners of authenticity by adhering to standardised and certified procedures. It is authority all the way down.

For example, the Netherlands Institute for Sound & Vision has a Core Trust Seal (CTS) and its predecessor Data Seal of Approval (DSA). These internationally recognised seals of approval verify that the institute meets requirements reflecting the core characteristics of a trusted data repository.[10]

The heritage institutes note that internet publications are by definition a different case in contrast to other digital objects they ingest, such as television or radio broadcasts. Internet publications are always a snap-shot of an evolving environment, instead of the end-product of a process (e.g. video, report, or book). This verification of information – and of the PoP – that is mutable in the outside world can only be determined at the time of ingestion for the expression at the time of ingestion. The institutions also indicate that finalised products, like video, can consist of multiple independent expressions, where each section could warrant an independent signature.

For heritage institutions, this means that the verification of the signature of the content, in the case of PoP, needs to be stored in a static manner. For example, by providing an additional signature to signed content that the content was properly verified upon ingestion. It might be the case that an expression in the collection of an heritage institution is not touched for many

[10] See Beeld en Geluid verkrijgt CoreTrustSeal

years, and in that time the verification process particular to PoP can break. Ideally this verification is stored transparently and in an immutable manner.[11]

The heritage institutions of the project have no intention of signing their own publications at the moment. They do use cryptographic hashes on (some of)[12] their digital objects to ensure that the object is not corrupted or changed when ingested and moved inside their collections. It is important to note that heritage institutions frequently make a presentation copy (or proxy) of a digital object. I.e. to ensure they can be accessed on the web or to minimise the size of the file for their audience. A cryptographic hash can thus only be applied on the authentic original ingested object. They have not employed technology that verifies if the format shifting has resulted in altered content in the expression.

However, the institutions intend to maximise the utility of digital signatures when they are identified in digital objects upon ingestion. Meaning that they need to abstract the signature from the expression and add it to the metadata of the ingested expression. This way the signature becomes searchable and queryable by users of the heritage institute.

Finally, the institutions indicate that the signatures themselves can be interesting topics of study as well (i.e. to question how much content of a publisher is signed over a period of time), and that the chosen solution needs to be technologically stable and available in the sense of decades instead of in years.

Means and implementation

As mentioned, PoP has adopted IRMA as their main technology and infrastructure. IRMA is an infrastructure and a technology with the same name that allows an issuer to provide an attribute to a local wallet. The local wallet (the IRMA app) keeps that attribute and can provide it upon request to a verifier (e.g. a platform).

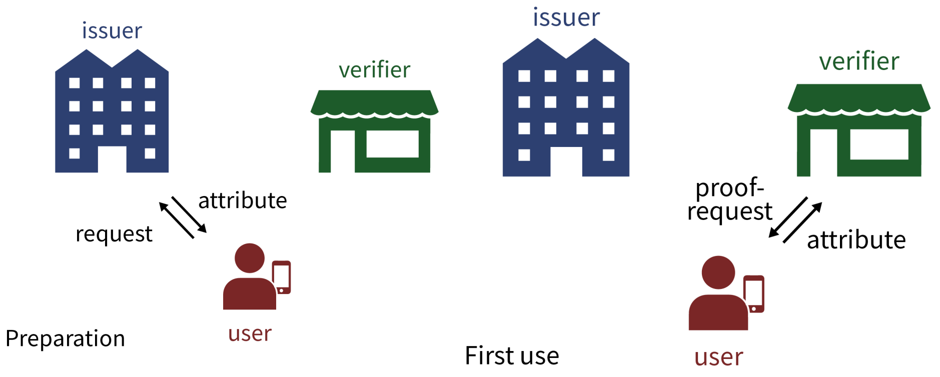


Fig 3: Basic working of IRMA

For example, a journalist (the user, with an IRMA wallet) could theoretically ask the Netherlands Union of Journalists to verify their status as a journalist (the issuer). The issuer then provides a

[11] Additionally, inspired from the ARCHANGEL project, hashes of ingested media could be published, even if the ingested material cannot be published by the archive. To provide a transparency register for material that is not publicly accessible yet.

[12] Sound and Vision uses MD5 on their video, audio files, and web archive, not on static images.

signed attribute to the wallet of the user. The user uses this attribute to prove that they are a journalist to other parties (verifiers), without having to transmit their identity. They only communicate that the issuer has assigned them the attribute and the verifier can therefore assume that that attribute belongs to the user.

The Union of Journalists could, of course, ask for other attributes (as a verifier) to verify the identity of the user before issuing the attribute. I.e. by asking for a name or address that the user obtained from a municipality, which can ask for another attribute or other authorization schemes to validate the user it is providing an attribute to.

IRMA also allows signing of documents[13], in such a way that the user does not have to be involved to prove their attribute upon public verification. It is this signing mechanism that is adopted in the PoP protocol. A PoP signature thus contains sufficient information to assure an audience that the verifier has proven that the document is signed with a verified attribute. No interaction between the signer and the audience is necessary.

In fact, a – cryptographic hash of – the media expression itself is used during the signature and verification. Meaning that if the media expression is altered, the signature is no longer valid (can no longer be proved).

IRMA does at its core have aspects of 'traditional' signing services. IRMA adopts a Public Key Infrastructure, hosted at the Dutch top level domain registry SIDN, to ensure that the person who claims to hold a public key has added a certificate to the document as a digital signature. Examples of traditional signing services are PandaDoc, DocuSign and, to some extent, PKI Overheid[14].

[13] Using Fiat–Shamir heuristic, see Fiat–Shamir heuristic - Wikipedia

[14] PKIOverheid is not a full-featured signature service like PandaDoc and DocuSign, but it allows signing documents using its public key infrastructure.

Landscape analysis

The desk research has yielded an overview of several of the most interesting and relevant technologies and initiatives that either are similar to the PoP in goal, or in adoption of technology. A survey of these technologies and initiatives, including a concise SWOT analysis per initiative, can be found in Addendum 1 of this report.

Initiative name	Category	Scope / Main use	Main user group	Open / closed	State
Contentauthenticity.org	Coalition for Content Provenance and Authenticity (C2PA)	CAI is an implementation of C2PA that focuses on displaying C2PA's manifest to a general audience	General audience	Open Source[15]	Research & Development
Project Origin	Coalition for Content Provenance and Authenticity (C2PA)	Project Origin is an infrastructural extension of C2PA, i.e. for hosting C2PA manifests	Creators and general audience	Open Source	Research & Development
Wordproof	Hash-to-blockchain	Service for business and the general public to see if an expression is copied and to verify that an expression is not changed for the audience of the expression.	Publishing platforms	Open source	Running service
Proof of Existence	Hash-to-blockchain	Hash a media expression and put that hash on BitCoin to prove the existence of a document at the time of registration.	Content creators	Open source	Running service
ARCHANGEL	Hash-to-blockchain	Hashing media expression of	Archives	Closed	Proof of concept, No

[15] Open source code is announced, but not available at time of writing.

Initiative name	Category	Scope / Main use	Main user group	Open / closed	State
		archives and distribute the hashes among in a decentralised blockchain with other archives	and their users	source	longer active
PandaDoc	Digital Signature Service	Sign digital document	General public	Closed source	Running service
DocuSign	Digital Signature Service	Sign digital document	General public	Closed source	Running service
PKI Overheid	Digital Signature Service	Public Key Infrastructure for the Dutch government	General public	Closed source	Running service
Signicat.com	Digital Identity Service	Digital identity services for identify proofing and signatures	General public	Closed source	Running service
Sovrin.org	Digital Identity Service	Decentralised digital identity services for identify proofing and signatures or claims	General audience	Open source	Running service

Initiative name	Category	Scope / Main use	Main user group	Open / closed	State
Takenode.org	Other relevant	Create a certificate of ownership with explicit permissions for reuse of that content	Content creators	Open source	Running service
Monetising Open Video Assets	Other relevant	Community-run database of rights ownership claims with identifiers for video	Content creators	Open source	Running service
Rewrited.news	Other relevant	Watchdog that hashes media expression to detect any changes over time	General public	Open source	Proof of concept, No longer active
Sourcer	Other relevant	Ranking and analysing news publications.	General public	Closes source	Start up

The **Coalition for Content Provenance and Authenticity (C2PA)** developed a technical specification for providing content provenance and authenticity. The specification is "designed to enable global, opt-in, adoption of digital provenance techniques through the creation of a rich ecosystem of digital provenance enabled applications for a wide range of individuals and organisations while meeting appropriate security requirements."[16] The specification is implemented in the projects **ContentAuthenticity.org**, and **Project Origin**.

A similar initiative is **MOVA/ISCC** that develops a standard with a universal identifier for digital content using a similarity-preserving fingerprint. Instead of working with a consortium that tries to integrate a specification into products it attempts to develop an ISO standard without.

Several initiatives that were classified as *hash-to-blockchain* have been explored. These initiatives create a proof of existence claim and store these in a distributed ledger, like the bitcoin blockchain. By storing the cryptographic hash on a distributed ledger a third party can verify that the signer had access to a media expression on a certain date. Examples of these types of initiatives that were examined are **Wordproof, Proof of Existence**, and **ARCHANGEL**.

Several **traditional digital signing services** were also analysed. These offer services for using public-private key cryptography for signing digital documents. They hold a centralised Public Key Infrastructure to be able to verify that the signer held the private key connected to a certain public key. Examples are **PandaDoc**, **DocuSign**, and to a certain extent **PKI Overheid**.

Additionally, **Sovrin,** a competing digital identity service to IRMA, was explored. This very similar service used a distributed ledger and digital identity for which you can control what you share to allow signing of documents.

Finally some other notable services were investigated that do not simply fit in the above categories. **Takenode.org** allows you to create and sign, with IRMA, a certificate of your content similar to Proof of Existence; it stores the certificate centrally. **Rewrited.news** is a no longer operating proof of concept project that acted more as a watchdog, by hashing media expression from reputable media outlets it provided an overview of how and when a media outlet changed their media expression. They stored the hash of the outlet on a public blockchain**.**

[16] See C2PA Implementation Guidance

SWOT

Based on these analyses, the following Strengths, Weaknesses, Opportunities and Threats of PoP become apparent. Strengths and Weaknesses come from inside the project. Opportunities and Threats are external to the project.

Strengths	Weaknesses
What are PoP's defining strengths in relation to similar initiatives? ● Open specification ● Public institutions ● Sufficient technological expertise	What are PoP's defining weaknesses in relation to similar initiatives? ● No simple user experience ● Not available on social media platforms ● Attached metadata ● False negatives, unsigned expressions
Opportunities	**Threats**
Given the similar initiatives, what are possible opportunities to mitigate the weaknesses? ● Storing metadata (certificates) on an external (distributed) service ● Aligning with other initiatives like C2PA and MOVA ● Further open up the PoP consortium ● Heritage institutions as providers of provenance and authentication services	Given the similar initiatives and PoP's strengths, what are remaining threats to PoP: ● External temporary funding ● Low adoption ● Technological vendor lock-in

Strengths

Similar to C2PA, PoP tries to develop an **open specification** on how to share and verify certain aspects of a media expression. Developing an open specification allows other parties to adopt the specification, without needing to contact or ask for permission from any third party. This increases its chances of broad adoption, even if the consortium no longer supports or develops the project.

Just like ARCHANGEL, PoP includes **public institutions** in its consortium. Public institutions are less prone to change in adopting technologies, and once technologies have been adopted they are likely supported for a longer period than private entities. Therefore increasing its stable adoption.

Similar to most of the initiatives introduced above, the PoP project has **sufficient technological expertise**. It is supported by both practical and theoretical experts on technologies like IRMA, hashing and web technologies.

Weaknesses

All of the initiatives, including PoP, have **not managed to develop and successfully deploy a simple user experience for copying and distribution** of signed media expressions, while keeping the signature of the media expression intact. The Content Authenticity Initiative tries to address this barrier by including many media platforms and tool makers in their consortium, but none of the platforms and tool makers of CAI have taken C2PA into production yet.

PoP intends to combat misinformation and fake news, but fails to bring the technology to the platform where misinformation is spread most easily: on **social media platforms**.[17] Either the project has to try to include these platforms to adopt the specification of PoP or combat misinformation using PoP via additional means that are currently out of scope, like looking at the added value of watchdogs, technology research on content moderation, or try to improve media literacy.

PoP, like the standard C2PA, **attaches** the **metadata** to the expression itself. The 'proof' cannot live independently from it. Project Origin tries to mitigate this by researching a centralised cloud storage of C2PA metadata. Currently there is no way to retrieve PoP metadata once it is no longer attached to the expression. Copying and pasting media expressions without the tools that support PoP – or similar initiatives like C2PA – destroy the chain of provenance.

It is argued by the project that adopting PoP, or a similar initiative, enhances the reliability of the online media. Signed media expressions can now be verified as being expressions vouched for by a specific publisher, or journalist. However, this creates the risk of false negatives. **False negatives** occur when a signed media expression is used on a platform that does not support, or strippes, the PoP manifest. Meaning that a signed expression cannot be verified. Even though the proof is no longer accessible, it still exists. Given an envisioned ecosystem where PoP is broadly adopted, such an expression is consumed with distrust as other expressions from the same publisher will likely have a signature.

Opportunities

There are two ways to mitigate the risk of losing metadata when copying a signed media expression as discussed in the weaknesses section. Some initiatives, like **Project Origin, Wordproof, Proof of Existence, and Sovrin**, are using Decentralised Ledger Technology to verify that a certain aspect belongs to a media expression. They use a (cryptographic) hash to uniquely identify the expression and look up its (reference to) metadata in a decentralised ledger. PoP could explore features for storing signature metadata in a distributed **external store**. This could have an added side-effect of raising the transparency of the signed media expressions.

The project could also think about **attaching itself to existing initiatives**, where Project Origin seems to be the best match to PoP. It is actively trying to address most of the weaknesses identified in PoP and has most of the strengths as well. As C2PA deals mostly with visual media, "provenance from glass to glass" (from camera lens to monitor) the embedded manifest could

[17] See for example Shao C, Hui P-M, Wang L, Jiang X, Flammini A, Menczer F, et al. (2018) Anatomy of an online misinformation network. PLoS ONE 13(4): e0196087. https://doi.org/10.1371/journal.pone.0196087 who are also the developers of Hoaxy

be signed in a PoP context, enhancing both propositions. C2PA does not, however, seem to have many public institutions attached to it. Finally, PoP could serve as an additional tool for initiatives like **Wordproof** or **Sourcer** to further strengthen the authority position of the services that these initiatives provide.

If PoP cannot attach itself to existing projects, it could attempt to create a more **open public consortium** around its standards. Running the risk of developing a competing standard to the C2PA specification. If PoP does not want to continue to maintain its own infrastructure and standards it could also bring its lessons learned regarding attribute-based signing to other similar projects like C2PA. An important caveat to remember is that the intention of the project is to be proof of concept, not a full fledged infrastructure to be adopted by all online publishers.

Additionally, it can also see how the two standards can complement each other by developing a method to include the C2PA manifest in the certification when signing a media expression. The consequences of this method are not completely clear and merit additional research.

Finally, there is an opportunity for **heritage institutions to provide additional services** to their users by signing, and or verifying media at the source. They have an opportunity to become an additional source of authenticity.

There are also means to attach reproducible identifiers to a file that can survive small changes to the media file and up to some extent on conversion of the expression in another file format.[18]

Threats

Similar to other initiatives, like ARCHANGEL, TakeNode.org, the PoP project and its underlying technology, IRMA is currently exclusively funded by **external temporary funds and subsidies**. If the project is not collectively maintained and promoted by key publishers, technology and infrastructure providers, there is a substantial risk that the project will remain in a research phase.

There's a risk the project might **not be widely adopted** by its public sector partners. If the project fails to be adopted, then long-term investments and support seems less likely. Additionally, consumers of a signed media expression do need to feel urgency to validate the signed expression and become wary of unsigned expressions for the project to have a substantial impact on the digital public space. An important caveat to remember – and to repeat – is that the intention of the project is to be proof of concept, not a full fledged infrastructure to be adopted by all online publishers.

The project relies on the installation of a **browser extension** or the use of **javascript** in a browser. Privacy aware browsers no longer automatically allow javascript to be executed by default. Equally, each browser has its own extension ecology that needs to be maintained and promoted. Although this is changing with effort like the WebExtensions Community Group (WECG)

[18] For example commonsmachinery/blockhash and pHash.

Recommendations

This publication is part of the first phase of the PoP project, it introduced aspects of the PoP project – its goals and ambitions – and provides a SWOT analysis based on a comparative study of similar initiatives (Addendum 1) and a GAP analysis (Addendum 2) in order to strengthen the continued development of the PoP project.

PoP is a project that works on the challenge of providing trustworthy media expressions whose provenance can be traced back to authoritative sources to strengthen a proper functioning of the digital 'public space'. Combating misinformation by providing means of knowing and being able to prove the authenticity of a media expression is only part of the story.

The SWOT and GAP analysis of PoP identified that the project is meeting its project expectation and adoption by developing an open standard, developing and exploring tools for the consumption of PoP signed material.

For longevity of the project the project could look further into the following areas, in addition to continue on their development road map:

1. **Research external storage location of metadata** (the signature) of a media expression. Currently the signature of the PoP lives attached to the expression itself. Incorrect copying can easily destroy the signature and it can subsequently no longer be reproduced without going to its original source. This can, but doesn't need to be, be done on a distributed blockchain. Other initiatives have shown that centralised solutions are also possible.
2. **Develop Support for multiple media formats**. This objective is already achieved for text and images, but it is worth looking into audio and video as well.
3. **Explore collaboration with similar initiatives.** The largest weakness of the project is its adoption rate. Without substantial adoption the project will not gain traction to be further developed or used by third parties.
4. **Add initial publication platform to signature.** The partners in the project that publish signed content argue that the original publication platform could be just as important as the confirmation that the expression is signed. Consider adding a metadata field as part of the signature that holds the canonical URL of the original publication location.
5. **Improve user experience by exploring quoting text while keeping signature intact.** Explorations are under way to facilitate copying of signed sections of a media expression by copying the HTML that includes the signature. Explore whether it is possible to select a quote and mark up the copied html to include the entire signature, but only show the selected quote.
6. **Distinguishing between signed and unsigned material on pages that contain both.** This could be in scope of the project, but for the proof of concept it would require an action of the user to create this view to distinguish between signed and unsigned material.
7. **Research storing verification of a PoP in a static way for archiving purposes.** This is currently out of scope for the project. PoP could be used to sign ingested material for the heritage sector, but it requires additional research if this is the right approach.

Colofon

This work was commissioned by the Netherlands Institute for Sound & Vision.

About IP Squared

IP^2 is a one-man strategic information consultancy firm run by Maarten Zeinstra, LL.M. M.Sc., who combines his experiences of being an Information Professional and an Intellectual Property Lawyer (jurist).

Licence

Figures

All figures, except 1 and 3 are all rights reserved, they are used in this publication as quote to clarify the workings of discussed tools or technologies.

- Figures 1 and 3 contain icons that were developed by Creative Stall, licensed under a Creative Commons attribution 4.0 licence.
- Figure 2 was taken from the irma.app/docs/what-is-irma on May 11, 2022, by Privacy by Design Foundation and SIDN.
- Figure 4 was taken from C2PA's explainer documents.
- Figure 5 was taken from proofofexistance.com.
- Figure 6 is the author's own certificate of a document on TakeNode.org.
- Figure 7 is a screenshot of Sources, from GetSourcer.com.

Addendum 1 – Similar initiatives

There are several other technologies and implementations of these technologies that address authenticity of provenance information in some form or another. This section deals with these initiatives. Some of the discussed initiatives are technologically close to PoP, like C2PA. Others are more aligned with the soft goals of PoP, like WordProof and MMGA.

The following initiatives will be described:

1. Coalition for Content Provenance and Authenticity (C2PA) and its implementations
    - Contentauthenticity.org
    - Project origin
2. Hash-to-blockchain initiatives
    - Wordproof
    - Proof of Existence
    - ARCHANGEL
3. Traditional digital signing services
    - PandaDoc
    - DocuSign
    - PKI Overheid
4. Digital identity service
    - Signicat.com
    - Sovrin.org
5. Other noteworthy
    - Takenode.org
    - Monetising Open Video Asset
    - Rewrited.news
    - Sourcer

Each initiative is concisely introduced, a summary of the adopted technologies is given, and for each initiative the following key indicators are described:

- **Governance** – Who are the main stakeholders of the initiative?
- **Adoption** – What is the widescope use of the implementation by the general public, consortium, or platforms?
- **Implementability and adaptability** – How easily can this implementation be adopted, given the needs of the PoP project?
- **Durability** – How durable is the implementation, what are its weakest links and/or single points of failure?
- **Interoperability** – Can the implementation be adopted to further strengthen the PoP project? Does the project use/describe an existing open standard?

This overview is followed by a summary of the strengths, weaknesses, threats and opportunities of the initiative in relation to the needs of PoP.

Coalition for Content Provenance and Authenticity

The Coalition for Content Provenance and Authenticity (C2PA) developed a technical specification for providing content provenance and authenticity. The specification is "designed to enable global, opt-in, adoption of digital provenance techniques through the creation of a rich ecosystem of digital provenance enabled applications for a wide range of individuals and organisations while meeting appropriate security requirements."[19]

C2PA adopts a model for storing and accessing cryptographically verifiable information whose trustworthiness can be assessed based on the below presented trust model.

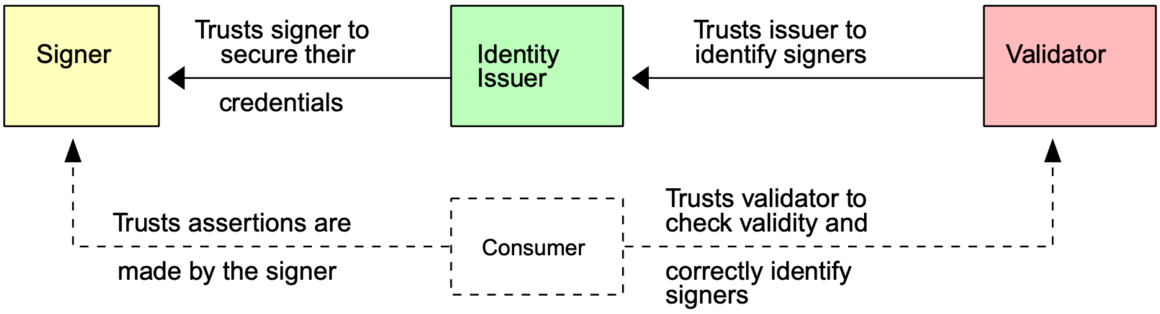

Signer
Trusts signer to secure their credentials
Identity Issuer
Trusts issuer to identify signers
Validator
Trusts assertions are made by the signer
Consumer
Trusts validator to check validity and correctly identify signers

Fig. 4 diagram demonstrating the workings of C2PA

C2PA is in part a data standard for recording provenance information about a media expression. Next to the goal of who authenticated a media expression – similar to PoP, C2PA proposes an ecosystem to describe who, how, when and where the expression is created, edited and altered.

C2PA adopts multiple certification authorities for verification of eSignatures, using trust lists; these can differ per application that adopts the infrastructure. At least some of these authorities would need physical world verification for them to be trustworthy (i.e. Netherlands Union of Journalists).

C2PA is a specification of metadata that needs to reside within the media expression. Meaning that it heavily relies on good faith actors that do not remove metadata from the expression, e.g. to minimise size of the expression, or when moving the expression to a different file format.

It does, however, allow for 'soft binding' of media identifiers to their expressions.[20] These are perceptual hashes or watermarking that can be reproduced, even if the file format of the expression is changed and the provenance metadata is stripped. With the reproduced identifier, the provenance metadata of the expression can subsequently be recovered.

Governance – C2PA is backed by a large consortium of about 33 members. Its steering committee consists of larger IT-organisations specialised: Adobe, Arm, BBC, Intel, Microsoft,

[19] See https://c2pa.org/specifications/specifications/1.0/guidance/Guidance.html
[20] See C2PA Implementation Guidance

Sony, Truepic, and Twitter. The consortium will develop the technical specification for members of the consortium to implement in various projects.[21]

Adoption – The technical specification has been adopted in at least Microsoft's Project Origin Alliance and the Content Authenticity Initiative (CAI). Both are still in their proof of concept phase.

Implementability and adaptability – The C2PA specification can be seen as complementary to the PoP project. The PoP signature can be added as part of the signatures that C2PA already accepts.

Durability – C2PA seems a durable initiative, given the governance and widespread support of the project from larger organisations.

Interoperability – PoP can be made interoperable with C2PA for certain use cases, however the trade off is that interoperability runs the risk of exposing PoP to the weaknesses of C2PA.

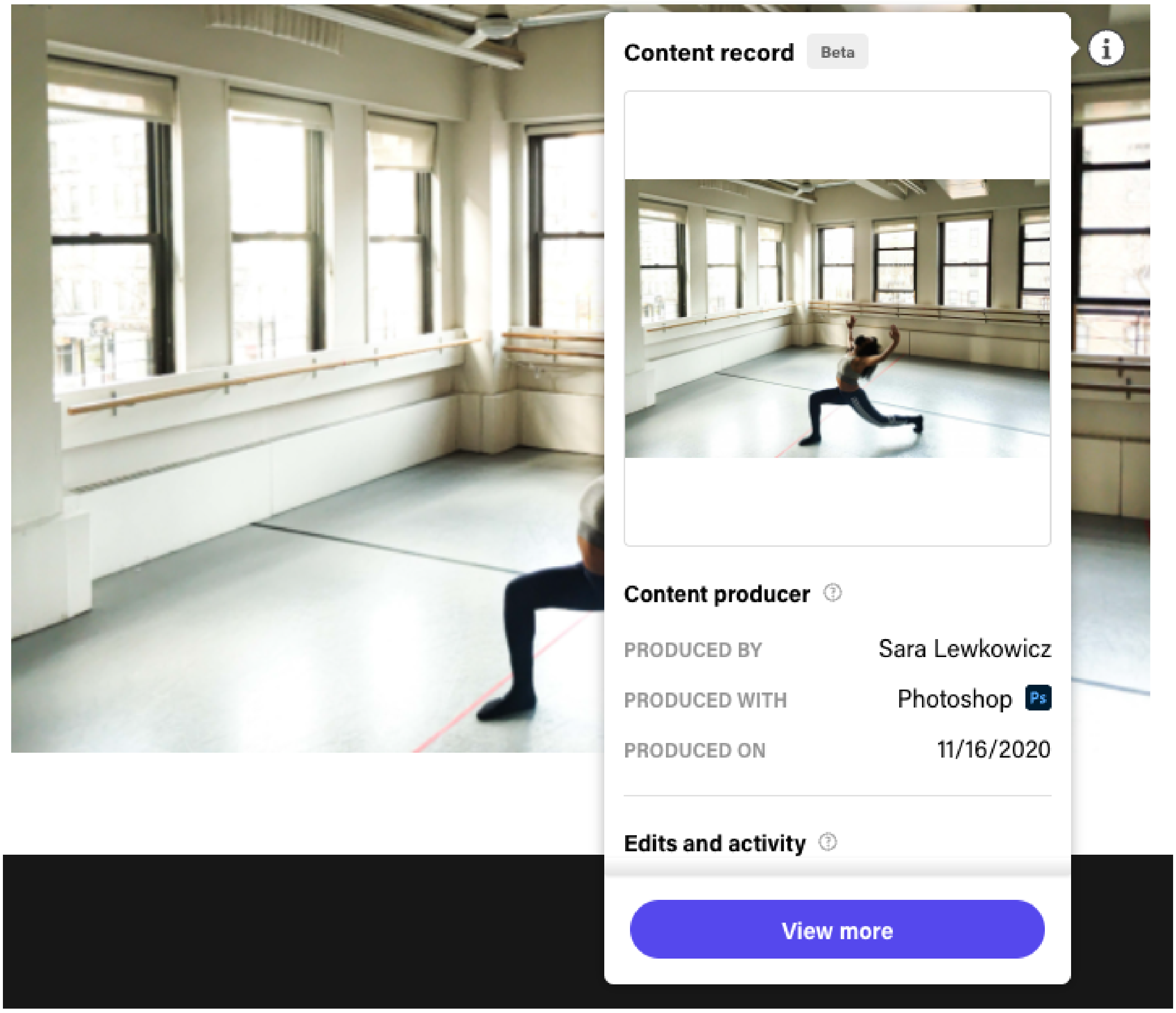
Implementations of C2PA

Content Authenticity Initiative

Content Authenticity Initiative[22] (CAI) adopts many features of C2PA and adds documentation and end-to-end open technical standards for creators, editors, publishers, media platforms, and consumers. The initiative has over 200 members[23] and publishes open source tools to work with media that implement the C2PA standards. These include a JS interface library, a command line utility to explore authenticity data and a full SDK to implement the creation of C2PA compatible data.

Users of CAI data store that data in the media expression itself, keeping the weakness of C2PA, but CAI wants to offer cloud services to store the CAI data outside of the media expression. This of course creates a single point of failure, a possible trust issue and a potential privacy leak with the signatures attached to the data. It would be possible for the hoster to keep track of who has a copy of which image and who are the creators of an image. The initiative developed a proof of concept site that demonstrates the working of their potential tool.[24]

[21] See Membership - C2PA
[22] See Content Authenticity Initiative
[23] See Members — Content Authenticity Initiative
[24] See Verify.contentauthenticity.org



Content record

Content producer

PRODUCED BY Sara Lewkowicz

PRODUCED WITH Photoshop

PRODUCED ON 11/16/2020

Edits and activity

Fig <X> Screenshot showing the working of CAI

Project Origin

Mircosoft's Project Origin adopts a 'Authentication of Media via Provenance' or AMP[25] initiative that is likely to implement the C2PA specification as part of their provenance manifest. Additionally, project Origin describes a method for authenticating streaming media, by creating cryptographically hashing small sections of the stream. The difference between the CAI and Project Origin in the place where the provenance data is stored. Microsoft proposed to use a custom distributed ledger, the Confidential Consortium Framework, to store provenance information.[26] This is a ledger where you can have decentralised trust but control accessibility of the ledger. I.e. when you want to distribute trust within an organisation or a group of organisations.

Finally, AMP introduces fragile watermarking technology to the AMP. Fragile watermarking is a technique that adds watermarks to a file that detect even the slightest change of the file. In a sense they

[25] See AMP: Authentication of Media via Provenance (arXiv:2001.07886 [cs.MM])
[26] See GitHub - microsoft/CCF: Confidential Consortium Framework

are similar to cryptographic hashes, whereas the hash is stored attached to the file, the watermark is part of the file.

SWOT

Strengths	Weaknesses
● Large network support ● Multiple technology implementation ● Open Source implementations ● Open specification	● Adoption by walled gardens cannot be assumed. ● Implementations are not yet in production,
Opportunities	**Threats**
● Integration of additional technology and extensions (e.g. watermarking, perceptual hash)	● Competing standards

Sovrin

Sovrin is very similar to IRMA. In contrast to IRMA, Sovrin adopts "public blockchains [that] can provide decentralized registration and discovery of the public keys needed to verify digital signatures."[27] IRMA on the other hand relies on a centralised PKI and they determine who can issue certificates. Whereas that is open in Sovrin.[28]

The main comparison here is the manner and scope of the centralisation in the two implementations and the data it offers to make available via certificates. IRMA is more centralised and determines which certificates and information (schemes) the service can issue. Sorvin does not have this and thus has a risk of a multitude of competing certifications with similar goals/ information that are not compatible with each other.

Governance – Sovrin is more decentralised and has more international support than IRMA has.

Adoption – Sovrin has broad stewardship across the world with almost 50 stewards.

Implementability and adaptability – Using IRMA and Sovrin together creates some issues on determining who the issuer of the certificate is. However, a system can be developed that allows certificates from both ecosystems to be used.

Durability – Sovrin is a more decentralised solution which does not rely on a single organisation to host and maintain a PKI.

Strengths	Weaknesses
● Distributed PKI ● Large community	● No strict scheme management.

[27] See Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust
[28] Nauta, Jelle & Joosten, Rieks. (2019). Self-Sovereign Identity: A Comparison of IRMA and Sovrin.

Opportunities	Threats
● PoP to become one of the accepted schema's	● Competing products that are more focussed on type of intervention.

Hash-to-DLT

There are several initiatives that aim to improve the trustworthiness of media expressions, next to Project Origin, that are using some sort of blockchain/distributed ledger technology and hashes of media expressions. Some examples are introduced below:

1. ARCHANGEL
2. Wordproof
3. Proof of existence

ARCHANGEL

ARCHANGEL is an international study to co-create and evaluate a Distributed Ledger Technology (DLT) service that stores (cryptographic) hashes of media expressions that are part of digital public archives. These hashes are used to ensure the integrity of the media expression.[29]

The proof of concept ledger is publicly accessible to allow the general public to verify the hash of the expression against the registered hash upon deposition of the archival object. The ledger is shared amongst multiple public institutions to ensure the integrity of the ledger itself. "In doing so, ARCHANGEL enables a shift from an institutional underscoring of trust, to a technological underscoring of trust."[30] [31]

Governance – Surrey University, Surrey Business School, and a consortium of stakeholders including The National Archives and the Open Data Institute (ODI).

Adoption – No implementation after the research project

Implementability and adaptability – No code was published, no service remained online after the project.

Durability – Conceptually durable, due to the use of public sector partners.

Interoperability – Conceptually interoperable, concepts can be adopted for similar initiatives.

This overview is followed by a summary of the strengths, weaknesses, threats and opportunities of the initiative in relation to the needs of PoP.

[29] https://www.archangel.ac.uk/about/

[30] See ARCHANGEL: Trusted Archives of Digital Public Documents (arXiv:1804.08342 [cs.DL])

[31] See ARCHANGEL: Tamper-proofing Video Archives using Temporal Content Hashes on the Blockchain (arXiv:1904.12059 [cs.CV])

Strengths	Weaknesses
- Public sector collaboration can mean longer term support - Public verification of works that are not publicly available	- Hash does not survive medium shifting, even though they did research into this. - Only as good as volunteer contributions by archives
Opportunities	**Threats**
- Scalability	- Proof of Concept, no follow up found

Wordproof

Wordproof is a timestamping service.[32] It allows its users to store a hash of a media expression on several public blockchains. This allows the publisher of that media expression to prove that their content has been (un)altered since the registration of the hash of the expression on the blockchain. This commits the publisher to openly communicating that and what they change to a media expression. E.g. that a news article has been updated since its first publication. Wordproof has additional services like storing versions of publications, checking whether the material appears on other platforms (i.e. possible copyright infringement).

Governance – Start-up that mainly seems to be working on grants and subsidies.

Adoption – Mainly adoption in the Dutch publishing sector.

Implementability and adaptability – The service can simply be implemented by publishing platforms, but do not serve most of the goals of PoP

Durability – The checks and hashes of a media expression are stored at one location, tying the durability with the existence of the organisation.

Interoperability – Wordproof offers complementary services that allow you to check whether the media expression is reused on other platforms.

This overview is followed by a summary of the strengths, weaknesses, threats and opportunities of the initiative in relation to the needs of PoP.

[32] see wordproof.com

Strengths	Weaknesses
● Authenticity is coupled to a commercial service that benefits publisher	● Is geared against sharing of publications ● Hashes are not stored publicly ● Hashes stored centrally stored
Opportunities	Threats
● Adopt Proof of Provenance to further commercial proposition	● Lack of interest from publishers to use the services

Proof of existence

Proof of Existence[33] is a service that allows you to write a cryptographic hash of your media expression directly in the BitCoin blockchain. This allows you to document ownership, timestamp (versions) of your expression, and check a received or future expression for integrity. It has no public-facing integration with other platforms.

Governance – the project is maintained by a small organisation, its code is open source and can easily be reproduced for similar purposes.

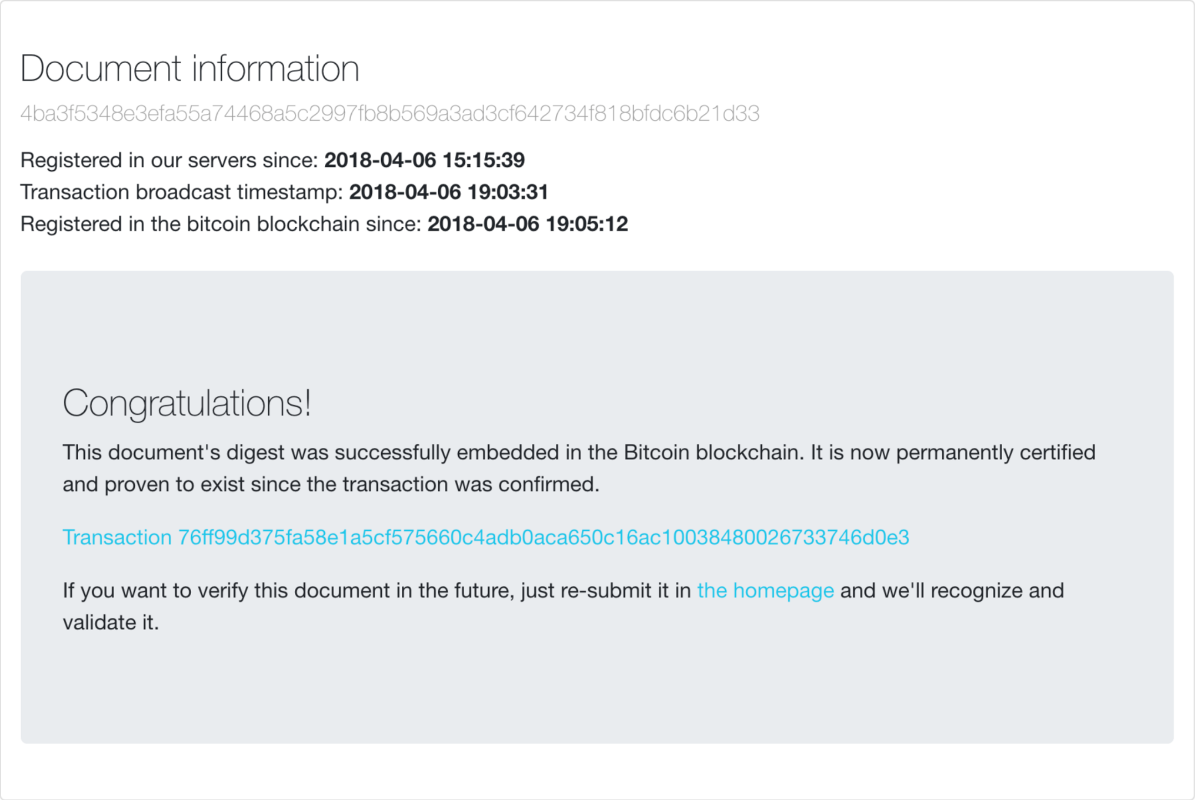
Adoption – Adoption can be checked by counting the number of “444f4350524f4f46” in the OP_RETURN code in Bitcoin. This requires a download of the entire bitcoin blockchain. Currently their users register one per every couple of days. This type of adoption is not relevant for the goals of PoP.

Implementability and adaptability – The technology of Proof of Existence can easily be implemented or reproduced.

Durability – Durability of Proof of Existence depends on the continued existence of the cryptocurrency that is used to register the identifiers of the file.

Interoperability – Storing distinct identifiers on a public blockchain as a concept can benefit some objectives of the project, if external verification of the PoP needs to be done in a manner that distributes authority.

[33] See proofofexistence.com



Document information

4ba3f5348e3efa55a74468a5c2997fb8b569a3ad3cf642734f818bfdc6b21d33

Registered in our servers since: **2018-04-06 15:15:39**
Transaction broadcast timestamp: **2018-04-06 19:03:31**
Registered in the bitcoin blockchain since: **2018-04-06 19:05:12**

Congratulations!

This document's digest was successfully embedded in the Bitcoin blockchain. It is now permanently certified and proven to exist since the transaction was confirmed.

Transaction 76ff99d375fa58e1a5cf575660c4adb0aca650c16ac10038480026733746d0e3

If you want to verify this document in the future, just re-submit it in the homepage and we'll recognize and validate it.

Fig. 5 Screenshot of a Proof of Existence registration.

Strengths	Weaknesses
● Based on BitCoin, blockchain unlikely to corrupt	● Based on BitCoin, transaction costs and duration varies
Opportunities	**Threats**
● Additional user interfaces	● Many competing possibilities

Traditional digital signing services

Digital signature technology has been around for over 40 years and has been regulated by law since the late 1990s, early 2000s. The past 30 years have seen multiple initiatives that adopt digital signatures like PandaDoc, DocuSign and to some extent PKI Overheid.

These services facilitate and standardise the process of signing an expression. They are a source of authority by issuing public-private key pairs (a digital certificate) that allows the user to sign an expression. A Public Key Infrastructure allows the other party to verify the certificate and verify that the expression was signed by the right party, and not mutated in transit.

Traditional signing services are a foundation upon which additional services like authentication and digital identity can be built. Services like Signicat.com and also IRMA already adopted some aspects of these technologies.

Governance – These projects usually have a stable governance structure, that in case of commercial parties that issue digital certificates.

Adoption – Adoption depends on the party that provides the certificate, but the technology is ubiquitous.

Implementability and adaptability – Public Key Infrastructures are stable and mature technologies that can be implemented.

Durability – Durability of these types of services rely on the single source of failure, the entity that issues the certificates. Similar to SIDN to the IRMA project.

Interoperability – Not relevant.

Strengths	Weaknesses
● Tried and tested technology	● Not tied to attributes
Opportunities	**Threats**
● Offer PoP as an additional infrastructure for other signing authorities.	● Private party controls the infrastructure

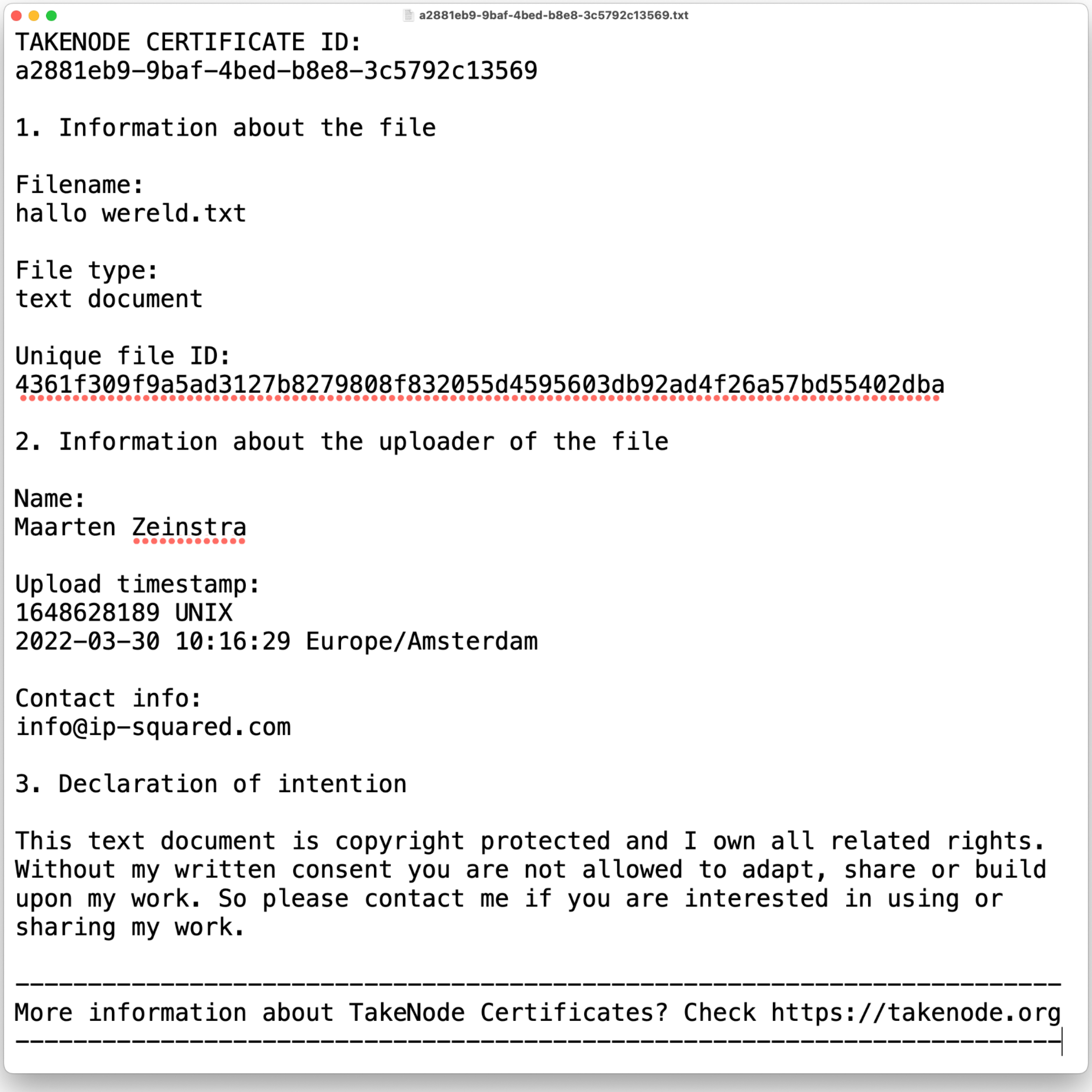
Other noteworthy

TakeNode.org

The Dutch initiative TakeNode.org[34] is most similar to PoP. It offers content creators a tool to register their 'Terms of Use'. Relevant information about the file, creator and intentions are packaged in a unique TakeNode Certificate. Sharing the TakeNode certificate as part of the content offers digital platforms and their users an easy-to understand and human readable mandate.

The certificate is also stored in a central server, and thus transparent. Anyone with either the certificate ID or the SHA-256 hash of the file that was registered can find all the registration information of the document.

[34] Note: the author of this document was involved in TakeNode.org.



```
TAKENODE CERTIFICATE ID:
a2881eb9-9baf-4bed-b8e8-3c5792c13569

1. Information about the file

Filename:
hallo wereld.txt

File type:
text document

Unique file ID:
4361f309f9a5ad3127b8279808f832055d4595603db92ad4f26a57bd55402dba

2. Information about the uploader of the file

Name:
Maarten Zeinstra

Upload timestamp:
1648628189 UNIX
2022-03-30 10:16:29 Europe/Amsterdam

Contact info:
info@ip-squared.com

3. Declaration of intention

This text document is copyright protected and I own all related rights.
Without my written consent you are not allowed to adapt, share or build
upon my work. So please contact me if you are interested in using or
sharing my work.

------------------------------------------------------------------------
More information about TakeNode Certificates? Check https://takenode.org
------------------------------------------------------------------------
```

Fig. 6 Screenshot of a TakeNode certificate

Governance – TakeNode is governed by the Open Netherlands Foundation, it is open source and allows you to connect with the digital identity services IRMA.

Adoption – TakeNode.org is a workable proof of concept project. Its adoption is not large.

Implementability and adaptability – Implementation and adaptability of the technology is rather straightforward.

Durability – The project has a single point of failure, the maintenance and durability of the central server that stores the certificates of the registration of documents. When that is no longer funded, or supported, all certificates can no longer be proved.

Interoperability – TakeNode has a different, but possibly complementary purpose to PoP. It is a Proof of Ownership and can store given permission for an expression. PoP does not describe any reuse permissions.

Strengths	Weaknesses
● Open Source, it can be adopted and built upon.	● Centralised, governed by a single NGO
Opportunities	**Threats**
● Foundational technology that can be repurposes, reused for other goals	● Low adoption leads to less recognisable, which in turn can lead to no practical application

MOVA and ISCC

Monetising Open Video Assets (mova) is a project to support filmmakers, archives and video distributors in benefiting from the new technology and revenue source of Web Monetization."[35] They try to achieve this goal by developing MOVA, "a distributed registry of rights and payment data connected to video files using another new technology, the International Standard Content Code (ISCC) and Holochain."[36]

ISCC tries to develop a "universal identifier for digital content"[37] that encodes text, images, audio, video or other content. The idea of the foundation, similar to C2PA, is to standardise in order to reach a larger audience. They however don't use the route of a large consortium, but of ISO standardisation[38]

According to its website ISCC is[39]:

1. a universal identifier for all kinds of digital content (text, image, audio, video)
2. a lightweight and similarity-preserving fingerprint
3. designed for cross-sector applicability (journalism, books, music, film, etc.)
4. designed to identify content in decentralised and networked environments
5. and most importantly it is free, open-source and transparent

Governance – Governance of the standard is handed over to Working Groups of the ISO organisation. This does not mean that they will be maintained in the following years

Adoption – There seems to be limited adoption of the standard (e.g. at CLink.ID).

Implementability and adaptability – There are various implementations[40] of the standard.

[35] See Monetising Open Video Assets
[36] idem.
[37] See About the ISCC - ISCC Foundation
[38] It is actively developed at ISO under ISO/AWI 24138.
[39] See ISCC Code
[40] See Resources - ISCC - Content Codes

Durability – The project is currently actively being developed[41] mostly by a single developer, which limits the project's durability.

Interoperability – The identifier that is developed in this standard can be adopted in the PoP project as additional metadata.

Strengths	Weaknesses
● Working towards ISO standardisation which might increase possibility for adoption by public institutions	● Active, but limited development ● ISO standard does not equal adoption of project ● Not many implementations
Opportunities	Threats
● Collaboration with other initiatives that work on similar initiatives	● No adoption of the standard.

Rewrited.news

Rewrited.news is a tool that allows you to check if a news-source has been rewritten since it has been published. The project was a proof of concept and has since closed down. The Minimal Viable Product is available as an open source tool.[42] It stored hashes in a blockchain of media content so other people can check whether an online source has been changed since the ingest of the expression in the ledger.

Governance – Proof of concept, no current ongoing governance.

Adoption – No adoption at the moment.

Implementability and adaptability – Open source tool that allows people to register a hash of a web expression on a blockchain.

Durability – Durability depends on the source code's dependencies and availability of the chosen blockchain.

Interoperability – The tool can be adopted to serve PoP by storing metadata (signatures) in a blockchain

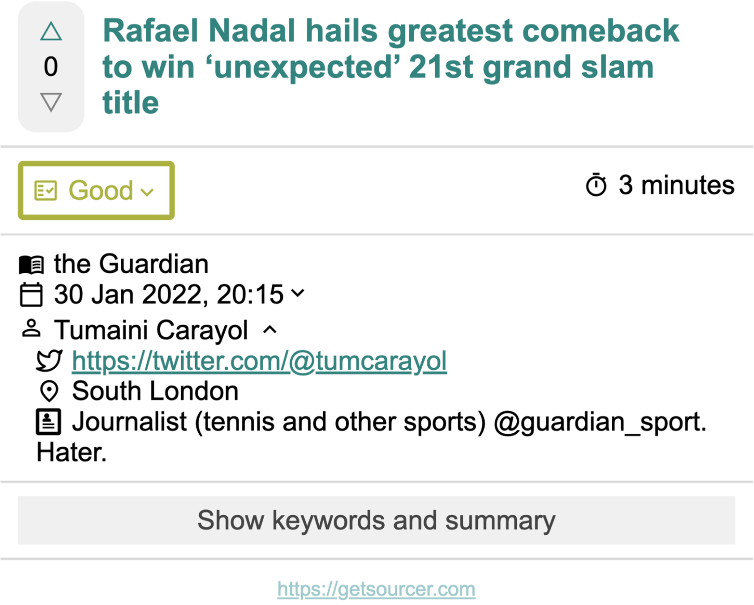
[41] See github.com/iscc/iscc-cli/network

[42] See GitHub - LedgerProject/BackMe.org_scraper-back-end

Strengths	Weaknesses
- Open source tools - MVP	- No funds or business model
Opportunities	**Threats**
- Collaboration with other initiatives that work on similar initiatives	- No adoption

Sourcer

Sourcer is a Dutch initiative that compares media expressions by automatically applying a CRAAP test[43] to them. This is done via a browser extension that shows the CRAAP score as well as scraped metadata from a site. A user can score an article and find similar articles based on key sentences in the article. A perceived weakness is that the CRAAP test is not an objective test, e.g. rating the news sources by the developers can lead to biassed algorithms.



△ 0 ▽

Rafael Nadal hails greatest comeback to win ‘unexpected’ 21st grand slam title

Good

3 minutes

the Guardian
30 Jan 2022, 20:15
Tumaini Carayol
https://twitter.com/@tumcarayol
South London
Journalist (tennis and other sports) @guardian_sport. Hater.

Show keywords and summary

https://getsourcer.com

Fig. 7 Screenshot of Sources, from GetSourcer.com

Governance – Private company, very much in a start-up fase

Adoption – Adoption via browser extension, no numbers known

Implementability and adaptability – Closed source, but open standard.

[43] See CRAAP Test - Evaluating Sources - Library Guides at University of the West of Scotland

Durability – Centralised service that relies on the company to make the determination of the CRAAP test.

Interoperability – The tool can provide additional inspiration for PoP, if PoP gets out of its proof of concept phase Sourcer might also scan for PoP manifests.

Strengths	Weaknesses
● Open standard (CRAAP) ● MVP	● Business model relies on trust of the subject CRAAP implementation ● Biassed algorithms
Opportunities	Threats
● Niche market for researchers and news investigators	● No adoption

Addendum 2 – GAP analysis

The consortium has thus far (May 2022) reached many of its objectives. During the development and discussion some new insights lead to additional needs, especially from the interviews. The gaps, these objectives that have not been achieved (yet), are described below. This GAP analysis is developed given the technologies used in PoP, the needs of the project's partners and the described needs of the project to its funders. The table holds an overview of the objectives of the projects from the project partners and project plan. It describes the status of these identified objectives at the time of writing. Finally it describes the identified gaps between these objectives and outcomes.

The objective is defined according to the needs of the project by project partners, described previously in this document and abstracted from the project plan. The two lists below capture these objectives in a compact manner

Objectives up until #10 are the needs, wishes and requirements identified by project partners in discussions, Objectives from #10 onwards are needs or requirements identified in the project plan

#	Description of objective	Status
1	Sign all media expressions (text, media) of an HTML document.	Achieved, except for audio and video
2	Incorporate signing workflow in content management systems.	Not yet achieved
3	Allow signing from third parties	Not yet achieved
4	Trace the original publication location of a signed expression	Not yet achieved
5	Validate signature of textual paragraphs	Achieved
6	Present validation of signature of textual paragraph	Achieved
7	Present signed textual paragraphs without context (i.e. edits made by css, or javascript).	Achieved

#	Description of objective	Status
8	Store verification of a PoP in a static way for archiving purposes.	Not yet achieved
9	Copy a quote from a signed expression and keep the signature	Partly achieved, depends on granularity of signature
10	Distinguishing between signed and unsigned material on pages that contain both.	Not yet achieved
11	Attach a certificate of authenticity to any form of content that is being distributed by a publisher.	Achieved, except for audio and video
12	Verify signed media expressions.	Achieved
13	Certification of authenticity should lead to higher ranking in distribution platforms.	Not yet achieved
14	Certification uses attributes of trusted institutions.	Not yet achieved
15	The implemented technology should be able to reduce the need to expose the identity of the signer	Achieved
16	The signing process should be intuitive	Achieved
17	Verification of the certificate should be intuitive	Not yet achieved
18	Content with a certificate should be able to distinguish from non-signed content	Achieved

Notes on objectives

2. Incorporate signing workflow in content management systems. Incorporating a signing workflow is foreseen in the Magnolia CMS, but that work has not been started during the writing of this document.

3. Allow signing from third parties. This additional objective might not be in scope of the project, as it requires additional research and development that is not foreseen.

13. Certification of authenticity should lead to higher ranking in distribution platforms. This is not in scope of the project, as this project is a proof of concept and it cannot be expected to be integrated in distribution platforms to such an extent.

14. Certification uses attributes of trusted institutions. This is in scope of the project; this is more a matter of configuration of the IRMA attributes. The choice of an attribute that is part of a trusted organisation is up to the party that signs the expression.

17. Verification of the certificate should be intuitive. The status of this objective is difficult to ascertain, as it is partly subjective, partly reliant on the technology and its dependencies, and partly defined by the adoption. It is the opinion of the author that this objective has not been reached in any of the investigated projects.