Aspekte der Medienherkunft, Authentizität und Rechte
JPEG Trust und Tokenisierung

Dipl.-Ing. Dipl.-Kfm. Philippe Rixhon

Webinar der Arbeitsgruppen Cloud Governance Workplace und
Informations- und Cybersicherheit der DVS – 29. Mai 2024

Examples of media manipulation

1860

Abraham Lincoln

Lincoln’s head was added on top of southern politician John Calhoun’s portrait.

1930

Joseph Stalin

Leaders remove people (from the images) whom they no longer wanted to associated.

1939

Canadian PM

William Lyon Mackenzie King removes King George VI from a photo with Queen Elizabeth to portray himself more powerful.

1945

Soviet Soldiers

Russian magazine removes the watches from soldiers’ wrists to ensure that their readers don’t think the soldiers were looting.

1989

Oprah Winfrey

TV guide edited the cover image where they used Oprah’s head on the body of Ann-Margaret.

1994

OJ Simpson

Time magazine edited OJ Simpson’s image after his arrest and made it darker and more sinister. Actual one was displayed in News Week.

2008

Iranian Missiles

The doctored image was released by the Iranian Government to show successful launch of four missiles when only three were successful.

2021

Deepfake Tom Cruise

Near realistic deepfake of Tom Cruise indicates the potential of AI based media manipulation. Image courtesy: Belgium VFX specialist Chris Ume.

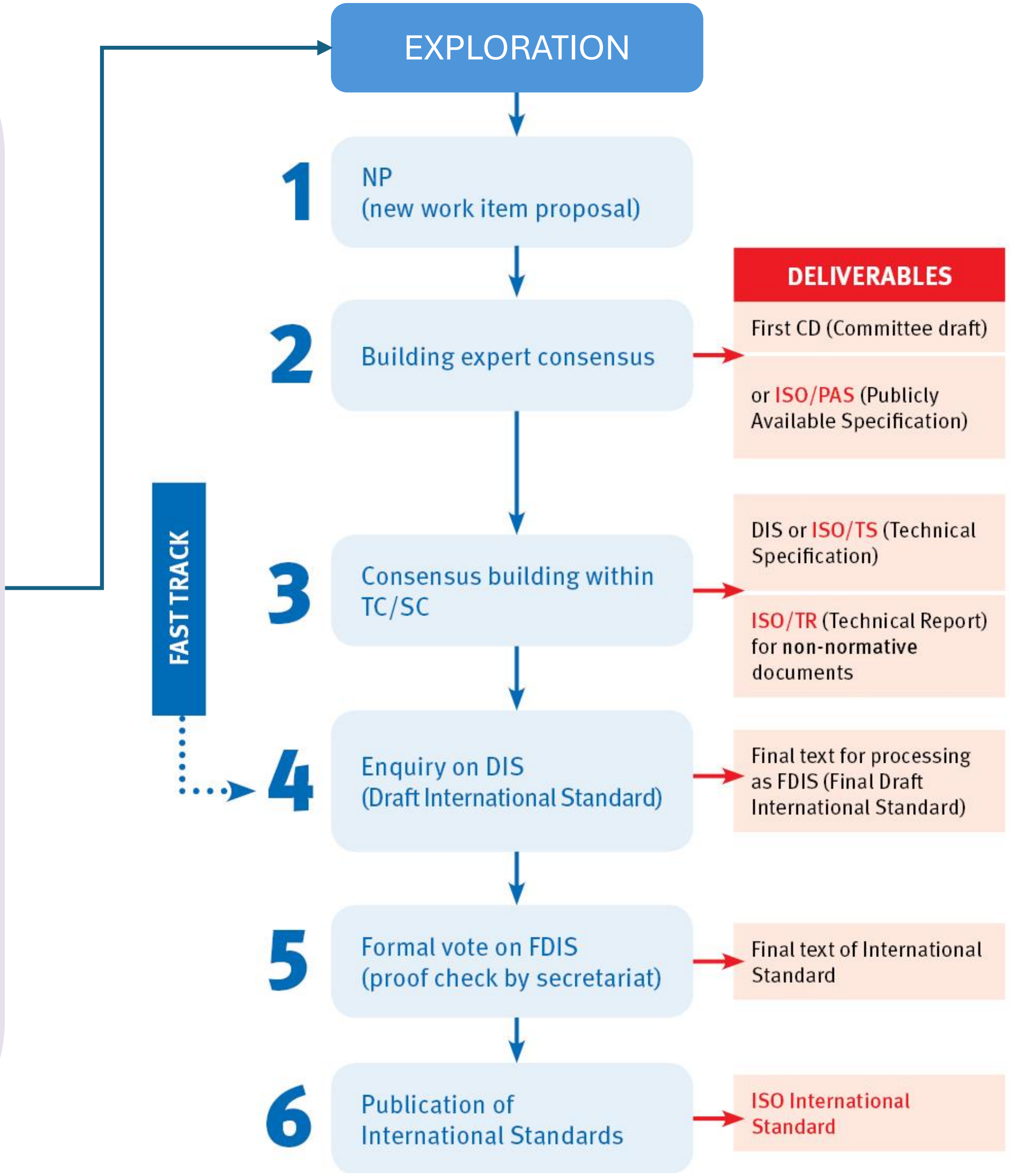
Impacts of media manipulation

- Political
- Social
- Economic

ISO standardisation process

JPEG Fake Media exploration

- Initiated in October 2020
- 5 workshops to engage with industry and stakeholders
- Identification of use cases and requirements
- Call for Proposals
- Completed in January 2023



EXPLORATION

FAST TRACK

1 NP (new work item proposal)

2 Building expert consensus

3 Consensus building within TC/SC

4 Enquiry on DIS (Draft International Standard)

5 Formal vote on FDIS (proof check by secretariat)

6 Publication of International Standards

DELIVERABLES

First CD (Committee draft)

or ISO/PAS (Publicly Available Specification)

DIS or ISO/TS (Technical Specification)

ISO/TR (Technical Report) for non-normative documents

Final text for processing as FDIS (Final Draft International Standard)

Final text of International Standard

ISO International Standard

Use cases

Misinformation and disinformation

- Media usage and breaking news
- Deepfake detection
- Content authenticity checking
- Content usage tracing
- Fraud in academic research
- Photographic framing

Forgery/media forensics

- Insurance fraud
- Mileage reporting photo
- Photo for cost charge
- Evidence of trial
- Media sharing on social media
- Credibility of AI training image data sets

Media creation

- Movie special effects
- Media transcoding
- Chroma keying or silhouette extraction

Media modification

- Image colorization and restoration
- Photo editing

Requirements

- Media creation and modification descriptions
- Metadata embedding and referencing
- Authenticity, integrity, and trust model

Responses to the Call for Proposals on JPEG Fake Media

Adobe / Coalition for Content Provenance and Authenticity

- C2PA Specifications

Huawei

- Provenance and Right Management for Digital Contents in JPEG Fake Media

Sony Group Corporation

- Methods to keep track provenance of media asset and signing data

Vrije Universiteit Brussel / Interuniversity Microelectronics Centre (imec)

- Media revision history tracking via asset decomposition and serialization

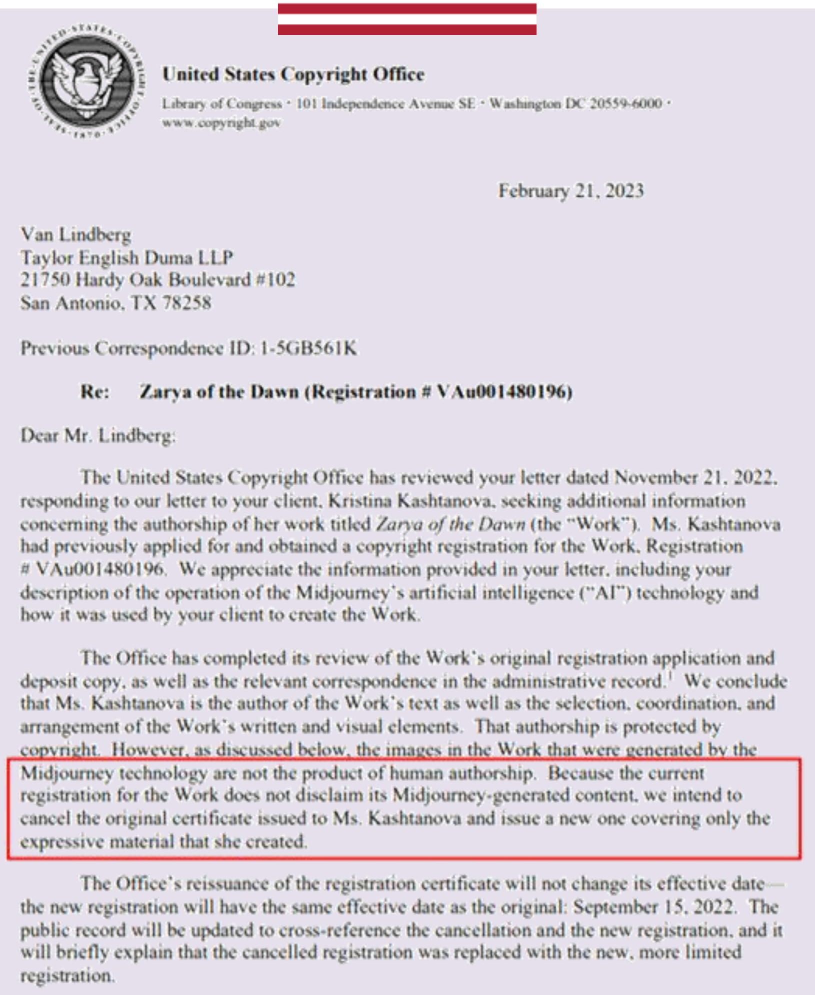
Universitat Politècnica de Catalunya

- Multimedia Information Protection And Management System (MIPAMS) Provenance module

Newcastle University

- TRusted mediA dIstribuTion (TRAIT)

The AI event and legislative responses



United States Copyright Office

Library of Congress · 101 Independence Avenue SE · Washington DC 20559-6000 ·
www.copyright.gov

February 21, 2023

Van Lindberg
Taylor English Duma LLP
21750 Hardy Oak Boulevard #102
San Antonio, TX 78258

Previous Correspondence ID: 1-5GB561K

Re: Zarya of the Dawn (Registration # VAu001480196)

Dear Mr. Lindberg:

The United States Copyright Office has reviewed your letter dated November 21, 2022, responding to our letter to your client, Kristina Kashtanova, seeking additional information concerning the authorship of her work titled *Zarya of the Dawn* (the "Work"). Ms. Kashtanova had previously applied for and obtained a copyright registration for the Work, Registration # VAu001480196. We appreciate the information provided in your letter, including your description of the operation of the Midjourney's artificial intelligence ("AI") technology and how it was used by your client to create the Work.

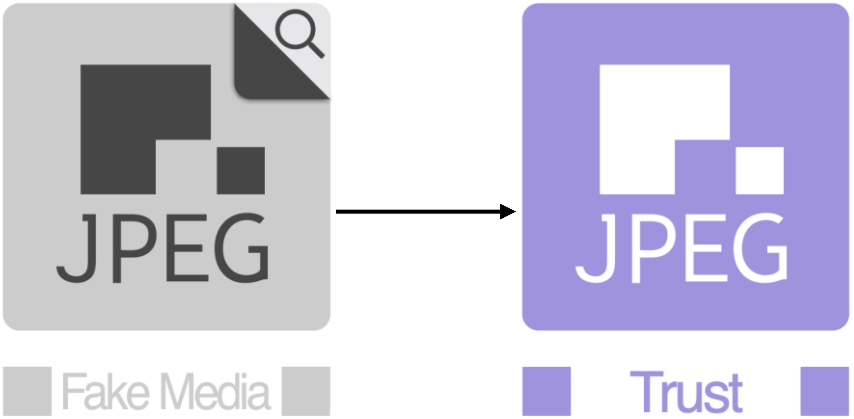
The Office has completed its review of the Work's original registration application and deposit copy, as well as the relevant correspondence in the administrative record.[1] We conclude that Ms. Kashtanova is the author of the Work's text as well as the selection, coordination, and arrangement of the Work's written and visual elements. That authorship is protected by copyright. However, as discussed below, the images in the Work that were generated by the Midjourney technology are not the product of human authorship. Because the current registration for the Work does not disclaim its Midjourney-generated content, we intend to cancel the original certificate issued to Ms. Kashtanova and issue a new one covering only the expressive material that she created.

The Office's reissuance of the registration certificate will not change its effective date—the new registration will have the same effective date as the original: September 15, 2022. The public record will be updated to cross-reference the cancellation and the new registration, and it will briefly explain that the cancelled registration was replaced with the new, more limited registration.

"Cyber Security Standards Practice Guide-Generative Artificial Intelligence Service Content Identification Method: 3.4 When images, audios, and videos generated by AI are output in files, extended fields must be added to the file metadata for identification. The extended field contains information such as the service provider name, content generation time, and content ID."

"Also, foundation models should have information obligations and prepare all necessary technical documentation for potential downstream providers to be able to comply with their obligations under this Regulation. **Generative foundation models should ensure transparency about the fact the content is generated by an AI system, not by humans.** These specific requirements and obligations do not amount to considering foundation models as high-risk AI systems but should guarantee that the objectives of this Regulation to ensure a high level of protection of fundamental rights, health and safety, environment, democracy and rule of law are achieved."

Establishment of JPEG Trust



“The scope of JPEG Trust is to provide a framework for establishing trust in media. This framework includes aspects of authenticity, provenance and integrity through secure and reliable annotation of the media assets throughout their life cycle.”

Establishing trust

Tackling disinformation

Reactive approach: detection of modifications and deep fakes

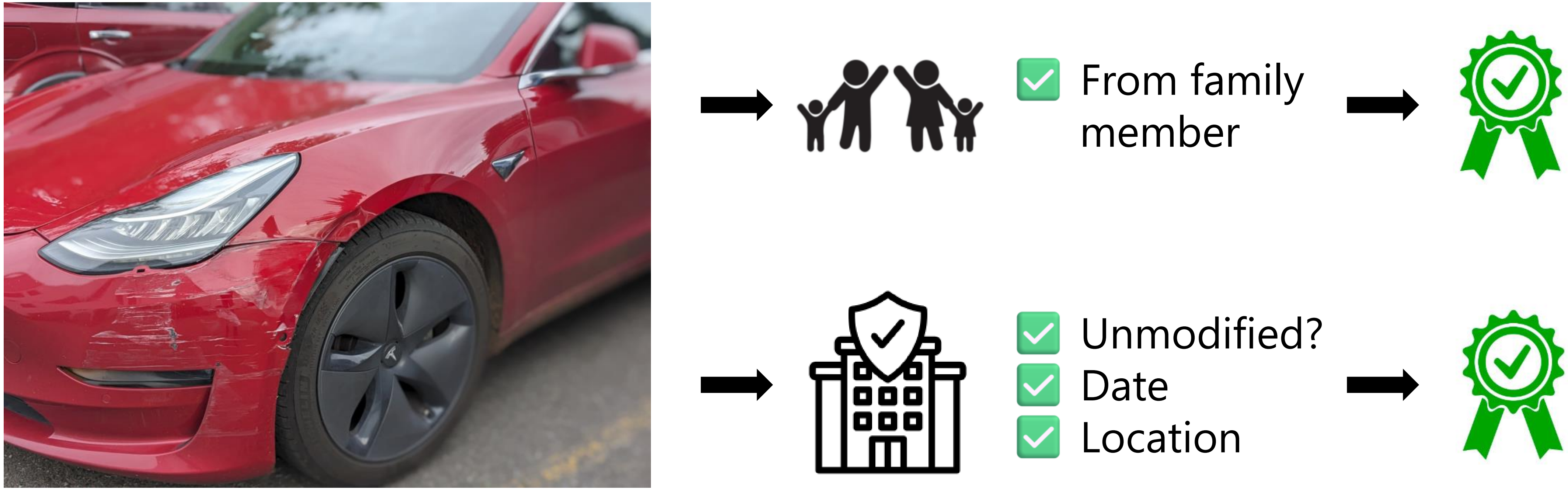
Proactive approach: signaling provenance

Collaborative approach: leveraging community feedback

Trustworthiness depends on the context

“JPEG Trust does **not explicitly define trustworthiness** but rather provides a framework and tools for **individuals**, **organisations**, and **governing institutions** to establish trust in accordance with the conditions **they specify**.”

Trust indicators



☑ From family member

☑ Unmodified?
☑ Date
☑ Location

JPEG Trust Part 1: Core Foundation

- Annotating provenance information
- Extracting and evaluating trust indicators
- Handling privacy and security concerns

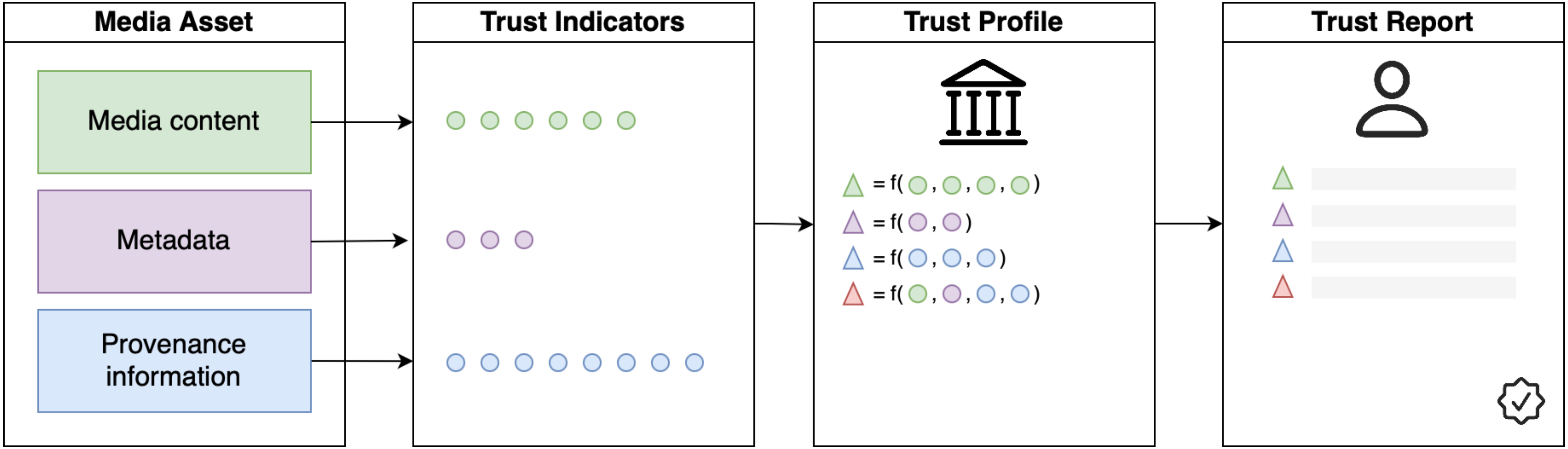
Annotating provenance information

- Embedding provenance annotations in media assets
- Securely link provenance annotations with associated media assets
- Model for expressing and embedding provenance annotations aligned with C2PA (Coalition for Content Provenance and Authenticity) specification
- Media assets with C2PA provenance annotations are compatible with the JPEG Trust framework
- Integrated in (upcoming) camera models of Leica, Sony and Nikon
- JPEG Trust adds additional provenance functionality such as signalling the extent of modifications

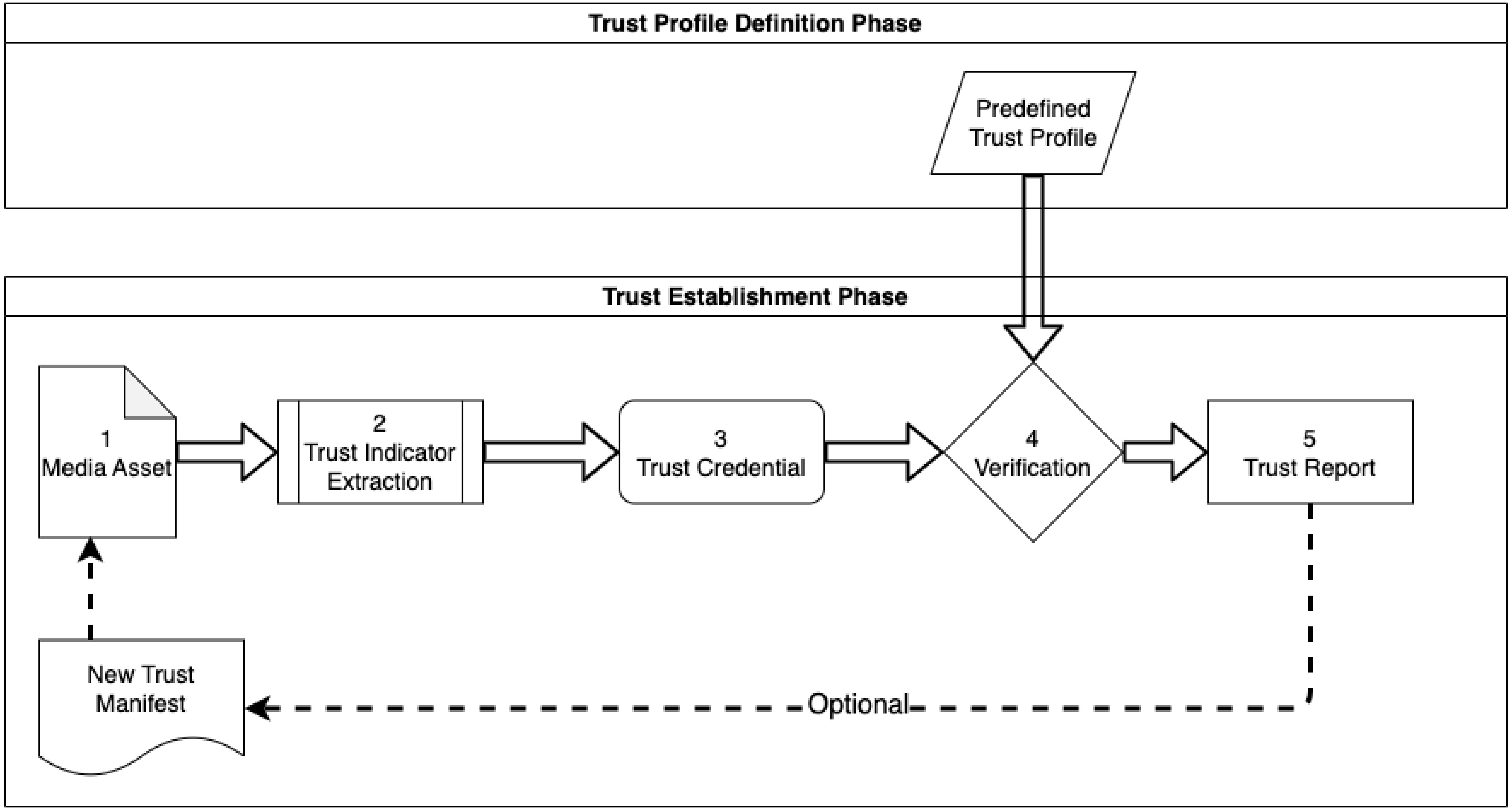
Extracting and evaluating trust indicators

- Trust Indicators can be extracted from:
  - media content
  - metadata, and
  - provenance information.
- Specific conditions for trustworthiness can be expressed in Trust Profiles.
- Trust profiles allow individuals, organizations, and governing institutions to evaluate relevant trust indicators according to the requirements for their specific usage scenarios.
- The resulting evaluation can be expressed in a Trust Report to make the information easily accessed and understood by the end user.

Extracting and evaluating trust indicators

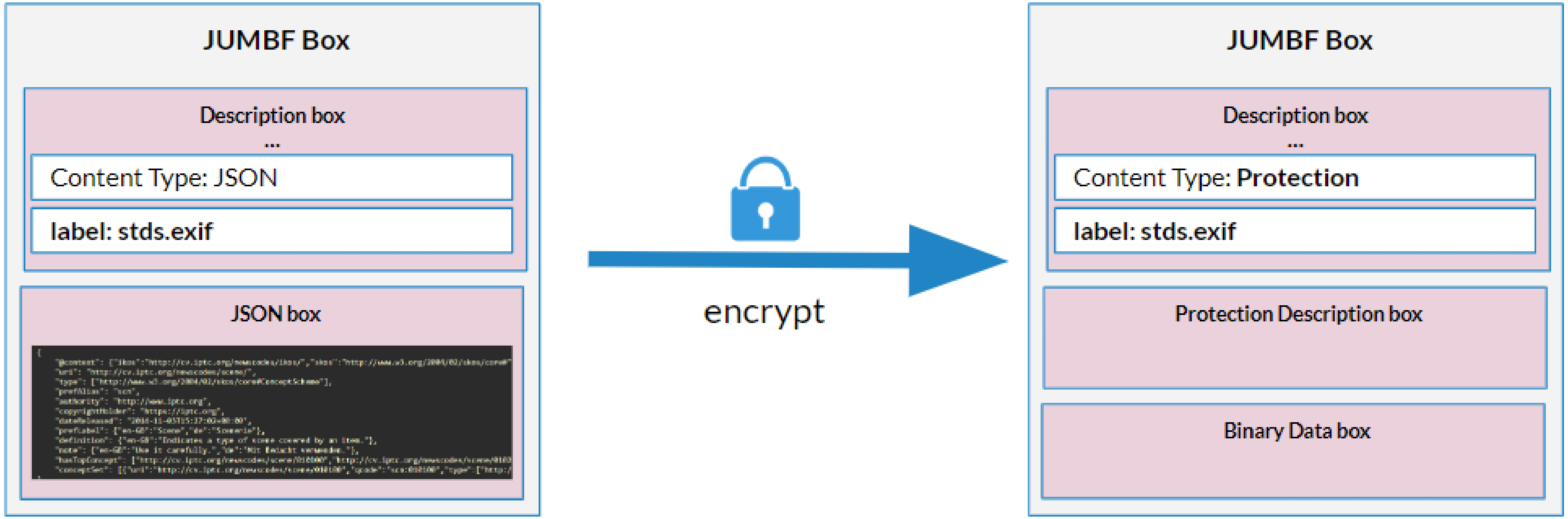


Extracting and evaluating trust indicators



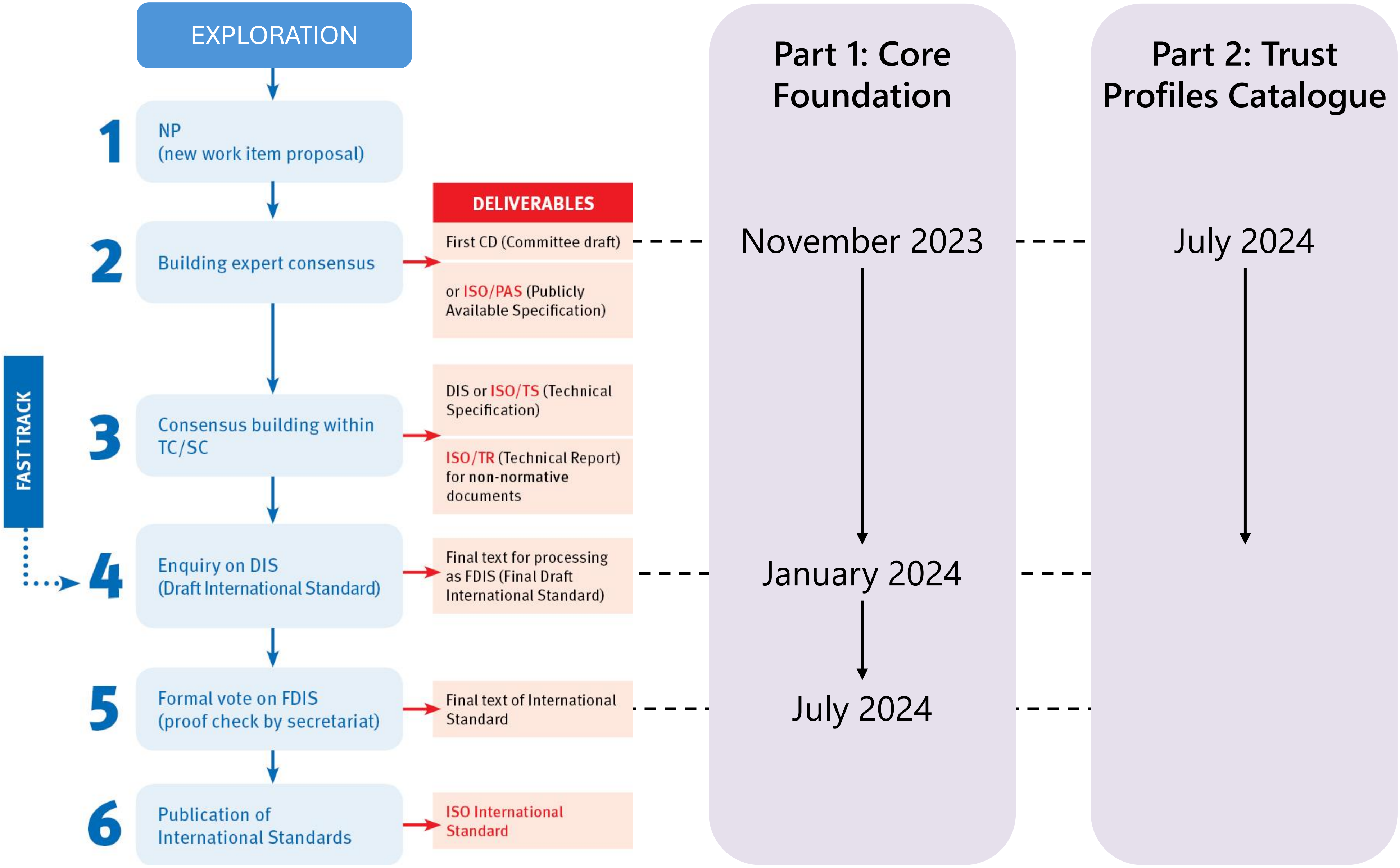
Handling privacy and security concerns

- Means to protect provenance annotations, including identification of actors
- Treated in line with JPEG Privacy and Security (ISO/IEC 19566-4)



```
{
    "@context": {"ikos":"http://cv.iptc.org/newscodes/ikos/","skos":"http://www.w3.org/2004/02/skos/core#"
    "uri": "http://cv.iptc.org/newscodes/scene/",
    "type": ["http://www.w3.org/2004/02/skos/core#ConceptScheme"],
    "prefAlias": "scn",
    "authority": "http://www.iptc.org",
    "copyrightHolder": "https://iptc.org",
    "dateReleased": "2014-11-03T15:37:00+00:00",
    "prefLabel": {"en-GB":"Scene","de":"Szenerie"},
    "definition": {"en-GB":"Indicates a type of scene covered by an item."},
    "note": {"en-GB":"Use it carefully.","de":"Mit Bedacht verwenden."},
    "hasTopConcept": ["http://cv.iptc.org/newscodes/scene/010100","http://cv.iptc.org/newscodes/scene/0103
    "conceptSet": [{"uri":"http://cv.iptc.org/newscodes/scene/010100","qcode":"scn:010100","type":["http:/
}
```

JPEG Trust timeline



EXPLORATION

1 NP (new work item proposal)

2 Building expert consensus

3 Consensus building within TC/SC

4 Enquiry on DIS (Draft International Standard)

5 Formal vote on FDIS (proof check by secretariat)

6 Publication of International Standards

FAST TRACK

DELIVERABLES

First CD (Committee draft)

or ISO/PAS (Publicly Available Specification)

DIS or ISO/TS (Technical Specification)

ISO/TR (Technical Report) for non-normative documents

Final text for processing as FDIS (Final Draft International Standard)

Final text of International Standard

ISO International Standard

Part 1: Core Foundation

November 2023

January 2024

July 2024

Part 2: Trust Profiles Catalogue

July 2024

The NFT event

© mundissima / Shutterstock.com

JPEG Trust

JPEG NFT exploration and synergies

Buyers need to assess the **trustworthiness** of the media assets.

NFTs provide an immutable record of a media transaction and hence also an **immutable record** in the **media provenance** chain.

Interoperable metadata:

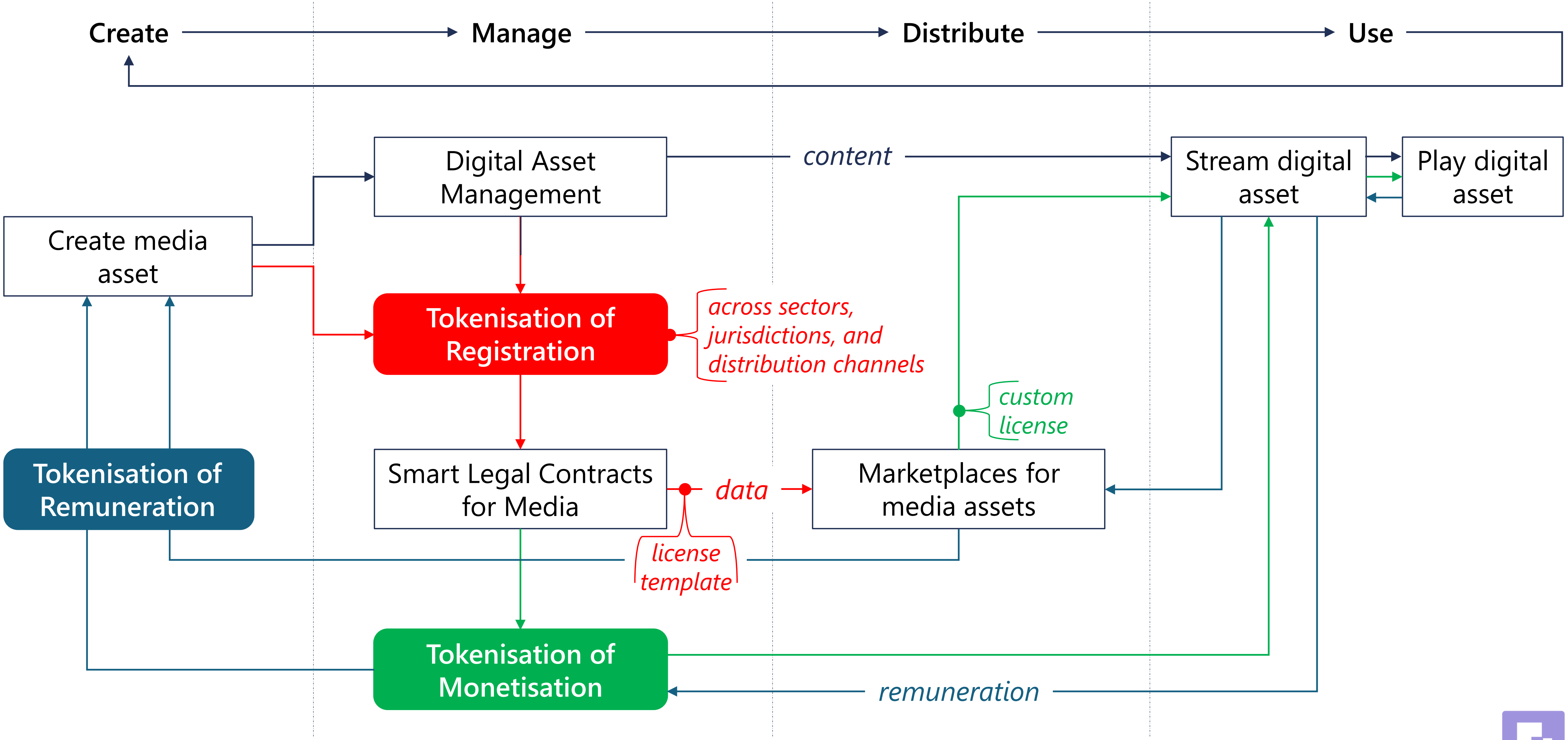
- Embedding and referencing
- Secure and bilateral linkage between metadata and media content

Identification of assets and actors:

- Perceptual hashes and visual media descriptors provide a solution to challenges in both NFT and Fake Media

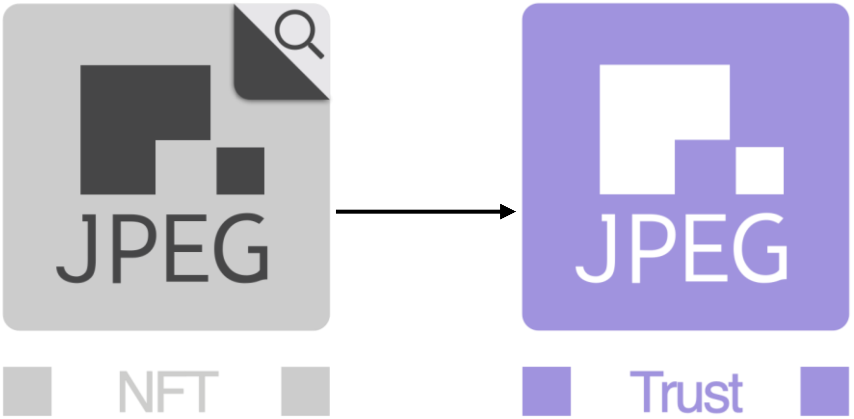
Use cases -> requirements -> call for proposals

UCL proposal: standardization of media tokenization



Create
Manage
Distribute
Use
Digital Asset Management
content
Stream digital asset
Play digital asset
Create media asset
Tokenisation of Registration
across sectors, jurisdictions, and distribution channels
custom license
Tokenisation of Remuneration
Smart Legal Contracts for Media
data
Marketplaces for media assets
license template
Tokenisation of Monetisation
remuneration

From exploration to international standard



The challenges to achieve interoperability in **media tokenization** will be addressed in JPEG Trust.

JPEG Trust contemplates a multi-layered model of media tokenization based on JPEG Trust **Core Foundation** of asset provenance and authenticity.

The first step is to extend support for **authorship** and **ownership** declarations.

Standardization of media tokenization – Layers

Layer		Protocol	Proposer
Remuneration layers	11 Trading		
	10 Remuneration		
	9 Royalty collection		
	8 Content delivery	OSI model	
Monetisation layers	7 Rights Smart Contract		
	6 Smart Legal Contract (executable)		
	5 Legal agreement (negotiated)		
Declaration layers	4 Smart terms of use (non-negotiated)	JPEG Trust / Media Tokenization	UCL
	3 Ownership	JPEG Trust / Media Tokenization	UCL
	2 Authorship	JPEG Trust / Media Tokenization	UCL
	1 Creation & Declaration	JPEG Trust / Core Foundation	C2PA

Contacts and more information

Key contacts

- Frederik Temmermans, frederik.temmermans@vub.be
- Sabrina Caldwell, sabrina.caldwell@anu.edu.au
- Philippe Rixhon, philippe@rixhon.net
- Touradj Ebrahimi, touradj.ebrahimi@epfl.ch

JPEG Trust information and documentation

- https://jpeg.org/jpegtrust